Save over $1,100 per user*

Up to $450 less expensive*

per user to upgrade to new PCs

Avoid up to $279 per user in VM costs*

Migrate files in minutes, not days*

*vs. migrating to macOS

Save time and money by migrating employee PCs to Windows 10

Migrating your PCs to Windows® 10 can be easier and cheaper than changing to macOS™

If your employees are still using Windows 7 for business operations, you might be concerned about which operating system to turn to next: should you migrate to Windows 10, or transition your whole business to macOS? You might have heard that macOS could save your company money compared to the Windows 10 platform, but there are a host of issues your company could encounter during a cross-OS switch.

At Principled Technologies, we did research and hands-on work to determine money and time costs associated with migrating to Microsoft Windows 10 versus transitioning to macOS. We found that if your company stays with a Windows environment, you could spend less time and money on a migration than if you were to switch to macOS. A Windows-to-Windows migration saves on both upfront and ongoing costs for your employees and system administrators alike. We also found that Windows System Center Configuration Manager (SCCM) offers the same features of a representative macOS management program, and then some.

If your company is at a crossroads with migration efforts, read our report to get a better sense of what each choice could entail.

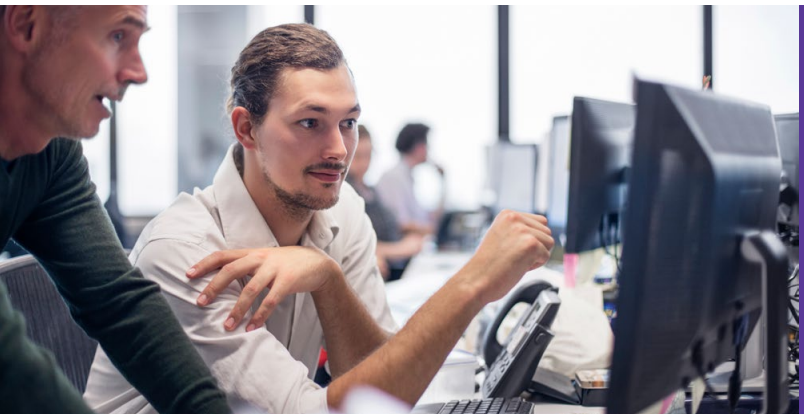
Windows 10: A cost-effective migration

If your company is considering a switch to macOS because of costs, you should know there are a number of hidden costs associated with a Windows 7-to-macOS migration.

Lower upfront costs

Assuming you don't purchase a new Windows device for every employee, the upfront cost of migrating your business to Windows 10 is markedly lower than purchasing new macOS-based equipment for your whole staff. For a 500-person company, purchasing new 13-inch MacBook Pro® with Retina® display laptops would cost $749,500—$1,499 per person. On the other hand, upgrading to Windows 10 Enterprise E3 is only a $311 investment per device—or $155,500 for 500 employees.

By upgrading to Windows 10 instead of transitioning to Macs, you could save over a thousand dollars per employee, or $594,000 for a full team of 500.



By upgrading to Windows 10 instead of transitioning to Macs, you could save over a thousand dollars per employee.

Lower ongoing costs

If your team is used to the Windows workflow, getting acclimated to macOS could cost your company more than you bargained for. For starters, you may have to schedule time-consuming and potentially costly retraining sessions to get your employees up to speed.

Another unexpected cost of a macOS migration: Windows programs your team relies on may be incompatible or otherwise buggy in a Mac software environment. In those cases, you would have a few options. One is to give your employees access to a virtual Windows 10 desktop client, but supporting that VM could be costly.

Another option would be to purchase licensed copies of Windows 10 for employees to run with Boot Camp®—that would raise costs by $199 dollars per device.[1] Purchasing copies of Parallels to run Windows 10 as a virtual machine would run an additional $80 per device.

Additionally, Mac hardware failures can be more costly to fix than on PCs, as performing physical maintenance on Mac computers is no small task. In a MacBook Pro, the RAM and battery pack are soldered and glued into the chassis itself, rendering a simple RAM or battery replacement difficult if not impossible. Furthermore, the Apple® Terms and Conditions prohibit any unauthorized modifications to your Mac systems, meaning you could void your warranty even attempting to fix a problem with a Mac by yourself.[2]

Saving time with a Windows 10 migration

File transfers can be a time-consuming process for IT administrators migrating from Windows 7 to macOS systems via the Apple tool "Windows Migration Assistant." By comparison, the effort required to migrate files and configuration settings from Windows 7 to Windows 10 is trivial. In the Principled Technologies datacenter, we simulated a Windows 7 to Windows 10 upgrade and compared it to the process of migrating a user's files using the Windows Migration Assistant from Apple. For a Windows 10 upgrade, we found it took only one and a half minutes to create and schedule an upgrade task sequence in SCCM that would target every computer in the company.

By contrast, it took us 2 minutes to set up a migration with the Windows Migration Assistant—and that's *per computer.* That means it would take 16.6 hours of hands-on IT time to complete the upgrades for 500 employees—more than two full administrator work days spent on a migration that would have taken just minutes for a Windows 10 upgrade.

In addition to the time associated with the actual migration event, keep in mind the retraining process we mentioned earlier. It's inevitable that your team won't be entirely comfortable with a Mac workflow. Any additional hiccups can mean a hit to your employees' productivity.

For a Windows 10 upgrade, we found it took one and a half minutes to create and schedule an upgrade task sequence that would target every computer in the company.

Adding devices

If after the big migration you need to add other devices to your company network, the Windows environment makes it easy to do so with little to no IT time required.

Managing Windows 10 PCs with Microsoft Intune allows you to set up an enrollment point to which your employees can connect and automatically configure their devices with your company network. After you've configured enrollment options, an employee simply has to log in with their company credentials. Once that's done, the setup process is automatic.

You can set up a enterprise-wide application store so that your employees can download company-sanctioned and modified applications without bothering the IT department, saving time that IT staff can use for higher-priority business items.

Purchasing new hardware? Windows migration still costs less.

Even if you do decide to purchase new devices for each of your employees, investing in new PCs can be less expensive than buying new Macs. A 13-inch PC—such as the Dell XPS 13 with Windows Pro and 7th gen Intel® Core™ i5—costs $450 less per user than the 13-inch MacBook Pro from 2016. A company purchasing 500 of these PCs would save $225,000 overall.

Windows 10 features mean you're not missing out

You may be considering a Mac migration because you heard macOS offers features Windows 10 doesn't have. In the box below, we present some valued Mac applications and services along with their Windows counterparts. We also list Windows 10 features for which there is no Mac equivalent.

Windows applications with corresponding Mac counterparts:

- Cortana® / Siri®
- Task View / Exposé®
- Microsoft Passport / AppleID 2-factor authentication
- Microsoft Hello / TouchID
- Device Guard / Gatekeeper
- Bitlocker® / FileVault® 2

Windows 10 features not available on Mac systems:

- Secure boot
- Windows Information Protection
- Enterprise Data Protection
- Credential Guard
- Windows Defender Advanced Threat Protection

In addition, proprietary legacy business applications often require a Windows environment to run, meaning that a switch to macOS would require even further investment in additional Windows licenses to run in partitions or VMs on the new Mac machines, as we mentioned in our cost analysis.

Management features

We also took a look at the common features of Windows System Center Configuration Manager and compared them to a representative macOS management tool, Filewave. We found SCCM features that save time for IT admins that are not replicated in Filewave. These include task sequences and user state migration.

SCCM task sequences give administrators the ability to create complex deployments with minimal scripting. Some difficult problems can be solved only by ordering commands in a specific sequence. For example, you may need to run a command before installing database software, then run another command before installing a set of management tools. Administrators can do this quickly in the SCCM interface, but it becomes a laborious chore when forced to use scripting, as required in Filewave.

Scripting, on which Filewave relies heavily, can be much more labor-intensive than using the customizable GUI-based commands available in SCCM. Here are a few common tasks that SCCM can perform readily but Filewave can perform only via scripting:

- Joining a domain
- Formatting and partitioning a disk
- Performing USMT actions
- Preparing a system for image capture
- Restarting a system and continuing a task sequence

Conclusion

Your employee PCs need a newer OS to keep your business running quickly and securely. If your company is already powered by Windows 7, switching to the macOS environment can lead to a number of costs and time-sinks that can affect your company's bottom line. Upgrading your employee systems to Windows 10 is a cost-effective, time-saving option for companies who know it is time to upgrade.

---

1 https://www.microsoftstore.com/store/msusa/en_US/pdp/Windows-10-Pro/productID.319935900?ICID=Windows_Win10Pro_ModE

2 http://www.apple.com/support/macbookpro/en/service_body.html

3 http://blog.parallels.com/2016/01/21/differences-microsoft-office-mac/

On October 25, 2016, we finalized the hardware and software configurations we tested. Updates for current and recently released hardware and software appear often, so unavoidably these configurations may not represent the latest versions available when this report appears. For older systems, we chose configurations representative of typical purchases of those systems. We concluded hands-on testing on November 18, 2016.

Appendix A: System configuration information

System	HP® ProBook 430	Apple MacBook Air
Display		
Screen size (inches)	13.3"	13.3"
Display resolution	1,366 x 768	1440 x 900
PPI	118	127.68
Dimensions		
Length	12.875"	12.75"
Width	9.25"	9"
Height	.75"	.5"
Weight	3.40	2.90
Hardware/Software		
CPU	Intel Core i3-4010U 1.7 GHz	Intel Core i5-4260U 1.4 GHz
Storage	Samsung® 128GB SSD	Apple 256GB SSD
OS	Windows 10 Enterprise	macOS Sierra 10.12.1

Appendix B: How we tested

Installing and configuring the infrastructure servers for SCCM

Configuring Windows Server® 2012 R2 servers

After installing Windows Server 2012 R2 Data Center edition on our R710 and installing Hyper-V®, we created 3 virtual machines with the same OS and installed all updates up to 10/25/2016, we configured Windows Server by making the following changes on each system.

Configuring Windows Update

1. In the left pane of the Server Manager window, click Local Server.
2. In the main frame, next to Windows Update, click Not configured.
3. In the Windows Update window, in the main pane, click Let me choose my settings.
4. Under Important updates, select Never check for updates (not recommended), and then click OK.
5. In the left pane, click Check for updates, and install all available updates.
6. Close the Windows Update window.

Configuring Windows Firewall

1. In Server Manager, click Tools → Windows Firewall with Advanced Security.
2. In the Overview section, click Windows Firewall Properties.
3. In the Domain Profile tab, for Firewall state, click Off.
4. In the Private Profile tab, for Firewall state, click Off.
5. In the Public Profile tab, for Firewall state, click Off.
6. Click OK.
7. Close the Windows Firewall Properties window.

Setting up Remote Desktop

1. In the Local Server tab of the Server Manager window, next to Remote Desktop, click Disabled.
2. In the System Properties window that appears, in the Remote Desktop section, select the Allow remote connections to this computer radio button, and click OK when the warning message appears.
3. Uncheck Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended), and click OK.

Disabling IE Enhanced Security Configuration

1. In the Local Server tab of the Server Manager window, next to IE Enhanced Security Configuration, click On.
2. In the Internet Explorer Enhanced Security Configuration window, select the Off radio buttons for both Administrators and Users, and click OK.

Installing Active Directory and DNS services

1. Power on the Domain Controller.
2. On the Domain Controller, open Windows PowerShell® as an administrator.
3. Run the following command:

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

4. When the installation is finished, close PowerShell.
5. Open Server Manager.
6. On the Welcome screen, click 2, and click Add roles and features.
7. At the initial Before you begin screen, click Next three times.
8. At the Server Roles screen, select Active Directory Domain Services.
9. On the pop-up window, click Add Features.
10. Click Next three times.
11. Verify the desired role is being installed, and click Install.
12. Once installation has finished, close the Add roles and features wizard.
13. In Server Manager, click the flag at the top, and select the Promote this server to a domain controller link.
14. Select Add a new forest, enter a root domain name of `test.local` and click Next.
15. On the Domain Controller Options screen, enter a password, and click Next.

16. On the DNS Options screen, click Next.
17. On the Additional Options screen, click Next.
18. On the Paths screen, click Next.
19. On the Review Options screen, click Next.
20. On the Prerequisites screen, verify all prerequisites have passed, and click Install.
21. Once Active Directory Domain Services finishes installing, click Finish, and restart the system.

Adding DHCP

1. Open Server Manager.
2. On the Welcome screen, click 2, and click Add roles and features.
3. At the initial Before you begin screen, click Next three times.
4. At the Server Roles screen, select DHCP Server.
5. On the pop-up window, click Add Features.
6. Click Next three times.
7. Verify the desired role is being installed, and click Install.
8. Once installation has finished, close the Add roles and features wizard.
9. In Server Manager, click the flag at the top of the screen 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.
13. In Administrative Tools, open the DHCP service.
14. Expand ad.test.local, then right-click IPv4, and select New Scope.
15. In the New Scope Wizard window, click Next.
16. At the scope name screen, name the scope Laptops, and click Next.
17. In the IP Address Range, enter the desired scope settings for your network.
18. Click Next four times.
19. At the Router screen, enter the gateway address to be used by the clients, and click Next.
20. Click Next three times.
21. At the Completing the New Scope Wizard screen, click Finish.
22. Join all systems to the domain. We named the systems as follows:
    - Domain Controller Server: ad.test.local
    - Certificate Authority Server: ca.test.local
    - SCCM Server: cm.test.local

Creating Containers and Extending the AD Schema

1. On the Domain Controller, run ADSI Edit.
2. On the toolbar, select Action → Connect to…
3. Accept the defaults by clicking OK.
4. Under Default Naming Context → DC- test, DC=local, right-click CN = System, and select New → Object…
5. Select Container, and click Next.
6. Under Value, we entered System Management. Click Next, then Finish.
7. Run Active Directory Users and Computers.
8. On the toolbar, select View, then click Advanced Features.
9. Under test.local > System, right-click System Management and choose Delegate Control.
10. Click Next.
11. Click Add.
12. Click Object Types, select Computers, and click OK.
13. Enter CM for object name, and click OK.
14. Click Next.
15. Select Create a custom task to delegate, then click Next.
16. Choose This folder, existing objects… and click Next.
17. Click Full Control, and click Next.
18. Click Finish.
19. Attach the SCCM installation media to the Domain Controller.
20. From the installation media, navigate to \SMSSETUP\BIN\X64. Right-click extadsch and run as administrator.
21. Review extadsch.log at the root of the system drive to confirm the operation was successful.

Creating Active Directory accounts for System Center Configuration Manager

1. On the Domain Controller, open Active Directory Administrative Center.
2. Under test (local), in the Tasks panel, click New, then select Group from the drop-down menu.
3. In the Create Group window, for Group name, use Kerberos Admins; for Group type, use security; and for Group scope, select Global.
4. Add Kerberos Admins as a member of the Domain Admins group.
5. Add the computer account of the SCCM server to the Kerberos Admins security group, and click OK.
6. Create an Organizational Unit for AMT managed systems called AMT Management.
7. Create a security group called AMT Control.
8. Add the Kerberos Admins group to the AMT Control security group.
9. Add CM to the domain administrator group.

Installing SQL 2014 SP2

1. Log into the SCCM server as domain\administrator.
2. Attach the installation media for SQL Server 2014 Standard Edition with Service Pack 2 (x64) and run the setup.exe file.
3. In the SQL Server Installation Window, select Installation from the menu on the left, and then select New SQL Server stand-alone installation or add features to an existing installation.
4. In the SQL Server 2014 Setup Window, select the free edition and click Next.
5. At the License Terms screen, accept the license terms and click Next.
6. At the Global Rules screen, select Use Microsoft Update to check for updates and click Next.
7. Wait while the installer checks prerequisites and installs rules. Once complete, check for compliancy and click Next.
8. At the Setup Role screen, select SQL Server Feature Installation, and click Next.
9. At the Feature Selection screen, under Instances Features, select Database Engine Services with Full-Text and Semantic Extractions for Search, and Data Quality Services, Reporting Services - Native, Management Tools - Basic, Management Tools - Complete, and SQL Client Connectivity SDK. Click Next.
10. Allow the Installation Rules check to run, and click Next.
11. At the Instance Configuration screen, select Default Instance and leave the default Instance ID. Change the root directory for the installation to the attached 500 GB virtual hard drive.
12. At the Disk Space Requirements screen, click Next.
13. At the Server Configuration screen, set Startup Type for Server Agent, SQL Server Database Engine, and Server Browser as Automatic, and click Next.
14. At the Database Engine Configuration screen, select Mixed Mode.
15. Enter a password for the system administrator (sa) account.
16. Click Add Current user.
17. Click next until you reach the Ready to Install screen.
18. Verify that the Summary is correct, and click Install.
19. Click Finish when prompted.
20. Open Microsoft SQL Server Management Studio.
21. Sign into your SQL database.
22. Right-click your SQL host, and select Properties.
23. Select the Memory page.
24. Change maximum server memory to `163848192`. Click OK.
25. In SQL Server Configuration Manager, expand the SQL Server Network Configuration tree, and click Protocols for MSQLSERVER.
26. Right-click Named Pipes, and click Enable.
27. Do the same for TCP/IP.
28. Click SQL Server Services in the tree.
29. Right-click SQL Server (Instance Name) and select properties.
30. On the Log On tab, change the Account Name to test\administrator. Enter the password and click Apply.
31. A popup will request to restart the service. Select Yes.

Installing the Certificate Authority

1. On the Certificate Authority Server, log in using the test.local\administrator account.
2. Launch Server Manager.
3. Click Add roles and features.
4. In the Add Roles and Features Wizard, click Next three times.
5. Select Active Directory Certificate Services. On the pop-up click Add Features.
6. Click Next twice.
7. Click Install. When complete click Close.

8. In Server Manager, click the flag and select the Post-deployment Configuration task.
9. In the AD CS Configuration Window, click Next.
10. Check the box for Certification Authority, and click Next.
11. Select Enterprise for the setup type, and click Next.
12. Choose Root CA for the CA type, and click Next.
13. Select Create a New Private Key, and click Next.
14. Accept all remaining defaults, and click Next through the remaining screens.
15. When prompted to begin configuration, click Configure.
16. To exit the wizard, click Close. Restart the server before continuing to the next steps.

Installing required Windows features and roles for System Center Configuration Manager

1. Sign into the SCCM server using the domain\administrator account.
2. Download the Windows Assessment and Deployment Kit for Windows 10 from the following website: https://go.microsoft.com/fwlink/p/?LinkId=526740
3. Run adksetup.exe.
4. Select Install the Assessment and Deployment Kit to this computer, and choose an installation path. Click Next.
5. When prompted to join the Customer Experience Improvement Program (CEIP), select No.
6. Accept the license agreement.
7. Select Deployment tools, Windows Pre-installation Environment features, and User State Migration Tool. Click Install.
8. Click Close when the install finishes.
9. In the Server Manager window, select Add roles and Features.
10. In the Add Roles and Features Wizard, click Next three times.
11. On the Server Roles screen, click Next.
12. Add the following Features by selecting them from the list:
    - .NET Framework 3.5
    - .NET Framework 4.5
        - ASP.NET 4.5
        - WCF Services
            - HTTP Activation
            - TCP Port Sharing
    - Background Intelligent Transfer Service (BITS)
        - IIS Server Extension
    - Remote Differential Compression
    - Remote Server Administration Tools
        - Feature Administration Tools
            - BITS Server Extensions Tools
13. Click Next twice.
14. At the Role Services screen, select the following services,
    - Web Server (IIS)
        - Common HTTP Features
            - Default Document
            - Directory Browsing
            - HTTP Errors
            - Static Content
            - HTTP Redirection
        - Health and Diagnostics
            - HTTP Logging
            - Logging Tools
            - Request Monitor
            - Tracing
    - Performance
        - Static Content Compression
        - Dynamic Content Compression
    - Security
        - Request Filtering

- Basic Authentication
- Client Certificate Mapping Authentication
- IP and Domain Restrictions
- URL Authorization
- Windows Authorization

- Application Development
  - .NET Extensibility 3.5
  - .NET Extensibility 4.5
  - ASP
  - ASP.NET 3.5
  - ASP.NET 4.5
  - ISAPI Extensions
  - ISAPI Filters
  - Server Side Includes
- FTP Server
  - FTP Service
- Management Tools
  - IIS Management Console
  - IIS 6 Management Compatibility
    - IIS 6 Metabase Compatibility
    - IIS 6 Management Console
    - IIS 6 Scripting Tools
    - IIS 6 WMI Compatibility
  - IIS 6 Management Scripts and Tools
  - Management Service

15. Click Next.
16. Click Install.
17. Run Windows Update, and install updates.
18. Restart the server.

Installing WSUS on the Configuration Manager Server

1. Sign into the SCCM server using the test.local\administrator account.
2. Open Server Manager.
3. In the Server Manager window, select Add roles and Features.
4. In the Add Roles and Features Wizard, click Next three times.
5. On the Server Roles screen, select Windows Service Update Services. Click Next until you reach the WSUS Role Services screen.
6. At the Role Services screen, select WID Database and WSUS Services. Click Next.
7. On the Content location selection screen, enter a location to store the updates. We used C:\wsusupdates
8. On the Confirmation screen, click Install. Once installation completes, close the Wizard.
9. In Server Manager, click the Flag at the top right and select Launch Post-Deployment Configuration. Wait for the configuration to complete.
10. Download and install the KB3095113 hotfix from https://support.microsoft.com/en-us/kb/3095113
11. Open an elevated Command Prompt window, and then run "C:\Program Files\Update Services\Tools\wsusutil.exe postinstall /servicing" (case sensitive, assume C: as the system volume).

Note: Do not launch WSUS Post-Installation tasks.

Installing System Center Configuration Manager 2012 R2 SP1

1. Sign into the SCCM server using the test.local\administrator account.
2. Attach the SCCM 2012 R2 SP1 Installation media to the management server.
3. Open splash.hta.
4. Click Install.
5. Read the Before You Begin section, click Next.
6. Choose Install a primary site. Do not choose the typical options.
7. Select Install the evaluation edition of this product and click Next.
8. Check the box to accept the License Terms, and click Next.
9. Accept the license agreements, and click Next.

10. Enter a path for the prerequisite file downloads. We used `C:\Downloads`
11. Select a language, and click Next for both server and client.
12. Enter a site code for the primary site. We used PTL.
13. Enter a Site Name. We used PTLab.
14. Choose an install path. We accepted the default install path.
15. Ensure that the console will be installed, and click Next.
16. Install as a primary stand-alone site.
17. Enter the SQL server name, and click Next.
18. Leave the default Database information, and click Next again.
19. Accept the default SMS provider, and click Next.
20. Select the option to Configure the communication method on each site system role.
21. Select Clients will use HTTPS when they have a valid PKI certificate and HTTPS-enabled site roles are available, and click Next.
22. Select HTTP for Management Point and Distribution point, and click Next.
23. Click Next three times.
24. Run the prerequisites check, and resolve any issues displayed.
25. Click Begin Install, and click Close when the installation is complete.
26. Download and install the installation for System Center R2 SP1 Configuration Manager from the following website: support.microsoft.com/kb/2922875/en-us
27. Download and install the cumulative update.

Configuring SCCM

Update Configuration Manager to latest version

1. In the Configuration Manager console, in the Administration Workspace, Under Overview, Cloud Services, click Updates and Servicing.
2. Starting with the earliest available update, right click and select Install Update Pack. Configuration Manager Updates Wizard, click Next.
3. At the Select Upgrade screen, without validating, click Next.
4. At the License Terms screen, accept the license terms and click Next.
5. At the Summary screen, click Next.
6. Once complete, click Close.
7. The console may request to update to the latest version. Click OK and allow the update to complete.
8. Repeat steps 2 through 6 until all updates are installed. We installed up to Configuration Manager 1606 with the latest hotfixes.

Configuring Network Discovery

1. In the Configuration Manager console, in the administration workspace, under overview, in the Hierarchy Configuration folder, select discovery methods.
2. Right click all discovery methods and make sure they are enabled.
3. Right click Active Directory System Discovery and select properties.
4. Under Active Directory Containers, click the orange start to add an Active Directory Container.
5. In the Active Directory Container Screen, under Path, select Browse. Select the OU Computers. Then click OK.
6. Click OK.
7. In the top panel, click Run Full Discovery Now.
8. Right click Active Directory User Discovery Properties and select properties.
9. Under Active Directory Containers, click the orange start to add an Active Directory Container.
10. In the Active Directory Container Screen, under Path, select Browse. Select the OU Users. Then click OK.
11. Click OK.
12. In the top panel, click Run Full Discovery Now.
13. Right click Network Discovery and select Properties.
14. Select the DCHP tab.
15. Check the box for Include the DHCP server that the site server is configured to use.

Configure the Active Directory

1. On the Domain Controller server, create a user called CM_JD and a second user called CM_NAA.
2. Download the configure permission in Active Directory for Windows deployment account from https://gallery.technet.microsoft.com/Configure-permissions-in-2326651a. Move the script to C:\Setup\Scripts on the Domain Controller.
3. Run the following scripts from PowerShell as administrator:

```
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned –Force

Set-Location C:\Setup\Scripts

.\Set-OUPermissions.ps1 -Account CM_JD -TargetOU "OU=Workstations,OU=Computers,OU=test.local"
```

Configure the Network Access Account

4. On the Configuration Manager server, in the Configuration Manager console, under the Administration tab, expand the Site Configuration Tree. Click Sites.
5. Right-click the PTT site, and select Properties.
6. In the Software Distribution Component Properties window, select the Network Access Account. Select Specify the account that accesses network locations. Click the orange star to add a new Network Access Account.
7. For user name, browse to find test.local\CM_NAA, enter the Password, and click Verify. For Network share, enter \\AD\sysvol and click Test Connection. If successful click OK, then OK again.

Creating the Deployment and Enrollment Collection

1. On the Configuration Manager server, in the Configuration Manager console, under the Asset and Compliance workspace, right-click Device Collection, and select Create Device Collection.
2. On the General screen, for name, type `Windows 10 Upgrade Targets`.
3. On the Limiting Collection screen, select All Desktop and Server Clients. Click Next.
4. On the Membership Rules screen, click Next.
5. Once created, click Close.
6. Repeat the steps above but name the collection Windows10UserEnroll.

Adding additional attributes to active directory system discovery

1. In the Configuration Manager console, in the administration workspace, under overview, in the Hierarchy Configuration folder, select Boundary Groups.
2. Right click and select Create Boundary Group.
3. On the General tab, give a name. We used test.local boundary.
4. Click add.
5. In the Add Boundaries Window, add the Default-First-Site-Name and click OK.

Enable PXE Support

1. In the Configuration Manager console, in the Administration workspace, in the Site Configuration folder, select Severs and Site System Roles.
2. Select cm.test.local and under Site System Roles, right click Distribution point, and select Properties.
3. On the PXE tab, check Enable the Enable PXE support for Clients option.
4. In the ports window click Yes.
5. Check the Allow this distribution point to respond to incoming PXE requests option.
6. Check the Enable unknown computer support option
7. Ensure that the Respond to PXE request on all network interfaces is checked.
8. Click Ok

Install MDT 2013 Update 2

1. Download the MDT 2013 Update 2 installation files from https://www.microsoft.com/en-us/download/confirmation.aspx?id=50407.
2. Run the installation and agree to all defaults.
3. Run the Configure ConfigMgr Integration tool.
4. In the Configure ConfigMgr Integration wizard, click Next.
5. Click Finish.

Creating the Deployment Share

1. On the SCCM server, open Deployment Workbench.
2. Under Deployment Workbench, right-click Deployment Shares, and select New Deployment.
3. In the New Deployment Share Wizard, select a Deployment share path.
4. On the Share screen, enter a share name. We used MDTBuildLab.
5. On the Descriptive Name screen, click Next.
6. On the Options screen, uncheck all boxes.
7. On the Summary screen, click Next.
8. On the Confirmation screen, click Finish.

Importing the Operating System Image

1. Mount the en_windows_10_enterprise_version_1607_updated_jul_2016_x64_dvd_9054264 to the Configuration Manager server.
2. From the DVD copy all files onto the Configuration Manager server. We stored ours at C:\Share\Windows\ISOs\en_windows_10_enterprise_version_1607_updated_jul_2016_x64_dvd_9054264\
3. Under the PTT Share Deployment share, right-click Operating Systems, and select Import Operating System Wizard.
4. On the Import Operating System Wizard, select Full set of source files, and click Next.
5. On the Source screen, for Source directory select the folder where you stored the Windows 10 Enterprise folders. We used C:\Share\Windows\ISOs\ en_windows_10_enterprise_version_1607_updated_jul_2016_x64_dvd_9054264\. Click Next.
6. On the Destination screen, click Next.
7. On the Summary screen, click Next.
8. On the Confirmation screen, click Finish.

Creating the Build and Capture Task Sequence

1. Under the PTT Share Deployment share, right-click Task Sequences, and select New Task Sequence.
2. In the New Task Sequence Wizard, enter a Task Sequence ID and Task Sequence name. We used `PTL001` and `Windows 10 Enterprise Build` and `Capture` respectively.
3. On the Select Template screen, select Standard Client Task Sequence from the radio menu, and click Next.
4. On the Select OS screen, select the image for Windows 8.1 Enterprise that you added in the previous section.
5. On the Specify Product Key screen, click Next.
6. On the OS Settings screen, for Full Name: type `PTTuser` and for Organization: type `PTT`. Click Next.
7. On the Admin Password screen, enter `Password1`, then click Next.
8. On the Summary screen, click Next.
9. On the Confirmation screen, click Finish.

Creating the Build and Capture Task Sequence

1. Right-click PTT Share, and select Properties.
2. On the PTT Share Properties Window, select the Rules tab.
3. Replace the current Rules with the following:

```
[Settings]
Priority=Default
[Default]
_SMSTSORGNAME=MDTBuildLab
UserDataLocation=NONE
DoCapture=YES
OSInstall=Y
AdminPassword=Password1
TimeZoneName=Eastern Standard Time
JoinWorkgroup=WORKGROUP
HideShell=YES
FinishAction=SHUTDOWN
DoNotCreateExtraPartition=YES
WSUSServer=http://cm.test.local:8530
ApplyGPOPack=NO
```

```
SLSHARE=\\CM\Logs$
SkipAdminPassword=YES
SkipProductKey=YES
SkipComputerName=YES
SkipDomainMembership=YES
SkipUserData=YES
SkipLocaleSelection=YES
SkipTaskSequence=NO
SkipTimeZone=YES
SkipApplications=YES
SkipBitLocker=YES
SkipSummary=YES
SkipRoles=YES
SkipCapture=NO
SkipFinalSummary=YES
```

4. Click Edit Bootstrap.ini.
5. Replace the text in Bootstrap.ini with the following:

```
[Settings]
Priority=Default
[Default]
DeployRoot=\\CM\PTTShare$
UserDomain=test.local
UserID=administrator
UserPassword=Password1
SkipBDDWelcome=YES
```

6. Save and exit the file.
7. Click OK.
8. Right-click PTT Share, and select Update Deployment Share.
9. Select Completely regenerate the boot images.
10. Once complete, Navigate to the Deployment Share in File Explorer.
11. In the boot folder, using PTT Build Lab x86 create an installation disk using the .iso.
12. Copy the .iso to the hypervisor.
13. On the hypervisor, mount the build and capture .iso onto a new VM, and boot to the disk. The VM will run the build and capture sequence.
14. Once the Build and Capture completes, the Image will be available at PTTShare\Captures. We named our image Windows10Entx64.wim and moved it to \CM\Share\Capture\

Add Windows 10 OS package

1. In the Software Library Workspace, under Overview, under operating Systems, right click Operating System Upgrade Packages and select Add Operating System Upgrade Package.
2. In the Operating System Upgrade Package wizard, click browse and navigate to the \\CM\Capture\ folder that contains the copied Windows 10 Enterprise installation files. Select that folder and click OK. Then click Next.
3. At the General screen, click Next.
4. At the Summary screen, click Next.
5. Click Close.

Upgrade your PC from Windows 7 Enterprise to Windows 10 Enterprise

Create the Windows 7 Upgrade to Windows 10 Task Sequence

1. Start the timer.
2. In the Software Library Workspace, under Overview, under operating Systems, right click Operating System Upgrade Packages and select Create New Task Sequence.
3. In the Create Task Sequence Wizard, select Upgrade an operating system from an upgrade package, and click Next.
4. At the Upgrade the Windows Operating System screen, click Browse and select the Windows 10 enterprise package. Click Next.
5. At the Include Update screen, select Available for installation – All software updates, and click Next.
6. At the Install Application screen, click Next.
7. At the Summary screen, click Next.
8. At the Completion screen, click Close.

Deploy the Windows 10 Task Sequence

1. In the Software Library Workspace, under Task Sequences, right click the Windows 7 Upgrade to Windows 10 task sequence and select Deploy.
2. In the Deploy Software Wizard, click Browse…
3. In the Select Collection Window select Windows 10 Upgrade Targets and click OK.
4. Click Next.
5. On the Deployment Settings screen, select Required.
6. On the schedule screen, check the box for Schedule when this deployment will become available.
7. For Assignment schedule click New…
8. In the Assignment Schedule Window, select assign immediately after this event and click OK.
9. Click Next.
10. On the User Experience screen, click Next.
11. On the Alerts screen, click Next.
12. On the Distribution Points screen, click Next.
13. On the Summary screen, click Next.
14. On the Completion screen, click Close.
15. Stop the timer.

Move your data from a PC to your Mac

Before starting we updated with all available updates as of 10/25/2016. Both systems started powered on and at the login screen. Both systems were wirelessly connected to our test network.

1. Start the timer.
2. On the PC, download the Windows Migration Assistant from https://support.apple.com/kb/DL1557?locale=en_US.
3. Install the Windows Migration Assistant using all defaults.
4. Open the Windows Migration Assistant on your PC.
5. In the Migration Assistant Window, click continue.
6. On the Mac, open the Utilities folder.
7. In the Utilities folder, open Migration Assistant.
8. In the Migration Assistant window, click continue.
9. In the credentials window, enter your credentials and click OK.
10. In the Migration Assistant window, click From a Windows PC and click continue.
11. On the Transfer Information to this Mac screen, select the Windows system when it appears and click continue.
12. On the PC, verify that the correct Passcode is displayed on both computers and click continue.
13. On the Mac, once the scan is complete, click Continue.
14. Stop the timer.

Setting up Enrollment via Intune

The following steps with configure SCCM and Intune for employee self-enrollment.

Creating an Intune account

1. Sign up for a trial account of Intune at https://www.microsoft.com/en-us/cloud-platform/microsoft-intune.
2. Using Internet Explorer, login to the Intune admin console at https://login.microsoftonline.com with the credentials you used in Step 1.

Configuring the Domain

1. In the Intune Admin Console, in the left panel, click the Admin Centers icon and select Azure AD.
2. In Active Directory, open your directory and select the Domains tab.
3. Select Add.
4. Enter test.local and click Add.
5. In the Admin center, under Users, click Add a User.
6. In the New user panel, add a Display name and User name for your user. We used WinEnroll.

Installing Microsoft Azure AD Connect

1. On the Domain Controller, go to http://go.microsoft.com/fwlink/?LinkId=615771, download and run the setup file.
2. In the Microsoft Azure Active Directory Connect window, check the box for I agree to the license terms and privacy notice and click Continue.
3. On the Express Settings screen, click Customize.
4. On the Install required components screen, click Install.
5. On the User Sign-In screen, select Do not configure. Click Next.
6. On the Sync screen, enter your onmicrosoft.com username and password. Click Next.
7. On the Connect your directories screen, for Forest enter test.local, for username, enter test.local\administrator and the password. Click Add Directory. Click Next.
8. On the Azure AD sign-in screen, check Continue without any verified domains and click Next.
9. On the Domain and OU filtering screen, click Next.
10. On the Identifying users screen, click Next.
11. On the Filtering screen, click Next.
12. On the Optional Features screen, click Next.
13. On the Ready to configure screen, click Install.

Configuring SCCM with Intune

1. On the Configuration Manager server, in the System Center Configuration Manager Console, in the Administration workplace, expand Cloud Services, and click Microsoft Intune Subscriptions, then click Add Microsoft Intune Subscription.
2. In the Create Microsoft Intune Subscription Wizard, click Next.
3. On the Subscription screen, click Sign In.
4. On the Set the Mobile Device Management Authority Window, check the box to confirm and click OK.
5. In the Subscription window, sign in using your Intune login information.
6. On the General tab, select the Windows10UserEnroll Collection.
7. For Company Name, we entered PTlabs.
8. For Configuration Manager Site Code, select PTL, and click Next.
9. On the Company Contact Information screen, click Next.
10. On the Device Enrollment Manager screen, click Next.
11. On the Multi-Factor Authentication screen, click Next.
12. On the Summary screen, click Next.
13. Once complete, click Close

Enrolling Windows 10 Enterprise via Intune

1. On the Windows 10 laptop, hit the Windows key and type `About your PC`, then hit enter.
2. In the settings Window, click Connect to work or school.
3. Click Connect.
4. On the Set up a work or school account window, enter WinEnroll@test.local.
5. On the Connect to a service window, log in using the WinEnroll@test.local account and click Sign In.
6. On the You're all set! screen, click Close.

This project was commissioned by Microsoft.

Facts matter.®