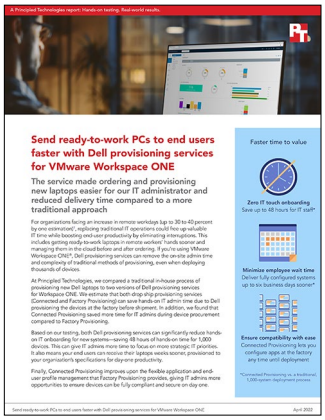

The science behind the report:

Send ready-to-work PCs to end users faster with Dell provisioning services for VMware Workspace ONE

This document describes what we tested, how we tested, and what we found. To learn how these facts translate into real-world benefits, read the report Send ready-to-work PCs to end users faster with Dell provisioning services for VMware Workspace ONE.

We concluded our hands-on testing on April 8, 2022. During testing, we determined the appropriate hardware and software configurations and applied updates as they became available. The results in this report reflect configurations that we finalized on February 15, 2022 or earlier. Unavoidably, these configurations may not represent the latest versions available when this report appears.

Our results

To learn more about how we have calculated the wins in this report, go to http://facts.pt/calculating-and-highlighting-wins. Unless we state otherwise, we have followed the rules and principles we outline in that document.

Table 1: Results of our testing

Time to complete one-time configuration for Workspace ONE orders (hh:mm:ss)	
Completing first order with Connected Provisioning	2:28:36
Completing first order with Factory Provisioning	2:50:42
Time saved using Connected Provisioning rather than Factory Provisioning for the first order	0:22:06
Percentage of time saved using Connected Provisioning rather than Factory Provisioning for the first order	12.9%

Table 2: Results of our testing

Estimated time to complete additional orders with Workspace ONE Connected and Factory Provisioning Orders using previous configuration details (hh:mm:ss)	
Reusing configuration details for additional order with Connected Provisioning (estimated)	0:00:00
Reusing configuration details for additional order with Factory Provisioning (estimated)	0:00:00
Time saved using Connected Provisioning rather than Factory Provisioning for the additional order that resuses configuration details	N/A

Table 3: Results of our testing

Estimated time to complete a new configuration for additional Workspace ONE Connected and Factory Provisioning orders (hh:mm:ss)	
Completing an additional order with a new configuration for Connected Provisioning (estimated)	0:13:31
Completing an additional order with a new configuration for Factory Provisioning (estimated)	2:20:42
Estimated time saved using Connected Provisioning rather than Factory Provisioning for the additional order using a new configuration	2:07:11
Percentage of estimated time saved using Connected Provisioning rather than Factory Provisioning for the additional order using a new configuration	90.4%

Table 4: Results of our testing

On-site admin time required after initial configuration (hh:mm:ss)			
Number of systems	Admin time (traditional method)	Admin time (Factory Provisioning for Workspace ONE)	Admin time (Connected Provisioning for Workspace ONE)
1	0:05:34	0:00:00	0:00:00
2	0:08:26	0:00:00	0:00:00
5	0:17:06	0:00:00	0:00:00
25	1:14:47	0:00:00	0:00:00
100	4:51:07	0:00:00	0:00:00
500	24:04:55	0:00:00	0:00:00
1,000	48:07:10	0:00:00	0:00:00

*We extrapolated values for configuring 25 or more systems. To calculate the extrapolated admin time for large deployments, we used the method of fewest squares to find the line of best fit for the data from our hands-on testing. For the traditional deployment, we determined the equation for the line of best fit was $y = 173.07x + 160.46$, where y was the amount of time required to deploy the system and x was the number of systems. The equation has a correlation coefficient of 0.99.

System configuration information

Table 5: Detailed information on the system we tested.

System configuration information	Dell Latitude 5420
Processor	
Vendor	Intel®
Name	Core® i5-1135G7
Core frequency (GHz)	2.40
Number of cores	4
Cache (MB)	8
Memory	
Amount (GB)	8
Type	DDR
Speed (MHz)	3,200
Graphics	
Vendor	Intel
Model number	Iris® Xe Graphics
Storage	
Vendor	Western Digital
Model Number	PC SN530
Amount (GB)	256
Type	M.2 NVMe SSD
Connectivity/expansion	
Wired internet	1 x 1 GbE Ethernet
Wireless internet	Intel Wi-Fi 6 AX201 2x2 160 MHz
Bluetooth	5.2
USB	1 x USB 3.2 Gen 1 port 1 x USB 3.2 Gen 1 port with PowerShare 2 x Thunderbolt 4 ports (powered)
Video	1 x HDMI 2.0 port
Battery	
Type	Lithium-Ion
Rated capacity (mAh)	3,150
Display	
Size (in)	14"
Type	FHD
Resolution	1,920 x 1,080
Touchscreen	No

System configuration information	Dell Latitude 5420
Operating system	
Vendor	Microsoft
Name	Windows 10
Build number or version	10.0.19043
BIOS	
BIOS name and version	Dell Inc 1.11.2
Dimensions	
Height (in)	.76
Width (in)	12.65
Depth (in)	8.35
Weight (lbs.)	3.03

How we tested

Report methodology overview

Our aim was to show three different methods of deployment: Connected Provisioning, Factory Provisioning, and a traditional process using Microsoft Endpoint Manager (formerly SCCM). To do this, we configured the basic tools for our local Configuration Manager Environment and our VMware Workspace ONE unified endpoint manager (UEM) environment. This included setting up the devices, adding applications, managing drivers and updates, and validating deployments. After completing all necessary configuration steps, we captured times for placing an order using each provisioning type. These steps included the following:

- Connected Provisioning
  - Attending an introductory meeting with the Dell team
  - Creating system tags in Workspace ONE
  - Assigning the tag to a Smart Group
  - Assigning applications to the Smart Group
  - Accepting the Connected Provisioning invitation in TechDirect
  - Creating a deployment profile in TechDirect
  - Completing the Export Compliance form
  - Attending a readiness assessment meeting
  - Capturing screenshots to verify settings with Dell engineering
  - Approving the technical specifications document
  - Attending the readiness review
  - Associating our completed order with the profile
- Factory Provisioning
  - Attending an introductory meeting with the Dell team
  - Completing the Export Compliance Form
  - Preparing the provisioning package file (PPKG)
  - Downloading the PPKG
  - Copying the PPKG to the verification VM
  - Running the PPKG validation
  - Validating the PPKG installation (OOBE)
  - Installing the Dell File Transfer software
  - Starting the file transfer
  - Completing the file transfer
  - Approving the technical specifications document
- Traditional process
  - Unboxing and powering on the devices
  - Starting the OS installation on the first device
  - Deploying Windows 10 and applications using task sequence
  - Initiating the first-time boot and applying updates
  - Repackaging the devices
  - Weighing the devices
  - Creating shipping labels
  - Printing and applying shipping labels

Infrastructure overview

The different provisioning methods shared infrastructure. Connected Provisioning and the traditional process required an Active Directory (AD) server, which the two services shared. Connected and Factory Provisioning required a Workspace ONE UEM console, which the two services shared.

For our Connected and Factory Provisioning environments, we used the Workspace ONE console. We configured our Workspace ONE UEM settings, installed the AirWatch Cloud Connector to connect our local AD server, and added applications and profiles for distribution to our provisioning devices. Then we added the necessary components to integrate our Workspace ONE environment with our local AD server.

Connected Provisioning requires ordering at least 200 system per year. For the purposes of this study, Dell waived that requirement.

Our local environment consisted of one server installed with VMware vSphere 7.0. We installed one Microsoft Windows Server 2022 AD server VM named "DC01" with Domain Name Service (DNS) and Dynamic Host Configuration Protocol (DHCP) roles installed on it. We also installed a management server (site server VM) named "Deployment" with Microsoft Endpoint Configuration Manager version 2111 (formerly known as SCCM) and Microsoft SQL Server 2019 Enterprise Evaluation Edition.

We used the following volumes on the DC01 VM:

- OS volume (40 GB)
- General sharing for CIFS (40 GB)

We used the following volumes on the Deployment VM, which was our Microsoft Endpoint manager:

- OS and Configuration Manager installation - 300 GB thin-provisioned
- DB - 200 GB thin-provisioned
- Logs - 40 GB thin-provisioned
- Backup - 40 GB thin-provisioned

After we installed Endpoint Manager, we installed the following roles to the VM:

- Component server
- Distribution point
- Service connection point
- Fallback status point
- Management point
- Site server
- Site database server (database)
- Site database server (transaction log)

Required installation media

We acquired the relevant installation media and keys for the following items:

- Microsoft Endpoint Configuration Manager 2103 - mu_microsoft_endpoint_configuration_manager_current_branch_version_2103_x86_x64_dvd_77e1425b
- SQL Server 2019 Enterprise Core - en_sql_server_2019_enterprise_core_x64_dvd_5e1ecc6b
- Windows 10 Enterprise x64

Application details

We deployed applications using either Workspace ONE or Configuration Manager. Microsoft Office requires separate steps for both environments, so we've included those steps in our methodology that follows Table 6.

Table 6: Details for the applications we installed on the devices.

Product	Filename	Install command	Uninstall command	URL
Google Chrome	GoogleChromeStandaloneEnterprise64.msi	msiexec /i "GoogleChromeStandaloneEnterprise64.msi" /qn	msiexec /x {27AE757E-4286-3D70-ACB1-4FEAC2F15FB9} /q	https://chromeenterprise.google/browser/download/#windows-tab
Notepad ++	Notepad++7_9_1.msi	msiexec /i "Notepad++7_9_1.msi" /q	msiexec /x {84AB9486-65EF-402E-B061-B128FBCEF91B} /q	https://sourceforge.net/projects/notepadmsi/
Slack	slack-standalone-4.23.0.0.msi	msiexec /i "C:\slack-standalone-4.23.0.0.msi" /qn	msiexec /x {9B7C2512-8A00-4207-8A9E-F837271B2524} /q	https://slack.com/help/articles/212475728-Deploy-Slack-via-Microsoft-Installer
VLC Media Player	vlc-3.0.16-win64.msi	msiexec /i "C:\vlc-3.0.16-win64.msi" /qn	msiexec /x {1BB20266-7C52-4909-B075-22156F75D22C} /qn	https://get.videolan.org/vlc/3.0.16/win64/vlc-3.0.16-win64.msi
Zoom	ZoomInstallerFull.msi	msiexec /i "C:\ZoomInstallerFull.msi" /qn	msiexec /x {1B8D4A17-201A-4113-A512-B7DEEF293AF1} /q	https://zoom.us/client/latest/ZoomInstallerFull.msi

Preparing the Configuration Manager environment

Creating a Microsoft Windows 2019 VM template

1. From VMware vCenter, boot the VM to the Windows Server 2019 installation media.
2. At the prompt to boot from the CD/DVD location, press any key.
3. Click Next.
4. Click Install now.
5. Click Windows Server 2019 Datacenter Edition (Desktop Experience), and click Next.
6. Click the checkbox beside I accept the license terms, and click Next.
7. Click the OS drive, and click Next.
8. After installation, enter a password for the Administrator, and click Finish.
9. Boot to Windows, and log in.
10. Disable the firewall, IE enhanced security, and auto logoff with group policy objects.
11. Install VMware tools.
12. In your VM's hardware, ensure that you are using VMXNET3 for the Network Adapter and VMware Paravirtual for the SCSI controller.
13. Select Windows Update, patch to the latest updates, and disable Windows Update.
14. Sysprep the device using the following command.
    - C:\Windows\System32\Sysprep.exe /generalize /oobe /shutdown /unattend
15. Close the server VM.
16. Clone and create "DC01" and "Deployment" VMs, and add necessary disk space as outlined in the Overview section.

Installing and configuring AD and DNS on the DC01 VM

1. To install Windows remote tools on the AD VM, open a PowerShell window, and run the following command:

```
Install-WindowsFeature RSAT-ADDS
```

2. When the installation finishes, close PowerShell.
3. Open Server Manager.
4. On the Welcome screen, click Add roles and features.
5. At the Before you begin screen, click Next three times.
6. At the Server Roles screen, select Active Directory Domain Services.
7. In the pop-up window, click Add features.
8. Click Next three times.
9. Verify the roles are correct, and click Install.
10. Once installation finishes, close the Add roles and features wizard.
11. At the top of the screen in Server Manager, click the flag, and select Promote this server to a domain controller.
12. Select Add a new forest, enter a root domain name, and click Next. We chose the name `test.local`.
13. On the Domain controller options screen, enter a password, and click Next.
14. On the DNS Options screen, click Next.
15. On the Additional Options screen, click Next.
16. On the Paths screen, click Next.
17. On the Review Options screen, click Next.
18. On the Prerequisites screen, verify all prerequisites have passed, and click Install.
19. Once AD Domain Services finishes installing, click Finish, and restart the system.
20. Open DNS by typing `dnsmgmt.msc` in a command prompt.
21. Traverse the DNS entries to reverse lookup, right-click, and select new zone.
22. Select primary zone, and click Next
23. Click to select all DNS servers running on domain controllers in this forest, and click Next.
24. Click IPv4 Reverse lookup, and click Next.
25. Enter an appropriate IP address range. For example, `192.168.0.x`.
26. Select Allow only secure updates, click Next, and click Finish.

Customizing Active Directory

1. Configure Active Directory users and computers, and edit the Domain Administrator account to never expire.

Installing DHCP on the DC01 VM

1. Open Server Manager.
2. On the Welcome screen, click Add roles and features.
3. At the Before you begin screen, click Next three times.
4. At the Server Roles screen, select DHCP Server.
5. In the pop-up window, click Add features.
6. Click Next three times.
7. Verify the desired role will install, and click Install.
8. Once installation finishes, close the Add roles and features wizard.
9. At the top of the screen in Server Manager, click the flag, and select Complete DHCP configuration.
10. In the DHCP Post-Install configuration wizard window, click Next.
11. At the Authorization screen, click Commit.
12. At the Summary screen, click Close.

Configuring DCHP on the DC01 VM

1. In Administrative Tools, open the DHCP service.
2. Expand test.local, right-click IPv4, and select New Scope.
3. In the New Scope Wizard window, click Next.
4. At the scope name screen, name the scope `Laptops`, and click Next.
5. In the IP Address Range, enter the desired scope settings for your network.
6. Click Next four times.
7. At the Router screen, enter the gateway address that the clients will use, and click Next.
8. Click Next three times.
9. At the Completing the New Scope Wizard screen, click Finish.
10. With the administrator@test.local account added as an administrator, join the Configuration Manager and Deployment VM to the test.local domain.
11. Log into the target server using the administrator@test.local user.

Creating the system management container

1. On the AD VM, open a command window, and run the following:

```
ADSI edit
```

2. On the toolbar, click Action → Connect to….
3. To accept the defaults, click OK.
4. Under Default Naming Context → DC=test, DC=local, right-click the System container, and click New → Object….
5. Select Container, and click Next.
6. Under Value, enter System Management, click Next, and click Finish.

Setting permissions for Configuration Manager on the DC01 VM

1. Open Active Directory Users and Computers.
2. On the toolbar, select View, and click Advanced features.
3. Under test.local → System, right-click Endpoint Configuration Manager, and click Delegate control.
4. Click Next.
5. Click Add.
6. Click Object types, click Computers, and click OK.
7. Enter the computer account for the Endpoint Configuration Manager server as an object name, add the domain administrator account, and click OK.
8. Click Next.
9. Select Create a custom task to delegate, and click Next.
10. Choose This folder, existing objects…, and click Next.
11. Click Full Control, and click Next.
12. Click Finish.

Extending the AD schema on the DC01 VM

To publish key information in a secure location, we needed to extend the AD schema for Configuration Manager. The extended schema helps for process deploying as well as for setting up clients and additional services that the Configuration Manager site system roles provide.

1. Extract the contents of Configuration Manager installation media to the DC01 AD VM.
2. From the installation media, navigate to \SMSSETUP\BIN\X64, right-click extadsch, and run as administrator.
3. To confirm the operation was successful, review extadsch.log at the root of the system drive. If successful, the log will include Successfully extended the Active Directory schema.

Setting up the Configuration Manager server on the deployment VM

Installing required roles

1. Create a deployment share at the root of the installation drive with read and write permissions for everyone. We named our deployment share.
2. Verify that the share is accessible. Our share location was \\deployment.test.local\deploymentshare.

Installing required roles

1. Log onto the Endpoint Configuration Manager server.
2. In an elevated PowerShell terminal, run the following commands:

```
Set-ExecutionPolicy Unrestricted
Import-module ServerManager
Add-WindowsFeature Web-Common-Http,Web-Static-Content,Web-Default-Doc,Web-Dir-Browsing,Web-Http-
Errors,Web-Http-Redirect,Web-Asp-Net,Web-Net-Ext,Web-ASP,Web-ISAPI-Ext,Web-ISAPI-Filter,Web-
Http-Logging,Web-Log-Libraries,Web-Request-Monitor,Web-Http-Tracing,Web-Basic-Auth,Web-Windows-
Auth,Web-Url-Auth,Web-Filtering,Web-IP-Security,Web-Stat-Compression,Web-Mgmt-Tools,Web-
WMI,RDC,BITS -Restart
```

Installing the Windows 10 Assessment and Deployment Kit (ADK) on the deployment VM

For additional information around the Windows ADK, review the documentation at https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install. The site contains the latest versions for both installations.

1. Download the Windows Assessment and Deployment Kit for Windows 10 from https://go.microsoft.com/fwlink/?linkid=2165884.
2. Click the executable adksetup.exe.
3. Click Next twice.
4. Accept the licensing agreement.
5. On the Select the features you want to install screen, select the following features, and click Install:
   - Deployment Tools
   - Imaging and Configuration Designer (ICD)
   - Configuration Designer
   - User State Migration Toll (USMT)
6. Using the link above, download the Windows PE add-on for the ADK.
7. Specify location, and click Next.
8. Select the following features to install:
   - Deployment Tools
   - Imaging and Configuration Designer (ICD)
   - Configuration Designer
   - User State Migration Tool (USMT)
9. Click next, and click Close.

Installing the Windows ADK Windows Preinstall Environment add-ons – Windows 10 on the deployment VM

1. Download adkwinpesetup.exe from https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install.
2. Run adkwinpesetup.exe.
3. Accept the default locations, and click Next.
4. Select Windows Preinstallation Environment (PE), click Install, and click Close.

Installing Microsoft SQL Server 2019 on the deployment VM

1. Log into the deployment Configuration Manager VM as `administrator@test.local`.
2. Attach the installation media for SQL 2019 enterprise core, and run the setup.exe file.
3. In the SQL Server Installation Window, from the left menu, select Installation, and select New SQL Server stand-alone installation or add features to an existing installation.
4. In the SQL Server 2016 Setup Window, select the evaluation edition.
5. On the License Terms page, accept the terms, and click Next.
6. On the Microsoft Update screen, check the box for Use Microsoft Update to check for updates, and click Next.
7. On the Feature Selection screen, under Instances Features, select Database Engine Services and locations for your instance root and Shared Features directory, and click Next. We used our second virtual volume.
8. On the Instance Configuration screen, select Default Instance, and leave the default Instance ID.
9. On the Server Configuration screen, set Startup Type to Automatic for all four services. Select Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service.
10. Select Collation.
11. In Collation, verify that the Database Engine is set to SQL_Latin1_General_CP1_CI_AS, and click Next.
12. In Database Engine Configuration, select mixed authentication mode.
13. Under Specify SQL Server administrators, click Add Current User, and click Add.
14. Add the Configuration Manager Admins group, and click OK.
15. In Data Directories, verify that the additional data drive is listed as the Data root directory.
16. In TempDB, enter the following settings:
    - Number of files: `1`
    - Initial size (MB): `1,024`
    - Autogrowth (MB): `512`
    - Data directories: [use default]
    - Initial size of TempDB log file (MB): `1,024`
    - Autogrowth (MB): `512`
    - Log directory: [use default]

17. In Memory, select Recommended. For Min Server Memory (MB), type `8,192`, and for Max Server Memory (MB), type `16,384`.
18. Click Next.
19. In Ready to Install, review your settings, and click Install.
20. Click Next.
21. At Ready to Install, run the SP2CU6 SQL server update.
22. Run Windows updates.

Installing Report Viewer and the SQL Server Management Studio on the deployment VM

1. Download the Report Viewer from https://www.microsoft.com/en-US/download/confirmation.aspx?id=6442, and install using all defaults.
2. In the SQL Server Installation Center, select Install SQL Server Management Studio.
3. Click the link to Download SQL Server Management Studio (SSMS).
4. From your Downloads folder, run SSMS-Setup-ENU.exe.
5. In the Microsoft SQL Server Management Studio installation wizard, click Install.
6. To restart your server after the installation completes, click Restart.

Changing SQL service to start as local system

1. Open SQL Server Configuration Manager.
2. Under SQL Service Services, right-click the SQL Server instance, and click Properties.
3. For Log on as, select Built-in account, and Local System. Click OK, and click Restart.

Installing Windows Server Update Services role on the deployment VM

1. Open Server Manager.
2. Click Add Roles and Features.
3. Select Windows Server Update Services, and click Next.
4. Uncheck WID Connectivity, select SQL Server Connectivity, and click Next.
5. Select an appropriate directory for Windows updates. We used \\deploy\wsusupdates\.
6. On the database instance selection screen, enter the database server name, and click Check Connection. Ensure you see the Successfully connected to server message, and click Next
7. Click Install.
8. Click Close.

Installing Endpoint Configuration Manager update 2002 on the deployment VM

1. Sign into the Endpoint Configuration Manager VM using the administrator@test.local account.
2. Attach the Configuration Manager update 2002 Installation media to the management server.
3. Open splash.hta.
4. Click Install.
5. Read Before You Begin, and click Next.
6. Choose Install a primary site.
7. Choose Use typical options.
8. Enter the product key, enter a Software Assurance Date, and click Next.
9. Check the boxes to accept the License Terms, and click Next.
10. Enter a path for the prerequisite file downloads, and click Next. We used User\Downloads\ConfigMgr.
11. Select a language, and click Next for both server and client.
12. On the Site and Installation Settings screen, enter a site code for the primary site and site name, and click Next. We used PTL and PTlabs, respectively.
13. On the Primary Site Installation screen, select Install the primary site as a stand-alone site, and click Next.
14. On the Database Information screen, leave the defaults, and click Next.
15. On the Database Information screen, click Next.
16. On the SMS Provider Settings screen, click Next.
17. On the Client Computer Communications Settings screen, select Configure the communication method on each site system role. Select Clients will use HTTPs when they have a valid PKI certificate…, and click Next.
18. On the Site System Roles screen, for client connections for both the management and distribution points, select HTTP. Click Next.
19. On the Diagnostic and Usage Data screen, click Next.
20. On the Service Connection Point Setup screen, click Next.
21. On the Settings Summary screen, click Next.
22. Click Install.

Enabling the PXE service on the distribution point on the deployment VM

1. Open Configuration Manager → Administration → Distribution points, and right-click Properties.
2. Navigate to PXE. Select the following, and click OK:
   - Enable PXE support for clients
   - Allow distribution point to respond to incoming PXE requests
   - Enable unknown computer support
   - Enable a PXE responder without Windows Deployment services

Adding a network access account

1. In the Configuration Manager console, navigate to Administration → Site Configuration → Sites.
2. Right-click the target site, and under Configure Site Components, select Software Distribution.
3. To add a new user, select Existing account in Network access account, and click the star.
4. Select the domain administrator account, and click OK twice.

Importing Windows 10 software for .wim creation on the deployment VM

1. On the Endpoint Configuration Manager VM, launch the Configuration Manager console.
2. Navigate to Software Library → Overview → Operating Systems Images.
3. Right-click Operating systems images, and click Add Operating System Image.
4. On the Data Source page, specify the path to Windows 10 2004 install.wim file. Note: This must be a UNC path to a file share. We used DC01.
5. Select 3 - Windows enterprise and x64, and Click Next.
6. Enter the image details for reference.
7. Click Next twice.
8. Close Add Operating System Wizard.

Creating a Windows 10 .wim file

1. Extract the Windows 10 installation ISO.
2. Find the index number of your image:

```
dism /Get-ImageInfo /ImageFile:[extracted win10 image root]\sources\install.wim"
```

3. Mount the package:

```
dism /mount-wim /wimfile:" [extracted win10 image root]\\sources\install.wim" /index:3 /
mountdir:"C:\Mount"
```

4. Add the update packages:

```
dism /Add-Package /Image:"C:\Mount" /PackagePath="C:\UpdateTools\UpdatePackages" /LogPath="C:\
UpdateTools\update.log"
```

5. Commit changes to the image:

```
dism /Unmount-wim /mountdir:"C:\Mount" /commit
```

6. Add computer account to Full Control of System Management Container.
7. Add computer account to the local administrator group for the site server.
8. Create a boundary and boundary group.

Importing application files to Configuration Manager

1. Download the application installer file, and copy it to the DC01 network share. For URLs, see Table 6.
2. In Configuration Manager, navigate to Open software library → Overview → Application Manager → Applications → Create new application.
3. In the Create Application Wizard, select Automatically detect information about this application from installation files, and click Browse for location.
4. Navigate to the share location, and select the relevant .msi file for the target application, and click Open. For example, we used \\[deployment server]]\deployment \applications\Chrome\GoogleChromeEnterpriseBundle64\Installers\ GoogleChromeStandaloneEnterprise64.msi for the Chrome installation.
5. Click Next.
6. In View imported information, click Summary.
7. In Summary, click Next.
8. Click Close.
9. Right-click the application, and select Distribute Content.
10. On the Distribute Content Wizard, click Next.
11. On the Content screen, click Next.
12. On the Content Destination screen, select Add, and select the target distribution point. Click Okay, and click Next.
13. On the Summary Screen, click OK.
14. Right-click the target application, and click Properties.
15. Select Allow this application to be installed from the Install Application task sequence action without being deployed.
16. For each of the following applications, complete steps 1 through 15:

    - Chrome
    - Notepad++
    - Slack
    - VLC media player 3.0.16 (64-bit)
    - Zoom

Note: We later refer to steps 9 through 15 as the Application Distribution steps.

Creating an Office 365 application package on the deployment VM

1. Click Software Library → Office 365 Client Management → Office 365 installer.
2. Name the package, select a location, and click Next.
3. Select the following, and click Next:

    - x64
    - Office 365
    - Office plus
    - Semiannual update
    - Newest version available
    - English

4. Accept the EULA.
5. Do not include Access, OneDrive, Skype for business (Groove), and publisher.
6. Click Finish and Submit.
7. To distribute the Office 365 content, complete the Application Distribution steps.

Creating a driver share on the deployment VM

1. On the Configuration Manager server, open File Explorer.
2. At the root of C:\, create a folder called `Drivers`.
3. Right-click the newly created folder, select Give access to, and select Specific People.
4. In the Network Access window, type `everyone`, and click Add.
5. Select Everyone, change Permissions Level to Read/Write, and click Share.
6. In the Configuration Manager Console, on the Software Library panel, Under Operating Systems, select Driver Packages.
7. In the toolbar, click Create Driver Package.
8. In the Create Driver Package window, type `DriverPackage01`. Click Browse.
9. Browse to the deployment server, and select the shared Drivers folder.
10. Create a new folder called `DriverPackages`. Select the DriverPackages folder, and click OK.
11. Click OK.
12. Right-click the new Driver package, and select Distribute Content. To distribute to the Deployment nodes, complete the prompts. Before continuing, wait until the package shows as distributed.

Adding drivers to the prepared task sequence for a new system

We downloaded the drivers for our testing from https://www.dell.com/support/kbdoc/en-us/000181846/latitude-5420-windows-10-driver-pack and added the drivers to our deployment share.

1. In Software Library, in Configuration Manager, under Operating Systems, select Drivers.
2. In Home, in the toolbar, click Import Driver.
3. Click Browse, and navigate to the Driver Share. Select the folder containing the drivers, and click OK.
4. Click Next.
5. Once the system finishes validating the driver information, verify that you've included the correct drivers, and click Next.
6. Select the Driver Package added earlier, and click Next. When asked to update the distribution points, click Yes.
7. Select the Boot image (x64), select to include only updates to the Boot Image, and click Yes. When asked to update the distribution points, click Yes twice.
8. In Summary, click Next.
9. Once complete, click Finish.

Creating a Configuration Manager task sequence to deploy Windows 10 on the deployment VM

1. Launch the Configuration Manager console.
2. Navigate to Software Library → Overview → Operating Systems → Task Sequences.
3. Right-click Task Sequences, and click Create Task Sequence.
4. Select Install an existing image package, and click Next.
5. Specify a task sequence as `windows 10 x64`, select Run as high performance power plan, and click Next.
6. Select the image.
7. Select Partition, and before installing the operating system, format the target computer. Deselect Configure task sequence for use with Bitlocker. Enable the administrator account, enter an administrator password, and click Next.
8. Specify the domain, OU, and administrator account, and click Next.
9. Select the Configuration Manager client you want, and click Next.
10. In State Migration, deselect all configuration state migration boxes, and click Next.
11. Do not include any software updates, and click Next.
12. On the Install Application screen, click the Add button.
13. Add the Slack, click OK, and click Next.
14. Confirm the settings, and click Next.
15. Click Close.

Editing the task sequence on the deployment VM

1. Open software library → Overview → Operating System → Task sequence.
2. Right-click the new sequence, and rename it `Windows x64 Traditional Deployment`.
3. Right-click the new sequence, and select Edit.
4. Add task sequence items, and reorder the tasks so that the sequence matches our Task Sequence below. Click OK.

Deployment task sequence

- Restart in Windows PE.
- Partition Disk 0 – BIOS.
- Partition Disk 0 – UEFI.
- Apply operating system.
- Apply Windows settings.
- Apply network setting.
- Apply device drivers.
- Setup Windows and Configuration Manager.
- Install Software Updates (to add this step, click Add. Under Software, navigate to Install Software Updates.).
- Select Install Software Updates, and for type of software update deployment, select Available. From cached scan results, deselect Evaluate software updates.
- Install applications.
- Restart computer (To add this step, click Add. Under General, navigate to Restart Computer.).
- For Specify what to run after restart - select the currently installed default operating system.
- Select Restart computer, and deselect Notify the user before restarting.

Deploy the task sequence to unknown systems

1. Right-click the deployment task sequence, and select Deploy.
2. In the Deploy Software Wizard, for Collection, click Browse.
3. Select All Unknown Computers, and click OK.
4. Click Next.
5. For Purpose in Deployment Settings, select Required, and for make available to the following, select Only media and PXE.
6. In Scheduling, enable Schedule when this deployment will become available, and create a new assignment for Assign immediately after this event and As soon as possible. Click Summary.
7. Click Next and Close.

Note that we completed steps 1 through 7 between each new system deployment.

Configuring the Workspace ONE UEM Console

Configuring our Workspace ONE Account

To configure our Workspace ONE account, we purchased a domain and connected it to an email service. We validated the email in Workspace ONE and completed the following tasks:

- Connect to Workspace ONE Access
- Auto-discovery
- Mobile single sign-on

Installing the Workspace ONE Cloud Connector

1. From your AD server, in the Workspace ONE UEM console, navigate to Groups and Settings → All Settings → System → Advanced → Site URLs.
2. Under AirWatch Cloud Messaging (AWCM), verify that Enable AWCM Server is enabled. Note the AWCM Server External Hostname.
3. To verify connectivity to the AWCM server, click Test Connection. Close the settings page.
4. Under Workspace ONE and AirWatch Cloud Connector (ACC) and Directory in Getting Started, click Configure.
5. Under Downlaod Installer in ACC and Directory, enter a Password for the ACC certificate. Confirm the password, and click Continue.
6. Once downloaded, run the AirWatch Cloud Configuration.
7. On the AD server, run the AirWatch Cloud Connector 21.9.0.0 Installer.
8. In the AirWatch Cloud Connector Installation Wizard, click Next.
9. Accept the License Agreement, and click Next.
10. Accept the Default Destination Folder, and click Next.
11. Enter the Certificate Password you used in step 5, and click Next.
12. Do not designate an outbound proxy, and click Next.
13. At the popup for adding registry keys for TLS 1.2, click OK.
14. Once complete, click Finish, and to reboot the VM, click Yes.
15. In the Workspace ONE UEM console, navigate to Groups and Settings → System → Enterprise Integration → Cloud Connector.
16. On the bottom of the page, click Test Connection, and verify that the Connector functions as expected.

Changing settings for the Workspace ONE account

1. From the Workspace ONE UEM console, navigate to Groups and Settings → Devices & Users → Windows → Windows Desktop → Staging & Provisioning.
2. For Workspace ONE Drop Ship Provisioning under the Workspace ONE Drop Ship Provisioning section, select Enable. Note that this affects both Factory and Connected Provisioning services.

Adding Applications in Workspace ONE

1. From the Workspace ONE UEM console, navigate to Apps and Books → Applications → Native.
2. Click Add → Application File.
3. Click Upload.
4. On the Add screen, click Choose File.
5. Navigate to the target application, and select the target file. Click Okay.
6. Click Save.
7. On the Application screen, click Save & Assign.
8. On the Assignment screen, click Next. (We did not create an assignment at this time.)
9. On the View Assignment screen, click Publish.

Creating the Office 365 application package for Workspace ONE

1. On the Deployment server, create a working folder. We used `C:\Office`.
2. Navigate to config.office.com, and create an XML file. We provide our example configuration.xml file below. Copy the configuration.xml file to the root of the working folder.
3. Download the Office Deployment Tool from https://www.microsoft.com/en-us/download/details.aspx?id=49117.
4. Extract the files to the working folder.
5. Create a new file named `Download.cmd`, and add the following code:

```
@echo off
pushd %~dp0
echo Downloading Office 365 Pro Plus Retail x64 source files
setup.exe /download configuration.xml
```

6. To begin the download, double-click Download.cmd.
7. Create a new file named `uninstall.xml`, and include the following code:

```
<Configuration>
<Remove>
<Product ID="O365ProPlusRetail">
<Language ID="en-us"/>
</Product>
</Remove>
<Display Level="None" AcceptEULA="TRUE"/>
</Configuration>
```

8. Once complete, compress the working folder into Office.zip.

Adding Office 365 to Workspace ONE

1. From the Workspace ONE UEM console, navigate to Apps and Books → Applications → Native.
2. Click Add → Application File.
3. Click Upload.
4. On the Add screen, click Add.
5. Navigate to and select the Office.zip file. Click Okay.
6. Click Save.
7. On the Application screen, configure the following application details, and click Save & Assign:
   - For the Supported Processor Architecture, select 64-bit.
   - For App Uninstall Process in Files, select Input for the Custom script type. For Uninstall Command, type `setup.exe /CONFIGURE uninstall.xml`.
   - For Install Command in Deployment Options, type `setup.exe /CONFIGURE configuration.xml`.
   - In When To Call Install Complete section, choose the following:
     - Identify Application By: Defining Criteria
     - Criteria Type: File Exists
     - Path: C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
8. In Assignment, click Next. (We did not create an assignment at this time.)
9. In View Assignment, click Publish.

Creating the target profile

1. From the Workspace ONE UEM console, Navigate to Devices → Profiles & Resources → Profiles.
2. Click Add → Add Profile.
3. In Add Profile, select Windows.
4. In Device Type, select Windows Desktop.
5. In Select Context, select Device Profile.
6. We made the following changes on the nested menus, and clicked Save & Publish. We added a Custom Setting to add an additional user.

- General
  - Name: Connected Provisioning
  - Assignment Type: Auto
  - Track Profile Status during OOBE Provisioning: Yes
- Password
  - Password Complexity: Simple
  - Require Alphanumeric Value: Require
  - Password Expiration (days): 0
- Wi-Fi
  - Service Set Identified: [pt-temp-wifi]
  - Hidden Network: No
  - Auto-Join: Yes
  - Security Type: WPA2 Personal
  - Encryption: TKIP
  - Password: [Relevant Password]
- Firewall
  - Domain Firewall: Disable
  - Private Firewall: Enable
  - Public Firewall: Enable
- Antivirus
  - Real-time Monitoring: Enable
  - Scan Interval, Full Scan Required: Yes, Every Day at 11 PM
- Encryption (Bitlocker Encryption)
  - Encrypted Volume: OS Drive
  - Encryption Method: System Default
  - Only Encrypt Used Space During Initial Encryption: False
  - Force Encryption: False
  - Keep System Encrypted at All Times: True
  - Enable BitLocker To Go Support: True
  - Authentication Mode: TPM
  - Remaining Settings: False
- Windows Updates (Windows 10)
  - Windows Update Source: Microsoft Update Service
  - Update Branch: Semi-Annual Channel
  - Update Installation Behavior, Automatic Updates: Install Updates Automatically (recommended)
- Personalization
  - Desktop Image: We uploaded a desktop image at 1,920 x 1,080 resolution.
  - Lock Screen Image: We uploaded a lock screen image at 1,920 x 1,080 resolution.
- Custom Settings
  - Target: OMA DM Client
  - Make Commands Atomic: True
  - Install Settings: [Shown below]
  - Remove Settings: [Shown below]

Custom settings code

Install settings

```
<Add>
  <CmdID>5c9baa60-34d9-479c-a607-3a0421c1662b</CmdID>
  <Item>
    <Target>
        <LocURI>./Device/Vendor/MSFT/Accounts/Users/testuser/Password</LocURI>
      </Target>
    <Meta>
      <Format xmlns="syncml:metinf">chr</Format>
      <Type>text/plain</Type>
    </Meta>
    <Data>[Password]</Data>
  </Item>
</Add>
<Add>
  <CmdID>119e1c0d-34de-4f2c-b612-3bea0b1e20d9</CmdID>
  <Item>
    <Target>
        <LocURI>./Device/Vendor/MSFT/Accounts/Users/testuser/LocalUserGroup</LocURI>
      </Target>
    <Meta>
      <Format xmlns="syncml:metinf">int</Format>
      <Type>text/plain</Type>
    </Meta>
    <Data>2</Data>
  </Item>
</Add>
```

Remove settings:

```
<Add>
  <CmdID>5c9baa60-34d9-479c-a607-3a0421c1662b</CmdID>
  <Item>
    <Target>
        <LocURI>./Device/Vendor/MSFT/Accounts/Users/testuser/Password</LocURI>
      </Target>
    <Meta>
      <Format xmlns=”syncml:metinf”>chr</Format>
      <Type>text/plain</Type>
    </Meta>
    <Data>Password1!</Data>
  </Item>
</Add>
<Add>
  <CmdID>119e1c0d-34de-4f2c-b612-3bea0b1e20d9</CmdID>
  <Item>
    <Target>
        <LocURI>./Device/Vendor/MSFT/Accounts/Users/testuser/LocalUserGroup</LocURI>
```

```
      </Target>
    <Meta>
      <Format xmlns="syncml:metinf">int</Format>
      <Type>text/plain</Type>
    </Meta>
    <Data>1</Data>
  </Item>
</Add>
```

Timing activies

Our timings include multiple meetings. Meeting length might not be consistent, and for our calculations, we used estimated values in place of actual values.

Connected Provisioning

Attending an introduction meeting with the Dell team

To begin the Connected Provisioning process, Dell held a 30-minute meeting to discuss the project and introduce our Dell project manager and engineering team. This meeting covered both Connected and Factory Provisioning, so we used this time for both processes.

Completing the Export Compliance form

1. Under Export Compliance in Connected Provisioning in TechDirect, click Start.
2. Under What would you like to do?, select Read and sign the standard export terms.
3. Select I agree to Standard Export Terms listed above, and click Submit.

Creating system tags in Workspace ONE

1. Navigate to Groups & Settings → Devices & Users → Advanced → Tags.
2. Click Create Tag.
3. In Create Tag, type the name `ConnectedConfiguration`, and for Type, choose Device. Click Save.

Assigning the tag to a smart group

1. Navigate to Groups & Settings → Groups → Assignment Groups.
2. Click Add Smart Group.
3. For name in Create New Smart Group, type `ConnectedProvisioningSmartGroup`.
4. Select Tags, and choose the newly created ConnectedConfiguration tag.

Assigning applications to the smart group

1. In Workspace ONE, navigate to Apps & Books → Applications → Native.
2. Select the target application, and click Assign.
3. In Assignment, click Add Assignment.
4. In Distribution, enter the information below, and click Create.
   - Name: [Name for deployment]
   - Assignment Group: [Add the Connected Provisioning Smart Group]
   - Delivery begins: [Immediately]
   - App Delivery Method: Auto
   - Hide Notifications: True
   - Allows User Install Deferral: False
   - Display in App Catalog: False
   - Click Save.
   - Click Publish.
5. Complete steps 1 through 4 for each application.

Accepting the Connected Provisioning invitation in TechDirect

To enable the Connected Provisioning page in your TechDirect profile, use the link in the Welcome to Connected Provisioning email. This time reflects the time required to open Outlook, find the email, click the link, and sign into the account.

Creating a deployment profile in TechDirect

1. In Connected Provisioning in TechDirect, click Create New.
2. For step 1 Unified Endpoint Management (UEM) provider, select Workspace ONE Drop Ship Provisioning. Click Next.
3. For step 2 Provisioning account details, enter your Organization Group UUID and relevant Tag used in the previous task (this information can be found in your Workspace ONE UEM console). Click Validate.
4. For step 3 Operating System, we selected the following:
   - Edition: Windows 10 Pro
   - Version: 21H1
   - Language: English (US)
5. At the Summary screen, click Submit.

Attending the Readiness Assessment meeting

We attended a meeting with the Dell engineering team to review our Workspace ONE environment and verify that we were ready for deployment. During this meeting, the Dell team asked for details about our environment to determine if they could move forward with our Connected Provisioning order. During the call, they requested that we send screenshots of our profile and apps.

Capturing screenshots to verify settings with engineering team

To show that our order was correctly configured, we captured images of our profile and sent them to the engineering team for validation. We also included details about the applications that we would deploy during our Connected Provisioning order.

Approving the Technical Specifications document

The Dell project manager sent a technical specification document via email. The technical specification document included details about the order and provided an opportunity to correct any mistakes. We reviewed the PDF to validate the included information and gave our approval via email.

Attending the Readiness Review meeting

We attended a meeting to discuss the details of our environment. During this meeting, we discussed the state of our environment, the requirements for our order, the details of our system image, how we would handle change management within our company, and recommendations for each area that we might implement.

Associating the order

1. In Connected Provisioning in TechDirect, click Orders.
2. In Orders, select your order, and click Select Profiles.
3. Under the profile that you created previously, click Use this Profile.
4. When prompted with Ready to assign connected Provisioning to your order(s)?, click Yes, continue. Verify that the screen says You've successfully assigned Connected Provisioning to your selected order(s).

Assigning your profile as the default profile

1. In TechDirect, navigate to Services → Connected Provisioning → Profiles.
2. Under Default profile, click Yes, assign a default profile.
3. In the verification pop-up, click Yes, I'm sure.
4. Find the Connected Provisioning profile, and click Make Default.
5. In the verification pop-up, click Yes, continue.

Completing this step took 35 seconds. However, these steps do not complete the first order. Completing these steps saves time for additional orders, but we did not include this timing in any of our calculations.

Factory Provisioning with Workspace ONE

Completing the Export Compliance Form

1. We completed a separate Export Compliance form for Factory Provisioning. We received the form via email from our Dell project manager. We reviewed and signed the form digitally, and we then sent the form back to the project manager via email.

Preparing the PPKG file

1. From the Workspace ONE UEM console, navigate to Devices → Lifecycle → Staging → Windows.
2. In Windows, click New.
3. In New Provisioning Package, enter a name for the package.
4. In Onboarding Methods, select Drop Ship Provisioning – Offline.
5. In Configurations, enter the following values, and click Next:
   - Active Directory
     - Active Directory type: Workgroup
   - OOBE configuration
     - EULA page: Hide
     - Privacy settings: Hide
     - Online account settings: Hide
     - Operating system language: English
     - Region and keyboard settings: Hide
     - Region and keyboard settings: English – US
   - System configuration
     - Workgroup: PTlabs
     - Remove Windows 10 consumer apps: Yes
     - Product key: [Enter a valid Windows 10 Product Key]
     - Create local user: Yes
     - Local username: ptuser
     - Local user password: [Enter a valid password]
     - Make administrator: Yes
     - Administrator password: [Enter a valid password]
     - User account control: Disabled
   - Workspace ONE enrollment
     - Enrollment server: [Enter the web address of the Enrollment server]
     - Enrollment OG: [Enter the value of your Enrollment OG]
     - Staging account: [Enter the staging account]
     - Staging password: [Enter the staging account password]
6. In Application, select the applications that you added during setup, and click Next: We used the following:
   - Chrome for Business 64-bit
   - Notepad++(64-bit)
   - Office
   - Slack (Machine – MSI)
   - VLC media player 3.0.16 (64-bit)
   - Zoom
7. In Summary, click Save and Export.
8. In Overwrite Confirmation, click Yes, Export.

Downloading the PPKG file

1. Once available, click Downlaod Provisioning Files, and select PPKG.
2. Once the PPKG download has started, click Download Provisioning Files, and select Unattend XML/.

Copying the PPKG to the Validation VM

1. Copy the PPKG, unattend.xml, and VMware Workspace ONE Provisioning Tool to the Validation VM.

Validating the PPKG validation

1. Run the VMwareWS1ProvisioningTool.msi file.
2. From the root of C:\, double-click VMwareWS1ProvisioningTool.
3. In the VMware Workspace ONE Provisioning Tool, select the PPKG and configuration file locations.
4. Once the PPKG finishes copying, disconnect from the remote session, and connect via the vSphere client.
5. Open network adapter settings, and disable the network adapter.
6. In the VMware Workspace ONE Provisioning Tool, click Apply Full Process. We stopped our first timer at this point, and started our second timer.
7. After the previous step completes, in OOBE, click Next.
8. Click Limited Setup.
9. Click Continue with limited setup.
10. Reenable the network adapter, and using RDP, connect to the device.
11. Copy C:\ProgramData\Airwatch\UnifiedAgent\Logs\PPKGFinalSummary to the same folder as the PPKG on your local device.

Installing the Dell File Transfer software

1. Navigate to https://delivery.dell.com/download/download.html, and download the Dell File Transfer Application (.exe).
2. Download the VMware Workspace ONE® Provisioning Tool™ 3.2 for Windows from VMware Workspace ONE® Provisioning Tool™ 3.2 for Windows
3. Run the downloader, and accept the default location.

Starting the PPKG File Transfer

1. In the File Transfer EULA in the Dell File Transfer tool, accept the EULA, and click Next.
2. Sign in using your Dell TechDirect credentials.
3. In Project Selection, select the project number corresponding to your order, and click next. Note: You should have received an email with the project number from your Dell point of contact.
4. Select the files to upload, including the PPKG, the PPKG validation log, and the unattend.xml files. Click Next.
5. Click scan.
6. Click Upload.

We then ended the Starting the PPKG File Transfer timer and started the Completing the PPKG File Transfer timer. Once the file showed as successful, we alerted our Dell representative that we had uploaded the file.

Approving the Technical Specifications document

After we uploaded our PPKG files, the Dell engineering team sent us a Technical Specifications document to review and approve. We timed how long it took our administrator to review the documentation and respond to the email.

Traditional process

Unboxing and plugging in the laptop

1. Open and remove the system packaging. Return packaging materials to the original box.
2. Unwrap the power cord, and plug it into a power strip near the deployment switch.
3. Plug the system into the power cord and wired networking. Open the laptop lid.

Starting the OS installation on each laptop

1. Boot the target system.
2. To bring up the boot menu during boot, press F12.
3. Select the BIOS Setup menu.
4. In BIOS setup, select storage.
5. Select AHCI/NVME instead of RAID. Click Apply, and exit.
6. During reboot, press F12.
7. Select boot to IPv4.

Deploying Windows 10 and applications via task sequence

Allow the system to boot to the boot image and load the task sequence. To skip the 180-second countdown before starting the task sequence, click OK when prompted. We did not count this as admin time because the task did not take significant time and the administrator can continue working on other systems while the task sequence media loads.

Initiating the first-time boot and applying updates

Once you've completed the system deployment, log into each system. We did not count this as admin time because the task did not take significant time and the administrator can continue working on other systems while the task sequence media loads.

Repackaging the laptop

1. Once complete, shut down the target laptop.
2. Unplug all cables, and wrap the power cord.
3. Repackage the laptop to match how it arrived. To seal the box, apply tape.

Weighing the laptop

1. For one of the target laptops, record the weight and box dimensions.

Creating a shipping label

We captured the time to create the shipment and corresponding labels on FedEx.com to ship each system in the scenario to the same address.

Printing and applying shipping labels

1. Print the label created in the previous task, and attach it to the target system.
2. Place the target system in a designated shipping area.

Read the report at https://facts.pt/2BI1dJI ▶

This project was commissioned by Dell and VMware.

Principled Technologies®

Facts matter.®