Niagara^{AX} Security Best Practices

July 3, 2012

Disable the Guest User

A station's UserService is designed so that whenever the built-in user "guest" is enabled, someone attempting to access the station will automatically be signed into the station as the Guest user--whether there is a password set for the Guest user or not. What that person is then capable of doing once inside the station is dependent on what permissions are assigned to user "guest". If the user attempts to do something that the Guest user does not have permissions to do, the user is then prompted to sign in as a *different* user, who does have the correct permissions.

By default, the "guest" user is *disabled*. We recommend keeping the "guest" user disabled. Then no one can access the station that wasn't given their own login credentials.

Use Strong Passwords

The stronger the password, the harder it will be for someone to hack into your station. From the property sheet of the UserService, you can configure to require strong passwords for *all station users*. See the "UserService properties" subsection in the "About Security" section of the *NiagaraAX User Guide* for more details.

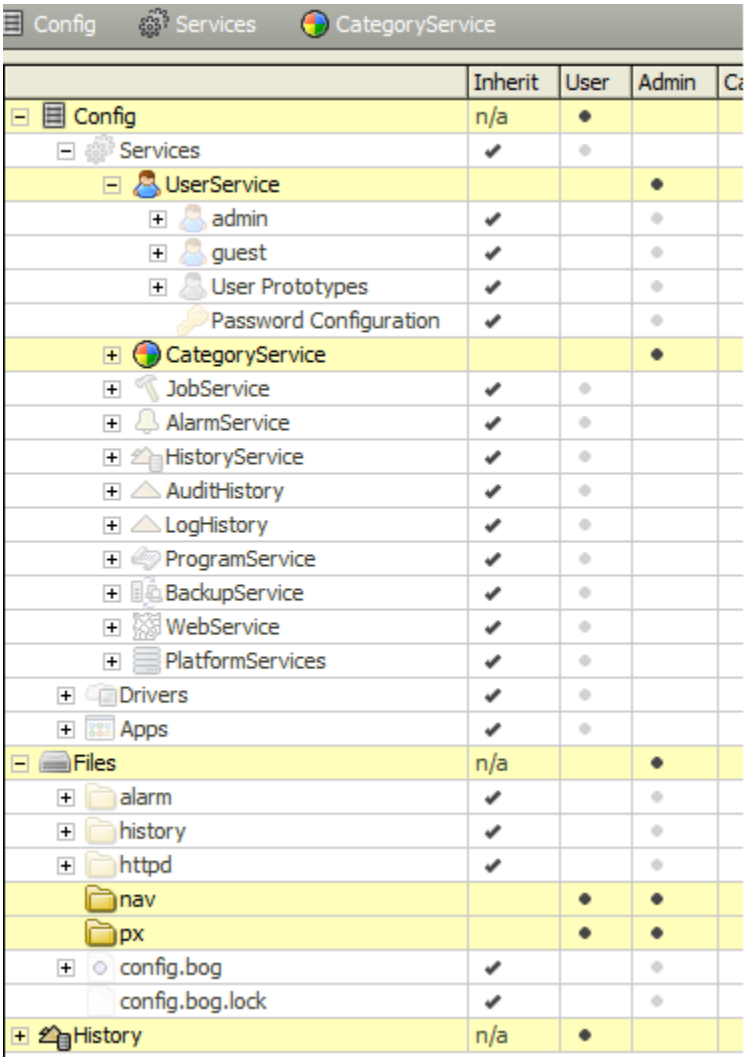
Use the Lock Out Feature

Use the "Lock Out" feature in the UserService, enabled and configured from the service's property sheet. Then if someone is trying to "hack" into the station by constantly retrying different passwords for a user, and the specified number of incorrect login attempts occur in a set time period, that user is "locked out" for the specified time period. See the "Lockout notes" subsection in the "About Security" section of the *NiagaraAX User Guide* for more details.

Limit User Permissions

Only allow users access to the specific things that they need to do their jobs. This is especially important when it comes to the *file system*. If you give a user access to the entire file system, you have potentially given that user access to the entire station configuration.
Specifically, the config.bog file, located in the station's root directory, can be a security risk. Security should be configured to limit access permissions of the user to only folders the user is required to access such as px, images, and nav folders. To setup, create a new category using the Category Manager. Using the Category Browser assign only file folders that you need users to access such as file:^px, file:^nav, etc. to the newly created category. Setup the user permissions to only include file permissions of the newly created file category. Keep in mind that by default all objects are assigned to category index 1 (Category1, or whatever the first Category component is named).

Example Category Browser view



You should also be careful about which *Services* you allow your users access to. Specifically the UserService and CategoryService provide security risks if allowed to be accessed by all users. For more information about the UserService, Users, Categories, and properties/permissions, see the "About Security" section in *NiagaraAX Users Guide*. Note a subsection "UserService security notes" explains a special permissions scheme for a station's UserService.