

MMC Windows 10 Production Build Checklist

To create build document, complete the setup variables below.

Ensure the Computer Asset in CMDB is set to a "Reserved" status before you start the build

Demographic information

CASD ticket number:	<input type="text"/>
Date:	<input type="text"/>
Technician name:	<input type="text"/>
Colleague name:	<input type="text"/>
Domain ID:	<input type="text"/>
Employee ID:	<input type="text"/>
Computer name:	<input type="text"/>
Computer model:	<input type="text"/>
Serial number:	<input type="text"/>
Asset number:	<input type="text"/>

*Computer setup variables

	Yes	No
Information on - Build Troubleshooting	<input type="radio"/>	<input type="radio"/>
Information on - Deleting Machine Objects from SCCM	<input type="radio"/>	<input type="radio"/>
Information on - Preparing W10 USB Drive	<input type="radio"/>	<input type="radio"/>
Information on - Dell Model Bios Settings	<input type="radio"/>	<input type="radio"/>
Information on - HP Elite X360 & G2 Model Bios Settings	<input type="radio"/>	<input type="radio"/>
Information on - HP Dragonfly Bios Settings	<input type="radio"/>	<input type="radio"/>
Build Info - Computer is a Laptop ?	<input type="radio"/>	<input type="radio"/>
Build Info - Colleague an Existing user ?		
Backup Info - Backup performed to USB Hard Drive ?	<input type="radio"/>	<input type="radio"/>

Backup Info - Computer has Offline File Synchronization enabled?	<input type="radio"/>	<input type="radio"/>
Information on - Japanese Keyboard Layout to 106/109	<input type="radio"/>	<input type="radio"/>
Information on - HP Active Pen Setup	<input type="radio"/>	<input type="radio"/>
Information on - HP Supplemental Guide	<input type="radio"/>	<input type="radio"/>
Hardware Info - Computer model is Dell 5510 - 5550 ?	<input type="radio"/>	<input type="radio"/>
Hardware Info - Computer uses a WD15 Docking Station	<input type="radio"/>	<input type="radio"/>
Information on - SCCM AD HOC Profiling	<input type="radio"/>	<input type="radio"/>
Information on - Dynamic MIF Utility (DMU)	<input type="radio"/>	<input type="radio"/>
Information on - Smart Office Configurations	<input type="radio"/>	<input type="radio"/>

Windows 10 - Production Build Checklist

CASD ticket number	Date	Colleague name	Domain ID	Employee ID
Technician name	Computer name	Computer model	Serial number	Asset number
Existing user?	Offline Files?	Dell 5510/5520/5530/5540/5550?		

Build Troubleshooting

Troubleshooting Steps

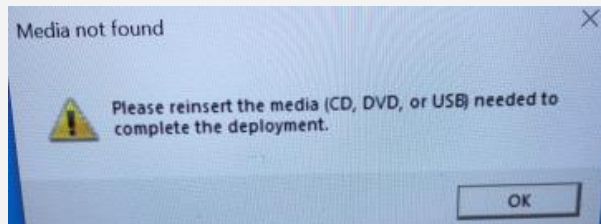
USB Build Drive (DAD Drive)

1. If your previous build process failed and you find your USB drive not being found in BIOS you will need to rebuild or decrypt your drive.
2. On your machine with Encryption exemption in place connect your USB Drive and you will verify if the "EFI" folder has been renamed to EFI.WIP in the USB Drive. You will manually rename this folder back to "EFI". This folder is renamed when files are written back to the USB drive when a machine build fails.
3. Once the "EFI" folder is renamed you will need to decrypt your USB build drive again before you continue to build new machines.

USB Build Drive (DAD Drive) not found message

1. When building the PC if you see the "Media not found" pop-up message as shown below.

Media not found



2. You need to perform the following steps:
 - a. You need to press F3 or (Fn+F3 depending on model) to enable mouse and keyboard.
 - b. Unplug the USB Stick.
 - c. Plug it back in.
 - d. Click "OK" on "Media not found" message to resume the build of the PC.

General BIOS Error Messages/LTI Build Process Error Messages

1. Loading FreeDOS No KERNEL SYS - **UEFI was not selected in BIOS Setup.**
2. Dirty Environment found - **LTI Build Process failed or Win10 machine was rebuilt without UEFI selected in BIOS Setup.**
3. Computer object not in expected location - **Rebuild of Win7 machine needs to be moved in correct OU for Win10 machines. Click "Yes".**

Deleting Machine Objects from SCCM when Redeploying Workstations

Redeploying Workstation Steps

To prevent software from being incorrectly pushed to a machine when being redeployed:

1. Launch the ADHOC Profiling Tool.
2. Navigate to the Administration Menu and select "SCCM Machine Deletions".
3. Enter the former machine owner's name or Employee ID or you can also enter the specific machine name if user information unknown.
4. Click "Search" in the Actions Panel on the left side of the screen.
5. Select the machine from the results list.
6. Click the "Delete From SCCM" icon in the Actions Panel on the left side of the screen to remove the machine from SCCM.

Note: KB Article#456170 covers this process

Build Preparation

Preparing USB Drive

To determine what build you should be using based on OPCO and colleague please review the deployment matrix:

<http://mgmti.mmc.com/teams/do/windows/win10/SitePages/Deployment%20Schedule.aspx>

Disk Prep Utility - Rufus

1. Copy rufus-3.1.exe from location below to 'C:\Support\' of local workstation used to format the drive.
\\mgd.mrshmc.com\sysvol\mgd.mrshmc.com\scripts\Win7ADScripts\Tools

Rufus Configuration

1. Launch the executable with MGD\xxx_Do account (Admin rights are required)
2. Ensure the correct USB drive is selected under Device on the Rufus interface.
3. Set Partition Scheme to MBR partition scheme for BIOS or UEFI
4. Set File System to Large FAT32 (Default)
5. Set New Volume Label as MMC_WIN10
6. Click Create a bootable disk using and ensure option is set to FreeDOS

7. Create a bootable disk using open is checked with FreeDos selected
8. Click Start once all options are selected
9. Confirmation Screen will be displayed once drive formatting has completed

Win10 Full Source Script by Region

APAC	Robocopy /MIR /FFT \\aumel61ns3vf4.MGD.MRSHMC.COM\apac_deskeng\$\Win10Build\20H2\USB D: (D: or the letter for the USB drive)
EMEA	Robocopy /MIR /FFT \\gbbbed61ns1bv5.emea.mrshmc.com\emea_deskeng\$\Win10Build\20H2\USB D: (D: or the letter for the USB drive)
NASA	Robocopy /MIR /FFT \\dfwnsmgtisrv01.mgd.mrshmc.com\nasa_deskeng\$\Win10Build\20H2\USB D: (D: or the letter for the USB drive)

Windows 10 - 20H2 Build

1. Connect your USB drive(s).
2. Open an Elevated Command Prompt it should show Administrator at the top of the Command Prompt window.
3. Execute Win10 Full Source Download command based on your region as shown above to start the copy/update to your USB drive.
4. Command prompt when complete will show you how many files were copied over close the window and decrypt your drive after the update/copy.

Notes:

1. Ensure to run the script while connected to a computer with the EEFF exception policy applied.
2. Always decrypt the USB Drives before and after you run the full source script to ensure the DAD drive will function properly. Failure to do this can result in core applications and drivers not installing on the builds.
3. Make sure you label your drives for the OS Install that is prepared on the drive.
4. To update changes to the build sticks, run the correct Full Source Command associated to your region to build the USB drive. Decrypt after the update.

Dell Hardware Specific Bios Settings

Note: Not all hardware models are covered at present and as we obtain them we will add to the build documentation.

Un-supported models - The Win10 20H2 Bare metal and IPU builds does support the E7440, Optiplex 7010 and 7020 (as of Aug 10th) - for the desktop models DE have stated specific pre-requisites -

In order to prepare the Dell 7010/7020 Desktop models for a Win10 - 20H2 - SM will need to ensure the following :

IPU Build -for desktops assigned to colleagues : (remote / in the office)

- Install the Intel driver support assistant - update the Intel RapidStorage driver - (7020 model only)
- Install the Dell DCU - update the BIOS/Drivers.
- Schedule the IPU with the Win10 team.

BM build: -for shared desktops in offices (conference/file rooms etc.)

- Perform a BM Win10-20H2 build & ensure the DCU option is checked
- Install the Intel driver support assistant - update the Intel RapidStorage driver - (7020 model only)

Laptop Bios Settings

1. When first turning on computer begin tapping F12 at the Dell Logo
2. On Boot Menu arrow down to "Other Options" and choose "Bios Setup" and select "Enter"
3. Navigate to Secure Boot Enable>Set Secure Boot to Disabled. On New Dell Bios: Navigate to Boot Configuration>Secure Boot>Enable Secure Boot>Turn off
4. Exit BIOS and Save Changes. Machine will reboot.

HP Hardware Specific Bios Settings

Note: Not all hardware models are covered at present and as we obtain them we will add to the build documentation.

Laptop Bios Settings

1. When first turning on computer begin tapping ESC at startup.
2. On "HP Computer (Bios) Setup".
3. AHCI can be ignored as this option is not relevant
4. Legacy ROM support & Secure boot are a single option
 - a. Advanced>Secure Boot Configuration = Select Legacy Support Enable and Secure Boot Disable
5. Go to Advanced>Boot Options = Uncheck Fast Boot
6. Go to Advanced>Option ROM Launch Policy>Configure Option ROM Launch Policy = All UEFI
7. Save changes to BIOS and Reboot PC

Important: You may see a message asking you to verify a number code before making a change to secure boot make note of the number.

HP Dragonfly Specific Bios Settings

Note: Not all hardware models are covered at present and as we obtain them we will add to the build documentation.

Laptop Bios Settings

1. When first turning on computer begin tapping F10 at startup.
2. On "HP Computer (Bios) Setup".
3. Go to Advanced>Boot Options = Uncheck Fast Boot
4. Legacy ROM support & Secure boot are a single option
 - a. Advanced>Secure Boot Configuration = Select Legacy Support Enable and Secure Boot Disable
5. Save and exit Bios.
6. After reboot begin tapping F10 at startup to re-enter HP Computer Bios Setup.
7. Go to Advanced>Option ROM Launch Policy>Configure Option ROM Launch Policy = All Legacy
8. Save changes to BIOS and Reboot PC

Important: You may see a message asking you to verify a number code before making a change to secure boot make note of the number.

Provision for Remote Access (New Colleagues)

Open <http://quickrequest.mmc.com> on your browser to push appropriate AD Group Permissions needed to access VPN and OWA;

- a) On the main page of quickRequest click on the icon "Application Access".
- b) On the menu opened on the left, select the option "Remote Access Management".
- c) Select the "Remote Access Management" option.
- d) Add the user first and/or last name and click the "Search" button.
- e) Select the appropriate colleague to populate all the necessary information in the form.
- f) Active Directory group memberships will be selected automatically for VPN access; If colleague requires remote access for OWA, mark the group for OWA.
- g) In the Action section, select the option "Set up new user (No remote access or token).
- h) In the Token Type section, select "Soft".

i) Click the button "Add to Cart" to proceed.

j) A new page will be open for you to review the requests added to the Cart, click the "Submit Request" button to complete the process.

Begin Build Process

Ensure the Computer Asset in CMDB is set to a "Reserved" status before you start the build.

Perform Data Backup

Backup is performed using the DDMT Software. The software is designed to work with both Windows 7 and Windows 10. The software consists of two folders a DDMT and a DellPCBackup folder. The backup and restore applications exist in the DDMT folder and backups are saved into the DellPCBackup folder. Both folders should be copied to the external USB drive or shared network location used for this purpose.

\\mgd.mrshmc.com\sysvol\mgd.mrshmc.com\scripts\Win7ADScripts\Tools\DDMT

Note: USB External Drive (500GB) is recommended for Backup Drive (DDMT).

Important: If performing manual backups ensure data is fully decrypted before restoring back to new machine or existing machine.

☐ Connect Old (Source) PC to network and power on

☐ Log into McAfee Drive Encryption

☐ Log into Windows as User and wait until Desktop is fully loaded.

☐ Synchronize all Offline Files in 'Sync Center' completely.

☐ Right-click on the **Lync/Skype for Business** icon in the System Tray and select 'Exit'.

☐ While pressing the 'SHIFT' key, right-click on 'Launch_PCBackup.exe' from the **DDMT** folder and select 'Run as different user'.

☐ Enter your "MGD\USERNAME_do" account credentials.

☐ Select 'Yes' for the **User Access Control** prompt.

☐ When prompted "**Files and Folder v.4.2**" was detected on this PC.....Proceed with the uninstall?". Select "**No**" as EEFF is no longer installed with the image and is accessible on the new build.

☐ Select '**USB Drive**' in the Migration Type to Perform and click 'Next'.

☐ It will automatically fill out the folder name with the machine's Serial Number. If it is OK, click 'Start'.

If you prefer to use User's AD ID as a folder name, click 'Back'.

☐ Select the **Deployment DAD USB** drive from the drop-down list that you would like to use to store the migration data. If your drive does not appear, click on 'Rescan'.

☐ Click 'Next' enter User's **AD ID** in the '**Unique Folder Name Value**'.

☐ Click 'Next' and 'Start'.

☐ Upon completion of the DMT backup process, the window "**Data Backup Completed Successful**". Click 'OK'

☐ Verify that the USMT.MIG file was created in **DellPCBackup\FolderName\USMT**.

☐ **Unplug** in the DAD Deployment USB hard drive from the Old (Source) PC and **shut down** the PC.

☐ Select '**Network Location**' in the **Migration Type** to Perform and click 'Next'

☐ Fill out the information for the target location, such as replacement PC or utility server.

Enter **Backup Server**: [server name / machine name / IP Address]

Enter **Share Name**: [share name]

Enter **Unique Folder Name Value**: [folder name]

☐ Click 'Next' and 'Start'.

☐ Upon completion of the DMT backup process, the window “**Data Backup Completed Successful**”. Click 'OK'.

☐ Verify that the **USMT.MIG** file was created in the target location and **shut down** the old PC.

Staging Process

☐ Windows 10 Build Installation

1. Start computer and immediately start tapping **F12 key** for boot options menu and choose the USB Staging Drive
2. Select the USB device listed under UEFI section to ensure proper load
3. Review Welcome screen (connect power and network if not already present) New feature in window provides you which Windows version you are using in the build stick and the date it was updated.

If build stick is out of date you will be prompted to update before proceeding

NOTE: DO NOT remove the USB stick until instructed to do so later in the build process.

4. Select the appropriate parameters (**OPCO***, **City**, **Domain**) from Configure MMC Settings configuration within LTI,
5. Check the Additional PC Options (Run hardware vendor updates automatically for drivers & firmware for SD WAN enabled sites only) and 'check' Ensure SCCM Client is up to date on build drive, click 'Next'

IMPORTANT: USER ACCOUNT AND COMPUTER MUST BE IN THE SAME DOMAIN ALWAYS

6. The followings should be selected/entered:
 - a) **Primary User** – [AD User Name]
 - b) **Builder ID** –[Tech ID]
 - c) **Is user remote or office based?** – [Office or Remote User]
 - d) **Is this user's primary computer?** Yes or No
 - e) **Is this a call center PC?** Yes or No
 - f) **Which Office 2016 architecture should be installed?** 32-bit or 64-bit
7. MMC CMDB Configuration:
 - a) Enter Asset Tag
 - b) Define Asset Role by default Loaner PC is set to "No". Change to "Yes" if you are setting up a Loaner PC.

NOTE: DO NOT select to install Office 64bit unless you have formal OpCo IT Approval. No other approval is accepted. This is only released for production for Guy Carpenter use at this time!

8. Click 'Next'.
9. Select the appropriate parameters (UI Languages) from Language Packs configuration within LTI click 'Next'.
10. Select the appropriate Regional parameters (Language to install (**Make sure you select the Language to install according to your Country i.e. Spanish for Spain**), Time and currency format, Keyboard Layout, Time zone) from Locale and Time configuration within LTI, click 'Next'.

The 'LTI Installation' progress bar will display and show progress as the build proceeds.

The PC will reboot automatically and login to windows automatically as the build processes

NOTE new feature: The machine should never lock during the build. The build will proceed automatically showing Configuration Manager (SCCM) running progress bar. This process can take an additional 30 minutes or more while waiting for SCCM reboot to be needed.

If you see that the build fails you will see an alert screen similar to the screenshot below.

If error showed above occurs press F5 to see the screen with some details of what caused the failure. (If the failure was a result of the Dell Command Update tool; you must start the build again not selecting the box to "Run hardware vendor update"). Otherwise review the reason for the failure and respond accordingly.

Upon Completion, the PC will wait at the Windows 10 Ctrl-Alt-Del Login Screen

11. Remove USB Flash Drive

12. Login to computer with MGD\username_do account

SCCM Wakeup and Profiling

☐ **DMU Activation**

NOTE: Only complete DMU if there is no restart prompt. After restart the DMU will open again and you can complete.

DMU should launch automatically (may take up to 10 minutes). **Only perform the below manual steps if DMU is not automatically launched during this time period.**

Manual steps to launch DMU

1. Open a command prompt and enter the following commands

```
cd\  
cd program files\  
cd MMC  
cd dmu  
dmu /logonchecks
```

☐ 2. **Choose your build type**– For all other build types see Information on DMU

Standard Build - Computer assigned to specific Colleague

Language: Select Language

Note: Leave Language at English(Default) as DMU does not manage the font change properly.

Employee ID: Enter Employee ID

Machine Type: Select Laptop, Desktop or VM

Remote User: Select appropriate

Primary Machine: Select Yes (No selected by default)

3. Click on “**Validate**” and verify colleague information is correct and click on “**OK**”

4. Click on “**Build**”

5. Close Command Window.

6. You may log out of machine but **don't restart** prior to 30 minutes after DMU setup.

SCCM Core Application Installs/Hardware Drivers & Firmware (BIOS) Updates Required

Allow Core Applications to begin installing and restarting system where required. Proceed with hardware driver and firmware installs from the manufacturer's website in non-SD WAN enabled sites.

Note: If after 3 hours none of the core applications are installed, notify Win10 Tactical and Deployment Leads by opening a CA Incident ticket with machine name and domain and assign to the MGTI GL Win10 Tier 3 Supt queue.

After Core Application installation completes (except MDE), login as colleague to proceed with next build steps.

Perform Data Restore

NOTE: If colleague is an O365 user DO NOT log into OneDrive before performing data restore.

Important: If performing a manual backup and restore ensure you fully decrypt all files before restoring to a new computer or existing computer.

☐ While pressing the ‘SHIFT’ key, right-click on ‘**Launch_PCRestore.exe**’ from the **DDMT folder** and select ‘**Run as different user**’.

☐ Enter your “**MGD\USERNAME_do**” account credentials.

☐ Select ‘**Yes**’ for the User Access Control prompt.

☐ Select ‘**USB Drive**’ in the Migration Type to Perform, click ‘**Next**’

- ☐ Select the **Deployment DAD USB** drive from the drop-down list that you would like to use to restore the migration data from. If your drive does not appear, click on '**Rescan**', click '**Next**'.
- ☐ Delete the auto-filled information in the '**Enter Folder**' Used for the Backup and click on '**Browse**'.
- ☐ Browse to the USB drive **\\DellPCBackup\FolderName (do not include USMT)** and click '**OK**', click '**Next**'.
- ☐ Verify the USB migration selections – USB Drive Letter and Backup Store Path and click '**Start**'.
- ☐ Upon completion of the DMT restore process, the window "**Data Restore Completed Successful**". Click '**OK**'.
- ☐ Delete the '**USMT.mig**' file from the **DAD Deployment USB hard drive**.
- ☐ **Unplug** in the **DAD Deployment USB hard drive**.

☐ Select '**Network Location**' in the Migration Type to Perform.

☐ Fill out the information for the **USMT MIG** location, such as replacement PC or utility server.

Enter **Restore Server**: [**server name / machine name / IP Address**]

Enter **Share Name**: [**share name**]

Enter **Unique Name Used for Backup**: [**folder name (do not include USMT)**]

- ☐ Click '**Next**' and '**Start**'.
- ☐ Upon completion of the **DMT restore process**, the window "**Data Restore Completed Successful**". Click '**OK**'.
- ☐ Delete the '**USMT.mig**' file from the **USMT location**.

☐ **How to setup Japanese Keyboard Layout to 106/109**

KB Article#455671 covers setup instructions

Process to change Japanese Keyboard Layout from 101/102 to 106/109. Requires elevated rights account(i.e._do, _app, etc.) to perform required changes in the Japanese Keyboard layout.

- 1. Click the Windows logo i.e. Start button.**
- 2. Select "Settings"**
- 3. Select "Language"**
- 4. Select "Region & Language"**
- 5. Select the language "Japanese" to show the available options.**
- 6. Click the "Options" to show available keyboard layouts to Japanese language.**
- 7. Click in the "Add Keyboard or Change the Layout" Option**
- 8. Choose "Japanese Keyboard (106/109)"**
- 9. Close all screens and restart the computer so the changes can take effect**

User Software Configuration

Login with colleague account

Run from C:\Support\BuildScripts\MGTI_Build_Config.cmd

Zoom

- 1. Select "Sign in" then select "Sign in with SSO"**

2. Verify "MMC" is entered for the company domain and select "Continue"

3. Close Settings Window

Outlook 2016 - Allow email to fully download while you continue with the build steps (If you see the M365 Authorization window ensure you configure MS Teams & OneDrive accordingly)

M365 MS Teams & OneDrive - Sign into both applications with colleague's primary email address and accept the defaults. (If MS Teams is not found on device push the application from ADHOC Profiling Tool or download from the Web application portal for MS Teams.)

Install Printers

Option 1. Based on your region you may install printers using regional printer scripts for your local print servers.

Option 2. Open File Explorer>Type \\\"Print Server Name\" hit \"Enter\".

Locate desired printer(s) and double-click print device to install the print drivers and printer.

Note: You may get a prompt to install print drivers. Select \"Install\".

Option 3. Local printers may require download of drivers from manufacturer's website to install.

Note: Verify network printers are installed and you have set the default printer.

V24 Wireless (see build info pages for wireless troubleshooting)

1. Disconnect Ethernet Cable

2. Network connection Icon should change from Direct Connection to a Wireless Connection

3. Click on the icon and list of available wireless networks should appear

4. Choose V24 and select Connect. V24 wireless should connect.

5. Reconnect Ethernet Cable

Install McAfee Drive Encryption

1. Install “McAfee_Drive_Encryption_x64-7.2.9.17-R1” from ‘Software Center’. Select ‘Continue’ to run the package when prompted.

****Note: It is imperative that you install the most recent BIOS update from the vendor prior to installing McAfee Drive Encryption.****

2. Restart the PC after McAfee Drive Encryption finishes installing.

3. Log back in with User’s Domain account.

If prompted select "Continue" at the MMC Deployment Message 'The new hard drive encryption software has been successfully installed on your computer...'

4. Navigate to C:\Support folder and double click on MDE.bat. (This batch file runs all the actions from the McAfee Agent Monitor which will speed up the Encrypting process of the drive)

Note: Computer must not be delivered unless confirmed MDE installed and fully encrypted or an approved exemption from Security is documented. HP models require MDE_USB and MDE_OSK tags to be applied to the machine by your region's Level 2 MDE Support Tech when MDE is installed.

After installation of MDE and reboot is performed removal of the SCCM Build Mode needs to be performed before delivery of machine to colleague.



Quality Assurance Checklist

Verify **Drive Mappings are shown** (Run "Map My Drives" from desktop if not shown) (**Local Developer Administrators do not map drives**).

Click on the **McAfee icon** in the Notification Area, select **Update Security** to allow McAfee Agent to update.



Click on the **McAfee icon** in the Notification Area, select **McAfee Endpoint Security** to open ENS, click "Update Now" to allow virus definitions to update.

Click on the **McAfee icon** in the Notification Area, navigate to **Quick Settings>Show Drive Encryption Status** and verify that C: is **encrypted**

Log out of the user's profile and sign in with your MGD_DO Account. Run the "Finalize Build" Shortcut on the desktop this will update CMDB, trigger return SCCM to Normal Mode, and generate the MGTI System Report that will display on your screen.

Notes:

Validate all Core Apps have installed by reviewing the MGTI System Report displayed on screen. If upon review of the Missing Core Apps tab you note that there are Core Apps missing review Software Center and remediate as appropriate.

If CMDB Automation fails to update CMDB you must update Asset manually.

Build Process Complete

Documentation and Asset Management

Deploy the new machine and send out an email “**New Hire Communication**”.

<http://mgti.mmc.com/teams/do/SitePages/NewHireDocumentation.aspx>

Change Order

Add **Configuration Items** assigning hardware action to **Change**

Required for Compliance: Attach completed checklist to the CA Ticket (Change Order or Incident) when build is complete.

HP Active Pen Setup

Pairing the Bluetooth pen with your tablet

1. Turn on your tablet.
2. Turn on the pen by tapping the tip to any surface.
3. Press and hold the Bluetooth on top button for 5 seconds to enable Bluetooth pairing. When the pen is ready to be paired with a device, the Bluetooth light slowly flashes blue.
4. From the tablet, type Bluetooth in the taskbar search box, and then select "Bluetooth settings".
5. Select Devices, select Connected devices, and then follow the on-screen instructions.
6. The following table defines the actions of the Bluetooth status light.

Bluetooth Status Light

Slowly flashing	The pen is in pairing mode.
Rapidly flashing blue	The pen has paired successfully.
Blinks blue when the Bluetooth button is clicked	The pen is working normally.
Blinks red when the Bluetooth button is clicked	The Pen needs to be charged.

6. Link to pairing video for HP Active Pen: <https://www.youtube.com/watch?v=7AtnvtCH2yM>.

Note: HP Active Pen is only available for the HP Elite X2 G4 2in1 Tablet.

HP Supplemental Build Guide

Download a copy of the HP Elite X360 and G2 Supplemental Build Guide from here for more HP machine information: [HP Elite X360 and G2 Supplemental Build Guide version 3](#).

Download a copy of the HP Driver Update document: [HP Driver Update](#)

Dell Precision M5510 - 5550

Issue - No internal Ethernet component.

Required: **Generic USB Ethernet Adapter** and **Thunderbolt Ethernet Adapter**

Build Process Differences

1. Boot with the Dell Ethernet-thunderbolt adapter and install as usual.

2. When you reach the point to do a Server Sync switch to a Generic USB Ethernet adapter to be able to perform a server sync.

3. During the LTI Process “**join the domain**”, You will receive an error which will not allow you to continue. When that happens replace the adapter Ethernet-USB adapter with the Dell Ethernet-thunderbolt. Either pursue the install, or restart the computer (the install will restart from step 6 and should progress as usual)

(Suggestion: connecting both Dell Ethernet and Generic USB to network ports when building to avoid any prompting)

WD15 USB-C Dock

Applies to new certified hardware models, Dell 7280/7480/5520

Applies to existing certified hardware model, Dell Precision M5510

With the latest round of laptops the E is gone from the name as the E-dock is no longer compatible, instead

the new laptops (as well as the older 5510) are equipped with a USB-C port and therefore a new USB-C dock will be used. Like the old dock the new one is a single connection to provide access to all the peripherals such as keyboard, mouse, screen & network, as well as power the laptop.

Note:

1. Connecting an unpowered laptop to the USB-C dock automatically powers it on.

2. If a laptop supports Thunderbolt the LTC must ensure ‘Thunderbolt Adapter Boot Support’ is enabled in the BIOS to ensure the external [USB] Keyboard & Mouse is available during the MDE prompt at login.

Dock Firmware Updates Required

In addition to confirming/updating (flashing) the Firmware of the laptop, LTCs should also ensure the Firmware of the docking station is up to date each time a system is rebuilt. After the PC is built fully refer to the instruction on how to do this here: <http://www.dell.com/support/article/us/en/04/SLN301970/wd-15-dockbios---drivers-installation-guide>

AD HOC PROFILING

ADHOC Profiling Tool– This replaces the SCCM Collection Management Utility (CMU) to advertise programs to Windows computer with the upgrade of SCCM from 2007 to 2012. The tool is located at the following URL: <http://w7appprofiling.mrshmc.com/Profiling/UI/Default.aspx>

If you cannot access the tool you will need to be added to one of the following groups:

GLB-MGTI-Desktop_Ops

MGTI-DO-Deskside_Admins-S-G

MGD\GLB-MGTI_SD_Tier1_Analysts-S-G

Information on profiling and how to use the tool is available at http://mgti.mmc.com/home/Pages/windows7_app_profiling.aspx

Dynamic MIF Utility

The Dynamic MIF Utility (DMU) automates the creation of the MIF file during the workstation build process and manages updates to the MIF file when a colleague's HR data changes; for example, when someone transfers to a different department or location.

Build Methods

A complete range of build types are available to be used for specific scenarios. Review the below and use the build method that best fits the situation.

Build for a specific colleague with known Employee ID

1. This is the standard build process where a computer is being assigned to a specific colleague and the employee ID is already available.
2. This is the preferred build method and should be used for the majority of builds.

Pre-Build where Employee ID is unknown

1. This build option introduces efficiency to situations that require a high volume of builds, fast turnaround time and an employee ID is not yet available.
2. A finalize option then completes the build once the employee ID becomes available and must always be used before moving the computer into production.

NOTE: Less information added to the prebuild selections may be preferred as if any mismatch occurs when finalizing DMU it will generate an ORBCDL error. This requires manual deletion of the MIF then reboot and enter the EEID for a specific colleague to finalize.

Training Computer

1. This should be used for shared computers – not in a Call Centre – such as test computers, hot desks, loaners, kiosk computers, etc.
2. Known HR values including business, department and location are entered to trigger profiled applications to install.

Call Center by Employee ID

1. This is the standard build for Call Centre computers where ad hoc applications need to be deployed to subsets or individuals within the Call Centre.

Call Center by Department

1. This is the standard build where Call Centre computers are not allocated to specific colleagues.
2. Known HR values including business, department and location are entered to trigger profiled applications to install.

DMU Commands

1. DMU Initial Activation after install if no MIF File Present

C:\program Files\MMC\DMU\DMU.exe /logonchecks

2. DMU to re-profile a computer for a new colleague (Create new MIF)

C:\program Files\MMC\DMU\DMU.exe /forcenew 123456 (123456 should be the CA Ticket #)

3. DMU to run HR Changes. Will prompt colleague major changes required.

C:\program Files\MMC\DMU\DMU.exe /actionmajor 123456

Smart Office Configuration

Smart Office Drivers

DisplayLink Driver 9.1.1462.0-R1

All sites will use Cisco Jabber

☐ Cisco Jabber Configurations for APAC (Tokyo,Coniston,Brisbane,Wellington), EMEA, and NASA

1. Push Cisco Jabber 12.9.3.54813-R1 from App Profiling tool
2. Jabber will install automatically from Software Center and prompt for a restart
3. Open Cisco Jabber Application
4. Enter (Employee ID)@mrshmc.com
5. Enter Network Password
6. Hit "Next" on all questions to complete initial setup
7. Click on person icon in top left of application, go to settings, ensure tick box "Start Cisco Jabber when my computer starts" is selected.
8. Click on Audio tab and setup Ringer, Speaker, and Microphone accordingly.
9. Hit "Apply" and "OK" to save settings changes.