VeriStand 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 VeriStand, both on Windows where the editor and gateway live and on the NI Linux RT targets where deployments normally run. It is intended for those who are responsible for setting up VeriStand in their organization. The guide provides recommendations to help you secure your VeriStand installation and ensures that it meets your organization's security requirements.

While the recommendations are based on the VeriStand 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 VeriStand are not covered by this guide and may have their own Secure Configuration Guides.

CHAPTER

TWO

WINDOWS

Paths to Secure

VeriStand allows plugins in the form of MEF plugins (for the VeriStand editor) and Custom Devices (for System Explorer and the deployed system definition). These can allow arbitrary code execution without user action other than running the editor or loading a VeriStand project.

The following folders should be set with limited permissions to prevent plugins from being improperly added or modified:

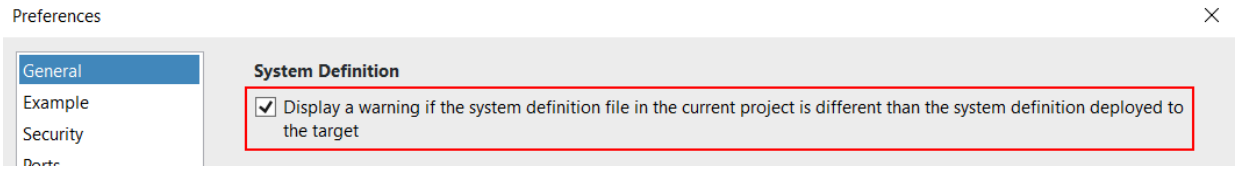
```
<Public Documents>\National Instruments\NI VeriStand 2025
<ProgramData>\National Instruments\NI VeriStand 2025
```

Editor and Gateway Configuration

In the VeriStand editor (veristand.exe), open **File > Preferences** and make sure the following options are set properly.

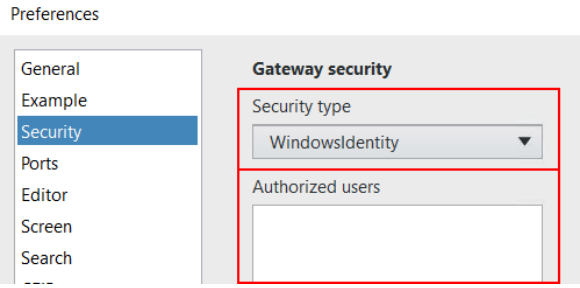
General Tab

Select **Display a warning if the system definition file in the current project is different than the system definition deployed to the target**.



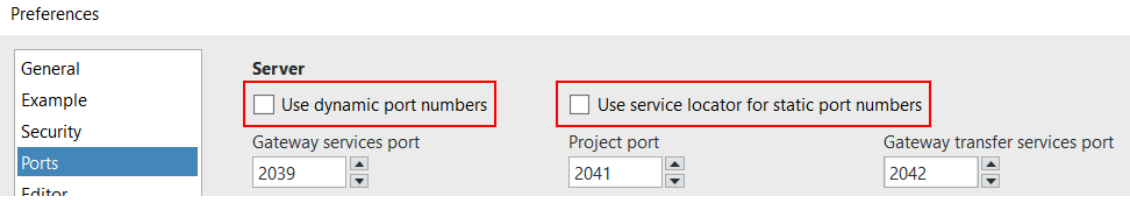
Security Tab

Make sure **Security type** is set to **Windows Identity**. This ensures the gateway's API is only accessible to authorized users. By default this is the Windows user that launched it; additional authorized users can be set in `Authorized Users` text box, in the form `[domain]\[user]`.



Ports Tab

Deselect **Use dynamic port numbers** and **Use service locator for static port numbers**.



WireGuard

WireGuard is available for Windows at wireguard.com/install. Once installed, any NI Linux RT target or other Windows machine that it will need to directly communicate with must be added as a peer.

Firewall

All ports should be blocked by default except as noted below. The open ports should only be open across the WireGuard tunnels.

The ports to open vary depending on whether the VeriStand gateway is local or remote to the machine deploying the system definition. The port numbers are configurable in the **VeriStand Editor > File > Preferences > Ports tab**.

Local Gateway (Normal Configuration)

By default, the VeriStand gateway runs on the same machine as where the system definition is being deployed from. In this case, it needs the following ports open on the relevant WireGuard tunnels:

Port Setting Name	Default Port	Open To
Gateway transfer services port	TCP 2042	All NI Linux RT targets
UDP Direct Stream Local port	UDP 56441	All NI Linux RT targets

Remote Gateway (Advanced Configuration)

In an advanced setup, the VeriStand gateway can be configured to run on a different Windows machine than where the system definition is being deployed from. In this case, it needs the following ports open on the relevant WireGuard tunnels:

Port Setting Name	Default Port	Open To
Gateway services port	TCP 2039	Windows machine deploying the system definition
Project port	TCP 2041	Windows machine deploying the system definition
Gateway transfer services port	TCP 2042	All NI Linux RT targets
UDP Direct Stream Local port	UDP 56441	All NI Linux RT targets

Additional Considerations

This section provides additional considerations when securing a system with VeriStand installed. These are optional, but they can help you avoid common pitfalls and 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.

User Education

When a user deploys a system definition, they are prompted for the WebDAV username and password (discussed in the section on configuring NI Linux RT targets), including an option to save these values. Users should be instructed not to save these values, as they are saved insecurely as plain text in the project file.

CHAPTER

THREE

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 VeriStand, the main effects are:

- WireGuard is installed
- A block-by-default firewall is installed
- NI-Auth and NI System Web Server are removed
- NI software must be installed using the NI Hardware Configuration Utility or the command line (the system is no longer accessible via Measurement Automation Explorer)

Ensure the VeriStand Engine is Installed

Install the VeriStand engine via NI Hardware Configuration Utility if it is not already installed. Some of the following steps reference folders and permissions that are created as part of its install.

Paths to Secure

VeriStand deployments run from `/c/ni-rt/NIVeriStand`. Permissions should be changed so that only `lvuser` can access it, since that is the user both VeriStand and the WebDAV server (configured later) run as.

```
sudo chmod -v -R go-rwx /c/ni-rt/NIVeriStand
```

WebDAV Setup

An alternative WebDAV provider is needed since NI System Web Server is removed by the SNAC configuration. We recommend Apache (available via the `main/core2-64` feed), since the version provided supports the all the WebDAV functions VeriStand requires and has good error logs when things don't work.

WebDAV Server Requirements

A replacement WebDAV server should be more locked down than the default NI System Web Server:

1. Don't provide any web server functionality other than what is required for WebDAV
2. Use a WebDAV-only login and not a system account that could also be used for SSH and other Operating System functions
3. Provide access only to the paths necessary for VeriStand to function: `/c/ni-rt/NIVeriStand/` and `/C/ni-rt/NIVeriStand/`
4. Run as `lvuser:ni` so that files VeriStand deploys can be run by LabVIEW Run-Time Engine

Example Apache WebDAV Setup

Below is an example of how to set up Apache.

Installation and Initial Setup

```
# Install Apache
sudo opkg update
sudo opkg install apache2 apache2-utils

# Set up /files directory - the VeriStand engine must be installed␣
↪before running these
sudo mkdir -v -p /usr/share/apache2/default-site/files/c/ni-rt
sudo ln -v -s /c/ni-rt/NIVeriStand /usr/share/apache2/default-site/
↪files/c/ni-rt/NIVeriStand
sudo ln -v -s c /usr/share/apache2/default-site/files/C
sudo chown -v -R lvuser:ni /usr/share/apache2/default-site/files

# Set up DavLockDB directory
sudo mkdir -v -p /usr/local/apache/var
sudo chown lvuser:ni /usr/local/apache/var

# Set up WebDAV user
sudo mkdir -v -p /etc/apache2/
sudo htpasswd -c /etc/apache2/webdav.passwd [username]
```

Configuration Updates

After Apache is installed, update the configuration file at `/etc/apache2/httpd.conf`:

- Enable the modules `mod_auth_digest.so`, `mod_dav.so` and `mod_dav_fs.so`
- Change `User` and `Group` to `lvuser` and `ni` (this allows LabVIEW to run the files placed by WebDAV)
- Remove all `<Directory ...>` listings other than the `<Directory />` that denies access to the whole filesystem
- Add the WebDAV setup:

```
DavLockDB "/usr/local/apache/var/DavLock"
Alias "/files" "/usr/share/apache2/default-site/files"

<Location "/files">
    Options Indexes FollowSymLinks
    Dav On
    AuthType Basic
    AuthName "WebDAV"
    AuthUserFile "/etc/apache2/webdav.passwd"
    Require valid-user
</Location>
```

After making these changes, restart Apache with `sudo apachectl restart`.

WireGuard

WireGuard is installed and set up as part of the SNAC configuration. The Windows machine hosting the VeriStand gateway must be added as a peer. If communication is required between NI Linux RT targets, they will also need to be added as each other's peers.

Firewall

The firewall should be set up to only allow connections on the WireGuard tunnel (which defaults to the `work` zone).

```
# For WebDAV
sudo firewall-cmd --add-service=http --zone=work --permanent

# For the VeriStand engine
sudo firewall-cmd --add-port=2040/tcp --zone=work --permanent
sudo firewall-cmd --add-port=2050/tcp --zone=work --permanent
```

(continues on next page)

(continued from previous page)

```
# Enable firewall rules
sudo firewall-cmd --reload
```

Testing WebDAV

Once the previous sections are completed the WebDAV setup can be tested. Testing should happen from the Windows machine that hosts the gateway to ensure the gateway can access the WebDAV server properly.

Using the RT target's WireGuard IP address, the following URLs can be tested:

URL	Expected Result
`http://[target]/`	"403 Forbidden" error
`http://[target]/files/`	shows `C/` and `c/` as the only child items
`http://[target]/files/c/ni-rt/NIVeriStand/`	shows `Logs/` as the only child item (more if VeriStand has already run)

CHAPTER

FOUR

SPECIAL CONSIDERATIONS

IPv4-over-IPv6 network support via WireGuard

VeriStand only supports IPv4 networking, but WireGuard supports both IPv4 and IPv6. WireGuard can be configured to connect to other peers via IPv6 by specifying an IPv6 `Endpoint` but set its own `Address` and peers' `AllowedIPs` to IPv4 addresses. This allows VeriStand to work over an IPv6 network.