Introduction to Computing at the CBU Overview

Jeff Berry

MRC Cognition and Brain Sciences Unit, Computing group

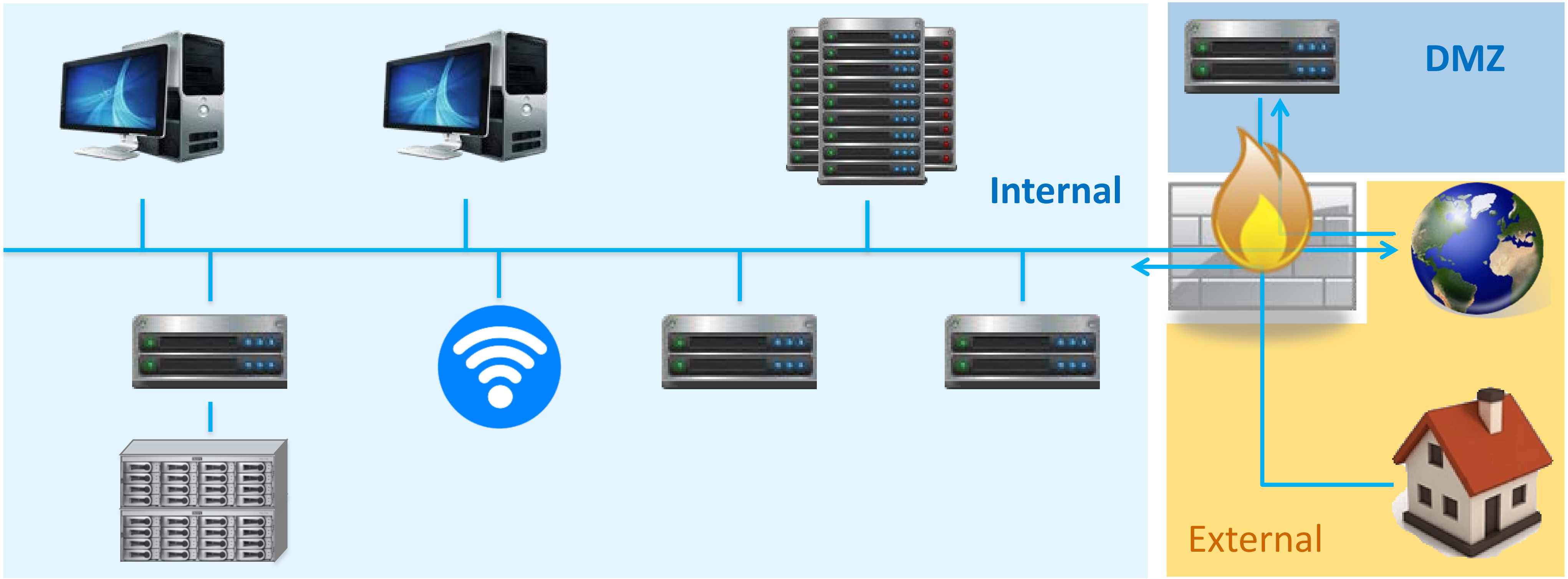
Computing Resources

Desktops
(Win 10/11, Mac OSX)

Testing and shared access machines
(Win 10, some legacy Win7)

High Performance Compute Cluster
(Linux)

Web services
(www, FTP, SSH, online experiments, cloud storage)



Network data storage
(Home space, shared group space, secure data area, imaging data storage)

WiFi

Email
(Microsoft Exchange. Outlook, Webmail, Mobile devices)

Infrastructure Services
(authentication / user accounts, software portal, online room booking)

Remote access

VPN
(Virtual Private Network)

A VPN is an encrypted channel which allows a remote machine to be placed 'virtually' on a different network. The unit VPN allows remote machines to function as if they were behind the firewall and access unit resources.

- unit machines have a built-in VPN client
- Windows 10/11 machines can use Capsule VPN
- other machines can use the vpn portal site
- connections to the VPN use the usual unit credentials

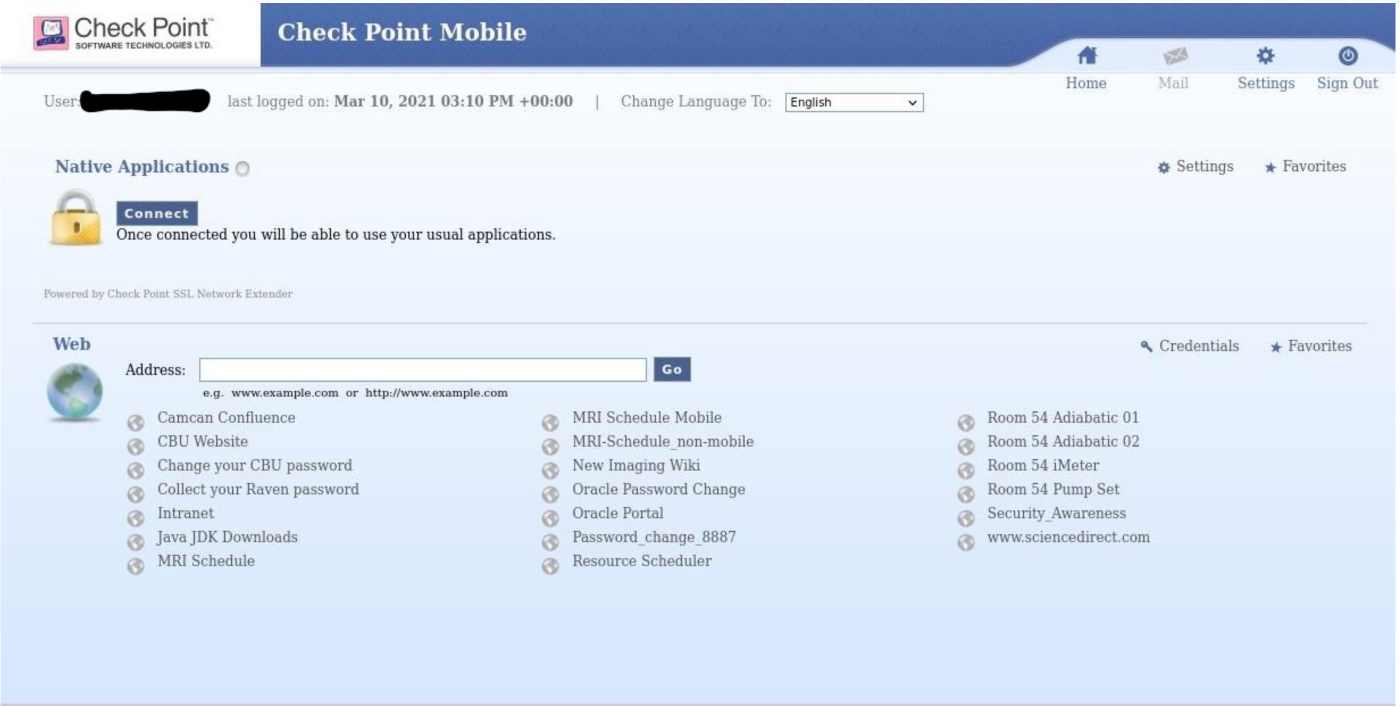
More information at:
http://intranet.mrc-cbu.cam.ac.uk/home/01-working-from-home-off-site/
(but wait ... how does one access the intranet without vpn'ing?)

VPN portal
intranet access

The CBU VPN portal is the entry point for all the VPN services

https://portal.mrc-cbu.cam.ac.uk/sslvpn

After logging in with unit credentials, some internal websites are available immediately.



User: [redacted] last logged on: Mar 10, 2021 03:10 PM +00:00 | Change Language To: English

Native Applications

Once connected you will be able to use your usual applications.

Powered by Check Point SSL Network Extender

Web

Address:

e.g. www.example.com or http://www.example.com

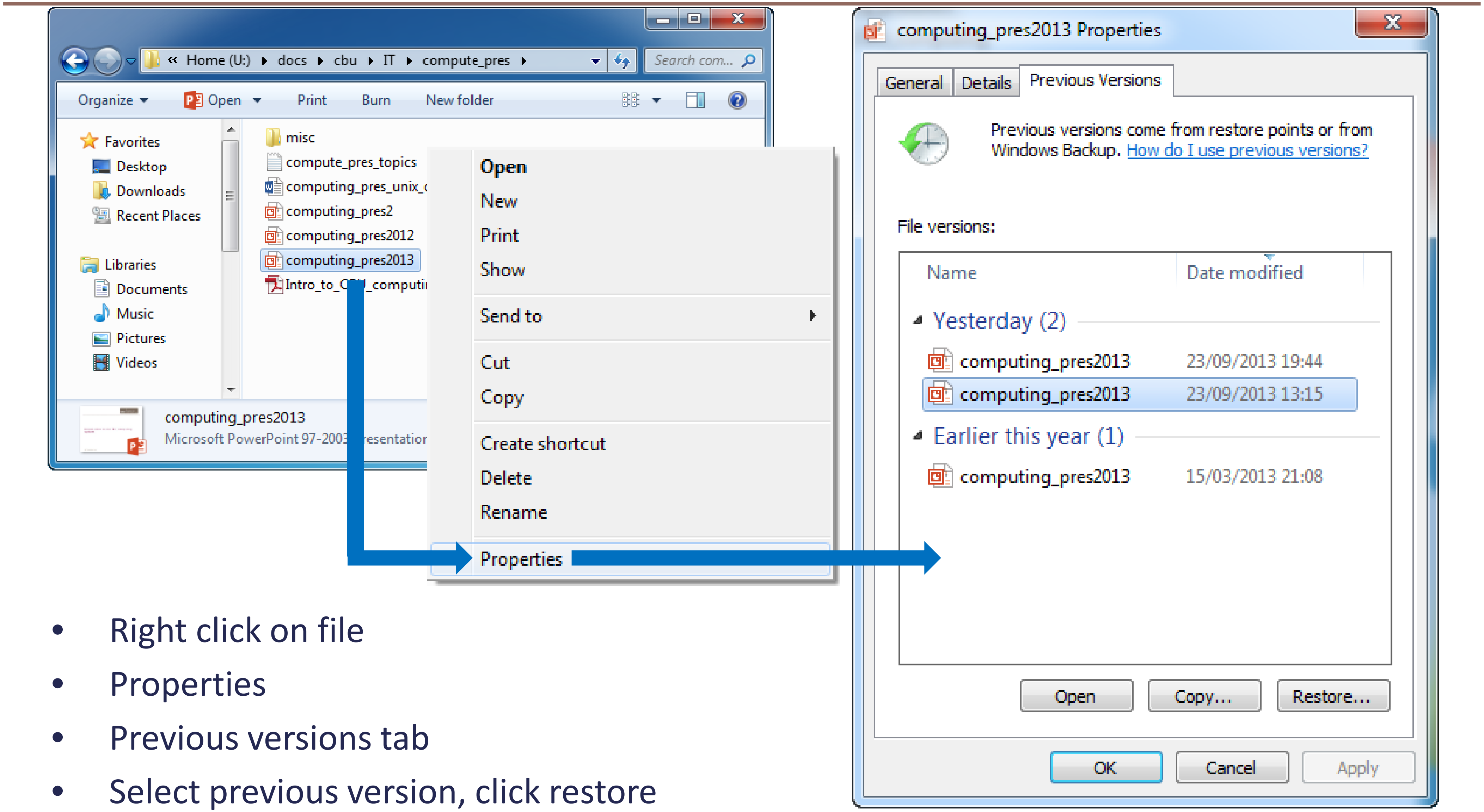
- Camcan Confluence
- CBU Website
- Change your CBU password
- Collect your Raven password
- Intranet
- Java JDK Downloads
- MRI Schedule
- MRI Schedule Mobile
- MRI-Schedule_non-mobile
- New Imaging Wiki
- Oracle Password Change
- Oracle Portal
- Password_change_8887
- Resource Scheduler
- Room 54 Adiabatic 01
- Room 54 Adiabatic 02
- Room 54 iMeter
- Room 54 Pump Set
- Security_Awareness
- www.sciencedirect.com

Network Storage
Home Space

Home space:

- /home/<userid> on Linux (e.g. /home/xy01)
- U: on Windows (by default)
- Personal to you, by default not accessible to anybody else
- Snapshot backups – hourly / nightly / weekly
- Intended to store scripts, figures, documents etc – things that can’t be recreated programmatically.
- Limited space – not intended for large amounts of data
- Used by Linux to store application settings, preferences, etc

Restoring home space from a snapshot - Windows



Previous versions come from restore points or from Windows Backup. How do I use previous versions?

File versions:

Name	Date modified
Yesterday (2)	
computing_pres2013	23/09/2013 19:44
computing_pres2013	23/09/2013 13:15
Earlier this year (1)	
computing_pres2013	15/03/2013 21:08

- Right click on file
- Properties
- Previous versions tab
- Select previous version, click restore

Network Storage
Shared Spaces

Shared research group areas:

- Created to allow members of specific labs / research groups to share data
- Access limited to members of the relevant research group

Imaging spaces:

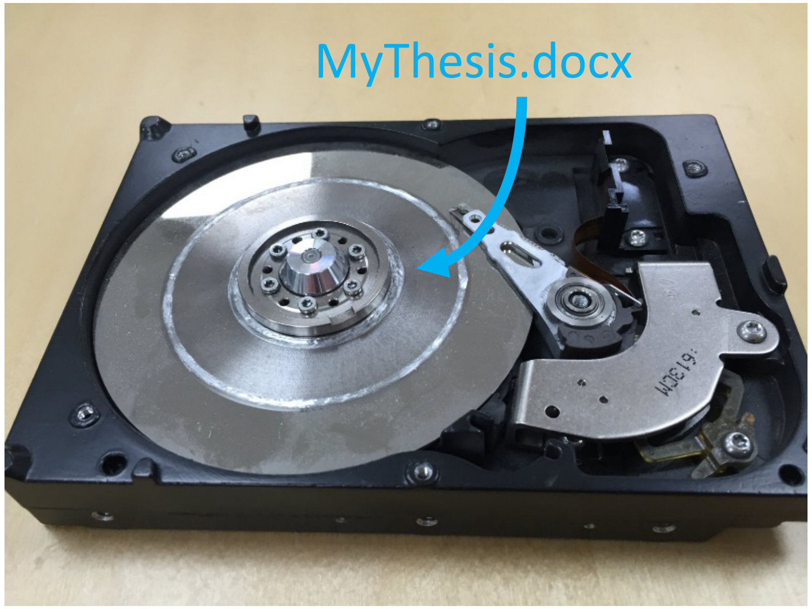
- Large storage spaces typically used for imaging data and processing
- Organized by group or project, with limited access
- Individuals can have directories/folders in the shared group area
- Usually accessible from Windows and Linux, but primarily Linux oriented

NB: On Linux, group areas/imaging spaces are ‘automounted’ – they must be explicitly referenced the first time they are accessed, simply ‘looking for them’ will not work

Network storage - Best Practice

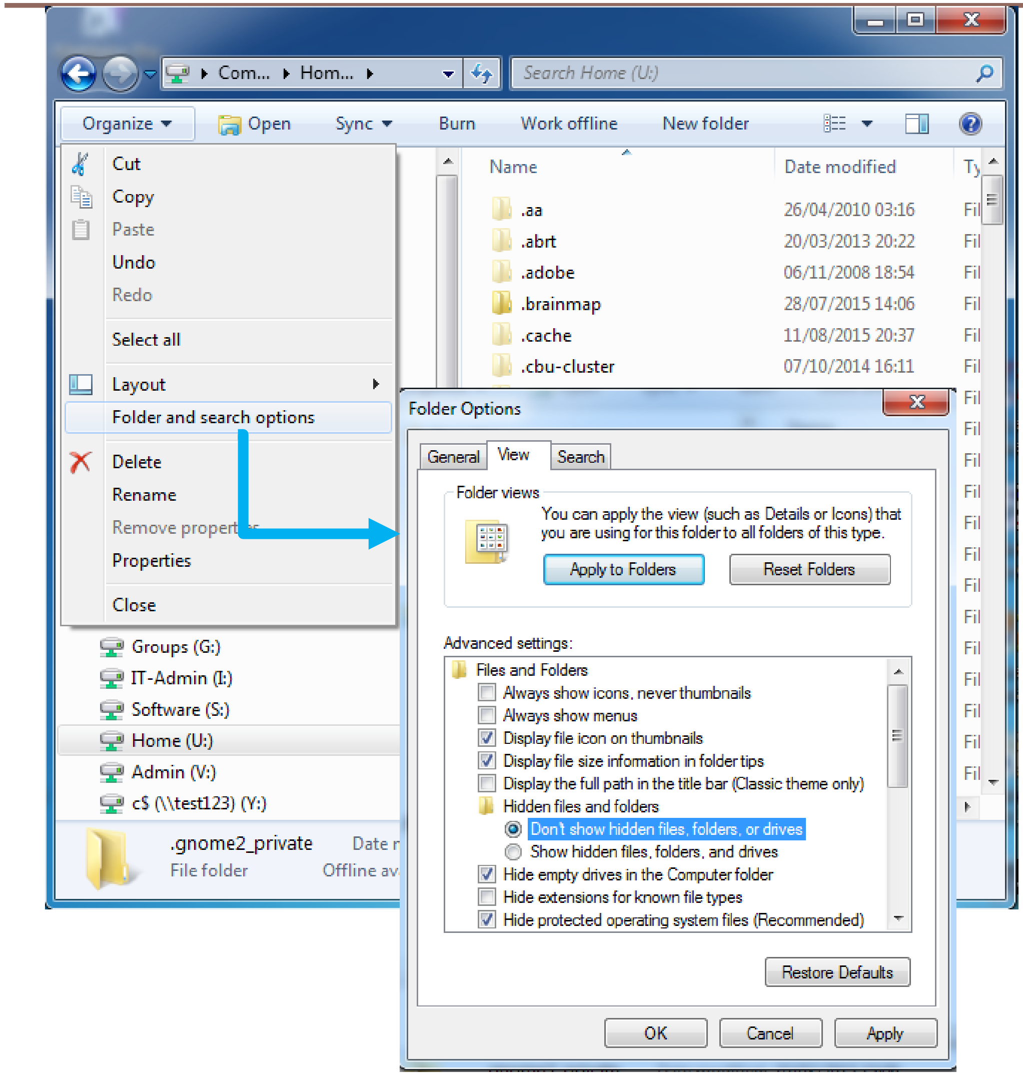
Home space:

- Try to get into the habit of storing documents in your home space.
  - Home space is backed up – desktop hard drives aren’t.
  - You can access your home space from almost every machine – you don’t have to create multiple copies of data, or move data around on removable media



- Use your home space to store anything you can’t easily recreate (documents, figures, scripts). Don’t use it for imaging data – space is limited!
- Data is replicated off-site – in the worst case scenario, analyses could be re-created from raw data and code stored in your home space

Network storage - Best Practice



Name	Date modified	Ty
.aa	26/04/2010 03:16	Fil
.abrt	20/03/2013 20:22	Fil
.adobe	06/11/2008 18:54	Fil
.brainmap	28/07/2015 14:06	Fil
.cache	11/08/2015 20:37	Fil
.cbu-cluster	07/10/2014 16:11	Fil

.gnome2_private Date r
File folder Offline av

Folder views

You can apply the view (such as Details or Icons) that you are using for this folder to all folders of this type.

Advanced settings:

Files and Folders
- □ Always show icons, never thumbnails
- □ Always show menus
- ☑ Display file icon on thumbnails
- ☑ Display file size information in folder tips
- □ Display the full path in the title bar (Classic theme only)
- Hidden files and folders
  - ● Don't show hidden files, folders, or drives
  - ○ Show hidden files, folders, and drives
- ☑ Hide empty drives in the Computer folder
- □ Hide extensions for known file types
- ☑ Hide protected operating system files (Recommended)

- When you browse your home space in Windows, you may see a lot of files whose names start with a "."
- These are used by Linux for storing system settings, preferences, etc – don't be tempted to "tidy" or move them!
- Instead, mark anything you don't want to see as hidden
  - right click, properties, check "hidden"
- Configure windows explorer not to show hidden files
  - click the "Organise" menu in windows explorer, select "Folder and search options", click the "View" tab, select "Don't show hidden files, folders, or drives")

Network storage - Best Practice

Imaging / group storage:

- Clean up after your analyses – e.g. delete intermediate pre-processing images once you’ve finished with them
- If you are using AA version 4, make sure garbage collection is turned on
- Don’t copy raw data from /mridata or /megata into your /imaging directory
- Don’t create multiple copies of the same files
- You can read data from your group’s or project’s imaging space – you don’t need to copy data from one directory/folder to another

Software

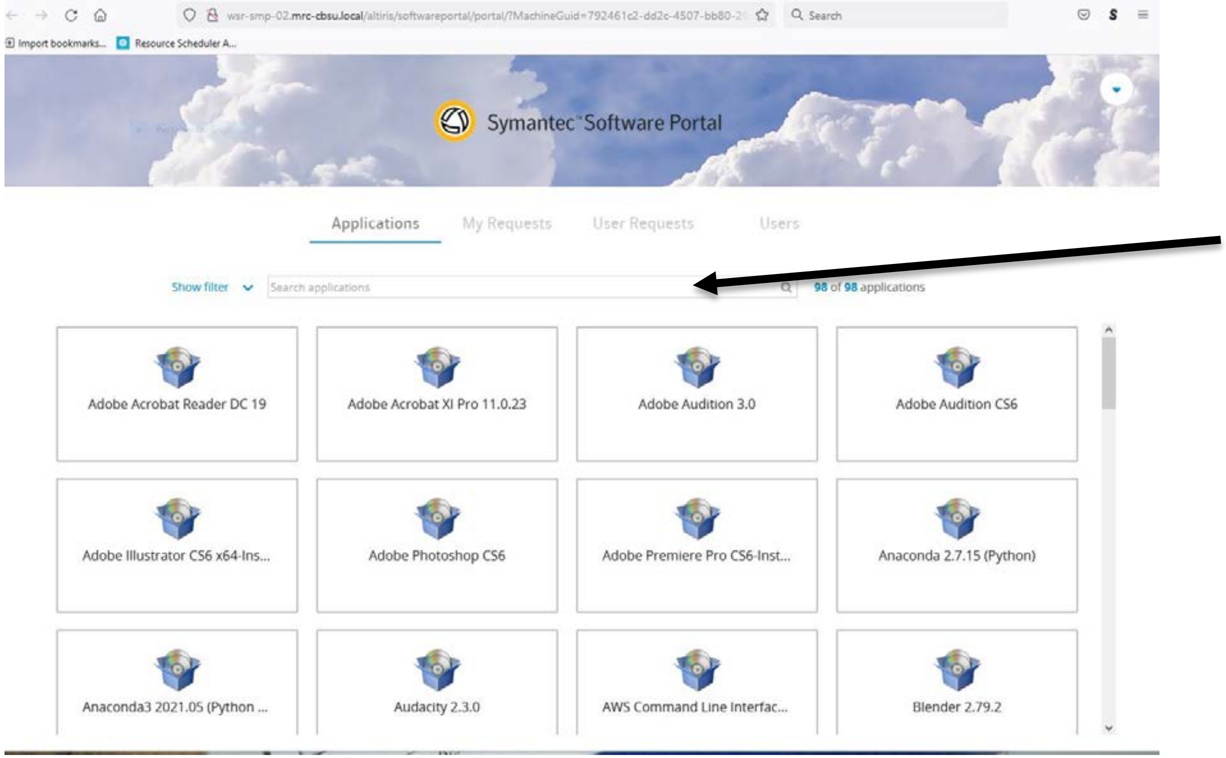
- Desktop PC – many common productivity /stats packages are available:
  - Office, Endnote
  - SPSS, Matlab
  - Adobe Photoshop/Illustrator/Acrobat

- Stimulus delivery software:
  - Eprime, Presentation, Matlab (Psychtoolbox, Cogent)
  - Write your own (Matlab, VB, python)

- Compute cluster:
  - Matlab, SPM, FSL, Freesurfer, Python (Anaconda, inc Spyder), R/Rstudio
  - /imaging/local/software, or /hpc-software
  - http://imaging.mrc-cbu.cam.ac.uk/imaging/AvailableSoftware

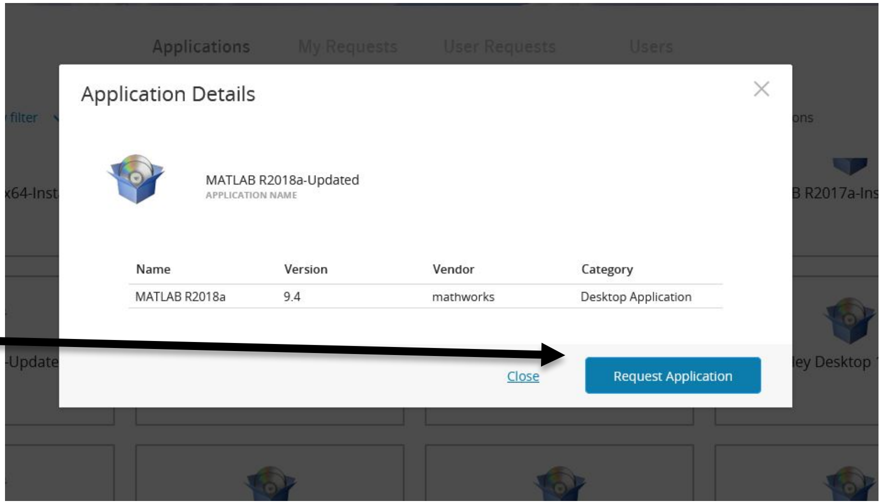
Self Service Software Portal

http://wsr-smp-01.mrc-cbsu.local/Altiris/SoftwarePortal/UserPortal/Home.aspx
(on unit machines, there is usually a desktop link)



Search by name

Then select it and 'Request Application



MATLAB R2018a-Updated
APPLICATION NAME

Name	Version	Vendor	Category
MATLAB R2018a	9.4	mathworks	Desktop Application

Security and Usage Policies

- Full policies available on the intranet (http://intranet.mrc-cbu.cam.ac.uk/administration/induction/) and in your induction pack
- By signing up for a CBU computing account, you are agreeing to abide by those policies

- **General principles:**
  - Protect other peoples' personal data
  - Protect our machines, data and users
  - Protect the integrity and reputation of the MRC and UoC
  - Avoid participating in, facilitating, or encouraging illegal or inappropriate activities

Data Protection - Protecting other peoples' data

- We have a **legal** obligation to protect the rights and privacy of staff, participants and members of the public
- There are serious consequences for non-compliance

- Data Protection Act (DPA; 2018) based on the EU General Data Protection Regulations (GDPR)
- Designed to protect data relating to identifiable, living people.
- Defines how this personal data can be used
- Attempts to balance legitimate needs to use personal data with the rights of individuals to privacy.
- Participant data, but also data from other members of the public – e.g. workshop attendees

Data Protection – What is personal data?

- What counts as personal data?
  - "**Any** information relating to an individual person who can be identified directly or indirectly by reference to an identifier"
  - Data that is about or clearly relates to an **identifiable**, **living individual**
  - Data that could be used to learn something about an individual or compromise their privacy
  - Anonymised or aggregated data is not covered by the Data Protection Act
- Special category personal data – data which may cause distress if released:
  - Medical information, information about political views, ethnicity, sexual orientation.

Data Protection – What is personal data?

Types of identifier (not exhaustive):

- Name
- Address
- Email address
- Telephone number
- Official ID numbers (e.g. national insurance number, NHS number, passport number, driving license number, etc)
- Date of birth
- Birthplace
- Genomic information
- Face, fingerprints, or handwriting
- Credit card numbers
- IP address
- Digital identity
- Login name, screen name, nickname, or handle

Data Protection - Protect yourself

- Context is important – can an individual be identified by taking into account other data held by the same data controller, or other publically available information?
- Think carefully about whether your data could identify an individual person – e.g. rare medical conditions, facial information in structural MRI, and so on
- Be careful of dicom data – dicom headers can contain personally identifiable data such as name or date of birth
- CBU dicom data does not contain name, and date of birth is obscured

Data Protection – Legal requirements

- You must have a lawful basis for processing personal data
  - Research in the public interest, consent

- You must abide by the data protection principles
  - Processed lawfully and fairly, collected for specific purpose and not processed further, relevant and limited to what is necessary, processed in a manner that ensures security

- You must respect data subject rights
  - Right to be informed, right of access, right to erasure, right to rectification

Data Protection - Protect yourself

Processed lawfully and fairly, collected for specific purpose

- In practice:
  - Explain what information you'll collect, what you'll use it for, and who will be able to access it (information sheet, privacy statement)
  - Only use data for purposes to which participants have consented.
  - Never share participants' personal information with anyone unless you have explicit authorisation to do so.

Data Protection - Protect yourself

Collected for specific purpose and not processed further, relevant and limited to what is necessary

- In practice:
  - Separate research and personal data.
  - Where possible, **anonymise your data**, only keep personal data where it is necessary
  - Alternatively pseudonymise data by replacing personal identifiers with id numbers
  - Minimise data (e.g. replace DoB with age in months, recode descriptive data, obscure variable names)
  - Destroy participant contact details when you have finished with them
  - Don’t share participant contact details with anyone, even other members of the unit

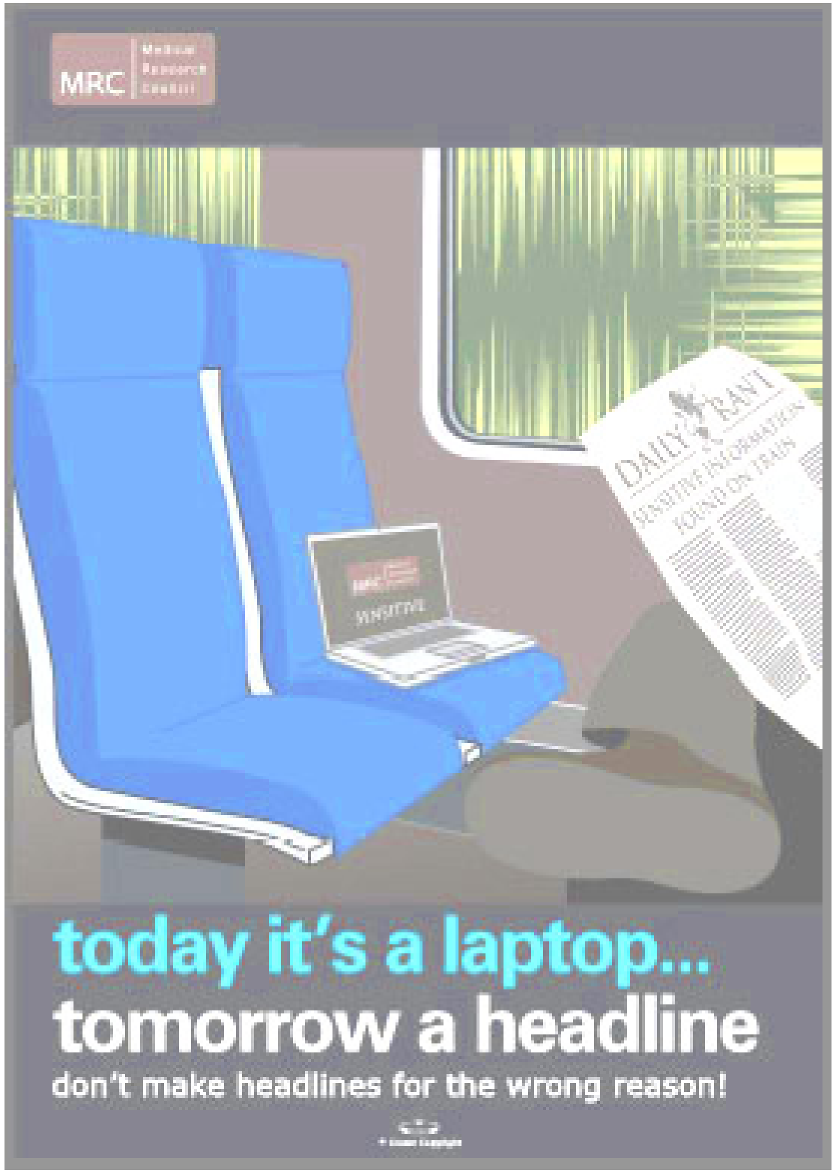
Data Protection - Protect yourself

Processed in a manner that ensures security

- In practice:
  - Store electronic personal data (and keys linking ID numbers to personal data) in our secure data area
  - Store paper data in a locked drawer or filing cabinet
  - Protect personal data with appropriate file system permissions
  - Don’t transfer personal data using laptops, removable media, email or cloud storage.
  - If you must transfer data this way, the data **must** be encrypted.
  - Uploading personally identifiable data to cloud storage risks breaking the law as most cloud storage providers won’t guarantee that the data will remains in EU, or protected with adequate security.

Data Protection - Protect yourself

- Get permission before importing or exporting large amounts of data from our system
- Treat other peoples' personal data in the way you would want your own personal data to be treated.
- If in doubt, ask!


MRC Medical Research Council
DAILY RANT
SENSITIVE INFORMATION FOUND ON TRAIN
SENSITIVE
today it's a laptop...
tomorrow a headline
don't make headlines for the wrong reason!

Security – Protect our machines, data and users

- Common security threats:
  - Phishing
  - Malware
  - Password attacks and compromised accounts

Security - Phishing

- Attempts to obtain sensitive information by deception – passwords, usernames, financial details, sensitive institutional information
- Email is the most common route, but not the only one. Phishing can also occur via the phone or face to face.
- Often combined with attempts to install malicious software (malware)
- Phishing attacks have been on the rise during and after the pandemic with the increase in WFH
- Common tactics include:
  - Asking you to open an email attachment
  - Asking you to click on a link in an email
  - Asking you to input details on website
  - Asking you to download and install software

Security – Avoiding common threats

- Treat any unexpected emails with extreme caution, **even if they seem to come from an address you recognise**, particularly if they ask you to
  - Download files
  - Follow a link
  - Open an attachment
  - Enter your details on a web site
  - Provide personal details
- Please be extremely cautious about opening email attachments, particularly attachments that can contain executable code (e.g. MS Office documents).
- Do not allow any embedded code or macros to run, or enable editing mode, unless you are absolutely certain of the document’s origins.
- Hover your mouse over any hyperlinks to see the true target, even if you think the message may be legitimate. If the target is completely unrelated to the text, treat the email with extreme suspicion.
- If you are in any doubt at all, don’t download any files or open any attachments, and contact it-help for advice

Security – Malware

- Email is the most common route for dissemination of malicious code, but it is by no means the only one:
  - Infected files (transferred by removable media, downloaded from the internet, etc)
  - Code embedded in documents (e.g. macros in MS Office applications)
  - Self propagating (worms)
  - Software downloaded from the internet (including from apparently legitimate sites)
  - Software with a dual or hidden purpose (trojans)
  - Bundled with legitimate software (“drive by install”)
  - Sharing pirated software or media
  - Code run by malicious web sites

Security – Avoiding common threats

- Avoid installing software or running code / containers unless you are **absolutely** sure both the software and the source you are obtaining it from are reputable.
- Be very careful of "drive by installs" – unwanted software bundled with legitimate packages.
- If you are in any doubt, please do not download or install the software - even some supposedly reputable sites will bundle unwanted applications along with the software you have requested
- Be very careful of software that allows remote access to CBU computing systems, e.g. remote support packages like Team Viewer. Only use this software with people you know, and make sure the software is not still running after you have finished.
- Do not allow web sites to run active content (e.g. java, JavaScript) unless you are absolutely certain the site is reputable.

Security – Passwords

- Use a strong password
  - CBU minimum requirements:
    - 10 characters
    - Characters from 3 of the 4 following groups: Numbers, uppercase letters, lowercase letters, non-alphanumeric characters
    - Not based on name or username
- Use a password that is unique to your CBU account
- **Don’t share your password with anyone else**, even other members of the unit
- Don’t use anyone else’s account or allow anyone else to use your account

Security – Avoiding common threats

- Don’t leave open sessions unattended.
  - Log out or lock your screen whenever you leave your desktop PC (windows + L)
  - Close your x2go sessions and VNC viewers
  - Log out of SSH sessions
- Be careful of people asking for details over the phone, asking you to visit technical support websites.
- In all cases, if you are at all in doubt, please send an email to it-help@mrc-cbu.cam.ac.uk and we will try to help.

Computing Support

- Computing group intranet pages:

  http://intranet.mrc-cbu.cam.ac.uk/computing

- Question and answer site:

  http://forum.mrc-cbu.cam.ac.uk/qa

- Imaging wiki:

  http://imaging.mrc-cbu.cam.ac.uk/

- Methods group and software gurus:

  http://imaging.mrc-cbu.cam.ac.uk/imaging/AvailableSoftware

- IT helpdesk

  it-help@mrc-cbu.cam.ac.uk

- Try to provide as much diagnostic information as possible – exact circumstances under which an error occurs, what you have tried to fix the problem, error messages, etc.

Jeff

Howard

Anthony

Russell