Security Module Reference

Configure users, roles, and permissions.

Reference Security | Tutorial | How-to Guide | Reference

Security Module (Reference) provides comprehensive authentication, authorization, and access control for FrameworX solutions.

This reference covers the module's configuration interfaces, runtime behavior, and integration with enterprise security systems.

Configuration Interfaces
Module Components
Runtime Behavior
Security Namespaces
Configuration Storage
Security Features
Best Practices Checklist
Troubleshooting
Security Module Links

Configuration Interfaces

Component	Location	Purpose
Users	Security Users	Define local user accounts
Permissions	Security Permissions	Configure role-based access groups
Policies	Security Policies	Set password and session requirements
RuntimeUsers	Security RuntimeUsers	View external/dynamic users
Monitor	Security Monitor	Track active sessions (runtime only)

Module Components

Users

Local users defined within the solution configuration. Includes three pre-defined accounts:

- **Administrator** - Full system access (set password immediately)
- **Guest** - Anonymous/default access
- **User** - Generic login account

[Security Users (Reference)] for detailed configuration

Permissions

Role-based access control groups defining what users can access in Designer and Runtime.

Pre-defined groups: Administrator, Engineering, Supervisor, Operator, Maintenance, Guest

[Security Permissions (Reference)] for detailed configuration

Policies

Security requirements for passwords, sessions, and electronic signatures.

Pre-defined policies: Default, Enhanced, Critical

[Security Policies (Reference)] for detailed configuration

RuntimeUsers

Dynamic users from external sources:

- External SQL databases
- Active Directory integration
- LDAP server authentication
- Script-created users

[Security RuntimeUsers (Reference)] for detailed configuration

Monitor

Real-time view of connected users and active sessions during runtime.

[Security Monitor (Reference)] for detailed configuration

External Authentication

Integration with enterprise authentication systems:

- Windows Active Directory
- LDAP servers
- Custom authentication providers

[Windows AD / LDAP Server (Reference)] for detailed configuration

---

Runtime Behavior

Authentication Flow

1. Check for local Engineering User
2. If not found, check RuntimeUsers database
3. If not found, check AD/LDAP (if configured)
4. If no valid user, default to Guest

Permission Evaluation

Permissions are evaluated at multiple levels:

- **Solution Level** - Overall access to the solution
- **Module Level** - Access to specific modules (Tags, Alarms, etc.)
- **Display Level** - Access to specific displays
- **Object Level** - Access to individual controls/elements

Session Management

- Automatic session timeout based on policy
- Concurrent login restrictions
- Session monitoring via Security Monitor
- Programmatic access via @Server.GetAllConnections()

Security Namespaces

Client Namespace

Runtime information about current user:

- `@Client.UserName` - Current logged user
- `@Client.CurrentUser` - User object with all properties
- `@Client.LogOn(username, password)` - Login method
- `@Client.LogOff()` - Logout method

Security Namespace

Security management methods:

- `@Security.CreateUser()` - Create RuntimeUser dynamically
- `@Security.ValidateUser()` - Verify credentials
- `@Security.ChangePassword()` - Update user password

Configuration Storage

Solution Database

Local users, permissions, and policies are stored in the solution database (.dbsln file).

RuntimeUsers Database

External users stored in:

- Default: SQLite database (Dataset.DB.RuntimeUsers)
- Optional: SQL Server, PostgreSQL, or other databases
- Encrypted storage for credentials

Security Features

Compliance Support

- **FDA 21 CFR Part 11** - Electronic signatures, audit trail, password policies
- **NERC CIP** - Account monitoring, session management, audit logging
- **ISA-99/IEC 62443** - Zone security, role-based access

Advanced Features

- Multi-factor authentication support
- Certificate-based authentication
- Single Sign-On (SSO) via AD
- Encrypted credential storage
- Session replay protection

Best Practices Checklist

Initial Setup

- **Change default passwords** immediately
- **Configure policies** before creating users
- **Define permission groups** based on roles
- **Test authentication** before deployment

Maintenance

- Review user accounts quarterly
- Monitor failed login attempts
- Update passwords regularly
- Audit permission changes
- Document security model

Troubleshooting

Issue	Check
Cannot login	Credentials, account status, policy restrictions
Permission denied	Group membership, module access, display security
Session timeout	Policy settings, inactivity timer
AD authentication fails	Domain configuration, network connectivity

---

Security Module Links

Explanation - to understand concepts

Modules / User Interactions / Security Module

Tutorials - to learn by doing

Tutorials / User Interactions / Security Module Tutorial

How-to Guides - to accomplish specific tasks

Reference - technical details

In this section...
