Expectations

Our Single Sign-On implementation, "MyST SSO", provides easy access to many web sites for a significant period of time after a single login.

All Day SSO

"All Day SSO" for web sites should be expected under the following conditions:

1. You use 1 web browser and don't close it
2. You don't log out of SSO
3. Your computer doesn't change its IP address
4. You consider 9-12 hours "all day"

If you try to access an SSO protected website outside of these conditions, you will be prompted to login to establish a new SSO session.

Browsers and sessions

MyST SSO is effective for web sites accessed through a normal modern web browser (Firefox, Chrome, Safari, etc.). It uses features of modern browsers to establish login sessions with multiple diverse websites.

MyST SSO is not affected by your system login nor does it affect SSH, Remote Desktop, or other services that have not been integrated with it.

Due to the nature of how web browsers store and use sessions, sessions created in one browser are irrelevant to other browsers. However, sessions are shared between tabs and windows of the same browser.

Therefore:

- The *Single* aspect of SSO is naturally limited to a single web browser
- Separate web browsers can have independent SSO sessions
- Completely closing a web browser, including all tabs and windows, will end any SSO sessions associated with that browser
- Closing some, but not all, tabs/windows of a browser will not end your SSO session in that browser

Stable client IP address

A security feature of MyST SSO sessions is the requirement to have a stable client IP address.   This protects SSO sessions created on one system from being stolen and used on another.

As a result, when a computer system has its IP address changed, any SSO sessions established on that computer will be invalidated. Additional use of SSO protected web sites will require a new SSO session to be created.

Specifically, a computer's IP address *may change* after any of the following events:

- Changing from a wired connection to WiFi, or vice-versa
- Changing WiFi networks (eg. Internal, Guest, EduRoam)
- Moving from one building to another, including between Muller and The Rotunda
- Connecting to or disconnecting from the VPN
- Waking up from sleep mode or hibernation mode

Timeout

MyST SSO is configured to have sessions that last 9 hours from the last contact with the SSO server, up to a maximum of 12 hours since the initial login. This is a security feature.

Logout

Logging out from an SSO enabled web site will commonly end your main SSO session. If you don't wish to end your SSO session, simply close the browser tab of any website you are done with.

To manually end your SSO session, see: Logout.

Summary

MyST SSO:

1. only works with web sites that are enabled for SSO
2. is only effective within a single web browser
3. is not affected by your system login
4. ends when you close a browser
5. ends when you logout
6. ends when your computer changes its IP address
7. ends after 9-12 hours