GitLab for SMPH FAQ

The DoIT GitLab instance (https://git.doit.wisc.edu/) is available to SMPH groups to host your codebase, track issues, collaborate on code, and continuously build, test, and deploy your app with built-in GitLab CI/CD. For a general overview of the service from an SMPH perspective, see the GitLab service page for SMPH.

- What are the benefits of using git.doit.wisc.edu?
- What features are available?
- What are some best practices and guidelines for SMPH users of GitLab?
- What can I store in GitLab?
- What is the difference between the "SMPH" and "SMPH (Public)" top level groups?
- Who can request new groups and projects?
- How do I request a new group?
- How do I get added to a group or manage group membership?
- How do I request a new project?
- How do I create a group or project?
- What permissions or role should I grant someone when I add them to my group or project?
- Can I restrict someone from inheriting a more powerful role?
- Can GitLab be used for research?
- Can external people collaborate? What about UWH employees?
- How do I migrate my project to GitLab?
- How do I know if DoIT GitLab is a good fit for my needs?
- How can I get more help on using GitLab?
- Other resources
- Related articles

What are the benefits of using git.doit.wisc.edu?

Using git.doit.wisc.edu frees you from licensing, installing, and maintaining your own instance of Git. This instance features the Ultimate tier features of GitLab. SMPH department IT Directors can request delegated administration of groups and projects for their department.

What features are available?

This instance is licensed at the Ultimate tier. See https://about.gitlab.com/features/.

Note that Service Desk for GitLab projects is now available. It is turned on by default. This allows others to create confidential issues in your project without an account by posting to a special email list. You can disable this feature by going to Settings General Service Desk.

What are some best practices and guidelines for SMPH users of GitLab?

Upon request, departments will have a group created for them by Application Support in SMPH. If there are multiple teams/groups/centers in the department, the IT directors may want to create a subgroup for them.

Groups and projects under the SMPH top level group should always require authentication. Groups and projects under SMPH (Public) top level group are intended to be publicly accessible without authentication.

Projects should not exceed 2 GB in size and cannot be used to store restricted data, sensitive data, PHI or any other class of data that's not for general consumption.

Projects should follow the SMPH GitLab – Public, Internal, Sensitive, and Restricted Data Guidelines.

What can I store in GitLab?

GitLab is primarily used as a code repository. It should not be used for data storage. The DoIT GitLab Projects document has important information on restrictions and appropriate use. In particular, projects should not exceed 2 GB in size and cannot be used to store restricted data, sensitive data, PHI or any other class of data that's not for general consumption.

Unpublished research and code or intellectual property that is not intended for the public may need extra care to ensure it is protected appropriately.

What is the difference between the "SMPH" and "SMPH (Public)" top level groups?

Groups and projects that need to be accessed by the public or anyone without authentication are located under the SMPH (Public) folder. Groups and projects that are internal and require authenticating with a UW-Madison NetID are located under the SMPH folder.

Who can request new groups and projects?

SMPH IT directors can request a group for their department. Employees within that department can request a subgroup for their team, center, initiative, or group that will be nested within the department group. Authorized team members will be able to create projects (i.e., repositories) within that subgroup.

How do I request a new group?

There are several ways you can request a GitLab group for your GitLab projects:

- Ask your IT director; they can be delegated to create GitLab groups for teams in their department;
- Email the SMPH Application Support team or submit a request through their Service Desk Ticket Portal;
- or ask the DoIT Shared Tools team.

How do I get added to a group or manage group membership?

If the group is not private, individuals can find the group and request membership. The designated owners of a group can invite, remove, and manage the members. **The person being added should FIRST log into https://git.doit.wisc.edu to provision their account before an attempt is made to add them to the group.** This is a requirement if the user is from uwhealth.org domain. You should then look up their account by NetID, not email. If no match is found for their NetID, it means they have not yet logged in to https://git.doit.wisc.edu.

Invite members

You're inviting members to the **State Animals** group.

GitLab member or email address

| bbadger |

No matches found   ses

Select a role

| Guest   ⌄ |

How do I request a new project?

If a team already has a subgroup, the owner or maintainer of that group can create a project for you. Otherwise check with your IT director, the SMPH Application Support team, the DoIT Shared Tools team. More information about GitLab projects is available at DoIT GitLab Projects.

How do I create a group or project?

Subgroup owners can create groups and projects. Members with the Developer role can create projects. See How to Create GitLab Groups and Projects for details on how.

What permissions or role should I grant someone when I add them to my group or project?

Key permissions for groups:

- Guests have limited visibility into groups.
- Developers can create projects in groups. (This can be restricted.)
- Owners can manage members and create/delete subgroups.

Key permissions for projects:

- Guests can view code and pages, and create comments and issues.
- Developers can view analytics, run CI/CD pipelines, move issues, create and approve merge requests, create/edit milestones and releases, create branches, push to unprotected branches.
- Maintainers can manage team members, edit web hooks and project settings, push to protected branches, manage push rules.
- Owners can rename, transfer, or delete projects.

More information about GitLab permissions can be found at https://git.doit.wisc.edu/help/user/permissions.

Note: Permissions can only be increased for sub-groups; you cannot further restrict a person's role. See below.

Can I restrict someone from inheriting a more powerful role?

No. GitLab only supports increasing permissions with sub-groups; you can't remove roles that they inherit from a parent group. See https://docs.gitlab.com/ee/user/group/subgroups/#override-ancestor-group-membership. You may notice that there are several members of your group that you don't recognize. These are members of SMPH IT that are responsible for security, administration, or management of the SMPH area of GitLab.

Can GitLab be used for research?

Researchers may use GitLab to manage the **source code** for projects but they **should not use it to store research data**, especially sensitive and restricted. It the work is in the public domain, it can be under the SMPH (Public). If the work is proprietary, private, or unpublished it can be under SMPH as long as it is viewable only to appropriate authenticated users and appropriate controls are in place. See SMPH GitLab – Public, Internal, Sensitive, and Restricted Data Guidelines, DoIT GitLab for Research, and DoIT GitLab Projects for more information.

In all cases, projects should not exceed 2 GB in size and cannot be used to store restricted data, sensitive data, PHI or any other class of data that's not for general consumption.

> ⚠️ A risk assessment is currently underway that will help determine what additional controls may need to be put in place for proprietary, private, or unpublished source code that is considered sensitive.

Can external people collaborate? What about UWH employees?

Yes, but they will need a NetID. The current recommendation is to invite vendors and external collaborators to a relevant Manifest group that allows external invites. If your department already has an appropriate group, you can invite them to that group. If your department does not, you can the SMPH Application Support team and ask them to invite the person to the SMPH External Collaborators group. Once the person accepts the invite, they are given an opportunity to create a NetID if they do not already have one. For more information, see Manifest - Using a Manifest Group to Invite People to Create Identities (NetIDs).

There is a special case for UW Health employees, who often have a UW NetID but do not have an @wisc.edu email address. They will need to be able to use MFA Duo also, in order to log into GitLab with their NetID. Once that's set up, just let the DoIT Shared Tools team know the user's NetID and they can add it to their list of NetIDs that are allowed access, even though they're not UW-Madison staff. They can then log in and create their account. After that, you can invite them to the project you want them to access with whatever permission level you choose.

How do I migrate my project to GitLab?

See DoIT GitLab Resources for Migrating to git.doit.wisc.edu. It may be best to engage the DoIT Shared Tools team for assistance with project migration.

How do I know if DoIT GitLab is a good fit for my needs?

Reach out to the DoIT Shared Tools team and they will contact you to perform a Git Needs & Requirements Analysis.

How can I get more help on using GitLab?

- The DoIT Shared Tools team manages the instance and can provide general support and advice.
- The SMPH Application Support team can provide limited assistance with group management.
- The DoIT Shared Tools team maintains a number of GitLab KB documents, including a list of other online resources.
- You can also post questions to the UW Dist Dev CoP (UW Distributed Developers Community of Practice) Tools channel in Teams.

Other resources

- DoIT GitLab instance
- GitLab service page for SMPH
- DoIT GitLab KB documents
- DoIT GitLab Projects
- DoIT GitLab for Research
- Other online resources
- UW Dist Dev CoP Tools channel in Teams

Related articles

- SMPH GitLab – Public, Internal, Sensitive, and Restricted Data Guidelines
- How to Create GitLab Groups and Projects
- GitLab for SMPH FAQ