Manitou Single Sign-on - Overview

Design Goal

The design goal of this project is to allow organizations to manage the users that are allowed to log in to Manitou from a third party Single Sign On (SSO), Open ID Connect (OIDC) Identity Provider (IDP). Once the users exist in the IDP, the user can log in and depending on their group membership, determine a Manitou role. Depending on the IDP, you can set up multi-factor authentication as well.

Limitations

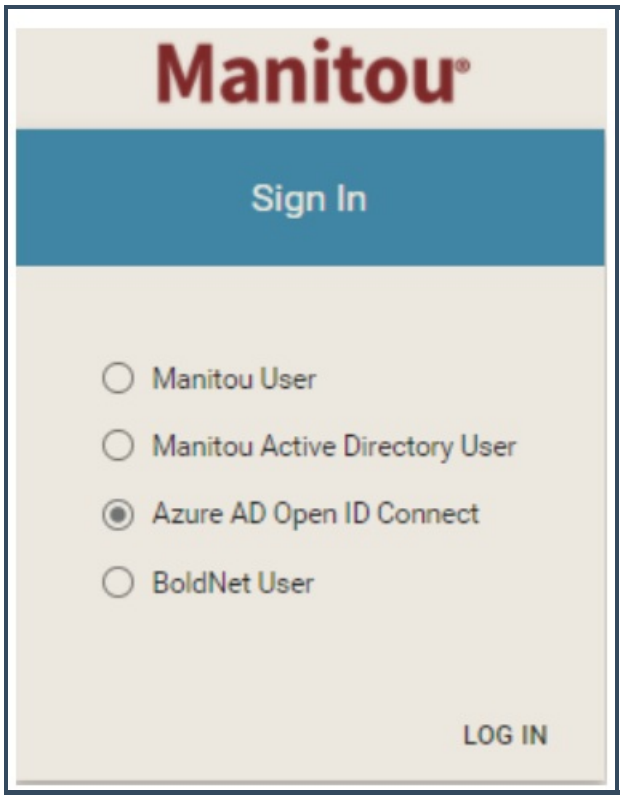
- Due to the complex nature of the permission hierarchy in Manitou, permissions are still managed in Manitou. Permissions are tied to Manitou groups, Manitou groups are tied to IDP groups, and SSO users are assigned to Manitou groups by assigning them to the corresponding SSO group.
- User records are automatically created in Manitou for SSO users at the time of login. However, these records are never removed due to their need in historical reference. They must be manually removed if desired.
- SSO login names (not user names) must be less than 200 characters in length.
- Single Sign-out is not currently supported.
- SSO is only for Manitou Users, not BoldNet Users.
- You can only authenticate to one IDP. Multiple IDPs are not supported.
- SSO logins are only available in the Manitou Web Client. Neither Operator Workstation nor Supervisor Workstation support SSO logins.

Requirements

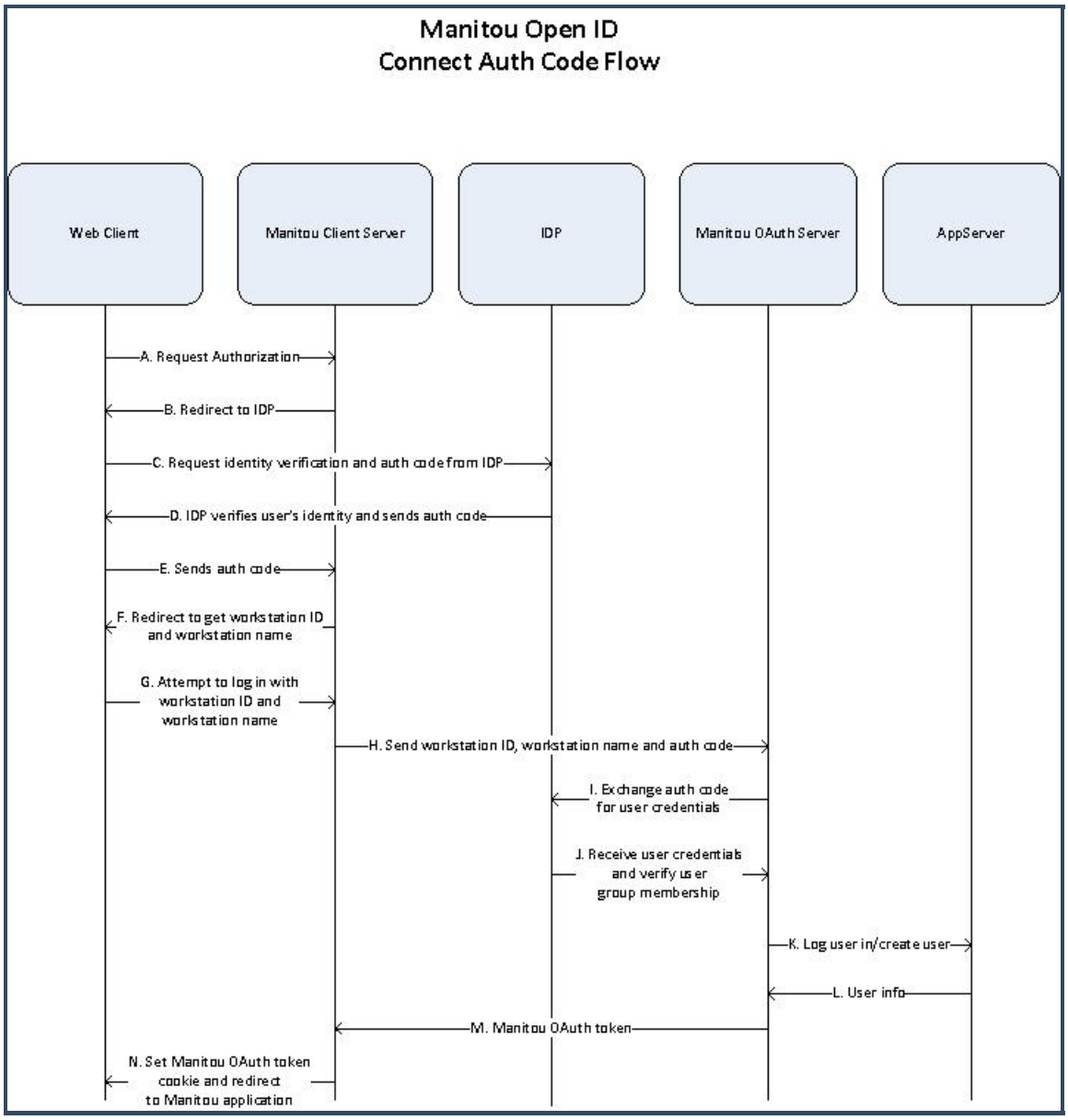
- Manitou web clients and the IIS server that hosts the Manitou web software must be able to connect to the IDP over secure HTTPS connections. Make sure the firewall allows this.
- Active Directory Integration must be licensed in Manitou.

Implementation

When SSO is configured, the Manitou login screen has a new login option.



Notice that there are no login or password fields to enter when the SSO provider is selected. That's because the IDP will verify your identity. If you are certain you want to log in as an SSO user, you can also skip the login page altogether. Instead of having a shortcut that takes you to the Manitou/Login page, you can go to Manitou/SSOLogin and it will initiate the login process with the IDP (for example,).



To keep referential integrity in Manitou, a USR record is created the first time an SSO user successfully authenticates. This record is kept up to date on subsequent logins as the user's name and group membership change. By default, permission is delegated to the user's group but can be managed on a per-user basis by a supervisor (after the first login, of course).

Creation of USR record and mapping IDs

Because Manitou user IDs are limited to 12 characters, and names are limited to 35 characters, some considerations had to be made to provide seamless mapping between SSO users and Manitou users. First, a new field had to be established to identify a user record as being one that is mapped to an SSO user and to hold the SSO username for reference. The new field on the USR table is ADUSER and will hold the username identifier for the user.

Since every Manitou user must have a unique user ID, these must be generated. Also, since the user ID (rather than the Name) is displayed in reports and activity UI, it must be reasonably identifiable and can't be a GUID or random

sequence. However, since the field is only 12 characters and must contain an arbitrarily long username from SSO, some encoding is required.

This ID is generated in the following way:

1. Take the SSO login name, remove spaces, and take the first 12 characters
2. If this name doesn't clash with an existing one, use it as-is
3. If and while it does clash, use the first 10 (for two-digit suffixes) or 11 (with one-digit suffixes) characters, with a numeric suffix in the range 1-99.

Example:

SSO Login	Manitou ID
bobsmith@mydomain.com	bobsmith@myd
King ~~Charles~~ III	King~~Charl
King ~~Charles~~ IV	King~~Charl1
King Phillipe II, the great and powerful@domain.com	KingPhillipe

Note that password records are created in Manitou, but are created with random strong passwords, and are never used for actually logging in SSO users. The system requires these records to data consistency, but will never allow a login where ADUSER is set using the Manitou password.

Group Mapping

Manitou users are assigned authorizations through the use of groups. By default, Manitou ships with several groups, such as Administrator, Supervisor, Operator, etc. IDPs also allow user groups to classify users. When an SSO user is created/updated automatically in Manitou, its Manitou group assignment is determined by which group that user is a member of in the IDP. Manitou will look for a specific group membership relation in the OAuth web.config setting OidcGroupMapping to determine if it is a Manitou group.

These IDP groups can be at any level in the hierarchy and can have any scope. However, for Azure they must be Security groups not Distribution groups. See Manitou Single Sign-on - Azure Open ID Connect for more information.