InstrumentStudio Secure Configuration Guide

Emerson T&M

Release: 1.0

September 20, 2025

CONTENTS

Prepared By

Emerson
8027 Forsyth Boulevard
Saint Louis, Missouri 63105
USA

Revision History

Date	Version	Description
10/01/2025	1.0	Initial release of document

How to Contact Us

For questions about this document, contact security@ni.com.

CHAPTER

ONE

PURPOSE

This guide describes how to secure InstrumentStudio. It is intended for users who are responsible for setting up InstrumentStudio in their organization. The guide provides recommendations to help you secure your installation of InstrumentStudio and ensures that the installation meets the security requirements of your organization.

While the recommendations are based on the 2025 Q4 release of InstrumentStudio, they are applicable to other versions unless otherwise noted. NI recommends that you consult version-specific documentation where available, especially when using significantly older releases. Other NI drivers or products installed by InstrumentStudio are not covered by this guide and might have their own Secure Configuration Guides.

CHAPTER

TWO

WINDOWS

InstrumentStudio Plugins

InstrumentStudio can host plugins written in LabVIEW or C# to extend the functionality of InstrumentStudio for application-specific needs. Plugins allow for arbitrary code to run in the InstrumentStudio environment, which might impact the security of InstrumentStudio. Ensure that all plugins that you install are trusted.

By default, plugins are installed in the **Addons** directory in the InstrumentStudio install location. A custom plugin location can be specified through **File » Preferences » Plugins**. Specifying a custom plugin location requires write access to the InstrumentStudio folder. The custom location is stored in the **ProtectedPreferences.xml** file, which is found in the same directory as the InstrumentStudio executable. The custom location can reference any file path. Ensure that only authorized users and trusted processes are allowed to modify or access the updated location.

Measurement Plug-Ins

InstrumentStudio supports the display of measurement plug-ins as panels in the InstrumentStudio environment. Measurement plug-ins are reusable measurements that are written in Python or LabVIEW. A measurement plug-in runs as a service, so its execution is separate from the InstrumentStudio application. The same measurement plug-in can be used by both InstrumentStudio and TestStand.

InstrumentStudio automatically discovers measurement plug-ins that are locally available or available through an NI Plug-In Library. Panels can be created for measurement plug-ins through the **Edit Layout** dialog in InstrumentStudio. When a measurement plug-in panel is created or an existing panel is loaded, InstrumentStudio automatically executes the code in the associated measurement plug-in service. InstrumentStudio can also monitor calls to measurement plug-ins that are made by other applications, such as TestStand.

Before installing a measurement plug-in or accessing one through an NI Plug-In Library, ensure that the measurement plug-in is trusted. A measurement plug-in service can run code and access files based on the permissions available to the service.

Applications communicate with measurement plug-ins through the gRPC interface. Measurement plug-ins only allow localhost connections but anyone with machine access can communicate with a measurement plug-in through the gRPC interface.

Remote Connections

InstrumentStudio supports connecting to remote hosts for the following use cases:

- Creating panels for remote instruments using the NI gRPC Device Server
- Downloading measurement plug-ins from an NI Plug-In Library

The connection to the remote host is not secure in these cases. Data is not encrypted and user authentication is not required. The connection only requires that InstrumentStudio has access to the remote host and that the host allows the connection. We strongly recommend only connecting to trusted hosts on a secure network.

The servers for the NI Plug-In Library and NI gRPC Device Servers can be configured to only accept connections from expected client machines. See the user manual for these applications for more information.

When installed, InstrumentStudio does not specify any remote connections. If a user adds a remote connection, InstrumentStudio remembers the connection configuration and automatically connects during future launches of InstrumentStudio if necessary.

The configured connections can be viewed and modified through **File » Preferences » Remote connections**.

Services

The table below lists the services that InstrumentStudio installs.

Service Name	Display Name
NI.Discovery.V1.Service.exe	NI Discovery Service
NI.GrpcDeviceServerActivationService.exe	NI gRPC Device Activation Service
NI.IODiscovery.V1.Service	NI I/O Discovery Service
NI.Monitoring.V1.Service	NI Monitoring Service
NI.ParameterPassing.V2.Service.exe	NI Parameter Passing Service
NI.PinMap.V1.Service	NI Pin Map Service
NI.Scpi.V1.Service	NI SCPI Service
NationalInstruments.Sequencing.WebServer	NI Sequencing WebServer
NationalInstruments.SequencingService	NI Sequencing Service
NI.SessionManagement.V1.Service	NI Session Management Service

Additional Considerations

This section provides additional considerations when securing a system with InstrumentStudio installed. These are optional, but they can help you improve the security of your system.

Installing the Latest Components

NI Package Manager does not always install the latest versions of dependencies, especially when upgrading. To ensure that you have the latest security fixes and dependency versions, do the following steps:

1. Open NI Package Manager.
2. Select the “Updates” tab.
3. Update all items shown.

Update Service

If you do not want Update Service to run, you can prevent it from installing automatically. If Update Service is already installed, you can disable it. For more information, see How to Disable or Prevent Installation of NI Update Service.

NOTE: You will no longer receive critical Windows security update notifications. You must manually check for and install any critical security updates as outlined in *Installing the Latest Components*.

Customer Experience Improvement Program

The Customer Experience Improvement Program is enabled by default after installation. The program collects usage data that helps improve NI products. To see if this program is installed, open the Windows Start Menu and go to **All Programs » National Instruments » NI Customer Experience Improvement Program**. If this location does not appear, the program is not installed.

If the program is installed and you want to opt out of data collection, follow the instructions at NI Customer Experience Improvement Program.

NI Error Reporting

NI Error Reporting allows you to send crash reports and internal warning reports that are related to NI products. For information on how to disable NI Error Reporting, see How Do I Disable NI Error Reporting (NIER).

Hardware Configuration Utility

Overview

The Hardware Configuration Utility (HWCU) is a tool designed to assist users in configuring and managing hardware settings on both their local system and remote network devices. It provides a user-friendly interface for accessing various hardware-related options and features, making it easier for users to optimize system performance and troubleshoot hardware issues across multiple devices.

Password Protection

Any network hardware, including NI Linux Real-Time (RT) systems, should always be configured with a strong password to protect against unauthorized access. Setting a password helps ensure that only trusted users can modify system settings, access sensitive data, or perform administrative tasks. Without a password, the system is vulnerable to security breaches, which could compromise hardware, data integrity, and network safety. For best practices, choose a password that is complex and unique, and update it regularly to maintain robust security.

Location Information in ToolTips

When connecting to remembered remote systems, you can check that that cached information is correct by hovering over the name in the connection drop down. This will display the location information for the selected system. This allows confirmation of the remote system's identity and location before connecting.

Offline install

Offline installation is a mechanism for installing software onto a NI Linux RT system that does not have internet access. To use this feature, you must first install the *NI Linux Real-Time Offline Installation Support* package on the host computer. Once the package is installed, the offline installation workflow is initiated from HWCU when you open the manage software dialog for a connected NI Linux RT device. During this workflow, HWCU will prompt you to start a temporary web server and select a port (default: 9100). The web server hosts installation files for the RT system and only runs while the manage software dialog is open; it stops automatically when the dialog is closed.

> **Note**
>
> Offline installation is only supported for NI Linux RT systems that are not configured for SNAC mode.