**Standard Operating Process**

**(SOP) for**

**Wipro Tech Transition\_Unix\_Linux\_Add SSH Key\_v1.2.docx**

**Prepared By**

****

**Jitendra Kumar Singh, Wipro Technologies**

# 

# 1. Contents

[**1.**](https://wipro365-my.sharepoint.com/l) Introduction **3**

[**2.**](https://wipro365-my.sharepoint.com/l) Purpose **3**

[**3.**](https://wipro365-my.sharepoint.com/l) Scope **3**

[**4.**](https://wipro365-my.sharepoint.com/l) Responsibilities **3**

[**5.**](https://wipro365-my.sharepoint.com/l) Summary **3**

[**6.**](https://wipro365-my.sharepoint.com/l) Procedure **3**

[**7.**](https://wipro365-my.sharepoint.com/l) Verify Requested Configuration **4**

[**8.**](https://wipro365-my.sharepoint.com/l) About SSH KEYS **4**

[**9.**](https://wipro365-my.sharepoint.com/l) Create the RSA Key Pair **4**

[**10.**](https://wipro365-my.sharepoint.com/l) Copy the RSA-Public Key Pair Client Machine **5**

[**11.**](https://wipro365-my.sharepoint.com/l) Close Server Request Form **5**

[**12.**](https://wipro365-my.sharepoint.com/l) Close Help Desk Case **5**

[**13.**](https://wipro365-my.sharepoint.com/l) Communicate handoff to customer **5**

# Document Details

|  |  |
| --- | --- |
| Project Name | Wipro Tech Transition\_Unix\_Linux\_Add SSH Key\_v1.2.docx |
| Account |  |
| Current Version | 1.0.0 |
| List of Contributors | Linux |
| Document Name/ID | Unix\_Linux\_Add SSH Key\_v1.2.docx |

# Revision History

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Version | Date of Revision | Next Review Date | Description | Author  (Wipro) | Reviewed By (Wipro) | Approved By  (XXXXXX) |
| 1.0.0 | 22-March-2023 | 22-March-2023 | Unix\_Linux\_Add SSH Key\_v1.2.docx | Jitendra Kumar Singh |  |  |

**Introduction**

Setting up SSH Keys to New Servers (both physical and virtual) is required at Wipro as a standard SA task.

**Purpose**

The purpose of this document is to describe the procedures that are required to Add SSH keys for new servers within Wipro, whether physical or virtual.

**Scope**

This document encompasses all of the activities that a systems admin must complete for Add SSH Keys new servers and turning them over to the application owners.

**Responsibilities**

The Systems Administrator performs the Activity.

**Summary**

The main activities in the document are described on Section 2 Procedure.

Section 3 Handling of exceptions, describe how to perform special activities like the handling of incidents and troubleshooting where required.

**Procedure**

Setting up a new Unix Server and passing it off to the customer requires the following steps:

**Verify Requested Configuration**

1. New client Server Information(IPAddress,Hostname,Server Role, Server Owner).
2. User details for which we need to create a RSA key (root,local users).
3. Source Server  to generate the RSA key.

**About SSH KEYS:**

SSH keys provide a more secure way of logging into a virtual private server with SSH than using a password alone. While a password can eventually be cracked with a brute force attack, SSH keys are nearly impossible to decipher by brute force alone. Generating a key pair provides you with two long string of characters: a public and a private key. You can place the public key on any server, and then unlock it by connecting to it with a client that already has the private key. When the two match up, the system unlocks without the need for a password. You can increase security even more by protecting the private key with a passphrase.

**Create the RSA Key Pair**

All The first step is to create the key pair on the Source machine.

1. Login as user(test) to the client host
2. Run the command , to generate a RSA key   
   #ssh-keygen –t rsa
3. Once the command executed , you will get a few Questions like to save the file in which location, enter the passphrase. If you want we can set else we can leave Empty so it will take default value.

Enter file in which to save the key (/home/test/.ssh/id\_rsa):  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:

1. The Entire key generation process Looks like below:

**Copy the RSA-Public Key Pair Client Machine**

Once the key pair is generated, it's time to place the public key on the client server that we want to use.

we can copy the public key into the new machine's authorized\_keys file with the ssh-copy-id command.

1. Run the command from the source host to copy the RSA-Public key to client host

# ssh-copy-id [test@192.168.56.20](mailto:test@192.168.56.20)

2. The Entire copy key process as follows

Now we can go ahead and log into [test@192.168.56.20](mailto:test@192.168.56.20)  and it will not be prompted for a password. However, if we set a passphrase, it will be asked to enter the passphrase at that time (and whenever else you log in in the future).

**Close Server Request Form**

**Close Help Desk Case**

**Communicate handoff to customer.**