PhiLSOC Access Setup

macOS user manual and certificate enrollment guide

PhiLSOC | Sovereign SOC Command Center

Purpose

Use this guide to install the signed PhiLSOC Access Setup application, enroll a PhiLSOC client certificate, and open the Sovereign SOC Command Center from Google Chrome or Safari.

Application	PhiLSOC Access Setup for macOS
Console	https://console.philsoc.net/app
Manual version	1.0 - August 2026

1. Before you begin

You need the following items before starting:

Required	What to prepare
Supported Mac	A Mac running macOS 15 or newer.
Signed app	The official PhiLSOC signed and notarized ZIP package. Obtain it only through the approved PhiLSOC distribution channel.
Certificate package	Your assigned **.p12** or **.pfx** file. The app accepts a regular file up to 1 MB.
One-time password	The password sent through a separate approved channel. Do not forward or store it with the certificate package.
Browser	Google Chrome or Safari installed in the Applications folder.
Internet	Connectivity to https://console.philsoc.net.

> **Security rule**
>
> Keep the certificate package and its password in separate channels. Enter the password only in PhiLSOC Access Setup. The app clears it after each installation attempt and does not save it.

Install the application

1

Open the downloaded ZIP

Double-click the signed PhiLSOC ZIP file. macOS expands it into **PhiLSOC Access Setup.app**.

2

Move the app to Applications

Drag **PhiLSOC Access Setup.app** into the **Applications** folder. This gives the app a stable location for future use.

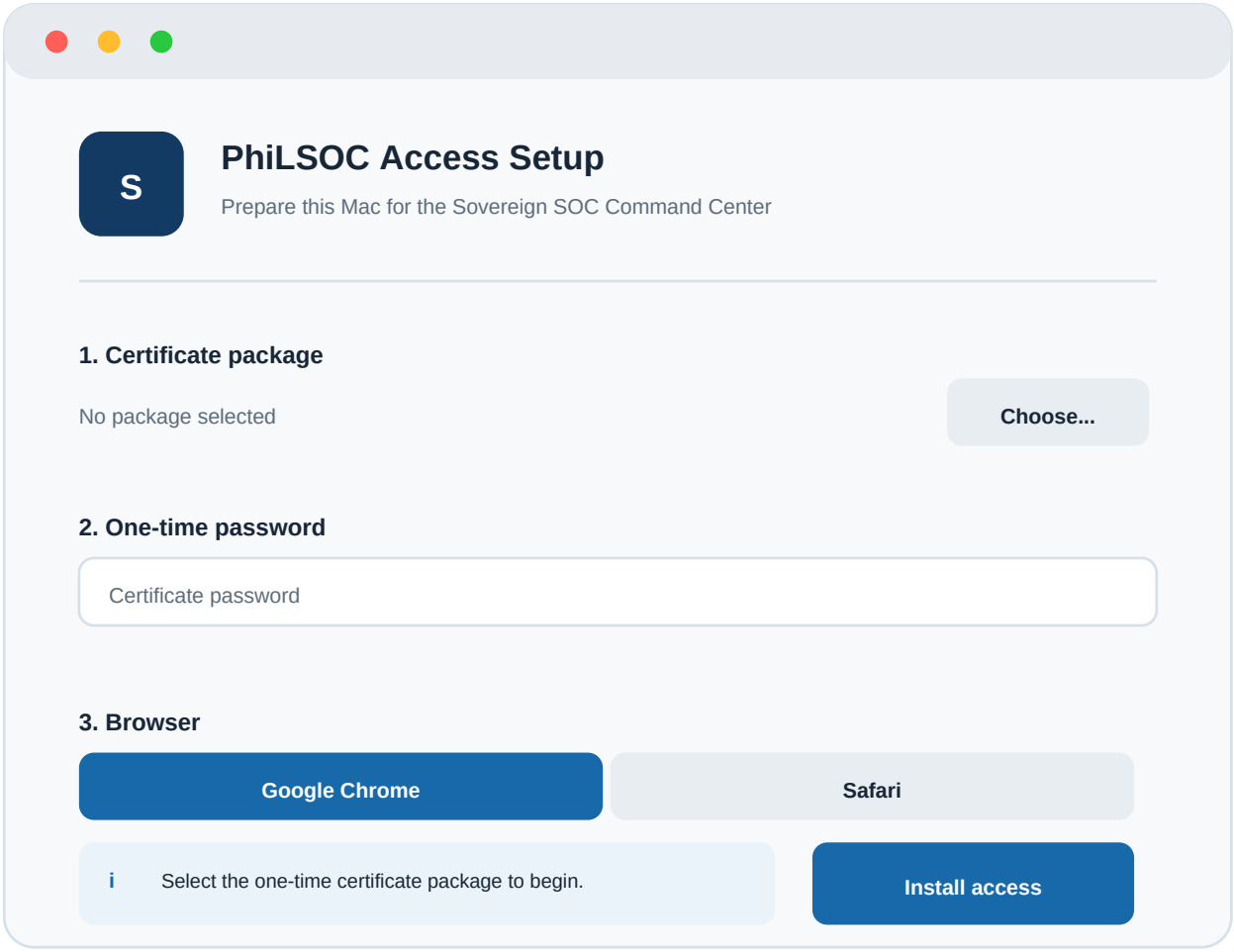
3

Open the app

Open the Applications folder and double-click **PhiLSOC Access Setup**. The notarized release should open normally. If macOS asks whether to open an app downloaded from the Internet, confirm only after verifying that the developer is **Jose Arnold Bagabaldo**.

2. Enroll your PhiLSOC access

The app presents three inputs and performs validation before it changes your login keychain.



1 ## Choose the certificate package

Select **Choose...**, locate the assigned **.p12** or **.pfx** file, and select it. The status changes to **Package selected. Enter its one-time password.**

2 ## Enter the one-time password

Type the password supplied through the separate channel. It is masked while you type and is cleared after success or failure.

3 ## Select the browser

Choose **Google Chrome** or **Safari**. Select the same browser you intend to use for the PhiLSOC console. The selected browser must already be installed in Applications.

4 ## Install access

Select **Install access**. The app validates the package, its complete certificate chain, expiry, approved PhiLSOC root, and device issuer before importing the identity.

3. Approve macOS and finish

1

Approve the trust request

macOS may ask for permission to add the approved PhiLSOC root certificate to your login keychain. Review the prompt and approve it. If requested, use your Mac login credentials or Touch ID directly in the macOS prompt.

2

Wait for the success message

A successful installation displays: **Access is ready for [device identity]. Certificate expires [date].** The **Open PhiLSOC** button becomes available.

3

Open the console

Select **Open PhiLSOC**. The app opens **https://console.philsoc.net/app** in the browser you selected.

4

Allow the browser to use the identity

On first use, the browser or macOS may ask which client certificate to use or may request access to its private key. Select the PhiLSOC identity and approve access. Do not select an unrelated Apple Developer certificate.

> **Successful result**
>
> The Sovereign SOC Command Center opens instead of the nginx message **400 Bad Request - No required SSL certificate was sent**.

What the app changes

Item	Action
Client identity	Imports the approved PhiLSOC certificate and private key into your login keychain.
Root trust	Adds the pinned PhiLSOC pilot root as trusted for the browser selected in the app.
Password	Uses it only during the installation attempt, then clears it from the app.
Browser	Opens the console URL; the browser supplies the client identity during the secure connection.

4. Troubleshooting

Message or symptom	What it means	What to do
400 Bad Request - No required SSL certificate was sent	The browser did not present a valid PhiLSOC client certificate.	Run the app again, select the browser you are actually using, reinstall the assigned package, then fully quit and reopen that browser.
Select a PhiLSOC .p12 or .pfx package	The selected file type is not supported.	Choose the original .p12 or .pfx file supplied by PhiLSOC. Do not rename another file type.
The one-time certificate password was not accepted	The password and package do not match, or the password was entered incorrectly.	Re-enter the password exactly. Confirm that it belongs to the selected package. Request a replacement through the approved channel if needed.
Package does not contain a complete PhiLSOC identity chain	The package is incomplete or is not the approved PhiLSOC enrollment package.	Stop. Obtain a new package from the PhiLSOC administrator. Do not bypass the validation.
Package is not anchored by the approved PhiLSOC root	The certificate chain is not issued by the root pinned in the app.	Do not install it manually. Report the package to PhiLSOC support and request a verified replacement.
Google Chrome or Safari is not installed	The selected browser is missing from Applications.	Install the browser in Applications, or select the other supported browser.
macOS did not approve PhiLSOC trust	The trust change was canceled or rejected.	Run installation again and approve the macOS prompt. If it continues, ask your Mac administrator to check keychain permissions.

5. Ongoing use and security

After enrollment, you normally open the console directly in the same browser. Keep the app for renewal or repair, but do not reuse old enrollment packages unless PhiLSOC instructs you to do so.

Certificate renewal

1

Watch the expiry date

The app shows the certificate expiry date after a successful installation. Arrange renewal before that date.

2

Use the newly issued package

For renewal, select the new .p12 or .pfx package and its new one-time password. Installing a new identity does not require you to remove unrelated certificates.

3

Test access immediately

Select Open PhiLSOC and confirm that the console opens in the selected browser before discarding the delivery messages.

Safe handling checklist

DO	DO NOT
Use only the signed and notarized PhiLSOC app.	Disable macOS security controls to force an unknown copy to run.
Receive the certificate and password through separate approved channels.	Email or chat the certificate and password together.
Select only the assigned PhiLSOC identity in browser prompts.	Choose an Apple Developer ID or another personal certificate for console access.
Report a lost computer or exposed package promptly.	Continue using a certificate that PhiLSOC has revoked or replaced.

When contacting support

Provide your Mac model, macOS version, selected browser, the exact status message shown by the app, and the time the error occurred. Do not send the certificate package, its password, or private-key material in an ordinary support message.

Direct console address

https://console.philsoc.net/app