

Guidelines

Using SURE

SURE has been established with funding from the Australian Government National Collaborative Research Infrastructure Strategy (NCRIS) as part of the Population Health Research Network (PHRN)

Contents

| | |
|--|---------------|
| Introduction | 1 |
| SURE Support | 1 |
| Security guidance on authentication credentials | 1 |
| Security and incident management | 2 |
| Additional security tips | 2 |
| Systems maintenance | 2 |
| Accessing SURE | 3 |
| What do I need in order to log on? | 3 |
| How to log in | 3 |
| Options for launching your SURE virtual machine | 4 |
| SURE virtual machine | 7 |
| Software configuration | 7 |
| Network structure | 8 |
| Functionality | 8 |
| Logging out, timeouts and re-authentication | 9 |
| The Curated Gateway | 10 |
| Permissions for the Curated Gateway | 10 |
| Transferring files | 11 |
| Inbound File Transfer | 13 |
| Uploading a file for use in SURE | 13 |
| Downloading an approved file within SURE | 14 |
| Outbound File Transfer | 15 |
| Uploading a file for export out of SURE | 15 |
| Curation | 16 |
| Downloading an approved file for use outside of SURE | 16 |
| File logging and audit | 17 |

Introduction

This guide provides information on using SURE systems, contacting the SURE team and security guidance around your SURE access credentials.

SURE Support

Visit our [Frequently asked questions](#) page on the Sax Institute website or contact the SURE support team:

Email: sure.admin@saxinstitute.org.au

Telephone: +61 2 9195 6060

The SURE team is available to provide support Monday – Friday from 9:00 am to 5:00 pm (Australian Eastern Standard time or Daylight Savings time excluding NSW public holidays).

Please inform us any time your email address changes, so we can update your information.

Security guidance on authentication credentials

Below is a list of important security information that SURE users should be aware of in relation to the handling of their SURE authentication credentials, including SURE usernames, passwords and one time passcodes.

SURE users must not:

- Divulge your SURE username to anyone who is not a SURE team member.
- Divulge a one time passcode to anyone.
- Divulge any password to anyone. It will never be requested by a SURE team member via email, phone, face-to-face or other communication means.
- Use any SURE password as the login password for any other account.
- Store any password with other materials or information that is required for SURE access.

SURE users must notify the SURE team immediately:

- In the event that a password or one time passcode has potentially been revealed to any other person.
- In the event a passcode-generating device (such as a physical passcode generator or mobile phone) is lost or stolen.

Security and incident management

All users are given training on common information security risks during SURE Training. SURE users are to notify the SURE team about any changes in the system that they have not been notified about such as:

- changes to the login procedure
- changes to access to a workspace, folder or files
- changes to the appearance of any aspect of the facility including, but not limited to, the appearance of unusual notifications, icons, etc.

If a SURE user believes that there has been an incident that has compromised the security of SURE, the user must notify the SURE team immediately. Such incidents requiring notification include, but are not limited to, authentication materials (usernames, passwords and passcode generators) that may have been lost, stolen, damaged or unintentionally shared with another individual.

Additional security tips

Some additional security tips:

- Set up a screen lock on the computer you use to access SURE that is automatically activated after no more than 15 minutes.
- It is good practice to activate the screen lock on your local computer before leaving your desk.

Systems maintenance

SURE system software and infrastructure maintenance will need to be performed routinely and will typically be scheduled to occur on the last Friday of each month.

Urgent upgrades may need to be performed at short notice outside of scheduled maintenance times. Notifications for scheduled maintenance will be sent by email to the SURE users' nominated email addresses.

Accessing SURE

What do I need in order to log on?

To log on to SURE, a user needs authentication credentials that are supplied to each user following completion of the registration and training requirements.

These credentials are:

- A **username**
- A **passphrase**
- A **one time token/passcode**
- An **SSL certificate** installed on the local computer

If a user is part of more than one SURE workspace, the same credentials are used to access SURE and for each of the virtual machines.

How to log in

Your user credentials may be used to log in to:

- the SURE Access Gateway <https://access.sure.org.au/> – for access to your virtual machine
- the SURE Curated Gateway for transferring files into and out of your SURE workspace:
 - the External Curated Gateway <https://cg.sure.org.au/> (accessible from your computer)
 - the Internal Curated Gateway <https://cg2.sure.local> (accessible from your SURE virtual desktop)

When logging in to a SURE gateway from your computer, a pop up window entitled **User Identification Request** will prompt you to use your SSL certificate to access the site. Click **OK** and the web page will load.

SURE log in

Users can log on to the SURE Access Gateway or the SURE Curated Gateway by entering their username, password and a one time passcode.

To generate a one time passcode, open the app that your SURE soft token is set up in (miToken or Google Authenticator) and copy the generated 6 digit passcode into the Token box of the login screen.

Under Desktops, click on the desktop icon displaying the name of the workspace you want to access to launch your virtual machine.

Options for launching your SURE virtual machine

Once you have logged in to the Access Gateway, you have the option to either:

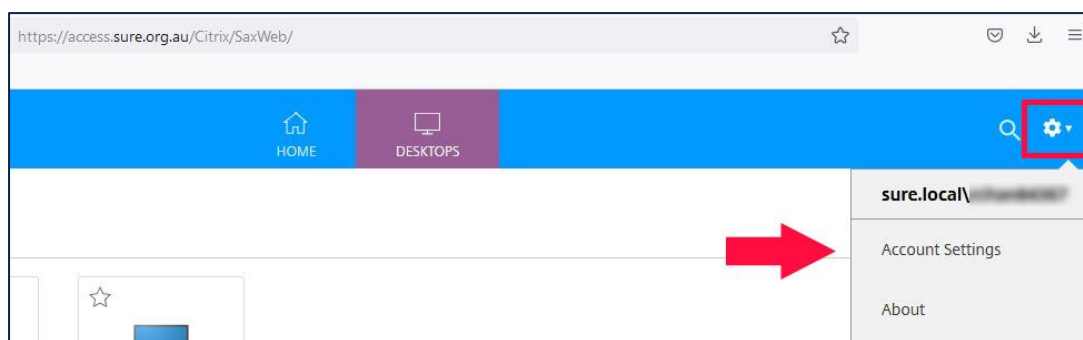
1. Use the desktop client for Citrix Receiver / Citrix Workspace

About this option: Citrix Workspace is not compatible with virtual machines in the previous SURE Access Gateway (<https://access2.sure.org.au>). Please continue to use Citrix Receiver until all of your SURE virtual machines are accessible via the new Access Gateway.

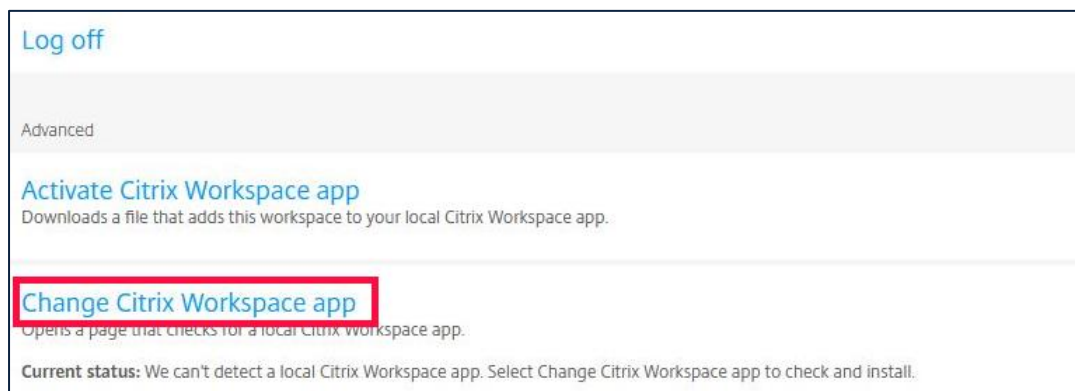
2. Set Citrix Receiver/Workspace to work within your browser (using HTML5)

About this option: There is a known issue between the Citrix HTML5 offering and the Firefox browser, where particular keyboard inputs (including [and \) do not work. We recommend using Google Chrome for HTML5 if you regularly use these keys for coding or commands.

You can change between these options in the new SURE Access Gateway by clicking on cog in the header bar, and selecting **Account Settings**.

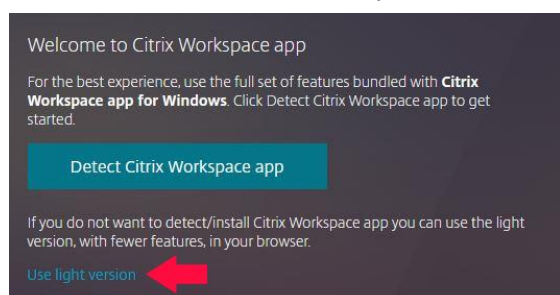


Follow that by clicking on **Change Citrix Workspace app**.



To use the **browser** version:

Select **Use light version** and your virtual desktop will launch within the browser, so you no longer need to have Citrix Receiver/Workspace installed.

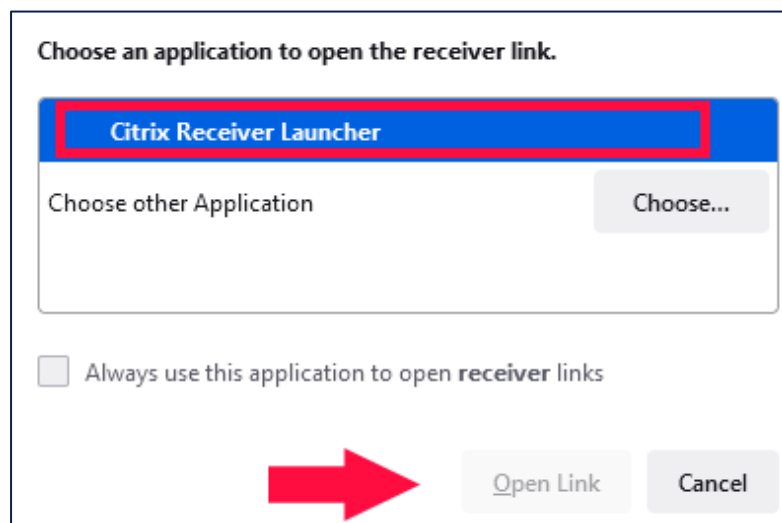


To use the **desktop client**:

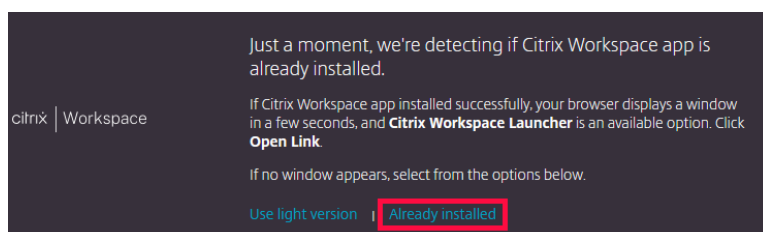
First select **Detect Citrix Workspace app**



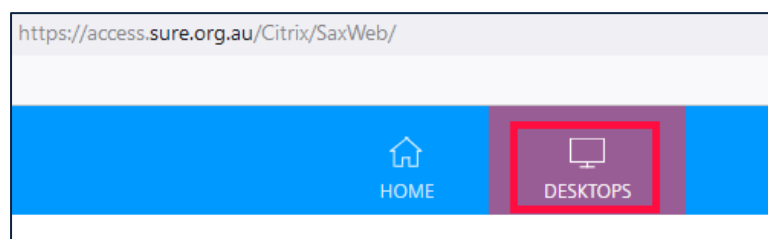
If already installed, select **Citrix Receiver Launcher** (or Workspace) and then click on **Open Link**.



Follow that by clicking on **Already installed**

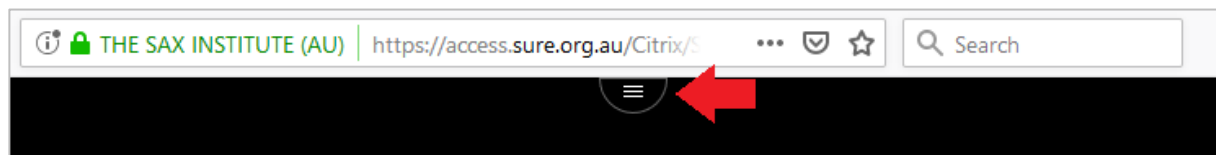


and then select the **DESKTOPS** icon in the header bar.



You will then be able to select the desktop icon for your virtual machine to launch it in the Citrix desktop client.

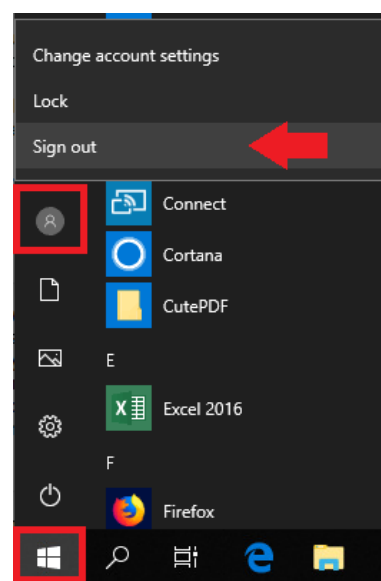
You will find some controls for the desktop window when you click the dropdown tab at the top of the window.



These include:

- Making the window **full screen**
- **Restoring** the window from full screen to normal size
- **Disconnecting** from your virtual machine (e.g. if you have analysis running that you want to return to later, rather than logging out).

You can also close the virtual machine and sign out if you have completed and saved your work.



To sign out:

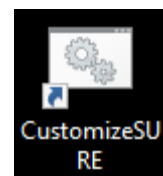
- Go to the Windows/Start menu
- Select the user icon
- Then click Sign out

SURE virtual machine

Software configuration

Some statistical applications (such as SAS, Stata and R) require particular configuration changes in a SURE user's account to work within the secure environment. Previously, we provided steps in the SURE Internal wiki for how to configure these.

In your new virtual machine, we have provisioned a small application you can run to carry out all the setup steps required for these applications for you. On your desktop, you will see an icon called **CustomizeSURE**.



Double-click the icon to run the application. Once it has completed, you can open and run your applications.

Installing packages in R

A local copy of the CRAN package repository is provided in SURE.

To install packages in R please first follow the steps above for **Software configuration**.

1. Run the latest R GUI program
2. In the menu bar, select **Packages > Install package(s)...**
3. From the popup Packages window, select the packages you want to install

Installing packages in Stata

To install packages in R please first follow the steps above for **Software configuration**.

Local copies of various Stata package repositories are provided within SURE, including:

- **Stata Journal:** The Stata Journal is a refereed, quarterly journal containing articles of interest to Stata users. Type `net cd sj` at the top level directory.
- **Stata Technical Bulletin:** The Stata Technical Bulletin was published from 1991 until 2001. Type `net cd stb` at the top level directory.
- **Boston College SSC archive:** Programs posted to Statalist. Type `net cd ssc-ideas` at the top level directory.

To locate a package and install it, use the commands `net cd` to change directory and `net install` to run the package installation. To return up a level in the directory, use the `net cd ..` command.

Network structure

The workspace contains the following drives that are accessible from your virtual machine:

Local disk

- **C: drive** – each virtual machine will have a local disk or C drive. This is used for system or program files on the virtual machine, and is also used as a temporary scratch disk for your applications to use when processing data or analysis.

Files that you wish to keep should not be saved to the C drive.

This drive will be renewed each time you log out of SURE or restart your SURE virtual machine, and as such, files created here will not be retained. It is recommended that this is where you direct temporary files for statistical programs (see the internal SURE wiki for more information). The storage space available is dependent on the type of virtual machine that has been requested for you.

Network drives

The network drives share the total file server storage amount allocated to your workspace.

- **H: drive** – a personal drive for each individual user to save their own personal working files.
- **G: drive** – a shared network drive for the workspace. This should be used to store data files, output and other files that you want to share with other users in your workspace.

Functionality

A number of functions on a SURE virtual machine have been disabled to enhance the security of SURE and minimise the risk of disclosure of confidential information. These include:

- Access to the internet (users will only be able to access local sites on SURE servers)
- Send/receive email
- Users will not be able to connect to a local printer and print from SURE
- Users cannot use the clipboard to copy and paste files between SURE project workspaces or with local computer
- Windows Fax and Scan

This list may not be exhaustive. If you have a query about something that is not working or want to discuss functionality, please contact the SURE team.

Logging out, timeouts and re-authentication

When you are ready to exit SURE, you will have the following options:

- **Disconnect** – To keep the remote session running (for example, if you are running some analysis that will take some time to complete), simply close the Citrix Receiver virtual desktop window (using the X in the top left hand corner)
- **Log off** – If you do not have any applications running, save your work, and from the Windows/Start menus, select Log off to close your VM.
- **Lock** – If you are stepping away from your workstation, please lock the screen to ensure your SURE session is not visible to any other parties.
- **Restart** – Use this option to refresh your machine following any updates or to clear temporary files from your scratch disk.
- **Shut down** – It is not advisable to shut down your virtual machine through Citrix Receiver as you may then have difficulty starting it. If you do shut down your machine and you are then unable to access it, please contact the SURE team for assistance.

The SURE Access Gateway will time out after 15 minutes of inactivity. After you have launched your virtual machine, you will remain logged in even if the Access Gateway site times out.

After launching your virtual machine, you will be disconnected from the remote desktop window if you have not touched the keyboard or mouse for 60 minutes. It will not log you out of the virtual machine, so any programs running will continue.

If the SURE Access Gateway has timed out, go to <https://access.sure.org.au>, to log in and launch your virtual machine.

The Curated Gateway

The Curated Gateway is a specialised application that has been developed to transfer files into and out of the SURE facility. All other methods of file transfer into and out of SURE, such as the use of removable media, clipboard functions, email and via the internet, have been disabled for security reasons.

The Curated Gateway consists of two components. One component is accessible outside of SURE (the **External Curated Gateway**) and one component is accessible within SURE (the **Internal Curated Gateway**).

The **External Curated Gateway** is accessible via the internet using the SSL Certificate and login credentials provided for SURE. It is used for uploading inbound files that a user requires within SURE and downloading outbound files created in SURE for use outside of SURE such as final research outputs for publication.

The **Internal Curated Gateway** is used for downloading inbound files to use within SURE after they have been reviewed or for uploading outbound files created in SURE for review to access outside of SURE.

All files that pass through the Curated Gateway must be reviewed before they are made available within SURE or outside of SURE. All files that pass through the Curated Gateway and all actions to those files are logged and may be subject to audit at any time by identified systems administration or management staff that are part of the SURE team.

Permissions for the Curated Gateway

When a new SURE account is created, permissions are assigned for each user based on requirements of the Data Custodians and the Authorised Delegate. Permissions for each user with access to a workspace will be detailed on the application form. It is possible to assign no permissions for the Curated Gateway to a SURE user.

| Curated Gateway permissions | Description | Example of type of user |
|-----------------------------|--|---|
| UPLOAD | A user can upload inbound and outbound files to the Curated Gateway for review | Researchers, analysts and data custodians |

| Curated Gateway permissions | Description | Example of type of user |
|-----------------------------|---|--|
| DOWNLOAD | A user can download inbound and outbound files to the Curated Gateway following review | Researchers and analysts |
| CURATE | Reviews inbound files containing unit record data entering SURE. A user with curate permissions must accept a file before it is available to a user within SURE | Data Custodian, Chief Investigator or an approved delegate |
| NO PERMISSIONS | A user does not have permission to upload, download or review any files in the Curated Gateway (this may be required as a condition of some workspaces) | PhD student or overseas-based researcher |

Transferring files

To upload files to use within SURE, go to the External Curated Gateway at <https://cg.sure.org.au/>.

Log on the External Curated Gateway using the same authentication details that were supplied to you for SURE (username, password and one time passcode).

The screenshot shows a web browser window with the address bar displaying 'https://cg2.sure.org.au/login'. The page has a blue header with the SURE logo (Secure Unified Research Environment) and the title 'Site B External Curated Gateway Login'. The main content area is a login form with three input fields labeled 'Username:', 'Password:', and 'Token:'. Below these fields are two buttons: 'Help' and 'Login'.

There are 4 tabs in the External and Internal Curated Gateway:

- **Inbound** – lists files that have been uploaded to the Curated Gateway for review to use within SURE
- **Outbound** - lists files that have been uploaded to the Curated Gateway for review to use out of SURE

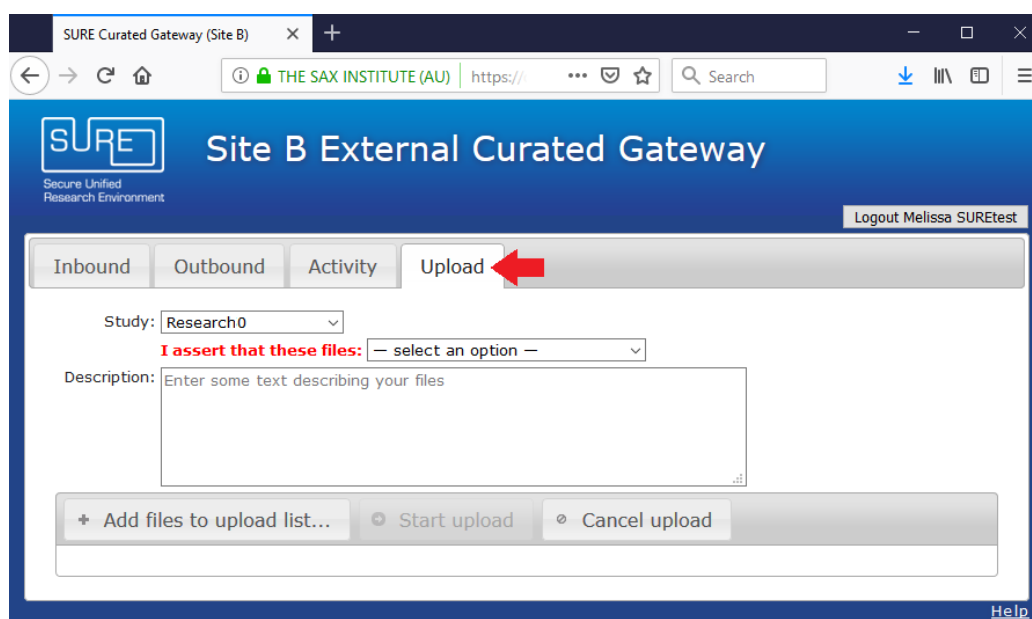
-
- **Activity** – contains a list of recent Curated Gateway activity that has occurred for the project that an investigator is involved in.
 - **Upload** – select this tab to upload a file to use within SURE.

You can sort the list of inbound and outbound files according to column. You can also search all entries in the Inbound and Outbound tabs and modify how many entries are displayed per page in the list of files.

Inbound File Transfer

Uploading a file for use in SURE

1. Go to the External Curated Gateway at <https://cg.sure.org.au/>.
2. Select the **Upload** tab
3. Select the project you are uploading to in the **Study** dropdown. If you only have access to one project, this will be populated for you.
4. Select an option under **I assert that these files:** to confirm whether the file does or does not contain unit record data.
5. Enter a description for the file to advise the workspace Curator of the purpose for importing it into SURE, e.g. an article on methodology, program script for data cleaning, etc. The text box can be expanded by dragging the bottom right-hand corner. If you are uploading a data file, please include any metadata that you have to accompany the data set (e.g. data course, temporal coverage, number of records, number of columns) in the description text box or as a separate file upload.



6. Click **+ Add files to upload list...** and locate the files you wish to upload from your local computer.
Note. More than one file can be uploaded at a time.
7. Click **Start Upload** to upload the selected files. You will not be able to upload a file until you have input your selections and description as per steps 2-4 above.

Once a file has been uploaded, it will be displayed in the list of inbound files with the status 'Awaiting scanning.' Following virus scanning, the status of the file will change to 'Awaiting review.'

Notification

An email is sent to a user via their nominated email address to notify them of actions taken on a file and of changes in the status of files they have uploaded (e.g. a file has been checked and approved to enter SURE).

Downloading an approved file within SURE

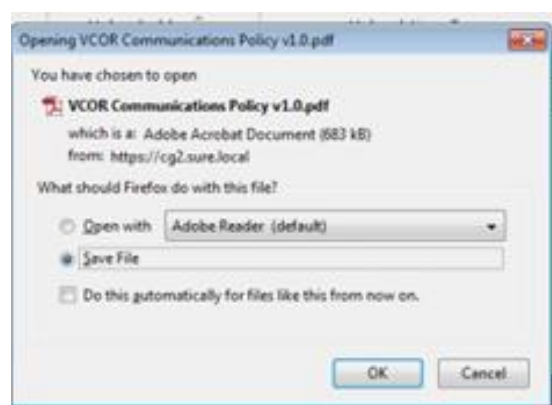
To download a file after the file has been accepted, log on to SURE and launch your virtual machine.

Once the Windows desktop appears, open the Firefox browser icon from the desktop.

Log into the Internal Curated Gateway <https://cg2.sure.local> using your username, password and one time passcode. The file that has been accepted for download should be visible (if it is not visible, click on the **Actions** header to sort the files so that the files that are ready to download are displayed at the top). Click **Download**.



A window will appear prompting the user to **Open**, **Save** or **Cancel** the file. It is recommended that you save a file when first retrieving it from the Curated Gateway to a location on the network drive of your workspace.



Outbound File Transfer

Files taken out of SURE should not be disclosive. Disclosure relates to the inappropriate attribution of information to a data subject, whether an individual or an organisation. Disclosure has two components: identification and attribution.¹

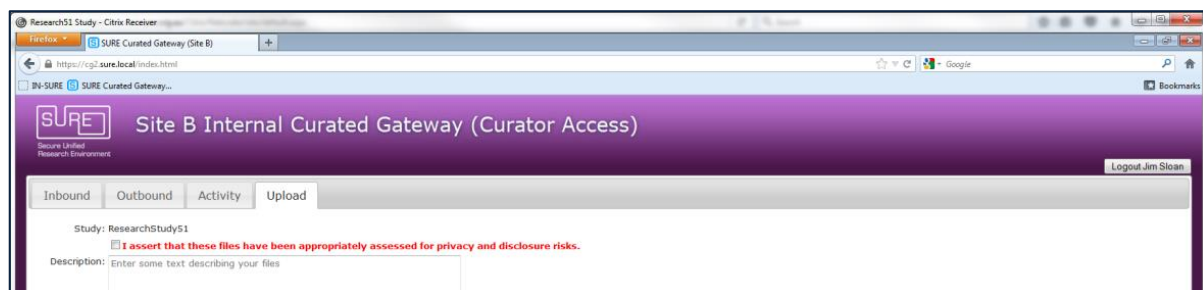
To minimise the risk of disclosing identifying information, a user should only upload files to use outside of SURE that contains research output at a level of detail suitable for publication. The SURE environment contains word processing and presentation software in addition to software packages to conduct statistical analysis so that researchers can prepare drafts of articles, conference presentations and other papers within the SURE environment.

Summary data and other research output, needs to be assessed by researchers on a case-by-case basis for disclosure risk. Users will need to assert that all files taken out of SURE have been assessed for privacy and disclosure risks. Principles of statistical disclosure control are covered in the SURE Researcher Training Program and a list of references will be included as part of the training materials.

Uploading a file for export out of SURE

To upload a file for use outside of SURE:

1. Open the internet browser within your SURE virtual machine and log on to the Internal Curated Gateway at <https://cg2.sure.local> using your username, password and token.
2. Click on the **Upload** tab



¹ This definition is taken from the ESSNET Glossary on Statistical Disclosure Control (Version last updated May 2009). Accessed from <http://neon.vb.cbs.nl/casc/glossary.htm> on 14 February 2012.

3. Click **+ Add files** and search for the files you wish to upload from your network folder in SURE.
Note: More than one file can be uploaded at a time.
4. Click **Start Upload** to upload the selected files. Note: You will not be able to upload a file until text is added to the **Description** field and you have **checked the box** next to the assertion that files have been appropriately assessed for privacy and disclosure risks.

Notification

Users will be sent an email to notify them of actions they have taken on a file within the Internal Curated Gateway and of changes in the status of files that they have uploaded (e.g. a file has been checked and accepted and is now available to download from the External Curated Gateway).

Curation

Outbound files uploaded to the Internal Curated Gateway for use outside of SURE are reviewed and accepted by the Curator prior to being made available to download from the External Curated Gateway.

Downloading an approved file for use outside of SURE

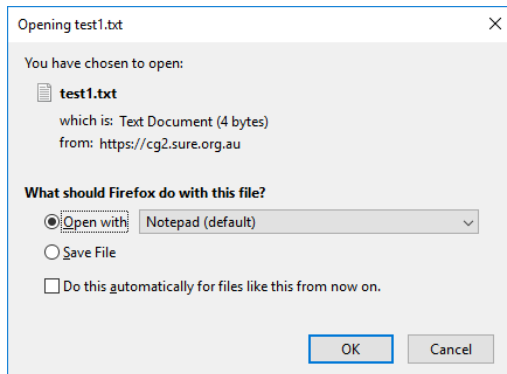
1. Log on to the External Curated Gateway at your assigned gateway <https://cg.sure.org.au/> using your username, password and token.
2. Click **Outbound** tab

| File name | File size | Study | Uploaded by | Upload time | Description | Current state | Actions |
|------------|-----------|-------|-------------|-------------------------|------------------------------|---------------|----------|
| test1.txt | 4 | | | Fri Feb 1 15:51:05 2019 | test | accepted | download |
| Readme.txt | 285 | | | Wed Jul 6 16:54:55 2016 | test upload from cgi in 5106 | accepted | download |

Any file that has been accepted for download should be visible. If it is not visible, click on the Actions header to sort the files so that files ready to download are displayed at the top.

Note: File access from the External Curated Gateway will expire after 2 weeks. If a file for download has expired, you can **Refresh** the file from the Internal Curated Gateway to make it visible for download from the External Curated Gateway.

3. Once you select Download, a window will appear prompting the user to Open, Save or Cancel the file. It is recommended that you save a file to your local computer when downloading it from the External Curated Gateway.



File logging and audit

A log of all files uploaded and downloaded to the Curated Gateway is kept and a copy is taken of all files. This enables the movement of files into and out of the Curated Gateway to be audited.