Technical White Paper: **2022**

VMware Workspace ONE Design Handbook

Your step-by-step guide to the digital workspace

Roy D. McCord, II
Senior Staff Architect, VMware Professional Services

vmware®

Table of contents

Part 1: Setting the Stage

Introduction and historical perspective

Let's get my biases and opinions out of the way. I think that digital workspace technology has been one of the biggest disruptors in business in recent years. Not just in IT, but in business as a whole!

Smartphones and mobile device management (MDM) tools such as VMware Workspace ONE® (formerly AirWatch) changed everything when it comes to end-user computing, and more specifically, how companies interact with their customers. With widespread adoption of intelligent mobile devices in the early 2010s, consumers' preferences changed forever. More specifically, iPhone and Android devices provided a platform to streamline everyday tasks like never before. Users began to expect and demand a consumer-style experience on their work devices. This grew to the point that offering MDM technologies at work became a competitive advantage for companies, and it remains this way today. Providing a positive digital employee experience is a huge factor when hiring and retaining top talent.

While I can't prove these opinions were ever stated aloud, these are the thoughts that went through employees' minds when working with their IT organizations during this period:

• "Why is this company-issued device so much worse than my personal device? Why do I need to carry two devices at all?"

• "Is that really the approval process I have to go through?"

• "Do I really have to wait four hours while you image my machine?"

No more imaging machines; no more company-issued mobile devices; no more long approval processes. Employees just wanted to be allowed to access company resources on their mobile device without compromising privacy. The same desire for a simplified, consumer-like experience on work devices ultimately led to a very important question:

• "Why do we need 'work-specific' devices anyway? Can't I just use my own?"

This, in turn, led to widescale adoption of bring your own device (BYOD) programs. Samsung and Google understood this trend faster than others and introduced containerized solutions early on that allowed consumers to separate their personal and professional data and applications on a single device.

This began with primarily smartphones, and for half a decade, the mobile and desktop/laptop worlds were managed separately. Once MDM technologies such as AirWatch began to prove how easy device management could be for administrators, laptops and desktops followed suit. Apple built out a suite of APIs that allowed macOS to be managed very similarly to iOS devices. Microsoft followed suit with enhanced and simplified systems, starting most significantly with Windows 10.

VMware has been at the forefront of this transformation from the beginning. From MDM in the early 2010s, to BYOD, to the Employee Experience group, and ultimately to the Anywhere Workspace: VMware has been the most significant driver of the evolution of modern software to support modern business processes.

This book aims to help organizations that have decided to adopt Workspace ONE technologies get the absolute most they can out of the solution. We'll cover the end-to-end process from road mapping to requirements gathering, from physical design to logical design, from rollout and adoption to benchmarking and optimization. Last and most importantly, I've provided a number of real-world examples so you can practice for yourself.

Qualifications, caveats and notes about the text

This wouldn't be a very complete technical work if it didn't come with a healthy list of assumptions and cautions. Before we begin, please heed the advice below.

First, and I can't stress this enough, please engage the help of a professional digital workspace consultant to plan, design, implement and roll out your Workspace ONE solution. Having led and worked with these professionals for years, I can tell you that they are truly incredible.

Working with a trusted consultant not only greatly improves the chances of a successful project, but it can also bring you perspectives from what has made other organizations successful in past implementations. For example, I'm sure it's quite helpful to read a book about how to wire a house, but I would still make sure to hire a professional electrician when it was time to wire something up.

Second, modern technology moves very quickly. While I predict and hope that the foundational principles of this book will remain relevant over the course of years, the technical specifics are likely to change over the course of months. Always verify the latest features, architectural specifications, and configurations on docs.vmware.com.

Third, this book does not aim to be a commercial. Although I'm currently employed by VMware, these recommendations are my own and have not been influenced by anything other than my experience and professional expertise. Still, I will reiterate here the importance of working with a professional digital workspace consultant (and architect where necessary) when building and designing Workspace ONE solutions.

Fourth, the views expressed in this book are my own and do not necessarily reflect the views of VMware, Inc. or its employees, partners, customers or stakeholders.

Develop a roadmap using the outcome-focused approach

The biggest reason that some organizations stumble out of the gate with Workspace ONE designs (or any technical designs, for that matter) is that they don't take the time to develop a proper roadmap using a repeatable, introspective process. What are the problems the business is facing? How does this manifest in IT? What IT capabilities do we need to build in order to solve for these deficiencies? Will these capabilities address the business issues previously discussed?

In best-of-breed IT organizations, capabilities and services are not developed in a vacuum. These groups rarely follow the "build it and they will come" mentality. Instead, they are laser-focused on their role in supporting the business and driving new capabilities to give the organization a consistent competitive advantage in the market. In short, great IT organizations are thinking WAY past the data center.

The worst IT organizations skip directly to IT capability and stop there. How do they decide what capability to build? Generally, the highest-paid person in the room drives the discussion, or the person with the strongest technical voice overwhelms the decision-making process. Instead of focusing on the needs of the business, the organization instead focuses on spending valuable time and capital building a solution that likely should have remained a side project.

This is the reason VMware developed the Outcome-Focused Approach (OFA), as well as the value models that inform it. The Outcome-Focused Approach is VMware's approach to IT maturity and has been used by organizations all over the globe to help develop short-term and long-term roadmaps. The foundation of the approach is built on a simple process shown below.[1]

1. VMware Outcome-Focused Approach - vmware.com/professional-services/outcome-focused-approach

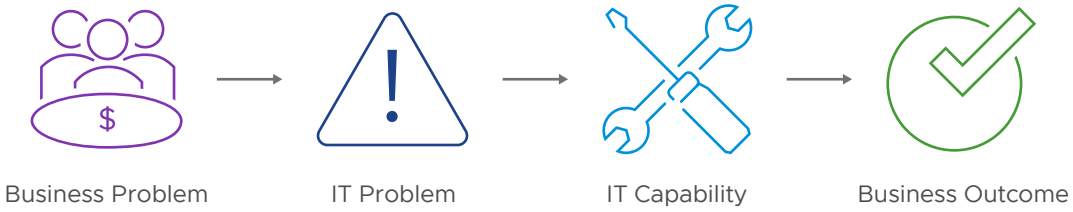

Figure 1: From business problems to business outcomes.

It's a powerful and simple concept, but so many organizations focus on only the second and third steps (or even worse, just the third). Succeeding with this process requires a strong interlock between your IT organization and key business leaders. Since Workspace ONE is so focused on outcomes for end users, you should make sure that your human resources (HR) department has a seat at that virtual table as well.

Before we go any further, it would be prudent to fully define the word "capability" as it's used in the Outcome-Focused Approach. A capability is not merely a set of technical tools built for an intended purpose. These capabilities can be matured either through self-development, with the assistance of a partner or third-party, or by engaging VMware directly. A true capability comprises the people, process, and technology required to provide a specified value back to the business. It probably comes as no shock that a large percentage of IT groups put far less emphasis on people and process than they should. Will the organizational model need to change as our technology evolves? What manual processes can be automated? Asking the right questions generally leads to more important questions. Don't be afraid to ask them.

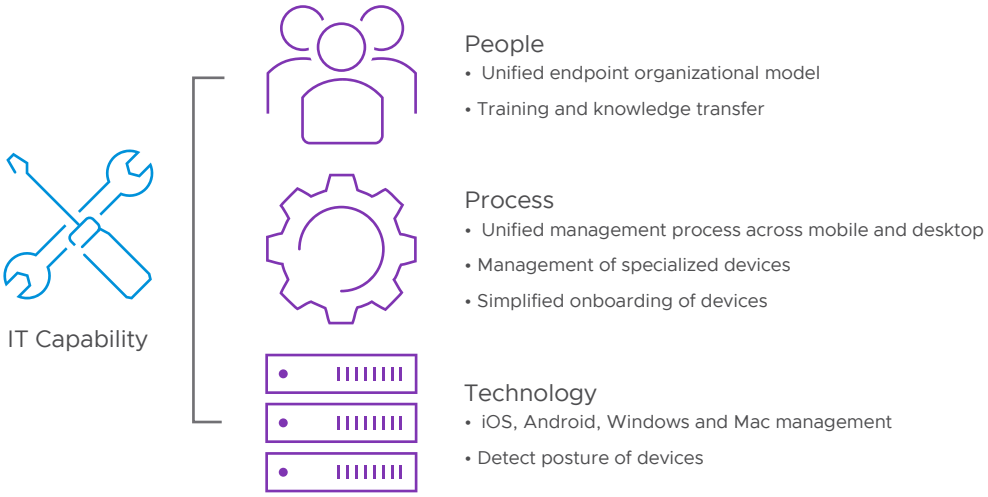

Figure 2: IT capabilities.

User communities and use cases

After you've charted a course and set a few initial goals, you'll need to determine which groups of users will receive the technology (user communities) as well as the manner in which that technology will be presented to them for one or more given purposes (use cases). Planning at this stage can tend to be cyclical in nature, so don't hesitate to return and double check your roadmap from the previous stage, or even to return to this step for retrospective at a future time.[2]

2. Use Case Definition - techzone.vmware.com/resource/business-drivers-use-cases-and-service-definitions

User communities

The first big decision is how to logically segment your users. Generally, the IT department has some precedent in how to rationally group the user base either through directory services or some other software package. When working with customers, I find that they often choose to segment the user base in one of the following two ways:

- By geography – AMER, EMEA, APJ, ANZ or sometimes by country, state or locality for smaller firms.
- By function – HR, finance, sales, education, field, etc.

How do you make this decision? I generally counsel customers to think deeply across two primary factors. Once you ask the right questions, I find the answers start to become obvious fairly quickly.

- What are the major differences in user experience between groups? Will a device in EMEA behave differently or present different applications and options than one in ANZ? Will a device in human resources present different applications and options than one in finance or sales?
- Are there different administrative concerns among different device sets? Are only EMEA-based IT admins allowed to manage EMEA devices? Are there unique administrators in sales or another business unit that need access to only a subset of these devices?

Segmentation will need to occur wherever you find differences. If administration and user experience differ primarily across GEO, segment by GEO. If administration and user experience differ primarily across function, segment by function. If these considerations vary across both of these elements, adjust accordingly.

Once you're ready to have a go at an initial list of user communities, list them out. We'll be referencing back to this frequently throughout the rest of the planning phase.

Use cases

Next, we'll need to decide what these user communities need in order to perform their jobs most effectively. The term "use case" might be the most overused one in the technology world today, and it tends to mean something a little different depending on what technical area you're focused on. For the purposes of Workspace ONE design, we'll use the terms "use case," "user experience" and "user story," mostly interchangeably. For us, a use case is a combination of applications, profiles, configurations and resources, utilized in such a way to promote an efficient use of a device for a specific set of purposes. To put it more succinctly…

> Use case = a user community + collection of apps/profiles/configurations/resources.

Figure 3: Use case definition.

So, let's start figuring out our use cases. What applications do your user communities need to do their jobs more effectively? Relating back to your desired outcomes and capabilities, what do your user communities need in order to build these? For example, your organization might have a team of field sales executives who travel frequently. They need access to secure mobile email, a suite of sales applications, regularly updated sales content, as well as booking and sales tracking applications. There's your use case #1. Your business may also have a team of developers. These developers need access to the latest coding tools and IDEs, secure mobile email, and possibly virtual desktops for testing. You now have use case #2. Practice your empathy by putting yourselves in the shoes of your target user community for a day. What tools and resources do they need to do their jobs from any device, anywhere? Better yet, ask them directly or hold focus groups. Make sure to certify that these use cases align with any business or technical requirements you've outlined and confirm that they help drive toward the goals and roadmap we outlined in the previous sections.

Allow me to close by mentioning a crucial point about use cases for Workspace ONE. In other technology areas, use cases are often dictated by the infrastructure. For the digital workspace, the opposite applies: the infrastructure you need is dictated by the use cases you've chosen. For example, if you've established a use case that one of your user communities needs tunneled application access to an internal resource, you will need to have a VMware Tunnel™ server to achieve the use case sufficiently.

Use cases are the most important factor when designing a Workspace ONE system. All other design decisions will be based upon the use cases you choose to implement. Make sure that these are carefully planned out in detail. Also, I highly recommend calling out your use cases explicitly in your project plan and tracking progress against their design, implementation, rollout and adoption regularly.

Requirements, assumptions, constraints and risks

Before jumping into developing a project plan, I always recommend detailing the following items:

- Business requirements: These are any requirements that are imposed by business (non-IT) factors that will affect the design for the solution. An example might be, "The leaders of the sales organization require all sales users to have mobile access to the global sales events calendar."
- Technical requirements: These are any requirements imposed by the current situation in IT. There are many categories of technical requirements: usability, security, manageability, etc. An example might be, "The system must house any administrative console behind two firewalls. Users must be on the internal network (or connected to the VPN) to connect to the administrative portal."
- Constraints: These are limitations that are unique to any specific business or technical situation. An example might be "The current mail system is on an out-of-date version of the software. This is a requirement due to a software integration that does not support the latest version. The mail system must remain on the previous version until this is mitigated by the vendor."
- Assumptions: These are any necessary items that we assume must be true for the design to function properly. An example might be, "The new server that will host the virtual machines for this system is on order. We assume that this will be delivered, installed and managed prior to installation of Workspace ONE."
- Risks: Risks are self-explanatory for the most part. For our purposes, a risk is any situation that could lead to potential failure of the solution. Some of these will be directly related to the requirements, constraints and assumptions you outlined in the previous section, which is why we leave this category for last. Also, make sure to list one or more mitigation steps for each risk you outline. An example might be, "There is a risk that the ongoing directory services migration could fail, leaving us without an active directory (AD) integration point temporarily." The mitigation might be, "We will discuss timing of the migration with the directory team and will encourage them to host a backup copy in a separate LDAP system."

Don't be bashful or embarrassed when listing these items out. Be up front and truthful about the current situation across both the business and your IT org. This is another area where a trained VMware consultant can really provide a great benefit. It's helpful to work with someone who has seen a variety of technical and business situations and can level-set which items are the most important.

Document all the items you can think of in a safe place like a shared team spreadsheet. Requirements, constraints, assumptions and risks should be revisited with your project manager on a regular basis throughout the entire project, as these items tend to change more quickly than most people assume.

Project planning (establish KPIs, focus on time-to-value)

There are many different opinions on how to structure a project, and none of them are inherently better or worse than any of the others. So, instead of getting into an endless debate over waterfall vs. agile, I'll provide two overriding principles for how to structure your Workspace ONE implementation for maximum success.

The first principle is to establish key performance indicators (KPIs) during the design phase of the project (or at least prior to implementation). This is the time to reflect on both your goals and list of user communities for the project. Which user communities are involved? What are you hoping to drive for each of those communities as a part of this project? Set S.M.A.R.T. (specific, measurable, achievable, realistic, time-bound) goals for each of these KPIs and establish touchpoints or milestones throughout your project plan. If some numbers don't meet your expectations, at least you will be able to change course during the project as opposed to after it's wrapped up.

What are some common examples of KPIs used for Workspace ONE projects, you ask? There are quite a few. "Devices managed" or "users enrolled" represent table stakes, but some companies get pretty creative with what they measure based on their goals for the solution. Some firms will measure times for common tasks before and after using a managed device and will utilize this as a tracking metric. If you're more focused on identity and access, you may want to measure the improvement in login times before and after implementing single sign-on (SSO). It's a bit of a cop-out, but these will certainly differ based on your unique implementation and business goals.

The second principle is to focus on minimizing time-to-value. For Workspace ONE, value is all about the number of devices on the platform and the increased employee productivity, satisfaction or customer revenue they ultimately helped drive in a given amount of time (i.e. your KPIs). For that reason, I recommend listing out your KPIs clearly and having dedicated touchpoints throughout the program to take measurements and check the numbers. Your most foundational KPI for the Workspace ONE platform will always be device or user count, so make sure to make this a fundamental part of your project plan. What is the minimum viable product (MVP) that you need in order to start enrolling devices? Think about a project phasing methodology that helps you promote these ideologies.

You might look at these two principles and challenge that I'm pushing you toward utilizing an agile methodology for your project. In truth, either waterfall or agile can be used to achieve these principles if done correctly. While agile might lend itself more to this approach directly out-of-the-box, you could employ a phased system with milestones if using waterfall. Work with your project management team to figure out what best suits your specific situation. This is another area where engaging with a VMware consulting expert can really help.

You should also take a hard look at your own IT organization and think about a program methodology that suits it best. While we talked earlier about altering processes and training personnel, your ability to do that prior to project kickoff will be limited. While I recommend challenging your organization to grow, also be realistic about what they will be able to execute, especially on a timeline.

Part 2: Logical Design

Primary components of the solution

I've never been a big fan of logical or conceptual designs. Having an engineering background, I'm always anxious to dive into the weeds of the solution, knowing or hoping that I'll figure out the big picture as I go along. As I've gotten more experience with unique customer situations and my understanding of the technology world has become broader, I'm finding more and more need to locate and comprehend quality logical design diagrams.

Note that both diagrams I'll show contain the Desktop and Application Virtualization components of the Horizon suite, which we won't cover in-depth in this book. For more information on VDI design, I'd recommend Johan van Amersfoort's two-part VDI Design Guide series, which can be purchased from Amazon or a number of other bookstores.

Below is the first logical diagram I really like for the VMware digital workspace. In the upper-left corner, we have the ultimate focus of every EUC project: employees and end users. These users access endpoints that are managed by UEM. By using single sign-on (SSO) and potentially multi-factor authentication (MFA), those same users are accessing applications through a self-service catalog based on a number of conditional or contextual access policies. Pulling these aspects together in dashboards

provides an aggregated view complete with environment-wide analytics. These items directly comprise the access management portion of the solution. Integration with virtual desktops and applications is represented with the Horizon suite of products. All of this sits along an intelligence engine comprised of a decision engine, notifications, remediations, automations and analytics. An API framework provides the glue that holds the solution together and also offers integrations with trust network partners to provide mobile threat defense, cloud access security, and endpoint detection and response.[3]

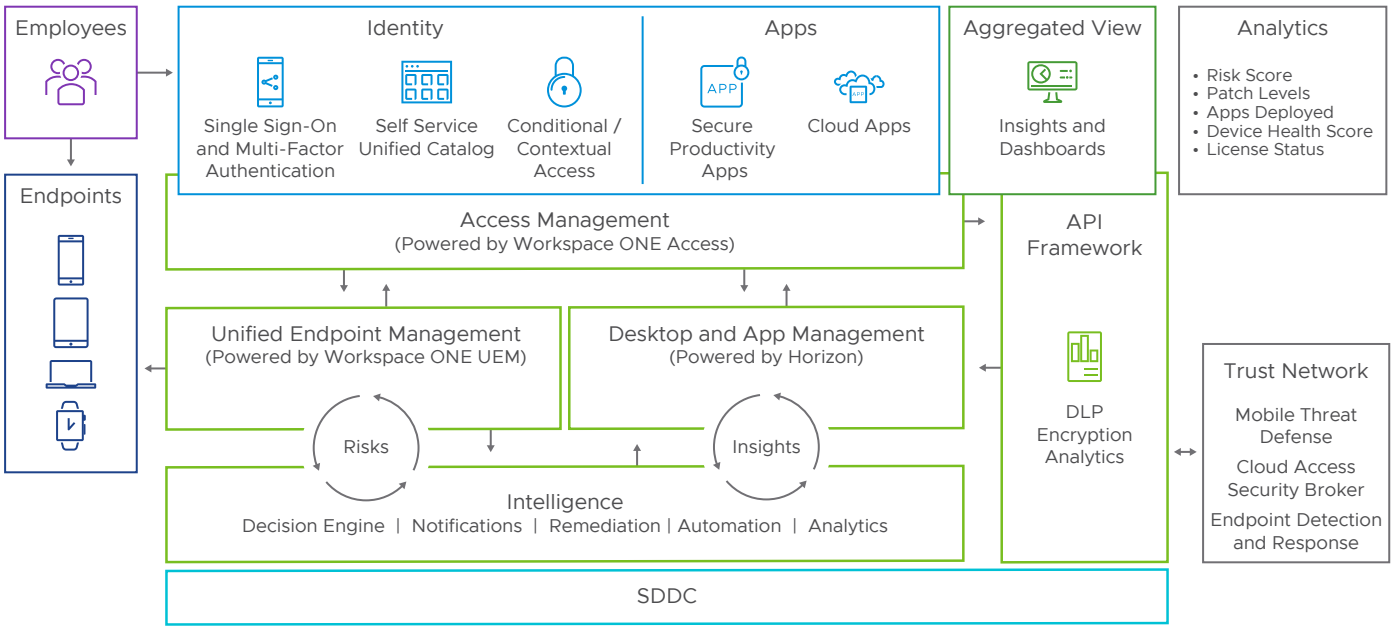

Figure 4: Digital Workspace comprehensive logical diagram.

Where the first diagram comprised the entire VMware Digital Workspace, the second diagram (below) dives more directly into Workspace ONE. Four outward categories of benefits are provided to users and administrators of the solution. The first is a top-rate digital employee experience. The second is simplified management of endpoints. The third is visibility and insights, which would also include automation and remediation. The final category is solution-wide security of the digital ecosystem. Next, platform-wide intelligence allows for automation, insights and reporting across the entire solution. Underneath, a number of platform services are provided by the stack including UEM, app lifecycle management, zero trust conditional access, VDI and published apps, mobile flows and secure apps, and SDKs. The context of these services is important, which is represented by the next row. Management of devices, things, virtual appliances, applications and potentially the network comprises the solution. Lastly, the solution is bolstered by the support of an ecosystem of integration partners as well as a robust API platform.

3. Digital Workspace Reference Architecture - techzone.vmware.com/resource/vmware-workspace-one-and-horizon-reference-architecture-overview

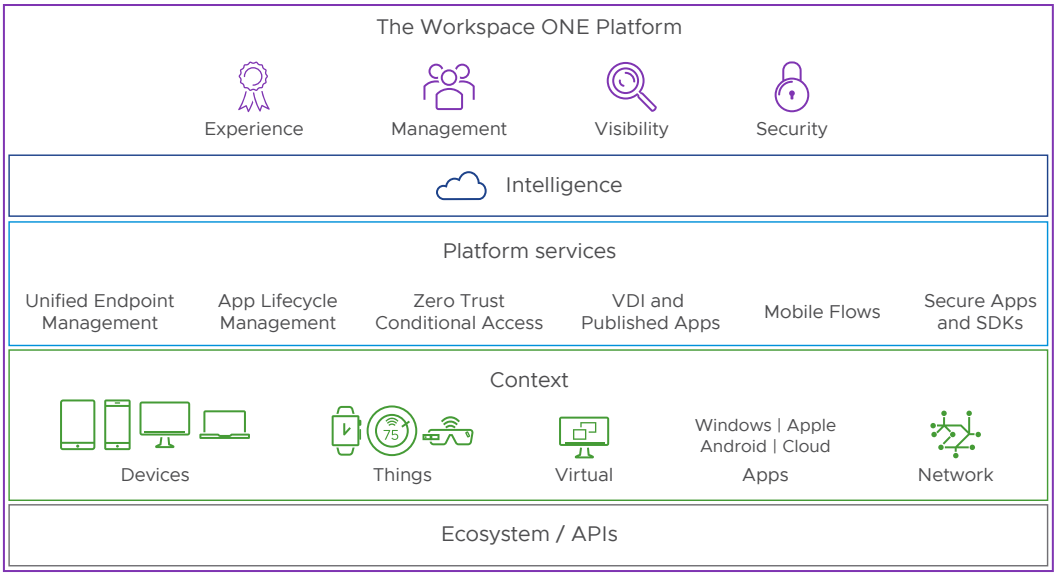

Figure 5: Workspace ONE logical diagram.

Ultimately, your unique solution will be dependent on the use cases you outlined earlier and the features those use cases will require. While I'm biased to recommend that you adopt the entire solution, I'm not foolhardy enough to recommend that you do it all at once. Rome wasn't built in a day, and neither were the best digital workspace environments. Attack a few use cases that are aligned to your business goals and keep evaluating the situation for places to add value through new capabilities comprised of people, process and technology.

Part 3: Physical Design

Software as a service (SaaS) or on-prem?

By the time you're reading this book, the question of whether to implement your Workspace ONE solution in a SaaS environment or on premises might have been made for you. Still, it's an important decision, which is why it's often the first question that a VMware design consultant or architect will ask. This is because the decision of SaaS vs. on-premises has a ripple effect through the entire architectural and solution design process.[4]

Key Decision Alert!

Will you choose SaaS or on-premises? While the decision might ultimately be made for you, the result will affect many of the future design decisions throughout this process. Choose wisely based on your business needs and IT situation!

Factors to keep in mind

So, let's hypothesize that the decision has not already been made on your hosting model. What factors should you keep in mind when faced with this decision? Below are the pros and cons I always walk through with customers when they are working to decide.

4. Workspace ONE Recommended Architecture Guide - docs.vmware.com/en/VMware-Workspace-ONE-UEM/2105/UEM_Recommended_Architecture/GUID-AWT-RECARCH-INTRO

- Server monitoring and maintenance: Simply put, in a world where you've purchased a SaaS tenant, the number of servers (virtual or otherwise) will be greatly reduced, although not totally eliminated. If going with an on-premises solution, you will be on the hook for the long-term monitoring and maintenance of the network, servers, etc. for the core components of the solution.
- Initial time to value: If going with the SaaS option, you can literally have your first device enrolled within minutes. When choosing on-premises, you'll need to install (or work with an expert to install) at least the core components of the solution to get started. For more on the core components, check out the "Physical Design" section later in the book.
- Upgrades: When choosing SaaS, upgrades are performed automatically for you by VMware. If you purchased the dedicated SaaS option, you will have the choice of when to upgrade to the latest version. When using shared SaaS, upgrades happen automatically as the latest generally available (GA) version of the software is released. If you choose an on-premises solution, you will need to perform the upgrades yourself, although VMware has professional services available to assist.
- Cost: There are some cost differences when choosing between SaaS or on-premises. With SaaS, your per-device license cost is generally slightly higher. This is to make up for the maintenance costs of the core servers. With on-prem you will spend additional up-front funds on resources for those core components, as well as the additional cost of deployment assistance. You'll also spend more time and effort maintaining and monitoring core servers over time.
- Data storage: While cloud-based solutions have been ubiquitous over the past decade, some firms still have business or security-focused reasons to keep data on premises. While the Workspace ONE SaaS solution is incredibly secure, I never argue with a CISO who brings a requirement that data remain on premises.
- Supportability: As someone who has been working with and around Workspace ONE for almost nine years, I can say pretty safely that on-premises environments introduce a lot of additional variables into the equation. Sometimes these additional variables can make troubleshooting more difficult. The simple fact that the core components are now living on an unknown network and unknown infrastructure presents new stages into any troubleshooting sequence that usually means more time.

What's your recommendation?

Though not a common occurrence, I am sometimes asked by prospective customers, "What is your recommendation on SaaS vs. on-premises, Roy?" I begrudgingly have to tell you that in 100 percent of these instances, I gave the classic consulting answer, "It depends." It depends on all the factors above and the importance of each in any given customer situation. It depends on inputs from your CISO, your short and long-term budget situation, your leadership, your company's culture, and your end users.

However, I also generally recommend that customers observe the trends of modern IT. The world is going to the cloud, and it's happening faster than most people expected. When I began designing Workspace ONE solutions for customers back in 2013, almost all of them had on-premises mail systems. Now, at least 90 percent of them are bringing cloud-based mail solutions. While directory services have been slower to move, I've still been surprised with how many companies are now choosing to utilize the cloud for this purpose.

If none of the factors in the previous section jumped out strongly for you, and all other things are equal, I will typically recommend choosing the SaaS option. The reason? Simplicity. IT administrators are under pressure like never before. If you have an opportunity to simplify your solution and therefore your long-term responsibilities, I'd recommend taking it.

Mapping core on-premises components

Note: While these sections do not apply to Workspace ONE administrators making use of VMware's SaaS offerings, reading them will still help you comprehend the underpinnings of how the solution works.

Workspace ONE UEM components

Workspace ONE UEM has three core on-premises components: device services, console services, and the database. Each of these components is described in detail below:

Device services: The device services server, often referred to colloquially as the "DS" server, manages communication from the MDM solution to devices. It manages queueing and deployment of profiles, app packages, and content to devices. Note that since mobile devices were not designed to have open ports (for security reasons), all communication originates at the device itself. To put it simply, the device must initiate the request, not the other way around. Remember our diagram in the Logical Design section earlier when looking to understand communication flows among mobile devices, cloud messaging, and device services.

The DS server also typically houses the AirWatch Cloud Messaging (AWCM) instance for the environment. AWCM can be utilized in place of certain third-party cloud messaging providers and is also used for certain intra-server communication flows. For very large instances of Workspace ONE (100,000+), you may want to consider separating the AWCM role onto its own server, especially if you will be utilizing it as a primary cloud messaging provider for certain device types.

When deciding where to place the DS server, security is typically the primary concern. Are you comfortable with devices from a coffee shop making requests to a server on your internal network? Most CISOs are certainly not comfortable with that idea. For this reason, it's typically recommended that you place your DS server(s) in the demilitarized zone (DMZ) of your corporate network. This allows the DS server to act as a gatekeeper of sorts, without exposing your internal network to potentially unknown device requests.

Console Services: The console server, sometimes abbreviated "CN," manages all administrative access to the environment. Accessing the console allows administrators to configure profiles, applications, device access rules, etc. It's also the configuration hub for integration components that we will discuss in the next section.

The CN server also generally is where the application programming interface (API) instance for Workspace ONE UEM is located. The API is utilized when administrators want to automate or script certain commands outside of the console graphical user interface (GUI). The API is also used for certain intra-server commands. Again, for large environments, or in situations where your organization wants to script or automate API-based commands, you always have the option of splitting the API role onto its own server(s).

The debate over where to place the CN server is often more heated and open to differing views. At the end of the day, the decision ultimately comes down to the comfort level of the security team. If the team is comfortable with placing the console in the DMZ, it potentially simplifies the process for administrators to login from external locations. The risk, however, is that this ease-of-access opens a vector for potential malicious attacks such as dedicated denial of service (DDoS). Most of the deployments I've personally done have featured an internal console server, but there is not a one-size-fits-all recommendation here except to consult the security experts at your organization before making a final decision.

Key Decision Alert!

Where will you place the console server? Installing in the DMZ may be more convenient for administrators to login from outside the network, but you leave an administrative system open to potential threats. We typically recommend installing behind the corporate firewall but have seen instances in which other security mitigations make the DMZ more viable. Again, it's all about the unique attributes of your organization and its IT makeup.

Database: The last primary component of the Workspace ONE UEM on-premises system is the database instance. This is housed in a Microsoft SQL™ server. The database stores all of the device records, user information, profile configurations, system settings, defaults, OGs and every other piece of data that gets displayed in the console. The database must have communication to both the CN and DS servers in order for them to function properly. For instance, commands to push a profile to a specific device are first queued in the database before getting picked up by the DS server.

The database is almost always located in the internal network behind secure firewalls for security purposes.

Now that we've covered all the primary components, let's build our first super-simple network diagram. We'll build on this throughout the following sections as we add components, but for now, these are the foundational pieces you'll need to build the bare minimum on-premises setup. Again, if you are utilizing a SaaS environment, all these things are taken care of for you.

A Note About Cloud Messaging

In the "Device Services" section above, we mentioned a bit about cloud messaging. It's important to understand how communication flows function between cloud messaging services, the device and Workspace ONE (specifically the DS server). This will help you better comprehend how commands are pushed to devices.

First, let's outline the types of cloud messaging services:

• APNS: Apple Push Notification Service[5]

• FCM: Firebase Cloud Messaging (formerly GCM – Google Cloud Messaging)[6]

• WNS: Windows Push Notification Services (WNS)

• AWCM: AirWatch Cloud Messaging

The key thing to remember is that mobile devices do not have open ports. You can't technically "push" anything to a device, even though mobile administrators do sometimes utilize this term to describe the flow. Mobile devices receive profiles, configurations and other information through cloud messaging. When you first configure your Workspace ONE UEM environment, you'll register with APNS and FCM. This will allow you to manage Apple iOS and Google Android devices once enrolled.

Once your Workspace ONE UEM environment is registered with third-party cloud messaging, these services are aware that you will alert them when a device has an active command in its system. The device, once enrolled, is also aware of the cloud messaging service and knows to establish a connection with it to check for new commands on a given interval. For this reason, the actual communication flow that describes the flow of initiated commands between these three parties (third-party cloud messaging, Workspace ONE DS, the device itself) is best visualized by a diagram such as the one below:

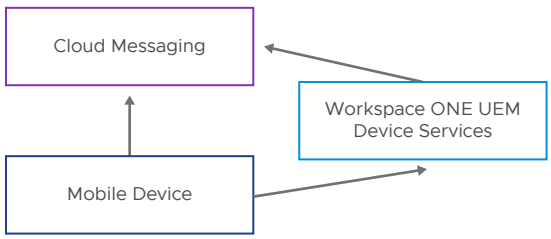

Figure 6: Foundations of MDM and cloud messaging.

5. Apple Push Notification Service - developer.apple.com/library/archive/documentation/NetworkingInternet/Conceptual/RemoteNotificationsPG/APNSOverview
6. Firebase Cloud Messaging - firebase.google.com/docs/cloud-messaging

When a new profile, configuration or other resource is assigned to a device, Workspace ONE alerts third-party cloud messaging, effectively saying, "Hey, remember that device I manage that you're aware of? I've got something for it. Next time it checks it, please tell it I have a resource."

On the next check-in interval for the device, it reaches out to cloud messaging. The cloud messaging server replies with, "Hey, you know that system that manages your enterprise resources? They have a message or resource for you. Go ahead and check in with them as soon as possible to get it." The device then reaches out to the DS server, receives the message, and then downloads any resource (profile, notification or otherwise) that the system has ready for it.[7]

While there are some exceptions to this sequence, and while you could certainly provide a more detailed back-and-forth than what's provided here, this is the primary flow that describes the fundamentals of modern MDM. The reason I go into this detail is that so many people assume that the opposite of this description is true. For instance, on my first week at AirWatch back in 2013 (this was before the acquisition by VMware), my technical lead asked me to draw this communication flow as I assumed it worked. My diagram was literally the exact opposite of the truth. For this reason, I always take a little extra time to diagram out this foundational principle of MDM.

Key Decision Alert!

Does it make sense to implement Workspace ONE Access for your organization right away? While some organizations sometimes choose to start with UEM and leave Access for a later project, I generally recommend against this. Implementing Workspace ONE Access and UEM simultaneously will help your organization take advantage of one of the most powerful features of the Workspace ONE suite: mobile single sign-on. If you are considering a BYOD program, Workspace ONE Access is a must-have and should probably be implemented in tandem with UEM.

Workspace ONE Access components

The on-premises footprint for Workspace ONE® Access™ is very straight-forward. It is comprised of a single server role, the Workspace ONE Access appliance, which can be deployed as a single node or as a series of three or more nodes for high-availability purposes. The appliance comes in the form of an Open Virtualization Appliance (OVA) file that can be easily deployed in your VMware ESXi™ hypervisor or other virtualization environment.[8]

Sizing and scaling for Workspace ONE core components

One of the biggest decisions you'll face during a Workspace ONE design is the sizing and scaling of your underlying infrastructure. How many virtual machines will you need? What resourcing should they contain with regards to CPU and RAM?

Luckily VMware provides scaling factors to help you make this determination. As of version 2105, the scaling factors below are recommended. Regardless of the current version, always verify the latest sizing and scaling recommendations on docs.vmware.com.

7. Apple Push Notification Service (APNs) - docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/iOS_Platform/GUID-ApplePushNotificationService
8. Workspace ONE Access Appliance - docs.vmware.com/en/VMware-Workspace-ONE-Access/20.10/workspace_one_access_install/GUID-0FABD001-050B-4A54-B100-2FA4E8F55613

Console Server Sizing				
	Up to 5K Devices	Up to 25K Devices	Up to 50K Devices	Up to 100K Devices*
Virtual Machines (Load-Balanced)	1	1	2	2
CPU Cores (each)	4	4	4	4
RAM (GB) (each)	8	8	8	8
Storage (GB) (each)	50	50	50	50

Device Services Server Sizing				
	Up to 5K Devices	Up to 25K Devices	Up to 50K Devices	Up to 100K Devices*
Virtual Machines (Load-Balanced)	1	2	3	4
CPU Cores (each)	4	4	4	4
RAM (GB) (each)	8	8	8	8
Storage (GB) (each)	50	50	50	50

Workspace ONE UEM Database Server Sizing				
	Up to 5K Devices	Up to 25K Devices	Up to 50K Devices	Up to 100K Devices*
CPU Cores	4	8	8	16
RAM (GB)	16	32	64	128
DB Size (GB)	100	250	500	750
Trans Log Size (GB)	40	100	200	400
Temp DB (GB)	40	100	200	300
Avg IOPs	150	750	1500	2000
Peak IOPs	300	1500	3000	6000

Workspace ONE Access Appliance Server Sizing					
	Up to 1K Devices	Up to 10K Devices	Up to 25K Devices	Up to 50K Devices	Up to 100K Devices*
Virtual Machines (Load-Balanced)	1	3	3	3	3
CPU Cores (each)	4	4	4	8	8
RAM (GB) (each)	8	8	8	16	32
Storage (GB) (each)	100	100	100	100	100

Workspace ONE Access Appliance Server Sizing					
	Up to 1K Devices	Up to 10K Devices	Up to 25K Devices	Up to 50K Devices	Up to 100K Devices*
CPU Cores (each)	2	2	4	8	8
RAM (GB) (each)	4	4	8	16	32
Storage (GB) (each)	50	50	50	50	50

*Note that at 100,000+ devices, it is recommended to have dedicated API and AWCM servers with separate scaling recommendations. Please check docs.vmware.com for the latest sizing and scaling recommendations.

A note about high-availability (HA) and disaster recovery (DR)

After viewing the sizing and scaling recommendations above, you may ask, "What happens if I lose a server?" or "What happens if I lose a data center?" Both are valid questions that you should be asking.

The sizing guidelines for VMware are designed to provide a minimum supported level of resourcing that still provides the optimal user experience for both administrators and end users. They do not account for the need for providing a highly-available environment or one that is resilient against disaster situations.

Before we get too deep into the weeds, let's clarify how I define HA and DR, as I have heard some debate on the topic. For the purposes of this book, I define high-availability as a set of mitigation steps meant to provide resiliency against the loss of a single server or VM within a given data center. I define disaster recovery as a set of mitigation steps meant to provide resiliency against the loss of an entire data center.

For these reasons, I recommend following very simple guidelines for HA and DR as it pertains to Workspace ONE. To provide adequate HA, add at least one load-balanced server (with identical specs) to the recommendations above (n+1) within the same data center. To adequately provide DR, you will duplicate the entire network topology (including the extra server(s) for HA) into a separate data center (2n) with suitable failover methodology in place.

Key Decision Alert!

Do you need HA? Do you need DR? The answer to the first question is almost always "yes." The second can get a bit more complicated. Is it a policy to implement DR for your IT systems? While implementing DR is a best practice, it's best to understand how Workspace ONE fits into the rest of your on-premises IT infrastructure. Over the long-term, however, I always recommend making a plan to implement DR as soon as it is possible.

Workspace ONE UEM integration components

Out-of-the-box, Workspace ONE UEM has all the tools you need to manage devices, configure profiles and policies, manage and distribute applications, and run basic reports. However, there are other integration components and servers that will greatly augment the functionality of your environment. Note that these components are optional but add additional capabilities that will be extremely helpful in helping you achieve the capability roadmap we laid out earlier.

VMware AirWatch Cloud Connector™ (ACC): The AirWatch Cloud Connector (ACC) is a server that helps integrate your Workspace ONE UEM environment with your enterprise resources. The most common of these is active directory (AD) or a lightweight directory access protocol (LDAP) instance for directory services. Integrating Workspace ONE with directory services will allow users to log in with their AD/LDAP credentials instead of utilizing another, unique set of login creds solely for Workspace ONE. The ACC is also used to integrate with certificate authorities (CAs), Syslog, and other enterprise services.

Just a quick note: The CN server is able to perform all of these integrations without use of the ACC. So why is it necessary? Security! Would you like a cloud-based console reaching out to your domain controller (DC) over port 443 all the way through your firewalls? Most CISOs would faint at the very notion! The ACC allows for a secure connection from the internal network out to VMware's cloud services to provide these necessary integrations without opening any unnecessary firewall exceptions.

For on-premises environments with the CN server hosted on the internal network, the ACC is usually not necessary. However, it can be helpful at offloading integration tasks for on-premises environments as well. It is also recommended if you choose to house your CN server in the DMZ for security reasons.

The ACC server is almost always housed in the internal network so it can directly integrate with enterprise components without the need to open additional firewall rules.

A few final notes about the ACC server and what makes it such an elegant solution to the problem of secure enterprise integration. Much like the discussion we had about mobile devices earlier, the UEM console never needs to initiate a connection to the ACC. The ACC actually reaches out to the UEM console through AWCM. Since the ACC is always the party establishing communication, you do not need to open any special ports to the ACC from the UEM SaaS environment. Another benefit to this configuration? Since there are no inbound connections to the ACC, you will not need to load-balance traffic when installing more than one for HA purposes. Just install one or more additional ACCs on the same subnet, and you're good to go. The ACC will detect the additional server(s) through AWCM and load balance requests automatically.[9]

Unified access gateway (UAG)

The unified access gateway (UAG) is a server that maintains many integration server roles. It is utilized for both on-premises and SaaS Workspace ONE UEM environments. The UAG, and thus the server roles below, are typically housed in the company DMZ. The following server roles are housed within the UAG server application.

- VMware Tunnel: The VMware Tunnel server provides the ability for applications to tunnel securely into the internal network to access corporate resources. Have an internally-developed application that needs access to an internal database? Using the Workspace ONE SDK alongside the VMware Tunnel can make this configuration possible. The Tunnel server also supports

9. AirWatch Cloud Connector - docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/WS1-ACC.pdf?hWord=N4IghgNiBc4JYCcDuYAuBjAFgAnRA9gK4Amu+AduQKbqr4IgC+QA

per-app VPN, which provides the ability for device-side segmentation of traffic through a VPN. Need to provide users the capability to access internal websites from a coffee shop, but don't want to load down your VPN with a bunch of unnecessary internet traffic? Setting up per-app VPN alongside adequate tunnel configurations makes this simple.[10]

- Content Gateway: The Content Gateway allows the Workspace ONE Content application (formerly AirWatch Content Locker) to integrate with internal or external file stores such as SharePoint™, Google Drive™, traditional on-premises file servers, and others. One of the most unique use cases I saw for the Content Gateway was for a customer I worked with a few years ago. This firm had a fleet of sales representatives that traveled the country and held daily meetings with retail buying agents. Every day, each seller would be shipped a new binder of sales information (flyers, customer notes, etc.) to the hotel at which they'd be staying. The cost of printing and shipping these binders was overwhelming. We replaced the solution with the Workspace ONE Content application, the Content Gateway server, and an integration to an internal file server. With the proper configuration, each seller was able to access all the unique sales material for each day on their tablet device. The customer saved a ton of money, and the solution was better for the environment as well.
- Secure Email Gateway (SEG): The Secure Email Gateway (SEG) server acts as a mail proxy for devices to access internal mail servers. While the recent prevalence of cloud-based mail servers has made these situations less common, the SEG is still a great way to secure your on-premises mail infrastructure. Instead of requiring potentially compromised devices to access your mail system with requests, the SEG can be configured to proxy these requests based on device compliance rules.

Prior to integration with the UAG, each of these roles comprised separate servers, and you still technically have that option today. If you prefer, you can create separate VMs for your VMware Tunnel, Content Gateway and SEG servers. However, the simplicity of utilizing the UAG for these purposes means that most customers choose the UAG method. If using the VMware Tunnel and/or Content Gateway roles, I typically recommend installing UAG in a front-end/back-end topology, meaning you will install a UAG front-end in the DMZ followed by a UAG back-end in the internal network. This provides security and trackability of network traffic from end to end for these roles. The SEG role is typically installed on a machine located in the DMZ.

Key Decision Alert!

Do you need a UAG? It all depends on what resources your devices need access to? On-premises email? Internal content stores? API endpoints? Intranet sites? If you said "yes" to any of these, you may need a UAG!

Workspace ONE Access integration components

Workspace ONE Access uses one simple integration component: the Workspace ONE Access Connector server. The Workspace ONE Access Connector server typically lives in the internal customer network and integrates with AD, RADIUS and RSA SecurID to assist with user authentication.[11]

The Connector server is fairly simple in nature. It reaches out to the Workspace ONE Access appliance server (typically in the DMZ) over port 443 to establish communication (similar to the ACC for Workspace ONE UEM). Since it is generally located in the internal network, there is no need to open firewall ports for integration to AD, RADIUS or other services.

The Workspace ONE Access Connector server contains three separate services: directory sync, user auth and Kerberos auth. You can choose to install these services all on the same server or on separate servers if you prefer. Sizing for the connector is highly dependent upon which combination of services you choose to install where, so I will refrain from reprinting every combination here. Just as before, always make sure to check docs.vmware.com for the latest sizing and scaling recommendations.[12]

10. VMware Tunnel - docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/WS1_Tunnel_Linux.pdf?hWord=N4IghgNiBcIG4FsDuYBOBTABAFwK4Dt90oBfIA
11. Workspace ONE Access Connector - docs.vmware.com/en/VMware-Workspace-ONE-Access/services/Workspace ONE_access_connector_install/GUID-271C47F6-856C-40F0-97AB-A8AD95025F9C
12. Workspace ONE Access Connector Sizing - docs.vmware.com/en/VMware-Workspace-ONE-Access/services/Workspace ONE_access_connector_install/GUID-6A070A5E-3DC3-4D2F-AE5B-8A8201310C92

Part 4: Solution Design

Creating an organization group (OG) structure

Remember earlier when we mapped out our user communities and use cases? All that pre-planning is going to pay huge dividends now, because it will save you a lot of time when contemplating how to logically organize users, groups, devices, configurations and settings within your Workspace ONE UEM environment.

There are many ways to segment devices within Workspace ONE UEM, and everyone seems to have their preference. I will not argue with administrators who prefer to throw all devices in a single group and then use device types or tags to logically separate them. However, for the first-time admin, I always highly recommend using the most foundational form of logical segmentation: organization groups (OGs).

Organization groups are the foundation of Workspace ONE's multi-tenant infrastructure. Profiles, configurations and settings can all be configured at "parent" OGs and then either inherited or overridden at "child" OGs.

When designing OG structures, we typically use the same logic utilized earlier:

- What are the major differences in user experience between groups?
- Are there different administrative concerns among different device sets?

Both of these are reasons why devices may need to be separated. Use cases and administration are generally the deciding factors in how to plan out an OG structure. Let your "user communities" table from the previous section be your guide as much as possible here.

A lot of great OG structures have been initially mapped out in a very rough fashion on a scrap of paper or the back of a napkin. Just make sure to move it into a more legitimate document before too long.

Once you come to a decision on how to create your OG structure, I always recommend mapping it out in a tool such as Microsoft Visio™, Microsoft PowerPoint™, Miro™, or some other easy mapping tool. You should be able to create something similar to the map below:

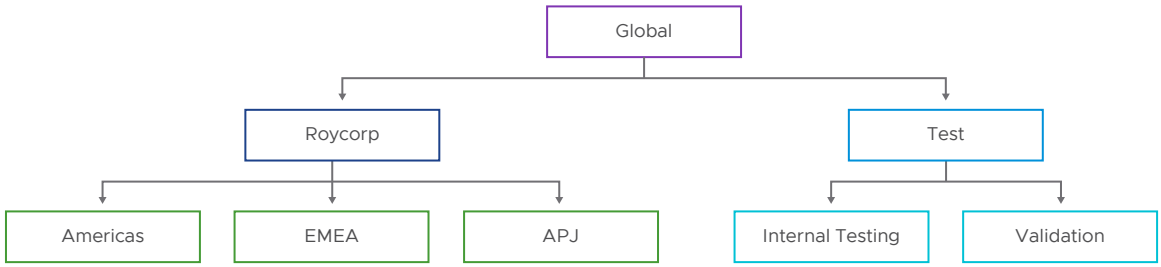

Figure 7: An organization group (OG) diagram.

Enterprise integration

After we've planned out our environment structure using OGs, we'll want to complete the primary enterprise integration tasks. The term "enterprise integration" comprises all the items below.

- Certificate authorities
- Content Gateway
- Directory services

- Email (SMTP)
- VMware Tunnel
- VMware Tunnel Proxy
- Peer distribution
- Third-party proxies
- Pull service installers
- SMS
- Syslog
- Workspace ONE Access

We will not be covering every single configuration option within the Workspace ONE UEM console. This book is designed to lead you down the design path intended to make you most successful with the most common configurations for success. At the risk of overstating this point, this is where the help of a knowledgeable VMware consultant can help you customize a solution that fits your unique needs. I've ordered the sections below in the order I recommend you undertake your design for enterprise integration.

Key Decision Alert!

Which enterprise systems will you connect to? Granting access to internal systems (in a secure fashion) can improve employee productivity and reduce frustration, especially when implementing BYOD and/or work-from-anywhere initiatives.

Directory services

The most significant of these steps is hooking the system up to directory services so that corporate users will be able to enroll their devices using directory credentials. This will also allow administrators to utilize directory-based credentials when logging into the system. If you have a SaaS tenant of Workspace ONE UEM, you will need to install the ACC server in your network to integrate with directory services securely. If you are planning to use Workspace ONE UEM on-premises, you have the option of integrating to directory services directly.

Certificate authorities

This area of the console will help you integrate with a number of different types of certificate authorities (CAs). Hooking up to a CA will allow you to deliver certificates directly to a mobile device for the purposes of authentication, typically against a VPN or Wi-Fi network. After configuring the ACC to communicate with the CA, you'll need to configure a certificate template as well as a certificate payload in the associated profile you'd like to use the certificate against.

Email (SMTP)

Do not confuse this enterprise integration step with full email integration. Integration with your corporate Simple Mail Transfer Protocol (SMTP) instance effectively allows you to redirect the automated emails sent from the Workspace ONE console to be sent directly from your organization. Let's say you'd like an automated email to be sent to a user if their device becomes compromised. By default, that email will be sent to users from Workspace ONE. While you can customize these messages and templates, some administrators would prefer these emails to come directly from the organization. Integrating directly with an SMTP endpoint allows you to do just that.

Workspace ONE Access

This is where you will integrate your Workspace ONE Access tenant with your Workspace ONE UEM environment. Integrating with the Identity & access features of Workspace ONE Access provides the ability to front-load the end-user experience with applications rather than device management. We will talk much more about Workspace ONE Access in the sections below.

VMware Tunnel

We spoke in depth about the VMware Tunnel back in the Unified Access Gateway (UAG) section earlier. The VMware Tunnel allows for secure per-application tunneling from external devices into endpoints (websites, servers, etc.) in the corporate network. When using the tunnel role, we typically recommend a front-end/back-end configuration, where a front-end tunnel is installed in the DMZ, and a back-end tunnel is installed in the internal network.

Content Gateway

We also covered the Content Gateway when discussing the UAG. The Content Gateway specifically allows the VMware Content application to access both internal and external corporate file stores.

Mobile single sign-on (SSO) with Workspace ONE Access

Background and significance of mobile SSO

No technological leap in the mobile world was as significant as the slick introduction of mobile single sign-on (SSO). When SSO became part of the UEM toolbox in the mid-2010s, it opened a whole new world of possibilities to mobile administrators. More than that, it made mobility experts question the very foundations of MDM. The question that changed everything was…

- Why do we have to lead the employee experience with the hassle of device enrollment? Why can't we make the application catalog the front-end of the experience?

This was a bold idea. Identity & access was not a new technology area. Companies had been utilizing SAML and OAuth-based identity providers for years. But, when combined with mobile management, the prospect of true, seamless mobile SSO became a possibility. Workspace ONE Access was born.

It's astounding just how much Workspace ONE Access has improved my personal employee experience at VMware. If I need to check my retirement account or my HSA balance, I access the tools through Workspace ONE Access. If I need to use internal tools to help develop new professional services offerings, I log in through Workspace ONE Access. If I need to fill out an expense report, I use Workspace ONE Access to sign on seamlessly. No more remembering 1,000 passwords. I remember one, and I'm good to go. The best part is that this experience flows directly over to my mobile device as well. Let's say I'm on the golf course and realize I forgot to submit that expense report yesterday? I use the Intelligent Hub app on my phone to access it directly. No more rushing to the clubhouse in the middle of the best round of my life to beg the staff to let me use their computer. Mobile SSO has truly been a transformative technology. What's more, this is the technological advance that evolved MDM into the Digital Workspace.

As we'll cover in more depth later, mobile SSO also made bring-your-own-device (BYOD) a much more viable solution for the average user. Mobile SSO pushed the enrollment requirement back to only the applications where it was absolutely necessary. Otherwise, users were free to access applications without any specific corporate controls on the device. If you need more security, the tool can integrate with MFA providers. If you already have a major identity provider, we can configure authentication chains where either the existing provider or Workspace ONE Access is the front-end. The flexibility of the solution is another major plus.

Identity provider vs. service provider

Identity & access management is a big topic. I'm not going to attempt to cover all the foundations of security assertion markup language (SAML)-based authentication, but I do feel it's important to cover the basic flows, especially the difference between an identity provider (IdP) and a service provider (SP).

The identity provider is effectively the portal that the user will login to and interact with. It handles the initial authentication with the user and then directs the request back to the service provider. The service provider is exactly what it says: it provides a service that the user is hoping to receive. For example, if I am hoping to update my sales numbers in a work-based portal, that sales portal is the service provider. The chart below helps describe the authentication flow between a user agent, the IdP and the SP.

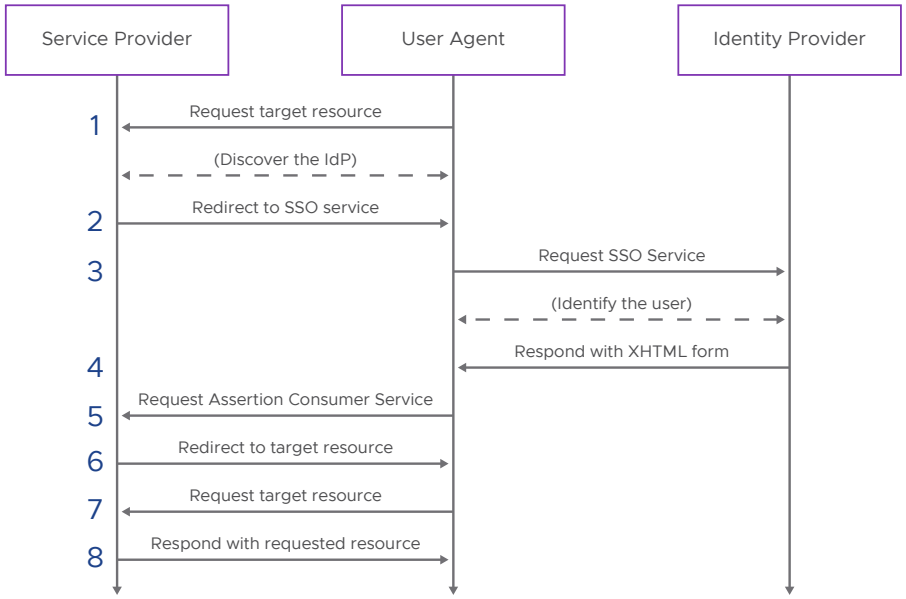

Figure 8: SAML authentication basics.

Why do we need to cover this? Because when designing solutions, Workspace ONE Access can be configured either as the IdP or the SP depending on the needs of the customer. If the company has no existing IdP, Workspace ONE Access can be configured as an IdP and then each of the individual services will be SPs. If the company would like to keep their existing IdP as the front-end, Workspace ONE Access can be configured as the SP for mobile SSO.

Workspace ONE hub services

Workspace ONE Hub Services is a set of features that co-exists within the Workspace ONE Access platform, specifically designed to help administrators offer an all-in-one portal for end users to access applications, teams and information within the firm. End users will access these features through the Intelligent Hub application or through the Hub portal (i.e., Workspace ONE Access catalog).

Hub Services is just that, a series of additional services provided to improve employee experience with a one-stop-shop experience. These services include the unified application catalog, notifications, people search, employee self-service, digital badge, virtual assistant, custom tab, branding and templates. While the unified application catalog is the "feature presentation" so to speak, the other services allow users to reduce the number of portals they must go to for company information. The people search feature set eliminates the need to do complex organizational searches through the company directory to perform employee lookups. The digital badge feature provides an extra layer of physical security for organizations, allowing the Workspace ONE Intelligent Hub application to act as a digital badge for physical access to office locations.

Note that not all these features are included in the on-premises version of Workspace ONE Access. Please check docs.vmware.com for the latest supportability table.

Workspace ONE Access – things to consider

Implementing Workspace ONE Access is now effectively a universal recommendation when I work with new customers. If you are considering a BYOD program, I go from 99 percent to 100 percent. The only exceptions to this that come to mind are more specialty-focused use cases: kiosk devices, rugged devices, use cases with single-app mode, etc. Otherwise, I generally approach design discussions as one all-in process that includes both UEM as well as identity & access. The addition of all the Hub Services features only compounds that recommendation further.

Just as with UEM, you'll need to make the decision on whether to utilize an on-premises solution or purchase a SaaS tenant. Most of the firms I've worked with have chosen to make the same decision for both UEM and Access (i.e., if one uses a SaaS tenant for Workspace ONE UEM, they also choose to implement Workspace ONE Access in SaaS fashion), and I generally agree with that direction. The SaaS footprint for Workspace ONE Access is so small (a simple connector), that it makes a lot of sense for companies to choose this option. My recommendation remains the same: Choose the option that works best for your security team and end users.

Key Decision Alert!

Will you implement Workspace ONE Access as a true IdP? Regarding the IdP vs. SP decision, it mostly depends on what is currently in place as it pertains to Identity Management. If no other IdPs exist, then Workspace ONE Access will take the place of the IdP. If there is another IdP that must be integrated with, the next decision point is "Which service will provide the front-end?" Factors that play into that decision are usually focused on end user comfort with existing systems .

Mobile application management (MAM)

Mobile application management (MAM) is one of the foundations of effective endpoint management. From the beginning of mobile device management, the ability to deliver applications automatically (or present them via a catalog) was an attractive feature for mobile administrators.

MAM has certainly expanded with the introduction of Workspace ONE Access, but the foundations remain the same. There are six primary types of applications supported by Workspace ONE UEM for distribution to devices.[13]

- Internal applications: These are apps that you or your company has developed and that you have the physical application package files for.
- Public applications: These are applications that are available on third-party app stores such as the Apple Store or Google Play Store. These can be either free or paid.
- Purchased (custom): Custom purchased apps allow you to leverage the Apple App Store for distribution without making your application fully available to the public. This requires Apple Business Manager to help identify valid devices and/or users.
- Purchased (VPP): These are applications purchased through the Apple Volume Purchase Program (VPP). The program allows you to purchase paid applications in bulk and then have Workspace ONE manage the licensing for you.
- Web links: These are direct links to web pages that will show up as application icons on a user's device.
- SaaS: These are web applications presented through Workspace ONE Access.

13. Mobile Application Management - docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/Application_Management/GUID-AWT-MAMINTRODUCTION

Developing a good strategy for application distribution is important to a quality Workspace ONE design. Which apps will be presented to which users? Which applications are limited by licensing? Which apps should be automatically distrusted vs. optional? Getting input directly from users, preferably during a pilot rollout phase, is the best way to confirm your approach and make adjustments if necessary. I recommend creating a MAM design plan where your primary applications are clearly listed with the associated user communities they will be distributed to, as well as the distribution method (automatic or optional).

Mobile email management (MEM)

Mobile email management (MEM) can mean different things to different people. Ultimately, it's all about getting corporate email securely on users' devices. Over the years, however, this space has evolved significantly, which has led to numerous options being available. I'll try to break them all down one by one.[14]

Approaches to MEM

Direct profile-based email delivery: This is the simplest way to deliver email to devices. Configure a profile with the Exchange ActiveSync (EAS) payload that directs the device's native mail client to a specific email endpoint. That's all there is to it. This option does not provide any additional protections other than those provided by your email system. It merely simplifies the process of configuring the devices appropriately.

Secure Email Gateway (SEG): The Secure Email Gateway (SEG), which is now SEGv2, is a proxy-based solution to mobile email management. The SEGv2 role can be installed on the UAG front-end server in the client DMZ. This is coupled with an email profile that directs the device to request email from the SEG directly, not the email's client access endpoint. The SEG receives the command, checks the device against its most recent approved device list (updated based on enrollment status, compliance status, and other rules that you configure), and then redirects the command to the email system. Think of the SEG as a bouncer for your email environment. Because it is a physical proxy, there are two specific functions it provides that no other MEM option can: hyperlink transformation and attachment encryption.

PowerShell integration: Workspace ONE UEM can directly utilize PowerShell-based commands to turn on and off access to email based on device ID. If the system detects that the device breaks a configurable compliance rule (compromised status, disallowed device type, disallowed device OS, etc.), the system can send a PowerShell command to the email endpoint to deny access. This works for both on-premises Microsoft Exchange™ and Microsoft 365™ email environments. The best part is that PowerShell integration does not require any additional hardware. It can perform all the same tasks as a SEG with the exceptions of hyperlink transformation and attachment encryption.

App-Based Delivery: The most modern approach is one in which a managed application, such as VMware Boxer™ is delivered to the device with the configuration pre-loaded. When you configure the Boxer application to be delivered to managed devices, you also configure application-specific configurations (sometimes called AppConfig) to deliver mail to devices. This is especially popular with cloud-based mail systems as it streamlines the configuration process considerably.

Pure SSO-Based Access: If you don't need to direct email to an application (think modern management use cases), and you have a cloud-based mail system that supports SAML-based authentication, you can configure Workspace ONE Access to authenticate to the mail system using SSO. This is popular for laptop and desktop management scenarios, especially for BYOD or non-managed device access.

Choosing the MEM approach

What MEM approach is right for your organization? As always, it depends on what you're trying to support. Here are a few things to keep in mind when deciding.

- If you absolutely require hyperlink transformation or attachment encryption, the SEG is required.
- Application-based delivery has become very popular in recent years due to its feature richness and simplified user experience.

14. Mobile Email Management - docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/WS1_MEM_Doc.pdf

- If you are not utilizing mobile devices and just need web-based authentication to email, consider the pure SSO-based access option.
- If you have cloud-based email, consider that utilizing a mail proxy will result in a "hair-pinning" effect (i.e. directing external traffic to the internal network only to direct it externally again). If this is not a concern, and your network can handle it, then just make sure to carefully weigh the benefits and costs.

Once again, I often get asked, "Roy, which MEM option do you recommend for us?" My answer is usually, "The simplest one that provides the security you need." Analyze each option and determine if it provides the security you desire for your email endpoint(s). From that list, choose the one that provides the simplest experience for your end users. This will reduce calls to your support center and help you sleep easier at night, too.

Device compliance, enrollment security and privacy

Device compliance rules

Device compliance is one of the most foundational security features of Workspace ONE UEM. The idea is simple: If you want to get access to corporate resources, there are a few simple rules you must follow. Device compliance is the feature that allows administrators to set and customize these rules. For example, administrators likely don't want devices that access company resources to be jailbroken or rooted (compromised). They may also desire that certain applications known to be malicious not be present on the device. Other admins may want to avoid supporting certain device types, operating systems or versions.

This is a great area to work on directly with your CISO or security architect. Think about your device fleet and user community. If you are planning to utilize full enrollment for devices and/or deploy company-issued devices, device compliance rules are a foundational element of the solution I would not recommend you skip.[15]

Enrollment security and restrictions

Another key step is setting up restrictions pertaining to enrollment. Some organizations will limit the number of devices a user can enroll; others will restrict the types of devices that can be enrolled in the system; others will choose to leave the system more open. The most common restrictions are related to limiting enrollment to known users and/or groups.

Why would you want to restrict enrollment? Some companies are more license-conscious than others and would like to maintain a firm grip on how many enrolled devices are in the system. Some organizations don't have support (profiles, rules, applications) for certain platforms configured (e.g., iOS vs. Android), and would like to ensure that the user experience is well-handled. Restricting to known users and groups will ensure that only users that have been added through a directory or manual sync will be able to access the system.

I may sound like a broken record, but this is an area where no two companies will be exactly alike. If license count is not a big concern, and if you have adequate handling for major platforms, why would you not want more users on the system? I'm sure some orgs have a good answer to that, but it will generally be specific to the business situation.

Privacy settings and transparency

Implementing secure and transparent privacy restrictions in Workspace ONE is a vital step in building end-user trust of the platform. When working with customers, I always take extra time to stress the importance of these decisions.

Workspace ONE privacy settings effectively decide two things: what device and user information is tracked by the portal, and which remote device actions are allowed by administrators. The first category describes items that are automatically reported based on device info (first name, last name, device-friendly name, phone number, etc.). The second category includes actions such as enterprise wipe (in which the corporate data is removed), device/factory wipe (in which the entire device is wiped) and others. If you are implementing a BYOD program in which devices are ever enrolled, the importance and sensitivity of these decisions just went up by a few orders of magnitude.

15. Workspace ONE UEM Compliance - docs.vmware.com/en/VMware-Workspace-ONE/services/WS1-Access-deploymentguide/GUID-EF834B6D-C3EC-48BA-B38D-1574F7E4B773

My advice is to call a meeting with representatives from your legal organization and achieve the following:

1. Decide on a list of privacy settings that is palatable for all parties.
2. Document the settings and reasoning behind them in a privacy document. Ensure that this is transparent, stored somewhere safe, and easy to access by employees.
3. Further document these items in the EULA that will be approved by users upon enrolling.

One of the big keys to a successful UEM rollout is building trust with your user community. Emphasizing transparency in the process will greatly improve your chances of doing this effectively.

Other security settings and profiles of note

There are a host of other security-focused options and configurations within the Workspace ONE console that I haven't mentioned. Enforcing a password or PIN on managed devices is typically recommended. Most organizations tend to impose a few options in the restrictions profile for enrolled users. Hopping over to Workspace ONE Access, most administrators prefer additional levels of authentication for requests originating from off the corporate network. As you'll see later, Workspace ONE Intelligence introduces the ability to automate many of these rules and use data analytics to identify threats. What's more, new features in this area are popping up all the time. Confirm the latest settings on docs.vmware.com during the design process to ensure your strategy is optimal.

A note about BYOD

Bring-your-own-device (BYOD) programs have been around almost as long as MDM software. Having to carry two different devices (one personal, one corporate) quickly became cumbersome on users, especially as the footprint of the average mobile device continued to grow throughout the 2010s. For many organizations, BYOD was the perfect solution. Allow users to utilize their own devices and access corporate resources. This simplified the end-user experience and generally saved the company on device and mobile costs. It was a win for all parties.

Still, the solution came with a number of considerations to keep in mind. As an IT organization, do you allow support for all device types? Do you require full enrollment of devices? What privacy concerns (both real and perceived) does this raise? Do you limit the device-oriented actions that administrators can take based on this use case?

Two things came along that greatly simplified these discussions: Workspace ONE Access and the introduction of multiple personas on mobile devices.

Workspace ONE Access allowed administrators to put the user experience first and the device management second. If the user needs to access a secure application that should require device enrollment, the administrator can require the user to enroll the device to access it. If this isn't the case, the user will not need to have their device enrolled. This "enrollment only if" approach greatly improved the comfort level for BYOD users.

Around the same time, many device OEMs began offering the ability to manage personal and work personas on a single device. This allowed end users to effectively separate their application experiences on a single device. What's more, it allowed users to "turn off" their work applications on weekends or during vacations. Digital wellbeing for the win!

My point is that there is no "BYOD button" in Workspace ONE. Implementing a BYOD program means a lot of different things based on your specific technical and business situation. Many of the factors that make for a successful BYOD program are non-technical in nature. Working with your end users to understand privacy concerns is crucial. Ultimately what you'll be left with is a series of changes and small configurations to privacy settings, enrollment rules, administrative settings, application-access rules in Workspace ONE Access, and others. The key to these configurations having any sort of meaningful outcome is close engagement with your user base, an open mind to their concerns, and transparency regarding the capabilities of the solution.

Basics of modern management

Modern management, specifically referring to unified management of Windows and macOS laptops and desktops cohesively alongside mobile devices, is an absolutely huge topic, one that is honestly worthy of an entire book. In an attempt to summarize in a few short pages, I will lay out the foundational principles of modern management and attempt to summarize as best as possible. Once again, this should not take the place of stand-alone guidance on modern management.[16]

The five pillars of modern management

VMware sometimes uses a construct called the "Five Pillars of Modern Management" when describing the solution for Windows and macOS devices. Since most firms managing Windows devices previously utilized a number of PC Lifecycle Management (PCLM) tools to oversee deployments, many of the pillars tend to be focused on effective migrations away from these legacy tools to modern equivalents such as Workspace ONE UEM.

Pillar 1 – users & devices

The first pillar is focused on getting users onto the system and devices enrolled. While it's a simple idea, the sheer number of options can be overwhelming. Many companies opt to utilize out-of-box enrollment (OOBE) as it provides a great end-user experience when receiving a new device. Firms can further this automation through a process called drop-ship provisioning, which works with device manufacturers to have the device partially enrolled prior to being shipped to the user. Of course, you also have the option of basic hub enrollment.

Having used OOBE for new devices, I can tell you that it drastically improves the experience of receiving a new device. Taking it a step further with drop-ship provisioning can really simplify the process for IT. If you're just starting out, it's great to use more basic enrollment methodologies, but I recommend you do so with the intention to further streamline down the road.

Pillar 2 – policy management

The second pillar focuses on device policies and profiles. For customers moving from an SCCM-managed environment, this generally involves a lengthy process of inspection on current device rules and restrictions. Here, I will issue a strong recommendation: Do not attempt to recreate all your SCCM configurations in Workspace ONE. The entire point of modern management is to do things more efficiently, not the exact same on a different system. Even though it takes more up-front work, go through the process of justifying your current rules and envision how the same outcomes (or likely better) can be achieved through a more modern approach.

Pillar 3 – application management

The third pillar focuses on managed applications. Having utilized other PC lifecycle management (PCLM) tools in the past, I personally feel this is the area where the administrative experience is most greatly improved in the modern management world. Still, I would recommend that this design phase is the perfect time to perform an inventory of the applications you have in the enterprise today. How can the list be simplified? Do you really need to support eight messaging apps? Should you still be supporting that decade-old web browser? Think about a simpler, end-user-focused approach that streamlines application access and cuts down on cognitive load for your users.

Pillar 4 – update management

The fourth pillar is around how to manage periodic updates for devices. In the Windows realm, Workspace ONE UEM supports both Windows Server Update Services (WSUS) and Windows Update for Business (Sometimes abbreviated WU4B). The focus for this pillar is often on how to best manage and distribute upgrades, how to create a set of distribution rings, and which user communities should receive updates on what schedule.

16. Windows Desktop Device Management - docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/Windows_Desktop_Device_Management/GUID-uemWindeskDeviceManagement

Pillar 5 – security & compliance

The final pillar involves setting up security profiles and compliance rules for devices. Once again, attempting to recreate all the security provisions in the previous PCLM tools is not my recommended approach. Use this opportunity to take a fresh look at your organization's security needs and create a set of restrictions profiles and compliance rules that meet the honest needs of your company.

Closing recommendations for modern management

As I stated in the introduction, modern management is a massive topic and could fill the pages of another book altogether. This is definitely an area where I recommend working with a professional, as the technology changes quite frequently. An experienced consultant will be up to date on the latest enhancements and will also be able to front-end use cases that have been successful with other implementations.

Part 5: Environment Optimization and Monitoring

Workspace ONE Intelligence

One of the most exciting new tools in the Workspace ONE suite is undoubtedly Workspace ONE Intelligence. This tool allows administrators to gain insights into their entire digital workspace, as well as enforce security and compliance measures across the enterprise. A few high-level use-cases are below:

• Create and subscribe to weekly reports on non-compliant devices in your environment.

• Create a single, custom dashboard with all the pertinent information you need to manage your devices and applications.

• Utilize key integrations such as Slack or ServiceNow to create automations.

Workspace ONE Intelligence is primarily comprised of four feature sets: dashboards, automations, reports and digital employee experience management. We'll cover each in the sections below.[17]

Dashboards

The first primary feature area of Workspace ONE Intelligence is dashboards. Dashboards provide a valuable visualization tool for administrators and provide near-endless customization. For instance, for administrators looking to drive device enrollment, you can set up a widget showing the number of enrollments in the past week. For the security conscious, you could set up widgets showing the number of compromised devices sorted by department or OS version.

One of the biggest benefits of Workspace ONE Intelligence dashboards is the ability to expand use cases beyond just the IT organization. Human Resources (HR) administrators may want to understand how quickly new applications are being adopted or how many users have unenrolled their devices recently. Leaders in finance or other organizations may have different needs. As an IT administrator, this is a great way to make good on our initial design promise to provide valuable capabilities back to the business.

Automations

The automation feature of Workspace ONE Intelligence is designed to make your life as an IT administrator easier. Every automation is a mental thread you get back! Should compromised devices be automatically warned or even unenrolled? Should devices receive a notification upon receiving a new application? Think about all the small administrative tasks you need to accomplish each day/week/month. Many of them can likely be automated away with Workspace ONE Intelligence.

17. Workspace ONE Intelligence - docs.vmware.com/en/VMware-Workspace-ONE/services/intelligence-documentation/GUID-intel_products_container

This is an area that customers often have a difficult time designing during the implementation of Workspace ONE as it creates a sort of "chicken and the egg" problem. For this reason, I generally recommend setting up one "no brainer" automation to practice utilizing the toolset. After that, I advise that administrators will likely need to design and create new automations as needs arise and evolve.

Reports

Reports are a great expansion of the dashboards feature set we discussed earlier. Let's say your CIO expects a weekly write-up on compromised devices each Monday morning. You could start working on manually checking your device list each Sunday afternoon… or you could set up a weekly report subscription with Workspace ONE Intelligence. Setting up a report subscription is an effective means of getting a more detailed subset of data on a regular basis. Keep in mind that you can always run a report off-cycle or as a one-off to get quick information as well. I'd recommend thinking about what types of data you'll need on a regular basis in order to set up some initial reports when designing the solution.

Digital Employee Experience Management (DEEM)

Digital Employee Experience Management (DEEM)[18] is a feature set within Workspace ONE Intelligence that helps administrators understand the quality of the digital employee experience among the company's users. DEEM harvests information from managed devices to provide telemetry data that can be utilized for decision-making or even automatically acted upon in some cases. One use case is the ability to see the total number of OS crashes over time. If you find that these have gone up significantly in the past month, you may determine that a recent OS update is causing crashes to occur. You could also gain insight into the average boot and shutdown times of devices to see how they are changing. One of the most interesting use cases I've seen is that of battery health. If the system detects that a device has a poorly-performing battery, an automation can be configured to automatically alert the user and submit a request for a new battery on their behalf.

Ultimately the data is utilized to generate a user experience score as well as an organization experience score. Using the data to maximize these scores will help ensure your IT organization is a valuable asset to the business.

Part 6: Building Real Designs (with Examples)

Assumptions and disclaimers

With any proper design, certain assumptions will need to be made to account for time and space constraints. The four examples below are meant to get you thinking about the proper high-level steps to designing a Workspace ONE implementation. With that said, here are a few disclaimers to keep in mind:

- These examples are not reflective of any specific designs I have performed in the past. They are meant to be illustrative of common customer needs and requirements.
- The diagrams are simplified. When performing designs for customers, more detailed diagrams are always utilized. These detailed diagrams include ports and protocols, server information, load-balancing details, etc.
- The diagrams in this book are designed to get you started, but are not a substitute for a proper design, preferably performed with a VMware architect.
- Whenever not explicitly called out, I always assume that the customer has given us a requirement for the console server to be placed in the internal network.
- All diagrams are shown with a simplified network architecture, which assumes a simple DMZ and internal network separated by two firewalls. Again, these diagrams are meant to call out specific design principles, not replicate exact, complex network architectures.

18. Digital Employee Experience Management - docs.vmware.com/en/VMware-Workspace-ONE/services/intelligence-documentation/GUID-19_intel_deem

- Some servers and services have been grouped together for simplicity and brevity.
- If not otherwise listed, it is assumed that licensing is always in place for the solutions being proposed.
- All designs are open for debate! The examples I've described often do not give all of the information needed to make extremely specific decisions about architecture or configuration. In these cases, we've assumed the most common situation or outcome. For the most part, that particular item was not overtly pertinent to the design quality I was attempting to highlight in that given example.

Example 1: Basic MDM

CGHM business and IT background

Compu-Global-Hyper-Mega-Net[19], or CGHM for short, is a small 50-person company headquartered in the United States. The company is just getting started, has raised a small amount of initial capital from investors, and has begun speculation on potential entry into the internet retail space. The momentum and press so far have been enough to attract the interest of Microsoft for a potential acquisition.

While CGHM has several talented engineering and design-focused employees, its main threat comes in the form of individual property (IP) theft. Based on the strong press, CGHM has already become the target of phishing attacks and hacking attempts. Most shockingly, its small physical office on Evergreen Terrace has had multiple break-in attempts, which makes hosting physical infrastructure risky. Compliance and the ability to quickly wipe devices are big MDM selling points for CGHM.

CGHM would like to offer mobility management to its employees in a secure way. The company also has a small internal iOS application that it has developed to assist its employees with research and development tasks. This application has no need to contact any enterprise resources and is wholly contained in the cloud. CGHM has no desire to manage identity & access and would prefer to utilize a more vanilla-style solution focused on base MDM for the time being. Being extremely security focused, CGHM plans to purchase iOS devices for its employees and manage them directly.

You've been hired as a consultant to help design a Workspace ONE-based solution and help CGHM achieve their business and IT goals. How do you proceed?

CGHM's Workspace ONE design

You begin by asking leadership about the different types of users at CGHM. You quickly find that CGHM is really just one large user community. Being such a small organization, there are no formal team structures or sub-orgs. You are made aware that the 50 people in the org all really need the same thing: secure email and access to the CGHM internal iOS application. This becomes your one and only use case: CGHM employees. Administration will be performed by a single individual who is familiar with MDM concepts, but does not have much hands-on experience.

You need to conduct a series of workshops to uncover any business and technical requirements, as well as assumptions, constraints and risks. This is how you uncover the strong need for a robust set of device-side compliance rules that can be automated, tracked and monitored. Through this process, you're also able to determine that a SaaS solution likely makes the most sense for CGHM based on its inherent risks to physical security and small footprint. Understanding the need for strong device control leads you to determine that full enrollment of corporate-owned devices is a good starting point for CGHM.

Jumping into solution design, you determine that CGHM uses Active Directory for its directory services with on-premises domain controllers (DCs). The company does not utilize a third-party IdP. There is only one physical location for CGHM, and each of its employees report in person on most days. There is a single corporate Wi-Fi network that is secured through an active directory certificate services (ADCS) certificate. CGHM would like to distribute mobile email to all its users from its on-premises-based mail solution. The company's email team has a firm requirement that confirms compliance status using a mail proxy before allowing a device to access mobile email.

19. Compu-Global-Hyper-Mega-Net is a fictitious company owned by Homer Simpson in the TV show The Simpsons - simpsons.fandom.com/wiki/Compu-Global-Hyper-Mega-Net

Based on what you know so far, you plot out the network architecture diagram below for the solution.

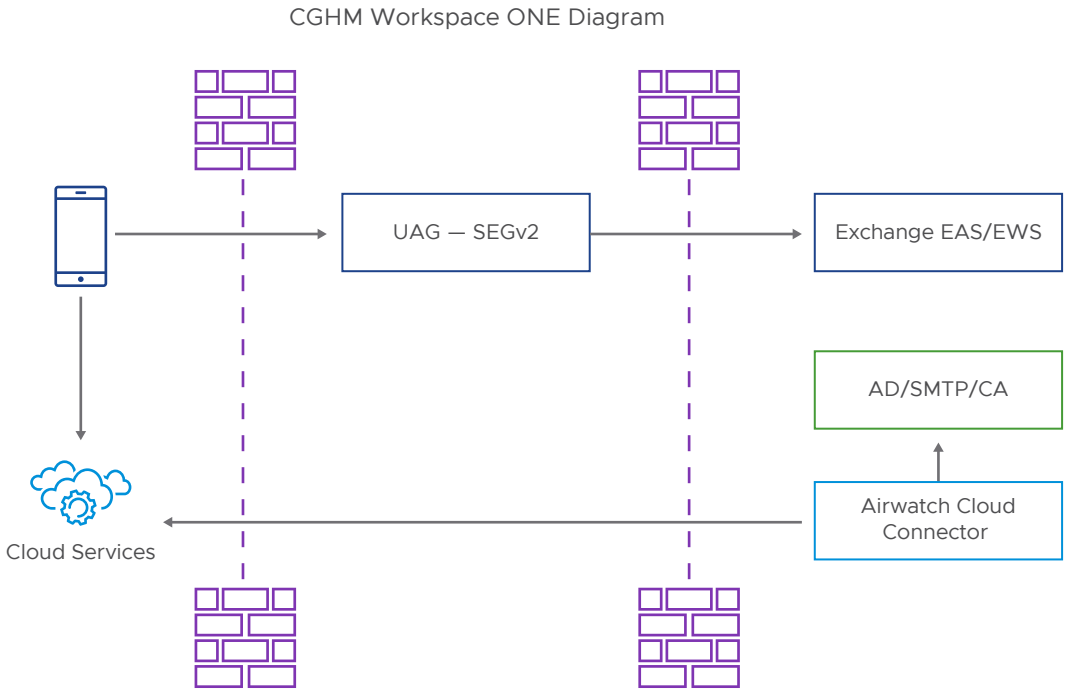

Figure 9: CGHM network architecture diagram.

Let's break down why these decisions were made. We established earlier that a SaaS option would be utilized for the Workspace ONE UEM core components based on CGHM's physical security risk and small footprint. The ACC has been designed to live in the internal network so that it can integrate with Active Directory. The SEG role (installed on the UAG) will be placed in the corporate DMZ based on the requirement to proxy mail traffic and inspect device posture. We have no need for the Content Gateway or VMware Tunnel as no use case for these was brought to us by CGHM. There is no requirement for identity & access management currently. Having established a basic network architecture and high-level solution design, you're also able to map out an initial OG hierarchy.

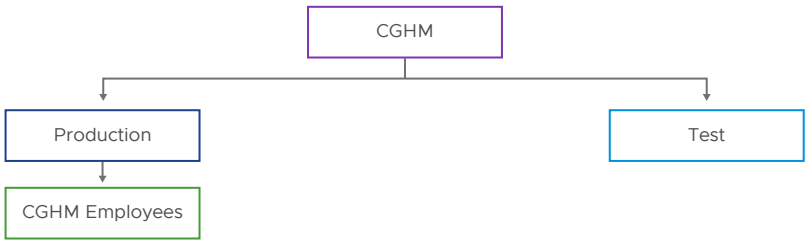

Figure 10: CGHM organization group hierarchy.

You next work with CGHM's project management team to develop a project plan for the implementation of Workspace ONE and its rollout. You find that CGHM prefers agile-based methodologies for project management. Working with the team, you create the following project plan, making sure to minimize time-to-value (first enrollment) and prioritizing adoption and rollout support for end users. You also hash out a simple end-user communication and promotion plan, which is included in the overall program workbook. You also identify a few simple KPIs to track as the rollout progresses. A rough Gantt chart is below:

Phase/Sprint	1	2	3	4	5
Kickoff	•				
Design	•	•			
Implement		•	•	•	
Pilot			•	•	
Rollout				•	•

Figure 11: CGHM simplified project plan.

As you finalize the design, you interview members of the IT organization and find that one individual has significant interest and background knowledge in MDM but lacks practical experience. You work with leadership to identify one additional administrator that will assist with day-to-day MDM tasks, effectively giving the organization a two-person mobility team. You recommend that both administrators achieve VCP-DW certificates within the next six to twelve months.

CGHM's Results

Inspired by the project, CGHM goes on to provide MDM capabilities for its 50 employees within six short weeks. You spend another month working to drive more adoption of the program and achieve a 95 percent adoption rate among qualified employees. Measuring against your KPI goal of 85 percent adoption, CGHM interprets the solution as a huge success. Most importantly, the company's CEO and CISO have reported better and more restful sleep since the mobile security solution was put into place. Having completed all the recommended training, the new small mobility team feels confident in supporting any questions that arise from end users. Being careful not to pry into confidential matters, you overhear that the additional security capabilities have made CGHM an even more attractive purchase target for one large technology firm in particular. On your way out of the office after attending the final status report, you overhear a conversation about "writing a lot of checks."

Having completed a successful design and implementation for CGHM, you close the project by recommending the next step on the roadmap for the company. You identify that the company has no capabilities in identity & access management. This becomes a logical next step for the company in order to provide secure access to applications from any device in a secure fashion. Having been impacted by the events of 2020, CGHM would like to explore offering a more user-centric approach to endpoint and user management.

Example 2: Mobile SSO-driven BYOD

Flancrest Enterprises' business and IT background

Flancrest Enterprises[20] is a US-based supplier of pens and writing utensils. While manufacturing is outsourced, Flancrest still employs approximately 1,000 people: 250 in design, 450 in sales, 100 in marketing, 50 in IT, 50 in HR, and 100 split among finance and other back-office roles. The company is very technology-forward and prefers to spend IT dollars on ongoing

20. Flancrest Enterprises is a fictitious company owned by Ned Flanders on the TV show The Simpsons - simpsons.fandom.com/wiki/Flancrest_Enterprises

subscriptions to cloud providers instead of maintaining large on-premises data centers. The firm's IT group is more focused on building new capabilities and does not wish to own ongoing monitoring, maintenance and upgrades of on-premises servers where possible. Flancrest's ultimate goal is to empower its employees to be productive, regardless of their work location.

To achieve this goal, Flancrest would like to provide its 1,000 employees with a suite of productivity applications, including the ability to create and edit documents, spreadsheets, presentations, etc. Other common applications include HR software, timesheet and payroll applications, and access to internal company websites. The company also makes use of web-based modeling tools for its 250 product designers. Its mail system is managed in the cloud.

Flancrest does not intend to issue company-managed mobile devices. It does, however, offer a stipend for employees to purchase a new mobile device every three years. It also contributes a small amount to employees once per month to help offset mobile data costs. Flancrest recommends the users stick to either Apple iOS or Android-based devices.

You've been hired as a consultant to help design a Workspace ONE-based solution and help Flancrest achieve their business and IT goals. How do you proceed?

Flancrest Enterprises' Workspace ONE design

You begin by working with the customer to list out the user communities being supported by the first rollout for Flancrest. You are made aware of the 1,000-person user base and how it is divided among departments. You ask and find that all users are US-based and supported by the same IT administrators. You then identify two key use cases: general knowledge worker and designer. Working with the company, you determine that all users need access to the same suite of productivity applications. However, designers also require access to a design program that is license-limited. You find that the design team's specific applications require API-based calls into an internal database of previous architectures. The third-party application that makes these calls supports per-app VPN directly out-of-the-box.

You need to conduct a series of workshops to uncover any business and technical requirements, as well as assumptions, constraints and risks. The one major item that comes from this series of interviews is that the company has very strong technical leadership that would like access to reporting and insights on their team's device and application metrics. Through this process, you're also able to determine that a SaaS solution likely makes the most sense for Flancrest based on its proclivity to pay for hardware support and spend IT dollars and effort on building new capabilities. This leads you to the conclusion that a BYOD program would be the best solution for Flancrest.

Jumping into solution design, you determine that Flancrest uses Active Directory for its directory services with on-premises domain controllers (DCs). The company does not utilize a third-party IdP. After the events of 2020, Flancrest Enterprises shut down its physical office locations and has gone 100% virtual. For that reason, it does not need to provide access to any specific Wi-Fi networks. However, its CISO does require that any authentication requests from external networks (which will be all of it in this case) go through MFA with the company's RSA-based solution. Flancrest would like to distribute mobile email to all its users from its cloud-based mail solution. The customer would like to control copy/paste and other restrictions from the email and productivity suite. You explain that either the Outlook for Mobile or the VMware Boxer application can provide those controls, but note that the Outlook option requires Company Portal/Authenticator and another registration step for end users. Based on these pros and cons, Flancrest settles on utilizing VMware Boxer.

Based on what you know so far, you plot out the network architecture diagram below for the solution.

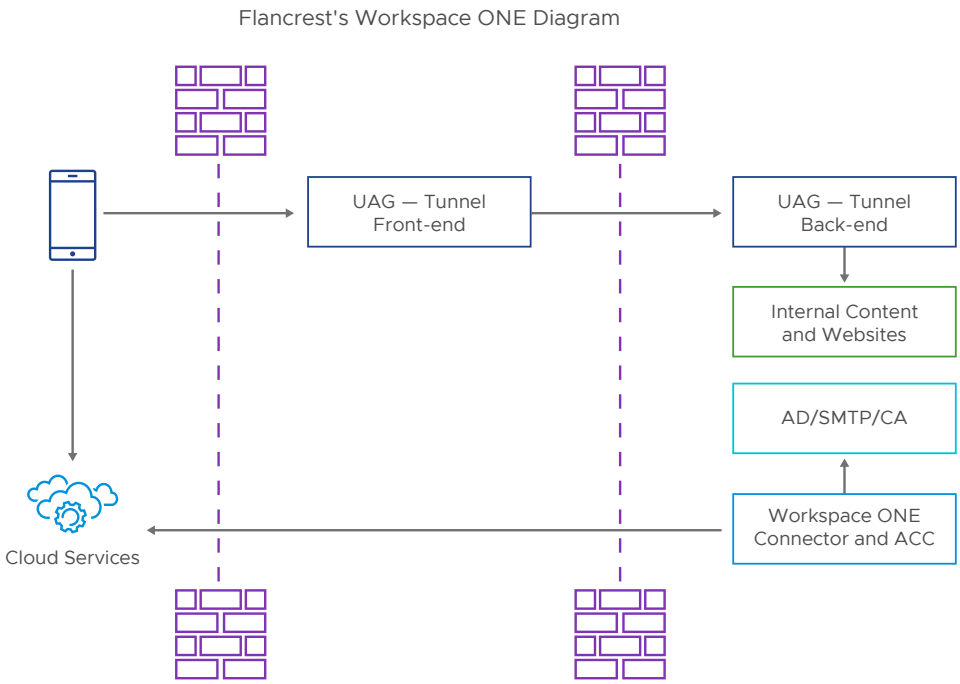

Figure 12: Flancrest's network architecture diagram.

Let's break down why these decisions were made. We established earlier that a SaaS option would be utilized for the Workspace ONE core components (both UEM and Access) based on Flancrest's proclivity for cloud-based options and desire to avoid unnecessary server maintenance. The ACC has been designed to live in the internal network so that it can integrate with Active Directory. We will share this server with the Workspace ONE Access connector for the same purpose. The UAG front-end and back-end servers will support both Android-based mobile SSO as well as the application-tunneling features needed for the design team's specialty app. We have no need for the Content Gateway as no use case for it was brought to us. The SEG role is unnecessary as we will be connecting to cloud-based mail, have no need for the additional SEG features such as hyperlink transformation, and plan to distribute mail directly to the Boxer application.

Having established a basic network architecture and high-level solution design, you're also able to map out an initial OG hierarchy. Your preliminary diagram is below.

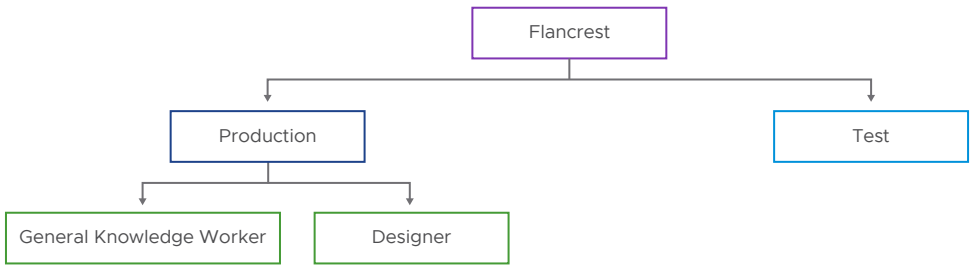

Figure 13: Flancrest Enterprises' organization group hierarchy.

Next, having worked through a rough set of overall guidelines for application access earlier in the design, you work with IT to create an initial list of applications for Workspace ONE Access. You note in the design that all application access from offsite (which is all access currently) will require MFA through the company's RSA solution.

You next work with Flancrest's project management team to develop a project plan for the implementation of Workspace ONE and its rollout. You find that Flancrest prefers to work in a waterfall-based program methodology but is open to using phasing and milestones. Working with the team, you create the following project plan, making sure to minimize time-to-value (first enrollment) and prioritizing adoption and rollout support for end users. For this reason, the general knowledge worker use case is chosen to be the MVP and be implemented first. You also hash out an end-user communication and promotion plan, which is included in the overall program workbook. You also identify a few simple KPIs to track as the rollout progresses. A rough Gantt chart is below:

Phase/Week	1	2	3	4	5	6	7	8	9	10
Kickoff	•									
Design	•	•								
Implement		•	•	•	•	•				
Pilot						•	•	•		
Rollout							•	•	•	•
End-User Comms		Heads-up			Pilot		Rollout			

Figure 14: Flancrest's simplified project plan.

As you finalize the design, you interview members of the IT organization and find that many are unfamiliar with the basic concepts of UEM and identity & access. You work with leadership to identify five admins that will comprise the new "mobility team." This team will own monitoring and maintenance of the integration servers (ACC and UAGs), administration of the UEM and Access consoles, and support for end users. You recommend a series of training courses and certifications for each of the administrators. The level 1 admins (support-focused) will work to achieve VCA-DW certifications. The level 2 admins (administration and maintenance-focused) will work to achieve VCP-DW certifications over the next six to twelve months.

Flancrest Enterprises' results

With your help, Flancrest goes on to provide UEM and identity & access capabilities for all its 1,000 employees within a few short months. You spend another three months working to drive more adoption of the program and achieve a 90 percent adoption rate among qualified employees. Working with the IT organization, you also capture some rough productivity metrics for the design team. Remote design tasks that used to take almost 30 minutes with previous tools are now only taking 15 minutes. Measuring against your KPI goals of 80 percent adoption and a 30 percent reduction in design task time, the company views the technical solution as an overwhelming success. Having completed all the recommended training, the new mobility team has been given glowing reviews from end users and leadership alike. End users especially like the freedom that the solution provides. Instead of stressing about potential missed emails and the inability to do work from anywhere, they feel confident in the company's mobile work initiatives.

Having completed a success design and implementation for Flancrest, you close the project by recommending the next step on the roadmap for the company. You identify that the firm has approximately 1,000 Windows-based devices currently managed by SCCM. You suggest that these are moved to a modern management-based solution for the firm's next project.

Example 3: Modern management design

Technical Resource Consulting's business and IT background

Technical Resource Consulting (TRC) is an IT consulting firm located in London, United Kingdom. TRC has field offices in ten major countries around the world and generates the majority of its revenues from onsite IT consulting services, which have been performed for customers in over 100 countries. The company currently has 1,500 employees: 1,000 in consulting services, 200 in marketing, 100 in IT, and the remaining 200 split between HR, finance, legal, corporate and back-office roles. The firm considers itself to be technology-forward based on its business model, but its IT group sometimes has trouble keeping up with the latest technology advances. Still, it aims to move to a user-centric model that allows its very distributed workforce to be efficient and productive from anywhere.

One area where the company has fallen behind is in desktop and laptop management. TRC has utilized SCCM for almost twenty years, and its desktop management team has a collective 115 years of experience in the technology. TRC would like to move to a modern management model based on Workspace ONE UEM. The company adopted Workspace ONE last year for its mobile use cases and would like to use the same instance for desktop management.

Ultimately the desire to shift to modern management has been driven by two factors: employee experience and user productivity. Employees have consistently noted laptop issues and slow wait times as significant hindrances to performance in recent employee surveys. In the realm of productivity, an internal consulting team determined that a standard consulting employee spends one week per year in downtime with laptop issues. The company wants to reduce this greatly using Workspace ONE. This will be the company's vehicle to push policy updates in an increasingly "work-from-home" world.

TRC would like to provide a true user-centric experience on laptops and desktops to its consulting users. This would include basic enrollment of devices and access to corporate applications on Windows devices. The company has not yet adopted any macOS-based devices. All laptops are purchased by the company and delivered to employees. No BYOD model has been deemed appropriate for laptop use cases at this time.

You've been hired as a consultant to help design a Workspace ONE-based solution and help TRC achieve their business and IT goals. How do you proceed?

Technical Resource Consulting's Workspace ONE design

You begin by working with the customer to list out the user communities being supported by the first rollout for TRC. You are made aware of the 1,500-person user base and how it is divided among departments. You determine that all users are supported by a central IT support organization. You then identify two key use cases: office worker and consulting worker. Working with the company, you determine that all users need access to the same suite of productivity applications. Consulting users, however, also need access to a few additional applications that are license-restricted.

You need to conduct a series of workshops to uncover any business and technical requirements, as well as assumptions, constraints and risks. You are informed about the existing on-premises Workspace ONE UEM environment that was implemented for mobile users. You are given a list of applications that need to be supported and find that most are web-hosted and support SSO. TRC would like to configure Workspace ONE Access as the service provider and its existing IdP provider as the identity provider. The company's CISO would like to utilize MFA using its existing RSA-based solution when a user attempts to access applications from a network other than Wi-Fi located at the company HQ or field offices.

Pivoting to solution design, you are also informed that the company utilizes many different vendors for laptops and there is no desire to implement drop-ship provisioning at this time. You find that the company utilizes Azure AD and has a premium license. The company utilizes a well-known 3rd-party IdP but has not implemented any integrations with Workspace ONE. The company already utilizes cert-based authentication for its onsite Wi-Fi networks for the mobile use case. In the previous implementation, the company implemented Workspace ONE in an on-premises fashion. As a part of that project, it also

implemented a front-end and back-end UAG for tunneling purposes. You recommend that the customer should consider moving its on-premises Workspace ONE UEM environment to a SaaS instance. TRC agrees with this direction in the long-term, but decides to stick with the on-premises instance for now.

One of the most interesting tidbits you gleaned from the requirements-gathering phase was the need to promote employee experience. For this reason, you propose implementation of Workspace ONE Intelligence and its DEEM feature set. The customer is excited by the prospect and gives it the green light for this project.

You are given the previous network architecture diagram for the implementation of Workspace ONE. You confirm that this is up-to-date after interviews with the IT group.

Based on what you know so far, you update the diagram as shown below.

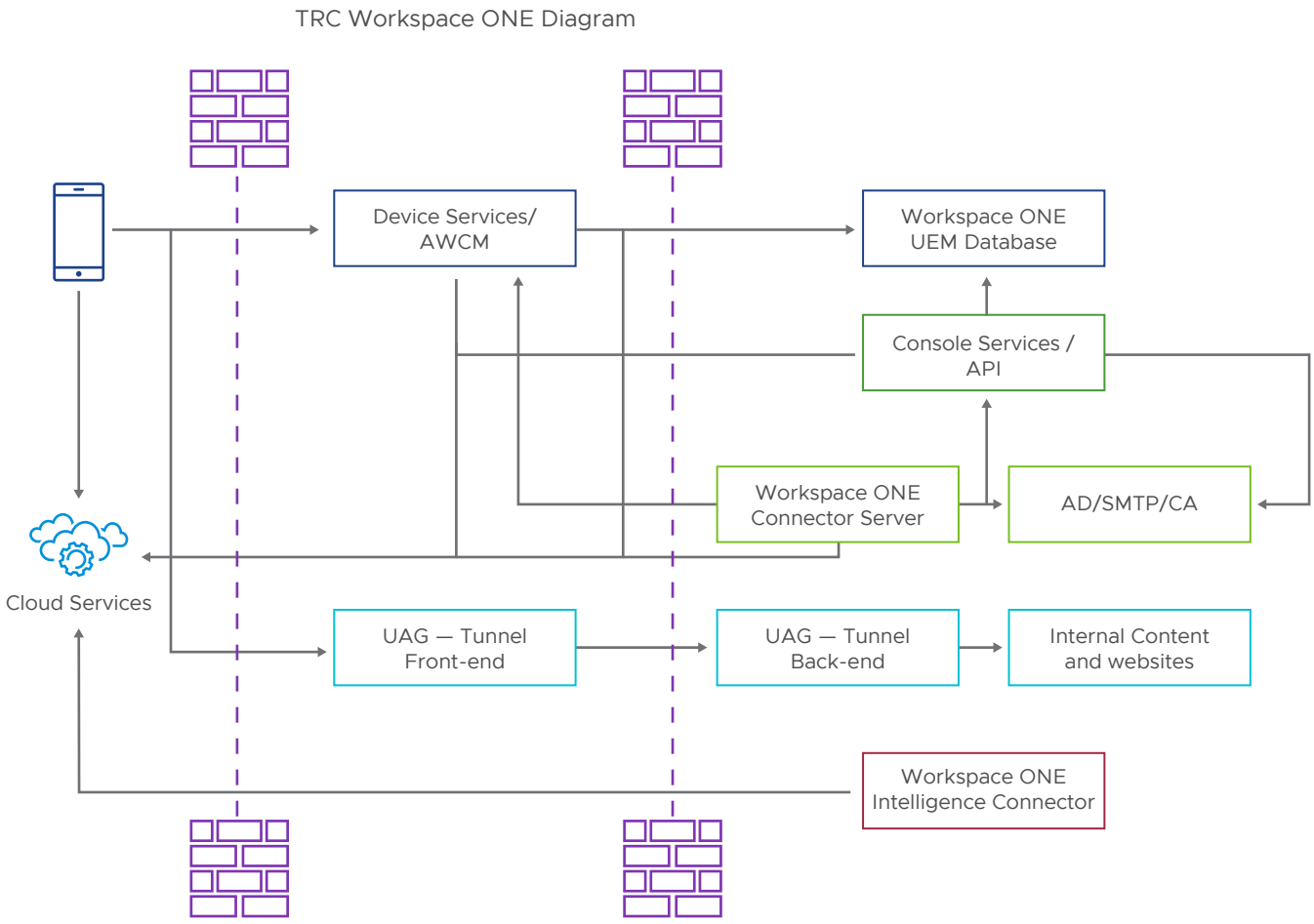

Figure 15: TRC network architecture diagram.

Let's break down why these decisions were made. The company already had Workspace ONE UEM implemented, so we will focus on the net-new components. No requirements were brought that would result in any additional components to the UEM infrastructure. The only change is the desire to implement access to corporate applications from anywhere. This requirement will require implementation of Workspace ONE Access. Since the company has expressed desire to place the primary components in the cloud, we only need to add the Workspace ONE Access connector for application access. Although we are adding Workspace ONE Intelligence, the core components for this solution live in the cloud as well. We only need to add the Workspace ONE Intelligence Connector in the internal network.

Having established a basic network architecture and high-level solution design, you're also able to map out an initial OG hierarchy. Your preliminary diagram is below.

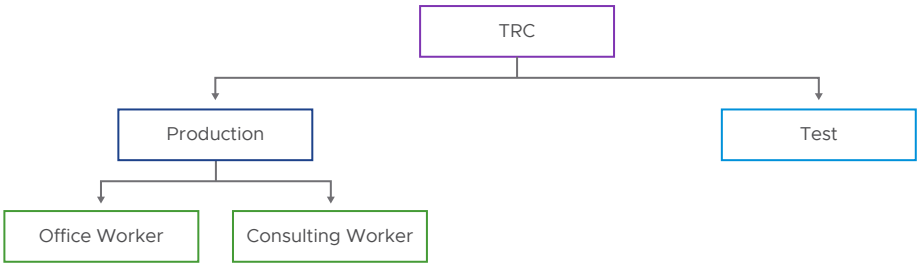

Figure 16: TRC organization group hierarchy.

Next, having worked through a rough set of overall guidelines for application access earlier in the design, you propose a rule set for Workspace ONE Access focused on the existing web-hosted SSO applications. The configuration will feature Workspace ONE Access as the service provider and TRC's existing IdP provider as the identity provider. If a user attempts to access any application on a network other than office Wi-Fi, the company's MFA solution will trigger a token request.

You add Workspace ONE Access as an IdP to the customer's existing IdP. It will be utilized to handle all initial authentication traffic. You explain to the company's CISO that this configuration will allow Workspace ONE Access to verify device management status and compliance status on application access attempts. Any device that passes management and compliance checks is granted access to single sign-on to every application regardless of location. If a device is not managed or compliant, RSA integration is implemented to still allow access to the applications from external networks. This solution allows the primary IdP to own all authorization and claims, while allowing Workspace ONE Access to own primary authentication.

You also hash out a rough list of DEEM automations to assist administrators in improving employee experience.

You next work with TRC's project management team to develop a project plan for the implementation and its rollout. You find that TRC prefers to work in a waterfall-based program methodology but is open to using phasing and milestones. Working with the team, you create the following project plan, making sure to minimize time-to-value (first enrollment) and prioritizing adoption and rollout support for end users. It is determined that both the general office worker and consulting worker use cases can be implemented in parallel based on the overlap in requirements. You also hash out an end-user communication and promotion plan, which is included in the overall program workbook. You also identify a few simple KPIs to track as the rollout progresses. Based on the business requirements laid out earlier, you propose two KPIs: employee experience score and average employee downtime. The company would like to improve both by 50 percent within the first year.

A rough Gantt chart is below:

Phase/Week	1	2	3	4	5	6	7	8	9	10	11	12
Kickoff	•											
Design	•	•										
Implement		•	•	•	•	•						
Pilot – Office Worker						•	•	•				
Pilot – Consulting							•	•	•			
Rollout – Office Worker									•	•	•	•
Rollout – Consulting										•	•	•
End User Comms		Heads-up			Pilot 1	Pilot 2		Rollout 1	Rollout 2			

Figure 17: TRC's simplified project plan.

As you finalize the design, you interview members of the IT organization. You find that there is an existing mobility team focused on administration of Workspace ONE UEM, but that there is not much cross-training or knowledge-sharing between this team and the desktop-management team focused on SCCM solutions. To remedy the situation, you recommend VCP-DW certifications for the lead architects of the desktop team. You recommend VCP-DA certifications for the five existing support members of the desktop team. Lastly, you recommend a cross-training program in which each desktop team member will shadow a member of the mobility team for no less than one month on a rotating basis. This will allow the team to gain additional experience on the Workspace ONE platform.

Technical Resource Consulting's results

It's been three months since the completion of the design for TRC, and the project has so far been a huge success. Since very little new on-premises infrastructure was required, the installation process took only a few days to install and verify the software.

The initial rollout to new users takes a bit more time than you hoped due to shipping delays and working with a busy subset of users, but you are able to achieve 75 percent adoption within three months. This is seen as a huge win by leadership. They estimate that the company will hit 100 percent within the next three months. Working with the IT organization, you also capture some rough productivity metrics for the design team. Although there has not been enough time to measure downtimes for productivity metrics, the first batch of employee review scores have been overwhelmingly positive: a 60 percent improvement over last quarter's scores. Having completed all the recommended training, the desktop team has begun helping end users directly on the Workspace ONE platform. Anecdotal evidence suggests that cross-training with the mobility team was the key to this seamless cutover.

Having completed a successful design and implementation for TCR, you close the project by recommending the next step on the roadmap for the company. Now that Workspace ONE Access has been implemented for desktop users, implementing this functionality for mobile users would be a logical next step.

Example 4: The one where everything goes wrong

BB Clothiers' business and IT background

BB Clothiers is a US-based retail clothing business that formed in the 1910s. The events of 2020 and 2021 have been tough on the company, and it has been forced to close 50 percent of its retail locations. BB was slow to develop an online presence and chose instead to double down on physical locations. This gave them a strong nationwide presence and significant brand awareness among US shoppers. However, this overextension into brick-and-mortar left them overly exposed to the events of 2020.

BB, like most US retailers, outsources its manufacturing to third parties. The company directly employs 4,200 workers: 3,000 retail workers, 600 members of the design org (encompassing new clothing designers, buyers and materials sourcing), 400 back-office employees (comprised of HR, finance, and corporate management), and 200 IT workers distributed across the US. The company is typically slow to adopt new technologies. It maintains a single data center at its corporate headquarters in Silver City, New Mexico, and prefers to run most software on-premises for historic reasons. The firm's IT group is overwhelmed with maintaining older, often unsupported systems and typically spends most of its time on support requests from retail stores.

The company does not seem to have clear goals for the software, just to "implement mobile" as per their technology leadership group. When pressed for more information, the group responded that they were "fighting fires with the retail managers" and hung up before you could achieve any clearer information.

Despite a lack of background information, you've been hired as a consultant to help design a Workspace ONE-based solution and help BB achieve their business and IT goals. How do you proceed?

BB Clothiers' Workspace ONE design

Based on the lack of background information, you are anxious to begin the discovery phase. You begin by attempting to take note of BB's current IT situation and making a roadmap based on building capabilities. However, before you can start, the company's CTO insists that you are wasting your time and that the project "is already three months behind." When you express the importance of building a clear roadmap, the CTO responds that "nobody will read it anyway." You begrudgingly relent.

You then work with the customer to list out the user communities being supported by the first rollout for BB. You are made aware of the 4,200-person user base and how it is divided among departments. You then find that each region has a local IT support team that assists the retailers with IT support and new capability buildout. You're instructed that there is significant friction between the local IT leaders and the corporate IT team. When you attempt to reach out to the local IT leaders for guidance or information, your calls and emails are ignored. Without any better information, you propose a single use case to serve as an MVP: corporate users. However, you are overruled by the company's CTO, who exclaims, "The whole point of this project is to fix the retailers!" Your arguments unfortunately go unheeded. So relentingly, retail workers is forced as the first use case.

When you attempt to establish a list of business requirements, technical requirements, assumptions, risks and constraints for the project, you receive a now-familiar response: "We don't have time for that, and we wouldn't read it anyway."

Hoping to gain momentum with solution design, you find that retail workers generally need access to secure email, but some regions have implemented their own email systems unbeknownst to corporate. You're told "not to support these shadow IT solutions and only provide the mail from the corporate server." This has left a hodgepodge of systems to support. Different regions also provide different applications, different device support, and many are side-loading hacked applications from the Google Play store. After significant effort, you are able to determine that most retail sites continue to use the on-premises AD system. You are unable to find any information about the applications on the retail side despite numerous conference calls,

emails and inquiries. Since you know so little, you're forced to make assumptions based on your previous retail implementations. You make the assumption that identity & access are not needed and that each retail user will receive his or her own device. You are also forced to assume that the retail application does not need any tunneling functionality into the corporate network, as you do not want to design or install any unnecessary components without cause. You document these assumptions in your project workbook, but nobody reads it.

Based on what you know so far, you plot out the network architecture diagram below for the solution.

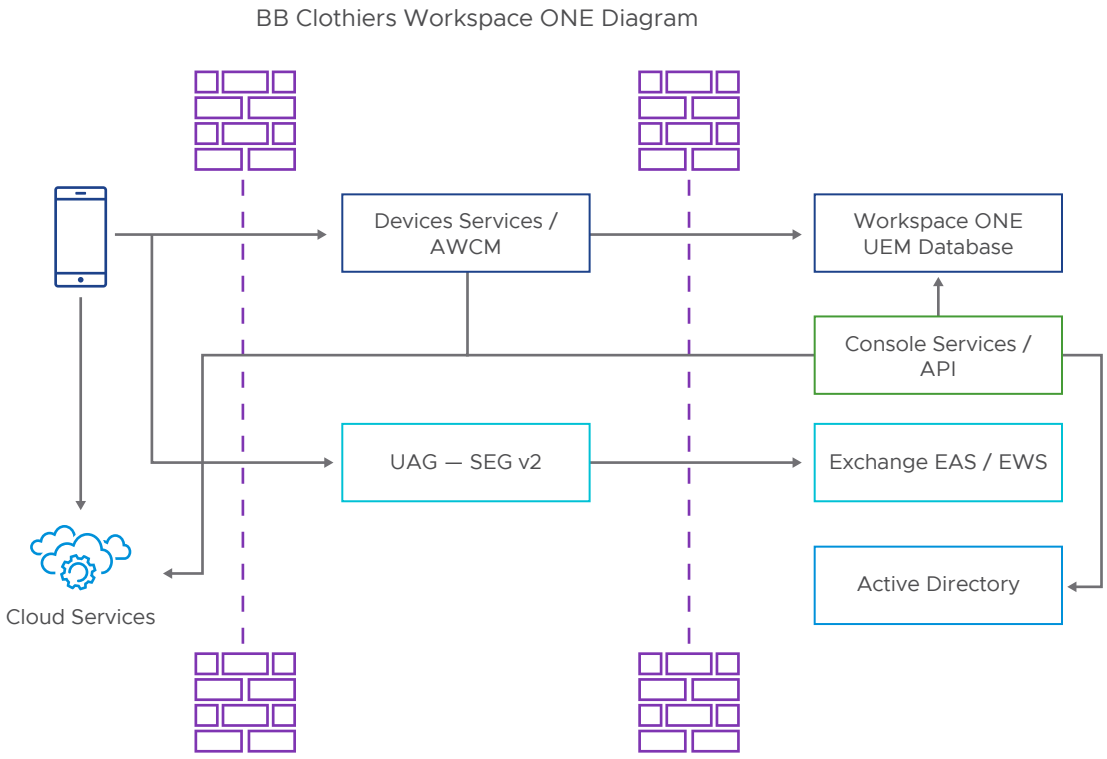

Figure 18: BB Clothiers' network architecture diagram.

Having established a basic network architecture and high-level solution design, you map out an initial OG hierarchy. Your preliminary diagram is below.

Figure 19: BB Clothiers' organization group hierarchy.

Both diagrams are approved quickly, leading you to believe they were not reviewed thoroughly. You raise this as a risk in the project management workbook, but again, the workbook is not consulted by BB regularly.

Staying on trend, BB does not offer you any project management assistance or contact points within the company. You are forced to create a basic project plan without customer input. You choose a simple waterfall-based plan that implements our single use case of retail workers. You further assume that adoption and rollout activities can be performed all in one shot. At this point, your frustration is causing you to rush through decisions. You create a very basic communication plan consisting of a few simple emails from corporate and from yourself. In your frustration, you forget to plan or track any KPIs, thinking that "nobody would care" due to your previous experience with these types of inquiries to BB leadership. Sadly, you give up on the project plan before even sharing it with BB leadership.

As a final insult, no one from the customer IT team attends the meeting you had set up to discuss long-term ownership of the solution by IT. This is a huge red flag, so you call the CTO directly to raise the issue. The CTO responds, "Support will own it. I already got it approved by them. They know MDM. Just get the design and install done, and they'll be fine." Without any way to understand the team structure, their skillset, or their training needs, you unfortunately must proceed without a clear plan for operationalization of the solution.

BB Clothiers' results

Eighteen months later, the project to provide mobility solutions for BB Clothiers is still ongoing with no clear end in sight.

After an implementation based on a surprising lack of background information, the solution was handed off to the support organization. The firm's technology leadership team had not engaged support previously, meaning that they were surprised by the release of the technology into their hands. "How are we supposed to manage this?" was a common refrain. One surprising complaint from both corporate IT leadership and the local leaders was that the service was installed on-premises. "We don't want to manage these servers!" was a frequent complaint. The original plan to develop UEM capabilities and delivery of email and applications to retail workers hit many snags and is still in limbo today. After installing and configuring the system to integrate with BB's corporate mail server, you found that none of the retail locations were actively utilizing these mail systems. You also found that the side-loaded applications from the Google Play Store were no longer supported by Google, meaning they could not be managed by Workspace ONE UEM. You called this out to corporate as an extreme security issue (unmanaged, unsupported applications accessing company email on rogue email servers). The CISO has stressed that the company will look into it.

After 18 months, only 20 users are fully-managed on the system, and these are all members of the local IT team that you were eventually able to recruit to assist with testing by enrolling into the TEST organization group. At this point, there is no clear way forward for what needs to be built, how the company will rationalize its disparate systems, or who will own the UEM system going forward. Since you did not establish clear KPIs, there is no tracking toward success. However, the 20 users on the system represents a 0 percent adoption rate since no retail workers have enrolled in the system.

After this failure, you schedule an in-person meeting with the CTO. Unfortunately, the meeting does not go well. You decide to leave the project. You find out months later that the company decided to scrap the system completely.

BB Clothiers' lessons learned

What a disaster the design for BB Clothiers was! Ultimately, the lesson isn't that the architect could have done many things differently during the design other than refuse to perform it altogether. However, zooming out, I'll argue that the story represents a cautionary tale that stresses the importance of the following aspects of a quality design:

- Good designs are deliberate. They are not rushed. A good design is thorough in nature and takes into account the existing customer situation, their business requirements and technical situation, and important assumptions, risks and constraints. Not having these important pieces of information should be a blocker for producing a quality design.

- Communication is key, specifically with the business. What sunk this design worse than anything was the lack of communication with the retail business stakeholders. Despite the fact that IT leadership ignored the architect's requests for quality information and design review, the design still could have been successful had the architect been able to establish a meaningful dialog with the retail stakeholders.
- Deciding what to measure is important. If you don't know where you're aiming, you'll miss every time. Not having clear KPIs and success metrics meant that the architect had no platform to defend himself or herself when met with a difficult final discussion with the CTO. Since the customer had no clear roadmap or goals, it was impossible to determine if or when they would be met.
- Key design decisions are key. Missing on the "on-premises vs. SaaS" design decision was costly. This is one where the architect should have called a "time-out" and expressed the extreme importance of getting this one right. Changing a configuration can be done at any time. Changing hosting is not easy and has vast implications from infrastructure, cost, licensing and maintenance.
- People and process are just as important as technology. Remember the equation early in the book. Capability = people + process + technology. That isn't just window dressing. The story with BB Clothiers is a good illustration of technology failing because nobody was there to own it or manage it properly once it was deployed.
- Being a great architect means knowing how to ask the right questions. No explanation necessary.

My guess is that many of you can relate closely to this story. Most technology professionals have been a part of one or two projects that have gone sideways, so hopefully I didn't hit too close to home and cause any painful flashbacks. The reason I wrote this example is because the problems I called out are not uncommon. Being deliberate and following a systematic design methodology is more time-consuming than jumping right into configuration in the short-term. In the long-term, however, it leads to more meaningful outcomes and more successful implementations of operationalized technology capabilities that solve real business problems.

Part 7: Conclusion

Final thoughts and recommendations

"The only true wisdom is in knowing you know nothing."

Socrates

We've now come to the end of our journey. We've gone through the complete end-to-end process for designing effective Workspace ONE solutions.

I hope, more than anything, that reading this book has presented you with even more questions. The world of Workspace ONE and mobility management are ever-changing as the needs of the modern workforce evolve. Being an effective engineer, architect, designer or developer means never resting on your laurels and always being open to new ideas and solutions.

If you'd like to continue your study, I'd highly recommend taking the following actions:

- Make sure to sign up for the latest news and releases on MyWorkspaceONE.
- Check out the VMware Digital Workspace Tech Zone: techzone.vmware.com
- Follow the VMware Customer Experience and Success blog, where I happen to be an author: blogs.vmware.com/customer-experience-and-success

Note: Every effort has been made to provide copious references to the technical information listed in this document. However, the nature of mobile technologies is extremely dynamic. For the latest on VMware products, please refer to docs.vmware.com.

Part 8: About the Author, Appendix

About the author

Roy McCord is a senior staff architect with VMware Professional Services. Day-to-day, he is focused on designing, architecting, and promoting VMware's suite of end user computing service offerings. Roy is a three-time graduate of the Georgia Institute of Technology in Atlanta, GA, where he achieved BS-CmpE, MSECE and MBA degrees. He has continued his education with two professional certificates from Stanford University. He holds VCP-DW, DW-SME, TOGAF and PMP certifications. Roy's blog can be found at: blogs.vmware.com/services-education-insights/author/rmccordvmware and he can be followed on Twitter at @Renaissance_Roy.

Appendix: Glossary and Acronym Descriptions

ACC	AirWatch Cloud Connector
AD	Active Directory
ADCS	Active Directory Certificate Services
API	Application Programming Interface
APNS	Apple Push Notification Service
Assumption	Any necessary item that we assume must be true for the design to function properly.
Business Requirement	Any requirement that is imposed by business (non-IT) factors that will affect the design for the solution.
BYOD	Bring-Your-Own-Device
CA	Certificate Authority
Capability	The combination of people, process and technology necessary to provide a specific value-set back to the business or a set of users.
CISO	Chief Information Security Officer
CN	Console (Server)
Competency	A combination of capabilities necessary to be proficient in a specific technical focus area.
Constraint	A limitation that is unique to this specific business or this specific technical situation.
DC	Domain Controller

(DDoS)	Dedicated Denial of Service
DEEM	Digital Employee Experience Management
DR	Disaster Recovery
DMZ	Demilitarized Zone
DS	Device Services (Server)
EMM	Enterprise Mobility Management
EUC	End User Computing
FCM	Firebase Cloud Messaging (formerly GCM – Google Cloud Messaging)
GA	General Availability or Generally Available
GUI	Graphical User Interface
HA	High-Availability
IDE	Integrated Development Environment
IdP	Identity Provider
IP	Intellectual Property
IT	Information Technology
KPI	Key Performance Indicator
LDAP	Lightweight Directory Access Protocol
MDM	Mobile Device Management
MEM	Mobile Email Management
MFA	Multi-Factor Authentication
MVP	Minimum Viable Product

OAuth	Open Authorization
OFA	Outcome-Focused Approach
OG	Organization Group
OS	Operating System
OVA	Open Virtualization Appliance
PCLM	PC Lifecycle Management
PMP	Project Management Professional
Risk	Any situation that could lead to potential failure of the solution. All listed risks should also list one or more mitigation steps.
SaaS	Software-as-a-Service
SDK	Software Development Kit
SEG	Secure Email Gateway
SMART	Specific, Measurable, Achievable, Realistic, Time-Bound
SMTP	Simple Mail Transfer Protocol
SSO	Single Sign-On
Technical Requirement	Any requirement imposed by the current situation in IT. There are many categories of technical requirements: usability, security, manageability, etc.
TOGAF	The Open Group Architecture Framework
UAG	Unified Access Gateway
UEM	Unified Endpoint Management
VM	Virtual Machine
VPN	Virtual Private Network

WS1	Workspace ONE
WSUS	Windows Server Update Services
WU4B	Windows Update for Business (unofficial/colloquial)

Item No: 1263300aq-tech-wp-tech-vmw-ws-one-dsgn-hndbk-uslet 3/22