Queen Mary
University of London

Queen Mary
University of London

IT Services

Getting to know your Windows Staff Desktop

v17.0

Introduction 4

Managed Staff Desktop Service 4

Managed Research Desktop Service (mRDS) 4

The First Day 5

The VPN Provisioning Tunnel 5

Logging into the Provisioning Portal 5

After Provisioning Log In 6

Checking and Installing Software 7

Software Updates 7

Hardware Drivers - Dell Update 7

Software Updates – Windows Update 7

Rights and Restrictions 8

ITS Policy 8

ITS Documentation and Information 8

Administrator Rights 8

Applications 8

The OS - Windows 10 9

Your Start Menu 9

Finding your computer name 9

Signing out, shutting down or Restarting your PC 10

Signing Out 10

Shutting Down or Restarting 10

Security 11

Forticlient (CLN-MS only) 11

Windows Defender (CLN-RS, CLN-TS) 11

Working with Applications 12

Self-Service 12

Software Centre 12

Install 13

Repair and Uninstall 13

Synchronising Your Machine for Changes 13
Company Portal 14
Apps on the taskbar 14
Pinning apps you have open 15

Microsoft Teams 16

BitLocker – Hard Drive Encryption 17

Eduroam (and other Wi-Fi) - for QMUL laptop users 18

Fortinet VPN 19

VPN Connection Troubleshooting 19

File Services 21

The OneDrive app 21
Folder Locations 22
OneDrive Status indicators 23
Managed research desktop file storage 24

Virtualization using VirtualBox 25

Launching your Virtual Machine 25
Installing Quick Start Virtual Machines 25
Using the Quick Start VM Demo 26
Using your USB devices in your Virtual Machine 27
Custom VM Method 29
Removing Virtual Machines 29

Introduction

Welcome to the Windows Managed Service. You should hopefully have your shiny, new (or transferred) QMUL laptop. This guide will help get you started and cover some features of Windows & applications and working policies & processes that can assist with safe and productive working.
For more information, visit the QMUL ITS Self-Help Web Site , with guides and help on getting the most out of your tools.

Managed Staff Desktop Service

The Managed Staff Desktop Service was originally designed as an administrative work environment but has grown to cover a good spectrum of different roles at QMUL. By utilising multiple management platforms like SCCM, Azure and Active Directory, we can provide a well secured and somewhat adaptable system. Primarily the service deployment for a Windows device is defined by the device name prefix in SCCM (e.g. CLN-MS-…)

Managed Research Desktop Service (mRDS)

Predominantly aimed at research staff and students, mRDS provides an additional secure Virtual Machine for users to download and experiment with software as they please. The device still runs on a centrally managed service, but users can open a Virtual Machine also known as, Play Area / Dev Environment / Sandbox, to carry out their research requirements, whilst not compromising the security of the wider QM network.

mRDS inherits all the security and management features of the standard managed service including access to the wide and rich list of packaged application/software. A Virtual Machine is integrated as part of the mRDS build and this is the secure safe space/environment where users will have **full administrative rights** to carry out their testing, development, research, and teaching work.

Depending on your work requirements, you may be given an mRDS device with an integrated Virtual Machine. Further details on how to access your Virtual Machine are below.

File storage options for mRDS are slightly different, in that typical network share storage is blocked and provided instead via the Research Data Store. An mRDS device can be identified with the computer name prefix, **CLN-RS-...**

The First Day

So, you have plugged in your laptop and switched it on. There are 2 main scenarios to consider here:

- You collected your laptop directly from IT Services
- Your laptop was delivered to you at a remote location.

For the first scenario, the engineer will help get you set up when you collect the laptop or you can connect the device to the QM wired network yourself to get started. The second scenario, however, needs a unique step to load your user profile onto the device. This activates the VPN so you can finish onboarding your managed device.

The VPN Provisioning Tunnel

Firstly, you'll need to contact the Service Desk to enable the provisioning portal for your user account. Once they've confirmed it's added to the group, you can continue with the following instructions. To load your profile onto the device for the first time logging in, please follow these steps:

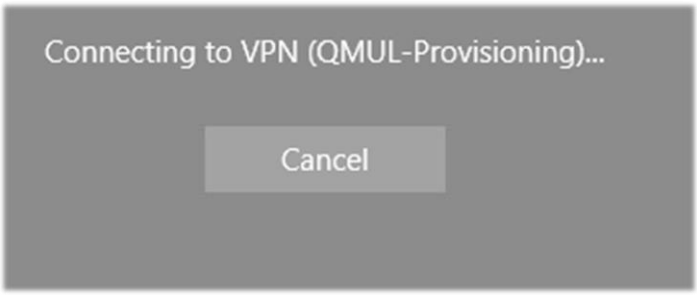
Logging into the Provisioning Portal

When you first get your machine, you are required to log into the provisioning portal at the Windows login prompt. This is done by:

1. Selecting sign in options at the Windows logon prompt and clicking the Fortinet shield

2. This will reveal the login options for the FortiClient VPN. The machine will be joined to the QM domain, so you can tick the Use my Windows credentials for VPN check box and then enter your QM standard user account.
3. **IMPORTANT:** You need to select the Provisioning option. You may need to scroll down to see it and the scroll bar can be hard to spot at first.

4. After hitting ENTER or clicking the right arrow button next to the password entry box, the logon process will begin and indicate that it is trying to connect to the VPN. This will take longer than a normal logon, due to the initial VPN connection and device sync.



5. Once the VPN connection is successful a prompt will appear providing this information. During the logon process the user settings (group policy) will run and the user certificate necessary for the normal VPN connection will be installed. The FortiClient icon in the bottom right will have a golden padlock to illustrate that it is connected.

After Provisioning Log In

Once you arrive on the desktop, be sure to spend at least 5-10 minutes before restarting or logging off to ensure all pre-requisites are deployed to your user profile. After this point, you will need to use “QMUL” or “mRDS” VPN profiles in Forticlient for normal access to QMUL resources. Read the Fortinet VPN section for more information

Checking and Installing Software

Once you are connected to the VPN, your computer will continue to synchronise with QMs on-premises systems. Expect this phase to take an hour or more. You can view the progress of your application installations by opening Software Centre from the start menu and checking the Installation Status page. You can also peruse and select from the available list of optional applications to install and Software Centre will handle these in a queued fashion.

Software Updates

An important part of setting up your laptop is making sure it gets up to date as soon as possible. Before this is completed, you may find functionality of the computer is sub-optimal. To resolve this, you need to run updates in two places.

Hardware Drivers - Dell Update

- Search for **Update** in the **start menu** and open **Dell Command | Update.**
- Once the app has opened, hit the **Check** button.
- Once the driver scan has finished, it should present you with the ability to run updates and restart. Hit the button to continue and make sure you haven't got anything important left to save (although you'll have some time before any restarts occur).
- **IMPORTANT - Make sure you have plugged in the power supply and do not disconnect any USB devices during the driver installations.**

Software Updates – Windows Update

- Type **Update** in the **Start Menu** and select **Check for Updates**.
- Once the window opens, hit the Check for Updates button.
- Windows should download and install updates in the background.
- If a restart is required at any point, it will ask you to restart when convenient. It's usually best to do this as soon as possible before you get too deep into work.

Rights and Restrictions

ITS Policy

As with all QM-managed devices, usage of a managed device must be in line with the provisions set out in the ITS Policy. The virtual environment, while self-managed, also requires adherence to many of these provisions.

ITS Documentation and Information

You can find an additional range of guides and information on ITS offerings in the Self-Help section of the QMUL ITS web site. You can also submit comments directly on these documents as feedback for review and improvement.

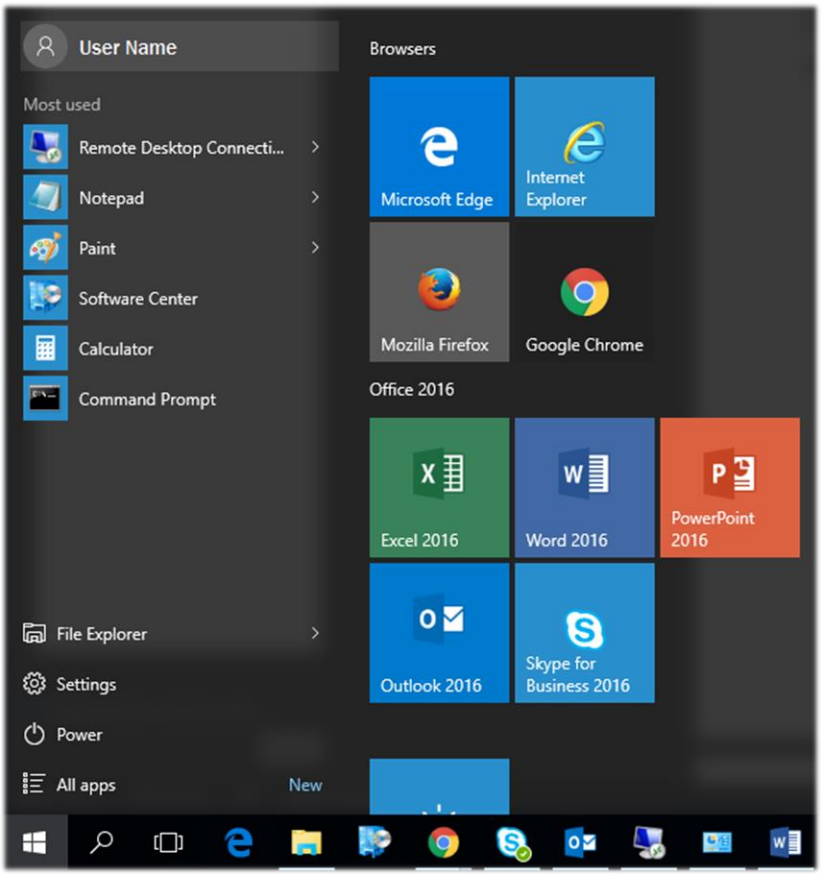
Administrator Rights

With all QM-managed devices, users are not given access to admin rights on their host machines. The virtual environment provided on mRDS devices is specifically designed to mitigate this requirement for most use cases.

Applications

While QMUL provides a large library of software for deployment, there are crucial factors dictating access to this software. The main criteria here are licensing and security. You may need to contact your faculty management and / or Business Support to gain licensed access to an application. Some applications may pose a security or compliance risk (particularly data storage solutions and communication tools) and cannot be made available to managed devices users. Again, the mRDS virtual environment can mitigate this scenario for software that you own / is free and is licensed for use according to your situation.

The OS - Windows 10
Your Start Menu



The tiles on the right show your web browsers and some office apps, and the list on the left shows your most used apps. To view all available apps, click "All apps" in the bottom left-hand corner of the menu. You can also search for an app from the start menu; simply open the start menu and begin typing the name of the app you are searching for.

You can return to the Start menu from wherever you are by pressing the Windows button on your keyboard.

Finding your computer name

There are several ways to find your computer name besides looking at the Service Tag sticker on the underside of the laptop.

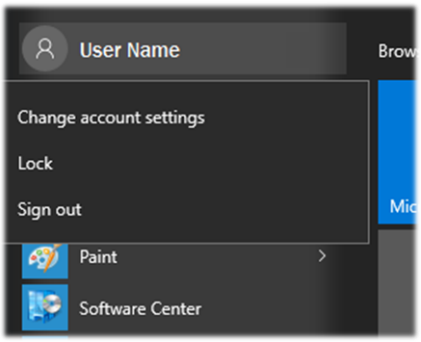
- Hold the ‘Windows’ key then hit ‘x’, followed by ‘y’.
- Open the start menu and search for name and select the ‘View Your PC Name’ option.

Signing out, shutting down or Restarting your PC

To help maintain a healthy working device, we strongly recommend you schedule weekly restarts. This helps it stay up to date and resolve certain pending operations.

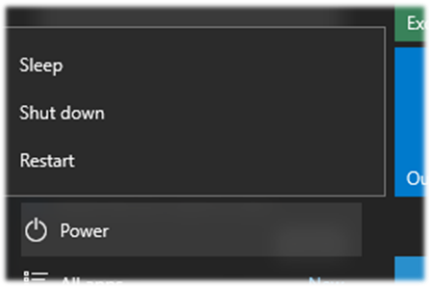
Signing Out

On the Start menu, click on your name, you will then be presented with three options: "Change account settings", "Lock" and "Sign out".

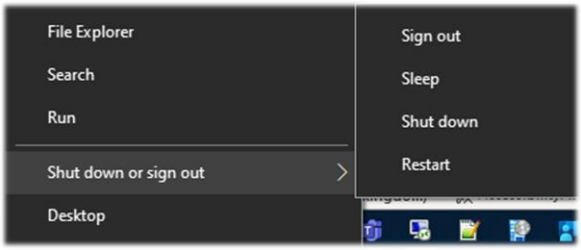


Shutting Down or Restarting

On the Start menu, click "Power", you will then be presented with three options: "Sleep", "Shut down" and "Restart". **It is recommended that you restart your device, at least once per week.**



Additionally, by right clicking the start button or hitting WINDOWS KEY + X, you can see the auxiliary start menu and perform the same power functions.



Security

Forticlient (CLN-MS only)

The Forticlient VPN function is only a subsystem of Forticlient's comprehensive security client features. Forticlient handles Malware protection, Vulnerability Scanning and more.

Windows Defender (CLN-RS, CLN-TS)

Microsoft Defender for Endpoint (MDE) is an enhanced version of the standard Windows Defender security platform built into Windows. It provides additional protection and intelligence on threats both based on your device and acting from a remote source.

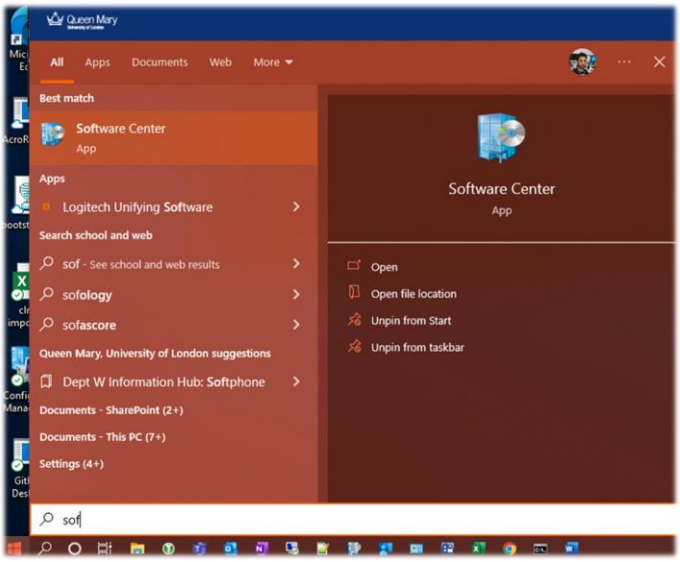
Working with Applications

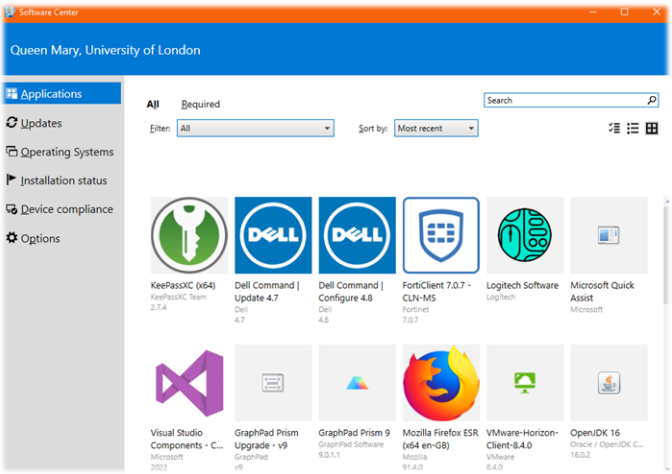
Self-Service

The key tools of the managed self-service experience are the Software Centre and Company Portal. Most fixed devices on campus will only have Software Centre, while Managed laptops usually have both. From here you can synchronise your machine's app profile, check for and install updates, run a device compliance check and synchronise the device with the management systems. Apps will not necessarily show up in both Software Centre and Company Portal, so it is good to check both apps, particularly if you are expecting some software to be available.

Software Centre

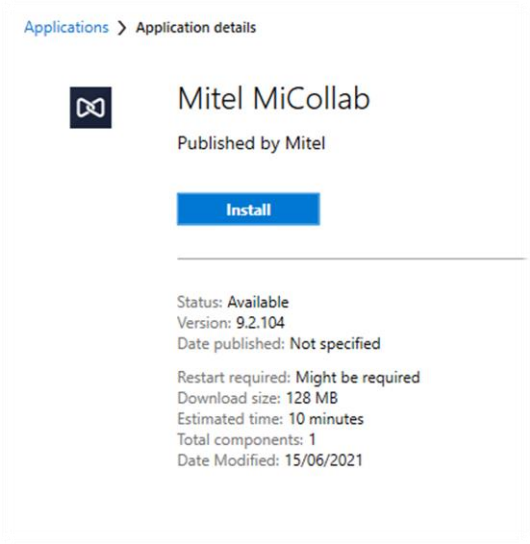
This app requires a connection to QMUL servers, so it will only function on the VPN or directly on the campus network (e.g., wired connection). You can find it by beginning to type Software Centre in the start menu.





Install

Click on the desired app and hit install. You may be asked to restart at a convenient time once the installation is completed, but for most applications, this is not necessary. This will often be available as an option before an app is scheduled to force installation. Should you need to get it out of the way at a more convenient time (e.g., not during a meeting), this should serve you well. Always be prepared for an unsolicited restart just in case... To this end, always make sure all work and data is saved to reduce the risk of trouble later.

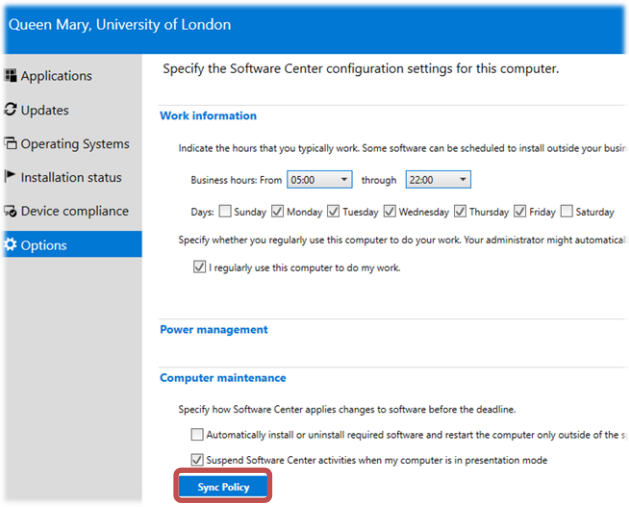


Repair and Uninstall

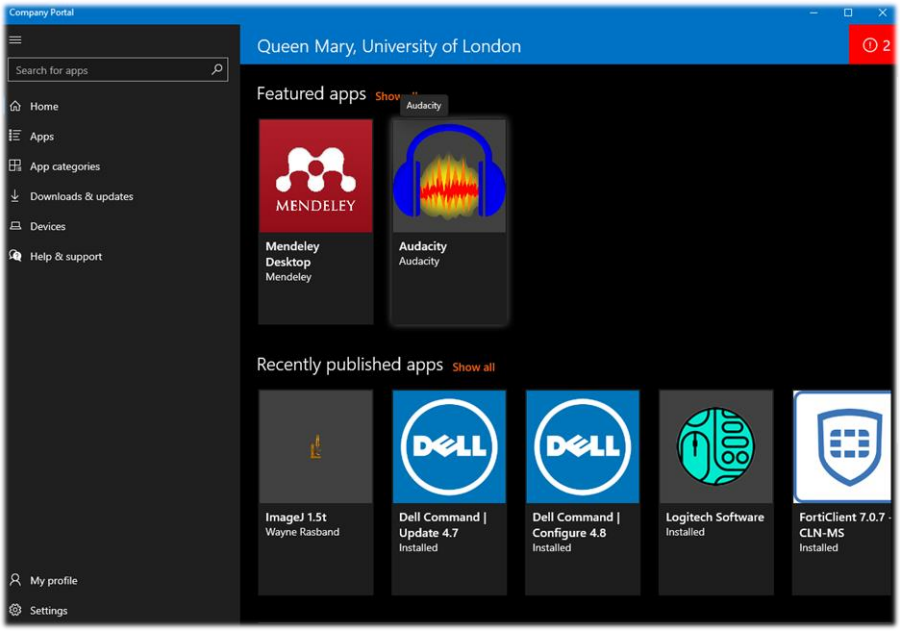
Once an app is installed, the install button will be replaced with an uninstall and / or repair button. These actions will not necessarily be available for any given app (indicated by a grey icon), particularly if the app is force installed onto the machine. The repair button can also be used for special functions like running a special task in an app (e.g., scan for updates)

Synchronising Your Machine for Changes

When expecting changes to your apps (e.g., new apps should be available), you can use the **Sync Policy Button** to speed up the process of making those available. This may not work as quickly as you expect but can help expedite matters. This is sometimes used when in consultation with an IT support staff member, though. You can find it in **Start Menu : Software Centre : Options : Computer Maintenance : Sync Policy**



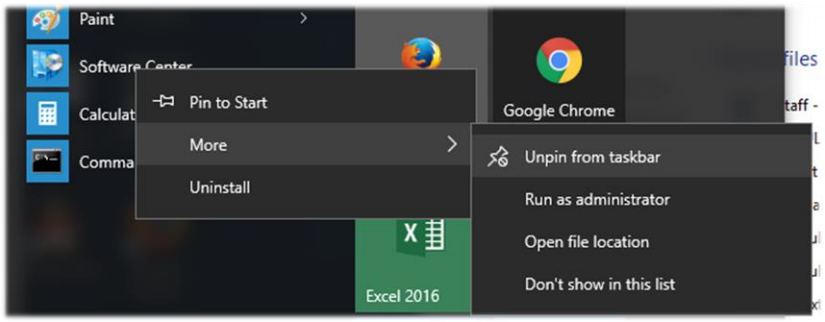
Company Portal



Installation is very much like Software Centre, in that each app has its own page and the available actions are located there, along with a description and metadata. There is no repair button available here, although a Reinstall button can sometimes be used. Synchronising policy is again handled in the options page.

Apps on the taskbar

Most apps can be "pinned" to either the taskbar, the Start menu, or both. This will ensure that a shortcut to that app is always available. To see pinning options for an app, simply right click its shortcut. The example below is from an app shortcut on the Start Menu, but you can right click on any app shortcut, for example on the taskbar or the desktop.



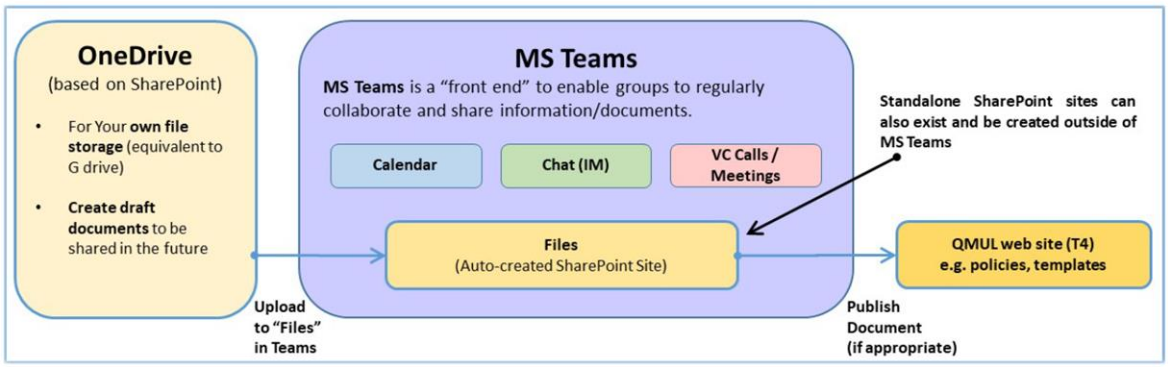
Pinning apps you have open

If you are already using an app, you can pin it to the taskbar without going to the Start screen.

- Right-click the app button on the taskbar.
- From the options that appear, click Pin this program to taskbar. The app you pinned will stay on your taskbar even after you close the app.

Microsoft Teams

Microsoft Teams is the University's recommended and supported online collaboration tool. Teams is integrated with other Microsoft 365 (formerly known as Office 365) products. It brings together everything you need to collaborate with groups of colleagues in one online workspace. As a conduit between OneDrive for Business and SharePoint Online, you can leverage its features Inc. Calendar, Chat (IM) and Voice and Video Calls/Meetings to share information and documents.



In **Microsoft Teams**, teams are groups of people brought together for work, projects, or common interests. Teams are made up of channels. Each channel is built around a topic, like "Team Events," a department name, or just for fun. Channels are where you hold meetings, have conversations, and work on files together.

A guide can be downloaded here: MS Teams Guide [PDF 1,245KB]

BitLocker – Hard Drive Encryption

BitLocker is a hard drive encryption program for Windows laptop users which may prompt you to set a PIN when you first sign into your laptop. This PIN will then bind to the encryption already present on your laptop hard drive, adding another layer of protection against unauthorised use. You will be required to enter your PIN each time you start your laptop.

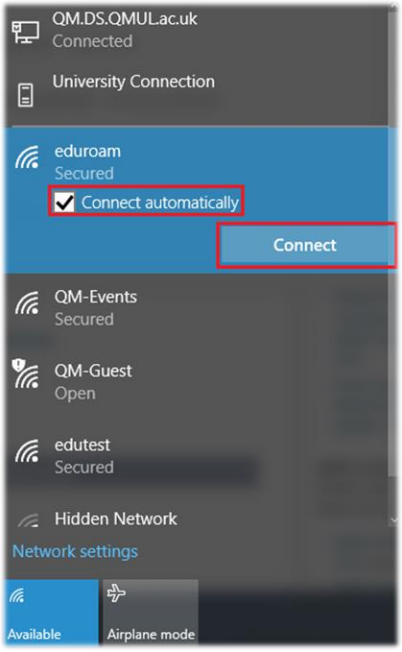
If you enter your PIN incorrectly, or forget it, you can access the recovery PIN from the IT Helpdesk.

Eduroam (and other Wi-Fi) - for QMUL laptop users

There are a few wireless networks available around the campus. The network you should mostly use to connect your laptop to the network is '**eduroam'**.

Connecting to eduroam

If you are a QMUL laptop user, the easiest way to see available wireless networks is to click on the wireless icon in the notification area of your taskbar, which is located at the right end of the taskbar.

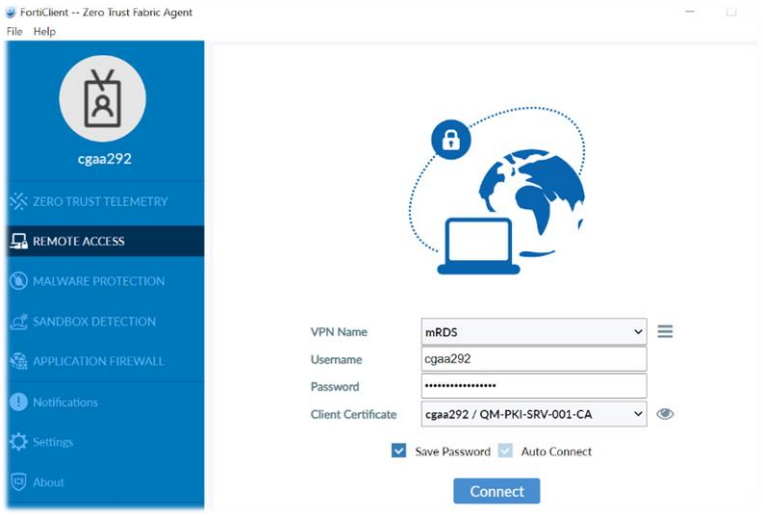


Upon choosing eduroam, you will be prompted for your **QMUL username and password**. You will need to enter your username in the format abc123@qmul.ac.uk (please note that this is **NOT your email address**).

Do not forget to tick the **'Connect automatically'** box, so you do not have to enter your credentials each time you connect. Click **Connect**.

Fortinet VPN

ITS may set this up for you, ensuring your machine is able to connect to the QMUL VPN to access necessary internal resources. Make sure the VPN Name is either **“QMUL” or “mRDS”**. Once configured, the 'Client Certificate' field should display '**[your username] / QM-PKI-SRV-001-CA**'

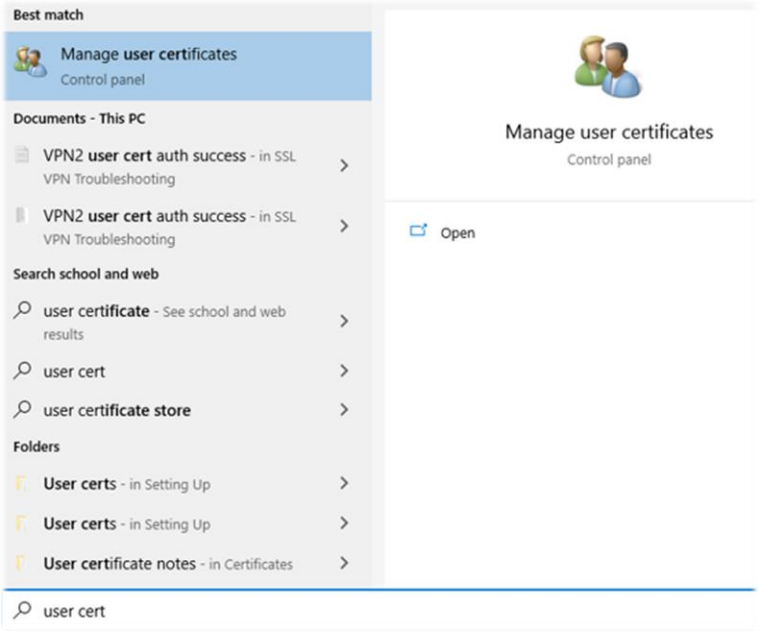


Once the VPN is successfully connected, you should see a small orange lock on the Fortinet Icon in the Taskbar Tray

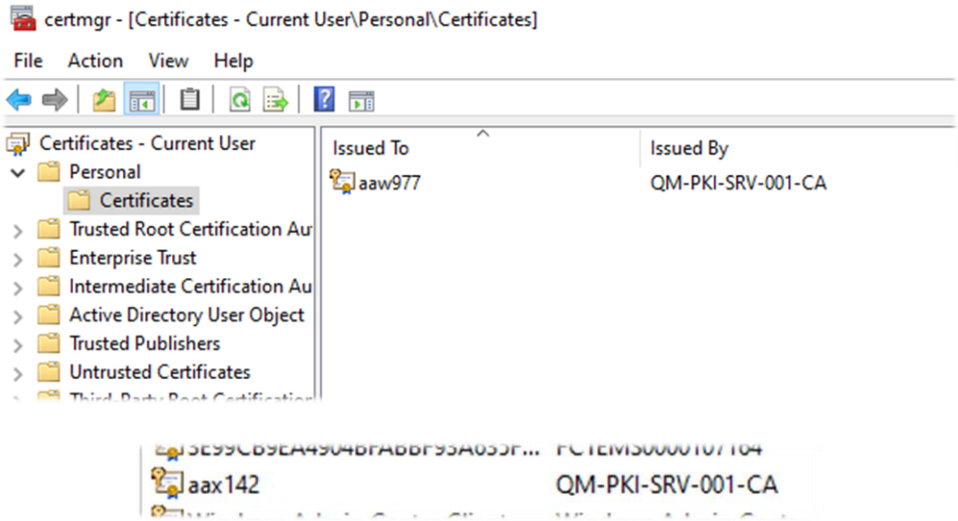
VPN Connection Troubleshooting

Certificate installation can be confirmed by checking the users certificate store.

1. From the Windows search bar type **user cert** and then select the Manage user Certificates.



2. From the window that is displayed, under Certificates – Current User select the Personal folder and then Certificates folder.
   The pane to the right should show the user certificate which is issued to the username of the user in question. The Issued by field should show **QM-PKI-SRV-001-CA.** If this is not the case, please contact IT support to remedy the situation.



For further information, please visit:
https://www.its.qmul.ac.uk/support/self-help/user-guides-for-the-fortinet-vpn-(forticlient)/

File Services

The primary storage location for the managed research desktop service is OneDrive which provides 5TB of space for personal files. This ensures that all important documents are synchronised with the Microsoft cloud and therefore not at risk if a device is lost or damaged. OneDrive has a built-in capability to share files or folders. It is not particularly good at synchronising large numbers of files (Uses a lot of computer power during processing). Synchronising large files will consume a lot of bandwidth.

For collaborative purposes, SharePoint provides a self-service capability to create and manage sites with up to 25TB of capacity. Document libraries on sites can be mounted on file explorer in windows for ease of use. Since it uses the same synchronisation technology as OneDrive, it is not brilliant with large numbers of files and will not accept some file extensions.

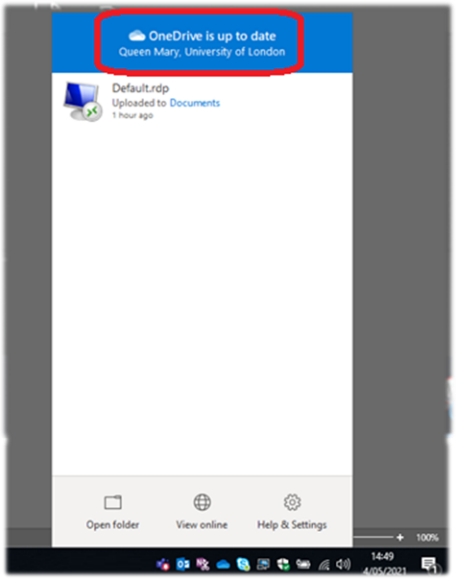
For HPC storage see the following link: https://docs.hpc.qmul.ac.uk/storage/ The drawback of this is that it does not allow direct access to data to modify from a client, so has to be downloaded and then re-uploaded if modified unless being run on the HPC.

In some circumstances, however, SharePoint, OneDrive and HPC storage are not suitable storage locations and an SMB or NFS mount is required instead. This is most likely to be encountered when performing testing or development on code that will later be run on the HPC; or for other computational analysis.

The OneDrive app

In bottom-right hand corner of your taskbar, you should see the OneDrive Icon, indicating that the OneDrive app is running.

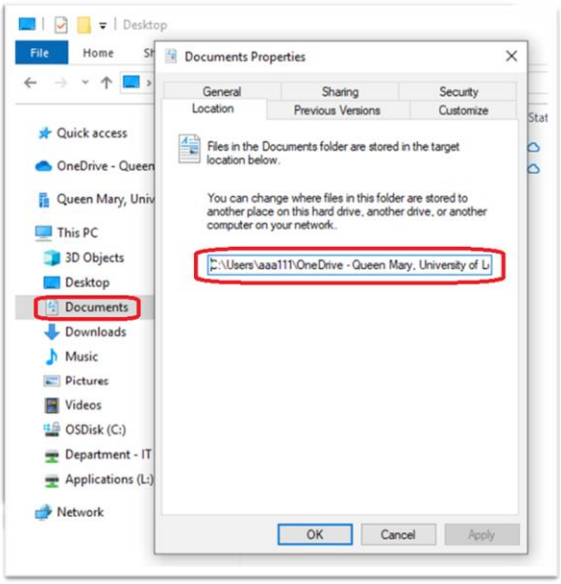
To ensure you are signed into OneDrive as expected, you can click on the icon, and the OneDrive app will show you that it is either up to date, or currently updating. If it does not, you may not be signed into OneDrive



Folder Locations

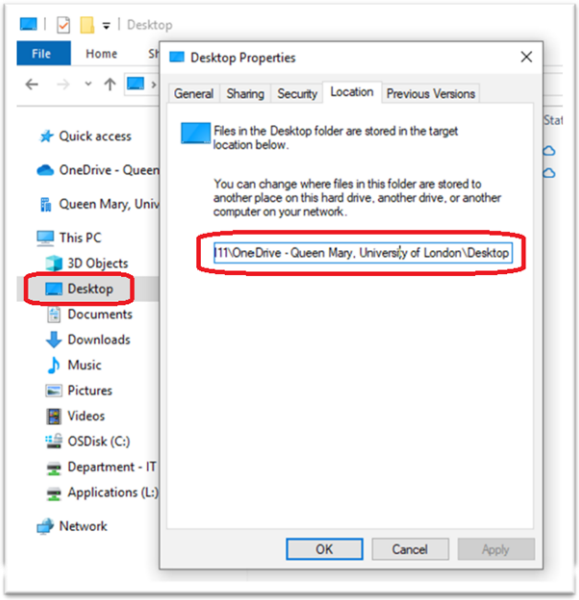
The default folders you use to save your files will be in '**OneDrive - Queen Mary, University of London**'. To check this is working correctly for you, right click your **Documents** folder icon under **'This PC'** in the file explorer, select **Properties** and check the Location tab. You should see:

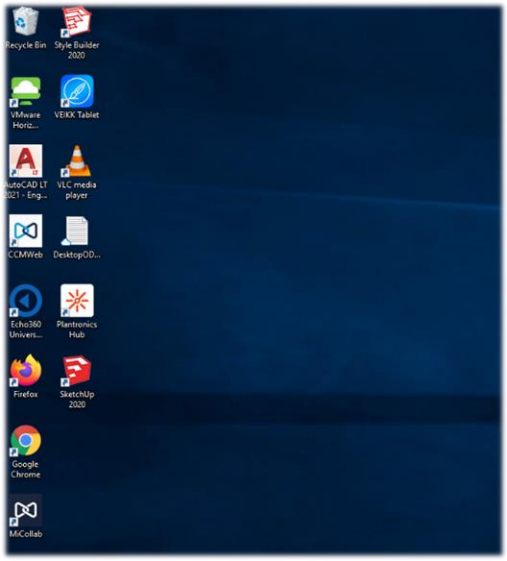
C:\Users\[your username]\OneDrive - Queen Mary, University of London\Documents



Your Desktop should show:

C:\Users\[your username]\OneDrive - Queen Mary, University of London\Desktop



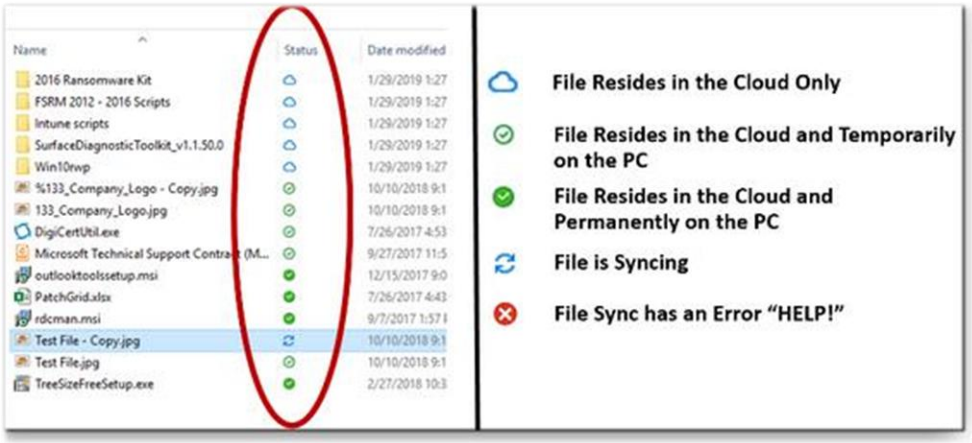


Your desktop will show the contents of this folder as desktop icons. If either of these do not display OneDrive paths, please contact IT Services.

OneDrive Status indicators

Many icons will display a OneDrive indicator, such as the small cloud logo on this notepad file:

These will either be on the icon for the file itself, or in the 'Status' column in your file explorer. For a full list of what these indicators mean, see below:

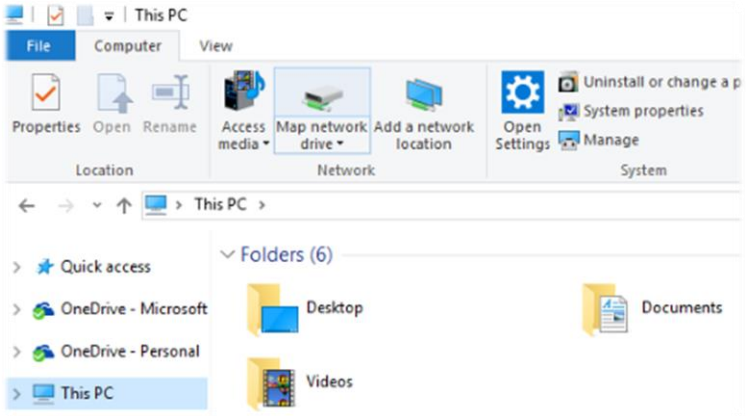


Managed research desktop file storage

In some circumstances, SharePoint, OneDrive and HPC storage are not suitable storage locations, where a shared network drive would be more useful instead. This is most likely to encountered when performing testing or development on code that will later be run on the HPC; or for other computational analysis.

You have 150GB initially, with more available via approved request.
Please Note: There is no replication or alternative backups. For better data security, you should migrate data to Onedrive / Sharepoint when dormant.

Map a network drive to get to it from File Explorer in Windows without having to look for it or type its network address each time.
Open **File Explorer** from the taskbar or the **Start menu**, or press the **Windows logo key + E**.
Select **This PC** from the left pane. Then, on the **Computer** tab, select **Map network drive**.



1. In the **Drive** list, select a drive letter. (Any available letter will do.)
2. In the **Folder** box, type \\mrds-smb.qm.ds.gul.ac.uk\h3. To auto-connect when signing into your PC, select **Reconnect at sign-in**.
3. Select **Finish**

.

Note: If you cannot connect to a network drive or folder, the computer you are trying to connect to might be turned off, or you might not have the correct permissions. Try contacting your network administrator.

Virtualization using VirtualBox

VirtualBox is the heart of the self-managed environment, wherein you can run tests, build research toolsets and experiment. If running computationally intensive workloads, it is advisable to develop a toolset suite, then request ITS to package this environment/suite for use natively on your managed device to harness more of the power of your device.

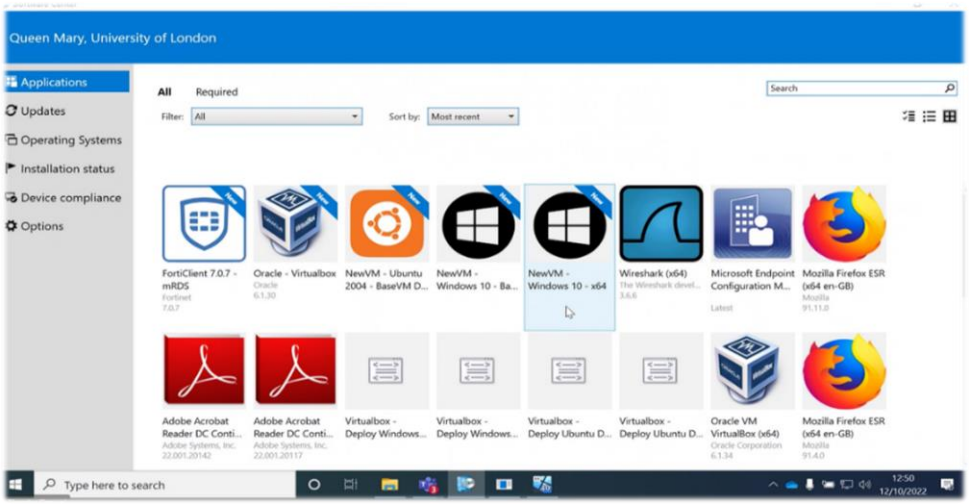
More information on using Virtualbox can be found in the vendor's documentation.

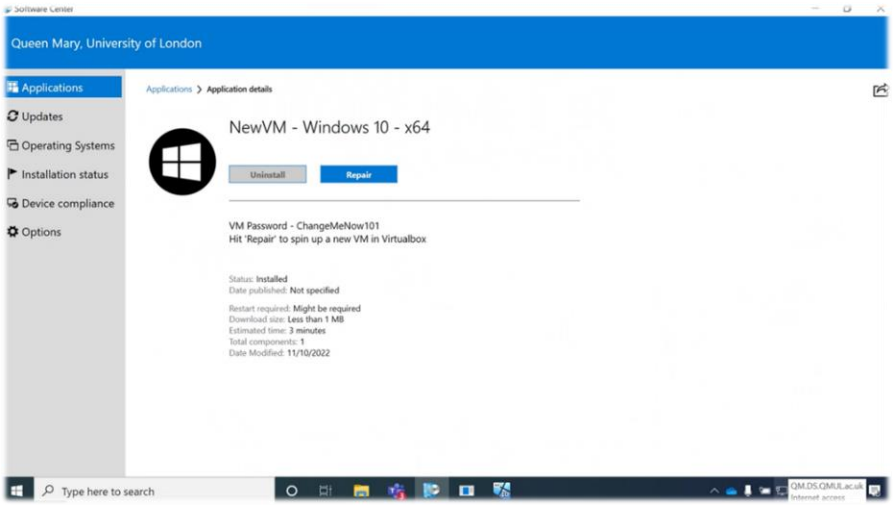
Launching your Virtual Machine

Your new laptop will come with VirtualBox pre-installed and some components to create new VMs with. You can quickly fire up a new "Quick Start" VM in Software Centre with choice of Windows (10 & 11) and Linux (Ubuntu 2204 LTS) flavours. While the Quick Start VMs will satisfy a wide range of requirements, we still recommend you learn to create your own VMs. Custom VMs allow you to optimise your environment to your specific circumstances.

Installing Quick Start Virtual Machines

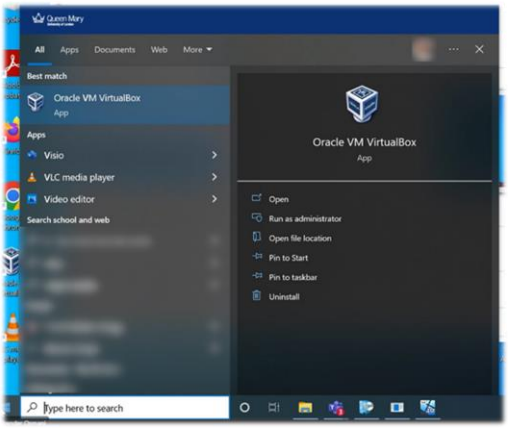
Search for and launch 'Software Center' from the Start menu.





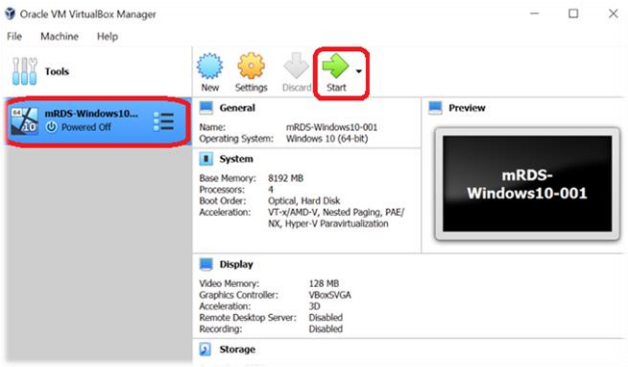
Select the required VM's operating system (Windows or Ubuntu) and click 'Install' or 'Repair' to add this VM to VirtualBox.

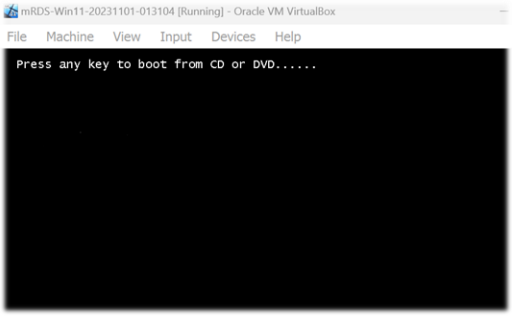
Using the Quick Start VM Demo



To launch your VM, first search for and launch VirtualBox from the Start menu or from the icon on the desktop.

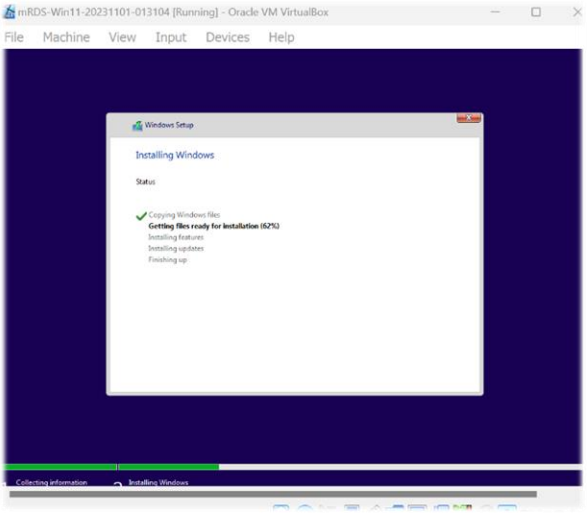
Select the VM on the left and launch by double-clicking it or clicking the green arrow.

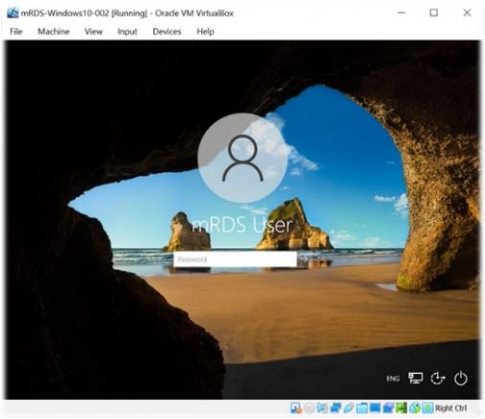




You may need to press a key when it appears to launch the installation process. If you miss it, reset the VM via the Machine menu to try again.

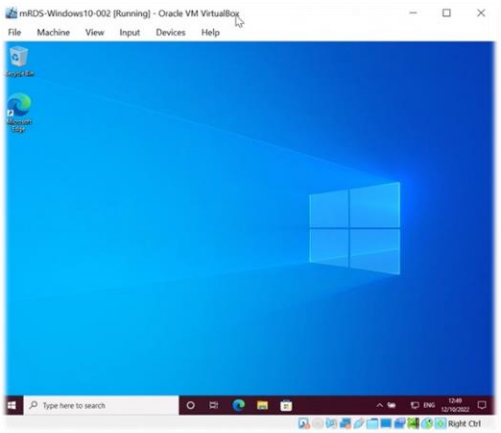
Virtualbox will proceed to create your new VM and should take around 15 minutes to complete. You can leave this in the background while you work.

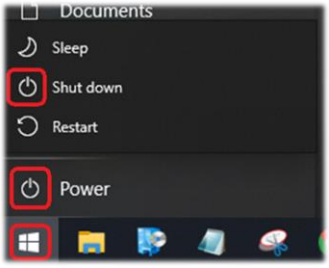




Once your VM has started up, you can log in with the password **'ChangeMeNow101'**

Once you login, you will have administrator access to the VM and be able to install any applications required. Again, we recommend you learn to create your own VMs early on. This way, you can make any the beginner mistakes before you have VMs you can't afford to lose access to.

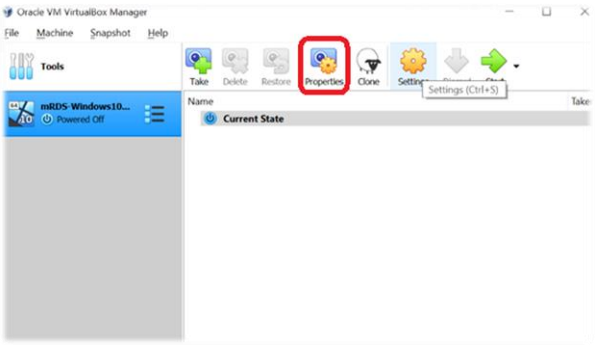


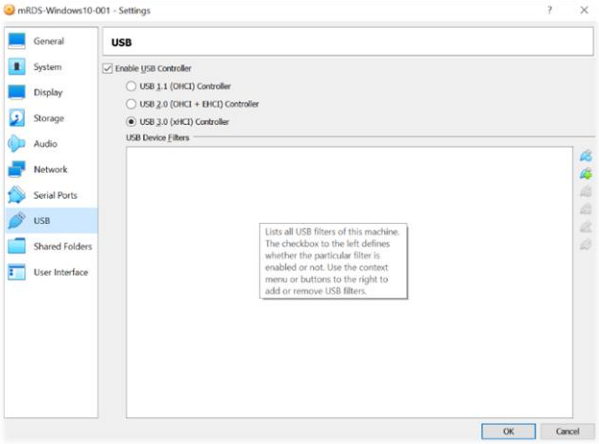


Once you are finished using your VM, shut it down either by going to Machine > ACPI Shutdown in the menu at the top of the window, or clicking the Start menu and going to 'Shutdown' as you would on a normal PC.

Using your USB devices in your Virtual Machine

From the main VirtualBox window, select your VM and click Settings.



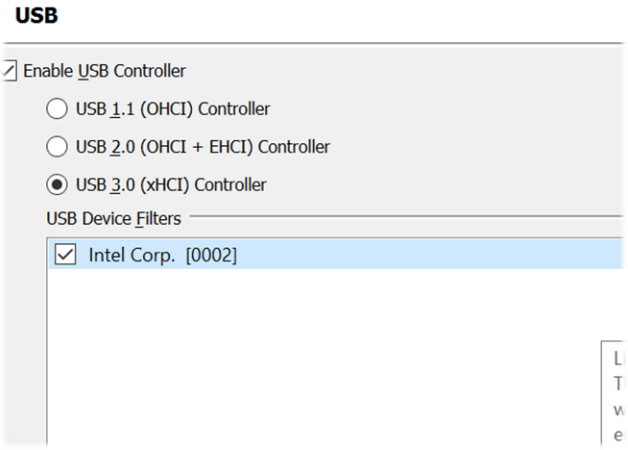


Select the USB submenu on the left-hand side of the settings window.

Click on the green plus icon.

Select the required device.

The USB device should now appear in the USB Device Filters list. You may now use your USB device in your VM.

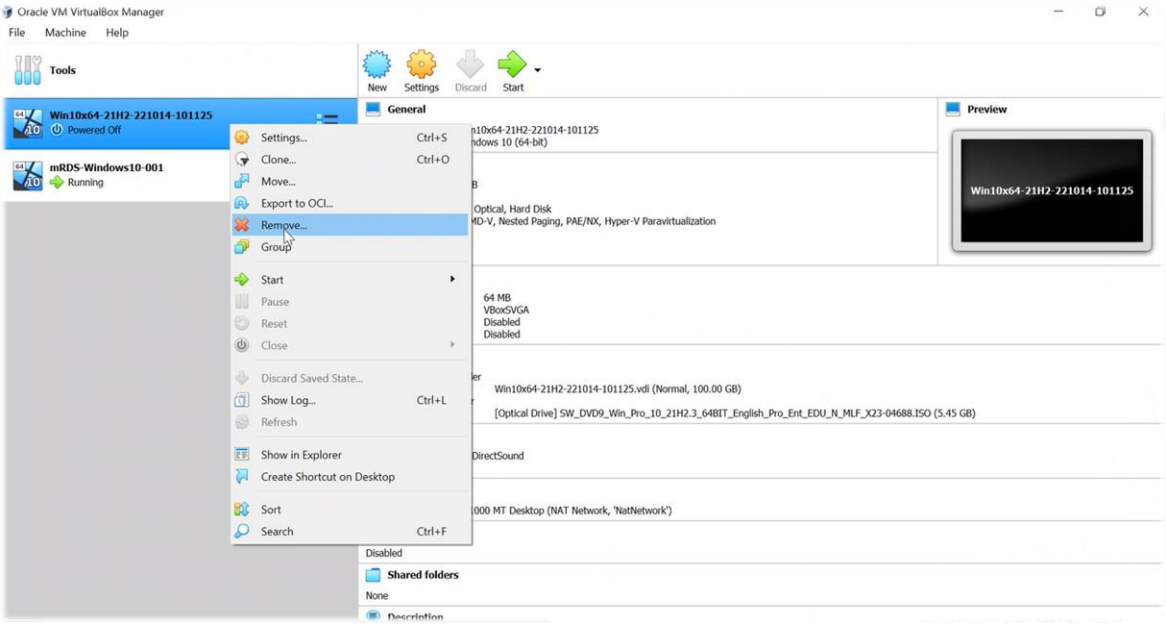
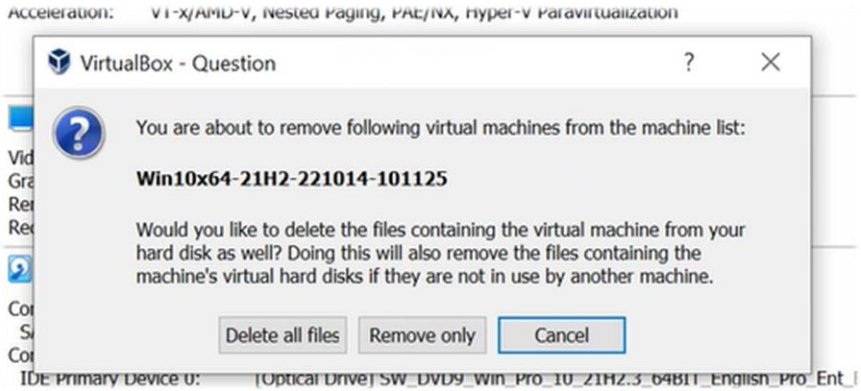


Custom VM Method

For information on building custom VMs, please refer to these links:
https://docs.oracle.com/cd/E26217_01/E26796/html/qs-create-vm.html
https://www.virtualbox.org/manual/ch01.html#create-vm-wizard

Removing Virtual Machines

If you wish to remove any VM, in VirtualBox right click a VM and click Remove.



In the window that pops up, click 'Delete all Files'. **Please note: This cannot be undone.**