

Troubleshooting Windows 10 Deployments

in Workspace ONE UEM

Darren Weatherly (he/him)
Sr. Technical Marketing Architect, VMware

Josue Negrón (he/him)
EUC Staff Architect, VMware

SESSION ID EUS2638

#vmworld #EUS2638



A graphic for vmworld 2021 set against a dark blue, textured background resembling a night sky or galaxy. The text "vmworld" is in a white, lowercase, sans-serif font with a registered trademark symbol (®) to the upper right. Below it, "2021" is in a larger, white, sans-serif font. The graphic is decorated with white, glowing orbital lines and small, glowing satellite-like icons.

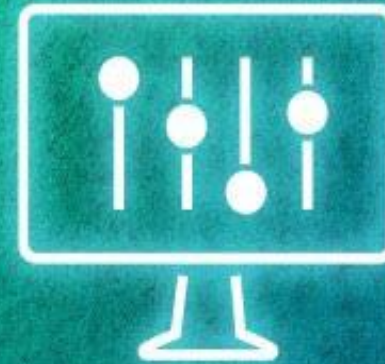
Darren Weatherly

Senior Solutions Architect, VMware
@CtrlAltDarren



Josue Negrón

Staff Solutions Architect, VMware
@josuejnegrón



Agenda

Solution Overview

Collecting System Information

Troubleshooting

Application Deployments

Windows MDM Policies and Baselines

Windows Updates

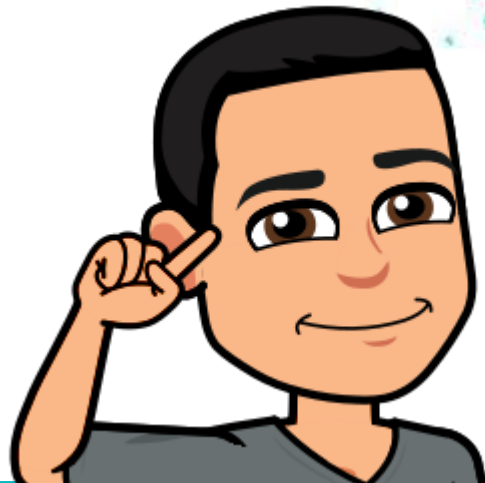
Enrollment and Onboarding

Workspace ONE Assist

DEEM/Intelligence

Troubleshooting Cheat sheet

Windows Modern Management Solution Overview



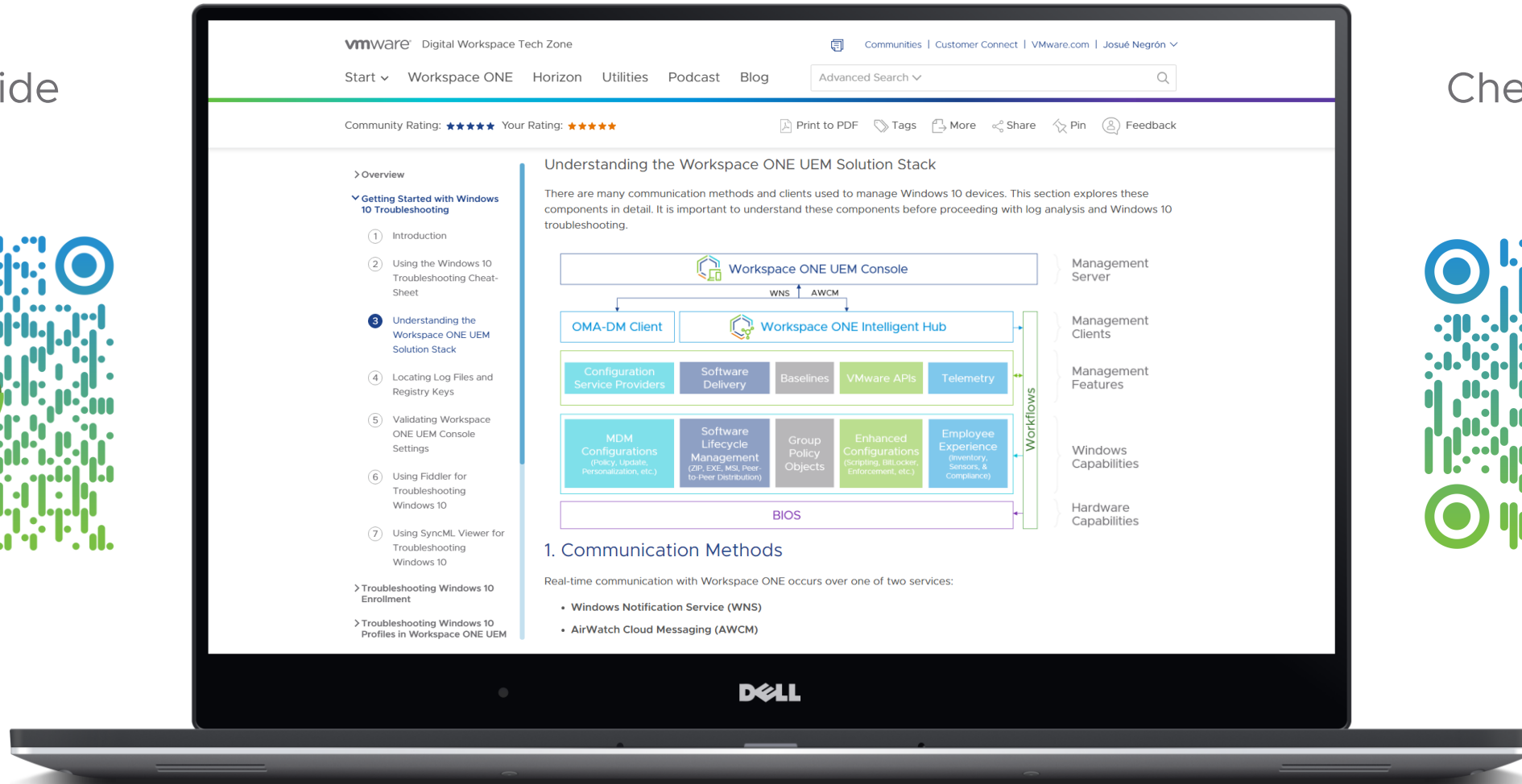
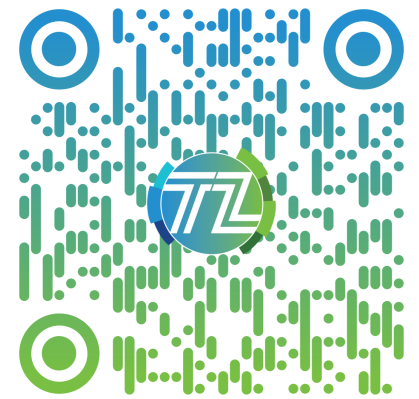
Windows 10 Troubleshooting Operational Tutorial

<https://via.vmware.com/W10Troubleshooting>

Full Guide



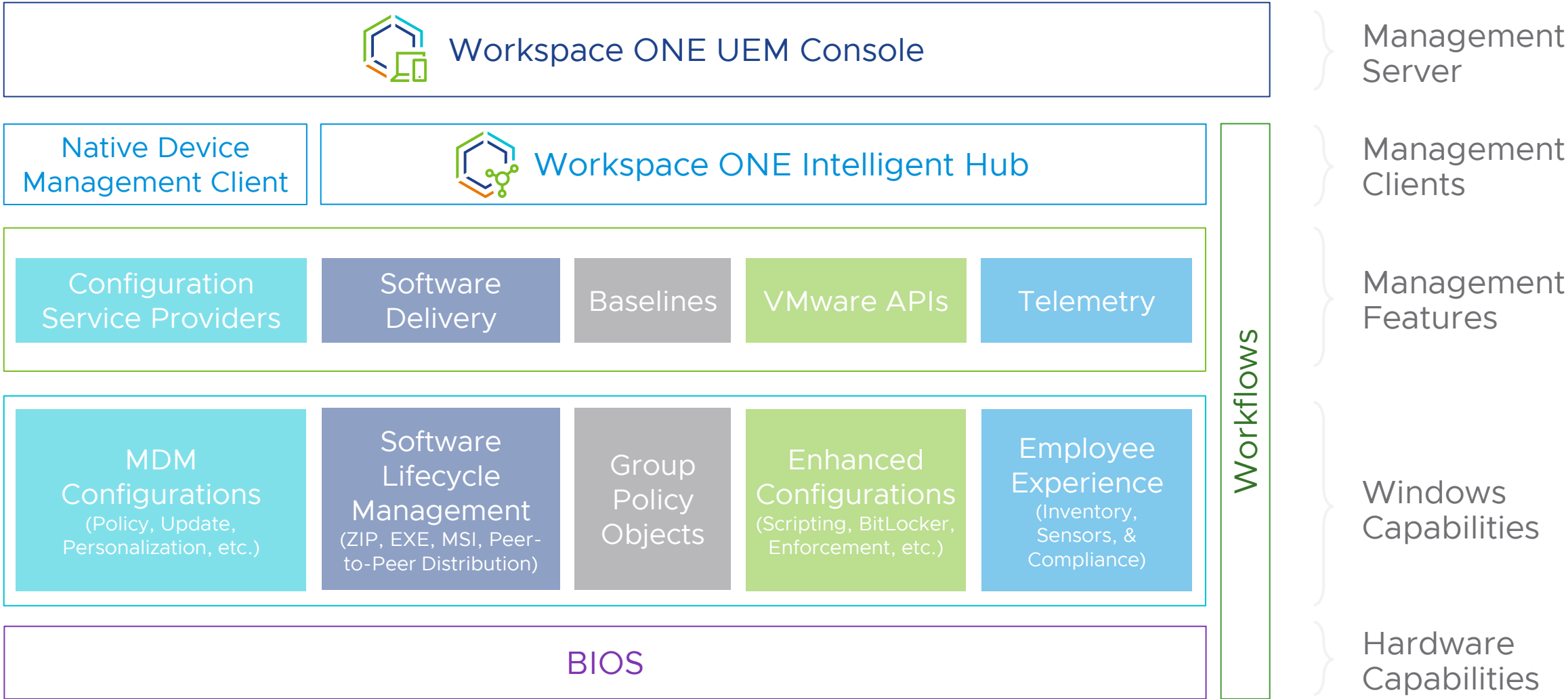
Cheat Sheet



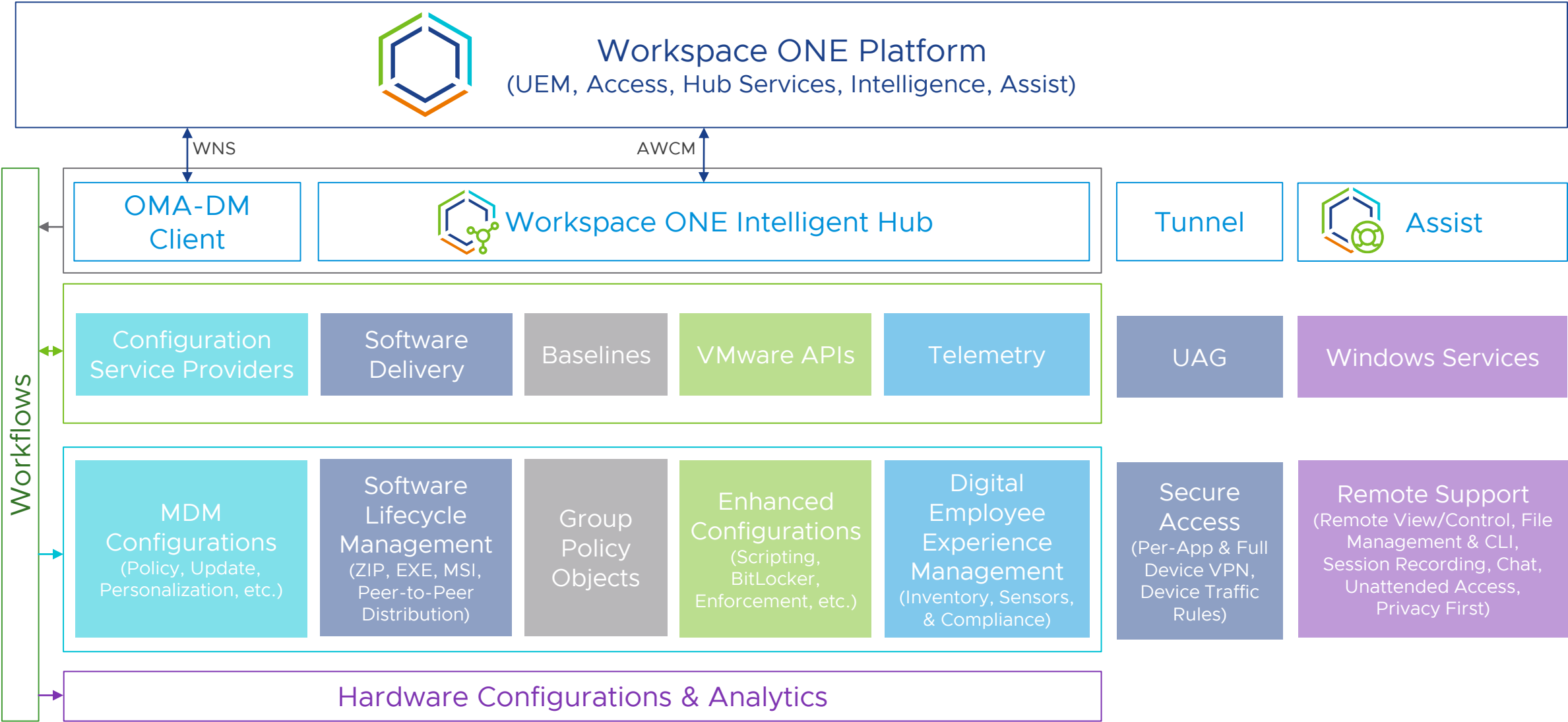
Windows Modern Management Solution Stack



WINDOWS
OVERVIEW



Windows Modern Management Solution Stack



Windows 10 Management Clients

Click to edit optional subtitle



WINDOWS
OVERVIEW

Clients	Uses
OMA-DM	Native MDM client built into the device which uses WNS. Used for device communication, enrollment, profile configuration using Microsoft CSPs, software distribution metadata delivery using VMware CSPs.
Workspace ONE Intelligent Hub	Used for communication, profiles, policies, workflows, sensors, scripts, and product provisioning. Allows end-users to access the unified app catalog, people search, notifications, and account settings.
Software Distribution Client	Used to install Win32 apps.
Dell Client Command Suite	Enables OEM updates and BIOS settings.
Workspace ONE Assist Client	Allows for remote control, file management, and executing remote shell commands using Remote Assist.
Workspace ONE Tunnel Client	Workspace ONE Tunnel enables secure access for mobile workers and devices.
VMware Digital Experience Telemetry	Allows for sending telemetry data directly to Workspace ONE Intelligence.

Collecting System Logs

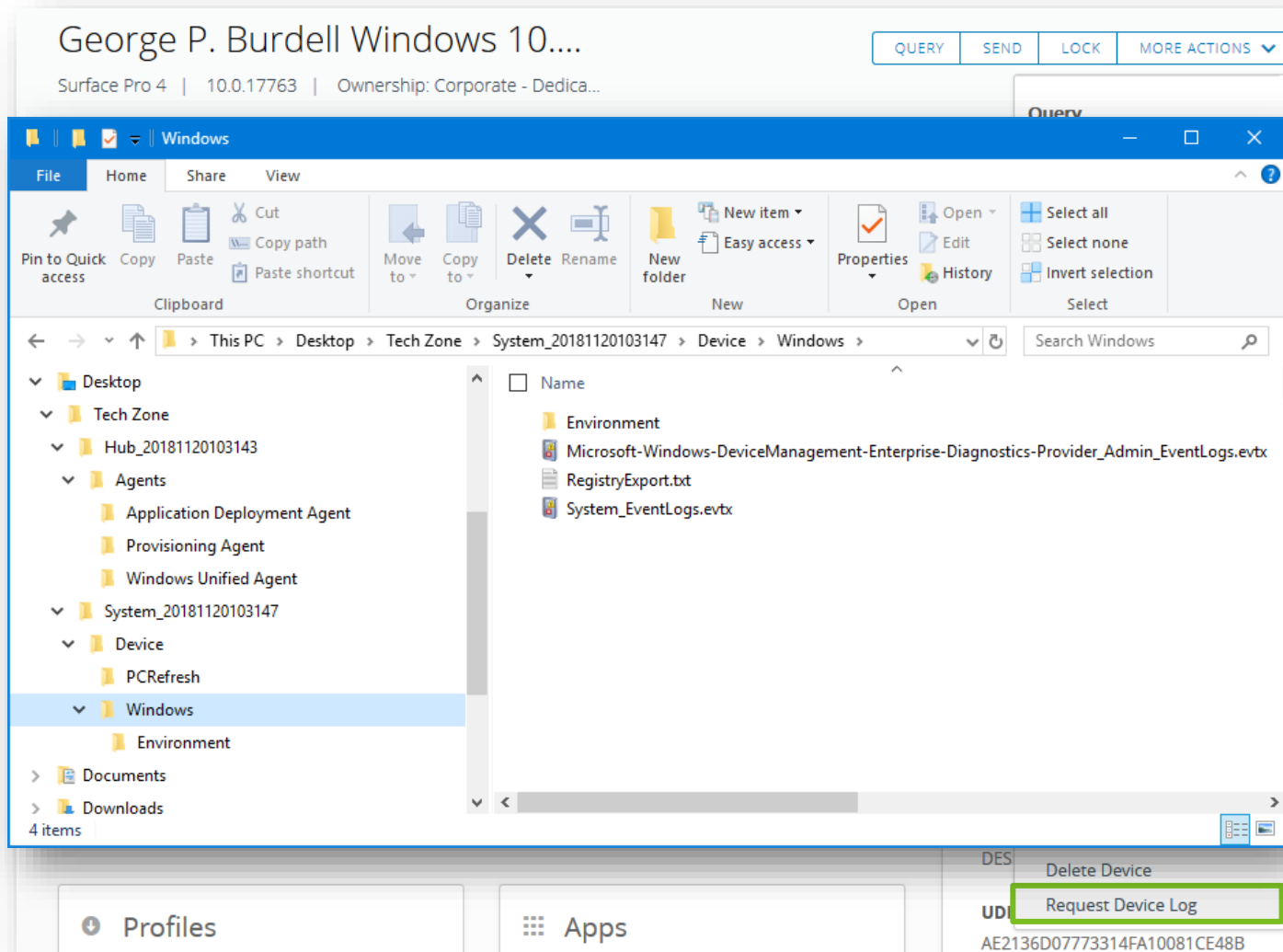


Improved Diagnostics with Remote Log Collection

Remotely collect logs for faster troubleshooting



COLLECTING
SYSTEM INFO



Overview

Provides admins the ability to collect logs from managed Windows 10 devices without having to physically access the device. You can choose to collect [Hub](#) or [System](#) logs, which includes logs on Software Distribution, Intelligent Hub, PC Refresh, MDM and System Event Logs, and other environment data.

Benefits

Allows admins to quickly troubleshoot remotely. Possible use-cases include validating app or profile pushes, or even if the Enterprise Reset occurred successfully.

Intelligent Hub Log Collection

End users have the ability to collect logs as well



COLLECTING
SYSTEM INFO

Collecting logs from the Intelligent Hub

- Right click system tray – Troubleshoot – Collect Logs or Hub Status
- Launch Hub – Click your Name – Collect Logs or Hub Status
 - Note: Collecting logs locally will omit detailed admin-only logs for security reasons. Admins can obtain more details by remotely collecting logs.

Windows Advanced Diagnostic Report

- C:/Users/Public/Documents/MDMDiagnostics/MDMDiagReport.html
- Very detailed with CSP certificates etc.



Your management log files will be exported here:

C:\Users\Public\Documents
\MDMDiagnostics

Export

Advanced Diagnostic Report

Your IT or support person may want additional information to help with troubleshooting.

Create report

Collecting System Information

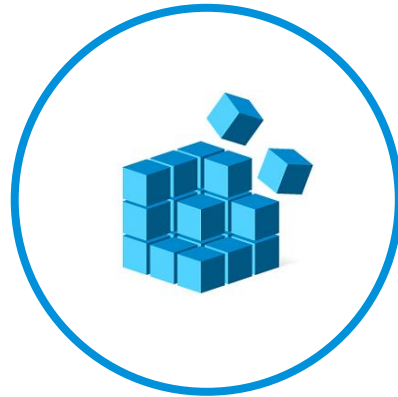
Collecting Device Information



COLLECTING
SYSTEM INFO



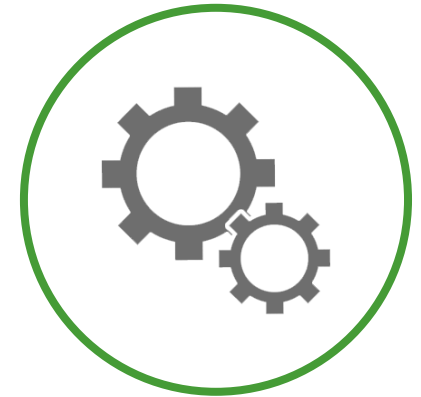
Windows Event
Log



Windows
Registry



Windows
Processes



Windows
Services

LIVE DEMO:

Remote Log Collection from the Workspace ONE UEM Console

Changing the Default Logging Levels

%ProgramFiles(x86)%\Airwatch\AgentUI*.config



```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <section name="entityFramework" type=
      "System.Data.Entity.Internal.ConfigFile.EntityFrameworkSection,
      EntityFramework, Version=6.0.0.0, Culture=neutral,
      PublicKeyToken=b77a5c561934e089" requirePermission="false" />
  </configSections>
  <appSettings>
    <add key="serilog:minimum-level" value="Debug" />
    <add key="serilog:using:File" value="Serilog.Sinks.File" />
    <add key="serilog:write-to:File.path" value=
      "%programdata%\Airwatch\UnifiedAgent\Logs\TaskScheduler-.log" />
    <add key="serilog:write-to:File.shared" value="true" />
    <add key="serilog:write-to:File.formatter" value=
      "Serilog.Formatting.Compact.CompactJsonFormatter, Serilog.Formatting.Compact" />
    <add key="serilog:write-to:File.retainedFileCountLimit" value="10" />
    <add key="serilog:write-to:File.rollingInterval" value="Day" />
    <add key="LocalAccountExclusionList" value="Guest,HomeGroupUser$" />
  </appSettings>
  <connectionStrings>
    <add name="awWindowsAgentProviderDbEntities" providerName=
```

Log Level	Description
None	Disables logging for the service.
Error	Only captures ERROR events.
Warning	Captures both WARN and ERROR events.
Information	Captures informational level logs for the service. This is the default level for most services. This includes INFO, ERROR, and WARN events.
All, Verbose, Debug	Most verbose option, used for gathering debug logs. This option should only be used when actively troubleshooting, then reverted back to the Information level. This level includes INFO, ERROR, WARN, and DEBUG events.

Log Collection Options



COLLECTING
SYSTEM INFO



Pro Tips and Tools

Becoming a Windows troubleshooting expert



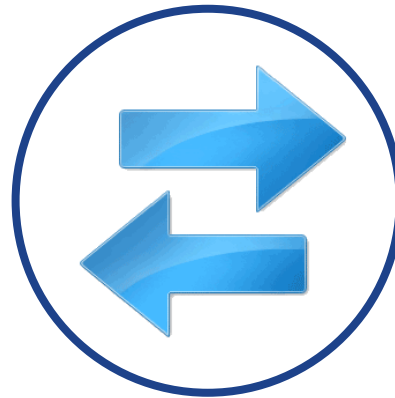
COLLECTING
SYSTEM INFO



Fiddler



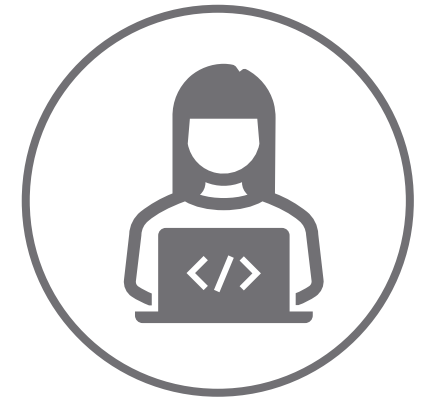
Postman



SyncML
Viewer

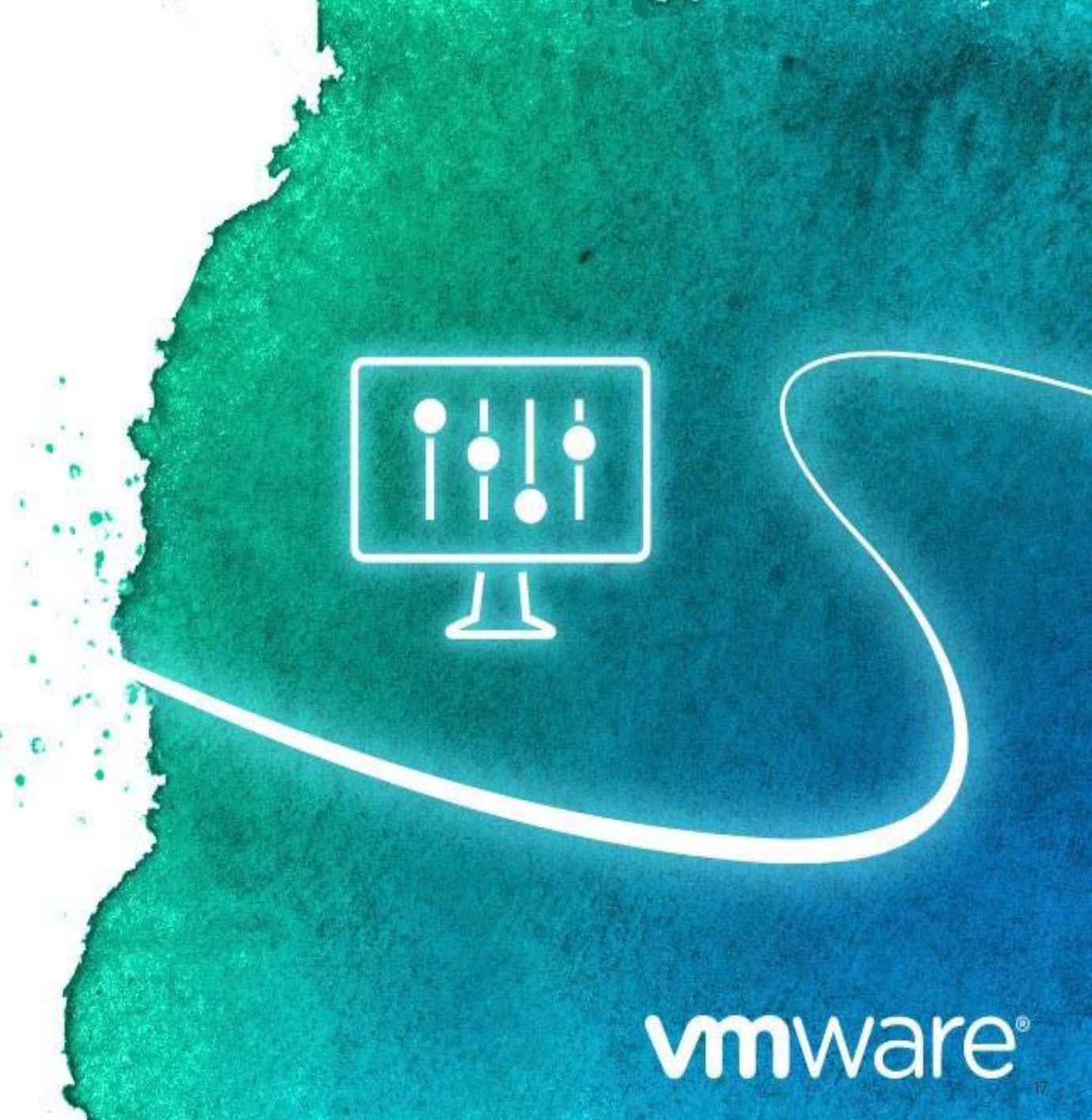


Workspace
ONE Discovery
Fling



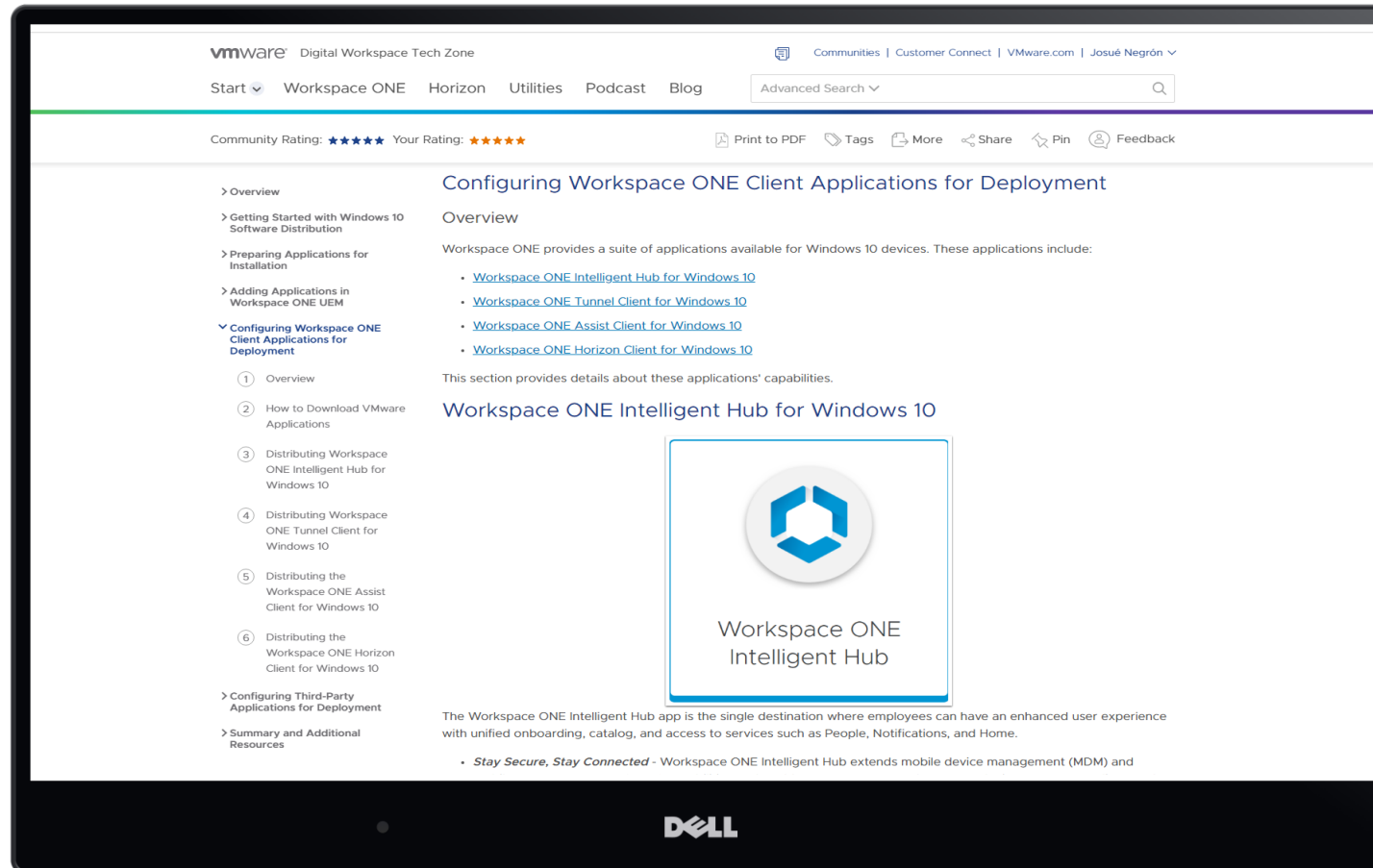
Browser
DevTools
(Network tab)

Troubleshooting



Deploying Traditional Win32 Applications Tutorial

<https://via.vmw.com/deploywin32>

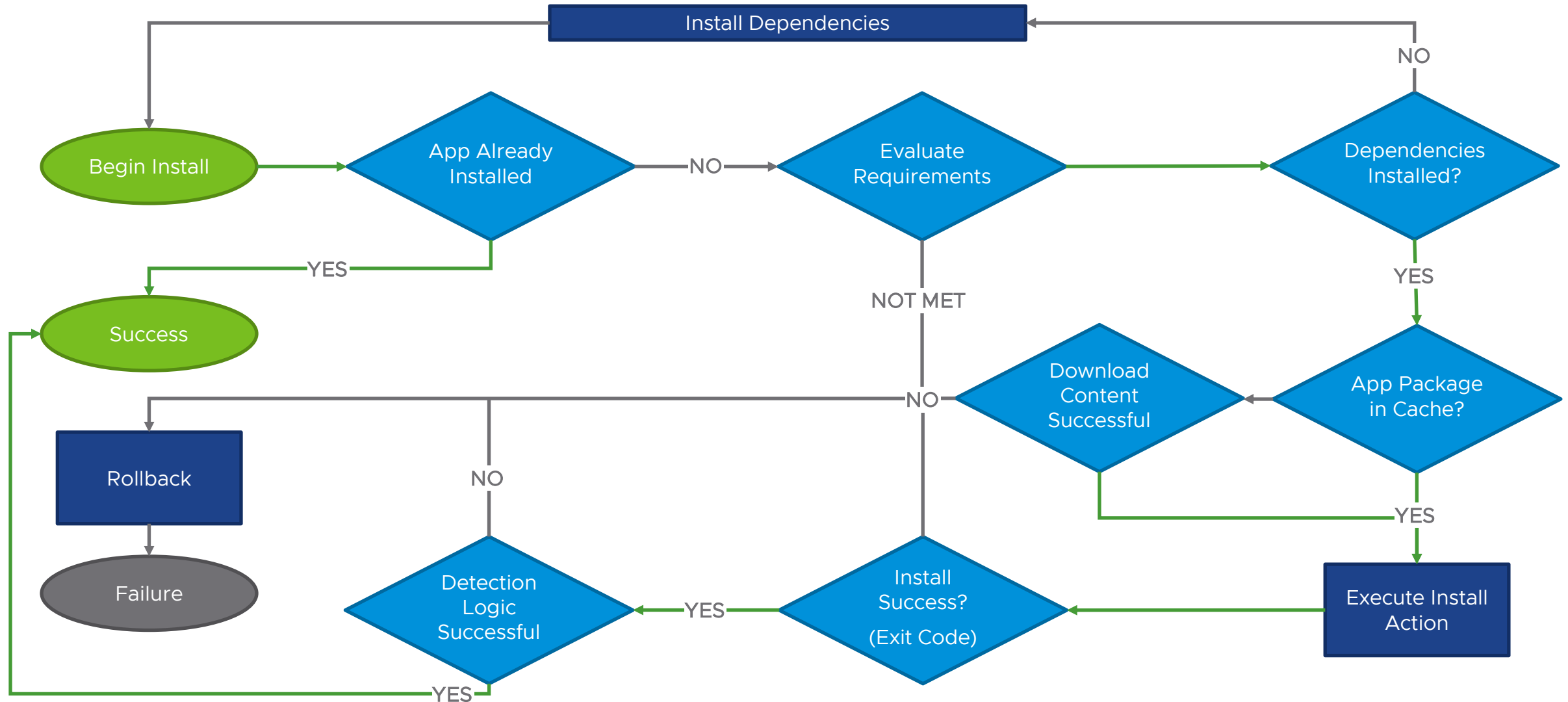


Client Side Win32 App Workflow

Complex background logic to surface end-user and admin simplicity



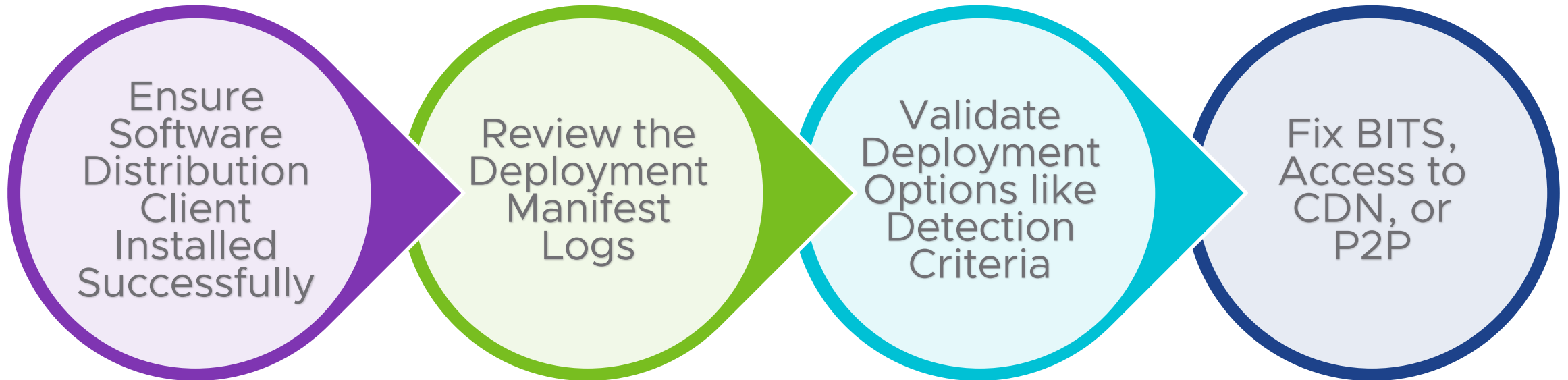
SOFTWARE
DISTRIBUTION



Troubleshooting Software Distribution



SOFTWARE
DISTRIBUTION



Software Distribution Logs and Registry Keys

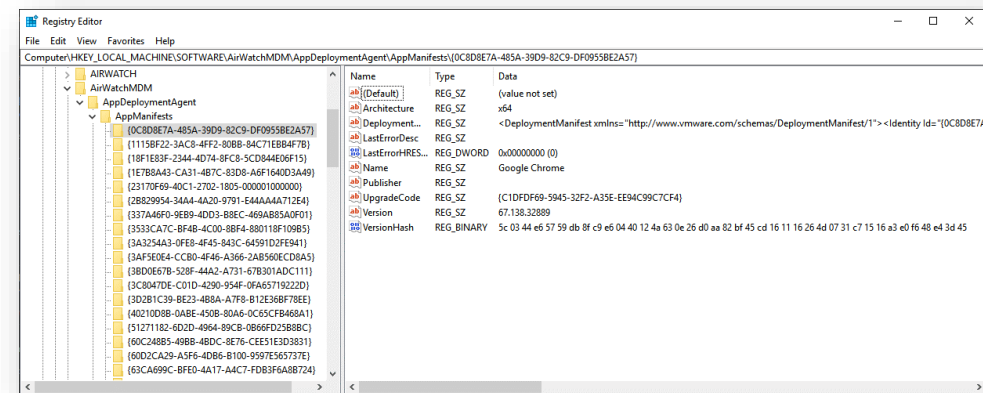
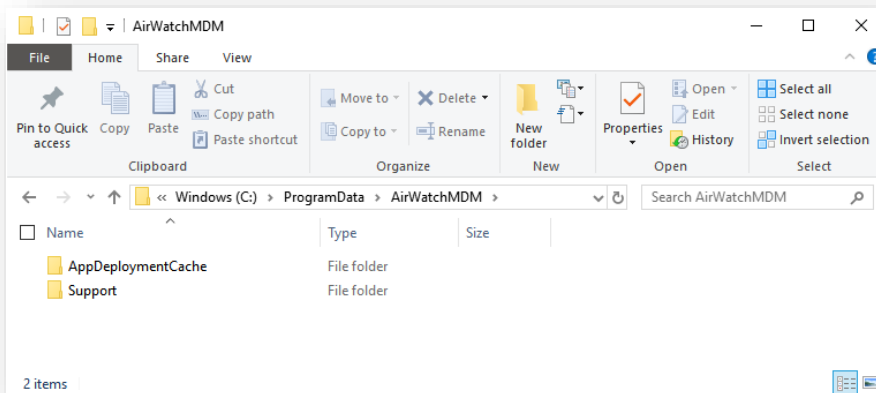


Cache and Support Logs:

- Located at <C:\ProgramData\AirWatchMDM>, this contains two folders:
 - AppDeploymentCache folder stores all downloaded content.
 - Support folder stores Software Distribution client logs.

Registry Entries:

- To check installation status of Software Distribution client:
<HKLM\SOFTWARE\Microsoft\EnterpriseDesktopAppManagement\MSI>
- For SFD apps: <HKLM\SOFTWARE\AirWatchMDM\AppDeploymentAgent> - this contains information around the configuration, content download, and deployment results.



Software Distribution Registry Folders



ContentManifest Folder

Contains URLs the client will use to download the installers and any associated files:

- Main app package
- Patches & Transforms
- Scripts

Dependency apps will have their own entry.

Queue Folder

Two of the most useful troubleshooting features are contained within this folder:

The [DeploymentLog](#) entry contains the log of the current deployment, including any error codes and a description of the last error, if applicable.

The [StatusCode](#) entry is a mapping to which part of the process the client is currently undertaking (download, dependency evaluation, installation, etc.).

AppManifest Folder

Contains all information provided when configuring the app:

- Deployment options
- Install and uninstall commands
- Supported architecture
- Version

Dependency apps will have their own entry.

The name of the app manifest entry matches the [AppID](#) given in the console.

Software Distribution Considerations

MSI vs EXE vs ZIP



SOFTWARE
DISTRIBUTION

- MSI apps don't require any additional configurations from the admin; ZIPs and EXEs require [uninstall command](#), [install command](#), and [detection criteria](#) to be added.
 - MSI uploads parse version, app name, product code, etc.
 - ZIP and EXE uploads use autogenerated information.
- ZIPs must contain either an EXE or MSI file.
- Folder name(s) for ZIPs will have to be included in the installation path, if applicable.

Edit Application - Slack v 3.2.0

Internal | Status: Active | Managed By: Digital Workspace Tech Zone | Application ID: {6...

Details | Files | Deployment Options | Images | Terms of Use

Name* Slack ⓘ

Managed By Digital Workspace Tech Zone

Application ID* {6A469396-3A6B-59A7-9699-AF5518F007}

Actual File Version* 3.2.0

Build Version {9D4D89AF-C112-4708-831A-53ECED5A6}

Version 3.2.0 ⓘ

Supported Processor Architecture ⓘ

Is Beta ⓘ

Save Failed

Uninstall Command required

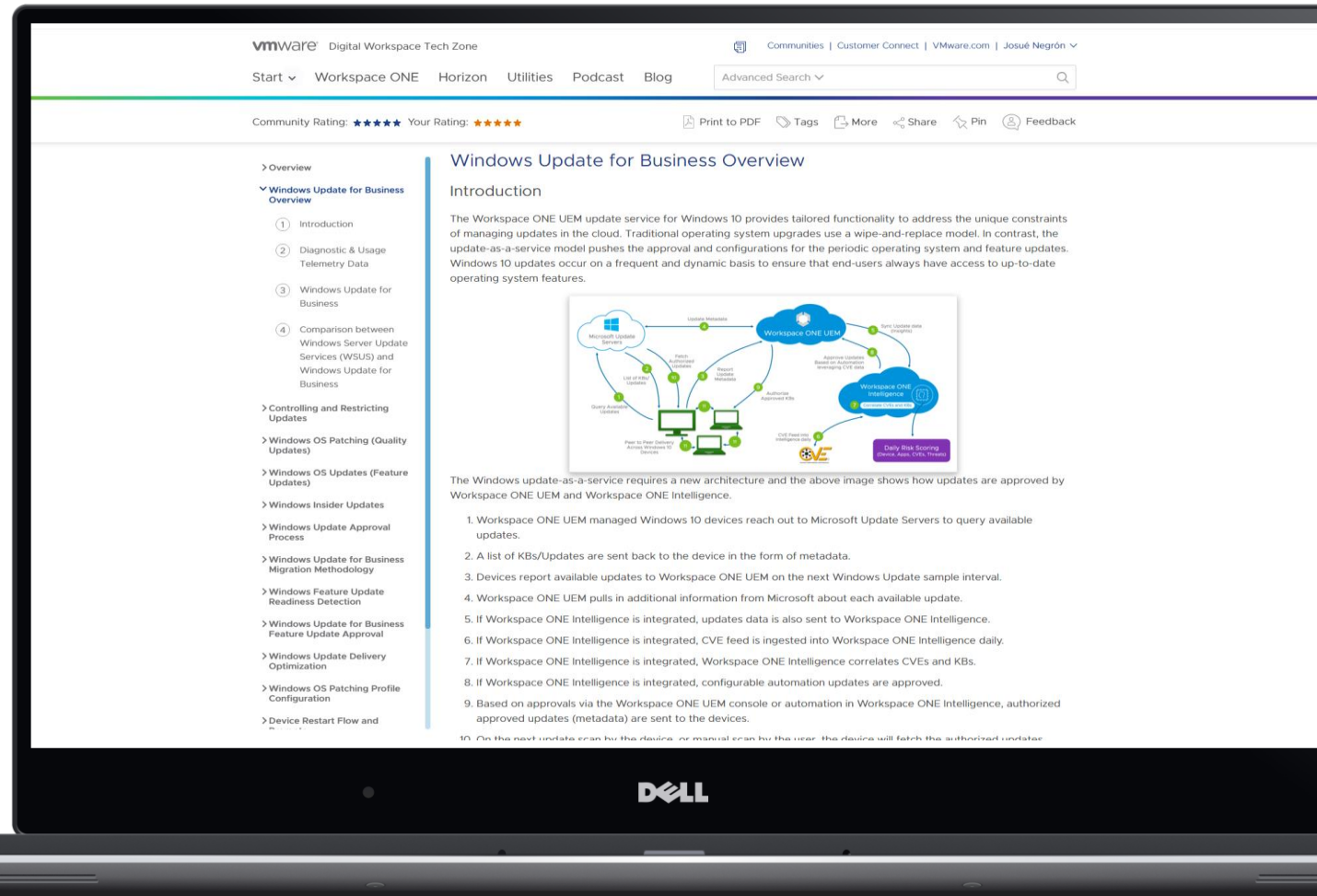
Install Command required

⚠ View incomplete fields or errors

SAVE & ASSIGN CANCEL

Understanding Windows 10 Policies (Baselines & MDM) Tutorial

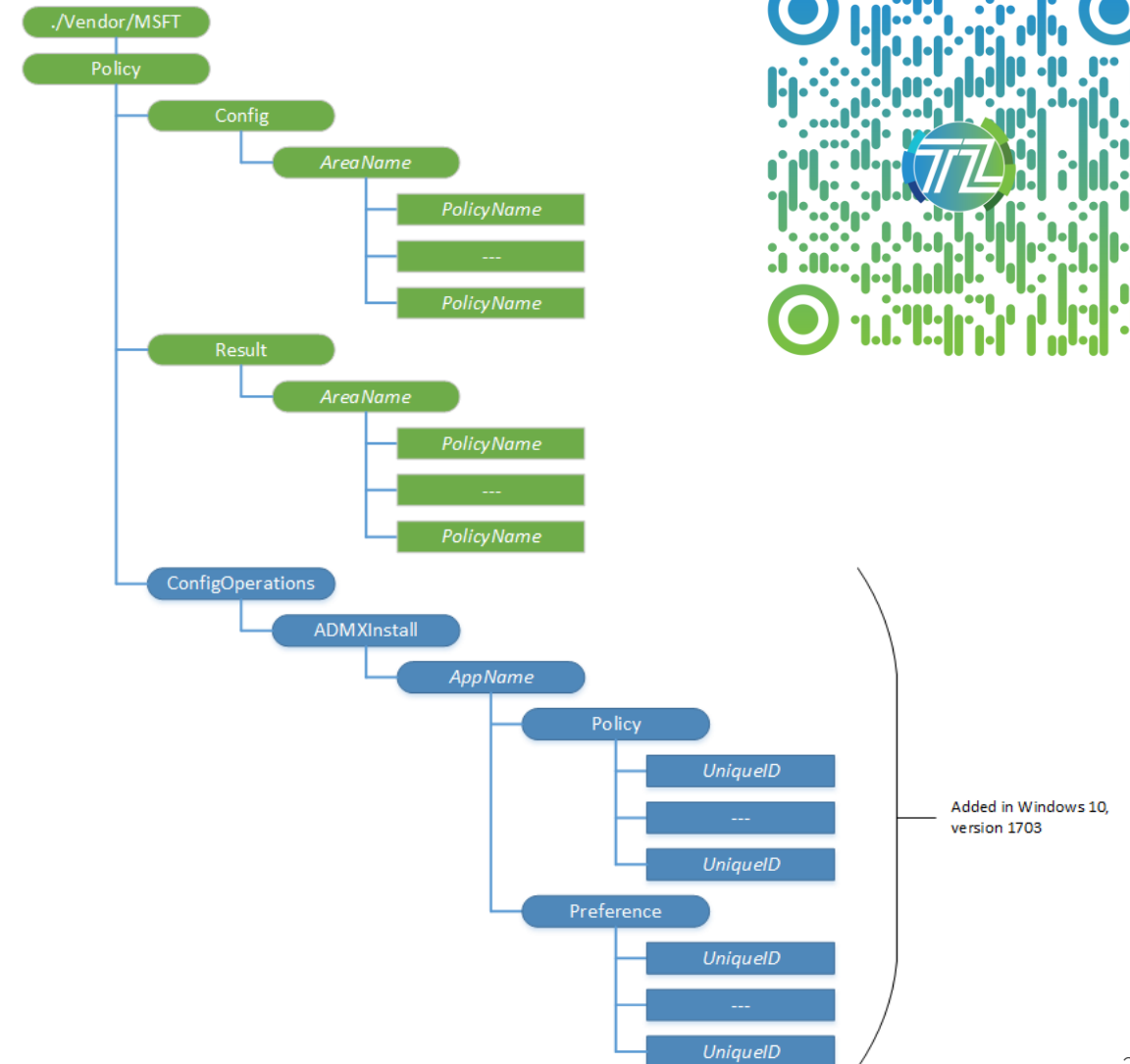
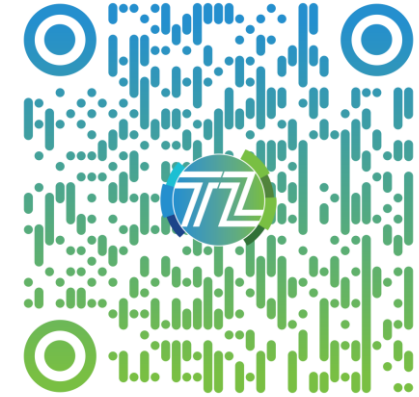
<https://via.vmw.com/WindowsUpdates>



Acronyms and Concepts to Learn



CSP – Configuration Service Provider
DDF - Device Description Framework
OMA-CP – Open Mobile Alliance - Client Provisioning
OMA-DM - Open Mobile Alliance – Device Management
WAP – Wireless app protocol
SyncML – Synchronization Markup Language



Anatomy of a SyncML



```
<SyncML xmlns='SYNCML:SYNCML1.2'>
```

```
<SyncHdr>
```

```
<VerDTD>1.2</VerDTD>
```

```
<VerProto>DM/1.2</VerProto>
```

```
<SessionID>11</SessionID>
```

```
<MsgID>1</MsgID>
```

```
<Target>
```

```
<LocURI>F7E8281A92511D40A9B1BC972BCC0AE7</LocURI>
```

UDID

```
</Target>
```

```
<Source>
```

```
<LocURI>https://ds1000.awmdm.com/DeviceServices/Dm.svc/token/j03ux</LocURI>
```

Mgmt Server

```
</Source>
```

```
</SyncHdr>
```

```
<SyncBody>
```

```
<CmdID>cb17d15b-c7e7-4036-9d15-28744b2e6dd6</CmdID>
```

Command ID

```
<Get>
```

```
<CmdID>cb17d15b-c7e7-4036-9d15-28744b2e6dd6</CmdID>
```

```
<Item>
```

```
<Target>
```

```
<LocURI>./DevDetail/SwV</LocURI>
```

Location URI

```
</Target>
```

```
</Item>
```

```
</Get>
```

```
<Final/>
```

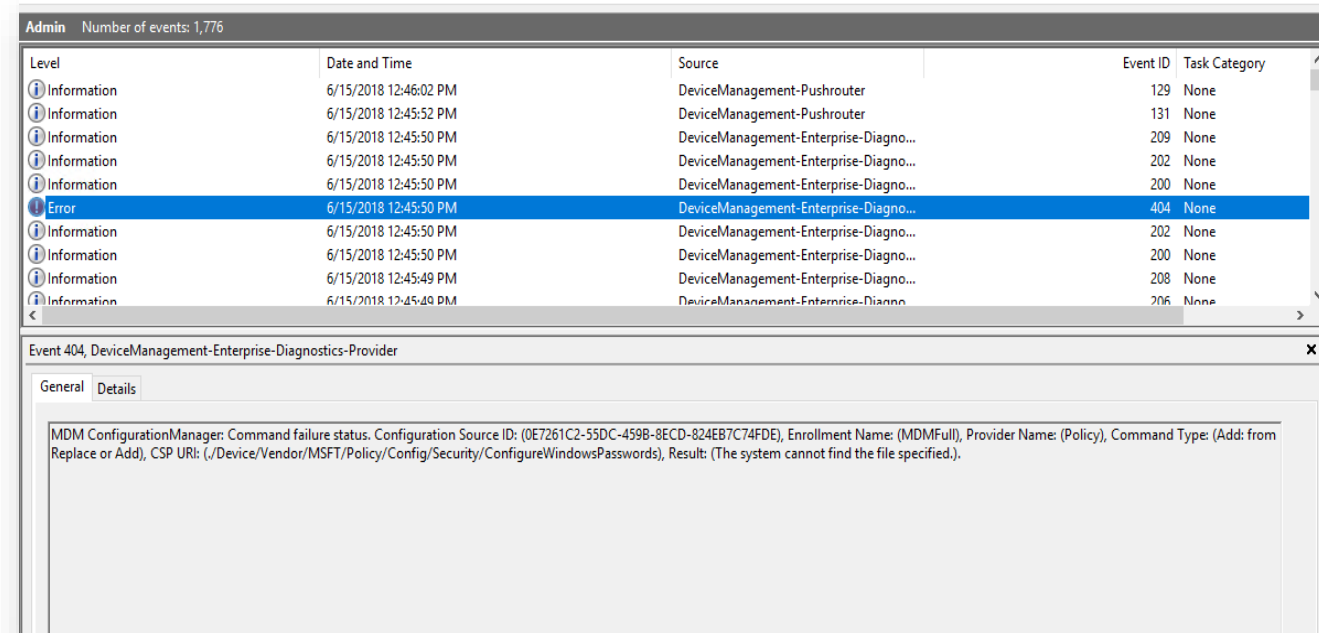
```
</SyncBody>
```

```
</SyncML>
```

Profile Troubleshooting Steps



1. Check Event Viewer logs for failure message: [App and Service Logs > Microsoft > Windows > DeviceManagement-Enterprise-Diagnostics-Provider > Admin](#).
 - Look for Event ID "404" and the offending LocURI/Setting.
2. Confirm setting is supported on the Windows 10 version being used.
3. Confirm that the correct action is used - Add/Replace/Delete.
4. For Custom Settings:
 - Check that XML is in between CDATA tags.
 - Confirm that the correct data format is sent.
5. In Fiddler check error codes.
<http://bit.ly/SyncMLCodes>



Baseline High Level Architecture

Baseline Components



CONFIGURATION
MANAGEMENT

Workspace ONE UEM

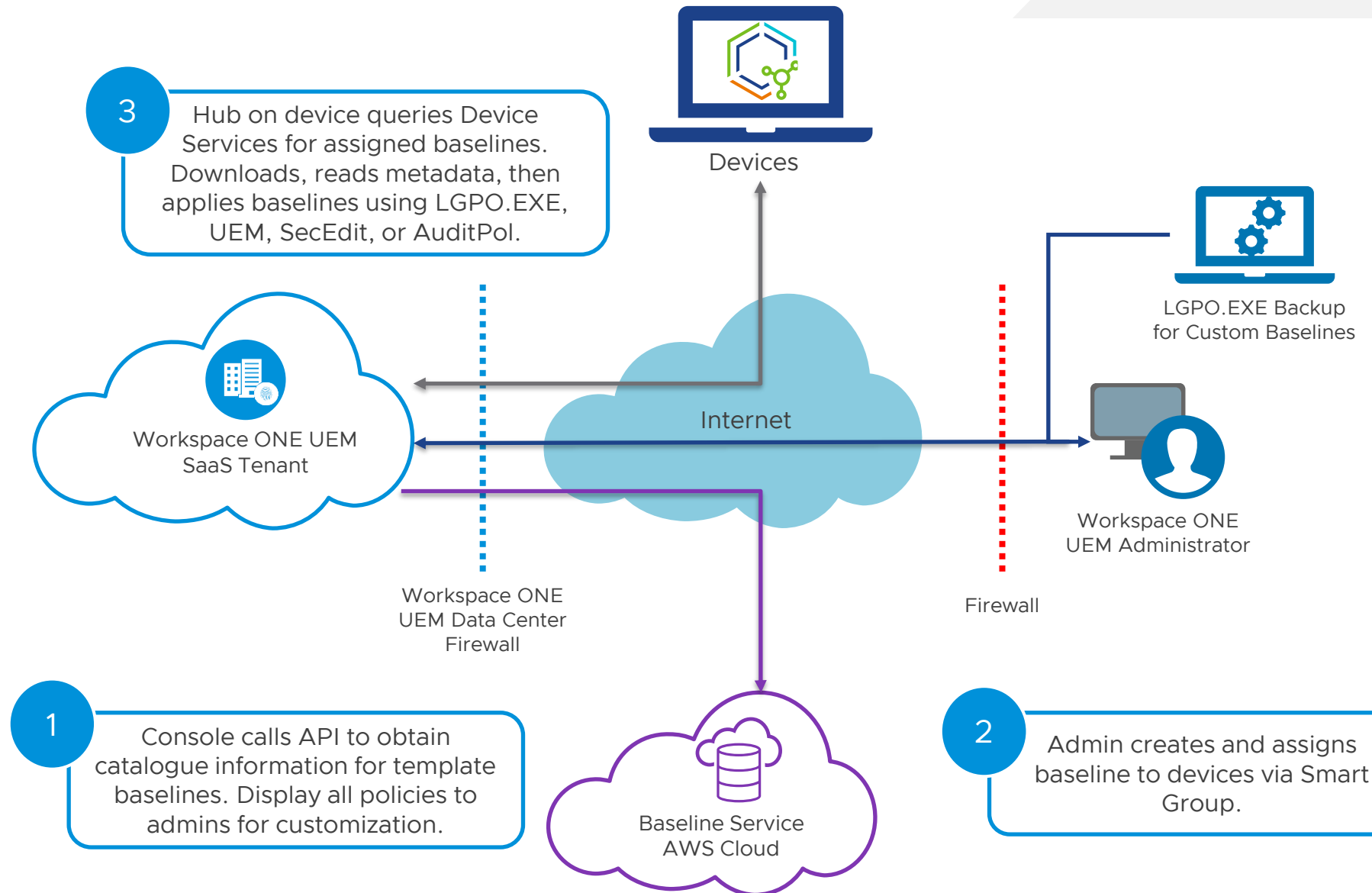
The administrator manages and assigns baselines to devices from the Workspace ONE UEM Console. The console uses APIs to interact with Baseline Service. Device Services returns assigned Baseline to device.

Baseline Service

This service maintains the catalogue information for template baselines.

Devices

Workspace ONE Intelligent Hub queries Device Services to download assigned baselines. Hub uses LGPO, UEM agent, or native features to apply policies.



Troubleshooting & Helpful Hints



Ensure you have deployed LGPO.EXE to the device for custom baselines

Helpful Hints

Workspace ONE Intelligent Hub will first check if LGPO.EXE (for custom) is located at %ProgramData%\AirWatch\LGPO, if not present, Hub will check at every 15, 30, 60, 120, 240 minutes. Once LGPO.EXE is available, Baseline will be applied to the device.

Hub receives real-time notification via AWCM as well as pre-defined intervals. (e.g. every 6 hours or sampling frequency).

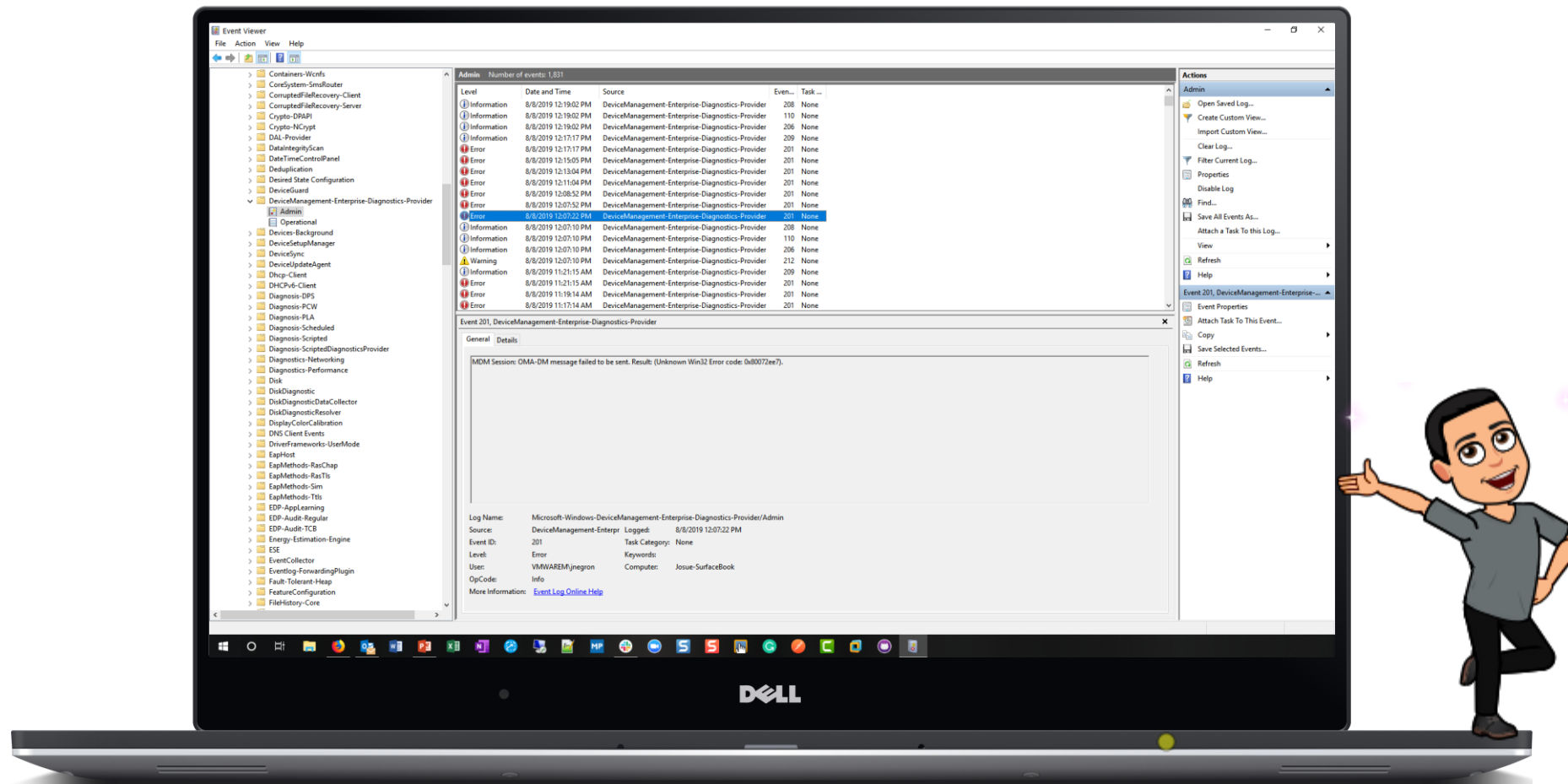
Troubleshooting

Browse and see if C:\Program Files (x86)\AirWatch\AgentUI has Baseline and BaselineBackup folders, if not, Baselines are not getting downloaded to the device.

Leverage the Troubleshooting tab to see details, filter Module to Baseline. The following events are logged for Baselines: Query Requested/Confirmed/Failed, Install Failed/Confirmed, Removal Confirmed/Failed, Status Update Failed.

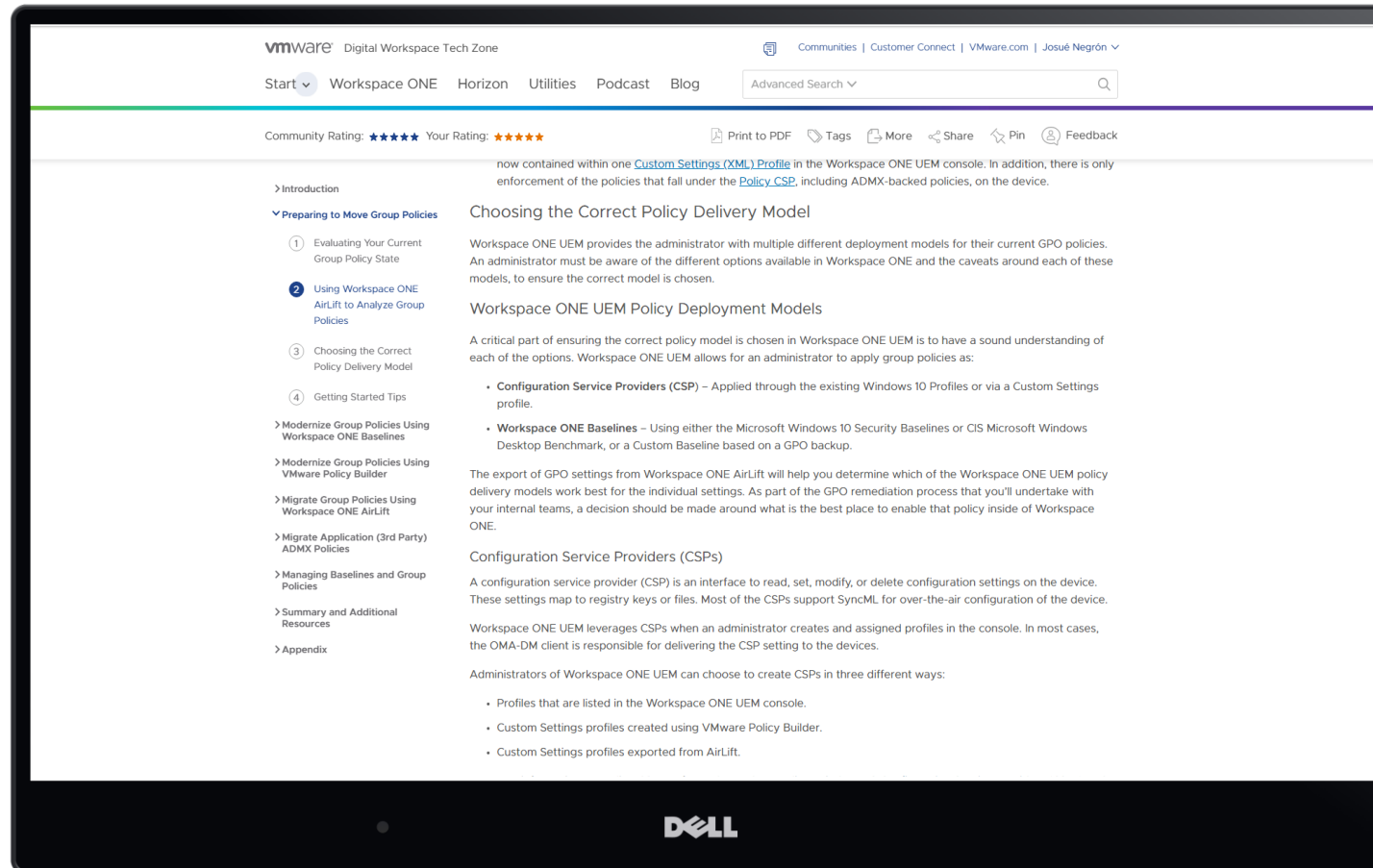
Using Fiddler, SyncML Viewer and Event Viewer

Understanding communication and how to find errors



Managing Windows Updates for Windows 10 Tutorial

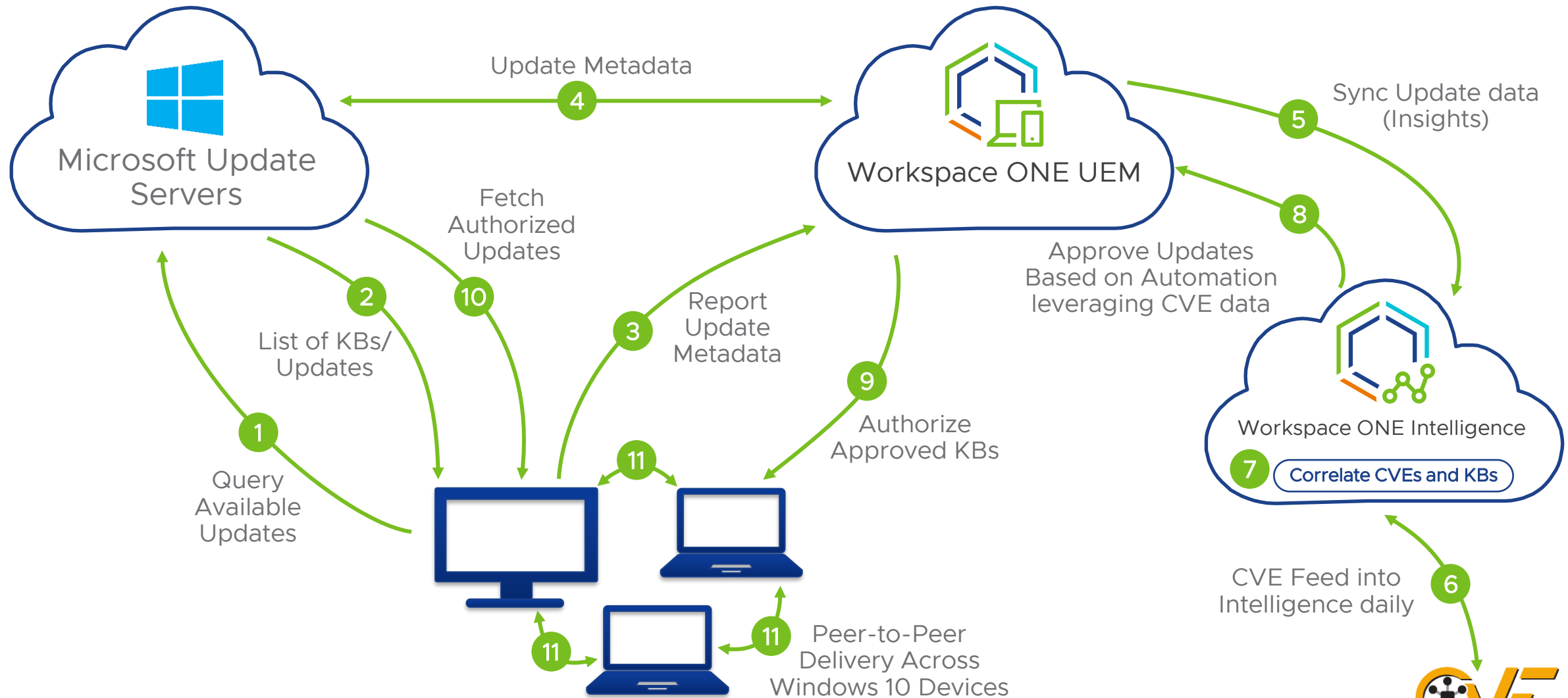
<https://via.vmw.com/WindowsUpdates>



Windows as a Service Requires a New Architecture



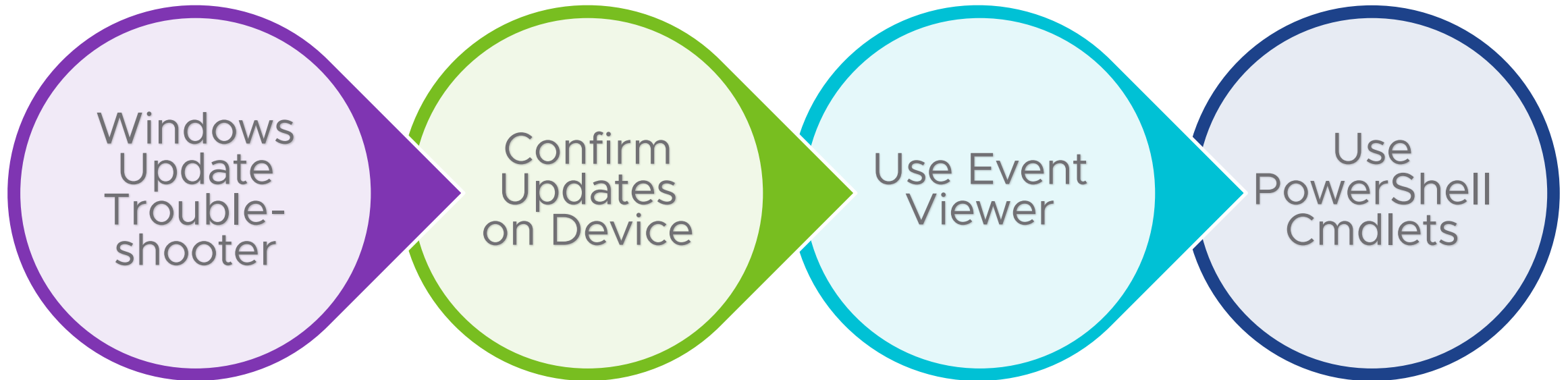
OS PATCH
MANAGEMENT



Troubleshooting Windows Updates



OS PATCH
MANAGEMENT

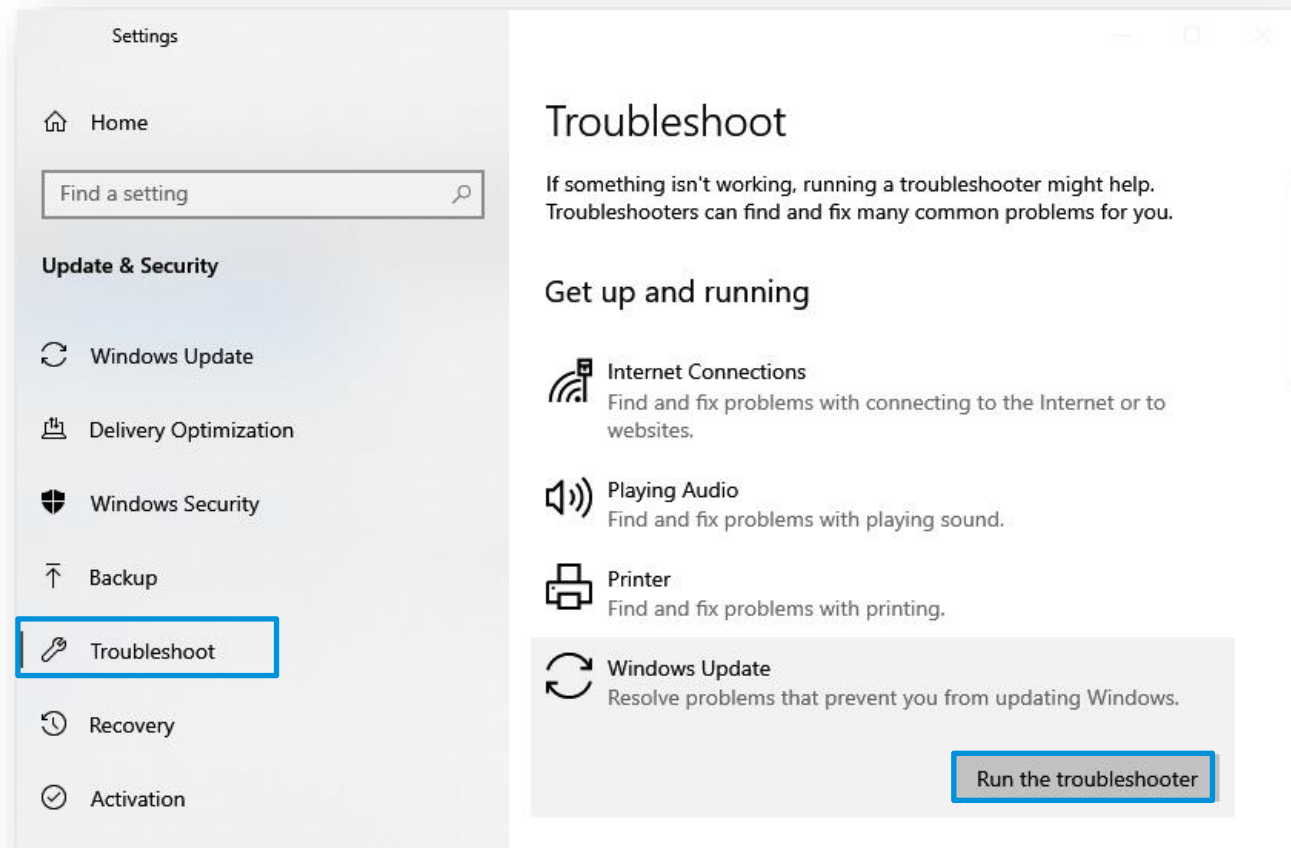


Run Windows Updates Troubleshooter

Navigate to [Windows Settings > Update & Security > Troubleshoot > Windows Update](#), then select [Run the Troubleshooter](#).

This tool will do the following automatically:

1. Stops the Windows Update Service.
2. Clears out the download cache ([C:\Windows\SoftwareDistribution](#)).
3. Restarts the Windows Update Service.

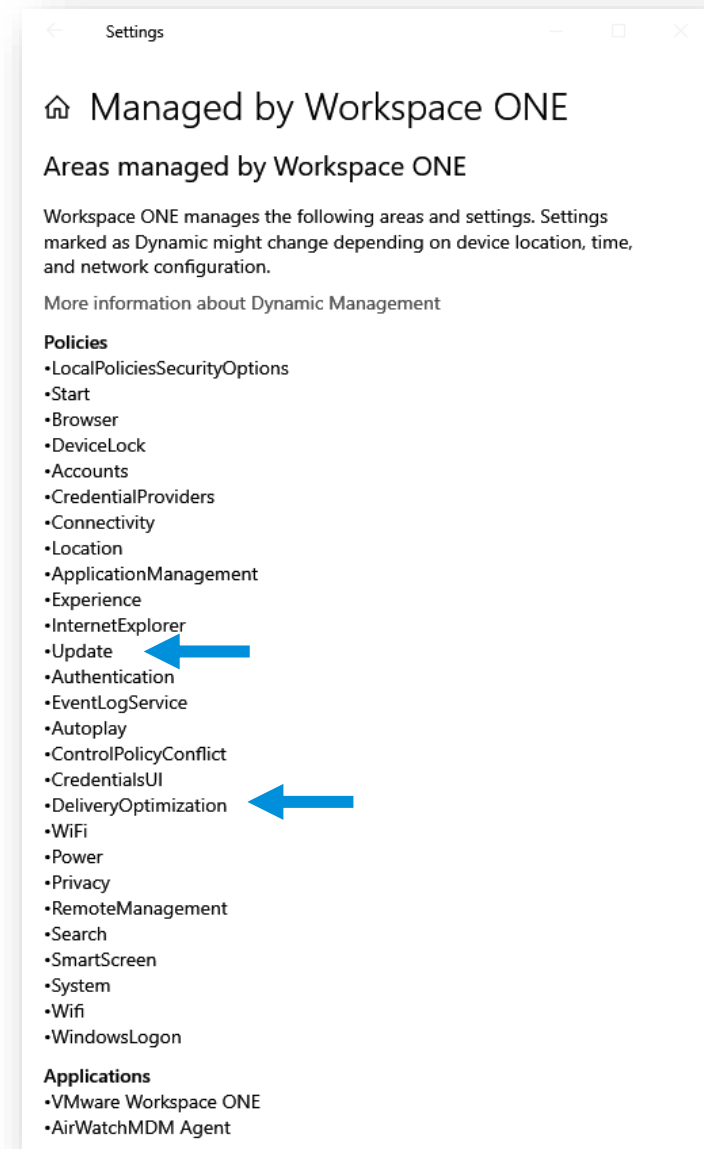


Confirm Updates on Device

Validate the device received the profile

We can validate that the device installed the Windows Update profile by navigating to [Windows Settings > Accounts > Access Work or School](#), then selecting on our enrollment account, then selecting [Info](#).

Verify that you see [Update](#) under [Areas managed by Workspace ONE](#), if you have configured Delivery Optimization, verify that you see entry as well.



Confirm Updates on Device

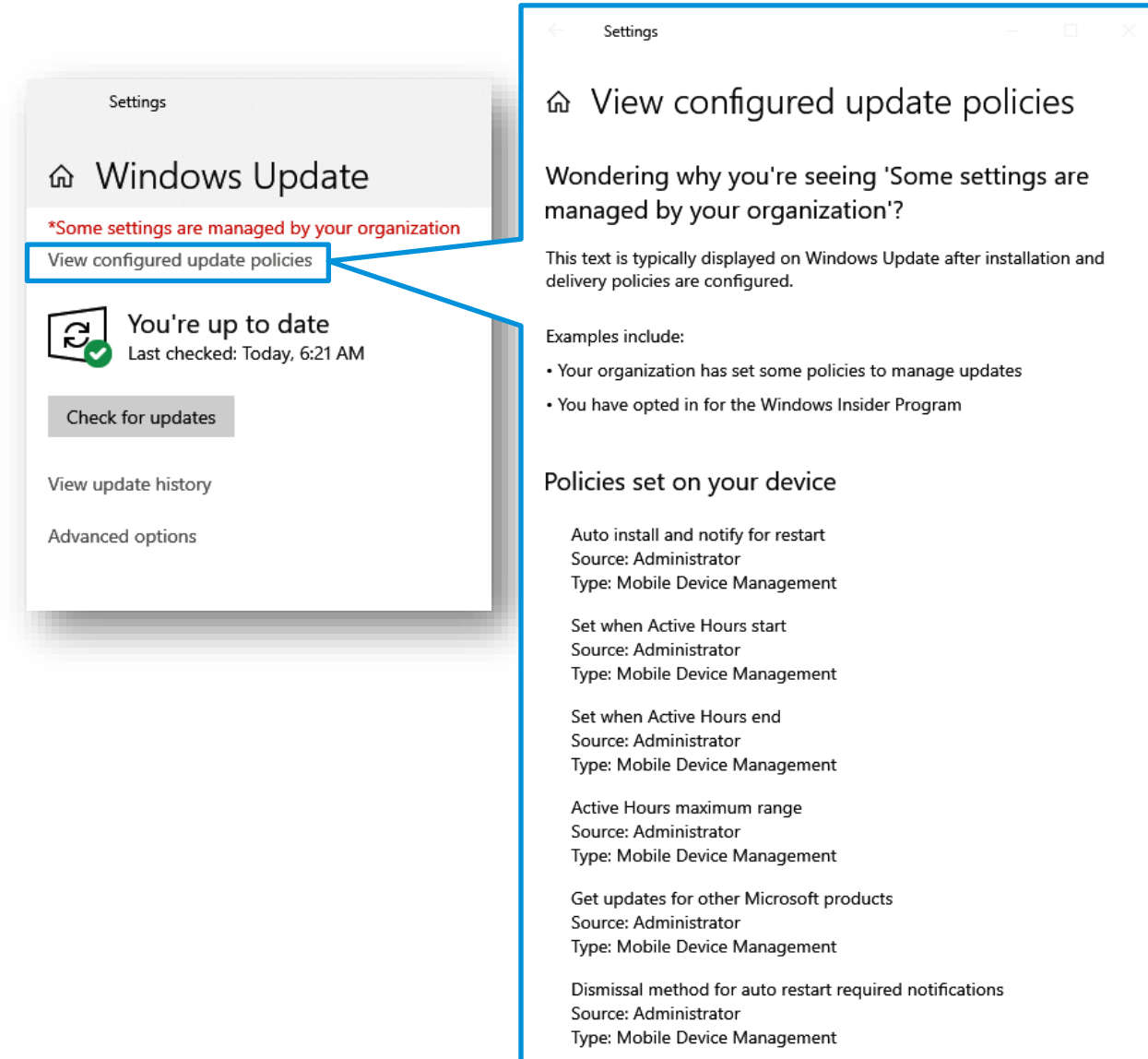
Validate Windows Update UI shows correct values

Navigate to [Windows Settings > Update & Security > Windows Update](#), then select [View Configured Update Policies](#).

If you do not see [Some settings are managed by your organization](#), then perform these steps:

1. Restart the Windows Update Service (wuauserv), then select [Check for Updates](#).
2. Close and re-open settings and the settings should be updated.

See read-only settings that Workspace ONE UEM is managing. Where are the values?




The image shows a Windows Settings window with the 'Windows Update' section selected. A red banner at the top states '*Some settings are managed by your organization'. Below this, a button labeled 'View configured update policies' is highlighted with a blue box. A callout from this button points to a larger, detailed view of the 'View configured update policies' screen. This screen explains that the text 'Some settings are managed by your organization' is typically displayed after installation and delivery policies are configured. It lists examples: 'Your organization has set some policies to manage updates' and 'You have opted in for the Windows Insider Program'. Below this, a section titled 'Policies set on your device' lists several settings, all managed by the Administrator via Mobile Device Management (MDM). These settings include: 'Auto install and notify for restart', 'Set when Active Hours start', 'Set when Active Hours end', 'Active Hours maximum range', 'Get updates for other Microsoft products', and 'Dismissal method for auto restart required notifications'.

Settings

Windows Update

*Some settings are managed by your organization

[View configured update policies](#)

 You're up to date
Last checked: Today, 6:21 AM

[Check for updates](#)

[View update history](#)

[Advanced options](#)

View configured update policies

Wondering why you're seeing 'Some settings are managed by your organization'?

This text is typically displayed on Windows Update after installation and delivery policies are configured.

Examples include:

- Your organization has set some policies to manage updates
- You have opted in for the Windows Insider Program

Policies set on your device

Auto install and notify for restart
Source: Administrator
Type: Mobile Device Management

Set when Active Hours start
Source: Administrator
Type: Mobile Device Management

Set when Active Hours end
Source: Administrator
Type: Mobile Device Management

Active Hours maximum range
Source: Administrator
Type: Mobile Device Management

Get updates for other Microsoft products
Source: Administrator
Type: Mobile Device Management

Dismissal method for auto restart required notifications
Source: Administrator
Type: Mobile Device Management

Confirm Updates on Device

Validate configured values using Regedit

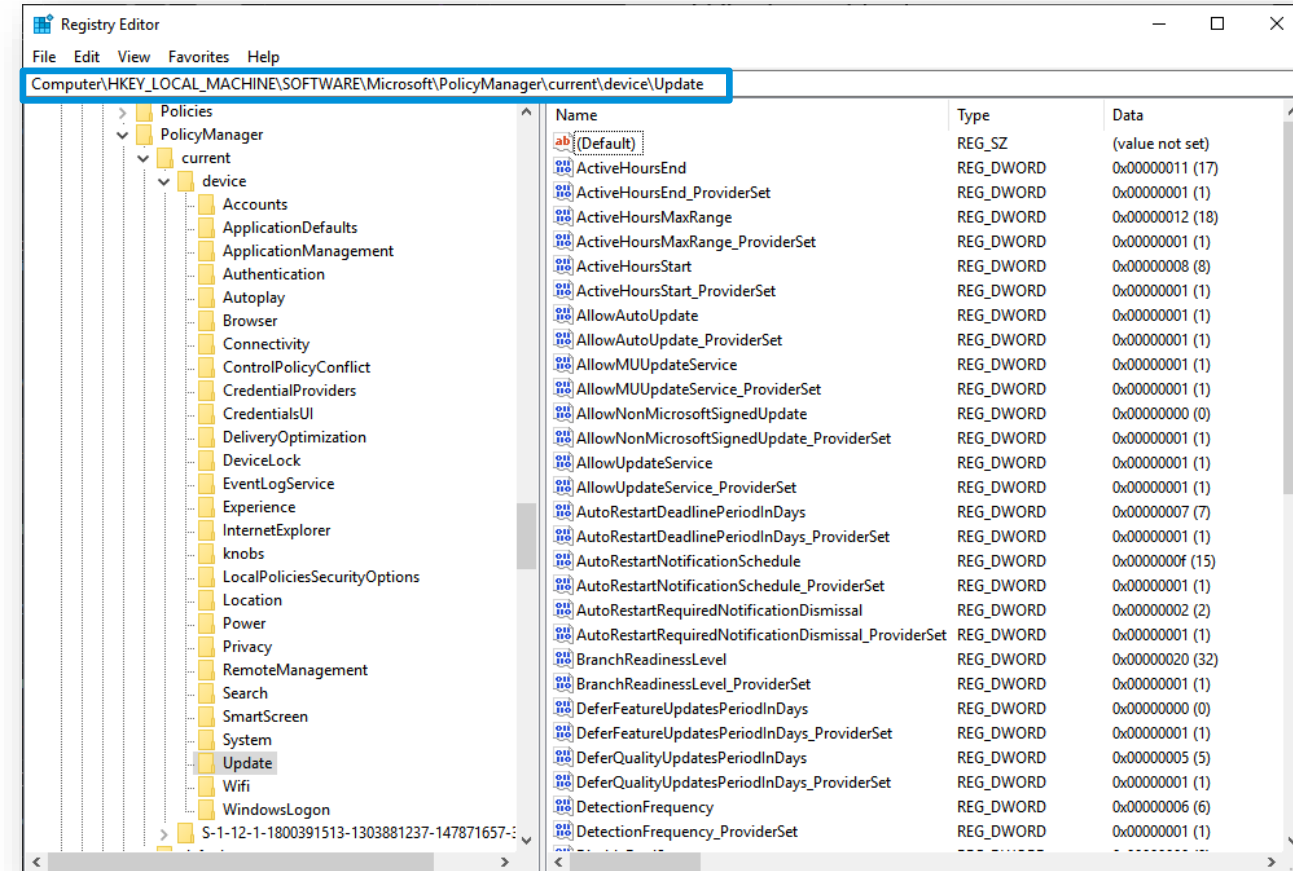


OS PATCH
MANAGEMENT

Using Regedit, navigate to [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\current\device\Update](#).

This registry location shows only what was sent through MDM. If the domain is pushing out settings using GPO, these settings could be overridden on the device.

Note: If you are using GPO to configure Windows Updates and you want to use Workspace ONE UEM, consider sending down a custom settings profile leveraging [VMware Policy Builder](#) to deploy the MDM Wins Over GP setting, part of the [Policy/Control Policy Conflict CSP](#).

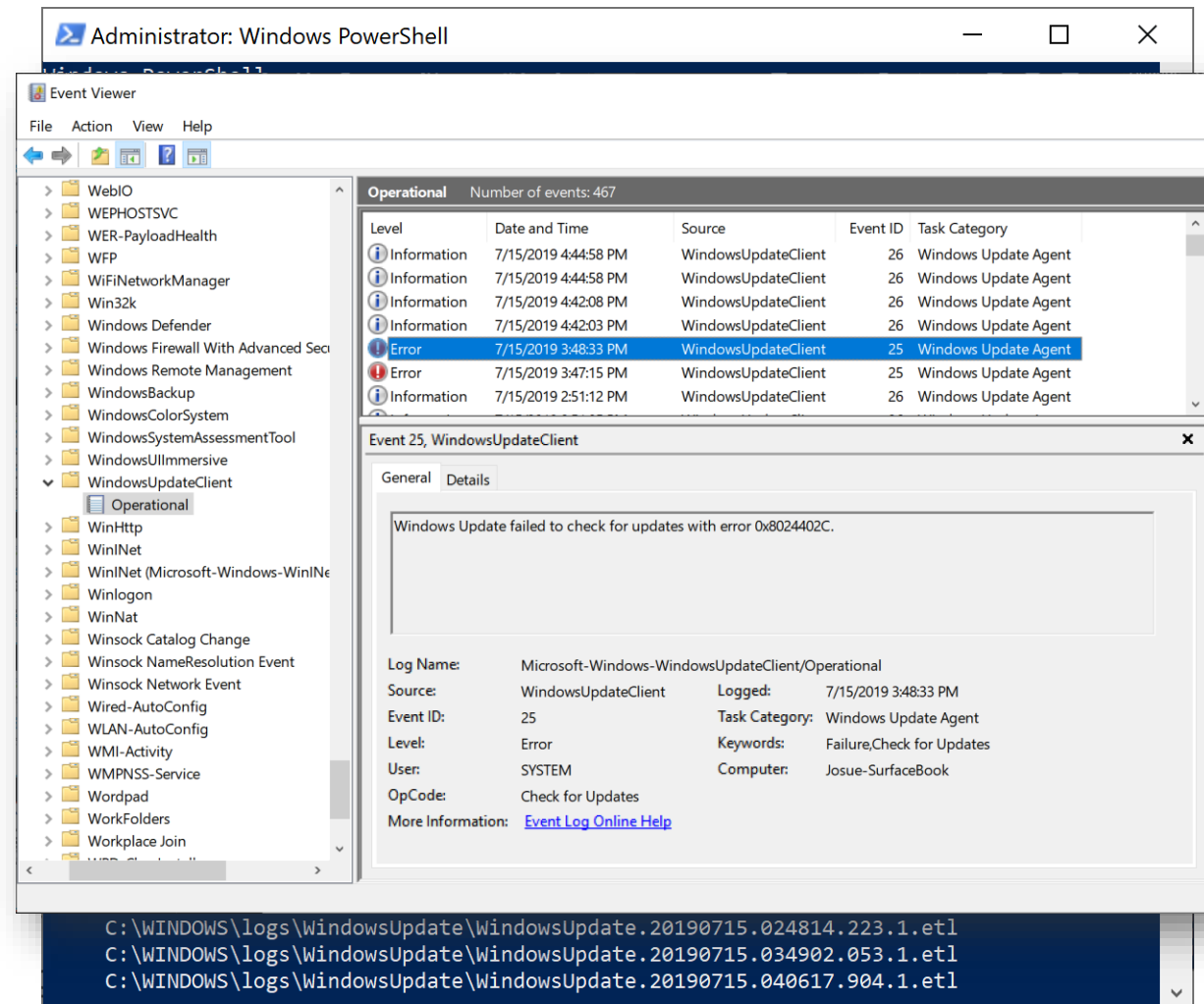


Using Event Viewer & PowerShell

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.



The screenshot shows an Administrator: Windows PowerShell window in the background. In the foreground, the Event Viewer application is open, displaying the 'Operational' log for the 'Microsoft-Windows-WindowsUpdateClient' source. The log shows several events, with the most recent one (ID 25) highlighted as an error. The details pane for this event shows the message: 'Windows Update failed to check for updates with error 0x8024402C.' Below the details, the event's metadata is displayed, including the log name, source, event ID, level, user, and task category.

Level	Date and Time	Source	Event ID	Task Category
Information	7/15/2019 4:44:58 PM	WindowsUpdateClient	26	Windows Update Agent
Information	7/15/2019 4:44:58 PM	WindowsUpdateClient	26	Windows Update Agent
Information	7/15/2019 4:42:08 PM	WindowsUpdateClient	26	Windows Update Agent
Information	7/15/2019 4:42:03 PM	WindowsUpdateClient	26	Windows Update Agent
Error	7/15/2019 3:48:33 PM	WindowsUpdateClient	25	Windows Update Agent
Error	7/15/2019 3:47:15 PM	WindowsUpdateClient	25	Windows Update Agent
Information	7/15/2019 2:51:12 PM	WindowsUpdateClient	26	Windows Update Agent

Event 25, WindowsUpdateClient

General Details

Windows Update failed to check for updates with error 0x8024402C.

Log Name: Microsoft-Windows-WindowsUpdateClient/Operational
Source: WindowsUpdateClient
Event ID: 25
Level: Error
User: SYSTEM
OpCode: Check for Updates
More Information: [Event Log Online Help](#)

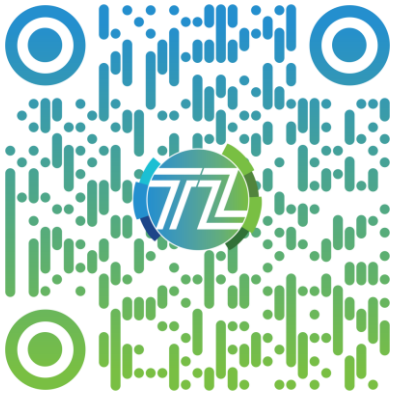
Logged: 7/15/2019 3:48:33 PM
Task Category: Windows Update Agent
Keywords: Failure, Check for Updates
Computer: Josue-SurfaceBook

C:\WINDOWS\logs\WindowsUpdate\WindowsUpdate.20190715.024814.223.1.etl
C:\WINDOWS\logs\WindowsUpdate\WindowsUpdate.20190715.034902.053.1.etl
C:\WINDOWS\logs\WindowsUpdate\WindowsUpdate.20190715.040617.904.1.etl

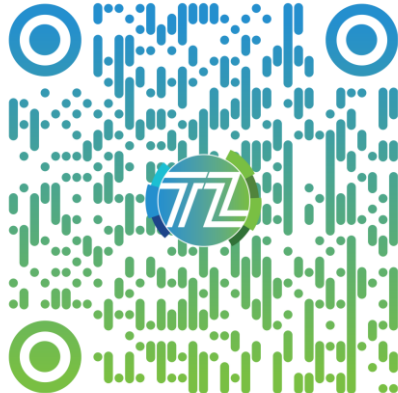
Onboarding Methods & Windows Security Design Tutorial

<https://via.vmw.com/W10Onboarding> & <https://via.vmw.com/WindowsSecurity>

Onboarding
Methods



Security
Design



vmware Digital Workspace Tech Zone

Communities | Customer Connect | VMware.com | Josué Negrón

Start Workspace ONE Horizon Utilities Podcast Blog

Advanced Search

Community Ratings: ★★★★★ Your Rating: ★★★★★

Print to PDF Tags More Share Pin Feedback

Overview

Meeting Windows 10 Security Priorities

Determining Your Use Cases

▼ Selecting an Onboarding Workflow

1 Introduction

2 Understanding Onboarding Options

3 Selecting an Onboarding Workflow

Configuring Workspace ONE Profiles

Delivering and Managing Software

Managing Windows 10 Updates

Summary and Additional Resources

Selecting an Onboarding Workflow

The following figure is a decision tree intended to help you select an appropriate onboarding workflow. Examine the tree to determine which enrollment flows best suit your organization. Then, refer to the descriptions of the enrollment flows in following sections to learn more.

Figure: Windows 10 Onboarding Decision Tree

Agent-Based Enrollment

The agent-based enrollment method now uses VMware Workspace ONE Intelligent Hub (formerly known as AWAgent). 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.

To walk through this enrollment workflow, see the article [Enrolling Your Windows 10 Device with a Basic Account](#).

Microsoft Azure Active Directory Enrollment

Workspace ONE UEM integrates with Azure AD, providing a robust selection of onboarding workflows that apply to a wide

vmware ©2021 VMware, Inc.

39

Check Device Root Certificate



ONBOARDING

Ensure that:

- The Device Root Certificate is generated.
- The Device Root Certificate is of type **PFX** and not **CER**.
- The certificate is generated at your Organization Group and **not Global**.
 - Global is sufficient for on-premises users, if issues occur then generate at the Customer Organization Group.

The Device Root Certificate is used for more than just Windows 10, please reach out to your VMware representative to see how generating a new certificate at your OG impacts your environment.

The screenshot shows the 'Settings' window for 'Digital Workspace Tech Zone'. The left sidebar lists categories: System, Advanced, and Devices & Users. Under 'Advanced', 'Device Root Certificate' is selected. The main panel displays the certificate details:

Device Root Certificate ⓘ

ⓘ This certificate is used to authenticate SDK-enabled applications that require certificate based authentication, including authentication for the VMware Tunnel - Proxy service.

Type	Pfx ←
Issued to	O=ws1beta.airwlab.com/Digital Workspace Tech Zone, CN=AwDeviceRoot
Issued by	O=ws1beta.airwlab.com/Digital Workspace Tech Zone, CN=AwDeviceRoot ↑
Valid From	7/11/2018
Valid To	7/11/2038
Thumbprint	6C7703A31E9CC8A0880991F03487DF4C3465160F

EXPORT

Check Agent and Shared Device Settings



ONBOARDING

Intelligent Hub Settings

- ✓ Product Provisioning, BitLocker, Local Enforcement and so on require the Intelligent Hub app.
- ✓ Confirm that the Hub app is published to devices at [Devices & Users > Windows > Windows Desktop > Intelligent Hub App](#).
- ✓ **Note:** For devices that do not support Win32 apps, e.g. HoloLens, Surface Hub, etc., then ensure the Hub push is disabled.

Shared Device Settings

- ✓ 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](#).
- ✓ If this mode is not changed, then users will be prompted for a Group ID after reassignment. This can negatively impact user experience.

Validate Azure AD Settings



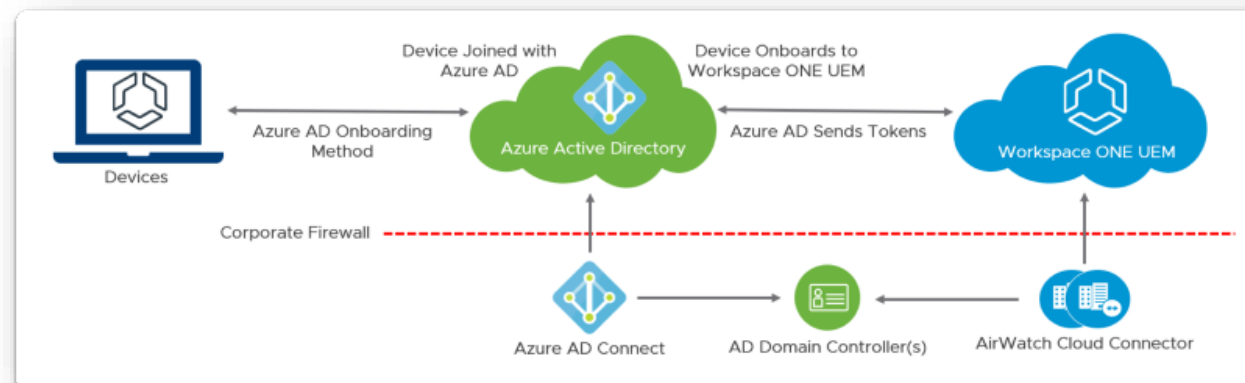
ONBOARDING

Confirm that Azure AD integration is configured in the Workspace ONE UEM console and that the information is correct.

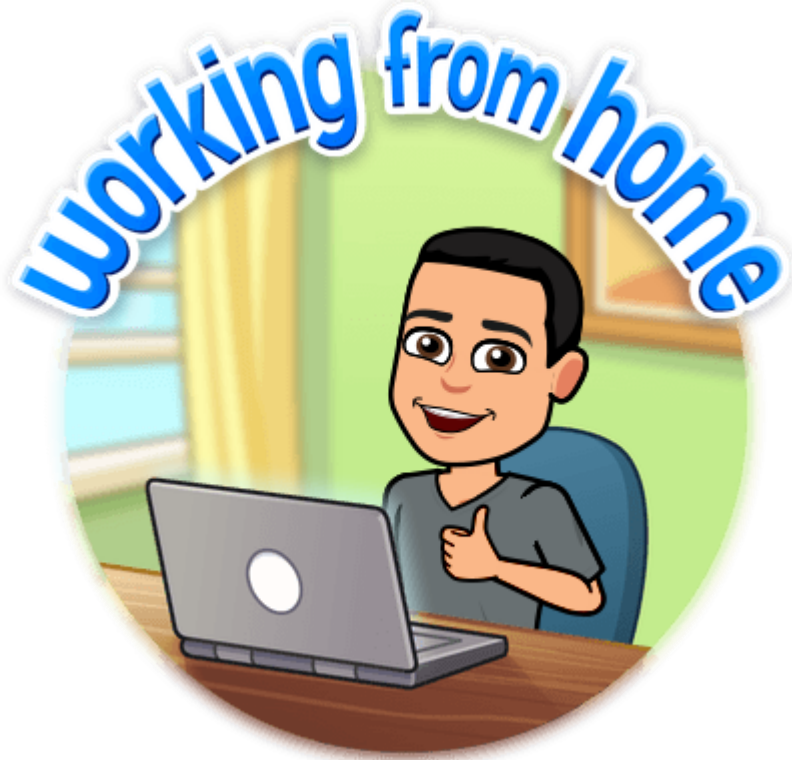
- If you cannot save the Azure AD settings, save the [Directory Services](#) options then enable [User Azure AD for Identity Services](#).

Common Errors:

- Not adding the on-premises app in Azure for URLs other than “.awmdm.com”
- Not matching the Immutable ID Mapping Attribute.
- Not using the correct data type for Immutable ID.
 - Ensure that [Binary](#) is used for objectGUID and [String](#) for any non-GUID value.

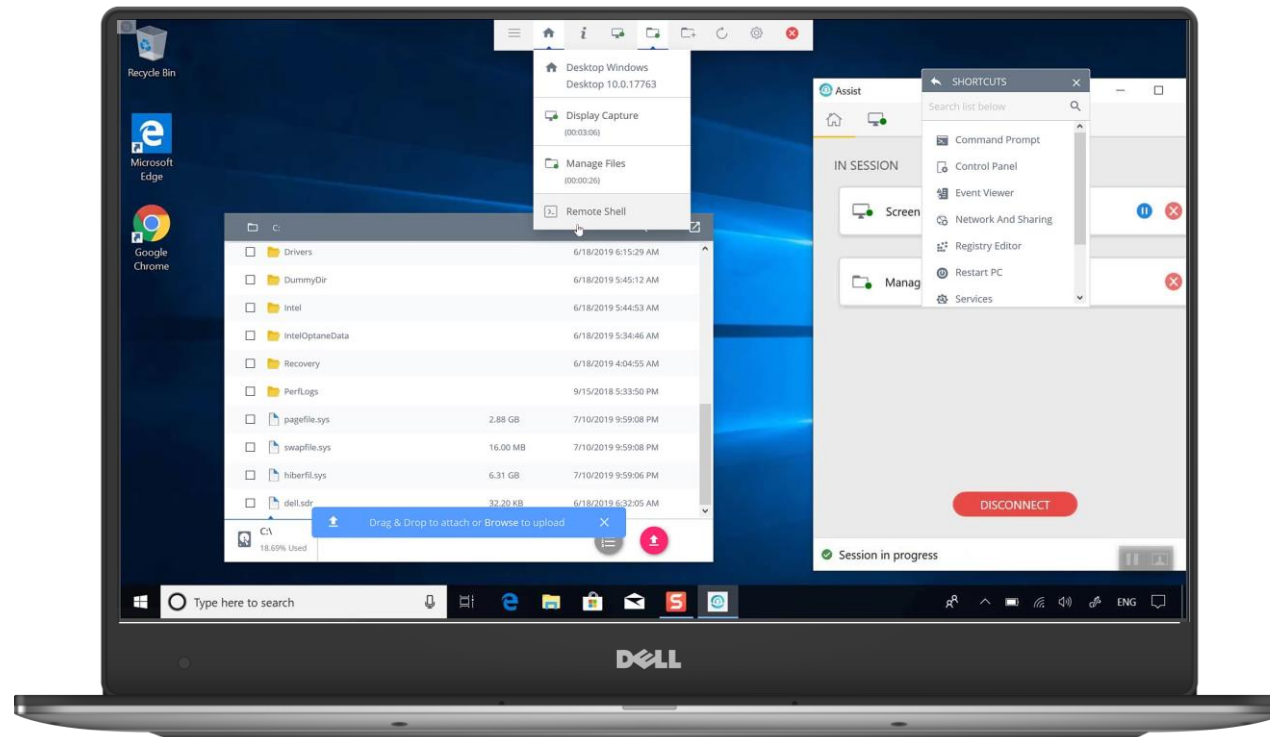


Remote Support



Workspace ONE Assist

Solution Overview



- [View](#) and [control](#) desktops in real-time to quickly assist employees with tasks or issues, directly from the Workspace ONE UEM console
- Notify employees when their screen is visible and enable them to pause a remote session for [enhanced privacy](#)
- Access desktops' [command-line](#) shell to execute Microsoft PowerShell commands, as well as registry and digital signature certificate stores
- Highlight items and guide employees through various tasks with [Screen Draw](#)
- View a virtual, on-screen version of the remote desktop's [keyboard](#) to easily support employees across various keyboard layouts and languages
- [Record](#) remote sessions for escalations and training
- [Chat](#) with remote users and [Invite](#) subject matter experts to on-going remote sessions for quicker resolution of issues

Empower Employees Across the Entire Android, iOS, Windows CE, Windows 10, and macOS Device and App Lifecycle

Troubleshooting & Helpful Hints



REMOTE
SUPPORT

Helpful Hints

Ensure you have deployed the Workspace ONE Assist client to the device and the Workspace ONE UEM console reflects that the client has been installed.

Ensure the Windows 10 device is able to communicate with the Workspace ONE Assist server.

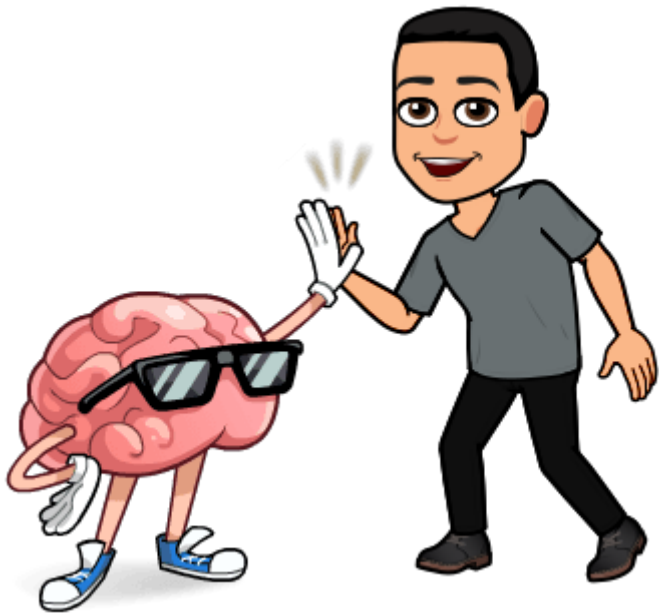
Troubleshooting

Client Logs are located

[%ProgramData%\AetherPal\appcache\Data\Logs](#).

Workspace ONE Assist console logs can be accessed by selecting the information icon, then Logs. You can view and export the console logs.

Digital Employee Experience Management

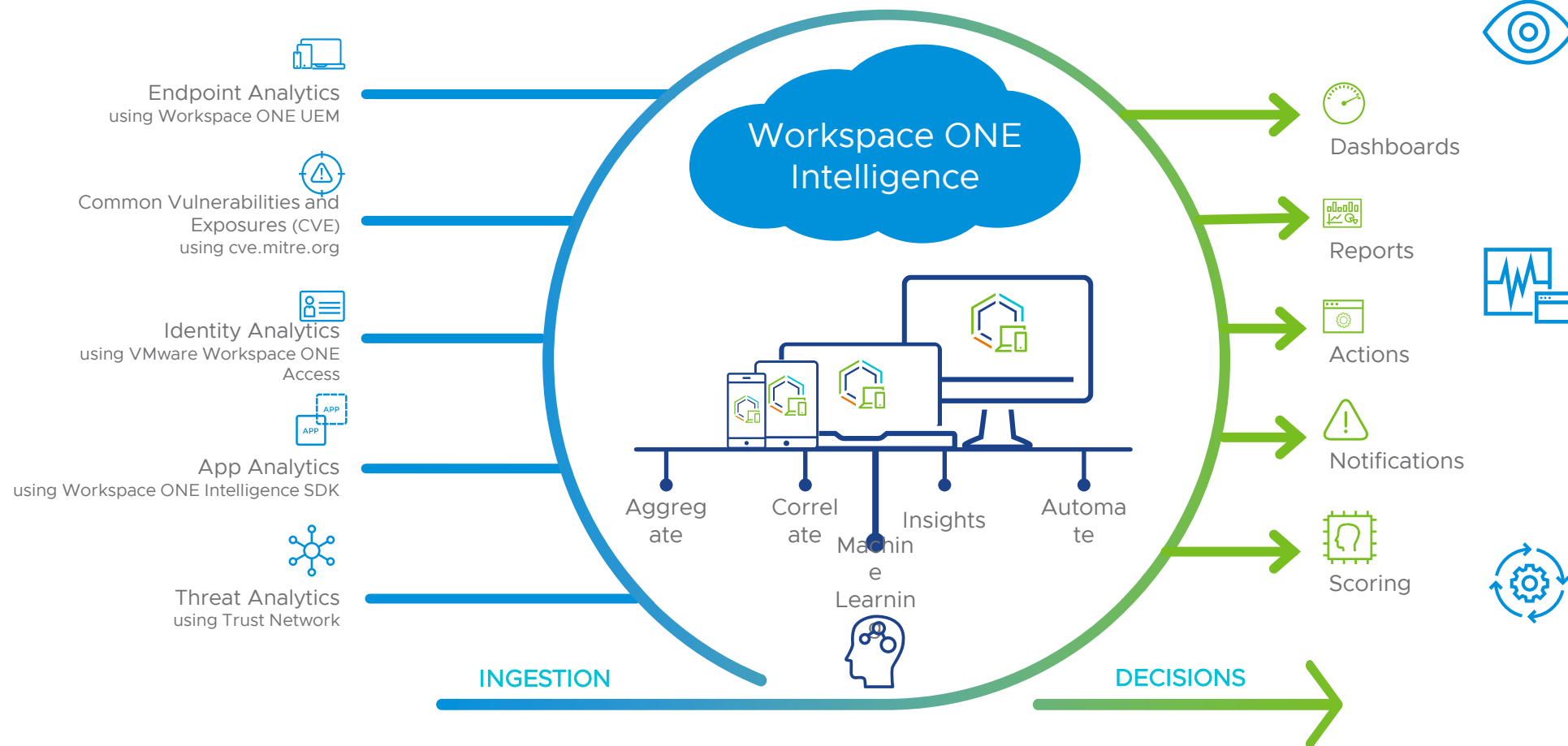


Workspace ONE Intelligence

Insights and automation for the modern digital workspace



EMPLOYEE
EXPERIENCE



Integrated Insights: Get complete visibility into your digital workspace and enable data driven decisions across your entire environment.



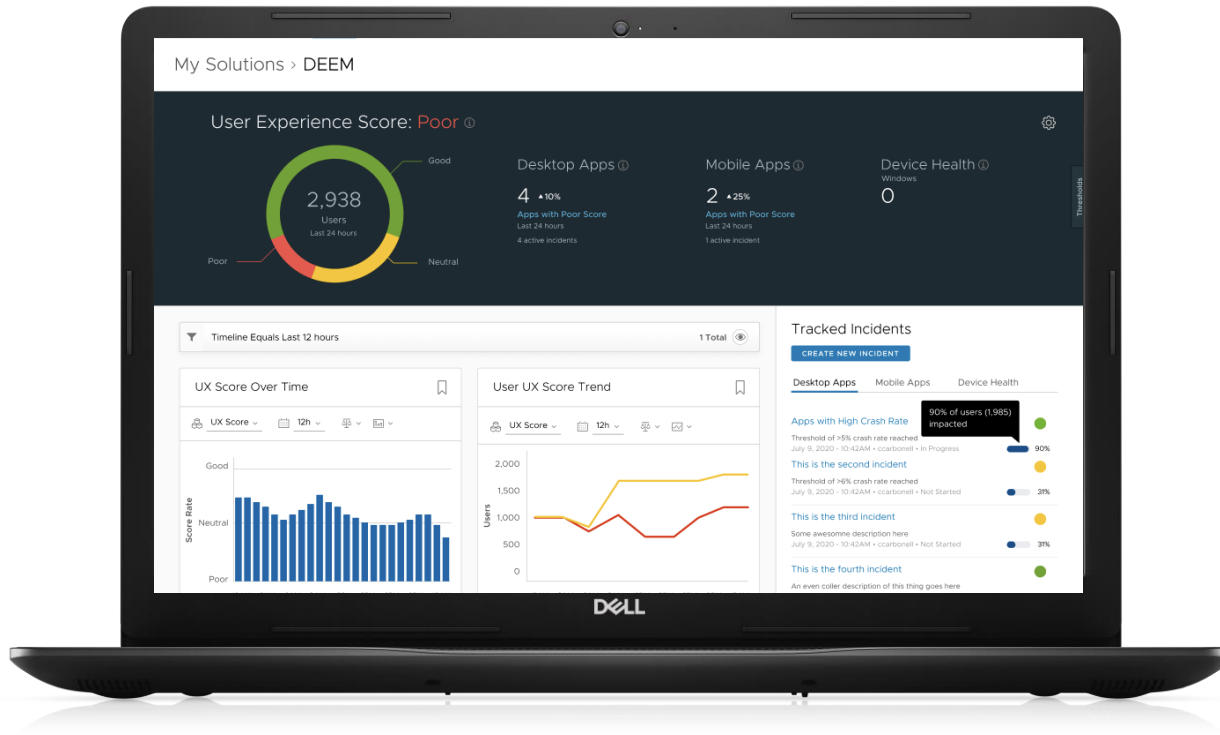
App Analytics: Optimize app development and deployments across the organization to quickly resolve issues, reduce escalations and increase user experience.



Powerful Automation: Automate processes to increase security hygiene across your environment, meet compliance requirements and increase employee productivity.

VMware's Digital Employee Experience Management

Improve employee engagement by creating a seamless digital workspace



Track workspace KPIs impacting digital employee experience **across desktop and mobile**

Get real-time visibility and **proactively identify issues**

Perform **root cause analysis**

Predict potential issues that may arise in the future

Design and automate a fix and notify users

Delight your remote workforce with exceptional employee experience and increased productivity

Digital Employee Experience Platform

Available Event Types for Desktop



EMPLOYEE
EXPERIENCE

Apps	User Actions	Display	Devices	Services	OS Update	Device Perf
<ul style="list-style-type: none">•Application Start•Application Crash•Application Hang•Application Change•Application Exit	<ul style="list-style-type: none">•Logon•Logout•Lock•Unlock	<ul style="list-style-type: none">•Screen Saver On•Screen Saver Off•Sleep•Wake	<ul style="list-style-type: none">•Boot•Shutdown•Unexpected Shutdown•Blue Screen of Death	<ul style="list-style-type: none">•Service Start•Service Stop	<ul style="list-style-type: none">•Patch update•Patch uninstalls	<ul style="list-style-type: none">•CPU Usage•CPU Temp•Memory Fault•Battery Discharge Rate•Hard Drive Remaining space•IOPS

Windows 10 Troubleshooting Cheat Sheet

<https://via.vmware.com/W10CheatSheet>



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.

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/Scripts, Workflows, Baselines, unified app catalog, Hub Services, and Product Provisioning. Communicates using AWCM.
Software Distribution Client (SFC)	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
Windows Notification Service (WNS)	Provides real-time communication for the built-in OMA-DM client.
AirWatch Cloud Messaging (AWCM)	Provides real-time communication for the Workspace ONE Intelligent Hub.
Content Distribution Network (CDN)	Used when downloading apps from Workspace ONE UEM.
Device Health Attestation	Cloud service used for determining device posture, can also be hosted on-premises.
Business Store Portal	Access to apps from the Business Store Portal, also used if pushing online BSP apps.
Azure AD Authentication	Used when leveraging Azure AD for any authentication, including enrollment.
Windows Updates	Endpoint used for Windows Update downloads of apps and OS updates.

Hostnames & Ports

WNS	wins.windows.com over 80443 (IP List - https://via.vmware.com/e10/WNS)
AWCM	awcm#88.awmdm.com:443 (SaaS) and 2001 (On-Premises)
CDN	cdn.awmdm.com:443
has.spserv.microsoft.com	443
bsprints.mp.microsoft.com	443
login.microsoftonline.com	443
mp.microsoft.com	over 80443

For all networking requirements, visit <https://via.vmware.com/W10Endpoints> & <https://ports.vmware.com>.

DEPLOYING PROFILES

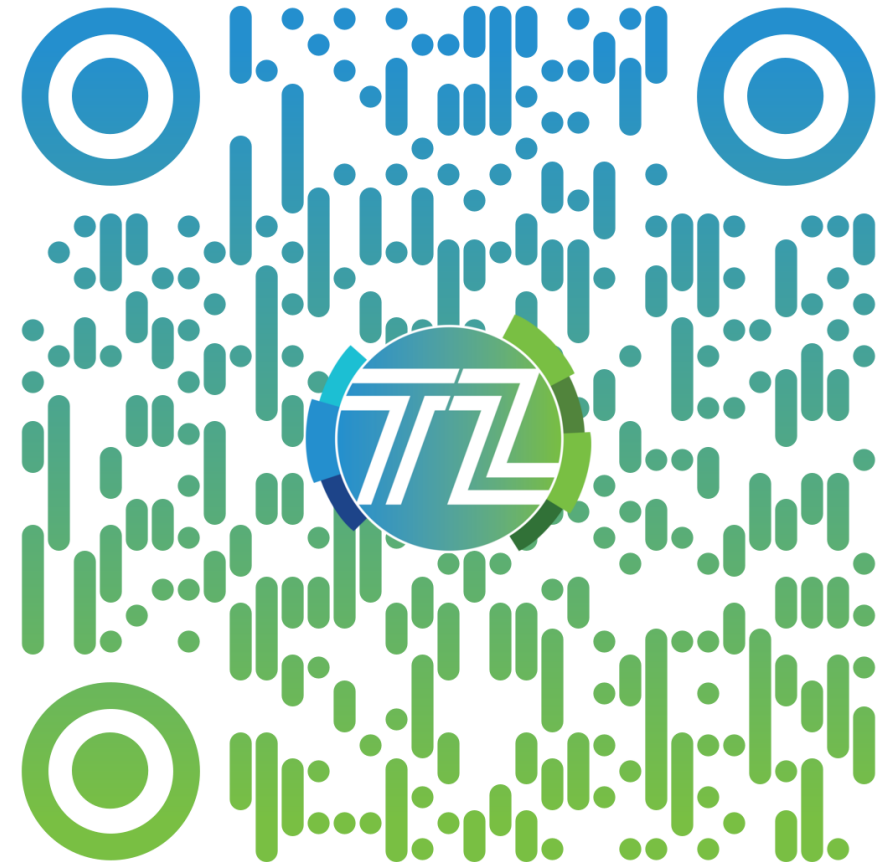
- Check Event Viewer logs for failure message (404): App and Service Logs > Microsoft > Windows > DeviceManagement-Enterprise-Diagnostics-Provider > Admin.
- Confirm that the correct action is used - Add/Replace/Delete/Exec.
- For Custom Settings: <https://via.vmware.com/W10CustomSettings>
 - Check that 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](https://via.vmware.com/SyncMLCodes)
- In Fiddler, check error codes: <https://via.vmware.com/SyncMLCodes>

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-UpdateClient\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 bcaststatus from PowerShell, then run perform, add BranchCache counters, view data using the Report View.





techzone.vmware.com

Your Fastest Path to Understanding,
Evaluating and Deploying VMware Products

Other Tech Zone Sites

go.techzone.vmware.com

CARBON BLACK TECH ZONE

carbonblack.vmware.com

THE CLOUD PLATFORM TECH ZONE

core.vmware.com

NETWORKING AND SECURITY TECH ZONE

nsx.techzone.vmware.com

VMWARE CLOUD TECH ZONE

vmc.techzone.vmware.com



vmworld®
IMAGINE
that



©2021 VMware, Inc.

Thank you!

vmworld[®]
IMAGINE
that