Alarms Global Settings Reference

Apply system-wide alarm configuration.

Alarms Global Settings (Reference) define system-wide configurations for alarm management, logging, and audit trail functionality. It configure:

- Alarm historian database
- System startup behavior
- Alarm handling parameters
- Audit trail logging
- FDA 21 CFR Part 11 compliance

Access via **Alarms** **Global Settings**

Configuration Sections
Database Configuration
Startup Behavior
Shift-Based Limits
Audit Trail Configuration
FDA 21 CFR Part 11 Compliance
Runtime Access
Best Practices Checklist
Troubleshooting

Configuration Sections

Alarm Logging Database

Setting	Description	Default
Database	Database type (SQLite, SQL Server, etc.)	SQLite
Connection	Connection string	Local file
Life Time	Days to retain alarm data (0 = forever)	0

Note: Life Time function not compatible with PostgreSQL TimeScaleDB extension

Alarm Handling

Setting	Description	Default
Initial Disable Time on Startup	Seconds to suppress alarms after startup	00:00:00
Ignore Alarms During TimeDeadband	Ignore alarms during deadband period	False
Enable LimitsByShift	Enable shift-based alarm limits	False
LogUserFullName	Log full user name vs username	False

Audit Trail

Setting	Description	Default
Enable Audit Trail	Activate audit logging	False
User Logon /Logoff	Log user sessions. From FrameworX 10.1.6, also logs each electronic-signature outcome on the operator client: accepted, refused with the reason, canceled, or canceled because the signed-in user changed. See Security Policies Reference.	False
Open /Close Displays	Log display navigation	False
Remote Connections	Log client connections	False
Custom Messages	Log custom audit messages	False

Tag Changes	Log all tag value changes	False
Datasets	Log database operations	False
Operator Actions	Log operator commands	False
Save Reports	Log report generation	False
System Warnings	Log system events. From FrameworX 10.1.6, this includes the license and maintenance plan expiration notices. See Licensing Procedures Reference.	False
MCP Custom Tools	Log every execution of a solution-authored MCP Custom Tool invoked via the AI Runtime Connector. From FrameworX 10.1.6, the option also logs every built-in AI Runtime tool call, read-only tools such as `runtime_get_value` and `runtime_browse_object_model` included. See AI Runtime Connector for the AI client architecture.	True

---

Database Configuration

Supported Databases

- SQLite (default, embedded)
- SQL Server
- PostgreSQL
- MySQL
- Oracle

Connection String Examples

SQLite (default):

```
Provider=System.Data.SQLite;Data Source=_ExecutionPathAndName_.dbAlarm
```

SQL Server:

```
Server=localhost;Database=AlarmHistory;Trusted_Connection=true;
```

PostgreSQL:

```
Host=localhost;Database=alarms;Username=user;Password=pass;
```

Startup Behavior

Initial Disable Time

Prevents nuisance alarms during startup:

- System initializes without triggering alarms
- Tags stabilize to normal values
- After timeout, normal alarm processing begins

Example: Set to 00:01:00 (1 minute) for complex systems

TimeDeadband Handling

When enabled:

- Alarms ignored during group deadband period
- Prevents alarm flooding
- Useful for known transient conditions

Shift-Based Limits

When **Enable LimitsByShift** is active:

- AlarmItems use Limit, Limit1, Limit2
- Different thresholds for different shifts
- Automatic switching based on schedule

See [Alarm Limits by Shift] for configuration

Audit Trail Configuration

Enabling Audit Trail

1. Check **Enable Audit Trail**
2. Select events to log
3. Configure database (uses alarm database)
4. View in AlarmViewer with List = "AuditTrail"

Custom Messages

Add via script:

```
@Alarm.GlobalSettings.AuditTrail.AddCustomMessage(
    message: "Batch completed",
    areaName: "Production",
    objectName: "Reactor1",
    value: "500",
    itemName: "BatchID",
    auxValue: "Grade A",
    comment: "Normal completion"
);
```

Runtime Control

```
// Enable/disable options at runtime
@Alarm.GlobalSettings.AuditTrail.UserLogonLogoff = true;
@Alarm.GlobalSettings.AuditTrail.TagChanges = false;
```

FDA 21 CFR Part 11 Compliance

For regulatory compliance:

1. **Enable Audit Trail** - Required
2. **User Logon/Logoff** - Track user access
3. **Operator Actions** - Record all changes
4. **System Warnings** - Log system events
5. **Tag Changes** - Track process modifications

Configure retention:

```
Life Time = 2555 days (7 years)
```

Runtime Access

Access settings programmatically:

```
// Check audit trail status
bool auditEnabled = @Alarm.GlobalSettings.AuditTrail.IsEnabled;

// Add custom message
@Alarm.GlobalSettings.AuditTrail.AddCustomMessage("Process started");

// Check database connection
string dbConnection = @Alarm.GlobalSettings.Database.Connection;

// Modify settings
@Alarm.GlobalSettings.LogUserFullName = true;
```

Best Practices Checklist

- [ ] **Size database appropriately** - Audit trail generates significant data
- [ ] **Set reasonable retention** - Balance compliance vs storage
- [ ] **Test startup delays** - Find optimal disable time
- [ ] **Selective audit logging** - Only log necessary events

- [ ] **Regular database maintenance** - Archive old data
- [ ] **Document settings** - For compliance audits
- [ ] **Monitor database growth** - Prevent storage issues

Troubleshooting

Database connection failed:

- Verify connection string
- Check database service running
- Confirm network access
- Review user permissions

Audit trail not logging:

- Confirm Enable Audit Trail checked
- Verify specific options enabled
- Check database write permissions
- Review disk space

Alarms triggering at startup:

- Increase Initial Disable Time
- Enable Ignore During TimeDeadband
- Review startup sequence

Database growing too large:

- Set Life Time appropriately
- Archive old data regularly
- Consider separate audit database
- Optimize logged events

In this section...
