Introduction to the Symbian Platform Guide

Overview

AirWatch provides complete mobility management solutions for Symbian enterprise deployments. The AirWatch Mobile Device Management (MDM) solution enables companies to manage corporate, employee-owned (BYOD), or shared Symbian devices throughout the entire mobile lifecycle. AirWatch also supports the AirWatch Cloud Messaging (AWCM) service for the Symbian platform, allowing administrators to push down messages or notifications to devices from the AirWatch Admin Console.

In this Guide

- **Before you Begin** – This section covers the basic requirements and other topics that would help you get started with the solution.
- **Symbian Device Enrollment** – Explains how to enroll Symbian devices into the AirWatch Admin Console.
- **Symbian Device Profiles** – Explores the AirWatch Admin Console features, such as enabling services for the agent, deploying profiles and credentials, controlling profile time schedules, etc.
- **MDM Agent for Symbian** – Learn more about how the AirWatch Agent is used to secure devices and how to configure its settings for Symbian devices.
- **Managing Symbian Devices** – Explains how easily devices can be managed from the AirWatch Admin Console.
- **Keep in Mind** – Lists out few exceptions and points that would help you to manage devices effectively.

Supported Platforms

AirWatch supports the following Symbian platforms and operating system (OS) versions:

- Symbian S60 3rd Edition, OS 9.3, FP1 and FP2
  
  **Note:** S60 3rd edition FP1 only supports the following features; Asset tracking and MDM commands (such as Device Lock, Device Wipe, Passcode Reset, and Enterprise Wipe).

- Symbian S60 5th Edition, OS 9.4

- Symbian ^3 Anna, OS 9.5

- Nokia Belle, OS 10.1
  
  **Note:** Nokia Belle OS 10.1 FP1 and FP2 are not supported.
## Supported Devices

The AirWatch Agent is known to work with the following devices.

<table>
<thead>
<tr>
<th>Model</th>
<th>Edition</th>
<th>OS</th>
<th>Firmware</th>
</tr>
</thead>
<tbody>
<tr>
<td>E71</td>
<td>Symbian S60 3rd Edition, FP1</td>
<td>9.2</td>
<td>300.21.012</td>
</tr>
<tr>
<td>E5</td>
<td>Symbian S60 3rd Edition, FP2</td>
<td>9.3</td>
<td>071.003</td>
</tr>
<tr>
<td>E72</td>
<td>Symbian S60 3rd Edition, FP2</td>
<td>9.3</td>
<td>081.001</td>
</tr>
<tr>
<td>C6</td>
<td>Symbian S60 5th Edition</td>
<td>9.4</td>
<td>41.0.01</td>
</tr>
<tr>
<td>5800 Xpress music</td>
<td>Symbian S60 5th Edition</td>
<td>9.4</td>
<td>60.0.003</td>
</tr>
<tr>
<td>C7</td>
<td>Symbian ^3 Anna</td>
<td>9.5</td>
<td>022.014</td>
</tr>
<tr>
<td>N8</td>
<td>Nokia Belle</td>
<td>9.5</td>
<td>025.008</td>
</tr>
<tr>
<td>E6</td>
<td>Symbian ^3 Anna</td>
<td>9.5</td>
<td>026.001</td>
</tr>
<tr>
<td>N8</td>
<td>Symbian ^3</td>
<td>9.5</td>
<td>014.002</td>
</tr>
<tr>
<td>701</td>
<td>Nokia Belle*</td>
<td>10.1</td>
<td>111.030.0609</td>
</tr>
</tbody>
</table>

*Nokia Belle FP1 and FP2 are not supported*
Before You Begin

Overview

The Before you Begin topic provides the information that helps you with the initial setup, configuration, and understanding of the requirements essential for a smooth user experience.

In this Section

- **Supported Platforms** - Lists out the Symbian platforms that are supported by AirWatch
- **Supported Devices** - Lists out the Symbian devices that are supported by AirWatch.
- **Pre-requisites** - Lists out the prerequisites to enroll a Symbian device via the web-based process.
- **Recommended Reading** - The list of documents that would help you get a comprehensive understanding of the solution.

Supported Platforms

AirWatch supports the following Symbian platforms and operating system (OS) versions:

- Symbian S60 3rd Edition, OS 9.3, FP1 and FP2

  **Note:** S60 3rd edition FP1 only supports the following features; Asset tracking and MDM commands (such as Device Lock, Device Wipe, Passcode Reset, and Enterprise Wipe).

- Symbian S60 5th Edition, OS 9.4
- Symbian ^3 Anna, OS 9.5
- Nokia Belle, OS 10.1

  **Note:** Nokia Belle OS 10.1 FP1 and FP2 are not supported.

Supported Devices

The AirWatch Agent is known to work with the following devices.

<table>
<thead>
<tr>
<th>Model</th>
<th>Edition</th>
<th>OS</th>
<th>Firmware</th>
</tr>
</thead>
<tbody>
<tr>
<td>E71</td>
<td>Symbian S60 3rd Edition, FP1</td>
<td>9.2</td>
<td>300.21.012</td>
</tr>
<tr>
<td>E5</td>
<td>Symbian S60 3rd Edition, FP2</td>
<td>9.3</td>
<td>071.003</td>
</tr>
<tr>
<td>E72</td>
<td>Symbian S60 3rd Edition</td>
<td>9.3</td>
<td>081.001</td>
</tr>
<tr>
<td>Model</td>
<td>Edition</td>
<td>OS</td>
<td>Firmware</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------------------</td>
<td>-----</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td>Edition, FP2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C6</td>
<td>Symbian S60 5th Edition</td>
<td>9.4</td>
<td>41.0.01</td>
</tr>
<tr>
<td>5800 Xpress music</td>
<td>Symbian S60 5th Edition</td>
<td>9.4</td>
<td>60.0.003</td>
</tr>
<tr>
<td>C7</td>
<td>Symbian ^3 Anna</td>
<td>9.5</td>
<td>022.014</td>
</tr>
<tr>
<td>N8</td>
<td>Nokia Belle</td>
<td>9.5</td>
<td>025.008</td>
</tr>
<tr>
<td>E6</td>
<td>Symbian ^3 Anna</td>
<td>9.5</td>
<td>026.001</td>
</tr>
<tr>
<td>N8</td>
<td>Symbian ^3</td>
<td>9.5</td>
<td>014.002</td>
</tr>
<tr>
<td>701</td>
<td>Nokia Belle*</td>
<td>10.1</td>
<td>111.030.0609</td>
</tr>
</tbody>
</table>

*Nokia Belle FP1 and FP2 are not supported

**Prerequisites**

- **URL** – This URL is specific to your organization and brings you to the enrollment screen.
- **Group ID** – The Group ID associates your device with your corporate role and is defined in the AirWatch Admin Console.
- **User Credentials** – The username and password allows you to access the AirWatch environment. These can be the same as the network directory services credentials or your administrator can define new credentials for you in the console.

**Recommended Reading**

Symbian Device Enrollment

Overview

In order for Symbian devices to communicate with the AirWatch Admin Console, you or the end user must install an agent. This agent facilitates the communication between the device and the AirWatch Admin Console. This process of downloading and installing the agent and creating the communication between the device and AirWatch is called Enrollment. Enrollment enables you to control, manage, and monitor devices.

You can enroll a Symbian device using a web-based process. To ensure this process happens smoothly, several settings are configured in the AirWatch Admin Console. For more information, see Configuring Symbian Agent Settings.

In this Section

- **Prerequisites** - This section lists out the requirements that are essential before enrolling a device.
- **Steps to Enroll** - Explains the step-by-step process required to enroll a Symbian device into the AirWatch Admin Console.

Prerequisites

To enroll a Symbian device via the web-based process, the below information is required:

- **URL** – This URL is specific to your organization and brings you to the enrollment screen.
- **Group ID** – The Group ID associates your device with your corporate role and is defined in the AirWatch Admin Console.
- **User Credentials** – The username and password allows you to access the AirWatch environment. These can be the same as the network directory services credentials or your administrator can define new credentials for you in the console.

Steps to Enroll

Follow these steps in order to make a Symbian device available for remote management through the AirWatch MDM application:

1. Verify you received the URL, Group ID, and credentials. See Prerequisites mentioned in the above section.
2. Authenticate your corporate identity:
   - Enter the enrollment URL provided by your administrator.
   - Enter your **Group ID** and then, select **Next**.
   - Enter your **User Name** and **Password** in the fields provided and then, select **Next**.
• The End User License Agreement screen displays. Select Accept.

**Note:** The End User License Agreement (EULA) and Device Ownership screen appears only if it is enabled for your location group by your administrator.

3. Download and install the AirWatch Agent to complete the Enrollment process.
   • After authenticating with your credentials, the **Download** screen displays. Select **Ok** to begin downloading the agent. After selecting the agent to download, the **Download Details** screen displays.

   ![Download Screen](image1)

   After the agent downloads onto your device, the **Install** screen displays.

4. Select **Ok** to confirm that you want to install the AirWatch Agent. An **Install** screen displays asking you to select where you want to install the AirWatch application. You can select the Phone memory, Mass memory, or the Memory card.
**Note:** Please note that by default the configuration files are saved in the phone memory (this is the recommended location).

**Note:** After the above step, Nokia Smart Installer screen appears only for Symbian S60 3rd Edition and Symbian S60 5th Edition, select **OK** to proceed to the next step.

The AirWatch Agent proceeds with the installation on your device. When finished, a screen appears informing you about the AirWatch Agent capability.

5. Select **OK** to proceed.
6. If the screen prompts you to launch AirWatch, select No and then tap Continue.

**Note:** If you choose Yes, you get the following screen which displays ‘Enrollment is not complete. Please tap Continue button on the browser to finish enrollment. Pressing OK will close the application.’ Select OK to go back to the browser and then select Continue.

The Installation Complete screen displays and enrollment begins. The Enrollment in Progress bar indicates the status of the enrollment on your device.
The message **Enrollment Success** displays on the screen.

7. **Select OK.**
   - If no SIM card is installed on the device and if the SIM card does not have the capability of sending a phone number to the AirWatch Admin Console server, the phone number box appears in the next screen. Enter your phone number to launch the AirWatch Agent on the device.

Enrollment is complete. The Symbian device is now available for remote management through the AirWatch application.
**Note:** If you are facing any issues with the enrollment, you are advised to restart your device.
Device Profiles

Overview

Once Symbian devices are enrolled in the AirWatch system, you can push security profiles on them. Profile policies ensure the Symbian devices follow a defined set of rules as mentioned in the Admin Console. These profiles provide the flexibility to manage devices as per requirements. For example, you may want to set a very complex password on devices carrying sensitive information as compared to others. You can configure the passcode policy profile with complex passcode settings and push these settings onto the required devices. Supported and non supported profiles can be viewed on the device from the Installed Profiles tab.

In this Section

- **Configuring Profile General Settings** — Each profile has General settings you must configure. This section explains the options and settings you can configure as part of the General tab.

- **Deploying a Passcode Payload** — Covers the multiple fields and levels of complexity for a passcode policy in the AirWatch Admin Console.

- **Deploying a Corporate Wi-Fi** — Details the steps required to push Wi-Fi settings to devices.

- **Deploying Corporate VPN** — Details deploying corporate VPN settings directly to managed devices so end users can remotely and securely access corporate infrastructure.

- **Deploying an Exchange Active Sync** — Creates an Exchange ActiveSync profile to allow the end user to access corporate email infrastructures from the device.

- **Deploying Certificates** — Covers certificate-based authentication for Symbian devices and the configuration options available in the AirWatch Admin Console.

- **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:
     o **Managed** – The profile is removed.
     o **Manual** – The profile remains installed until removed by the end user.
   • **Assignment Type** – Determines how the profile is deployed to devices:
     o **Auto** – The profile is deployed to all devices automatically.
     o **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.
     o **Interactive** – This is a unique assignment type in which the profile integrates with third-party systems to deploy a specific payload to a device.
     o **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:
     o **Always** – The end user can manually remove the profile at any time.
     o **With Authorization** – The end user can remove the profile with the authorization of the administrator.
     o **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:
     o **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 a Passcode Policy**

Deploying Passcode profiles enables you to configure different passcode policies on different devices based on the corporate requirements. For example, you may require complex passcodes for corporate devices as compared to employee owned device passcodes. Configure the Passcode profile and push these settings on these devices.

   **Note:** Passcode policy is supported on Symbian S60 5th Edition, 3rd Edition, Anna, and Belle but not on Symbian ^3 devices (PR1.1 and PR1.2).

To enforce a Passcode profile, follow the steps detailed below:

1. Navigate to Devices ►Profiles ►List View and select Add and then select Symbian.

2. Configure General settings for the profile.

3. Select the Passcode profile.

4. Configure the Passcode settings, including:

   - **Complexity** – Allow simple values for quick access or require alphanumeric passcodes for security. You can also require X number of complex characters (@, #, &, !, ? and so on) in the passcode. You can also set the maximum and minimum length of the passcodes. For example, users with access to extremely sensitive content can be required to use more stringent passcodes.

   - **Maximum Number of Failed Attempts** – Prevent unauthorized access by blocking access after the set number of attempts. This helps prevent illegitimate users from attempting to repeatedly access content for which they do not have permission. For example, if set to 11, then if a user were to enter a wrong passcode eleven times in a row the device will automatically perform a full device wipe. If set to None, the Erase Data option is turned off, and after six failed attempts the device will be disabled for some time.

   - **Maximum Passcode Age** – Enforce renewal of passcodes at selected interval. The Passcodes that are changed more frequently may be less vulnerable to exposure to unauthorized parties. On renewal/expiry, the end user has to create a new passcode for the device (steps to create a new passcode is described below).

   - **Maximum/Minimum Passcode Change Interval** - Set restriction on the number of times a passcode can be changed in the specified time interval.

**To set new passcode on device**

Once you push the Passcode profile onto a device, the device gets locked. The device user has to perform certain steps in order to set a new passcode:
1. Enter the lock code. The lock code expired warning appears.
   • The first step is not required for devices with a disabled Lock Code.
2. The **New lock code** prompt displays. Enter the new lock code and tap **OK**.
3. The **Verify New Lock** code prompt displays. Re-enter the lock code and tap **OK**.
4. The new lock code is now set on the device.

**Note:** If you cross the maximum attempts of entering the correct lock code, the device is reset to default factory settings.

**Note:** After un-enrollment, the device passcode is always reset to 12345.

Some scenarios to keep in mind

- **Scenario 1** - Suppose a passcode policy is not pushed and an Enterprise Wipe (unenrollm) is performed on the device. The passcode does not get reset.
- **Scenario 2** - Suppose a passcode policy is pushed on a device and an Enterprise Wipe is performed on the device. The passcode gets reset to 12345.

## Deploying Corporate Wi-Fi

Wi-Fi profiles push corporate Wi-Fi settings directly to managed (enrolled) devices for instant access to corporate Wi-Fi networks.

To configure a Wi-Fi payload, follow the steps detailed below:

1. Navigate to **Devices ➤ Profiles ➤ List View** and select **Add** and then select **Symbian**.
2. Configure **General settings for the profile**.
3. Select the **Wi-Fi** profile.
4. Configure the Wi-Fi settings, including:
   - **Service Set Identifier** – Configure Wi-Fi profiles, select the appropriate wireless protocols and security settings for the Wi-Fi network.
   - **Proxy** – Establish access to a proxy server.
   - **Multiple Accounts** – Add multiple Wi-Fi accounts within the same Wi-Fi profile by selecting the plus (+) sign.
5. Select **Save & Publish** when you are finished to push the profile to devices.

**Note:** When a Wi-Fi profile is removed from the device, the corresponding access point gets removed regardless if it is connected or not. In such cases, the next priority Wi-Fi access point takes precedence. When pushed back again, it connects automatically. The Access Points priority can be configured on the device.

## Deploying Corporate VPN

VPN profiles push corporate virtual private network settings to corporate devices so that users can securely access corporate infrastructures from remote locations.
To enforce a VPN profile, follow the steps detailed below:

1. Navigate to Devices ►Profiles ►List View and select Add and then select Symbian.
2. Configure General settings for the profile.
3. Select the VPN profile.
4. Configure the VPN settings, including:
   - **VPN Provider** - Select the VPN provider as Cisco Any Connect.
   - **Server** - Enter the hostname or IP address of the server being connected to.
   - **VPN Group** - Enter the group name of the VPN for the user to access.
   - **Username** - Enter the username to access the VPN.
   - **Multiple Accounts** – Add multiple VPN accounts within the same VPN profile by selecting the plus (+) sign.
5. Select Save & Publish when you are finished to push the profile to devices.

**Note:** Deleting a VPN profile from the AirWatch Admin Console removes the profile from the agent, but it does not terminate the connection which is already active unless it is disconnected manually. Please note that the VPN point remains on the VPN Client even after disconnecting.

**Note:** When configuring a VPN connection on the device, the Cisco Any Connect client always takes the first value in the Server drop-down, regardless of what server name has been specified in the profile.

### Deploying an Exchange Active Sync

Exchange Active Sync profile pushes the EAS mail settings directly to managed devices.

To configure Exchange ActiveSync payloads, follow the steps detailed below:

1. Navigate to Devices ►Profiles ►List View and select Add and then select Symbian.
2. Configure General settings for the profile.
3. Select the Exchange ActiveSync profile.
4. Configure the Exchange ActiveSync settings, including:
   - **Exchange ActiveSync Host** - Enter the EAS server address.
   - **Login Information** - Leverage user account info to simplify authentication.
   - **Settings** - Set how many days to sync mail and calendar entries once mail is configured.
   - **Peak Days for Sync Schedule** - Select the preferred day and time when mail should sync, also select whether to allow syncing when roaming.
   - **SSL** - Use SSL to encrypt mail traffic over port 443.
5. Select Save & Publish when you are finished to push the profile to devices.
Deploying Certificates

The Credential profile pushes certificates onto the device and enables encrypted communication between the device and the AirWatch Admin Console. The certificate authority (CA) and certificate template are defined at Devices ► Certificates ► Certificate Authorities and Devices ► Certificates ► Certificate Authorities respectively.

**Note:** Do not change the label of the personal certificates displayed on the device during the installation process.

1. Navigate to Devices ► Profiles ► List View and select Add. Select Symbian.
2. Configure General settings for the profile.
3. Select the Credentials profile.
4. Configure the Credentials settings, including:
   - **Credential Source** – Use the dropdown menu to select either Upload or Defined Certificate Authority.
     **Note:** The remaining payload options are source-dependent. If you select Upload, you must upload a new certificate. If you select Defined Certificate Authority, you must choose a predefined certificate authority and Template.
   - **Credential Source** - Select the Upload or Define Certificate Authority option from the drop-down.
   - **Certificate Authority** - Select the CA from whom the certificate was signed.
   - **Certificate Template** - Select the template of the certificate.
   - **Credential Name** - Enter a name for the certificate. (This option is available only on selecting the Upload option).
   - To Upload, as an administrator, you must have the certificate. Once uploaded, this certificate gets added in the AirWatch Admin Console. Once installed on the device, it can be viewed on the specific 'Device Details' panel from the Dashboard. To remove or revoke the certificate, navigate to Devices ► Certificates ► List View.
     The types of certificates that are supported are .pfx and .cer (X509). The installation of the '.pfx' cert requires a shared key, which has to be provided to the end user. The '.cer cert' on the other hand gets installed without any user interaction.
5. Select Save & Publish when you are finished to push the profile to devices.

**Note:** A Private key of the certificate is stored only once during the first time installation of the certificate on the device and is present on the device until a Restore Factory Settings action is performed. Please note that the private key gets deleted from the Symbian key store while deleting a profile or during enterprise wipe.

**Note:** Un-enrolling removes the x509 certificate but not the .pfx certificate from the device. This is a platform limitation.
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 MDM Agent for Symbian

Overview

For the communication to happen between the Symbian device and AirWatch, you need to first configure the Symbian agent settings available in the AirWatch Admin Console.

Configuring Settings

To configure, navigate to Groups & Settings ►All Settings ►Devices & Users ►Symbian.

- **Agent Application** - Configure the agent application with the following:
  - **Download Path** - Enter the server path from where the agent is available for download.
  - **SIS Display Name** - Enter the name of the agent application file.

- **Agent Settings** - Configure the agent with the following:
  - **Heartbeat Interval (min)** - Select the time interval in minutes of sending the heartbeat sample from the device to the server.
  - **Data Sample Interval (min)** - Select the time interval in minutes for the agent to collect the data sample.
  - **Agent Polling Interval (min)** - Select the time interval in minutes for the agent to check for any profiles that might have been pushed to the device.
  - **Administrative Passcode** - Enter a passcode. This passcode is required to perform administrative actions on the device. For example, changing any agent settings, deleting the agent etc.
  - **Collect Location Data** - Enable GPS on the device to collect the location details.
  - **Ignore SSL Errors** - Select the checkbox to ignore any SSL errors.
  - **Use AWCM** - Select the checkbox if AWCM is being used for communication.
  - **Default Drive for Application Install** - The default drive on the device where the apps get installed.

Once the configuration is complete and saved, Symbian devices can be enrolled into AirWatch.

Enabling GPS Tracking

Enabling GPS on the AirWatch Admin console enables you to track the whereabouts of your device fleet. To enable GPS tracking:

1. Navigate to Groups & Settings ►All Settings ►Devices & Users ►General ►Privacy. Select the ownership of the devices.
2. Navigate to Groups & Settings ►All Settings ►Symbian ►Agent Settings. Select the Collect Location Data check box.
GPS on the devices is now enabled and you can now keep a tab on your device's location. Please note that if either of the above two options are not selected, GPS will not be enabled on the devices.

**Communicating through the Secure Channel**

The Secure Channel certificate enables all the communication 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 **Block Non-Secure Channel Device Access** for Symbian platform and click **Save**.
Managing Symbian 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

- Using the Device Dashboard – Covers stats and data about your devices available in the Device Dashboard.
- Using the Device List View – Details how to use the Devices List View to search for, filter, and perform remote actions on multiple Windows Mobile devices.
- Using the Device Details Page – Walks through the ways you can manage Windows Mobile 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 (SSP) – View relevant device information for enrolled devices and perform remote actions such as clear passcode, lock device, or device wipe from your device or PC.

Un-enrolling Symbian Devices

Un-enrollment means the removal of the enrolled Symbian device and its corresponding data from the AirWatch Admin Console. Once un-enrolled, the Symbian device cannot be managed and monitored from the AirWatch Admin Console. Un-enrollment is recommended when you encounter any of the following scenarios:

- If the device user leaves the company, then you can manually unenroll the device.
- If the device is lost, then you can send the Enterprise Wipe MDM command.

The Enterprise Wipe action can be performed from the Device Dashboard, Search Device, and Device Details page.

If the end user wants to un-enroll the device, it can be done on the device screen by deleting the agent manually and providing the admin passcode when prompted. This admin passcode should be provided to the end-user. The end user can also unenroll the device from the Self Service Portal.
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
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** – View general statistics such as enrollment status, compliance, last seen, platform/model/OS, Organization Group, contact information, serial number, power status, storage capacity, physical memory and virtual memory.

• **Compliance** – This tab shows the compliance status of the device, including the name and level of all compliance policies that apply to the device. It is important for end users to take note of these policies to ensure devices remain compliant and operate as intended.

• **Profiles** – View all MDM profiles currently installed on a device.

• **Apps** – View all apps currently installed or pending installation on the device.

• **Location** – View current location or location history of a device.

• **User** – Access details about the user of a device as well as the status of the other devices enrolled to this user.

The menu tabs below are accessed by clicking **More** from the main Device Details tab.

- **Network** – View current network (Cellular, Wi-Fi, Bluetooth) status of a device.
- **Security** – View current security status of a device based on security settings.
- **Restrictions** – View the types of restrictions that currently apply to the device.
- **Notes** – View and add notes regarding the device. For example, note the shipping status or if the device is in repair and out of commission.
- **Certificates** – Identify device certificates by name and issuant. This tab also provides information about certificate expiration.
- **Terms of Use** – View a list of End User License Agreements (EULAs) which have been accepted during device enrollment.
- **Alerts** – View all alerts associated with the device.
- **Shared Device Log** – View history of device in terms of Shared Device, including past check-ins and check-outs and current status.
- **Event Log** – View history of device in relation to MDM, including instances of debug, information and server check-ins.
- **Status History** – View history of device in relation to enrollment status.
- **Attachments** – Add files associated to 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.

- **Device Query** - Device sends comprehensive MDM information to the AirWatch console.
- **Reset Passcode** - Reset the existing passcode.
- **Send Message** - Send an Email or SMS Message.
- **Lock Device** - Triggers the device’s locking mechanism.
- **Enterprise Wipe** - Removes AirWatch profiles and apps.
- **Device Wipe** - Performs a full factory reset.

**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.
Using the Self-Service Portal (SSP)

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.

- **Compliance** – This tab shows the compliance status of the device, including the name and level of all compliance policies that apply to the device. It is important for end users to take note of these policies to ensure devices remain compliant and operate as intended.

- **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.

• **Certificates** – This tab displays a detailed listing of certificates currently assigned to and installed on the device. From the Certificates view, you can deactivate, renew or remove a certificate, if allowed.

• **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.

• **Device Query** – Manually requests the device to send a comprehensive set of MDM information to the AirWatch Server.

• **Reset Passcode** – Resets the passcode on the selected device.

• **Send Message** – Sends an Email, SMS (text) 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.
Appendix – Additional Considerations

The following exceptions and notes help you as an administrator to manage your devices effectively.

- Presently performing an Enterprise Wipe from Dashboard, SSP or manually un-enrolling the device removes Calendar entries on Symbian Anna devices and Belle but not on Symbian S60 3rd Edition and S60 5th Edition devices (5800 Xpress music).
- Syncing of Recurring Calendar entries is not supported.
- If the agent is installed on an SD card, performing a SD card wipe to the device removes the agent but the 'MDM Handler' remains on the device.

On Nokia 5800 Xpress Music devices:
  - When the maximum number of failed passcode attempts is set to ‘n’ time and you try to enter the passcode incorrectly for the (n-1) times, the device freezes (this is a limitation of this device).
  - Email account may not be removed even when EAS profile is deleted.

- The access points (for example, GPRS access points) are not defined for Symbian^ Belle and Anna devices. You have to manually configure the access point as ‘Internet’ on receiving an EAS profile in the device. To do that, on the device, navigate to Menu ► Email ► Settings ► Mail for Exchange ► Mailbox ► Adv.mailbox settings ► Access point and then select Internet option.
- The Uninstaller.exe file still exists even after un-enrolling the device because of platform restrictions. This can be manually deleted or left as it is, as it does not affect the functionality.
- Currently the GPS feature works only if Nokia maps are pre-installed on the device.
- If an app is packaged with smart installer then the name of the installer package needs to be same as the inner package. Only then the app gets uninstalled (this is an application management functionality).
- If an agent is installed in the Phone Memory and a Storage Device (SD) card wipe command is sent from the AirWatch Admin Console, the SD card gets formatted. Selecting “Check for Command” on the device after this closes the agent. This is an expected behavior.
- S60 3rd edition FP1 (Nokia E71 Device) does not support apps. The apps which are pushed from the AirWatch Admin Console are listed under the ‘Apps’ tab on the dashboard. It displays a status as Pending Installation.