NETWORK TECHNOLOGIES INCORPORATED
1275 Danner Dr Tel:330-562-7070
Aurora, OH 44202 Fax:330-562-1999
www.networktechinc.com

# 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 ).

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.

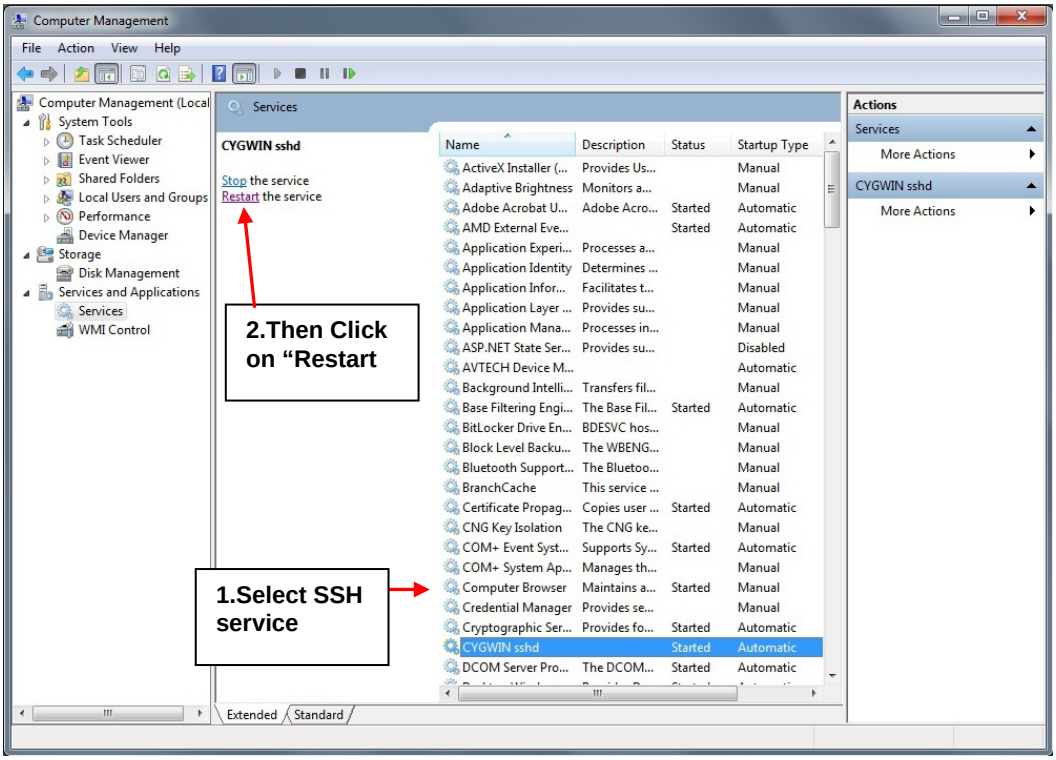
5. Download the RSA Public Key to the Windows computer. The downloaded file will have the default name **`id_rsa.pub`**.

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`**

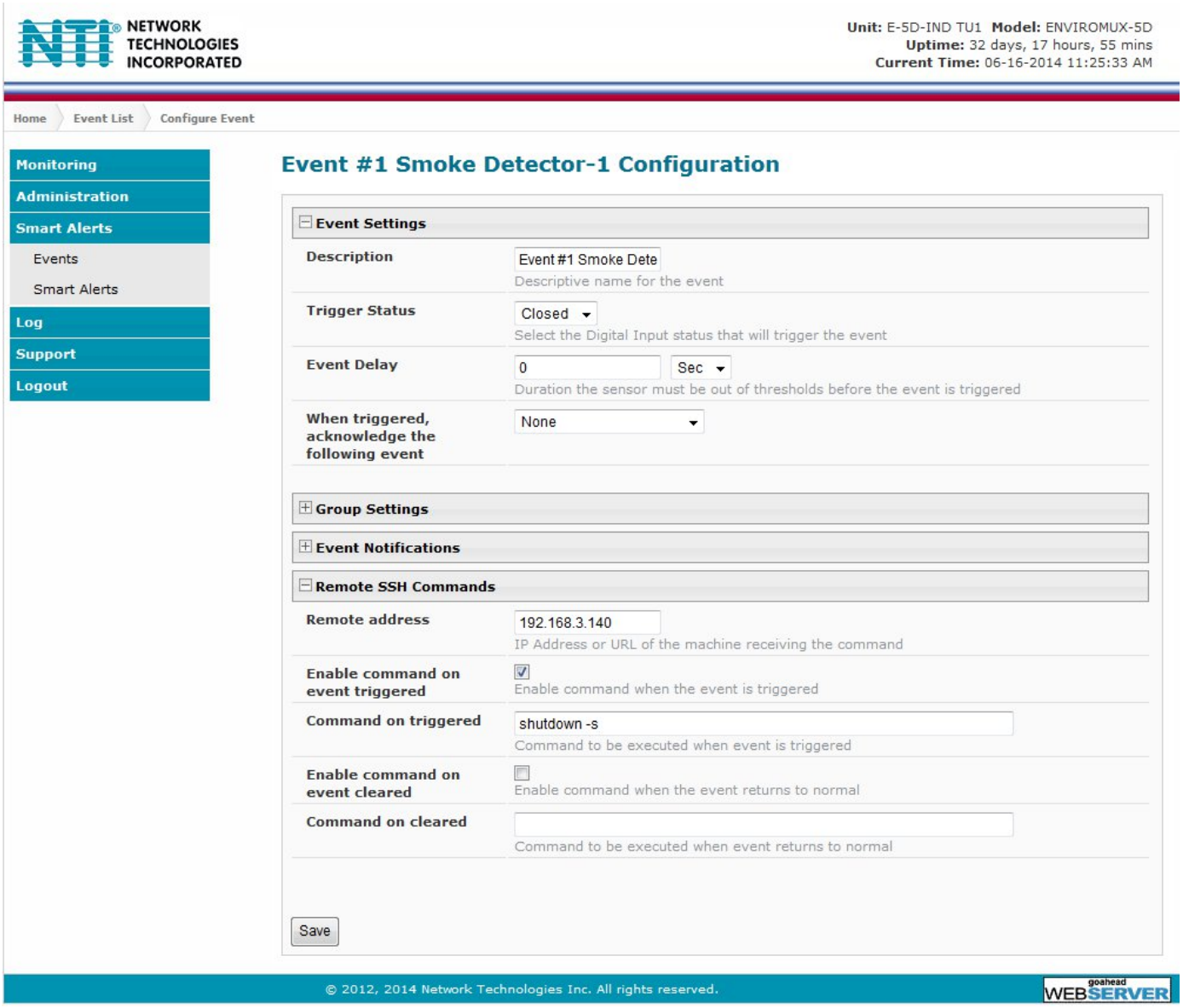
8. Then, to make the change take effect, restart the SSH server. To do this, **right** click on “Computer” (in the Start Menu) and click on “Manage”. Locate the SSH server in the list of Services and select it. Then click on “Restart”.




**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 ).




**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_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
```

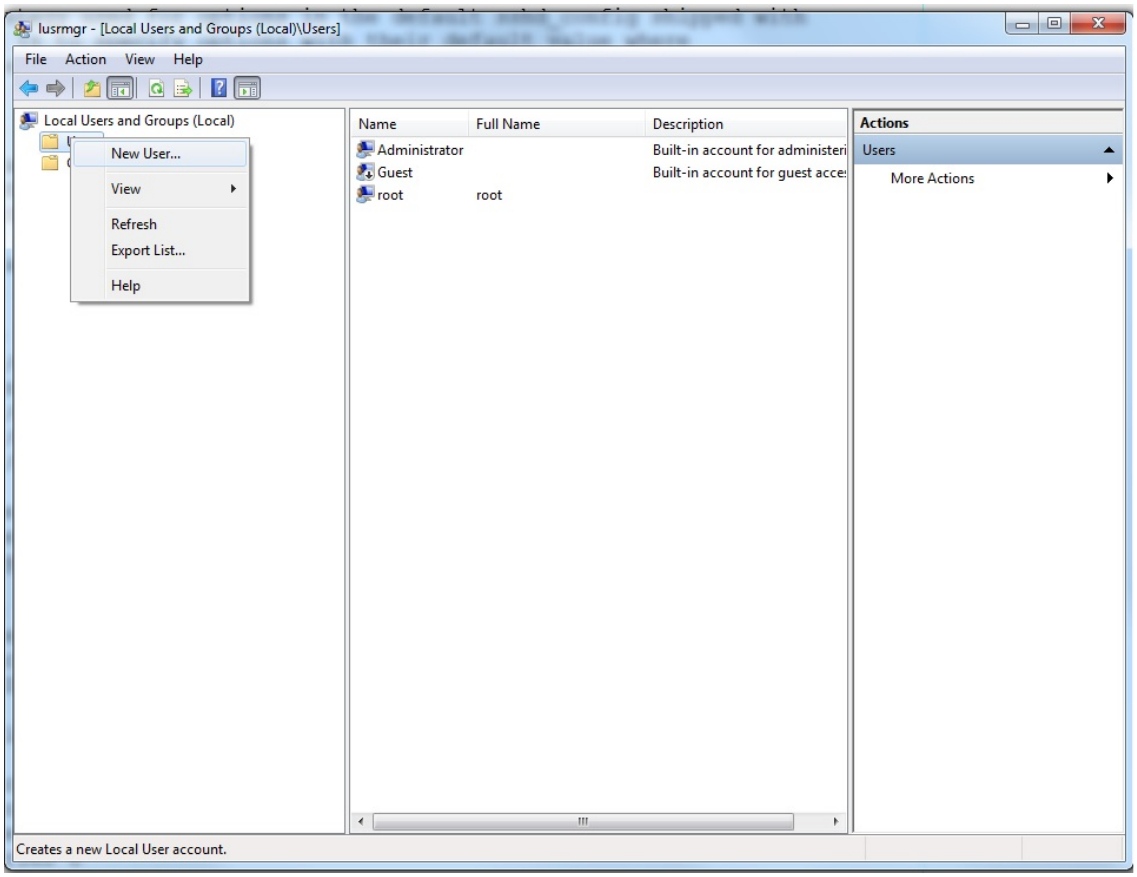
please use the below command instead:

```
     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

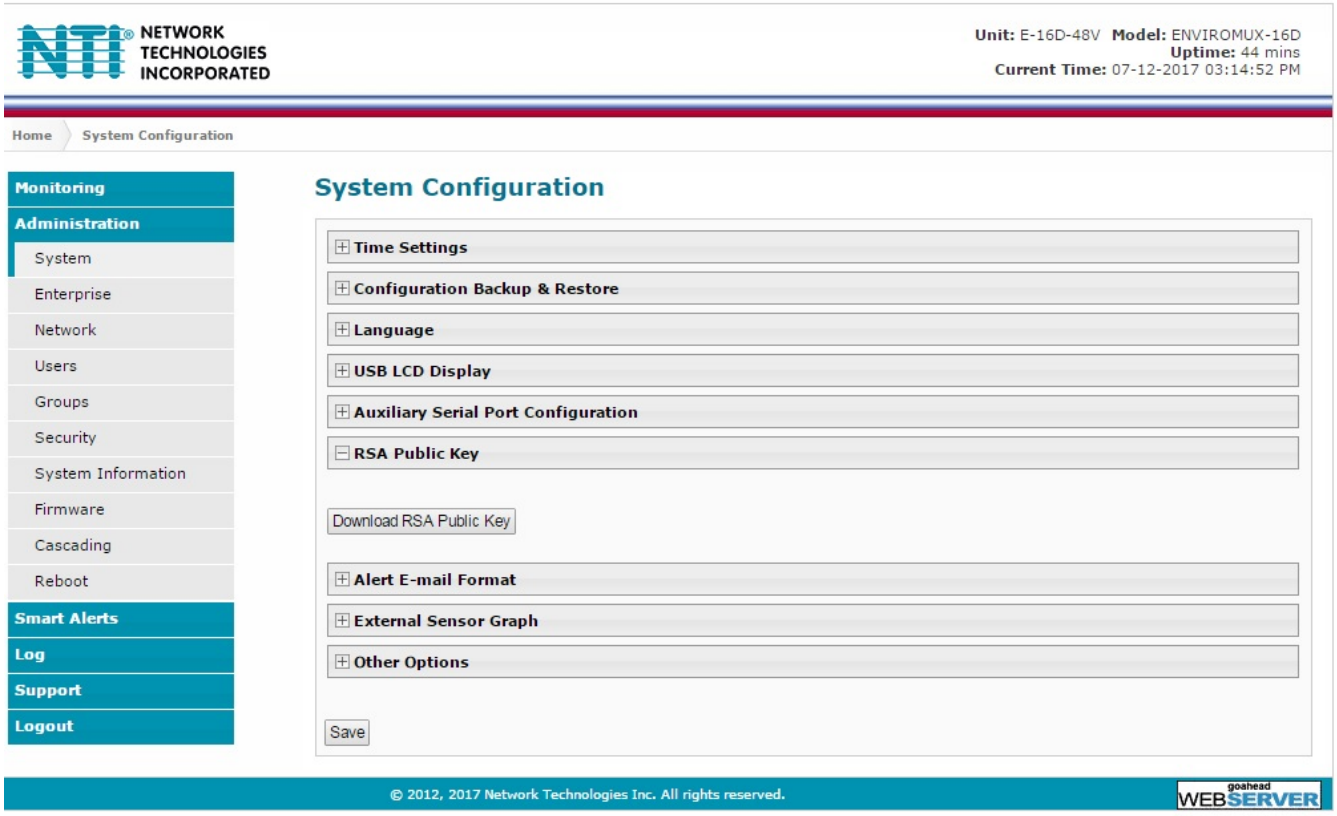
2. Add E-xD user to Windows SSH service user list.
   a. E-xD logs in as user root. If you do not have a 'root' user on the PC add this user by going in to Control Panel -> Manage User Accounts -> 'Advanced' tab -> Advanced -> Right click on User and add New User as shown in root_user.jpg. User password 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`**




**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

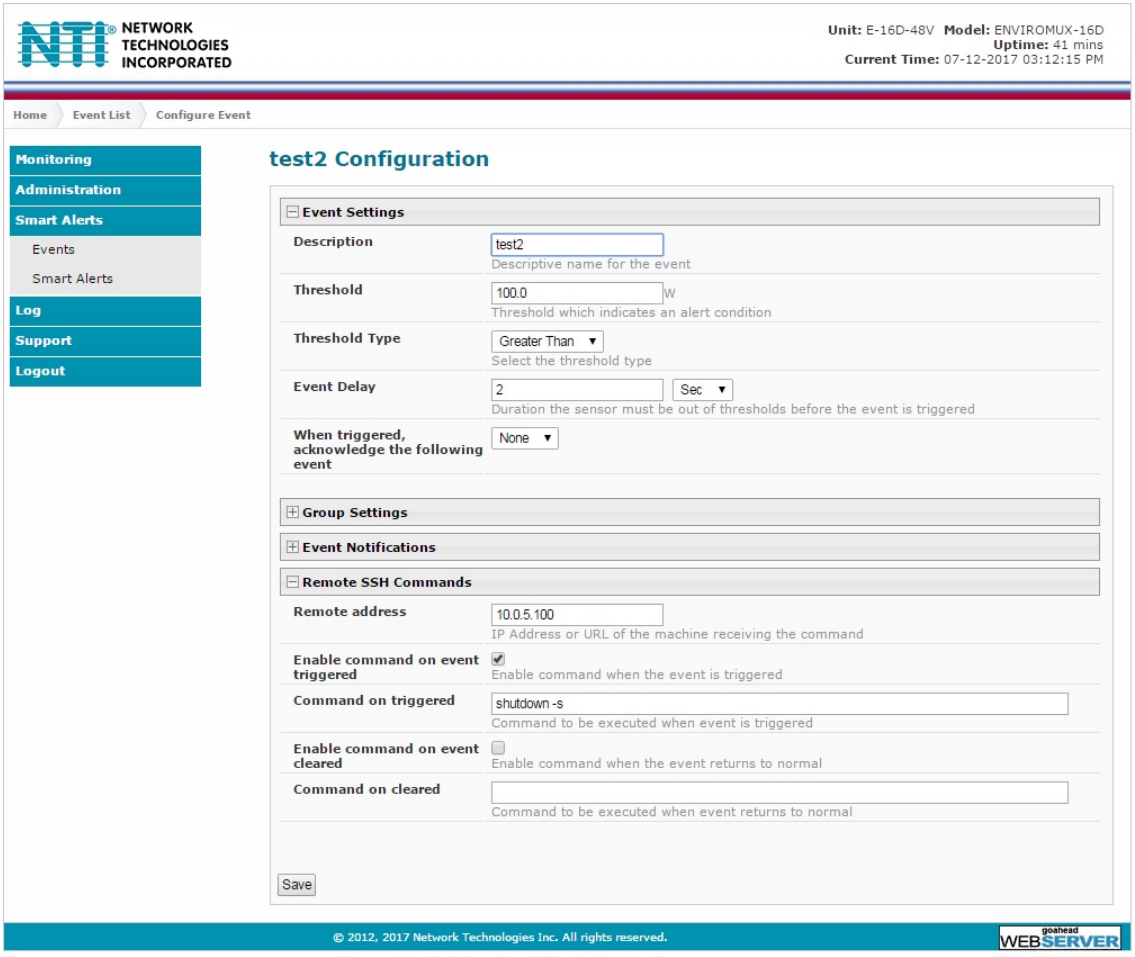



**Figure 2- Configure Event for Remote SSH Command**

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.**