Manitou - Active Directory Support

12/22/2023 11:30 am EST

Design Goal

The design goal of this project is to allow organizations to manage the users that are allowed to connect to Manitou in Active Directory rather than in Manitou. Once the users exist in Active Directory, Manitou can find them and depending on their AD group membership, determine a Manitou role. In addition, Manitou will have the ability to validate a domain user's password.

Limitations

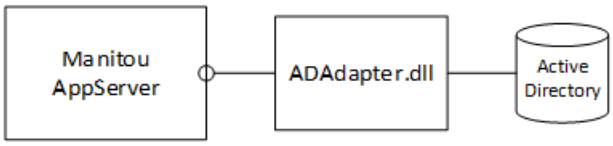
- Due to the complex nature of the permission hierarchy in Manitou, permissions are still managed in Manitou. Permissions are tied to Manitou groups, Manitou groups are tied to AD groups, and AD users are assigned to Manitou groups by assigning them to the corresponding AD group.
- Due to technical and security considerations, single sign-on is currently not supported. The user will be required to provide their domain username and password when logging in to Manitou.
- Because a username and password are required at sign-on, authentication types other than username/password (like smart cards) are currently not supported).
- User records are automatically created in Manitou for AD users at the time of login. However, these records are never removed due to their need for historical reference. They must be manually removed if desired.
- Active Directory logon names (not user names) must be less than 200 characters in length.

Requirements

- The Manitou application server must reside within a domain containing the Active Directory forest for which users should be validated.
- Active Directory Integration must be licensed in Manitou.
- The Active Directory Adapter library (ADAdapter.dll) must reside in the same folder as the Manitou Application Server.
- This functionality is only supported in Manitou 2.0 or later.
- Active Directory login is only supported in ManitouNEO. Legacy clients only support standard Manitou logins.
    - **Due to the client support mentioned above, logins to the Supervisor Workstation MUST be stock Manitou logins.**

Implementation

The core implementation is in a new library, **ADAdapter.dll**, that must reside in the same folder as the Bold Application Server. This library provides the interface between the application server and the Active Directory system:



The system is capable of simultaneously handling stock Manitou logins and AD logins. To achieve this, a new server call was implemented to handle AD logins separate from stock logins. They provide all of the same functionality, apart from where they validate user information. As a result, the ManitouNEO UI will prompt for which type of authentication you'd like at login time, and treat the credentials accordingly.

To keep referential integrity in Manitou, a USR record is created the first time an AD user successfully authenticates. This record is kept up to date on subsequent logins as the user's contact point 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 a seamless mapping between AD 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 AD user and to hold the AD username for reference. The new field on the USR table is ADUSER and will hold the username identifier for the user, in format. This format will be used even if the domain\username format is used at the time of login.

If only a username without a domain is provided at login time, the server will attempt to look up the user using the domain to which the Manitou Application Server computer is assigned.

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 AD, some encoding is required.

This ID is generated in the following way:

1. Take the AD login name (without domain information), remove spaces, and take 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:

AD Login	Manitou ID
	
MYDOMAIN\King ~~Charles~~ III	King~~Charl
MYDOMAIN\King ~~Charles~~ IV	King~~Charl1

King Phillipe II, the great and 	KingPhillipe

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

IMPORTANT! **Since Active Directory users are validated using standard domain password validation methods, repeated invalid password failures while logging in to Manitou can cause the user to be temporarily locked out of the domain, depending on the domain lockout policy.**

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. Active Directory also allows using groups to classify users. When an AD user is created/updated automatically in Manitou, its Manitou group assignment is determined by which group that user is a member of in AD. Manitou will look for a specific group membership name to determine if it is a Manitou group. These group names begin with " "Manitou Group – " and end with the Manitou group name. It is up to an Active Directory administrator to create and correctly name these groups. Manitou does not want to be an AD Administrator and will not create any groups in AD automatically.

These AD groups can be at any level in the hierarchy and can have any scope. However, **they must be Security groups** not Distribution groups.

In addition, **an AD user must resolve to one and only one of these Manitou groups**, either directly or through membership in another AD group that maps to a Manitou group. The user can belong to any number of non-Manitou groups or OU's.

Example:

If you want your AD user to have access to this user group in Manitou	Create an AD security group with this name and add the AD user as a member of that group
Supervisor	Manitou Group - Supervisor
Data Entry	Manitou Group - Data Entry
supersecretoperators	Manitou Group - supersecretoperators

Installation

Installation of this integration is very straightforward, as there is no configuration to be done. Installation can be done by following these steps:

1. Ensure the Manitou installation is of a compatible version (see requirements).
2. Ensure the Manitou client in use is of a compatible version (see requirements).
3. Ensure that every server that runs appserver.exe is participating in the domain for which users will be authenticated.

4. Ensure ADAdapter.dll exists in the Manitou directory alongside appserver.exe on any machines that are going to be running a Bold Application Server.

5. Ensure that each Manitou server is licensed for “Active Directory Integration”.

6. Create groups in Active Directory for every Manitou user group that should be mapped to Active Directory users (see Group Mapping).

7. Assign domain users to these newly created groups as necessary to allow access.

MWC setup

If you want to log into NEO with Active Directory, set the following in your NEO Client’s Web.Debug.Config file:

```
<add key="AllowADLogin" value="true" />
```

Once you have it licensed, your domain login is assigned a Manitou group and your web.config set you will see something like this: