

CUSTOMER INSTALLATION GUIDE

Valerus Web Client

Installing the Certificate Trust Chain

Release 26.100 and Up

Document details	
Product	Vicon Valerus VMS — Web Client
Software release	Valerus 26.100
Applies to	Valerus 26.1 and later, using Google® Chrome® or Microsoft® Edge® on Microsoft Windows® or macOS® with M Chips
Audience	End users and site administrators
Document version	1.0

1. Overview

The Valerus 26.100 Web Client streams live and recorded video over a secure HTTPS connection. To establish that connection, your browser must trust the security certificate presented by the Valerus server.

Because the Valerus server issues its own certificate, Chrome and Microsoft Edge do not recognize it until the Vicon certificate trust chain has been installed on your computer. Before that is done, you may see one or more of the following:

- A "Not secure" warning beside the address bar.
- A message reading "Video playback requires HTTPS. This page was loaded over an insecure connection."
- A "Trouble Playing Video?" dialog, or camera panes that remain black or stuck on "Connecting..."

This guide walks you through installing the certificate. It is a one-time process per computer and takes approximately two minutes.

Note: Installing this certificate only tells your computer to trust your own Valerus server. It does not change any other browser or security settings.

What you will achieve

Once complete, the "Not secure" warning disappears, the browser connects over HTTPS without prompting, and live and recorded video play normally in all camera panes.

2. Before you begin

Please confirm the following before starting:

Requirement	Details
Valerus release	Valerus 26.1 or later installed and running on your server.
Supported browser	Google Chrome or Microsoft Edge, current version.
Operating system	Microsoft Windows, or macOS on an Apple® computer. The installation method differs by platform — see section 3.
Server access	You can reach the Valerus Web Client and sign in.
Permissions	Windows: no special rights are needed to install for your own user account; installing for all users on a shared computer requires local administrator rights. macOS: a Mac login password is required to install the certificate trust profile.
Downloads allowed	The browser and any endpoint-protection software must permit the download of the certificate file from your Valerus server — the Valerus Certificate Installer (.exe) on Windows, or the Valerus Certificate Trust Profile (.mobileconfig) on macOS.

Which option should I choose? (Windows): On a personal workstation, choose Current user only — it needs no administrator rights. On a shared or operator workstation used by several people, choose All users on this computer so every user benefits from a single installation.

3. Installation procedure

The certificate is installed differently depending on your operating system. Follow section 3a if you are using a Windows computer or section 3b if you are using a Mac. Only one of the two needs to be completed.

3a. Windows — Chrome and Microsoft Edge

On Windows, the certificate is installed by a small signed application downloaded from your Valerus server.

Step 1 — Switch the session to HTTPS

If Valerus Web Client was opened over HTTP, the browser displays "Not secure" in the address bar and the camera pane reports that video playback requires HTTPS. Click Reload this page over HTTPS.

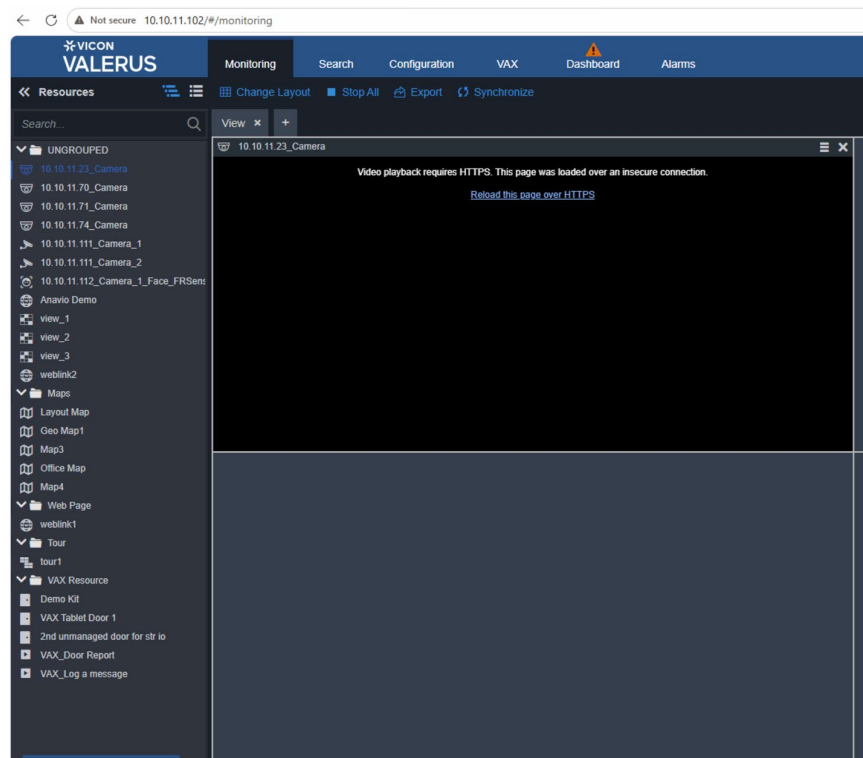


Figure 1. The Valerus Monitoring page loaded over HTTP, showing the "Reload this page over HTTPS" link.

Step 2 — Download the Valerus Certificate Installer

The page reloads over HTTPS. Because your computer does not yet trust the server certificate, Valerus displays the "Trouble Playing Video?" dialog. Click Download Valerus Certificate Installer and save the file when prompted.

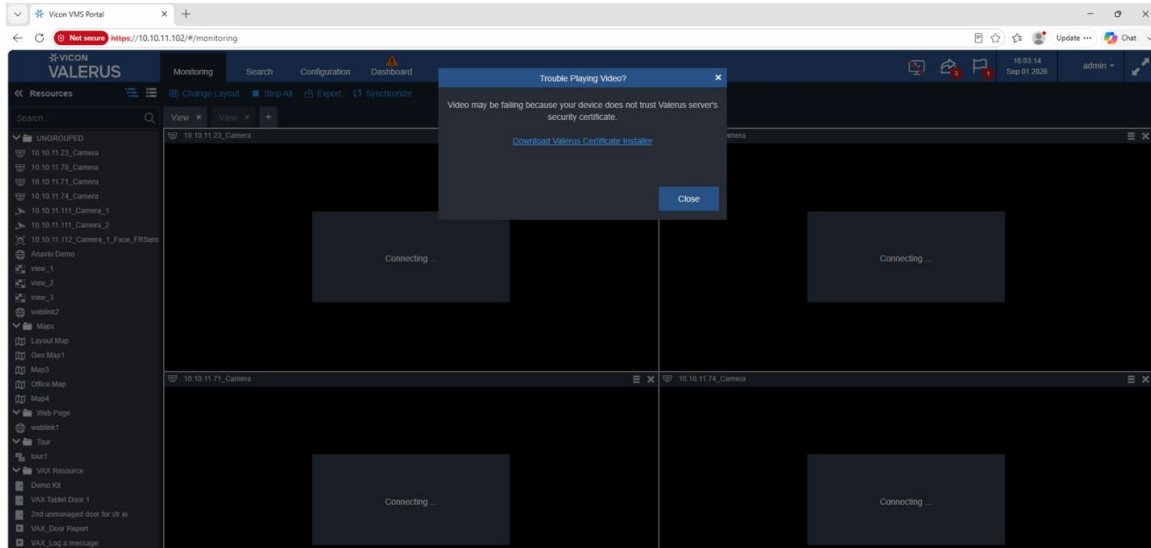


Figure 2. The "Trouble Playing Video?" dialog with the certificate installer download link.

Step 3 — Run the installer and choose a scope

Open the downloaded file, Valerus Certificate Installer.exe, from your browser's Downloads list. The Vicon Certificate Trust Installer opens and asks who the certificate should be installed for. Select All users on this computer or Current user only and click Install.

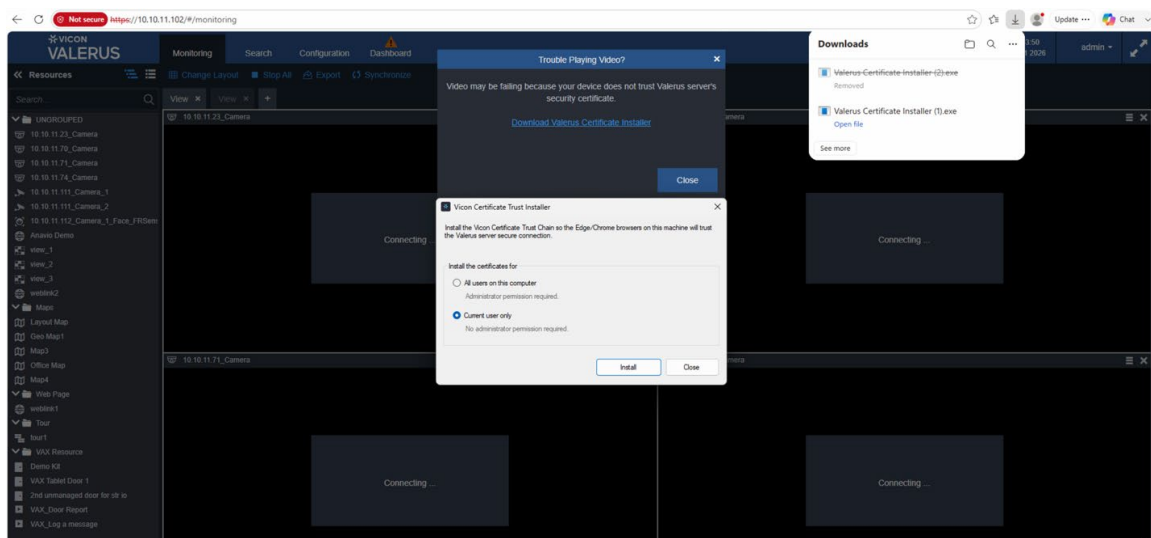


Figure 3. Selecting the installation scope in the Vicon Certificate Trust Installer.

Step 4 — Approve the Windows security warning

Windows asks for confirmation to install a root certificate from Vicon Root CA. This prompt is expected. Review the certificate thumbprint if your security policy requires it and click Yes.

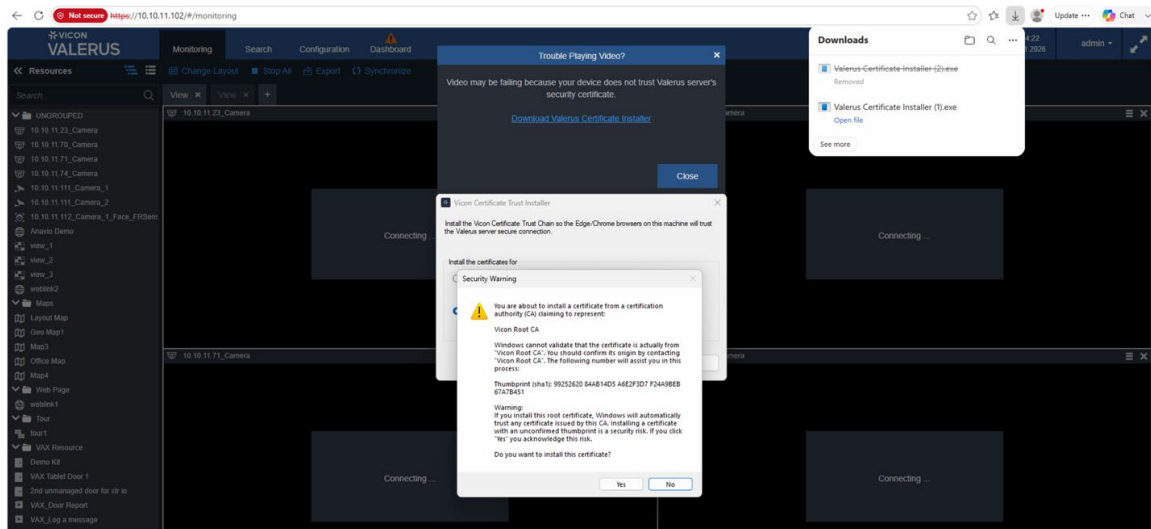


Figure 4. The Windows Security Warning confirming installation of the Vicon Root CA certificate.

Step 5 — Confirm the installation completed

A confirmation message reports that the Valerus certificate trust was installed successfully and asks you to close and reopen your browser. Click OK and close the installer.

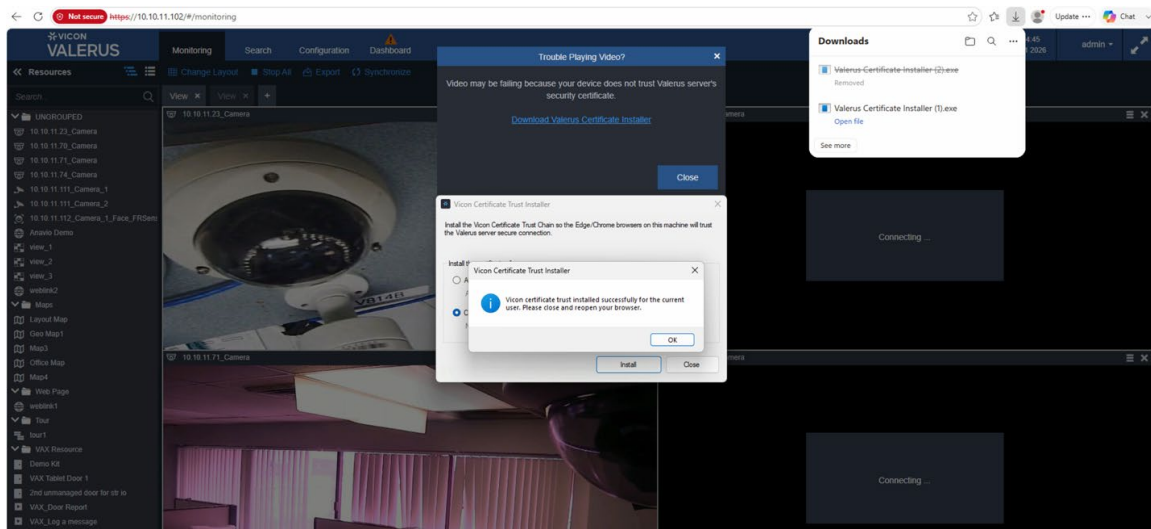


Figure 5. Successful installation confirmation.

Step 6 — Close and reopen the browser

Close all browser windows completely; reopen the browser and navigate to the Valerus Web Client again. The "Not secure" warning no longer appears and video plays normally.

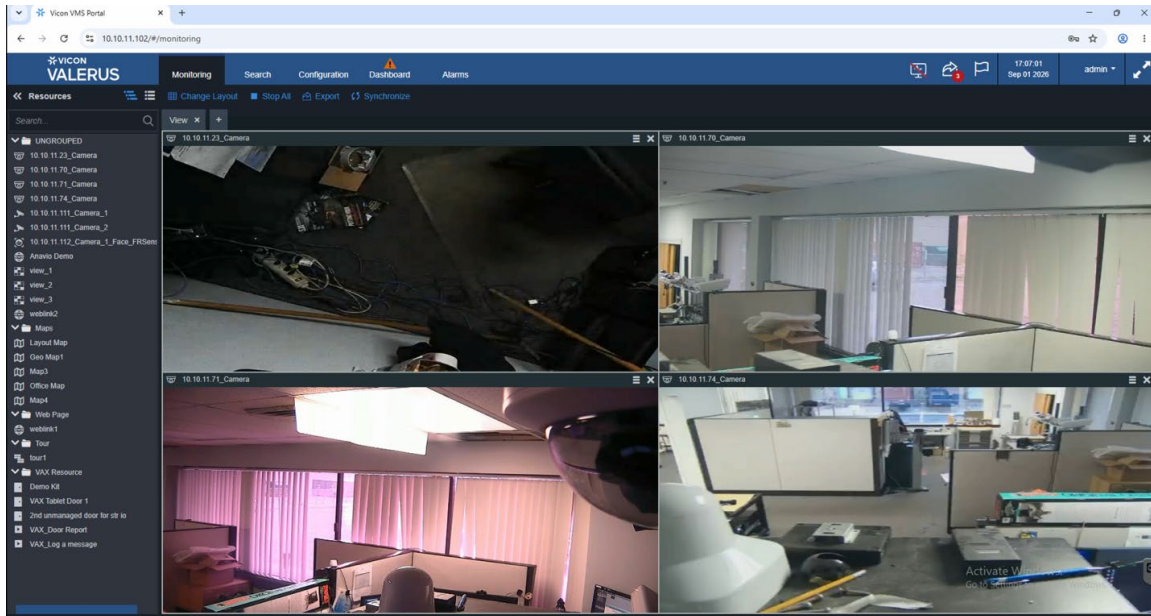


Figure 6. The Valerus web client after installation — no security warning, with all camera panes streaming.

Important: The browser must be closed entirely, not just the Valerus tab. Certificates are read when the browser starts, so an open browser will continue to show the old warning.

3b. macOS — Chrome and Microsoft Edge

On macOS, the certificate is supplied as a certificate trust profile, which is installed through System Settings rather than by running an application. The downloaded profile is only valid for a short time, so complete steps 2 to 4 in one sitting.

Time limit: The trust profile must be installed within 8 minutes of downloading it. If it expires, simply download it again from the same dialog.

Step 1 — Switch the session to HTTPS

If Valerus Web Client was opened over HTTP, the browser displays "Not secure" in the address bar and the camera pane reports that video playback requires HTTPS. Click Reload this page over HTTPS.

Step 2 — Download the Valerus Certificate Trust Profile

The page reloads over HTTPS. Because your Mac does not yet trust the server certificate, Valerus displays the "Trouble Playing Video?" dialog. Click Download Valerus Certificate Trust Profile and allow the download if Chrome or Edge asks for confirmation.

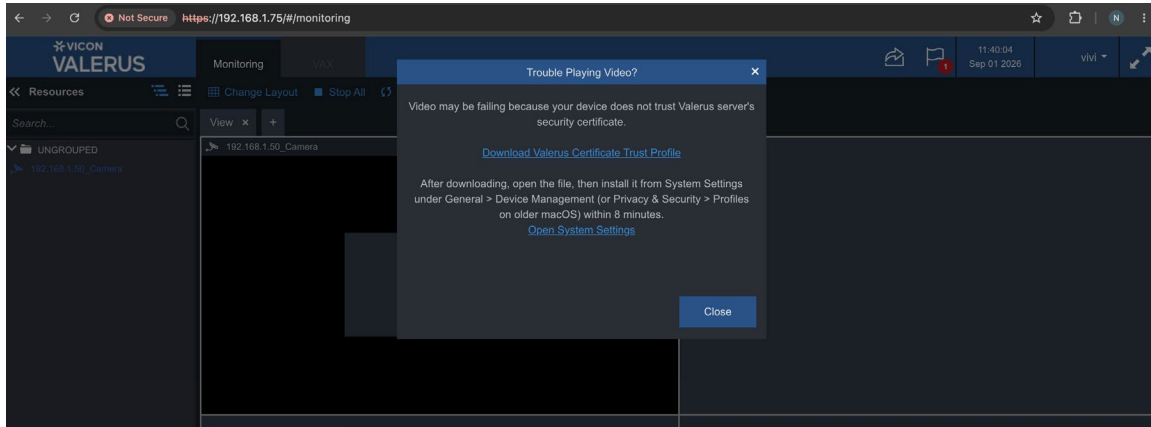
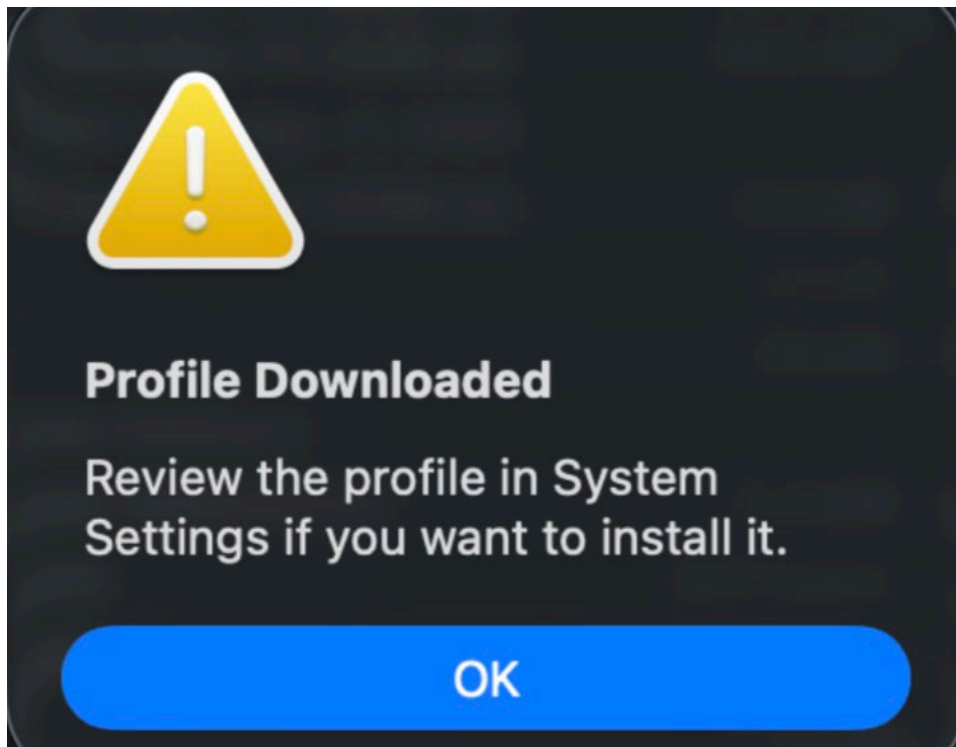


Figure 7. The macOS version of the "Trouble Playing Video?" dialog, offering the Valerus Certificate Trust Profile.

Step 3 — Open the downloaded profile

Open the downloaded file from your browser's Downloads list or from the Downloads folder in Finder (Valerus Certificate Trust.mobileconfig). macOS accepts the profile and holds it as a pending download; nothing is installed yet. A notification confirming that the profile has been downloaded and is ready to review may display.

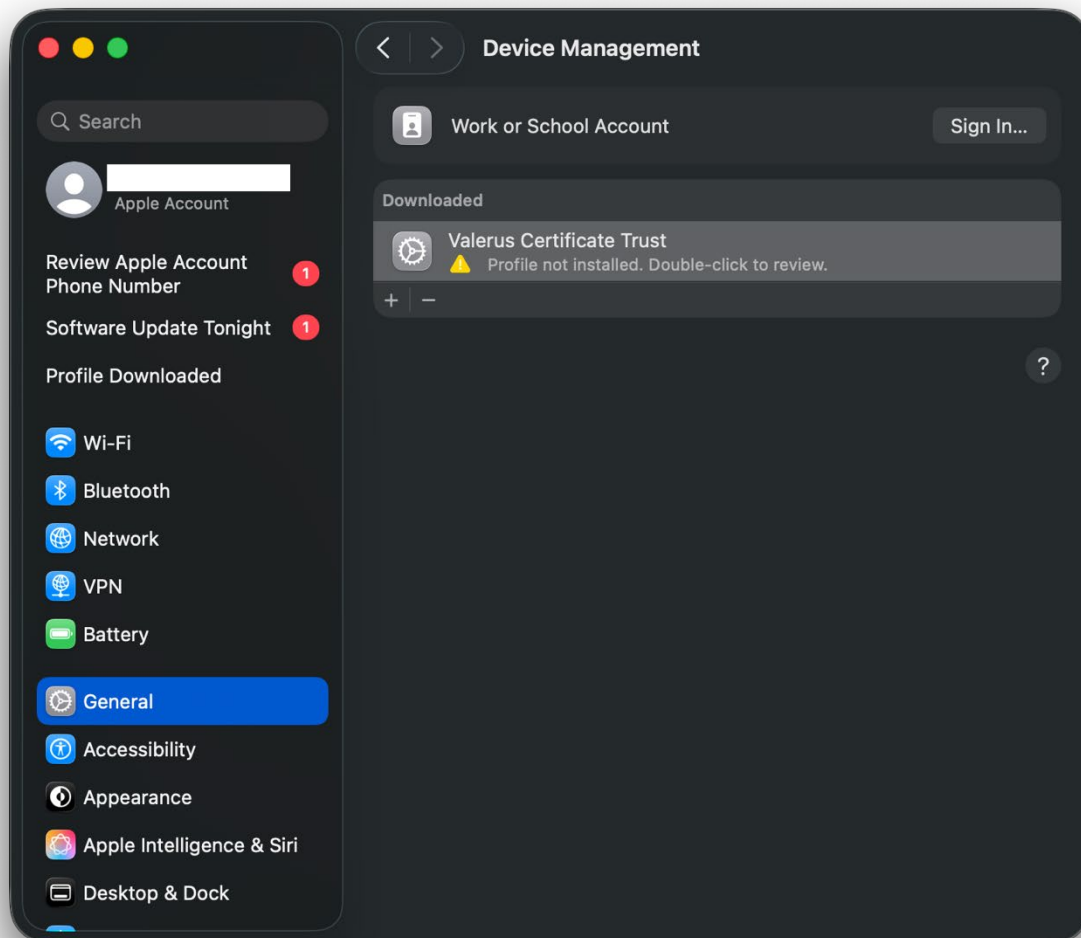


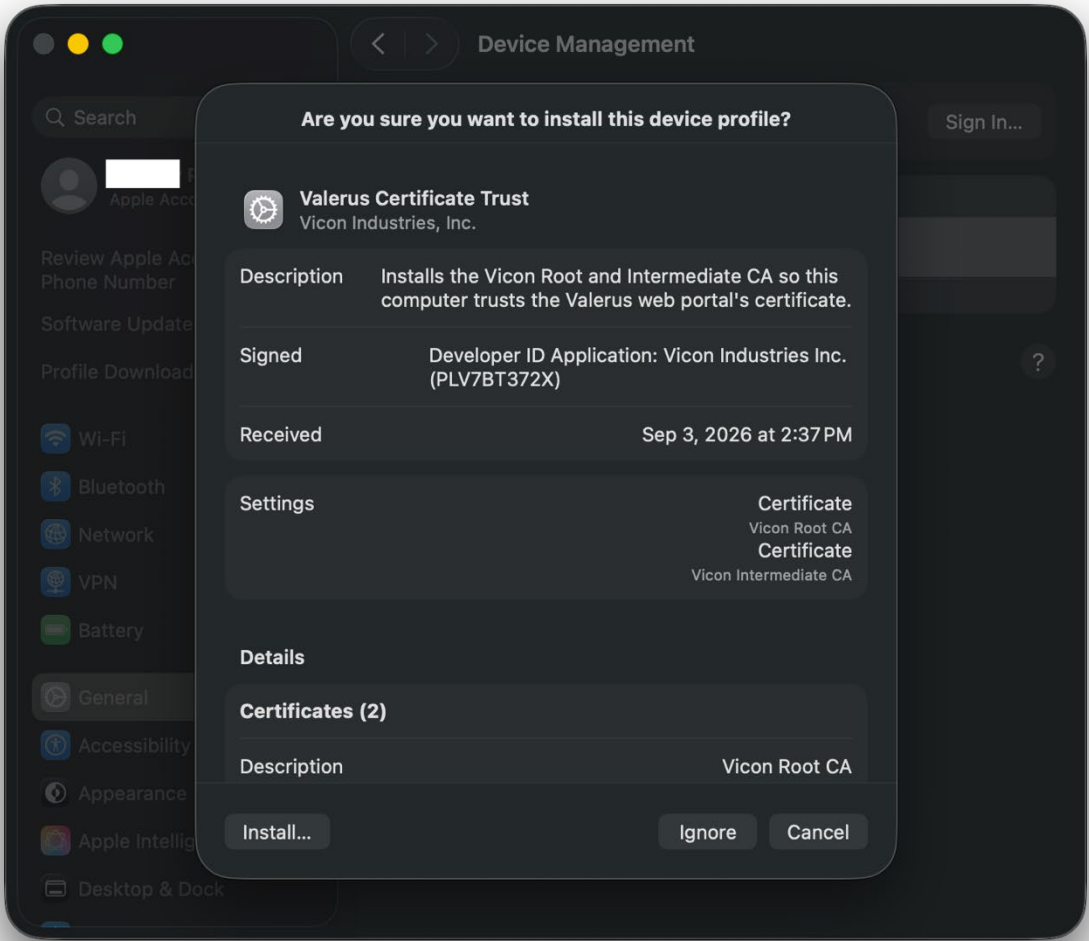
Step 4 — Install the profile in System Settings

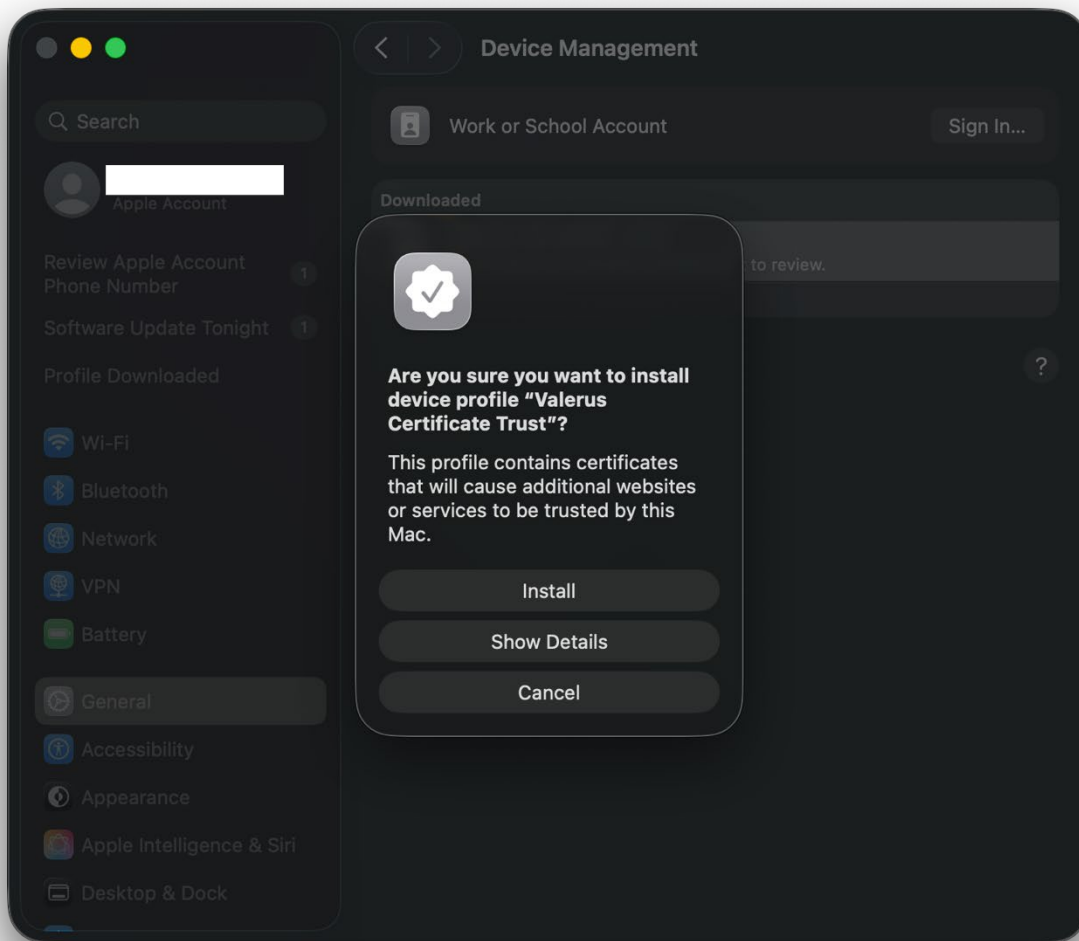
Click Open System Settings in the Valerus dialog, or open System Settings manually and go to:

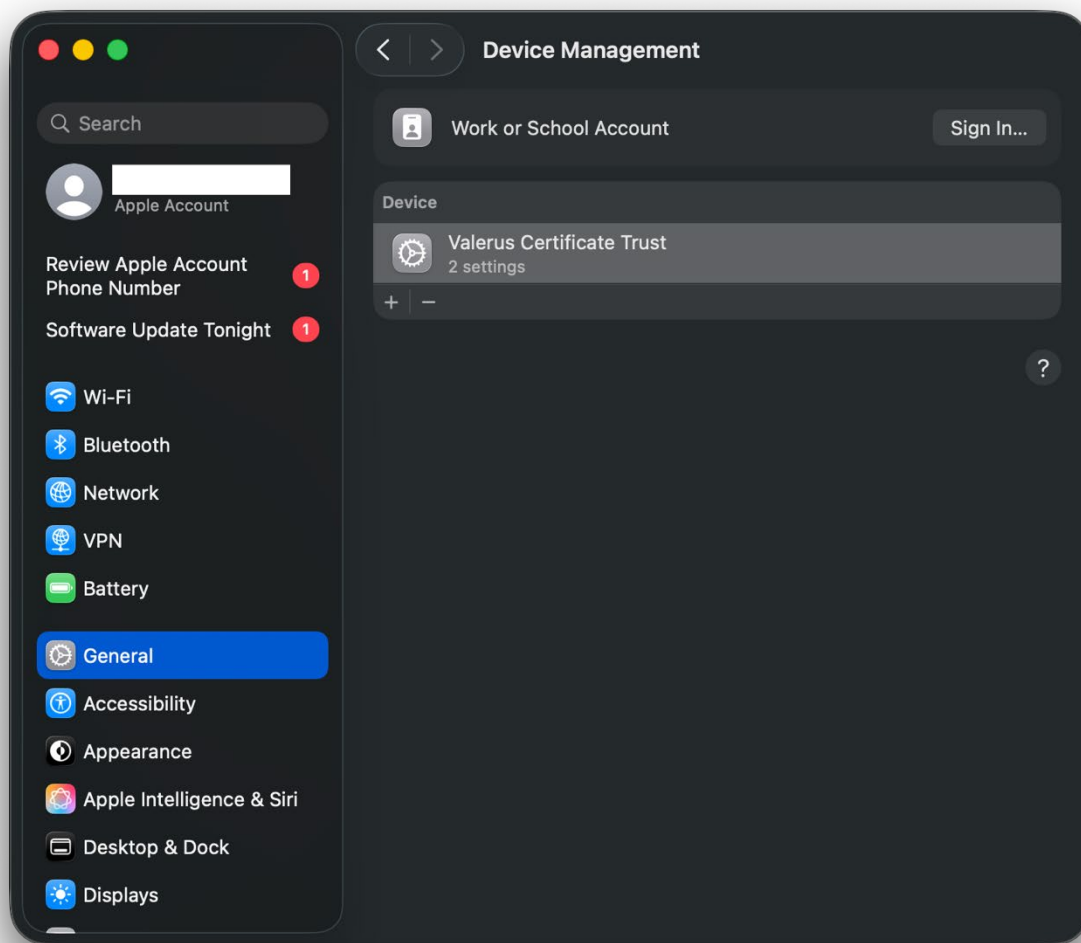
- macOS Ventura and later: General › Device Management (shown as VPN & Device Management on some releases).
- Older versions of macOS: Privacy & Security › Profiles, or System Preferences › Profiles.

Double-click the downloaded Valerus profile, click Install, confirm when asked, and enter your Mac login password. The profile then appears in the list of installed profiles.









If the profile is not listed, it has most likely expired. Return to the Valerus tab, click Download Valerus Certificate Trust Profile again, and install it again immediately.

Step 5 — Close and reopen the browser

Quit the browser completely — press Command-Q, or choose Quit from the browser menu, rather than just closing the window. Reopen the browser and navigate to the Valerus Web Client again. The "Not secure" warning no longer appears and video plays normally.

Important: Closing the last window does not quit an application on macOS. If the browser is still running in the Dock, it continues to use the old certificate list and the warning will remain.

4. Verifying the installation

The installation is successful when all of the following are true:

- The address bar shows the standard padlock or site-information icon rather than "Not secure."
- The "Trouble Playing Video?" dialog no longer appears when you open a view.
- Live video appears in every camera pane instead of a black panel or "Connecting...". On macOS, the Valerus profile is also listed in System Settings under Device Management.

If any of these are not true, see the troubleshooting steps below.

5. Troubleshooting

Symptom	Likely cause	What to do
"Not secure" warning still appears after installation.	The browser was not fully closed and reopened.	Close every browser window, wait a few seconds, then reopen the browser and reload the Valerus Web Client.
Video plays for one user but not another on the same PC.	The certificate was installed for the current user only.	Re-run the installer while signed in as the affected user or run it once with All users on this computer using administrator rights.
The certificate installer will not download or is removed automatically.	Browser download protection or endpoint security is blocking the .exe file.	Choose Keep in the browser download prompt or ask your IT team to allow the file. The installer is published by Vicon and downloaded directly from your own Valerus server.
The Install button does nothing, or the installer reports insufficient permissions.	All users on this computer was selected without administrator rights.	Select Current user only or ask an administrator to run the installer.
Video still fails after the warning has cleared.	A network, camera, or server-side issue unrelated to the certificate.	Confirm the cameras are online in Configuration; contact support with the camera name and the time of the failure.
The warning returns after the Valerus server is upgraded, replaced, or its address changes.	The new server presents a different certificate.	Repeat this procedure once against the new server address.
macOS: the downloaded profile does not appear in System Settings.	The trust profile expired before it was installed. It is valid for 8 minutes.	Return to the Valerus tab, download the profile again, and install it immediately.
macOS: the warning remains even though the profile is installed.	The browser was closed but not quit, so it is still running.	Press Command-Q to quit the browser fully, or right-click it in the Dock and choose Quit and reopen it.

6. Frequently asked questions

Do I have to repeat this on every computer?

Yes. The certificate is trusted per computer, so each workstation used to view Valerus needs the installer run once. Installing for all users covers everyone who signs in to that machine.

Is it safe to install a root certificate?

The installer adds only the Vicon Root CA certificate, which allows your computer to verify your own Valerus server. It grants no other access and can be removed at any time — on Windows from the Certificate Manager, and on macOS by removing the Valerus profile in System Settings.

Will this affect other websites or applications?

No. Trust is limited to certificates issued by the Vicon Root CA for your Valerus system.

Validity of certificate?

825 days since upgrade/installation. Renews automatically on next Valerus upgrade.

Can our IT department deploy this centrally?

Yes. Larger sites usually prefer to distribute the certificate to all workstations centrally — through Group Policy on Windows, or an MDM solution such as Jamf or Intune on macOS — rather than having each user run the installer. Contact us and we will provide the certificate file and guidance.

What if my organization uses its own certificate?

The Valerus server can be configured to use a certificate issued by your own CA. Valerus certificate is still required for video streaming.

Is the macOS procedure different from Windows?

The end result is the same, but the mechanism differs. Windows uses a signed installer that adds the Vicon Root CA to the certificate store. macOS uses a certificate trust profile installed through System Settings. Both are one-time actions per computer, and both are removable at any time.