



UNIX shutdown action on securityProbe

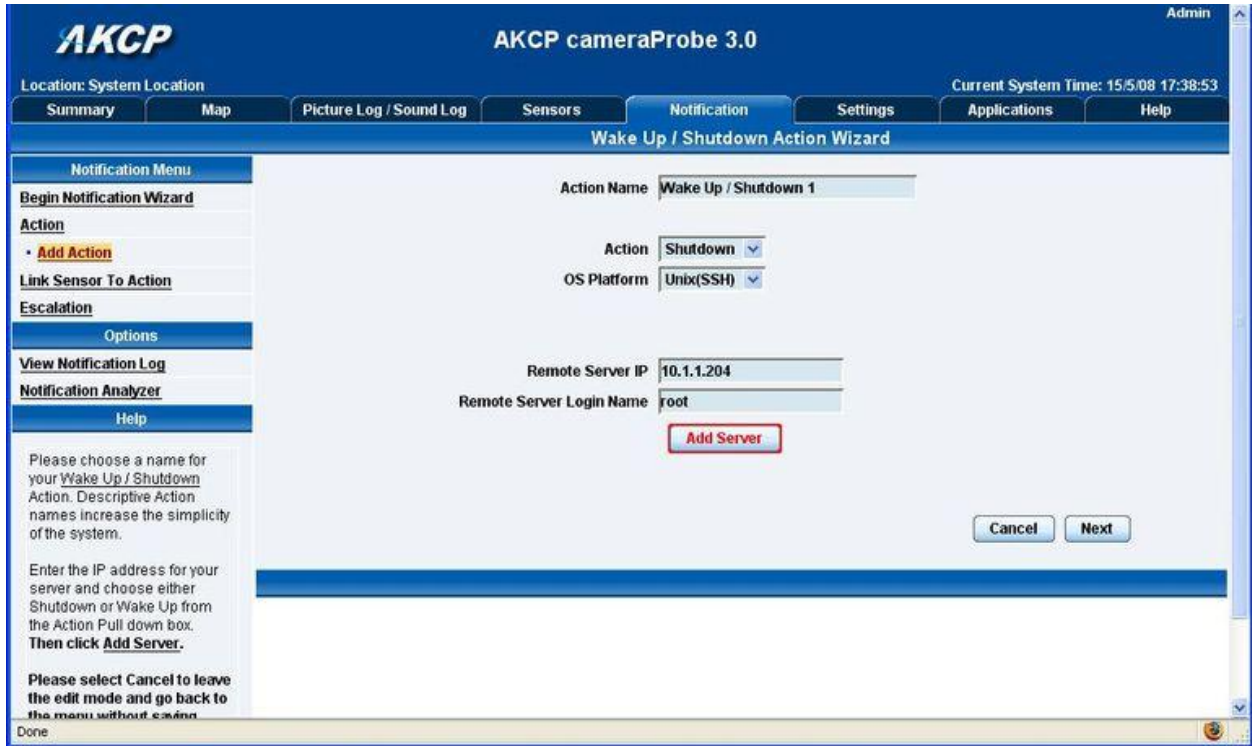
Setup of UNIX shutdown action and notification

The screenshot shows the AKCP cameraProbe 3.0 web interface. The top navigation bar includes 'Summary', 'Map', 'Picture Log / Sound Log', 'Sensors', 'Notification', 'Settings', 'Applications', and 'Help'. The 'Notification' tab is active, and the 'Wake Up / Shutdown Action Wizard' is displayed. The left sidebar contains a 'Notification Menu' with options like 'Begin Notification Wizard', 'Action', 'Add Action', 'Link Sensor To Action', 'Escalation', 'Options', 'View Notification Log', 'Notification Analyzer', and 'Help'. The main configuration area has the following fields:

- Action Name: Wake Up / Shutdown 1
- Action: Shutdown
- OS Platform: Windows
- Remote Server IP: 192.168.0.XXX
- Remote Server Login Name: User
- Remote Server Password: (empty)
- Confirm Remote Server Password: (empty)

Buttons include 'Add Server', 'Cancel', and 'Next'. A 'Done' status is visible at the bottom left.

1. Create new Action
 - Select the "Notifications" page, then "Add Action" from the left panel
 - You can rename the action in the "Action Name" box



AKCP Admin
AKCP cameraProbe 3.0
 Location: System Location Current System Time: 15/5/08 17:38:53
 Summary | Map | Picture Log / Sound Log | Sensors | **Notification** | Settings | Applications | Help

Wake Up / Shutdown Action Wizard

Notification Menu

Begin Notification Wizard

Action

- **Add Action**

Link Sensor To Action

Escalation

Options

View Notification Log

Notification Analyzer

Help

Please choose a name for your Wake Up / Shutdown Action. Descriptive Action names increase the simplicity of the system.

Enter the IP address for your server and choose either Shutdown or Wake Up from the Action Pull down box. **Then click Add Server.**

Please select Cancel to leave the edit mode and go back to the menu without saving.

Done

Action Name

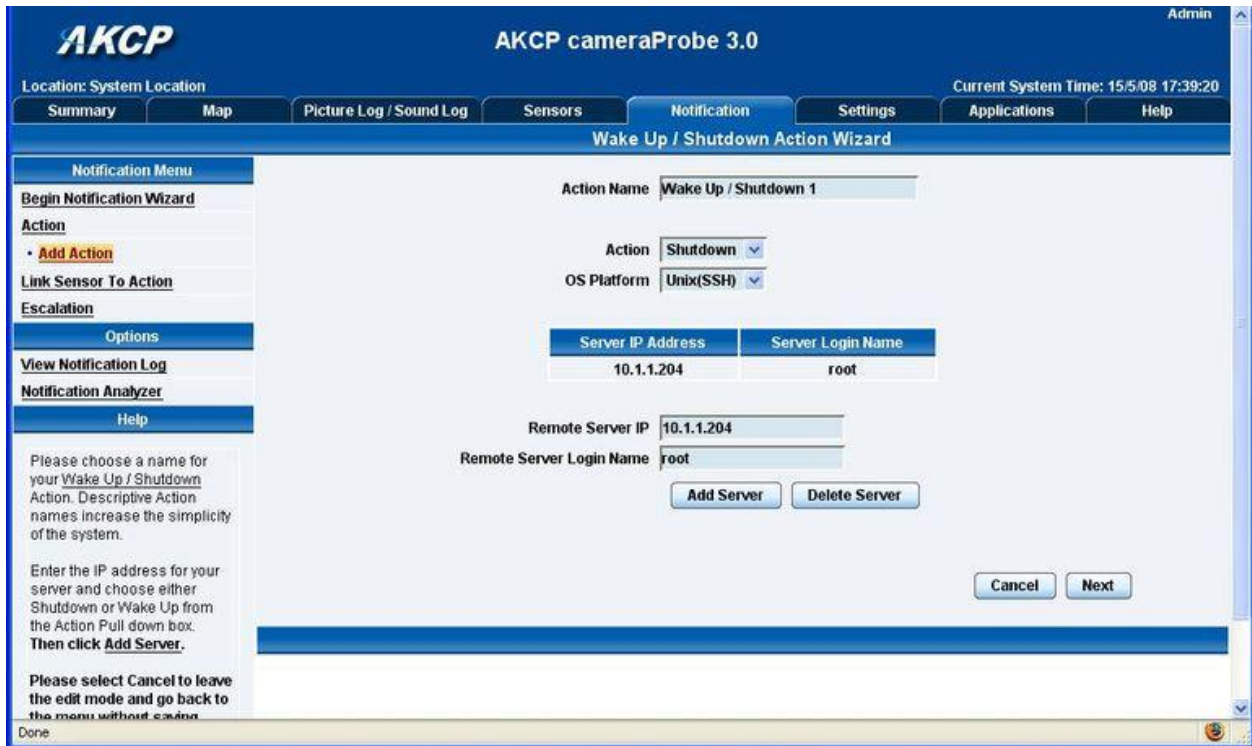
Action

OS Platform

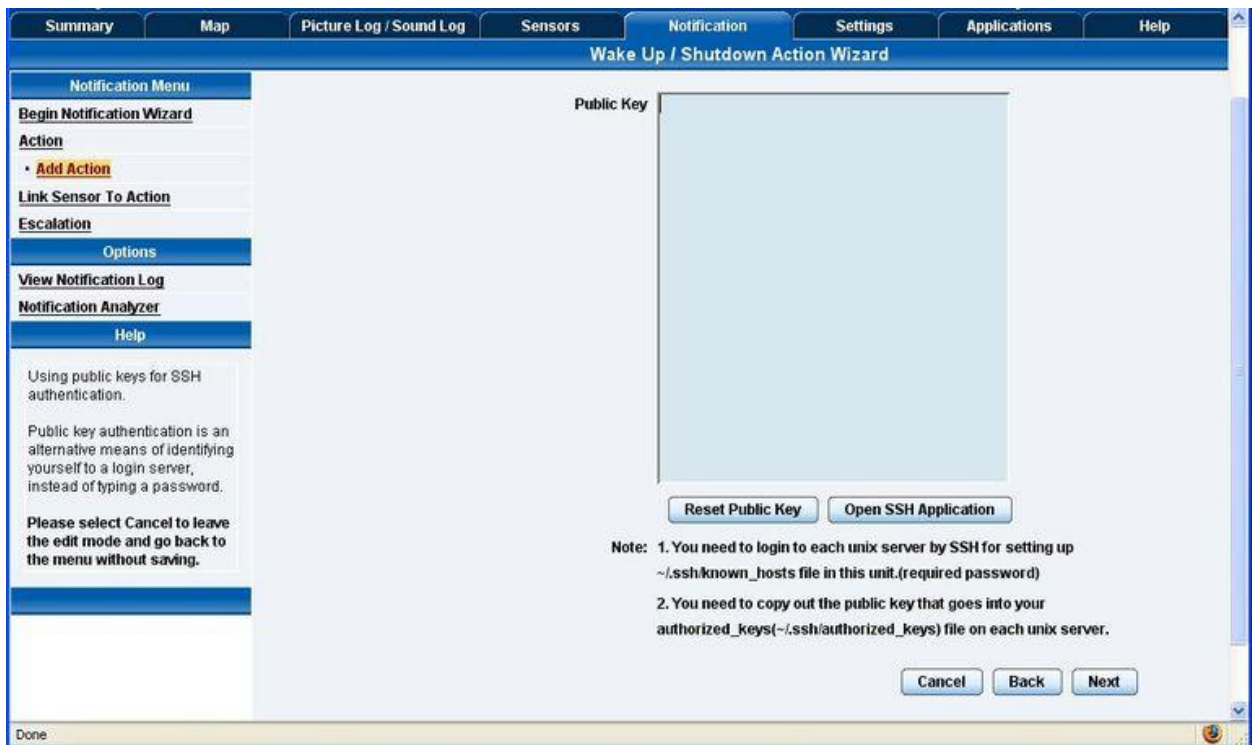
Remote Server IP

Remote Server Login Name

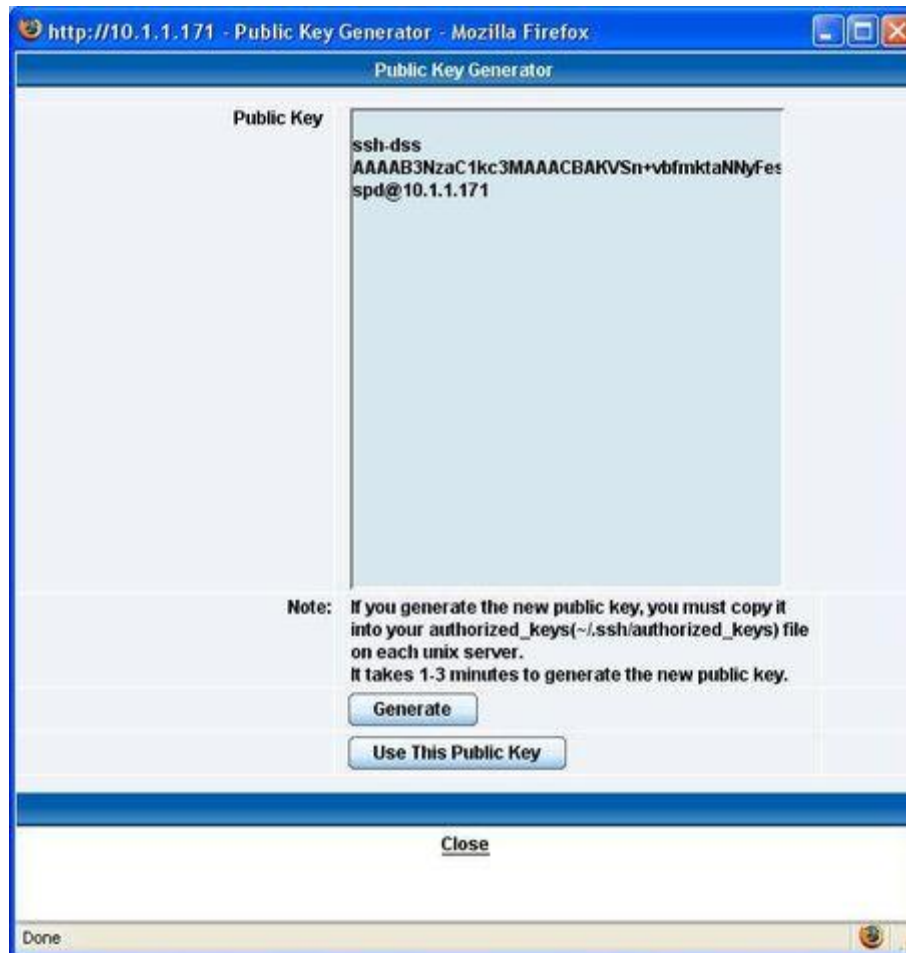
2. Select "Shutdown" from the "Action" drop down menu,
3. Select "UNIX (SSH)" from the "OS Platform" drop down menu
4. Input your servers IP address into the "Remote Server IP" box
5. Input your log in username into the "Remote Server Login Name" box



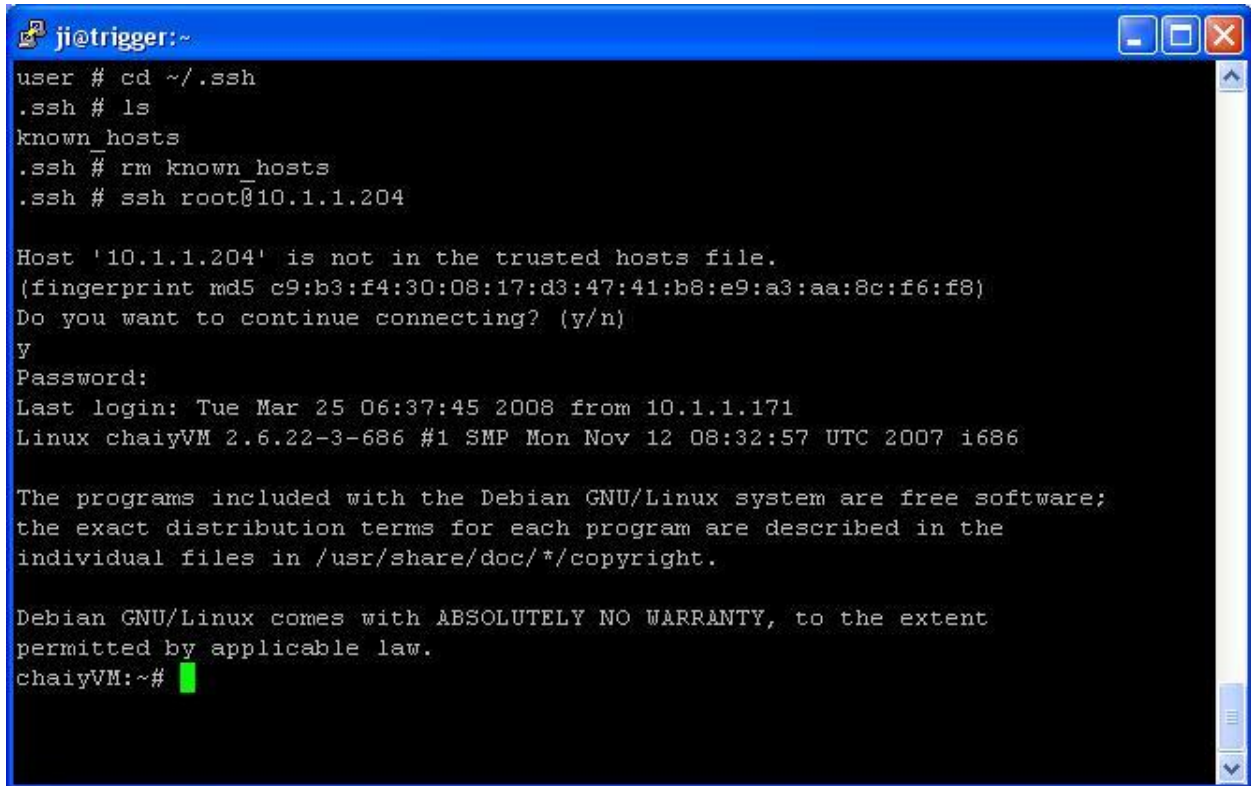
6. Click on "Add Server". Add additional IP's if needed. Click "Next"



7. Click "Reset Public Key" (If you already have a Public Key, skip this step and proceed to step number 11 below)



8. After clicking "Reset Public Key" a new Window will then pop up, press "Generate"
9. The unit will now generate a new public key. It will normally take approximately 1 to 3 minutes for the system to generate the new public key, so please be patient
10. After the public key has been generated, press "Use This Public Key"

A screenshot of a terminal window titled 'ji@trigger:~'. The terminal shows a sequence of commands and their outputs. The user navigates to the '~/.ssh' directory, lists files, and removes the 'known_hosts' file. Then, they attempt to SSH to 'root@10.1.1.204'. The terminal displays a warning that the host is not in the trusted hosts file, shows the fingerprint, and asks for confirmation to continue. The user responds 'y', and the terminal shows the password prompt and the login banner for a Debian GNU/Linux system. The prompt changes to 'chaivyVM:~#'.

```
ji@trigger:~  
user # cd ~/.ssh  
.ssh # ls  
known_hosts  
.ssh # rm known_hosts  
.ssh # ssh root@10.1.1.204  
  
Host '10.1.1.204' is not in the trusted hosts file.  
(fingerprint md5 c9:b3:f4:30:08:17:d3:47:41:b8:e9:a3:aa:8c:f6:f8)  
Do you want to continue connecting? (y/n)  
y  
Password:  
Last login: Tue Mar 25 06:37:45 2008 from 10.1.1.171  
Linux chaivyVM 2.6.22-3-686 #1 SMP Mon Nov 12 08:32:57 UTC 2007 i686  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
chaivyVM:~#
```

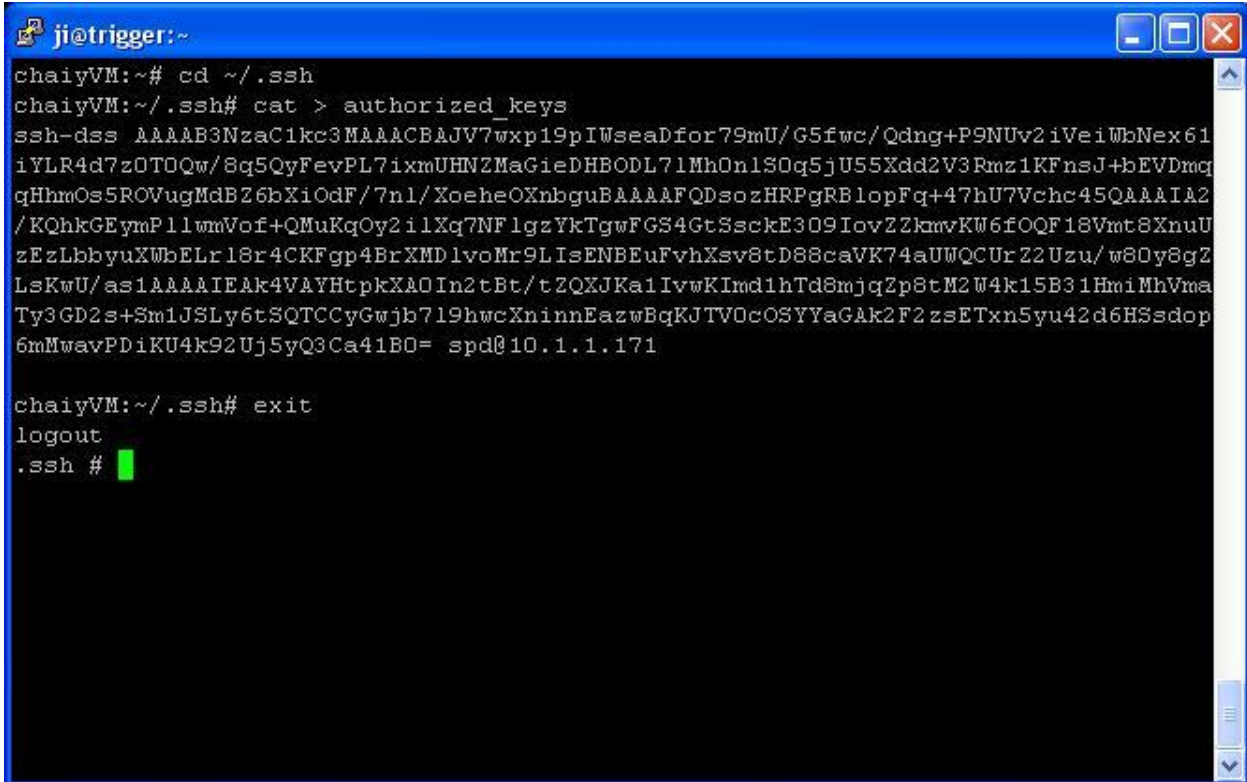
11. Open a Telnet or SSH session to the unit

```
cd ~/.ssh  
ls  
rm known_hosts
```

12. Make sure to delete the know_hosts file to ensure generate a new list of hosts when using this command shown above

```
ssh <user>@<IP>  
When  
<user> is User name in server  
<IP> is IP address of server
```

13. Then connect to the server by using this command shown above



```

jj@trigger:~
chaivyVM:~# cd ~/.ssh
chaivyVM:~/.ssh# cat > authorized_keys
ssh-dss AAAAB3NzaC1kc3MAAACBAJV7w_xp19pIWseaDfor79mU/G5fwc/Qdng+P9NUv2iVeiWbNex61
iYLR4d7zOT0Qw/8q5QyFevPL7ixmUHNZMaGieDHBODL71MhOn1S0q5jU55Xdd2V3Rmz1KFnsJ+bEVDmq
qHhmOs5ROVugMdBZ6bXiOdF/7n1/XoeheOXnbguBAAAAFQDsozHRPgRBlopFq+47hU7Vchc45QAAAAIA2
/KQhkGEymP1lwmVof+QMuKqOy2i1Xq7NF1gzYkTgwFGS4GtSsckE309IovZZkmvKW6fOQF18Vmt8XnuU
zEzLbbyuXWbELr18r4CKFgp4BrXMD1voMr9LIsENBEuFvhXsv8tD88caVK74aUWQCUrZ2Uzu/w80y8gZ
LsKwU/as1AAAAIEAk4VAYHtpkXADIn2tBt/tZQXJKa1IvwKImd1hTd8mjgZp8tM2W4k15B31HmiMhVma
Ty3GD2s+Sm1JSLy6tSQTCCyGwjb719hwcXninnEazwBqKJTV0cOSYYaGak2F2zsETxn5yu42d6HSsdop
6mMwavPDiKU4k92Uj5yQ3Ca41B0= spd@10.1.1.171

chaivyVM:~/.ssh# exit
logout
.ssh # █

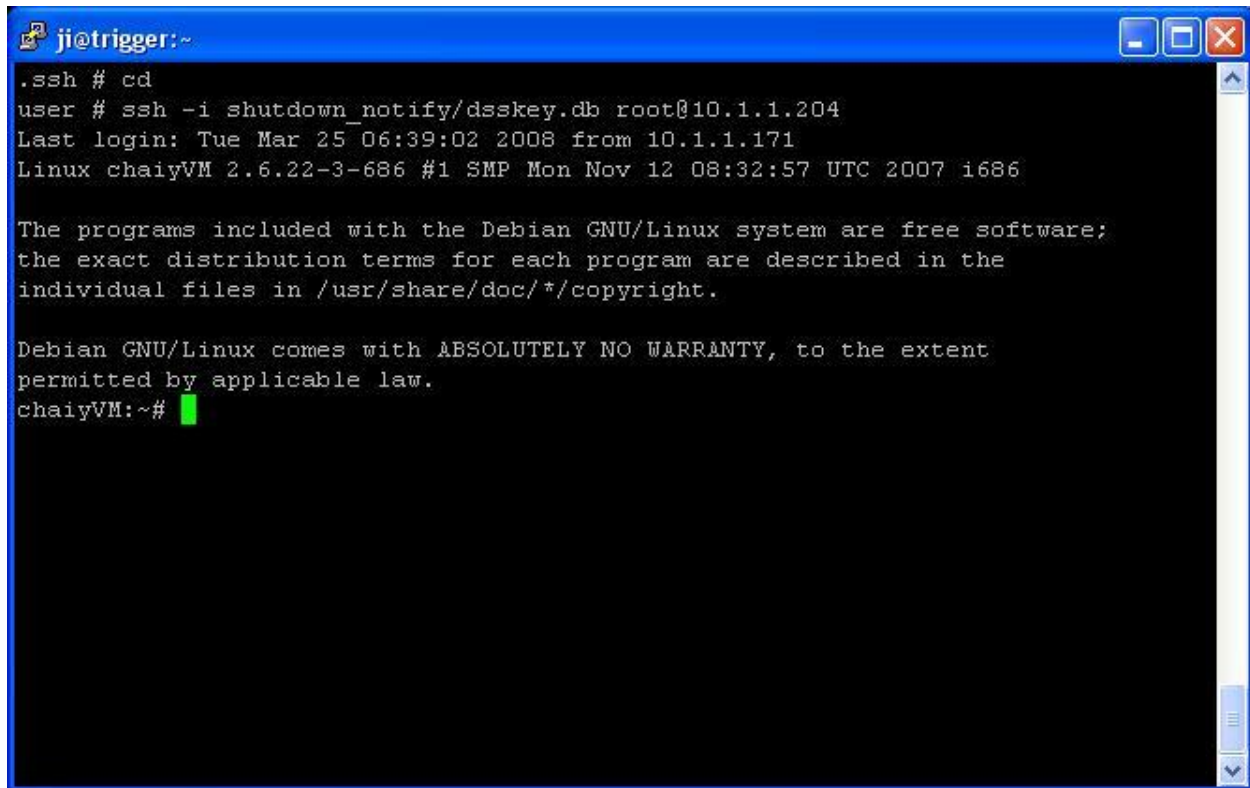
```

```

cd ~/.ssh
cat > authorized_keys
#copy public key from web interface and press (for putty can press by right click)
#press Enter button and press Ctrl + c for exit cat command

```

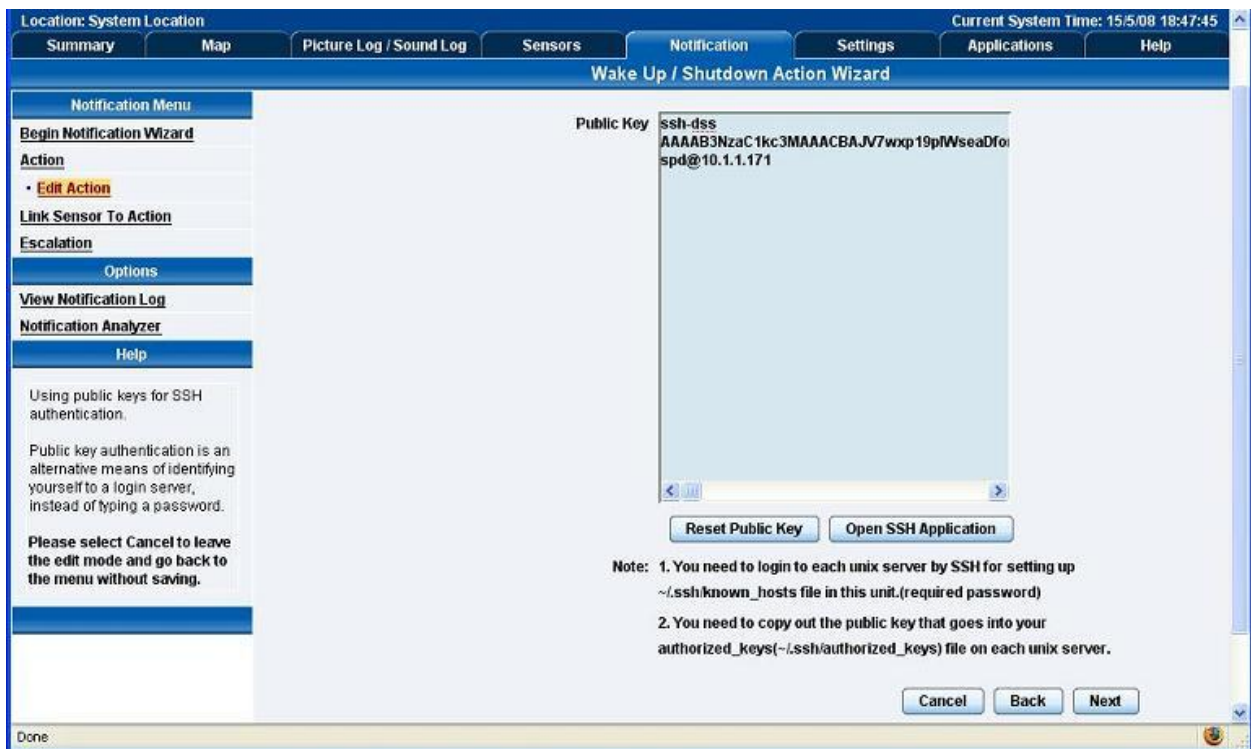
14. After connecting to the server, create an authorized_keys file by using this command shown above
15. Then disconnect from the server and connect to the unit



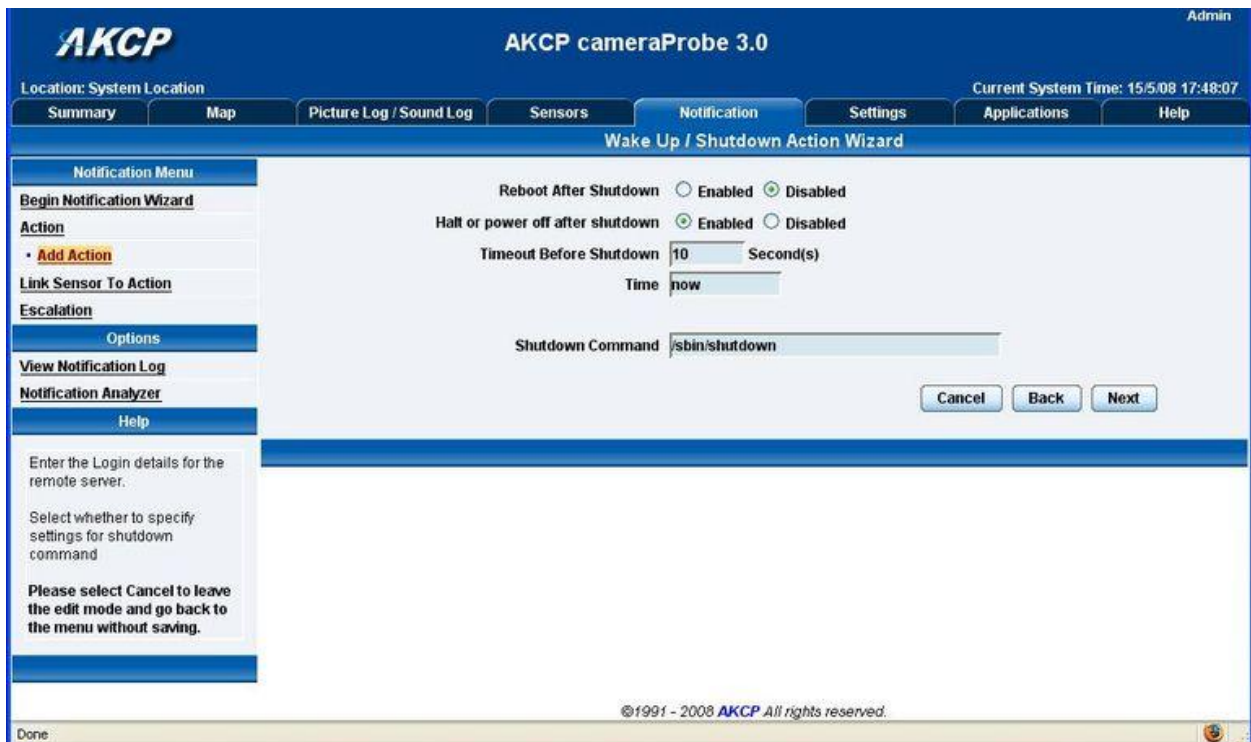
```
jj@trigger:~  
.  
ssh # cd  
user # ssh -i shutdown_notify/dsskey.db root@10.1.1.204  
Last login: Tue Mar 25 06:39:02 2008 from 10.1.1.171  
Linux chaivm 2.6.22-3-686 #1 SMP Mon Nov 12 08:32:57 UTC 2007 i686  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
chaivm:~#
```

```
ssh -I /flash1/user/shutdown_notify/dsskey.db <user>@<IP>  
When  
<user> is User name in server  
<IP> is IP address of server
```

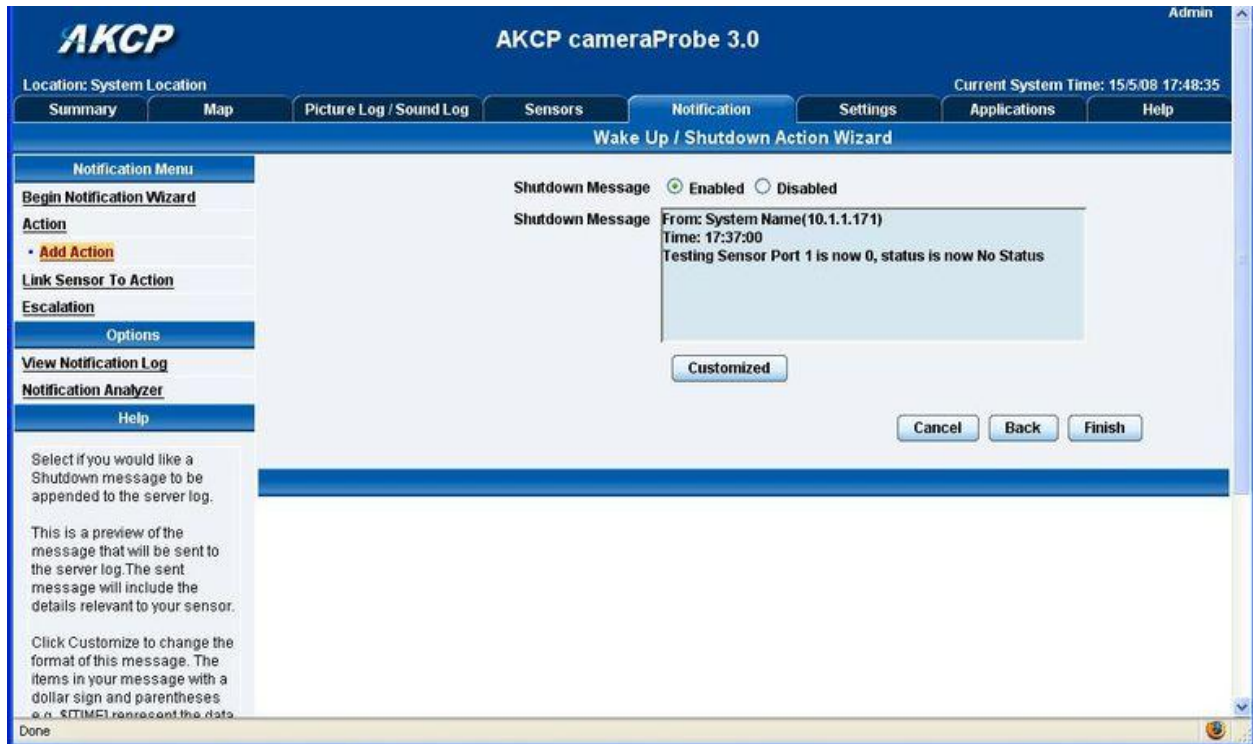
16. Now test the public key by using this command shown above



17. Return to the units web interface and click "Next"



18. You can now set the other settings in the Shutdown action and click "Next"



19. You can also enable a shutdown message to be sent by first choosing "Enabled", then entering your message in the "Shutdown Message" box, then clicking "Finish"