



Knowledge Connects
Technology

VMware HUB

- ▶ [About Us](#)
- ▶ [Knowledge Base](#)
- ▶ [Tools](#)
- ▶ [Forums](#)
- ▶ [Downloads](#)
- ▶ [Contact Us](#)

VMware ESX Service Console

- [How to Allow Access to VMware ESX for a Service or Management Agent](#)
- [How to Determine the VMware ESX Service Console Firewall Security Level](#)
- [How to Set the VMware ESX Service Console Firewall Security Level](#)
- [How to Open a Port in the VMware ESX Service Console Firewall](#)
- [How to Close a Port in the VMware ESX Service Console Firewall](#)
- [How to Change the Default SSH Configuration](#)

How to Allow Access to ESX for a Service or Management Agent:

You can configure firewall properties to allow access for a service or management agent.

Procedure:

1. Log in to a vCenter Server system using the vSphere Client.
2. Select the host in the inventory panel.
3. Click the **Configuration** tab and click **Security Profile**.
The vSphere Client displays a list of active incoming and outgoing connections with the corresponding firewall ports.
4. Click **Properties** to open the Firewall Properties dialog box.
The Firewall Properties dialog box lists all the services and management agents that you can configure for the host.
5. Select the services and agents to enable.
The Incoming Ports and Outgoing Ports columns indicate the ports that the vSphere Client opens for the service. The Protocol column indicates the protocol that the service uses. The Daemon column indicates the status of daemons associated with the service.
6. Click **OK**.

[>>Top>>](#)

How to Determine the VMware ESX Service Console Firewall Security Level:

How to Configure the VMware ESX Service Console Firewall Security Level:

Procedure:

1. Log in to the service console and acquire root privileges.
2. Use the following two commands to determine whether incoming and outgoing traffic is blocked or allowed.
esxcfg-firewall -q incoming
esxcfg-firewall -q outgoing

High
Incoming ports blocked by default.
Outgoing ports blocked by default.

Medium
Incoming ports blocked by default.
Outgoing ports not blocked by default.

Low
Incoming ports not blocked by default.
Outgoing ports not blocked by default.

[>>Top>>](#)

How to Set the VMware ESX Service Console Firewall Security Level: How to Configure the VMware ESX Service Console Firewall Security Level:

Procedure:

1. Log in to the service console and acquire root privileges.
2. Run one of the following commands to set the service console firewall security level.
To set the service console firewall to medium security:
esxcfg-firewall --allowOutgoing --blockIncoming
To set the virtual firewall to low security:

Ads by Google



[Dns Firewall](#)

Most Secure DNS Service. Quality Reliability and Scalability 24/7.
www.UltraDNS.com

[Vmware](#)

Optimize, Extend, & Accelerate Your Infrastructure. Free EMC Whitepaper
www.emc.com/virtual-desktop

[VMware vSphere Courses](#)

vSphere, vCenter, I3, ESX Training Act Now. Get Free Geek Gear w/Class
www.rocksolidtechnical.com/VM

[ESX Performance Dashboard](#)

Instant visibility, reports, & more Download a free trial today!
netreo.com/v2trial

[Virtualization 2.0 Ready](#)

Single Agent Monitors all the VMs Monitor 80 apps, pinpoint rootcause
www.GInnovations.com

esxcfg-firewall --allowIncoming --allowOutgoing

To return the service console firewall to high security:

esxcfg-firewall --blockIncoming --blockOutgoing

3. Use the following command to restart the vmware-hostd process.
service mgmt-vmware restart

[>>Top>>](#)

How to Open a Port in the VMware ESX Service Console Firewall:

Procedure:

1. Log in to the service console and acquire root privileges.
2. Use the following command to open the port.
esxcfg-firewall --openPort ,tcp|udp,in|out,
is the vendor-specified port number.
Use tcp for TCP traffic or udp for UDP traffic.
Use in to open the port for inbound traffic or out to open it for outbound traffic. is a descriptive name to help identify the service or agent using the port. A unique name is not required.
For example: **esxcfg-firewall --openPort 6380,tcp,in,Navisphere**
3. Run the following command to restart the vmware-hostd process.
service mgmt-vmware restart

[>>Top>>](#)

How to Close a Port in the VMware ESX Service Console Firewall:

Procedure:

1. Log in to the service console and acquire root privileges.
2. Use the following command to close the port.
esxcfg-firewall --closePort ,tcp|udp,in|out,
The argument is optional.
For example:
esxcfg-firewall --closePort 6380,tcp,in
3. Use the following command to restart the vmware-hostd process. **service mgmt-vmware restart**

[>>Top>>](#)

How to Change the Default SSH Configuration:

You can change the default SSH configuration.

Procedure:

1. Log in to the service console and acquire root privileges.
2. Change to the **/etc/ssh** directory.
3. Use a text editor to perform any of the following actions in the **sshd_config** file.
To allow remote root login, change the setting to yes in the following line.
PermitRootLogin no
To revert to the default SSH protocol (Version 1 and 2), comment out the following line.
Protocol 2
To revert to the 3DES cipher and other ciphers, comment out the following line.
Ciphers aes256-cbc,aes128-cbc
To disable Secure FTP (SFTP) on SSH, comment out the following line.
Subsystem ftp /usr/libexec/openssh/sftp-server
4. Save your changes and close the file.
5. Run the following command to restart the SSHD service. **service sshd restart**

[>>Top>>](#)