Below is a collection of screenshots comparing the AirWatch Agent and Workspace ONE Intelligent Hub on iOS for enrollment and in-app experience.

<table>
<thead>
<tr>
<th>ID</th>
<th>Feature</th>
<th>AirWatch Agent (Before)</th>
<th>Intelligent Hub (After)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Welcome Screen</td>
<td><img src="image1.png" alt="AirWatch Agent Welcome Screen" /></td>
<td><img src="image2.png" alt="Intelligent Hub Welcome Screen" /></td>
</tr>
</tbody>
</table>

The multi-step enrollment process begins with authentication.

Choose authentication method:

- Email Address
- Server Details
- QR Code

Privacy Policy
<table>
<thead>
<tr>
<th></th>
<th>Enrollment (URL &amp; Group ID)</th>
<th>Autodiscovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td><img src="image1" alt="Server Details" /></td>
<td><img src="image2" alt="Autodiscovery" /></td>
</tr>
<tr>
<td>3</td>
<td><img src="image3" alt="Email Address" /></td>
<td><img src="image4" alt="QR Code" /></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>4</td>
<td>QR Code</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Username &amp; Password</td>
<td></td>
</tr>
</tbody>
</table>
Token

Optional Prompts

Authentication Token
Token
Check Activation Email

Device Ownership
Employee Owned
Corporate - Shared
Corporate - Dedicated

Ownership
Additional information is required to provide you with access to productivity apps and other resources.

- Employee Owned
- Corporate Owned

Corporate - Dedicated

Asset Number
Optional

Next
8  Choose Organization Group

9  Terms of Use
10  App Permissions

Enable Device Management
To enable your device, you will be redirected to Safari and Settings

Why?
• Access your company resource
• Remove company data in the event of loss or theft

Redirect & Enable

11  Multi User Staging

Group ID
Username
Password
Login

Workspace Services
This is required before the app can be installed. You automatically receive:

- Direct installation of all corporate resources.
- Secured corporate network access.
- Synchronized apps and content on all of your devices.
- An enhanced app experience that will make you more productive.
12 Device Info

13 App Passcode
Nothing to see here.
You have no messages.
Support
Privacy

Your privacy matters.

VMware Workspace ONE collects information to provide secure access to your work data and applications. Below you will find an overview of data collected by Workspace ONE and Agent to provide optimal performance, security, and support. For information about how your company handles information collected by Workspace ONE, please contact your company.

Contact your company’s IT administrator if you want to find out how to un-enable your device and discontinue access to this app.

Data collected by Agent

Tap here for an overview of the data that this app may collect about device hardware, diagnostics, and diagnostic logs. Your company has access to this data and some data collected may be visible to your IT administrator.

Agent permissions

Tap here for an overview of the device permissions that this app will require to function properly. These permissions can be changed in your device settings but may impact app performance.

Data collected by Hub

Tap here for an overview of the data that this app may collect about device hardware, diagnostics, and diagnostic logs. Your company has access to this data and some data collected may be visible to your IT administrator.

Hub permissions

Tap here for an overview of the device permissions that this app will require to function properly. These permissions can be changed in your device settings but may impact app performance.