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 ............................................. 13
  Business Drivers and Requirements ...................................... 13
  Use Cases ....................................................................... 13
  Meeting Business Requirements with Workspace ONE .......... 14
Workspace ONE Services ....................................................... 15
  Mobile Device Management Service ..................................... 16
  Mobile Productivity Service ............................................... 17
  Mobile Application Workspace Service ................................. 18
Architecture Principles and Concepts ..................................... 19
  VMware 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
  VMware AirWatch ............................................................ 26
    Installation and Initial Configuration ................................... 27
    Next Steps ................................................................. 27
  VMware Enterprise Systems Connector ................................ 27
    Design Overview ........................................................ 27
    AirWatch Cloud Connector Design Considerations ............... 28
    VMware Identity Manager Connector Design Considerations ... 29
Email Integration ................................................................. 30
AirWatch Secure Email Gateway Proxy Model ...................... 31
Direct PowerShell Model ...................................................... 32
Supported Email Infrastructure and Models ......................... 32
Key Design Considerations ................................................. 33
Next Steps ............................................................... 33
Microsoft Office 365 Basic Authentication Conditional Access ................................. 34
Content Integration .......................................................... 34
Content Management Overview ......................................... 34
Data Protection in AirWatch Content Locker ....................... 36
Content Gateway .......................................................... 36
Key Design Considerations ................................................. 36
Conditional Access .......................................................... 37
Multifactor Authentication ............................................... 39
Standalone MAM and Adaptive Management ....................... 39
Enabling Adaptive Management ........................................ 41
Data Loss Prevention ....................................................... 41
VMware Verify ........................................................... 43
VMware Verify Architecture ............................................. 43
Resource Types ........................................................... 45
SaaS Apps ................................................................. 45
ThinApp Packaged Apps .................................................. 46
VMware Horizon Apps and Desktops ................................. 47
Native Mobile Apps ......................................................... 47
Unified App Catalog ....................................................... 48
Mobile Single Sign-On ...................................................... 48
iOS SSO ...................................................................... 48
Mobile SSO for Android .................................................. 49
Windows 10 SSO .......................................................... 49
VMware Horizon 7 ......................................................... 49
Logical Architecture ....................................................... 50
Next Steps for Horizon 7 .................................................... 50
VMware Unified Access Gateway ................................................................. 51
Design Overview ................................................................................. 52
Network Deployment Options .............................................................. 52
Load Balancing .................................................................................. 52
Next Steps for VMware Unified Access Gateway .............................. 52

Physical Environment Design .............................................................. 53
Active Directory ................................................................................ 53
DNS ..................................................................................................... 53
Certificate Authority ........................................................................ 53
Load Balancer .................................................................................... 53
Firewall and External Access Networking ........................................... 53

Service Integration Design ................................................................. 54
Common Components and Settings ...................................................... 55
VMware Identity Manager and VMware AirWatch Integration .......... 55
Enterprise Connector and Directory Integration Configuration Wizard 56
VMware Enterprise Systems Connector Setup ................................... 56
Active Directory Integration ................................................................. 57
VMware Identity Manager Integration ............................................... 58
VMware Identity Manager Connector Configuration ........................ 59
Catalog Population ............................................................................ 59
Device Profile - Single Sign-On .......................................................... 60
Mobile Device Management Service ............................................... 61
Applications ....................................................................................... 62
Mobile Productivity Service ............................................................... 63
Conditional Access Policy Configuration ......................................... 67
Mobile Application Workspace Service ........................................... 68

Workspace ONE User Experience ...................................................... 70
About the Authors and Contributors .................................................. 77
Executive Summary

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

This white paper provides a reference architecture for the Workspace ONE product. This example architecture and deployment addresses key business requirements, such as enabling business mobility for employees, and targets use cases such as mobile knowledge workers.

The paper includes three example services—Mobile Device Management, Mobile Productivity Service, and Mobile Application Workspace Service—which address everything from basic mobile management and secure identity-based access to full virtual desktop access on mobile devices with seamless single sign-on (SSO) across all applications.

Figure 1: VMware Workspace ONE Logical Architecture Overview
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 software-as-a-service (SaaS) 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, to provide secure access via operating system (OS) native, third-party, or managed mobile email clients, such as VMware Boxer™. Similarly, access to corporate and user content is provided through a flexible approach of integrating with on-premises file servers, Microsoft 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 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 SSO. This feature allows use of capabilities, such as Apple Touch ID on an iPhone, fingerprint readers on Android devices, and Microsoft Windows Hello on a Surface Pro, to provide a password-free and secure means of logging in to all the applications that 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. When additional means of authentication are required, you can also easily implement a secure and easy-to-use solution.

Additionally, Workspace ONE integrates with VMware Horizon® either to cloud-hosted virtual desktops and applications with VMware Horizon Cloud Service™ or to VMware Horizon 7 on-premises virtual desktops and published applications. 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.
To deliver the defined services, the Workspace ONE components are deployed in varying combinations and configurations to meet specific user requirements. The reference architecture details the configurations needed to integrate both the Workspace ONE components and corporate end-user services.

![Workspace ONE iOS App](image)

**Figure 2: Workspace ONE iOS App**

After deployment, the Workspace ONE services provide a consistent, secure, and straightforward 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. This portal removes the need for users to remember passwords, and users can access applications 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 from a single catalog.

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

The Workspace ONE reference architecture 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 and supporting partners design and validate the reference architectures, which address common use cases, such as enterprise desktop replacement, remote access, and disaster recovery.

VMware reference architectures offer:
- 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 covers integrating the key components of a Workspace ONE Enterprise Edition implementation. It provides detailed configuration information and example architecture. The result is a description of cohesive services that address typical business use cases. This reference architecture does not provide scalability models, performance data, or stress-testing metrics.

Note: Links within this document refer to content on VMware Documentation and MyAirWatch. The content on the VMware site is openly accessible, but the content on the AirWatch site requires logging in to an account. You can create a free account to access that material.

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

You should have:
- A solid understanding of the mobile device landscape
- Deep experience regarding the 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
- Knowledge of 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, you need to understand the business requirements, reasons, and objectives for undertaking the project. From there, you can identify the needs of the users and organize these needs into use cases with understood requirements. You can then align and map those use cases against a set of integrated services provided by Workspace ONE.

![Diagram of Reference Architecture Design Methodology]

A Workspace ONE design uses a number of components to provide the services that address the identified use cases. Before you can integrate and deliver these services, you must design and build the required components in a modular and scalable manner to allow for change and growth. Then you 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 involves reevaluating previous decisions to determine their impact on them and whether they require a change.
Workspace ONE Solution Overview

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, you can enjoy key features such as:

• **Self-service access to cloud, mobile, and Windows apps**
  - After end users are authenticated through the Workspace ONE app, they can instantly access mobile, cloud, and Windows applications with one-touch SSO.

• **Choice of any device, employee or corporate owned**
  - Facilitate adoption of bring-your-own-device (BYOD) programs by putting choice in the hands of end users. 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 need higher levels of security.
  - Provision, deliver, update, and retire applications in real time.

• **Secure productivity apps: mail, calendar, docs, and social**
  - End users 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 are edited and shared.

• **Data security and endpoint compliance with conditional access**
  - By 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

VMware Identity Manager provides the solution’s identity-related components. These components include authentication using username, password, two-factor authentication, certificate, Kerberos, mobile SSO, and inbound SAML from third-party VMware Identity Manager systems. VMware Identity Manager also provides SSO to entitled web apps and Windows apps and desktops delivered through either VMware Horizon or Citrix.

 VMware AirWatch delivers the enterprise mobility management portion of the solution. VMware AirWatch allows device enrollment and uses profiles to enforce configuration settings and control of users’ devices. It also enables a mobile application catalog to publish public and internally developed applications to end users. You can also develop compliance policies to alert administrators to compromised devices or wipe a device that is running unapproved applications. You can integrate VMware AirWatch with enterprise directories, such as Active Directory, for authentication and user...
management. To facilitate mobile productivity, VMware AirWatch can integrate with email systems and content repositories.

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

Workspace ONE supports adaptive management that allows users to download and use less sensitive or secure apps from the Workspace ONE catalog. When the user downloads a sensitive or secure app, the user is asked to go through the device enrollment process directly from within Workspace ONE. With the device enrolled, the 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
A solution based on Workspace ONE can address a wide-ranging set of business requirements and use cases. In this reference architecture, the solution targets the most common requirements and use cases as seen in customer deployments to date.

Business Drivers and Requirements
The top common key business drivers addressed by Workspace ONE are:

• Provide greater business mobility by offering 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 provisioning time.
• Simplify root cause analysis and reduce time to resolution of user issues.
• Provide a comprehensive and flexible platform for device deployment and management.
• Allow users to access corporate applications, especially the Microsoft Office 365 suite, 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 represent common user scenarios. For example, a finance or marketing user can be considered a mobile knowledge worker use case. Some common use cases are described in Table 1.

<table>
<thead>
<tr>
<th>USE CASE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task-Based Worker</td>
<td>Users who typically use a mobile device for a single task through a single application.</td>
</tr>
<tr>
<td></td>
<td>• Uses a highly managed mobile device for a small number of tasks, such as inventory control, product delivery, or retail applications.</td>
</tr>
<tr>
<td></td>
<td>• Communications tools, such as email, might be restricted to only sending and receiving email with internal parties.</td>
</tr>
<tr>
<td></td>
<td>• Device is typically locked down from accessing unnecessary applications. Access to public app stores is restricted or removed entirely.</td>
</tr>
<tr>
<td></td>
<td>• Device location, full device wipe, and other features are typically used.</td>
</tr>
<tr>
<td>Mobile Knowledge Worker</td>
<td>Many roles fit this profile, such as a hospital clinician or an employee in finance, marketing, HR, health benefits, approvals, and travel.</td>
</tr>
<tr>
<td></td>
<td>• These workers use their own personal device (BYOD), a corporate device they personally manage, or a managed corporate device with low restrictions.</td>
</tr>
<tr>
<td></td>
<td>• Typically allowed to access email, including personal email, along with public app stores for personal apps.</td>
</tr>
<tr>
<td></td>
<td>• Is likely subject to information controls over corporate data, such as DLP controls, managed email, managed content, and secure browsing.</td>
</tr>
<tr>
<td></td>
<td>• Needs access to SaaS-based applications for HR, finance, health benefits, approvals, and travel, as well as native applications where those apps are available.</td>
</tr>
<tr>
<td></td>
<td>• A great candidate for SSO because the need to access many diverse apps and passwords becomes an issue for users and help desk.</td>
</tr>
<tr>
<td></td>
<td>• Privacy is typically a concern that might prevent device enrollment, so adaptive management and clear communication regarding the data gathered and reported to VMware AirWatch is important to encourage adoption.</td>
</tr>
</tbody>
</table>
Table 1: Common Use Cases

Meeting Business Requirements with Workspace ONE

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

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

The service is defined by your unique business requirements and use cases, and identifies the technology or feature combinations that will satisfy those unique requirements. After you define the service, you define the service quality—performance, availability, security, management, and monitoring requirements.

The remainder of this document details the design to satisfy each service definition.

The list of services are not exclusive or prescriptive; each environment is different. Adapt the services to your particular use cases. You can add or remove components as needed. You can also combine multiple services to address more complex use cases.

Table 3 lists the core components 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</td>
<td>Virtual desktops and Remote Desktop Services (RDS) published applications delivered either through Horizon Cloud or VMware Horizon 7</td>
</tr>
<tr>
<td>VMware Boxer</td>
<td>Secure email clients</td>
</tr>
<tr>
<td>VMware AirWatch Browser™</td>
<td>Secure web browser</td>
</tr>
<tr>
<td>AirWatch Content Locker</td>
<td>Mobile content repository</td>
</tr>
<tr>
<td>VMware Enterprise Systems Connector (VMware AirWatch Cloud Connector™ + VMware Identity Manager Connector)</td>
<td>Directory sync to enterprise directories</td>
</tr>
<tr>
<td>VMware Unified Access Gateway™</td>
<td>VMware Tunnel™, and content gateway</td>
</tr>
<tr>
<td>VMware AirWatch Secure Email Gateway™</td>
<td>Email proxy service</td>
</tr>
</tbody>
</table>

Table 3: Core Components
Mobile Device Management Service

**Overview:** Many organizations have deployed mobile devices and have lightweight management capabilities, like simple email deployment and device policies, such as a PIN requirement, device timeouts, and device wiping. But they lack a comprehensive and complete management practice to enable a consumer-simple, enterprise-secure model for devices.

**Use Cases:** Static Task Workers

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

**Table 4:** Unique Requirements of Static Task Workers

**Blueprint**

Figure 5 shows a high-level blueprint of a Workspace ONE Standard deployment and the available components.
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 SSO and multifactor authentication, and access to productivity tools. However, from an enterprise perspective, providing this much access to corporate information means instituting a greater degree of control, such as 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 Workers, 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>SSO</td>
<td>• VMware Identity Manager and VMware AirWatch</td>
</tr>
<tr>
<td>Managed email</td>
<td>• VMware Boxer</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>

Table 5: Unique Requirements of Mobile Knowledge Workers and Contractors

Blueprint

Figure 6 shows a high-level blueprint of a Workspace ONE Advanced deployment and the available components.

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

**Overview:** Recognizing that some applications are not available as a native app on a mobile platform and that some security requirements 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 VMware Horizon–based resources, enables this scenario.

Many current VMware Horizon users benefit by adding the Workspace ONE catalog capabilities as a single, secure point of access for their virtual desktops and applications.

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

<table>
<thead>
<tr>
<th>UNIQUE REQUIREMENTS</th>
<th>COMPONENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to virtual apps and desktops</td>
<td>• Horizon Cloud or VMware Horizon 7</td>
</tr>
<tr>
<td></td>
<td>• VMware Enterprise Systems Connector</td>
</tr>
</tbody>
</table>

**Table 6: Unique Requirements of Contractors and Mobile Knowledge Workers**

**Blueprint**

Figure 7 shows a high-level blueprint of a Workspace ONE Enterprise deployment and the available components.
Architecture Principles and Concepts

The Workspace ONE platform is comprised of VMware Identity Manager and VMware AirWatch. While each product can operate independently, integrating both of them is what enables the Workspace ONE product to function. VMware Identity Manager and VMware 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. Users who have VMware Identity Manager or VMware AirWatch deployed on premises can also take advantage of the latest versions of the software and deploy Workspace ONE.

Advantages of a cloud-hosted Workspace One implementation:

- 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 are made available in the on-premises version shortly afterwards.

For this document, the approach taken is to use cloud-hosted VMware AirWatch and VMware Identity Manager with on-premises VMware Horizon 7 for the Mobile Workspace Service.
VMware AirWatch and VMware Identity Manager Integration
VMware Identity Manager and VMware AirWatch are 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 straightforward. Comprehensive documentation is available to highlight the exact steps in integration.

While VMware Identity Manager and VMware AirWatch are the core components in a Workspace ONE deployment, you can deploy a variety of other components depending on your business use cases. In Figure 8, you can use AirWatch Secure Email Gateway for access to an on-premises exchange server or use VMware Unified Access Gateway to provide the VMware Tunnel™ or VPN-based access to internal resources. Refer to the VMware My AirWatch resources for documentation of the full range of components that apply to a deployment.

Figure 8: Sample Workspace ONE Architecture

Many other enterprise components can 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 necessary.
Workspace ONE Logical Components and Concepts

In implementing Workspace ONE, you can deploy a number of components either on premises or cloud hosted. You should also understand some key concepts for device management, security and compliance, and application access.

- **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 an SSO experience across resource types.

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

- **VMware Enterprise Systems Connector™** – Consists of two different services (AirWatch Cloud Connector and VMware Identity Manager Connector) bundled within a single Windows-based installer. This bundle allows for ease of deployment of both connectors needed to sync with their respective cloud-hosted service.

- **AirWatch Cloud Connector** – Provides organizations the ability to integrate VMware AirWatch with their back-end enterprise systems. It runs in the internal network, acting as a proxy that securely transmits requests from VMware AirWatch to the organization’s critical enterprise infrastructure components. Organizations can leverage the benefits of VMware AirWatch Mobile Device Management™, 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 SSO across SAML-based applications, VMware Horizon-based apps and desktops, and VMware ThinApp® packaged apps. It is also responsible for authentication policy based on networks, applications, or platforms.

- **VMware Identity Manager Connector** – Windows-based installer (VMware Enterprise Systems Connector) responsible for directory sync and authentication between an on-premises Active Directory and the VMware Identity Manager service. A legacy Linux-based virtual appliance is also available.

- **Device enrollment** – Process by which a device is brought under management in a VMware AirWatch environment. Enrollment allows the device to be managed, device profiles and applications distributed, and content delivered or removed. Enrollment also allows extensive reporting based on the device’s check-in to the VMware 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. Where other applications require device enrollment, the Workspace ONE app can initiate enrollment for the user.

- **Mobile SSO** – One-touch SSO 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, it uses technology known as the Key Distribution Center (KDC). For Android, the authentication method is called Mobile SSO for Android. And for Windows 10, it is called Cloud Certificate.

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

- **Unified application catalog** – Combines VMware Identity Manager and VMware AirWatch application catalogs and presents them on the Workspace ONE app Catalog tab.
• **Email integration** – VMware AirWatch supports integration with email services, such as Microsoft Exchange, GroupWise, Lotus Notes, and Google Apps for Work. You can integrate email in three different ways: through AirWatch Secure Email Gateway, PowerShell integration, or Google Apps for Work integration. AirWatch Secure Email Gateway requires a server to be configured in the data center. PowerShell communicates directly with Exchange ActiveSync on Exchange 2010 or later or Microsoft Office 365. VMware AirWatch integrates directly with the Google cloud services and does not need additional servers.

• **Content integration** – The VMware AirWatch Mobile Content Management™ solution helps organizations address the challenge of securely deploying content to a wide variety of devices using a few key actions. An administrator can leverage the AirWatch Console to create, sync, or enable a file repository. After configuration, this content deploys to end-user devices with AirWatch Content Locker. Access to content can be either read-only or read-write.

• **Conditional access** – Both VMware Identity Manager and VMware AirWatch have ways to evaluate compliance. When users register their devices into Workspace ONE, samples containing data used to evaluate compliance are sent to the AirWatch cloud service 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, corresponding actions configured in the AirWatch Console are taken. VMware Identity Manager includes an access policy option that you can configure to check the VMware 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 SSO to the VMware Identity Manager portal if the device is out of compliance. When the device is compliant again, the ability to sign in is restored. You can enforce these actions based on the network users are on, the platform they are using, or the applications being accessed. In addition to checking VMware AirWatch for device compliance, VMware Identity Manager can evaluate compliance based on network range of the device, type of device, operating system of device, and credentials.

• **Secure browsing** – Using AirWatch Browser instead of a native browser or third-party browser ensures that access to sensitive web content is secure and manageable.

• **Data loss prevention (DLP)** – Forces documents or URLs to open only in approved applications to prevent accidental or purposeful distribution of sensitive information.

• **VMware Verify** – Multifactor authentication solution that enables using an iOS, Android, or Chrome app with a push-notification, one-time password, or SMS message as an additional factor when accessing resources through VMware Identity Manager.

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

• **VMware Unified Access Gateway** – Virtual appliance that allows Internet-based access to internal, on-premises resources, such as on-premises Horizon 7 desktops or published applications, on-premises web servers or content.

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

To deliver the Workspace ONE services outlined above and to address your use cases, you first need to design and build out the infrastructure components.

This section includes a low-level design of each product or area to consider. For more information, refer to the installation guides.

Workspace ONE Native Mobile Apps

For many users, their first end-user experience of Workspace ONE is likely through the Workspace ONE native mobile app. Available for each OS, the Workspace ONE app allows users to leverage the best technologies on each platform and experience a consistent look and feel across mobile apps and browsers. Features like Apple Touch ID 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 VMware AirWatch application types that have been enabled for a user or a device.
• A launcher to access SaaS and VMware Horizon virtual desktops and apps and ThinApp packaged apps, making discovery easy for end users.
• The ability to search across an enterprise’s entire deployment of app resources to find apps.
• SSO technology to allow simple user access to resources without remembering each site’s password.

Figure 9: Workspace ONE for Windows 10

The Workspace ONE native app is available from the various app stores and can be deployed through VMware AirWatch as part of a device enrollment process.
VMware Identity Manager

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

- **A user portal**, branded as Workspace ONE, which provides browser-based access to different types of applications, including SaaS-based web applications (such as Salesforce, Dropbox, and Concur), VMware Horizon-based applications and desktops, RDSH-based applications and desktops, ThinApp packaged apps, and Citrix-based applications and desktops. The portal simplifies application access for end users.

- **Enterprise identity management** to sync and extend on-premises directory credentials (such as Active Directory) to SaaS and native mobile applications.

- **Enterprise SSO** 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 easily while providing enterprise security and compliance controls to ensure that the right users have access to the right applications.

![Figure 10: User Workspace Delivered by VMware Identity Manager](image)
Design Overview
You can implement VMware Identity Manager using on-premises or SaaS-based implementation models. In an on-premises implementation, VMware Identity Manager is deployed as a Windows installer to handle authentication and provide SSO services to applications and desktops. In a SaaS-based implementation, a VMware Identity Manager Connector (virtual appliance or Windows installer) synchronizes user accounts from an on-premises directory to the VMware Identity Manager Service. Applications can then be accessed from a browser-based portal. You can use multiple appliances on premises for redundancy and scale.

Install and Initial Configuration
Because the VMware Identity Manager tenant is cloud based, you do not have to make design decisions regarding database, network access, or storage considerations. The VMware Identity Manager service scales to accommodate virtually any organization size.

Connectivity to the VMware Identity Manager service is through outbound port 443. This connection is used for directory synchronization, authentication, and syncing 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 involves logging in to the VMware Identity Manager service with the provided credentials at a URL similar to https://<company>.vmwareidentity.com.

For information, see the VMware Identity Manager Documentation, and select VMware Identity Manager Cloud from the drop-down menu.
Next Steps

Integrate VMware Identity Manager and VMware AirWatch

You must integrate VMware AirWatch and VMware Identity Manager in Workspace ONE for a number of reasons. Workspace ONE uses VMware Identity Manager for authentication and SaaS and VMware Horizon application access. Workspace ONE uses VMware AirWatch for device enrollment and management. The integration process is documented in Architecture Principles and Concepts.

VMware AirWatch

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

• **A device management platform** allowing full life-cycle 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 Console](image-url)
**Design Decision:** For this design, VMware AirWatch is implemented in a cloud-hosted model. Cloud hosting ensures that the latest VMware AirWatch features can be used without the need to upgrade on-premises infrastructure.

**Installation and Initial Configuration**
Because VMware AirWatch is being implemented as a cloud-based offering, installation of on-premises servers is not necessary for the core services. A VMware AirWatch tenant is provisioned, and an email provides details of the tenant name and login credentials. For the initial configuration, you log in with the provided credentials to the tenant with a naming convention similar to https://<companyname>.awmdm.com. You can redirect this to a custom URL, if needed.

Initial configuration of the VMware 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 VMware AirWatch, see the most recent VMware AirWatch Mobile Device Management Guide in AirWatch Resources.

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

**Next Steps**
*Integrate VMware Identity Manager and VMware AirWatch*
You must integrate VMware AirWatch and VMware Identity Manager in Workspace ONE for a number of reasons. Workspace ONE uses VMware Identity Manager for authentication and SaaS and VMware Horizon application access. Workspace ONE uses VMware AirWatch for device enrollment and management. The integration process is documented in Architecture Principles and Concepts.

**VMware Enterprise Systems 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 strategy allows an administrator to manage user accounts in Active Directory, have those accounts reflected in VMware AirWatch and VMware Identity Manager, and handle authentication to prevent the storage or synchronization of passwords outside of the enterprise.

VMware Enterprise Systems Connector provides a bundled, Windows-based installer of both connectors needed to integrate with each respective cloud service. You can deploy each service independently within separate Windows Server instances to provide high availability and disaster recovery architectures.
AirWatch Cloud Connector Design Considerations
AirWatch Cloud Connector is installed on a Windows Server on-premises after downloading the VMware Enterprise Systems Connector from the AirWatch Console.

<table>
<thead>
<tr>
<th>REQUIREMENT</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual machine or physical server</td>
<td>1 CPU core (2.0+ GHz). An Intel processor is required. 2 GB RAM or more</td>
</tr>
<tr>
<td></td>
<td>1 GB disk space for AirWatch Cloud Connector, Windows OS, and .NET runtime. An additional 5 GB of disk space is recommended for 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 7: AirWatch Cloud Connector Specifications

Server Requirements
AirWatch Cloud Connector supports installation on the following Windows Server versions:
• Windows Server 2008 R2
• Windows Server 2012
• Windows Server 2012 R2
AirWatch Cloud Connector also requires installation of .NET Framework 4.5.2.

Network Requirements
All traffic from AirWatch Cloud Connector is outbound from the server to the VMware AirWatch service and occurs over ports 80 or 443.

An outbound proxy or other connection management software or hardware must not terminate or reject the outbound connection from the AirWatch Cloud Connector. The outbound connection must remain open at all times.

For more information, see the most recent AirWatch Cloud Connector guide for SaaS customers in AirWatch Resources.

Load Balancing and Availability
AirWatch Cloud Connector traffic is load-balanced by the AirWatch Cloud Messaging component. It does not require a separate load balancer. Multiple AirWatch Cloud Connectors in the same organization group that connect to the same cloud messaging server for high availability can all expect to receive traffic (an active-active configuration). How traffic is routed is determined by the component and depends on the current load.
VMware Identity Manager Connector Design Considerations
The VMware Identity Manager Connector is installed on a Windows Server on-premises after downloading the VMware Enterprise Systems Connector from the AirWatch Console.

System Requirements
Table 8 lists the minimum system requirements for the virtual appliance (up to 1,000 users).

<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>50 GB</td>
</tr>
</tbody>
</table>

Table 8: VMware Identity Manager Connector Minimum System Requirements

<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 load-balanced servers, each with 4 CPU cores</td>
<td>2 load-balanced servers, each with 4 CPU cores</td>
<td>2 load-balanced servers, each with 4 CPU cores</td>
<td>2 load-balanced servers, each with 4 CPU cores</td>
</tr>
<tr>
<td>RAM (GB) per server</td>
<td>6 each</td>
<td>8 each</td>
<td>16 each</td>
<td>16 each</td>
</tr>
</tbody>
</table>

Table 9: VMware Identity Manager Connector System Scaling 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 the 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.</td>
</tr>
</tbody>
</table>

Table 10: VMware Identity Manager Connector Networking Considerations

For configuration information regarding communication ports, IP addresses for whitelisting, and addresses for the VMware Identity Manager service, see 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. A load balancer is required only in instances where an inbound connection to the connector is needed, mainly if Kerberos authentication is required.
To set up failover, 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 need to manually select another connector instance as the sync connector, because directory sync can be enabled on only one connector at a time.

For more information, see Configuring Failover and Redundancy for Connector Appliances in VMware Identity Manager Connector Installation and Configuration.

Active Directory Server Support

VMware Identity Manager supports user synchronization and authentication with other directories supporting LDAP.

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. To address these considerations, VMware AirWatch supports multiple methods of connecting devices to email infrastructure.

One challenge is that many organizations are moving to cloud-based email services, such as Microsoft Office 365 and Google Apps for Work. These services provide fewer email control options than the on-premises models that the enterprise has worked with. Previously, AirWatch Secure Email Gateway was deployed inside a corporate firewall and handled many aspects of secured email delivery to devices.

The next section looks at the connectivity models and the pros and cons of each.
AirWatch Secure Email Gateway Proxy Model

The AirWatch Secure Email Gateway 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 Console, the AirWatch Secure Email Gateway Proxy server allows or blocks email for every mobile device it manages. The AirWatch Secure Email Gateway Proxy server relays traffic only from approved devices. This relay protects the corporate email server by not allowing devices to directly communicate with it. Instead, the AirWatch Secure Email Gateway Proxy server filters all communication requests to the corporate email server.

Figure 13: AirWatch Secure Email Gateway Architectures
Direct PowerShell Model

In the PowerShell model, VMware AirWatch adopts a PowerShell administrator role and issues commands to the Exchange ActiveSync infrastructure to permit or deny email access based on the policies defined in the AirWatch Console. PowerShell deployments do not require a separate email proxy server, and the installation process is simpler.

---

**Figure 14:** Microsoft Office 365 Email Architecture

**Supported Email Infrastructure and Models**

To compare, these models support the following mail infrastructure:

<table>
<thead>
<tr>
<th>DEPLOYMENT MODEL</th>
<th>CONFIGURATION MODE</th>
<th>MAIL INFRASTRUCTURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy model</td>
<td>AirWatch Secure Email Gateway (proxy)</td>
<td>Microsoft Exchange 2010, 2013, and 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, and 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 11:** Supported Email Deployment Models
Microsoft Office 365 requires additional configuration for the AirWatch Secure Email Gateway proxy model. VMware AirWatch recommends the direct model of integration with cloud-based email servers. Table 12 summarizes the pros and cons of the deployment features of AirWatch Secure Email Gateway 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>AirWatch Secure Email Gateway</td>
<td>Real-time compliance Attachment encryption Hyperlink transformation</td>
<td>Additional servers needed Office 365 must be federated with Workspace ONE to prevent users from directly connecting to Office 365</td>
</tr>
<tr>
<td>PowerShell</td>
<td>No additional on-premises servers required for email management</td>
<td>No real-time compliance sync Not recommended for deployments larger than 100,000 devices VMware Boxer must be used to containerize attachments and hyperlinks in AirWatch Content Locker and AirWatch Browser</td>
</tr>
</tbody>
</table>

Table 12: AirWatch Secure Email Gateway and PowerShell Feature Comparison

**Key Design Considerations**

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

For more information on design considerations for mobile email management, see the most recent VMware AirWatch Mobile Email Management Guide in AirWatch Resources.

**Design Decision:** Because this design includes Microsoft Office 365 email, the PowerShell model is used with VMware Boxer. 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**

- Configure Microsoft Office 365 email through PowerShell
- Configure VMware Boxer as an email client for deployment as part of device enrollment
Microsoft Office 365 Basic Authentication Conditional Access

By default, Microsoft Office 365 basic authentication is vulnerable because credentials are entered in the app itself rather than to an IDP in a browser, as with modern authentication. However, with Workspace ONE, you can easily enhance the security and control over Microsoft Office 365 active flow.

You can now control access to Office 365 Active flows based on the following access policies in VMware Identity Manager:

- Network range
- Device OS type
- Group membership
- Email protocol
- Client name

Figure 15: Microsoft Office 365 Active Flow Conditional Access Policies

Content Integration

Mobile content management (MCM) can be a critical component to a device deployment. Ensuring that content is safely stored in enterprise repositories and available to end users when and where they need it with the 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 that the enterprise requires.

Content Management Overview

1. **AirWatch Managed Content Repository** – VMware AirWatch admins with the appropriate permissions can upload content to the repository and have complete control over the files that are stored in it.

2. **Corporate File Server** – Pre-existing repository that resides within an organization’s internal network or a cloud service. Depending on an organization’s structure, the VMware AirWatch administrator might not have administrative permissions for the corporate file server.
3. **AirWatch Content Locker** – The app that deploys to end-user devices, enabling access to content within the configured set of parameters.

4. **Personal Content Repository** – End users have complete control over the files stored here. End users can add 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.

5. **Content Gateway** – Provides secure access to content repositories or internal file shares. You can run it as a service on VMware Unified Access Gateway or as a standalone installer.

---

Figure 16: Mobile Content Management with VMware AirWatch

You can integrate AirWatch Content Locker with a large number of corporate file services, including Box, Google Drive, network shares, various Microsoft services, and most WebDAV supporting sites. It is beyond the scope of this document to highlight all of them.

For full design considerations for mobile content management, see 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 13.

<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</td>
</tr>
<tr>
<td>Enable Printing</td>
<td>Allows an application to print from devices</td>
</tr>
<tr>
<td>Enable Camera</td>
<td>Allows applications to access the device camera</td>
</tr>
<tr>
<td>Enable Composing Email</td>
<td>Allows an application to use the native email client to send emails</td>
</tr>
<tr>
<td>Enable Data Backup</td>
<td>Allows wrapped applications to sync data with a storage service like iCloud</td>
</tr>
<tr>
<td>Enable Location Services</td>
<td>Allows wrapped applications to receive the latitude and longitude of the device</td>
</tr>
<tr>
<td>Enable Bluetooth</td>
<td>Allows applications to access Bluetooth functionality on devices</td>
</tr>
<tr>
<td>Enable Screenshot</td>
<td>Allows applications to access screenshot functionality on devices</td>
</tr>
<tr>
<td>Enable Watermark</td>
<td>Displays text in a watermark in documents in the AirWatch Content Locker</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>Lists the applications that are allowed to open documents</td>
</tr>
</tbody>
</table>

Table 13: Data Loss Prevention Features

Content Gateway

Content Gateway provides a secure and effective method for end users to access internal repositories. Users are granted access only to their approved files and folders based on the access control lists defined in your internal repository via AirWatch Content Locker. To prevent security vulnerabilities, Content Gateway on Linux servers supports only Server Message Block (SMB) v2.0 and SMBv3.0. SMBv2.0 is the default. Content Gateway offers basic and relay-endpoint architecture models for deployment.

You can also deploy Content Gateway as a service on VMware Unified Access Gateway 3.1.

For more information, see the AirWatch Content Gateway Guide.

Key Design Considerations

Because this environment is configured with Microsoft Office 365, SharePoint-based document repositories are configured as part of the AirWatch Content Locker implementation. DLP controls are used in the Mobile Productivity Service and Mobile Application Workspace profiles to protect corporate information.
Conditional Access
Conditional access in Workspace ONE allows administrators to create access policies to resources beyond the evaluation of user identity and valid credentials. Combining VMware AirWatch and VMware Identity Manager, administrators can evaluate the target resource being accessed, source network from within the request is coming, and the type of device and current compliance status of the device being used. With these criteria, access policies can then provide a stepped-up authentication challenge only when needed or deny access when secure conditions are not met.

Configuration of compliance starts in the AirWatch Console. Compliance policies are created by determining a criterion to check, such as a jail-broken 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 14.

<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 the policy in case of the following:</td>
</tr>
<tr>
<td></td>
<td>• Blacklisted apps are installed on the device.</td>
</tr>
<tr>
<td></td>
<td>• Non-whitelisted apps are installed on 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 rule 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 rule 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, checks the device’s data usage when it is in roaming.</td>
</tr>
<tr>
<td>Free-Disk Space</td>
<td>This policy, when assigned to a device, checks and restricts the devices disk space usage.</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 rule 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

<table>
<thead>
<tr>
<th>COMPLIANCE POLICY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Last Check-In</td>
<td>A device is compliant with this policy if it has checked in at least once within the number of hours or days set by the admin. The policy runs based on the scheduler and not on the rules.</td>
</tr>
<tr>
<td>MDM EULA Acceptance</td>
<td>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 rules.</td>
</tr>
<tr>
<td>NA</td>
<td>This rule provides information on the profiles installed in the device. It does not impact any compliance policies.</td>
</tr>
<tr>
<td>Firewall Status</td>
<td>A device is non-compliant with this policy if the firewall is disabled.</td>
</tr>
<tr>
<td>Automatic Updates</td>
<td>A device is non-compliant with this policy if automatic updates are disabled.</td>
</tr>
<tr>
<td>Laptop Encryption</td>
<td>A device is non-compliant with this policy if the device is not encrypted.</td>
</tr>
</tbody>
</table>

Table 14: Access Policy Rules

With the AirWatch REST API, the definition of a device's compliance status can be extended beyond what is available within the AirWatch Console by leveraging an integration with one or more of the extensive list of VMware Mobile Security Alliance (MSA) partners.

For more information, see Mitigate Mobile Threats with Best-of-Breed Security Solutions.

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

![Figure 17: Enable Compliance Check and Authentication Through AirWatch](image-url)
**Figure 18: Device Compliance Policy**

It is also necessary to ensure that the device's universally unique identifier (UDID) is captured in VMware AirWatch and used in the compliance configuration. This feature works with Mobile SSO for iOS, Mobile SSO for Android, and certificate cloud deployment authentication methods.

**Note:** You must use the Device Compliance authentication method after first using a method that obtains the device UDID. Evaluating device compliance first does not result in a positive validation of the device’s status.

**Multifactor Authentication**

VMware Identity Manager supports chained, two-factor authentication. The primary authentication methods can be username and password or mobile SSO. You can combine these authentication methods with RADIUS, RSA Adaptive Authentication, and VMware Verify as secondary authentication methods to achieve additional security for access control.

**Standalone MAM and Adaptive Management**

Workspace ONE supports a variety of device and application management approaches. Standalone MAM 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 use SSO to access other VMware apps, 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, jail broken), 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, users can enroll their device into VMware AirWatch right from the Workspace ONE app, instead of downloading VMware 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 are prompted to enroll when they try to download, for example, Salesforce1, from the catalog.

![Figure 19: Adaptive Management](image)

No Star * icon indicates user can access without enrollment

Star * icon indicates app which requires management access
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.

![Image of AirWatch Application Deployment for Adaptive Management]

**Figure 20: AirWatch Application Deployment for Adaptive Management**

Data Loss Prevention

Apps that have been built for VMware AirWatch deployment can take advantage of app wrapping to be deeply integrated with VMware AirWatch management. App wrapping applies policies to a mobile app without changing the app itself. The app can also 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 adding a watermark to content when viewed on a device. You can configure these features on a platform level with iOS- or Android-specific profiles applied to all devices, or you can associate a specific application for which additional control is required.
VMware AirWatch applications, including VMware Boxer, 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 typically are not enabled for it out of the box.

**Figure 21: AirWatch Data Loss Prevention Settings**
Another set of policies can restrict actions a user can take with email. For managed email clients, such as VMware Boxer, restrictions can be set to govern copy and paste, prevent attachments from being accessed, or force all hyperlinks in email to use a secure browser, such as AirWatch Browser.

![AirWatch Boxer Content Restriction Settings]

Figure 22: AirWatch Boxer Content Restriction Settings

**VMware Verify**

VMware Verify is a two-factor authentication mechanism that allows using an iOS, Android, or Chrome app to enable multifactor authentication through VMware Identity Manager. It can use push notifications to a mobile device, which users can accept or deny. When the user’s device does not have cellular reception, such as in airplane mode when traveling, the user can open the VMware Verify app and use a one-time passcode (a soft token). Also, if you have users with flip phones, they can receive a one-time passcode over SMS. You can implement VMware Verify as the only type of authentication or as an additional factor when chained.

**VMware Verify Architecture**

VMware Verify can be enabled through the built-in identity provider in VMware Identity Manager. End users configure it when they authenticate against VMware Verify for the first time when they register their phone with the service. Additional devices can be enabled after the initial device is used to create a “circle of trust” to authorize the additional devices.
VMware Verify is already preconfigured in the cloud-hosted VMware Identity Manager product. For the on-premises version, contact VMware AirWatch support staff to get the security token required for the VMware Verify Adapter.

Figure 23: VMware Verify
Resource Types
A Workspace ONE implementation can include a number of different types of applications used in the enterprise.

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 an SSO 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 included, a wizard walks you through configuring the app and entitling users.

Figure 24: Add a New Application from the Cloud Application Catalog
Figure 25: Cloud Application Catalog

ThinApp Packaged Apps
ThinApp is a Windows 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. The VMware Identity Manager Connector must be deployed to enable using ThinApp apps in a Workspace ONE deployment.
VMware Horizon Apps and Desktops

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. Through the VMware Horizon clients available for native mobile platforms, access to these resources can be easily extended to mobile devices. You must deploy the VMware Identity Manager Connector to provide access to VMware Horizon 7 resources from the VMware Identity Manager cloud-hosted service. The connector enables you to sync entitlements to the service. It requires a means of accessing the resources from the Internet, such as VMware Unified Access Gateway.

![Figure 26: ThinApp Packaged Apps and VMware Horizon Application Configuration](image)

Native Mobile Apps

Native mobile apps from the Apple App Store, Google Play, or the Microsoft Windows Store have brought about new ways of easily accessing tools and information to make users more productive. A challenge has been making the available apps easy to find, install, and control. VMware AirWatch has long provided 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 VMware AirWatch service for distribution to end users.

![Figure 27: VMware Native Mobile Apps](image)
Unified App Catalog

When VMware 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 is enabled. This catalog pulls entitlements from both platforms and displays them appropriately in the Workspace ONE native app on a mobile device. The Workspace ONE client determines which apps to display and to which platform. For example, iOS apps appear only to devices running iOS, and Android apps appear only on Android devices.

Figure 28: Unified Catalog in VMware Identity Manager

Mobile Single Sign-On

One of the hallmark features of the Workspace ONE experience is mobile SSO technology. The ability to sign in to the app once and gain access to the entitled applications is a core capability. This capability can help address security concerns and password-cracking attempts and vastly simplifies the end-user experience for a mobile user. A number of methods enable the capability on both VMware Identity Manager and VMware AirWatch, as well as to the SaaS apps that users access. SAML becomes a bridge to the apps, but each native mobile platform requires different technologies to enable SSO.

iOS SSO

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 typically requires 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 VMware Workspace ONE Quick Configuration Guide.

**Mobile SSO for Android**
Workspace ONE offers universal Android mobile SSO, which allows users to sign in to enterprise apps securely without a password. Android mobile SSO technology requires the use of VMware Tunnel to authenticate users against SaaS applications.

**Windows 10 SSO**
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. VMware AirWatch can integrate with an on-premises CA through AirWatch Cloud Connector or an on-demand VPN.

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

**VMware Horizon 7**
VMware Horizon 7 allows users to create and broker connections to Windows virtual desktops, Linux virtual desktops, RDSH applications and desktops, and physical machines.

Table 15 lists the core VMware Horizon 7 components and features.

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizon Connection Server</td>
<td>An enterprise-class desktop management server that securely brokers and connects users to desktops running on VMware vSphere® virtual machines, physical PCs, blade PCs, or RDS.</td>
</tr>
<tr>
<td>Horizon Administrator</td>
<td>A web application that is part of the Horizon Connection Server, allowing administrators to configure the server, deploy and manage desktops, control user authentication, initiate and examine system events, and carry out analytical activities.</td>
</tr>
<tr>
<td>VMware Instant Clone Technology</td>
<td>Provides single-image management with automation capabilities. You can rapidly create automated pools or farms of instant-clone desktops or RDSH servers from a master image. The technology reduces storage costs and streamlines desktop management by enabling automatic updating and patching of hundreds of images from the master image. Instant Clone Technology accelerates the process of creating cloned virtual machines over the previous View Composer linked-clone technology. In addition, instant clones require less storage and are less expensive to manage and update.</td>
</tr>
<tr>
<td>View Composer</td>
<td>View Composer works with the Connection Servers and VMware vCenter Server®. It is the legacy method that enables scalable management of virtual desktops by provisioning from a single master image using linked clone technology.</td>
</tr>
<tr>
<td>Horizon Agent</td>
<td>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>Allows a physical device to access a virtual desktop or RDS application in a VMware Horizon deployment. You can also use an HTML client from devices for which installing software is not possible.</td>
</tr>
<tr>
<td>VMware Unified Access Gateway</td>
<td>Provides a method to secure connections in access scenarios requiring additional security measures, such as over the Internet. For more details, see VMware United Access Gateway.</td>
</tr>
</tbody>
</table>
### Table 15: VMware Horizon 7 Components and Features

#### Logical Architecture

This section focuses on the following core elements of View in VMware Horizon 7.

- Horizon Connection Server
- Horizon Agent
- Horizon Client
- View Composer (only required for deploying linked-clone pools)

Figure 29 shows the high-level logical architecture of these core Horizon 7 elements.

![VMware Horizon 7 Logical Architecture](image)

**Next Steps for Horizon 7**

A reference architecture was published to provide extensive information on building a VMware Horizon 7 environment. For more information, see the Horizon 7 Enterprise Edition Reference Architecture.
VMware Unified Access Gateway

VMware Unified Access Gateway is an optional component in a Workspace ONE deployment. It allows secure remote access from outside the corporate network to internally hosted resources, such as VMware Horizon desktops and published applications, and internal content, such as intranet sites and web applications. It was previously called Access Point.

VMware Unified Access Gateway is typically deployed within the corporate DMZ and provides secure remote access for users to access various edge services and resources within the corporate network.

Figure 30: VMware Unified Access Gateway Logical Architecture

VMware Unified Access Gateway can support multiple use cases and provide secure edge access to:

- VMware Horizon desktops and apps
- Reverse proxy (VMware Identity Manager on-premises)
- VMware Tunnel (per app tunnel and proxy services)
- Identity bridging
- Content Gateway (Content repositories or internal file shares with AirWatch Content Locker)

It also provides options for additional authentication methods from the DMZ:

- Smart card support
- Certificate
- SAML pass-thru support
- RADIUS support
- RDS SecurID support
Design Overview
A successful VMware Unified Access Gateway deployment is dependent on good planning and a robust understanding of the platform. This section discusses the design options and details the decisions that are made to satisfy the design requirements.

Network Deployment Options
You can deploy VMware Unified Access Gateway with one, two, or three network interface controllers (NIC). The decision is determined by your network requirements and discussions with the security teams to ensure compliance with company policy.

- **One network interface** – External, internal, and management traffic are all on the same NIC.
- **Two network interfaces** – External traffic is on one NIC. Internal and management traffic are on another NIC.
- **Three network interfaces** – External, internal, and management traffic all use their own NIC.

Load Balancing
It is highly recommended to use a load-balanced virtual IP (VIP) when deploying VMware Unified Access Gateway to ensure that the environment can provide local redundancy and also scale up or down with demand.

Using a load balancer facilitates greater flexibility by enabling IT administrators to perform maintenance, upgrades, and changes in the configuration without impacting users.

Next Steps for VMware Unified Access Gateway
An extensive reference architecture was published to provide information on building a VMware Horizon Enterprise environment that includes guidance on design for VMware Unified Access Gateway. For more information, see the Horizon 7 Enterprise Edition Reference Architecture.
Physical Environment Design
Several environment resources are required to support a Workspace ONE deployment. In most cases, they already exist.

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

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

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

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

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

Load Balancer
To remove a single point of failure from some components, VMware recommends deploying multiple instances and use a third-party load balancer. This practice provides redundancy and also spreads the load and processing across multiple instances of the component. To ensure that the load balancer does not become a point of failure, most load balancers allow multiple nodes to be set up in an HA or master-slave configuration.

Firewall and External Access Networking
External access to on-premises VMware Horizon 7 resources must be enabled through VMware Unified Access Gateway to access virtual apps and desktops from Internet-based mobile devices.

- Internal users connect to the VMware Identity Manager and VMware AirWatch services and any Horizon Connection Server over port 443. iOS devices that use mobile SSO also communicate to the KDC service in VMware Identity Manager over port 88.
- External users accessing VMware Horizon resources are redirected by the VMware Identity Manager service over port 443, which then communicates through the VMware Unified Access Gateway for Connection Servers over port 443.

More details are in the Network Ports in VMware Horizon 7 whitepaper and diagrams.
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.

Table 16 lists the parts required for each service. The rest of this section details the design and configuration of each service.

<table>
<thead>
<tr>
<th>Service</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>VMware AirWatch</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>VMware Enterprise Systems 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>VMware Horizon 7 or Horizon Cloud</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>VMware Unified Access Gateway</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

Table 16: Service Requirements
Common Components and Settings
There are common components and settings that are used in multiple services. To avoid repeating each individual service, they are outlined in the design first.

VMware Identity Manager and VMware AirWatch Integration
To successfully integrate VMware Identity Manager and VMware AirWatch, you can use the Workspace ONE Getting Started wizards. The Enterprise Connector & Directory wizard walks you through setting up the VMware Enterprise Systems Connector to allow the components of Workspace ONE, VMware AirWatch, and VMware Identity Manager to communicate with your Active Directory.

Documentation for this process is available in the VMware Workspace ONE Quick Start Guide.

Figure 31: Common Application Service Components
Enterprise Connector and Directory Integration Configuration Wizard

Use the Workspace ONE wizards to set up the enterprise connector, directory integration, and identity manager integration.

![AirWatch Console](image)

Figure 32: Enterprise Connector & Directory Configuration Wizard

VMware Enterprise Systems Connector Setup

The Enterprise Systems Connector is a unified connector consisting of AirWatch Cloud Connector and VMware Identity Manager Connector. It is used in the Mobile Device Management service and the Mobile Productivity service. The VMware Enterprise Systems Connector provides the ability to integrate VMware AirWatch and VMware Identity Manager with an organization's back-end enterprise systems. It is enabled in the AirWatch Console and downloaded to a Windows Server in the enterprise to enable communication between Active Directory and the Workspace ONE service. See the VMware Enterprise System Connector Installation and Configuration for more information.
Set up a password to download the Enterprise Connector installer. Use this password while running the installer on the virtual machine.

**Figure 33: VMware Enterprise Systems Connector Setup**

**Active Directory Integration**
When the Enterprise Connector is set up, enter your Active Directory and bind authentication information to integrate it with VMware AirWatch. Because you are making connections from Enterprise Connector, ensure that networking and server IPs and hostnames can be resolved.

**Figure 34: Active Directory Configuration Wizard**
VMware Identity Manager Integration

In the final step of the configuration wizard, enter the VMware Identity Manager and the authentication information.

**Figure 35: VMware Identity Manager Configuration**

Because you will be using VMware Identity Manager to authenticate users for SSO, select **No** for the prompt to use AirWatch to authenticate users.

**Figure 36: Select No to Use AirWatch to Authenticate Users**
VMware Identity Manager Connector Configuration
The VMware Identity Manager Connector provides connectivity to sync with the user directory, such as Active Directory. The VMware Identity Manager Connector also provides user authentication and integration with Horizon View, along with following capabilities:

• VMware Identity Manager Connector authentication methods, such as password, RSA Adaptive Authentication, RSA SecurID, and Radius
• Kerberos authentication for internal users
• Citrix-published resources

See the VMware Identity Manager Connector Configuration section to set up VMware Identity Manager Connector along with Directory Integration.

Catalog Population

<table>
<thead>
<tr>
<th>VMware Identity Manager Catalog Population</th>
<th>Configuration Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>SaaS Apps</td>
<td>• From the Catalog tab, choose Add Applications from Cloud Catalog. Integration documentation exists for several popular SaaS apps. • You can manually create SaaS apps that do not have a template in the cloud catalog with appropriate parameters. • Entitle the appropriate users of the applications being published, and choose whether the entitlement is automatic or manual.</td>
</tr>
<tr>
<td>View in VMware Horizon 7</td>
<td>• For the Mobile Application Workspace Service, because VMware Horizon resources are published, the View application pools must be published. Entitlements are synced from the VMware Horizon environment to VMware Identity Manager. • Horizon Connection Servers are added into the VMware Identity Manager catalog. • For external publishing, VMware Unified Access Gateway allows access to the VMware Horizon desktops and applications. See the Horizon 7 Enterprise Reference Design for more information.</td>
</tr>
</tbody>
</table>

Table 17: Configuration Considerations for a VMware Identity Manager Catalog Population
Native Mobile Apps

- In the AirWatch Console, you use the Apps and Books node 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 are then assigned to Smart Groups as appropriate.
- Application configuration key values are provided to point the Workspace ONE app to the appropriate VMware Identity Manager tenant.
- Recommended apps to deploy include the Workspace ONE app and popular VMware AirWatch apps, such as VMware Boxer, AirWatch Content Locker, and AirWatch Browser.

<table>
<thead>
<tr>
<th>VMWARE AIRWATCH CATALOG POPULATION</th>
<th>CONFIGURATION CONSIDERATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Profile Configuration</td>
<td>• Device profiles provide key settings that are applied to devices as part of enrollment in VMware AirWatch. The settings include payloads, such as credentials, passcode requirements, and other parameters used to configure and secure devices. Different payloads are configured in different services for this document, but SSO is a common requirement across all devices and use cases, so it is discussed in the Common Settings section below.</td>
</tr>
<tr>
<td>iOS SSO</td>
<td>• The iOS platform uses the Mobile SSO authentication adapter. The authentication adapter is enabled in VMware Identity Manager, added to an access policy, and a profile is deployed that provides the appropriate certificate payloads to support trust between the user, the iOS device, VMware AirWatch, and VMware Identity Manager.</td>
</tr>
<tr>
<td></td>
<td>• Run through the Mobile SSO Getting Started wizard to enable Mobile SSO in your environment.</td>
</tr>
<tr>
<td></td>
<td>• The Mobile SSO wizard creates an SSO profile that uses a certificate issued by the AirWatch Certificate Authority.</td>
</tr>
<tr>
<td>Android SSO</td>
<td>• Android uses the Mobile SSO authentication adapter. It is enabled in VMware Identity Manager, added to an access policy, and a profile is deployed to support SSO.</td>
</tr>
<tr>
<td></td>
<td>• Run through the Mobile SSO Getting Started wizard to enable Mobile SSO in your environment.</td>
</tr>
<tr>
<td></td>
<td>• The Mobile SSO wizard creates the necessary VMware Tunnel device profile, publishes the VMware Tunnel application, and creates the required network rules.</td>
</tr>
<tr>
<td></td>
<td>• For more information, see the VMware Workspace ONE Quick Configuration Guide.</td>
</tr>
<tr>
<td>Windows 10 SSO</td>
<td>• Windows 10 SSO uses certificate authentication. A certificate is generated from AirWatch CA through a SCEP profile. When a device profile is deployed, the appropriate certificates are generated for the user and installed on the user’s device. The Certificate (cloud deployment) authentication adapter is enabled to use Windows 10 SSO.</td>
</tr>
<tr>
<td></td>
<td>• The user is prompted to select a certificate at Workspace ONE app launch.</td>
</tr>
<tr>
<td></td>
<td>• For device compliance checking to function, part of the certificate request template for VMware AirWatch must include a SAN Type of DNS Name with a value of UDID={DeviceUid}.</td>
</tr>
</tbody>
</table>

Table 18: Configuration Considerations for a VMware AirWatch Catalog Population

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 are applied to devices as part of enrollment in VMware AirWatch. The settings include payloads, such as credentials, passcode requirements, and other parameters used to configure and secure devices. Different payloads are configured in different services for this document, but SSO is a common requirement across all devices and use cases, so it is discussed in the Common Settings section below.</td>
</tr>
<tr>
<td>iOS SSO</td>
<td>• The iOS platform uses the Mobile SSO authentication adapter. The authentication adapter is enabled in VMware Identity Manager, added to an access policy, and a profile is deployed that provides the appropriate certificate payloads to support trust between the user, the iOS device, VMware AirWatch, and VMware Identity Manager.</td>
</tr>
<tr>
<td></td>
<td>• Run through the Mobile SSO Getting Started wizard to enable Mobile SSO in your environment.</td>
</tr>
<tr>
<td></td>
<td>• The Mobile SSO wizard creates an SSO profile that uses a certificate issued by the AirWatch Certificate Authority.</td>
</tr>
<tr>
<td>Android SSO</td>
<td>• Android uses the Mobile SSO authentication adapter. It is enabled in VMware Identity Manager, added to an access policy, and a profile is deployed to support SSO.</td>
</tr>
<tr>
<td></td>
<td>• Run through the Mobile SSO Getting Started wizard to enable Mobile SSO in your environment.</td>
</tr>
<tr>
<td></td>
<td>• The Mobile SSO wizard creates the necessary VMware Tunnel device profile, publishes the VMware Tunnel application, and creates the required network rules.</td>
</tr>
<tr>
<td></td>
<td>• For more information, see the VMware Workspace ONE Quick Configuration Guide.</td>
</tr>
<tr>
<td>Windows 10 SSO</td>
<td>• Windows 10 SSO uses certificate authentication. A certificate is generated from AirWatch CA through a SCEP profile. When a device profile is deployed, the appropriate certificates are generated for the user and installed on the user’s device. The Certificate (cloud deployment) authentication adapter is enabled to use Windows 10 SSO.</td>
</tr>
<tr>
<td></td>
<td>• The user is prompted to select a certificate at Workspace ONE app launch.</td>
</tr>
<tr>
<td></td>
<td>• For device compliance checking to function, part of the certificate request template for VMware AirWatch must include a SAN Type of DNS Name with a value of UDID={DeviceUid}.</td>
</tr>
</tbody>
</table>

Table 19: Configuration Considerations for Device Profiles
Mobile Device Management Service

The mobile device management service brings an organization that has minimal device management capabilities, such as Exchange ActiveSync policies applied for passcode, wipe, and other basic settings, under an MDM strategy.

The devices are initially configured to support adaptive management, with some less critical applications enabled for SSO, while other applications require enrollment. Employees are encouraged, but not required, to enroll their devices. Users can use their native email clients, email apps available from the public app stores, or VMware Boxer.

![Diagram of VMware Workspace ONE Application](image)

**Figure 37: Mobile Device Management Service**
Adaptive Management

- Adaptive management enables applications such as WebEx and Concur to be used with mobile SSO across all platforms without device enrollment. Other applications, such as HR sites, ADP, or Salesforce, require device enrollment to have a high degree of control over the device.
- Users are encouraged to download the Workspace ONE app from a public app store.
- Applications that are deemed to have a higher risk to user or company data are set to require management in the VMware AirWatch device profile.

Active Directory – Cloud Password Authentication

- VMware Identity Manager is configured with a policy to use the cloud password from the built-in identity provider and authenticate via the VMware Enterprise Systems Connector to the Active Directory account.

Email Access

- Users are provided appropriate documentation on how to configure their device for native or third-party email client access. If users choose to install VMware Boxer, their email configuration is automatically pushed to the device. Typically, users are provided with the Exchange ActiveSync Server address (outlook.office365.com) and their email address and password.

Enrollment

- Enrollment is completed through the Workspace ONE application. If a user accesses an application that has been deployed as management required in VMware AirWatch, the enrollment process is initiated.
- Upon enrollment into Workspace ONE, end users have all applications available to them. They can also use mobile SSO after they have enrolled, because they have a device profile with the appropriate payloads deployed to authenticate with the appropriate SSO technology.
- Additional compliance information is passed to VMware Identity Manager. If the device is no longer in compliance, the user loses access to the VMware Identity Manager applications.

<table>
<thead>
<tr>
<th>DEVICE MANAGEMENT SERVICE DETAILS</th>
<th>CONFIGURATION CONSIDERATIONS</th>
</tr>
</thead>
</table>
| Adaptive Management               | • Adaptive management enables applications such as WebEx and Concur to be used with mobile SSO across all platforms without device enrollment. Other applications, such as HR sites, ADP, or Salesforce, require device enrollment to have a high degree of control over the device.  
• Users are encouraged to download the Workspace ONE app from a public app store.  
• Applications that are deemed to have a higher risk to user or company data are set to require management in the VMware AirWatch device profile. |
| Active Directory – Cloud Password Authentication | • VMware Identity Manager is configured with a policy to use the cloud password from the built-in identity provider and authenticate via the VMware Enterprise Systems Connector to the Active Directory account. |
| Email Access                      | • Users are provided appropriate documentation on how to configure their device for native or third-party email client access. If users choose to install VMware Boxer, their email configuration is automatically pushed to the device. Typically, users are provided with the Exchange ActiveSync Server address (outlook.office365.com) and their email address and password. |
| Enrollment                        | • Enrollment is completed through the Workspace ONE application. If a user accesses an application that has been deployed as management required in VMware AirWatch, the enrollment process is initiated.  
• Upon enrollment into Workspace ONE, end users have all applications available to them. They can also use mobile SSO after they have enrolled, because they have a device profile with the appropriate payloads deployed to authenticate with the appropriate SSO technology.  
• Additional compliance information is passed to VMware Identity Manager. If the device is no longer in compliance, the user loses access to the VMware Identity Manager applications. |

**Table 20:** Configuration Considerations for Device Management Service

Applications

<table>
<thead>
<tr>
<th>APPLICATION TYPES</th>
<th>CONFIGURATION CONSIDERATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>SaaS Applications</td>
<td>• SaaS applications are added from the Workspace One SaaS cloud catalog and entitled to appropriate users.</td>
</tr>
<tr>
<td>Native Mobile Apps</td>
<td>• Applications are added to the AirWatch Console. Privileged apps have the Require Management option selected; other apps do not.</td>
</tr>
</tbody>
</table>

**Table 21:** Configuration Considerations for Application Types
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. When 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 are required to enroll using the AirWatch Agent because of the higher level of control and security required for 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 use VMware Boxer 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 Microsoft Office 365, so federation with the Microsoft Office 365 service is enabled to allow SSO to the Office service and with the native mobile Microsoft Office 365 apps.</td>
</tr>
<tr>
<td>Data Loss Prevention</td>
<td>• DLP components are enabled within VMware Content Locker and VMware Boxer to prevent the use of unapproved applications, ensuring that data cannot be inadvertently or purposely copied to other apps using copy and paste.</td>
</tr>
<tr>
<td>Multifactor Authentication</td>
<td>• Multifactor authentication through VMware Verify is used when users need 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 SSO-based authentication. VMware Verify is also required on personally owned, non-managed PCs using only the browser to access SaaS apps.</td>
</tr>
</tbody>
</table>

Table 22: Configuration Considerations for Mobile Productivity Services
Federation to Microsoft Office 365

- Allows VMware Identity Manager to authenticate login requests to the Microsoft Office 365 service, accomplished using the Microsoft Federated Identity approach for Microsoft Office 365.
- For information about this configuration, see the video walkthrough and Converting Office 365 to a Federated Domain for Single Sign-On and Changing Office 365 Parameters to Workspace in Setting Up Resources in VMware Identity Manager.

Enable Federation in the Microsoft Office 365 or Azure AD Portals

- Sync Active Directory user accounts through the Azure AD or Microsoft Office 365 portals.
- Use PowerShell scripting to configure the Microsoft Office 365 service to authenticate through Workspace One as a federated identity provider. A set of PowerShell scripts with appropriate parameters and signing certificates establish trust between Microsoft Office 365 and VMware Identity Manager.
- **Note:** An important criterion to make Microsoft Office 365 integration work is ensuring that the attribute ObjectGUID is synced from AD to the VMware Identity Manager service.

Configure Microsoft Office 365 SAML Apps in VMware Identity Manager

- Using the templates in the Cloud Application Catalog, configure the Microsoft Office 365, WS-fed based template to allow authentication against VMware Identity Manager for Microsoft Office 365-based apps and resources, such as email, SharePoint, Lync, and other Microsoft Services.

<table>
<thead>
<tr>
<th>MICROSOFT OFFICE 365 FEDERATION</th>
<th>CONFIGURATION CONSIDERATIONS</th>
</tr>
</thead>
</table>
| Federation to Microsoft Office 365 | • Allows VMware Identity Manager to authenticate login requests to the Microsoft Office 365 service, accomplished using the Microsoft Federated Identity approach for Microsoft Office 365.  
• For information about this configuration, see the video walkthrough and Converting Office 365 to a Federated Domain for Single Sign-On and Changing Office 365 Parameters to Workspace in Setting Up Resources in VMware Identity Manager. |
| Enable Federation in the Microsoft Office 365 or Azure AD Portals | • Sync Active Directory user accounts through the Azure AD or Microsoft Office 365 portals.  
• Use PowerShell scripting to configure the Microsoft Office 365 service to authenticate through Workspace One as a federated identity provider. A set of PowerShell scripts with appropriate parameters and signing certificates establish trust between Microsoft Office 365 and VMware Identity Manager.  
• **Note:** An important criterion to make Microsoft Office 365 integration work is ensuring that the attribute ObjectGUID is synced from AD to the VMware Identity Manager service. |
| Configure Microsoft Office 365 SAML Apps in VMware Identity Manager | • Using the templates in the Cloud Application Catalog, configure the Microsoft Office 365, WS-fed based template to allow authentication against VMware Identity Manager for Microsoft Office 365-based apps and resources, such as email, SharePoint, Lync, and other Microsoft Services. |

Table 23: Configuration Considerations for Microsoft Office 365 Federation
### Email Configuration

<table>
<thead>
<tr>
<th><strong>Email Configuration</strong></th>
<th><strong>Configuration Considerations</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Integration with Microsoft Office 365 Through PowerShell</td>
<td>• VMware AirWatch issues commands through PowerShell to Exchange in Microsoft Office 365. Devices communicate directly with Exchange ActiveSync in the Microsoft Office 365 service. Full configuration information is in the most recent VMware AirWatch PowerShell Administration Guide in <a href="#">AirWatch Resources</a>.</td>
</tr>
<tr>
<td>Configure PowerShell Roles in Office 365</td>
<td>• PowerShell requires specific roles to be established in the Microsoft Office 365 Admin portal for Exchange. These roles enable the execution of PowerShell commandlets from VMware AirWatch to the Microsoft Office 365 service.</td>
</tr>
<tr>
<td>Configure Block - Quarantine Rules</td>
<td>• To prevent unpermitted devices from connecting to the Exchange Server, devices can be blocked or quarantined until they have enrolled. PowerShell commands are used to set the appropriate policy. These rules are not needed for environments where enrollment is not required.</td>
</tr>
<tr>
<td>Configure Email Compliance Policies</td>
<td>• Compliance policies for email include a range of options for controlling managed and unmanaged devices. Choices include if a managed device is required for email sync, if only certain email clients can sync mail, if device encryption is required for email sync, or if jail-broken or otherwise compromised devices are allowed.</td>
</tr>
</tbody>
</table>
| Configure ActiveSync Profiles for Email Clients | • Configure the Exchange ActiveSync payload for the device profiles to enable email sync. The hostname for Microsoft Office 365 is typically outlook.office365.com.  
• The domain, username, and email address are configured with lookup values. Make sure that these values are available in the directory and properly mapped from AD through the VMware Enterprise Systems Connector. |

Table 24: Configuration Considerations for Email

### Content Configuration

<table>
<thead>
<tr>
<th><strong>Content Configuration</strong></th>
<th><strong>Configuration Considerations</strong></th>
</tr>
</thead>
</table>
| Content Integration with Microsoft Office 365 | • Established through the AirWatch Console under the Content node.  
• From here, you configure templates for the SharePoint libraries in Microsoft Office 365, to sync to the mobile devices.  
• Full configuration information is in the most recent VMware AirWatch Mobile Content Management (MCM) Guide in [AirWatch Resources](#). |
| Create Office 365 SharePoint Document Libraries | • Use [https://portal.office.com](https://portal.office.com) to log in to Microsoft Office 365 and create SharePoint sites with document libraries containing content. |
| Create Content Templates in AirWatch for Automatic Deployment | • In the AirWatch Console, access the Content node, select Templates, and then select Automatic.  
• Configure SharePoint Office 365 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 is synced, choose Allow Offline Viewing.  
• If content is used with other apps, select Allow Open in Third Party Apps.  
• Review other security settings per your enterprise policy.  
• Assign appropriate groups to the repository. |
| Deploy AirWatch Content Locker | • Requiring AirWatch Content Locker as an automatic deployment to groups of users who using content from SharePoint ensures access to content. |

Table 25: Configuration Considerations for Content
<table>
<thead>
<tr>
<th>DATA LOSS PREVENTION CONFIGURATION</th>
<th>CONFIGURATION CONSIDERATIONS</th>
</tr>
</thead>
</table>
| DLP Configuration on a Global Basis | - You can set DLP configuration on a global basis, platform basis, or per application deployment.  
- For DLP settings to take effect, the application must support the DLP settings by being built with the AirWatch SDK or through app wrapping for an internal application.  
- VMware Boxer, AirWatch Content Locker, and AirWatch Browser are built using the SDK and honor the settings chosen. |
| Add the SDK Profile for iOS or Android Defaults | - SDK profiles allow global configuration of DLP settings that are applied to applications on the platform for which the profile is defined. Settings include enabling or disabling:  
  - Printing  
  - Composing email  
  - Location services  
  - Data backup  
  - Camera  
  - Watermarking  
  - Ability to open documents in certain apps |
| Enable Custom Policies for AirWatch Content Locker and VMware Boxer as Necessary | - AirWatch Content Locker can use the default policies defined in the SDK profile or be overridden. Require MDM Enrollment is an important setting to ensure that content is being accessed by devices that have previously enrolled. |
| Confirm Email Compliance Policies | - When configuring VMware Content Locker policies, it is useful to ensure that the email compliance policies match corporate standards, including requiring having a managed device to receive email. |

Table 26: Configuration Considerations for Data Loss Prevention
Enable a Built-in Authentication Adapter in VMware Identity Manager

- VMware Verify is an authentication method within VMware Identity Manager. Configuration consists of selecting a check box.

Add VMware Verify to Access Policies

- To use an authentication method, you add it to a policy. You can configure VMware Verify as a standalone authentication method in a policy, but it is typically chained with other methods to implement multifactor authentication. To use it in conjunction with Mobile SSO for iOS, click the icon and add VMware Verify. This action authenticates via Mobile SSO, then prompts for VMware Verify credentials.

Install VMware Verify

- VMware Verify is available from the Apple App Store, Google Play Store, and as an add-in for Chrome on Windows and macOS.

Enroll Phone with VMware Verify

- When users access VMware Verify for the first time, they are asked for a phone number. The phone number is then associated with the VMware Identity Manager service, and a notification is sent to the user’s device to enroll it.
- After enrollment, the user’s phone is issued an authentication token. If the phone can receive push notifications, it lets the user choose to allow or reject the authentication.

Register Additional Devices

- You can register additional devices for the end user by leveraging a previously registered device.
- When registering an additional device, an authentication request is sent to a previously registered device for verification.

<table>
<thead>
<tr>
<th>VMWARE VERIFY CONFIGURATION</th>
<th>CONFIGURATION CONSIDERATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable a Built-in Authentication Adapter in VMware Identity Manager</td>
<td>VMware Verify is an authentication method within VMware Identity Manager. Configuration consists of selecting a check box.</td>
</tr>
<tr>
<td>Add VMware Verify to Access Policies</td>
<td>To use an authentication method, you add it to a policy. You can configure VMware Verify as a standalone authentication method in a policy, but it is typically chained with other methods to implement multifactor authentication. To use it in conjunction with Mobile SSO for iOS, click the icon and add VMware Verify. This action authenticates via Mobile SSO, then prompts for VMware Verify credentials.</td>
</tr>
<tr>
<td>Install VMware Verify</td>
<td>VMware Verify is available from the Apple App Store, Google Play Store, and as an add-in for Chrome on Windows and macOS.</td>
</tr>
<tr>
<td>Enroll Phone with VMware Verify</td>
<td>When users access VMware Verify for the first time, they are asked for a phone number. The phone number is then associated with the VMware Identity Manager service, and a notification is sent to the user’s device to enroll it. After enrollment, the user’s phone is issued an authentication token. If the phone can receive push notifications, it lets the user choose to allow or reject the authentication.</td>
</tr>
<tr>
<td>Register Additional Devices</td>
<td>You can register additional devices for the end user by leveraging a previously registered device. When registering an additional device, an authentication request is sent to a previously registered device for verification.</td>
</tr>
</tbody>
</table>

Table 27: Configuration Considerations for VMware Verify

Conditional Access Policy Configuration

<table>
<thead>
<tr>
<th>ACCESS AND COMPLIANCE POLICIES</th>
<th>CONFIGURATION CONSIDERATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware AirWatch Compliance</td>
<td>Create a compliance policy for the appropriate platforms through the AirWatch Console. Criteria for evaluation can include jail-broken 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 an email notification to the user, then an email notification to an administrator, and ultimately blocking access to email if the device is not remediated in time.</td>
</tr>
<tr>
<td>VMware Identity Manager Compliance</td>
<td>VMware Identity Manager compliance checking is enabled via the policy configuration. Policies include device compliance with the AirWatch authentication adapter and other authentication methods, such as a password. You can use the policies in conjunction with network ranges, OS platforms, or specific applications, allowing varying requirements to evaluate whether an application can launch based on where users are, which device they are using, and how they are authenticating.</td>
</tr>
</tbody>
</table>

Table 28: Configuration Considerations for Access and Compliance Policies
Mobile Application Workspace Service

The Mobile Application Workspace Service has a similar configuration to the Mobile Productivity Service, but also includes access to VMware Horizon applications. VMware Horizon resources can be synced into Workspace ONE through an outbound-only connection from the VMware Enterprise Systems Connector on-premises. This method allows entitlements to sync to the service. Inbound access to the Horizon Connection Servers, virtual desktops, and applications is still required. Therefore, VMware Unified Access Gateway is also part of this solution.

Components in the Mobile Application Workspace have the following unique characteristics.

<table>
<thead>
<tr>
<th>VMware Identity Manager Connector</th>
<th>• 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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Horizon Entitlements</td>
<td>• Enabled through the VMware Identity Manager catalog by connecting to the View pools that expose user-entitled apps and desktops to both Horizon Cloud and VMware Horizon 7.</td>
</tr>
<tr>
<td>VMware Unified Access Gateway</td>
<td>• Enables external Horizon clients to securely access on-premises-based VMware Horizon 7 resources for virtual apps and desktops.</td>
</tr>
</tbody>
</table>

Table 29: Unique Characteristics of the Mobile Application Workspace Service

Figure 39: Dedicated Power Workspace Service – Applications
Deploy VMware Enterprise Systems Connector

- The connector is a Windows-based service that is installed on Windows Server. It is deployed and activated against a VMware AirWatch and VMware Identity Manager SaaS tenant. It is responsible for directory sync and user authentication. Instructions for deploying the connector are in *Deploying VMware Identity Manager Connector* in *VMware Identity Manager Connector Installation and Configuration*.
- The connector can support View entitlement sync when configured as an outbound only connector, which does not require 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 are in *Configure the Built-In Identity Provider for Authentication* in the *VMware Identity Manager Administration Guide*.
- This authentication method, when enabled, is referred to as Password (Cloud Deployment).

Configure Directory Sync

- After the connector is deployed, directory synchronization is performed to sync Active Directory users and groups to the VMware Identity Manager service. For more information, see *Configuring Active Directory Connection to the Service* in *VMware Identity Manager Connector Installation and Configuration*.

Enable Horizon 7 (View) Pools in VMware Identity Manager Catalog

- To make Horizon 7 resources available in the Workspace ONE app, View pools must be added through the VMware Identity Manager catalog. User entitlements for apps and desktops are made available through the VMware Horizon configuration and automatically appear in the Workspace ONE app and in a web browser.

Provide Access to VMware Horizon 7 from External Devices

- To access the resources made available through VMware Horizon, you must establish a means of access from Internet-based devices.
- You can configure VMware Unified Access Gateway along with True SSO to allow egress and provide connectivity to the VMware Horizon 7 Connection Servers. See *Deploying and Configuring Unified Access Gateway*.

Table 30: Configuration Considerations for VMware Identity Manager

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

Table 31: Configuration Considerations for VMware Horizon Client
Workspace ONE User Experience

Workspace ONE provides a consistent end-user experience, regardless of device. 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 OS on which it is deployed. This means that the user experience is the same for every OS, 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 one-touch authentication that uses mobile SSO features. On Windows 10, the native app can use Windows Hello to authenticate using a camera and facial recognition.

The following sequence provides a tour of the basic user experience on an enrolled iPad Pro iOS device:

1. In Workspace ONE from any device, select an app.

![Figure 40: Workspace ONE Windows 10 App and Workspace ONE iOS App](image)
2. The home screen of an enrolled iPad Pro configured to the Mobile Productivity Service displays the Workspace ONE Touch ID:

![Home Screen with Enrolled Device and Workspace ONE App Pushed Through Enrollment](image1)

*Figure 41: Home Screen with Enrolled Device and Workspace ONE App Pushed Through Enrollment*

3. Select the Touch ID for Workspace.

![Touch ID Integrated with iOS SSO](image2)

*Figure 42: Touch ID Integrated with iOS SSO*
4. In Workspace, the Bookmarks tab displays the SaaS and VMware Horizon apps.

Figure 43: Bookmarks for SaaS and VMware Horizon Apps

5. You can select the Catalog tab to see available apps that are not yet installed.

Figure 44: Unified App Catalog
6. The SAML SSO to AirWatch Self-Service Portal authenticates you.

![Figure 45: SAML SSO to AirWatch Self-Service Portal](image)

7. In the My Devices tab, you can select the following actions:

![Figure 46: My Device Tab](image)
8. The iOS home screen displays native apps:

![Figure 47: Native Apps on iOS Home Screen](image)

9. The AirWatch Content Locker Home Screen displays the My Content and Corporate Content repositories:

![Figure 48: AirWatch Content Locker Home Screen](image)
10. Select a repository to delve deeper:

![Figure 49: AirWatch Content Locker Repository](image)

11. Select another repository to explore further:

![Figure 50: Alternative Repository](image)
12. Select the Inbox to view email notifications:

![Image of VMware Boxer]

**Figure 51: VMware Boxer**
About the Authors and Contributors
This version of the Reference Architecture was updated by:

• Camilo Lotero, Senior Technical Marketing Manager in End-User-Computing Technical Marketing, VMware
• Shardul Navare, Senior Technical Marketing Architect in End-User-Computing Technical Marketing, VMware
• Graeme Gordon, Senior Staff End-User-Computing Architect in End-User-Computing Technical Marketing, VMware
• Adarsh Kesari, Senior Systems Engineer, AirWatch Sales Engineers in End-User-Computing Technical Marketing, VMware
• Roger Deane, Senior Solution Architect Manager in End-User-Computing Technical Marketing, VMware
• Chris Avedissian, Technical Marketing Manager in End-User-Computing Technical Marketing, VMware

The Reference Architecture for earlier versions, upon which some of the current version is based, was originally written by:

• Kevin Sheehan, Senior Product Manager, VMware
• Matt Coppinger, Director in End-User-Computing Technical Marketing, VMware
• Jim Yanik, Senior Manager in End-User-Computing Technical Marketing, VMware

To comment on this paper, contact VMware End-User-Computing Technical Marketing at euc_tech_content_feedback@vmware.com.