

CertAid 2.2.6 for MacOS

CertAid 2.2.6 for MacOS

On this page:

[Install/Renew Certificates](#)
[Using CertAid 2.x to Configure Existing Certificates on Mac OS X 10.10 & newer](#)
[See Also](#)

Install/Renew Certificates

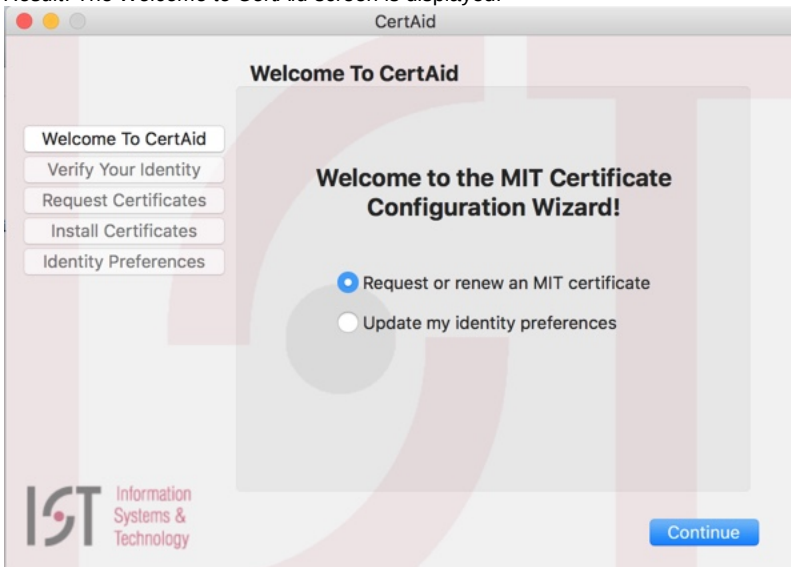
Follow these steps to install/renew your certificates for use in Safari and Chrome on Mac OS X 10.10 and newer.

 CertAid will not successfully install on versions prior OS X 10.10

1. [Download](#) and launch CertAid.

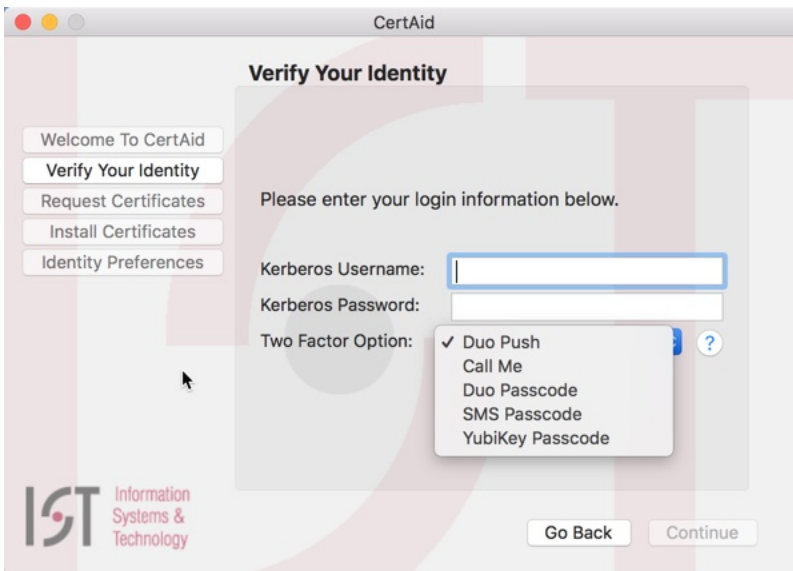
Note: Install any updates if prompted. If you receive a message that states "Certaid can't be opened because the identity of the developer cannot be confirmed", please go to this link: [Mac OS X - Identity of developer cannot be confirmed](#)

Result: The *Welcome to CertAid* screen is displayed.



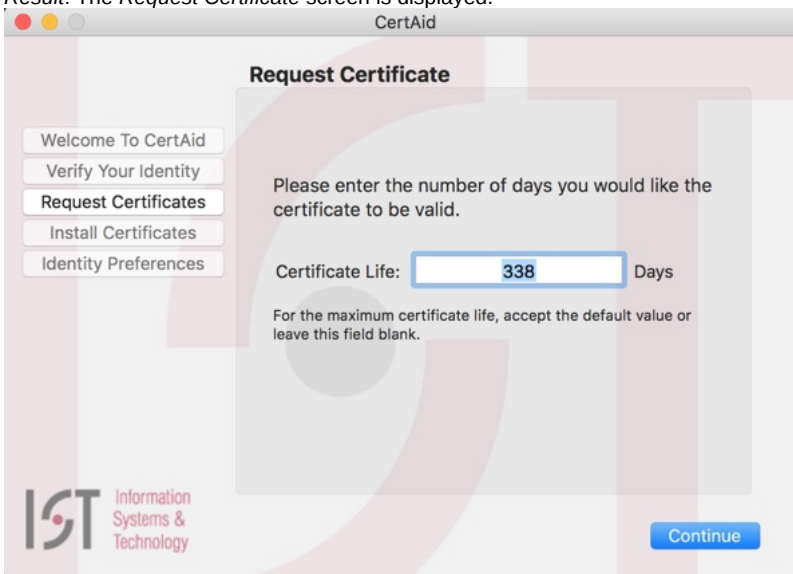
2. Select **Request or renew an MIT certificate** and click **Continue**.

Result: The *Verify Your Identity* screen is displayed.



The screenshot shows the 'Verify Your Identity' screen in the CertAid application. On the left, there is a sidebar with buttons: 'Welcome To CertAid', 'Verify Your Identity' (which is highlighted), 'Request Certificates', 'Install Certificates', and 'Identity Preferences'. The main area has the title 'Verify Your Identity' and a prompt: 'Please enter your login information below.' There are three input fields: 'Kerberos Username:', 'Kerberos Password:', and 'Two Factor Option:'. The 'Two Factor Option' dropdown menu is open, showing options: 'Duo Push' (selected with a checkmark), 'Call Me', 'Duo Passcode', 'SMS Passcode', and 'YubiKey Passcode'. At the bottom right, there are 'Go Back' and 'Continue' buttons. The IST Information Systems & Technology logo is in the bottom left corner.

3. Enter your Kerberos username and Kerberos password, select your **two-factor (Duo) authentication** option, and click **Continue**.
Result: If you used the "Duo Push," "SMS Passcode" or "Call Me" option, you will receive a push notification or call. If you used a Duo or Yubikey passcode, proceed to step 5.
4. Complete your Duo two-factor authentication by accepting the push or entering the code you're given by SMS or phone call.
Result: The *Request Certificate* screen is displayed.



The screenshot shows the 'Request Certificate' screen in the CertAid application. The sidebar on the left is the same as the previous screen, but 'Request Certificates' is now highlighted. The main area has the title 'Request Certificate' and a prompt: 'Please enter the number of days you would like the certificate to be valid.' There is a text input field for 'Certificate Life:' with the value '338' entered, followed by the word 'Days'. Below this, a note states: 'For the maximum certificate life, accept the default value or leave this field blank.' At the bottom right, there is a blue 'Continue' button. The IST Information Systems & Technology logo is in the bottom left corner.

5. Enter a Certificate Life, or leave the default value (the maximum certificate life), and click **Continue**.
Note: Most users should accept the default value.
Result: The *Install Your Certificates* screen is displayed.

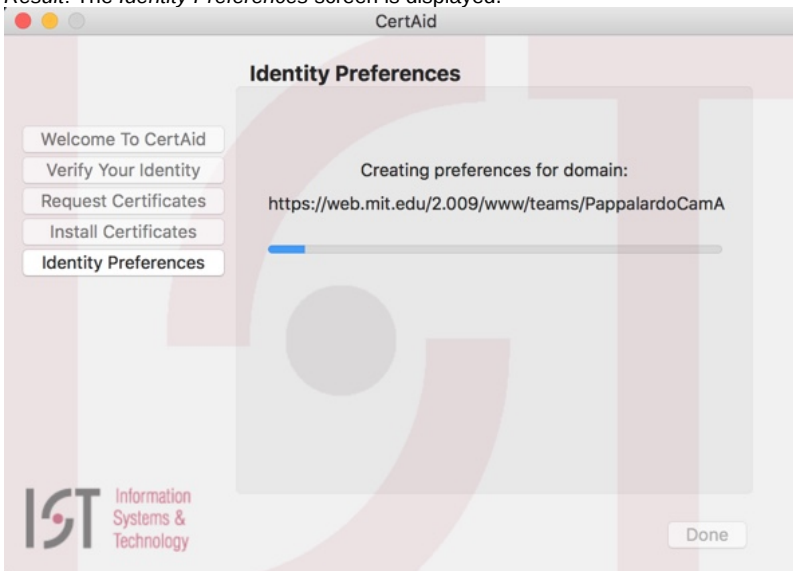


Note: If CertAid finds one or more existing certificates, you will be asked if you want to delete them. If you have used S/MIME for email encryption, do not delete your certificates. For more information, see [Should I Delete My Old or Expired Personal Certificate?](#).

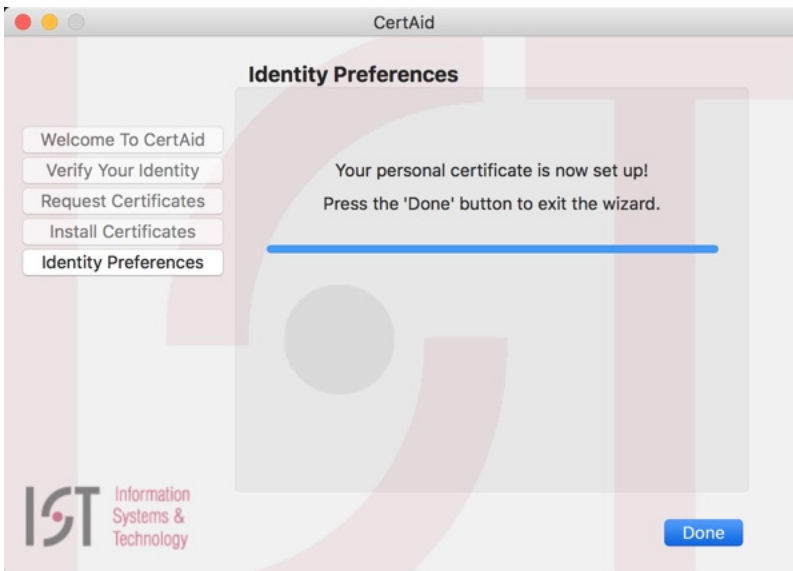
Note: If you are prompted for a keychain password on each certificate added during this step (not just once or twice), manually remove all mit.edu trusted site entries from the users keychain and try again.

- The *Install Your Certificates* window displays the progress of installing the MIT Certificate Authority and your personal certificate. Once these steps are completed, click **Continue**.

Result: The *Identity Preferences* screen is displayed.

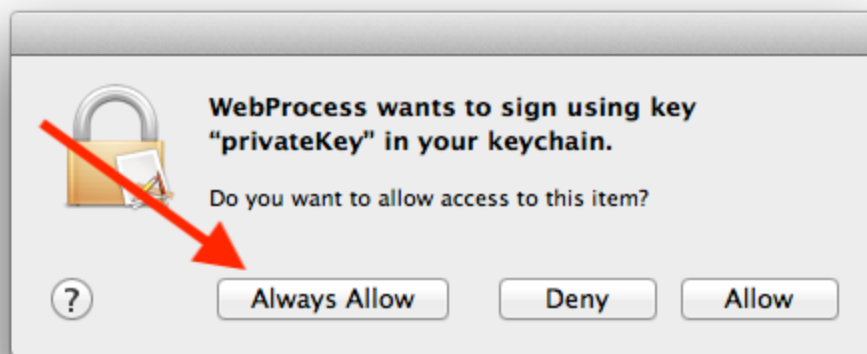


- The *Identity Preferences* window displays the progress of configuring your personal certificate to work with certain certificate-protected MIT websites. Once completed, click **Done**.



Result: CertAid quits.

8. The first time you attempt to use your new certificate, you will see this prompt. Click **Always Allow**. If prompted for a password, enter the logon password for the MacOS user account.



 You *must* select **Always Allow**, otherwise this prompt will continually recur. This is often mistaken for a failed password entry attempt, but it is the expected behavior when **Allow** is clicked instead of **Always Allow**.

Using CertAid 2.x to Configure Existing Certificates on Mac OS X 10.10 & newer

- [archive:CertAid for Safari and Google Chrome]

See Also

- [CertAid Landing Page](#)
- [Certificates Landing Page](#)