MANAGING YOUR ACTOR'S SSH KEYS

After adding an appliance Actor, you can manage your Actor's SSH keys in the Actions menu.

TO MANAGE AUTHORIZED SSH KEYS

1. Click **Environment** > **Actors**.
2. In the Network Actors table, locate the Actor you want to configure, open its Action menu, and click **Manage credentials**.
3. To check the status of the SSH protocol, click **Check SSH Status**. The status displays in a card at the top of the page.
4. To enable or disable SSH, click the appropriate button. A card displays to show the status and the SSH Status field updates.
5. To view the authorized keys, click **Refresh Authorized Keys**. The system displays any authorized keys.
    - To update the authorized SSH Keys:
        a. Click **Refresh Authorized Keys** to display existing keys.
        b. Add your ssh id_rsa key(s) to the text box.

(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629cf4263b2606144059e0a3/n/set-authorized-ssh-keys.png)

Setting authorized SSH keys

        c. Click **Set Authorized SSH Keys**.

    - To set an SSH Password, select **Enabled for SSH Password Auth**.
        a. Enter and Confirm the Login Password.
        b. Click **Set Password Authentication**.

    - To disable Password Authentication for SSH Keys:
        a. Change SSH Password Auth to Disabled.
        b. Click **Set Password Authentication**.