



Vera C. Rubin Observatory
Rubin Observatory Project Office

Summit Onboarding Procedure

Diego Tapia, Cristian Silva

ITTN-045

Latest Revision: 2021-05-31

DRAFT



Abstract

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

Draft

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

Document source location: <https://github.com/lstt-it/ittn-045>

Draft

Contents

1 Introduction	2
2 Requesting an IPA account	3
2.1 Rubin Server Authentication	6
2.1.1 SSH Keys Creation	7
2.1.2 Linux and MacOS	7
2.1.3 Windows OS	8
2.1.4 Add Public Key Into IPA	11
3 Requesting Domain Credentials	15
4 Requesting Nublado Access	15

Draft

Summit Onboarding Procedure

Draft

1 Introduction

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

The access to servers (ssh) and VPN is controlled by the IPA backend. To request an IPA account please refer to the section Requesting an IPA Account

The access to Nublado is controlled by a Github backend. To request Nublado access please refer to Requesting Nublado Access.

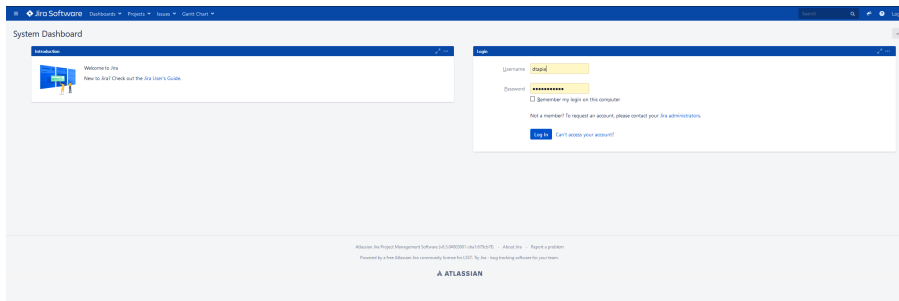
The access to Wifi is controlled by domain credentials. To request Domain Credentials please refer to Requesting Domain Credentials.

Draft

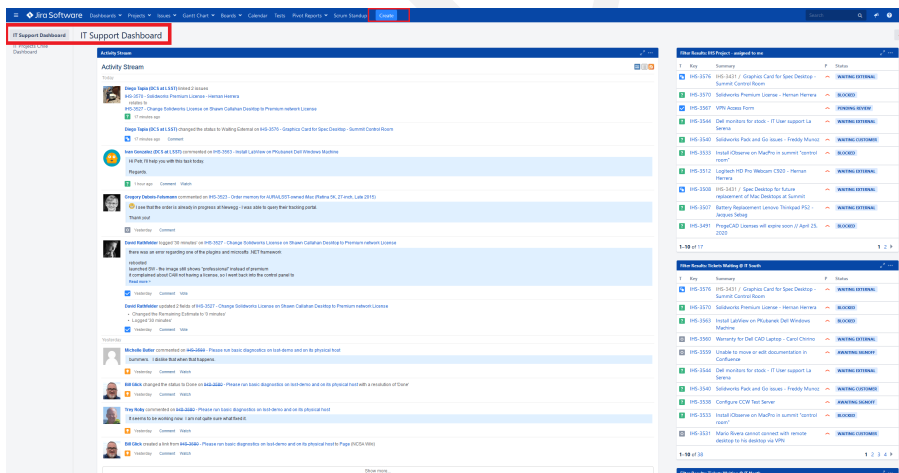
2 Requesting an IPA account

To request an IPA account, it is required for the user to create a Service Request ticket inside the IT User Support Dashboard. Please check the example below.

Head over to <https://jira.lsstcorp.org> and log in with your domain account credentials.



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



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

- Project: IT Helpdesk Support (IHS)
- Issue Type: Service Request
- Summary: IPA Account Creation / VPN Access - "Insert your name here"
- Component: AAA
- Description: Please use the template provided below.

1. **Project:**

IT Help desk Support (IHS)

2. **Issue Type:**

Service Request

3. **Summary:**

IPA Account Creation / VPN Access - "Insert your name here"

4. **Component:**

AAA

5. **Description:**

Copy and Paste the following information and fill out the form.

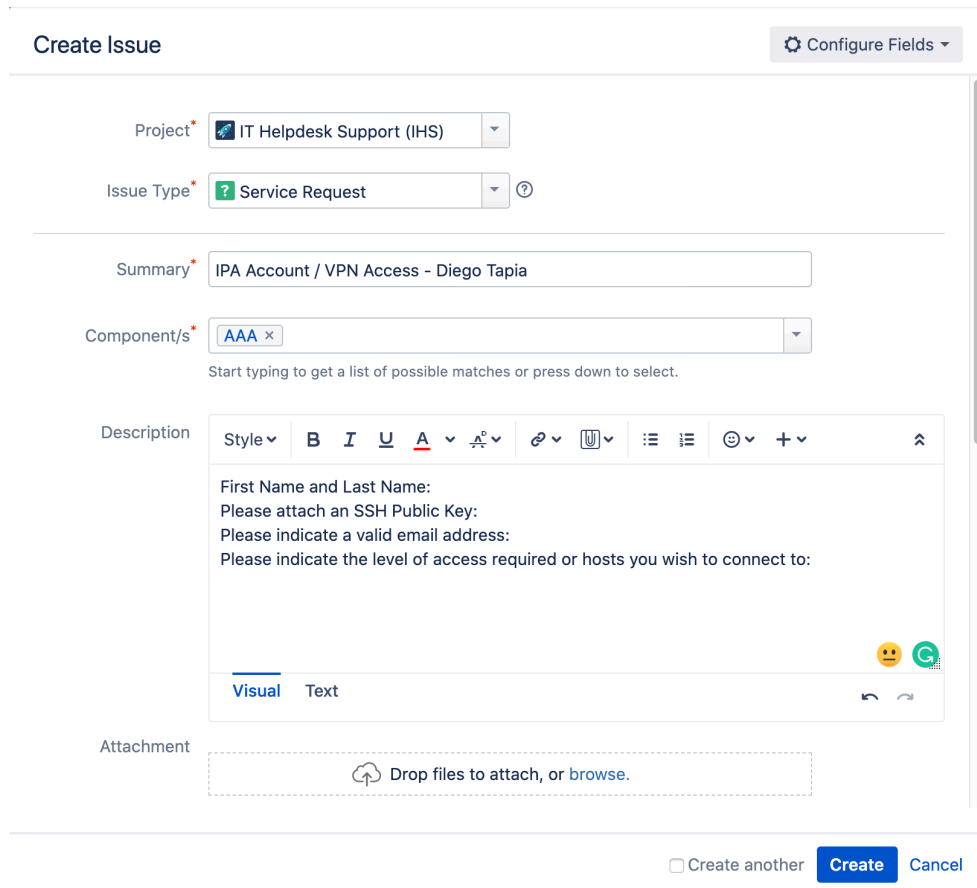
First Name and Last Name: (.....)

Please attach an SSH Public Key: (.....)

Please indicate a valid email address: (.....)

Please indicate the level of access required or hosts you wish to connect to: (.....)

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



Create Issue Configure Fields

Project* IT Helpdesk Support (IHS)

Issue Type* Service Request

Summary* IPA Account / VPN Access - Diego Tapia

Component/s* AAA

Description

First Name and Last Name:
Please attach an SSH Public Key:
Please indicate a valid email address:
Please indicate the level of access required or hosts you wish to connect to:

Attachment

Drop files to attach, or [browse](#).

Create another Create Cancel

IT User support will receive the request and will proceed with the account creation process. Once the account has been created and the services have been provisioned IT Support will be in contact with you via email to provide you with the account credentials and services you've been granted access too along with the website where you can change your temporary password.

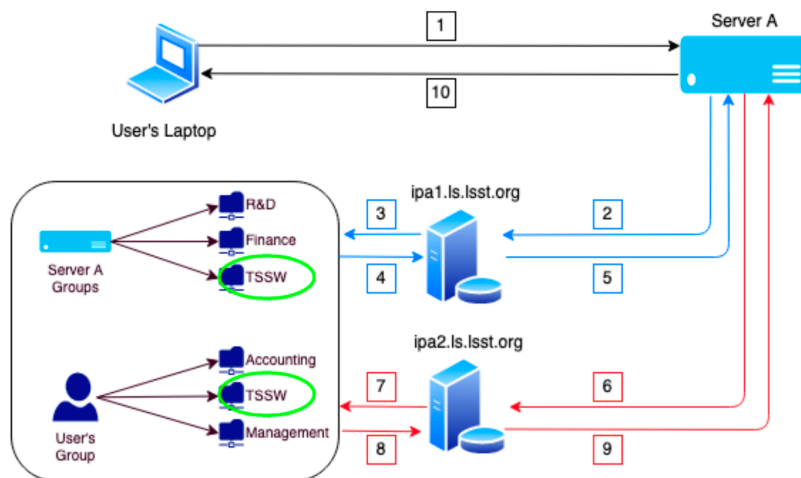
If you have any questions or concerns regarding the services provisioned please contact IT User Support at rubinobs-it-las@lsst.org

2.1 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 accounts and 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.is.sst.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 user 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.

2.1.1 SSH Keys Creation

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

2.1.2 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:seMcIk0bj0ZhXlKer5ik6e3mpAMisYdvZwziPddbAs 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:

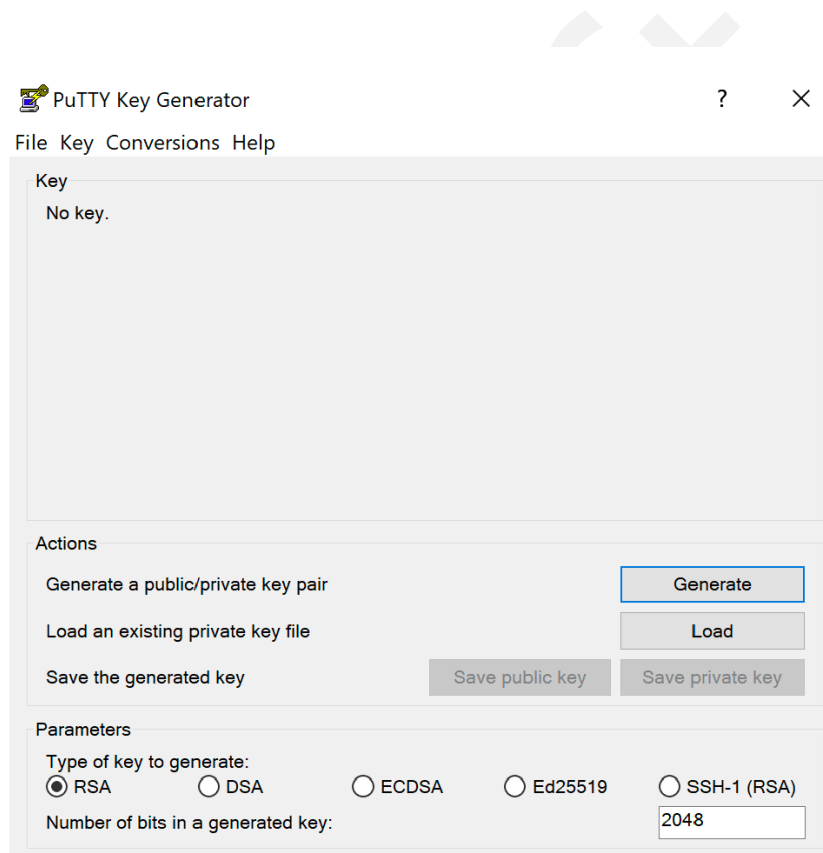
```
john@localhost:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/john/.ssh/id_rsa): /home/john/.ssh/rubin_rsa
Enter passphrase (empty for no passphrase): #HIT ENTER, DO NOT WRITE ANY CONTENT
Enter same passphrase again: #ENTER
Your identification has 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:seMcIk0bj0ZhXlKer5ik6e3mpAMisYdvZwziPddbAs 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, which is intended to be shared and publicly known.

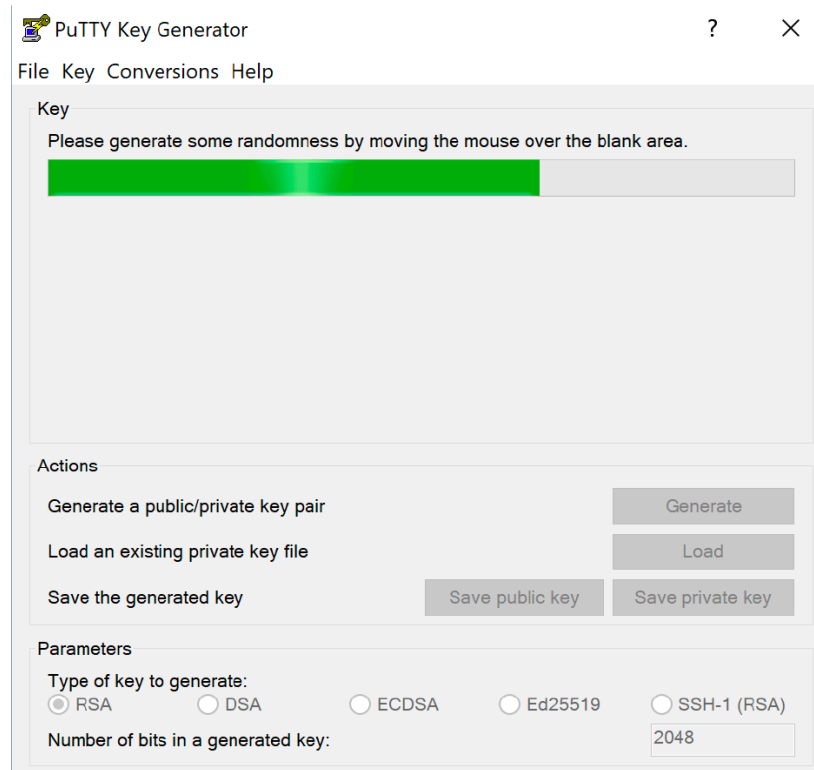
2.1.3 Windows OS

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):

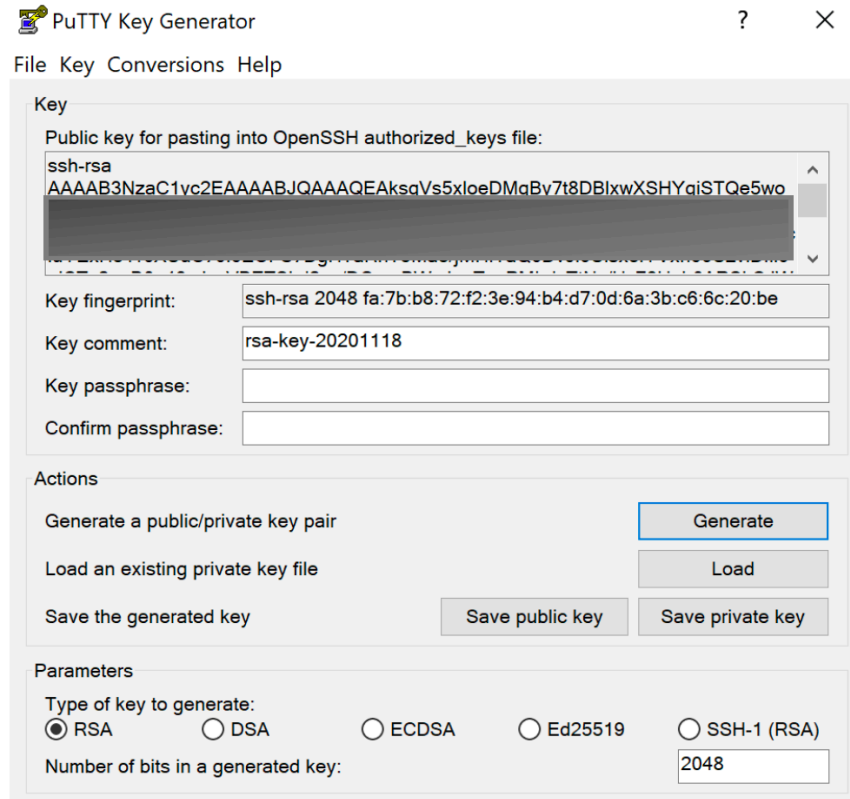


Click on generate:



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:

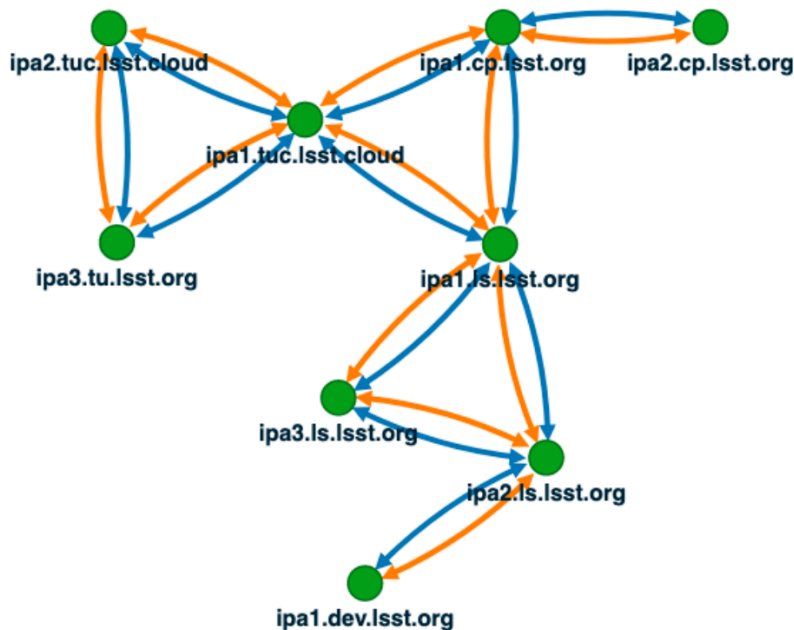


Now, save both keys into a well-known location. It is recommended (but not needed) to create a folder named "ssh" in the user's home directory, so when asked, you can easily find your keys in "/Users/<username>/ssh".

2.1.4 Add Public Key Into IPA

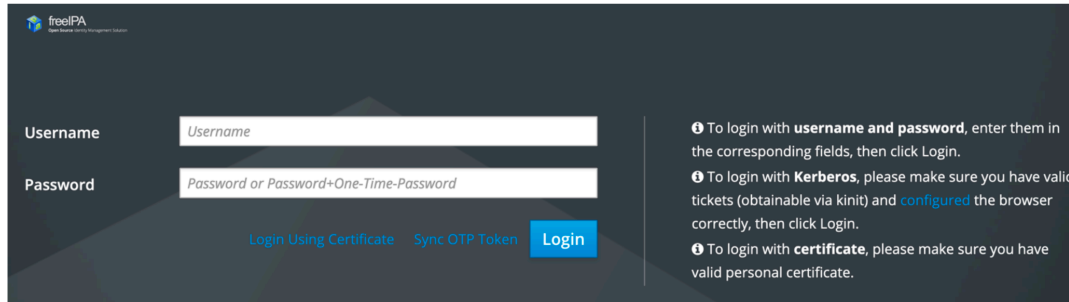
The IPA infrastructure is composed of a master server and several replicas, meaning that it does not matter in which one you modified your personal data, it will be propagated over the rest of the nodes.

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

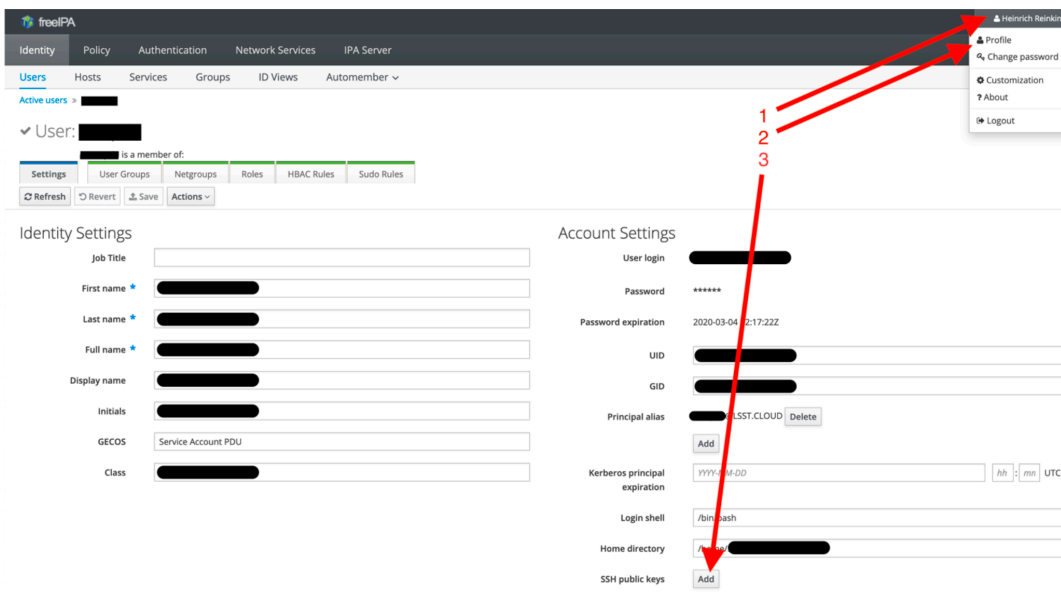


The orange arrows represent the DL (Domain Link), meanwhile the blue arrows the CA (Certificate Authority). The DL keeps the authenticity of the defined domain – i.e. server.local – and the CA is the responsible of emitting and signing the hosts certificates, to validate their authenticity.

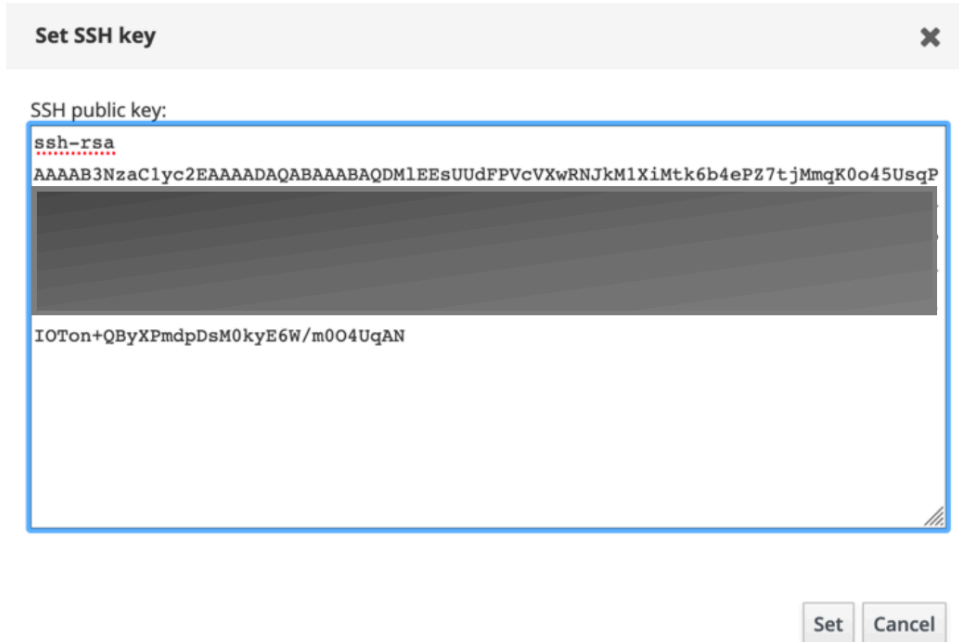
In order to add your public key into IPA, you must access through any of the http frontends, from either the replicas or master. Bear in mind that you must be either inside the network or connected through VPN. Let's use the BDC (Base Data Center) replica: open a web-browser and navigate to IPA Website.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



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:



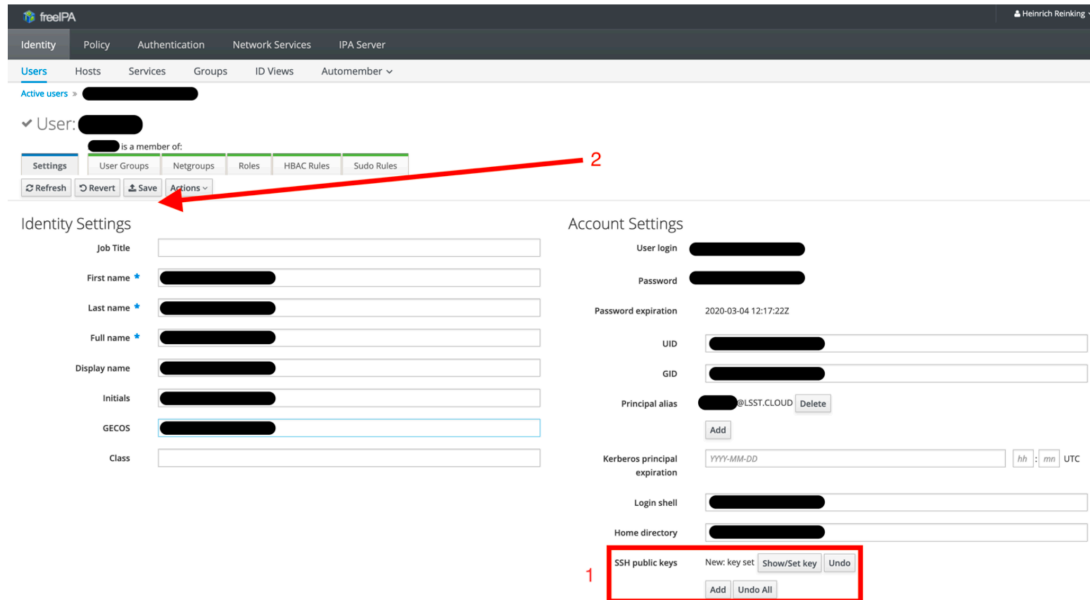
A pop-up window will appear, in which you must paste your public key:



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

```
----- BEGIN SSH2 PUBLIC KEY -----  
Comment: ""  
AAAAB3NzaC1yc2EAAAABJQAAAgEAgQuf5Sd1Z51XkjUPN2Fwusz2NGkO6ZDAzdV  
KvprMERiajyNnkU7JQw1V020L+IwFuyoJ0W5Zi6zjXzmDw1zTKPAN2vjoorBAyMoy  
w/JPwBeiEfc9nBLbNEgyWlnMsPNnTeLqHWfwCxrP58LHHJQDs18f1qLvJSM9XnYu  
bJgRJNS1TCAR37N7Y0zMuyS5ku/Xn3CwXI+DQdkE8TMXFuG8Jdd8EkSHTtDy/JM3  
VprMERiajyNnkU7JQw1V020L+IwFuyoJ0W5Zi6zjXzmDw1zTKPAN2vjoorBAyMoy  
cZ2NGa+kfxJXe5unDi4Pi0wSvo9y5HzqEzYWdpXYEqnzVeXiUquSI/+mhT7tgRjE  
+dEnuG5GYpd6pVrg34BBkAFP9Gmd4kd9F18LWf0h968xkUo7IN7IVHuPQRRiUATb  
XF0FHD62Y/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:



The screenshot shows the freeIPA web interface. The top navigation bar includes Identity, Policy, Authentication, Network Services, and IPA Server. The main menu has Users, Hosts, Services, Groups, ID Views, and Automember. The 'Users' section is active, showing a list of users. A user is selected, and the 'Settings' tab is active. The 'Actions' menu is highlighted with a red arrow labeled '2'. The 'SSH public keys' section is highlighted with a red box labeled '1'.

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

3 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.

4 Requesting Nublado Access

The access to Nublado is controlled by Github, hence the user requesting access must have a Github account.

To request access open a DM ticket in Jira including:

- Name
- Email
- Github account

A member of the Square team will grant you access.