

VeraLab™ Guard Client
Computer Lab Management Suite

Installation Guide

Release 26.2 for Microsoft Windows

November 2026

VeraLab Client Installation Guide, Release 26.2.x for Microsoft Windows

Copyright © 2026 VeraLab Inc. All rights reserved.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

VeraLab programs, which include both the software and documentation, contain proprietary information. They are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the VeraLab programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

Contents

Send Us Your Comments ..... **ii**

Preface ..... **iii**

Audience iv

Organization v

Related Documentation vi

Conventions vii

1 Preinstallation Requirements **1-1**

System Requirements 1-2

Software Requirements for VeraLab Client 1-2

Hardware Requirements for VeraLab Client 1-2

Verifying Hardware Requirements 1-2

VeraLab Environment Setup 1-3

2 VeraLab Client Installation **2-1**

Installing VeraLab Client 2-2

Before You Install VeraLab Guard 2-2

Downloading VeraLab Software from the Web Site 2-2

Installing the VeraLab Guard Software 2-2

VeraLab Client Installation from Command Line 2-4

Setting the Server IP Address on the Client 2-4

Client Sign-In Modes 2-5

Using VeraLab Guard 2-6

Uninstalling VeraLab Components and Services 2-7

3 Postinstallation Configuration **3-1**

Reviewing Installed Components 3-2

Using VeraLab Guard Manager 3-3

Using Client Firewall 3-4

Using Client Lockscreen Banners 3-5

Send Us Your Comments

VeraLab Inc. welcomes your comments and suggestions on the quality and usefulness of this document. Your input is an important part of the information used for revision.

- Did you find any errors?
- Is the information clearly presented?
- Do you need more information? If so, where?
- Are the examples correct? Do you need more examples?
- What features did you like most?

If you find any errors or have any other suggestions for improvement, please indicate the document title and part number, and the chapter, section, and page number (if available). You can send comments to us in the following ways:

- Electronic mail: **support@veralab.com**
- Postal service:

  VeraLab Inc.
  99 S Almaden Blvd, Suite 600
  San Jose, CA 95113
  USA

If you would like a reply, please give your name, address, telephone number, and electronic mail address.

If you have problems with the software, please contact VeraLab Technical Support.

Preface

This manual is your primary source of introduction, preinstallation, installation, and postinstallation information for using VeraLab Guard Client.

This preface introduces you to the VeraLab Client Installation Guide, discussing the intended audience, structure, and conventions of this document. A list of related VeraLab documents is also provided.

This preface contains these topics:

- Audience
- Organization
- Related Documentation
- Conventions

Audience

The VeraLab Guard Client Installation Guide for Windows is necessary for anyone installing, configuring, or administering VeraLab Guard Client.

The VeraLab Guard Client Installation Guide is intended for Computer Lab Managers, Administrators, Technicians, and other lab personnel who perform the following tasks:

- Manage computer lab facility and personnel
- Perform system installation, administration, and setup

To use this document, you need Windows 7, Windows 8.1, or Windows 10/11 installed and tested on your computer system.

Organization

This guide contains the following chapters:

Chapter 1, “Preinstallation Requirements”

This chapter describes preinstallation requirements, third-party software, and operating system requirements for VeraLab Guard for Windows.

Chapter 2, “VeraLab Client Installation”

This chapter describes how to install and uninstall VeraLab Guard for Windows.

Chapter 3, “Postinstallation Configuration”

This chapter identifies postinstallation configuration tasks. Where appropriate, this chapter references other guides for procedures on performing these configuration tasks.

Related Documentation

This guide is part of a set for computer lab personnel using the VeraLab Computer Lab Management Suite. The other guides in the set are:

- *VeraLab Administrator's Guide*
- *VeraLab User's Guide*
- *VeraLab Server Installation and Upgrade Guide*

To download free release notes, installation documentation, white papers, or other collateral, please visit www.veralab.com.

Conventions

This section describes the conventions used in the text of this documentation set. We use various conventions to help you more quickly identify special terms. The following table describes those conventions and provides examples of their use.

Convention	Meaning	Example
Bold	Bold typeface indicates screen elements, such as elements of forms or menu items.	Select the **Available** checkbox.
Italics	Italic typeface indicates book titles or emphasis.	*You can not make currently used workstations unavailable.*
Bold Italics	Bold and italic typeface indicates screen names and areas.	The screen changes to ***Dashboard***.
< >	Angle brackets enclose variables or optional items.	The Dashboard `<counter_name>` page appears for that counter.

1 Preinstallation Requirements

This chapter guides you through the VeraLab Guard preinstallation procedures. This chapter covers the following topics:

- System Requirements
- VeraLab Environment Setup

> **Note** VeraLab uses a year-based version number. Release 26.2 is the second VeraLab release of 2026. Earlier version numbers referenced in this guide (for example, 5.x, 7.2, and 9.5) follow the previous numbering scheme.

System Requirements

Software Requirements for VeraLab Client

The following table shows the supported software environment.

Requirement	Value
System Architecture	32-bit and 64-bit
Operating System	VeraLab Client for Windows is supported on the following operating systems: ▪ Windows 7, Windows 8.1, Windows 10/11 ▪ Windows Server 2008 R2 ▪ Windows Server 2012 & 2012 R2 ▪ Windows Server 2016 ▪ Windows Server 2019 ▪ Windows Server 2022 ▪ Windows Server 2025 VeraLab Client for Windows is not supported on the following operating systems: ▪ Windows Vista ▪ Windows XP ▪ Windows 2000 ▪ Windows Server 2003 and 2003 R2
Network Protocol	▪ TCP/IP ▪ TCP/IP with SSL

Hardware Requirements for VeraLab Client

The following hardware components are required for VeraLab Client:

- RAM: 1 GB minimum, 2 GB and up recommended.
- Virtual memory: double the amount of RAM.
- Hard disk space: 10 MB minimum, 30 MB recommended.
- Processor: 800 MHz minimum, 1 GHz and up recommended.
- Video adapter: 256 color.

Verifying Hardware Requirements

To ensure that the system meets these requirements, follow these steps:

1. Determine the physical RAM size. For a computer using Windows 7, for example, open **System** in the control panel. If the size of the physical RAM installed in the system is less than the required size, then you must install more memory before continuing.
2. Determine the amount of free disk space on the system. For a computer using Windows 7, for example, open **Start → Computer**, right-click the drive where the VeraLab software is to be installed, and choose **Properties**.

VeraLab Environment Setup

It is important to complete your lab's environment setup before you start installing client software. During client software installation and registration with the VeraLab server you will be prompted to specify workstation attributes, such as image and which room it is assigned to. These setups are done on the VeraLab server and are specific to your organization. Once the VeraLab environment is properly configured, the client installation wizard will be able to pick up values from the server.

Starting with version 5.x, VeraLab supports a silent installation method on the client. Such an installation is performed using a pre-generated `config.ini` file. To generate the `config.ini` file, log in to **Administrator** (role) → **Setup** (menu) → **Stations** (task) → **Client Setup** screen. After generating `config.ini`, place that file next to the `veralab_client_setup.exe` file and run the installation. Every client where you run an installation using the `config.ini` file will pick up parameter values from that file.

> **Note** Beginning with Release 26.1, VeraLab automatically identifies each workstation by a unique Device ID and detects the computer model automatically, so you no longer need to select a workstation's model by hand. See "Reviewing Installed Components" in Chapter 3.

For more information and other installation methods, read Chapter 1 of the *VeraLab Administrator's Guide*.

2 VeraLab Client Installation

This chapter guides you through the VeraLab Guard Client installation procedures. This chapter covers the following topics:

- Installing VeraLab Client
- Client Sign-In Modes
- Using VeraLab Guard
- Uninstalling VeraLab Components and Services

Installing VeraLab Client

You can download the VeraLab software from the VeraLab Web site. This chapter describes how to install VeraLab Guard Client from hard disk.

> **Note** Beginning with Release 26.1, VeraLab ships a single, unified client. There is no longer a separate Standard, LDAP, or Novell client — one installer covers them all, and you no longer choose a client type during installation. How each workstation signs in is controlled centrally from the server. See "Client Sign-In Modes" later in this chapter. Any custom-built clients you use today continue to work as before.
>
> **Note** Clients that are already installed can be updated from the server with Remote Client Update (**Administrator** (role) → **Tools** → **Remote Client Update**). Starting with VeraLab 26.2, it is a guided three-step process: choose the update package, choose the stations, and confirm. See the *Administrator's Guide*.

Before You Install VeraLab Guard

Perform the following tasks before installing VeraLab Guard Client:

1. Review and satisfy applicable system and component requirements in Chapter 1, "Preinstallation Requirements."
2. Log on as a member of the Administrators group to the computer on which to install VeraLab Guard components.

Downloading VeraLab Software from the Web Site

To download the installation files:

1. Use any browser to access the software download page: `https://www.veralab.com/downloads_vl.jsp`.
2. Select a file system with enough free space to store and expand the files. On the file system that you just selected, create a temporary directory.
3. Download the executable file to the directory that you just created.

Installing the VeraLab Guard Software

Run the downloaded executable file and install the software, as follows:

Screen	Recommended Action
Welcome to the VeraLab Guard Setup Wizard	Click **Next**.
End-User License Agreement	Read the License Agreement and select the **I accept the agreement** radio button. Click **Next**.
Select Destination Location	Select the default location `C:\Program Files (x86)\VeraLab Inc\VeraLab Guard` or enter the full path to another directory.
Ready to Install	Click **Install**. The installation may take several minutes. The rest of the steps below will be displayed only if you are not using the silent installation

Screen	Recommended Action
	method with a `config.ini` file. For more information on how to use the `config.ini` file, see "VeraLab Environment Setup."
VeraLab Guard Settings	Type in the VeraLab Server hostname or IP address (see "Setting the Server IP Address on the Client" below). **Connection Password** has to be the same as specified in the Guard settings on the VeraLab Server. The default password is 'welcome'. You can test the connection by clicking the **Test Connection** button. For the connection test to succeed, the server has to be up and running, accepting connections from the client network on port 8080. If the connection test is successful, you will see connection details. To verify that the server hostname can resolve on your network, open a command prompt on the client and type `ping [yourveralabserverhost]`. To verify the Server IP address, log in to the VeraLab Server and use **Help & Links → Client Setup**. Selecting the **Advanced** tab will open advanced settings. The default value for **Client Listener Port** is 8087. You can keep the default value or select a custom port. Two checkboxes control the behavior of the client in case of a network outage. The default settings are recommended. Use the **Sync Screen Unlock Password from VeraLab Server** checkbox to control whether the workstation's screen unlock password is managed centrally by the server or entered locally. During the initial installation, before the client has connected to a server and its capabilities are unknown, this checkbox is selected by default and can be freely selected or cleared. After the first successful connection, the client determines whether the server supports centralized screen unlock password management. Once this is known, the checkbox is automatically set to the appropriate state and becomes disabled; its state cannot be changed unless a different server is configured. The checkbox state is also updated when you run Test Connection and when the settings are saved, provided the server is reachable. When the checkbox is cleared, type a local password in the **Screen Unlock Password** and **Confirm password** fields. A local password lets you unlock a workstation temporarily, bypassing access to the VeraLab server, or if connection to the server is lost. The minimum password length is 8 characters. Click **Apply Settings**. If the checkbox is cleared but the connected server does support centralized password management, the server-managed password is still used and any locally entered password is ignored.
VeraLab Guard Settings — Screen 2	On this screen you can input station details so a workstation can be automatically registered with the server. Select **Station Name**, **Room**, and **Image** from the drop-downs. The computer model is detected automatically and is no longer selected by hand. See "VeraLab Environment Setup" for reference. Click **OK**.
VeraLab Guard Settings — Screen 3	The client will perform several tests. You will see green check bullets next to succeeded tests, and red cross marks next to failed tests. You can click **Back** to modify settings or if you get any failures. Click **Finish**.

Screen	Recommended Action
Completing the VeraLab Guard Setup Wizard	Click **Finish** one more time to exit the installation.

Note As of Release 26.1, running **Test Connection** also shows the sign-in mode the client received from the server, so you can quickly confirm that a room is configured the way you intended. Workstation unlock passwords can also be managed centrally from the VeraLab server; see *Administrator's Guide*.

VeraLab Client Installation from Command Line

VeraLab client supports installation using the command line. Below is an example of silent installation using command-line parameters:

```
veralab_client_setup.exe /server=192.168.184.1 /password=welcome
/unLockPassword="Welcome123" /verysilent
```

Parameters such as `/server` (you can use IP or hostname), `/password`, `/unLockPassword`, and type of installation (`/silent` or `/verysilent`) must be followed by a value. If a password value has spaces, it has to be used within double-quotes; if no spaces, then no quotes are required.

Note Client-server connection password by default is set to "welcome". If you decide to use a different password, please update the same in VeraLab server settings (under **Tools → Settings → Guard**; in releases before 26.2 this category was named **Guard Settings**). See *Administrator's Guide* for more details.

Note This method ignores a custom config file; however, it will create a temporary config file and feed it to the installer program.

Setting the Server IP Address on the Client

Below are examples of how to specify a Server IP address in the ***VeraLab Guard Settings*** screen if a default or non-default installation of the server was performed:

- `192.168.0.1` — will automatically translate into `http://192.168.0.1:8080/veralab` (`veralab` is a default installation location on the web server).
- `192.168.0.1:8085` — will automatically translate into `http://192.168.0.1:8085/veralab` (you can specify a different web server port, if you chose a non-default port during server installation).
- `192.168.0.1/my_lab` — will automatically translate into `http://192.168.0.1:8080/my_lab` (if you renamed or installed several VeraLab instances on the web server).
- `192.168.0.1:8085/my_lab` — will translate into `http://192.168.0.1:8085/my_lab`.
- `https://veralab.myuniversity.edu:443` — if your VeraLab server is configured only for HTTPS connections and you are using the standard HTTPS port. Please note that the string has to be exactly as in the example, and include https, server hostname, and port number.

Note The same rules apply when using the Server hostname or FQDN instead of an IP address.

Client Sign-In Modes

Beginning with Release 26.1, how VeraLab clients sign in is controlled centrally from the server. The Client Modes task (**Setup → Client Modes**) lets you set the sign-in mode — per room or department — directly from the server. Three modes are available:

- **Standard Mode** — Clients sign in using their operating system (OS) username and password. This is the default for most environments, for example MSAD-enabled environments.
- **LDAP Mode** — Requires an autologon account. The OS login happens automatically in the background, then the VeraLab lock screen appears and prompts the user for their own username and password.
- **NetWare / eDirectory Mode** — Clients sign in using their Novell NetWare, Novell eDirectory, or NetIQ eDirectory credentials instead of their OS username. Available on Windows only.

Autologon accounts used by LDAP Mode are created and managed on the server under **Setup → Client Modes → Manage Autologon Accounts**. Usernames can be entered in UPN format (`user@mydomain.edu`) or down-level format (`MYDOMAIN\user`).

> **Note** Remote mode switching requires VeraLab client version 26.1 or later and takes effect without reinstalling or restarting the client. Sign-in-related changes (such as the lock screen) apply at the next login. If a client is switched out of LDAP Mode and no new login has occurred, the client will sign the current session out. Multiuser servers and thin clients always operate in Standard Mode, regardless of this setting.

Using VeraLab Guard

You can start using VeraLab Guard Client without rebooting the client workstation.

Depending on the selected settings, your computer may be locked upon rebooting. To manually unlock the screen, press the ‘space’ bar on the keyboard and enter the Lock Screen Password. If the workstation was configured for ‘strict’ mode, the workstation will lock up again during the next communication session with the server.

> **Note** For more information, refer to the *Administrator’s Guide* and *User’s Guide*.

Uninstalling VeraLab Components and Services

To uninstall VeraLab Guard Client and all its components:

1. Log on as a member of the Administrators group to the computer on which you installed VeraLab Guard components.
2. Go to **Start → Control Panel → Add or Remove Programs**, and select **VeraLab Guard**.
3. Click **Remove**.

> **Note** You can also uninstall the VeraLab Guard client by going to **Start → All Programs → VeraLab Guard**, and selecting **Uninstall VeraLab Guard**.

3 Postinstallation Configuration

This chapter guides you through the VeraLab Client postinstallation procedures. This chapter covers the following topics:

- Reviewing Installed Components
- Using VeraLab Guard Manager
- Using Client Firewall
- Using Client Lockscreen Banners

Reviewing Installed Components

VeraLab Guard installs and configures the following Windows Service:

- VeraLab Guard Service

This service is configured for Automatic Startup Type. To view the service and its status, go to **Start → Control Panel → Administrative Tools → Services**.

VeraLab Guard Client relies either on a fixed IP address or hostname. In order for VeraLab Guard to function properly, you have to ensure the following is true:

- Client IP address and hostname are entered on the VeraLab Server. To verify that the workstation exists on the server and has a correct IP address, log in to the VeraLab Suite, go to **Setup → Stations → Select a Room**, and find the workstation in the list.
- Every time the client boots up, it obtains the same IP or hostname, even if you are using DHCP.

> **Note** Beginning with Release 26.1, VeraLab also recognizes each workstation automatically using a unique Device ID, so stations stay correctly matched even after they are renamed or their hardware changes. The client reports its own computer model automatically, and a new on-demand refresh command lets you ask clients to report their latest Device ID and model from the server. See the *Administrator's Guide*.

Using VeraLab Guard Manager

VeraLab Guard Manager allows you to modify client settings without reinstalling VeraLab Guard Client.

To run VeraLab Guard Manager:

1. Log on as a member of the Administrators group to the computer on which you installed VeraLab Guard components.
2. Go to **Start → All Programs → VeraLab Guard**, and select **VeraLab Guard Manager**. Alternatively, type `veralab` in the Start (aka "Metro") menu, if using Windows 8.1.
3. Modify settings and click the **Apply Settings** button.
4. Check performed tests and click **Finish** to exit.

Starting with version 9.5, VeraLab Guard Manager lets you enable diagnostics locally. Previously, this functionality was available only through the Web Application UI or the Windows registry.

Enabling or Disabling Diagnostic Logging

To enable or disable diagnostic logging in VeraLab Guard Manager:

1. Log on as a member of the Administrators group to the computer on which you installed VeraLab Guard components.
2. Go to **Start → All Programs → VeraLab Guard**, and select **VeraLab Guard Manager**. Alternatively, type `veralab` in the Start (aka "Metro") menu, if using Windows 8.1 or higher.
3. Select the **Diagnostics** tab.
4. Click on the **Enable Logs** button.
5. Once the issue is reproduced, return to the **Diagnostics** tab and click on the **Save Logs to Desktop** button.
6. Click on the **Disable Logs** button and email the saved logs to **support@veralab.com**.

Using Client Firewall

By default, VeraLab client will open ports in firewalls coming standard with Windows. To verify open ports on Windows 7, go to **Control Panel → System and Security → Windows Firewall**. Open the **Advanced settings window → Inbound Rules** and find **VeraLab Guard Service** in the list.

If you are using any other firewall software on the client, you will need to 'train' the firewall or define port exceptions in order to enable connections with the VeraLab Server.

To verify that you can get screenshots and a list of processes on the client, log in to the VeraLab Server, go to **Tools → Monitoring**, select a room from the drop-down menu, and click the **Screenshot** or **Processes** icon. If the window displays a client's screenshot or a list of processes, then the client's firewall allows the connection with the server. If you get an error message, you need to refer to your firewall software manual.

Using Client Lockscreen Banners

Starting with version 5.x, VeraLab allows you to use client screen real estate for placing custom banners, such as a campus logo, announcements, etc. Banners can be static, which means one banner is displayed at all times, or changing, when multiple banners rotate every 20 seconds by default.

Starting with VeraLab 26.2, banner management is redesigned. On the ***Client Banners*** page you upload banners and choose the level at which each banner applies: Site Level, one set for a department, or a set per room. Banner files are kept within the department that owns them.

To change the default banner rotation interval, log in to the VeraLab Server, go to **Tools → Settings → Guard**, and change **Client Banners Rotation Interval (sec)**.

> **Note** To read more about how to set up client lockscreen banners, see Manager tasks in the *User's Guide*.