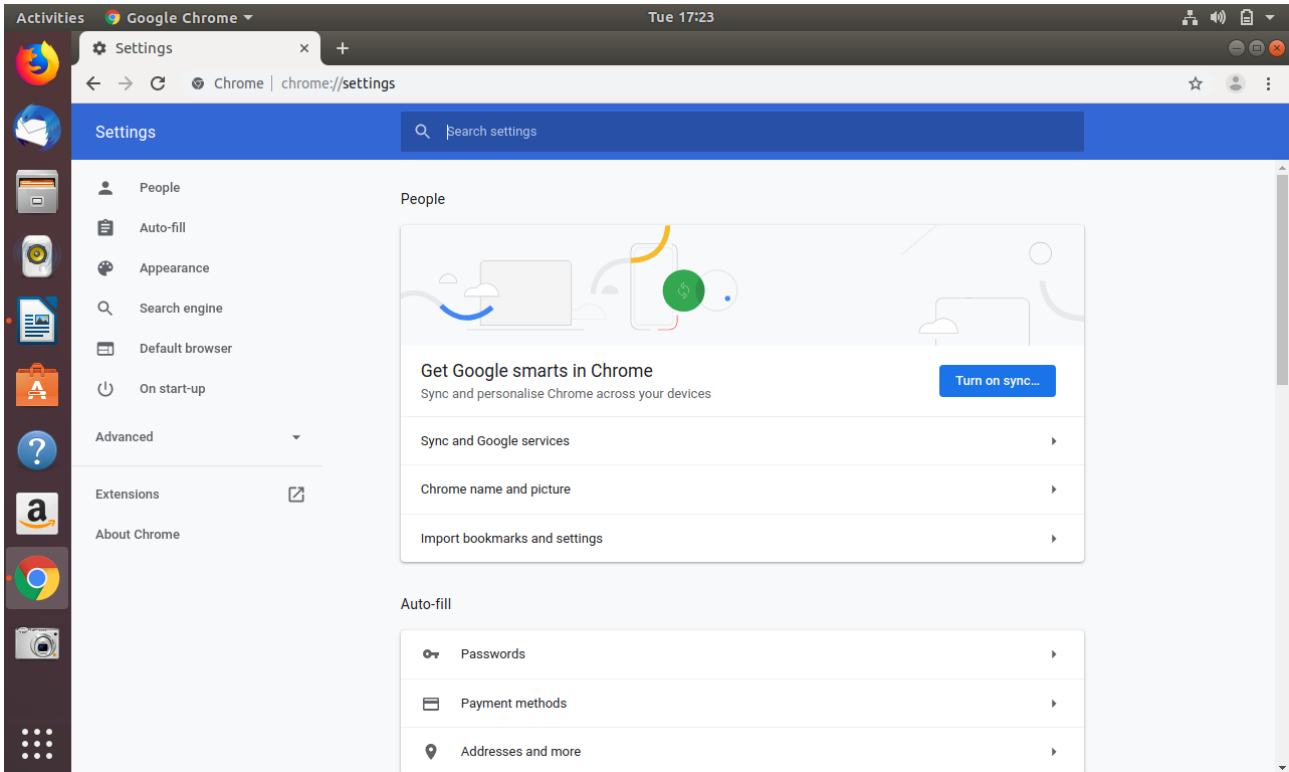


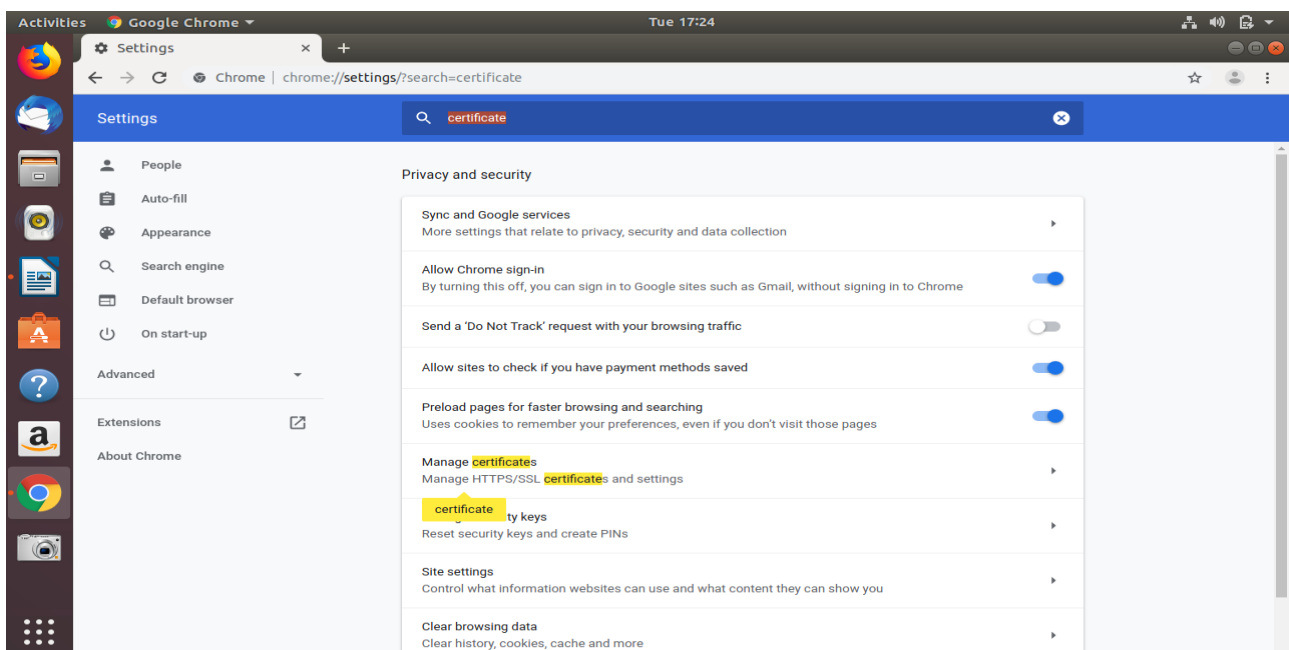
New IITD CA Certification Installation Procedure (Linux Operating System)

Google Chrome-

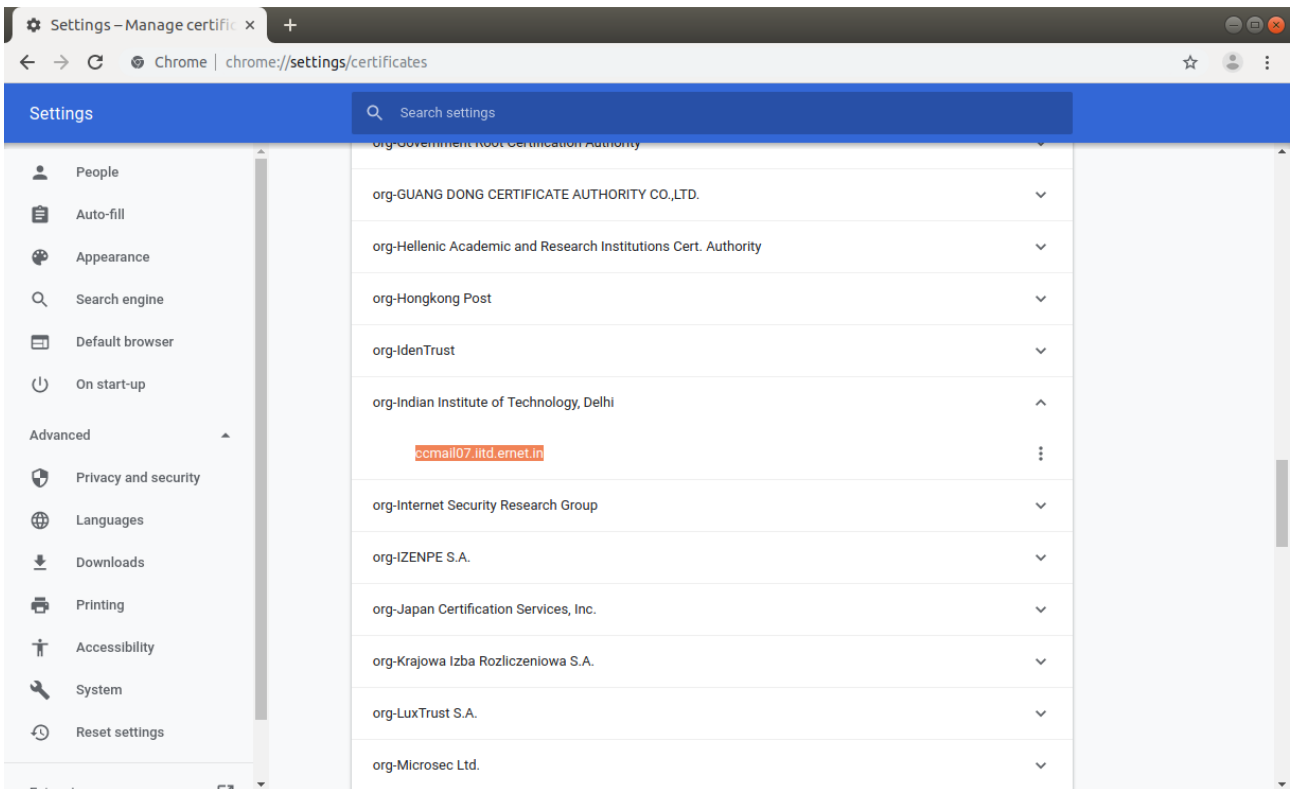
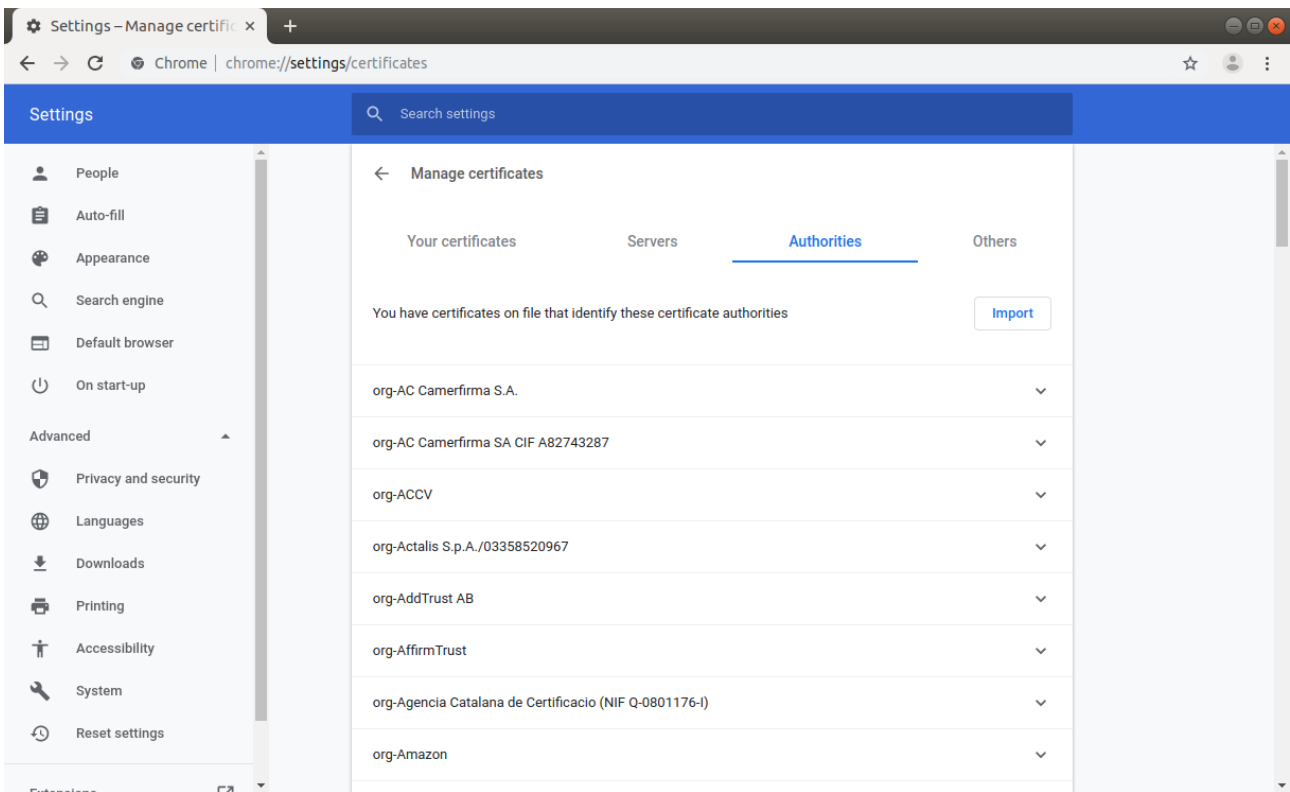
1. Open **Google Chrome** > click on **Menu option** & go to **Settings**



2. Search certificate and open “**Manage Certificate**” (If old IITD CA certificate not installed then go to step 4).



3. Click on “Authorities” and find Certificate of “org-Indian Institute of Technology, Delhi”, expand it and Delete it.



4. For New IITD CA certificate Installation, **Open below mentioned Link in Google Chrome**

http://www.cc.iitd.ac.in/CSC/index.php?option=com_content&view=article&id=53&Itemid=57

OR follow this path “iitd.ac.in/content/centres/certificate”

5. **Download [New IITD CA certificate](#) and open file location**

Certificates

administrator

All CSC and ACSS facilities that require users to provide their Kerberos passwords are set up over secure **TLS/SSL encrypted** channels. Examples of such facilities are web-pages using the [https protocol](#), [802.1x authentication](#) for wired or wireless networks, [ssh logins](#), [VPN connections](#), email access through [imap](#) and [SASL authentication](#) for [smtp](#).

Setting up of encrypted **TLS/SSL** connections require the server to present SSL certificates to the client, so that the client may authenticate the server. This is to prevent against possible [man in the middle attacks](#). **Please note that accepting a server certificate without verifying its authenticity makes a user vulnerable to attacks.**

IITD uses self-signed certificates for some services whereas it uses Letsencrypt/Entrust Certificates from Wifi/Mail services (see <https://letsencrypt.org/> and <https://www.entrust.com/>). Wifi/802.1x Network access as well as Mail clients and web browsers may ask to examine and accept these certificates every time on start up. The users are requested not to make it a practice of accepting such certificates. Instead, the users may download the old [IITD CA certificate](#) (valid upto Aug 27 10:55:31 2019 GMT) and install it as a valid CA ([certificate authority](#)). The old [CA certificate](#) (valid upto Aug 27 10:55:31 2019 GMT) can be installed through the [Preferences->Advanced->Certificates](#) tabs. You may require the old [IITD CA Certificate in DER format](#) (valid upto Aug 27 10:55:31 2019 GMT) for some systems.

In most operating systems & browsers the letsencrypt X3 CA and Entrust CA should be already available. If required you may download and install Let's Encrypt Authority X3 (IdenTrust cross-signed): [\[pem\] \[der\]](#) or from here [Letsencrypt X3 Intermediate certificate](#) and Entrust CA from here [Entrust Bundled Certificate](#).

Please see [HowTo: Import the CAcert Root Certificate into Client Software](#) for details (follow the procedure outlined in this link, but use Letsencrypt X3/IITD's [CA certificate](#) instead of CAcert's).

Please verify the SHA1 and MD5 fingerprints of the old [IITD CA certificate](#) before installing:

SHA1 Fingerprint=13:DD:BF:06:B5:04:33:2E:94:81:71:DD:14:E1:26:D7:B6:C0:93:18
MD5 Fingerprint=17:9F:C1:3E:D9:0B:24:E7:2E:DC:41:5C:14:F9:4B:3C

IITD new self-signed certificates for CA with validity upto Jun 22 05:28:29 2029 GMT are:

[New IITD CA certificate](#)

SHA1 Fingerprint=88:f6:de:a8:a3:b1:72:1c:3f:d3:47:2c:d3:08:17:d2:58:67:e5

MAIN MENU

- Home
- Facilities
- People
- Complaints and queries
- Frequently asked questions
- Getting started
- IITD IT usage policy
- IITD privacy policy
- Network access and monitoring policy
- Password reset policy

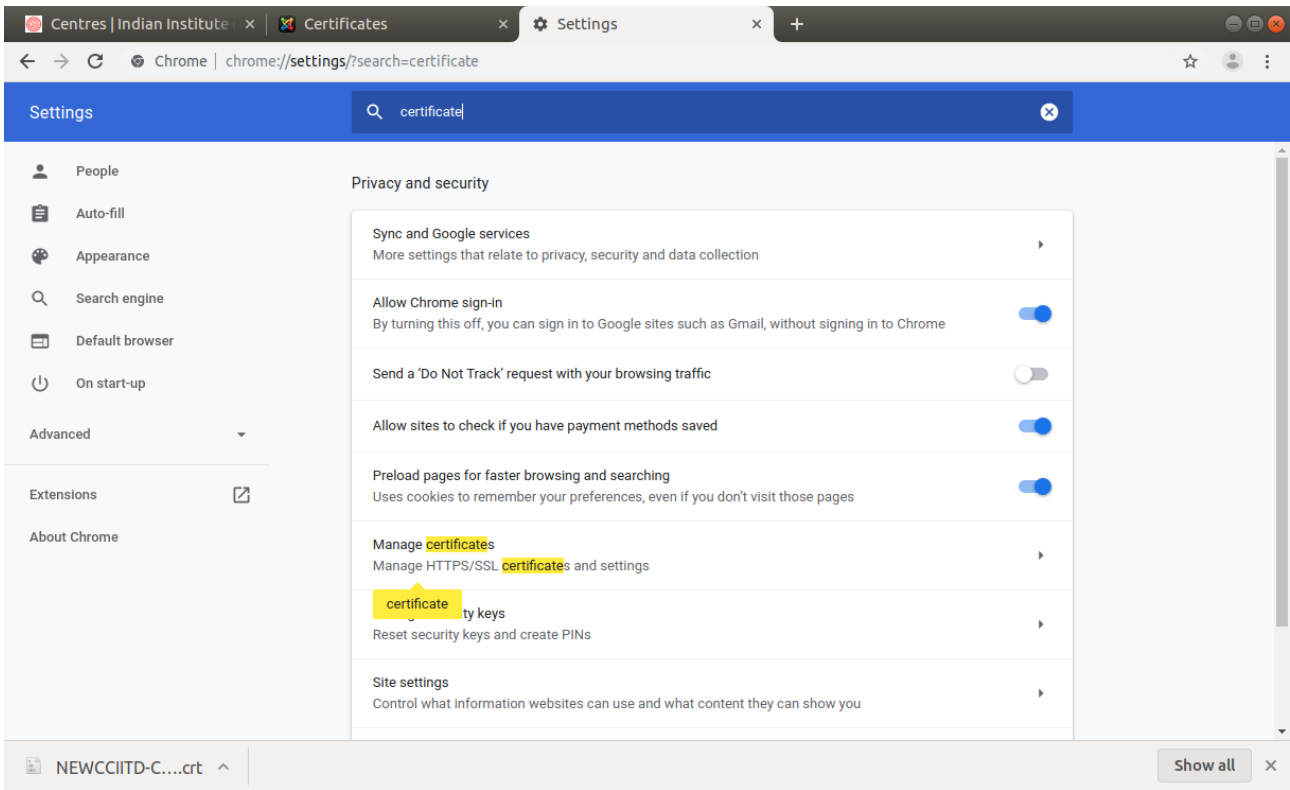
RESOURCES

- Change kerberos password
- Edit your LDAP profile
- Users and mailing lists
- Certificates**
- Home spaces and CIFS shares
- ownCloud
- Proxy for internet access
- Email
- User web pages
- Calendar server
- Network time servers
- Internet access for visitors

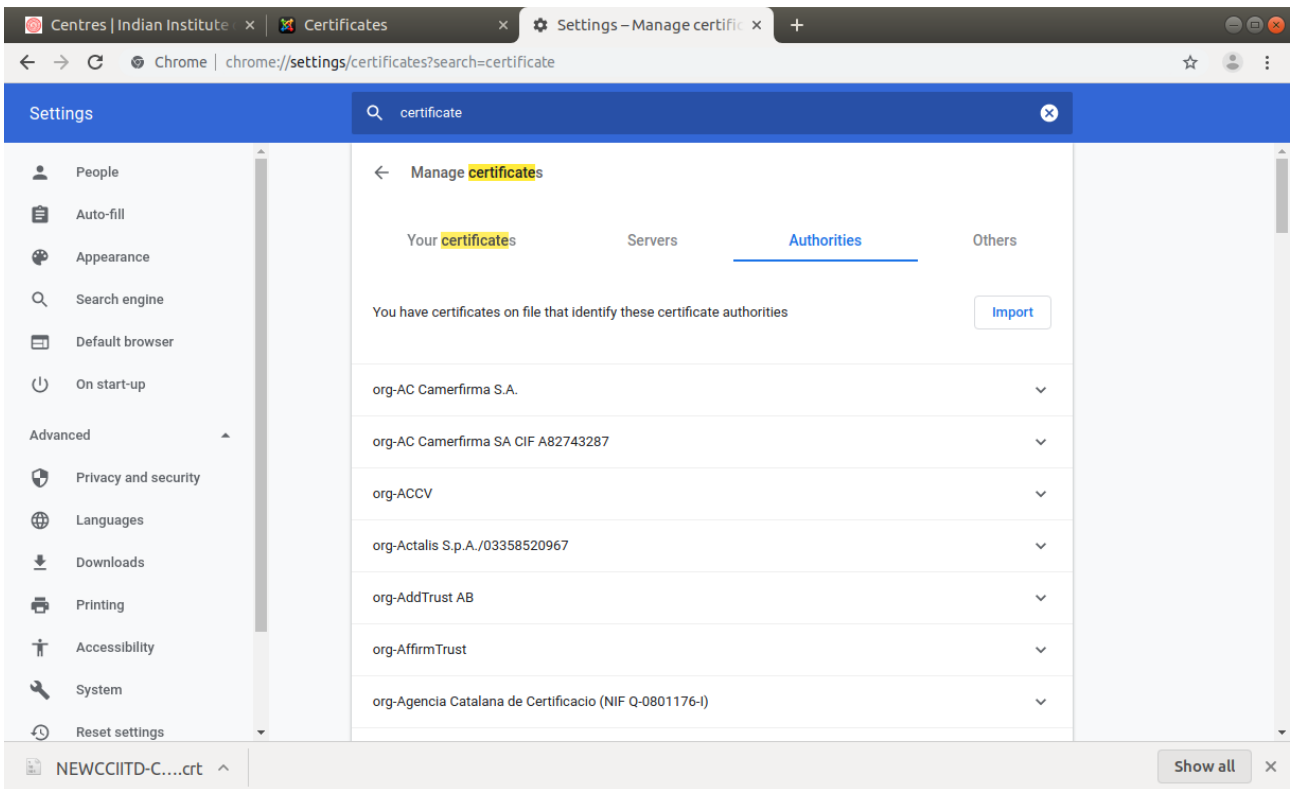
LATEST NEWS

- Office 365
- [Wired 802.1x Configuration Guide for Hostels](#)
- [Docker: Container Management Service](#)
- [Revision of IITD Internet Access Policies](#)
- [HPC@IITD: Padum](#)
- [New Software Repository](#)
- [New Disaster Recovery Data Centre](#)
- [Eduroom](#)
- [IIT Delhi new network backbone](#)
- [ownCloud](#)
- [Download server](#)
- [Software under Dreamspark](#)
- [Home space](#)
- [IITDWiki](#)
- [Apple device configuration](#)
- [SMTP auth](#)
- [Calendar server](#)
- [Private web pages](#)
- [Baadal: the IITD computing cloud](#)
- [Roundcube webmail](#)
- [Windows software](#)
- [Password reset policy](#)
- [CSC courses for 2011](#)
- [Digital signing of emails](#)
- [Mailing lists and aliases](#)

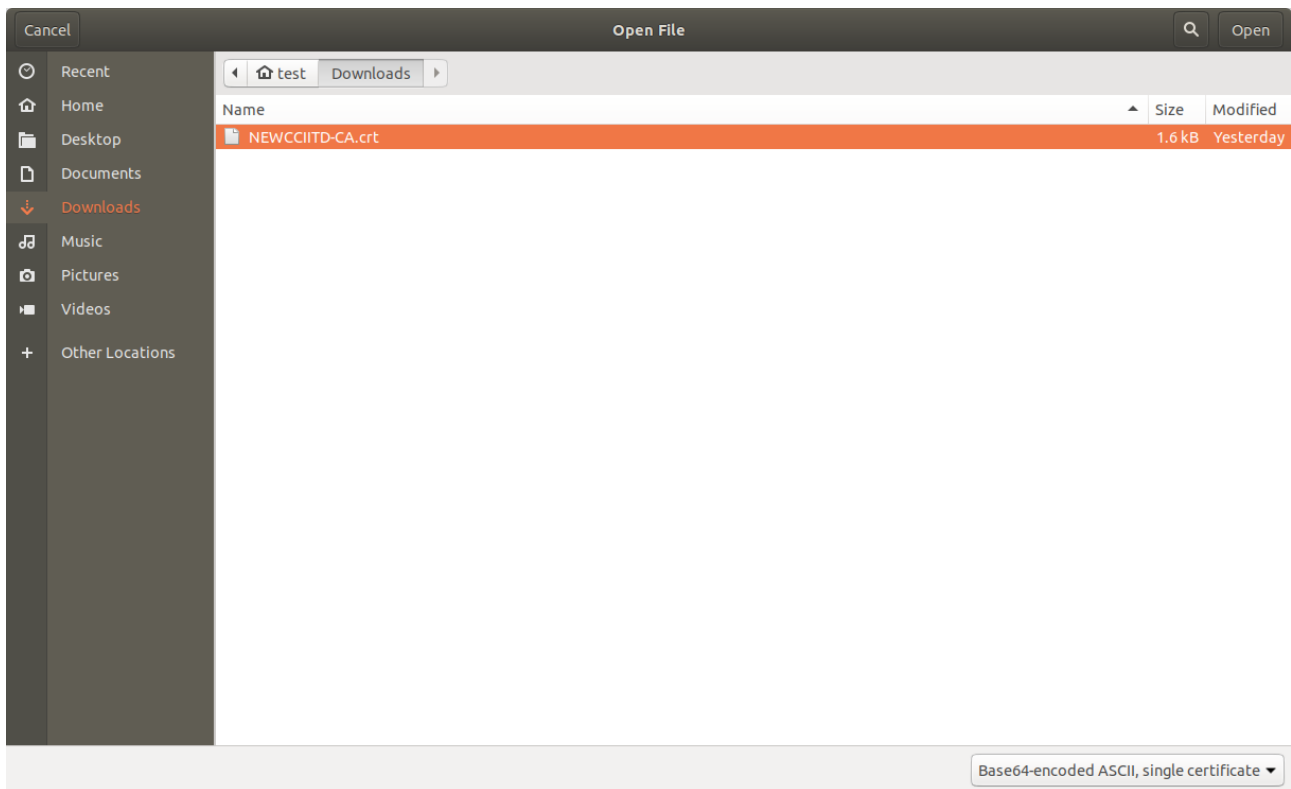
6. Go to Menu Option , Select Settings and Search Certificate.



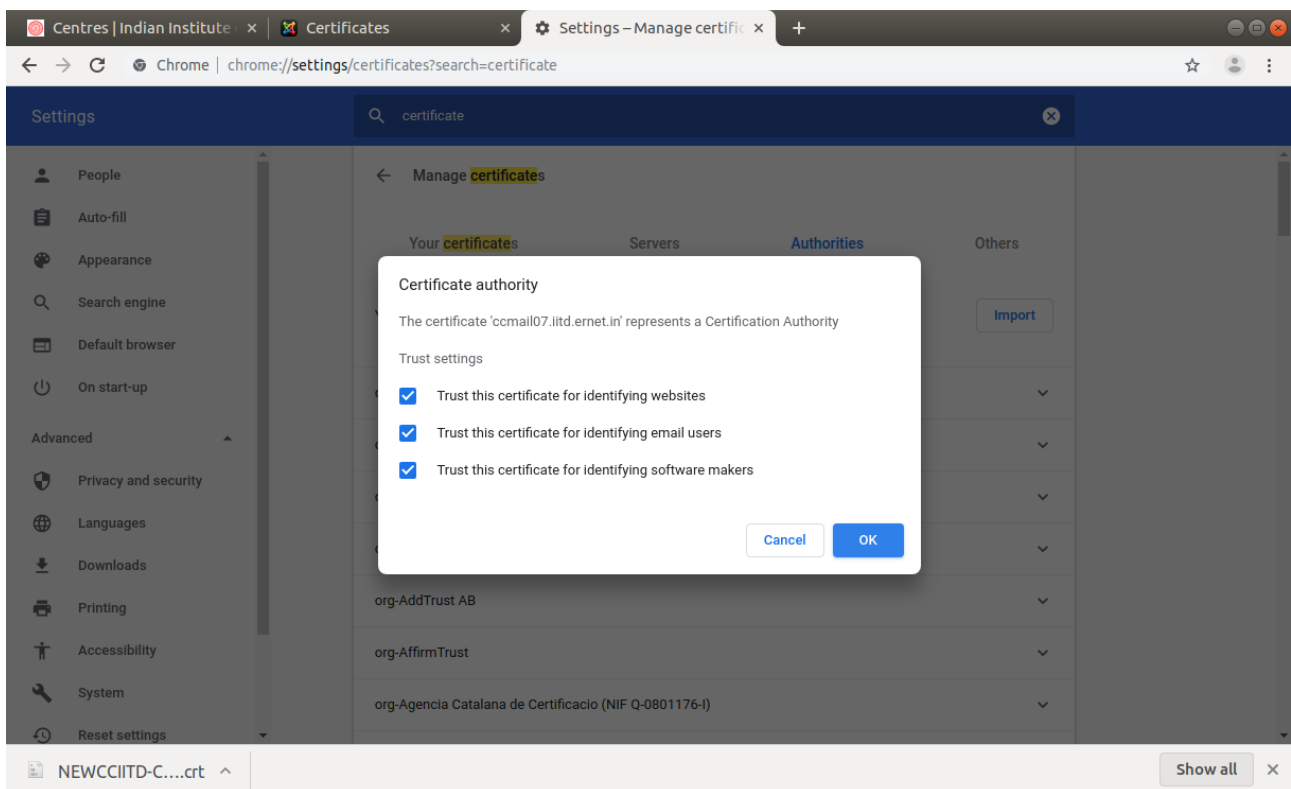
7. Select Authorities and Select Import.



8. Browse your **New IITD CA Certificate** (in step 5).



9. Follow the steps shown in Picture.



Now the certificate is installed.