Guidelines for off-campus workstation settings to enable access to Unisa Library's electronic resources

Disclaimer

The following RECOMMENDATIONS arise from commonly-reported problems or frequently asked questions (FAQs) from students using the Unisa Library systems and information resources.

It is important to note that each individual client's situation, hardware, software and configuration is unique and that no guarantee is made or implied in this troubleshooting guide.

The University of South Africa and Unisa Library accept no responsibility for actions arising from the use of this guide.

Last updated: October 2014

Contents

1. Introduction

Unisa Library subscribes to many valuable information resources and research databases. Before attempting to access the information resources or databases and the Library Catalogue, off-campus clients need to have certain hardware, software and settings in place.

Clients need to:

- Have the recommended hardware, software and Internet connections
- Download the required free software, such as Adobe Reader, and other software
- Possibly change some settings on their computers
- Register on MyUnisa, claim their MyLife email address and activate their password

These requirements and related aspects will be dealt with below. The solutions we **recommend** might involve changing some of the security settings on clients' PCs. Please note that the configuration of individual PCs and / or Internet browsers may affect their ability to transfer and display information correctly.

It is entirely up to clients whether they keep these changes in place after they have completed searching our information resources.

2. Steps taken by Unisa Library to ensure security

Unisa Library would like to assure clients that our technology, connectivity, security and authentication systems are all working optimally. We are committed to client privacy and we ensure this commitment in a number of ways:

a) Https secured pages on the Library Catalogue

The Library site and your access to e-resources is protected by **VeriSign SSL digital certificates.**
Using Secured Sockets Layer (SSL) technology, the personal information of clients is encrypted as it is passed to and from us. Clients will need to click **YES** on the Security Information box whenever this information box appears. The 'http**s**' in the URL of the My Library / Renewals / Login pages means that the pages and any personal information is protected.

b) The use of cookies

The Library web site requires that cookies be enabled on clients' PCs. The site is divided into public and private (secure) pages. Public pages are solely informational resources and clients will not be asked to provide any personal data to access these pages. Cookies (devices that are used to track client information) are used on public pages in order to enable client sessions. For example, *a cookie might track which database is visited and then store the database home page as a cookie for quick retrieval*. No sensitive information is tracked by these cookies and these cookies expire very soon after clients leave the site.

c) The use of personal information

The Library does not provide client information to any third party. All information provided on our secure, private pages is used for internal purposes only, mainly to gather usage statistics.

Pages on which clients are asked for personal information are completely secured by our use of SSL, or Secure Sockets Layer. SSL encrypts any data clients provide and the data is thus made inaccessible to anyone who is not authorized to view the information.

3. Recommended hardware and software and Internet connections

Internet Explorer (IE) is the standard browser of Unisa. Most Library databases are designed to be viewed on Internet Explorer and they may lose functionality when other browsers are used. Most of

the explanations below apply to Internet Explorer 9 and later versions.

a) Hardware (minimum standards – any improvement on these standards should be considered)

- Computer with a Pentium 4 processor, running at 2 GHz, 512 MB RAM (1028 – 2086 MB is recommended)
- Laser or ink-jet printer

b) Modem

We strongly recommend an ADSL line. A 56 KB modem may be used but the response times and downloads will be extremely slow with possible time-outs. This may be costly in the long run. We recommend 192 KB minimum.

c) Local Internet Service Provider

Clients need sufficient email capacity to ensure that emailed articles are not rejected by the service provider. 1 GB cap is the minimum requirement and this should be adequate for study and research purposes. It offers spare capacity for other non-study related activities.

d) Software

- **Microsoft Internet Explorer 9** or higher (Internet Explorer 9+ recommended) - Free download available at http://www.microsoft.com/

OR

- Other browsers like **Mozilla Firefox 31 & 32, Google Chrome 36 & 37, Opera 9.8 or Safari 7.0+** (for Macintosh users)
- **Adobe Reader** may be downloaded free of charge and is used to view and / or download the full-text PDF articles.
- **Adobe Flash Player** may be downloaded free of charge to enable computers to show multimedia files.

Equipment that does not meet these requirements may not produce the desired results and will frustrate efforts to access the information resources needed.

If Clients are unable to access the electronic services available, they are welcome to send the request for assistance via Ask a Short Question. If clients are unable to download full-text documents, they are welcome to request printed copies by completing a book request or a journal article request online form.

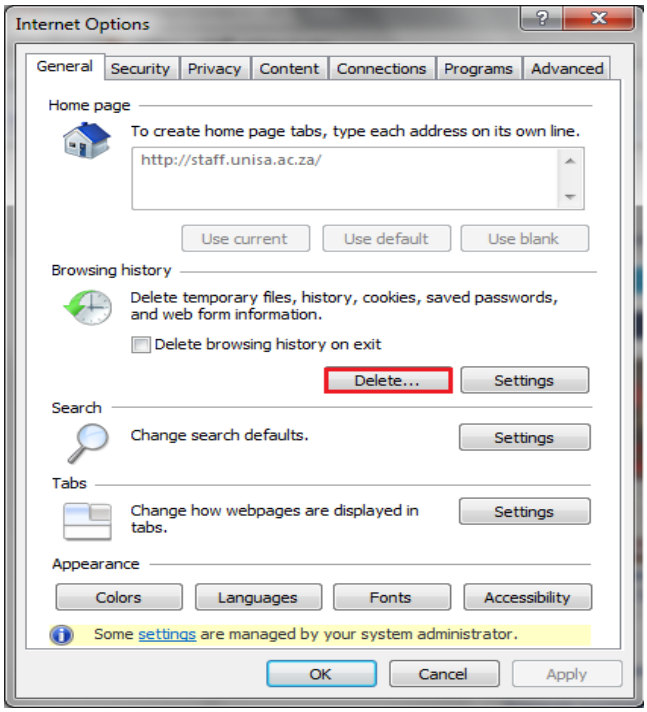
4. Recommended browser settings for Internet Explorer 9.0

The following explanation refers to IE version 9.0 and might look slightly different depending on the client's version of IE.

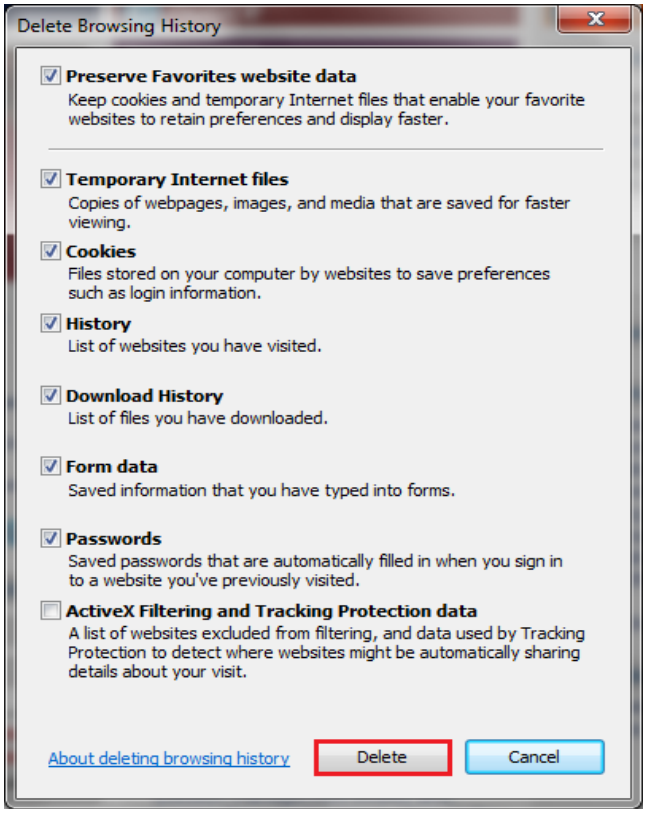
To check the settings or to make changes, go to "Tools"  on the menu bar and select "Internet Options". The Internet Options screen has 7 'tabs'. Click on each of the tabs mentioned below and make the recommended changes to the settings in order to have the correct set-up for your browser:

a) General Tab

The 'Temporary Internet Files', 'Cookies' (or) 'Cache', and 'History' files should be cleared regularly by clicking on the "Delete" button under the "Browsing History" heading.



After clicking on the "Delete" button, the "Delete Browsing History" window will appear. Select or check the "Temporary Internet Files", "Cookies", "History", "Download History", "Form Data", and "Passwords" check boxes and then click on the "Delete" button and follow the instruction to delete your history of previously visited web sites.

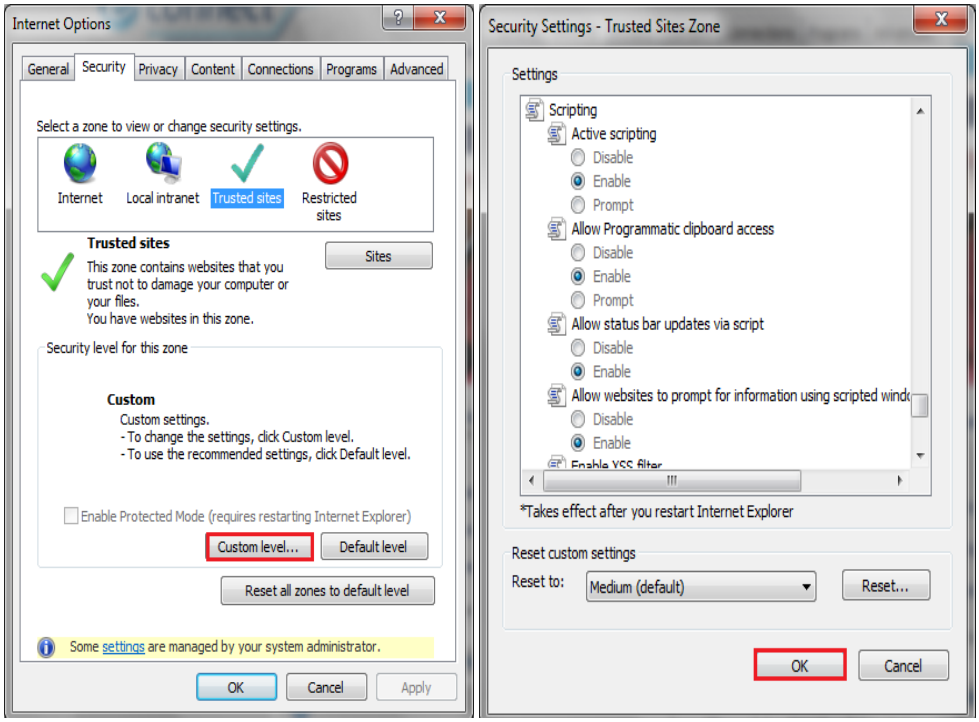


b) Security Tab

JavaScript must be enabled on the Internet browser because the Library Catalogue system uses it to dynamically create a client's lists of requests, exports and loaned items, and to view electronic resources.

Click on the '**Security' tab,** then Click on the "Custom level…" button, scroll down to

"Scripting" and make sure that the "Enable" radio button is selected for **ALL** entries in that category and then click on the 'OK' button.

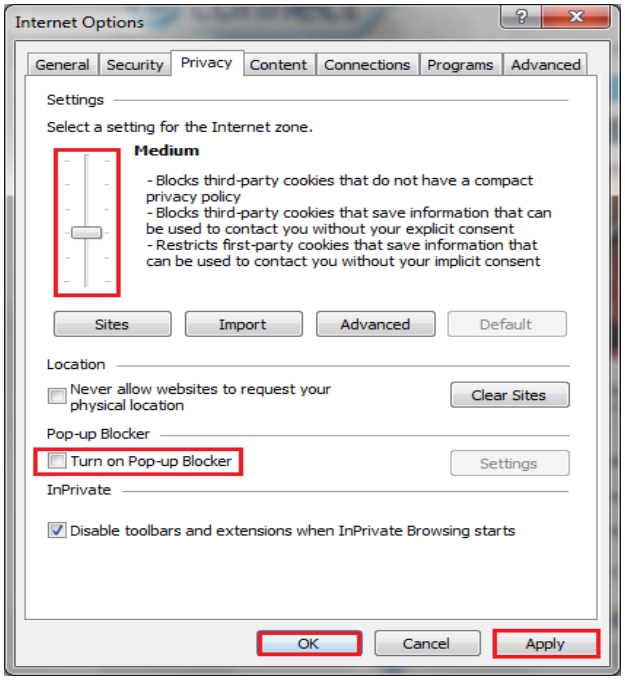


c) Privacy Tab

Several Library databases use pop-up windows as an integral part of their operation. The Library Catalogue maintains clients' login sessions by using a temporary browser-based cookie file. Clients' computers must therefore be able to accept these cookies. The Pop-Up Blocker should also be disabled.

To enable cookies:

Click on the **"Privacy" tab,** then move the slide to the **MEDIUM** setting and **de-select** the radio button "Turn on Pop-up Blocker" at the bottom of the screen under pop-up blocker, and then click on the "Apply' then "OK" buttons respectively.



If clients retrieve an empty screen when trying to access a database, or if they receive a "Validation Expired" message, it could be due to the **cookies** setting being too high. A known problem is that **large PDF files** in the Library Course Material collection (also known as e-reserves) do not open if the cookies' setting is set on **Medium**.

If clients are unable to download a PDF file from the e-reserves they could try changing the **cookies** setting to **Low** until they have downloaded the article(s) required.

Cookies settings for browsers other than Internet Explorer

Mozilla Firefox 32.0.3

a) Go to the top **menu bar**

b) Click on "Open Menu" 

c) Click on "Options"

- Click on the "Privacy" icon
  - then under the "History" option click on the "Firefox will:" dropdown menu and select "Use custom settings for history" option
  - select the 'Accept cookies from sites:' option
  - click on the "Accept third-party cookies:" dropdown menu and select the "Always" option
  - click on the "Keep until:" dropdown menu and select "they expire" option
- Click on the "OK" button

Google Chrome 37

a) Go to the top menu bar

b) Click on 'Customize and Control Google Chrome' 

c) Click on 'Settings'

d) Click on 'Show advanced settings…' at the bottom

e) Under the 'Privacy' option, click on the 'Content settings…' button

f) Under the "Cookies" option, click on the "Allow local data to be set (recommended)" option

g) Click on the "Done" button

Opera 25.0

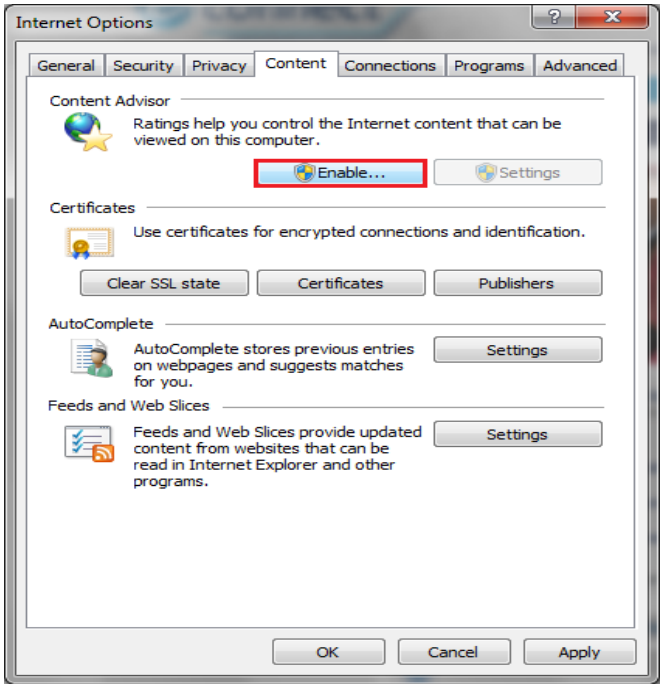
a) Go to the “Opera” button at the top left of the screen
b) Click on “Settings”
c) Click on “Privacy & Security”
d) Under the “Cookies” option, click on the “Allow local data to be set (recommended)” option

Safari 3.0.4

a) Go to the top right of the menu bar
b) Click on the dropdown arrow next to the tools button
c) Click on “Preferences…”
d) Click on “Privacy” tab
e) Under the “Block cookies:” option select “Never”

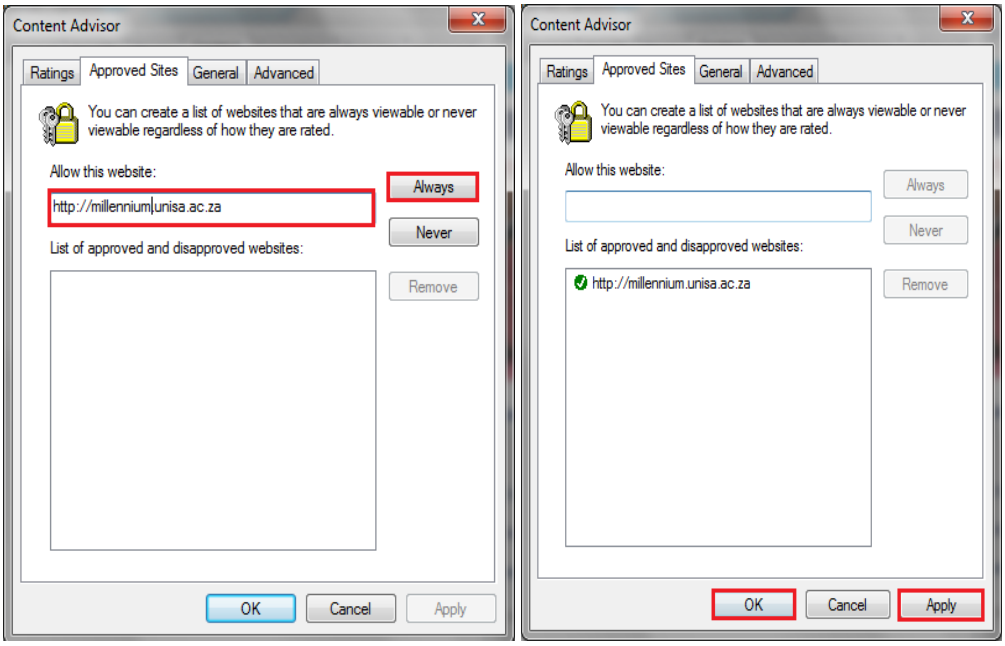
d) Content Tab

“Content Advisor” is one of the main causes of **login and record display problems**. We recommend that clients disable “Content Advisor” completely



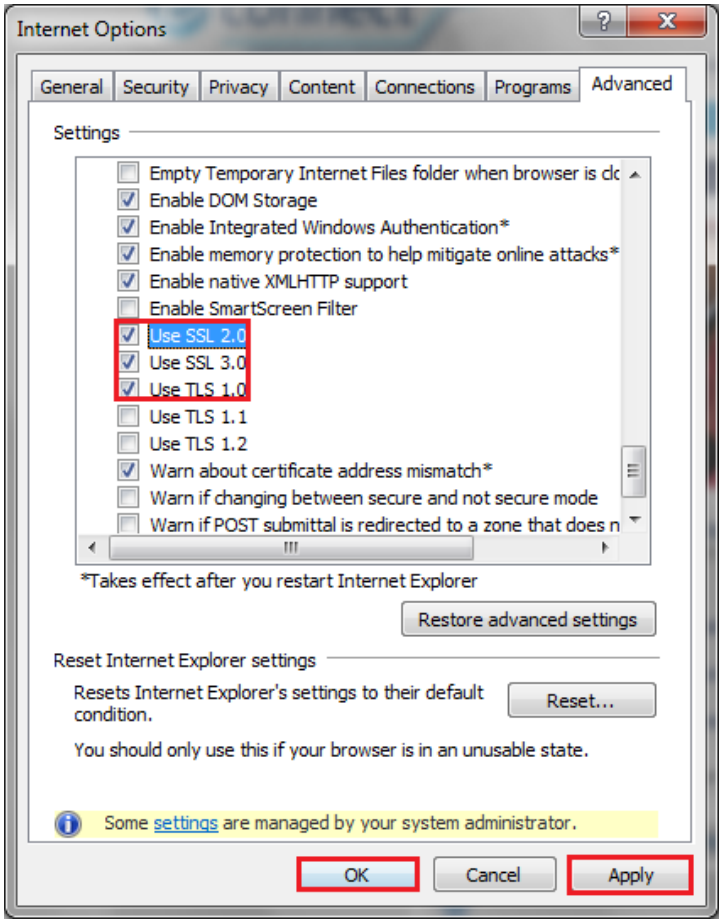
OR

Click the “Enable” button, and then click on the “Approved Sites” tab. Type “http://millennium.unisa.ac.za” and “http://oasis.unisa.ac.za” in the “text field”, and then click on the “Always” button. Click on “Apply” and then "OK" to save the changes.



e) Advanced Tab

SSL and **TLS** are security features that have been added to the Library Catalogue to safeguard clients' personal details. **SSL 2.0, SSL 3.0** and **TLS 1.0** should all be **enabled**.



5. Authentication of off-campus clients

Online access to most of the library's information resources is restricted by vendor license agreements to connections within the Unisa Network. To gain access to the Unisa Network, clients need to be **authenticated** as registered students or staff members of the University of South Africa.

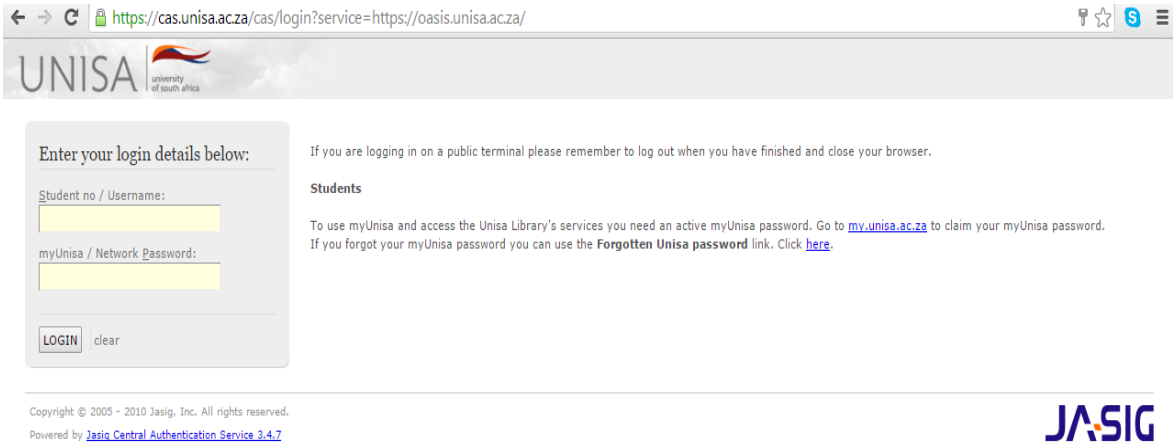
This login procedure uses a **JASIG Central Authentication Service (CAS) single sign-on** for students and staff.

Students:

Students need to use their **Student Number** and **myUnisa password**. If you do not have a myUnisa password, please go through this tutorial:
https://my.unisa.ac.za/cmsys/myUnisa/myLifeJoinActivate.html

Follow all the steps outlined in the tutorial and please make sure that you **activate** the password that was sent to your myLife email. **Please note that if the link is NOT activated within 24 HOURS the password will automatically be cancelled and you will have to request another password**.

You will then use your student number and myUnisa password for accessing the online library databases and services that require authentication. Once you have authenticated via the JASIG CAS system, there will be no need to log in again in the current session.



Error message: If you get a "Your credentials are Invalid" or similar error message, please contact the MyUnisa Support Centre at email: myUnisaHelp@unisa.ac.za and include the error message you received.

PLEASE NOTE: Do not confuse the **Library Catalogue PIN** with the myUnisa **Username and Password**; they are two separate entities.

The Library Catalogue PIN is created on the Library system once and will remain the same (unless a client chooses to change it or unless it is forgotten) for the duration of the studies with Unisa. Clients are encouraged to use their MyUnisa / Unisa passwords as their Catalogue PINs because they then need remember only the one PIN / password.

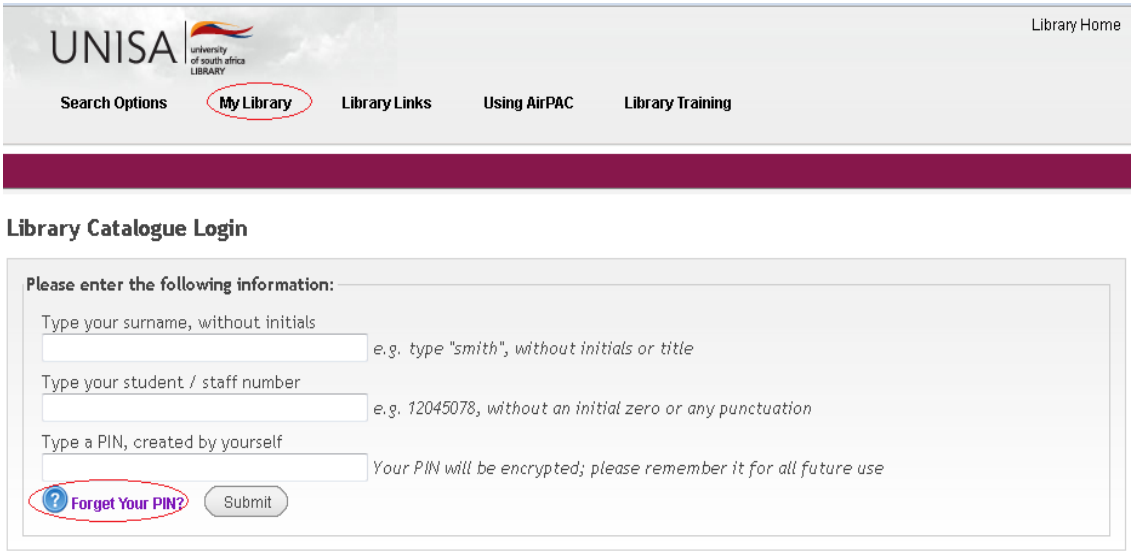
Staff:

Staff will use their **Campus Network username as login** and their **network password** - the same network username and network password they use every morning to log into the campus network.

Library Catalogue Login authentication

The Login to the Library Catalogue authentication screen appears when the "My Library / Renewals / Login" link in the **My Library** drop-down menu is clicked. If the client has already registered a PIN on the Library Catalogue, access is gained by entering the surname, student / staff number and the PIN that was created.

If the Library system rejects the PIN, or displays an 'Information supplied is Invalid' error, click on the "Forgotten your PIN?" button.



A **PIN Request form** will be offered. Fill in the required details and click the "Submit" button. An email message will be sent to the myUnisa email address or to the email address in the client record on the Library system. The client must respond to this email message to be able to create a new PIN.

If this is the first attempt to create a PIN on the Library Catalogue, please read these instructions and click "My Library / Renewals / Login" on the Library Catalogue (http://oasis.unisa.ac.za) to create and register the PIN first before attempting to access the Library's information resources.

6. Other factors that might affect access to information resources

a) The client's **own service provider** might not provide enough bandwidth (rate of data transfer), resulting in time-outs

b) The client's **workplace** computer or network may block access:

- The **security settings** on the workplace's firewall might create difficulties. Examples of errors resulting from a firewall problem may include:

  "The address you are trying to access is invalid"

  "You are not authorized to view this page"

  "This page cannot be displayed"
- The **workplace** might be using an older version of Internet Explorer or a different browser.
- The workplace's IT Department might have blocked **large files** (between 2.5 and 10 MB or more) or PDF attachments of full text articles that clients try to download.
- The workplace does not want **non work-related Internet traffic** on their network and places a low priority on it.
- The **settings** on the workstation may need to be changed as employers enable or disable various settings on employees' workstations. The privacy settings, for example, might not be set up to accept cookies.
- A personal laptop connected to an employer's LAN may be firewalled and access to the library systems could be blocked. Clients could try to disconnect from the LAN and use a high speed data connection.

Clients will need to discuss the following points with their employer's IT Department:

Find out what the **employer's policy** is on **internet usage** for non-work-related business, such as studies, personal use, and others, as well as check if the following URLs are permitted:

- http://oasis.unisa.ac.za/
- http://www.unisa.ac.za/

- https://oasis.unisa.ac.za/
- http://millennium.unisa.ac.za/
- https://millennium.unisa.ac.za/

Clients must also check whether the employer's IT Department has a list of sites that are **blocked**.

c) Unisa

- **Unisa's bandwidth** is heavily used during registration periods and this may cause slow access and time-outs during this time. Occasionally the network might go down over weekends while the ICT Department are busy with maintenance or other work
- **Unisa's Internet providers** TENET and Neotel can also be slow occasionally
- **Database vendors' downtimes** might also prevent access. Clients should consult the library's homepage for notices regarding the scheduled downtimes of any of the databases.

d) Anti-virus programs

Clients with home security protection software programs should make sure that their browser of choice is "white-listed" or "allowed" by their firewall. Check the settings of the anti-virus program and other cookie-blocking software installed on the computer as most of these programs are set to block cookies. If necessary, clients will then need to change the settings to allow cookies

e) Internet Cafés

Internet Cafes are not recommended for accessing databases and links to articles or downloading articles because students report slow response and download times with frequent time-outs and this adds to the expense of their sessions.

7. Reporting a problem

Before reporting a problem, **please ensure that you have access to the minimum system requirements** and that the recommended **settings are in place on your workstation**.

Common errors and problems that need to be reported:

- If you are prompted for a further database User ID and Password over and above your Login
- If you receive the following error message: '**BAD GATEWAY'** or **502** Error
- If you receive an "**Authentication failed**" type of error message

If your access problems persist after the settings of your computer have been changed and you have eliminated the other factors mentioned above, **please send an email to the Library and include the following information:**

- Your Name
- Student number / staff number
- Phone Number
- Whether you are working from your home or work computer
- If you are working from home, describe what **kind of access** you have (phone modem, DSL, etc.)
- Indicate the name(s) of the database(s) or functions on the Library Catalogue that you could not access
- Include any other details that could be helpful, for example, the wording of the error messages

Addresses for reporting problems:

- **Library Webpage problems** to lib-help@unisa.ac.za,
- **Library Catalogue problems** to lib-help@unisa.ac.za
- **Subject database and e-resource access problems** to bib-dbase@unisa.ac.za

Thank you.