



IDHS – Welcome Pack for Secure Data Handling

1. Document Information

Document Name	IDHS-Welcome-Pack-for-Secure-Data-Handling-v2.5.docx
Service	Identifiable Data Handling Solution (IDHS)
Author	Bhavesh Varsani (BV)
Contributors	
Issue Date	27/07/2017

2. Document History

Version	Date	Summary of change
1.0	09/03/2013	First Draft (BV)
1.1	12/06/2013	Document amended and sections added (BV)
1.2	17/06/2013	Sections for Dual factor amended (BV)
1.3	18/06/2013	Dual Factor Mobile App section added (BV)
1.4	22/07/2013	Added Token Management section (BV)
1.5	24/07/2013	Document released (BV)
1.6	01/08/2013	Section 7 and 8 Updated (BV)
1.7	30/08/2013	ICE Steps updated for password forget/expired (BV)
1.8	18/10/2013	Incorporated "Auto generated password" for secure mail out (BV)
1.9	10/03/2014	Incorporated Password Forgotten / Expired process changes (BV)
2.0	15/05/2014	Updated password policies (BV)
2.1	27/09/2014	Secure Print Section added (BV)
2.2	20/10/2014	Presentation update to Password policies defining password polices as applied to relevant portals (BV)
2.3	27/11/2014	Updated the Secure Data out section (BV)
2.4	22/09/2015	Password Policy Updates (BV)
2.5	27/06/2017	Updated file transfer out section to indicate that transfers can be cancelled before a file is downloaded (AJP)

Contents

1. Document Information	1
2. Document History	1
3 Introduction	5
4 Apply for IDHS Service	5
5 Register with UCL IDHS	5
5.1 Password Policy – Data and Apps Portal	5
5.1.1 Password Strength	5
5.1.2 Password Age	5
5.1.3 Password History	5
5.1.4 Password Expiry Notification	5
5.2 Password Policy – File Transfer Portal	5
5.2.1 Username Policy – Applies only to external users to UCL who can only send data in	5
5.2.2 General password policies	5
5.2.3 Password Strength	6
5.2.4 Password Age	6
5.2.5 Password History	6
5.2.6 Password Expiry Notification	6
6 General Overview	6
7 IDHS Data Handling	7
7.1 Setting up and use of UCL Dual Factor Self Service Console	7
7.1.1 First time logon with soft token (software)	7
7.1.2 First time logon with hard token	8
7.1.3 Download and Install Token Auto Generator software	9
7.1.4 First time logon to the Self-service Portal	13
7.1.5 Configure Question and Answers (Q&As) for ICE logon	14
7.1.6 Changing your IDHS Password	15
7.1.7 Changing your PIN for your Token	15
7.1.8 Downloading a software Token	15
7.2 In case of Emergency (ICE) Logon	18
7.2.1 Logon to the UCL Dual Factor Self Service Portal using ICE Logon	18
7.2.2 Report a lost token	20

7.2.3	Generate an Emergency Token.....	21
7.3	Accessing the IDHS Data Handling Gateway.....	21
7.4	Accessing Data within the IDHS Environment.....	22
7.4.1	Using Remote Apps.....	22
7.4.2	Using Virtual Desktops	23
7.5	Research Shared Folder area	24
7.5.1	Launching Research Shared folder area	24
7.5.2	Research Shared Folder usage.....	25
7.5.3	When sending Data out	25
8	Secure Data out.....	26
8.1	Via File Transfer	26
8.2	Via FTP	28
9	Secure Printing from IDHS	29
9.1	Pre-requisites	29
9.2	Applying for Print Service	29
9.3	Printing.....	29
9.3.1	Print from application.....	29
9.3.2	Release print jobs	29
10	Registering an external user.....	30
10.1	Step 1: Send invite by UCL IDHS Research space owner.....	30
10.2	Step 2: Register by External collaborator.....	31

3 Introduction

Welcome to the UCL IDHS service, maintained by the IT for SLMS Infrastructure Team. This welcome pack will guide you on how to access the IDHS system and handle data.

4 Apply for IDHS Service

Before accessing the system, you will need to apply to register with the UCL IDHS system information available at <https://www.ucl.ac.uk/aisc/services/handling-sens-data/tech-soln> (use Mozilla Browser).

5 Register with UCL IDHS

A user name will be created for you, complying with the “Username” and “Password” policies as shown below

5.1 Password Policy – Data and Apps Portal

The Policy below applies only to the Data and Apps portal

5.1.1 Password Strength

Minimum Password Length: 7

Password must meet complexity requirements, i.e mixture of Upper case, lower case, numbers and special characters.

5.1.2 Password Age

Password has to be changed every 90 days

5.1.3 Password History

You are not allowed to re-use any of your last 24 passwords

5.1.4 Password Expiry Notification

Password expiry notification emails are sent 20 days, 10 days, 5 days and each day less than 5 days before expiry. If password is not changed then passwords are automatically reset by the system, locking user out of the system.

5.2 Password Policy – File Transfer Portal

The Policy below applies only to the File transfer portal

5.2.1 Username Policy – Applies only to external users to UCL who can only send data in

Minimum User Name Length: 6

Maximum User Name Length: 64

Prohibited Characters: / \ : * ? " < > | @ _ ! # ' &

5.2.2 General password policies

Disable File Transfer account after:

3 Invalid login attempts

90 Days of inactivity

5.2.3 Password Strength

Minimum Password Length: 7

Minimum Number of Upper Case Letters: 1

Minimum Number of Lower Case Letters: 1

Minimum Number of Digits: 1

Minimum Number of Special Characters: 1

Allowable Special Characters: ~@#%&*()-_+=<>?/\;:[]{}.,

5.2.4 Password Age

Password has to be changed every 60 days

5.2.5 Password History

You are not allowed to re-use any of your last 24 passwords

5.2.6 Password Expiry Notification

Password expiry notification emails are sent 10 days, 5 days and 1 day before expiry. If password is not changed then passwords are automatically reset by the system, locking user out of the system.

6 General Overview



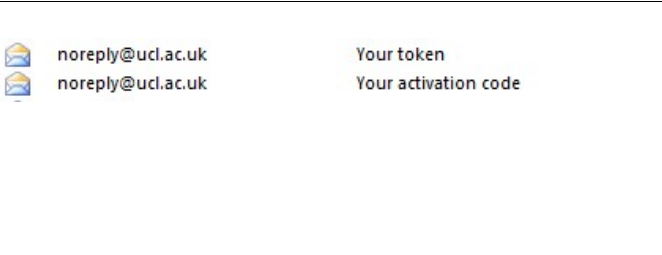
IDHS provides three key functions as:

1. Data transfer in via <https://filetransfer.idhs.ucl.ac.uk> (File Transfer Portal). File transfer in can be done in two ways as described in the “Data Transfer In welcome pack”:
 - a. Secure web for up to 5 individual files
 - b. Secure FTP using for bulk file transfers
2. Data handling via <https://accessgateway.idhs.ucl.ac.uk> (Data and Apps Portal)
 - a. User your IDHS username
 - b. Use authentication combination as:
 - i. Password for the IDHS account
 - ii. Combination of **PIN** and Auto Generated **Token**
3. Dual Factor – Self service console: Portal to self-register, install auto token generating system and managing via <https://registration.idhs.ucl.ac.uk/dss>
4. Secure data transfer out via “File Transfer App” via the portal <https://accessgateway.idhs.ucl.ac.uk>

7 IDHS Data Handling


7.1 Setting up and use of UCL Dual Factor Self Service Console

7.1.1 First time logon with soft token (software)

<p>https://registration.idhs.ucl.ac.uk/dss/</p>	<p>Navigate to the Dual Factor – Self Service Portal</p>
	<p>Enter your IDHS user account and click on continue</p>
	<p>Click on Channels and select your pre-registered email address</p> <p>Click continue</p>
	<p>Your email account should get two emails with subject lines</p> <p>Your activation code & Your token</p>

<p>Log in to application: Self-Service Console</p> <p>Step 1</p> <p>Login Name: <input type="text" value="inttester6"/></p> <p>Authenticator: <input type="text" value="One-Time Password"/></p> <p>This token/computer is created/registered by 1. Send yourself a activation code by select 2. Enter the activation code to activate your</p> <p>Channels: <input type="text" value="Email Me"/></p> <p>Activation Code: <input type="text" value="6058"/></p> <p><input type="button" value="Continue"/></p>	<p>Firstly, open the email with the subject line “Your activation code”</p> <p>By doing this this step, we are activating your token for use.</p> <p>Use the activation code provided in the email.</p> <p>Go back to the Dual Factor Self-service Portal and enter it there.</p> <p>Click on Continue</p>
<p>Log in to application: Self-Service Console</p> <p>Your token has been successfully activated.</p> <p>Step 1</p> <p>Login Name: <input type="text" value="IntTester6"/></p> <p>Authenticator: <input type="text" value="One-Time Password"/></p> <p>One-Time Password: <input type="text"/></p> <p><input type="button" value="Continue"/></p>	<p>You will see a message that the token has successfully been activated</p>
<p>NEXT Steps</p>	<p>To download, install and configure the associated software that auto generates your token Section 7.14 of this document</p>

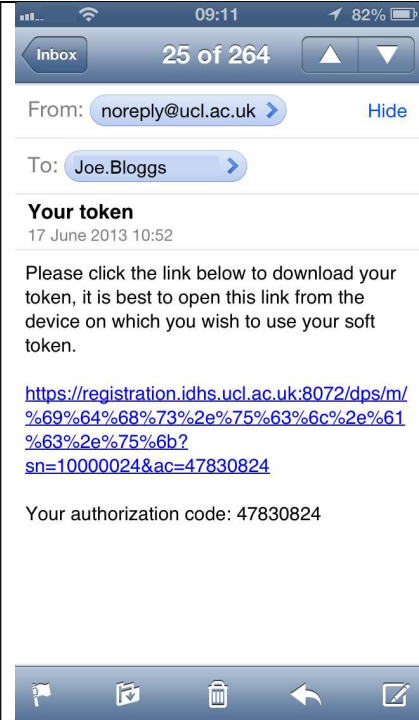

7.1.2 First time logon with hard token

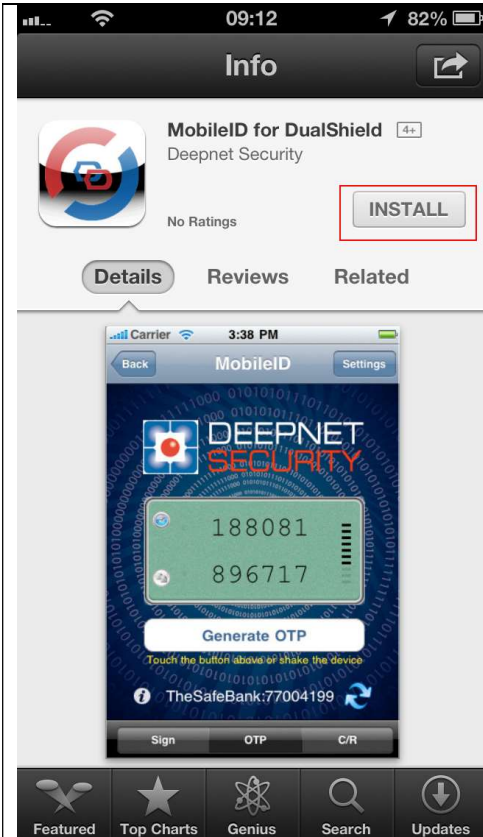
	<p>You have already been provide with a hard token as a new user</p>
	<p>Carry on with section7.1.3: First time logon to the Self-service Portal</p>

7.1.3 Download and Install Token Auto Generator software

7.1.3.1 Mobile App Instructions

7.1.3.1.1 iPhone, iPod touch and iPad

 <p>Your token 17 June 2013 10:52</p> <p>Please click the link below to download your token, it is best to open this link from the device on which you wish to use your soft token.</p> <p>https://registration.idhs.ucl.ac.uk:8072/dps/m/%69%64%68%73%2e%75%63%6c%2e%61%63%2e%75%6b?sn=10000024&ac=47830824</p> <p>Your authorization code: 47830824</p>	<p>Using your iPhone, iPod touch or iPad, Open the email with the subject line “Your token”</p> <p>By doing this step you are downloading & installing the application that auto generates the token and installing the token on your device</p> <p>Click on the link in the email</p>
 <p>MobileID Installation iPhone/iPod touch/iPad</p> <p>Step 1.</p> <p>If you have not installed the MobileID software, then click the button below to install the software first:</p> <p><input type="button" value="Install Software"/></p> <p>Step 2.</p> <p>If you have installed the MobileID software, then click the button below to install your MobileID token:</p> <p><input type="button" value="Install Token"/></p>	<p>A browser within your device will open up as shown in the screenshot.</p> <p>Complete Step 1 by clicking on “Install Software”</p> <p>This will launch the Apple Store where you can download and install the free app</p>



Click on Install.

Note: If you have a password for your Apple App Store, please enter your own credentials to allow the install of the software.

Wait for the “MobileID for DualShield” app to install on your device.



Once successfully installed, carry on with the next step




Once your **App has installed**, Go back to the browser page and you will notice Step 1 as complete.



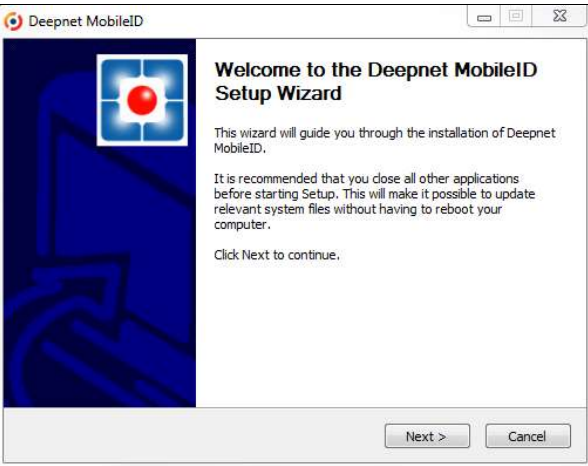
Carry on with **Step 2 to Install Token** on your device



Click on **Install Token**

	<p>Enter your IDHS username and IDHS password</p> <p>Click on continue</p>
	<p>The token is now available on your device.</p> <p>The token refreshes every 60 seconds.</p> <p>Before using the token, click on generate OTP button to get the latest token</p>
<p>Next Step</p>	<p>Carry on with section 7.1.3 First time logon to the Self-service Portal of this document</p>

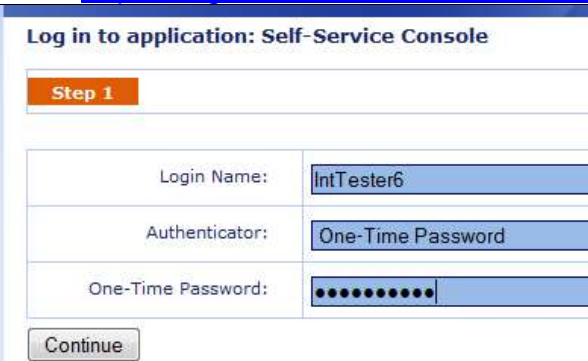

7.1.3.2 Desktop PC Instructions

	<p>Open the email with the subject line “Your token”</p> <p>By doing this step you are downloading and installing the application that auto generates the token</p> <p>Click on the link and enter your IDHS credentials</p>
---	---

 <p>The screenshot shows a web form titled "Download MobileID Token". It contains three input fields: "Domain:" with a dropdown menu showing "idhs.ucl.ac.uk", "User Name:" with a text box containing "inttester6", and "Password:" with an empty text box. Below the fields is a "Continue" button with a document icon.</p>	
 <p>The screenshot shows a page titled "Download MobileID token". It lists several options: "Windows Mobile", "Windows Mobile 6 [+]", "J2ME version", "J2ME MIDP 2.0 [+]", "PC Desktop", "PC Desktop" (highlighted with a red box), and "USB Flash Driver".</p>	<p>Download the PC Desktop and install the software.</p> <p>This is a PC option. For Mobile devices, you will be presented with suitable options</p>
 <p>The screenshot shows a "Deepnet MobileID Setup Wizard" window. The title bar says "Deepnet MobileID". The main text reads: "Welcome to the Deepnet MobileID Setup Wizard. This wizard will guide you through the installation of Deepnet MobileID. It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer. Click Next to continue." At the bottom, there are "Next >" and "Cancel" buttons.</p>	<p>Click on Next → Agree T&Cs and finish installing</p>

 <p>The screenshot shows the MobileID application window with the title 'MobileID'. It contains a 'Token Help' menu, a message 'You have to set a PIN to protect your tokens:', a 'Please enter your PIN:' field, a 'Please confirm your PIN:' field, and a 'GO' button.</p>	<p>Launch the installed software “Deepnet MobileID” from your PC</p> <p>Start → All Programs → Deepnet security → MobileID</p> <p>Enter your PIN: Default is 1234</p>
 <p>The screenshot shows the MobileID application window with the title 'MobileID - idhs.ucl.ac.uk:DNMT10000019'. It features the MobileID logo, a digital display showing '290541', a 'GO' button, a calendar icon, and the 'DEEPNET SECURITY' logo with the text 'powered by'.</p>	<p>You will get an Auto generated Token that changes every 60 Seconds.</p>
<p>Next Step</p>	<p>Carry on with section 7.1.3 First time logon to the Self-service Portal of this document</p>

7.1.4 First time logon to the Self-service Portal

<p>URL: https://registration.idhs.ucl.ac.uk/dss/</p>	<p>Go to the self-service portal</p>
 <p>The screenshot shows the 'Log in to application: Self-Service Console' page. It has a 'Step 1' indicator and three input fields: 'Login Name:' with 'IntTester6', 'Authenticator:' with 'One-Time Password', and 'One-Time Password:' with masked characters. A 'Continue' button is at the bottom.</p>	<p>Enter your One-Time password</p> <p>If your pin were 1111 and Auto generated token is 290541</p> <p>One-Time Password = 1111290541</p>
 <p>The screenshot shows the 'Reset PIN' page with the message 'Your must reset the PIN for token 10000024'. It has three input fields: 'Old PIN:', 'New PIN:', and 'Confirm New PIN:'. A 'Continue' button is at the bottom.</p>	<p>This step only occurs the first time you log in.</p> <p>Change your pin here</p>

Welcome to your self-service console

7.1.5 Configure Question and Answers (Q&As) for ICE logon

Click on My Account and navigate to the "Question and Answers" Tab

This set up is required to be configured to access the system "In Case of and Emergency" (ICE Logon)

Create at least 3 Q&As

Ques	Answer
1	What is my mother's maiden name?
2	Where is my birthplace?
3	What is the title of my favourite game?

These questions will be used to access the system and **generate emergency tokens**

7.1.6 Changing your IDHS Password

My Account

General Questions & Answers Password

Old Password:

New Password:

Confirm:

Click on **Password** tab to change your IDHS account password

Click on **EDIT** to enable the fields

Then enter the passwords as prompted and click on **save**

7.1.7 Changing your PIN for your Token

QUALSHIELD UCL Dual Factor Self Service Console

Home My Account My Tokens My Certificates My Site Stamp Emergency Report Help Logout

My Tokens

Serial	Description	Product	Shared With	Status	Edit	Delete
1 10000062		MobileID/Time-Based		ACTIVE	▼ Edit	Delete
2 20007000		SafeID/Time-Based		ACTIVE	▼ Edit	Delete

Create Register

On the Security and Token Portal, click on “My Tokens”

MobileID/Time-Based = Soft Tokens
SafeID/Time-Based = Hard Tokens

Serial	Status	Edit	Delete
1	ACTIVE	▼ Edit	Delete
2	ACTIVE	▼ Edit	Delete

Disable
Synchronize
Reset PIN

Click on the ▼ next to the token

Click on **Reset PIN**

Reset PIN

PIN:

Confirm:

Enter the **NEW 4 digit PIN**

Note: you can only use a PIN once.

7.1.8 Downloading a software Token

QUALSHIELD UCL Dual Factor Self Service Console


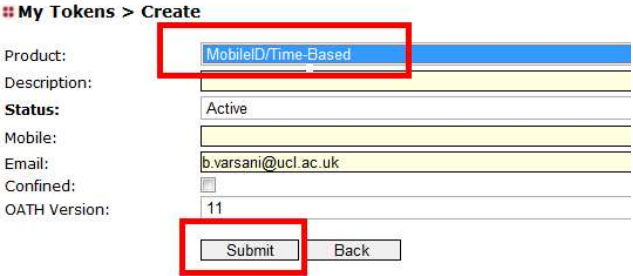
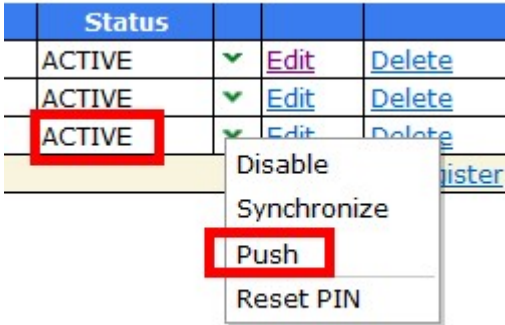
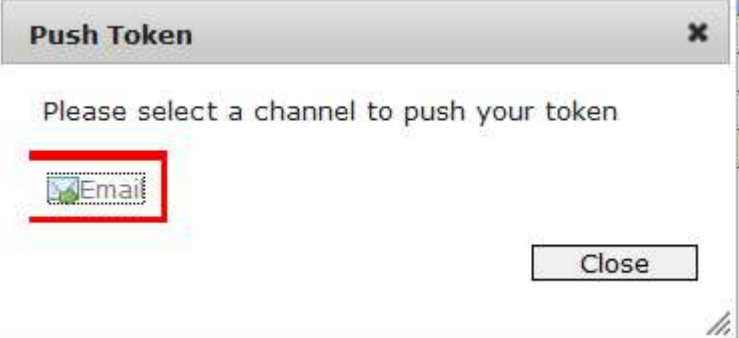
Home My Account My Tokens My Certificates My Site Stamp Emergency Report Help Logout

My Tokens

Serial	Description	Product	Shared With	Status	Edit	Delete
1 10000062		MobileID/Time-Based		ACTIVE	▼ Edit	Delete
2 20007000		SafeID/Time-Based		ACTIVE	▼ Edit	Delete

Create Register

On the Security and Token Portal, click on “My Tokens”

	<p>Click on Create</p>
	<p>Ensure Product is : MobileID/Time-Based</p> <p>Click on submit</p>
	<p>Activate Token by clicking on email you have been sent to your IDHS registered email with subject line Your Activation Code</p>
	<p>Once token is activated, the status will be ACTIVE</p> <p>Click on the ▼ next to the token</p> <p>Click on push</p>
	<p>Click on email</p>
<p>Next Steps</p>	<p>Carry on with steps as per section 7.1.3 Download and Install Token Auto Generator software</p>

7.2 In case of Emergency (ICE) Logon



This is a three step process as follows:

7.2.1 Logon to the UCL Dual Factor Self Service Portal using ICE Logon

This process can only be used if you have set up the Q&As as per section [7.1.4 Configure Question and Answers \(Q&As\)](#) of this document.

7.2.1.1 Password Forgotten / Expired process


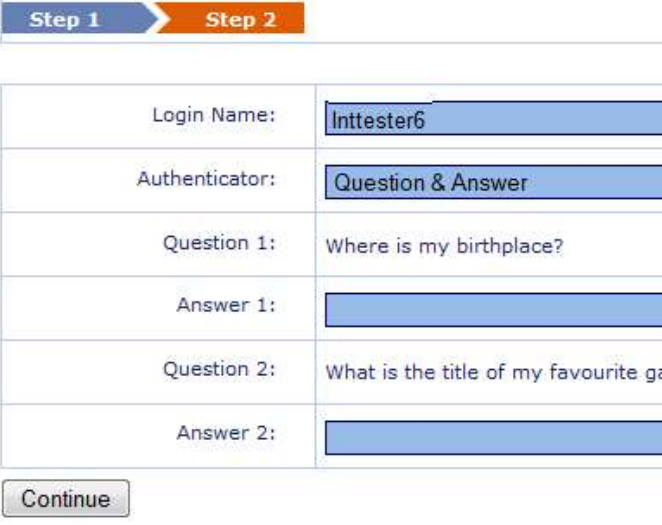
**** For this method you will require setting up a remote session with IT for SLMS Infrastructure team so they can view you go this stage and help you reset your password. They will need to enter your old password for you****

<p>https://registration.idhs.ucl.ac.uk/dss</p>	<p>Logging into self service to generate emergency tokens. Go to the Self service portal</p> <p>Note: This will only work if you have created these Q&As during the self service set up as defined in Click on “Use ICE logon steps” on top of the login name on the right</p>
	<p>Enter your IDHS username</p>
	<p>Select the Authenticator as One-Time Password</p> <p>Enter the One-Time Password (PIN+Token)</p>

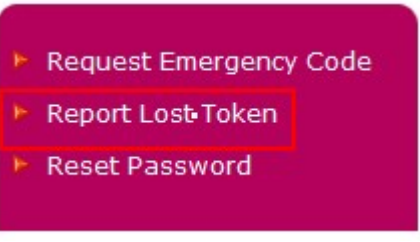
<p>Log in to application: Self-Service Console</p> <p>Step 1 Step 2</p> <p>Login Name: <input type="text" value="Inttester6"/></p> <p>Authenticator: <input type="text" value="Question & Answer"/></p> <p>Question 1: Where is my birthplace?</p> <p>Answer 1: <input type="text"/></p> <p>Question 2: What is the title of my favourite game?</p> <p>Answer 2: <input type="text"/></p> <p><input type="button" value="Continue"/></p>	<p>Enter the answers to the Questions previously set up</p> <p>Click one Continue</p>
<p># My Account</p> <p>General Questions & Answers Password</p> <p>Old Password: <input type="text"/></p> <p>New Password: <input type="text"/></p> <p>Confirm: <input type="text"/></p> <p><input type="button" value="Edit"/></p>	<p>Change Password</p> <p>Click Myaccount → Password</p> <p>Click on EDIT to enable the fields</p> <p>Then enter the passwords as prompted and click on save</p>

7.2.1.2 Token Lost / not working

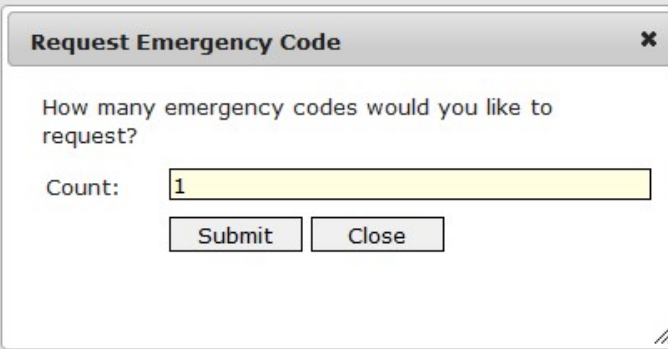

<p>https://registration.idhs.ucl.ac.uk/dss</p>	<p>Logging into self service to generate emergency tokens. Go to the Self service portal</p> <p>Note: This will only work if you have created these Q&As during the self service set up as defined in</p>
<p>Use ICE logon steps</p> <p><input type="text"/></p>	<p>Click on “Use ICE logon steps” on top of the login name on the right</p> <p>Enter your IDHS username</p>

	<p>Select the Authenticator as Static Password</p> <p>Enter the IDHS Password</p>
	<p>Enter the answers to the Questions previously set up</p> <p>Click one Continue</p>
	<p>Continue with section 7.2.2 Report a lost token of this document</p>

7.2.2 Report a lost token

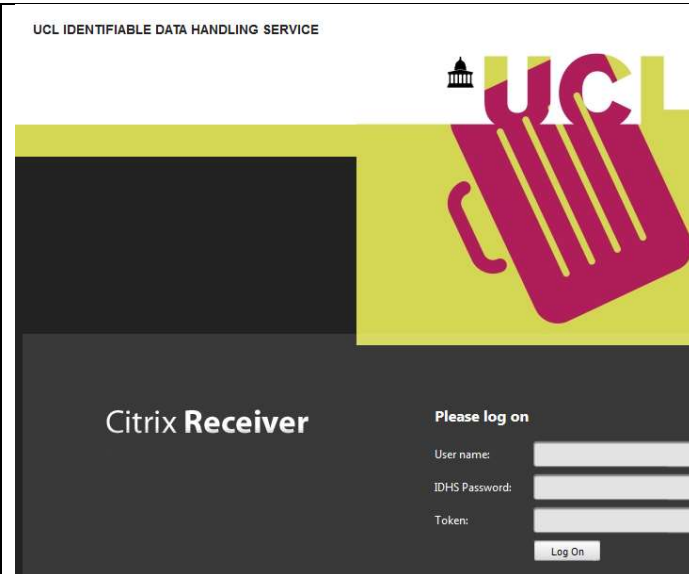
	<p>Click on Report or Report Lost Token</p> <p>This will notify the IDHS Service service desk with the problem you have occurred by logging a Service Desk Ticket on your behalf.</p>
	<p>Continue with section 7.2.3 Generate an Emergency Token of this document</p>

7.2.3 Generate an Emergency Token

	<p>Click on Emergency to create emergency tokens → select number and click on submit</p> <p>The emergency tokens are used to access the IDHS service when you don't have access to the DeepNet Auto token generator or lost your token</p> <p>You can ONLY use this token ONCE</p> <p>You can then use this token to login to the IDHS access gateway service (for data handling) and the Dual factor self service portal with your IDHS credentials</p>
	<p>Generate emergency token</p> <p>Select the Token by ticking the check box</p> <p>You can either EMAIL it to your IDHS registered email address OR use it to access the gateway</p> <p>You can ONLY use this token ONCE</p>
	<p>Use this Emergency token as a one time login to access the UCL IDHS Secure Data Handling Gateway</p>
Next Steps	<p>Section 7.3 Access the IDHS Data Handling Gateway</p>

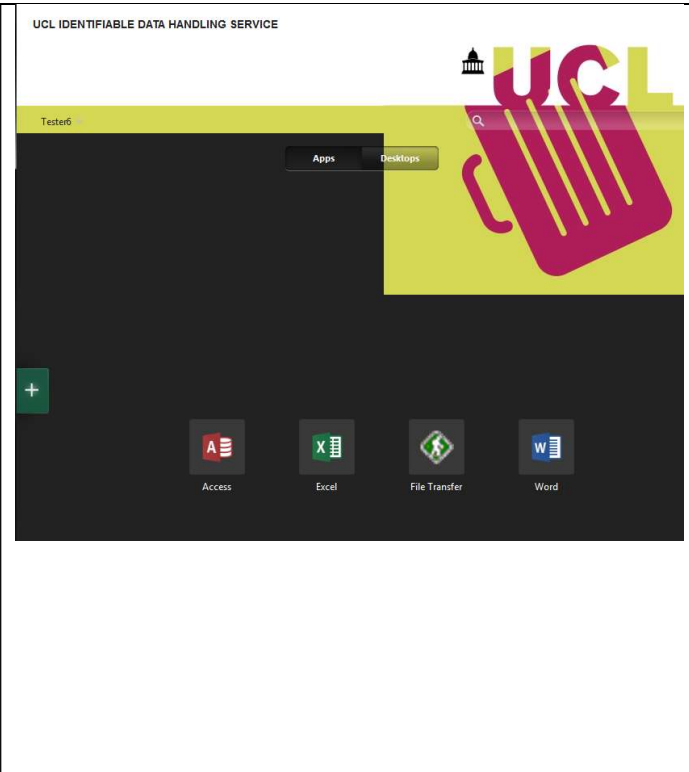

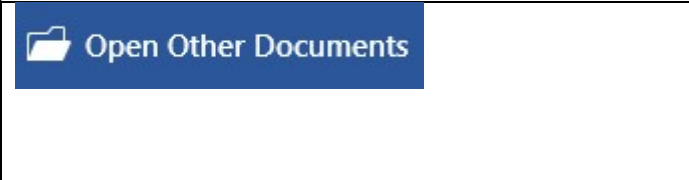
7.3 Accessing the IDHS Data Handling Gateway

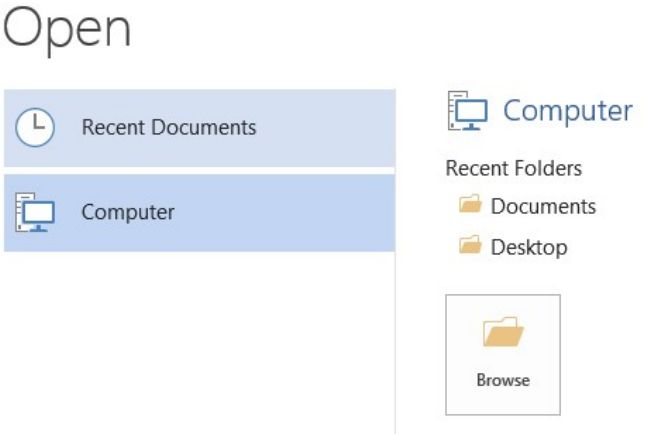
URL =	https://accessgateway.idhs.ucl.ac.uk
-------	---

	<p>Login using registered IDHS Username.</p> <p>With dual authentication as:</p> <p>IDHS Password AND TOKEN (PIN+TOKEN)</p> <p>If your pin were 1111 and Auto generated token is 29054, then your token will be 111129054</p> <p>If using emergency token then TOKEN= the emergency token by itself (without the PIN)</p>
---	--

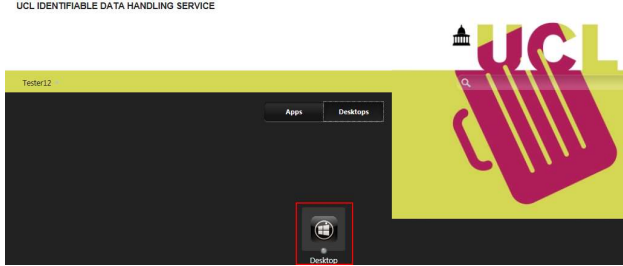

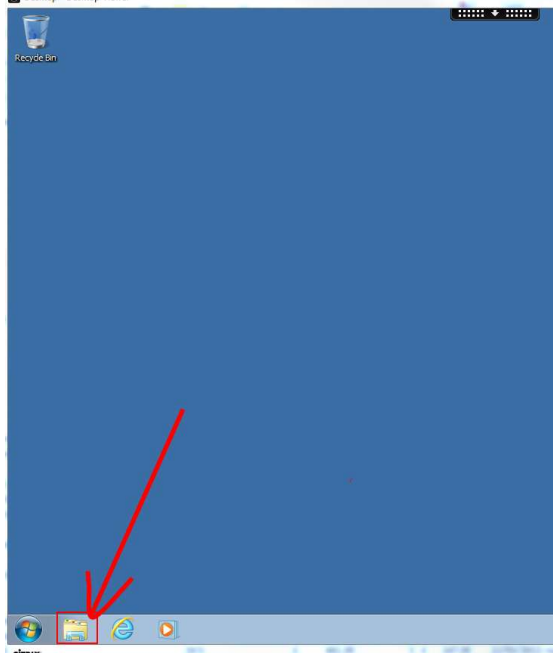
7.4 Accessing Data within the IDHS Environment

7.4.1 Using Remote Apps

	<p>Once successfully logging in, you will receive “app” options as shown.</p> <p>If options not available as screenshot, click on “Apps”</p>  <p>Word – is to launch the word app Excel – is to launch the excel app Access – is to launch the access app. File Transfer – is the link to the IDHS transfer in portal as https://filetransfer.idhs.ucl.ac.uk Click this link to send data out securely.</p>
	<p>Click on app. Word as shown in this example.</p> <p>Once the app launches, click on open other documents</p>

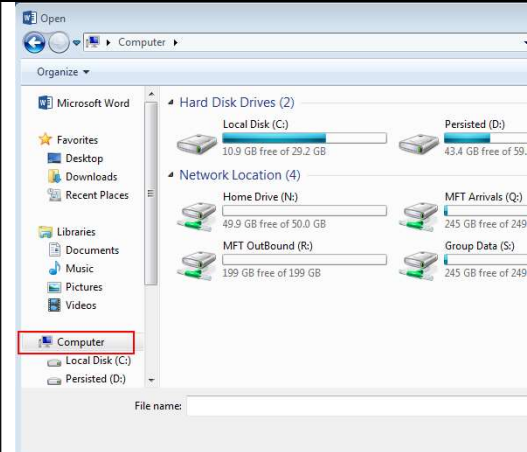
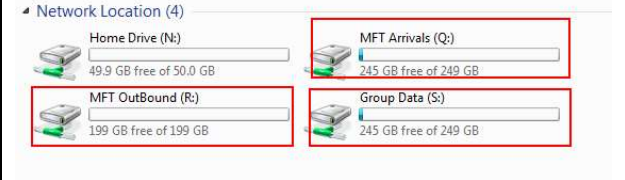
	<p>Click on Computer → Browse → Computer.</p>
<p>Next Step</p>	<p>Section 7.5.1 “Launching Research Shared Folder area” of this document</p>

7.4.2 Using Virtual Desktops

	<p>Once logged in, to use a Desktop to access the data, click on “Desktops”</p>  <p>Then click on Desktop icon as squared on the screenshot on the left.</p> <p>This will launch a virtual desktop.</p>
	<p>A new window citric session will open.</p> <p>To view the data click on the Windows Explorer icon as shown</p>
<p>Next Step</p>	<p>Section 7.5.1 “Launching Research Shared Folder area” of this document</p>

7.5 Research Shared Folder area

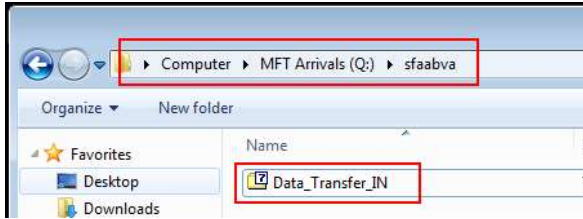
7.5.1 Launching Research Shared folder area

	<p>Click on Computer on the left hand Menu</p>
<p>There are three possible locations where data exists: MFT arrivals, Group Data and MFT Outbound</p> <p>Both MFT arrivals and Group Data will have a folder within it for each Research space that a user will have access to.</p> 	<p>MFT Arrivals* is where the encrypted data arrives when sent in.</p> <p>Group Data is where data needs to be decrypted and stored. This is the location where the data should be transferred to.</p> <p>MFT Outbound is where data you want to send out should be copied to before sending the data out. Then follow section 8 “ sending data out” of this document</p> <p>All three folders except MFT Arrivals* should have the same Research space name.</p> <p>MFT Arrivals* will have the usernames of the sender as the folder name.</p> <p>*Data that a user sends into the IDHS system will be under their own username within the MFT Arrivals</p>

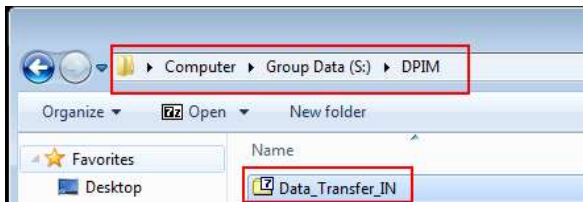
7.5.2 Research Shared Folder usage

7.5.2.1 When receiving data

Transfer data from the “**Username**” of the sender within **MFT Arrivals**:



To the same **research space** within **Group Data**



For the purpose of this document, the sender of data is **sfaabva**

Data should be transferred from **MFT arrivals** to the relevant **Group Data** folder then decrypt the data to complete the process.

MFT arrivals should NOT be used for storing data.

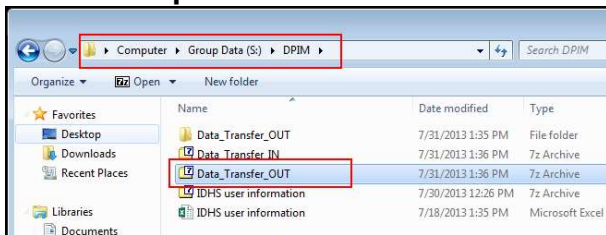
MFT arrivals folder should have encrypted documents sent in. Once you move the data to Group Data folder Decrypt the data. The password for decryption should be provided to you by the sender of the data

As a guide please view the IDHS encryption document
On how to decrypt the data.

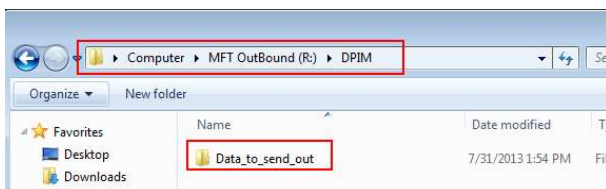
<https://www.ucl.ac.uk/isd/itforslms/services/handling-sens-data/tech-soln/IDHS-Service-Quick-Links>

7.5.3 When sending Data out

Transfer data from the **Research space** within **Group Data**:



To the same **research space** within **MFT Outbound**



For the purpose of this document, Research space name is “DPIM”

Data should be transferred from **MFT outbound** to the relevant **Research Group Name** folder.

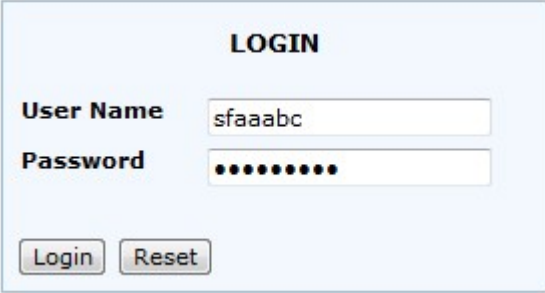



MFT Outbound should NOT be used for storing data.


MFT Outbound folder should have encrypted documents ready to send out. Once you move the data to MFT Outbound folder, follow [section 8 “Send Data out” of this document](#)

8 Secure Data out


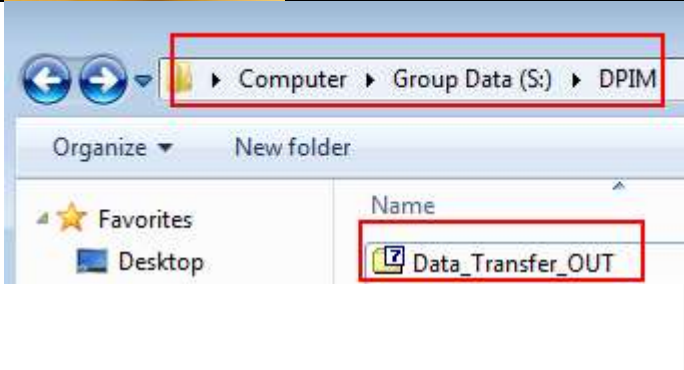
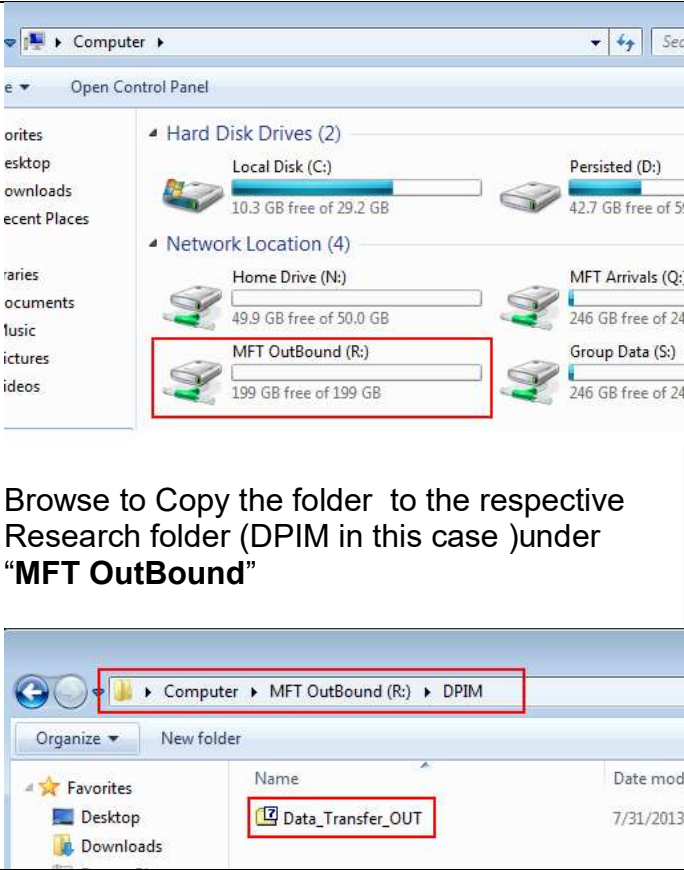

Before using this section, ensure that you have copied the data you want to send out to the folder for your relevant research group name under **MFT Outbound using the Data and applications portal** <https://accessgateway.idhs.ucl.ac.uk>

8.1 Via File Transfer

<p>https://filetransfer.idhs.ucl.ac.uk</p>	<p>File Transfer Portal</p>
	<p>Login to the File Transfer portal</p>
	<p>Click on secure mail</p>
	<p>Click on new message</p>
	<p>Fill in the To field, subject and message</p>

<p>Options</p> <p><input checked="" type="checkbox"/> Password Protect Package</p> <p><input checked="" type="checkbox"/> Expire Package Expire after <input type="text" value="5"/> days</p> <p><input checked="" type="checkbox"/> Limit Downloads Limit each file to <input type="text" value="1"/> downloads per recipient</p> <p><input type="checkbox"/> Send Me A Copy</p> <p><input type="checkbox"/> Read Receipt</p>	<p>Under options, note a password for the secure email is ticked. This password will be auto generated and Encrypts the data</p> <p>When you send the package this password will be displayed to you</p> <p>Enter days of expiry</p> <p>Enter download limits</p>						
<p>Attachments</p> <p>Attach a file stored locally on my computer</p> <p>Attach a file from my workspace</p>	<p>Attach file or files you want to send out.</p> <p>Click on Attach a file from my workspace</p>						
<p>Location <input type="text" value="/MFT OutBound/DPIIM"/></p> <table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>File Name</th> <th>Da</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>Data_Transfer_OUT.7z</td> <td>31/</td> </tr> </tbody> </table>	<input type="checkbox"/>	File Name	Da	<input checked="" type="checkbox"/>	Data_Transfer_OUT.7z	31/	<p>Browse to Location (Research Group Folder) under the MFT Outbound folder</p> <p>Select the file to send</p> <p>Click attach file</p>
<input type="checkbox"/>	File Name	Da					
<input checked="" type="checkbox"/>	Data_Transfer_OUT.7z	31/					
<p>Messages</p> <p>File '/MFT OutBound/DPIIM/Data_Transfer_OUT.7z' was attached successfully</p>	<p>View successful attached message and click on close</p>						
 <p>UCL Identifiable Data Transfer</p> <p>Secure Mail File Manager My</p> <p>+ New Message Drafts Outbox</p> <p>SECURE MAIL</p> <ul style="list-style-type: none"> • Password was set to: s5n453xtvq • Package is being sent 	<p>Click on send.</p> <p>Note the password “auto generated” by system</p> <p>This password will be required by end user to download the package</p>						
	<p>Notify user the password to download package.</p> <p>NB: In the case that you want to cancel a transfer, the Data Safe Haven support team can remove the file before it is downloaded. Contact your usual support channels for help.</p>						

8.2 Via FTP

	<p>Encrypt the folder first. Using the “Desktop” version of IDHS</p>
	<p>Locate the files to be transferred from the “Group Data” Drive and respective research folder.</p> <p>In this case from research folder “DPIM”</p> <p>Folder to transfer is the encrypted folder as “Data_Transfer_OUT”</p>
 <p>Browse to Copy the folder to the respective Research folder (DPIM in this case)under “MFT OutBound”</p>	<p>Copy the folder to send out to location as shown</p>
	<p>Ask user to make an FTP connection and download the files from the MFT Outbound Folder.</p>
	<p>Provide the receiver the password to decrypt.</p>

9 Secure Printing from IDHS

9.1 Pre-requisites

- Completed physical risk assessment and part of an audit programme. If studies have a current successful IG Toolkit submission (via the UCL Information Governance Advisory service) then the Information Asset Owner (usually the PI) can apply for secure printing service

Note: if studies have NOT completed a physical risk assessment and not part of an Information Governance Audit programme, then the Information Asset Owner should request a physical risk assessment by emailing slms.pid@ucl.ac.uk

9.2 Applying for Print Service

- Complete the form as <http://www.ucl.ac.uk/isd/itforslms/services/handling-sens-data/tech-soln/docs/using-IDHS/application-forms/IDHS-New-Service-Request-Form>.
 - Service name – state as “Secure Print Service”
 - Project Name – Your study name (same name as the share already on IDHS)
 - Notes / Further info: Printer Make, Model and IP address
 - Add members to access the “Services”: Add users name, username and service that they require access to
 - Where it asks for the Information Asset Owners signature, this is the data owners signature (usually the PI)
 - Send a completed and signed form as below to your usual IDHS route channels. If not sure visit <http://www.ucl.ac.uk/isd/itforslms/about/contact>

9.3 Printing

Once secure printing has been set up, log on to the “Data Safe Heaven” (aka IDHS) <https://accessgateway.idhs.ucl.ac.uk> and open your document that you would like to print.


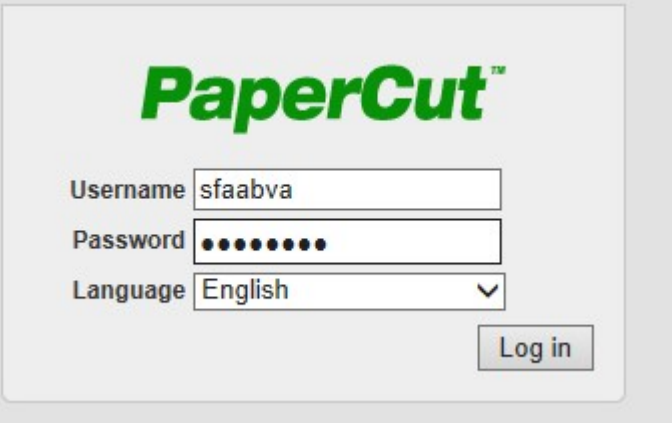
Printing is a two stage process as below:

9.3.1 Print from application

Print the document to the preferred printer. If you have rights to print to more than one printer, ensure you are selecting the printer that you want to print to.



9.3.2 Release print jobs

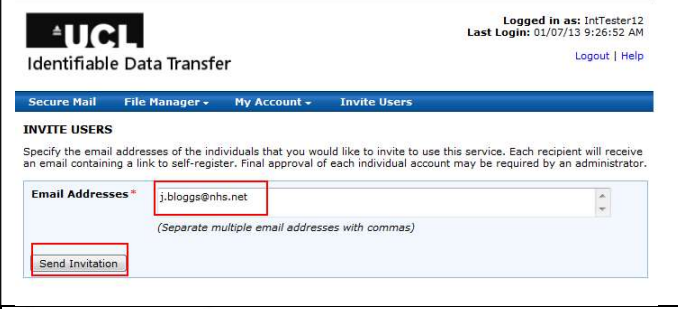
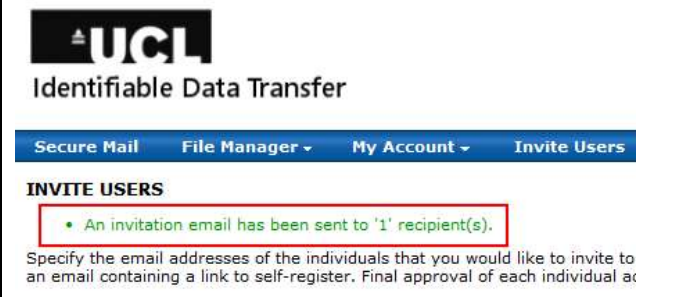
This feature has been added as a queue management allowing users to queue up jobs till they are ready to release them and collect them.

 <p>Secure Printing</p>	<p>Launch "Secure Printing" Application Either as an "app" or within "Secure Desktop"</p>																
 <p>PaperCut™</p> <p>Username <input type="text" value="sfaabva"/></p> <p>Password <input type="password" value="••••••••"/></p> <p>Language <input type="text" value="English"/> ▼</p> <p><input type="button" value="Log in"/></p>	<p>Login using your UCL IDHS credentials</p>																
<p>Jobs Pending Release</p> <p>Jobs awaiting approval prior to printing are listed below:</p> <p><input type="button" value="Release All"/> <input type="button" value="Cancel All"/> <input type="button" value="Refresh Now"/> <input checked="" type="checkbox"/> Auto refresh (Refresh in: 52)</p> <table border="1"> <thead> <tr> <th></th> <th>Submit Time ▼</th> <th>Printer</th> <th>Document</th> <th>Client</th> <th>Pages</th> <th>Cost</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>🕒</td> <td>Sep 25, 2014 10:47:27 AM</td> <td>slmsidhsprint01 SABRE_V3</td> <td>Microsoft Word - Document1</td> <td>IDHSXAWA002</td> <td>1</td> <td>0.00</td> <td><input type="button" value="[print]"/> <input type="button" value="[cancel]"/></td> </tr> </tbody> </table>		Submit Time ▼	Printer	Document	Client	Pages	Cost	Action	🕒	Sep 25, 2014 10:47:27 AM	slmsidhsprint01 SABRE_V3	Microsoft Word - Document1	IDHSXAWA002	1	0.00	<input type="button" value="[print]"/> <input type="button" value="[cancel]"/>	<p>Release Print job to printer</p>
	Submit Time ▼	Printer	Document	Client	Pages	Cost	Action										
🕒	Sep 25, 2014 10:47:27 AM	slmsidhsprint01 SABRE_V3	Microsoft Word - Document1	IDHSXAWA002	1	0.00	<input type="button" value="[print]"/> <input type="button" value="[cancel]"/>										

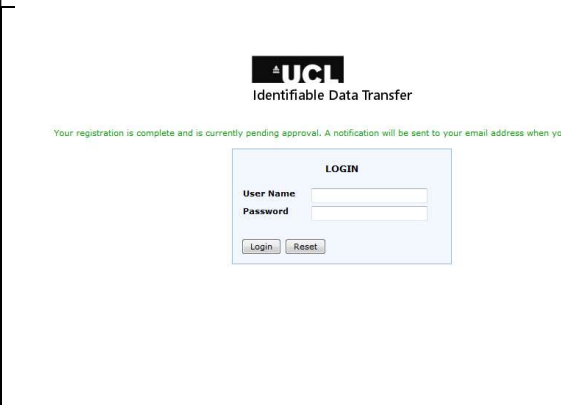
10 Registering an external user

10.1 Step 1: Send invite by UCL IDHS Research space owner

<p>https://filetransfer.idhs.ucl.ac.uk</p>	<p>Browse to the filetransfer portal</p>
 <p>LOGIN</p> <p>Environment UCL IDHS</p> <p>User Name <input type="text"/></p> <p>Password <input type="password"/></p> <p><input type="button" value="Login"/> <input type="button" value="Reset"/></p>	<p>Login using your UCL IDHS credentials</p>
 <p>UCL Identifiable Data Transfer</p> <p>Secure Mail File Manager ▼ My Account ▼ Invite Users</p>	<p>Click on Invite Users from the menu</p> <p>Note: This will only show on the menu if you have specific permissions to invite users</p>

	<p>Type the email address of external collaborator to send and invite to.</p> <p>Click on Send invitation</p>
	<p>Confirmation message that the invite has been sent</p>

10.2 Step 2: Register by External collaborator

<p>Invitation Request</p> <p>You have been invited to join UCL IDHS File Transfer. Please click the link below to continue with the registration.</p> <p>Click here to register</p> <p>If the link above does not open, copy and paste the following URL into your browser: https://filetransfer.idhs.ucl.ac.uk/register?token=13905b89-3b27-4dcf-8685-7b69867c5e86&invited=true</p> <p>This link will expire after 24 hours. Please contact your account representative if you have any trouble registering.</p>	<p>The external collaborator now registers by clicking on the email they receive.</p> <p>Note: This link expires after 24 hours</p>
<p>Please enter the information below and click Submit.</p> <p>Login Credentials</p> <p>User Name * <input type="text" value="exttester13"/></p> <p>Password * <input type="password" value="....."/></p> <p>Confirm Password * <input type="password" value="....."/></p> <p>Contact Information</p> <p>Email Address <input type="text" value="b.varsani@ucl.ac.uk"/></p> <p>First Name <input type="text" value="Bhavesh"/></p> <p>Last Name <input type="text" value="Varsani ExtTester13"/></p> <p>Organization <input type="text"/></p> <p>Phone <input type="text"/></p> <p><input type="button" value="Submit"/> <input type="button" value="Cancel"/></p>	<p>External user will register with fields as shown.</p> <p>Click on Submit</p>
	<p>External users can now automatically log in.</p> <p>Please provide them with the “Welcome Pack for Data Transfer IN”</p> <p>Available at: https://www.ucl.ac.uk/isd/itforslms/services/handling-sens-data/tech-soln/welcome-packs</p>

End of Document