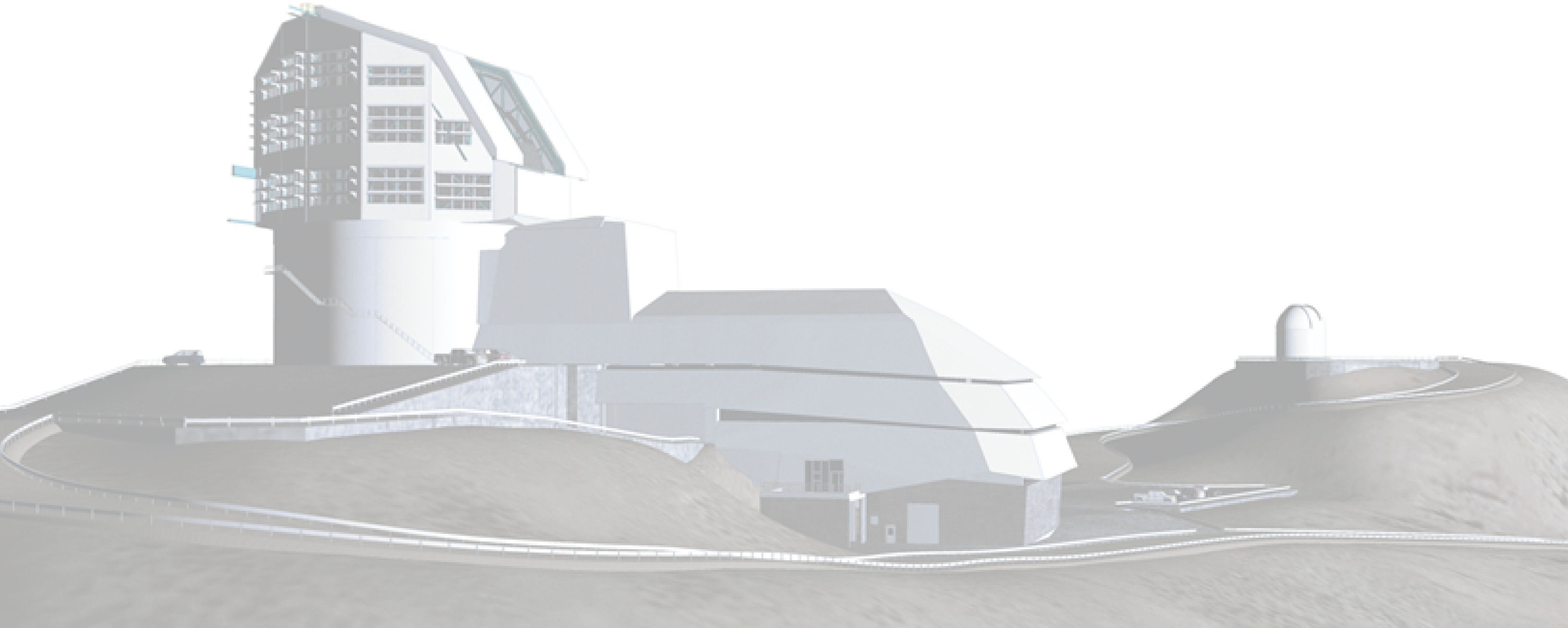
Vera C. Rubin Observatory
Rubin Observatory Project Office

Rubin Onboarding and Offboarding Procedure

Diego Tapia, Cristian Silva

ITTN-045

Latest Revision: 2024-11-28



Abstract

This ITTN was created to document the procedure of requesting access to the various services located at the summit.

Change Record

Version	Date	Description	Owner name
1	2021-04-12	Unreleased.	Cristian Silva
2	2021-05-01	First Draft	Diego Tapia
3	2021-05-27	Second Draft	Cristian Silva
4	2021-05-31	Third Draft	Diego Tapia
5	2021-06-15	Nublado details	Frossie Economou
6	2021-06-29	First Release	Cristian Silva
7	2024-07-12	SQuaRE services update	Ivan Gonzalez
7	2024-11-22	Added Offboarding and re-structured services	Cristian Silva

Document source location: `https://github.com/lsst-it/ittn-045`

Contents

Rubin Onboarding and Offboarding Procedure

1 Introduction

The access to servers and services of the summit are managed by several backends.

To access Rubin services, please refer to the section Access to Rubin Services

The access to Wifi at the Summit is controlled by domain credentials. To request Domain Credentials please refert to Requesting Domain Credentials.

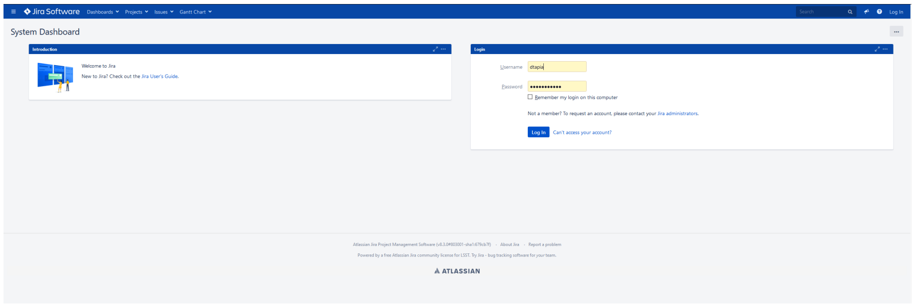
2 Onboarding

2.1 Requesting a Summit Account

To request an Summit account, it is necessary to create a Service Request ticket inside the IT User Support Dashboard. This ticket is usually created by the manager of the user needing the account.

Please check the example below.

Head over to https://rubinobs.atlassian.net/ and log in with your domain account credentials.



Welcome to Jira

New to Jira? Check out the Jira User's Guide.

Username: dtapia

Password: ●●●●●●●●●●●

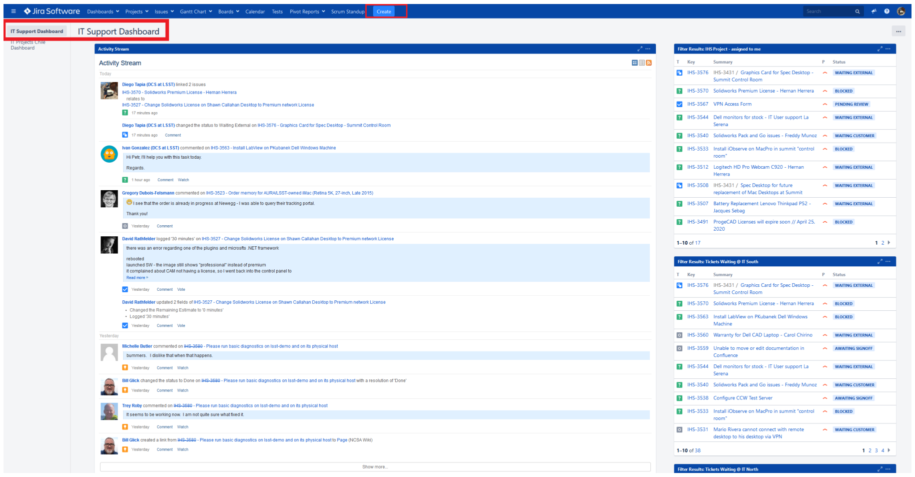
□ Remember my login on this computer

Not a member? To request an account, please contact your Jira administrators.

Atlassian Jira Project Management Software (v8.3.0#803001-sha1:679cb7f) · About Jira · Report a problem

Powered by a free Atlassian Jira community license for LSST. Try Jira - bug tracking software for *your* team.

Once logged in the user will be prompted with the following windows if not similar. Before creating the ticket, it is required for the user to check that he is in the proper dashboard for this particular case the IT Support Dashboard



Activity Stream

Today

Diego Tapia (DCS at LSST) linked 2 issues
IHS-3570 - Solidworks Premium License - Hernan Herrera
relates to
IHS-3527 - Change Solidworks License on Shawn Callahan Desktop to Premium network License
17 minutes ago

Diego Tapia (DCS at LSST) changed the status to Waiting External on IHS-3576 - Graphics Card for Spec Desktop - Summit Control Room
17 minutes ago · Comment

Ivan Gonzalez (DCS at LSST) commented on IHS-3563 - Install LabView on PKubanek Dell Windows Machine

> Hi Petr, I'll help you with this task today.
>
> Regards.

1 hour ago · Comment · Watch

Gregory Dubois-Felsmann commented on IHS-3523 - Order memory for AURA/LSST-owned iMac (Retina 5K, 27-inch, Late 2015)

> 😀 I see that the order is already in progress at Newegg - I was able to query their tracking portal.
>
> Thank you!

Yesterday · Comment

David Rathfelder logged '30 minutes' on IHS-3527 - Change Solidworks License on Shawn Callahan Desktop to Premium network License

> there was an error regarding one of the plugins and microsfts .NET framework
>
> rebooted
> launched SW - the image still shows "professional" instead of premium
> it complained about CAM not having a license, so I went back into the control panel to
> Read more »

Yesterday · Comment · Vote

David Rathfelder updated 2 fields of IHS-3527 - Change Solidworks License on Shawn Callahan Desktop to Premium network License
- Changed the Remaining Estimate to '0 minutes'
- Logged '30 minutes'

Yesterday · Comment · Vote

Yesterday

Michelle Butler commented on ~~IHS-3580~~ - Please run basic diagnostics on lsst-demo and on its physical host

> bummers. I dislike that when that happens.

Yesterday · Comment · Watch

Bill Glick changed the status to Done on ~~IHS-3580~~ - Please run basic diagnostics on lsst-demo and on its physical host with a resolution of 'Done'
Yesterday · Comment · Watch

Trey Roby commented on ~~IHS-3580~~ - Please run basic diagnostics on lsst-demo and on its physical host

> It seems to be working now. I am not quite sure what fixed it.

Yesterday · Comment · Watch

Bill Glick created a link from ~~IHS-3580~~ - Please run basic diagnostics on lsst-demo and on its physical host to Page (NCSA Wiki)
Yesterday · Comment · Watch

Filter Results: IHS Project - assigned to me

T	Key	Summary	P	Status
	IHS-3576	IHS-3431 / Graphics Card for Spec Desktop - Summit Control Room	^	WAITING EXTERNAL
?	IHS-3570	Solidworks Premium License - Hernan Herrera	^	BLOCKED
✓	IHS-3567	VPN Access Form	^	PENDING REVIEW
?	IHS-3544	Dell monitors for stock - IT User support La Serena	^	WAITING EXTERNAL
?	IHS-3540	Solidworks Pack and Go issues - Freddy Munoz	^	WAITING CUSTOMER
?	IHS-3533	Install iObserve on MacPro in summit "control room"	^	BLOCKED
?	IHS-3512	Logitech HD Pro Webcam C920 - Hernan Herrera	^	WAITING EXTERNAL
	IHS-3508	IHS-3431 / Spec Desktop for future replacement of Mac Desktops at Summit	^	WAITING EXTERNAL
?	IHS-3507	Battery Replacement Lenovo Thinkpad P52 - Jacques Sebag	^	WAITING EXTERNAL
?	IHS-3491	ProgeCAD Licenses will expire soon // April 25, 2020	^	BLOCKED

1–10 of 17 · 1 2 ▸

Filter Results: Tickets Waiting @ IT South

T	Key	Summary	P	Status
	IHS-3576	IHS-3431 / Graphics Card for Spec Desktop - Summit Control Room	^	WAITING EXTERNAL
?	IHS-3570	Solidworks Premium License - Hernan Herrera	^	BLOCKED
?	IHS-3563	Install LabView on PKubanek Dell Windows Machine	^	BLOCKED
	IHS-3560	Warranty for Dell CAD Laptop - Carol Chirino	^	WAITING EXTERNAL
	IHS-3559	Unable to move or edit documentation in Confluence	^	AWAITING SIGNOFF
?	IHS-3544	Dell monitors for stock - IT User support La Serena	^	WAITING EXTERNAL
?	IHS-3540	Solidworks Pack and Go issues - Freddy Munoz	^	WAITING CUSTOMER
?	IHS-3538	Configure CCW Test Server	^	AWAITING SIGNOFF
?	IHS-3533	Install iObserve on MacPro in summit "control room"	^	BLOCKED
	IHS-3531	Mario Rivera cannot connect with remote desktop to his desktop via VPN	^	WAITING CUSTOMER

1–10 of 38 · 1 2 3 4 ▸

On the ticket creation window fill out the template using the information provided below:

- Project: IT Helpdesk Support (IHS)
- Issue Type: Service Request
- Summary: Onboarding <user>
- Component: AAA
- Description: <description>

<user>: Name of the user to onboard.

<description>: Use the following template:

- First and Last Name: ……
- SSH Public Key: ……
- Email Address: ……
- Services: list needed services from Rubin Services

Once all the information is filled out, select the Create option located at the bottom to create the ticket inside IHS IT Support Dashboard.

Once the account has been created and the services have been provisioned, the user will be contacted via the email provided in the ticket. The user will then need to change the password of the account created. Instructions to change the password will be sent via email.

If you have any questions or concerns please contact #devops-team in Rubin Observatory's Slack workspace

2.2 Rubin Services

The following services can be requested:

- RSP for Summit, includes:
  - Chronograf
  - Nublado
- RSP for La Serena
  - Chronograf
  - Nublado
- ArgoCD for Summit
- LOVE
- Standard baremetal access for Camera Subsystems (LSSTCam, ComCam, Auxtel)
- Sudo access for Camera Subsystems (LSSTCam, ComCam, Auxtel)
- Kubernetes access for Summit
- Kubernetes access for Base
- Kubernetes access for Tucson
- TTS access
- BTS access
- 1Password vault (vaults must be specified)
- Dev access for TTS, includes
  - ArgoCD
  - K8s
  - 1Password vault
- Dev access for BTS, includes
  - ArgoCD

- K8s
- 1Password vault

Follow instructions in ITTN-045, and file a single IHS ticket to request access to the service(s) needed.

Access to some systems must have prior authorization by systems owners.

For security reasons, 2FA is used in VPN and some services, but they are independent. For example, if you need to access Summit RSP you must create a 2FA entry and to access Base RSP you will also need to create a separate 2FA that is independent of the Summit RSP entry. When you log in for the first time to one of these services you will be able to configure your 2FA token.

Resources details of each site can be found in the following links

a) TTS.

b) BTS.

c) Summit.

2.3 Access to Github Ogranizations

a) lsst-it (docker-compose-ops-repo, explicitly).

  - File an IHS ticket

b) lsst-ts (argocd-csc scripts).

  - Submit and Email or Slack request to Rob Bovill (rbovill@lsst.org).

2.4 Requesting Domain Credentials

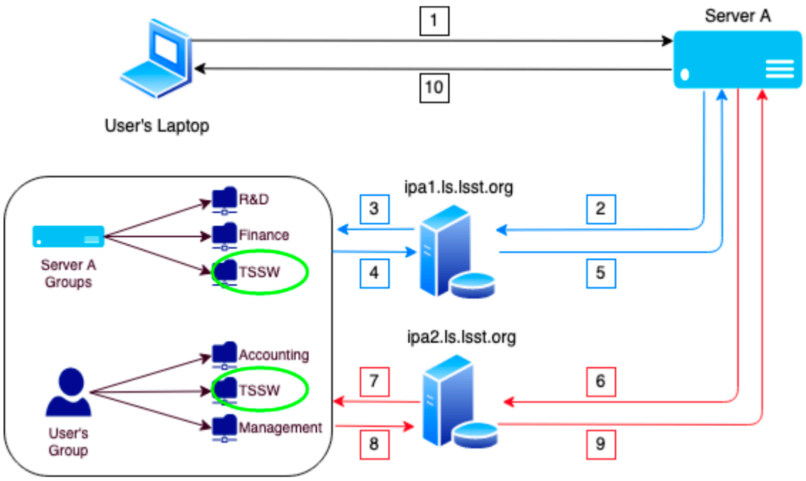
To request Domain Account Credentials, it is required that an Onboarding form is filled out by the manager or supervisor in charge at Onboarding Form. Once the onboarding form is filled out and submitted with the information requested, IT North will process the credentials and will contact the person requesting the access.

3 Rubin Server Authentication

All Rubin Observatory's servers are set to authenticate through FreeIPA and Asymmetric Cryptography through Secure Shell (ssh), and all other mechanisms are blocked. This means, all local accountsand password authentication are not allowed, so once the servers are admitted to IT's network and infrastructure, all previous local accounts, passwords, permissions, users and groups IDs (uid and gid).

When a new user arrives, or a user that does not yet have credentials, it is requested to create a RIC (Request for IPA Credentials) following the instructions above.

Then, comes an important part of the process: setting and creation of the Asymmetric Cryptography, also known as public-key cryptography.



(1) The user presents its private ssh-key, (2) If the primary IPA Server is reachable (ipa1.ls.lsst.org), the Rubin's Server (Server A) presents the user's private key to ipa1, (3) The IPA Server checks against the common database(among all replicas) if the users exists and matches the private against the stored public key; if the user exists, it also checks if the group who it belongs has sufficient privileges to access, (4) The Server fetches the Database information, (5) The IPA Server either grants or denied access to the User's Laptop to Server A, (10) The permission

granted/denied is send to the User's Laptop. If the Primary IPA Server isn't reachable after timeout, it does the same operation over the failover (red) Server, following path 6 -> 7 -> 8 -> 9 instead of 2 -> 3 -> 4 -> 5.

3.1 SSH Keys Creation

Depending on your OS, is the instructions you will need to follow:

3.2 Linux and MacOS

First, log into your local machine, then search and open a terminal window. Once there:

```
john@localhost:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/john/.ssh/id_rsa):      #HIT ENTER, DO NOT WRITE ANY CONTENT
Enter passphrase (empty for no passphrase):                        #ENTER
Enter same passphrase again:                                       #ENTER
Your identification has been saved in /home/ john /.ssh/id_rsa.
Your public key has been saved in /home/ john /.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:seMcIk0bqj0ZhXlKer5ik6e3mpAMisYdvZwziPddbAs john@localhost
```

If the John, already has a pair of private/public keys – and for personal reasons don't want to reuse them – you can set a new pair by changing the name of the keys and adding a config file, so that the local ssh agent includes that key as well:

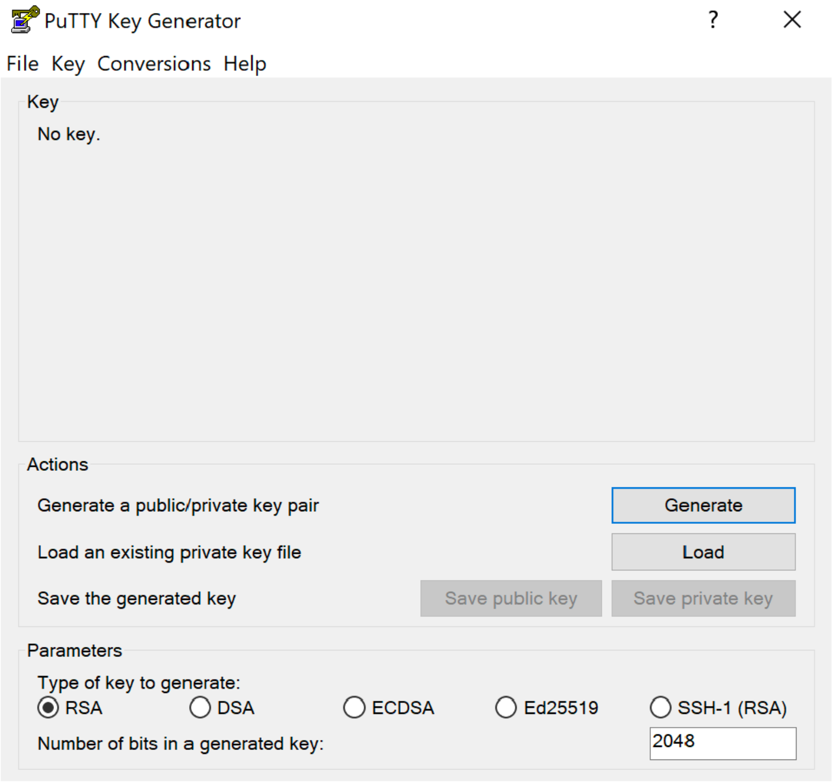
```
john@localhost:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/john/.ssh/id_rsa): /home/john/.ssh/rubin_rsa
Enter passphrase (empty for no passphrase):                        #HIT ENTER, DO NOT WRITE ANY CONTENT
Enter same passphrase again:                                       #ENTER
Your identification has been saved in /home/ john /.ssh/rubin_rsa.
Your public key has been saved in /home/ john /.ssh/rubin_rsa.pub.
The key fingerprint is:
SHA256:seMcIk0bqj0ZhXlKer5ik6e3mpAMisYdvZwziPddbAs john@localhost
john@localhost:~$ echo -ne "IdentityFile /Users/hreinking/.ssh/id_rsa\nIdentityFile /Users/hreinking/.ssh/rubin_rsa\n" > ~/.ssh/config
john@localhost:~$ chmod 644 ~/.ssh/config
```

The id rsa file contains your private key, which by no reason must be shared or known by another person, this will not only compromise the integrity of the server but also related user's data, account access etc. On the other hand, the id rsa pub contains the public key, whis is intended to be shared and publicly known.

3.3 Windows OS

Windows does not natively have a native ssh mechanism. There are several third-party applications, designed to satisfy such need, but we are going to use PuTTY9, which is an Open-Source software SSH and Telnet client Putty Client.

Once PuTTY is installed, we will use a complementary tool (already installed along with putty) called PuTTYgen (you can open it by typing it into Windows Search box):



No key.

Generate a public/private key pair

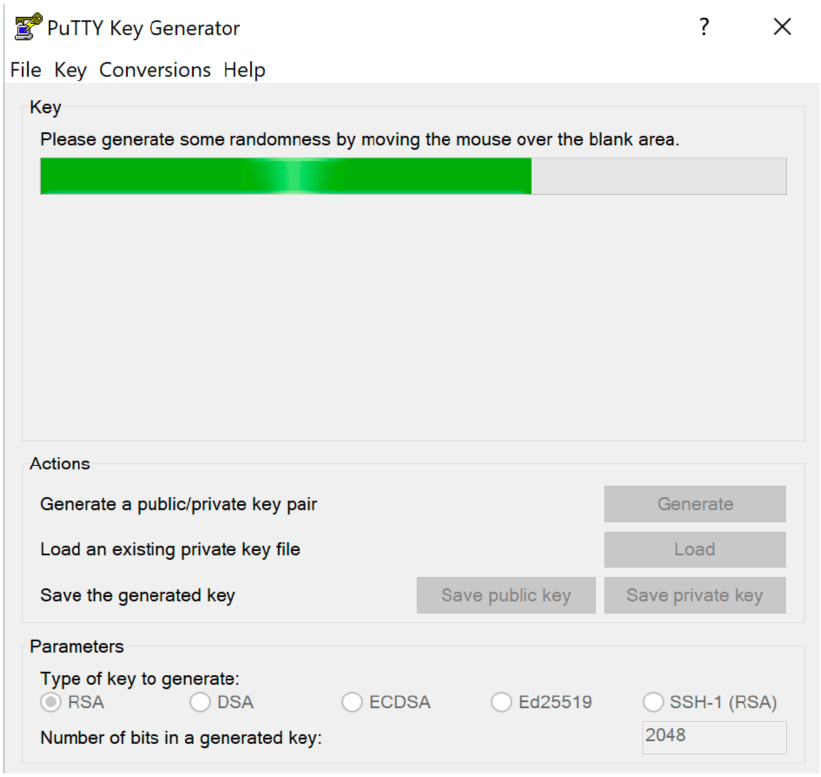
Load an existing private key file

Save the generated key

Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ Ed25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Click on generate:



Please generate some randomness by moving the mouse over the blank area.

Generate a public/private key pair

Load an existing private key file

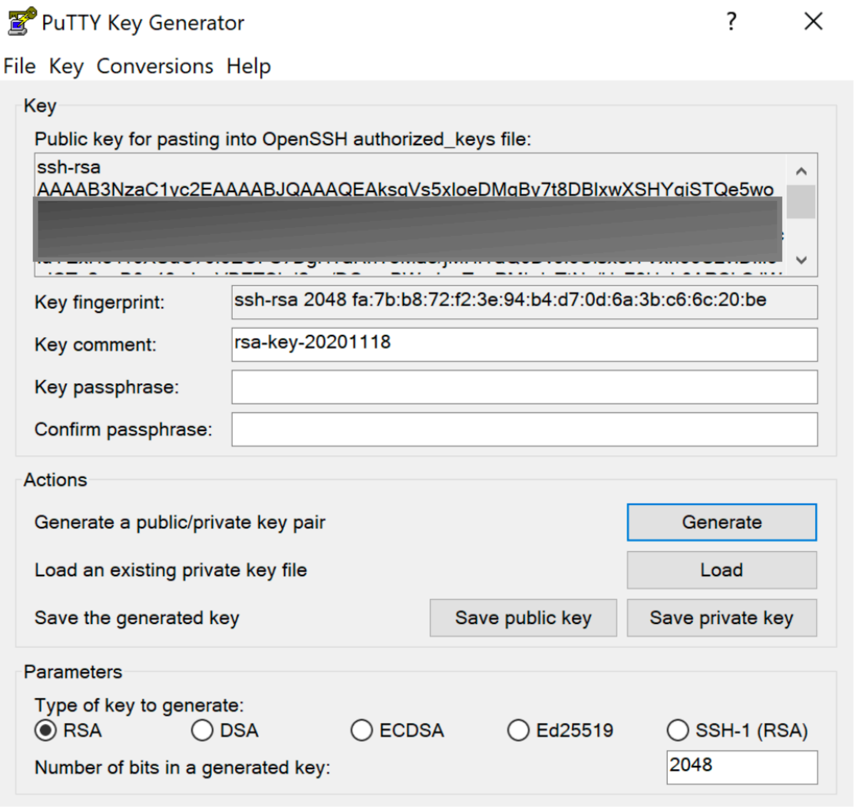
Save the generated key

Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ Ed25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

In order to create a random key, you must move the mouse over the surface, so the progress bar moves.

Once concluded, you should see something like:



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAksqVs5xloeDMqBy7t8DBlxwXSHYqiSTQe5wo
[redacted]
```

Key fingerprint: ssh-rsa 2048 fa:7b:b8:72:f2:3e:94:b4:d7:0d:6a:3b:c6:6c:20:be

Key comment: rsa-key-20201118

Key passphrase:

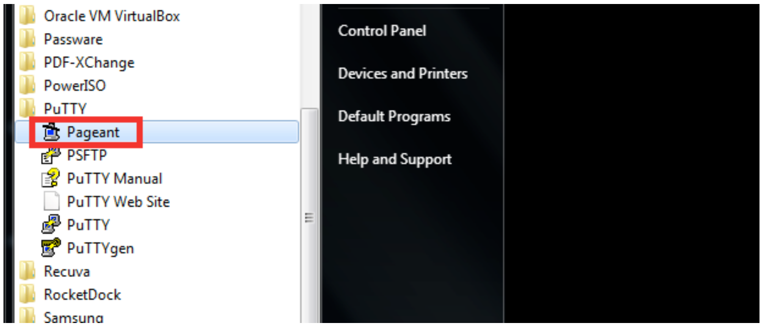
Confirm passphrase:

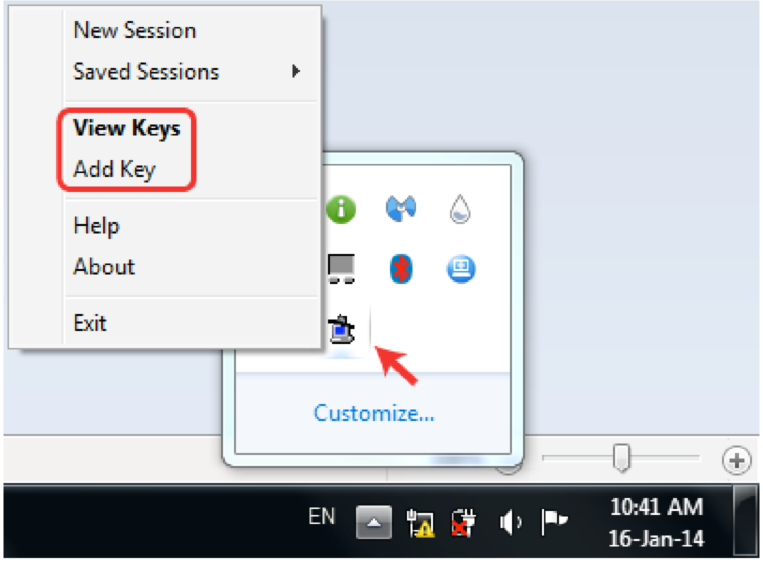
Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ Ed25519 ○ SSH-1 (RSA)

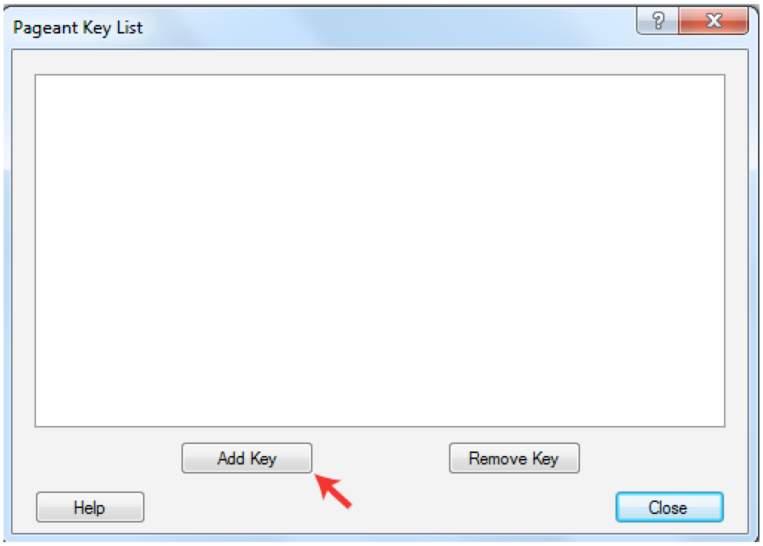
Number of bits in a generated key: 2048

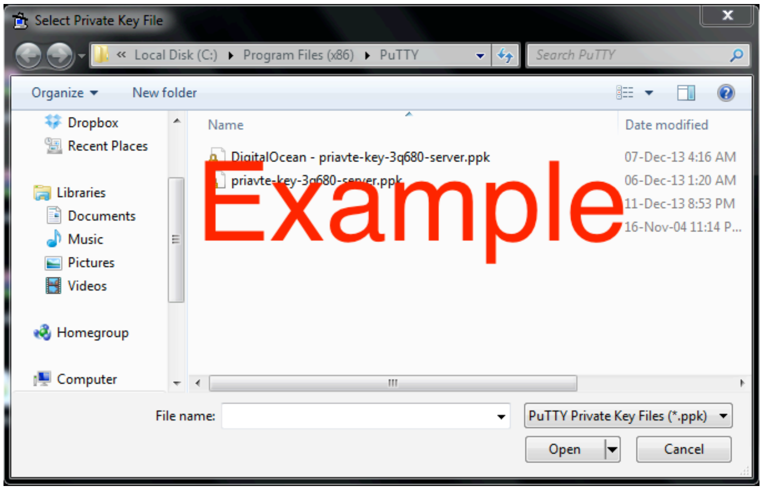
Now, save both keys into a well-known location. It is recommended (but not needed) to create a folder named “ssh” in the user’s home directory, so when asked, you can easily find your keys in “/Users/<username>/ssh/”.

The next images will show you how to load the ssh private key in the Pageant app.









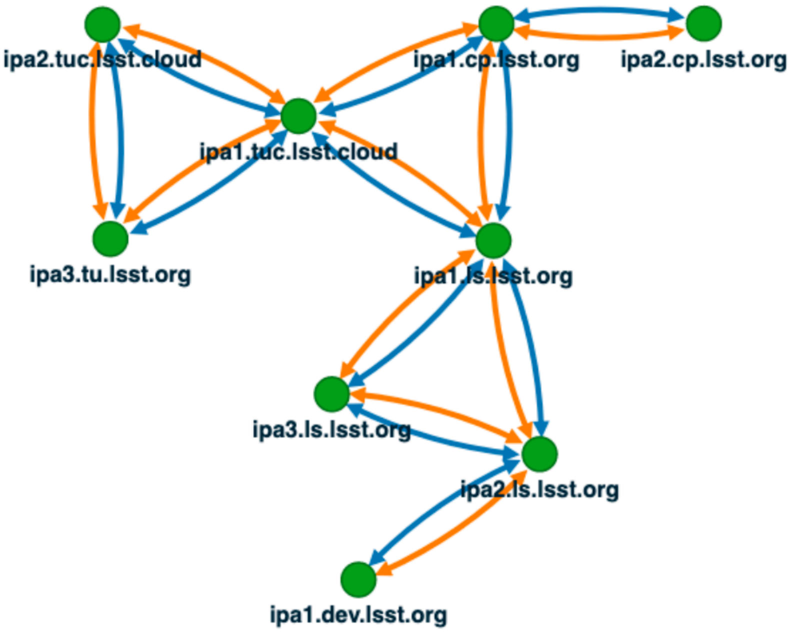
Name	Date modified
DigitalOcean - priavte-key-3q680-server.ppk	07-Dec-13 4:16 AM
priavte-key-3q680-server.ppk	06-Dec-13 1:20 AM
	11-Dec-13 8:53 PM
	16-Nov-04 11:14 P...

Once you have your private key loaded in the Pageant app, you need to upload your public ssh key to the jira ticket in order for the IT Team to format the ssh keys.

3.4 Add Public Key Into IPA

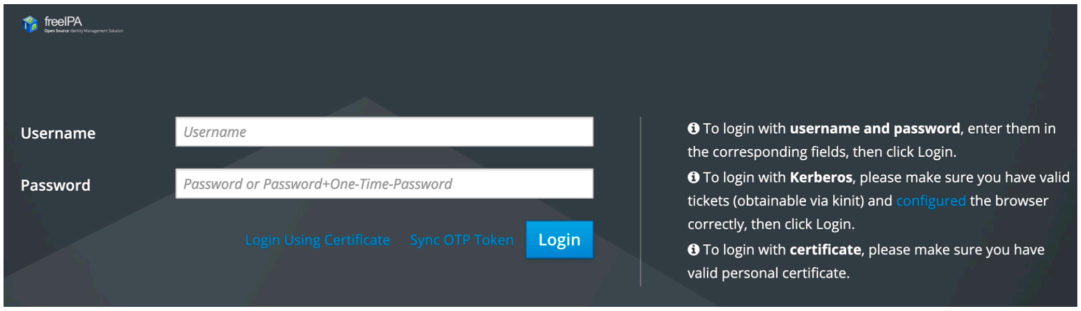
The IPA infrastructure is composed of a master server and several replicas, meaning that it does not matter in which one you modified your personal data, it will be propagated over the rest of the nodes.

The IPA Topology (Image below) is designed in such way, that in the worst-case scenario, at least one source of authentication will remain.



The orange arrows represent the DL (Domain Link), meanwhile the blue arrows the CA (Certificate Authority). The DL keeps the authenticity of the defined domain – i.e. server.local – and the CA is the responsible of emitting and signing the hosts certificates, to validate their authenticity.

In order to add your public key into IPA, you must access through any of the http frontends, from either the replicas or master. Bear in mind that you must be either inside the network or connected through VPN. Let's use the BDC (Base Data Center) replica: open a web-browser and navigate to IPA Website. You should see a welcoming screen:



Username: Username

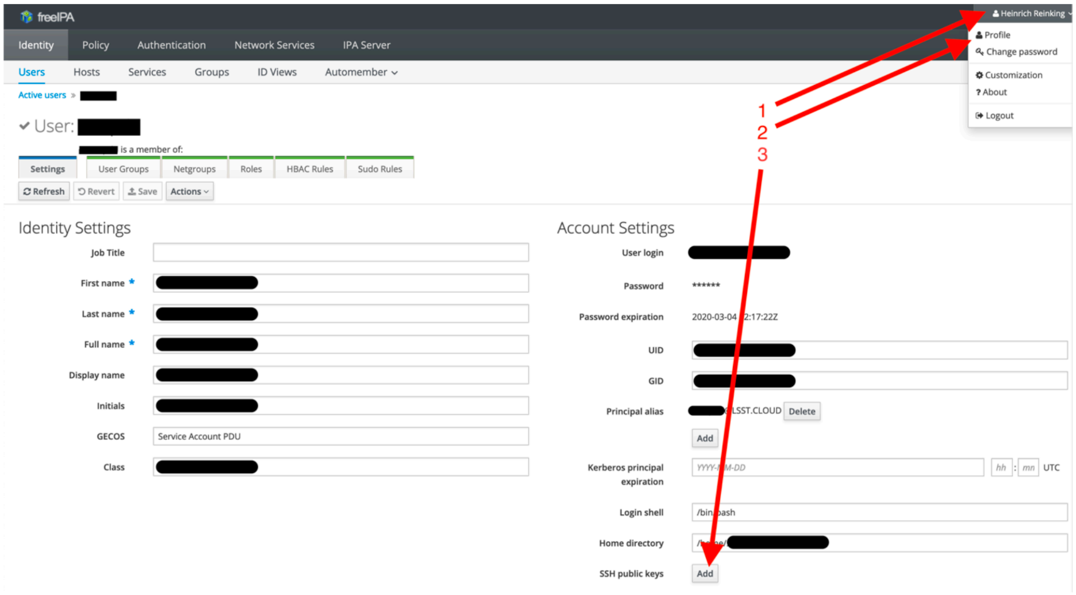
Password: Password or Password+One-Time-Password

To login with **username and password**, enter them in the corresponding fields, then click Login.

To login with **Kerberos**, please make sure you have valid tickets (obtainable via kinit) and configured the browser correctly, then click Login.

To login with **certificate**, please make sure you have valid personal certificate.

If it's the first time you log in, the system will force you to change your password (also if it has expired). Once successfully logged in the platform, (1) in the upper right corner click your username, (2) profile, and then (3) Add:



Active users » [redacted]

User: [redacted]

[redacted] is a member of:

Identity Settings

Job Title:

First name *: [redacted]

Last name *: [redacted]

Full name *: [redacted]

Display name: [redacted]

Initials: [redacted]

GECOS: Service Account PDU

Class: [redacted]

Account Settings

User login: [redacted]

Password: ******

Password expiration: 2020-03-04 2:17:22Z

UID: [redacted]

GID: [redacted]

Principal alias: [redacted]@LSST.CLOUD

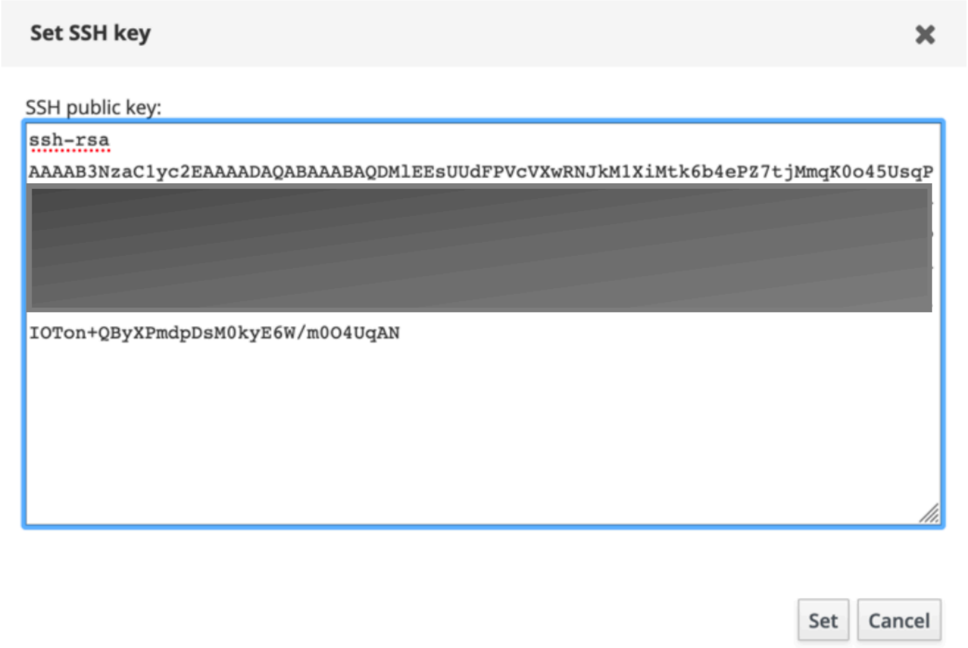
Kerberos principal expiration: YYYY-MM-DD hh : mn UTC

Login shell: /bin/bash

Home directory: /home/[redacted]

SSH public keys

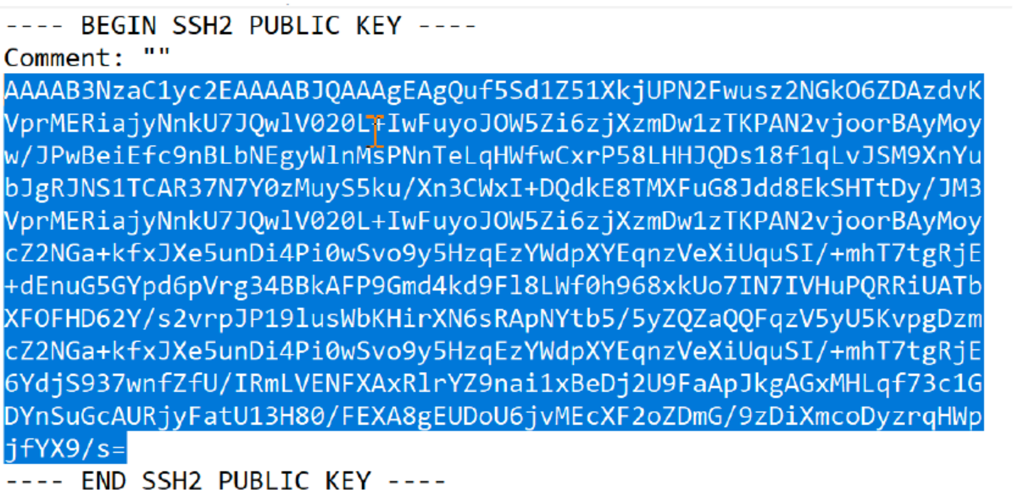
A pop-up window will appear, in which you must paste your public key:



SSH public key:

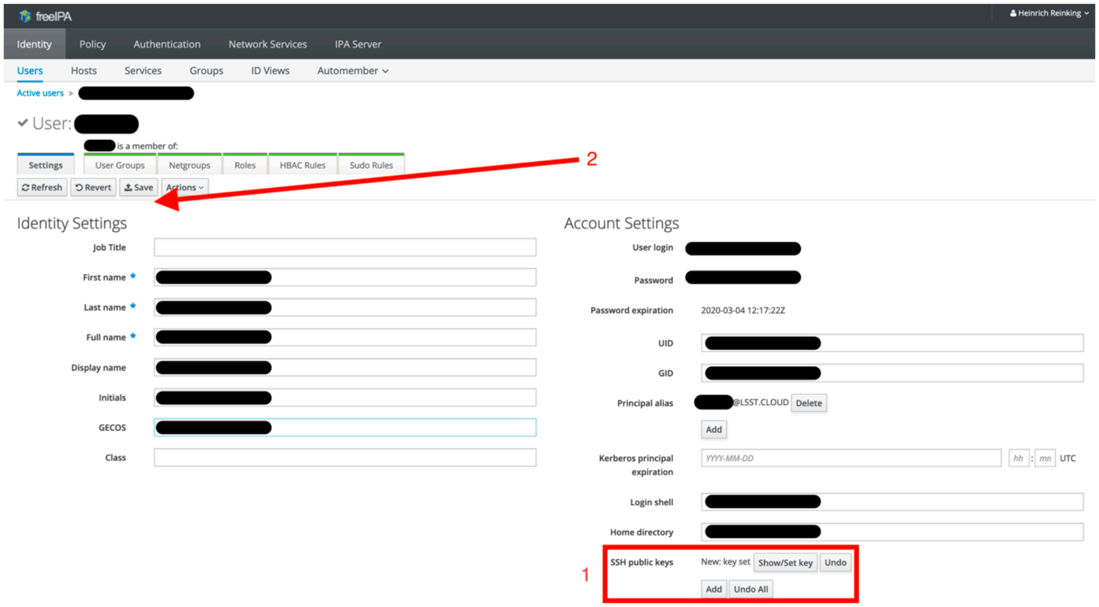
```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDMlEEsUUdFPVcVXwRNJkM1XiMtk6b4ePZ7tjMmqK0o45UsqP
[redacted]
IOTon+QByXPmdpDsM0kyE6W/m0O4UqAN
```

If you are importing a key generated with PuTTY, must use only the selected section:



```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: ""
AAAAB3NzaC1yc2EAAAABJQAAAgEAgQuf5Sd1Z51XkjUPN2Fwusz2NGkO6ZDAzdvK
VprMERiajyNnkU7JQwlV020L+IwFuyoJOW5Zi6zjXzmDw1zTKPAN2vjoorBAyMoy
w/JPwBeiEfc9nBLbNEgyWlnMsPNnTeLqHWfwCxrP58LHHJQDs18f1qLvJSM9XnYu
bJgRJNS1TCAR37N7Y0zMuyS5ku/Xn3CWxI+DQdkE8TMXFuG8Jdd8EkSHTtDy/JM3
VprMERiajyNnkU7JQwlV020L+IwFuyoJOW5Zi6zjXzmDw1zTKPAN2vjoorBAyMoy
cZ2NGa+kfxJXe5unDi4Pi0wSvo9y5HzqEzYWdpXYEqnzVeXiUquSI/+mhT7tgRjE
+dEnuG5GYpd6pVrg34BBkAFP9Gmd4kd9Fl8LWf0h968xkUo7IN7IVHuPQRRiUATb
XFOFHD62Y/s2vrpJP19lusWbKHirXN6sRApNYtb5/5yZQZaQQFqzV5yU5KvpgDzm
cZ2NGa+kfxJXe5unDi4Pi0wSvo9y5HzqEzYWdpXYEqnzVeXiUquSI/+mhT7tgRjE
6YdjS937wnfZfU/IRmLVENFXAxRlrYZ9nai1xBeDj2U9FaApJkgAGxMHLqf73c1G
DYnSuGcAURjyFatU13H80/FEXA8gEUDoU6jvMEcXF2oZDmG/9zDiXmcoDyzrqHWp
jfYX9/s=
---- END SSH2 PUBLIC KEY ----
```

If everything was set correctly, click Set, and you will find yourself in the previous window:



Active users » [redacted]

User: [redacted]

[redacted] is a member of:

Identity Settings

Job Title
First name * [redacted]
Last name * [redacted]
Full name * [redacted]
Display name [redacted]
Initials [redacted]
GECOS [redacted]
Class

Account Settings

User login [redacted]
Password [redacted]
Password expiration 2020-03-04 12:17:22Z
UID [redacted]
GID [redacted]
Principal alias [redacted]@LSST.CLOUD Delete
Add
Kerberos principal expiration YYYY-MM-DD hh : mn UTC
Login shell [redacted]
Home directory [redacted]
SSH public keys New: key set Show/Set key Undo
Add Undo All

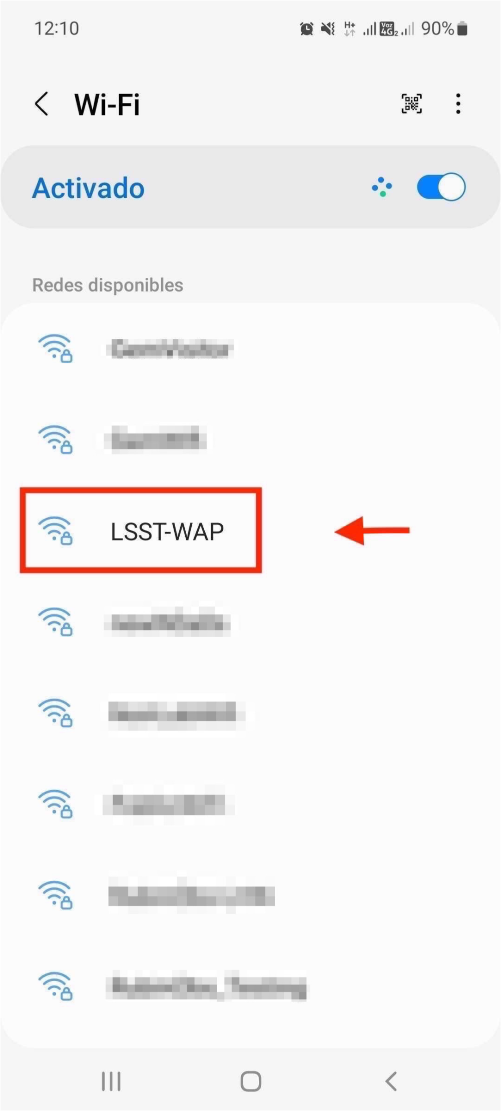
(1) A “New:key set” should now appear and in order for the changes to take place, (2) click on Save.

4 Accesing the Rubin Observatory WIFI network

Once the onboarding form is complete and the AUP form is submitted, IT will contact you to hand out your Domain account credentials concluding the onboarding process. These credentials depending on the level of access requested by the manager will give you access to services such as Jira, Confluence, Docushare, Exchange and most importantly the Rubin Observatory WIFI network named ”LSST-WAP”, this WIFI SSID can be found both at Cerro Pachon and La Serena Base facility.

4.1 Android Mobile Device

To connect your mobile device to the LSST-WAP wifi network please follow the instructions on the images below.



12:10 90%

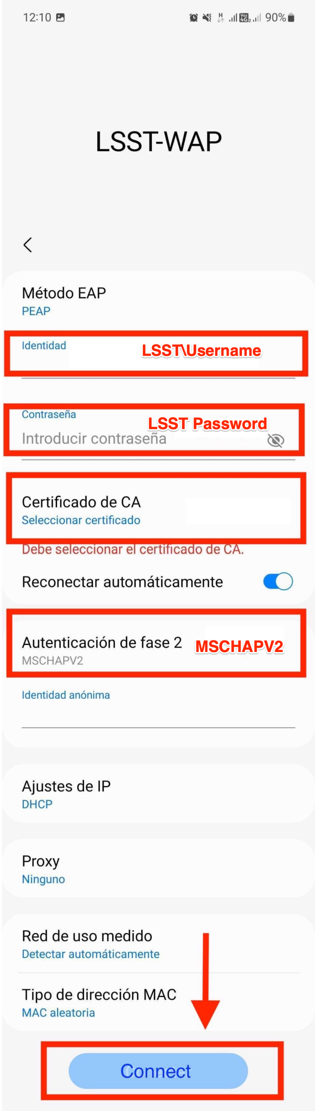
Wi-Fi

Activado

Redes disponibles

LSST-WAP

1.) Select the LSST-WAP WIFI Network from the list.



12:10 90%

LSST-WAP

Método EAP
PEAP

Identidad
LSST\Username

Contraseña
Introducir contraseña
LSST Password

Certificado de CA
Seleccionar certificado

Debe seleccionar el certificado de CA.

Reconectar automáticamente

Autenticación de fase 2
MSCHAPV2
MSCHAPV2

Identidad anónima

Ajustes de IP
DHCP

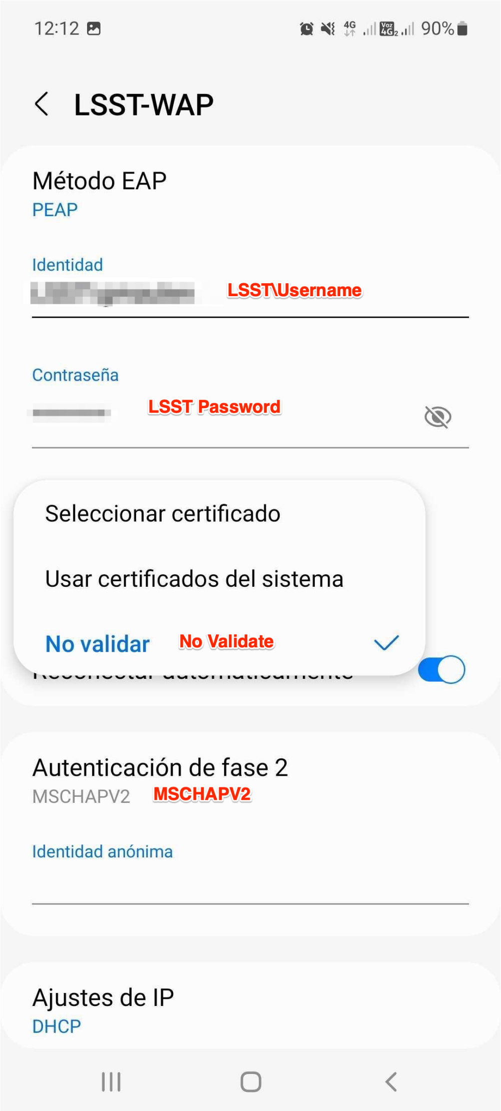
Proxy
Ninguno

Red de uso medido
Detectar automáticamente

Tipo de dirección MAC
MAC aleatoria

Connect

2.) Fill out the fields highlighted in red as show on the image.



12:12 90%

LSST-WAP

Método EAP
PEAP

Identidad
[redacted] LSST\Username

Contraseña
[redacted] LSST Password

Seleccionar certificado

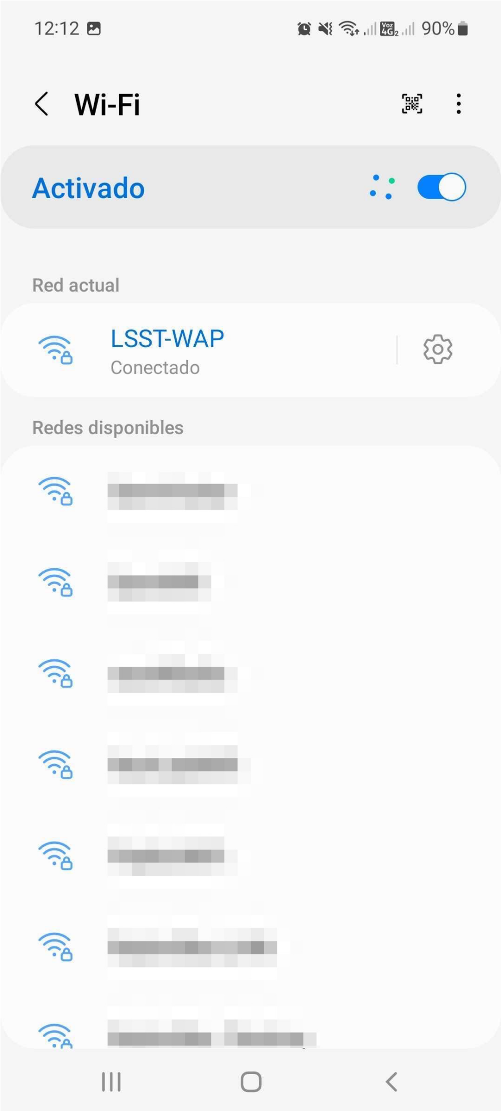
Usar certificados del sistema

No validar No Validate ✓

Autenticación de fase 2
MSCHAPV2 MSCHAPV2

Identidad anónima

Ajustes de IP
DHCP



12:12 90%

Wi-Fi

Activado

Red actual

LSST-WAP
Conectado

Redes disponibles

[redacted]

[redacted]

[redacted]

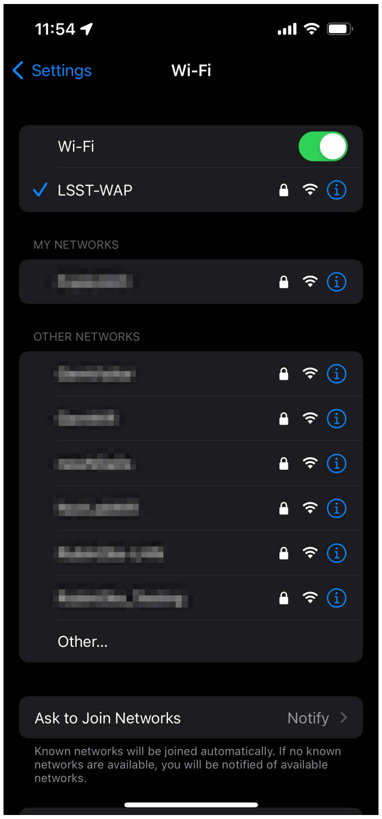
[redacted]

[redacted]

[redacted]

[redacted]

4.2 Apple Mobile Device



11:54

< Settings Wi-Fi

Wi-Fi

✓ LSST-WAP

MY NETWORKS

[redacted]

OTHER NETWORKS

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

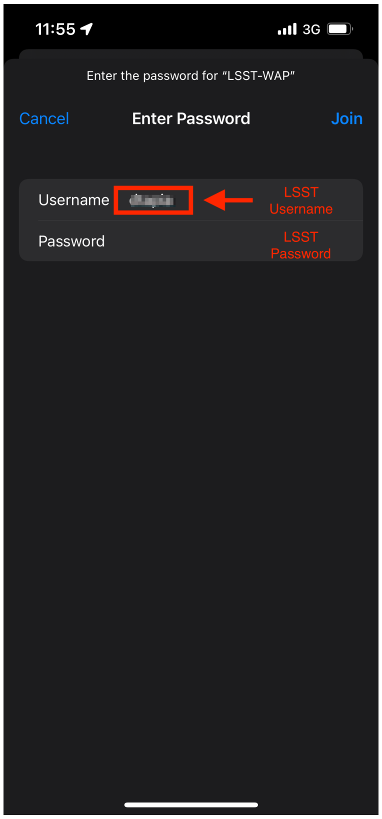
[redacted]

Other...

Ask to Join Networks Notify >

Known networks will be joined automatically. If no known networks are available, you will be notified of available networks.

1.) Select the LSST-WAP WIFI Network from the list.



11:55 3G

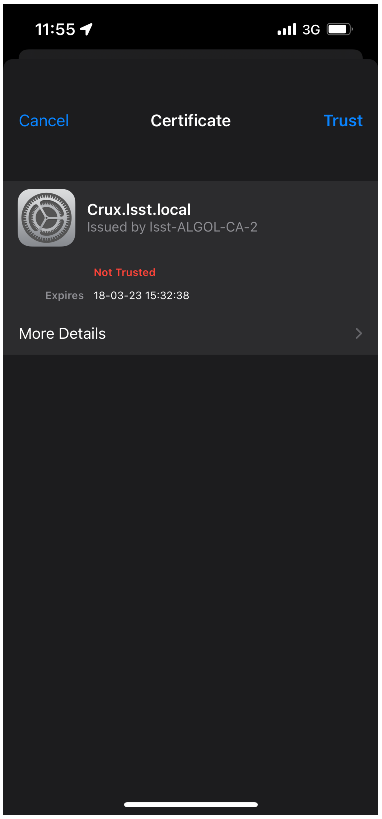
Enter the password for "LSST-WAP"

Cancel Enter Password Join

Username [redacted] LSST Username

Password LSST Password

2.) Log in with your domain account credentials as shown on the images.



11:55 3G

Cancel Certificate Trust

Crux.lsst.local

Issued by lsst-ALGOL-CA-2

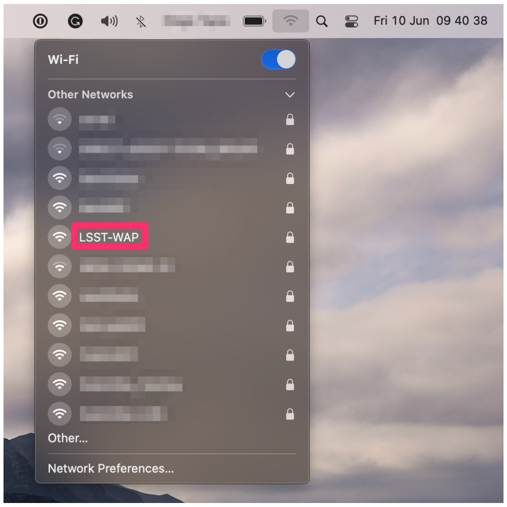
Not Trusted

Expires 18-03-23 15:32:38

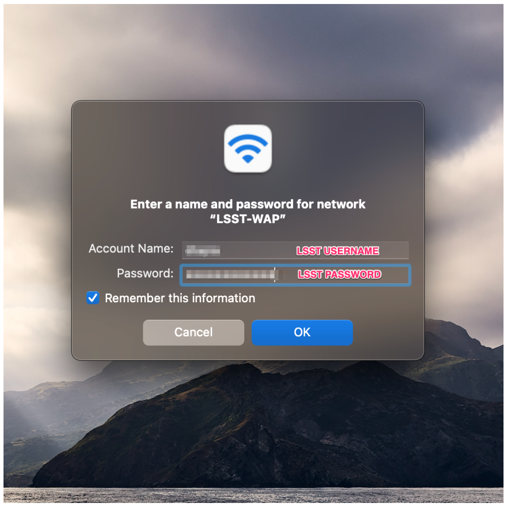
More Details >

3.) Accept the certificate and hit on the trust button to connect.

4.3 MacOS



1.) Select the LSST-WAP WIFI Network from the list.



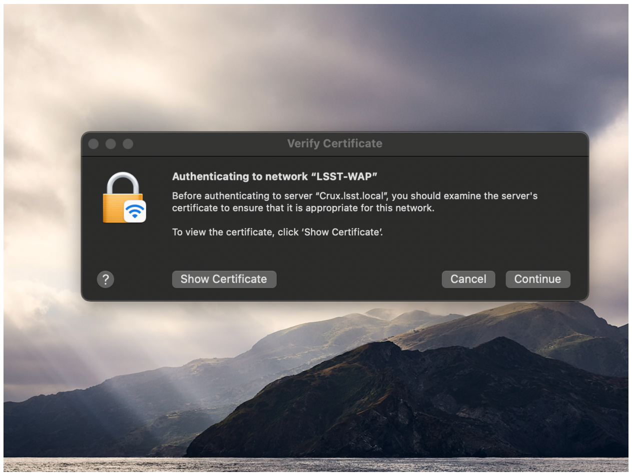
Enter a name and password for network “LSST-WAP”

Account Name: [redacted] LSST USERNAME

Password: [redacted] LSST PASSWORD

☑ Remember this information

2.) Log in with your domain account credentials as shown on the images.



Verify Certificate

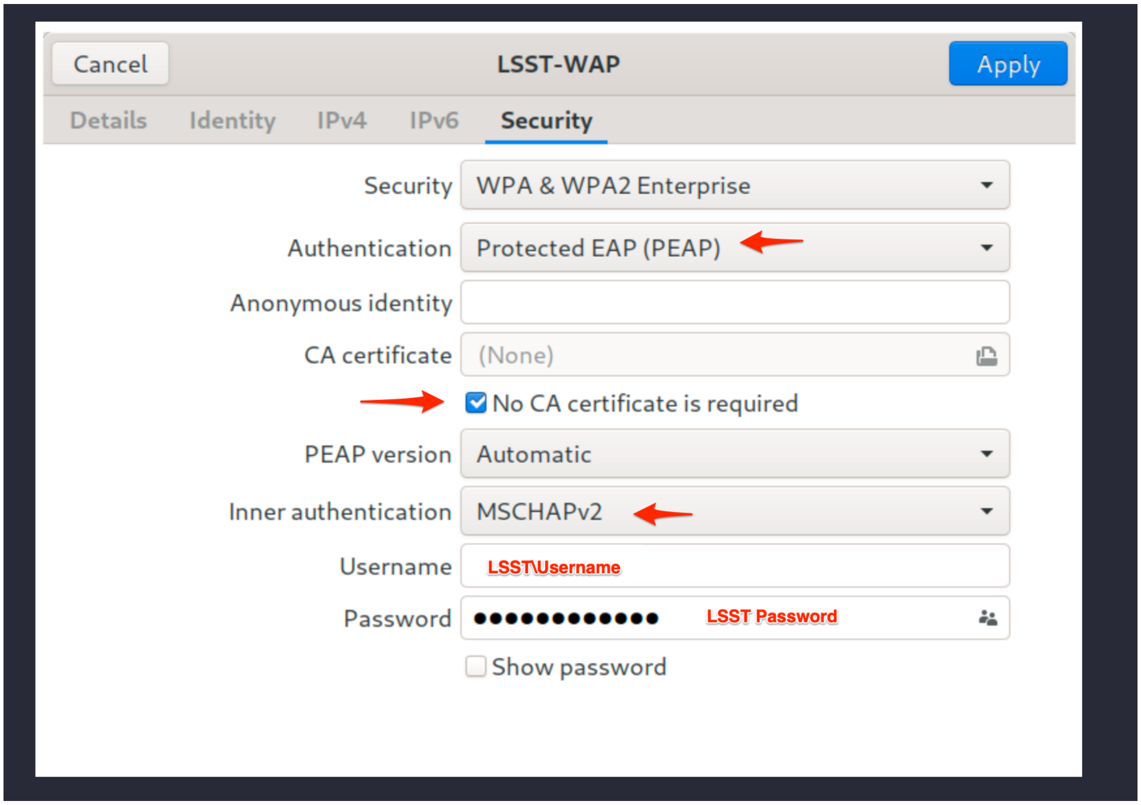
Authenticating to network “LSST-WAP”

Before authenticating to server “Crux.lsst.local”, you should examine the server's certificate to ensure that it is appropriate for this network.

To view the certificate, click ‘Show Certificate’.

3.) Accept the certificate and hit continue to connect.

4.4 Linux



Security: WPA & WPA2 Enterprise

Authentication: Protected EAP (PEAP)

Anonymous identity:

CA certificate: (None)

☑ No CA certificate is required

PEAP version: Automatic

Inner authentication: MSCHAPv2

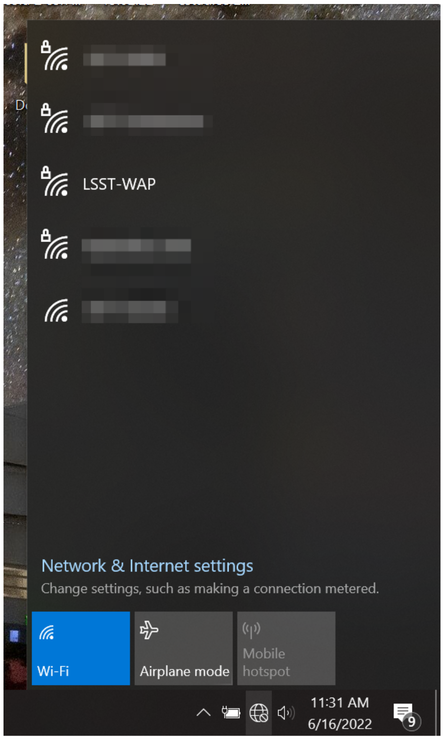
Username: LSST\Username

Password: ●●●●●●●●●●●● LSST Password

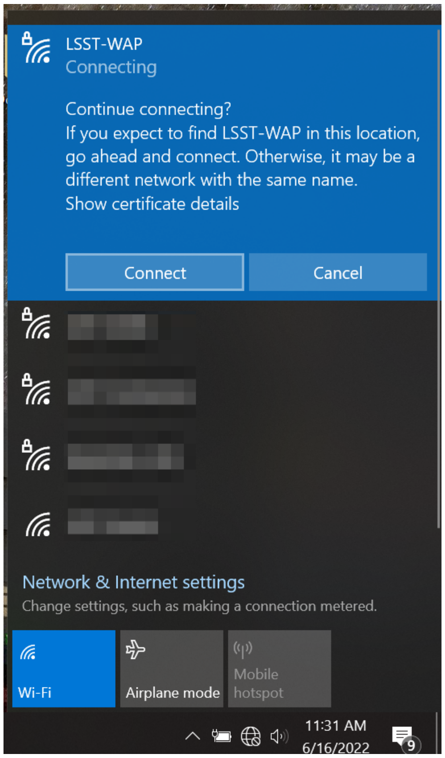
□ Show password

Use the following network configurations settings to setup the LSST-WAP WIFI Network on Linux laptop computers.

4.5 Windows



1.) Select the LSST WAP WIFI Network from the list if at La Serena Base or Cerro Pachon.


LSST-WAP
Connecting

Continue connecting?
If you expect to find LSST-WAP in this location, go ahead and connect. Otherwise, it may be a different network with the same name.
Show certificate details

2.) Select connect, log in with your domain account credentials both username and password.

5 Offboarding

File an IHS ticket with the following information:

- Project: IT Helpdesk Support (IHS)
- Issue Type: Service Request
- Summary: Offboarding <user>
- Component: AAA
- Description:

<user>: Name of the user to offboard.

Offboarding tickets must be created by the manager of the user to offboard, and if it's time sensitive, please contact by email or Slack the DevOps manager.

The user will be offboarded from the following services

- Summit Services
- Active Directory
- Slack
- 1Password
- Github

6 Auditing

Visitors can be provided with temporary accounts, which will have separate records maintained for them. These accounts are scheduled for deactivation on the last day of each month through an automated process.

However, this deactivation can be prevented if the manager responsible for the visitor explicitly overrides the process to exclude the account from the deactivation cycle.

The current list of temporary accounts is available at https://rubinobs.atlassian.net/l/cp/ddeM4LkA, where managers should also record any overrides.