

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.





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/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 Requesting Nublado Access

15



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

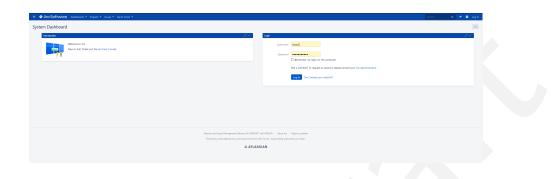
The acccess to Nublado is controlled by a Github backend. To request Nublado access please refer to Requesting Nublado Access.

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://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

Dashbaard IT Si	pport Dashboard	
719	Aching Steam y ² ···	Fibur Results: HS Project - anigned to me
	Activity Stream	T Key Summary P Status
	The set has 0C18150108923888	IHG-3576 IHG-3431 / Graphics Card for Spec Desitop - A WARTING DOTTIONS, Symmit Control Report
	Begin page (EXELISI)) ment 2 mane Belo 2017 - Seldenta Pernian Literara - Hernan Herna Interne II	😫 145-3570 Soldworks Premium License - Hernen Herrera 🕋 1600600
	Holden III H5-5027 - Change Deldents Loosse en Shann Calaba Desting in Pernant netres Loonee	🖬 INS-3567 VIIN Access Form 🔷 PUNCING REVEN
	Deep Tapla (CC) at LSST) dramped the status to Walking Galerian on 146-3576 - Graphics Carefor Specific Gareria	INS-354 Del monitors for stock - IT User support La A WARTING SETTINAL Servica
	S of minutes app Comment	145-3540 Salidworks Pack and Go issues - Freddy Munoz WINTING CONTINUES.
	Par Concepte CIRCS at 1.5572 permential on PIG-3055 - Install LaiMonn on Photomes Dell Windows Madrine III Petr, III help you with this tack holes	In6-3533 Install Observe on Machine is summit "centrel R00000 room"
	Reprin.	INS-3512 Logitech HD Pro Webcam C920 - Heman Automic Distance, Herman
	Therapy Connect Valo Therapy Connect	INS-3500 INS-3631 / Spec Desktop for future reducement of Mac Desktop at Summit
	Compared to constraints on the constraints on the cost of constraints on the cost of constraints and constraints on the cost of constraints on the cost	🖬 145-3507 Battery Replacement Lenove Thinkpad PS2 - 👝 (WRITHS DITTERS).
	Tability (mmet	Aropus Sebag PE-3431 ProgrCAD Licenses will expire scon // April 25. K00000
	Vestory Comment Second Statisticaler Logger 20 minutes' on HSU327- Charge Soldwards Lorense on Diawn Californi Desting to Premium Indexin Lorense	2020
	term transmer region of means or models? - Long or observes comes or column cannot be any comment or means to be any column columns. Dense the second column columns are set of the second column columns of the second column columns.	1-50 of 17
	entered and the second se	Film Results: Telets Making () IT South
	Ecomplianted plotted. Delli Echteaning a license. so 1 weet back this his contral panel in Read and >>	T Key Sammary P States
	Z Valaday Canned Van	INS-3576 INS-3431 / Graphics Card for Spec Desistop - A WRITING EXTERNAL Sammit Control Room
	Devid Partiteter updated 2 hids of Hid-3027 - Change Soldworks License on Steam California Cesiting to Permism network License Changed the Remaining Estimate to Innotesty	🖬 145-3570 Salidworks Prenium License - Hernan Hernera 🛛 🗮 🛤 👀 🕬
	- Laged 20 minuter	IPG-3563 Instal LatView on PKubanek Del Windows R000000 Machine
	Yester Sar	🔄 195-3550 Warranty for Dell CAD Laptop - Carol Chino 🔷 🗰 Westies Different
	Michele Refer commented on H6-2664 - Plause not basic disposition on taxif dema and on its physical host bummwr, Lidslike Rutz when Rutz Lagoens.	Ind-3559 Utable to move or edit documentation in A ARANTINE MEMORY Configurate
	Visionity Connent Weigh	195-3545 Del monitors for stock - If User support La A WARTING DETERMIN Serves
	Bit Galor categorithe statum to Does on Sel2-2200-Preserven taxo: dagnetistic service-band on its physical next with a restation of Done	InS-3540 Soldworks Pack and Go issues - Freddy Mannez WINTING COSTOMER
		🖬 195-3338 Configure CCW Test Server 🔷 🗾 Annu Test Selectri
	They Note commented on Nucleater-Present ministration and on the project meet	Info-3533 Instal (Coverse on Machto in summit 'control mocean)
	Visional West	ING-3531 Mario Rivera cannot cannett with remote Watering Controlment
	M Citick created a link how H4-3480-Please run basic dispersites and acid one and on its physical hearts for gap (NCGA Wei) Uncertain Comment Tests	desitop to his desitop via VPN 1-58 af 38 1.2.3



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 × Start typing to get a list of possible matches or press down to select.	•
Description	Style × B I <u>U</u> A × A × ∂ × U × ∷≣ ∷≣ ⊙ ×	+~ *
	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 conne	ect to:
	Visual Text	<mark>:: ©</mark>
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

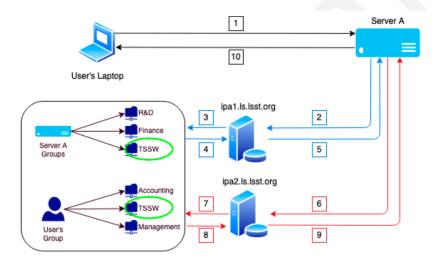


2.1 Rubin Server Authentication

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): #HIT ENTER, D0 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:



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			? ×
File Key Conversions Help			
Key No key.			
Actions			Generate
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: RSA DSA		0	0
C NSA O DSA	ECDSA	C Ed25519	O SSH-1 (RSA)



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 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:

PuTTY Key Generator ?							
File Key Conversions Help							
Key	Key						
Public key for pasting into OpenSSH authorized_keys file: ssh-rsa AAAAB3NzaC1vc2EAAAABJQAAAQEAksqVs5xloeDMqBv7t8DBlxwXSHYqiSTQe5wo							
						AAAAB3NzaC1vc2EA	AAABJQAAAQEAksaVs
			21 0 0 001				
Key fingerprint:	ssh-rsa 2048 fa:7b:b8:	72:f2:3e:94:b4:d7:0d:6a	a:3b:c6:6c:20:be				
Key comment:	rsa-key-20201118						
Key passphrase:							
Confirm passphrase:							
Actions							
Generate a public/priva	ate key pair		Generate				
Load an existing privat	te key file		Load				
Save the generated key Save public key Save private key							
Parameters							
Type of key to generat							
0		SA 🔿 Ed25519	O SSH-1 (RSA)				
Number of bits in a ger	nerated key:	Number of bits in a generated key: 2048					

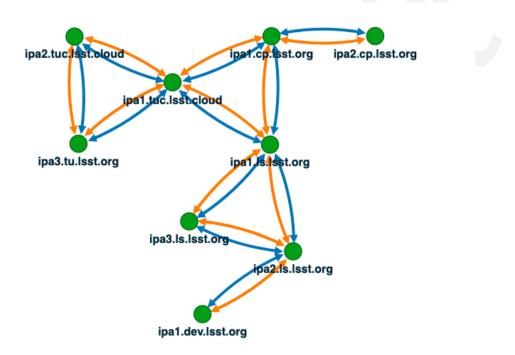
Now, save both keys into a well-known location. It is recommended (but not needed) to create a folder named "ssh" in the user's home directory, so when asked, you can easily find your keys in "/Users/<username>/ssh/".



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:

freeIPA New New York transmission		
Username	Username	 To login with username and password, enter them in the corresponding fields, then click Login.
Password	Password or Password+One-Time-Password Login Using Certificate Sync OTP Token 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:

🏇 freeIPA				🔺 Heinrich Reinking 🗸
Identity Policy Au	thentication Network Services IPA Server			♣ Profile ♣ Change password
Users Hosts Servi	ices Groups ID Views Automember ~			Customization
Active users >				? About
✓ User:			2	(+ Logout
is a me	mber of:		3	
Settings User Groups			i i	
2 Refresh D Revert 2 Sav	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		Add	
Class		Kerberos principal	YYYY-I M-DD	hh : mn UTC
		expiration		
		Login shell	/bin bash	
		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	
	11.
Set Cano	cel

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:

🏂 freelPA						≜ Heinrich Reinking ~
Identity Policy Aut	hentication Network Services					
Users Hosts Servic	es Groups ID Views	Automember ~				
Active users >						
✓ User:						
Settings User Groups	nber of: Netgroups Roles HBAC Ru	les Sudo Rules		2		
C Refresh C Revert & Save						
Identity Settings			Acc	ount Settings		
Job Title				User login		
First name *				Password		
Last name *				Password expiration	2020-03-04 12:17:22Z	
Full name *					LOLO US OF TELEVILLE	
Display name				UID		
				GID		
Initials				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 proccess 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.