Niagara^{AX} Security

Niagara^{AX} Security Overview

TRIDIUM®
revolutionary://software.solutions

3951 Westerre Parkway, Suite 350
Richmond, VA 23233
Ph: 804.747.4771
Fx: 804.747.5204
www.tridium.com

Niagara^{AX} Security

Niagara^{AX} includes a comprehensive security model that provides a high degree of flexibility in managing access privileges to a Niagara^{AX} station (a JACE, ^{AX}Supervisor, or a Workbench-based tool such as Tridium's Vykon WorkPlace^{AX}). The security model addresses two kinds of connections that can be made to a Niagara host: a platform connection and a station connection.

Platform connection

Platform connection refers to a connection from a Workbench-based engineering tool (e.g., the Vykon WorkPlace^{AX}) to the host's "platform daemon". The platform daemon is a compact executable that is pre-installed on every JACE controller. It provides support for tasks that allow setup and management of a Niagara host. The platform daemon monitors a different TCP/IP port for client connections than does a Niagara station and uses "host-level" authentication for access. Host-level access is controlled by a set of user accounts and passwords which are separate from any station user account and are part of the host operating system. On an ^{AX}Supervisor running on a Windows host, for example, platform user accounts would be part of the Windows user accounts.

The host-level user account provides Administrator Level access making the platform connection the highest level of access to a Niagara host. It is used to copy a new station database to the host, or start and stop the station on the host, among other management functions. Note that the actual user name and password for the platform daemon account can be same as a station user name and password, but the accounts are different. For example, the user would need to enter the user name and password into the logon dialog for the platform even if that user was logged into the station.

Station connection

Station connection refers to a connection by a person using either a Workbench-based tool or a web browser to a Niagara^{AX} station, or connection by one station to another station. The Niagara^{AX} security mechanism determines if a station connection is allowed, what can be accessed, and what operations can be performed.

The Niagara^{AX} security model is based on the concept of Users, Permissions, and Categories. Anything that needs to be protected (components, files, histories) is grouped into one or more categories. Each user is granted a set of permissions in each category. This combination of categories and permissions then defines exactly what each user can do with each object in the system. The following sections explain the various aspects of Niagara^{AX} station security:

Users

Typically a "User" represents a human user who needs to connect to a Niagara station, but it can also be used to represent machine accounts for machine to machine (station to station) connections. Every station has two built-in users that cannot be deleted or renamed: "admin" and "guest". User "admin" is always a super user, meaning it has all permissions in every category and can thus access everything in a station. User "guest" is disabled by default. If enabled it provides station access from a web browser with no authentication (user is not prompted to login). User "guest" can then navigate to any object that has been assigned read permission for the user account "guest". Every user of the system should be given a unique user name and password to make the audit logs more valuable.

Users have properties that define how the user navigates around the station, their language preferences, time and unit preference, etc. The main properties of a User related to security and station connection are their login credentials (e.g., user name, and password). Whenever a connection attempt is made these credentials are checked against the users that have been configured in the station. This process is called Authentication (more detail is provided on this topic below).

Users are stored in the station's local database by default and looked up by the station's User Service. Alternatively, users can be looked up using the Lightweight Directory Access Protocol (LDAP). LDAP provides a central location for administering users of a Niagara System. In addition to storing the login credentials, a user profile can be stored in the LDAP server. This user profile can then be matched to a pre-configured user in the Niagara system to grant the user who is logging in the same privileges as the pre-configured user. For example, a Niagara station could be configured with a 'template user' called "Engineering". This user "Engineering" could then be assigned as a profile to User1, User2, etc. in the LDAP server. When any user who has been assigned this "Engineering" profile in the LDAP server is logged into the Niagara station and authenticated via LDAP, they will have the same access rights and privileges that the "Engineering" user has in the Niagara station.

Authentication

Whenever a station connection attempt is made, the user's login credentials are authenticated. There are three authentication points in the Niagara Framework:

1. *Workbench-to-station via Fox*
   (Fox is the standard communication protocol used for communication within the Niagara System):

The user is prompted for a user name and password which is used to authenticate the Fox connection. The default authentication mechanism is Digest authentication which encrypts the password so that it is not passed in clear text. If LDAP is used then basic authentication must be configured between the Workbench and the station because the station needs the password in text to pass on to the LDAP server. Secure Sockets Layer (SSL) can be used between the station and the LDAP server to connect to the SSL port of the LDAP server.

2. *Station-to-station via Fox*:

The concept is the same as the Workbench-to-station connection but instead of prompting for a user name and password, a pre-configured user name and password stored under the proxy for the station being connected to is used. This pre-configured user name and password (typically with super user permissions) must correspond to a valid user in the station being connected to.

3. *Web browser-to-station (HTTP)*

The user is prompted for a user name and password unless the "guest" user account is enabled. The default authentication mechanism is a cookie. Note that in a multi-station installation if the Niagara stations are installed on a DNS domain and accessed using the full DNS name, you can configure stations so that a browser user is authenticated only once (upon initial station connection). In this scenario the same credentials used in the initial login are used in other station connections that the user navigates to via hyperlinks from the original station.

Secure Connections via SSL

Niagara^{AX} supports SSL (Secure Sockets Layer) to provide secure communications between a web browser and the station. SSL works by using a private key to encrypt data that's transferred over the SSL connection between the web browser and the Niagara^{AX} station thus providing privacy, authentication and message integrity over the public Internet. URLs that begin with HTTPS indicate that an SSL connection will be used. HTTPS can be enabled from the Web Service in the Niagara^{AX} station if required.

Categories

A Category is simply a name for a logical grouping of items or components. Categories are typically named to reflect what the grouping contains. For example, the “Lighting” category group might contain objects related to lighting and the “Floor 1” category might contain objects related to Floor 1. Any object that needs to be protected with individual security rules can be assigned to one or more categories. If an object is not explicitly assigned to any category it inherits the categories of its parent.

Objects store the categories they belong to as a variable length bit string so they can belong to as many categories as needed. Since each object stores the categories it belongs to the Niagara^{AX} security model provides excellent performance and scalability.

Permissions

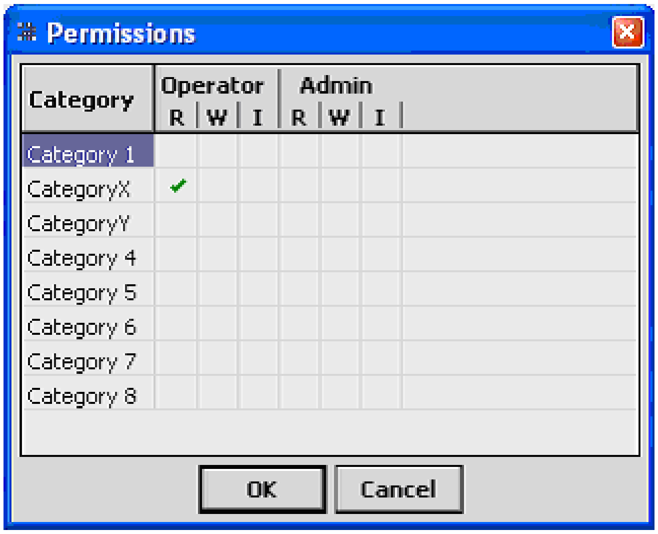
Permissions define what rights a user has within each of the categories in the station. There are two Niagara permission levels: operator and admin. Within each level, separate options exist for read access, write access and invoke (action) access.

Every user in the station is configured with a permissions map. This map grants the user permissions for each category defined in the station, thereby granting the user permissions for objects assigned to that category. This provides tremendous flexibility. For example, if a user lacks read permissions on any object that object would not be visible in the client display. Super users are automatically assigned every permission in every category for every object.

An example follows on the next page.

Example

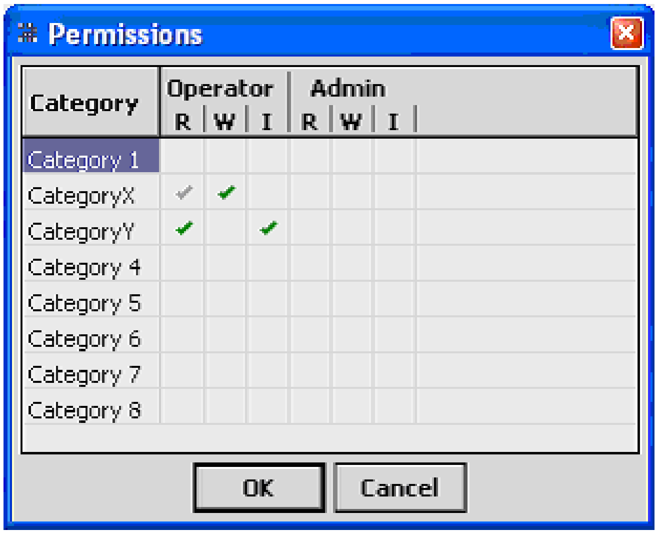
To illustrate how users, permissions and categories interact consider the following example:



Category	Operator			Admin		
	R	W	I	R	W	I
Category 1						
CategoryX	✓					
CategoryY						
Category 4						
Category 5						
Category 6						
Category 7						
Category 8						

User1 has operator read permission in CategoryX. The screen shot at left shows the Permissons settings for User1

User2 has operator read/write permission in CategoryX and read/invoke in CategoryY. The screen shot below shows the Permissons settings for User2



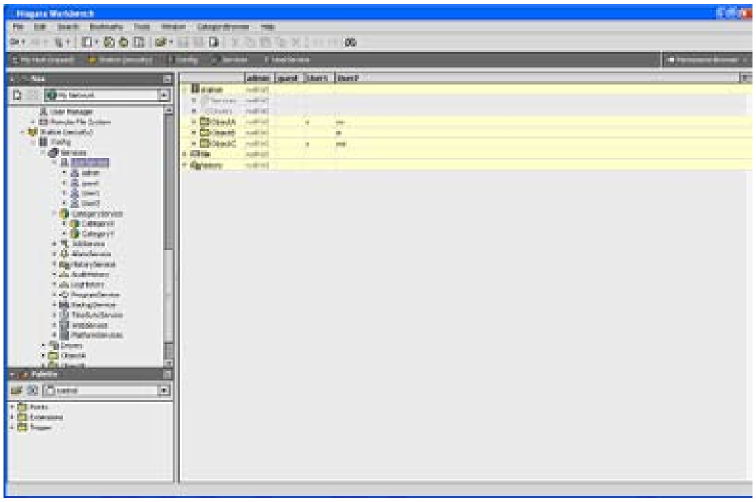
Category	Operator			Admin		
	R	W	I	R	W	I
Category 1						
CategoryX	✓	✓				
CategoryY	✓		✓			
Category 4						
Category 5						
Category 6						
Category 7						
Category 8						

ObjectA in CategoryX (User1 can read, User2 can read/write)

ObjectB in CategoryY (User1 can do nothing, User2 can read/invoke)

ObjectC in CategoryX and CategoryY (User1 can read, User2 can read/write/invoke).

Niagara^{AX} Security

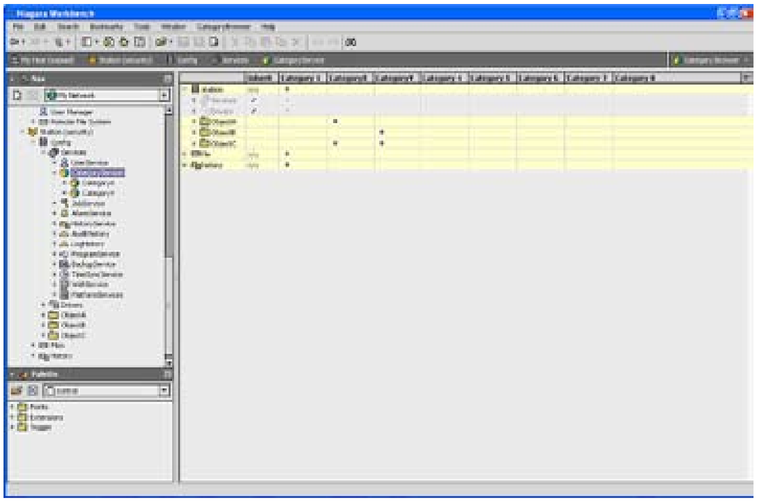


The screen shot below shows the Permissions Browser View that shows user privileges for each object at a glance.

Note that User2 gets read, write, and invoke permission on ObjectC. Permissions are merged so User2 got read/write because ObjectC was in CategoryX and got read/invoke because it was also in CategoryY.

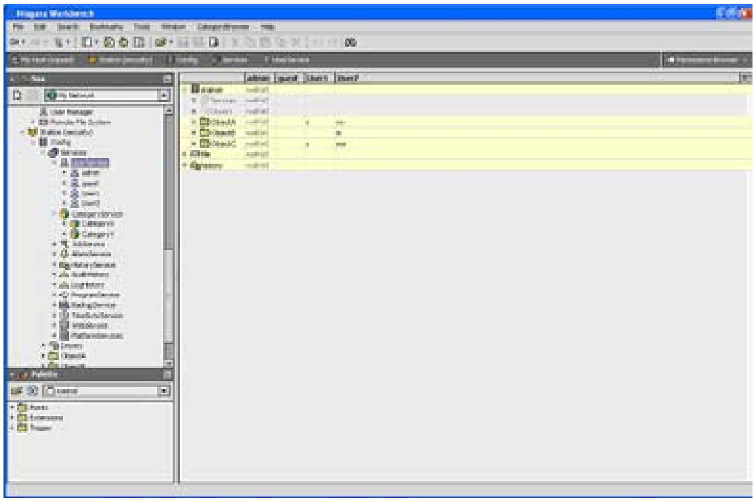
Tools

GUI tools are available for setting up all aspects of Niagara^{AX} security. These tools make the task of configuring Users, Categories and Permissions easy. Platform views provide an interface to setup host level users. The User Service is used to setup users in a Niagara station. Categories are setup using the Category Manager. The Category Browser and Permissions Browser provide an intuitive graphical view to look at who has what access to what objects in the entire station database.



The screen shot at left shows the Category Browser View that shows which object belongs to which category at a glance.

Niagara^{AX} Security



Platform User Manager View

Niagara^{AX} security vs. Niagara R2 security

Niagara R2 provides a robust security model. Niagara^{AX} builds on the R2 security model and provides better performance and scalability. Niagara R2 allowed for only eight “SecurityGroups”. Niagara^{AX} provides unlimited (limited by host memory of course) Categories.

Niagara^{AX} provides additional features related to security:

- Digest authentication
- LDAP support
- HTTPS support
- Single signon from a web browser if using DNS configuration
- User-friendly graphical tools to manage security in a Niagara system

TRIDIUM®

revolutionary://software.solutions®

www.tridium.com

Information and specifications published here are current as of the date of publication of this document. Tridium, Inc. reserves the right to change or modify specifications without prior notice. The latest product specifications can be found by contacting our corporate headquarters, Richmond, Virginia. Products or features contained herein may be covered by one or more U.S. or foreign patents.

3951 Westerre Parkway, Suite 350 Richmond, VA 23233 Ph: 804.747.4771 Fx: 804.747.5204 www.tridium.com