WHITE PAPER–JANUARY 2021

From Theory to Practice: Top Considerations for Migrating to Windows 10 Modern Management with VMware Workspace ONE

vmware®

Table of contents

LEARN MORE

For more information about Workspace ONE, visit *https://www.vmware.com/products/workspace-one.html*.

To explore Workspace ONE UEM, visit *https://www.vmware.com/products/workspace-one/unified-endpoint-management.html*.

The Rise of Modern Management

Modern management of Windows 10 desktops is no longer an option but rather a necessity. Legacy management systems for a fleet of Windows desktops are typically a patchwork of software applications and result in a chaotic and often unstable environment. Traditional approaches use multiple administrative tools to manage the PC lifecycle, including separate tools for staging and imaging, maintaining drivers, managing OS updates, configuring firewall, antivirus and encryption policies, and more. The remedy is a modern management system that delivers policies, patches and applications from the cloud. This approach unravels the legacy management challenges, inserts integrated tools, and adds to security and visibility.

With the acceleration of remote desktop computing in 2020 and 2021, and with the likely continuation of a high level of remote desktop use in the future, migrating to Windows 10 modern management is more urgent than ever. Deploying a cloud-first management and security strategy is the modern way to manage your Windows 10 desktops. A cloud native solution to Windows 10 desktop management adds efficiency and security, as well as saves time and money.

VMware offers a work-from-anywhere solution for managing Windows 10 desktops: the VMware Workspace ONE® platform. Workspace ONE is the only complete and cloud native Windows 10 modern management solution that eliminates the need for complex on-premises infrastructure, cloud gateways, and hybrid management tools. The solution's cloud native architectural approach reduces the complex on-premises infrastructures of the past while keeping the ability to design secure edge strategies. This leaves each company in control of their architecture, while removing the headache of managing it.

The Workspace ONE platform offers the following features to migrate your Windows 10 devices to modern management:

- Administrative console that unifies enterprise mobility management (VMware Workspace ONE Unified Endpoint Management [UEM]).
- Ability to set up monitoring and automation of Windows 10 desktops (VMware Workspace ONE® Intelligence).
- End-user digital workspace that is a unified application catalog, notification center, self-service portal, and more (VMware Workspace ONE® Intelligent Hub). Users access and sign up for applications through the Intelligent Hub and receive notifications about new applications, plus alerts about their devices. They can also self-service their devices and applications. From this platform, end users can navigate to all their corporate applications and services, including native Windows 10 applications, virtual applications, web applications, and virtual desktops. Includes optional services that you can deploy to users.
- Desktop lifecycle management tool that simplifies the transition from traditional PC lifecycle management to modern management with Workspace ONE UEM (VMware Workspace ONE® AirLift).
- Storehouse of hundreds of commonly used prepackaged and preconfigured apps that IT can instantly deploy to end users' Workspace ONE Intelligent Hub catalog (Enterprise App Repository, part of Workspace ONE UEM). The applications in the repository are kept up to date and pretested across the last three OS builds, ensuring a guaranteed installation.
- Platform that allows you to create customized workflows for resource actions to be applied to devices in a specific order, according to granular criteria that you set up (VMware Freestyle Orchestrator).
- Support tool that empowers IT and help desk staff to remotely view and control Windows devices directly from the Workspace ONE console (VMware Workspace ONE® Assist).

- Automated intelligence tool that looks at and remediates user experiences with applications, the operating system, and performance (Digital Employee Experience Management [DEEM]). Displays analytics for key performance indicators that impact employee experiences, such as start time, shutdown time, and login and logout events. Gathers data from Windows devices and sends it to Workspace ONE Intelligent Hub, which in turn sends the data to Workspace ONE Intelligence for display and interaction on dashboards.
- An automated virtual assistant with a natural-language-processing chat feature (VMware AVA, included in Workspace ONE Intelligent Hub). Users can ask for help to find the right tools, troubleshoot problems, order new devices, open tickets, manage their tasks, and more.
- Feature that allows you to keep all your devices secure with settings and configurations based on industry-standard policies (Workspace ONE Baselines). Includes a catalog of thousands of policy settings to apply to your devices.
- Service that enables you to configure drop-ship devices to deliver to new users with virtually no IT touch or user downtime (Drop Ship Provisioning for Workspace ONE, a feature of Workspace ONE UEM).

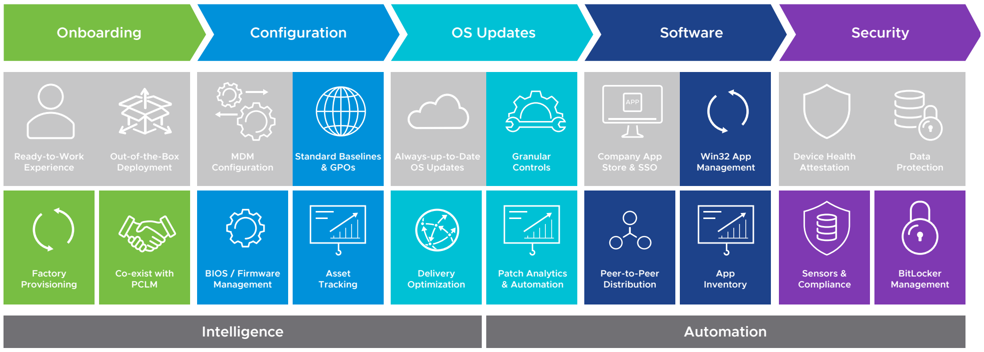


FIGURE 1: Workspace ONE integrates access control, application management and multiplatform endpoint management into a single platform.

The goal of this paper is to provide an overview and guidance around key considerations when migrating to modern management of Windows 10 desktops with Workspace ONE.

Migration options: goodbye device-based approaches, hello personas

Legacy management of Windows 10 devices uses a device-based approach, so a configuration is applied regardless of who is using the device. This method worked well when Windows machines were largely stationary in an office because a single update could be defined and efficiently applied to every device. However, this is not the world we now live in.

The inherent inflexibility of the device-based approach, where a single update affects every device at the same time, no longer fits with today's anywhere workforce, making it a poor choice for migration. Modern management uses a persona-based approach, which recognizes that employees use their devices for more than one task and often in more than one context. A persona—sometimes called a use case—is a group of people that are leveraging resources or services made available through purpose-built architectures. Within a persona, you can have many different roles.

With a persona-based approach, large groups of similar people can be addressed at once. Using an agile approach, you begin the migration journey focused on one persona broken into distribution rings. The first ring contains a small number of users, and you address all the tasks of that persona. After a successful rollout to the first ring, you can apply changes to the subsequent distribution rings, culminating in the complete management of the first persona. By using distribution rings, you can test, confirm, adjust, and scale a rollout throughout the journey.

Regardless of the size of your organization, you can benefit from a persona-based approach because you can incrementally move people from existing solutions while tweaking and improving procedures as you expand the migration.

These are some examples of personas that various organizations have chosen. We recommend a total of three to six personas, which may or may not come from this list.

- IoT
- Kiosk devices
- Back-office devices
- Factory-based devices
- Laboratory devices
- Highly secure departments

A key part of the persona-based approach is to start with a persona that is basically standard rather than a corner or edge use case.

The journey to Windows 10 modern management

Think of the migration to modern management of Windows 10 desktops as a journey, not a sudden change. You can take on the stages of the migration as time, funding and staffing allow. And each organization's journey from legacy to modern management is different. The reward is incremental: Time and cost savings build up over time, no matter how quickly you do the migration.

The steps to the migration are

Step 1: Plan the migration

Step 2: Lay the groundwork for the migration

Step 3: Roll out and support the migration

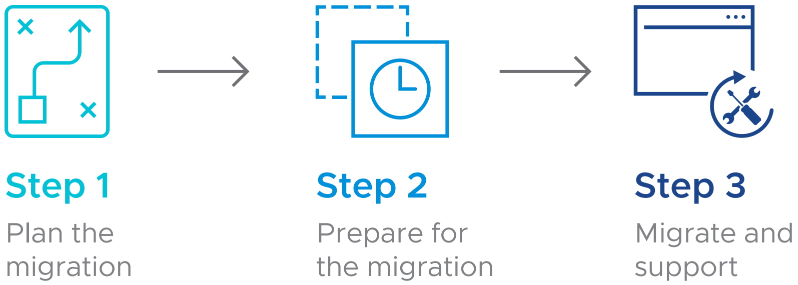


FIGURE 2: Windows 10 Modern Management Migration

Step 1: Planning the Migration

To plan your organization’s migration to modern management of Windows 10 desktops, you must

- Define your organization’s user personas and tasks
- Define requirements across personas
- Map legacy to modern-management options
- Build a migration project schedule with task dependencies

Defining your organization’s user personas and tasks

Defining three to six personas is a reasonable target. Fewer personas do not allow enough opportunity for improvement of your migration process, and more personas complicate the migration and increase costs.

Each persona has a set of tasks, and tasks can repeat over different personas. However, you will find an architectural, procedural deviation between these groupings that will define it as a new persona.

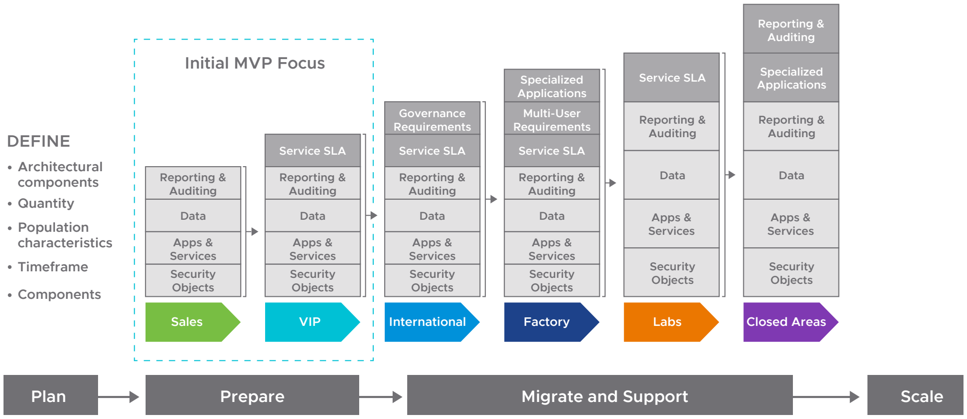


FIGURE 3: Migration Overview

Defining requirements across personas and building a migration schedule

After you have defined your personas and tasks, you are ready to establish a list of items to work on, or *backlog*. The goal is to work in *sprints,* or blocks of time, allotting 2 to 3 weeks per block. You estimate which tasks you can complete in a sprint and keep refining your projections as you move the project forward. Typically, each sprint has a theme (also known as an *epic*), so you can let the teams that you are working on know which functions will be ready at the end of the sprint. This flexible process lets you better respond to changes as they occur. The objective is to achieve outcomes along your journey and not wait until the end to see if that is the right thing for your organization.

Start with a *minimum viable product (MVP)* that you would need to manage your base persona. (See Figure 3 for an example.) Subsequently, you map deltas or incremental requirements across more complex personas. For example, in most organizations, a persona might be Sales or on-the-go professionals who rely on basic work profiles, such as email and network configuration, and data protection policies, and primarily use SaaS and cloud applications. As you move through the sprints, you can additional requirements such as those around VPN profiles, stringent compliance, classic Win32 applications, and so on.

Mapping legacy to modern management options

When mapping legacy to modern management, you must consider processes, procedures, applications and tools. You are not just replacing a tool but changing the way IT interacts with users. You will most likely need to move some of your tool type data to the new platform, such as for applications, so you must decide how to do that. For instance, Workspace ONE AirLift simplifies the transition from a traditional PC lifecycle management system to modern management with Workspace ONE UEM.

For *group policy* rationalization and migration to modern management, Workspace ONE AirLift communicates with Microsoft Active Directory. For *application* rationalization and migration to Workspace ONE UEM, Workspace ONE AirLift interacts with ConfigMgr.

Step 2: Laying the Groundwork for the Migration

To prepare for the migration:

- Determine which architectural components of Workspace ONE to deploy
- Set up groups
- Enable VMware Workspace ONE Intelligent Hub integration
- Configure privacy and device ownership settings
- Perform domain and Azure integration
- Set up device collections
- Configure work profiles
- Migrate applications
- Configure updates
- Set up compliance requirements
- Set up for drop-ship onboarding
- Set up monitoring and automation

We discuss each of these prerequisites briefly here.

Determining which architectural components of Workspace ONE to deploy

With many users working remotely, including users on personal devices, privacy considerations are key. Users' personal applications and data must be respected, and the organization's applications and data protected.

For all your personas or use cases, list existing technologies, and decide which new architectural components of Workspace ONE to integrate first. The Workspace ONE platform gives you access to various products and features, and you choose which to deploy.

We recommend deploying as much of Workspace ONE as possible for the best user and administrator experience.

Setting up groups

You use a Workspace ONE smart group to specify which platforms, devices and users receive an assigned application, book, compliance policy, work profile or provision. The customizable smart groups provide a mechanism for you to assign resources based on privacy needs and device ownership.

Enabling Workspace ONE Intelligent Hub integration

The Workspace ONE Intelligent Hub is essential to your end users' experience. Deploy it, and consider configuring additional Workspace ONE Intelligent Hub services, such as Custom Branding, Home tab, and People Search.

Configuring privacy and device ownership settings

End users who work on their own devices (BYOD users) are particularly concerned about the privacy of their personal content on a device that is managed by Workspace ONE UEM. You must assure employees that their personal data is not subject to corporate oversight.

With Workspace ONE UEM, you can ensure the privacy of personal data. You create customized privacy policies based on the device ownership type.

Performing domain and Azure integration

Workspace ONE UEM integrates well with Microsoft Active Directory (AD) and Microsoft Azure Active Directory (AAD), providing you with a selection of onboarding workflows that apply to a wide range of Windows 10 use cases.

To migrate workloads, you must integrate Workspace ONE AirLift with ConfigMgr and the Active Directory domain.

Setting up device collections

Workspace ONE AirLift connects your ConfigMgr device collections to Workspace ONE UEM smart groups.

For your key personas, migrate all device collections to Workspace ONE so that when you complete your configurations, you can assign them to smart group mappings.

Configuring work profiles

Legacy Windows management uses GPOs to manage devices. With Workspace ONE modern Windows management, work profiles are the primary mechanism for managing devices. Work profiles are sets of controls deployed to individual devices. Each profile consists of settings, configurations and restrictions. When combined with compliance policies, a work profile enforces corporate rules and procedures.

For example, with Workspace ONE, users do not enter a password for Wi-Fi; instead, their ability to use Wi-Fi is certificate-based within a work profile. Users connect to Wi-Fi automatically when they log in, as specified in their work profile.

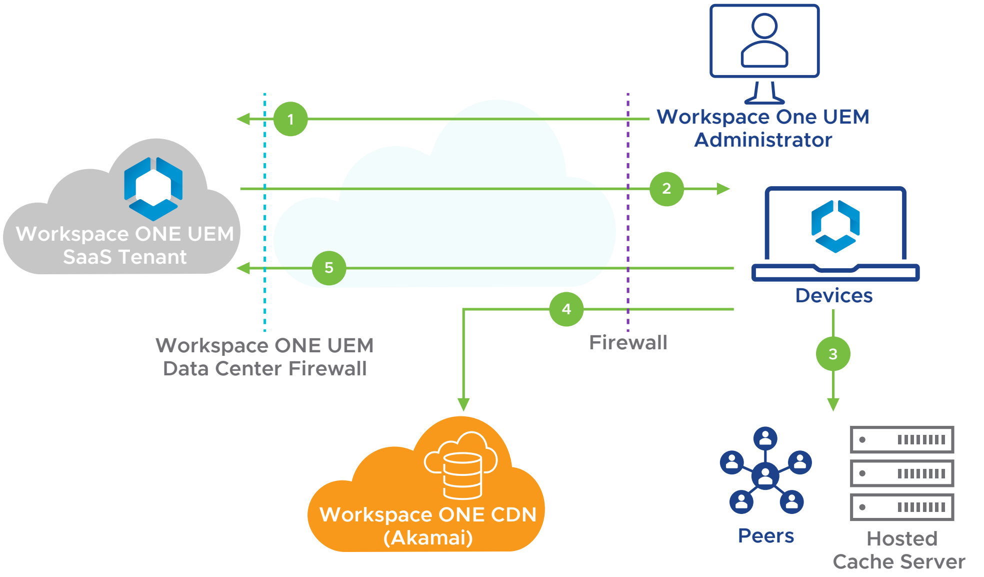
Similarly, users connect automatically to the VPN when they log in because of their specific work profile.

Migrating applications

Migrating applications involves three main steps:

- Migrate Windows applications, and assign these applications to smart groups or personas
- Set up peer-to-peer and cloud delivery
- Set up the Workspace ONE Intelligent Hub application catalog

The Workspace ONE UEM software delivery architecture is backed by a content delivery network (CDN) and peer-to-peer technology integration. This means that end users can get their applications installed no matter where they are without the need for a complex infrastructure.


Workspace One UEM Administrator
1
2
Workspace ONE UEM SaaS Tenant
5
Devices
4
3
Workspace ONE UEM Data Center Firewall
Firewall
Workspace ONE CDN (Akamai)
Peers
Hosted Cache Server

1. Application configured in Workspace ONE UEM
2. Workspace ONE UEM requests to install application
3. Device reaches out to peers or host for cache if configured
4. Device will reach out to CDN if no peer distribution configured
5. Fallback to device services server to obtain application

FIGURE 4: Workspace ONE Software Distribution Architecture

Migrating and assigning Windows applications

With Workspace ONE UEM, you can deliver most types of applications to Windows 10 devices: Universal Windows Platform (UWP) applications, cloud-based applications, hosted or remote applications, and classic Windows applications.

You can use Workspace ONE AirLift for the migration, and the Enterprise App Repository to speed up the addition of Windows applications directly into Workspace ONE UEM.

Setting up peer-to-peer and cloud delivery

You can set up cloud and peer-to-peer delivery of applications with Workspace ONE. If you subscribe to Workspace ONE with the SaaS model, VMware supplies a CDN. With a CDN, your users receive applications and application updates automatically from the cloud. When a geographically remote device requests an application download, the device is directed to the nearest cloud-delivery network and node and downloads the application from there. After the first download request, application downloads are cached at CDN nodes.

Organizations with on-premises Workspace ONE can integrate with their own CDN to achieve the same benefits.

Workspace ONE UEM offers the peer distribution system as another method to deploy your Windows applications to enterprise networks. Peer-to-peer application delivery reduces the time to download large applications and benefits organizations with

- Multiple devices in one office location
- Remote office locations with low bandwidth
- A branch-office structure
- Offices with a high latency against the CDN and Device Services Server

For these peer-to-peer downloads, Workspace ONE supports Adaptiva, a peer-to-peer software distribution tool, and the native branch-cache built into Windows 10. You can use Workspace ONE peer distribution or a peer distribution system that partners with Adaptiva.

Setting up the application catalog

Be sure to set up the Workspace ONE Intelligent Hub for users to access the migrated applications.

Configuring updates

Workspace ONE UEM follows the update-as-a-service model and pushes out periodic Windows operating system and feature updates. Traditional operating system upgrades use a wipe-and-replace model, but Workspace ONE UEM operating system updates occur on a frequent and dynamic basis. Therefore, end users always have access to up-to-date operating system features.

Workspace ONE UEM uses Windows Update for Business (WUfB), which is cloud-driven, instead of Windows Server Update Services (WSUS). The legacy WSUS requires many granular controls and high storage costs because of the requirement to store updates on-premises. With WUfB, users download updates online according to their work profiles.

After you set up WUfB and configure update policies, you define user persona distribution rings and the update policies for each distribution ring. In Workspace ONE, these are called *assignment groups*.

You can randomize distribution groups to spread risk among target groups, or build distribution rings that take into account the criticality of getting the updates. Be sure to allow time for testing and validation before applying updates to sensitive rings.

Your first-line distribution ring must be small and composed of users who are tolerant of preliminary testing and able to give accurate technical feedback, such as the IT group. Later distribution rings can be the majority of users, an approach that tests your assumptions from the smaller groups. The final distribution rings are outliers and small pockets of atypical users.

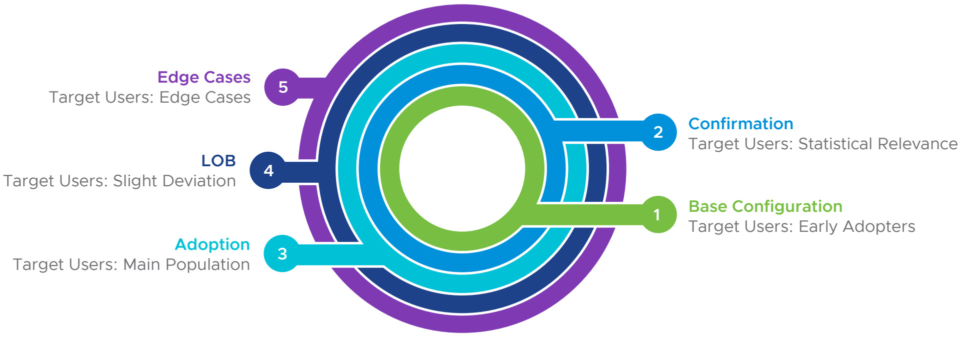

Edge Cases
Target Users: Edge Cases
5
LOB
Target Users: Slight Deviation
4
Adoption
Target Users: Main Population
3
2
Confirmation
Target Users: Statistical Relevance
1
Base Configuration
Target Users: Early Adopters

FIGURE 5: Deploy a ring approach to configure updates.

Setting up compliance requirements

To secure the Windows 10 devices in your environment, you must set up encryption and compliance.

Group Policy Object (GPO) baselines and benchmarks

With modern management, you are moving to cloud-based group policies and other configurations. A large part of leveraging cloud-based group policies starts with assessing your current policy landscape and determining if these policies need to move over to Workspace ONE UEM. Workspace ONE AirLift simplifies the validation and conversion of your current traditional group policies (GPOs) to Mobile Device Management–based policies.

If you currently do not have group policies on your domain or prefer to start over, you can leverage Workspace ONE Baselines. Workspace ONE Baselines helps keep all your devices secure with industry-standard settings and configurations based on the CIS Microsoft Windows Desktop Benchmark and the Microsoft Windows 10 Security Baseline templates. Workspace ONE Baselines uses a cloud-based micro-service that handles a catalog of thousands of policy settings to apply to devices. You can create or add to baselines using this catalog of policies based on the Microsoft ADMX files. These baselines are based on and function similarly to GPOs.

Encryption and BitLocker

With Workspace ONE UEM, you can manage the encryption lifecycle and configure automated encryption for Windows 10 devices. To do this, you migrate from McAfee Management of Native Encryption, configure a BitLocker Encryption profile, and verify the encryption settings applied.

Compliance, Health Attestation and restrictions

You can use Workspace ONE UEM to establish user trust, assess the device posture, and enable data loss prevention.

To establish user trust, Workspace ONE UEM uses robust identity features. These features include two-factor authentication, which requires that an enrolled, managed and compliant device meets two forms of authentication.

To assess device posture, Workspace ONE UEM evaluates, locally enforces, and remediates devices with its compliance engine, which is a Workspace ONE UEM tool that ensures that all devices abide by specified policies. A policy can include basic security settings or more critical security configurations.

You use the Workspace ONE UEM Console to specify escalation steps, disciplinary actions, grace periods and messages.

To minimize the risk of data loss, Workspace ONE UEM maximizes native Windows Information Protection capabilities. Data loss prevention on devices controls data propagation into the cloud.

Scripts and sensors

VMware Freestyle Orchestrator is a no-code IT orchestration platform that lets you create complex and customized workflows that are applied to devices with flexibility and speed. You organize resource actions to be applied to devices in a specific order according to granular criteria that you set up. The resources you can use in a workflow are

- Applications (internal only)
- Conditions
- Groups
- Profiles
- Sensors
- Scripts
- Error handling

Setting up for drop-ship onboarding

With Workspace ONE, you can deliver fully configured Windows 10 devices to users' desks so that new users can be immediately productive. This drop-ship onboarding releases IT from laborious setup for each user. And with an increased number of remote workers, the time savings is substantial.

How do you do drop-ship delivery of devices to new users? Drop Ship Provisioning for Workspace ONE lets Windows-device OEMs and VMware administrators provide a user experience with virtually no IT touch or user downtime. Configurations, settings and applications are preloaded at the factory. Now, instead of waiting for applications and settings to download and apply, the user has a ready-to-work experience on first boot of the device. And if IT does a device reset or recover at a later time, Zero Touch Restore functionality allows applications and management to persist, which minimizes downtime.

Setting up monitoring and automation

Workspace ONE Intelligence allows you to set up monitoring and automation of Windows 10 desktops and integrates with Workspace ONE UEM to provide unified visibility and real-time data.

Monitoring with reports and dashboards

Workspace ONE Intelligence is a service that aggregates and correlates data from multiple sources to give visibility into the entire Windows environment through reports and dashboards. You can use reports to gain insights and use dashboards to visualize data and enforce device compliance.

Setting up automation

Automation in Workspace ONE Intelligence uses parameters to trigger a workflow. You can customize the workflow to act on specific scenarios in your Workspace ONE environment.

Following are some examples of the use of Workspace ONE Intelligence automation:

- **Battery health** – You can automate the detection of Windows 10 devices that have poor battery health. Windows devices that cannot last a full workday without requiring a charge are disruptive and reduce employee mobility and productivity. Automating battery replacements can help you improve employee experience, increase productivity, and maximize device lifespan.
- **Patch remediation** – You can automate patch remediation for your Windows 10 desktops with Workspace ONE Intelligence. You create a dashboard in Workspace ONE Intelligence that shows all devices currently missing a critical Windows update. You can also create an automation that notifies users when to update their devices. Combining device management capabilities with Workspace ONE UEM allows IT administrators to report and approve patch deployment.
- **Sensors-based automation** – Sensors allow you to flexibly meet your InfoSec compliance requirements by enabling query of any system parameter—from silicon to software—and making it available for reporting and automated remediation. For example, using Sensors scripting, admins can query desired app version, encryption status, registry key values, and more and use Intelligence automation to resolve compliance drift.

Step 3: Rolling Out and Supporting the Migration

Now that you have planned the migration and completed the prerequisites, migrate your organization's Windows 10 desktops, stage by stage, persona by persona, on a schedule.

Your first persona must be a small group that can tolerate your learning curve for the migration. Based on your experience with this first group, you can tweak and modify the process, and proceed to the next persona. By the time you reach your final 20 percent of users, you will have a proven methodology.

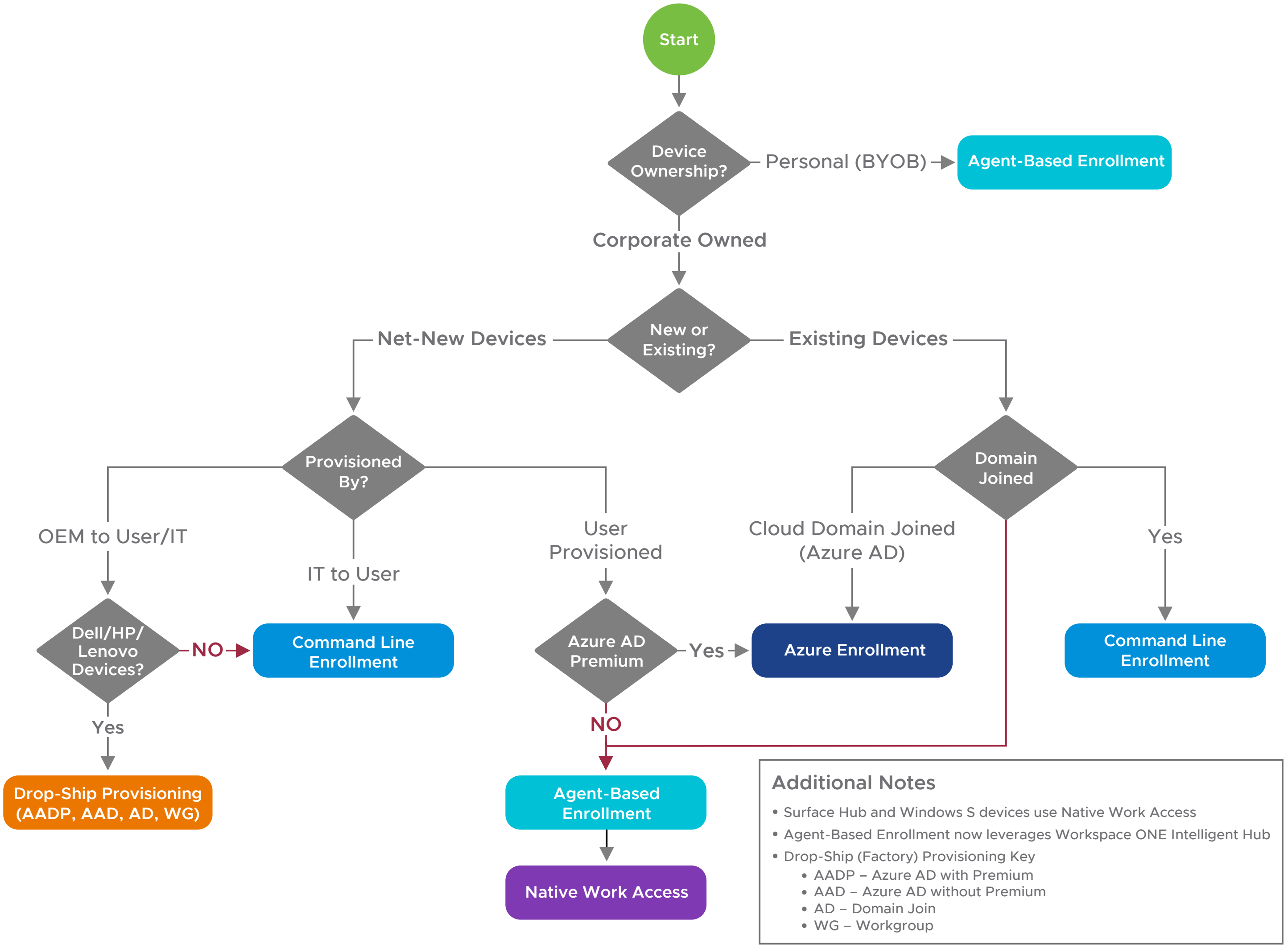
Workspace ONE provides mechanisms to support the work life of end users, including remote support and access to applications.

Enrollment options

Gathering Windows 10 desktops into Workspace ONE modern management is called *enrollment*. If a device is net new, you drop-ship. If a device already exists, you push down the Workspace ONE Intelligent Hub.

You can adapt the following decision tree to your organization to help you determine enrollment options for Windows 10 desktops. Possible onboarding workflows in this decision tree are:

- **Drop-ship provisioning** – Windows device OEM and VMware administrators can provide a virtually zero IT touch and virtually zero user downtime experience. Configurations, settings and applications are preloaded at the factory. Instead of waiting for apps and settings to download and apply, you can have a ready-to-work experience on first boot of the device.
- **Microsoft Azure Active Directory enrollment** – Workspace ONE UEM integrates with Azure AD, providing a robust selection of onboarding workflows, including Autopilot and enrolling during the out-of-box-experience.
- **Agent-based enrollment** – Leveraging the VMware Workspace ONE Intelligent Hub for Windows 10, lets end users enroll their own devices, giving them flexibility and control while reducing IT overhead.
- **Command-line enrollment** – Provides the greatest admin flexibility using command parameters. You can automate enrollment using your existing PCLM tools or domain.



Additional Notes

- Surface Hub and Windows S devices use Native Work Access
- Agent-Based Enrollment now leverages Workspace ONE Intelligent Hub
- Drop-Ship (Factory) Provisioning Key
  - AADP – Azure AD with Premium
  - AAD – Azure AD without Premium
  - AD – Domain Join
  - WG – Workgroup

FIGURE 6: Windows 10 Onboarding Decision Tree

Day 2 engagement and support

Workspace ONE Intelligent Hub

Workspace ONE Intelligent Hub is key for users to have continued engagement with IT. It is a centralized catalog for enterprise applications and notifications, as well as a portal for employees to interact with IT and perform self-service on their devices and applications.

With VMware AVA, part of Workspace ONE Intelligent Hub, users can interact with a natural-language-processing chat function to get help finding the right tools, troubleshooting problems, ordering new devices, opening tickets, managing their tasks, and more.

Remote support with Workspace ONE Assist

With Workspace ONE Assist, you can remotely view or control users' devices directly from the Workspace ONE console while maintaining employee privacy and trust.

Proactive support with Digital Employee Experience Management

Digital Employee Experience Management (DEEM) allows you to give proactive support to Windows 10 users by displaying analytics for key performance indicators. DEEM enhances supportability of your Windows 10 desktops.

Get Started

Migrating to modern management of Windows 10 desktops is a journey, not a sudden flip of a switch. Your plans leading up to implementing the migration are key, so you will want to take your time on the plan and then methodically carry it out.

Workspace ONE brings Windows 10 management, employee experience and workforce supportability to a new level. To learn more about how cloud native modern management with Workspace ONE simplifies operations, hardens security and delivers ready-to-work experiences to your employees everywhere, check out the *Workspace ONE hands-on lab*.

LEARN MORE

- Visit the *VMware TechZone*
- Check out the two-part VMworld customer session on cloud-first management:
  - *Real-World Steps to Cloud-First Management (Part 1 of 2)*
  - *Practical Steps to Cloud-First Management (Part 2 of 2)*

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com

Item No: FY21-6168-VMW-WIN10-MOD-MGMT-WKSP1-WP-USLET-WEB-20210120 1/21