VMWARE WORKSPACE ONE REFERENCE ARCHITECTURE: VALIDATED INTEGRATION DESIGN
Table of Contents

Executive Summary ................................................. 5
VMware Reference Architectures ................................. 8
  Audience .................................................................. 8
Reference Architecture Design Methodology ...................... 9
Workspace ONE Solution Overview .............................. 10
  Platform Integration ............................................. 11
Business Drivers and Use Cases Definition ...................... 12
  Business Drivers and Requirements ............................ 12
  Use Cases ................................................................ 13
  Meeting Business Requirements with Workspace ONE ........ 14
Workspace ONE Services Definition .............................. 15
  Mobile Device Management Service ............................ 16
  Mobile Productivity Service .................................... 17
  Mobile Application Workspace Service ....................... 18
Architecture Principles and Concepts ............................. 19
  AirWatch and VMware Identity Manager Integration ........ 20
  Workspace ONE Logical Components and Concepts ........ 21
Workspace ONE Component Design ............................. 23
  Workspace ONE Native Mobile Apps .......................... 23
  VMware Identity Manager ..................................... 24
    Design Overview ................................................ 25
    Install and Initial Configuration .............................. 25
    Next Steps ....................................................... 26
  AirWatch ............................................................ 26
    Installation and Initial Configuration ...................... 27
    Next Steps ....................................................... 27
  AirWatch Cloud Connector and VMware Identity Manager Connector ........................ 27
    Design Overview ................................................ 27
    ACC Design Considerations .................................. 28
    VMware Identity Manager Connector Design Considerations .................................. 29
    Key Design Considerations .................................. 30
Email Integration ................................................................. 30
Secure Email Gateway Proxy Model ...................................... 31
Direct PowerShell Model ..................................................... 32
Key Design Considerations .................................................. 33
Next Steps ................................................................. 33
Content Integration .......................................................... 34
Content Management Overview ........................................... 34
Data Protection in AirWatch Content Locker ................................ 35
Key Design Considerations .................................................. 35
Conditional Access ........................................................... 36
Standalone MAM and Adaptive Management ............................ 38
  Enabling Adaptive Management ........................................... 39
Data Loss Prevention .......................................................... 40
VMware Verify .................................................................. 42
  Verify Architecture ........................................................ 42
Resource Types ............................................................ 43
  SaaS Apps .................................................................. 43
  ThinApp Packaged Apps .................................................. 43
  Horizon Apps and Desktops .............................................. 44
  Native Mobile Apps ....................................................... 44
  Unified App Catalog ....................................................... 45
Mobile Single Sign-On ....................................................... 45
  iOS SSO Overview ........................................................ 45
  Android SSO Overview .................................................. 46
  Windows 10 SSO Overview .............................................. 46
View in Horizon 7 ............................................................ 46
  Logical Architecture ....................................................... 47
Next Steps for Horizon ...................................................... 47
Access Point ............................................................... 48
  Design Overview ........................................................ 48
Access Point 2.5 and 2.7 ....................................................... 48
Network Deployment Options ............................................. 48
Next Steps for Access Point ................................................. 48
Executive Summary

VMware Workspace™ ONE™ combines identity and mobility management to provide frictionless and secure access to all the apps and data employees need to work, wherever, whenever, and from whatever device they choose.

This white paper provides a reference architecture for the Workspace ONE product. The reference architecture is an example architecture and deployment, based on addressing key business requirements such as enabling business mobility for employees and targeting use cases such as mobile knowledge workers.

Taking the example business requirements and use cases, distinct services are defined encompassing the components from Workspace ONE. Three example services—Mobile Device Management, Mobile Productivity Service, and Mobile Application Workspace Service—address everything from basic mobile management and secure identity-based access through to full virtual desktop access on mobile devices and seamless single sign-on across all applications.

![Figure 1: VMware Workspace Logical Architecture Overview](image)

Workspace ONE and the services that address business requirements are based on a unique hybrid cloud architecture. Mobile device and identity services are delivered via VMware AirWatch® and VMware Identity Manager™ cloud-hosted offerings. These services in combination with the Workspace ONE app deliver unified and seamless access to SaaS-based applications, public mobile applications, and on-premises virtual applications or virtual desktops. The final key component to the architecture is a lightweight set of appliances that secure integration between cloud-based and on-premises services.
Workspace ONE integrates with a corporate email solution, whether on-premises or cloud-based, in order to provide secure access via OS native, third-party, or managed mobile email clients (i.e., AirWatch Inbox or VMware Boxer). Similarly, access to corporate and user content is provided through a flexible approach of integrating with on-premises file servers, Office 365-based content, third-party cloud storage providers, and VMware AirWatch Content Locker™.

The Conditional Access and Adaptive Management features in Workspace ONE address the very significant concerns of providing easy and trusted end-user access to business applications, while ensuring an enterprise level of security around providing that access.

Making end-user access to applications seamless is a sure way to encourage adoption of those apps, so Workspace ONE introduces One-Touch Mobile single sign-on (SSO). This feature allows use of capabilities such as TouchID on an iPhone, fingerprint readers on Android, or Windows Hello on a Surface Pro to provide a password-free yet completely secure means of logging into all the applications end users need.

Further building on security themes, Workspace ONE provides options for Data Loss Prevention (DLP) and multifactor authentication (MFA) technology to ensure that enterprise information is protected on mobile platforms, and when additional means of authentication are required, a secure yet easy-to-use solution can be easily implemented.

Additionally, Workspace ONE integrates with VMware Horizon 7, the virtual desktop and remote application product. This integration provides fast SSO access to a Windows 10 desktop or set of Windows applications for those users that require it.

The solution integrates tightly with infrastructure services such as Microsoft Active Directory, DNS, certificate services, and edge services such as load balancing and firewalls to provide a highly available, secure, and federated solution.

In order to deliver the defined services, the Workspace ONE components are deployed in varying combinations and configurations to meet the specific user requirements. The reference architecture details these configurations needed to integrate both the Workspace ONE components and corporate end-user services.

![Figure 2: Workspace ONE iOS App](image)
After deployed, the Workspace ONE set of services provides a consistent, secure, and simple way for users to easily access corporate applications and data. The Workspace ONE mobile app and the Workspace ONE portal provide a single place for all users to go for application access. Access is made simple as it removes the need for users to remember passwords, and applications can be accessed at the touch of an icon regardless of where those applications or services are deployed. The Workspace ONE app also provides the ability for users to self-serve additional applications as needed via a single catalog for all types of resources they require.

This reference architecture underwent design validation, component design and build, service build, integration, user workflow, and testing to ensure that the all objectives were met, the use cases were delivered properly, and that real-world implementation is achievable.

The Workspace ONE reference architecture clearly illustrates how Workspace ONE can deliver a modern digital workspace that meets key business requirements and common use cases for the increasingly mobile workplace.
VMware Reference Architectures

VMware reference architectures are designed and validated by VMware and supporting partners to address common use cases, such as enterprise desktop replacement, remote access, and disaster recovery.

VMware reference architectures offer customers:

- Standardized, validated, repeatable components
- Scalable designs that allow room for future growth
- Validated and tested designs that reduce implementation and operational risks
- Quick implementation, reduced costs, and minimized risk

This reference architecture is designed to cover the integration of key components of a Workspace ONE implementation. It does not provide scalability models, performance data, or stress-testing metrics.

A validated integration design (VID) is intended to provide detailed configuration information and example architecture for deploying all products in an integrated manner.

This Workspace ONE VID presents high-level design and low-level configuration for the key features and integration points of Workspace ONE to form cohesive services to address typical business use cases.

**Note:** Links within this document refer to content on https://www.vmware.com/support/pubs/ as well as on https://my.air-watch.com. While the content on the VMware site is openly accessible, the content on the AirWatch site requires logging into an account. Readers can create a free account to access that material.

**Audience**

This reference architecture guide helps customers, IT architects, consultants, and administrators involved in the early phases of planning, designing, and deploying Workspace ONE and mobile solutions.

The reader should have:

- A solid understanding of the mobile device landscape
- Deep experience regarding capabilities and configuration of mobile operating systems
- Familiarity with device management concepts
- Knowledge of identity solutions and standards such as SAML authentication
- Understanding of enterprise communication and collaboration solutions, including Microsoft Office 365, Exchange, and SharePoint
- Basic concepts of virtualized apps and desktops
Reference Architecture Design Methodology

To ensure a successful Workspace ONE deployment, it is important to follow proper design methodology. To start, we need to understand the business requirements, reasons, and objectives for undertaking the project. From there, we can identify the needs of the users, and organize these needs into use cases with understood requirements. We can then align and map those use cases against a set of integrated services provided by Workspace ONE.

Figure 3: Reference Architecture Design Methodology

A Workspace ONE design uses a number of components to provide these highly available services to address the identified use cases. Before we can integrate and deliver these services, we first need to design and build any required components. This should be done in a modular and scalable manner to allow for change and growth.

Then we can bring the parts together to deliver the integrated services to satisfy the use cases, business requirements, and the user experience.

As with any design process, this is cyclical and previous decisions should be reevaluated to determine if later decisions impact them and require a change.
Workspace ONE Solution Overview

VMware Workspace ONE is a simple and secure enterprise platform that delivers and manages any app on any device by integrating identity, application, and enterprise mobility management. It is available as a cloud service or for on-premises deployment. The platform is comprised of several components—VMware AirWatch, VMware Identity Manager, VMware Horizon 7, and the Workspace ONE mobile apps supporting the most common mobile platforms.

With this latest release, customers can now enjoy key features such as:

- **Self-service access to cloud, mobile, and Windows apps**
  - After they are authenticated through the Workspace ONE app, employees can instantly access mobile, cloud, and Windows applications with one-touch single sign-on.

- **Choose to use any device: employee or corporate owned**
  - Facilitate adoption of BYOD programs by putting choice in the hands of employees. Give the level of convenience, access, security, and management that makes sense for their work style.
  - Enable flexible application access policies, allowing some applications to be used prior to enrollment into device management, while requiring full enrollment for apps that require higher levels of security.
  - Provision, deliver, update, and retire applications in real time.

- **Secure productivity apps: Mail, Calendar, Docs, and Social**
  - Employees can use the included mail, calendar, contacts, documents, chat, and enterprise social capabilities while policy-based security measures protect the organization from data leakage by restricting how attachments and files can be edited and shared.

- **Data Security and endpoint compliance with Conditional Access**
  - Combining identity and device management, Workspace ONE can enforce access decisions based on a range of conditions including strength of authentication, network, location, and device compliance.
  - Policy controls ensure that IT can protect against compromised devices.

- **Real-time app delivery and automation**
  - Taking advantage of new capabilities in Windows, Workspace ONE allows desktop administrators to automate application distribution and updates. This automation, combined with virtualization technology, helps ensure application access as well as improve security and compliance.
Platform Integration
Workspace ONE is comprised of several core components: VMware Identity Manager, VMware AirWatch, and the Workspace ONE native apps.

VMware Identity Manager provides the identity-related components of the solution. This includes authentication using username password, 2FA, certificate, Kerberos, mobile SSO, and inbound SAML from third-party VMware Identity Manager systems. It also provides SSO to entitled apps where the apps can be either Web apps or Windows apps and desktops delivered through Horizon or Citrix.

AirWatch delivers the enterprise mobility management portion of the solution. AirWatch enables device enrollment through profiles defined to enable configuration and control of users’ devices. It also enables a mobile application catalog to publish public or internally developed applications to end users. Compliance policies can also be developed to alert administrators to compromised devices, or perform a device wipe on a device that is running unapproved applications. AirWatch can also be integrated to enterprise directories such as Active Directory for authentication and user management. In order to facilitate mobile productivity, AirWatch can integrate with email systems and content repositories.

The Workspace ONE native app is available for iOS, Android and Windows 10 devices. The app consolidates the AirWatch and VMware Identity Manager catalogs into a single catalog to bring native mobile, SaaS-based, and virtual apps and desktops to users in a simple manner, and through single sign-on technology, makes it easy for users to access the applications they need.

Workspace ONE supports adaptive management that allows users to download and use less critical apps from the Workspace ONE catalog. If the user downloads a critical app from the catalog, the user is asked to go through the device enrollment process right from within Workspace ONE. With the device enrolled, a higher degree of control and security makes it possible for the user to access a greater range of apps and data.
Business Drivers and Use Cases Definition
A solution based on VMware Workspace ONE can address a wide-ranging set of business requirements and use cases. In this particular reference architecture, the solution targets the most common requirements and use cases as seen in customer deployments to date. These should be easily modified to fit differing circumstances.

Business Drivers and Requirements
Any technology solution should directly address critical business requirements and drivers. Each and every design choice should center on a specific business requirement. Business requirements could be driven by the “end user” or by the team deploying EUC services. The top-8 common key business drivers addressed by Workspace ONE are:

• Provide greater “business mobility” by providing mobile access to modern and legacy applications via laptop, tablet, and smartphone.
• Reduce user support calls and incidents by simplifying and securing access to applications.
• Allow fast provisioning of and secure access for internal users and third-party suppliers to line-of-business applications.
• Centralize management and security of corporate devices to meet compliance standards.
• Reduce application management overhead and application provisioning time.
• Simplify root cause analysis and time to resolution of user issues.
• Provide a comprehensive and flexible platform for device deployment and management.
• Allow users to access corporate applications, especially Office 365, and corporate data from their own devices.
Use Cases

Use cases drive the design for any EUC solution and dictate which technologies are deployed to meet user requirements. Use cases can be thought of as common user scenarios; for example, a finance or marketing user may be considered a “mobile knowledge worker” use case. Some common use cases are described here.

<table>
<thead>
<tr>
<th>USE CASE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Task-Based Worker   | Task-based workers are those users who typically use a mobile device for a single task through a single application. These applications might include inventory control, product delivery, or retail tools. A device in this category is usually very locked down and presents only apps required for the task.  
  • Uses a mobile highly managed device for a small number of tasks, such as inventory control, product delivery, or retail applications.  
  • Communications tools such as email might be restricted to only sending and receiving email with internal parties.  
  • Device is typically locked down with unnecessary applications, games, and access to public app stores restricted or removed entirely.  
  • Device location, full device wipe, and other features are typical of this profile.                                                                 |
| Mobile Knowledge Worker | A mobile knowledge worker could be a hospital clinician or a company employee in finance or marketing. Many roles in an organization would fit this profile.  
  • User could be using their own personal device (BYOD), a corporate device they personally manage, or a managed corporate device with low restrictions.  
  • Typically allowed to access email, including personal email, along with public app stores for personal apps.  
  • Likely subject to information controls over corporate data—DLP controls, managed email, managed content, and secure browsing.  
  • Needs access to SaaS-based applications for HR, finance, health benefits, approvals, and travel, as well as native applications where those apps are available.  
  • A great candidate for single sign-on as the need to access many diverse apps and passwords becomes an issue for users and help desk.  
  • Privacy is typically a concern that might prevent device enrollment, so adaptive management and clear communication as to data gathered and reported to AirWatch is important to encourage adoption. |
| Contractor          | An external contractor can require access to specific line-of-business applications, typically from a remote or mobile location.  
  • Likely needs access to an organization’s system for performing specific functions and applications, but access might be of finite time period, to a subset of resources and applications.  
  • When no longer affiliated with the organization, all access to systems must be terminated immediately and completely, and all corporate information removed from device.  
  • Typically needs access to virtual apps or VDI-based desktops and might use multiple devices not under company control to do so. Includes mobile devices as well as browser-based devices. |

Table 1: Common Use Cases
Meeting Business Requirements with Workspace ONE  

Any technology implementation will have business requirements justifying the time and expense of putting a new set of capabilities in place. For a mobile deployment, there are obviously many reasons an enterprise would consider a Workspace ONE deployment. Some of the typical business requirements are described in Table 2.

<table>
<thead>
<tr>
<th>BUSINESS DRIVER</th>
<th>WORKSPACE ONE SOLUTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile access</td>
<td>Workspace ONE is designed to provide a “consumer-simple, enterprise-secure” method of accessing all types of applications end users might need from a wide variety of platforms. It is the first solution that brings together identity, device management, application catalogs, and mobile productivity.</td>
</tr>
<tr>
<td>Reduced support calls</td>
<td>Integration with VMware Identity Manager and AirWatch provides single sign-on (SSO) capabilities to a wide range of platforms and applications. By leveraging SSO technology, password resets become unnecessary.</td>
</tr>
<tr>
<td>Fast provisioning and access</td>
<td>Workspace ONE can support a wide range of device access scenarios, simplifying the onboarding of end-user devices. Adaptive management allows a user to download an app from a public app store, and access some published applications. If they need to access more privileged apps, then they are prompted to enroll their device from within the app itself rather than via an agent.</td>
</tr>
<tr>
<td>Centralize and secure</td>
<td>AirWatch provides aggregation of content repositories including SharePoint, network file shares, and cloud services. Files from these repositories can then be synced to AirWatch Content Locker for viewing and secure editing. AirWatch policies may also be established to prevent distribution of corporate files in order to control where files can be opened and by which apps, as well as prevent such functions as copy/paste into other apps or printing.</td>
</tr>
<tr>
<td>Reduce application management</td>
<td>By providing end users with a single application catalog for native mobile, SaaS, and virtualized applications, application management can be significantly improved. While both VMware Identity Manager and AirWatch have their own app catalogs, the end user only sees the consolidated catalog in the Workspace ONE app.</td>
</tr>
<tr>
<td>Improve time to resolution</td>
<td>Both AirWatch and VMware Identity Manager include dashboards and analytics that can help users understand what a profile of application access and device deployment looks like in the enterprise. Knowledge of which applications users are accessing can help identify issues with licensing or even potential attempted malicious activities against enterprise apps.</td>
</tr>
<tr>
<td>Comprehensive and flexible platform for corporate-owned or BYOD strategies</td>
<td>The flexibility of BYOD can introduce challenges for enterprise IT related to device management. Workspace ONE and features like adaptive management can simplify end-user enrollment and empower application access in a secure fashion to drive user adoption.</td>
</tr>
</tbody>
</table>

Table 2: Business Drivers and Workspace ONE Solutions
Workspace ONE Services Definition

From our business requirements we outlined several typical use cases and their requirements. Taking the business requirements and combining them with a use case(s) enables the definition of a service.

The service defines the unique requirements and identifies the technology or feature combinations that will satisfy those unique requirements. After the service has been defined, you can define the service quality that will be associated with that service. This will include performance, availability, security, management, and monitoring requirements to meet with SLAs.

**The remainder of this document will detail the design to satisfy each of the service definitions.**

Do not treat the list of services as exclusive or prescriptive; each environment is different. Adapt the services to the particular use cases. In some cases, that may mean adding additional components while in others it may be possible to remove some that are not required. You could also look to combine multiple services together to address more complex use cases.

The following are core components that are referenced in these use cases.

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>FUNCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware AirWatch</td>
<td>Enterprise mobility management</td>
</tr>
<tr>
<td>VMware Identity Manager</td>
<td>Identity platform</td>
</tr>
<tr>
<td>Workspace ONE app</td>
<td>End-user access to apps</td>
</tr>
<tr>
<td>VMware Horizon 7</td>
<td>Virtual desktops and RDS remoted apps</td>
</tr>
<tr>
<td>Boxer/AirWatch Inbox</td>
<td>Secure email clients</td>
</tr>
<tr>
<td>AirWatch Browser</td>
<td>Secure Web browser</td>
</tr>
<tr>
<td>AirWatch Content Locker</td>
<td>Mobile content repository</td>
</tr>
<tr>
<td>AirWatch Cloud Connector™</td>
<td>Directory sync to enterprise directories</td>
</tr>
<tr>
<td>VMware Identity Manager Connector</td>
<td>Directory sync to enterprise directories</td>
</tr>
</tbody>
</table>

*Table 3: Core Components*
Mobile Device Management Service

**Overview:** Many organizations have deployed mobile devices and have lightweight management capabilities today. These capabilities might include simple email deployment and device policies such as a PIN requirement, device timeouts, and device wipe capabilities, but lack a more comprehensive and complete management practice to enable a consumer-simple, enterprise-secure model for devices.

**Use Cases:** Static Task Worker

<table>
<thead>
<tr>
<th>UNIQUE REQUIREMENTS</th>
<th>COMPONENTS</th>
</tr>
</thead>
</table>
| Provide device management beyond simple policies | • Workspace ONE native app  
• VMware Identity Manager authentication  
• AirWatch Cloud Connector                     |
| Enable adaptive management capabilities   | • Workspace ONE native app  
• Adaptive management  
• Workspace services device enrollment       |

**Blueprint**

*Figure 5: Mobile Device Management Service Blueprint (Dimmed boxes are not needed for this service.)*
Mobile Productivity Service

**Overview:** Organizations with a more evolved device management strategy are often pushed by end users to enable more advanced mobility capabilities in their environment. This includes tools like single sign-on, multifactor authentication, and access to productivity tools. From an enterprise perspective, however, providing this much access to corporate information means a greater degree of control must be instituted. This includes blocking native email clients in favor of managed email, requiring synced content into approved repositories, and managing which apps can be used to open files.

**Use Cases:** Mobile Knowledge Worker, Contractors

<table>
<thead>
<tr>
<th>UNIQUE REQUIREMENTS</th>
<th>COMPONENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multifactor authentication</td>
<td>• VMware Verify</td>
</tr>
<tr>
<td>Single sign-on</td>
<td>• VMware Identity Manager and AirWatch</td>
</tr>
<tr>
<td>Managed email</td>
<td>• Boxer and AirWatch Inbox</td>
</tr>
<tr>
<td>Enterprise content synchronization</td>
<td>• AirWatch Content Locker</td>
</tr>
<tr>
<td>Secure browsing</td>
<td>• AirWatch Browser</td>
</tr>
</tbody>
</table>

**Blueprint**

*Figure 6: Mobile Productivity Service Blueprint (Dimmed boxes are not needed for this service).*
Mobile Application Workspace Service

**Overview:** Recognizing that some applications will not be available as a native app on a mobile platform and that some security requirements might dictate on-premises application access, virtualized applications and desktops become a core part of a mobility strategy. Building on the mobile productivity service, and adding access to Horizon-based resources, enables this scenario.

There are also many current VMware Horizon customers who will benefit by adding the Workspace ONE catalog capabilities as a single, secure point of access for their virtual desktops and applications.

**Use Cases:** Contractor, Mobile Knowledge Worker

<table>
<thead>
<tr>
<th>UNIQUE REQUIREMENTS</th>
<th>COMPONENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to virtual apps and desktops</td>
<td>• Horizon 7 and RDS applications</td>
</tr>
<tr>
<td></td>
<td>• Identity Manager Connector</td>
</tr>
</tbody>
</table>

**Blueprint**

![Mobile Application Workspace Service Blueprint](image)

*Figure 7: Mobile Application Workspace Service Blueprint (Dimmed boxes are not needed for this service.)*
Architecture Principles and Concepts

The Workspace ONE platform is comprised of VMware Identity Manager and VMware AirWatch. While each of these products can operate independently, it is the integration of the two of them that enables the Workspace ONE product to function. Both VMware Identity Manager and AirWatch are available as on-premises and cloud-hosted products.

As more organizations embrace cloud technologies, due to the benefits of constantly updated software and lower management overhead, new deployments of Workspace ONE are recommended as cloud hosted. Other customers who might have VMware Identity Manager or AirWatch deployed on premises can take advantage of the latest versions of the software and deploy Workspace ONE.

Advantages of a cloud-hosted implementation of VMware Identity Manager and AirWatch include:

• Highly available platforms
• Regional availability across the globe
• Highly scalable to the largest enterprise organization requirements
• Lower CapEx expenditures
• Highest level of security monitoring and immediate patching
• Availability of latest software innovations

Some features of both platforms might initially be available only in cloud-hosted deployments. Typically, those features will be made available in the on-premises version shortly afterwards.

For this document, the approach taken will be to use cloud-hosted AirWatch and VMware Identity Manager, with on-premises Horizon 7 for the Mobile Workspace Service.
AirWatch and VMware Identity Manager Integration

Figure 8: Sample Workspace ONE Architecture
VMware Identity Manager and AirWatch have been built to provide tight integration between identity and device management. This integration has been simplified in recent versions to ensure that configuration of each product is relatively simple. Comprehensive documentation is available to highlight the exact steps in integration.

While VMware Identity Manager and AirWatch can be considered the core components in a Workspace ONE deployment, there are a variety of other components that could potentially be deployed depending on the business use cases. In Figure 8, the Secure Email Gateway might be used for access to an on-premises Exchange Server, or the AirWatch Tunnel™ Server or VMware Access Point 2.7 might be used to provide VPN-based access to internal resources. Refer to the My AirWatch Web site resources for documentation of the full range of components that might apply to a deployment.

There are many other enterprise components that would typically be integrated into a Workspace ONE deployment. These components include technologies such as a Certificate Authority, Active Directory, file services, email systems, SharePoint servers, external access servers, or reverse proxies. This document assumes that these enterprise systems are in place and functional if they are necessary.

**Workspace ONE Logical Components and Concepts**

In implementing Workspace ONE, a number of components can be deployed either on premises or cloud hosted. There are also a number of key concepts around device management, security and compliance, and application access that should be understood.

- **Workspace ONE native mobile apps** – Native apps available for iOS, Android, and Windows 10 that present a unified application catalog across VMware Identity Manager resources and native mobile apps, allow ease of finding and installing enterprise apps, and provide a single sign-on experience across resource types.

- **AirWatch SaaS tenant** – Cloud-hosted instance of the AirWatch service. AirWatch acts as the mobile device management (MDM), mobile content management (MCM), and mobile application management (MAM) platform.

- **AirWatch Cloud Connector** – The AirWatch Cloud Connector (ACC) provides organizations the ability to integrate AirWatch with their back-end enterprise systems. The ACC runs in the internal network, acting as a proxy that securely transmits requests from AirWatch to the organization’s critical enterprise infrastructure components. This allows organizations to leverage the benefits of AirWatch Mobile Device Management (MDM), running in any configuration, together with those of their existing LDAP, certificate authority, email, and other internal systems.

- **VMware Identity Manager tenant** – Cloud-hosted instance of the VMware Identity Manager. VMware Identity Manager acts as an identity provider by syncing with Active Directory to provide single sign-on across SAML-based applications, Horizon-based apps and desktops, and ThinApp packaged apps. It is also responsible for authentication policy based on networks, applications, or platforms.

- **VMware Identity Manager Connector** – Virtual appliance responsible for directory sync and authentication between an on-premises Active Directory and the VMware Identity Manager service.

- **Device enrollment** – Process by which a device is brought under management in an AirWatch environment. Enrollment allows the device to be managed, device profiles and applications distributed, content delivered or removed. Enrollment also allows extensive reporting based on the devices check in to the AirWatch service.

- **Adaptive management** – Process by which an end user can install the Workspace ONE app on a device and log in with credentials giving access to some applications without device enrollment. Other applications will require device enrollment, and the Workspace ONE app can initiate enrollment for the user.
• **Mobile SSO** – One touch single sign-on technology available for all platforms that Workspace ONE is supported on. The implementation on each OS is based on features provided by the underlying OS. For iOS, this uses technology known as the Cloud KDC. For Android, the authentication method is called Android SSO. And for Windows 10, it is called Cloud Certificate.

• **Resource types (SaaS apps, native mobile, virtual desktops and apps)** – Workspace ONE supports a variety of applications exposed through the VMware Identity Manager and AirWatch catalogs. This include SaaS-based SAML apps, Horizon apps and desktops, and ThinApp packaged apps delivered through VMware Identity Manager, and native mobile applications through the AirWatch catalog.

• **Unified application catalog** – The unified application catalog is the combined VMware Identity Manager and AirWatch application catalogs presented within the Catalog tab of the Workspace ONE app.

• **Email integration** – AirWatch supports integration with email services, most commonly Microsoft Exchange as well as GroupWise, Notes, and Google Apps for Work. There are three different ways to integrate email: through a server component called the Secure Email Gateway (SEG), through Direct PowerShell integration, or Direct Google Apps for Work integration. The SEG requires a server to be configured in the data center, while PowerShell integration does not require a server, but directly communicates with Exchange ActiveSync on the Exchange 2010 or later or Office 365.

• **Content integration** – The AirWatch Mobile Content Management (MCM) solution helps organizations address the challenge of securely deploying content to a wide variety of devices using a few key actions. Leverage the AirWatch Admin Console to create, sync, or enable a file store known as a repository. After configured, this content deploys to end-user devices with the AirWatch Content Locker. Access to content can be either read-only or read/write.

• **Conditional access** – Both VMware Identity Manager and AirWatch have ways to evaluate compliance. When users enroll their devices through the AirWatch Agent application, samples containing data used to evaluate compliance are sent on a scheduled basis. The evaluation of this sample data ensures that the device meets the compliance rules set by the administrator in the AirWatch console. If the device goes out of compliance, the corresponding actions configured in the AirWatch console are taken.

VMware Identity Manager includes an access policy option that can be configured to check the AirWatch server for device compliance status when users sign in from the device. The compliance check ensures that users are blocked from signing in to an application or using single sign-on to the VMware Identity Manager portal if the device goes out of compliance. When the device is compliant again, the ability to sign in is restored. This can be enforced based on the network the user is on, the platform they are using, or applications being used.

• **Secure browsing** – Use of the AirWatch Browser instead of the native browser or third-party browser to ensure that access to sensitive Web content is secure and manageable.

• **Data Loss Prevention (DLP)** – Ability to force documents or URLs to only be opened in approved applications to prevent accidental or purposeful distribution of sensitive information.

• **VMware Verify** – Multifactor authentication solution to enable use of an iOS, Android, or Chrome-based app, with a one-time password or SMS message as an additional factor when accessing resources through VMware Identity Manager.

• **Horizon 7** – Infrastructure for VDI and published desktops (VDI or RDS-based desktops published through VMware Horizon) and published apps (virtual applications published through VMware Horizon).

• **VMware Access Point** – Virtual appliance that allows Internet-based devices to access resources hosted on Horizon servers.

The next section of this guide details the design of each of these components.
Workspace ONE Component Design

To be able to deliver the Workspace ONE services outlined above and to address the use cases, we first need to design and build out the infrastructure components required.

This section includes a low-level design of each of the products or areas that need to be considered. This is not an exhaustive design or installation guide and it is recommended that you also refer to the installation guides.

Workspace ONE Native Mobile Apps

The end-user experience for a Workspace ONE deployment will likely be for many users via the Workspace ONE native mobile app. Available for each operating system, the Workspace ONE app allows users to leverage the best technologies on each respective platform for a delightful user experience, at the same time as it presents a consistent look and feel across mobile apps as well as a browser. As a native app, features like TouchID on an iOS device, or Windows Hello on Windows 10, can be used.

The app provides:

- A unified app catalog comprised of VMware Identity Manager and AirWatch application types that have been enabled for a user or a device.
- A launcher to access SaaS- and Horizon-based virtual desktops and apps, and ThinApp packaged apps, making discovery easy for end users.
- Search functionality to search across an enterprise’s entire deployment of app resources to find apps.
- Single sign-on technology to allow simple user access to resources without the need to remember multiple passwords for every site.

Figure 9: Workspace ONE for Windows 10
The Workspace ONE native app is available from the respective app stores for users to download on their own devices, and can be deployed through AirWatch as part of a device enrollment process. Many other features of the Workspace ONE native app are discussed in detail as they are enabled due to the features found in AirWatch and VMware Identity Manager to make up the solution.

**VMware Identity Manager**

VMware Identity Manager provides a number of key capabilities for Workspace ONE implementations. Among them are:

- **A portal**, branded as Workspace ONE, which provides browser-based access to different types of applications including SaaS-based Web applications (such as Salesforce.com, Dropbox, Concur, and many others), Horizon-based applications and desktops, RDSH-based applications and desktops, ThinApp packaged apps, and Citrix-based applications and desktops. The portal is designed to make application access simple for end users.

- **Enterprise identity management** to sync and extend Active Directory environments to SaaS and native mobile applications.

- **Enterprise single sign-on** to ensure that users have a single identity to log in with for internal, external, and virtual-based applications.

- **A self-service app store**, to allow end users to identify and be entitled to applications in a simple way, while providing enterprise security and compliance controls to ensure the right users have access to the right applications.

![Figure 10: User Workspace Delivered by VMware Identity Manager](image-url)
**Design Overview**

VMware Identity Manager can be implemented using on-premises or SaaS-based implementation models. In an on-premises implementation, a VMware Identity Manager virtual appliance is used to handle authentication and provides single sign-on services to applications and desktops. In a SaaS-based implementation, a VMware Identity Manager Connector virtual appliance is used to synchronize user accounts from Active Directory to the VMware Identity Manager Service. Applications can then be accessed from a browser-based portal. Multiple appliances can be used on premises for redundancy and scale.

As of the VMware Identity Manager 2.7 release (June 2016) the SaaS-based implementation allows access to Horizon-based desktops and applications. This requires the use of the VMware Identity Manager Connector appliance, which will be used in the Mobile Application Workspace Service.

![Figure 11: VMware Identity Manager Logical Design with VMware Identity Manager Connector for Horizon Access](image)

**Design Decision:** With the inclusion of access to Horizon-based resources, this document will detail the use of a SaaS-based VMware Identity Manager implementation.

**Install and Initial Configuration**

Because the VMware Identity Manager tenant is cloud based, there are no design decisions to be made regarding database, network access, or storage considerations. The VMware Identity Manager service is able to scale to accommodate virtually any size organization.

Connectivity to the VMware Identity Manager service will be through outbound port 443 connections. This connection will be used for directory synchronization and authentication, as well as syncing of entitlements for resources such as View desktops and apps. Organizations can take advantage of this configuration with no additional inbound firewall ports opened to the Internet.
Initial configuration will involve logging into the VMware Identity Manager service with the provided credentials at a URL similar to https://<company>.vmwareidentity.com.

For information on VMware Identity Manager SaaS-based implementation, see the VMware Identity Manager Documentation. Note that there are multiple versions of the documentation. Select VMware Identity Manager Cloud from the drop-down menu.

Next Steps
Integrate VMware Identity Manager and AirWatch

Because Workspace ONE uses VMware Identity Manager for authentication, and SaaS and Horizon application access, and uses AirWatch for device enrollment and management, the products must be integrated. The integration process is documented in Architecture Principles and Concepts.

AirWatch

AirWatch is one of the key pillars of a Workspace ONE implementation. It is responsible for device enrollment, a mobile application catalog, policy enforcement regarding device compliance, as well as integration with key enterprise services such as email, content, and social media. AirWatch is available as an on-premises or cloud-hosted product. AirWatch features include:

- **A device management platform** allowing full lifecycle management of a wide variety of devices, including phones, tablets, and ruggedized and special-purpose devices.
- **Application deployment capabilities** providing automatic deployment or self-service application access for employees.
- **User and device profile services** to ensure that users and devices are subject to configuration according to the needs of the enterprise to ensure compliance with security requirements and simplify end-user access to applications.
- **Productivity tools** including an email client providing secure email functionality, a content management tool for securely storing and managing content, a Web browser to ensure secure access to corporate information and tools, and enterprise social media applications for collaboration and chat.

![AirWatch Administrator Console](image-url)
**Design Decision:** For this design, AirWatch will be implemented in a cloud-hosted model. This ensures that the latest AirWatch features can be used without the need to upgrade on-premises infrastructure.

**Installation and Initial Configuration**

Because AirWatch is being implemented as a cloud-based offering, installation of on-premises servers is not necessary for the core AirWatch services. An AirWatch tenant will be provisioned, and an email will be provided with details of the tenant name and login credentials. Initial configuration will be accomplished by logging in with provided credentials to the tenant, which will have a naming convention similar to [https://<companyname>.awmdm.com](https://<companyname>.awmdm.com) and can be redirected to a custom URL if needed.

Initial configuration of the AirWatch environment is beyond the scope of this document. It assumes that at least a basic functional tenant has been configured. For information on getting started with AirWatch, see the most recent VMware AirWatch Mobile Device Management Guide in AirWatch Resources.

After initial configuration, integration and directory sync will be implemented using the appropriate connector between the enterprise directory and AirWatch and VMware Identity Manager services.

**Next Steps**

*Integrate VMware Identity Manager and AirWatch*

Because Workspace ONE uses VMware Identity Manager for authentication and SaaS and Horizon application access and uses AirWatch for device enrollment and management, the products must be integrated. The integration process is documented in Architecture Principles and Concepts.

**AirWatch Cloud Connector and VMware Identity Manager Connector**

**Design Overview**

An important design choice in configuring a Workspace ONE environment is the directory synchronization and authentication strategy to an enterprise directory. This allows an administrator to manage user accounts in Active Directory, have those accounts reflected in AirWatch and VMware Identity Manager, and to handle authentication to prevent the storage or synchronization of passwords outside of the enterprise.

There are two options for connecting AD to AirWatch and VMware Identity Manager: the AirWatch Cloud Connector (ACC) and the VMware Identity Manager Connector. While both connectors offer similar scale and high availability options, there are some features associated with each connector that will guide a design decision toward one connector.

<table>
<thead>
<tr>
<th><strong>AIRWATCH CLOUD CONNECTOR</strong></th>
<th><strong>VMWARE IDENTITY MANAGER CONNECTOR</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Advantages</strong></td>
<td><strong>Advantages</strong></td>
</tr>
<tr>
<td>• One connector used by both AirWatch and VMware Identity Manager</td>
<td>• Horizon on-premises support</td>
</tr>
<tr>
<td>• Lightweight setup, only 11.6 MB download and install on Windows server</td>
<td>• Supports all authentication methods including integrated Windows Authentication</td>
</tr>
<tr>
<td><strong>Disadvantages</strong></td>
<td><strong>Disadvantages</strong></td>
</tr>
<tr>
<td>• Does not support on-premises Horizon, ThinApp packaged apps, and Citrix</td>
<td>• Requires VMware vCenter™ to deploy</td>
</tr>
<tr>
<td>• Does not support third-party 2FA using RADIUS integration and Kerberos Integrated Windows Authentication SSO from domain-joined Windows machines</td>
<td>• More complicated configuration than ACC</td>
</tr>
</tbody>
</table>

*Table 4: Connector Comparison Between AirWatch Cloud Connector and VMware Identity Manager Connector*
ACC Design Considerations

The ACC is installed on a Windows Server on premises after downloading from the AirWatch console.

<table>
<thead>
<tr>
<th>REQUIREMENT</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM or physical server</td>
<td>1 CPU core (2.0+ GHz)*</td>
</tr>
<tr>
<td></td>
<td>*An Intel processor is required.</td>
</tr>
<tr>
<td></td>
<td>2 GB RAM or higher</td>
</tr>
<tr>
<td></td>
<td>1 GB disk space for the ACC application, Windows OS, and .NET runtime. AirWatch recommends an additional 5 GB of disk space for use with logging.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NUMBER OF USERS</th>
<th>UP TO 10,000</th>
<th>10,000 – 50,000</th>
<th>50,000 – 100,000</th>
<th>100,000 – 200,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU cores</td>
<td>2</td>
<td>2 load-balanced servers with 2 CPU cores</td>
<td>2 to 3 load-balanced servers with 2 CPU cores</td>
<td>2 load-balanced servers with 4 CPU cores</td>
</tr>
<tr>
<td>RAM (GB) per server</td>
<td>4</td>
<td>4</td>
<td>8</td>
<td>16</td>
</tr>
</tbody>
</table>

Table 5: ACC Specifications

Server Requirements

ACC supports installation on the following Windows Server versions:

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

ACC also requires installation of .NET Framework 4.5.2.

Network Requirements

All traffic from the ACC is outbound from the ACC server to the AirWatch service and occurs over ports 80 or 443.

An outbound proxy or any other connection management software or hardware must not terminate or reject the outbound connection from the ACC. The outbound connection required for use by ACC must remain open at all times.

Additional details on the ACC can be found in the most recent VMware AirWatch Cloud Connector (ACC) Guide for SaaS Customers in AirWatch Resources.

Load Balancing and Availability

ACC traffic is automatically load-balanced by the AirWatch Cloud Messaging (AWCM) component. It does not require a separate load balancer. Multiple ACCs in the same organization group that connect to the same AWCM server for high availability can all expect to receive traffic (an active-active configuration). How traffic is routed is determined by AWCM and depends on the current load.
VMware Identity Manager Connector Design Considerations

The VMware Identity Manager Connector is deployed as a virtual appliance through the vSphere Client or the vSphere Web Client. It requires versions 5.0 U2 and later of vSphere and VMware ESXi™.

System Requirements

The virtual appliance has the following minimum system requirements:

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>MINIMUM REQUIREMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>2</td>
</tr>
<tr>
<td>RAM</td>
<td>6 GB</td>
</tr>
<tr>
<td>Storage</td>
<td>24 GB</td>
</tr>
</tbody>
</table>

Table 6: VMware Identity Manager Connector System Requirements

Networking Considerations

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>MINIMUM REQUIREMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS and IP address</td>
<td>Must have forward and reverse DNS entries and an IP address for virtual appliance.</td>
</tr>
<tr>
<td>Firewall port</td>
<td>Make sure that the outbound firewall port 443 is open from the connector instance to the vmwareidentity.com URL. As of the June 2016 release of the VMware Identity Manager service, all traffic from the connector to the service can be configured to be outbound-only.</td>
</tr>
<tr>
<td>Storage</td>
<td>24 GB</td>
</tr>
</tbody>
</table>

Table 7: VMware Identity Manager Connector Networking Considerations

Full configuration information regarding communication ports, IP addresses for whitelisting, and addresses for the VMware Identity Manager service can be found in System and Network Configuration Requirements in VMware Identity Manager Connector Installation and Configuration.

Load Balancing and Availability

Configure the connector for failover and redundancy by deploying multiple connector virtual appliances in a connector cluster that is fronted by a load balancer. If one of the appliances shuts down, the connector is still available.

To set up failover, first install and configure the first connector virtual appliance, create a directory that uses it as the identity provider, and add the connector to the load balancer. Then deploy additional connector appliances and associate them with the Identity Provider page of the first connector, before adding them to the load balancer. As a result, multiple connector appliances are all associated with the same directory.
After setting up failover, the connector is highly available. Traffic is distributed to the connector virtual appliances in the cluster based on the load-balancer configuration. Specifically, authentication is highly available. If one of the connector instances shuts down, authentication is still available because one of the other connector instances is used. For directory sync, however, in the event of a connector instance failure, you will need to manually select another connector instance as the sync connector. This is because directory sync can only be enabled on one connector at a time.

More information can be found in Configuring Failover and Redundancy for Connector Appliances in VMware Identity Manager Connector Installation and Configuration.

Active Directory Server Support

**Key Design Considerations**
A key design consideration is whether or not Horizon-based apps and desktops will be deployed as part of a Workspace ONE implementation. If Horizon apps and desktops will be used, then the VMware Identity Manager connector must be used, as the ACC does not have support for those resources. If Horizon resources will not be accessed, the ACC is the recommended approach for deployment. Only one connector is necessary for sync and authentication.

**Design Decision:** The mobile management service and the mobile productivity service are primarily mobile scenarios, so for these scenarios we will be implementing the ACC for directory sync and authentication. For the mobile application workspace scenario, since we have Horizon resources to access, we will be implementing the VMware Identity Manager connector and using SAML authentication from AirWatch to the VMware Identity Manager user directory.

**Email Integration**
Workspace ONE allows for flexibility of choice when it comes to devices and email clients. While this allows a user to choose the client they prefer, it also potentially opens the enterprise up to data leakage due to a lack of control over what happens to email messages after they reach a device. In order to address these considerations, AirWatch supports multiple methods of connecting email infrastructure to devices.

One challenge in this area is that many organizations are moving to cloud-based email services, such as Office 365 and Google Apps for Work, and these services provide fewer email control options than the on-premises models the enterprise has worked with in the recent past. Previously, the Secure Email Gateway (SEG) would have been deployed inside a corporate firewall and handled many aspects of secured email delivery to devices. Now, modern methods such as direct PowerShell integration to an Exchange Server or Office 365 offer simpler connectivity, but with somewhat less control over email delivery and compliance.

In the next section, we will look at the models for connectivity and the pros and cons of each.
Secure Email Gateway Proxy Model
The Secure Email Gateway (SEG) Proxy server is a separate server installed in-line with your existing email server to proxy all email traffic going to mobile devices. Based on the settings you define in the AirWatch Admin Console, the SEG Proxy server makes allow or block decisions for every mobile device it manages. The SEG Proxy server relays traffic only from approved devices. This relay protects the corporate email server by not allowing any devices to directly communicate with it. Instead, the SEG Proxy server filters all communication requests to the corporate email server.

Figure 13: Secure Email Gateway Architectures
Direct PowerShell Model
In the PowerShell model, AirWatch adopts a PowerShell administrator role and issues commands to the Exchange ActiveSync (EAS) infrastructure to permit or deny email access based on the policies defined in the AirWatch Admin Console. PowerShell deployments do not require a separate email proxy server and the installation process is simpler.

Figure 14: Office 365 Email Architecture

Supported Email Infrastructure and Models

<table>
<thead>
<tr>
<th>DEPLOYMENT MODEL</th>
<th>CONFIGURATION MODE</th>
<th>MAIL INFRASTRUCTURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy model</td>
<td>Secure Email Gateway (proxy)</td>
<td>Microsoft Exchange 2010, 2013, 2016 IBM Domino with Lotus Notes Novel GroupWise (with EAS) Google Apps for Work</td>
</tr>
<tr>
<td>Direct model</td>
<td>PowerShell model</td>
<td>Microsoft Exchange 2010, 2013, 2016 Microsoft Office 365</td>
</tr>
<tr>
<td>Direct model</td>
<td>Google model</td>
<td>Google Apps for Work</td>
</tr>
</tbody>
</table>

Table 8: Supported Email Deployment Models

Office 365 requires additional configuration for the SEG proxy model. AirWatch recommends the Direct model of integration with cloud-based email servers.
Table 9 summarizes the pros and cons of the deployment features of SEG and PowerShell to help you choose which deployment is most appropriate.

<table>
<thead>
<tr>
<th></th>
<th>PROS</th>
<th>CONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEG</td>
<td>Real-time compliance</td>
<td>Additional server(s) needed</td>
</tr>
<tr>
<td></td>
<td>Attachment encryption</td>
<td>ADFS must be configured to prevent end users from directly connecting to Office 365 (around SEG)</td>
</tr>
<tr>
<td></td>
<td>Hyperlink transformation</td>
<td></td>
</tr>
<tr>
<td>PowerShell</td>
<td>No additional on-premises servers required for email management</td>
<td>No real-time compliance sync</td>
</tr>
<tr>
<td></td>
<td>Mail traffic is not routed to on-premises servers before being routed to Office 365, so AFS is not required</td>
<td>Not recommended for larger deployments (larger than 100,000 devices)</td>
</tr>
</tbody>
</table>

**Table 9: SEG and PowerShell Feature Comparison**

**Key Design Considerations**

AirWatch recommends using the Secure Email Gateway (SEG) for all on-premises email infrastructures with deployments of more than 100,000 devices. For deployments of less than 100,000 devices, or cloud-based email, PowerShell is another option for your email management.

Full design considerations for mobile email management can be found in the most recent VMware AirWatch Mobile Email Management Guide in AirWatch Resources.

**Design Decision:** Because this design includes Office 365-based email, the PowerShell model will be used and the AirWatch Inbox will be used for mail. While this decision limits employee choice of mail client and removes native email access in the mobile productivity service, it provides the best protection available against data leakage of corporate information.

**Next Steps**

- Configuration of Office 365 email through PowerShell
- Configuration of AirWatch Inbox as an email client for deployment as part of device enrollment
Content Integration

Mobile content management (MCM) can be a critical component to a device deployment. Taking care to ensure that content is safely stored in enterprise repositories, available to end users when and where they need it, with appropriate security controls, is paramount. The MCM features found in AirWatch present a flexible means of providing users with the content they need matched with the security control the enterprise requires.

Content Management Overview

1. **AirWatch Managed Content Repository** – Refers to a repository where AirWatch Administrators with the appropriate permissions can upload content to and have complete control over the files that get stored within it.
2. **Corporate File Server** – Refers to a preexisting repository that resides within an organization’s internal network or a cloud service. Depending on an organization’s structure, the AirWatch Administrator may or may not have administrator permissions for the corporate file server.
3. **AirWatch Content Locker** – Refers to the app that deploys to end-user devices, enabling access to content within the configured set of parameters.
4. **Personal Content Repository** – Refers to a location where end users have complete control over the files that get stored within it. End users add Personal Content Repository files on their devices with AirWatch Content Locker, from any supported Web browser with the Self-Service Portal, and from their personal computer with AirWatch Content Locker Sync.

Figure 15: Mobile Content Management with AirWatch
AirWatch Content Locker can be integrated with a large number of corporate file services, including, but not limited to, Box, Google Drive, Network Shares, OneDrive, OneDrive for Business, OneDrive for Business via ADFS, SharePoint, SharePoint via ADFS, SharePoint Office 365, SharePoint Personal (My Sites), and most WebDAV supporting sites. It would be beyond the scope of this document to highlight all of them.

Full design considerations for mobile content management can be found in the most recent VMware AirWatch Mobile Content Management Guide in AirWatch Resources.

### Data Protection in AirWatch Content Locker

AirWatch Content Locker provides a considerable amount of control over the types of activities that a user can perform with documents that have been synced to a mobile device. Applications must be developed using AirWatch Software Development Kit (SDK) features or wrapped to use these restrictions. Data loss prevention features that can be controlled are described in Table 10.

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Copy And Paste</td>
<td>Allows an application to copy and paste on devices when set to Yes</td>
</tr>
<tr>
<td>Enable Printing</td>
<td>Allows an application to print from devices when set to Yes</td>
</tr>
<tr>
<td>Enable Camera</td>
<td>Allows applications to access the device camera when set to Yes</td>
</tr>
<tr>
<td>Enable Composing Email</td>
<td>Allows an application to use the native email client to send emails when set to Yes</td>
</tr>
<tr>
<td>Enable Data Backup</td>
<td>Allows wrapped applications to sync data with a storage service like iCloud when set to Yes</td>
</tr>
<tr>
<td>Enable Location Services</td>
<td>Allows wrapped applications to receive the latitude and longitude of the device when set to Yes</td>
</tr>
<tr>
<td>Enable Bluetooth</td>
<td>Allows applications to access Bluetooth functionality on devices when set to Yes</td>
</tr>
<tr>
<td>Enable Screenshot</td>
<td>Allows applications to access screenshot functionality on devices when set to Yes</td>
</tr>
<tr>
<td>Enable Watermark</td>
<td>Displays text in a watermark in documents in the AirWatch Content Locker when set to Yes</td>
</tr>
<tr>
<td>Limit Documents to Open Only in Approved Apps</td>
<td>Controls the applications used to open resources on devices</td>
</tr>
<tr>
<td>Allowed Applications List</td>
<td>Applications that are allowed to open documents</td>
</tr>
</tbody>
</table>

**Table 10: Data Loss Prevention Features**

### Key Design Considerations

Because this environment is configured with Office 365, SharePoint-based document repositories will be configured as part of the AirWatch Content Locker implementation. DLP controls will be used in the Mobile Productivity Service and Mobile Application Workspace profiles to protect corporate information.
Conditional Access

Compliance in Workspace ONE can be evaluated not just on if a device has been compromised or the user has access to an application, but on other criteria such as the type of device being used, if it is enrolled in management, or even the network range that the user is trying to access an app from. Combined, VMware Identity Manager and AirWatch offer a very powerful capability to evaluate if an application should be accessed.

Configuration of compliance starts in the AirWatch console. Compliance policies are created by determining a criterion to check, such as a jailbroken or rooted device, an action to take, such as an email to an administrator or a device wipe, an escalation to further actions if the device is not returned to compliance within a set time, and an assignment to devices or users. Examples of rules are listed in Table 11.

<table>
<thead>
<tr>
<th>COMPLIANCE POLICY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Lists</td>
<td>A device is non-compliant with this policy in case of the following:</td>
</tr>
<tr>
<td></td>
<td>• Blacklisted apps are installed in the device.</td>
</tr>
<tr>
<td></td>
<td>• Non-whitelisted apps are installed in the device.</td>
</tr>
<tr>
<td></td>
<td>• The required apps are not installed.</td>
</tr>
<tr>
<td></td>
<td>• The version of the installed app is different from the one defined in the policy.</td>
</tr>
<tr>
<td>Last Compromised Scan</td>
<td>A device is compliant with this policy if the last compromised scan has happened within the time duration defined in the policy. The corresponding sample is for the Last Compromised Scan policy.</td>
</tr>
<tr>
<td>Passcode</td>
<td>A device is compliant with this policy if a passcode is set in the device by the user. The corresponding sample provides information on the passcode and encryption status of the device.</td>
</tr>
<tr>
<td>Device Roaming</td>
<td>A device is non-compliant with this policy if the device is in roaming.</td>
</tr>
<tr>
<td>Copy of Windows</td>
<td>A device is compliant with this policy if the OS installed in the device is genuine.</td>
</tr>
<tr>
<td>Anti-Virus</td>
<td>If this policy is assigned to a device, the compliance status of the device depends on the usage of the antivirus application installed in the device.</td>
</tr>
<tr>
<td>Roaming Cell Data Usage</td>
<td>This policy, when assigned to a device, helps to check the data usage by the device when it is in roaming.</td>
</tr>
<tr>
<td>Free-Disk Space</td>
<td>This policy, when assigned to a device, helps to check and restrict the usage of disk space by the device.</td>
</tr>
<tr>
<td>SIM Card Change</td>
<td>A device is non-compliant with this policy if the SIM card is changed.</td>
</tr>
<tr>
<td>Device Model and OS version</td>
<td>A device is compliant with this policy if the model and OS of the device meet the condition that is defined in the policy. The corresponding sample provides information on the OS version, model, IMEI number, model number, and capacity of the device.</td>
</tr>
<tr>
<td>Device Compromised Status</td>
<td>A device is compliant with this policy if the status (compromised or not compromised) of the device meets the condition that is defined in the policy. The policy runs again if the beacon compromised status is different (changes from jailbroken to not and vice versa).</td>
</tr>
<tr>
<td>Interactive Certificate Profile Expiry</td>
<td>A device is non-compliant with this policy if the interactive certificate profile expires within the number of days defined in the policy. The corresponding sample gives information about the certificates.</td>
</tr>
</tbody>
</table>
COMPLIANCE POLICY | DESCRIPTION
---|---
Device Last Check-In | A device is compliant with this policy if it has checked in at least once within the number of days set by the admin. The policy runs based on the scheduler and not on the samples.

MDM EULA Acceptance | A device is compliant with this policy if the user accepts the EULA. The policy runs based on the scheduler and does not depend on the samples.

NA | This sample provides information on the profiles installed in the device. It does not impact any of the compliance policies.

Firewall Status | A device is non-compliant with this policy if the firewall is disabled.

Automatic Updates | A device is non-compliant with this policy if automatic updates are disabled.

Laptop Encryption | A device is non-compliant with this policy if the device is not encrypted.

Table 11: Example Rules

To incorporate the device posture from AirWatch with VMware Identity Manager, the option to enable Device Compliance needs to be enabled when configuring AirWatch–VMware Identity Manager integration, and the Device Compliance (with AirWatch) authentication method must be enabled.

![Edit Policy Rule](image)

**Figure 16: Device Compliance Policy**

It is also necessary to ensure that the universally unique identifier (UDID) of a device is captured in AirWatch and used in the configuration of compliance. This feature works with Mobile SSO for iOS, Mobile SSO for Android, and Certificate cloud deployment authentication methods.
Standalone MAM and Adaptive Management

Workspace ONE supports a variety of device and application management approaches. Standalone mobile application management allows a user to download the Workspace ONE app from public app stores and immediately take advantage of entitled apps and corporate published native mobile apps. The benefits of this approach include:

- IT can distribute corporate-approved public mobile apps to unmanaged devices through the Workspace ONE app catalog.
- With the Workspace ONE app installed, users can now single sign-on (SSO) into other apps provided by VMware, including AirWatch Browser and AirWatch Content Locker, or any custom app built using the AirWatch SDK.
- When an unmanaged device is out of compliance (for example, jailbroken), the system quickly takes action to protect company data. When a violation is detected, all company data is removed from the Workspace ONE app, AirWatch productivity apps (for example, AirWatch Content Locker), and any custom app built using the AirWatch SDK.

For apps that require a higher level of security assurance, the user can enroll their device into AirWatch right from the Workspace ONE app instead of downloading the AirWatch Agent. All entitled apps are listed in the catalog. Apps that require enrollment are marked with a lock icon. When the user tries to download an app with a lock icon, the enrollment process is triggered. For example, users can download a conferencing app, such as WebEx, without enrollment. But they will be prompted to enroll when they try to download, for example, Salesforce1 from the catalog.

Figure 17: Adaptive Management
Enabling Adaptive Management

Enabling adaptive management is done on an application-by-application basis within the AirWatch console. Within an application profile, an administrator can choose to require management of a device prior to allowing use of that app.

![AirWatch Application Deployment for Adaptive Management](image)

**Figure 18:** AirWatch Application Deployment for Adaptive Management

**Design Decision:** Adaptive Management will be used in the Device Management Service.
Data Loss Prevention

Apps which have been built for AirWatch deployment and take advantage of “app wrapping” to be deeply integrated with AirWatch management can take advantage of controls designed to make accidental, or even purposeful, distribution of sensitive information more difficult. DLP settings include the ability to disable copy and paste, prevent printing, disable the camera or screen shot features, or require a watermark to be added to content when viewed on device. These features can be configured on a platform level, with iOS- or Android-specific profiles applied to all devices, or can be associated with the deployment of a specific application where additional control might be required.

AirWatch applications, including AirWatch Inbox, AirWatch Content Locker, and AirWatch Browser are built to the AirWatch SDK and can natively take advantage of these capabilities due to their conformity to the AirWatch platform. Other applications can be wrapped to include such functionality but will typically not be enabled for it out of the box.

![Figure 19: AirWatch Data Loss Prevention Settings](image-url)
Another set of policies can restrict actions a user can take with email. For managed email clients, such as AirWatch Inbox, restrictions can be set to govern copy/paste, prevent attachments from being accessed, or force all hyperlinks in email to use a secure browser such as the AirWatch Browser.

Figure 20: AirWatch Inbox Content-Restriction Settings
VMware Verify

VMware Verify is a two-factor authentication mechanism that allows use of an iOS, Android, or Chrome app to enable multifactor authentication through VMware Identity Manager. It can use push notifications to a mobile device, use a time-based one-time passcode in the Verify app, or an SMS message sent to a registered device to ensure access. Verify can be implemented as the only type of authentication, or “chained” to require it as an additional factor.

Verify Architecture

Verify is a hosted solution that can be enabled through the built-in identity provider in VMware Identity Manager. Configuration is performed by the end user when they authenticate against Verify for the first time, where they will register their phone with the service. Additional devices may be enabled for Verify after the initial device is used to create a “circle of trust” in which additional devices can be authorized by the initial device.

Verify is available in the cloud-hosted VMware Identity Manager product, and will be added to the on-premises product in the future.

Figure 21: VMware Verify
Resource Types
A Workspace ONE implementation can include a number of different types of supported apps in the enterprise. This includes SaaS, ThinApp packaged apps, Horizon, and native mobile apps.

SaaS Apps
SaaS apps include hosted apps such as Concur, Salesforce, or other cloud-based applications that are often authenticated via standards such as SAML or WSFed to provide a single sign-on experience for end users. Often browser based, these applications are published through VMware Identity Manager. The cloud application catalog in VMware Identity Manager includes templates with many of the configuration parameters preconfigured to make federating with the SaaS provider easier. For other providers, if a template is not provided, a wizard is provided to help walk through configuration of the app and then entitle users to it.

Figure 22: Cloud Application Catalog

ThinApp Packaged Apps
ThinApp is a Windows application virtualization solution that can accelerate deployment by isolating applications from the underlying operating system to eliminate application conflict. The apps are packaged for distribution from file shares in the enterprise. In a Workspace ONE implementation, they can be published to Windows-based systems through VMware Identity Manager and deployed to physical or virtual machines. While the VMware Identity Manager cloud-hosted service supports ThinApp packaged apps, the VMware Identity Manager Connector must be deployed in order to enable the option to use them in a Workspace ONE deployment.
Horizon Apps and Desktops
The roots of Workspace ONE go back to the VMware Horizon suite of products and the idea of delivering virtual desktops and hosted apps through a Web browser to make application and desktop access easy for end users. The capability to deliver virtual apps and desktops continues to be a significant value for Workspace ONE users. VMware Identity Manager can be integrated with a VMware Horizon implementation to expose the entitled apps and desktops to end users, and through the Horizon clients available for native mobile platforms, access to these resources can be easily extended to mobile devices. In order to provide access to VMware Horizon resources from the VMware Identity Manager cloud-hosted service, the VMware Identity Manager Connector must be deployed in order to sync entitlements to the service, and a means of accessing the resources from the Internet, such as Access Point, is necessary.

Figure 23: ThinApp Packaged Apps and Horizon Application Configuration

Native Mobile Apps
Native mobile apps from the Apple App Store, Google Play, or the Windows Store have brought about new ways of easily accessing tools and information to make users more productive. A challenge has been making those applications available to users to easily find, install, and control. AirWatch has been a leader in this area for a long time, providing a platform for distribution, management, and security of these apps. Apps can be published from the app stores themselves, or, for internally developed apps, they can be uploaded to the AirWatch service for distribution to end users.

Figure 24: AirWatch Native Mobile Apps
Unified App Catalog

When AirWatch and VMware Identity Manager are integrated and apps from both platforms are going to be enabled for end users, the option to use the Unified Catalog in VMware Identity Manager will be enabled. This will pull entitlements from both platforms and display them appropriately in the Workspace ONE native app on a mobile device. The Workspace ONE client will determine which apps should be displayed to which platform; iOS apps will only appear to devices running iOS, Android apps will appear on Android devices.

![Figure 25: Unified Catalog in VMware Identity Manager](image)

Mobile Single Sign-On

One of the hallmark features of the Workspace ONE experience is mobile single sign-on technology. The ability to sign into the app once and have access to the entitled applications is a core capability and can help address security concerns and password cracking attempts, and vastly simplify the end-user experience for a mobile user. While the technology, when implemented well, seems “simple,” the reality of the situation is that mobile single sign-on across iOS, Android, Windows 10, SaaS apps, native mobile, and Horizon can be very complicated to implement. There are a number of methods to enable the capability on both VMware Identity Manager and AirWatch, as well as to the SaaS services that users will access. SAML becomes a bridge to the apps, but each native mobile platform requires different technologies to enable SSO.

iOS SSO Overview

Kerberos-based SSO is the recommended SSO experience on managed iOS devices. VMware Identity Manager offers a built-in Kerberos adapter, which can handle iOS authentication without the need for device communication to your internal Active Directory servers. In addition, AirWatch can distribute identity certificates to devices, eliminating the requirement to maintain an on-premises CA.

Alternatively, enterprises can use an internal KDC for SSO authentication, but this will typically require the provisioning of on-demand VPN. Either option can be configured in the Standard Deployment model, but the built-in KDC must be used in the Simplified Deployment model that is referenced in the documentation linked below.
Android SSO Overview
Workspace ONE offers universal Android mobile single sign-on, which allows users to sign in to enterprise apps securely, without the need for a password. Android mobile single sign-on technology requires the use of the AirWatch Tunnel application to authenticate users against SaaS applications.

Windows 10 SSO Overview
Certificate-based SSO is the recommended experience for managed Windows desktops and laptops. An Active Directory Certificate Services or other CA is required to distribute certificates for this implementation. The AirWatch service can integrate with an on-premises CA through the AirWatch Cloud Connector or through an on-demand VPN.

Configuration of mobile single sign-on for iOS, Android, and Windows 10 devices can be found in the VMware Workspace ONE Quick Configuration Guide.

View in Horizon 7
View in Horizon 7 allows us to create and broker connections to Windows virtual desktops, Linux virtual desktops, Remote Desktop Server (RDS) hosted applications and desktops, and physical machines.

This core part of View in Horizon 7 includes the following components and features:

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Connection Server</td>
<td>Horizon Connection Server is an enterprise-class desktop management server that securely brokers and connects users to desktops running on vSphere virtual machines, physical PCs, blade PCs, or Microsoft Terminal Services.</td>
</tr>
<tr>
<td>Horizon Administrator</td>
<td>The Horizon Administrator interface is a Web application that is part of the Horizon Connection Server, allowing administrators to configure the Connection Server, deploy and manage desktops, control user authentication, initiate and examine system events, and carry out analytical activities.</td>
</tr>
<tr>
<td>View Composer</td>
<td>View Composer works with the Connection Servers and a VMware vCenter Server®. It is one of the methods that enables scalable management of virtual desktops by provisioning from a single master image. It reduces storage cost by using VMware linked-clone technology and streamlines desktop management by enabling automatic updating and patching of hundreds of images from the master image.</td>
</tr>
<tr>
<td>Horizon Agent</td>
<td>The Horizon Agent is a software service that is installed on all guest virtual machines, physical systems, or RDS Hosts that allows them to be managed by Horizon Connection Servers.</td>
</tr>
<tr>
<td>Horizon Client</td>
<td>The Horizon Client allows a physical device to access a virtual desktop or RDS-based application in a Horizon deployment. (It should be noted that there is also the option to use an HTML client from devices where installation of software is not possible).</td>
</tr>
<tr>
<td>Access Point</td>
<td>Access Point provides a method to secure connections in access scenarios requiring additional security measures such as over the Internet. (A separate section on Access Point details the design and implementation of this).</td>
</tr>
<tr>
<td>Remote Desktop Services (RDS) hosts</td>
<td>Microsoft RDS hosts for providing hosted applications and session-based remote desktops to end users.</td>
</tr>
<tr>
<td>vSphere and VMware vCenter</td>
<td>The vSphere product family includes VMware ESXi and vCenter Server, and is designed for building and managing virtual infrastructures. The vCenter Server system provides key administrative and operational functions such as provisioning, cloning, and virtual machine management features, which are essential for a virtual desktop infrastructure.</td>
</tr>
</tbody>
</table>

Table 12: Components and Features
Logical Architecture
This section will focus on the following core elements of View in Horizon 7.
• Horizon Connection Server
• View Composer (only required where linked-clone pools will be deployed)
• Horizon Agent
• Horizon Client
The diagram below shows the high-level logical architecture of these core Horizon elements.

Figure 26: Horizon Logical Architecture

Next Steps for Horizon
Recently, an extensive VID document was published to provide extensive information on building a Horizon environment. See the Horizon 7 Enterprise Edition Reference Architecture: Validated Integration Design for more information.
Access Point
Access Point is an optional component in a Workspace ONE deployment, depending on if remote access from outside the corporate network to internally hosted View desktops and applications is required. Access Point is typically deployed within the corporate DMZ and acts as a proxy host for connections to your company’s resources.

Design Overview
A successful deployment of Access Point is dependent on good planning and a robust understanding of the platform. This section discusses the design options and details the design decisions that are made to satisfy the design requirements.

Access Point 2.5 and 2.7
There are two different releases of Access Point. A brief overview of the differences is discussed here:

• Version 2.5 only supports connection to View desktops and applications.
• Version 2.7 only supports connections to on-premises VMware Identity Manager appliances and AirWatch integration for device and per-app VPN services.

A future update to Access Point will support Horizon, VMware Identity Manager, and AirWatch.

Design Decision: Only Access Point 2.5 will be used to satisfy the requirements of the design as VMware Identity Manager is cloud hosted and View is on premises.

Network Deployment Options
Access Point can be deployed with one, two, or three Network Interfaces (NIC). The decision will be determined by your network requirements and discussions with the security teams to ensure compliance with company policy.

Next Steps for Access Point
Recently, an extensive VID document was published to provide extensive information on building a Horizon environment. See the Horizon 7 Enterprise Edition Reference Architecture: Validated Integration Design for more information.
Physical Environment Design

Several environment resources are required to support a Workspace ONE deployment. In most cases these will already exist.

**Active Directory**

Workspace ONE is usually configured to an Active Directory domain structure for user authentication and management. Standard best practice for an Active Directory deployment should be followed to ensure that it is highly available.

**DNS**

Domain Name System (DNS) is widely used in a Workspace ONE environment where the VMware Identity Manager Connector is deployed. Follow standard design principles for DNS making it highly available. Additionally, ensure that forward and reverse zones have been implemented.

**Certificate Authority**

A Microsoft Enterprise Certificate Authority (CA) is often used for certificate-based authentication, single sign-on, and email protection. A certificate template is created within the Microsoft CA and is used by AirWatch to sign Certificate Signing Requests (CSR) that are issued to mobile devices through the Certificate Authority integration capabilities in AirWatch and Active Directory Certificate Services.

Details on setting up a Microsoft CA can be found in Set Up an Enterprise Certificate Authority in View Administration.

**Design Decision:** A Microsoft Enterprise Certificate Authority will be set up to support certificate authentication for Windows 10 devices.

**Load Balancer**

To remove a single point of failure from some components, we can deploy more than one instance and use a third-party load balancer. This not only provides redundancy but also allows the load and processing to be spread across multiple instances of the component. To ensure that the load balancer itself does not become a point of failure, most load balancers allow for setup of multiple nodes in an HA or master/slave configuration.

**Firewall and External Access Networking**

Internal access to Horizon resources will need to be enabled through Access Point in order to allow virtual apps and desktops to be accessed from Internet-based mobile devices.

- Internal users will connect to the VMware Identity Manager and AirWatch services over port 443 and to any Horizon Connection Server again over port 443. iOS devices that use mobile single sign-on will also communicate to the AirWatch service over port 88.
- External users accessing Horizon resources are redirected by the VMware Identity Manager service over port 443, which then communicates through the Access Points for Connection Servers over port 443.
Service Integration Design

With a thorough understanding of the components and concepts that make up the Workspace ONE product offering, the next step is to assemble the appropriate components and configure them according to the services designed to fit the use cases defined earlier.

The table below details the parts required for each service. The rest of this section will detail the design and configuration of each of the services.

<table>
<thead>
<tr>
<th>Service Requirement</th>
<th>Device Management Service</th>
<th>Mobile Productivity Service</th>
<th>Mobile Application Workspace Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Identity Manager</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>AirWatch</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>AirWatch Cloud Connector</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VMware Identity Manager Connector</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>VMware Verify</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Adaptive management</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Device enrollment</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Native mobile apps</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SaaS apps</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Unified app catalog</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Mobile email management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile content management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DLP restrictions</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Secure browsing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile SSO</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Conditional access</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View in Horizon 7</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Access Point</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

Table 13: Service Requirements
Common Components and Settings
There are common components and settings that will be used in multiple services. To avoid repeating in each individual service they will be outlined in the design first.

VMware Identity Manager and AirWatch Integration
In order for VMware Identity Manager and AirWatch to successfully be integrated, there are several points of integration that will be enabled within the respective consoles to establish trust between each service.

Documentation for this process is available in the VMware Workspace ONE Quick Configuration Guide with additional information and details available in the VMware Identity Manager Documentation Center.

Figure 27: Common Application Service Components

<table>
<thead>
<tr>
<th>AIRWATCH</th>
<th>CONFIGURATION CONSIDERATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Account Certificate</td>
<td>• An Admin account for VMware Identity Manager must be added to the AirWatch service, and an associated certificate exported from the console and imported into the VMware Identity Manager console.</td>
</tr>
<tr>
<td>Admin API Key</td>
<td>• REST Admin API access is required to allow the VMware Identity Manager to communicate with the AirWatch environment. This key will be created in the AirWatch tenant, and then copied into the VMware Identity Manager console.</td>
</tr>
<tr>
<td>Enrolled User API Key</td>
<td>• REST Enrolled User API key is required to allow user-based access to the AirWatch service from VMware Identity Manager. This key will also be created in the AirWatch tenant and then copied into the VMware Identity Manager console.</td>
</tr>
<tr>
<td>Directory Integration with VMware Identity Manager</td>
<td>• In the AirWatch console, the VMware Identity Manager node under Enterprise Integration is used to allow directory integration and sync between AirWatch and VMware Identity Manager. The configuration consists of providing the VMware Identity Manager tenant URL, local VMware Identity Manager admin account and password. A directory name is provided.</td>
</tr>
<tr>
<td></td>
<td>• If there are needed directory attributes in the existing directory that must be brought into the directory, such as objectGUID needed by Office 365 customers, they can be mapped during this integration.</td>
</tr>
</tbody>
</table>
## AirWatch Configuration Considerations

<table>
<thead>
<tr>
<th><strong>AirWatch</strong></th>
<th><strong>Configuration Considerations</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>AirWatch Integration in the VMware Identity Manager Portal</td>
<td>In the Identity &amp; Access Management tab in the VMware Identity Manager administration console, the AirWatch node is designed to simplify integration of the services. By providing the AirWatch tenant URL, the Admin Certificate exported from the AirWatch console, the API Key, and the appropriate AirWatch Group ID, configuration is enabled between VMware Identity Manager and AirWatch.</td>
</tr>
<tr>
<td>Enable Integration Features</td>
<td>Enable Unified Catalog allows the native mobile applications published in AirWatch to co-exist with the VMware Identity Manager applications in the Workspace ONE application.</td>
</tr>
<tr>
<td>Enable Device Compliance</td>
<td>Allows the use of the Device Compliance authentication adapter to evaluate AirWatch device health prior to providing access to applications. This will be applied in VMware Identity Manager access policies later.</td>
</tr>
<tr>
<td>Enable ACC Password</td>
<td>This option will allow a user to enter their Active Directory password through the AirWatch Cloud Connector as a new authentication adapter. This will be applied in VMware Identity Manager access policies later.</td>
</tr>
</tbody>
</table>

### AirWatch Cloud Connector

<table>
<thead>
<tr>
<th><strong>AirWatch Cloud Connector</strong></th>
<th><strong>Configuration Considerations</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>ACC Installation</td>
<td>The AirWatch Cloud Connector will be used in the Mobile Device Management Service and the Mobile Productivity Service. The ACC is enabled in the AirWatch console, and downloaded to a Windows Server in the enterprise to enable communication between Active Directory and the AirWatch service. See the AirWatch Cloud Connector Install Overview for more information.</td>
</tr>
</tbody>
</table>

### Catalog Population

<table>
<thead>
<tr>
<th><strong>VMware Identity Manager Catalog Population</strong></th>
<th><strong>Configuration Considerations</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>SaaS Apps</td>
<td>From the Catalog tab, choose Add Applications from Cloud Catalog. Integration documentation exists for a number of popular SaaS apps. Other SaaS apps that do not have a template in the cloud catalog can be manually created with appropriate parameters. Be sure to entitle the appropriate users of the applications being published and choose whether the entitlement is automatic or manual.</td>
</tr>
<tr>
<td>View in Horizon 7</td>
<td>For the Mobile Application Workspace Service, since Horizon resources will be published, the View Application pools must be published. Entitlements will be synced from the Horizon environment to VMware Identity Manager. Connection Servers will be added into the VMware Identity Manager catalog. For external publishing, Access Point will publish the Horizon Connection Servers to incoming mobile devices. See the Reference Design for more information.</td>
</tr>
<tr>
<td>AIRWATCH CATALOG POPULATION</td>
<td>CONFIGURATION CONSIDERATIONS</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------</td>
</tr>
</tbody>
</table>
| Native Mobile Apps          | • In the AirWatch console, the Apps and Books node is used to assign apps from the public app stores to their respective device platforms. Apps are defined by platform (iOS, Android, Windows, and more) and located in the app store for that platform.  
  • The apps will then be assigned to Smart Groups as appropriate.  
  • Application configuration key values will be provided to point the Workspace ONE app to the appropriate VMware Identity Manager tenant.  
  • Recommended apps to deploy include the Workspace ONE app, as well as other popular AirWatch apps such as AirWatch Inbox, AirWatch Content Locker, and AirWatch Browser. |

**Device Profile / Single Sign-On**

<table>
<thead>
<tr>
<th>DEVICE PROFILES</th>
<th>CONFIGURATION CONSIDERATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Profile Configuration</td>
<td>• Device profiles provide key settings that will be applied to devices as part of enrollment in AirWatch. This includes “payloads” such as credentials, passcode requirements, and other parameters that will be used to configure and secure devices. Different payloads will be configured in different services for this document, but single sign-on is a common requirement across all devices and use cases, so it will be discussed in the Common Settings section below.</td>
</tr>
</tbody>
</table>
| iOS single sign-on | • The iOS platform uses the Mobile SSO (for iOS) authentication adapter for SSO. The authentication adapter is enabled in VMware Identity Manager, added to an access policy, and a profile is deployed that provides appropriate certificate payloads to support trust between the user, the iOS device, AirWatch, and VMware Identity Manager.  
  • Make sure to follow the VMware Workspace ONE Quick Configuration Guide carefully to enable the authentication adapter and device profile in order for iOS SSO to work.  
  • The AirWatch Certificate Authority will be used to enable iOS Mobile SSO. |
| Android single sign-on | • Android uses the Mobile SSO (for Android) authentication adapter for SSO. Again, it will be enabled in VMware Identity Manager, added to an access policy, and a profile will be deployed to support SSO.  
  • A requirement of the Android solution is the AirWatch tunnel client and configuration of the Tunnel Server node under Enterprise Integration in the AirWatch console. The user will need to invoke the Tunnel client prior to single sign-on to a SAML-enabled application.  
  • As of June 2016, there is also a requirement for an AirWatch Tunnel Server to be deployed and accessible from Internet-based machines. This requirement will be removed in the future. Check the documentation to know if that configuration is still required in your implementation.  
  • Additional details on the Android SSO configuration can be found in the VMware Workspace ONE Quick Configuration Guide. |
Windows 10 single sign-on

- Windows 10 SSO uses certificate authentication to perform SSO. A certificate is generated from an Enterprise CA and published to the AirWatch console. When a device profile is deployed, appropriate certificates are generated for the user and installed onto their device. The Certificate (cloud deployment) authentication adapter will be enabled to use Windows 10 SSO.
- The user will be prompted to select a certificate at Workspace ONE app launch.
- Make special note in the VMware Workspace ONE Quick Configuration Guide that in order for device compliance checking to function, part of the certificate request template for AirWatch must include a SAN Type of DNS Name with a value of UDID={DeviceUid}.

Mobile Device Management Service

The mobile device management service will be used to bring an organization which might have minimal device management capabilities, such as Exchange ActiveSync policies applied for passcode, wipe, and other basic settings, under an MDM strategy.

- The devices will initially be configured to support adaptive management, with some less critical applications enabled for single sign-on, while other applications will require enrollment.
- Employees will be encouraged, but not required, to enroll their devices.
- Users will be able to use their native email clients, email apps available from the public app stores, or AirWatch Inbox initially. Eventually, standardization on Boxer would be an approach to consider.

Figure 28: Mobile Device Management Service
DEVICE MANAGEMENT SERVICE DETAILS | CONFIGURATION CONSIDERATIONS

Adaptive management
• Adaptive management will be configured in order to provide access to applications such as WebEx or Concur to be used with mobile single sign-on across all platforms without device enrollment. Other applications, such as HR sites, ADP, or Salesforce, will require device enrollment in order to have a high degree of control over the device.
• Users will be encouraged to download the Workspace ONE app from the public app stores.
• Applications that are deemed to have a higher risk to user or company data will be set for Require Management in the AirWatch device profile.

Active Directory / Cloud Password authentication
• VMware Identity Manager will be configured with policy to enable the Cloud Password from the built-in identity provider and authenticate via the ACC to their Active Directory account.

Email access
• Users will be provided appropriate documentation on how to configure their device for native or third-party email client access. If they choose to install AirWatch Inbox, they will have their email configuration automatically pushed to the device for them. Typically, a user will be provided with the Exchange ActiveSync (EAS) Server address (outlook.office365.com) and provide their email address and password.

Enrollment
• Enrollment will be completed through the Workspace ONE application. If a user accesses an application that has been deployed as “management required” in AirWatch, the enrollment process will be initiated.
• Upon enrollment into Workspace ONE, the users will have all applications available to them. They will also be able to use mobile single sign-on after they have enrolled, since they will have a device profile with appropriate payloads deployed to authenticate with the appropriate SSO technology.
• Additional compliance information will be passed to VMware Identity Manager and if the device is no longer in compliance, the user will lose access to the VMware Identity Manager-based applications.

Applications
APPLICATION TYPES | CONFIGURATION CONSIDERATIONS

SaaS applications
• SaaS-based applications will be added from the VMware Identity Manager cloud catalog and entitled to appropriate users.

Native mobile apps
• Applications will be added to the AirWatch console. Privileged apps will have the Require Management box selected, other apps will not.

Mobile Productivity Service
The Mobile Productivity Service builds on the previous service in that it begins with devices that have been enrolled with the AirWatch Agent and are fully managed at deployment, and as new devices are brought into the organization, they are essentially quarantined until enrolled.
Devices in this service have the following characteristics:

<table>
<thead>
<tr>
<th>MOBILE PRODUCTIVITY SERVICE DETAILS</th>
<th>CONFIGURATION CONSIDERATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device enrollment</td>
<td>• All devices in the Mobile Productivity Service will be required to enroll using the AirWatch Agent. This is due to the higher level of control and security that is required of devices that are likely to have valuable enterprise data on them.</td>
</tr>
<tr>
<td>Email restrictions</td>
<td>• Native and third-party email apps are blocked, and all users will use AirWatch Inbox for increased security.</td>
</tr>
<tr>
<td>Content access</td>
<td>• AirWatch Content Locker is pushed to the device and configured for secure access to corporate repositories.</td>
</tr>
<tr>
<td>Secure browsing</td>
<td>• AirWatch Browser is pushed to the device to ensure that links to intranet sites are always opened in a secure browser.</td>
</tr>
<tr>
<td>Email access</td>
<td>• Email and content are delivered from Office 365, so federation with the Office 365 service is enabled to allow single sign-on to the Office service and with the native mobile Office 365 apps.</td>
</tr>
<tr>
<td>Data loss prevention</td>
<td>• Data loss prevention (DLP) components are enabled within AirWatch Content Locker and AirWatch Inbox to prevent the use of unapproved applications ensuring that data cannot be inadvertently or purposely copied to other apps using copy/paste restrictions.</td>
</tr>
<tr>
<td>Multifactor authentication</td>
<td>• Multifactor Authentication through VMware Verify is used when a user needs to access the Workspace ONE application and they are in a network range that is not within the corporate network. On corporate WiFi, users only need mobile single sign-on–based authentication. Verify is also required on personally owned, non-managed PCs using only the browser to access SaaS apps.</td>
</tr>
</tbody>
</table>

Figure 29: Mobile Productivity Service
### OFFICE 365 FEDERATION

**Federation to Office 365** will allow VMware Identity Manager to authenticate login requests to the Office 365 service. This will be accomplished using the Microsoft Federated Identity approach for Office 365. Documentation on this configuration can be found in a video walkthrough as well as in Converting Office 365 to a Federated Domain for Single Sign-On and Changing Office 365 Parameters to Workspace in Setting Up Resources in VMware Workspace Portal.

| **Enable federation in the Office 365 or Azure AD portals** | • Sync Active Directory user accounts through the Azure AD or Office 365 portals.  
• Configure through PowerShell scripting the Office 365 service to authenticate through VMware Identity Manager as a Federated Identity Provider. A set of PowerShell scripts with appropriate parameters and signing certificates will establish trust between Office 365 and VMware Identity Manager.  
• **Note:** One important criteria to make Office 365 integration work is to make sure the attribute ObjectGUID is being synced from AD to the VMware Identity Manager service. |
| **Configure Office 365 SAML apps in VMware Identity Manager** | • Using the templates in the Cloud Application Catalog, configure the SAML templates to allow authentication against VMware Identity Manager for Office 365-based apps and resources, such as email, SharePoint, Lync, and other Microsoft Services. |

### EMAIL CONFIGURATION

Email integration with Office 365 will be through PowerShell. AirWatch will issue commands through PowerShell to Exchange in Office 365 and devices will communicate directly with Exchange ActiveSync in the Office 365 service. Full configuration information can be found in the most recent VMware AirWatch PowerShell Administration Guide in AirWatch Resources.

| **Configure PowerShell roles in Office 365** | • PowerShell requires specific roles to be established in the Office 365 Admin portal for Exchange. This enables the execution of PowerShell commandlets from AirWatch to the Office 365 Service. |
| **Install and configure PowerShell on AirWatch servers** | • PowerShell must be installed on an AirWatch Server in the environment. In this case, it is installed on the ACC Server. |
| **Configure block/quarantine rules** | • In order to prevent devices from connecting to the Exchange Server that are not permitted to do so, devices can be blocked or quarantined until they have enrolled. PowerShell commands are used to set the appropriate policy. For environments where enrollment is not required for email access, this is not required. |
| **Configure Email compliance policies** | • Compliance policies for email include a range of options for controlling both managed and unmanaged devices. Choices include if a managed device is required for email sync, if only certain email clients will be allowed to sync mail, if device encryption is required for email sync, or if jailbroken or otherwise compromised devices will be allowed. |
| **Configure ActiveSync profiles for email clients** | • Configure the Exchange ActiveSync payload for the device profiles to enable email sync. Hostname for Office 365 is typically outlook.office365.com.  
• Domain, Username, and Email Address will be configured with lookup values and it is important to make sure these values are available in the directory and properly mapped from AD through the ACC. |
### CONTENT CONFIGURATION

<table>
<thead>
<tr>
<th>CONTENT CONFIGURATION</th>
<th>CONFIGURATION CONSIDERATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content integration with Office 365 is established through the AirWatch console under the Content node. From here, templates will be configured for the SharePoint libraries in Office 365 that will be made available to sync to the mobile devices. Full configuration information can be found in the most recent VMware AirWatch Mobile Content Management (MCM) Guide in AirWatch Resources.</td>
<td></td>
</tr>
<tr>
<td>Create Office 365 SharePoint document libraries</td>
<td>• Use the <a href="https://portal.office.com">https://portal.office.com</a> to log in to Office 365 and create SharePoint sites with document libraries containing content.</td>
</tr>
</tbody>
</table>
| Create content templates in AirWatch for automatic deployment | • In the AirWatch console, access the Content node, then select Templates, then Automatic.  
• Configure SharePoint O365 as the Repository Type.  
• Configure the Link field with the path to the SharePoint Document Library (for example, [https://<domain>.sharepoint.com/Sales_Material/Shared%20Documents/](https://<domain>.sharepoint.com/Sales_Material/Shared%20Documents/).  
• Enable Allow Write if read/write access is needed.  
• If content will be synced, choose Allow Offline Viewing.  
• If content will be used with other apps, select Allow Open in Third Party Apps.  
• Review other security settings per enterprise policy.  
• Assign appropriate groups to the repository. |
| Deploy Content Locker | • Requiring AirWatch Content Locker as an Automatic deployment to groups of users who will be using content from SharePoint will ensure access to content. |

### DATA LOSS PREVENTION CONFIGURATION

<table>
<thead>
<tr>
<th>DATA LOSS PREVENTION CONFIGURATION</th>
<th>CONFIGURATION CONSIDERATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLP configuration can be set on a global basis, a platform basis, or per application deployment. Note that for DLP settings to take effect, the application needs to support those settings by either by being built with the AirWatch SDK or through app wrapping for an internal application. In this scenario, the AirWatch Inbox, AirWatch Content Locker, and AirWatch Browser are all built using the SDK and will honor the settings chosen.</td>
<td></td>
</tr>
</tbody>
</table>
| Add SDK profile for iOS or Android defaults | • SDK profiles allow global configuration of DLP settings that will be applied to applications on the appropriate platform for which the profile is defined. Settings include enabling or disabling:  
- Printing  
- Composing email  
- Location services  
- Data backup  
- Camera  
- Watermarking  
- Open-in restrictions limiting ability to open documents in certain apps |
| Enable custom policies for AirWatch Content Locker and AirWatch Inbox as necessary | • AirWatch Content Locker can use the default policies defined in the SDK profile or be overridden if necessary. An important setting here is Require MDM Enrollment to ensure that content is being accessed by devices that have previously enrolled. |
| Verify Email compliance policies | • When configuring AirWatch Content Locker policies, it is also useful to ensure that the email compliance policies match corporate standards, including requiring a managed device, and thus enrolled, to be able to receive email. |
VMWARE VERIFY CONFIGURATION | CONFIGURATION CONSIDERATIONS
---|---
Enable built-in authentication adapter in VMware Identity Manager | VMware Verify is an authentication method found under the Built-in Authentication Adapter within VMware Identity Manager. Configuration consists of only an on/off check box.
Add VMware Verify to access policies | In order to use the authentication method, it must be added to a policy. It can be configured as a standalone authentication method in a policy, but is typically chained with other methods to create a multifactor authentication method. Adding it to Mobile SSO for iOS by clicking the icon and adding VMware Verify would first authenticate via SSO, then prompt for Verify credentials.
Install VMware Verify application | The VMware Verify application is available in the iOS App Store, Google Play Store, and as an add-in for Chrome on Windows and Mac OS.
Enroll phone with Verify | When attempting to access a resource for the first time when VMware Verify is enabled, the user will be asked for their phone number. This will associate their phone number with the VMware Identity Manager service and send a notification to the user’s device to enroll it.
| After this is done, the user’s phone is considered an authentication token and if it can receive push notifications, it will let the user choose to allow or reject the authentication.
Add additional devices | Additional devices can be added for the user and the initial device configured will receive a notification to allow or reject the addition of more devices to be used as authentication tokens.

Conditional Access Policy Configuration

| ACCESS AND COMPLIANCE POLICIES | CONFIGURATION CONSIDERATIONS |
---|---
AirWatch compliance | Create a Compliance Policy for appropriate platforms through the AirWatch console. Criteria for evaluation can include jailbroken or rooted devices, devices that have not checked into the AirWatch environment in a period of time, or the installation of blacklisted applications. The policy can include an escalation of notifications as “actions,” starting with email notification to the user, then email notification to an administrator, and blocking access to email if the device is not remediated in time. |
VMware Identity Manager compliance | VMware Identity Manager compliance checking is enabled via the Policy configuration. Policies will include the Device Compliance (with AirWatch) authentication adapter in addition to other authentication methods, such as Password (AirWatch Connector). These policies can be used in conjunction with network ranges, operating systems platforms, or specific applications, allowing varying requirements for additional means of evaluating if an application should launch depending on where the user is, what device they are using, and how they are authenticating. |
Mobile Application Workspace Service

The Mobile Application Workspace Service would have a similar configuration to the Mobile Productivity Service, but would also include access to Horizon-based applications. Access to Horizon resources was added to the VMware Identity Manager Cloud-Hosted service in the June 2016 release (version 2.7) and takes advantage of a new VMware Identity Manager feature that establishes an outbound-only connection from an on-premises deployment of a VMware Identity Manager Connector appliance to the Cloud-Hosted service. This allows entitlements to sync to the service. Inbound access to the Horizon Connection Servers, virtual desktops, and applications is still required and thus Access Point is also part of this solution.

Devices in the Mobile Application Workspace will have the following unique characteristics:

<table>
<thead>
<tr>
<th>MOBILE APPLICATION WORKSPACE SERVICE DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VMware Identity Manager Connector</strong></td>
</tr>
<tr>
<td>• The connector component of VMware Identity Manager is delivered as a virtual appliance that is deployed onsite and integrates with your enterprise directory to sync users and groups to the VMware Identity Manager service and to provide authentication.</td>
</tr>
<tr>
<td><strong>View entitlements</strong></td>
</tr>
<tr>
<td>• Enabled through the VMware Identity Manager catalog through connecting to the View Pools that expose user-entitled apps and desktops.</td>
</tr>
<tr>
<td><strong>Access Point</strong></td>
</tr>
<tr>
<td>• Enables Horizon clients to access intranet-based Horizon servers for virtual apps and desktops.</td>
</tr>
</tbody>
</table>

![Figure 30: Dedicated Power Workspace Service - Applications](image)
### VMWARE IDENTITY MANAGER CONFIGURATION

<table>
<thead>
<tr>
<th>CONFIGURATION CONSIDERATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deploy VMware Identity Manager Connector</strong></td>
</tr>
<tr>
<td>• The VMware Identity Manager Connector is a virtual appliance that is deployed through vCenter. It is deployed and activated against a VMware Identity Manager SaaS tenant and is responsible for directory sync and user authentication. Instructions for deploying the connector can be found in Deploying VMware Identity Manager Connector in VMware Identity Manager Connector Installation and Configuration.</td>
</tr>
<tr>
<td>• The connector can support View entitlement sync when configured as an outbound only connector, which does not require any inbound ports opened inbound at the network perimeter beyond the ports required to access View desktop and application resources. Instructions for enabling the outbound-only authentication adapters can be found in Configure the Built-In Identity Provider for Authentication in the VMware Identity Manager Administration Guide.</td>
</tr>
<tr>
<td>• This authentication method, when enabled, is referred to as Password (Cloud Deployment).</td>
</tr>
<tr>
<td><strong>Configure Directory Sync</strong></td>
</tr>
<tr>
<td>• After the connector is deployed, directory synchronization will be performed. This will allow Active Directory users and groups to be synced to the VMware Identity Manager Service. Information on sync can be found in Configuring Active Directory Connection to the Service in VMware Identity Manager Connector Installation and Configuration.</td>
</tr>
<tr>
<td><strong>Configure SAML authentication in AirWatch to VMware Identity Manager</strong></td>
</tr>
<tr>
<td>• Because AirWatch will also be using the VMware Identity Manager directory, SAML-based authentication will be configured in the AirWatch console under Settings &gt; Enterprise Integration – Directory Services. Providing the VMware Identity Manager idp.xml configuration file from the Catalog – Settings tab of VMware Identity Manager will populate the settings related to connecting the platforms and enabling authentication and enrollment.</td>
</tr>
<tr>
<td>• A wizard was added in AirWatch 8.4 to automate that process.</td>
</tr>
<tr>
<td><strong>Enable View Pools in VMware Identity Manager Catalog</strong></td>
</tr>
<tr>
<td>• To make Horizon resources available in the Workspace ONE app, the View Pools must be added through the VMware Identity Manager catalog. User entitlements for apps and desktops will be made available through the Horizon configuration and automatically appear in the Workspace ONE app and in a Web browser.</td>
</tr>
<tr>
<td><strong>Provide access to Horizon from external devices</strong></td>
</tr>
<tr>
<td>• In order to access the resources made available through Horizon, a means of access from Internet-based devices must be established. Access Point 2.5 can be configured along with True SSO in order to allow egress and provide connectivity to the Horizon Connection Servers. Information on Access Point can be found in Deploying and Configuring Access Point.</td>
</tr>
</tbody>
</table>

### CLIENT CONFIGURATION

<table>
<thead>
<tr>
<th>CONFIGURATION CONSIDERATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Horizon native apps</strong></td>
</tr>
<tr>
<td>• When using Horizon resources in Workspace ONE, the resources will appear on the Launcher page of the apps, but the resources will launch using the Horizon native mobile apps. For environments planning to access Horizon-based apps and desktops, an Automatic deployment of the native clients is recommended.</td>
</tr>
</tbody>
</table>
Workspace ONE User Experience

Consistent User Experience

A hallmark of the Workspace ONE end-user experience is consistency. The Workspace ONE native mobile applications are built using “responsive design” techniques, and implement an HTML5-based user experience wrapped in native APIs for the respective operating system on which is it is deployed. This means that the user experience is the same for every operating system, but as native apps, the apps can leverage features specific to each OS.

A good example of this is on iOS: The Workspace ONE app can use the latest technologies from Apple such as Touch ID to enable a one-touch authentication that uses the mobile single sign-on features for a consumer-simple experience. On Windows 10, the native app can use Windows Hello to be able to authenticate in the same manner using a camera and facial recognition.

Figure 31: Workspace ONE Windows 10 App
Figure 32: Workspace ONE iOS App

Mobile Productivity Service User Experience on iOS
Enrolled iPad Pro configured to the Mobile Productivity Service:

Figure 33: Home Screen with Enrolled Device and Workspace ONE App Pushed Through Enrollment
Figure 34: TouchID Integrated with iOS SSO

Figure 35: Launcher for SaaS and Horizon Apps
Figure 36: Unified App Catalog

Figure 37: SAML Single Sign-On to AirWatch Self-Service Portal
Figure 38: SAML Single Sign-On to AirWatch Self-Service Portal

Figure 39: Native Apps on iOS Home Screen
Figure 40: AirWatch Content Locker Home Screen

Figure 41: AirWatch Content Locker SharePoint Repository
Figure 42: AirWatch Inbox
About the Authors and Contributors

Kevin Sheehan is an End-User-Computing Architect in the VMware End-User-Computing Technical-Marketing Center of Excellence.

Graeme Gordon is a Senior End-User-Computing Architect in the VMware End-User-Computing Technical-Marketing Center of Excellence.

Jim Yanik is a Senior End-User-Computing Architect in the VMware End-User-Computing Technical-Marketing Center of Excellence.

Matt Coppinger is a Director in the End-User-Computing Technical-Marketing Center of Excellence at VMware.

A special thanks to the reviewers of this Workspace ONE VID:

• Alex Birch
• Jared Cook
• Dean Flaming
• Josue Fontanez
• Vikas Jain
• Colin Minihan
• Neil Tarbit