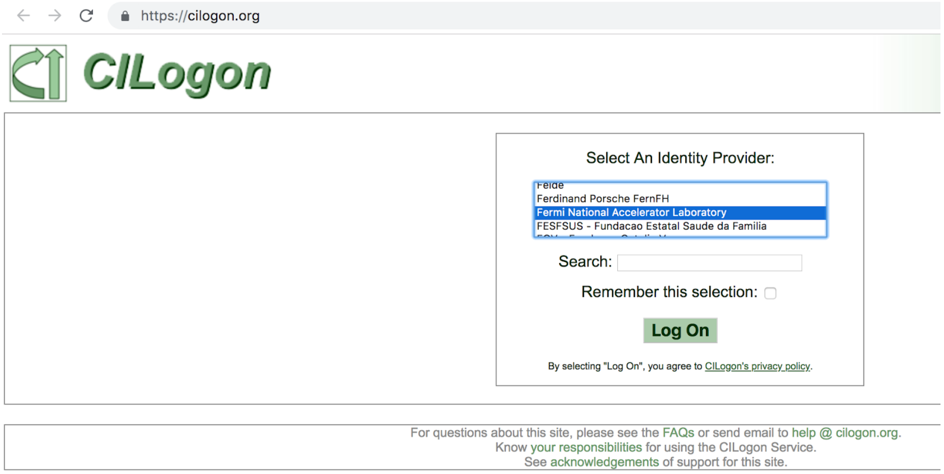
Security and Certificates in GlideinWMS

1. Go to CI Logon: https://cilogon.org/ and select the Identity Provider Fermi National Accelerator Laboratory.



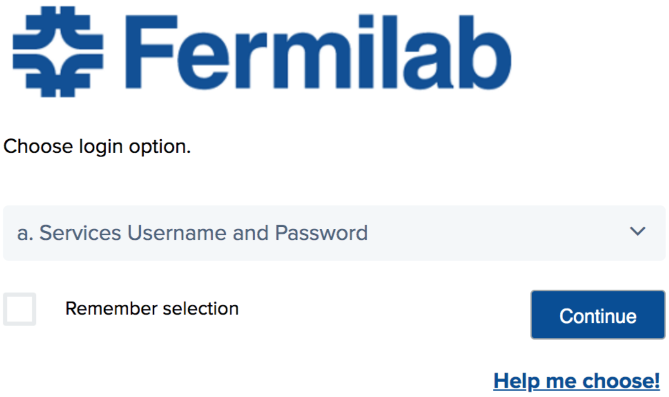
Select An Identity Provider: Fermi National Accelerator Laboratory

Remember this selection: □

By selecting "Log On", you agree to CILogon's privacy policy.

For questions about this site, please see the FAQs or send email to help @ cilogon.org.
Know your responsibilities for using the CILogon Service.
See acknowledgements of support for this site.

2. Provide your username and password (service account)

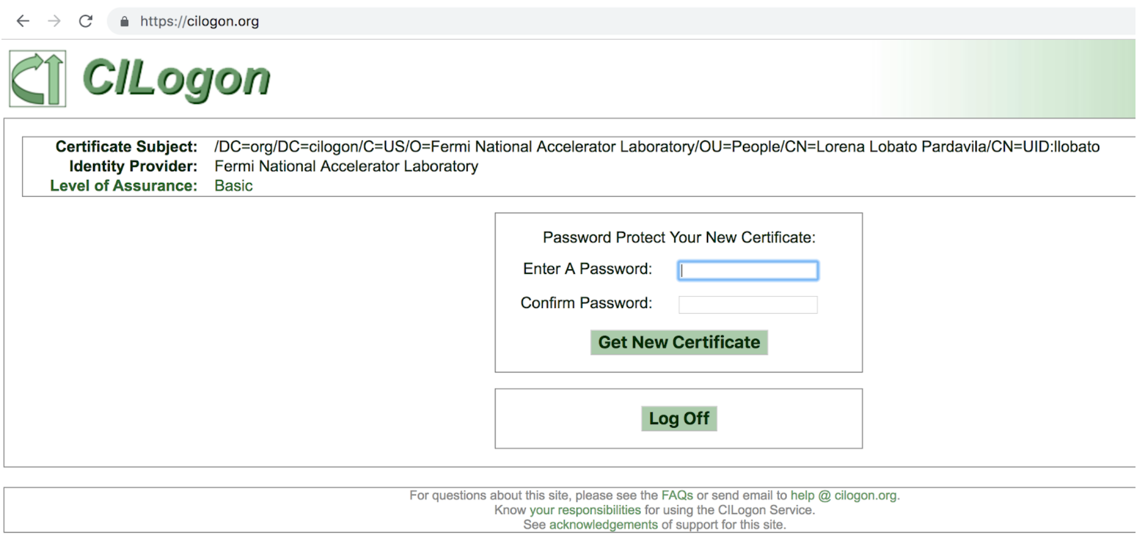


Choose login option.

a. Services Username and Password

□ Remember selection

3. Create a **private password** to protect your certificate and press “Get New Certificate”



https://cilogon.org

Certificate Subject: /DC=org/DC=cilogon/C=US/O=Fermi National Accelerator Laboratory/OU=People/CN=Lorena Lobato Pardavila/CN=UID:llobato
Identity Provider: Fermi National Accelerator Laboratory
Level of Assurance: Basic

Password Protect Your New Certificate:

Enter A Password:

Confirm Password:

For questions about this site, please see the FAQs or send email to help @ cilogon.org.
Know your responsibilities for using the CILogon Service.
See acknowledgements of support for this site.

4. Once you get your p12 certificate, place it in a specific location of your machine. To do so, enter the created password

   Now, let’s gonna talk about Kerberos

5. Create a Kerberos ticket:

```
~$: ssh root@any_virtual_machine.fnal.gov
Permission denied (gssapi-keyex,gssapi-with-mic).
        ~$: kinit
llobato@FNAL.GOV's password:
```

6. List your ticket

```
~$: klist
Ticket cache: FILE:/tmp/krb5cc_0_3mL8warQcB
Default principal: llobato@FNAL.GOV
Valid starting     Expires            Service principal
06/16/19 18:02:24  06/17/19 20:02:06  krbtgt/FNAL.GOV@FNAL.GOV
```

7. Ready to go. Access to the machine where your p12 certificate is:

```
        ~$: ssh root@fermicloud364.fnal.gov
System is booting up. See pam_nologin(8)
Last login: Wed Jun 12 11:50:31 2019 from 131.225.170.15
                    NOTICE TO USERS

   This  is a Federal computer (and/or it is directly connected to a
   Fermilab local network system) that is the property of the United
   States Government.  It is for authorized use only.  Users (autho-
   rized or unauthorized) have no explicit or  implicit  expectation
   of privacy.
```

…

8. Now, being located in the directory where you have your p12 certificate , let's going to extract the public certificate and the private key

```
(public certificate): bash-4.2$ openssl pkcs12 -in <yourcertificate.p12> -nokeys -out <mycert.pem>
Enter Import Password:
MAC verified OK
(private key):bash-4.2$ openssl pkcs12 -in <yourcertificate.p12> -nocerts -out <mykey.pem>
Enter Import Password:
```

□ If you get MAC verified OK, that's it, you got them both! You can check your DN and the timelife of your certificate

```
openssl x509 -noout -subject -in <mycert.pem>
subject= /DC=org/DC=cilogon/C=US/O=Fermi National Accelerator Laboratory/OU=People/CN=Lorena Lobato Pardavila/CN=UID:llobato
openssl x509 -enddate -noout -in <mycert.pem>
notAfter=May 26 16:40:06 2020 GMT
```

9. Use chmod to ensure the permissions over your cert and your key

```
$: chmod 644 <mycert.pem>
$: chmod 400 <mykey.pem>
```

From here, you must be familiarized with OSG software installation. For better performance, it's better if you install the software in a Fermicloud machine. If you have not done the training yet and you don't have any virtual machine created, stop here. Follow the Fermicloud training and then come back to this point.

10. In your VM, install OSG Certificate Authorities to trust roots for the public key infrastructure OSG uses to maintain integrity of its sites and services:

    ```
    ~$: yum install osg-ca-certs
    ```

11. Now that you have your certificate and your key, you'll use them to create the pilot proxy (you must be logged with your username)

```
(your_user@machine.fnal.gov)$: voms-proxy-init -valid 3333:33 -voms fermilab -cert mycert.pem -key mykey.pem -out pilot_proxy
Contacting voms1.fnal.gov:15001 [/DC=org/DC=opensciencegrid/O=Open Science Grid/OU=Services/CN=voms1.fnal.gov] "fermilab"...
Remote VOMS server contacted succesfully.

voms1.fnal.gov:15001: The validity of this VOMS AC in your proxy is shortened to 432000 seconds!
```

```
Created proxy in pilot_proxy.

Your proxy is valid until Mon Jul 01 05:16:36 CDT 2019
```

12. (For GlideinWMS installation)Create the proxy for the machine where your Frontend will be.

```
$: grid-proxy-init -cert /etc/grid-security/hostcert.pem -key /etc/grid security/hostkey.pem -valid 8888:0 -out vofe_proxy
```

13. As a ROOT, make frontend owner of both proxies)

```
$: chown frontend:frontend pilot_proxy
$: chown frontend:frontend vofe_proxy
```

14. To check the lifetime of any of the proxies…

```
$: voms-proxy-info -all -file pilot_proxy
```

```
subject   : /DC=org/DC=cilogon/C=US/O=Fermi National Accelerator Laboratory/OU=People/CN=Lorena Lobato Pardavila/CN=UID:llobato/CN=1374680570
issuer    : /DC=org/DC=cilogon/C=US/O=Fermi National Accelerator Laboratory/OU=People/CN=Lorena Lobato Pardavila/CN=UID:llobato
identity  : /DC=org/DC=cilogon/C=US/O=Fermi National Accelerator Laboratory/OU=People/CN=Lorena Lobato Pardavila/CN=UID:llobato
type      : RFC3820 compliant impersonation proxy
strength  : 2048
path      : /scratch/llobato/pilot_proxy
timeleft  : 346:49:26
key usage : Digital Signature, Key Encipherment, Data Encipherment
=== VO fermilab extension information ===
VO        : fermilab
subject   : /DC=org/DC=cilogon/C=US/O=Fermi National Accelerator Laboratory/OU=People/CN=Lorena Lobato Pardavila/CN=UID:llobato
issuer    : /DC=org/DC=incommon/C=US/ST=IL/L=Batavia/O=Fermi Research Alliance/OU=Fermilab/CN=voms1.fnal.gov
attribute : /fermilab/Role=NULL/Capability=NULL
attribute : /fermilab/nova/Role=NULL/Capability=NULL
timeleft  : 119:37:49
uri       : voms1.fnal.gov:15001
```