

# Vera C. Rubin Observatory Rubin Observatory Project Office

# **Summit Onboarding Procedure**

Diego Tapia, Cristian Silva

**ITTN-045** 

Latest Revision: 2024-05-03





### 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

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



# 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	Accesing the Rubin Observatory WIFI network	16
	4.1 Android Mobile Device	17
	4.2 Apple Mobile Device	19
	4.3 MacOS	20
	4.4 Linux	21
	4.5 Windows	22
5	Access to Nublado, EFD/Chronograph and other SQuaRE services	23
6	Software Deployment - Access and Prerequisites	24



# Summit Onboarding Procedure



# **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 acccess 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 refert to Requesting Domain Credentials.

# 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://rubinobs.atlassian.net/ 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

rt Dashlooard	IT Support	Dashboard			
i chia	Activity	(fram	1200	Fiber Results: HS Project - assigned to me	- 2
	Activit	ty Steam		T Key Summary	P. Status
	70407			IHS-3576 IHS-3431 / Graphics Card for Spec Desizop -	WRITING DITURNE
	1	Deep Tapas (PC) and ST 1000 2 Damage		54 DR-3520 Solidarida Parria et Linena - Hernan Herrera	
	1	Product V analogue Productor Localization Production Productine Productine Productine Pr		INC. 1567 VIN Arrays Down	A REAL POINT
		Photo		Information	- House and
		Diego Tapia (ICS at LSST) changed the status to Waiting Editorial on I+6-2570 - Straptics Card for Spec Dealting - Summit Cardiol Room		Service	A ANTIN DITIAL
		Consider app Comment		146-3540 Salidworks Pack and Go issues - Freddy Manoz	WINTING CUSTOMER
		Here Genoties CES & LSSS2 sommented on Pr0-3555 - Install LaWien on Photomet Machine		IHS-3533 Install (Observe on Machro in summit "control	A 8.0080
	•	H Petr, If help you with this task today.		reem	
		Repris.		Herman Herman	ANTINE DITURNE
		Trour ago Lummeri Viagos		IHS-3500 IHS-3431 / Spec Desktop for future	WANTING DITIONAL
	6	Gregory Debis-Lebisman converted on H5-522- Order memory to AUMA(551-anead Aur (Fatina 82, 27-ind, Lak 2015) Characteristic and tais interaction interaction and the automatical and the automatic		Inglacement of Mac Desitops at summit	ANTAL INTERN
	101	There you		Jacques Sebag	
		Website Comment		Int6-3491 ProgeCAD Licenses will opine soon // April 25. 2020	A.0000
		Devel Statisticities logged 38 minutes on HIS-3527 - Change Soldwards Ucense on Shawn California Desition to Premium retrieven Ucense		1-30-0117	
	1	there was an error regarding one of the plugins and microsofts JACT femework.			
		Hoholad Jaunché CVII - Iho Image JAB Johons "professional" Indead of premium		File Reads: Tickets Walling @ IT South	
		It compared about DAW not having a license, so I went back links the control panel its Read News'		T Key Summary	P. Status
		Valuetay Cumment Mos		INS-3576 INS-3431 / Graphics Card for Spec Desitop - Sammit Control Room	WATER DTIDAK
		Devid Deshielder spolate 2 hields of 146-3537 - Change Solidevola License on Sharen Calilatera Desitegio Prenium nativoli License		1HS-3570 Salidworks Premium License - Hernan Herrera	- B.0000
		Complete Normaling Community     Complete Normaling Community		IP6-3563 Instal LaWiew on Pflubanek Del Windows	. BLOCHED
		Valuety Connect VDs		Natine	
	Yesterd	0 Harden and an 10 Marca and an 10 Marca and an inclusion of an inclusion of an inclusion of an inclusion of an		Ins-350 Wanterly for Dail CAD Lapites - Carel Chines	A WALL DODAN
		Summer: 1 dalle That advertisel That Supports		Configence	A SAVING BENCH
		Visionity Comment Watch		IHS-3545 Del monitors for stock - IT User support La formation	WANTING DITIONAL
		Bit Block sharped the status to Does on 162,2020 - Press run hado diagnostics on instromen and on its physical hast with a resolution of Donn'		Service IPS, 35(2) Solidaevils Park and En issues - Freide Manue	ANTING OFFICIARY
	10	Validay Canada Web		Distance of the second second second	
		They Role commented to SEL2280 - Prease run tasks dampestos an test demo and on its physical hest		Information Consignation of High Server	And and Martin
		E neeros to be avoing new 1 arc not gate sure what field it.		Inc-3333 Initial coserve on Machine in Editory ream?	A BOORD
		Visiteday Comment Watch		IFG-3531 Mario Rivera cannot canned, with remote	WINTING CUSTOMIN
		DB Glock created a link hom H45-3640 - Presse run haald diagnostics on last-demo and on its physical healts Page (NCGA VIIII)		desitop to his desitop via VPN	



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 <sup>*</sup>	IT Helpdesk Support (IHS)	
Issue Type <sup>*</sup>	Service Request	
Summary*	IPA Account / VPN Access - Diego Tapia	
Component/s*	AAA × Start typing to get a list of possible matches or press down to select.	•
Description	Style $\checkmark$ B       I       U       A $\checkmark$ $?$ $?$ $!!       !!!       !!!       !!!       !!!       !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!$	+• * ect to:
Attachment	Drop files to attach, or browse.	
	□ Create and	other 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.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  $6 \rightarrow 7 \rightarrow 8 \rightarrow 9$  instead of  $2 \rightarrow 3 \rightarrow 4 \rightarrow 5$ .

#### 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):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your public key has been saved in /home/ john /.ssh/id\_rsa.
Your public key has been saved in /home/ john /.ssh/id\_rsa.
SHA256:seMcIk0bqj0ZhXlKer5ik6e3mpAMisYdvZwziPdbAs 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:



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.



#### 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):

💕 PuTTY Key Generator					?	$\times$
File Key Conversions Help						
Key No key.						
Actions						
Generate a public/private key pair				Gene	erate	
Load an existing private key file				Lo	ad	
Save the generated key		Save	public key	Save priv	vate key	
Parameters						
Type of key to generate:		A	O Ed25519		H-1 (RS/	۹)
Number of bits in a generated key:				2040		



#### Click on generate:

PuTTY Key Generator	? ×
File Key Conversions Help	
Key Please generate some randomness by moving the mouse over the bl	ank area.
Actions	
Generate a public/private key pair	Generate
Load an existing private key file	Load
Save the generated key Save public key	Save private key
Parameters	
Type of key to generate:         Image: RSA in the second	🔵 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:

PuTTY Key Generator ?					
File Key Conversions	Help				
Key Public key for pasting ssh-rsa AAAAB3NzaC1vc2EA	into OpenSSH authorize	ed_keys file: :5xloeDMqBv7t8DBIxwX	(SHYaiSTQe5wo		
Key fingerprint:	ssh-rsa 2048 fa 7b b8	72:f2:3e:94:b4:d7:0d:6a	13b;c6;6c;20;be		
Key angerprint.	rsa-key-20201118	/			
Key comment.	Key passphrase:				
Key passphrase:					
Confirm passphrase:					
Actions					
Generate a public/priv	ate key pair	[	Generate		
Load an existing priva	te key file		Load		
Save the generated ke	ey (	Save public key	Save private key		
Parameters					
Type of key to generat					
U RSA		A () Ed25519	2048		
Number of bits in a ge	nerated key:		2040		

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:

n freeIPA Agene laware and in foregrowere industry		
Username	Username	O To login with username and password, enter them in
		the corresponding fields, then click Login.
Password	Password or Password+One-Time-Password	• To login with <b>Kerberos</b> , please make sure you have valid
		tickets (obtainable via kinit) and configured the browser
	Login Using Certificate Sync OTP Token Login	<b>a</b> To login with <b>certificate</b> 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:

🏇 freeIPA		≜ Heinrich Reinking
Identity Policy Authentication Network Services IPA Server		A Profile
Users Hosts Services Groups ID Views Automember ~		Customization
Active users >		? About
✓ User:		( Logout
is a member of:		3
Settings User Groups Netgroups Roles HBAC Rules Sudo Rules		ĭ
C Refresh     D Revert     Actions ~		
Identity Settings	Account Settings	
Job Title	User login	
First name *	Password	*****
Last name *	Password expiration	2020-03-04 2:17:22Z
Full name *	UID	
Display name	GID	
Initials	Principal alias	LSST.CLOUD Delete
GECOS Service Account PDU		bbA
Class	Kerberos principal expiration	yyyx4M-DD [hh]:[mn] UTC
	Login shell	/bin pash
	Home directory	
	SSH public keys	Add



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

Set SSH key	×
SSH public key: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDM1EEsUUdFPVcVXwRNJkM1XiMtk6b4ePZ7tjMmqK0o45Us IOTon+QByXPmdpDsM0kyE6W/m004UqAN	₽ġ₽
Set Can	//.

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



---- END SSH2 PUBLIC KEY ----



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

🎓 freeIPA		L Heinrich Reinking ∽
Identity Policy Authentication Network Services IPA Server		
Users Hosts Services Groups ID Views Automember ~		
Active users >		
✓ User:		
Settings User Groups Netgroups Roles HBAC Rules Sudo Rules	2	
C Refresh ◯ Revert ▲ Save Actions >		
Identity Settings	Account Settings	
Job Title	User login	
First name *	Password	
Last name *	Password expiration	2020-03-04 12:17:22Z
Full name *		
Display name	UD	
	GID	
	Principal alias	@LSST.CLOUD Delete
GECOS		Add
Class	Kerberos principal expiration	YYYY-MM-DD hh : mn UTC
	Login shell	
	Home directory	
	SSH public keys	New: key set Show/Set key Undo
	1	Add Undo All

(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 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.



Network from the list.

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



12:12 🖪	資 🔌 46 Jil 麗 <sub>2 J</sub> il 90% 💼
< LSST-WAP	
Método EAP PEAP	
Identidad	T\Username
Contraseña LSST Passwo	rd Q
Seleccionar certificac	lo
Usar certificados del	sistema
No validar No Validat	
Autenticación de fase MSCHAPV2 MSCHAPV2	2
Identidad anónima	
Ajustes de IP DHCP	
III O	<





#### 4.2 Apple Mobile Device



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



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



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.



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



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



#### 4.4 Linux

Cancel	LSST-WAP	Apply
Details Identity IPv4 IPv6	Security	
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.



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



# 5 Access to Nublado, EFD/Chronograph and other SQuaRE services

A number of data services on the summit are operated by the SQuaRE team and are currently authenticated via Github. This includes the summit instance of the Science Platform, including the Notebook Aspect, intformally referred to as Nublado. It also includes the EFD (Engineering Facilities Database) and its web-based front end (Chronograph)

To gain access to your services you must (a) have a Github account and (b) it must belong to the right organisation and team.

If are a member of the Telescope & Site team, you are probably already a member of the Github lsst-ts organisation, and you merely need to check that you are in the summit-access team in that org.

If you are not, you need to be invited in the rubin-summit organisation and added to the rspaccess team. Ask on the #com-square Slack channel to be added to summit-access, mention your Github username and a number of people will be able to add you.

Note: Adding your Github username to your Slack profile is really helpful and saves you from being asked to supply it. To do that, select Edit Profile on Slack and sroll down until you find a field called Github Username.



### 6 Software Deployment - Access and Prerequisites

1. Follow instructions in ITTN-045, file an IHS ticket (1 of 3) to request access to IPA, the VPN and the Resources and Bare-Metal Machines for

- a) TTS.
  - Include access to the ArgoCD Admin and Tucson Teststand (TTS) 1Password vaults in the request.
- b) BTS.
  - Include access to the ArgoCD Admin and Base Teststand (TTS) 1Password vaults in the request.
- c) Summit.
  - Include access to the ArgoCD Admin and Summit 1Password vaults in the request.
- 2. Request for increased privileges.
  - a) For deployments and system administration, sudo privileges are required.
    - File an IHS ticket (2 of 3).
- 3.) Request access to the following Github Organizations.
  - a) lsst-it (docker-compose-ops-repo, explicitly).
    - File and IHS ticket (3 of 3).
  - b) lsst-ts (argocd-csc scripts).
    - Submit and Email or Slack request to Rob Bovill (rbovill@lsst.org).



- 4.) Access to kubectl and argocd CLI tool.
  - a) Install to local machine.
    - kubectl
      - \* TTS Configuration
      - \* BTS Configuration
      - \* Summit Configuration
    - argocd
      - \* Checkout the argo-csc repo, it contains scripts used during the deployment.
      - \* Create the \$HOME/.argocd\_auth file