

VMware AirWatch BlackBerry Platform Guide

Deploying and managing BlackBerry devices

AirWatch v8.4 and higher

Have documentation feedback? Submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

Copyright © 2016 VMware, Inc. All rights reserved. This product is protected by copyright and intellectual property laws in the United States and other countries as well as by international treaties. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Revision Table

The following table displays revisions to this guide since the release of AirWatch v8.4 and higher.

Date	Reason
March 2018	Initial upload.

Table of Contents

Chapter 1: Overview	5
Introduction to BlackBerry 10 and Legacy BlackBerry	6
In this Guide	6
Getting Started	9
Chapter 2: BES 10 Server Integration	10
Overview	11
AirWatch Integration Requirements	11
BES Integration Requirements	11
Connecting AirWatch to the BES 10 Server	11
Testing the Connection to the BES 10 Server	13
Using the MEM Feature for BlackBerry 10 Devices	13
Chapter 3: BlackBerry 10 Device Enrollment	14
Overview	15
AirWatch Autodiscovery Enrollment	15
Configure Autodiscovery Enrollment From a Parent Organization Group	15
Configure Autodiscovery Enrollment From a Child Organization Group	15
Enrolling Using the AirWatch BlackBerry 10 Agent	16
Staging a BlackBerry 10 Device	16
Post Enrollment for BlackBerry 10 Devices	16
BlackBerry 10 AirWatch Agent	17
Chapter 4: Device Profiles	19
Overview	20
Deploying Passcode BlackBerry 10 Payloads	20
Legacy BES Server Integration	20
AirWatch Integration Requirements	21
Connecting AirWatch to the Legacy BES Server	21
Testing the Connection to the Legacy BES Server	22
Chapter 5: AirWatch Agent for BlackBerry Legacy Devices	23

Overview	24
Enrolling Legacy BlackBerry Devices Using the Web	24
Configuring the AirWatch Legacy BlackBerry Agent	24
Using the AirWatch Legacy BlackBerry Agent	25
Communicating with Legacy BlackBerry through the Secure Channel	27
Chapter 6: Legacy Device Profiles	28
Overview	29
Deploying Legacy BlackBerry Device Payloads	29
Deploying Legacy BlackBerry Telecom Payloads	29
Deploying Legacy BlackBerry Advanced Payloads	30
Deploying Custom Settings Legacy BlackBerry Payloads	31
Chapter 7: Managing All BlackBerry Devices	32
Overview	33
Registration of BlackBerry 10 and Legacy BlackBerry Devices	33
Device Dashboard	34
Device List View	35
Using the Device Details Page	35
Migrating to New Platforms	37
Appendix: Appendix – BES Configuration	39
Overview	39
Adjusting the BES Integration Task	39
User and Device Privileges	40

Chapter 1:

Overview

Introduction to BlackBerry 10 and Legacy BlackBerry6

In this Guide 6

Getting Started 9

Introduction to BlackBerry 10 and Legacy BlackBerry

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 Console, configure devices and outlines the deployment of AirWatch profiles for BlackBerry 10 devices. It also explains functions that the AirWatch 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 and GPS locations, 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 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, such as GPS location and call and text history 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 Console. It also discusses the deployment of AirWatch profiles for these devices along with managing these devices in the AirWatch 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 VMware Enterprise Systems Connector in a SaaS environment.
- [BlackBerry 10 Device Enrollment](#) – Explains the enrollment process needed to establish initial communications with AirWatch.

- [AirWatch Agent for BlackBerry 10 Devices](#) – Explains the process of configuring and using AirWatch Agent for BlackBerry 10 devices.
- [Device Profiles for BlackBerry 10](#) – Explores the AirWatch 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 Console features, such as enabling services for the agent, deploying profiles and credentials, controlling profile time schedules, etc.
- [Managing All BlackBerry Devices](#) – Provides AirWatch 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-premises AirWatch deployments and how to adjust synchronization between the BES and AirWatch.

Platforms and Devices Supported

BlackBerry 10

AirWatch v8.1 supports the use of all BlackBerry devices.

Legacy BlackBerry

AirWatch v8.1 supports the use of all BlackBerry devices.

Agents and Versions Supported

BlackBerry 10

We always recommend using the latest version of agent posted on BlackBerry AppWorld. AirWatch v8.1 requires a minimum agent version of 1.2.

Legacy BlackBerry

We always recommend using 6.5 version agent for AirWatch v8.1.

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 Console.

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

Getting Started

Before you begin, AirWatch recommends that 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.

- If you are not running AirWatch in a SaaS environment, consider the benefits of upgrading it to the latest version.
- 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 Console.

Chapter 2:

BES 10 Server Integration

Overview	11
AirWatch Integration Requirements	11
BES Integration Requirements	11
Connecting AirWatch to the BES 10 Server	11
Testing the Connection to the BES 10 Server	13
Using the MEM Feature for BlackBerry 10 Devices	13

Overview

AirWatch can integrate with the BES 10 either in an on-premises environment or in a software as a service (SaaS) environment. In a SaaS deployment, BES integration requires the use of the VMware Enterprise Systems Connector. 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.

AirWatch Integration Requirements

To configure communication between the BES 10 and the AirWatch 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 Console and the BES 10 server:

1. Navigate to **Groups & Settings > All Settings > Device & Users > BlackBerry > BlackBerry 10 > BES 10 Settings**.
2. Enter the following settings:

Setting	Description
BES 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 10 server. The URL format is <i>https://<BES_URL>:38443</i> .

Setting	Description
BES Admin Username / Password	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.
Authentication Method	Ensure that the Authentication Method field is set to Active Directory or BlackBerry Administration Service .
Domain	Enter a domain for the BES 10 server in the Domain field.
Ignore SSL Errors	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.
BES Sync Batch Size	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 Console to the device.
Activation Code Expiration	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.
Message Type	Select either the Email or SMS radio button to determine the method used to deliver the BES Registration Message .
BES Registration Message	Select from the BES Registration Message drop-down a message the end user receives upon registration.

3. Select **Save**.

Testing the Connection to the BES 10 Server

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

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

Note: For more information about performing BES integration tasks, see the [Appendix: BES Configuration](#).

3. Select **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 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 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 **VMware AirWatch MEM Guide**.

Chapter 3:

BlackBerry 10 Device Enrollment

Overview	15
AirWatch Autodiscovery Enrollment	15
Configure Autodiscovery Enrollment From a Parent Organization Group	15
Configure Autodiscovery Enrollment From a Child Organization Group	15
Enrolling Using the AirWatch BlackBerry 10 Agent	16
Staging a BlackBerry 10 Device	16
Post Enrollment for BlackBerry 10 Devices	16
BlackBerry 10 AirWatch Agent	17

Overview

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

AirWatch Autodiscovery Enrollment

AirWatch makes the enrollment process simple, using an autodiscovery system to enroll devices to environments and organization groups (OG) using user email addresses.

Registration for Autodiscovery Enrollment

The server checks for an email domain uniqueness, only allowing a domain to be registered at one organization group in one environment. Because of this server check, register your domain at your highest-level organization group.

Autodiscovery is configured automatically for new Software as a Service (SaaS) customers.

Configure Autodiscovery Enrollment From a Parent Organization Group

Autodiscovery Enrollment simplifies the enrollment process enrolling devices to intended environments and organization groups (OG) using end-user email addresses.

Configure an autodiscovery enrollment from a parent OG by taking the following steps.

1. Navigate to **Groups & Settings > All Settings > Admin > Cloud Services** and enable the **Auto Discovery** setting. Enter your login email address in **Auto Discovery AirWatch ID** and select **Set Identity**.
 - a. If necessary, navigate to <https://my.air-watch.com/set-discovery-password> to set your myAirWatch password for Auto Discovery service. Once you have registered and selected **Set Identity**, the **HMAC Token** autopopulates. Click **Test Connection** to ensure that the connection is functional.
2. Enable the **Auto Discovery Certificate Pinning** option to upload your own certificate and pin it to the auto discovery function.

You can review the validity dates and other information for existing certificates, where you also have the option to **Replace** and **Clear** these existing certificates.

Select **Add a certificate** and the settings **Name** and **Certificate** display. Enter the name of the certificate you want to upload, select the **Upload** button, and choose the cert located on your device.
3. Select **Save** to complete an autodiscovery setup.

Instruct end users who enroll themselves to select the email address option for authentication, instead of entering an environment URL and Group ID. When users enroll devices with an email address, they enroll into the same group listed in the **Enrollment Organization Group** of the associated AirWatch user account.

Configure Autodiscovery Enrollment From a Child Organization Group

You can configure Autodiscovery Enrollment from a child organization group below the enrollment organization group. To enable an autodiscovery enrollment in this way, you must require users to select a Group ID during enrollment.

1. Navigate to **Devices > Device Settings > General > Enrollment** and select the **Grouping** tab.
2. Select **Prompt User to Select Group ID**.
3. Select **Save**.

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 select **Next**.
3. Enter your user name and password credentials supplied by your AirWatch admin and then select **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 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**. If you enable single staging, you can enroll using advanced staging option (enroll device on behalf of another user).

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 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 using 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 through email or SMS depends on the configuration in the AirWatch 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

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

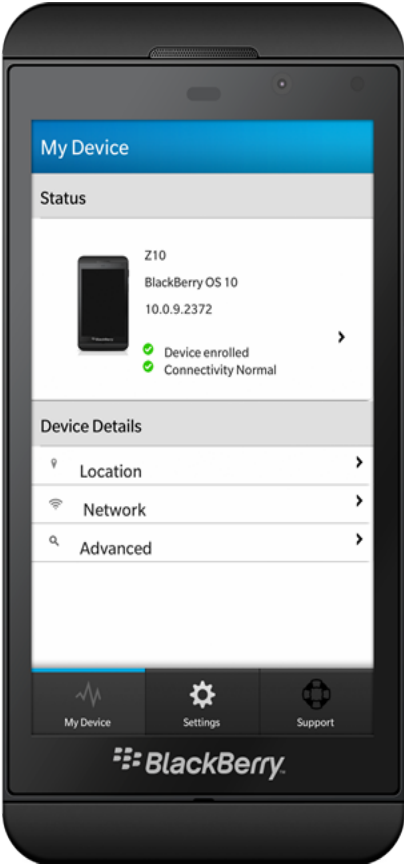
Configure the AirWatch Agent so that devices can communicate and enroll with it. Find configurations in the AirWatch Console **Groups & Settings > All Settings > Devices & Users > BlackBerry > BlackBerry 10**.

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

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	<p>View current MDM details for the device, including:</p> <ul style="list-style-type: none"> • Enrollment – View the enrollment status of the device. • Connection Status – View the connection status between the AirWatch Agent and the AirWatch 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	<p>View information about the AirWatch Agent, including:</p> <ul style="list-style-type: none"> • 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 .	

Chapter 4:

Device Profiles

Overview	20
Deploying Passcode BlackBerry 10 Payloads	20
Legacy BES Server Integration	20
AirWatch Integration Requirements	21
Connecting AirWatch to the Legacy BES Server	21
Testing the Connection to the Legacy BES Server	22

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.

ActiveSync is used to push down profiles to users. If you have multiple users who are using multiple OSs (for example BlackBerry 10, Android and iOS), all devices will receive the profile you push down. If a non-BlackBerry device is already being managed by a policy, conflicts could arise if the user is already assigned a policy 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.

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 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 the profile's **General** settings.
These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).
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

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 Console.

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

AirWatch Integration Requirements

To configure communication between the BES and the AirWatch 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 Console and the BES:

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

Setting	Description
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 <i>https://<BES_URL>/enterprise/admin/ws</i> .
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 <i>https://<BES_URL>/enterprise/admin/util/ws</i> .
BES Locale	Enter the country location of the BES. For example, en_US.
Authentication Method	Ensure that the Authentication Method field is set to Active Directory .
BES Username and Password	Enter the username and password needed to authenticate with the BES in the BES Username field and the BES Password field.
Domain	Enter a domain for the BES in the Domain field.

Setting	Description
Organization ID	Enter the applicable ID associated with the BES in the Organization ID field. This entry is typically 0 .
Sync Applications	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-premises environments. These settings are not visible in the AirWatch Console for SaaS environments unless you also have the VMware Enterprise Systems Connector.

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

Note: For more information about performing BES integration tasks, see the [Appendix – BES Configuration](#).

Chapter 5:

AirWatch Agent for BlackBerry Legacy Devices

Overview	24
Enrolling Legacy BlackBerry Devices Using the Web	24
Configuring the AirWatch Legacy BlackBerry Agent	24
Using the AirWatch Legacy BlackBerry Agent	25
Communicating with Legacy BlackBerry through the Secure Channel	27

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 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 select **Next**.
3. Enter your AirWatch user credentials and select **Enroll**.
4. Enter your email username and password so that this information appears in the Device Dashboard in the AirWatch 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. Select **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. Select **Download** and select **Yes** on the **AirWatch Agent Trusted Application status** screen.
9. Select **Save**, and select **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 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 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 Console:

Setting	Description
Heartbeat Interval	Set the time (in minutes) the agent waits before checking in with the AirWatch Console.
Data Sample Interval	Set the time (in minutes) the agent waits to collect data from the device.
Profile Refresh Interval	Set the frequency (in minutes) the profile list of each device will be refreshed on the server.
Collect Location Data	Set the AirWatch Agent to send GPS data to the AirWatch Console.
GPS Sample Interval	Set the interval at which the AirWatch Agent collects sample GPS data for the device.
Administrative Passcode	Set 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: <ul style="list-style-type: none"> ◦ 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	<p>View information about the device.</p> <ul style="list-style-type: none"> • General – View information on battery life and available memory. • Device Details – View information about location, network, and telecom data. <ul style="list-style-type: none"> ◦ 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	<p>Configure and view MDM settings on the device. You must have the Admin passcode to view and configure these options.</p> <ul style="list-style-type: none"> • Server – See the AirWatch Server URL that connects to the device. • Heartbeat – Configure and view information about synchronization. <ul style="list-style-type: none"> ◦ Transmission Frequency – Set the transmission interval of data to the AirWatch Console. ◦ Last Heartbeat Attempt – View the date and time of the last heartbeat sent to the AirWatch Console. ◦ Last Heartbeat Result – View the success or failure of the last heartbeat sent to the AirWatch Console. • Data Sampling – Configure and view information about data sampling. <ul style="list-style-type: none"> ◦ Host Port – Configure the port number to send data to the AirWatch Console. ◦ Transmission Frequency – Set the transmission interval to send data samples to the AirWatch 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 Console. ◦ Last Data Sampling Result – View the success or failure of the last data sample sent to the AirWatch Console. • Profile Refresh, Profile Refresh Interval – Set the interval to refresh the profile requests sent to the AirWatch Console. • Logging, Log Level – Send a log request to the AirWatch Console.

Option	Description
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 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** checkbox and select **Save**.

Chapter 6:

Legacy Device Profiles

- Overview 29
- Deploying Legacy BlackBerry Device Payloads29
- Deploying Legacy BlackBerry Telecom Payloads 29
- Deploying Legacy BlackBerry Advanced Payloads30
- Deploying Custom Settings Legacy BlackBerry Payloads31

Overview

This section talks about configuring general profile settings, deploying legacy blackberry device, telecom, and advanced payloads. There is also a section that talks about deploying custom settings legacy blackberry payloads.

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 the profile's **General** settings.
These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).
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 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 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** and then select **BlackBerry**.
2. Configure the profile's **General** settings.
These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).
3. Select the **Telecom** profile.

4. 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 AirWatch 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 AirWatch Console. Consider the battery life of the device when setting this option.
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 the profile's **General** settings.
These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on [AirWatch Resources](#).
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 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 Console. The AirWatch Console packages and pushes this custom XML profile to BlackBerry devices.

Chapter 7:

Managing All BlackBerry Devices

Overview	33
Registration of BlackBerry 10 and Legacy BlackBerry Devices	33
Device Dashboard	34
Device List View	35
Using the Device Details Page	35
Migrating to New Platforms	37

Overview

After your devices are enrolled and configured, manage the devices using the AirWatch Console. The management tools and functions enable you to keep an eye on your devices and remotely perform administrative functions.

You can manage all your devices from the VMware AirWatch Dashboard. The Dashboard is a searchable, customizable view that you can use to filter and find specific devices. This feature makes it easier to perform administrative functions on a particular set of devices. The Device List View displays all the devices currently enrolled in your AirWatch environment and their status. The Device Details page provides device-specific information such as profiles, apps, AirWatch Agent version and which version of any applicable OEM service currently installed on the device. You can also perform remote actions on the device from the Device Details page that are platform-specific.

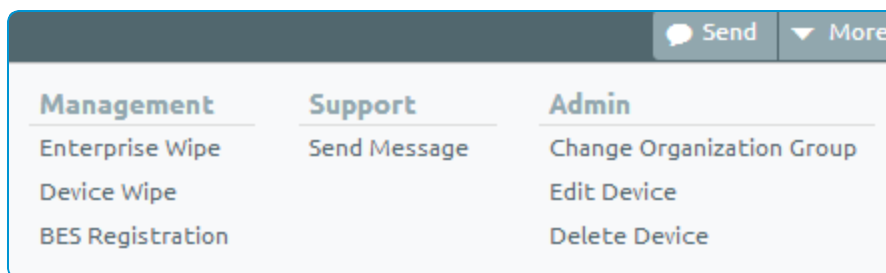
Registration of BlackBerry 10 and Legacy BlackBerry Devices

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 Agent. For Legacy BlackBerry devices, the AirWatch Admin can initiate BES registration from the AirWatch 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 Console
2. Search in the **Filter Grid** for BlackBerry devices.
3. Select the **Friendly Name** of the desired device. The details for that device displays.
4. Select the **More** drop-down in the upper right.
5. Select **BES Registration** from the drop-down window and follow the prompts.



Registration of Legacy BlackBerry Devices

1. Navigate to **Devices > List View > ADD DEVICE** in the AirWatch 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. Select 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 **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 using email or SMS.

Note: You can review the message that will be sent to the device user by selecting the **Message Preview** button.

12. Select **Save**.

Device Dashboard

As devices are enrolled, you can manage them from the AirWatch **Device Dashboard**. The **Device Dashboard** provides a high-level view of your entire fleet and allows you to act on individual devices quickly.

You can view graphical representations of relevant device information for your fleet, such as device ownership type, compliance statistics, and platform and OS breakdowns. You can access each set of devices in the presented categories by selecting any of the available data views from the **Device Dashboard**.

From the **List View**, you can take administrative action: send messages, lock devices, delete devices, and change groups associated with the device.

Device List View

Select **Devices > List View** to see a full listing of all devices.

The **Last Seen** column displays an indicator showing the number of minutes elapsed since the device has checked-in.

Select a device in the **General Info** column at any time to open the details page for that device.

Sort by columns and configure information filters to review device activity based on specific information. For example, sort by the **Compliance Status** column to view only devices that are currently out-of-compliance and target only those devices. Search all devices for a friendly name or user name to isolate one device or user.

Customize Device List View Layout

Display the full listing of visible columns in the **Device List** view by selecting the **Layout** button and choose the **Custom** option. This view enables you to display or hide Device List columns per your preferences.

There is also an option to apply your customized column view to all administrators. For instance, you can hide 'Asset Number' from the **Device List**.

Once all your customizations are complete, select the **Accept** button to save your column preferences and apply this new column view. You may return to the **Layout** button settings at any time to tweak your column display preferences.

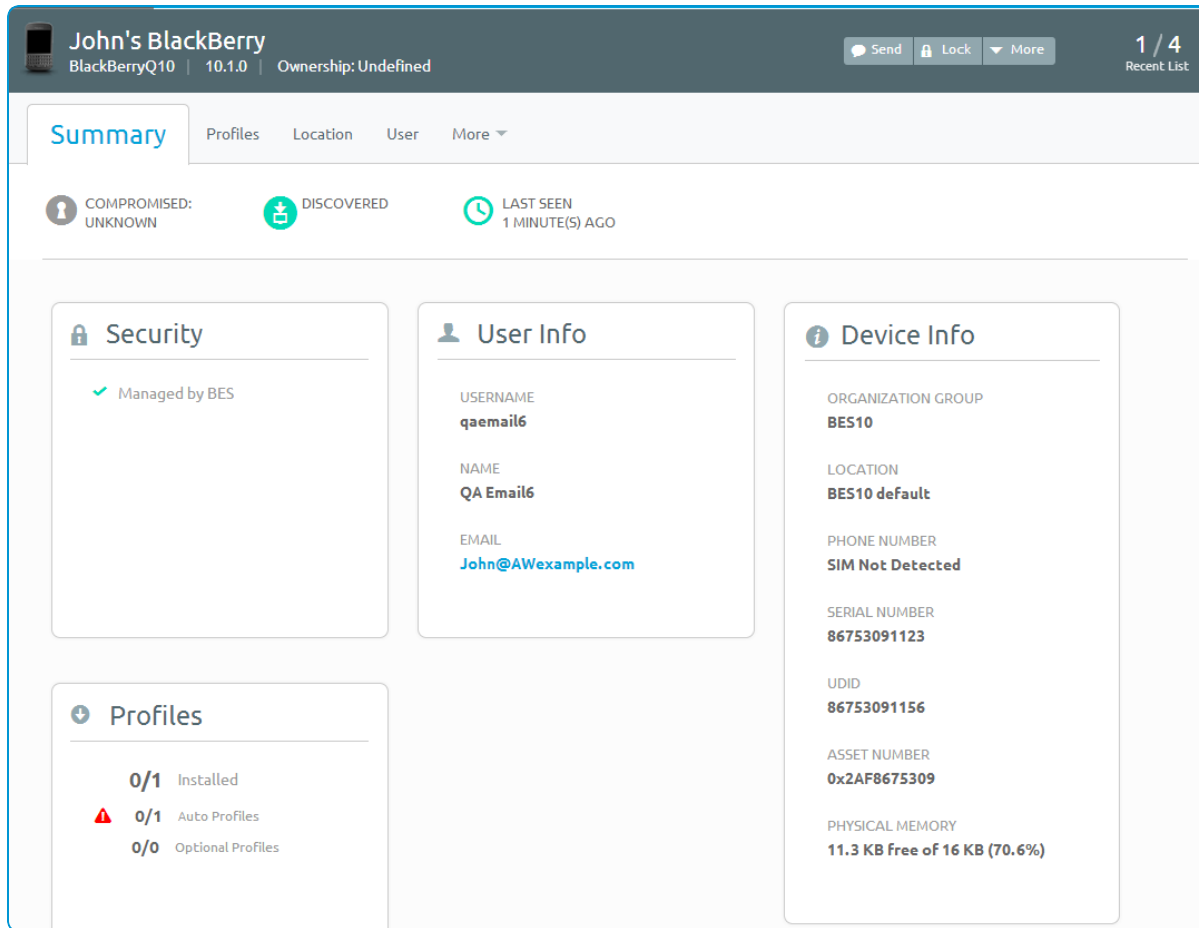
Search in Device List View

You can search for a single device for quick access to its information and take remote action on the device.

To run a search, navigate to **Devices > List View**, select the **Search List** bar and enter a user name, device friendly name, or other device-identifying element. This action initiates a search across all devices, using your search parameter.

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 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** – Selecting **More** 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.

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

Device Action Descriptions

- **Add Tag** – Assign a customizable Tag to a device, which can be used to identify a special device in your fleet.

- **BES Registration** – Register your BlackBerry device using this remote command and allow BES to manage the device instead of MDM. Applies only to BlackBerry 10 devices.
- **Change Organization Group** – Change the device's home organization group to another pre-existing OG. Includes an option to select a static or dynamic OG.
- **Change Ownership** – Change the Ownership setting for a device, where applicable. Choices include Corporate-Dedicated, Corporate-Shared, Employee Owned and Undefined.
- **Delete Device** – Delete and unenroll a device from the Admin Console. This action does not remove any data from the device itself, only its representation in the console.
- **Device Wipe** – Wipe a device clear of all data, including email, profiles and MDM capabilities and the device returns to a factory default state. This includes all personal user information if applicable. This action cannot be undone.
- **Edit Device** – Edit device information such as **Friendly Name**, **Asset Number**, **Device Ownership**, **Device Group** and **Device Category**.
- **Enterprise Reset** – Enterprise Reset a device to factory settings, keeping only the VMware AirWatch enrollment.
- **Enterprise Wipe** – Enterprise Wipe a device to unenroll and remove all managed enterprise resources including applications and profiles. This action cannot be undone and re-enrollment will be required for VMware AirWatch to manage this device again. Includes options to prevent future re-enrollment and a **Note Description** field for you to add any noteworthy details about the action.
 - Enterprise Wipe is not supported for cloud domain-joined devices.
- **Location** – Reveal a device's location by showing it on a map using its GPS capability.
- **Lock Device** – Lock the screen of a selected device, rendering it unusable until it is unlocked. Includes optional fields for a custom **Message**, **Phone Number**, and **Note Description**.
- **Send Message** – Send a message to the user of the selected device. Choose between **Email**, **Push Notification** and **SMS**.

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 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 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 using 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 Console, and it begins to periodically send asset information back to the AirWatch 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:

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.

Adjusting the BES Integration Task

If you have an on-premises 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 select **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 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	