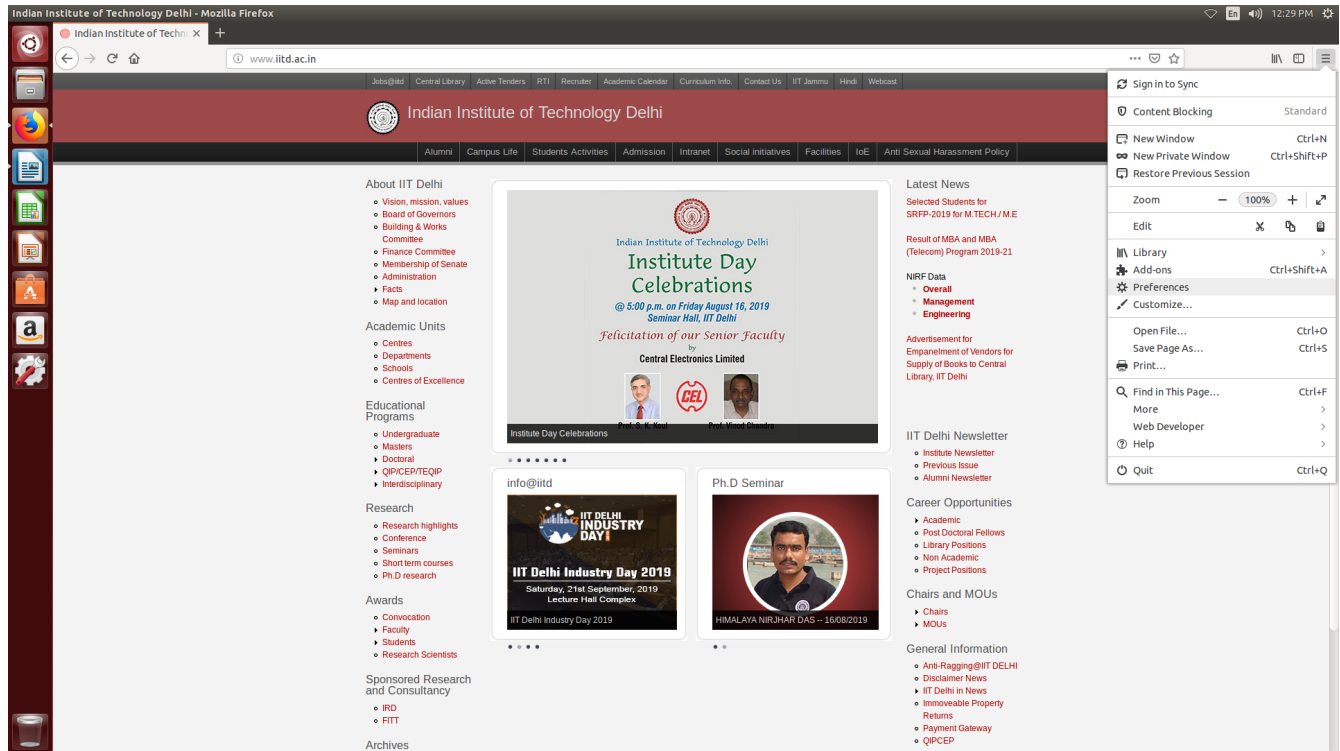


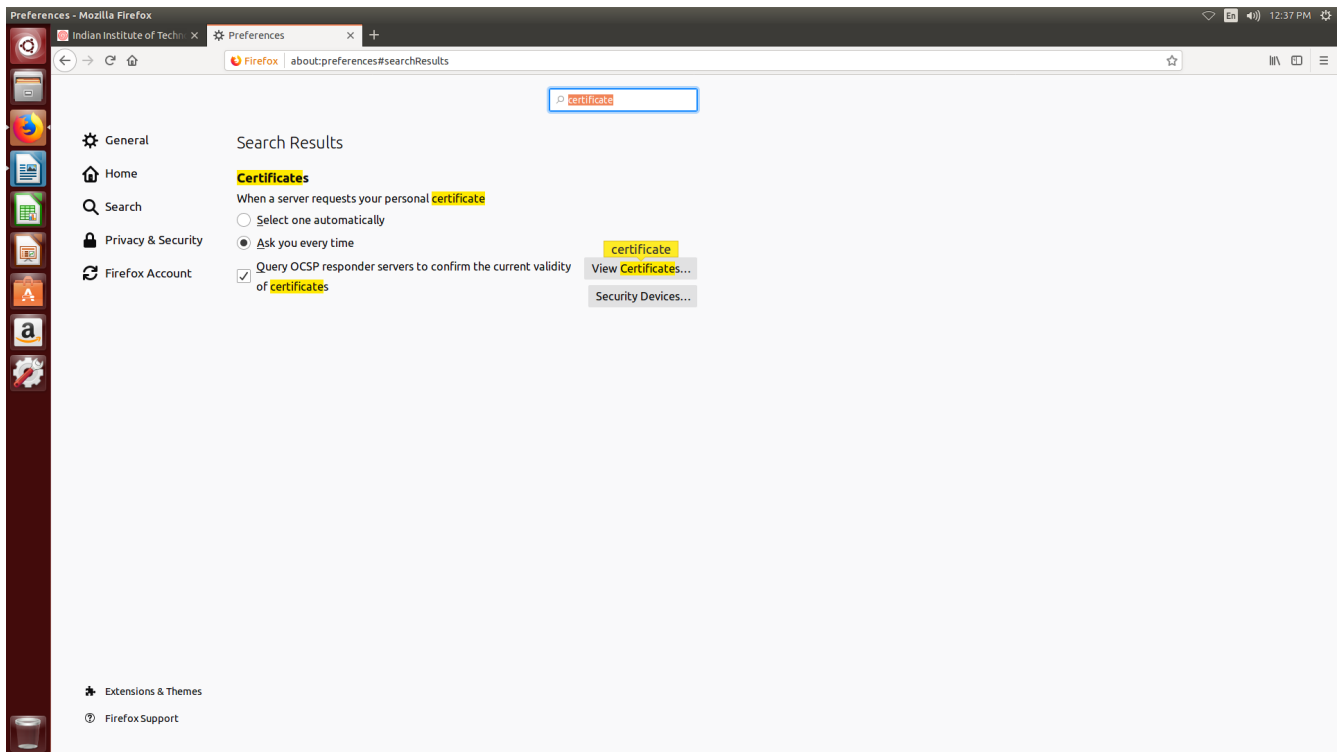
# New IITD CA Certification Installation Procedure (Linux Operating System)

## Mozilla Firefox –

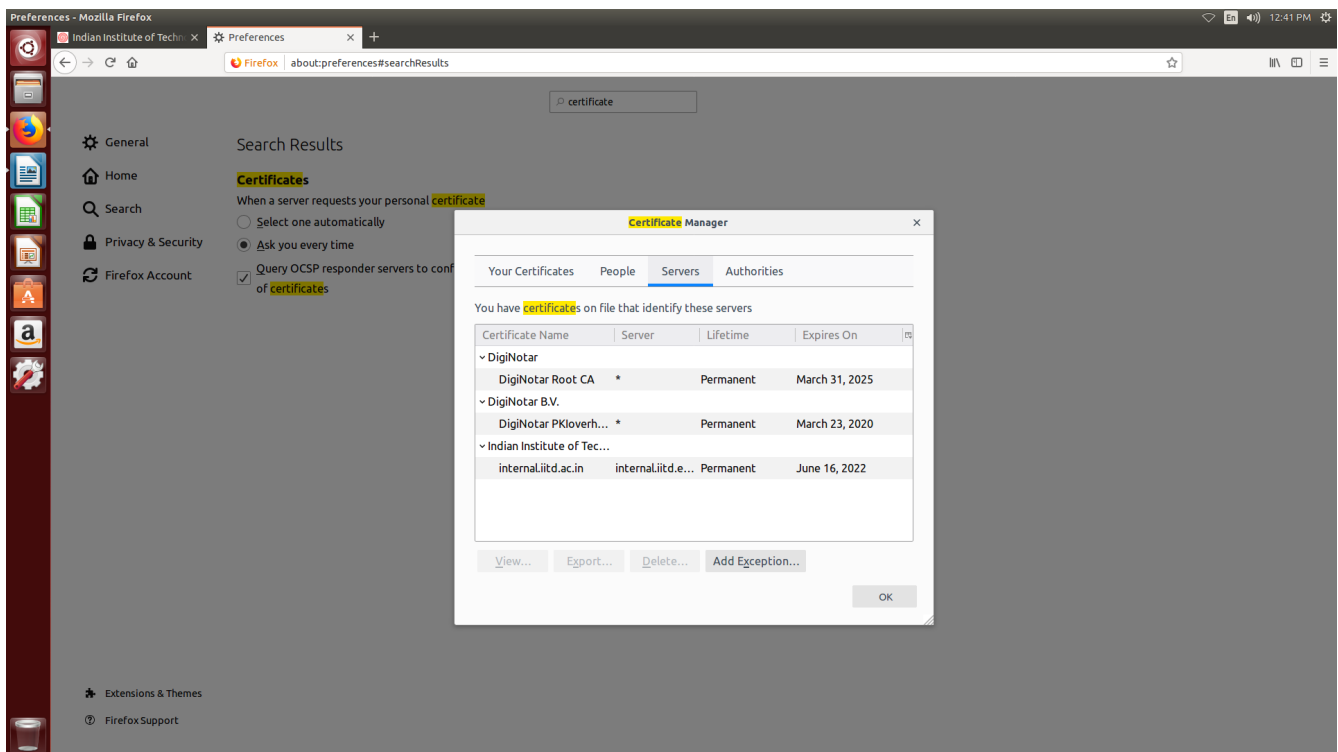
1. Open your Mozilla Firefox, **Open Menu** select **Preferences**.



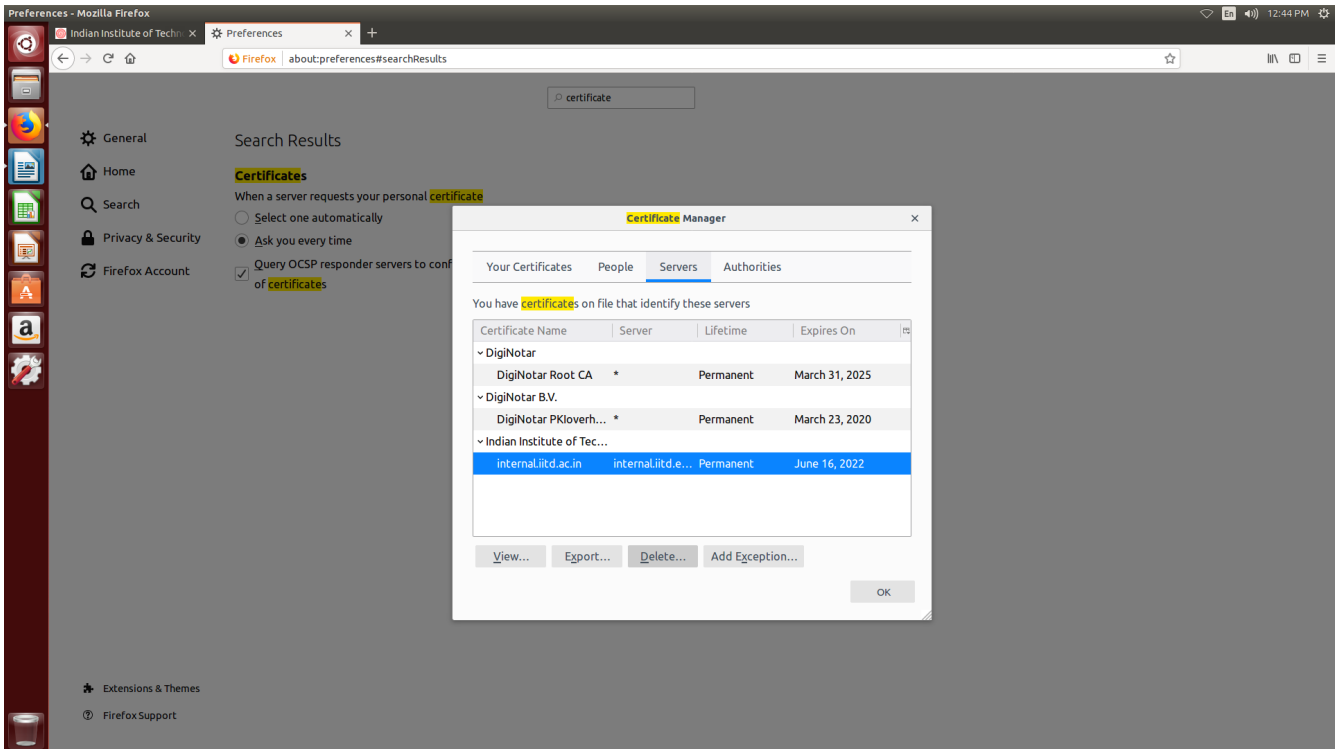
## 2. Search Certificate (If already installed old IITD CA certificate or go to Step 6).



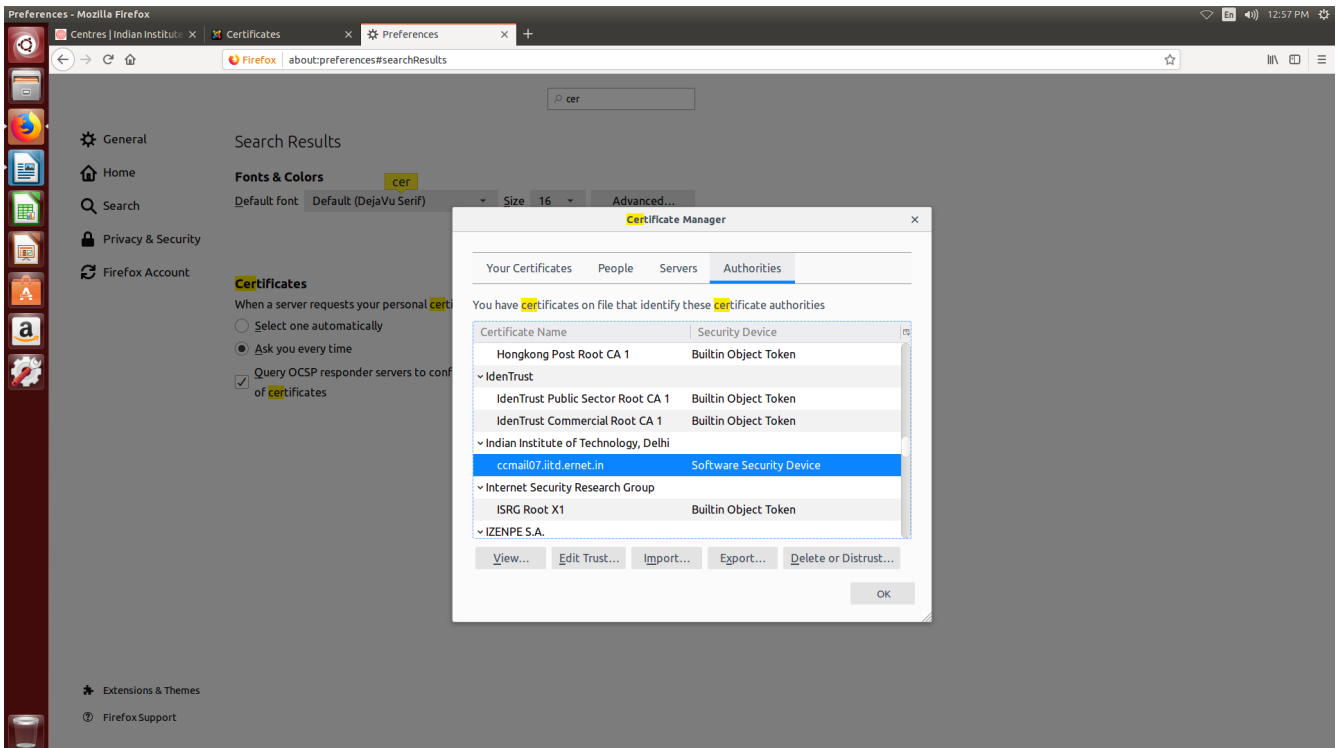
## 3. Click on View Certificate and go to Servers.



#### 4. Delete Indian Institute of Technology Delhi old entry (If Any).



#### 5. Change tab to Authorities > find the content “Indian Institute of Technology Delhi” and delete it also.



## 6. For New IITD CA certificate Installation, Open below mentioned Link

[http://www.cc.iitd.ac.in/CSC/index.php?option=com\\_content&view=article&id=53&Itemid=57](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](http://iitd.ac.in/content/centres/certificate)”.

The screenshot shows a web browser window displaying the 'COMPUTER SERVICES CENTRE' website. The page title is 'Certificates' and the URL is 'www.cc.iitd.ac.in/CSC/index.php?option=com\_content&view=article&id=53&Itemid=57'. The page content includes a navigation menu, a main menu, and a list of resources. The main content area is titled 'Certificates' and contains the following text:

All CSC and ACSIS facilities that require users to provide their Kerberos passwords are set up over secure TLSS/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 imaps and SASL authentication for smp.

Setting up of encrypted TLSS/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 Letencrypt/Entrust Certificates from WebMail services (see <https://letsencrypt.org/>) and <https://www.entrust.com/>). Wi&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 (IdeaTrust cross-signed): [ipomj@derj](#) 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 CAcerts).

Please verify the SHA1 and MD5 fingerprints of the old IITD CA certificate before installing:

SHA1 Fingerprint=13.DD.8F.06.B5.04.33.2E.94.91.71.D0.14.E1.26.D7.B6.C0.93.1B  
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=88.46.de.a8.a3.b1.72.1c.3f.d3.47.2.38.d3.08.17.d2.58.67.e5  
MD5 Fingerprint=b0.2a.b7.2c.7a.27.08.a8.62.40.a4.c6.04.4a.25.d5

**New IITD CA Certificate in DER format**

SHA1 Fingerprint=4a.f3.9d.e7.c7.5f.8b.5b.tc.42.ce.21.1b.c8.9f.08.09.2b.00.6b  
MD5 Fingerprint=15.54.db.e6.88.2d.c1.c.0fc2.2a.ae.0a.08.ce.5e

Please verify the SHA1 and MD5 fingerprints of the [New IITD CA certificate](#) / [New IITD CA Certificate in DER format](#) before installing

Last Updated on Tuesday, 25 June 2019 21:09

The left sidebar contains a 'MAIN MENU' with links to Home, Facilities, People, Com complaints and queries, Frequently asked questions, Getting started, IITD IT usage policy, IITD privacy policy, Network access and monitoring policy, and Password reset policy. Below this is a 'RESOURCES' section with links to 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, Web hosting service, IITD campus Wi, Wired 802.1x in Hostels, IITD student projects database, Windows software, Software repository, Cloud Computing as IITD, SVN & Git, and IITD Discussion forum. The right sidebar contains a 'LATEST NEWS' section with a list of recent updates, including Office 365, Wired 802.1x Configuration Guide for Hostels, Docker, Container Management Service, Revision of IITD Internet Access Policies, IITD-IITD Padm, New Software Repository, New Disaster Recovery Data Centre, Ejuram, IIT Delhi new network backbone, ownCloud, Download server, Software under Dreamsparts, Home space, IITDWiki, Apple device configuration, SMTP auth, Calendar server, Private web pages, Baafai, the IITD computing cloud, Roundcube webmail, Windows software, Password reset policy, CSC courses for 2011, Digital signing of emails, Mailing lists and aliases, Virtual web hosting, User web pages, NTP servers, VPN for Faculty/students, Complaint registration and monitoring system, IITD Discussion forum, Technopedia: IITD Wiki, SVN server, Moodle, Home spaces and CIFS shares, Microsoft active directory, IITD campus Wi, Software repository, and IITD student projects database.

## 7. Select Check Box and Click OK.

The screenshot shows the Firefox Web Browser displaying the 'Certificates' page on the Indian Institute of Technology Delhi website. The page title is 'COMPUTER SERVICES CENTRE' and the URL is 'www.cc.iitd.ac.in/CSC/index.php?option=com\_content&view=article&id=53&Itemid=57'. The page content includes a 'MAIN MENU' with links like Home, Facilities, People, and a 'RESOURCES' section with links like Change Kerberos password, Edit your LDAP profile, etc. A 'LATEST NEWS' section is also visible on the right. A 'Downloading Certificate' dialog box is open in the foreground, asking to trust a new Certificate Authority (CA) named 'ccmail07.iitd.ernet.in'. The dialog box contains the following text: 'Do you want to trust "ccmail07.iitd.ernet.in" for the following purposes?'. There are two checked checkboxes: 'Trust this CA to identify websites.' and 'Trust this CA to identify email users.' Below the checkboxes, it says 'Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available)'. There are 'View', 'Examine CA certificate', 'Cancel', and 'OK' buttons. The 'OK' button is highlighted.

## 8. Certificate installed successfully. You can check the certificate in step no. 5 > Authorities

The screenshot shows the Mozilla Firefox Preferences window, specifically the 'Certificates' section. The 'Authorities' tab is selected, displaying a list of installed certificate authorities. The list includes: 'Hongkong Post Root CA 1', 'IdenTrust', 'IdenTrust Public Sector Root CA 1', 'IdenTrust Commercial Root CA 1', 'Indian Institute of Technology, Delhi', 'ccmail07.iitd.ernet.in' (highlighted in blue), 'Internet Security Research Group', 'ISRG Root X1', and 'IZENPE S.A.'. The 'ccmail07.iitd.ernet.in' authority is listed as a 'Software Security Device'. At the bottom of the list, there are buttons for 'View...', 'Edit Trust...', 'Import...', 'Export...', and 'Delete or Distrust...'. The 'OK' button is at the bottom right of the dialog.