NI-DAQmx 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
07/01/2025	1.0	Initial release of document

How to Contact Us

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

CHAPTER

ONE

PURPOSE

This guide covers how to secure NI-DAQmx on Windows, Desktop Linux, and NI Linux RT. It is intended for those who are responsible for setting up a system using NI-DAQmx in their organization. The guide provides recommendations to help you secure your NI-DAQmx installation and ensures that it meets your organization's security requirements.

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

CHAPTER

TWO

PREREQUISITES

This section includes a list of prerequisite steps to apply additional security configurations that may be applicable depending on your application.

- LabVIEW Product Security.
- NI Linux Real-time Security User Guide.
- SystemLink Product Security.
- NI-Measurement and Automation Explorer (MAX) Remote System Security
- NI Hardware Configuration Utility (HWCU) User Manual

CHAPTER

THREE

WINDOWS

Services

The following table documents services that NI-DAQmx installs and uses on Windows.

Service Name	Display Name	Log On As
lkClassAds	NI PSP Service Locator	NT Service\lkClassAds
mxssvr	NI Configuration Manager	Local System
nidevldu	NI Device Loader	Local System
NINetworkDiscovery	NI Network Discovery	Local Service
nipal	NI Core Driver Services	NT Service\nipal
nipxicmsvc	NI PXI Chassis Management Service	Local System
nipxirmu	NI PXI Resource Manager	Local System
niroco	NI Route Coordinator	NT Service\niroco
nisds	NI Sync Domain Service	Local System
NiSvcLoc	NI Service Locator	Local Service
NISystemWebServer	NI System Web Server	Local System
NITaggerService	NI Variable Engine	Local System

Stopping these services will impact parts of the NI-DAQmx functionality, it is not recommended to stop these services.

Windows Install Locations

This section documents files that NI-DAQmx installs to shared or common locations. The documentation and example files are installed as writable, but shouldn't be a significant security risk based on the nature of those files.

- NI-DAQmx user documentation is installed to `C:\Users\Public\Documents\National Instruments\NI-DAQ\Documentation`

- NI-DAQmx C, CVI, and .NET examples are installed to `C:\Users\Public\Documents\National Instruments\NI-DAQ\Examples`
- Some NI-DAQmx .NET configuration and binaries are installed to the .NET Framework Global Assembly Cache (GAC).

Additional Considerations

This section provides additional considerations when securing a system that uses NI-DAQmx. These considerations are not required for the API to function, but they can help you avoid common pitfalls and improve the security of your system.

Installation

Install only the packages you will need. This includes installing only the ADE support for the languages you need. For example, if you are only developing in LabVIEW, do not install the "NI-DAQmx Support for .NET Framework" or "NI-DAQmx Support for C" packages.

If you will need to configure NI-DAQmx hardware, such as renaming devices, you will need to install *NI Hardware Configuration Utility* package.

NOTE: Python support is not available in the NI-DAQmx installer. You must install Python support from *nidaqmx-python* package on PyPI. It does not require any additional ADE support to be installed.

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.

Firewall

NI-DAQmx PCI, PCIe, PXI, PXIe, and USB devices are not affected by Windows firewall settings. See *Ethernet cDAQ Devices* for more information on firewall configuration for ethernet cDAQ devices.

CHAPTER

FOUR

DESKTOP LINUX

Services

The following table documents services that NI-DAQmx installs and uses on Linux Desktop.

Service Name	User	Description
nidevldu	root	NI Device Loader Service
nidrum	root	NI User-Mode Driver Service
nimxssvr	root	NI Configuration Manager
nipal	root	NI Core Driver Services
nipxicmsd	root	NI PXI Chassis Management Service
niroco	root	NI Route Coordinator
nisds	root	NI Sync Domain Service
nisvcloc	root	NI Service Locator

Stopping these services will impact parts of the NI-DAQmx functionality, it is not recommended to stop these services.

Installation Locations

This section documents files that NI-DAQmx installs to shared or common locations. These files are installed with owner-writable-only permissions, so there aren't any specific steps to take to further secure them. However, due to the nature of the install locations, they are being called out in this section.

- Some NI-DAQmx device configuration files are installed to `/usr/share/ni-daqmx`
- Some NI-DAQmx device firmware files are installed to `/usr/share/ni-firmware/ni-daqmx`
- NI-DAQmx driver DKMS source files are installed to `/usr/src`
- NI-DAQmx Public header files are installed to `/usr/include`

- NI-DAQmx error codes and descriptions are installed to `/usr/local/natinst/labview/errors`

Additional Considerations

This section provides additional considerations when securing a system that uses NI-DAQmx. These considerations are not required for the API to function, but they can help you avoid common pitfalls and improve the security of your system.

Installation

Install only the packages you will need. This includes installing only the ADE support for the languages you need. For example, if you are only developing in LabVIEW, do not install the "nidaqmx-devel" package and only install the "ni-daqmx-labview-support" package.

If you will need to configure NI-DAQmx hardware, you will need to install the *ni-hwcfg-utility* package.

NOTE: Python support is not available in the NI-DAQmx installer. You must install Python support from *nidaqmx-python* package on PyPI. It does not require any additional ADE support to be installed.

Customer Experience Improvement Program

The "Customer Experience Improvement Program" is enabled by default upon installation and is intended to collect usage data to support the improvement of NI products.

To check for the presence of the Customer Experience Improvement Program, look for the installation directory or search for "NI Customer Experience Improvement Program". If it not available, it is not installed.

If the program is installed and you would like to opt out of participation, follow the instructions in NI Customer Experience Improvement Program.

Firewall

NI-DAQmx PCI, PCIe, PXI, PXIe, and USB devices are not affected by Linux firewall settings. See *Ethernet cDAQ Devices* for more information on firewall configuration for ethernet cDAQ devices.

CHAPTER

FIVE

NI LINUX RT

Setting up the SNAC Configuration

The NI Linux RT Secured, Network-Attached Controller (SNAC) configuration should be applied before other steps in the NI Linux RT configuration. The SNAC configuration secures the NI Linux RT target and changes some settings. For the purpose of using NI-DAQmx, the main effects are:

- WireGuard is installed
- A block-by-default firewall is installed
- NI software must be installed to RT targets using the NI Hardware Configuration Utility or the command line (the system is no longer accessible via Measurement Automation Explorer)

Services

The following table documents services that NI-DAQmx installs and uses on Linux RT.

Service Name	User	Description
/usr/bin/ni_sysmgmt_mdns_publisher	admin	NI Systems Management mDNS Publisher
/usr/bin/niminionagent	admin	NI Minion Agent Service for Systems Management
/usr/bin/nirioserver	lvuser	NI RIO Server
/usr/bin/nisds	admin	NI Sync Domain Service
/usr/bin/nisvcloc	nobody	NI Service Locator
/usr/bin/ni-sync-remote	admin	NI-Sync Remote Server Daemon
/usr/bin/nivisaserver	lvuser	NI VISA Server
/usr/lib/x86_64-linux-gnu/ni-visa/niLx	admin	NI LXI Discovery Service
/usr/local/natinst/bin/nirtmdnsd	admin	NI RT mDNS Daemon
/usr/sbin/niDAQmxRemoteService	nidaqmx	NI-DAQmx Service for Remote Configuration and Deployment
/usr/sbin/nidevldu	admin	NI Device Loader Service
/usr/sbin/nidrum	admin	NI User-Mode Driver Service
/usr/sbin/nimxs	admin	NI Configuration Manager
/usr/sbin/niroco	admin	NI Route Coordinator
/usr/sbin/nisdchassisd	admin	NI Sync Domain Chassis Daemon

Stopping these services will impact parts of the NI-DAQmx functionality, it is not recommended to stop these services.

NI Linux RT Install Locations

This section documents files that NI-DAQmx installs to shared or common locations. These files are installed with owner-writable-only permissions, so there aren't any specific steps to take to further secure them. However, due to the nature of the install locations, they are being called out in this section.

- Some NI-DAQmx device configuration files are installed to `/usr/share/ni-daqmx`
- Some NI-DAQmx and cRIO device firmware files are installed to `/usr/share/ni-firmware/ni-daqmx`
- Some C-Series module configuration files are installed to `/usr/local/natinst/share/crio`
- NI-DAQmx and cRIO UIXML files are installed to `/usr/local/natinst/share/uixml`
- NI-DAQmx and cRIO driver DKMS source files are installed to `/usr/src`
- NI-DAQmx Public header files are installed to `/usr/include`
- NI-DAQmx and cRIO error codes and descriptions installed to `/usr/local/natinst/labview/errors`

- NI-DAQmx User documentation installed to `/usr/share/doc/ni-daqmx`

CHAPTER

SIX

API SECURITY CONSIDERATIONS

NI LabVIEW

This section includes information about NI-DAQmx LabVIEW API workflows that may have an impact on the security of your system.

Data Logging to TDMS

NI-DAQmx allows you to log acquired data to a TDMS file. This TDMS file is not encrypted.

Using Channels and Tasks

Channels and tasks are fundamental components of NI-DAQmx. Channels are software entities that encapsulate the physical channel along with other channel specific information that formats the data. Tasks are collections of one or more virtual channels with timing, triggering, and other properties.

There are a few ways to create and store NI-DAQmx channels and tasks:

- Using NI-MAX or the NI Hardware Configuration Utility, you can create and store channels and tasks for use in LabVIEW. These channels and tasks are stored unencrypted.
- Using the DAQmx Save Task VI node and DAQmx Save Channel VI node, you can store channels and tasks for use in LabVIEW. These channels and tasks are stored unencrypted.
- You can also store channels and tasks that are created within a LabVIEW project. Configuration stored this way is unencrypted and saved directly to the .lvproj project file.

Calibration Passwords

The DAQmx Initialize External Calibration VI node requires the user to provide a password to perform calibration. This password is a standard string input to the API node where the string cannot be longer than 4 characters. There are default passwords for most devices that are included in the documentation for the node. Additionally, users can change the calibration password using the DAQmx Change External Calibration Password VI node. This node also accepts standard string

inputs for the current and new passwords. This password system does not provide a high level of security.

TEDS Configuration

The DAQmx Configure TEDS VI node loads a Transducer Electronic Data Sheets (TEDS) configuration file from disk and applies that configuration to a DAQmx channel. Take care when storing TEDS configuration files used with this node to ensure they have not been tampered with.

Reserve Network Device

The DAQmx Reserve Network Device VI node allows the user to override an existing reservation by using the `override reservation?` input. This poses a potential security risk since the use of a network device could be interrupted by an outside actor.

CHAPTER

SEVEN

SPECIAL CONSIDERATIONS

This section includes special considerations that should be taken when using NI-DAQmx with CompactDAQ Systems (cDAQ) to ensure that a secure environment is maintained.

Ethernet cDAQ Devices

For use-cases involving ethernet cDAQ devices (cDAQ-9189, etc.), ensure that the network is a protected network because communications between the device and host over ethernet are unencrypted and susceptible to interception.

Firewall

If you are using an Ethernet NI-DAQmx device, you may need to configure the Windows firewall to allow outbound connections to the device.

Outbound rules

By default, most firewalls allows outbound connections. If you have disabled outbound connections and are using an Ethernet NI-DAQmx device, you will need to allow connections from any port to *<device ip>:80* and any port to *<device ip>:31415*.

Inbound rules

NI-DAQmx devices do not require any special inbound rules.

USB cDAQ Devices

For use-cases involving USB cDAQ devices (cDAQ-9179, etc.), ensure that the USB connection is secure because communications between the device and host over USB are unencrypted and susceptible to interception.