

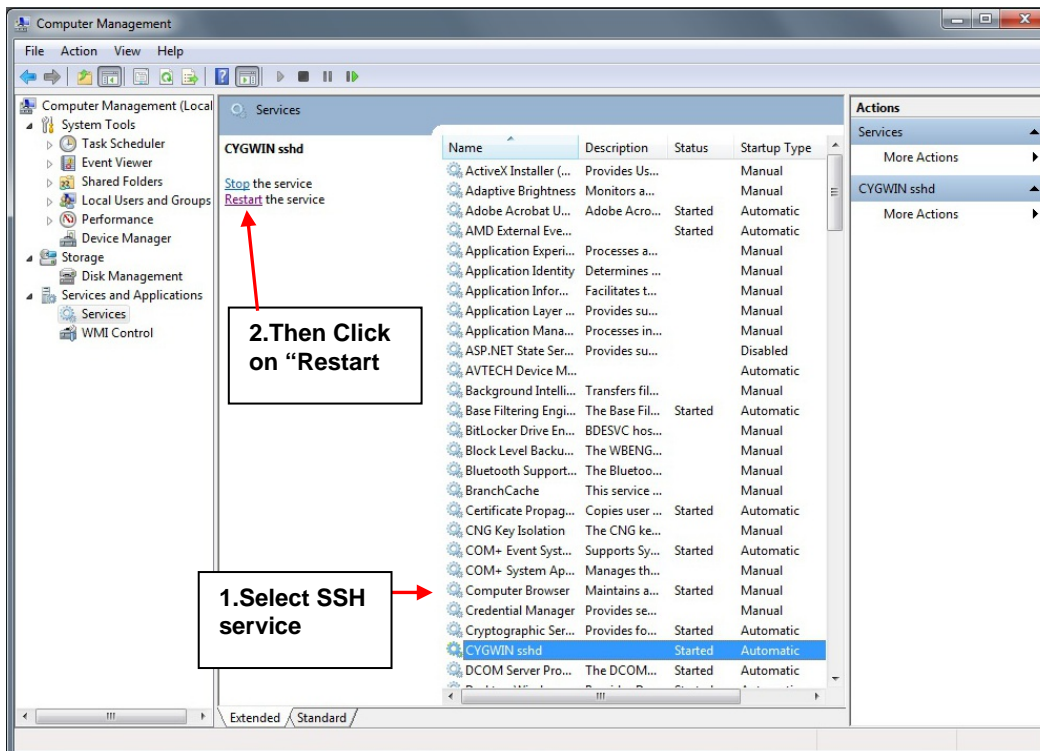
## SHUTDOWN WINDOWS SERVER USING REMOTE SSH COMMAND

Following the steps outlined below, a Windows server can be shutdown automatically by the ENVIROMUX SYSTEM. The E-xD can be used to shutdown any machines with SSH access including VMWare ESXi Host and Microsoft HyperV machines (see page 7).

### Cygwin Method

1. Setup a user account on the Windows PC named "root" (must be all lower case) and make sure user "root" has administrative privileges.
2. Install an SSH server on the Windows PC. (We used Cygwin for our test. We found instruction on Oracle for installation that was very helpful [http://docs.oracle.com/cd/E24628\\_01/install.121/e22624/preinstall\\_req\\_cygwin\\_ssh.htm](http://docs.oracle.com/cd/E24628_01/install.121/e22624/preinstall_req_cygwin_ssh.htm)).
3. Setup a user account in your SSH server named "root".
4. Check to make sure the SSH configuration file has RSA authorization enabled and if not, edit the SSH server configuration file to enable it (in cygwin the file was found at `c:\cygwin64\etc\sshd_config`). Other SSH servers might have different configuration filenames.
5. Download the RSA Public Key to the Windows computer. The downloaded file will have the default name `id_rsa.pub`.
6. Create a directory in the SSH server directory called `"/home/root/.ssh"` (i.e. `c:/cygwin64/home/root/.ssh` and don't forget to put the period before the "ssh").
7. On the computer to take the command, logged in as root, from the directory where the file was downloaded, type the command:  

```
$ cat id_rsa.pub >> /home/root/.ssh/authorized_keys
```
8. Then, to make the change take effect, restart the SSH server. To do this, **right** click on "Computer" (in the Start Menu) and click on "Manage". Locate the SSH server in the list of Services and select it. Then click on "Restart".



Restart CYGWIN service

9. Configure a Smart Alert to include an Event that will be used to trigger the shutdown of the Windows Server.

10. Within the Event configuration, apply the address of the Windows Server as the "Remote Address", place a checkmark in "Enable command on event triggered" and add a command to be executed as a Remote SSH command under "Command on triggered". (We used "shutdown -s" but there are more possibilities (<http://technet.microsoft.com/en-us/library/cc780360%28v=ws.10%29.aspx>)).

Unit: E-5D-IND TU1 Model: ENVIROMUX-5D  
 Uptime: 32 days, 17 hours, 55 mins  
 Current Time: 06-16-2014 11:25:33 AM

---

Home
Event List
Configure Event

**Monitoring**

**Administration**

**Smart Alerts**

Events

Smart Alerts

**Log**

**Support**

**Logout**

### Event #1 Smoke Detector-1 Configuration

**Event Settings**

**Description**   
Descriptive name for the event

**Trigger Status**   
Select the Digital Input status that will trigger the event

**Event Delay**    
Duration the sensor must be out of thresholds before the event is triggered

**When triggered, acknowledge the following event**

**Group Settings**

**Event Notifications**

**Remote SSH Commands**

**Remote address**   
IP Address or URL of the machine receiving the command

**Enable command on event triggered**   
Enable command when the event is triggered

**Command on triggered**   
Command to be executed when event is triggered

**Enable command on event cleared**   
Enable command when the event returns to normal

**Command on cleared**   
Command to be executed when event returns to normal

### Configure Event for remote shutdown

11. Be sure to click "Save" when finished.

## OPEN SSH Method

1. Setup SSH server on Windows machine with public key access. If this procedure is already done, skip to step 2
  - a. We are using OpenSSH for windows to setup SSH server. Any SSH server compatible for your Windows OS can be used.
  - b. Please install SSH to the location as in below link and execute the commands to setup SSH server and Setting up Public Key Authentication.
    - [https://winscp.net/eng/docs/guide\\_windows\\_openssh\\_server](https://winscp.net/eng/docs/guide_windows_openssh_server)
    - [https://winscp.net/eng/docs/guide\\_public\\_key](https://winscp.net/eng/docs/guide_public_key)
  - c. Make sure you can start the SSH service listed in your windows services list (services.msc application).
  - d. Troubleshooting:

\* During execution of SSH setup commands if you receive syntax error for

`powershell.exe -ExecutionPolicy Bypass -File .\FixHostFilePermissions.ps1 -Confirm:$false`  
 please use the below command instead:

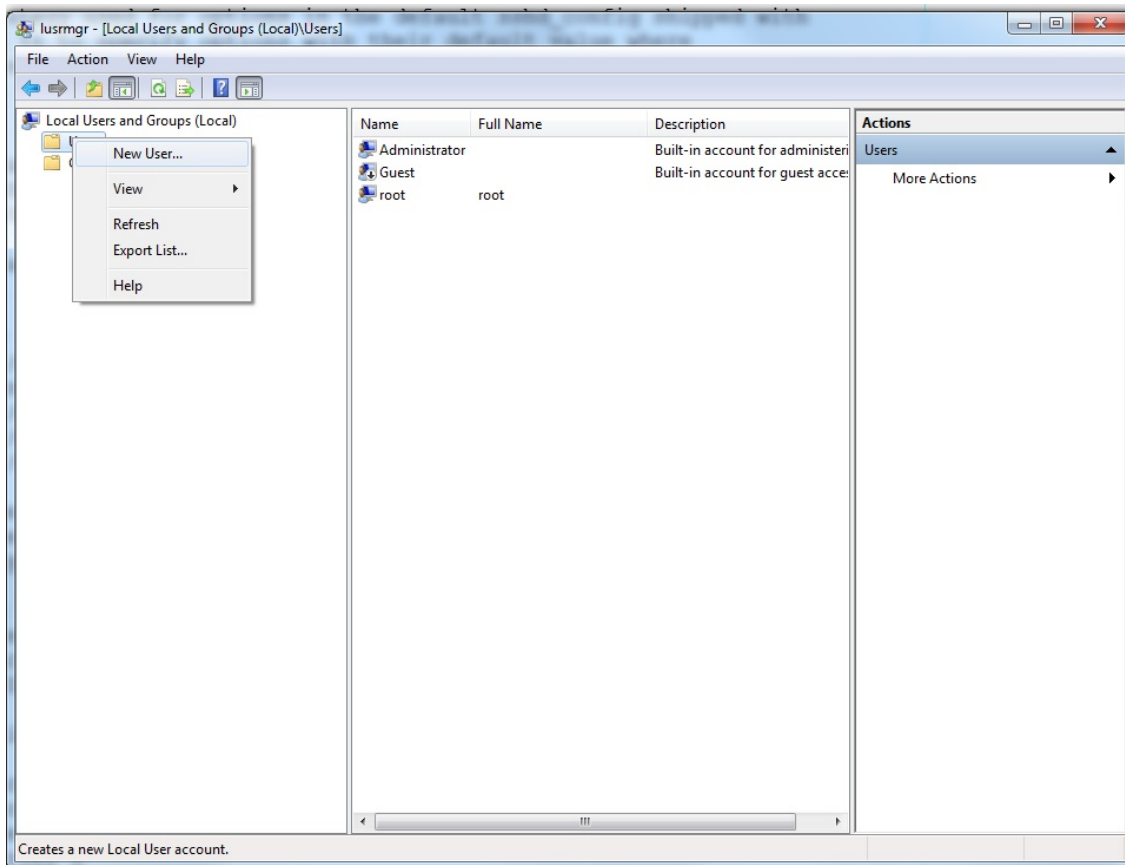
```
powershell.exe -ExecutionPolicy Bypass -File .\FixHostFilePermissions.ps1
```

\* During startup process if you receive error related to a permission issue, please make sure LOCAL SERVICE is added to "Replace a process level token". If not it can be added by opening the application secpol.msc -> Local Policies -> User Rights Assignment -> 'Replace a process level token' as mentioned in below link.

<https://social.technet.microsoft.com/Forums/en-US/419ba006-4413-4036-8c49-252b08593131/service-fails-to-start-error-1297-and-7000?forum=winserverDS>

2. Add E-xD user to Windows SSH service user list.

a. E-xD logs in as user root. If you do not have a 'root' user on the PC add this user by going in to Control Panel -> Manage User Accounts -> 'Advanced' tab -> Advanced -> Right click on User and add New User as shown in root\_user.jpg. User password can be anything you wish as this is not used by the E-xD.



**Add user "root" to PC**

b. Download RSA public key from E-xD as shown below and rename the file to 'authorized\_keys'. Place this file into the following path:

C:\Program files\OpenSSH\ssh\authorized\_keys

The screenshot shows the NTI Network Technologies web interface. At the top left is the NTI logo and 'NETWORK TECHNOLOGIES INCORPORATED'. At the top right, system information is displayed: 'Unit: E-16D-48V Model: ENVIROMUX-16D Uptime: 44 mins Current Time: 07-12-2017 03:14:52 PM'. Below this is a navigation bar with 'Home' and 'System Configuration'. A left sidebar contains a menu with categories: 'Monitoring', 'Administration' (with sub-items: System, Enterprise, Network, Users, Groups, Security, System Information, Firmware, Cascading, Reboot), 'Smart Alerts', 'Log', 'Support', and 'Logout'. The main content area is titled 'System Configuration' and contains several expandable sections: 'Time Settings', 'Configuration Backup & Restore', 'Language', 'USB LCD Display', 'Auxiliary Serial Port Configuration', 'RSA Public Key' (which is expanded to show a 'Download RSA Public Key' button), 'Alert E-mail Format', 'External Sensor Graph', and 'Other Options'. A 'Save' button is located at the bottom of the configuration area. The footer contains the copyright notice '© 2012, 2017 Network Technologies Inc. All rights reserved.' and the 'goahead WEB SERVER' logo.

### Download RSA Public Key

c. The permissions on this file needs to be limited to the user running SSH service. If not please disable Strict Mode in sshd\_config file as shown below. Please make sure the path of public key and pid file is correct and accessible by SSH service.

```
# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

# The default requires explicit activation of protocol 1
#Protocol 2

# HostKey for protocol version 1
#HostKey /etc/ssh/ssh_host_key
# HostKeys for protocol version 2
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key

# Lifetime and size of ephemeral version 1 server key
#KeyRegenerationInterval 1h
#ServerKeyBits 1024

# Logging
# obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
→LogLevel DEBUG3

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
→StrictModes no
#MaxAuthTries 6
#MaxSessions 10

#RSAAuthentication yes
#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile "C:\Program Files\OpenSSH\.ssh\authorized_keys"
PidFile "C:\Program Files\OpenSSH\logs\sshd.pid"
```

Figure 1- sshd\_config file

d. To troubleshoot any errors please set log level to DEBUG3 as shown in the image above.

3. Setup of SSH command on E-xD:

a. To test, try logging into windows machine using any user and password. You can also try testing public key authentication by generating your own SSH key and adding its rsa key to the authorized\_keys file.

b. Any windows commands can be executed on Windows machine through E-xD. To shutdown, add an event with remote SSH command 'shutdown -s' as shown below. Shutdown parameters like timeout can be configured as described in the link below:

<https://technet.microsoft.com/en-us/library/bb491003.aspx>

The screenshot displays the 'test2 Configuration' page in the NTI WebServer interface. The page is divided into several sections:

- Event Settings:** Includes fields for Description (test2), Threshold (100.0), Threshold Type (Greater Than), Event Delay (2 Sec), and When triggered, acknowledge the following event (None).
- Group Settings:** A collapsed section.
- Event Notifications:** A collapsed section.
- Remote SSH Commands:** This section is expanded and contains:
  - Remote address: 10.0.5.100
  - Enable command on event triggered:  (checked)
  - Command on triggered: shutdown -s
  - Enable command on event cleared:  (unchecked)
  - Command on cleared: (empty field)

A 'Save' button is located at the bottom left of the configuration area. The footer of the page includes the copyright notice '© 2012, 2017 Network Technologies Inc. All rights reserved.' and the 'goahead WEB SERVER' logo.

Figure 2- Configure Event for Remote SSH Command

c. To troubleshoot any issues please check event log on E-xD which should show a message if there was any error. Also SSH logs will be helpful to fix an issue.

## For shutting down VMWare ESXi Host and Microsoft HyperV machines with SSH

E-xD can be used to shutdown any machines with SSH access including VMWare ESXi Host and Microsoft HyperV machines .

To shutdown VMWare ESXi host use the command '**poweroff**' as below:

<https://kb.vmware.com/s/article/1013193>

To setup SSH access for VMWare ESXi please refer below link:

<https://kb.vmware.com/s/article/1002866>

To shutdown Microsoft Hyper-V, SSH needs to be installed with public key access.

Once SSH is installed '**Stop-VM**' command can be used as below:

<https://docs.microsoft.com/en-us/powershell/module/hyper-v/stop-vm?view=win10-ps>

Any of the above commands can be entered in the E-xD to perform auto shutdown as detailed in these instructions

For the E-xD product manual with all features and functions, click [here](#).