i-Vu® Pro v8.5

Life Sciences Best Practices Guide

 Verify that you have the most current version of this document from **www.hvacpartners.com**, the **Carrier Partner Community** website, or your local Carrier office.

Important changes are listed in **Document revision history** at the end of this document.

Contents

What is i-Vu® Pro for Life Sciences?

i-Vu® Pro for Life Sciences is a product bundle that includes licensed features and add-ons necessary to apply the product on a 21 CFR Part 11 compliant, or other validated site.

The i-Vu® Pro for Life Sciences license includes everything that the i-Vu® Pro Unlimited license includes, Advanced Security, Advanced Alarming, and Advanced Reporting, plus the LDAP/AD and Trend Export add-ons. Licensed features specific to Life Sciences include:

- Electronic records
- Electronic signatures
- Pre-configured critical variance tracking reports
    - Mean Kinetic Temperature (MKT)
    - Trend Values
    - Value Out of Range

See the i-*Vu® Pro v8.5 User Manual* for a complete description of i-Vu® Pro for Life Sciences capabilities.

i-Vu® Pro for Life Sciences v8.0 features and functionality were found to meet applicable FDA 21 CFR Part 11 requirements, according to a third-party assessment by Protocol Link. The assessment report is available upon request. All clients are encouraged to conduct an on-site audit of our Software Development Life Cycle (SDLC), as well as Development and Validation practices.

Requirements

To use the i-Vu® Pro v8.5 for Life Sciences features you must:

- Be running i-Vu® Pro v8.5 with a i-Vu® Pro for Life Sciences license
- Have the latest cumulative patch installed

Life Sciences best practices

Upgrading from a previous version of i-Vu® Pro

To convert a customer's license from a previous version of i-Vu® Pro (CIV-OPNPR) or i-Vu® Pro Unlimited (CIV-OPNPRUL) to i-Vu® Pro for Life Sciences v8.5 (CIV-OPNPRLS), contact your Carrier Regional Sales Manager. For general upgrade instructions see the *i-Vu® Pro v8.5 Upgrade Guide*.

Follow the steps below to ensure your system's previously validated drivers and programs are successfully transferred to the new, upgraded system.

Before performing the upgrade

- For controllers with sufficient memory, download source to the controller for ability to recreate the original programming by uploading from the controller.
- Control program names should contain the version number of your program to allow recognition of program differences.
- Run an equipment report
    - If upgrading from v7.0 or later, use custom report *Programs and Drivers* to list control program names and driver versions. To download the template for this report, see the *Carrier Partner Community* web page.
    - If upgrading from a version earlier than v7.0, use the *Equipment Checkout* report to list program names. There is no report for driver versions.

After performing the upgrade:

Run the equipment report again to compare against the report you ran before the upgrade.

Network and server security

Review the *Security Best Practices for an i-Vu® Pro v8.5 system* document and utilize the **Security Checklist** to configure the system securely and in compliance with site requirements.

System access policies

In addition to the user recommendations in the *Security Best Practices for an i-Vu® Pro v8.5 system* document, implement site system access policies in accordance with the site's requirements.

- On the **System Settings** > **Security** tab, configure or confirm the following:
  - Establish password policies, including complexity, reuse, and expiration requirements
  - Lock out operators after a specified number of failed attempts
  - Log out operators after a specified period of inactivity
- The LDAP/AD add-on is included with the i-Vu® Pro for Life Sciences license. This add-on can be used to authenticate operators using their i-Vu® Pro login names and LDAP/AD passwords. This enables the site's IT staff to manage password policy according to site IT policies.
- On the **System Options** > **Operators** tab, it is recommended that:
  - **Force user to change password at login** is selected to facilitate password secrecy for new operators
  - **Do not use automatic logoff for this operator** and **Exempt From Password Policy** are not selected for any operator
  - Run the **Security** > *Operator Information* report to determine if any existing users are exempt from **Automatic Logoff** or the system's **Password Policy**, and whether an operator can e-sign reports.
- Adding, editing, and deleting system operators is recorded electronically in the audit log.
- Periodically check for inactive or unused accounts and remove them.
  1. Go to the **System Options** > **Operators** tab.
  2. Run the **Security** > *Operator Information* report.
     NOTE A security report using the `sreview` manual command is also available. Review the following items.
     - Operators never logged in: ###
     - Operators last login > 180 days: ###
- Optionally, site specific procedures and third-party tools can be used, if required, to further control and monitor i-Vu® Pro access, for example:
  - Restrict access to a defined range of IP addresses.
  - Enable intrusion protection at the hardware level of the website server.
  - Record intrusion events in the server's monitored event logs.

Role-based access privileges

- On the **System Options** > **Privilege Sets** tab, establish role-specific privilege profiles to be assigned to individual operators.
- On the **System Settings** > **Security** tab, it is recommended that:
  - Location-dependent security is selected to limit operator privileges to the areas of the system that they are authorized for.
  - Strict operator log off, lock out, and password rules are configured.
- Ensure only authorized individuals are given the privilege to sign reports. Electronic signatures uploaded for use within the system are intended to be the legally binding equivalent of traditional handwritten signatures. The *Operator Information* report shows which operators can e-sign reports, which privilege sets they have, and their starting location.

- Ensure only authorized individuals are given the "Engineer System" privilege, which allows them to configure semantics tags for the *Out of Range* report.
- Disable the “Delete Non-Critical Alarms” and “Delete Critical Alarms” privileges for all operators to ensure that all alarms are represented on reports.

Establish policy for retaining audit trail information

- On the **System Settings** > **Security** tab, configure the system to **Log Audit Data to Database**. Configure the audit log retention period to comply with site retention policies.
- For each critical equipment for which change reasons should be captured in the audit log, on the **User Tree**, right-click the equipment, and select **Configure** from the drop-down list. Then, select the **Require operator to record any changes to control program and when acknowledging alarms** checkbox.

  NOTE In order to record change reasons for alarm acknowledgment, for each required alarm you must also enable **Alarm requires acknowledgment** or **Return requires acknowledgment** (or both).

Backup and restore

Ensure that your site has established adequate backup and restore procedures. See "To back up a system" in the *i-Vu® Pro v8.5Installation Guide*. If required, third-party software such as Neverfail can be utilized to configure a system for high availability.

Validate security settings

Run a security report using the `sreview` manual command. Use the resulting report to compare your configured settings to the recommended settings found in the *i-Vu® Pro Security Best Practices v8.5* document.

Verify Out of Range report parameters

Out of Range report parameters must be configured as semantic tags. See "To Configure Out of Range reports with Semantics" in the *i-Vu® Pro v8.5 Help* for details on report parameters.

To verify that the expected parameter values have been used for your scheduled Out of Range report, you can schedule one of the "Out of Range Tags" custom reports to run concurrently with your Out of Range report. To download the templates for these reports, see the " Support > Download > Training Materials > Custom Reports" section of the *i-Vu® Systems* web page.

Daylight Saving Time transitions

During certain Daylight Saving Time events, controller trend data may be preserved by quarantine at the server. A *Quarantine Summary* report indicates where quarantined data may exist in a system. The *Trend Value* report has an option to report on quarantined data.

Document revision history

Important changes to this document are listed below. Minor changes such as typographical or formatting errors are not listed.

Date	Topic	Change description	Code*
		No changes yet	

* For internal use only