Co-development Technologies

Shared Development Environments

- Atom
- Visual Studio Code (See Helpful Hints below)
- Screen share in one of the communication tools

Helpful Hints on How to use Visual Studio

Thanks to Chris Colvard for creating these hints for the 2019 Dev Congress.

- Install Visual Studio Code. It is free and has Win/Mac/Linux versions.
- Next install the Live Share Extension Pack. This includes the Live Share plugin and the Live Share Audio and Chat plugins.
- Once these are installed, read the quickstart for joining a live share.
- If you want, read the longer documentation about all you can share (editors, shells, servers, etc.) during the live share.
- During the Dev Congress, one person can create the live share, send the live share link on slack, and then others will join. The host doesn't need to be the person leading the swarm but should already have a checkout of the code and the test suite passing locally. The host should have a stable network connection to avoid others being kicked off the live share session. Also note that regardless of who makes code changes they will appear in any commits as the host of the live share so the host should always use `co-authored-by` in the commit messages to credit all who worked on the commit.

Communication

Institutions generally have communication channels that are available for use by developers for collaboration. Some of the common communication tools are listed in alphabetical order. As groups form, one of the members in the group can host from the platform they have available.

Video chat...

- BlueJeans
- Google Meet
- Webex
- Zoom (See Dealing with Zoom bombing below)

Text chat...

- Slack - recommended as this is the platform used by the Samvera community
  - developer-congress channel - used for general discussions of interest for the whole group
  - direct messages - used for sub-groups as they form

Dealing with Zoom bombing

Prevention

These prevention methods are listed from lowest barrier entry to the tightest security.

- Use a password when setting up zoom meeting. This is a very low barrier as you can provide the zoom link with the password and probably sufficient.
- If your group is small, you can use a waiting room and let people in as they join. This is effective at preventing unwanted zoom attendees, but it is easy to miss that someone is in the waiting room.
• Tightest security is to require users to log in to Zoom before joining the room, but this can be time consuming especially if anyone in the group doesn't already have a login. Combined with a waiting room, this is unlikely to experience issues.

Response to Unwanted Attendees

In the unlikely event that your development team is Zoom-bombed or interfered with in any way, the recommendation is to...

• immediately end the Zoom call
• post a new Zoom link in Slack channel: developer-congress

Recommendation

Use lowest barrier entry. If we experience problems, increase prevention efforts.