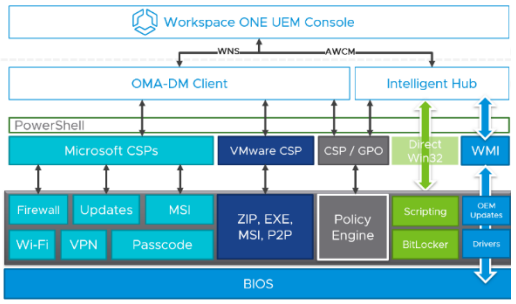
TROUBLESHOOTING WINDOWS 10 CHEAT SHEET

Use this checklist & troubleshooting tips as a reference for the next time you troubleshoot issues on Windows 10 using Workspace ONE UEM. For next steps, you can reach out to VMware or Microsoft Support. Be sure to send logs: use Remote Log Collection within Workspace ONE or generate the MDM Advanced Diagnostic Report.



Learn the fundamentals of managing Windows 10 with Workspace ONE UEM at https://techzone.vmware.com/understanding-windows-10-management

UNDERSTANDING THE BASICS

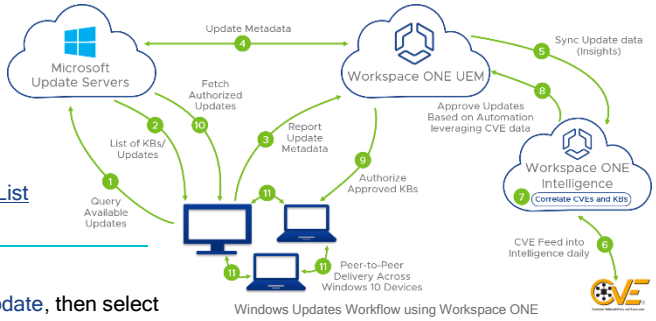
Clients	Uses
OMA-DM	Native MDM client built into the device. Used for device communication, enrollment, profile configuration Microsoft CSPs, software distribution metadata delivery, and VMware CSPs. Communicates using WNS.
Workspace ONE Intelligent Hub	Used for local enforcement, profiles, telemetry, Sensors, Baselines, unified app catalog, Hub Services, and Product Provisioning. Communicates using AWCM.
Software Distribution Client (SFD)	Used to install Win32 apps.
VMware Digital Experience Telemetry Client	Provides insights about apps, operating system stability, and performance.
Workspace ONE Assist Client	Allows for remote control, file management, and executing remote shell commands using Remote Assist.

Services	Description	Hostnames & Ports
Windows Notification Service (WNS)	Provides real-time communication for the built-in OMA-DM client.	*.wns.windows.com over 80/443 (IP List - http://bit.ly/W10WNS)
AirWatch Cloud Messaging (AWCM)	Provides real-time communication for the Workspace ONE Intelligent Hub.	awcm###.awmdm.com:443 (SaaS) and 2001 (On-Premises)
Content Distribution Network (CDN)	Used when downloading apps from Workspace ONE UEM.	CDN*.awmdm.com:443
Device Health Attestation	Cloud service used for determining device posture, can also be hosted on-premises.	has.spserv.microsoft.com:443
Business Store Portal	Access to apps from the Business Store Portal, also used if pushing online BSP apps.	bspmts.mp.microsoft.com:443
Azure AD Authentication	Used when leveraging Azure AD for any authentication, including enrollment.	login.microsoftonline.com:443
Windows Updates	Endpoints used for Windows Update downloads of apps and OS updates.	*.mp.microsoft.com over 80/443

For all networking requirements, visit http://bit.ly/W10Endpoints & https://ports.vmware.com.

DEPLOYING PROFILES

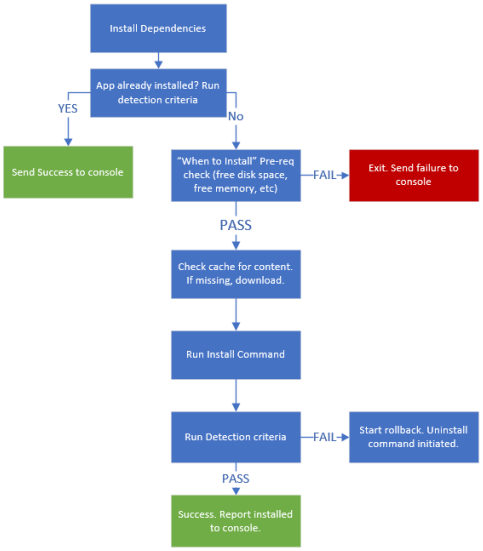
- ☐ Check Event Viewer logs for failure message (404): App and Service Logs > Microsoft > Windows > DeviceManagement-Enterprise-Diagnostics-Provider > Admin.
- ☐ Confirm that the correct action is used - Add/Replace/Delete/Exec.
- ☐ For Custom Settings: http://bit.ly/CustomSettingsProfile
  - Check that XML is in between CDATA tags.
  - Confirm that the correct data format is sent.
- ☐ Confirm setting is supported on the W10 edition/version being used: aka.ms/CSPList
- ☐ In Fiddler, check error codes: http://bit.ly/SyncMLCodes



Windows Updates Workflow using Workspace ONE

WINDOWS UPDATES

- ☐ Navigate to Windows Settings > Update & Security > Troubleshoot > Windows Update, then select Run the Troubleshooter.
- ☐ Verify that you see Update under Windows Settings > Accounts > Access Work or School, then selecting on our enrollment account, then selecting Info. Ensure you see Update under Areas managed by Workspace ONE, then under Policies.
- ☐ Using Regedit, navigate to and validate all of the configured update values are set correctly: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\current\device\Update
- ☐ Use Event Viewer to obtain more information about errors: Microsoft-Windows-WindowsUpdateClient/Operational.
- ☐ The following PowerShell cmdlets are helpful:
  - The Get-Hotfix cmdlet retrieves hotfixes (also called updates) that have been installed; the cmdlet also retrieves hotfixes or updates that have been installed manually by users.
  - The Get-WindowsUpdateLog cmdlet merges and converts Windows Update event trace log (ETL) files into a single, readable WindowsUpdate.log file.



SOFTWARE DISTRIBUTION

- ☐ Check installation status of Software Distribution client: 70 is ✓ but 30,60,120 is ✗ HKLM\SOFTWARE\Microsoft\EnterpriseDesktopAppManagement\MSI
- ☐ Review the registries under HKEY_LOCAL_MACHINE > SOFTWARE > AirWatchMDM > AppDeploymentAgent.
- ☐ Check the Queue path and the S-1-5-18/S-1-X-X path for any processes. Then, check the LastDeploymentLog and LastStatusCode for more details.
- ☐ Scripts are supported for Install, Uninstall, and Detection. The following lists examples for each type:
  - **PowerShell**: PowerShell -ExecutionPolicy Bypass -File file.ps1
  - **VBScript**: cmd /C file.vbs • **JScript**: cmd /C file.js
- ☐ BranchCache Status (P2P) run bcstatus from PowerShell, then run perfmon, add BranchCache counters, view data using the Report View.

CONSOLE SETTINGS & ENROLLMENT

- ☐ Check Device Root Certificate is generated and is of type PFX NOT CER in System > Advanced > Device Root Certificate.
- ☐ Confirm that the Hub app is published Devices & Users > Windows > Windows Desktop > Intelligent Hub Application.
- ☐ Staging workflows (command-line, PPKG, etc.) where the device is auto-reassigned to the end-user need to have "Fixed Organization Group" or "User Group Organization Group" set at Devices & Users > General > Shared Devices.
- ☐ For Azure-based enrollment, ensure Immutable ID Mapping Attribute is correctly set. Most commonly objectGUID or mS-DS-ConsistencyGuid. Ensure that Binary is used for objectGUID and String for any non-GUID value.

ENROLLMENT FLOWS

- ☐ Admin staging (staged enrollment to admin account, log out/login to domain user): msiexec /i AirwatchAgent.msi /quiet ENROLL=Y SERVER=[server] LGNAME=[og id] USERNAME=[staging username] PASSWORD=[password] Refer to http://bit.ly/HubCLI
- ☐ Brownfield domain joined (in domain user profile): msiexec /i AirwatchAgent.msi /quiet ENROLL=Y SERVER=[server] LGNAME=[og id] USERNAME=[staging username] PASSWORD=[password] ASSIGNTOLOGGEDINUSER=Y Refer to http://bit.ly/HubCLI
- ☐ Azure AD Premium: Enable Azure AD integration. Settings > System > Enterprise Integration > Directory Services > Azure AD Integration and Use Azure AD For Identity Services set to Enabled. Refer to http://bit.ly/AzureADEnroll

Important Event Viewer Log Locations

For a complete list of Windows Error Codes visit http://bit.ly/W10Errors

OMA-DM Communication

Collects every interaction between the device and Workspace ONE UEM

Event Viewer (Local) > Applications and Services > Microsoft > Windows > DeviceManagement-Enterprise-Diagnostics-Provider > Admin

Enterprise Data Protection (EDP) - Windows Information Protection (WIP)

Collects logs related to WIP and Audits

Event Viewer (Local) > Applications and Services > Microsoft > Windows > EDP *

AAD & User Device Registration

Collects all information related to Azure Active Directory and joining via AAD

Event Viewer (Local) > Applications and Services > Microsoft > Windows > AAD > Operational section

Event Viewer (Local) > Applications and Services > Microsoft > Windows > User Device Registration > Admin section

BitLocker

Collects BitLocker information, or use the `manage-bde -Status C:` command first

Event Viewer (Local) > Applications and Services > Microsoft > Windows > BitLocker-API and BitLocker-DrivePreparationTool

Important Device Registry Keys

All MDM Profiles/Apps Pushed to Device

Lists all the profiles (not values) pushed to the device, including applications. These are broken down by device/user profiles identified by user's SID.

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EnterpriseResourceManager\Tracked`

MDM Profiles and Values

Lists the device profiles default and updated values. These are broken down by device profiles and user profiles identified by user's SID.

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\current\device`

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\providers\{EnrollmentGUID}\default\Device`

MSI/Desktop Apps*

Status of Workspace ONE Intelligent Hub, Software Distribution Client (used for installing Win32 apps) and all MSI app installations before SFD is enabled.

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EnterpriseDesktopAppManagement`

Software Distribution Apps*

Status of app installations along with additional information.

`HKEY_LOCAL_MACHINE\SOFTWARE\AirWatchMDM\AppDeploymentAgent`

*The following folders are useful when troubleshooting apps:

AppManifests – Contain information about all of the settings selected in the console.

ContentManifests – Contain where the device can download the software, such as Device Services URL, CDN URL, and P2P Content ID.

Queue/S-1-5-X – Logs where S-1-5-18 contains apps pushed to the device and S-1-5-21-X contains apps pushed to the user.

Logging Directories

Workspace ONE Intelligent Hub

`%ProgramData%\AirWatch\UnifiedAgent\Logs`

AwclClient.log – Log contains communications between AWCM client and Workspace ONE UEM.

AWProcessCommands.log – Logs containing info regarding commands sent from Device Services to the Workspace ONE Intelligent Hub such as encryption/BitLocker, Baselines, Product Provisioning, etc.

AwAirWatchIpc.log – Contains user context process communications along with the status of all actions performed. For example, installing the Workspace ONE Intelligent Hub UI component, Toast Notifications, getting INet proxy, etc.

ComExecution.log – Log contains details regarding user engaged restart for app deployments.

DeviceEnrollment.log – After native OMA-DM enrollment, these logs capture additional enrollment steps performed by Workspace ONE Intelligent Hub.

HubStatus.html – Created after right clicking on the Workspace ONE Intelligent Hub and selecting Troubleshoot -> Hub Status. Contains details around required Services and enrollment details.

InstallerLog_HHMMSS_DDMMYYYY.log – Installer logs will be created for each action performed by the Workspace ONE Intelligent Hub Installer: upgrade, install, uninstall and repair.

NativeEnrollment.log – Log contains details about the native OMA-DM enrollment completed by the Workspace ONE Intelligent Hub based enrollments.

PowershellExecutor.log – Details of the PowerShell commands executed through product provisioning and Sensors.

TaskScheduler.log – Log contains details regarding Workspace ONE Intelligent Hub task scheduler such as Hub re-starts, device re-assignments, enrollment request/response, etc.

JobLogs\ProductProvisioningJobName_###.log – Contains either a success message (Jobs executed successfully) or more details regarding why your files/actions (Product Provisioning) script failed to process successfully. Each Product (Files/Actions) will contain a new log file, furthermore, each new attempt at re-pushing a Product will create a new log file. The standard naming format is Product Name followed by Job Number.

Recovery\RecoveryService.log – Provides details on the status of the Workspace ONE Intelligent Hub auto recovery functionality. This can be trigger by an admin in the Workspace ONE UEM console, by preforming the Repair Hub action, under More Actions.

`%appdata%\..\Local\Packages\AirWatchLLC.WorkspaceONEIntelligentHub_htcwkw4rx2gx4\LocalState\logs`

IntelligentHubLogsYYYY-MM-DD.log – This log contains details about the Workspace ONE Intelligent Hub UI component's operations. For example, enrollment request/response and Hub Services related details such as branding, entitlements, and other details.

Software Distribution Cache (requires admin elevation)	Baselines	Telemetry Client
`%ProgramData%\AirWatchMDM\AppDeploymentCache`	`C:\Program Files (x86)\Airwatch\AgentUI\BaselinesBackup`	`%programdata%\VMWOSQEXT\logger`

Workspace ONE AirLift

`%PROGRAMDATA%\VMware\VMware Airlift\logs`

AirLift-<current_date>.txt: AirLift Windows Service logs

AirLift-Tool-<current_date>.txt: AirLift Command Line Tool logs

AirLift Setup Logs: `%LOCALAPPDATA%\Temp`

Drop-Ship (Factory) Provisioning

`%SYSTEMDRIVE%\Temp\PpkgInstaller\PpkgInstallerLog.txt` – Log contains details from applying the PPKG onto the system.

`%ProgramData%\AirWatch\UnifiedAgent\Logs\PPKGFinalSummary.log` – Log contains details from VMware Workspace ONE Provisioning Tool.

Enterprise Reset

`C:\Recovery\OEM`

AWRefreshUnattend.xml: Unattend XML which executes RefreshRunOnce.cmd, deletes itself from Panther folder.

RefreshRunOnce.cmd: Completes the Workspace ONE Intelligent Hub command-line enrollment.

ResetConfig.xml: XML file which specifies what happens when a PC Reset is invoked; invokes VMwareRefreshBackup.cmd and then VMwareRefreshRecover.cmd to back up old PC and recover to new PC before resetting the device.

VMwareRefreshBackup.cmd: Backs up all enrollment data to C:\Recovery\OEM\VMware, Windows Refresh migrates C:\Recovery\OEM folder from old to new PC.

VMwareRefreshRecover.cmd: Restores all the backed-up data from old to new PC; copies AWRefreshUnattend.xml in the Panther folder as unattend.xml.

`C:\Recovery\OEM\VMware`

Contains logs and application data with the app deployment cache, Hub database with all configurations and settings, and registry settings with MDM device ID used to ensure the device checks in with the right console side record.

Go from zero to hero with the latest technical resources on the **VMware Digital Workspace Tech Zone @ techzone.vmware.com**!

Get the latest Windows 10 Troubleshooting Tutorial on Tech Zone @ http://bit.ly/W10Troubleshoot