

# InCommon Personal (Client) Certificates

## Overview

This will walk you through the process of obtaining and installing an InCommon Personal (Client) Certificate.

## Obtaining InCommon Personal (Client) Certificate

1. In your preferred browser (Chrome, Firefox, etc...) navigate to [www.uc.edu/infosec/services/cert.html](http://www.uc.edu/infosec/services/cert.html)



The screenshot shows a web browser window with the address bar containing [www.uc.edu/infosec/services/cert.html](http://www.uc.edu/infosec/services/cert.html). The page header includes the University of Cincinnati logo and navigation links: UC Home, Visit UC, Support UC, Directories, and UC Tools. A red banner reads "INFORMATION SECURITY SERVICES". Below this is a navigation menu with links for Home, Policies, Awareness, Services (highlighted), Account & Password Help, and Compliance & Law. The main content area is titled "Security Certificates" and contains the following text:

**Risk Management**

**Shredding**

**Security Certificates**

**Intel Security Endpoint Protection Services**

**Free Antivirus**

**Report an Incident**

**Contact Us**

**UCIT Homepage**

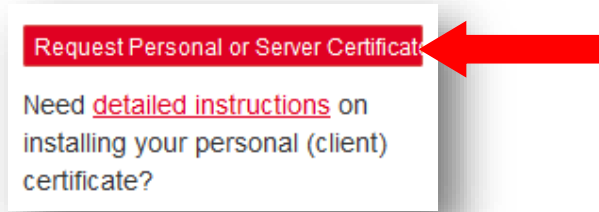
Public Key Certificates are electronic documents used to provide identification by using a digital signature and binding it to a public key. In order to properly identify a person or resource using a certificate, they must be validated against an issuing **Certificate Authority (CA)**. Most Web browsers and other Internet applications hold trust lists for the most common Certificates Authorities on the Internet.

All new personal and server electronic certificates used at the University of Cincinnati are issued by InCommon, a federation organized to provide trust frameworks and standards in order to share research institutions in the United States. Implementation of InCommon certificates revocation, and management of the certificates and ensures that all certificates are per unit charge for use of these certificates by UC staff, faculty and systems as the result of our enterprise license agreement with InCommons.

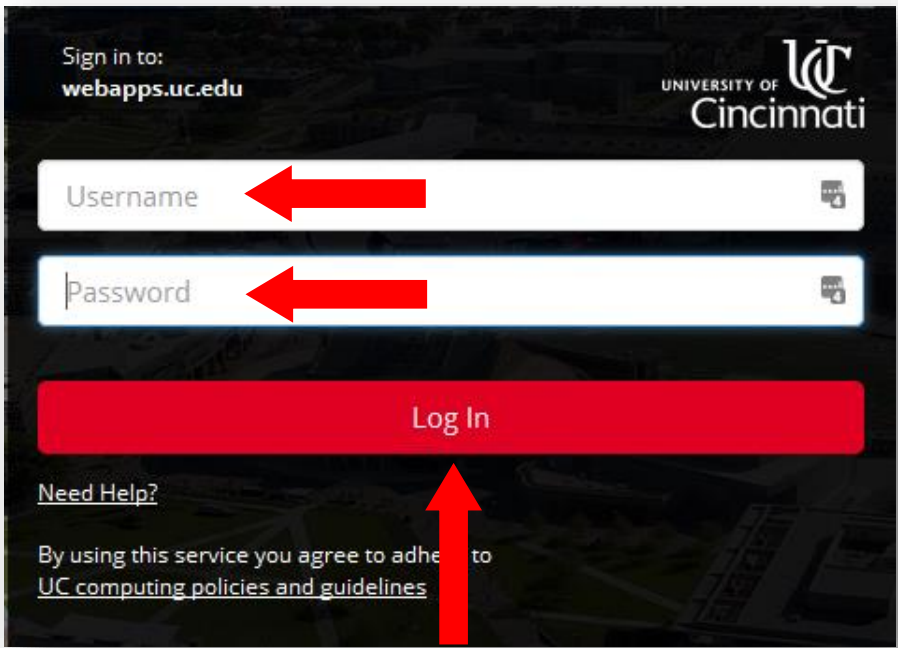
**SSL Certificates**

Secure Socket Layer (SSL) is a security protocol used to secure Internet connections. It's typically used as a secondary protocol that is layered on top of

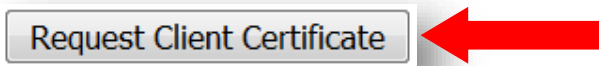
2. Select "Request Personal or Server Certificate" on the right



3. Enter your UC username and password, then click Login



4. Select "Request Client Certificate"



- The form will be pre-filled with everything other than “Pass-phrase” and “Re-type pass-phrase.” In these fields enter a strong pass-phrase that you can remember. Then click “Enroll.”

**S/MIME Certificate Enroll**

Access Code: \* [REDACTED]

First Name: \* [REDACTED]

Middle Name: [REDACTED]

Last Name: \* [REDACTED]

Email: \* [REDACTED]@ucmail.uc.edu


Pass-phrase: \* [REDACTED]

Re-type pass-phrase: \* [REDACTED]

[ENROLL] [CANCEL]

Red arrows point to the Pass-phrase and Re-type pass-phrase fields, and the ENROLL button.

- An email will be sent to your UC email account

 **InCommon**® Certificate Manager

---

**Confirmation**

---

**You have requested a S/MIME Certificate with the follow details:**

Email: [REDACTED]@ucmail.uc.edu,  
Name: [REDACTED]

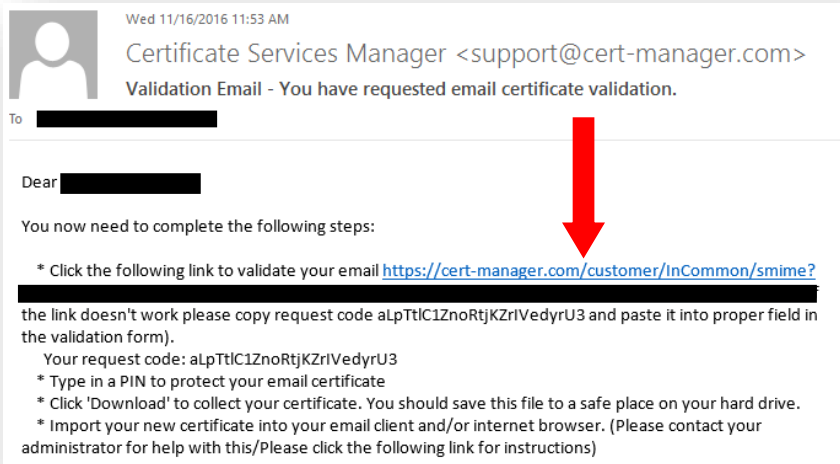
---

We have sent you an email containing an enrollment link in order to complete the rest of the enrollment process

---

[BACK]

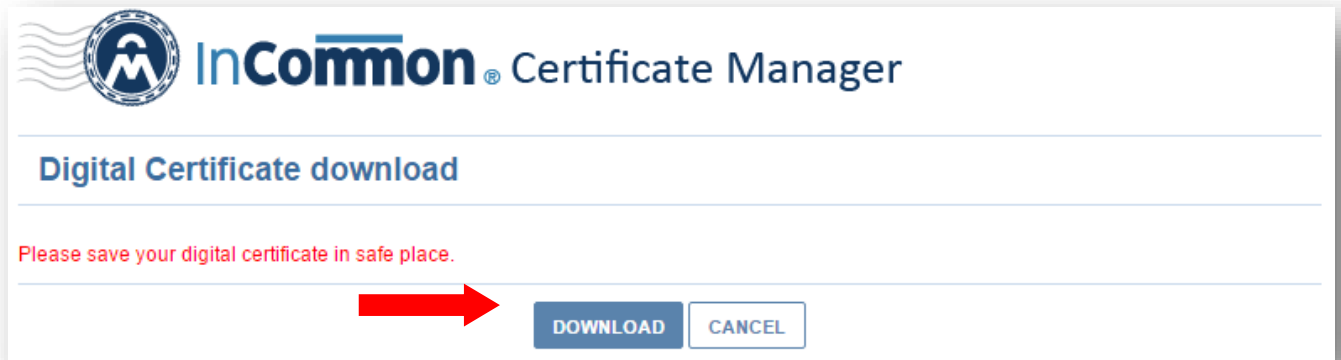
7. Open the email and click the link inside



8. Enter a PIN for the "PIN" and "Re-type PIN" fields. Enter an address if none is filled in for you. Then click Validate

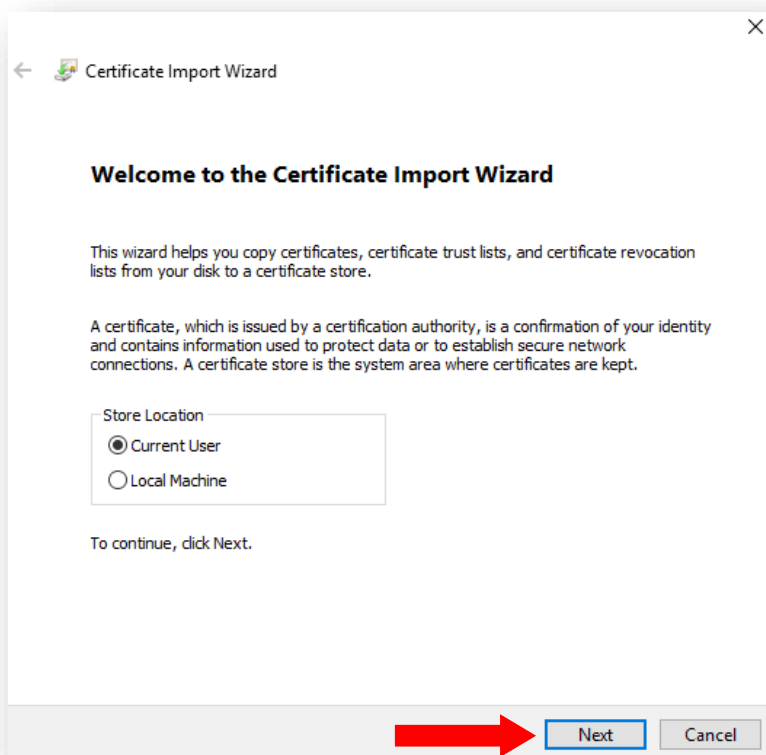


9. Click Download to download your certificate.

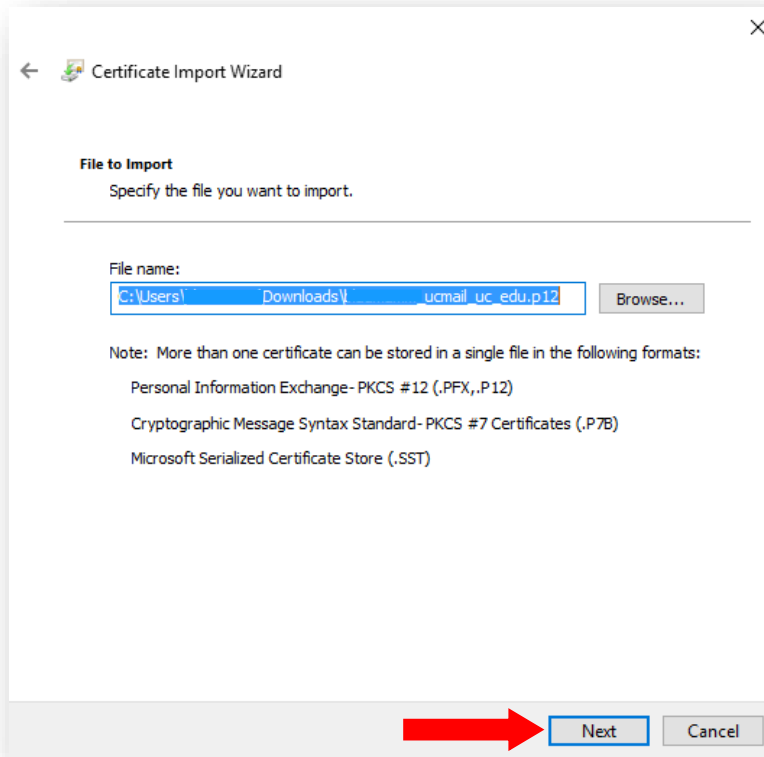


10. After downloading, it is important to move the file from your "Downloads" folder to a safe location

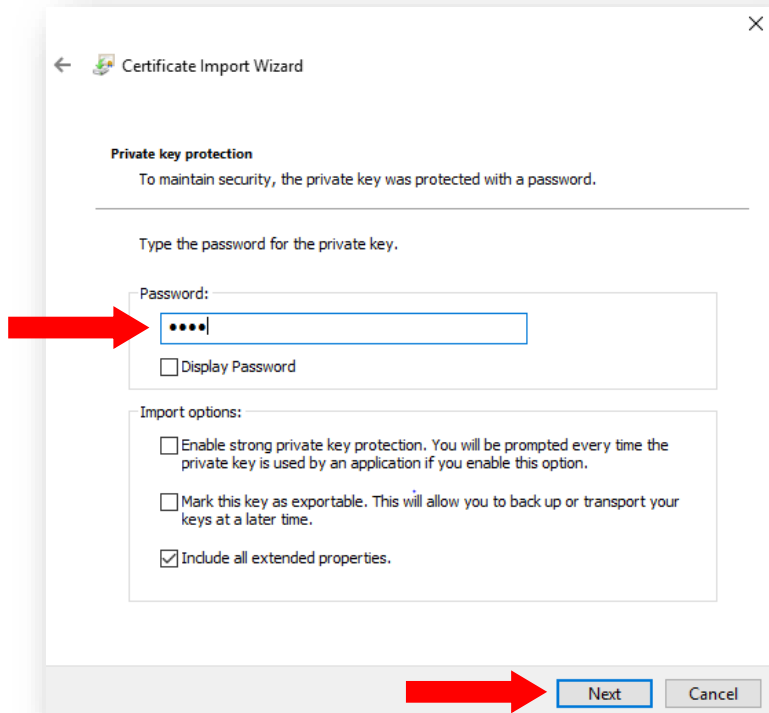
11. After you've moved the file, double-click it. On the pop-up window click "Next."



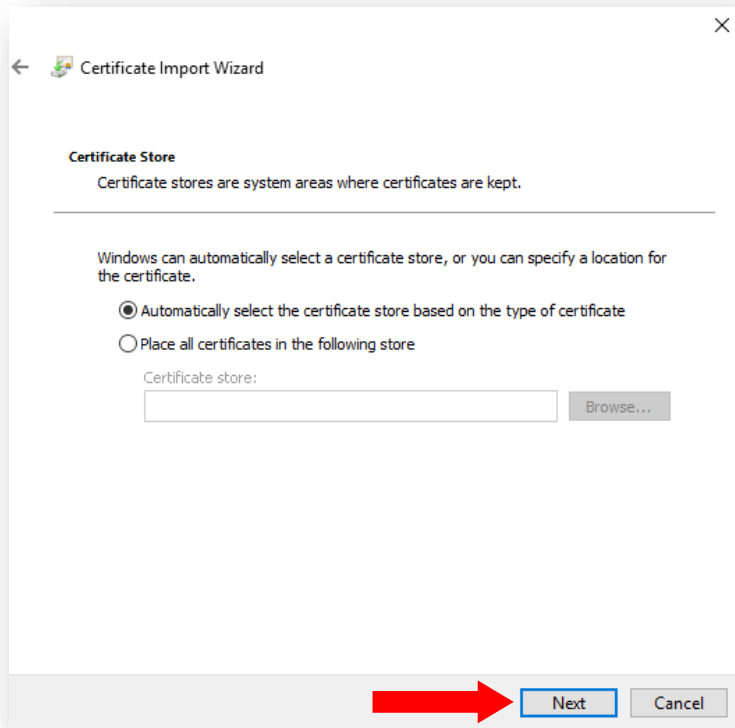
12. Click “Next.”



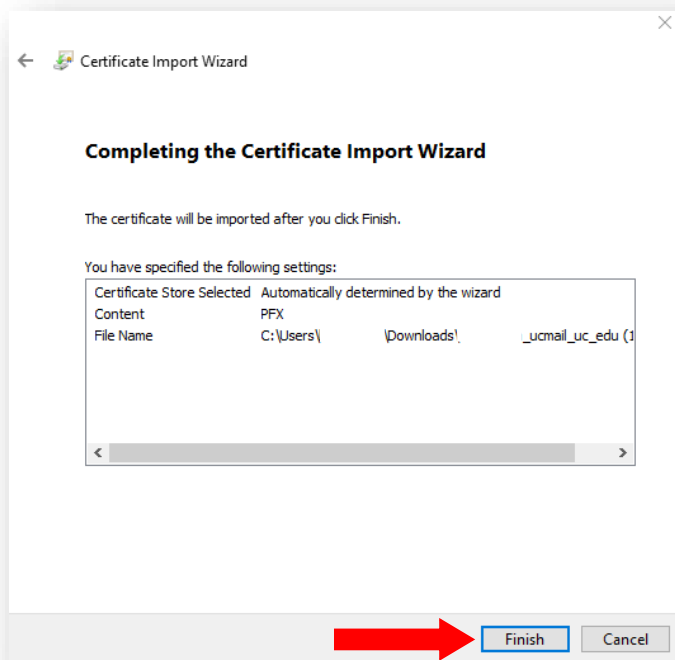
13. Enter the PIN you created in Step 8 and then click “Next.”



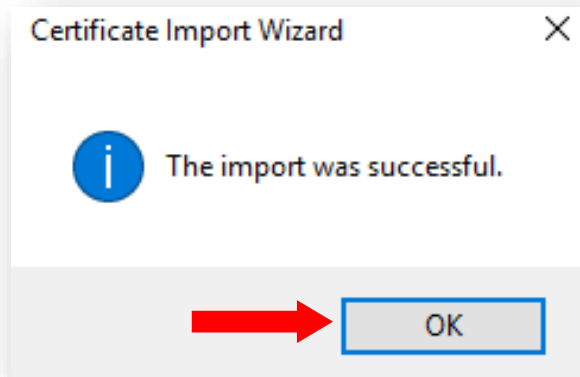
14. Click "Next."



15. Click "Finish."



16. If the setup was successful, the following window will be presented. Click "OK."



You have successfully obtained an InCommon Client Certificate!