VMware AirWatch Symbian Platform Guide

Deploying and managing Symbian devices

AirWatch v8.1 and higher

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

Revision Table

The following table displays revisions to this guide since the release of AirWatch v8.1 and higher.

Date	Reason
March 2018	Initial upload.

Table of Contents

Chapter 1: Overview

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 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 Console.
- Symbian Device Profiles – Explores the AirWatch Console features, such as enabling services for the agent, deploying profiles and credentials, controlling profile time schedules, etc.
- 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 Console.
- Keep in Mind – Lists out few exceptions and points that would help you to manage devices effectively.

Model	Edition	OS	Firmware
E71	Symbian S60 3rd Edition, FP1	9.2	300.21.012
E5	Symbian S60 3rd Edition, FP2	9.3	071.003
E72	Symbian S60 3rd Edition, FP2	9.3	081.001
C5	Symbian S60 3rd Edition, FP2	9.3	091.002
C6	Symbian S60 5th Edition	9.4	41.0.01
5800 Xpress music	Symbian S60 5th Edition	9.4	60.0.003
C7	Symbian ^3 Anna	9.5	022.014
N8	Nokia Belle	9.5	025.008
E6	Symbian ^3 Anna	9.5	026.001
N8	Symbian ^3	9.5	014.002
701	Nokia Belle*	10.1	111.030.0609
*Nokia Belle FP1 and FP2 are not supported			

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.

Model	Edition	OS	Firmware
E71	Symbian S60 3rd Edition, FP1	9.2	300.21.012
E5	Symbian S60 3rd Edition, FP2	9.3	071.003
E72	Symbian S60 3rd Edition, FP2	9.3	081.001
C5	Symbian S60 3rd Edition, FP2	9.3	091.002
C6	Symbian S60 5th Edition	9.4	41.0.01
5800 Xpress music	Symbian S60 5th Edition	9.4	60.0.003
C7	Symbian ^3 Anna	9.5	022.014
N8	Nokia Belle	9.5	025.008
E6	Symbian ^3 Anna	9.5	026.001
N8	Symbian ^3	9.5	014.002
701	Nokia Belle*	10.1	111.030.0609
*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 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.

Chapter 2:
Symbian Device Enrollment

Overview

In order for Symbian devices to communicate with the AirWatch Console, you or the end user must install an agent. This agent facilitates the communication between the device and the AirWatch 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 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 Console.

Prerequisites

To enroll a Symbian device using 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 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.

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**.

Steps to Enroll

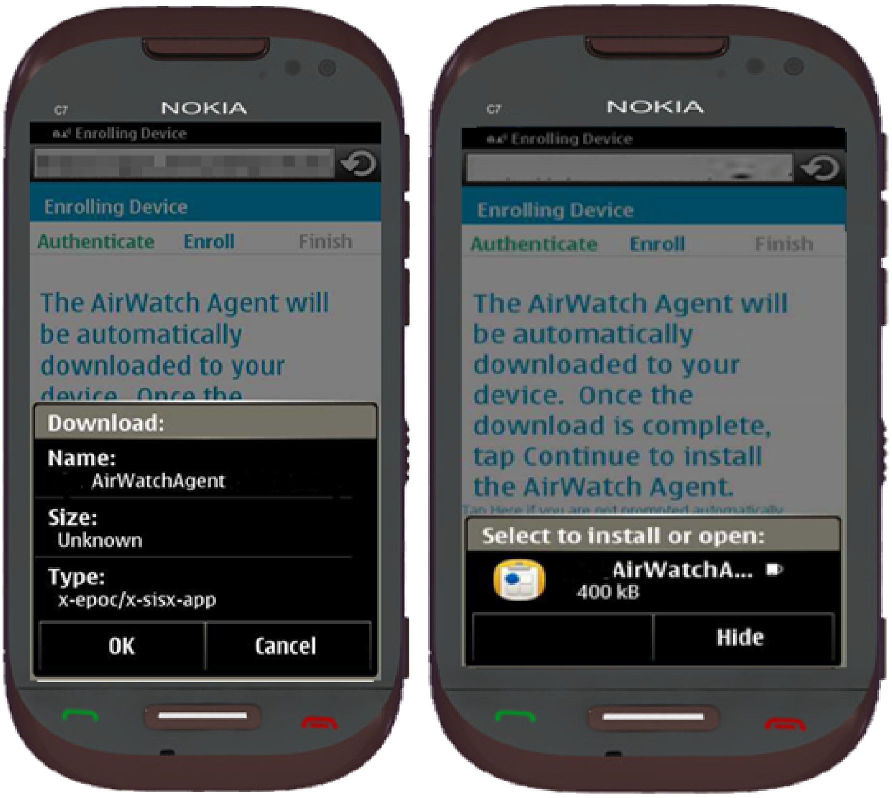
Follow these steps in order to make a Symbian device available for remote management through the AirWatch MDM application:

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.



The AirWatch Agent will be automatically downloaded to your device. Once the

Download:

Name: AirWatchAgent

Size: Unknown

Type: x-epoc/x-sisx-app

The AirWatch Agent will be automatically downloaded to your device. Once the download is complete, tap Continue to install the AirWatch Agent.

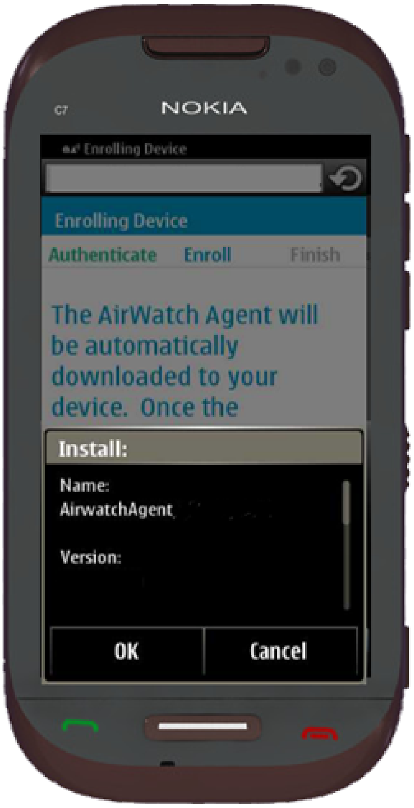
Tap Here if you are not prompted automatically

Select to install or open:

AirWatchA... 400 kB

   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.



Enrolling Device

The AirWatch Agent will be automatically downloaded to your device. Once the

Install:

Name:
AirwatchAgent

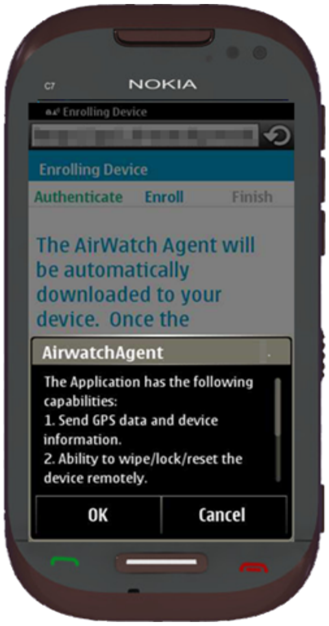
Version:

Note: Please note that by default the configuration files are saved in the phone memory (AirWatch recommends this 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.



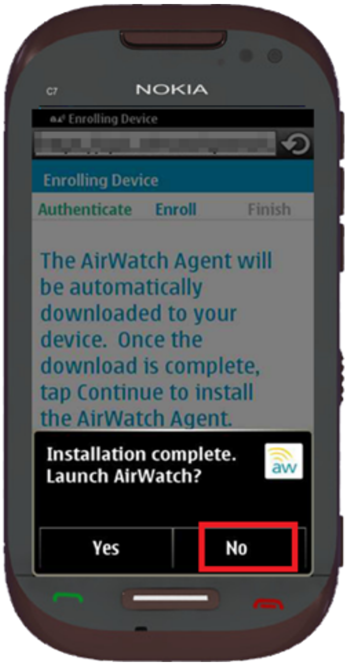
Enrolling Device

The AirWatch Agent will be automatically downloaded to your device. Once the

AirwatchAgent

The Application has the following capabilities:
1. Send GPS data and device information.
2. Ability to wipe/lock/reset the device remotely.

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

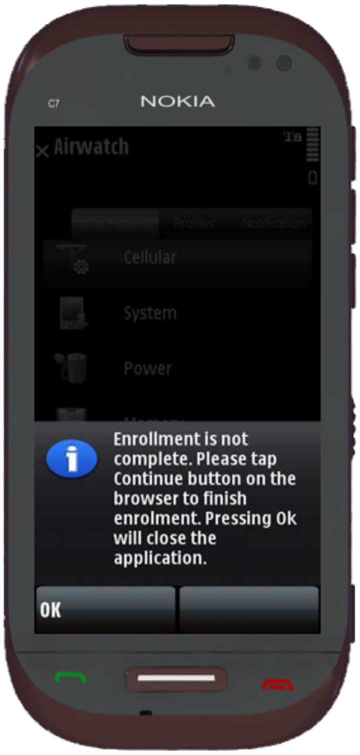


Enrolling Device

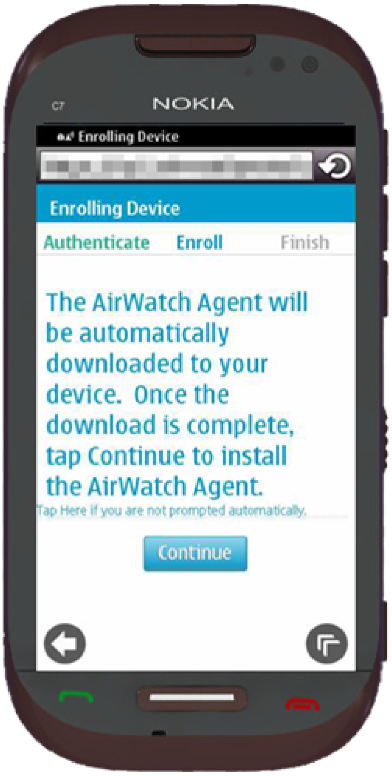
The AirWatch Agent will be automatically downloaded to your device. Once the download is complete, tap Continue to install the AirWatch Agent.

Installation complete.
Launch AirWatch?

> **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**.



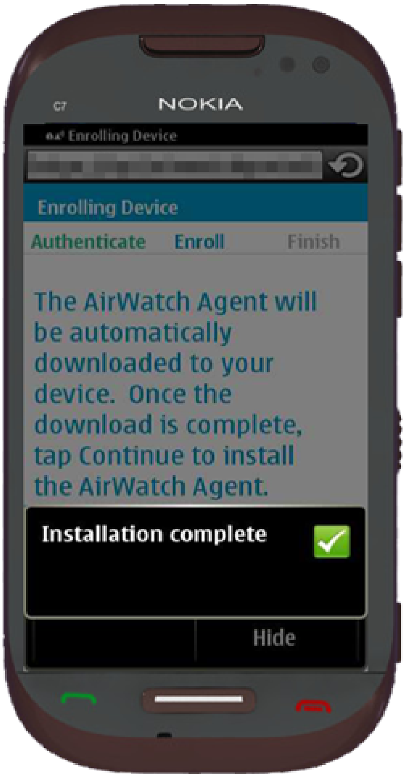
Enrollment is not complete. Please tap Continue button on the browser to finish enrolment. Pressing Ok will close the application.



The AirWatch Agent will be automatically downloaded to your device. Once the download is complete, tap Continue to install the AirWatch Agent.

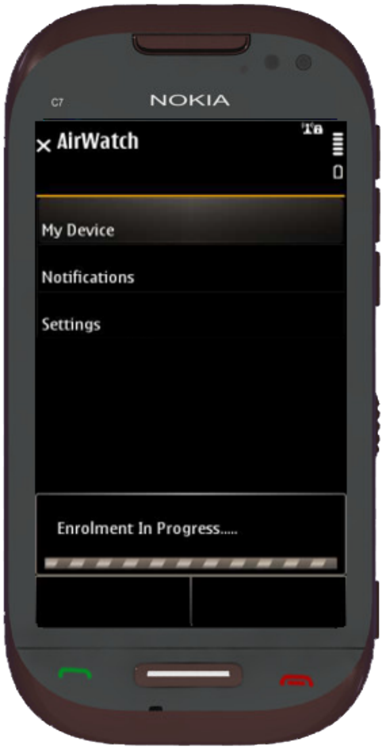
Tap Here if you are not prompted automatically.

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



The AirWatch Agent will be automatically downloaded to your device. Once the download is complete, tap Continue to install the AirWatch Agent.

Installation complete ✓

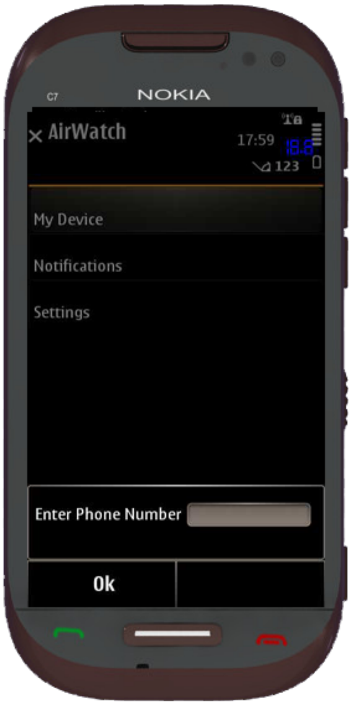


Enrolment In Progress.....

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 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.

Chapter 3:
Symbian 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.

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 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:
   - **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 (unenrollment) 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 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 **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 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 **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 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 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 **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 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 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 **Credentials** profile.
4. Configure the Credentials settings, including:
   - **Credential Source** – Use the drop-down 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 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.

Chapter 4: AirWatch 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 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:

Setting	Description
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.

Setting	Description
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 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 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 select **Save.**

Chapter 5:
Managing Symbian Devices

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.

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.

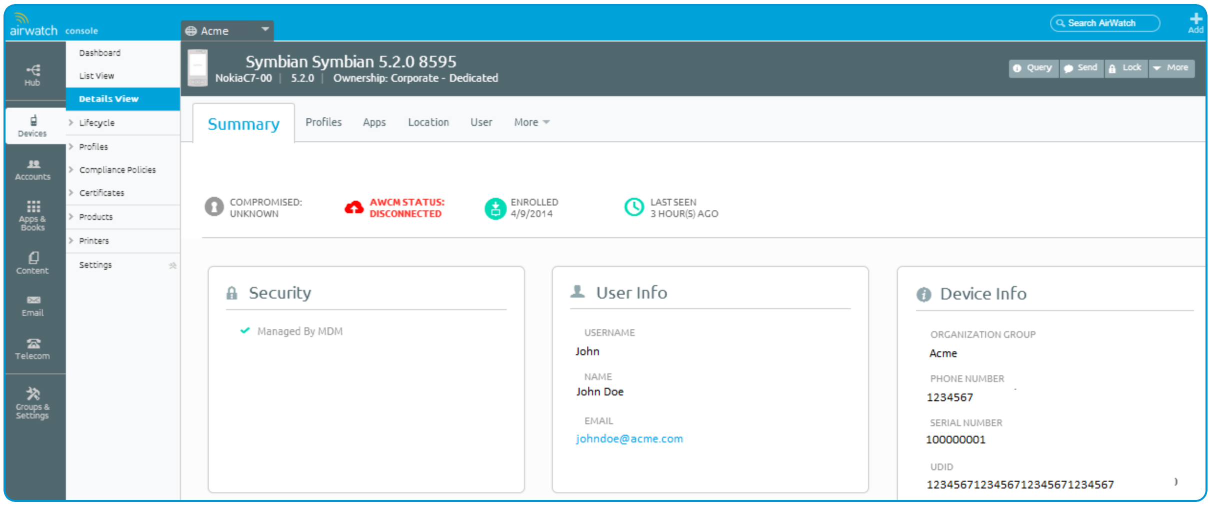
Search in Device List View

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.



Symbian Symbian 5.2.0 8595

NokiaC7-00 | 5.2.0 | Ownership: Corporate - Dedicated

COMPROMISED: UNKNOWN

AWCM STATUS: DISCONNECTED

ENROLLED 4/9/2014

LAST SEEN 3 HOUR(S) AGO

✓ Managed By MDM

USERNAME
John

NAME
John Doe

EMAIL
johndoe@acme.com

ORGANIZATION GROUP
Acme

PHONE NUMBER
1234567

SERIAL NUMBER
100000001

UDID
1234567123456712345671234567

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.
- **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 selecting **More** from the main Device Details tab.

- **Network** – View current network information (Cellular, Wi-Fi, Bluetooth, IMEI) of a device.
- **Security** – View current security status of a device based on security settings.
- **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.
- **Shared Device Log** – View history of device in terms of Shared Device, including past check-ins and check-outs and current status.
- **Status History** – View history of device in relation to enrollment status.
- **Targeted Logging** – View the logs for the Console, Catalog, Device Services, Device Management and Self Service Portal. A link is provided enabling you to configure targeted logging (**All Settings > Admin > Diagnostics > Logging**).
- **Attachments** – Use this storage space on the server for screenshots, documents and links for troubleshooting and other purposes without taking up space on the device itself.

Device Action Descriptions

- **Add Tag** – Assign a customizable Tag to a device, which can be used to identify a special device in your fleet.
- **Change Device Passcode** – Replace any existing device passcode used to access the selected device with a new passcode.
- **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.
- **Clear Passcode (Device)** – Clear the device passcode. To be used in situations where the user has forgotten their device's passcode.
- **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.
- **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**.
- **Query All** – Send a query command to the device to return a list of installed apps (including VMware AirWatch Agent, where applicable), books, certificates, device information, profiles and security measures.
- **Send Message** – Send a message to the user of the selected device. Choose between **Email**, **Push Notification** and **SMS**.

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 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 Console are listed under the ‘**Apps**’ tab on the dashboard. It displays a status as **Pending Installation**.