CloudShell

QualiX 2.3 Solution Pack

Installation and Configuration Guide

CloudShell 7.1 GA

Release Date: January 2017

Document Version: 2.0

Quali

Legal notice

Information in this document is subject to change without notice. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Quali Ltd.

Quali may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except if expressly provided in any written license agreement from Quali, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Quali, CloudShell, CloudShell Authoring, CloudShell Resource Manager, CloudShell Remote Runner, CloudShell Runtime, CloudShell Monitor, CloudShell Spy, CloudShell Portal, the Quali logo, the CloudShell logo, and the CloudShell application logos, and all other Quali product names and logos are trademarks or registered trademarks of Quali Ltd. The absence of a trademark from this list does not constitute a waiver of Quali intellectual property rights concerning that trademark.

All other trademarks, brand and product names are property of their respective holders.

Contents

Overview

This document describes how to download the QualiX installation files, perform the installation and configuration to provide a virtual appliance (VA). QualiX can run on a VA of type KVM or VMware. The QualiX VA allows you to integrate Remote Desktop capabilities directly into your browser.

As a CloudShell user, this enables you, directly from your browser, to remotely connect to and control machines that are present in a reservation.

Among the advantages of working with QualiX are:

- Makes working with Remote Desktop Protocol (RDP) a seamless, integrated experience without the need to use other tools to connect.
- Enables you to use other remote connections, such as SSH and Telnet sessions, to connect to and control machines in a reservation.
- Provides native support for copy and paste operations as well as file transfer. For more information, see Working with QualiX VM.

Requirements

- KVM (For Linux users)
- VMWare (For Windows users)
- ESXi version 5.5 - 6.0
- At least 1 CPU with 1 GB memory. See Modify Number of CPUs and Allocated Memory.
- KVM requires CPU with hardware virtualization support (Intel VT-x or AMD-V)
- Make sure network connectivity is established between the QualiX machine and Quali server machine

Note: When deploying QualiX, make sure that its time is set to the exact UTC time defined on Quali Server.

Support

- QualiX v2.3 supports CloudShell 7.0 and above
- ESXi version 5.5 - 6.0
- Integration with Amazon Web Services (AWS)

Downloading the QualiX Installation Files

The installation files for QualiX are available by downloading the **QualiX Server extension** from the Quali's Download Center. Download the files into a temporary location on your local machine.

Each folder contains an .md5 file with a list of files in that folder and their md5 checksum.

Note: Registration to the Quali Support Center is required. If you have not registered, click this link to register New registration.

Components of the QualiX Server extension

The Qualix Server extension comprises the following files that are required for installing QualiX:

Download Link	Downloaded File	Contents
QualiX VM Version 2.3 for VMWare	QualiX 2.3 vSphere.exe	VMWare installation files: • QualiX.mf • QualiX.ovf • QualiX-disk1.vmdk
QualiX VM Version 2.3 for KVM	QualiX 2.3 KVM.exe	KVM installation file: • QualiX.img

Installation and Configuration

This chapter includes the following:

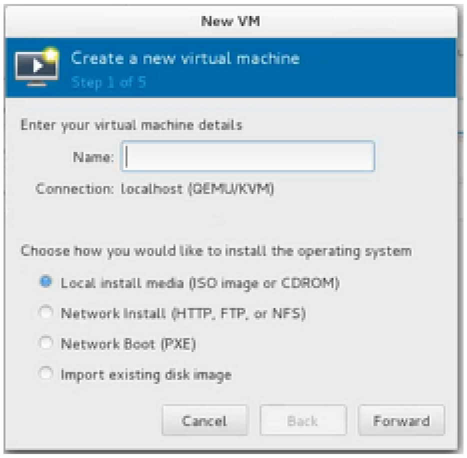
Create VM using the qcow2 Image File (KVM)

Use the following steps to use KVM to import the QualiX image and create a VM.

Note: Your CPU must have hardware virtualization support (Intel VT-x or AMD-V) to be able to use KVM.

To create a VM by importing the QualiX image:

1. Login to your machine as root user.
2. Navigate to the directory where the installation files were downloaded. Create a backup copy of the image file.
3. Move the image file to the directory where you want to place the VM.
4. In the Linux desktop, open Virt-manager Virtual Machine Manager and click **Create a new virtual machine** .



New VM

Create a new virtual machine

Step 1 of 5

Enter your virtual machine details

Name:

Connection: localhost (QEMU/KVM)

Choose how you would like to install the operating system

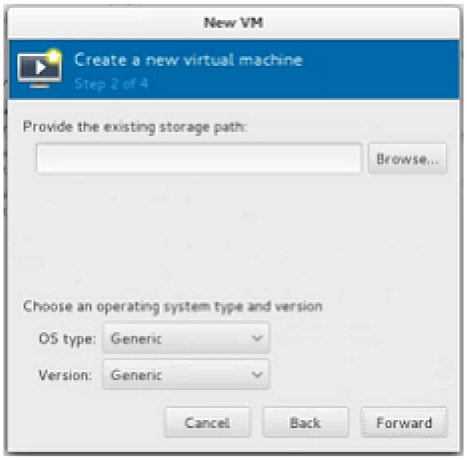
● Local install media (ISO image or CDROM)

○ Network Install (HTTP, FTP, or NFS)

○ Network Boot (PXE)

○ Import existing disk image

5. In the **New VM** window, in the **Name** field, enter a name for the VM.
6. Select **Import existing disk image** and click **Forward**.



New VM

Create a new virtual machine

Step 2 of 4

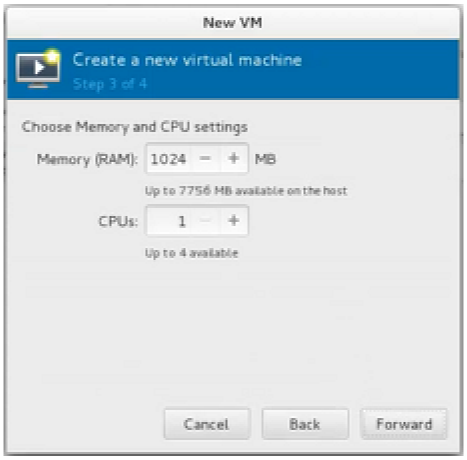
Provide the existing storage path:

Choose an operating system type and version

OS type: Generic

Version: Generic

7. Click **Browse** and navigate to the path of the image file. Select the image file and click **Open**. Click **Forward**.



New VM

Create a new virtual machine

Step 3 of 4

Choose Memory and CPU settings

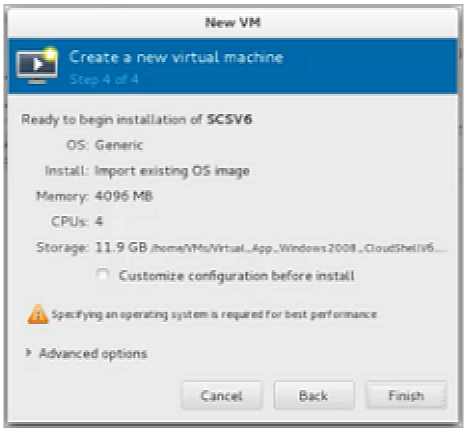
Memory (RAM): 1024 MB

Up to 7756 MB available on the host

CPUs: 1

Up to 4 available

8. For the memory and CPU settings, specify values that match your system. For the purposes of this procedure, the values 4 GB RAM (4096 MB) and 4 CPUs are specified. Click **Forward**.



New VM

Create a new virtual machine

Step 4 of 4

Ready to begin installation of **SCSV6**

OS: Generic

Install: Import existing OS image

Memory: 4096 MB

CPUs: 4

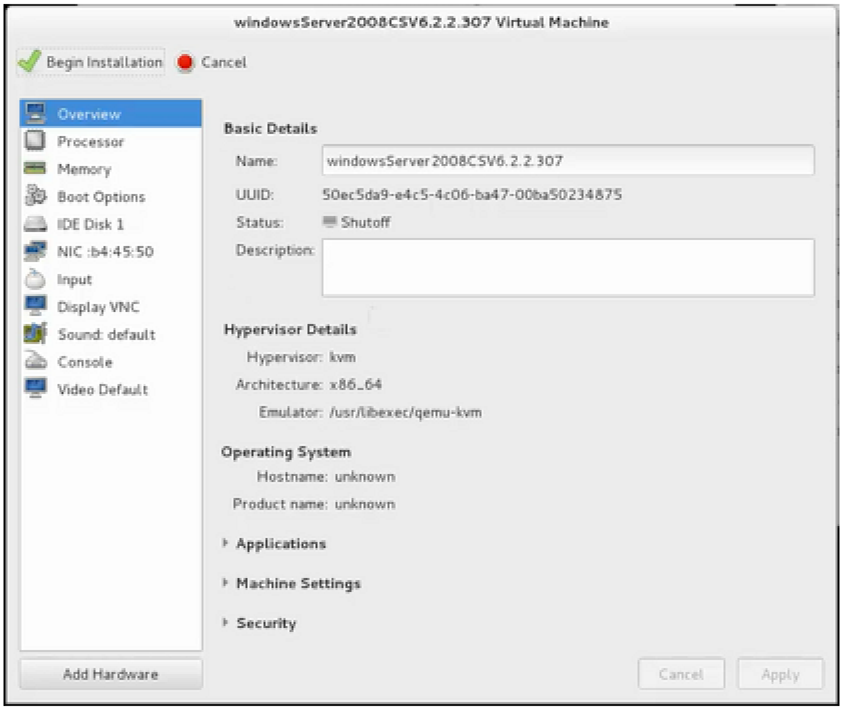
Storage: 11.9 GB /home/VMs/Virtual_App_Windows2008_CloudShellV6...

□ Customize configuration before install

Specifying an operating system is required for best performance

9. Select the **Customize configuration before install** option. Click **Finish**.

The details of the VM to be created are displayed.



Basic Details

Name: windowsServer2008CSV6.2.2.307

UUID: 50ec5da9-e4c5-4c06-ba47-00ba50234875

Status: Shutoff

Description:

Hypervisor Details

Hypervisor: kvm

Architecture: x86_64

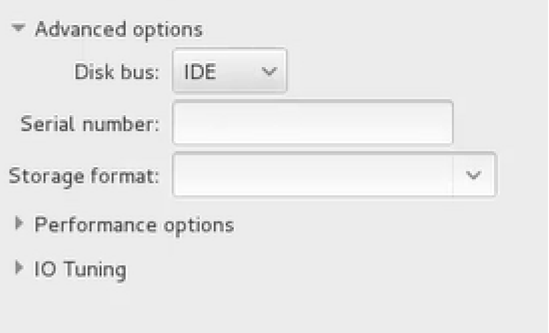
Emulator: /usr/libexec/qemu-kvm

Operating System

Hostname: unknown

Product name: unknown

10. From the left pane, select **IDE Disk 1**. Click **Advanced options**.



Disk bus: IDE

Serial number:

Storage format:

11. Ensure that IDE is selected in the **Disk bus** field.
12. In the Storage format field, select qcow2. Click **Apply**.
13. Click Begin Installation.

    The VM is created.

    After the installation of the QualiX VM, continue with Post Installation Configuration.

Create VM using the OVF Template (vSphere)

Use the following steps to use vSphere to deploy the QualiX template and create a VM.

To create a VM by deploying the OVF template:

1. In your local machine, login to vSphere with administrator credentials.
2. Click **File > Deploy OVF Template**.
3. In the **Deploy OVF Template** window, click **Browse**. Navigate to the directory where the installation files are located.
4. In the **Deploy from a file or URL** field, navigate to and then select the required OVF file.
5. Click **Next**. View the summary of the OVF template. If the displayed details are correct, click **Next** .

   The **End User License Agreement** page is displayed with the details of license agreements that are associated with the software that is installed in the OVF template.
6. Accept the license agreements to deploy the OVF template. If no license agreements are associated with the installed software, this screen does not appear. Click **Next**.
7. Enter the name for the deployed OVF template. The length of the name can be up to 80 characters long and should be unique within the VM folder. Names are case sensitive.
8. Select the folder location within the inventory for the virtual appliance. Click **Next**.
9. Specify Thin Provision. Click **Next**.
10. When the deployment has completed, click **Power On**.
11. Right-click the VM and select **Open Console**.
12. In the VM console window, check the **Settings Screen** to make sure that it uploaded without errors.

    After the installation of the QualiX VM, continue with Post Installation Configuration.

Post Installation Configuration

This section describes the configuration steps that are required after the first login to QualiX VM.

Log into the VM

To log into the new VM:

1. Power on the new VM.
2. Login as the root user.

   The default credentials are:

   Username: **root**

   Password: **Password1**

Enable Remote Connection from CloudShell Portal

This section explains how to configure QualiX support in Quali Server to allow end-users to connect to their devices and VMs from CloudShell reservations. To achieve this, you need to associate the QualiX machine with the remote access terminals you want to make available in CloudShell Portal.

Note: In order to connect to a device or VM from CloudShell Portal, the resource of the element must include the **User** and **Password** attributes. To learn how to add the attributes, see Prepare and Reserve Environment.

To enable SSL connection to reservation elements, perform the steps in Enable SSL Connection from CloudShell Portal.

To enable remote connection from CloudShell Portal:

1. In Quali server, open the following file in a text editor:

   `C:\ProgramData\QualiSystems\Settings\Global\ServerUniversalSettings.xml`

2. Under the `<ConfigurationSection name="LinkApplications">` tag, replace the lines of the relevant remote access terminals (Telnet, SSH, RDP, VNC) with the lines in this code sample:

   ```
   <key name="Telnet" pattern="http://<VM
   ```

```
IP>/remote/#/client/c/telnet{qid}?qtoken=
{qtoken}&amp;hostname=
{Address}&amp;protocol=telnet&amp;port=23&amp;username=
{User}&amp;password={Password}" icon-key="Telnet" />

<key name="SSH" pattern="http://<VM
IP>/remote/#/client/c/ssh{qid}?qtoken={qtoken}&amp;hostname=
{Address}&amp;protocol=ssh&amp;port=22&amp;username=
{User}&amp;password={Password}" icon-key="SSH" />

<key name="RDP" pattern="http://<VM
IP>/remote/#/client/c/rdp{qid}?qtoken={qtoken}&amp;hostname=
{Address}&amp;protocol=rdp&amp;port=3389&amp;username=
{User}&amp;password={Password}&amp;security=any&amp;ignore-
cert=true" icon-key="RDP" />

<key name="VNC" pattern="http://<VM
IP>/remote/#/client/c/vnc{qid}?qtoken={qtoken}&amp;hostname=
{Address}&amp;protocol=vnc&amp;port=5901&amp;username=
{User}&amp;password={Password}" icon-key="VNC" />
```

Note: The `qtoken` & `qid` keys are automatically filled out by the server and are related to CloudShell security enhancements. You do not need to configure anything related to these keys.

3. Replace `<VM IP>` with the IP of the QualiX machine.

   To find the IP of the VM, at the system prompt, run the `ifconfig` command. If you are using vSphere, VMware Tools also provides the machine's IP address (located in the vSphere **Summary** tab).

5. Save the file.

Enable SSL Connection from CloudShell Portal

This section explains how to configure secure remote connections to devices and VMs from CloudShell reservations.

Note: In order to connect to a device or VM from CloudShell Portal, the resource of the element must include the **User** and **Password** attributes. To learn how to add the attributes to a resource, see Prepare and Reserve Environment.

To enable SSL connection to reservation elements:

1. Make sure to perform the procedure in Enable Remote Connection from CloudShell Portal.
2. In Quali Server, open the following file in a text editor:
   `C:\ProgramData\QualiSystems\Settings\Global\ServerUniversalSettings.xml`
3. Scroll down to the `<ConfigurationSection name="LinkApplications">` tag.
4. In the `pattern` element of the remote access terminal lines, replace `http` with `https` and save the file.

   For example:

   ```
   <key name="Telnet"
   pattern="https://192.168.58.7/remote/#/client/c/telnet
   {qid}?qtoken={qtoken}&amp;hostname=
   {Address}&amp;protocol=telnet&amp;port=23&amp;username=
   {User}&amp;password={Password}" icon-key="Telnet" />
   ```

   Note: The `qtoken` & `qid` keys are automatically filled out by the server and are related to CloudShell security enhancements. You do not need to configure anything related to these keys.

5. Save the file.
6. (Optional) To change the SSL certificate, see https://tomcat.apache.org/tomcat-8.0-doc/ssl-howto.html.

Customize Remote Access Terminals

You can both customize the default access terminals, and add and customize your own access terminals in order to access your devices remotely from CloudShell Portal. You can also control which access terminals are available for which sets of equipment.

Adding new remote access terminals

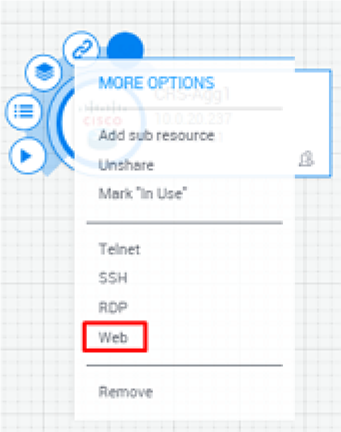
To add new remote access terminals:

1. Go to the `C:\ProgramData\QualiSystems\Settings\Global\ServerUniversalSettings.xml` file.
2. Under the `<ConfigurationSection name="LinkApplications">` tag, add the new remote access terminals.

   For example, to grant access to a webpage of a device, copy one of the default access terminals (for example, RDP/Telnet as shown in the Enable Remote Connection from CloudShell Portal), and simply change the settings described in the following steps.
3. Perform the following steps in the line of the appropriate remote access terminals:
4. Change the entire `pattern` value to be the URL of the desired webpage.
5. Change the `name` and `icon-key` to be the name you want to display for the remote access terminal in CloudShell Portal (for example `Web`).

   For example: `<key name="Web" pattern="http://quali.com" icon-key="Web" />`

   The specified link (in this case `Web`) is displayed in the **More Options** list in CloudShell Portal (together with the predefined links to the default access terminals):

   When you click the ("Web") link in an active reservation, the desired URL (quali.com for example) is displayed.

Customizing access terminals based on specific equipment

This section explains how to create an access terminal to a specific device. This is done by setting, in the remote access terminal, the name of an attribute that is on the resource so that when connecting to the device, the attribute value on the resource will be used.

To customize access terminals according to particular sets of equipment:

1. In Quali server, open the following file in a text editor `C:\ProgramData\QualiSystems\Settings\Global\ServerUniversalSettings.xml` file.
2. Embed attributes in the connection string in order to make it flexible according to the device from which you are trying to open an access terminal.

   You may embed any attribute inside the connection string in order to make it dynamic and based on the device from which you need the access. Any attribute you have existing in **CloudShell Resource Manager Client** may be referenced inside the connection string by placing it inside curly brackets {}.

   For example, you can edit:

   ```
   <key name="Web" pattern="http://quali.com" icon-key="Web" />
   ```

   with dynamic attributes like this:

   ```
   <key name="Web" pattern={web URL attribute} icon-key="{website
   name attribute}" />
   ```

3. Save the file.
4. In **Resource Manager Client**, create and attach your custom attribute to the resource models/families for which you would like to use the customized connection string.

   > To customize the common access terminals to specific sets of equipment, do the following:
   >
   > a. For each access to the device, create a unique set of attributes:
   >   - {access type} User (for example, SSH User)
   >   - {access type} Password
   >
   > b. Attach the attributes to the specific resource models for which you would like to have this access option.

5. Save your changes.
6. Return to the `ServerUniversalSettings.xml` file, and add the attributes in {} inside the matching connection string.

   For example, attributes **SSH User** and **SSH Password**:

   ```
   <key name="SSH"
   pattern="https://192.168.56.7/remote/#/client/c/ssh
   {qid}?qtoken={qtoken}&amp;hostname=
   ```

```
{Address}&amp;protocol=ssh&amp;port=22&amp;username={SSH
User}&amp;password={SSh Password}" icon-key="SSH" />
```

7. Keep the original `User` and `Password` attributes in a resource model if you need some server-side operations on it (connecting routes/auto load, etc.).

Modify Number of CPUs and Allocated Memory

At any time you can modify the number of CPUs being used and the amount of allocated memory.

Note: It is recommended to use 1 CPU with 1GB Memory.

Refer to the following table for the CPU and memory values:

Number of concurrent connections	CPU value	Memory values
100	1	1 GB
500	2	8 GB
1,500	2	16 GB

Prepare and Reserve Environment

This section guides you on how to configure resources that enable remote connection to the devices they represent, and how to connect to those devices from within CloudShell.

Note: The resource configuration steps must be performed for each resource for which you want to enable remote connection from CloudShell Portal.

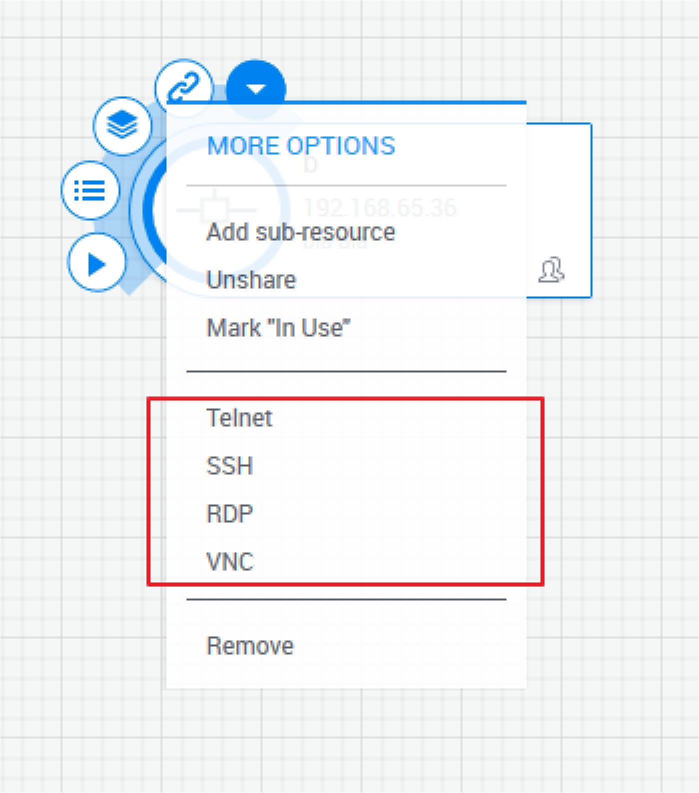
To prepare and then reserve an environment:

1. Restart the **Quali Server** service.
2. In **Resource Manager Client**, open the **Attributes** page and make sure the following attributes are configured:

Attribute	Attribute Type	Rules
User	String	Configuration, Setting
Password	Password	Configuration, Setting

3. In the **Resource Families** pane, add these attributes to the families or models of the physical and virtual devices to which end-users will connect. For example, the "bridge" family.
4. In **Resource Explorer**, create a resource that uses a model from the "bridge" family.
5. Double-click the resource, in the **Parameters** section, click the **Address** field and insert the IP with which you want to do a session (RDP, Telnet, SSH, and VNC).
6. Click the **Configuration** button in the top right corner of the page. Insert into the new attributes the User Name and the Password for your session.
7. Save your changes.
8. Log in to **CloudShell Portal** and click **Create an Environment**. Add the new resource.
9. Reserve the new environment.
10. In the environment's diagram, hover over the resource. In the **Actions** menu, the options you configured are displayed: Telnet, SSH, RDP, and VNC. Each option redirects you to the IP address you specified in the resource.

For example, all four remote access terminals:



Appendix

This appendix discusses a known issue and an optional procedure to remove a startup message.

Known Issues

Network Time Protocol Server	In certain cases Quali Server, QualiX and Client machines might be synced against different Network Time Protocol (NTP) servers and therefore have slight time differences, causing issues with token-based authentication. For information about how to resolve this issue, see http://support.ntp.org/bin/view/Support/WindowsTimeService.
Attribute of type Lookup cannot be used	In CloudShell Resource Manager, when defining or modifying attributes to be used in the connection string for QualiX features like SSH, TELNET and RDP, an attribute of type Lookup cannot be used.

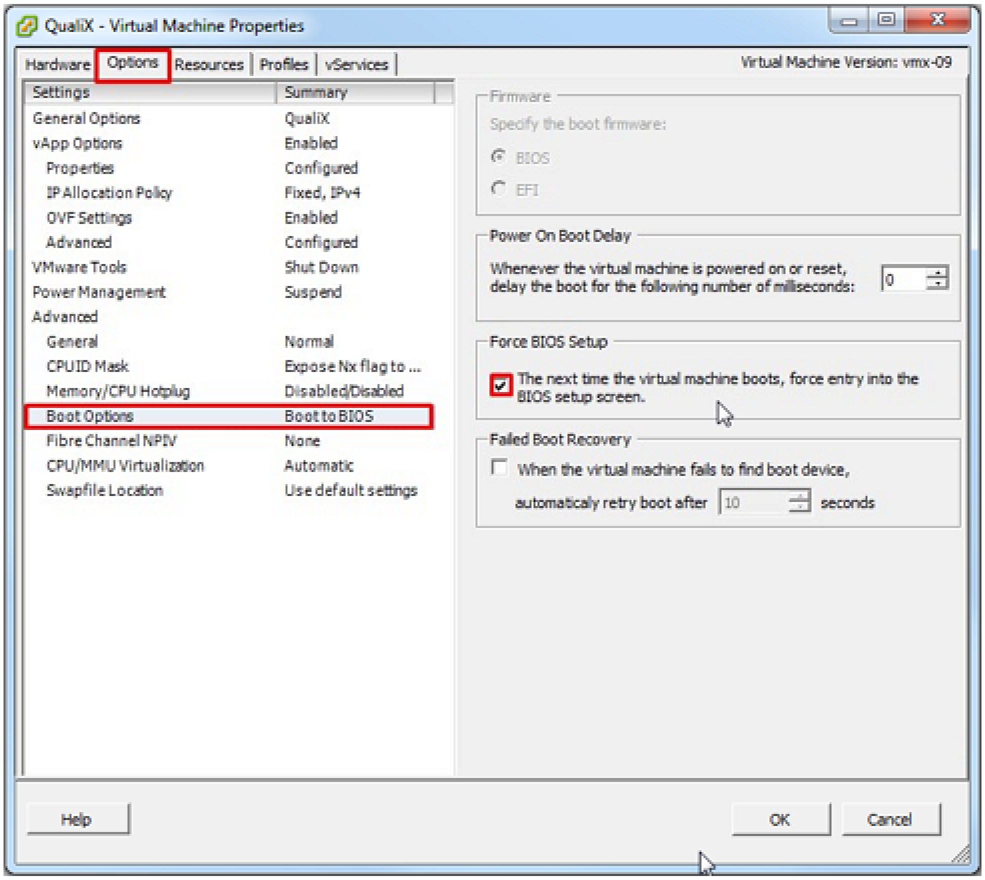
(Optional) Removing Message at Startup

Perform these steps to remove a message indicating that the VM is looking for a floppy drive at startup. These steps remove the floppy drive from the BIOS of the VM.

Note: The functionality of the VM is not affected whether these steps are performed or not.

To modify the VM settings:

1. In the desktop, open the VMware vSphere client.
2. Right-click the VM in the vSphere client and select **Edit Settings**.
3. Click the **Options** tab, select **Boot options**.
4. In the **Force BIOS Setup** area, select the option **The next time the virtual machine boots, force entry into the BIOS setup screen**.



Virtual Machine Version: vmx-09

Settings	Summary
General Options	QualiX
vApp Options	Enabled
Properties	Configured
IP Allocation Policy	Fixed, IPv4
OVF Settings	Enabled
Advanced	Configured
VMware Tools	Shut Down
Power Management	Suspend
Advanced	
General	Normal
CPUID Mask	Expose Nx flag to ...
Memory/CPU Hotplug	Disabled/Disabled
Boot Options	Boot to BIOS
Fibre Channel NPIV	None
CPU/MMU Virtualization	Automatic
Swapfile Location	Use default settings

Firmware

Specify the boot firmware:

● BIOS

○ EFI

Power On Boot Delay

Whenever the virtual machine is powered on or reset, delay the boot for the following number of milliseconds: 0

Force BIOS Setup

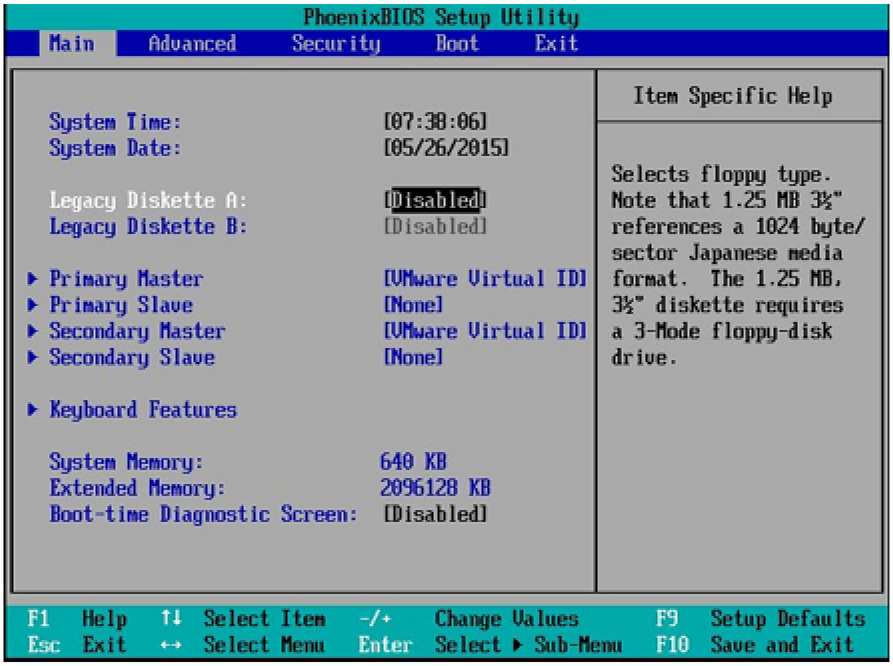
☑ The next time the virtual machine boots, force entry into the BIOS setup screen.

Failed Boot Recovery

□ When the virtual machine fails to find boot device, automaticaly retry boot after 10 seconds

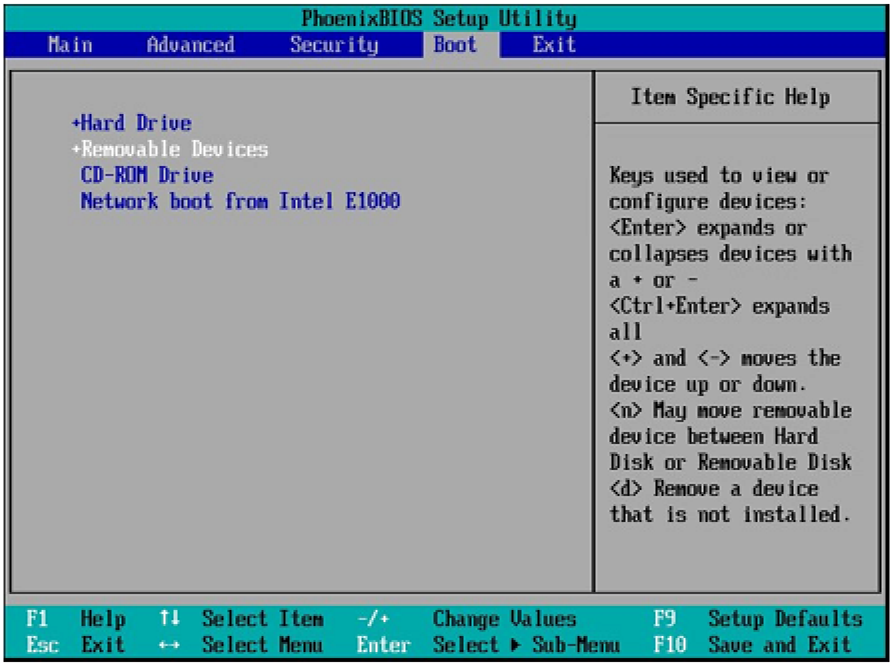
5. Click **OK**.
6. Restart the VM.

   On the restart of the VM, the **BIOS Setup Utility** is displayed.



```
                        PhoenixBIOS Setup Utility
  Main    Advanced    Security    Boot    Exit

                                                  Item Specific Help

  System Time:                  [07:38:06]
  System Date:                  [05/26/2015]      Selects floppy type.
                                                  Note that 1.25 MB 3½"
  Legacy Diskette A:            [Disabled]        references a 1024 byte/
  Legacy Diskette B:            [Disabled]        sector Japanese media
                                                  format.  The 1.25 MB,
▶ Primary Master                [VMware Virtual ID] 3½" diskette requires
▶ Primary Slave                 [None]            a 3-Mode floppy-disk
▶ Secondary Master              [VMware Virtual ID] drive.
▶ Secondary Slave               [None]

▶ Keyboard Features

  System Memory:                640 KB
  Extended Memory:              2096128 KB
  Boot-time Diagnostic Screen:  [Disabled]

F1   Help  ↑↓  Select Item  -/+    Change Values        F9   Setup Defaults
Esc  Exit  ↔   Select Menu  Enter  Select ▶ Sub-Menu    F10  Save and Exit
```

7. In the **Main** tab, change the value of the default **Legacy Diskette A** to **Disabled**.
8. Select the **Boot** tab.



```
                        PhoenixBIOS Setup Utility
  Main    Advanced    Security    Boot    Exit

                                                  Item Specific Help

     +Hard Drive
     +Removable Devices
      CD-ROM Drive                                Keys used to view or
      Network boot from Intel E1000               configure devices:
                                                  <Enter> expands or
                                                  collapses devices with
                                                  a + or -
                                                  <Ctrl+Enter> expands
                                                  all
                                                  <+> and <-> moves the
                                                  device up or down.
                                                  <n> May move removable
                                                  device between Hard
                                                  Disk or Removable Disk
                                                  <d> Remove a device
                                                  that is not installed.

F1   Help  ↑↓  Select Item  -/+    Change Values        F9   Setup Defaults
Esc  Exit  ↔   Select Menu  Enter  Select ▶ Sub-Menu    F10  Save and Exit
```

9. Modify the order that devices are set to boot. Move **Hard Drive** to the first position above **Removable Devices**.
10. Press **F10** to save and then exit the **Setup Utility**.

Working with QualiX VM

This section describes how to use functions to copy text to and from machines by using RDP through your browser. File transfer to and from client machines is also described. There is also an example of how to create attributes, a resource, a new environment and then reserve the environment.

Copying Text to and from Machines using RDP

Use the following steps to pass strings from the client machine to the machines to which you are connected with RDP.

To copy strings from the client machine:

1. In a browser in an RDP session, press **Ctrl + Alt + Shift**. The clipboard section displays in a pane on the left side of the screen.
2. Copy any string from the client machine to the clipboard.
3. Press **Ctrl + Alt + Shift** to close the pane and then paste the string to the machine you are connected to.

Transfer Files from the Client Machine

Use the following steps to transfer files from the client machine to the machine to which you are connected with RDP.

To transfer files from the client machine:

1. In the client machine, drag the specified file to a browser that is in an RDP session and press **Ctrl + Alt + Shift**. The side pane displays. Close this pane.
2. In the machine to which you are connected with RDP through the browser, open **My Computer** and select the new **G on Guacamole RDP** hard disk. Open this hard drive.
3. Move the file to the desktop.

Transfer Files to the Client Machine

Use the following steps to transfer files from the machine to which you are connected with RDP to the client machine.

To transfer files to the client machine:

1. In the machine to which you are connected with RDP through the browser, move the required file to the **Downloads** folder in the new **G on Guacamole RDP** hard disk.
2. Press **Ctrl + Alt + Shift** to open the side pane. The file that was transferred is available and can be saved to the required location.

Revision History

Solution pack version	CloudShell Version	Doc revision number	Description
2.2	7.0 EA	2.0	Create VM using the qcow2 Image File (KVM): fixed steps Known Issues: fixed/expanded timezone in TS drivers note Customize Remote Access Terminals
	7.0 GA Patch 1 [7.0.0.8538]	3.0	Added a note explaining the qtoken & qid keys in the Quali server file configuration following security improvements
		3.0	Updated link to the Solution Packs Download Center
		3.0	Support: Clarified supported CloudShell version; Connection between QualiX server and Quali server Components of the QualiX Server extension: retitled from "Components of the Guacamole Server library"; updated change log file name
	7.1 EA	1.0	no change applied
2.3	7.1 GA	1.0	Support for CloudShell integration with Amazon Web Services
	7.1 GA	2.0	Updated links to Quali's download center, the support portal, and the vSphere and KVM images Removed auto-created hyphens in code samples for long strings RDP remote access terminal code updated to support remote connections to Windows 10 machines Retitled "Configure Quali Server File" and "Configure SSL Support" to

Solution pack version	CloudShell Version	Doc revision number	Description
			Enable Remote Connection from CloudShell Portal and Enable SSL Connection from CloudShell Portal, respectively. Post Installation Configuration and Prepare and Reserve Environment: updated/simplified configuration procedures Moved Working with QualiX VM to the Appendix chapter