nor1
Upgrade Your Life®

On Prem - SFTP Configuration

Contents

Requirements - Opera Simple Reports via SFTP

For whitelisting extracts.nor1.com on the hotel side

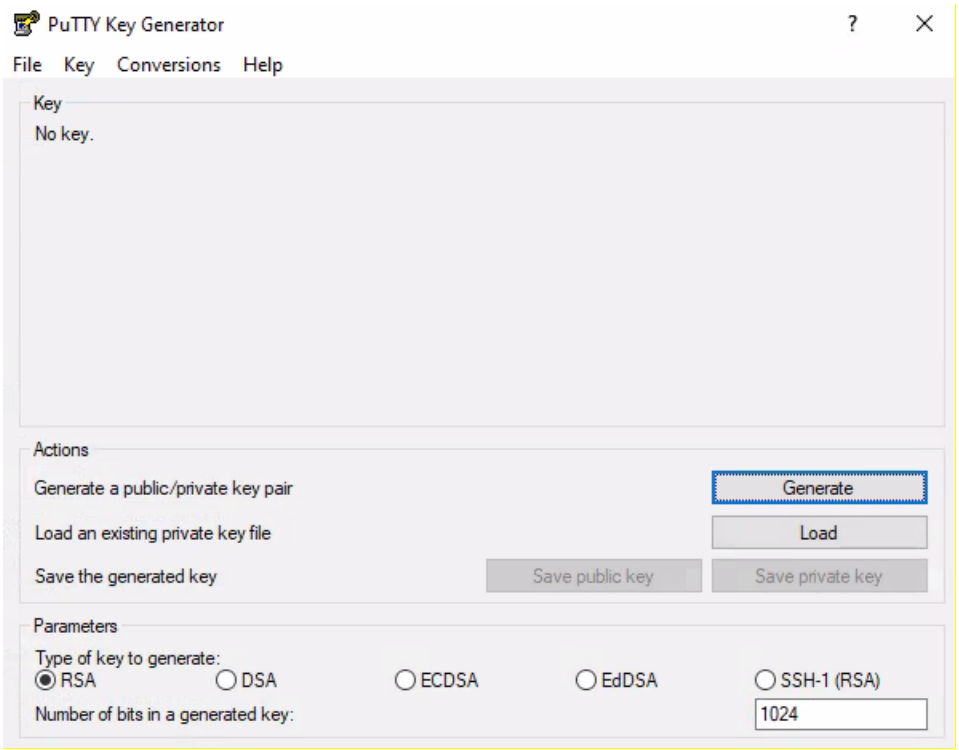
- 3.212.135.224
- 34.231.219.100
- They need to ensure they are allowing outbound traffic to those 2 IPs over port 22.
- The “first” IP is our current primary SFTP server. The “second” IP is going to be (in the future) our backup SFTP server

On a first call, request the Public IPv4 address of their Opera Application Server. To obtain this, navigate to https://www.whatismyip.com/

Creating a Public/Private Key Pair using Puttygen:

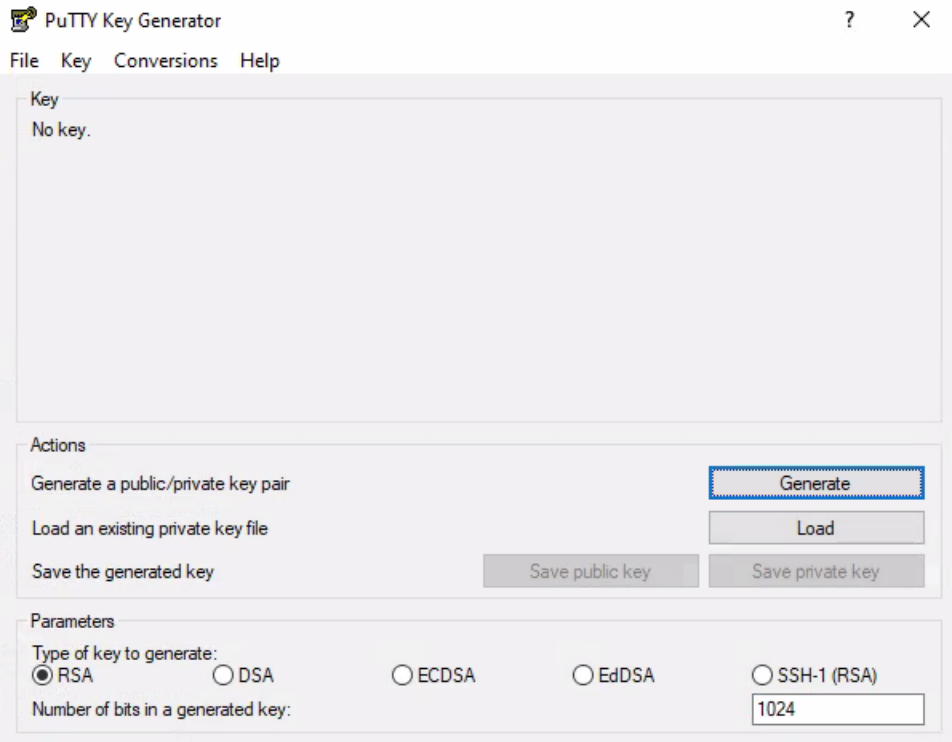
Download PuttyGen on the hotel´s server: https://puttygen.com/download.php?val=49

1. In the **Parameters** area, select “RSA”

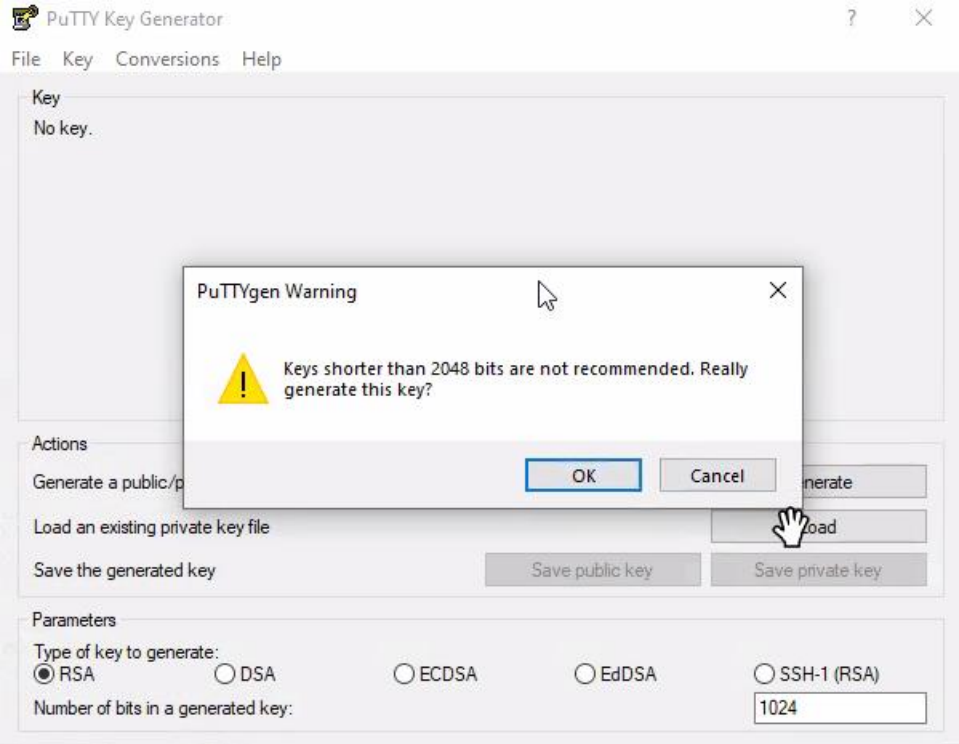


2. Change number of bits in a generated key from 2048 to 1024. Anything above 1024 will not work in Opera.

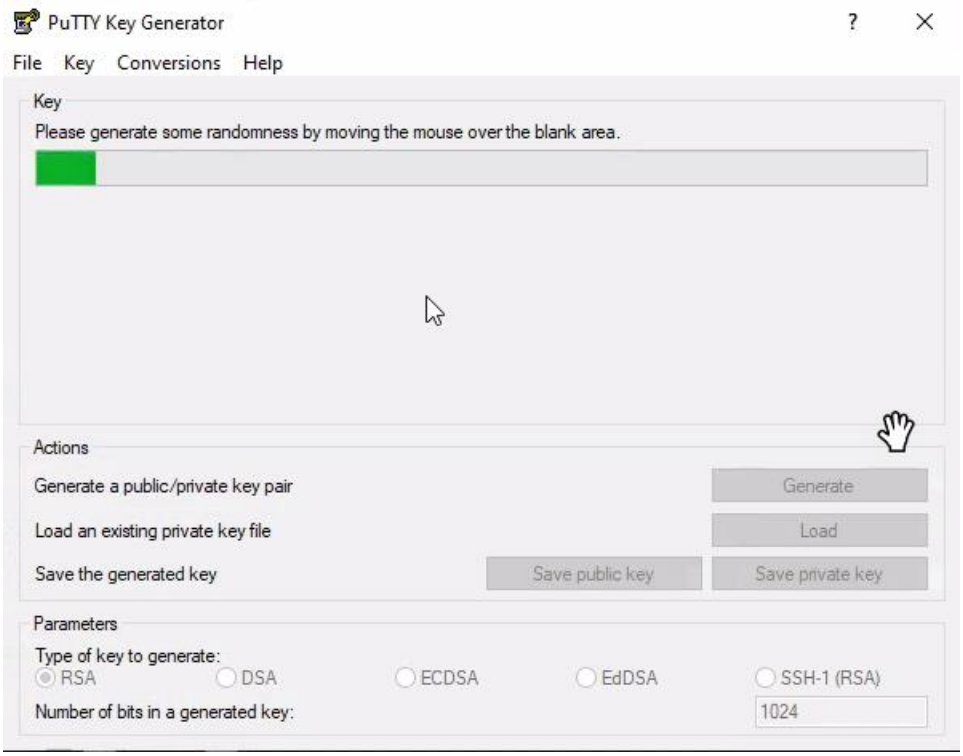
3. Click on Generate



4. From the next warning screen, click 'OK'

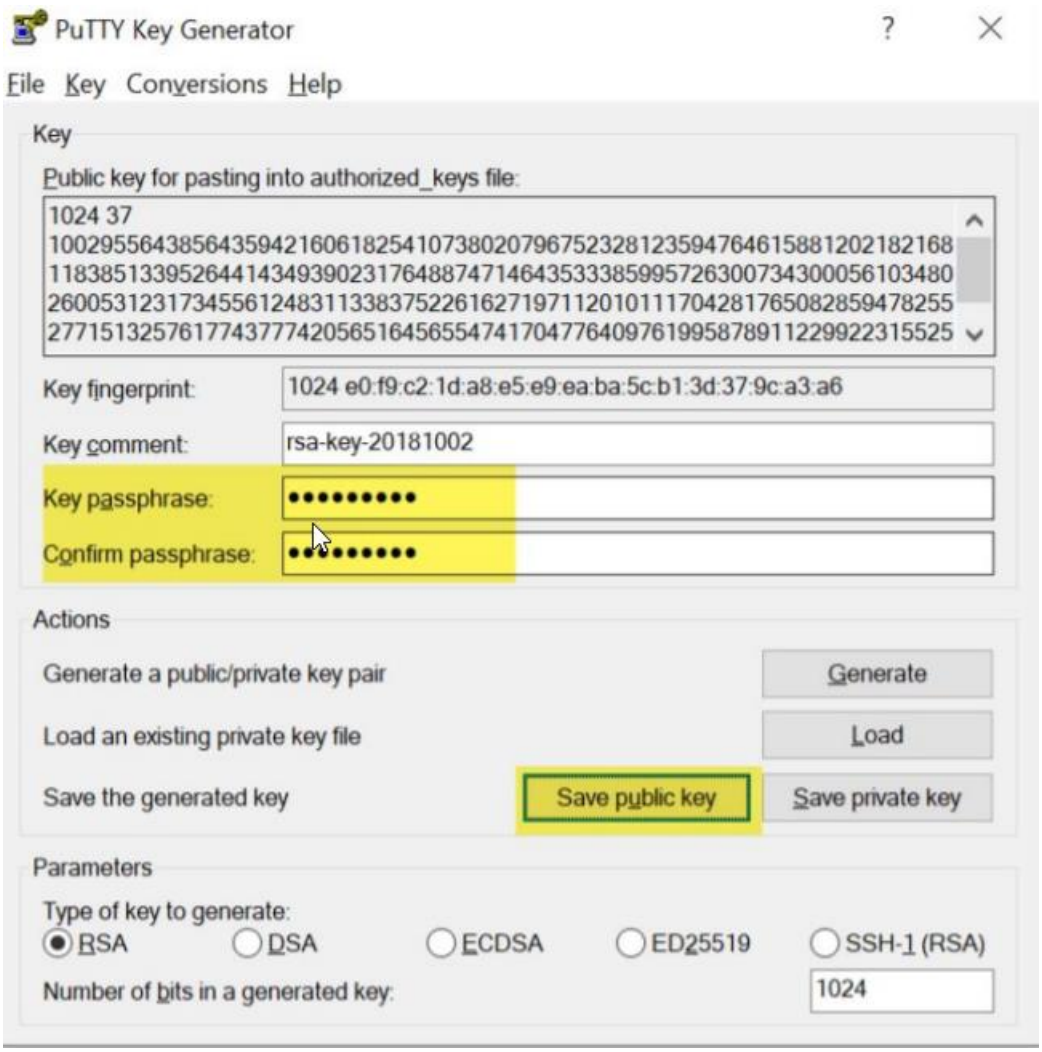


5. Keep moving the mouse over the blank space to generate the key faster (this makes a huge difference!)



6. Once generated, you will get an option to create a passphrase (i.e. password) . Create a passphrase and save the public key using 'Save public key'. Name the file “public_key.key”

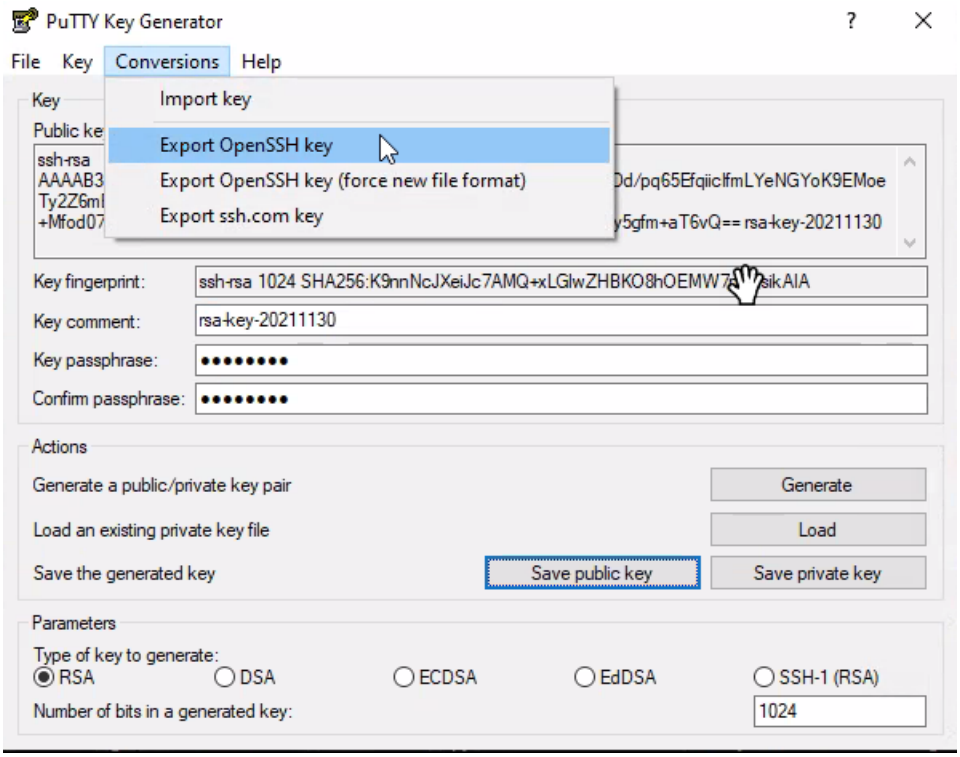
Please advise the contact the password will be used in the validation process and troubleshooting.



Select Save private key, and save it in desktop, this is a .ppk file

The standard Private Key can be used in the future to re-generate the public and SSH key if needed (migration, server loss, upgrades, etc.). The hotels should be advised to keep the private keys and their passwords secure and backed up, and never to send them to us as they should be treated as confidential. We only need the public key

7. Save the private key by going to 'Conversions' > Export Open SSHkey. Do not use the 'Save private key' option, it will not work in Opera.



Name the exported private key “Operaprivatekey.key’.

Checking the key, you can open the Public Key in a text editor and it should look like this:

---- BEGIN SSH2 PUBLIC KEY ----

Comment: "rsa-key-20211201"

AAAAB3NzaC1yc2EAAAADAQABAAAAgQCbLNMvwPlSToqTVCqNlqDJeyRodY0y6pXB

lV0rCq+Vdv3joX1k8MrIpeMrR4eMfWVa6h182XKzGTJEXrOKZIL6GP/lr/N+hahb

UveMmvvwruoR8ScZS1yeD4wmp9f2XpDtvMQDQ/Y+UW13OKyOTI0pYvtgXbfBRsgA

aRtEQ6UgCw==

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

8. Send this Public key to your email, and save it in a zip file

Create a ticket in Zendesk requesting **Whitelisting for SFTP and Account creation**, mention the Public IP and attach the Public Key zip file. Please consider turnaround time from 3-5 days.

*Emphasize in the Zendesk ticket that this request is for CM data sync reports *

Include in the Zendesk ticket "Please configure the file path for the reports"

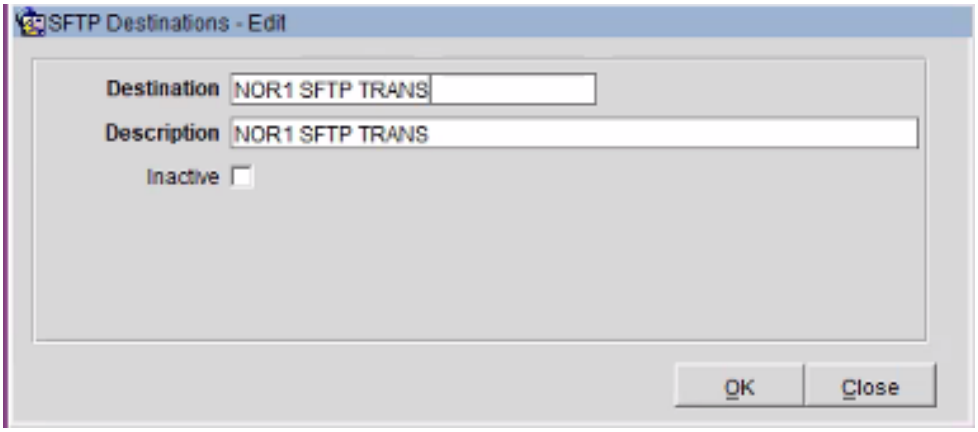
Note: The Public IP for SFTP needs to be of the application server . In most cases it will be the same IP(s) as their OXI server.

Note: Their public IP for SFTP needs to be of the application server. In most cases it will be the same IP(s) as their OXI server.

Configuring SFTP in OPERA

Access Opera Configuration > Property > Delivery Method > General > Click on ‘SFTP’ tab.

2. Click on the ‘NEW’ and configure the SFTP Destination as follows:

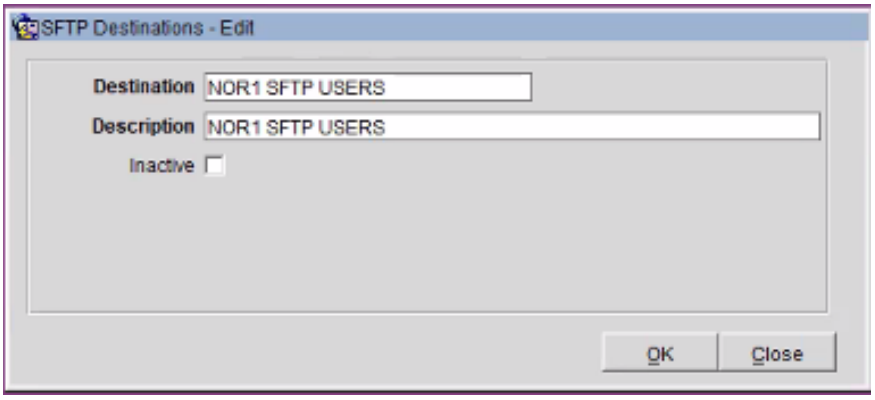


Destination: NOR1 SFTP TRANS

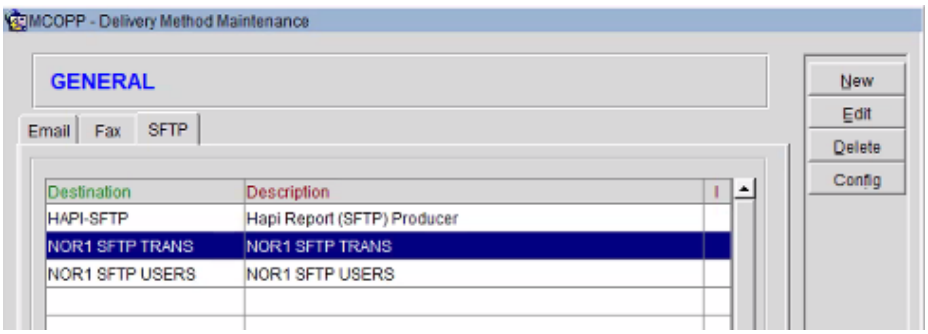
Description: NOR1 SFTP TRANS

Click ‘OK’ when Finished

Repeat the steps for User Activity Log with Destination and Description as NOR1 SFTP USERS



From the export Delivery Maintenance screen, click on the 'Config' button:



Configure the screen as follows:

Select the radio button for : SFTP - Public Key Authentication

HOST/URL: extracts.nor1.com

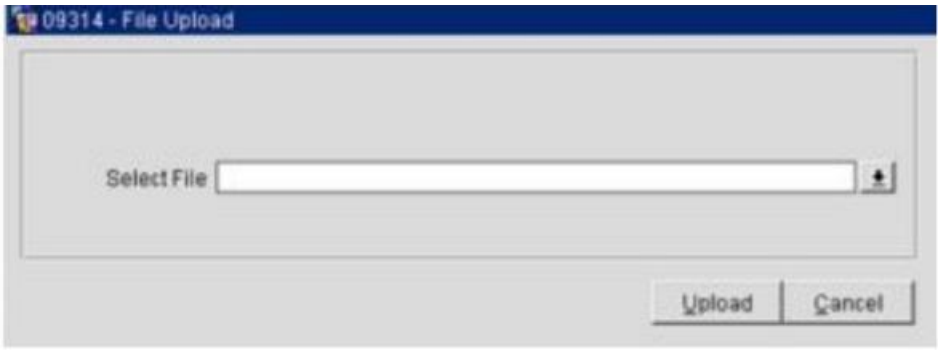
User ID: osr._ Nor1 will provide once you've sent them the Public Key and the Public IP Address (example: "osr.ihg")

Target Directory:

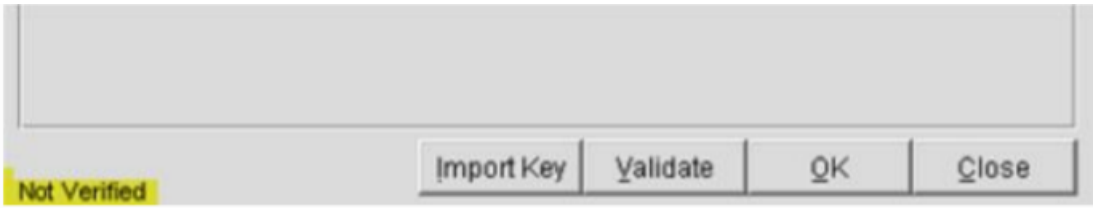
/transactions	for Nor1 5am, Nor1 10pm and Nor1 Recovery
/users	for User Activity Log

Private Key Password: Enter the passphrase/password entered when Private Key was created*

Next import the key by clicking on the ‘Import Key’ button. Upload the Private Key (named Opera*private_key.key*).



After the private key has been uploaded, the Export File Delivery configuration screen will show the key as ‘Not Verified’:



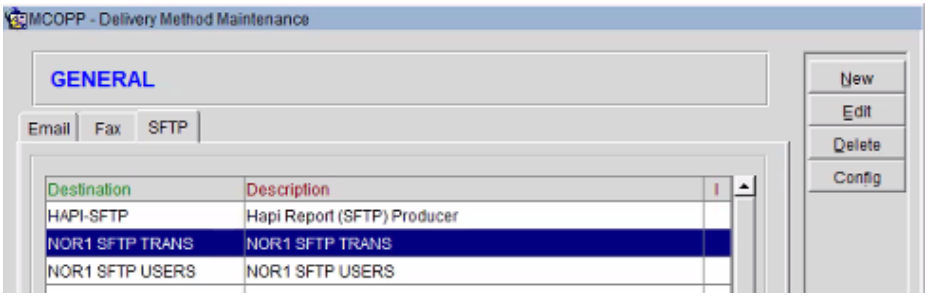
Repeat steps 4-6 for NOR1 SFTP USER.

Use the same passphrase and private key generated earlier.

Second call

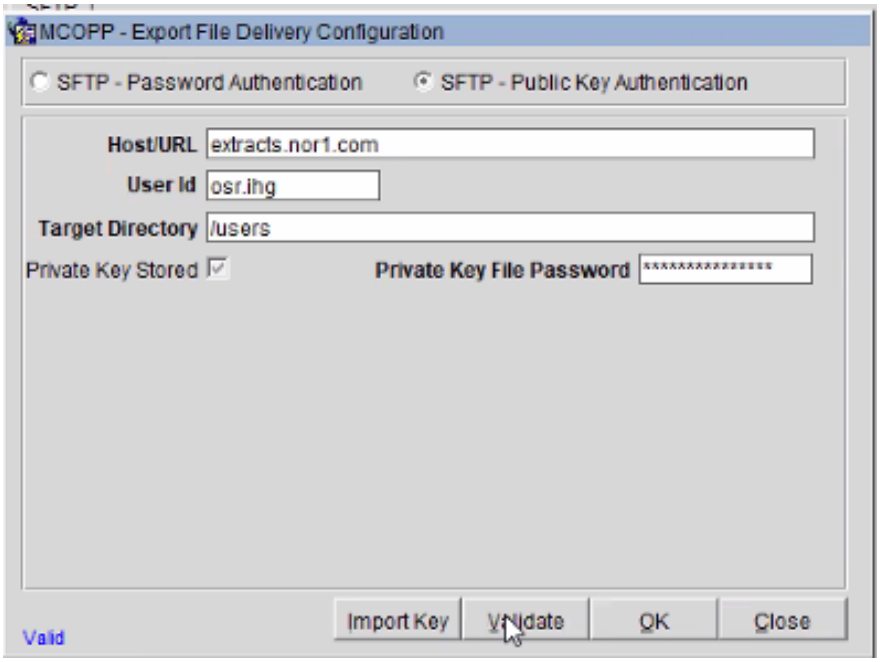
Access Opera Configuration > Property > Delivery Method > General > Click on ‘SFTP’ tab

From the export Delivery Maintenance screen, click on the ‘Config’ button:



After the private key has been uploaded, the Export File Delivery configuration screen will show the key as ‘Not Verified’:

Once Nor1 has whitelisted for the SFTP the IP address and Public/Private Key; verify the key by clicking on the ‘Validate’ button, Opera will check to ensure a connection can be made to NOR1. Upon successful validation, the key will change to Valid



Set up the OSR reports as usual.

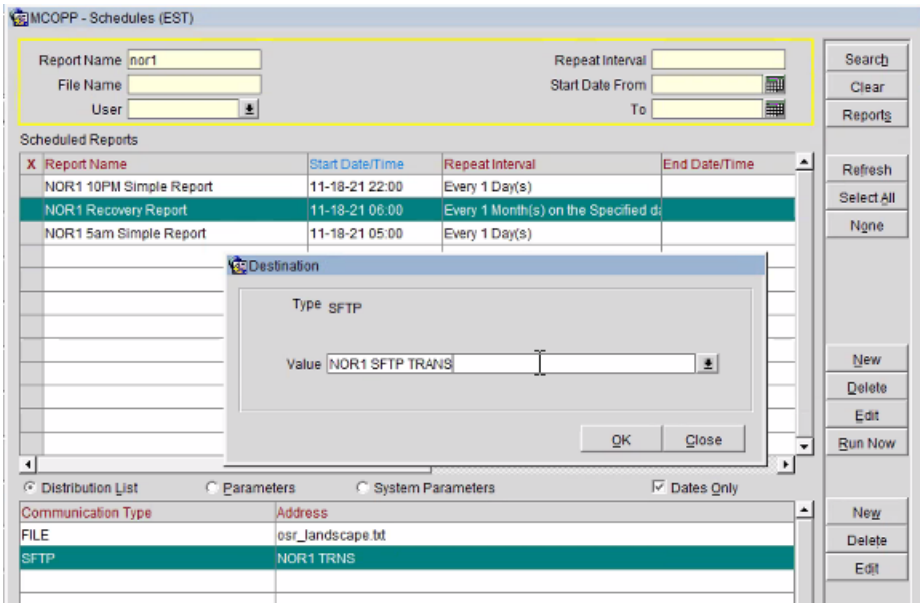
Schedule the report Opera > PMS > Miscellaneous > Reports Scheduler

- Nor1 5am/10pm/Recovery: send to Nor1 SFTP in Delimited Data Tab format
- User Activity Log: sent to Nor1 User SFTP in Delimited Tab format

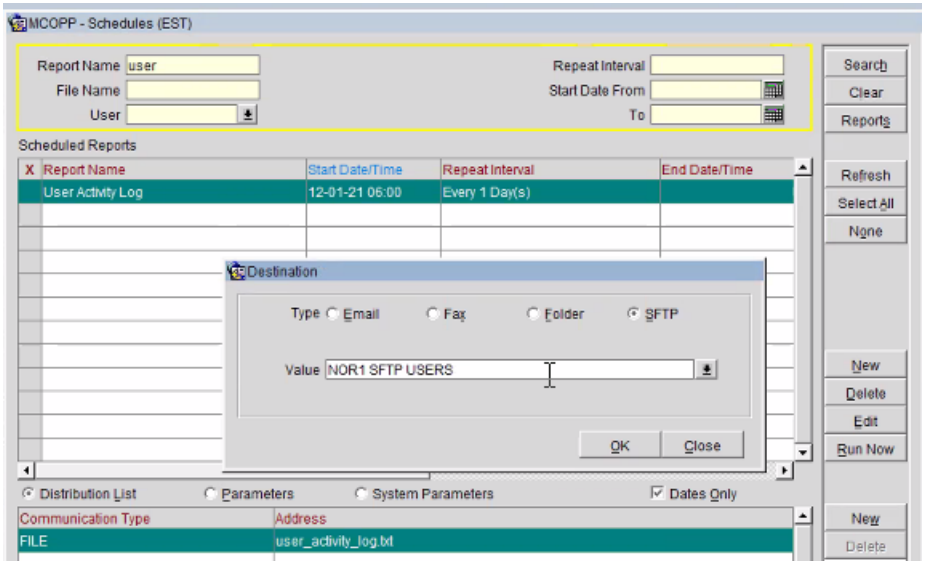
For the schedule, please select in the Distribution list:

Destination: SFTP

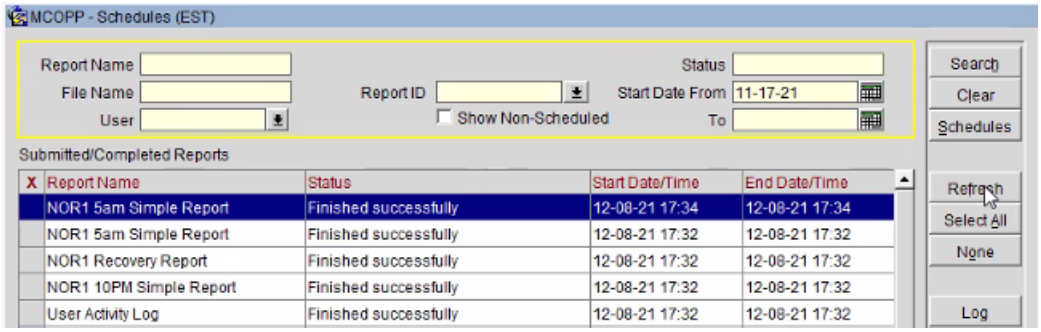
Select “NOR1 SFTP TRANS” for Nor1 5am, Nor1 10pm and Recovery Report



Select “NOR1 SFTP USERS” for User activity log



Select each report and **Run Now,** click on Reports to confirm the status as Successful



For whitelisting extracts.nor1.com on the hotel side

- 3.212.135.224
- 34.231.219.100
- They need to ensure they are allowing outbound traffic to those 2 IPs over port 22.