

This PDF was generated on October 2023 and was current at the time of download. To check for the latest version please visit
<https://techzone.omnissa.com/resource/workspace-one-frequently-asked-questions-faqs>

Workspace ONE Frequently Asked Questions (FAQs)

Omnissa Workspace ONE

Table of contents

Workspace ONE Frequently Asked Questions (FAQs) 3

Overview 3

 Audience 3

Getting Started 4

Access Management 5

Device Management 7

Enterprise Integration 9

Reporting and Analytics 11

User Administration 13

Windows Devices Lifecycle Management 14

Windows Devices Endpoint Security 17

Application and Patch Management 19

Configuration Management 21

Platform and Application Support 23

Technical Support 24

Summary 25

 Changelog 25

 About the Author and Contributors 25

 Feedback 25

Workspace ONE Frequently Asked Questions (FAQs)

Overview

The Workspace ONE Frequently Asked Questions (FAQs) document provides answers to some of the most popular Omnissa Workspace ONE FAQs. We will continue to grow this list of FAQs so check back regularly for updates.

Audience

This Workspace ONE FAQs document is intended for existing or prospective Workspace ONE IT administrators.

Getting Started

What is Workspace ONE?

Omniessa Workspace ONE is a digital platform that delivers and manages any app on any device by integrating access control, application management and multi-platform endpoint management. This enables IT to deliver a flexible digital workspace without sacrificing security and control. For more information, see [What is Workspace ONE?](#)

How does Workspace ONE work?

Workspace ONE is built on unified endpoint management (UEM) technology and integrates with virtual app delivery (Omniessa Horizon) on a common identity framework delivered by Omniessa Access. The primary end-user component is the Workspace ONE app. For more information, see [What is Workspace ONE?](#)

Is AirWatch now Workspace ONE?

Yes. The unified endpoint management (UEM) technology, Omniessa Workspace ONE UEM, that Workspace ONE is built on, was formerly known as AirWatch.

What capabilities does Workspace ONE provide?

Key capabilities of Workspace ONE include:

- Consistent, flexible endpoint management
- Adaptive management for BYOD programs
- Intelligent insights and automation
- Comprehensive digital workspace security
- Device-aware access policies
- Digital employee experience

What is the difference between Workspace ONE and Horizon?

Workspace ONE is a comprehensive platform that delivers and manages any app on any device, providing a complete digital workspace solution. Workspace ONE is composed of several components, one of which is Horizon, a platform for delivering virtual desktops.

How can I evaluate Workspace ONE?

The following evaluation guides walk you through a series of practical exercises to help you evaluate Workspace ONE.

Part 1: The [Evaluation Guide: Setting Up Workspace ONE Cloud](#) describes the process of setting up a cloud-based Workspace ONE environment.

Part 2: The [Evaluation Guide: Managing Apps and Devices with Workspace ONE Cloud](#) describes how to perform the most common day-2 operations, such as deploying apps to devices, configuring single sign-on for end users, and configuring compliance policies.

Access Management

How does Workspace ONE validate the posture of the endpoint, the user identity, and the security of the app connection prior to allowing access?

Zero Trust is not a single product, but a modern security framework based on the notion of never trust, always verify. Zero Trust is a conditional access control model that requires verification of trust prior to allowing application access, and when that access is granted, it is with least privilege.

Our Zero Trust solution is based on developing five pillars of trust:

- Device
- User Trust
- Transport Session
- Application Trust
- Data Trust

The principle of least privilege means granting only the required access to applications for the user to complete their job and no more. By never trusting, and always verifying, Zero Trust protects your data and applications not only at the start of a session but also with continuous verification of users and endpoints throughout an application session.

What are the requirements of a Zero Trust architecture?

- Continuous verification of endpoint compliance – For access to be granted, endpoints must be continuously verified to be compliant with your organization's security policies.
- Conditional access control to all applications – For a user to gain access to applications, they must prove their identity.
- Reduction of the attack surface – To protect your organization's applications and data, each user must be granted only the least-privilege access to get their work done, and nothing more.

How does Workspace ONE secure corporate data access from mobile devices?

Some Security features of Workspace ONE include:

- Encryption: Authenticate and encrypt traffic from apps on devices into the data center. Secure app data at-rest and in-transit with AES 256-bit encryption.
- Access Management - Empower IT to deliver application provisioning, a self-service catalog, multi-factor authentication and single sign-on (SSO) for all apps.
- Contextual Policies - Control authentication with conditional access policies based on device compliance state, user authentication strength, data sensitivity, user location, and more.
- Data Loss Prevention (DLP) Policies - Configure policies with modern management, including device-level data encryption, app denylists and Wi-Fi security. Monitor for threats ranging from malware and malicious apps to jailbroken devices. Automatically remediate with capabilities including remote lock, device wipe, and access control.

Unified Access Gateway supports per-app tunneling of native and web apps on mobile platforms to secure access to internal resources through the Tunnel Service.

For details, see [Configuring the Tunnel Edge Service: Workspace ONE Operational Tutorial](#).

How does Workspace ONE UEM provide data loss prevention (DLP) on different device types and operating systems?

Configure policies with modern management, including device-level data encryption, app denylists and Wi-Fi security. Monitor for threats ranging from malware and malicious apps to jailbroken devices. Automatically remediate with capabilities including remote lock, device wipe and access control.

For details, see [Data Loss Prevention](#) in the [Workspace ONE UEM Architecture](#) chapter.

Provide DLP for corporate email, applications, content and browsing

- Email: Use Boxer to provide secure email management on devices without advanced capabilities

- Encrypt email data/attachments
- Prevent email forwarding to deny-listed domains (Boxer for iOS)
- Disallow copy/paste to other apps or accounts
- Disallow screenshots (Workspace ONE Boxer or Android)
- Apps: Build additional security into internal apps with the Workspace ONE UEM Software Development Kit
 - Require authentication (e.g., AD, passcode, SSO across applications, local app data wipe)
 - Data encryption
 - Access control (e.g., compromised, compliant status, network, geo-fence)
 - Restrict copy/paste, photo roll, open with other applications
 - App tunnel (app-level VPN)
- Content: Use Workspace ONE Content for content and file security
 - Securely distribute, track, manage and encrypt corporate content on mobile devices
 - Open and store email attachments in Workspace ONE Content
 - Control user's ability to edit, copy/paste, save, share or open files in unauthorized applications with Workspace ONE Content
 - Use OS controls and native features to identify corporate email and separate it from personal data
- Browsing: Configure Workspace ONE Web with copy/paste and print restrictions
 - Require document links in Workspace ONE Content to open in Workspace ONE Web
- Containerization: Fully manage devices by requiring MDM enrollment or deploy individual components without requiring full device management using the Workspace ONE portal or standalone solutions for email, apps, content and browsing

For more information, see

- [Data Loss Prevention](#)

Does Workspace ONE UEM support multi-factor authentication?

Yes, you can use the built-in multi-factor authentication (MFA) for Workspace ONE UEM by enabling Verify (Intelligent Hub) on the Workspace ONE Access admin console. Verify (Intelligent Hub) is an MFA authentication method integrated with the Workspace ONE Intelligent Hub app. You must integrate Workspace ONE Access and Workspace ONE UEM with Hub services to use Verify (Intelligent Hub). Configure two-factor authentication in the Workspace ONE Access policy rules to require users to sign in using password authentication first and then the Verify (Intelligent Hub) passcode.

Workspace ONE also integrates with multi-factor authentication providers to deliver a range of mobile MFA features including push notification, TOTP code, and SMS. The solution supports multi-factor authentication through Okta Verify, Duo, PingID, RADIUS, RSA SecurID and RSA SecurID Access, and certificate-based authentication.

For more Workspace ONE Access FAQs, see [Workspace ONE Access Frequently Asked Questions \(FAQs\)](#).

Device Management

How does Workspace ONE UEM group devices and users for management and assignments?

Workspace ONE UEM uses several different types of groups to manage users, devices, apps, content, and more. You can optimize your unified endpoint management (UEM) strategy by using a combination of organization groups, smart groups, and user groups to streamline assignments and management.

Each of these groups can be easily managed in the Workspace ONE UEM console as assignment groups, such as:

- [Organization groups](#)
- [Smart groups](#)
- [User groups](#)

For more information, see:

[Evaluation Guide: Setting Up Workspace ONE Cloud](#)

[Evaluation Guide: Setting Up Workspace ONE Cloud](#)

What is a Workspace ONE UEM organization group?

Organization groups are similar to organizational units in Active Directory and are typically based on the internal corporate structure; geographical location, business unit, and department.

With organization groups, you can:

- Build groups for entities within your organization (for example, Company, Headquarters, Subsidiaries, Management, Salaried, Hourly, Sales, and so on).
- Customize hierarchies with parent and child levels (for example, 'Salaried' and 'Hourly' as children under 'Management'). You can block or allow inheritance settings.
- Integrate with multiple internal infrastructures at the tier level.
- Delegate role-based access and management based on a multi-tenant structure.
- Manage device profiles, apps, policies, and products based on preconfigured network IP address ranges.

What is a Workspace ONE UEM smart group?

Smart groups determine which platform, devices, and users receive profiles, compliance policies, applications, books, baselines, sensors, scripts, and so on. Smart groups offer more flexibility than organization groups. You specify criteria for a smart group and if a device (or user group) matches that criteria, they are added to the group.

You can:

- Deliver content and settings to user groups, individual users/devices, device platform, OS, model, device tags, and so on.
- Set profiles and compliance policies to include or exclude specific smart groups.
- View and edit the profiles and policies assigned to and excluding individual smart groups.

What is a Workspace ONE UEM user group?

User groups provide additional criteria to assign resources to devices based on user access rights and job roles. With user groups, you can:

- Align end users with LDAP/AD associations, streamlining user and device management.
- Assign profiles, applications, content, and compliance policies to groups of users according to existing groups and distribution lists.
- Automatically update assignments based on directory user group changes or require administrator approval.
- Set role-based access control to only allow approved administrators to change policy and resource assignments for certain user groups.
- Assign multiple groups simultaneously – even of differing types – to profiles, public apps, and compliance policies.

What is the Workspace ONE UEM compliance engine?

The Workspace ONE UEM compliance engine is an automated tool that continuously monitors devices and performs escalating actions to prevent noncompliance.

The compliance engine allows you to:

- Enforce compliance policies and set up automated actions for noncompliant activity.
- Create rules for passcode, application compliance, data usage, voice usage, SMS usage, compromised status, encryption status, profile expiration, last compromised scan, Terms of Use acceptance, model, OS version, security patch version, roaming status, and SIM card change.
- View rules and actions available by platform for simple setup and administration.
- Set severity levels to perform escalated actions based on user response time frame.
- Notify IT and end users of noncompliance automatically using customizable notifications:
 - Via SMS, email or push notifications (end users)
 - Via email (administrators)
- Automatically block access to corporate resources, wipe corporate profiles or devices.
- Reinstall assigned profiles and apps without user interaction when device is compliant again.
- Optionally perform actions on a device without marking it as non-compliant.

Can Workspace ONE UEM enforce an approved software version on the device before granting user access?

Yes, you can set restrictions to require approved OS versions, applications, and so on, to enable device access to corporate data. Use *device profiles* and *compliance policies* to enforce required or prohibited operating systems and applications.

You can perform automatic compliance actions from the Workspace ONE UEM admin console such as sending notifications, enterprise wipe, profile installation/removal and managed application removal.

To add or update commonly used third-party applications for Windows devices, use the Enterprise App Repository.

Can Workspace ONE UEM perform a remote device wipe?

Yes, from the Workspace ONE UEM admin console, you can perform a remote wipe on demand or based on compliance policies. Administrators can include a note for users when performing a device wipe.

There are two main options; additional options are available depending on the platform.

- *Enterprise Wipe* removes all corporate connections, applications, and content. The Workspace ONE Intelligent Hub remains on the device for easy re-enrollment. The device is unavailable to view on the console.
- *Full Device Wipe* performs a “factory reset” to remove all device data (available only on demand). The Workspace ONE Intelligent Hub is no longer on the device. The device is unavailable to view on the console.

Enterprise Integration

What is Workspace ONE UEM enterprise integration?

Many of your existing enterprise components can be integrated into a Workspace ONE deployment. For example, securely integrate with AD/LDAP, certificate authorities, email infrastructures and other enterprise systems both in a cloud and on-premises deployment model.

The following components can be configured from the Workspace ONE UEM admin console:

- Directory Services – Integrate with AD/LDAP for authentication and group membership, helping to ensure that users receive appropriate profiles and access to apps and content.
- Certificates and PKI – Integrate with Microsoft CA, CA, or SCEP certificate services providers such as MSCEP and VeriSign.
- Email Infrastructure – Manage and monitor mobile email through tight integration to your corporate email infrastructure.
- Proxy – Microsoft Exchange 2010/2013/2016/2019, IBM Domino with Lotus Notes, Novell GroupWise (with EAS), Google Apps for Work Beehive and other EAS.
- PowerShell – Exchange 2010/2013/2016/2019, Office 365/BPOS.
- Google – Google Apps for Business.
- UEM Edge Services on [Unified Access Gateway](#) to enable secure remote access from an external network to a variety of internal resources. Unified Access Gateway supports the following Workspace ONE UEM use cases:
 - Per-App Tunneling of native and web apps on mobile and desktop platforms to secure access to internal resources through the Tunnel service.
 - Secure on-premises email infrastructure that grants access only to authorized devices, users, and email applications based on managed policies. This capability leverages the Secure Email Gateway service integrated with Workspace ONE UEM.
 - Access from Workspace ONE Content to internal file shares or SharePoint repositories by running the Content Gateway service.
 - Reverse proxying of web applications.
 - Identity bridging for authentication to on-premises legacy applications that use Kerberos or header-based authentication.

Other components that can be integrated:

- Corporate Networks – Configure Wi-Fi and VPN network settings with automatic connections and centrally updated user credentials.
- File Systems – Integrate with existing file systems, including SharePoint, Google Drive, OneDrive, file servers and networks shares.
- APIs – Integrate with existing IT infrastructures and third-party applications.
- Security Information and Event Management (SIEM) – Integrate with SIEM solutions for enhanced logging of events occurring in the console.

Can I integrate Workspace ONE UEM REST APIs with existing infrastructures and third-party applications?

Yes. Workspace ONE UEM provides a collection of RESTful APIs (application programming interface) that allow external programs to use the core product functionality by integrating the APIs with existing IT infrastructures and third-party applications.

Using the simplified REST style of software architecture, Workspace ONE UEM REST APIs support a multitude of functionalities, including organization group, console administration, mobile application, mobile device, email, enrollment user, profile, smart group, and user group management.

Workspace ONE UEM REST APIs allow external systems to create, update, delete and modify entitlements for user through a system for cross-domain identity management (SCIM) API.

Available web services include user enrollment, device registration, device groups, organization group management, smart group management, user information, device data, search functions, custom attributes, remote device commands and bulk actions, device and system events and notifications, application groups, content management, VPP management, product provisioning, tags, and other systems management and operation information.

For more information, see:

- [Getting Started with Workspace ONE Intelligence](#)

Does Workspace ONE UEM integrate with directory services (AD/LDAP)?

Yes, Workspace ONE UEM integrates with your existing directory service (for example, Active Directory and Lotus Domino) and allows you to authenticate to Workspace ONE UEM using your existing credentials. Use the built-in wizard to quickly and easily configure integration.

By integrating Workspace ONE UEM with your directory services, you can:

- Manage user groups according to current user organization and permissions.
- Assign profiles, applications, compliance policies, and content based on a user's role and group membership.
- Ensure that a user receives the right access and restrictions for all relevant groups (if the user belongs to multiple groups).
- Detect any changes within the system with ongoing directory synchronization and automatically perform necessary updates across all devices for affected users.
- Automatically enterprise wipe devices when users are removed from user groups.
- Require administrative approval or admin PIN before any changes occur.

For more details, see [Active Directory Integration](#) in the Component Integration chapter of the [Reference Architecture](#).

Reporting and Analytics

Does Workspace ONE include built-in reporting features?

Yes, Workspace ONE includes robust reporting features that empower administrators to centrally monitor device fleets using the following:

- Built-in [Workspace ONE UEM reports](#). (For custom reports, Workspace ONE Intelligence is required.)
- [Workspace ONE Intelligence reports](#).
- [Workspace ONE Intelligence dashboards](#). With Workspace ONE Intelligence, you can customize reports and analyze trends using data from the complete Workspace ONE environment.
- [Workspace ONE Access User Engagement Dashboard](#).

What are Workspace ONE UEM reports?

Workspace ONE UEM reports allow you to:

- Run live reports directly from the web console using the built-in reporting engine.
- Customize fields on standard reporting templates across various categories including, applications, device content, device inventory, profiles, telecom, and user management.
- Create subscriptions to send custom-generated reports to specific recipients at scheduled intervals.
- Create bookmarks to save popular reports and easily regenerate them.

For more details, see [Workspace ONE UEM reports](#).

What are Workspace ONE Intelligence reports?

Workspace ONE Intelligence aggregates and correlates data from Workspace ONE UEM, Workspace ONE Access, Workspace ONE Intelligence SDK, and Trust Network Solutions. Reports powered by Workspace ONE Intelligence provide access to critical business intelligence data and are different from the reports created in the Workspace ONE UEM console.

Workspace ONE Intelligence reports allow you to:

- Analyze trends across device, application, and user business intelligence (BI) data and build reports for a complete view of your entire digital workspace environment.
- Use the Reports wizard to create a customized report using a starter template or a new report from scratch.
- Create or schedule reports to provide detailed historical data about the entire environment and device fleet; gather an initial snapshot of your deployment and continue to capture ongoing changes.
- View live previews of reports to see results before running the entire report. Run reports in seconds, with options to view or export in CSV format.
- Easily share reports with the rest of the organization as links to avoid encountering file size limitations when sending via email.

For more details, see [Getting Started with Workspace ONE Intelligence](#).

What are Workspace ONE Intelligence Dashboards?

With Workspace ONE Intelligence Dashboards, you can:

- Configure the Monitor pane to display the most important business drivers/events.
- View deployment information in real time on interactive dashboards which are available in graphical or tabular view.
- Navigate to a list view and filter to show a specific group of devices, enrollment, compliance, profiles, applications, content, telecom, email, and certificate summaries on one central screen.
- Take action, such as sending a message, on individual devices or groups of devices.
- View data in a variety of formats, including graphs, portlets, and grids.
- Export dashboard information to spreadsheet format (CSV file).

For more details, see [Getting Started with Workspace ONE Intelligence](#).

What is the Workspace ONE Access User Engagement Dashboard?

The Workspace ONE Access console provides user and device analytics on the User Engagement Dashboard which allows you to:

- Monitor device-level usage analytics on a per-user and per-app basis.
- Specify audit events and generate reports for a configurable time period.
- Audit events and include time, date, and identity of administrative changes to permissions and app access.

For more Workspace ONE Access FAQs, see [Workspace ONE Access Frequently Asked Questions \(FAQs\)](#).

What is the Workspace ONE UEM event log?

Events are records of administrative and device actions that the Workspace ONE UEM console stores in logs. Integrate with Syslog to send log and event data and export event log data to CSV or XLSX files.

Workspace ONE UEM allows you to:

- Configure which console and device events (for example, administration, configuration, interaction, session management) to send to syslog.
- Integrate with security information and event management (SIEM) solutions for enhanced logging of events occurring in the console.
- View events, filter by event type, category and module, and export events.
- Configure event logging settings based on severity levels, with the ability to send specific levels to external systems via syslog integration.
- Generate reports to track data over set time periods.

User Administration

How does Workspace ONE UEM manage role-based user administration for tiered roles?

Built-in and custom roles define the device groups that an IT administrator can access and manage, and restrict the depth of device management information and features available to each console user. For example, grant limited access within the console to help desk administrators and grant a greater range of permissions to the IT manager.

If the existing default roles are not suitable for your organization, use custom roles which allow you to customize as many unique roles as required. Choose from over 1,000 unique security permissions to define custom roles. You can set permissions to view (read-only), write, or update the system.

You have flexibility to authenticate console users with basic, directory services, or SAML credentials and configure Workspace ONE to enable/disable SAML authentication for administrators according to organization group membership.

Users can have multiple assigned roles and you can auto-assign roles to individual console users or groups with AD/LDAP integration.

How does Workspace ONE Access manage role-based user administration?

Workspace ONE Access has three predefined roles for role-based access control:

- The *super administrator* role can access and manage all features and functions in the Workspace ONE Access services.
- The *read-only administrator* role can view the details in the Workspace ONE Access console pages, including the dashboard and the reports, but cannot make changes. All administrator roles are automatically assigned the read-only role.
- The *directory administrator* role can manage users, groups, and directories. The directory administrator can manage directory integration for both enterprise directories and local directories within your organization. The directory administrator can also manage local users and groups.

You cannot modify or delete the predefined roles but you can create custom administrator roles that give limited permissions to specific services in the Workspace ONE Access console.

For more Workspace ONE Access FAQs, see [Workspace ONE Access Frequently Asked Questions \(FAQs\)](#).

How does Workspace ONE Intelligence managed role-based user administration?

Role-based access control (RBAC) has predefined roles that you can assign to admins for access to the resources they use. Assign a single role or combine roles for those admins who require permissions to your entire environment.

Workspace ONE Intelligence can get user data from Workspace ONE UEM. RBAC supports adding admins from Workspace ONE UEM from both the basic users and the directory-based users.

- *Basic users* are individual accounts that are not managed through an identity service. They require no enterprise infrastructure. These credentials exist only in Workspace ONE UEM and have no federated security.
- *Directory-based users* are managed in an identity service and are pulled into Workspace ONE UEM. These users access resources with their directory credentials and any changes made to their accounts sync with Workspace ONE UEM.

Windows Devices Lifecycle Management

How do I provision a Windows laptop for a new hire?

Workspace ONE UEM supports a variety of onboarding workflows that address multiple use cases. The onboarding method impacts other configuration decisions, and therefore is an important starting point when planning a Workspace ONE UEM deployment. To learn about the available onboarding options for Windows devices and evaluate which option is best for your organization, refer to the Onboarding section of [Desktop Lifecycle Management](#)

What is Agent-Based Enrollment?

The agent-based enrollment method uses Workspace ONE Intelligent Hub. The primary use case for agent-based enrollment is existing company-owned or BYOD devices that the end user self-onboards. The workflow is similar to the standard onboarding workflows for iOS and Android devices.

What is Microsoft Azure Active Directory Enrollment?

Workspace ONE UEM integrates with Azure AD, providing a robust selection of onboarding workflows that apply to a wide range of Windows devices use cases. However, Azure licensing requirements stipulate that you must purchase an additional Azure AD Premium license to complete this integration.

- Enterprises that are leveraging Azure AD typically use one of the following onboarding options for corporate-owned devices:
 - Enrolling using Out-of-Box-Experience
 - Enrolling using Azure AD Join
 - Enrolling with Windows AutoPilot
- For personal-owned (BYOD) devices:
 - Enrolling using Azure Connect

For details:

- See [Enrolling Windows Devices Using Azure AD: Workspace ONE Operational Tutorial](#).

What is Command-Line Enrollment?

Command line enrollment can be initiated for devices that you may want to migrate over to being managed by workspace ONE From another management tool. Command line enrollment is an automated method to onboard devices silently without user intersection, over to Workspace ONE. This method of onboarding uses the command-line parameters supported with the Workspace ONE Intelligent Hub.

Organizations using command-line enrollment typically use one of the following onboarding options:

- Enrolling domain-joined devices.
- Enrolling Workgroup devices.
- Enrolling using a Group Policy logon script.

or more details:

- See [Enrolling Windows Devices Using Command-Line: Workspace ONE UEM Operational Tutorial](#).

What is Drop Ship Provisioning?

Drop Ship Provisioning for Workspace ONE allows Windows Device OEM administrators to provide a virtually zero IT touch and virtually zero user downtime experience. Configurations, settings, and applications are preloaded at the factory. Now, 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. And if you need to perform a PC reset or recovery in the future, Zero Touch Restore functionality allows applications and management to persist, which minimizes downtime.

Drop Provisioning supports the following Workspace ONE onboarding methods:

- Azure AD Joining with Premium licenses.

- Azure AD Joining without Premium licenses.
- On-premises Domain Joining.
- Hybrid Domain Join with Azure.
- Workgroup.

For more details, see the [Drop Ship Provisioning: Workspace ONE Operational Tutorial](#).

What is your approach to building and maintaining images?

Windows modern management introduces a new management style that differs significantly from traditional management tools. With traditional management, admins would image devices and ensure these images updated with every Windows release. With modern management, all of the same configurations are delivered over the air after enrollment. Therefore, admins manage all configurations from the cloud, and when new devices are enrolled, the latest applications, configurations, policies, and personalization are all layered onto the device dynamically.

Workspace ONE UEM allows admins to manage OS updates and patches and applications updates from the cloud. Administrators can leverage Drop Ship Provisioning to have apps pre-loaded in the factory to reduce the need for applications to be installed over-the-air and have employees ready to work with applications pre-installed.

How does Workspace ONE UEM support asset management?

To manage assets, use Workspace ONE Intelligence reports with starter templates or customize pre-canned reports. You can select from categories that include Applications, Devices, Devices Risk Score, Device Sensors data, Profiles, Users, Vulnerabilities, and OS Updates. These reports provide the latest data extracted from your Workspace ONE UEM environment.

Workspace ONE UEM Collects data from the Windows device on a schedule, based on OMA-DM (Native MDM) queries, using Workspace ONE Sensors, and any additional data collected from the Intelligent Hub for Windows. Other data, such as application crash logs and telemetry, can be collected as part of Workspace ONE Intelligence Digital Employee Experience Management.

Workspace ONE Intelligence can filter data, to create the report on specific areas of your Workspace ONE UEM deployment. These filters use a specific logic to determine what information to include in the report, dashboard, or automation. They also represent the data the system collects.

Does Workspace ONE support administrator role-based access control for functions such as BitLocker key recovery, app distribution, and remote commands?

Yes. The Workspace ONE UEM admin portal uses role-based access controls (RBAC) to show admins only the preapproved devices/users/information. For example, help desk administrators within your enterprise might have limited access within the console, while the IT Manager has a greater range of permissions.

- This can include whether or not an admin has the right to Access the BitLocker recovery key, app distribution, and performing specific remote commands such as device wipe or enterprise wipe.
- The solution enables secure access to the Workspace ONE UEM console with a single access control layer for enabling and configuring access.

RBAC is supported in all Workspace ONE Services. Workspace ONE UEM, Workspace ONE Access and Workspace ONE Intelligence.

How can I deprovision a laptop - are there limitations to consider?

Workspace ONE UEM streamlines laptop deprovisioning by allowing for remote wipe of corporate data and access to corporate resources from a single console.

Devices need only an internet connection for a remote (enterprise) wipe. Devices do not require a connection to the internal corporate network. Wipe commands that can be performed are as follows:

- *Enterprise Wipe* removes all corporate data from the selected device and removes the device from Workspace ONE. All of the enterprise data contained on the device is removed, including MDM profiles, policies, and internal applications. The device will return to the state it was in prior to the installation of Workspace ONE. The user's personal data/content, however, is preserved on the device.
- *Device Wipe* removes all data from the selected device, including email, profiles, all data that is present, and mobile device management (MDM) capabilities. This action returns the device to factory default settings (including the

user's personal data/content as well as corporate data).

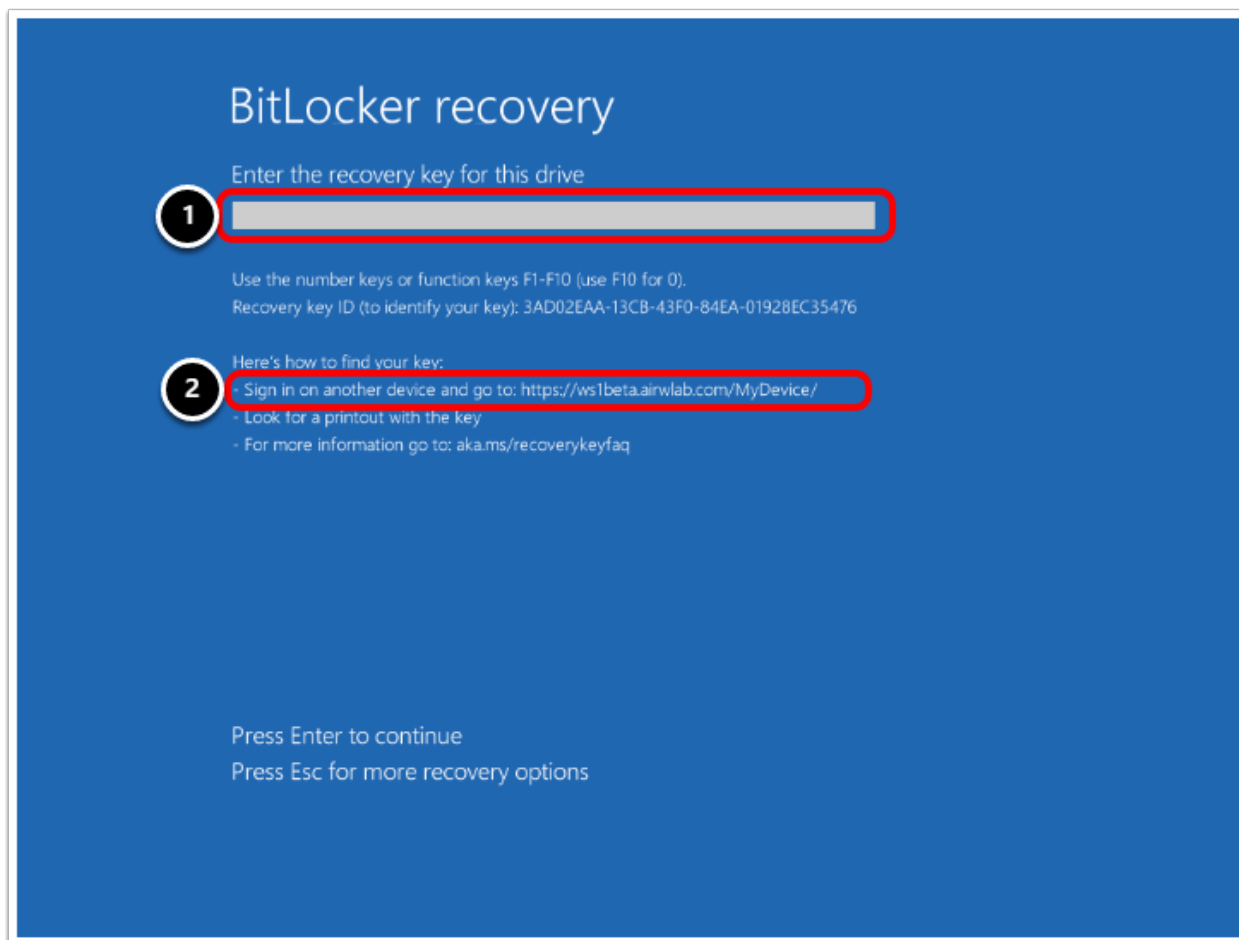
- *Enterprise Reset* - Enterprise Reset restores a device to a ready-to-work state when a device is corrupted or has malfunctioning applications. It re-installs the Windows OS while preserving user data, user accounts and managed applications. The device will re-sync auto-deployed enterprise settings, policies, and apps after the reset while remaining managed by Workspace ONE.

Windows Devices Endpoint Security

Can the end user perform encryption key recovery (for example, BitLocker)?

Workspace ONE UEM leverages role-based access controls (RBAC) for admins, allowing you to grant access to view recovery keys to the admins who require access.

End users can log into the self-service portal for BitLocker recovery key retrieval. You can turn off this feature using RBAC for the self-service portal controls. When using BitLocker encryption with Workspace ONE, the configure the self-service URL when Windows boots into BitLocker recovery.



How does Workspace ONE take advantage of Windows modern management?

Workspace ONE combines complete cloud-native, Windows modern management with intelligent automation to empower users, harden security, and simplify IT.

Workspace ONE leverages the EMM-based design of Windows to enable a mobility-centered strategy for Windows modern management. Our solution works alongside built-in Windows tools to streamline device lifecycle, app delivery, and end-to-end security for comprehensive device management.

With Workspace ONE, you can:

- Leverage modern EMM management efficiencies, while fully supporting traditional configuration policies such as group policies for end-to-end security.
 - Integrate with Microsoft Passport for Work and Windows Hello to enable multi-factor authentication for user verification, including biometric gestures.
 - Use the Workspace ONE compliance engine to deliver real-time visibility into device's health, encryption status, and image integrity through Windows Health Attestation.
- Deliver a broad range of apps to Windows devices, including SaaS, web, native, internal, and legacy Win32 through

intuitive app licensing and management tools.

- Support auto provisioning workflows and multiple software distribution methods including remote installation of apps, drivers, firmware updates, and other custom scripts.

For more information, see [Modernize Desktop Management](#) and [Modernize Mobile Management](#).

How does Workspace ONE support Windows devices that are not domain joined and/or corporate-owned?

If the Windows device is managed by another management tool or the device is not owned by the organisation, users have two options:

- Contractor Use Case - Access Workspace ONE via the web. This means that on the contractor use-case, the device can still be managed by another system, but the end user can access resources and single sign-on into web applications, virtual applications, and virtual desktops.
- Enroll in BYOD – If the device is personally-owned, the user can download and install the Intelligent Hub for Windows by visiting getwsone.com and enroll. Workspace ONE has robust privacy controls, to ensure that personal data remains on the device when offboarding, and any policies or applications can be applied to BYOD or corporate-owned devices.

How does Workspace ONE enforce conditional access to apps and resources based on factors such as endpoint health and network?

Workspace ONE UEM offers an industry-leading endpoint management solution and serves as the source of truth for device telemetry. Workspace ONE UEM allows administrators to define a 'compliant' state of a device and evaluate compliance based on one of the most robust set of data points in the industry. Workspace ONE Access can utilize this telemetry from Workspace ONE UEM to aggregate device, app, and user behavior data from multiple internal and external sources. Workspace ONE Intelligence leverages machine learning models to calculate a user risk score and enable conditional access based on device context, login risk, and user behavior.

How consistent is Workspace ONE device health monitoring, alerting, and remediation capability across endpoints on and off the corporate network?

Workspace ONE is cloud-native and allows real-time configuration across all policies – from silicon to software - With over-the-air BIOS and firmware configuration and 100% Windows GPOs with Workspace ONE Baselines. Devices need an internet connection to the Workspace ONE UEM server and can be fully managed on the internal network or outside of the internal corporate network.

Application and Patch Management

Does Workspace ONE UEM support Windows baselines?

Yes. You can create Windows baselines within the Workspace ONE UEM console by creating a Baseline Profile. Workspace ONE Baselines apply policies to devices that are domain-joined, Azure-joined, or workgroup devices. Workspace ONE Baselines remove the complexity of managing policies from a domain controller and deliver them from the cloud! Workspace ONE Baselines Support for Microsoft Security Baselines, CIS Benchmarks for Windows 10 and 11 devices.

Workspace ONE Baselines enables admins to:

- Deploy template or customize policies in seconds
- Manage MDM profile configurations and traditional Group Policy Objects (GPOs) in a single console.
- Customise and edit policies that match your AD GPOs or create new ones based on your business needs.
- Remove the need for third-party compliance tools. View and manage the policy compliance of your device fleet over the air in the Workspace ONE admin console.
- No need to force policies to apply with gpupdate /force
- No VPN is required to apply policies to remote workers

For details:

- See [Understanding Windows Group Policies](#)

What Windows file types can be distributed through Workspace ONE UEM?

Workspace ONE UEM supports applications delivery of MSI, MSIX, EXE and ZIP packages to devices. With Workspace ONE Scripts and Sensors, PowerShell scripts can query attributes on the device or to run a script.

Can Workspace ONE UEM manage both device security and application access?

Yes. For applications, the Workspace ONE Intelligent Hub delivers unified notifications, application install statuses, and a complete unified application catalog experience across Web, Windows, macOS, iPhone and iPad, and Android platforms for all your users. Workspace ONE can also enforce an application allowlist and denylist for all platforms.

Workspace ONE Intelligence with Carbon Black provides a modern, cloud-based enterprise security approach to secure users and endpoints. To manage risks related to modern-day cyber threats, Workspace ONE Intelligence with Carbon Black combines insights from Workspace ONE, an intelligence-driven digital workspace platform, with Carbon Black to deliver predictive and automated security in the digital workspace. Existing security tools provide IT with only limited visibility, focusing only on silos of security that provide legacy functionality. This results in a band-aid approach that impacts organizations with high-costs due to complexity and manual tasks involved in trying to secure a digital workspace.

Fortifying Intelligence, Carbon Black provides:

- Single Agent, Cloud Platform
- Streaming Prevention with Minimal False Positives
- Complete Endpoint Visibility
- Improved Efficiency Between Security & IT Ops

For more information, see [Integrating Workspace ONE Intelligence and Carbon Black](#).

Does the end user have flexibility to manage Windows OS updates to avoid user and device disruption?

Windows Updates allows for flexible end-user update capabilities. You can:

- Manage Windows Patches, on or off the network
- Force the install of updates but allow the user to schedule them.
- Enforce Active Hours to not disrupt the end user or force a reboot during work (active) hours.
- Check for updates but allow user to choose whether to download and install them.

For details, see [Managing Updates for Windows Devices: Workspace ONE Operational Tutorial](#).

How does Workspace ONE UEM support deploying Windows patches over a large device fleet?

Create a Windows Update profile to apply automatic or on-demand updates to groups of devices.

The Windows Updates console page lists all updates available for Windows devices. From this screen, you can see the patch status for an individual device, or a specific Windows patch itself.

Workspace ONE UEM uses Windows Update for Business and the Windows Update services to grab and apply updates.

Workspace ONE UEM takes a modern, cloud-native approach to manage Windows patches. Windows Update Management using Workspace ONE delivers updates on a frequent and dynamic basis. This ensures end users always have access to up-to-date operating system features.

Does Workspace ONE UEM support both CDN (cloud distribution networks) and peer-to-peer methods for Windows app distribution?

Yes, Workspace ONE UEM supports both CDN and peer-to-peer methods for Windows devices.

Workspace ONE UEM SaaS environments are integrated with Akamai's CDN network; on-premises customers can take advantage of this functionality by obtaining Akamai's CDN capabilities.

Workspace ONE Peer Distribution uses the native Windows BranchCache feature that is built into the Windows operating system. Workspace ONE UEM also partners with Adaptiva to offer an alternative peer distribution system.

Configuration Management

How does Workspace ONE UEM set and manage configuration policies on Windows devices?

When moving to modern management for Windows it's important to understand what policy is being delivered to whom and what ownership that user has. PCLM tools did not cater to BYOD devices.

Workspace ONE UEM combines the best of traditional management (PCLM) and EMM(MDM) toolsets to provide configuration policies for Windows devices. Workspace ONE can separate policies by ownership of the device, meaning when a device is unenrolled, user data stays intact.

Policies are delivered in two ways:

- Workspace ONE UEM baselines – Using either the Microsoft Windows Security Baselines or CIS Microsoft Windows Desktop Benchmark.
- MDM policies or configuration service providers (CSPs) – This mechanism is natively built into the operating system and applied through the existing Windows profiles or using a custom settings profile.

For details, continue to [What is a Workspace ONE UEM baseline?](#) and [What is a configuration service provider \(CSP\)?](#)

What is a Workspace ONE UEM baseline?

Workspace ONE baselines for Windows allow you to keep your devices secure and aligned with industry standards, such as CIS Benchmarks and the Windows security baselines. With Workspace ONE baselines, you set your preferred configuration over the air, including adding any additional policies, and your devices maintain these settings.

Following are some benefits of using baselines (with templates):

- Uses an industry validated template by CIS or Microsoft.
- Settings enforced at a reapplication interval.
- Baseline compliance is reported in the console.
- Settings are removed from the device when the baseline is unassigned.

What is a configuration service provider (CSP)?

A CSP is an interface to read, set, modify, or delete configuration settings on the device. These settings map to registry keys or files. Most of the CSPs support SyncML for over-the-air configuration of the device.

Workspace ONE UEM leverages CSPs when an administrator creates and assigned profiles in the console. In most cases, the OMA-DM client is responsible for delivering the CSP setting to the devices.

Workspace ONE UEM administrators can create CSPs using Profiles that are listed in the Workspace ONE UEM console.

Following are some benefits of using MDM policies, or CSPs:

- Uses Modern policies that are built for the cloud-native architecture.
- Uses the OMA-DM communication channel.
- New features/settings are likely to be implemented as CSPs rather than more legacy policy methods.
- Settings are removed from the device when the profile is deleted.
- Console-implemented CSPs are easy for an admin to visualize and edit.

For more information, see [Understanding Windows Group Policies: Workspace ONE Operational Tutorial](#).

Do Windows machines have to be joined to an on-premises domain to receive policy updates?

Traditional PC lifecycle management tools require Windows devices to be joined to the domain located on-premises for these policies and security settings to apply. If users are working remotely, typically, device-based VPNs are used to gain line of sight to the domain controller to update these Group Policy settings.

With Workspace ONE Baselines, Windows devices can be a member of a domain, Workgroup, or even pure Azure AD joined, removing the complex requirements for PCLM tools.

The benefits:

- No gpupdate /force
- No VPN required
- Query results over the air

With modern management, all devices need is an internet connection to check back in with the Workspace ONE UEM server. Compliance policies can be set to ensure devices check in at defined intervals. When the device doesn't check back in at defined intervals, then remediation steps can be taken.

Does Workspace ONE UEM apply different GPOs based on user profiles?

Workspace ONE UEM assignment groups is an umbrella term used to categorize certain management grouping structures within Workspace ONE UEM. Organization groups, smart groups, and user groups each have full feature sets and are distinct from each other.

One feature these groups have in common is the way they can be used to assign content to user devices easily. Assignment Groups enables an administrator to manage these three grouping structures from a single location.

For more details on these groups, see the Device Management section of this document.

Platform and Application Support

What platforms, and application types does Workspace ONE UEM support?

The following table depicts app types and supported OS platforms.

Application Type	Android	Chrome OS	macOS	iOS	tvOS	Windows Desktop
Internal applications	☐		☐	☐	☐	☐
Public applications (free and user paid)	☐	☐		☐		☐
Volume Purchased applications (VPP)			☐	☐	☐	
Custom Apps (Store-Based B2B)				☐		
Web links	☐		☐	☐		☐
SaaS apps with federated authentication	☐	☐	☐	☐		☐

Technical Support

What are the available support offerings for Workspace ONE?

- Our Support Services Team offers technical assistance to IT administrators for the solution
 - Our support team can be contacted via web or phone with response targets based upon incident severity
 - We provide support including a managed knowledge base, customer forum community, phone support, screen sharing and onsite services
 - With support centers around the world, we can offer 24/7/365 access for SaaS severity 1 issues
- All Support Services levels include access to our Customer Connect online community and unlimited online support requests

	Basic Support	Production Support
Designed for:	Non-critical applications and platforms that require support during normal business hours	Customers who have complex environments or advanced support needs
Coverage:	24/7/365 coverage for SaaS Severity 1 incidents 10/5 coverage for all incidents	24/7/365 coverage for SaaS Severity 1 incidents 10/5 coverage for all other incidents
Support requests:	Unlimited online, and phone requests	Unlimited online, and phone requests
Customer contacts:	4 designated customer contacts	6 designated customer contacts
Point of contact:	Account Services Team	Account Services Team

Summary

This document provided answers to the most popular Workspace ONE FAQs. Topics ranged from getting started to configuration, user administration, device management, application and patch management, and more.

Changelog

The following updates were made to this guide:

Date	Description of Changes
2024/09/17	
2024/01/25	
2023/10/24	
2022/06/16	
2021/07/09	
2021/04/15	
2021/02/01	

About the Author and Contributors

This document was created by:

- [Gina Daly](#), Technical Marketing Manager, Omnisia.

With significant contributions from:

- [Andreano Lanusse](#), Staff Architect, Omnisia.
- Alicia Restrepo, Senior Content Strategist, Omnisia.
- Darren Weatherly, alumni.
- Josué Negrón, alumni.

Feedback

Your feedback is valuable. To comment on this paper, either use the feedback button or contact us at tech_content_feedback@omnissa.com.

