Security in Freezerworks

Freezerworks employs several layers of security to protect your valuable data. You can restrict access:

- with **passwords and login security**
- using **software level security**
- by **encrypting connections** using TLS
- using a **Windows service** to start the application

Passwords and Login Security

The System Administrator may enable several options regarding password requirements, login attempts and automatic client logoff.

The **password** options include:

- Expiration of the user's initial password
- Expiration of passwords after a specific number of days
- Password recycling
- Case sensitive passwords
- Mixed case passwords
- Require numbers and letters
- Require a minimum length

When **login security** is enabled, the System Administrator can track successful and unsuccessful login attempts in the Login Audit Trail. This Audit Trail will display login attempts from all login sources: Desktop and Web Client. It will also display actions such as Successful Login, Invalid Password and Invalid User Name.

Automatic Client Logout prevents unauthorized access to Freezerworks by closing a Client/Server connection after a specified time of inactivity.

Software Level Security

The Security Level System in Freezerworks consists of four different approaches:

- User Roles
- Sample Owner Based Security
- Freezer Security
- Study Security (Pinnacle edition only)

These security levels can be used independently or in concert with one another depending on the needs of the organization.

Each of these is based on the concept of Roles, Users, and Groups. At minimum, the System Administrator must create Roles defining the functions or actions each Role is permitted. Each User is then assigned a Role. In order to use either the Owner Security or Freezer Security option, it is also necessary to create Groups and assign individual Users to those Groups.

Role Permissions

When the System Administrator creates a new User, a Role is assigned by which permission to use individual menu options is given or denied. This is the first level of security, and it overrides all others. If a User is not given permission to View Samples, those menu options will not be available for that user. They will appear “grayed out.” This type of security is functionally based, which means users are granted or denied permission to perform specific functions throughout the software program. For example, a User may be given permission to View Samples, without permission to Add Samples, Modify Samples, or Delete Samples.

Owner Security

When a Sample is created Freezerworks sets the Owner Name to the Group in which the User is a member. Owner Security is based on this Ownership. Sample Ownership may be reassigned by the System Administrator if samples are transferred to a different Group. When creating a new Group, the System Administrator assigns a Default Access Level to the Samples owned by that Group. Default Access Levels are: **No Access, View Only, Modify,** or **Modify and Delete**. This Default Access Level is the type of access ***other Groups*** will have to Samples owned by this Group. This Access Level is inherited by all related data as well including Aliquots, Transactions, Tests, and Results.

The four Access Levels work as follows:

- **No Access** – Samples will not be visible to other Groups. They will not appear in View Listings, Searches, Exports, Reports, or Explore Freezers.
- **View Only** – Samples will be visible to other Groups, but cannot be modified.
- **Modify** – Samples will be modifiable by other Groups, but cannot be deleted.
- **Modify and Delete** – Samples can be modified and deleted by other Groups.

In addition to the Default Access Level, the System Administrator may grant different levels of access to different Groups.

The Owner Security system is optional. It can be turned on or off by selecting the appropriate option located in the **System Admin** menu. The Default System Admin User has access to all samples regardless of security settings.

Freezer Security

When freezers are created, the System Administrator may restrict access to the aliquots stored in those freezers by setting each freezer's Access Level. Each freezer will have a Default Access Level that determines what type of access users will have to the freezer by default. There are four Access Levels to choose from: **No Access, View Only, Modify, Modify and Delete**.

The four Access Levels work as follows:

• **No Access** – Aliquots stored in this Freezer will not be visible to Users. They will not appear in View Listings, Searches, Exports, or Reports. The Freezer will not appear in Explore Freezers.

• **View Only** – Aliquots are visible to Users, but cannot be modified.

• **Modify** – Aliquots can be modified by Users, but cannot be deleted.

• **Modify and Delete** – Aliquots can be modified and deleted by Users.

In addition to the Default Access Level, the System Administrator may grant different levels of access to different Groups. The Freezer Security system is optional. It can be turned on or off by selecting the appropriate option located in **System Admin** menu. The Default System Admin User has access to all freezers regardless of security settings.

When both Owner Security and Freezer Security are enabled, Freezerworks checks access levels as follows:

1. **User permissions:** Does the user have permission to use the function? If yes, continue. If no, then stop.

2. **Owner Security:** Is the user a member of a group that has been assigned specific access to the owner's samples? If yes, then find the ***least*** restrictive group specific access and use that. If not, then use the default access level.

3. **Freezer Security:** If the user has at least *View* access to the Samples, then continue on with determining Freezer based access. Is the user a member of a group that has been assigned specific access to the freezer(s) in which this sample's aliquots are stored? If yes, then find the ***least*** restrictive group specific access and use that. If not, then use the default access level for the freezer.

Study Security

The Pinnacle Edition includes data management of Studies, modeled Visits, enrolled Patients and the Samples, Aliquots, and Tests associated with them. When creating a Study, the System Administrator may restrict access to it in a fashion similar to that described for Sample Ownership. The Access Levels are the same and function as follows:

- **No Access** – No data related to the Study will be visible including modeled Visits, enrolled Patients, Samples, Aliquots, Transactions, Tests, and Results.

- **View Only** – Study related data are visible to Users, but cannot be modified.

- **Modify** – Study related data can be modified by Users, but cannot be deleted.

- **Modify and Delete** – Study related data can be modified and deleted by Users.

When Study Security, Owner Security, and Freezer Security are enabled, Freezerworks checks access levels in the following order:

1. User permissions

2. Study Security

3. Owner Security

4. Freezer Security

Encrypt Client/Server Connections

Freezerworks Server contains an option to encrypt the TCP\IP connection. Its use allows you to reinforce communication security, but it will slow down the Client/Server connections. This option does not require any additional settings, and it is disabled by default.

Windows Services

Freezerworks Server can be run as an application using the FreezerworksServer.exe executable program, or as a service in Windows. A Windows Service is an executable object that is installed in a registry database maintained by the service control manager. The services database includes information that determines whether each installed service is started on demand or is started automatically when the system starts. The database can also contain logon and security information for a service so that a service can run even though no user is logged on. It also enables system administrators to customize security requirements for each service and thereby control access to the service.

Web Client

Access to Freezerworks using the Web Client (via the REST API) requires full user authentication for each request sent to the Web Server. All security rules described in this document are fully enforced. The connection can be set up to use HTTPS.