VeraLab™ Guard Mac Client
Computer Lab Management Suite

Installation Guide

Release 26.2 for macOS

November 2026

VeraLab Client Installation Guide, Release 26.2.x for macOS

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 Mac Client 1-2

Hardware Requirements for VeraLab Mac Client 1-2

Verifying Hardware Requirements 1-2

2 VeraLab Mac Client Installation **2-1**

Installing VeraLab Mac Client 2-2

Before You Install VeraLab Guard 2-2

Downloading VeraLab Software from the Web Site 2-2

Installing VeraLab Guard Client Software 2-2

Installing VeraLab Guard Client Package Silently 2-3

Client Sign-In Modes and Auto-Login 2-4

macOS Auto-Login Support 2-4

Using VeraLab Guard 2-5

Uninstalling VeraLab Components and Services 2-6

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 on macOS.

This preface introduces you to the VeraLab Mac 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 macOS is necessary for anyone installing, configuring, or administering VeraLab Guard Client.

The VeraLab Guard Mac 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 macOS 10.15 Catalina or higher 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 macOS.

Chapter 2, “VeraLab Mac Client Installation”

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

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 topic:

- System Requirements

> **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 and 9.5) follow the previous numbering scheme.

System Requirements

Software Requirements for VeraLab Mac Client

The following table shows the supported software environment.

Requirement	Value
System Architecture	x86-64 for Intel Macs or ARM64 (aarch64) for ARM-based Macs
Operating System	VeraLab Client for macOS is supported on the following operating systems: ▪ Apple macOS version 10.15 (Catalina) or higher.
Network Protocol	▪ TCP/IP ▪ TCP/IP with SSL

Hardware Requirements for VeraLab Mac Client

The following hardware components are required for VeraLab Mac Client:

- RAM: 2 GB minimum, 4 GB recommended.
- Virtual memory: double the amount of RAM.
- Hard disk space: 200 MB minimum, 500 MB recommended.
- Processor: Intel, macOS-compatible processor or higher.
- Display: 1024 x 768 or higher-resolution monitor displaying thousands of colors.
- Mouse or compatible pointing device.

Verifying Hardware Requirements

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

1. Determine the physical RAM size. To determine the total amount of installed RAM that is functional on your macOS system:
   – Go to the **Blue Apple** menu in the upper-left corner of your screen.
   – Select the first item, **About This Mac**.
2. Determine the amount of free disk space on the system. To check how much free space is available on your startup disk:
   – In Finder™, select your startup disk's icon. For most users, this is **Macintosh HD**.
   – Press the **Command-I** keyboard combination.
   – The **Get Info** window for the startup disk will open, showing the **Capacity**, **Available** (free space), and space **Used**.

2 VeraLab Mac Client Installation

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

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

Installing VeraLab Mac Client

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

> **Note** Beginning with Release 26.1, VeraLab ships a single, unified client and how each workstation signs in is controlled centrally from the server. You no longer choose a client type during installation. See "Client Sign-In Modes and Auto-Login" later in this chapter.

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 Client 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. You can also download to a desktop.
3. Download the image file (DMG) to the desktop or a directory that you just created.
4. Mount the disk image into the machine by double-clicking the file.

Installing VeraLab Guard Client Software

Once the `VeraLabGuard.dmg` file has been downloaded and mounted, perform the steps in the order below:

1. In the open Installer window, double-click on **Install VeraLab Guard**.
2. Click **Continue** in the Introduction screen.
3. Review the Software License Agreement and click the **Continue** button. Click the **Agree** button to accept license terms.
4. The current version supports only the standard installation type with all defaults. Click the **Install** button to continue with the installation.
5. Enter the username and password for the account with Administrator's privileges.
6. Once installation of files is completed, you will see the ***VeraLab Guard Settings*** window. Enter the VeraLab Server hostname or IP Address and the **Connection Password**. Use the **Sync Screen Unlock Password from VeraLab Server** option to control whether the screen unlock password is managed centrally by the server or entered locally, as described below.

During the initial installation, before the client has connected to a server and its capabilities are unknown, **Sync Screen Unlock Password from VeraLab Server** 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 option is automatically set to the appropriate state and becomes disabled; its state cannot be changed unless a different server is configured. The state is also updated when you run Test Connection and when the settings are saved, provided the server is reachable.

When the option is cleared, enter a local **Screen Lock Password**. A local password lets you bypass client authentication (Lock Screen) if connection to the server is lost and the client screen has been locked out. If the option 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.

> **Note** In Catalina and higher versions, a new prompt will be displayed to allow Screen Recording.

7. Click **Test Connection** to verify you can connect to the VeraLab server successfully.
8. Click **Apply Settings** to finish. You can click on the **Daemon** icon to verify that the client process has been started successfully.
9. Close the VeraLab Guard manager window.

> **Note** As of Release 26.1, running **Test Connection** also shows the sign-in mode the client received from the server. Workstation unlock passwords can also be managed centrally from the VeraLab server; see *Administrator's Guide*.

Installing VeraLab Guard Client Package Silently

Once the `VeraLabGuard.dmg` file has been downloaded and mounted, extract `Install VeraLab Guard.pkg` and save it in a directory of your choice. Perform the steps in the order below:

1. Create a script file in the same directory, for example `vl_script.sh` (see the sample script below). Save it and make it executable, for example `chmod +x vl_script.sh`.
2. Execute it with `sudo ./vl_script.sh` and propagate to other Macs in the lab.

```
#!/bin/bash
mkdir -p /Library/Application\ Support/VeraLab
rm -f /Library/Application\ Support/VeraLab/config.plist
/usr/libexec/plistbuddy -c 'Add serverip string "192.168.1.2"' \
  /Library/Application\ Support/VeraLab/config.plist
/usr/libexec/plistbuddy -c 'Add serverpassword string "welcome"' \
  /Library/Application\ Support/VeraLab/config.plist
/usr/libexec/plistbuddy -c 'Add unlockpassword string "password"' \
  /Library/Application\ Support/VeraLab/config.plist
installer -pkg "Install VeraLab Guard.pkg" -target /
```

Client Sign-In Modes and Auto-Login

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. On macOS, the following modes are available:

- **Standard Mode** — Clients sign in using their operating system (OS) username and password. This is the default for most 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.

> **Note** NetWare / eDirectory Mode is available on Windows only. Remote mode switching requires VeraLab client version 26.1 or later. Multiuser servers and thin clients always operate in Standard Mode, regardless of this setting.

macOS Auto-Login Support

Auto-login can be configured on macOS as well as on Windows. On macOS, auto-login applies after startup or reboot; unlike Windows, it cannot be triggered after a user logs out. Autologon accounts used by LDAP Mode are created and managed on the server under **Setup → Client Modes → Manage Autologon Accounts**.

Using VeraLab Guard

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 Mac Client and all its components:

1. Log on as a member of the Administrators group to the computer on which you installed VeraLab Guard Mac Client components.
2. Run the following: `sudo "/Library/Application Support/VeraLab/uninstall.sh"`.
3. Alternatively, you can mount the Client Setup file and run the uninstall from there using the **Uninstall VeraLab Guard** option.

> **Note** If you are re-installing the client and getting an error message saying "A newer version of this software already exists on this disk", try using the following command: `sudo pkgutil --forget com.veralab.macguard.pkg`.

3 Postinstallation Configuration

This chapter guides you through the VeraLab Mac 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 Mac Client installs and configures the following macOS Daemons:

- VeralabDaemon
- VeralabAgent

This daemon process is configured for Automatic Startup Type.

In order for VeraLab Guard to function properly, you have to ensure the following is true:

- When using an environment with static IP addresses, client IP addresses must be 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 host name or IP. The default behavior is set to recognize clients using their host names. Optionally, you can change this setting to use client IP addresses.

> **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. Release 26.1 also includes behind-the-scenes security improvements that further protect your managed macOS workstations. 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 Mac Client components. You can run the installer without Admin rights, but you will be asked for credentials at the end of installation.
2. Go to the **Applications** directory and run **VeraLab Guard**.
3. Modify settings and click **Apply Settings**.
4. Close the VeraLab Guard window to exit.

Using Client Firewall

If you are using 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 may want 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*.