Security Policies Reference

Define system-wide security policies.

Security Policies (Reference) enforce password requirements, electronic signatures, and session management rules for regulatory compliance and security best practices.

Security Policies provide:

- Password complexity requirements
- Electronic signature validation
- Session timeout management
- Account lockout rules
- Password aging controls

Policies enable FDA 21 CFR Part 11 compliance and other regulatory requirements.

Pre-Defined Policies
Configuration Properties
Identification Settings
E-Signature Settings
Session Management
Applying Policies
Compliance Scenarios
Best Practices
Troubleshooting

Pre-Defined Policies

Three standard policies are configured:

Policy	Use Case	Typical Settings
Default	Standard operations	Basic password, no timeout
Enhanced	Elevated security	Complex password, session timeout
Critical	Regulatory compliance	Strong password, e-signature, strict timeout

Configuration Properties

Property	Description	Required
Name	Unique policy identifier	Yes
Identification	Password and account rules	Yes
ESign	Electronic signature settings	No
Session	Timeout and auto-logoff	No
Description	Documentation text	No

Identification Settings

Password and account management rules:

Password Requirements

Property	Description	Range	Default
PasswordMinLength	Minimum characters	0-128	0 (no limit)
PasswordHistory	Previous passwords to remember	0-5	0
MinPasswordAge	Hours before change allowed	0+	0
MaxPasswordAge	Hours until expiration	0+	0 (never)

Account Security

Property	Description	Range	Default
UserNameMinLength	Minimum username length	0-128	0

BlockOnInvalidAttempts	Failed logins before lockout	0+	0 (no limit)
BlockAging	Hours until auto-unlock	0+	0 (manual)
AllowPasswordChange	Users can change own password	Yes/No	Yes
AllowShareUser	Multiple concurrent sessions	Yes/No	Yes

E-Signature Settings

Electronic signature requirements for critical actions:

Property	Description	Use Case
Enabled	Require e-signature	FDA compliance
TimeoutMinutes	Signature validity period	Re-authentication frequency

Configuring E-Signature

1. Enable in policy settings
2. Set timeout (e.g., 60 minutes)
3. Assign policy to users
4. Enable on controls requiring signature

Example:

csharp

```
// Check if e-signature required
if (@Security.Policy.ESign.Enabled)
{
    // Prompt for password
    if (!@Security.ValidateESignature())
    {
        return; // Action cancelled
    }
}
```

E-Signature Audit Trail

From FrameworX 10.1.6, each electronic-signature outcome on the operator client is recorded in the audit trail with the user and the result:

- **Accepted**: the signature is valid and the protected action runs.
- **Refused**: with the reason, for example an invalid password or a blocked account.
- **Canceled**: the operator canceled the prompt.
- **User changed**: the signed-in user changed while the prompt was open. The prompt closes and the protected action does not run.

Cancel takes precedence over a password check still in progress. When an operator presses OK and then Cancel before the check finishes, the signature is not accepted, the protected action does not run, the prompt does not reopen, and the audit trail records the cancellation. A wrong password entered before Cancel is also recorded as a refused signature.

These entries need **Enable Audit Trail** and **User Logon/Logoff** checked in **Alarms Global Settings**. In 10.1.5, electronic-signature prompts leave no audit record.

Electronic Signature on an Editable ComboBox

From FrameworX 10.1.6a, a ComboBox with **Is Editable** checked and its list closed writes the typed value before an action runs: a button, shape or symbol with an action, a hotkey, or the OK button of a dialog. When the Security settings of the ComboBox require an electronic signature, the press opens the signature prompt and does not run the action:

- **Signed**: the ComboBox writes the value. The operator presses again to run the action.
- **Canceled**: the field returns to the last written value, and the action does not run.

While an earlier signature is still valid (**TimeoutMinutes** above), no prompt opens, and the action runs at once with the new value. On the desktop client, a click elsewhere on the display also writes the typed value and opens the prompt. See ComboBox Control Reference.

Session Management

Automatic logoff configuration:

Property	Description	Options

AutoLogOff	Logoff trigger	None, Inactivity, Duration, Both
InactivityMinutes	Idle time before logoff	1-9999
DurationHours	Maximum session length	1-9999

AutoLogOff Modes

Mode	Behavior	Use Case
None	No automatic logoff	Dedicated stations
Inactivity	Logoff after idle time	Shared workstations
Duration	Logoff after time limit	Shift changes
Both	Either condition triggers	Maximum security

Applying Policies

Assign to Users

1. Navigate to **Security Users**
2. Select user row
3. Set **Policy** column
4. User inherits all policy settings

Missing Policy

From FrameworX 10.1.6, when the policy assigned to a user cannot be found, sign-ins by user name and password, by token, through OpenID Connect and through the built-in administrator sign-in use the policy of the **Guest** user for the session. The user keeps the same permissions, so solutions upgraded from an earlier version keep admitting the same users. Electronic signature, signature timeout, automatic log-off and password change follow the Guest user's policy, and the trace records a warning naming the user and the missing policy. Windows Authentication sign-ins are admitted as before.

The sign-in is refused with the error `PolicyNotFound` only when the Guest user's policy cannot be found either. To correct either case, assign an existing policy to the user in **Security Users**.

Runtime Behavior

csharp

```csharp
// Get current user's policy
string policyName = @Security.CurrentUser.Policy;

// Check policy settings
var policy = @Security.Policies[policyName];
bool requiresESign = policy.ESign.Enabled;
int passwordMinLength = policy.Identification.PasswordMinLength;
```

Compliance Scenarios

FDA 21 CFR Part 11

```
Policy: Critical
Identification:
  - PasswordMinLength: 8
  - PasswordHistory: 5
  - MaxPasswordAge: 2160 (90 days)
  - BlockOnInvalidAttempts: 3
ESign:
  - Enabled: True
  - TimeoutMinutes: 30
Session:
  - AutoLogOff: Both
  - InactivityMinutes: 15
  - DurationHours: 12
```

High Security Environment

```
Policy: Enhanced
Identification:
  - PasswordMinLength: 12
  - AllowShareUser: False
  - BlockOnInvalidAttempts: 5
  - BlockAging: 24
Session:
  - AutoLogOff: Inactivity
  - InactivityMinutes: 10
```

Best Practices

1. **Start with pre-defined** - Modify existing policies
2. **Document requirements** - Clear compliance needs
3. **Test thoroughly** - Verify all settings work
4. **Train users** - Explain policy changes
5. **Regular reviews** - Update as needed
6. **Gradual implementation** - Phase in restrictions
7. **Monitor compliance** - Track violations

Troubleshooting

Account locked:

- Check BlockOnInvalidAttempts
- Verify BlockAging timeout
- Administrator unlock required
- Review failed login attempts

Password rejected:

- Check PasswordMinLength
- Verify against PasswordHistory
- Confirm MinPasswordAge not violated
- Review complexity requirements

Unexpected logoff:

- Check Session settings
- Verify InactivityMinutes
- Review DurationHours
- Check client activity detection

E-signature issues:

- Verify policy enabled
- Check timeout not expired
- Confirm user has password
- Test signature validation

In this section...
