June 2024

LabVIEW Configuration for Secure Applications

Summary

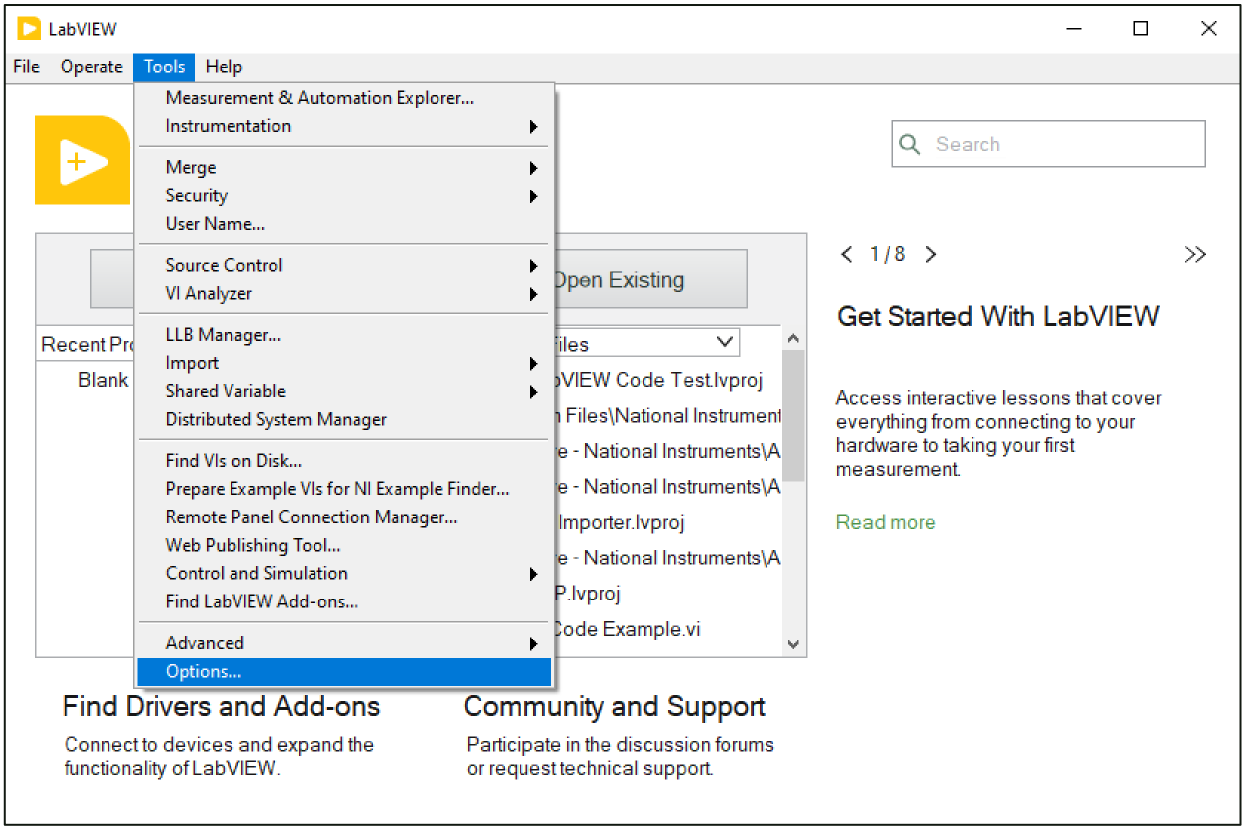
Developers using LabVIEW in some applications may require specific configurations to adhere with security controls. This document is designed to meet the requirements of NIST 800-53 rev5 and includes specific configuration recommendations for the LabVIEW Development environment. This applies to Base, Full, and Professional editions of LabVIEW.

This document was updated for use with LabVIEW 2024.

LabVIEW Configuration - Tools Options

LabVIEW configuration is performed from any LabVIEW screen with the toolbar visible.

Click Tools - > Options….



Get Started With LabVIEW

Access interactive lessons that cover everything from connecting to your hardware to taking your first measurement.

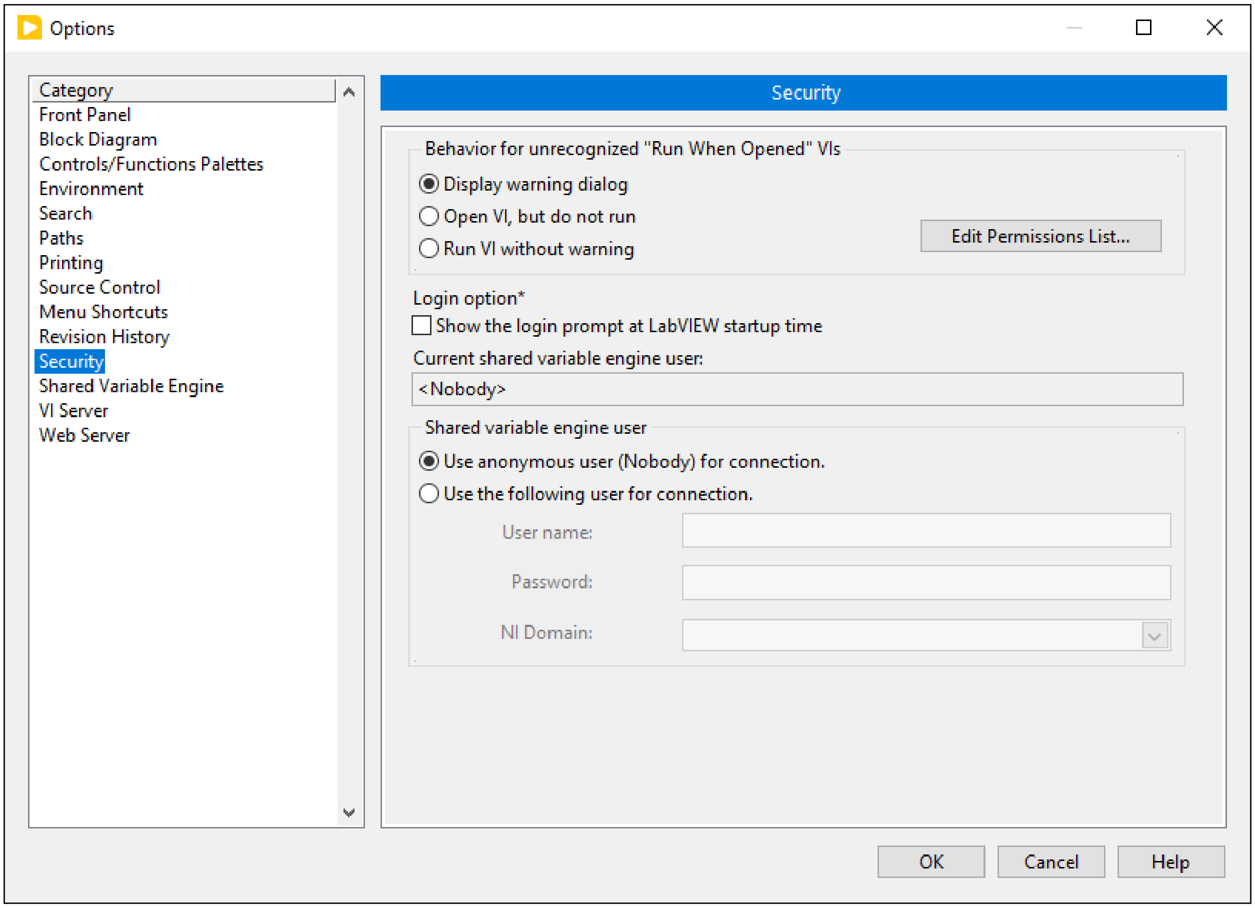
Find Drivers and Add-ons

Connect to devices and expand the functionality of LabVIEW.

Community and Support

Participate in the discussion forums or request technical support.

The Options menu is divided into 14 categories. Options for security are mostly found in the Security category, but some options that impact security may be found in other categories as identified below.



Security

Behavior for unrecognized "Run When Opened" VIs

● Display warning dialog

○ Open VI, but do not run

○ Run VI without warning

Login option*

□ Show the login prompt at LabVIEW startup time

Current shared variable engine user:

<Nobody>

Shared variable engine user

● Use anonymous user (Nobody) for connection.

○ Use the following user for connection.

User name:

Password:

NI Domain:

Category	Configuration Item	Description
Environment	Clear Password Cache	LabVIEW VIs can be locked using a user-defined password to prevent unauthorized users from viewing the source code in a program. When a user opens a locked VI, that user is prompted for the password. If successful, LabVIEW stores that password in a cache so that the user does not need to repeat the password on that computer. Clicking “Clear Password Cache” in this screen removes all of the passwords used so that the next user will need to re-enter the password. **For secure applications: C**lick this button at the end of each session where a password is used to unlock a VI.
Paths		When a VI is loaded into memory, LabVIEW looks for subVIs in directories as defined in this category. To reset this, check “Use Default”, or use trusted file locations. **For secure applications:** Verify that these paths have not been changed so that code is loaded from expected sources.

Revision History	Add Comments to VI Revision History	Using these options, a user can force the developer to enter comments and update the revision number each time a VI is saved or closed. **For secure applications**: Enable all of these options.
Revision History	User Name to Record in VI Revision History	When a comment is recorded, LabVIEW will record a user name. Depending on this option, it will record either the name associated with the LabVIEW registration, or with the OS user account. **For secure applications:** Check the OS user account option, and ensure that the computer account is not shared among users.
Security	Behavior for unrecognized “Run When Opened” VIs	VIs are stored as <name>.vi files. Users open these in the LabVIEW environment to edit the source code. There is an option with each VI to set it to “Run when opened.” **For secure applications:** Disable this behavior by selecting “Open VI, but do not run.” This will ensure that the user knows what code will run before running it.
Security	Login Option	LabVIEW has basic user tracking. By default, LabVIEW uses the Operating System user name as the LabVIEW user name. Selecting this option will force users to login as a user when LabVIEW is launched. For more information, see the LabVIEW User Accounts section below. **For secure applications:** Do not use LabVIEW user accounts for secure applications.
Security	Shared variable engine user	When using network shared variables, LabVIEW uses an anonymous user (Nobody) for the connection. When a system is configured to require a user to login as part of a shared variable connection, the account information can be entered here. For more information about using shared variables, visit https://www.ni.com/en-us/support/documentation/supplemental/06/using-the-labview-shared-variable.html#section--742452614 **For secure applications:** Leave this option as Use anonymous user. Change this only when used with an understanding of Shared Variable Engine security.
VI Server	Protocols	VI Server is a service that allows remote execution of the LabVIEW Development environment. By default, TCP support of VI Server is deactivated. **For secure applications:** Keep this box unchecked. By default, the ActiveX option for VI Server is enabled. **For secure applications:** Uncheck this box.
VI Server	Accessible Server Resources	These checkboxes control which features are available through VI Server when it is activated. **For secure applications:** Uncheck all four of these boxes.
VI Server	Machine Access	When activated, only the machines in this list have access through VI Server. By default, the local machine ID is allowed.

		For secure applications: Remove all machines from this list.
VI Server	User Access	When activated, users in this list have access through VI Server from any machine. By default, no users are allowed (users must access from an approved machine). **For secure applications:** Remove all users from this list.
Web Server	NI Web Server	By default, the Web Server is not activated. Clicking this button will let users configure the Web Server. If the Web Server is required for a secure application, configure the Web Server for “Secure remote access.” If the Web Server is not required, do not configure any access. **For secure applications:** Do not configure this access.
Web Server	Application Web Server	By default, the application web server is not activated. **For secure applications:** Do not activate this service without additional research into the web server security requirements.
Web Server	Remote Panel Server	The Remote Panel Server can publish images of the front panel of the LabVIEW program across the network. If this is required for an application, research proper security configurations for the server, including SSL. **For secure applications:** Leave this server box unchecked.

LabVIEW Services

The following services are installed as part of the LabVIEW installation, and start automatically with each Windows boot:

lkClassAds	NI PSP Service Locator
lkTimeSync	NI Time Synchronization
niauth	NI Authentication Service
NIDomainService	NI Domain Service
nimDNSResponder	NI mDNS Responder Service
NiSvcLoc	NI Service Locator

Stopping these services will impact parts of the LabVIEW functionality, it is not recommended to stop these services without first referring to the LabVIEW documentation at https://ni.com/docs.

LabVIEW User Accounts

LabVIEW has basic user management. Using the options in Tools -> Security -> Domain Account Manager, a user can configure accounts to log in. However, these accounts are only used within the

LabVIEW Data & Supervisory Control (LabVIEW DSC) package. LabVIEW Base, Full, and Professional do not use these accounts or enforce restrictions based on who is logged in.

Users can create programs with a database for user management, and must use this information in their LabVIEW program to manage access and rights. This requires experience with security applications and takes significant time.

If your application requires user management, NI recommends that you consider an automated test management tool like TestStand, or using a 3rd-party tool like the DMC UI palette, part of the DMC Flex Framework. See more information at https://www.dmcinfo.com/latest-thinking/case-studies/view/id/479/adding-user-authentication-to-your-labview-project.