LabVIEW™ Datalogging and Supervisory Control Module Run-Time System

Version 6.0

Welcome to the LabVIEW Datalogging and Supervisory Control module Run-Time System, the LabVIEW solution for all kinds of distributed data logging and automation needs. These release notes describe system requirements and installation. They also contain information that was not available for inclusion in the printed documentation, and a list of known issues.

Contents

Installation

The following sections describe how to install the LabVIEW Datalogging and Supervisory Control module Run-Time System on your computer.

Installing the LabVIEW Datalogging and Supervisory Control Module Run-Time System

1. Insert the LabVIEW Datalogging and Supervisory Control module Run-Time System CD in your CD-ROM drive
2. Run the installer as follows:
   a. If your computer system has the AutoPlay feature enabled, the installation will begin automatically.
   b. If your system does not use AutoPlay, run the following program:

      `x:\LabVIEW DSC Run-Time System Installer.msi`

      where *x* is the letter of your CD-ROM drive.
3. Follow the onscreen instructions.
4. Reboot your computer.

Required System Configuration

The LabVIEW Datalogging and Supervisory Control module Run-Time System runs on any system that supports Windows 98/95, Windows NT 4.0, or Windows 2000. A minimum of 32 MB of RAM and at least 60 MB of free disk space (for the system to use as swap space) is required for this version to run effectively. We recommend 128 MB of RAM and at least 127 MB of swap space available on your system. Increasing your computer resources will have a significant effect on performance of LabVIEW Datalogging and Supervisory Control module applications.

Additional Installations

In addition to the LabVIEW Datalogging and Supervisory Control module Run-Time system itself, you might need to install additional drivers for use with your application software during the LabVIEW Datalogging and Supervisory Control module Run-Time System setup. You might also need to install additional data servers for your application software. Consult the documentation for your application software for installation instructions.

Install the Application Software

Follow the instructions provided by the system developer for installing the application software. After installing the files, note the location of the `.scf` and `.ccdb` files.

Install the Required Servers

If your application software uses the NI-DAQ Server for LabVIEW, install the NI-DAQ Server from the LabVIEW Datalogging and Supervisory Control module Run-Time System CD. Other servers must be installed separately.

Update Preference Files

Consult the documentation for your application software to ensure any specific preference files for the application are placed in the correct locations. These files contain non-default settings for LabVIEW Datalogging and Supervisory Control module utilities such as `htv.ini`. You can edit these files with a simple text editor such as Notepad. Specific instructions about these preference files should be included with your application software.

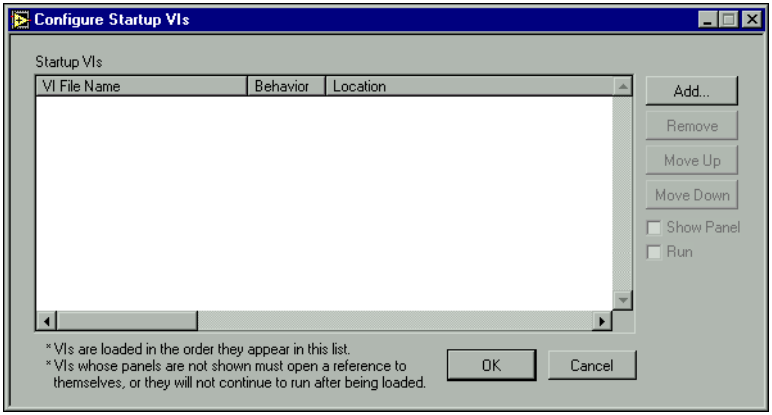
Finish Server Setup

If you are using National Instruments IAS/IAK device servers, you might need to resolve the paths to the servers stored in the `.ccdb` file. Use the Server Explorer to do this. The Server Explorer is installed when you install the LabVIEW Datalogging and Supervisory Control module. Start the Server Explorer from your Windows program menu or from the Tag Configuration Editor, select **File»Open…**, locate the `.ccdb` file for your application software, and choose **File»Set this file as Active CCDB**.

VI-based servers (if used by your application) provide their own Server Registration VIs, as described in your application software documentation.

Configure LabVIEW Startup

Launch the LabVIEW Datalogging and Supervisory Control module Run-Time System. The first time you run it, you might want to configure one or more startup VIs, as shown in the illustration below. These startup VIs are the user interface panels that appear when you launch the Run-Time System. Use the **Select Tools»Datalogging & Supervisory Control» Advanced»Startup VIs**. Use the Configure Startup VIs dialog box to locate the appropriate startup VIs, as identified in your application software documentation.



If your application starts the engine when it launches, and the servers are not registered properly, you will receive error messages identifying the servers that did not start. Consult your application software documentation for more information about which servers are required, and how to register them.

Known Issues

The following known issue exists in the LabVIEW Datalogging and Supervisory Control module Run-Time System, Version 6.0.

Tag Monitor Security

When you start the Tag Monitor from LabVIEW, the user currently logged in is set as the active user in the Tag Monitor. If the Tag Monitor continues running when a new user logs into LabVIEW who also has access to the Tag Monitor, the active user in the Tag Monitor *will not* change. In other words, User A will be logged into Tag Monitor while User B is logged into LabVIEW. You can always verify which user is logged into the Tag Monitor by examining the status bar at the bottom of the Tag Monitor window.

In certain situations, this may lead to undesired access to tag data. However, you can configure which users and groups have access to the Tag Monitor itself. If the user who logs in to LabVIEW does not have access to the Tag Monitor, the Tag Monitor will close.

At this time, the Tag Monitor does not support a direct login mechanism. However, if you launch the Tag Monitor from the command line, the following command line arguments are supported:

```
Tagmonitor.exe ["filename"] [-usr "username"] [-pwd
"password"]
```

`filename`	Fully qualified path to a Tag Monitor configuration file you have saved in the past; filenames with spaces must be enclosed in quotation marks
`-usr`	User login name; the user name must be enclosed in quotation marks
`-pwd`	Password for the user account specified with –usr; the password must be enclosed in quotation marks, and should not contain quotation marks within it

Corrections and Additions to LabVIEW Datalogging and Supervisory Control Module Run-Time System Documentation

The following sections contain information that has changed or that was unavailable for inclusion in the printed LabVIEW Datalogging and Supervisory Control module Run-Time System documentation.

Using the LabVIEW Application Builder with the LabVIEW Datalogging and Supervisory Control Module

You can create applications from VIs that use the LabVIEW Datalogging and Supervisory Control module using the LabVIEW Application Builder. When you install the Application Builder, the **Build Application** feature becomes available in the **Tools** menu.

If your application does not use any LabVIEW Datalogging and Supervisory Control features, you may use the Application Builder as you would with any LabVIEW application. If your application takes advantage of the features the LabVIEW Datalogging and Supervisory Control module adds to LabVIEW, you can still use the Application Builder to create an executable program using your VIs. However, additional software and files will be necessary for it to function correctly.

Building your Application

Before using the Application Builder with the LabVIEW Datalogging and Supervisory Control module, *you must install a patch* to enable the Application Builder to work with LabVIEW Datalogging and Supervisory Control module features. Install this patch by running the `Apply Application Builder Patch.vi`, located in:

`vi.lib\lvdsc\System\_distpatch.llb\Apply Application Builder Patch.vi`

This patch ensures that the Application Builder includes the correct VIs in your application. If not applied, your application may be missing VIs, or the Application Builder may fail to complete building your application.

After installing the patch, you build your application the same way as you would build any other LabVIEW application.

If your program uses VIs specific to the LabVIEW Datalogging and Supervisory Control module, the LabVIEW Datalogging and Supervisory Control Run-Time system must be installed on the computers you plan to run the application on. A dialog box reminding you of this pops up when the Application Builder finishes the build.

The Application Builder excludes VIs specific to the LabVIEW Datalogging and Supervisory Control module from the built application because they must be correctly installed on the target computer. The LabVIEW Datalogging and Supervisory Control Run-Time System correctly installs the LabVIEW Datalogging and Supervisory Control VIs as well as additional required software, providing all of the configuration tools, the Tag Engine, historical data logging, network data access, security, and other features provided by the LabVIEW Datalogging and Supervisory Control module.

What to Include with Your Application

You should include all VIs you have written for your application, as well as any external data files. For LabVIEW Datalogging and Supervisory Control–based applications, these files will commonly include:

- Tag configuration (`.scf`) files
- Preference files (`.ini`, `.cfg`) from the LabVIEW directory
- Hardware configuration files (such as `.iak` files for FieldPoint, MAX configuration data, and so on)
- The common configuration database file (`.ccdb`). This file can be identified by examining the title bar of the Server Browser utility (**Tools»Datalogging & Supervisory Control»Advanced»Server Browser**), or by examining the following value in the Windows Registry key:

  ```
  HKEY_LOCAL_MACHINE\Software\National
  Instruments\NI-Servers
  Value: Active CCDB
  ```

- Server software for all servers your application depends on for data. You may have to register VI-based servers yourself.

Other Information

Notice that for your application to work, you must put it in the same directory where you installed the LabVIEW Datalogging and Supervisory Control Run-Time System. This directory will contain `DSCRTS.EXE`. You will not need to run this executable if you have built your own.

Special Note Regarding the Security VIs

Some applications may only make use of the Security VIs available with the LabVIEW Datalogging and Supervisory Control module, and not any other of the module's VIs. These VIs may be redistributed without the LabVIEW Datalogging and Supervisory Control Run-Time System, but require that you include certain other VIs along with your executable application.

First, you must create a subdirectory called `vi.lib` in the same directory into which you install your application. The following files must be copied into `vi.lib` for security to work correctly:

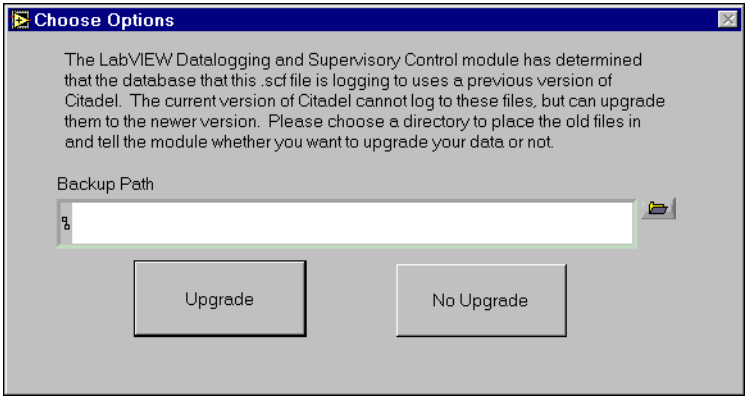
File or Directory Name	Destination Directory	What to Copy
`lv_init.vi`	`vi.lib`	file
`extensions\_core\*`	`vi.lib\extensions`	entire subdirectory
`extensions\LVSecurity.vi`	`vi.lib\extensions`	file
`extensions\_security_stubs.llb`	`vi.lib\extensions`	file
`extensions\security\*`	`vi.lib\extensions`	entire subdirectory

To include the **Security** submenu in your application's **Tools** menu, you should also create a `project` directory in your application's main directory. Then, copy the `LabVIEW\project\lvdsc\Security` folder into your application's `project` directory.

Citadel Historical Database File Conversion

The Citadel database has changed from the previous version used with BridgeVIEW or Lookout (earlier than 4.0). You can convert old database files to maintain data continuity, or you can start a new data directory and keep your old data segregated from new data.

The LabVIEW Datalogging and Supervisory Control module includes a conversion utility that opens automatically when you open a tag configuration file from BridgeVIEW or set the logging directory to a directory already containing an old database. The following dialog box appears, to guide you though the conversion process.



You may opt to convert your old database files or not to convert them.

Whether you convert your data or not, your old data is maintained by LabVIEW, which moves your old data files to a new location based on the path you enter in the **Backup Path** field. If you do not enter a new directory or path, LabVIEW will move the old data files to a subdirectory of your original data directory called `archive`.

If you chose to convert your old data files to the new format, LabVIEW will then convert your files. The amount of time for this process depends on the amount of data that needs to be converted. LabVIEW will then create a new database containing your old data.

If you choose not to convert your old data files, LabVIEW begins logging data in the new format to the same data directory it used before, starting with an empty database.

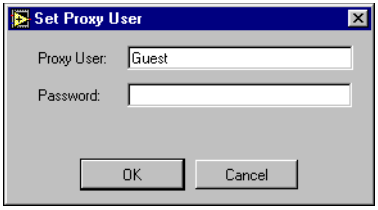
Note One effect of the data conversion process is that the updated data will show that all tag values were produced on the computer that did the conversion, even if the original data for the tags came from a number of different computers on your network. New data being logged will show the proper URL source for the data.

Network Data Access

To better control access to your data by anonymous network users, new configuration options have been added to the **Engine Configuration** options in the Tag Configuration Editor. Configuration options for a *proxy user* and *engine user* provide more flexible control over network access to data. You can also configure these options from **Tools»Datalogging & Supervisory Control»Options** in the **Advanced** tab. You must be logged on as an Administrator to change these options.

Proxy User

The proxy user is the account used for anonymous access to your data. You must specify the user name and password to use for the proxy user. The default setting for the proxy user is to use the built-in Guest user account, which has no password unless you add one.



The proxy user access rights take effect under the following conditions:

- No user is specified by the client attempting to connect to data in the Tag Engine
- An unrecognized user is specified by the client attempting to connect to data in the Tag Engine

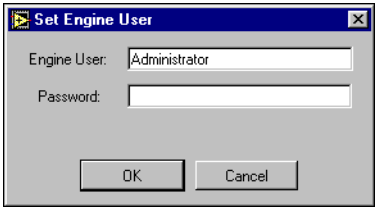
Examples of situations in which network data access security is enforced are:

- A DataSocket connection to tag data
- If the LabVIEW Datalogging and Supervisory Control module is installed with LabVIEW, the currently logged on user is used to determine access rights to tags in the Tag Engine, or to tags in other National Instruments Logos networking servers, such as Lookout or FieldPoint FP-1600 network interface modules
- If the LabVIEW Datalogging and Supervisory Control module is not installed, no user is specified
- From applications other than LabVIEW, no user is specified
- Any Lookout connection to a tag in the Tag Engine uses the current user in Lookout
- Any tags in another, separate Tag Engine that are connected through Logos networking to tags in the local Tag Engine use the engine user account on the remote computer

Engine User

The engine user is specifically used by the Tag Engine when a locally defined tag makes a connection to a National Instruments Logos networking data source. This configuration option is available to you because you may find it necessary to have access to tag values no matter who is operating the system. For example, a simple control rule may need to execute regardless of the user who is active in the system. For this reason, write access to the control tag must be guaranteed, no matter who the currently logged-in user might happen to be.

To configure the engine user in the Tag Configuration Editor, choose **Configure»Engine** and select the **System** tab. Click the **Engine User** button, and provide the user name and password for the account to use. The default setting is to use the built-in Administrator account.



To configure the engine user in the LabVIEW Datalogging and Supervisory Control module options, choose **Tools»Datalogging & Supervisory Control»Options** and select the **Advanced** tab. Click the **Engine User** button, and provide the user name and password for the account to use. The default setting is to use the built-in Administrator account.

Note If you change the password for the user account specified as the proxy user or engine user, you must re-apply these settings with the new password.

More Information and Updates

For information on LabVIEW Datalogging and Supervisory Control module updates and changes in the future, point your browser to

`ni.com/labviewdsc/`

To download the newest patches and other updates, see the National Instruments Software Library at

`http://digital.ni.com/softlib.nsf/web/all+software`

322956A-01 Oct00