VMware AirWatch Tizen Guide

AirWatch v8.4 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 v8.4 and higher.

Date	Reason
March 2018	Initial upload.

Table of Contents

Chapter 1:
Overview

Introduction to the Tizen Platform

AirWatch provides a robust set of mobility management solutions for enrolling, securing, configuring, and managing your Tizen device deployment. The AirWatch Console gives you several tools and features for managing the entire lifecycle of corporate and employee-owned devices. You can also enable end users to perform tasks themselves through the Self-Service Portal (SSP) and user enrollment, which will save you vital time and resources.

Finally, custom reporting tools and a searchable, customizable dashboard make it easy for you to perform ongoing maintenance and management of your device fleet.

Supported OS Versions and Requirements

Before deploying Tizen devices, you should consider the following prerequisites, requirements, supporting materials, and helpful suggestions from the AirWatch team. Familiarizing yourself with the information available in this section helps prepare you for deploying Tizen devices.

Supported Operating Systems

- 2.3
- 2.4

Requirements

Before using the procedures in this guide, please ensure you have the following:

- **Appropriate Admin Permissions** – Allows you to create profiles, policies and manage devices within the AirWatch Console.
- **Enrollment URL** – Links to your organization's enrollment environment and takes you directly to the enrollment screen. For example, **mdm.acme.com/enroll**.
- **Group ID** – Associates your device with your corporate role and is defined in the AirWatch Console.
- **Credentials** – Authenticates you as an end user in your AirWatch environment. These credentials may be the same as your network directory services or may be uniquely defined in the AirWatch Console.

Chapter 2:
Tizen Device Enrollment

Tizen Enrollment Overview

You can associate an email domain to your environment, which requires users to enter only an email address and credentials (and in some cases select a Group ID from a list) to complete enrollment. This is a simplified approach that leverages information end users likely already know.

Tizen devices must begin communicating with AirWatch to access internal content and features, which is facilitated using the AirWatch Agent. Available for download from the Tizen Store, the AirWatch Agent provides a single resource to enroll a device as well as provide device and connection details. Additionally, agent-based enrollment allows you to:

- Authenticate users using basic or directory services, such as AD/LDAP/Domino, SAML, tokens or proxies.
- Register devices in bulk or allow users to self-register.
- Define approved OS versions, models and maximum number of devices per user.

Email Autodiscovery

If you do not set up an email domain for enrollment, users will be prompted for the Enrollment URL and Group ID, which must be given to them.

Enrolling Requirements

The following information is required prior to enrolling your Android device:

If an email domain is associated with your environment – If Using Auto Discovery

- **Email address** – This is your email address associated with your organization. For example, **JohnDoe@acme.com**.
- **Credentials** – This **username** and **password** allow you to access your AirWatch environment. These credentials may be the same as your network directory services or may be uniquely defined in the AirWatch Console.

If an email domain is not associated with your environment – If Not Using Auto Discovery

If a domain is not associated with your environment, you are still prompted to enter your email address. Since auto discovery is not enabled, you are then prompted for the following information:

- **Enrollment URL** – This URL is unique to your organization's enrollment environment and takes you directly to the enrollment screen. For example, **mdm.acme.com/enroll**.
- **Group ID** – The Group ID associates your device with your corporate role and is defined in the AirWatch Console.
- **Credentials** – This unique username and password pairing allows you to access your AirWatch environment. These credentials may be the same as your network directory services or may be uniquely defined in the AirWatch Console.

To download the Agent and subsequently enroll aTizen device, you'll need the following information:

- **Enrollment URL** – The enrollment URL is AWAgent.com for all users, organizations and devices enrolling into AirWatch.

Enroll a Tizen Device with the AirWatch Agent

The enrollment process secures a connection between Tizen devices and your AirWatch environment. The AirWatch Agent is the application that facilitates enrollment and allows for real-time management and access to relevant device information.

Tizen devices use the Enrollment URL to first check and then download the AirWatch Agent. The AirWatch Agent provides a single resource to enroll a device as well as provides device and connection details. Additionally, the enrollment process allows you to:

- Authenticate users using basic or directory services, such as AD/LDAP/Domino, SAML, tokens or proxies.
- Authenticate users using pass through authentication using Single Sign On.
- Register devices in bulk or allow users to self-register.
- Stage devices for both standard and advanced single users.
- Define approved OS versions, models and maximum number of devices per user.

To enroll a device using the AirWatch Agent:

1. Navigate to **AWAgent.com** from your browser.

   AirWatch automatically detects if the AirWatch Agent is installed on your device and, if it is not, redirects you to the App Store to download it. You can also send the enrollment URL to devices using SMS text message.

2. Download and install the AirWatch Agent from the App Store, if needed.

3. Launch the AirWatch Agent or return to your browser session to continue enrollment.

   - If you have configured email autodiscovery, then it prompts you for your email address. In addition, you may be prompted to select your Group ID from a list.

   - If you have not configured email autodiscovery, then it will prompt you for the Enrollment URL and a Group ID.

4. Enter your username and password.

5. Follow the remaining prompts to complete enrollment.

   You may be notified at this time if your user account is not allowed or blocked because your account is blacklisted and not approved for enrollment.

For additional details about configuring enrollment options, refer to the Enrollment section of the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

Chapter 3:
Tizen Device Profiles

Tizen Device Profiles

Tizen device profiles ensure proper usage of devices, and device functionality. Profiles serve many different purposes, from letting you enforce rules and procedures to tailoring and preparing Tizen devices for how they will be used with AirWatch.

The individual settings you configure, such as those for restrictions and bookmarks, are referred to as payloads. In most cases, AirWatch recommends that you only configure one payload per profile, which means you will have multiple profiles for the different settings you want to push to devices.

Configure Wi-Fi Access for Tizen Devices

Configuring a Wi-Fi profile lets devices connect to corporate networks, even if they are hidden, encrypted or password protected. This can be useful for end users who travel to various office locations that have their own unique wireless networks or for automatically configuring devices to connect to the appropriate wireless network while in an office.

The Wi-Fi profile applies to the work profile and work managed device types.

To configure the Wi-Fi profile:

1. Navigate to **Devices > Profiles > List Views > Add**. Select **Add Profile**.
2. Select **Tizen** to deploy a Tizen profile.
3. 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.
4. Select the **Wi-Fi** payload, and then select **Configure**.

5. Configure **Wi-Fi** settings, including:

Setting	Description
Service Set Identifier	Provide the name of the network the device connects to.
Hidden Network	Indicate if the Wi-Fi network is hidden.
Security Type	Specify the access protocol used and whether certificates are required. Depending on the selected security type, this will change the required fields. If **None, WEP, WPA/WPA 2, or Any (Personal)** are selected; the **Password** field will display. If **EAP** is selected, the Protocols and Authentication fields display. • **Protocols** ○ Use Two Factor Authentication ○ SFA Type • **Authentication** ○ Identity ○ Anonymous Identity ○ Username ○ Password
Password	Provide the required credentials for the device to connect to the network. The password field displays when **WEP, WPA/WPA 2, Any (Personal), WPA/WPA2 Enterprise** are selected from the **Security Type** field.
Proxy	
Enable Wi-Fi Proxy	Enable to configure the W-Fi proxy settings.
Proxy Server	Enter the hostname or IP address for the proxy server.
Proxy Server Port	Enter the port for the proxy server.
Exclusion List	Enter the hostnames to exclude from the proxy. Hostnames entered here will not be routed through the proxy. Use the * as a wild card for the domain. For example: *.air-watch.com or *air-watch.com

6. Select **Save & Publish**.

Chapter 4:
Tizen Devices Management

Overview

You can manage the Tizen extension from the AirWatch Console after you successfully enable and register users' devices. This section walks you through the ways you can manage Tizen devices.

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.

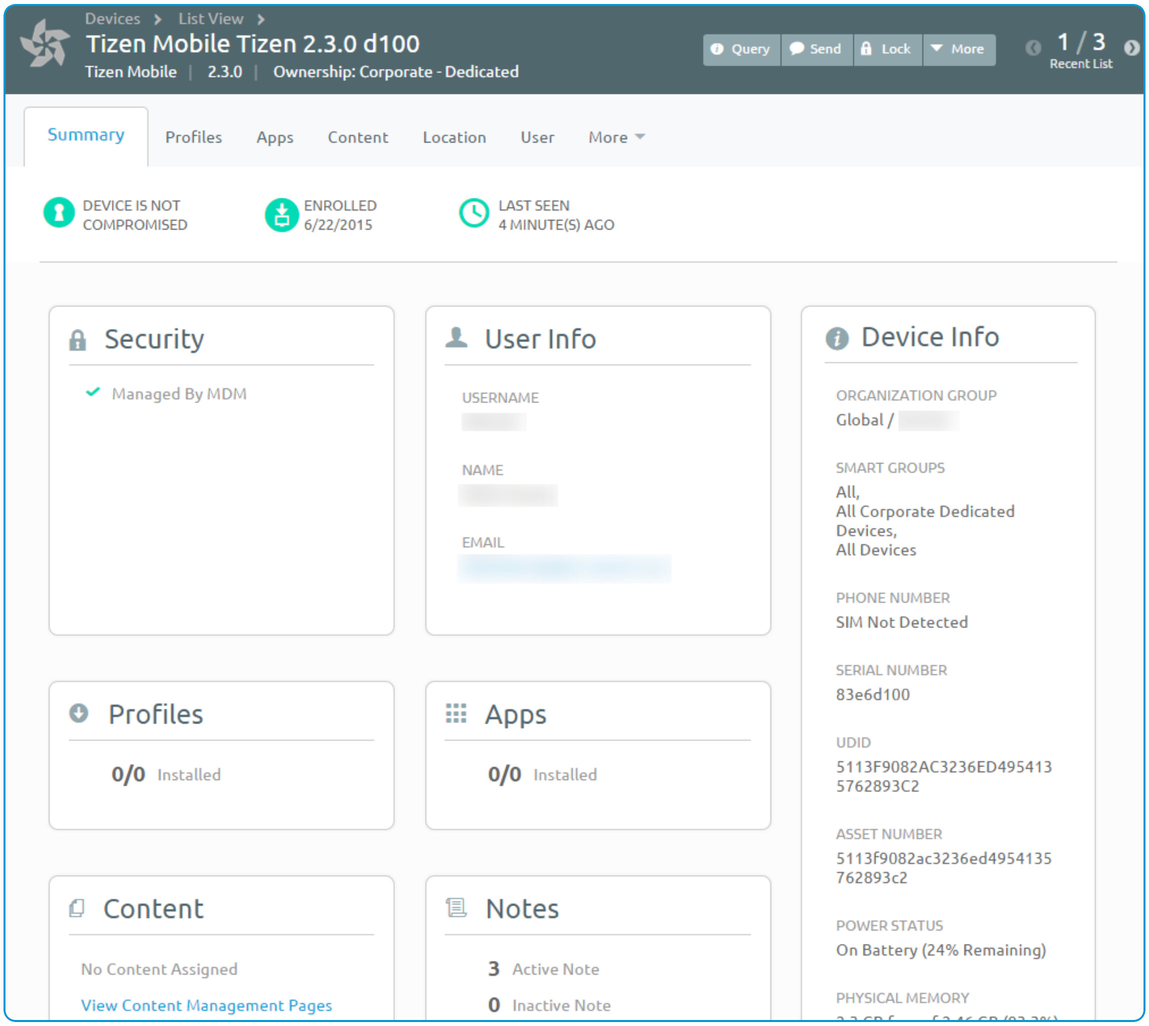
Search in Device List View

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.

Device Details

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.



Tizen Mobile Tizen 2.3.0 d100

Tizen Mobile | 2.3.0 | Ownership: Corporate - Dedicated

DEVICE IS NOT COMPROMISED

ENROLLED 6/22/2015

LAST SEEN 4 MINUTE(S) AGO

Security

✓ Managed By MDM

User Info

USERNAME
[redacted]

NAME
[redacted]

EMAIL
[redacted]

Device Info

ORGANIZATION GROUP
Global / [redacted]

SMART GROUPS
All,
All Corporate Dedicated Devices,
All Devices

PHONE NUMBER
SIM Not Detected

SERIAL NUMBER
83e6d100

UDID
5113F9082AC3236ED495413
5762893C2

ASSET NUMBER
5113f9082ac3236ed4954135
762893c2

POWER STATUS
On Battery (24% Remaining)

PHYSICAL MEMORY

Profiles

0/0 Installed

Apps

0/0 Installed

Content

No Content Assigned

View Content Management Pages

Notes

3 Active Note

0 Inactive Note

Use the **Device Details** menu tabs to access specific device information.

- **Summary** – You can 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** – You can view all MDM profiles currently installed on a device.
- **Apps** – You can view all apps currently installed or pending installation on the device.
- **Content** – You can view the status, type, name, version, priority, deployment, last update, date and time of views, acknowledged (reflecting whether required content has been acknowledged) of content on the device. This tab also provides a toolbar for administrative action (install or delete content).
- **Location** – You can view current location or location history of a device.

- **User** – You can access details about the user of a device as well as the status of the other devices enrolled to this user.

Additional menu tabs can be accessed by selecting **More** on the main **Device Details** tab.

- **Network** – You can view current network information (Cellular, Wi-Fi, Bluetooth, IMEI) of a device.
- **Security** – You can view current security status of a device based on security settings.
- **Notes** – You can 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** – You can identify device certificates by name and issuant. This tab also provides information about certificate expiration.
- **Terms of Use** – You can view a list of End User License Agreements (EULAs) which have been accepted during device enrollment.
- **Status History** – You can view history of device in relation to enrollment status.

Remote Actions

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

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

Actions	Descriptions
Query	Queries the device for all information.
Management	Locks the device or SSO session, reboot the device or perform an enterprise or device wipe.
Support	Performs support actions such as sending the device a message, finding the device by playing an audible tone.
Admin	Changes AirWatch Console settings, including changing organization group and editing/deleting devices from AirWatch MDM.