CITRIX®

XenClient Enterprise 5 Quick Start Guide

July 22, 2013

XenClient Enterprise Version 5.0

Table of Contents

About XenClient

Desktop virtualization solutions such as Citrix XenDesktop are already a core element of the IT strategy at many organizations because they provide IT with a server-hosted approach for centralizing the control, management and delivery of data, applications and desktops. This approach to desktop virtualization benefits both IT and end users. The cost and complexity of managing desktops for IT is reduced greatly while end users can access their desktops from any device with a seamless experience.

However, sometimes organizations cannot deploy server-hosted desktops because of environments that are disconnected or environments that have inconsistent or limited network connectivity, or even because of users with resource intensive requirements. This IT challenge is only set to grow as rapidly changing workstyles lead to growing numbers of mobile and disconnected workers who use corporate laptops beyond the reach of the enterprise network. These laptops often lack consistent network connections, making it difficult to centrally manage and secure them.

Citrix XenClient Enterprise, the local VM pillar of XenDesktop and its FlexCast delivery technology, addresses these challenges by extending desktop virtualization to offline laptops and PCs. XenClient provides enterprises with centralized management, enhanced reliability and high security through local virtual desktops.

How XenClient Works

The XenClient Enterprise solution is made up of two primary components:

1. **XenClient Engine** – XenClient is a true Type-1 Xen client hypervisor that runs on bare metal and provides high performance and security while offering a native user experience to end users. XenClient Engine utilizes the open source Xen hypervisor to let users run multiple local virtual desktops simultaneously, side-by-side and in complete isolation. Users of XenClient-powered devices can access their various virtual desktops anywhere, anytime—even while disconnected from the network.

2. **XenClient Synchronizer** – XenClient Synchronizer enables PCs with XenClient Engine to download centrally managed virtual desktops and run them locally. By using the Synchronizer, IT can centrally back up user data through a secure connection whenever the user connects to the Internet, define security policies, disable lost or stolen PCs, and restore a user's virtual desktop on any XenClient-based device as a part of XenDesktop Enterprise or Platinum Editions or as a standalone product.

Use Cases

XenClient Enterprise includes features such as centralized one-to many management, strong endpoint security and policy management, high resiliency with fast disaster recovery, simplified migration to new operating systems and PCs, and integrated helpdesk independent of the OS. It is used by organizations to:

- Allow IT admins to deploy a single golden image to thousands of PCs, regardless of hardware or vendor type, to eliminate PC device management headaches
- Extend the benefits of desktop virtualization to offline laptops by allowing users the ability to work from anywhere while IT maintains security and centralized control
- Secure and back up corporate data through an encrypted local virtual machine with automated backup and remote kill
- Simplify remote infrastructure by minimizing WAN traffic and remote IT resources to reduce PC support costs in branch and distributed offices
- Create a single hardware-independent image that is propagated to all end users to minimize the cost and disruption of OS migrations
- Manage shared PC images for kiosks, labs and training facilities with a flexible workspace that reliably snaps back to a pristine state
- Repurpose existing PCs as thin clients to reduce capital costs and future-proof virtual desktops

Test Ideas

The below test ideas assume that a XenClient Synchronizer has been deployed and configured and that one or more XenClient Engine(s) have been deployed and registered with the XenClient Synchronizer.

Central Management
1. Build one or more VM's from ISO files or VM Images on the XenClient Synchronizer
2. Create local users and groups on the XenClient Synchronizer
3. Publish the VMs and assign users to the VMs
4. Register a XenClient Engine(s) to the XenClient Synchronizer
5. Perform a 'Check Now' operation in the XenClient Engine and observe how the XenClient Engine downloads and installs any VMs assigned to it.

Patching & Updating

1. Update a VM that has been assigned to an Engine by installing an application such as Google Chrome or Mozilla Firefox by using the Synchronizer Console.
2. Republish the VM to the Engine.
3. Perform a 'Check Now' operation in the XenClient Engine.
4. Disable the network connection in the Engine while the update is downloading. Confirm that the update pauses.
5. Enable the network connection and verify that the update picks up at the same point.
6. Verify that the updated VM downloads and installs to the Engine.

Backup & Restore

1. Perform some typical user activities on one of the VMs in the XenClient Engine, such as creating icons on the desktop or creating a new text file with Notepad.
2. Perform a backup of the VM.
3. Undo the user activities performed in Step 1 in the XenClient Engine.
4. Restore the VM backup from Step 2 and confirm that the user activities from Step 1 have been persisted in the restored VM (i.e. the icon/files are restored).

Policy Management

1. Hide the hypervisor with a single VM that boots automatically by setting an Engine policy.
2. Block certain types of USB devices by configuring a USB filter policy for a VM.
3. Enforce a Lockout policy and an Expiration policy for a VM.

Remote Wipe/Kill

Remote Kill

⚠ This will result in the target system becoming unusable and will require a re-install of the XenClient Engine to recover the system. **Perform this test last!!!**

1. Backup all VMs on the target XenClient Engine.
2. Verify that the backups created on the above system have been recorded successfully from the XenClient Synchronizer Console.
3. Using the XenClient Synchronizer, remotely kill the computer running the target XenClient Engine
4. To speed the simulation along, perform a 'Check Now' operation on the target XenClient Engine.

Restore and Re-provision

At this point the underlying hypervisor will initiate a self-destruct operation that involves removing all data from the system in a secure unannounced fashion. Eventually, the machine will just stop running.

Now it is time to restore the user by re-installing and re-registering the XenClient Engine with the Synchronizer.

1. Re-deploy XenClient Engine(s) on the wiped machine.
2. Re-register the Engine with the XenClient Synchronizer using the same user.
3. After download and preparation has completed, start the VM and verify that the customizations and user data are completely intact on the system.

XenClient Synchronizer Deployment

Requirements

Hardware Requirements

The host must be a standalone (physical) server or a virtualized machine.

- Processor: 2 GHz Intel Xeon Dual Core
- Memory: 6 GB RAM (8 GB RAM recommended)
- Storage: 200 GB 10K RPM
- Networking: Single Port 1 Gbps Ethernet NIC

Software Requirements

The Synchronizer server must have the following operating system and supporting software deployed before installation:

- Windows Server 2008 R2 or Windows Server 2012 (required for virtual appliances)
- Microsoft Hyper-V (6.0.6002.18005 or higher)

If Microsoft Hyper-V is not found, installation will halt and prompt you to install it. The required version is bundled with the operating system.

Browser Requirements

Once installed, access Synchronizer through a Web browser (Internet Explorer 7, 8 and 9 is supported). Browser requirements include:

- Windows XP with SP3, Vista, Windows 7 or Windows 2008/2012 Server OS
- Microsoft .NET Framework 2.0 installed
- RDP ActiveX control enabled

BIOS Settings
For Hyper-V to operate correctly, the server must have the following BIOS settings enabled:

- Virtualization: enabled (checked)
- VT-d: enabled (checked)

Prerequisites

Step	Instructions
1	**Install** Microsoft Windows 2008 Server R2 or Windows 2012 Server on a physical server
2	**Add the Hyper-V role** to the server. See Section '*Adding Hyper-V to Windows 2008 Server*' in the XenClient Enterprise Synchronizer Installation Guide for detailed instructions on how to do this. Windows 2012 Server streamlines this process, adding an option from the Server Manager Dashboard called **Add roles and features**. Follow the onscreen wizard to add the **Hyper-V role** to Windows 2012 Server.
3	It is recommended that you **turn off Enhanced Internet Explorer Security** during installation of the Synchronizer. Turning this off prevents messages from being displayed during installation, which greatly slows the installation process. Status of IE Enhanced Security under Windows 2008 Server R2 Status of IE Enhanced Security under Windows 2012 Server

	Disable the "Enhanced Internet Explorer Security" Windows Component by clearing the checkbox or toggling the radio button: For Windows 2008 Server R2: 1. In the **Server Manager** tree, expand the roles to display options associated with the **Hyper-V Manager** 2. In the Server Manager window, select the **Configure IE ESC** link 3. Find and clear the checkbox for **Enhanced Internet Explorer Security** For Windows 2012 Server: 1. In the **Server Manager** sidebar, select **Local Server** 2. In the Server Manager window, select the status of **IE Enhanced Security Configuration** (**On** by default) 3. In the dialog that appears, select the radio button **Off** for Administrators When you start Internet Explorer, it warns you: **Caution:** Internet Explorer Enhanced Security Configuration is not enabled After installation, enable Enhanced Internet Security by following these same steps and filling the checkbox (2008) or selecting the On radio button (2012).

4	If the computer running the browser used to connect to Synchronizer uses Windows XP, **ensure that the RDP ActiveX control is enabled**. Otherwise, it will not function properly. It is disabled by default.
	
	Even if the browser is not running Windows XP, the RDP ActiveX control might still be set to Disabled. If you experience a "Cannot install RDP ActiveX control" message, the control may be disabled.
	
	1. In the browser, click on **Tools > Manage Add-ons**.
	2. In the dialog box, find Microsoft RDP Client Control and make sure that it is **Enabled (Status column)**.
	3. If you cannot find the RDP ActiveX control in the Manage Add-ons dialog, see http://www.winhelponline.com/blog/error-remote-desktop-web-connection-activex-control-could-not-be-installed-after-installing-windows-xp-sp3/ to fix a known issue with this control on Windows XP. For convenience the information is provided below:
	   a) Click **Start> Run**
	   b) Enter **Regedit.exe**
	   c) Navigate to the following branch: **HKEY_CURRENT_USER\Software\ Microsoft\Windows\CurrentVersion\Ext\Settings**
	   d) Double-click **Settings** to expand the branch
	   e) Right-click **{7584c670-2274-4efb-b00b-d6aaba6d3850}** and choose **Delete**
	   f) Click **Yes** when asked for confirmation.
	4. If your browser does not have the RDP ActiveX Control, please use **Windows Update** to install it.

5	If you are installing on a server with a firewall, **ensure that the below ports are available**. If not, create a rule manually to open these ports. Synchronizer installer does not create a firewall rule to open the ports used by it. In some cases, Windows Firewall may need to be turned off.

	Port	**Use**
	443	Used by XenClient Enterprise Engines to communicate with XenClient Enterprise Synchronizer. If not open, clients cannot register or otherwise communicate with XenClient Enterprise Synchronizer.
	8443	Used by Administrator to communicate with XenClient Enterprise Synchronizer UI.
	2179	Used by Hyper-V Management Service Console (RDP)
	1433	SQL database port; this port must be open on the server hosting the database (which may or may not be the Central Server). All servers (central and remote) need access to this port to open connections to the database server.
	389	Non-SSL port for LDAP to AD
	636	SSL port for LDAP to AD
6	In addition, the following applications or services **must not be installed or have been previously running** on the Windows 2008/2012 64bit server: • Apache Tomcat Server • Microsoft SQL, MySQL or SQLEXPRESS Database Server/Services • Java Runtime Environment (JRE) If these are installed, the installation includes tools to remove them cleanly. ℹ️ Back up any data within these applications that you want to preserve.	
7	Download the XenClient Enterprise Synchronizer installer (if you don't already have it) from the Citrix My Account download portal or the XenClient trial page. ℹ️ You will need to register with either website to gain access to the Downloads page.	

Synchronizer Installation
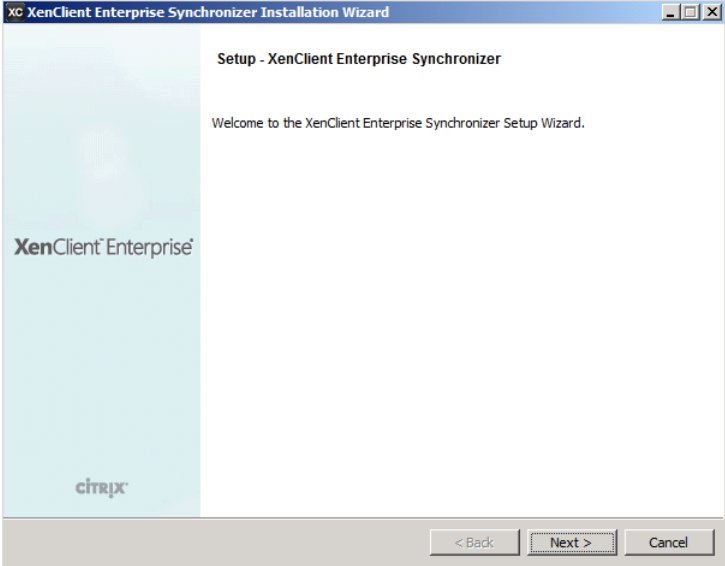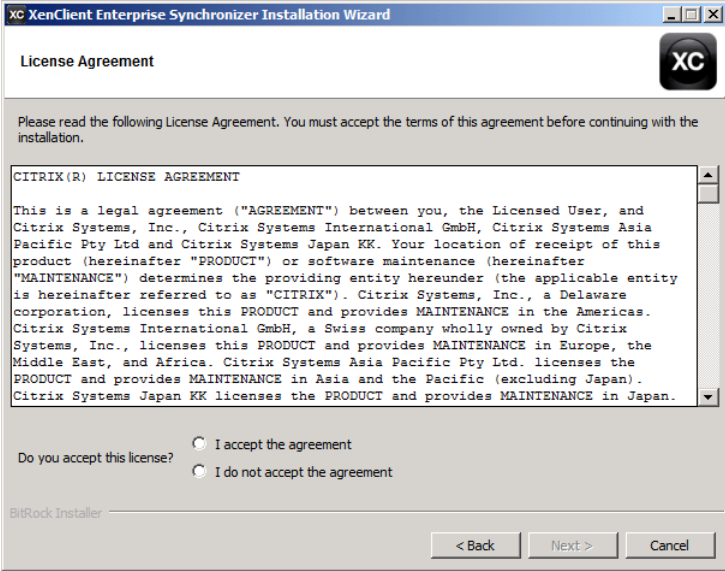
Start Synchronizer installation using the installation kit. For purposes of this installation, Synchronizer will be installed on a physical server with Hyper-V installed.
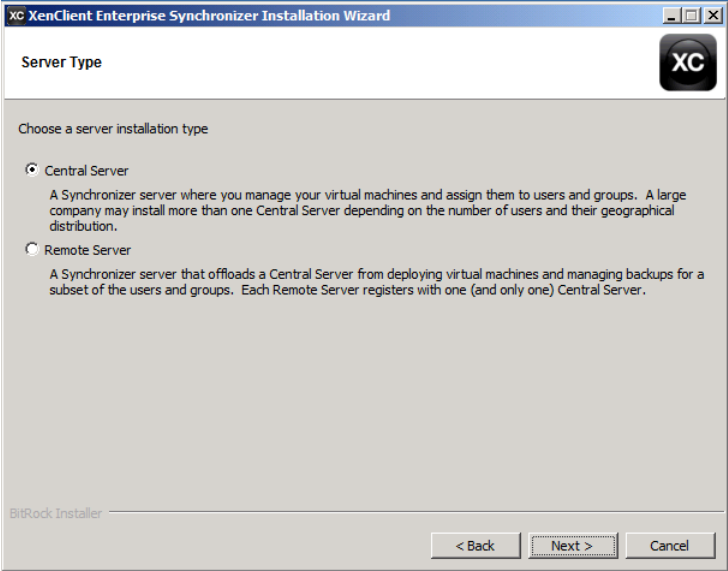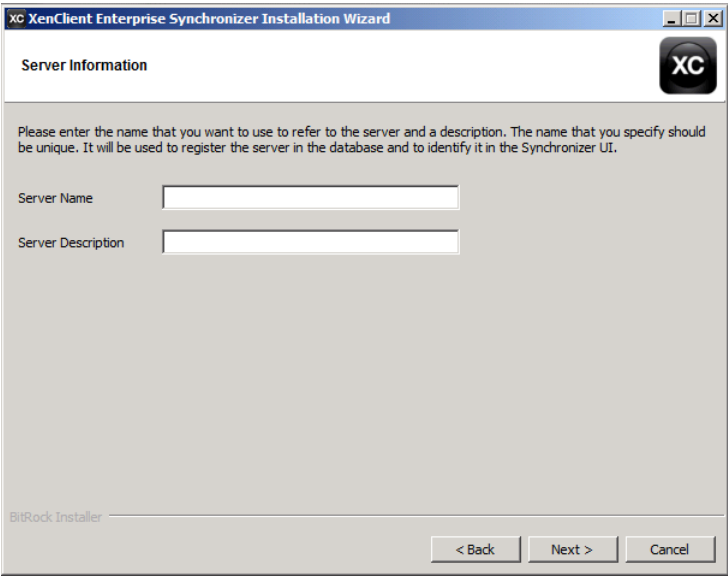
⚠️ Synchronizer requires administrative privileges to install successfully onto the Windows 2008/2012 Server operating system.

Synchronizer will set up the following as part of the installation process:

• Apache Tomcat Server 6.0
• Microsoft SQL Server 2005 Express (unless using database on another server)
• Microsoft SQL Server Management Studio Express
• Java Runtime Environment (JRE) 1.6.0_20
• Xenocode sample pack of Virtual Applications (optional)

Step	Instructions
1	The installation begins with a welcome screen: Click **Next** to continue.
2	The next screen shows the End User License Agreement for XenClient Enterprise Synchronizer. Please read thoroughly and choose **I accept the agreement**. Click **Next** to accept the agreement and continue the installation.
3	The Server Type screen appears. For Central Server installations, you manage your virtual machines and assign them to users and groups. For Remote Server types, the server offloads a Central Server from deploying virtual machines and managing backups for a subset of users and their groups.

	For the purposes of this installation, select the **Central Server** radio button and click **Next** to continue.
4	The Server Information screen appears. Enter the **Server Name**, and the **Server Description** then click **Next**.
5	The installer performs a few checks before proceeding: • It checks the host OS for Hyper-V role o If the host runs without a Hyper-V role, the installer interprets this as installing into a VM. It displays a pop-up telling you that it will perform a virtual appliance installation. • It checks that the server has adequate memory and storage space. A warning message is displayed if the server doesn't. The Installation directory screen then appears:
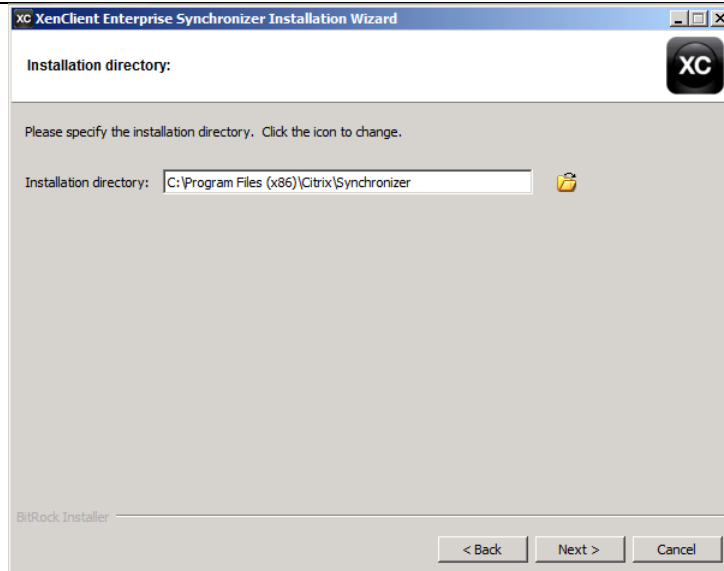
The default Installation folder is **C:\Program Files (x86)\Citrix\Synchronizer**.

Click **Next** to install in this folder or click the folder icon to select another folder.

Click **OK** to close the warning message. Citrix suggests freeing up enough disk space or selecting another server with adequate RAM.

| 6 | The next screen is the Tomcat configuration screen. Enter the Tomcat Install Directory, and ports for Tomcat. |
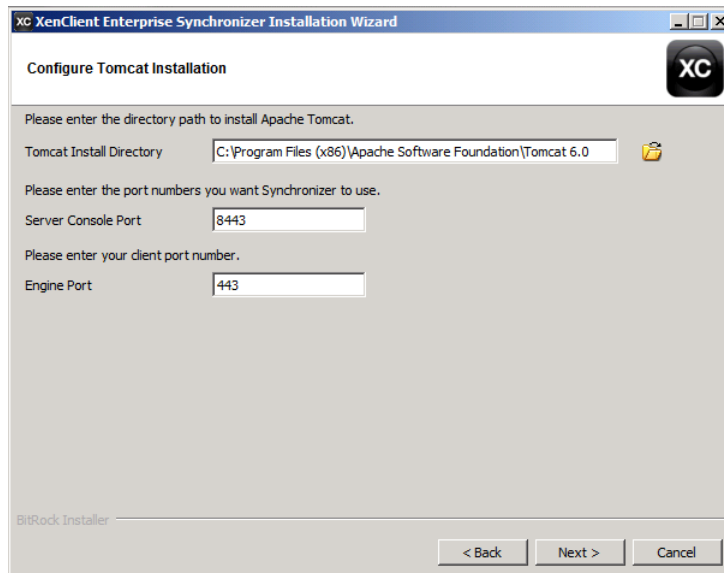
Additionally set the following information:

- **Tomcat Installation directory**: use the default of click the folder icon and browse to select another directory
- **Port for XenClient Enterprise Synchronizer**: Port used by XenClient Enterprise Engines and Administrators to connect to the Synchronizer.

	Default is 8443. • **Port for XenClient Enterprise Engines**: Port used by the Synchronizer to send virtual machines and queries to XenClient Enterprise Engines. Default is 443. ⚠ Both XenClient Enterprise Synchronizer and Tomcat have a /bin folder. **Do not install them in the same location**. Click **Next**.
7	The installer collects information for the Server's SSL Certificate. The installer creates a self-signed certificate to enable SSL on the XenClient Enterprise Synchronizer. You may install your own certificate obtained from RSA or other certificate authorities as described here: http://tomcat.apache.org/tomcat-6.0-doc/ssl-howto.html Enter the following for the SSL Certificate: • **Server name or fully qualified domain name**; use IP address if the name is not available. • **Company or organization name**. Do not include punctuation in the name. • **City** • **State/Province** • Select **Country** from the dropdown list Click **Next** to continue.
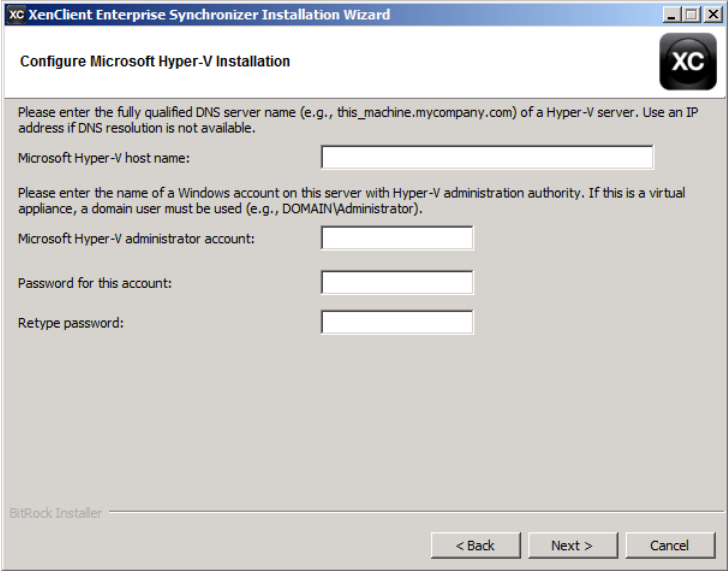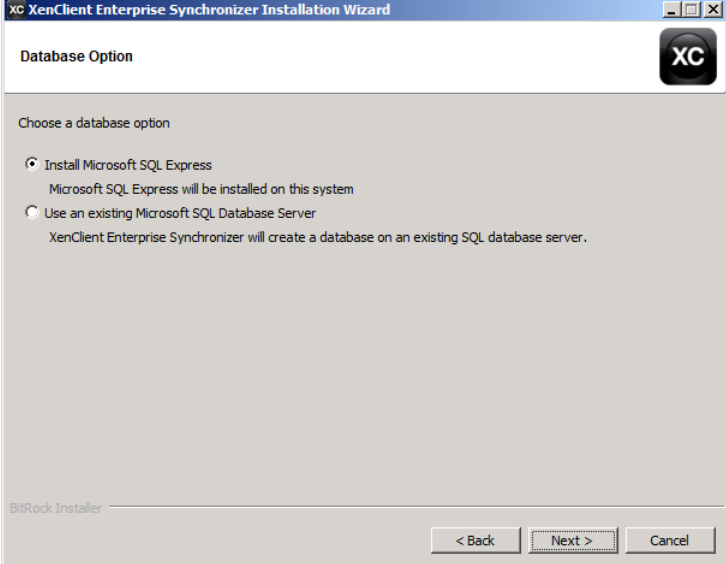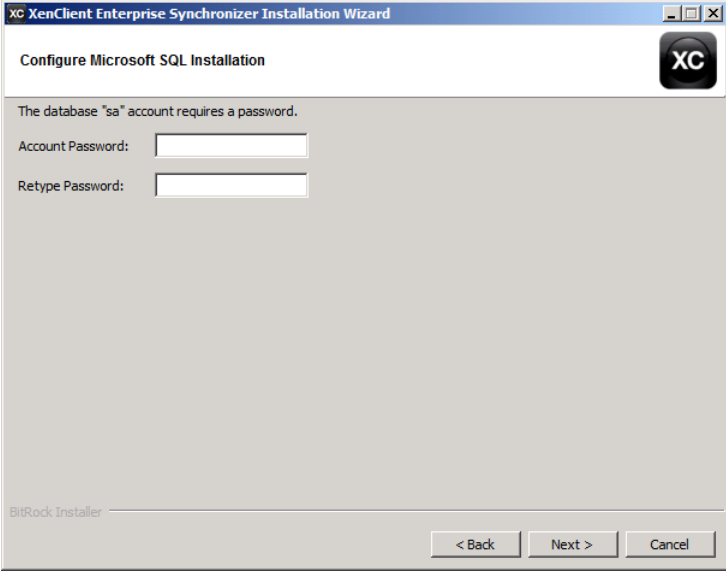
8	The installer collects information for Hyper-V. **XenClient Enterprise Synchronizer Installation Wizard** **Configure Microsoft Hyper-V Installation** Please enter the fully qualified DNS server name (e.g., this_machine.mycompany.com) of a Hyper-V server. Use an IP address if DNS resolution is not available. Microsoft Hyper-V host name: Please enter the name of a Windows account on this server with Hyper-V administration authority. If this is a virtual appliance, a domain user must be used (e.g., DOMAIN\Administrator). Microsoft Hyper-V administrator account: Password for this account: Retype password: BitRock Installer < Back Next > Cancel Enter the **user name** and **password** for the Hyper-V administrator account along with the fully qualified **Hyper-V host name**. Use an IP address if DNS resolution is not available. Enter a user name and password of an account with sufficient privileges to remotely manage Hyper-V. If this server is running inside of a VM, you may use the domain administrator account; if this server is installed into the base platform, you may use the local system administrator account. The installer checks that • the account and password exist • the account has local administrator rights If one or both of these validations fails, an appropriate warning message is displayed. Click **OK** and correct any problems with the account before continuing. Click **Next** to continue.
9	The Database Option screen appears. Synchronizer supports two database options; you can install Microsoft SQL Express, or use an existing Microsoft SQL Database Server.

	For the purposes of the installation, please choose **Install Microsoft SQL Express** and click **Next.**
10	For SQL Express on the host, the Installer collects information, including the database Administrator username and password. The database Administrator username must be **sa**. Enter the database administrator **username** and **password**. Click **Next**.
11	The Summary screen appears, listing all the information used to load Synchronizer and its supporting components:
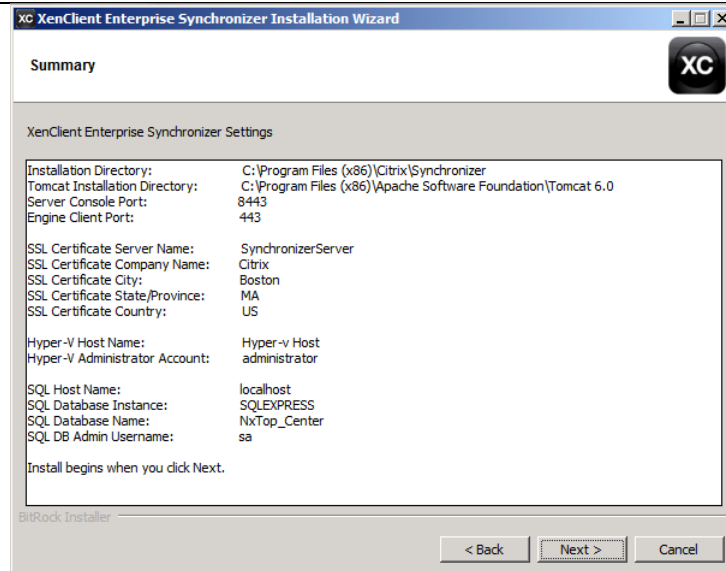
	  Review the information carefully. If you wish to change any of the values entered for configuration, click **Back** to browse to the appropriate screen, change the values, and then click **Next** until you return to this screen. Click **Next** to start the installation. To cancel the installation, click **Cancel.**
12	The components and Synchronizer are then installed on the server. Progress is displayed as each component completes. In the event of a failure during installation, correct the reported error. Then continue the installation from the point where it failed by restarting the installer. Installed components do not need to be reinstalled. When the software is installed, click **Finish**. The installer window will close. To complete Installation, you must restart the server.
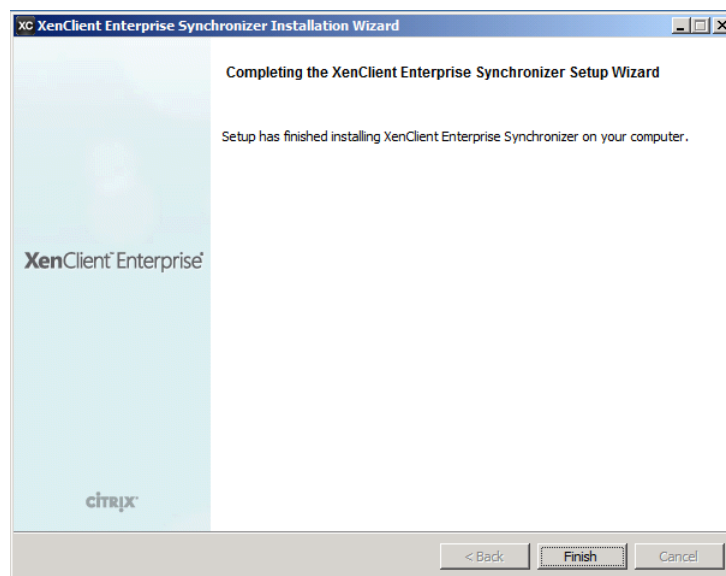
	After the server restarts, an icon for the **Synchronizer Console** appears on the server desktop.
13	**Verify connectivity** to the XenClient Enterprise Synchronizer: 1. Open a **Web browser**. 2. Browse to the XenClient Synchronizer **Management Console**: https://[servername]:8443/MgmtConsole *Note: You may also use the server's IP address if the server is not accessible via its name.* ⓘ If you cannot establish connectivity, consult your IT Administrator.

XenClient Synchronizer Configuration

Importing ISOs

An ISO is an installation file used to install operating systems and other software on a virtual machine. Synchronizer does not include the tools required to create ISO files. Your organization should select the tools you prefer, and create the ISOs to import into the Software Library as described below.

Step	Instructions
1	Copy the ISO into the import folder of Synchronizer (**C: \Program Files (x86)\Citrix\Synchronizer\File Import**)
2	Log into Synchronizer using a Web browser, and click **Software Library** in the navigation panel
3	Click the **Import** action. From the dropdown menu, choose **ISO**.
4	Enter a **Name** and **Description** to identify the item.
5	If the ISO is a CD/DVD, check the **OS Installation Media** checkbox.
6	Select the ISO from the dropdown box under **Specify file**.
7	Click **Finish**. The ISO is copied to the Synchronizer Library, and appears in the list of ISO Media. Once it is in the library, it can be used to create a VM.

Importing Virtual Machine Images

A Virtual Machine (VM) Image is a virtual copy of an installed operating system. A VM image is created from an installed operating system, including a (group) license. It is also called a Virtual

Hard Disk (VHD). The steps below give instructions on how to import a Virtual Machine Image into XenClient Synchronizer.

Step	Instructions
1	Copy the VHD into the import folder of Synchronizer (**C: \Program Files (x86)\Citrix\Synchronizer\File Import**)
2	Log into Synchronizer using a Web browser, and click **Software Library** in the navigation panel
3	Click the **Import** action. From the dropdown menu, choose **Virtual Machine Image**.
4	Enter a **Name** and **Description** to identify the item.
5	Select the VHD from the dropdown box under **Specify file**.
6	Click **Finish**. The VHD is copied to the Synchronizer Library, and appears in the list of Virtual Machine Images.

Creating Virtual Machines

A virtual machine (VM) is a container that is run on a computer by the Engine. In addition to the operating system and any installed applications, the VM may include virtualized applications and policies that control aspects of its operation, like backup, access, and USB use. When you create a VM, you are selecting and preparing the components for use.
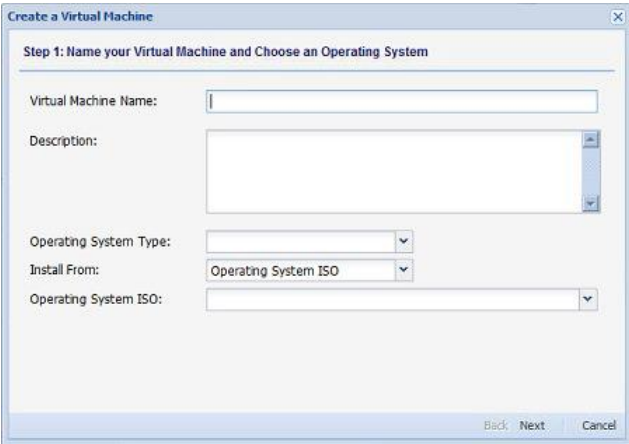
A virtual machine must include an operating system (OS). The operating system can be installed from an OS ISO file or from a VM image.
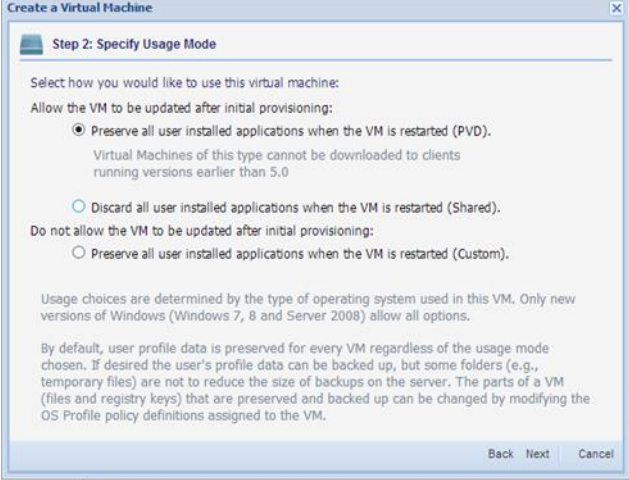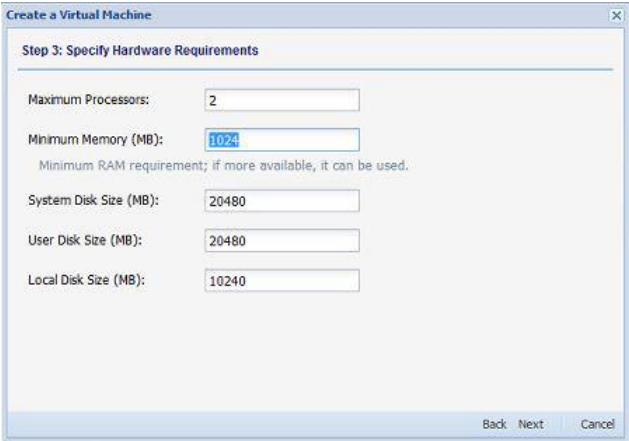
The steps below include creating a virtual machine, but do not include the steps required to assign a VM to users or groups, or to make a VM available to users. See section, Provisioning a User for these steps.
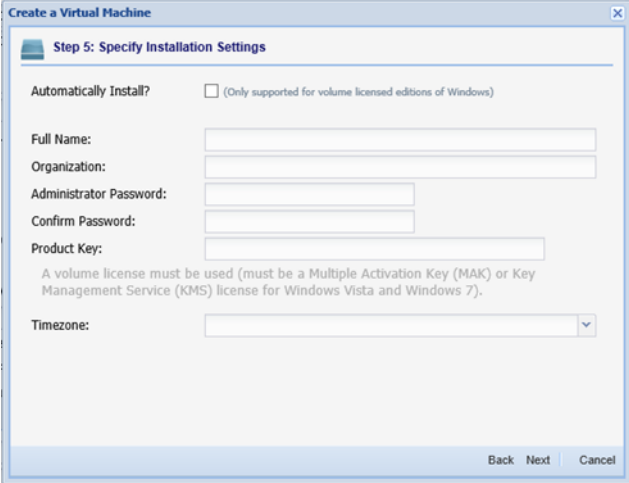
Once you begin to create a virtual machine, you can add, modify, or remove its components as needed without affecting users until the VM is published.

Consider the following before creating a virtual machine using the Synchronizer:

• Import the components to be used in the virtual machine into the Software Library. The components must include either an ISO or a VM image. See section, Importing ISOs or Importing Virtual Machine Images for how to import these components.

• Define the operating policies to be used. Policies are good practice, but are optional. Policies can be assigned to a virtual machine at a later point. See section, Policy Management on how to define policies.

Step	Instructions
1	Click the **Virtual Machines** navigation bar in the navigation panel. Then click **Create** in the Virtual Machines Actions panel.
2	Enter the **Name** and **Description** of the new virtual machine, and select the **Operating System Type** and source to **Install From** (ISO or VM image). Identify the specific **Operating System ISO** or **Virtual Machine Image** to use.
3	Decide if this virtual machine is **PVD**, **Custom** or **Shared**. Updates made to PVD and shared virtual machines are propagated to users assigned to that virtual machine; updates to custom virtual machines are not propagated once the VM has been downloaded.

	  Note: PVD virtual machines cannot be downloaded to clients running versions of XenClient earlier than 5.0
4	For all virtual machines, enter the **Processor**, **Memory,** and **Disk Size** requirements to be used by the image. This screen is automatically populated with default values.
5	Select the **default policies** to assign to the virtual machine. Policies can also be assigned to a virtual machine later.

6	For an ISO, decide whether to use **Automatic Installation**, and enter the information needed to run installation, including the **Administrator Password** and **Product Key**.
7	If you want to run this virtual machine immediately after creation, fill the checkbox and click **Finish**.

Creating Users

XenClient Enterprise allows administrators to create users to which VMs and policies are assigned. Users may also be organized into groups for ease of handling. See the next section, *Creating Groups* for more information on groups.
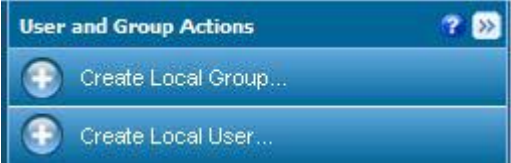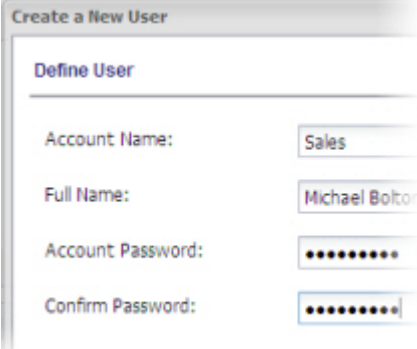
There are two types of users and groups: local users and groups and Active Directory users and groups.

Users are identified by color coded icons displayed in the navigation panel:

Local users and groups have an orange icon

Active directory users and groups have a blue icon.

The below steps give instructions on how to create a local user:

Step	Instructions
1	Click **Users** in the navigation panel.
2	Click the **Create Local User** action. **User and Group Actions** Create Local Group... Create Local User...
3	In the **Create a New User** screen, enter the required information: the **Account** and **Full Name** of the user, and the **Password** (including **Confirmation**). **Create a New User** **Define User** Account Name: Sales Full Name: Michael Bolton Account Password: ••••••••• Confirm Password: •••••••••
4	Click **Finish**. The user appears in the Users section of the tree.
5	To assign the user to a Group, click on the **Groups** tab for that user and select one or more groups to assign to the user. See the next section, *Creating Groups* for how to create a Group.
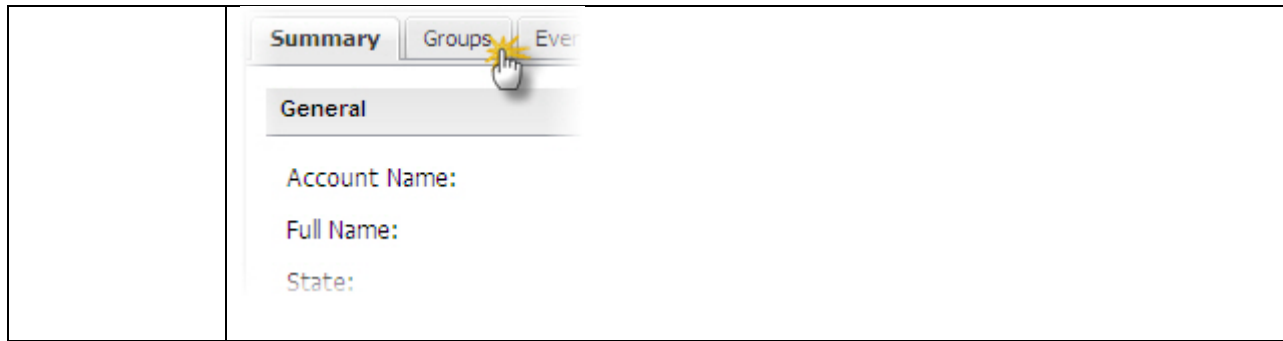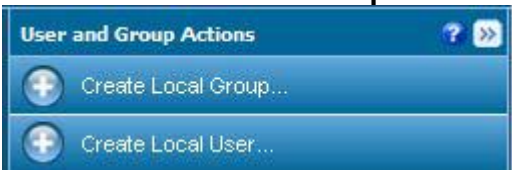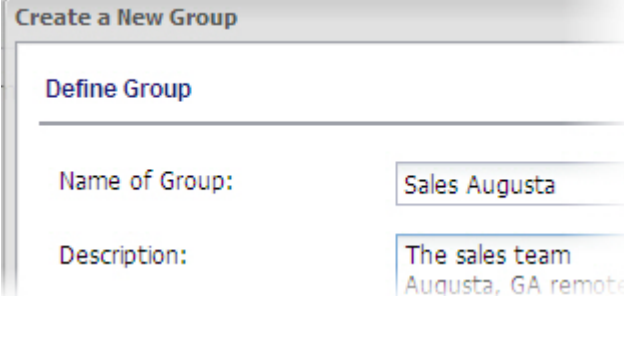
Creating Groups

Individual users can be organized into Groups to ease the handling of large numbers of users. If a VM or policy is assigned to the group, it is assigned to each member of the group as if it had been assigned to each user in that group individually.

If your organization uses an Active Directory (AD) for user identification, the AD organization can be imported into the Synchronizer and used to recognize your existing users in their organizational units. Groups can be local groups or AD groups.

The below steps give instructions on how to create a local group:

Step	Instructions
1	Click **Users** in the navigation panel.
2	Click the **Create Local Group** action.
3	In the **Create a New Group** screen, enter the **Name** and **Description** of the group and click **Finish**.

4	Click on the Users tab. Select the checkbox for each user you want to assign to the group. Alternately, clear the checkbox to remove the user from a group. See the previous section, Creating Users for how to create a user.
5	Click **Save** in the upper right portion of the workspace to apply the changes.

XenClient Engine Deployment

Requirements

Hardware Requirements

XenClient Enterprise Engine runs on a wide variety of business-class computers. Hardware requirements include:

• Intel or AMD dual-core processor with Intel-VT (VT-x) or AMD-V hardware virtualization technology.

Intel provides a tool to determine if the chip in your computer supports virtualization: http://processorfinder.intel.com/.

• 2 GB RAM; Citrix strongly recommends 4 GB to facilitate running multiple virtual machines simultaneously).

• 60 GB free disk space; running multiple operating systems may require significantly more disk space.

If you install onto the whole disk, the XenClient Enterprise Engine uses the full hard drive, replacing any natively installed operating systems and files. The whole disk is available for the XenClient Enterprise Engine and any virtual machines.

BIOS Settings

To support the Engine, the system must support virtualization. BIOS settings must also be configured to match the following criteria:

 • Virtualization: enabled (checked)

- VT: enabled (checked)
- Trusted Execution: off (unchecked)
- For Lenovo computers only:
  - Timer wake with battery: enabled

Compatibility Check

Run the Citrix XenClient Enterprise Platform Utility to find out if your Windows laptop or PC is compatible with XenClient Enterprise. The utility runs on Windows XP, Vista and Windows 7. System information will be sent securely to our database so there is no need to email any files.

1. Download the XCE_Check zip file
2. Expand the zip file
3. Run XCE_Check.exe

No software is installed on your PC.

Prerequisites

Step	Instructions
1	**Download** the XenClient Enterprise Engine Installation **ISO file** (if you don't already have it) from the Citrix My Account download portal or the XenClient trial page. You will need to register with either website to gain access to the Downloads page. In some cases it may be necessary to check the validity of the ISO file by verifying the MD5 checksum. A number of freeware tools are available for calculating and comparing MD5 files (for example: http://download.cnet.com/MD5-Checksum-Calculator/3000-2092_4-10964258.html).
2	Use the UNetbootin utility or comparable utility to **create a USB installer** from the ISO. You should have at least a 2GB USB stick in order to install the Engine. You can install the XenClient Enterprise Engine either through a USB memory stick, PXE Boot, or by installing from a CD or DVD. For purposes of this installation, the Engine will be installed through a USB memory stick. See the XenClient Enterprise Engine Installation Guide for how to install the Engine using PXE Boot or from CD/DVD media.

Step	Instructions
3	**Backup data** from the computer that you will be installing XenClient Engine on. The XenClient Enterprise Engine can be installed either onto the whole disk, or into unallocated space on a partitioned disk (dual boot). If you install onto the whole disk, the Engine uses the full hard drive, replacing any natively installed operating systems and files. The whole disk is available for Engine and any virtual machines. If you install into unallocated space on a partitioned disk, you need to use a disk partitioning tool to remove space from existing partitions. The Engine is then installed into that unallocated space. The unallocated space must include enough space for the Engine and any expected virtual machines. The Engine co-exists with an existing operating system instead of replacing it. Only one operating system can be operational at a time for a dual boot environment. For the purposes of this installation, the Engine will be installed onto the whole disk. See section *Dual Boot Installations* in the XenClient Enterprise Engine Installation Guide for how to create a dual boot environment.
4	**Configure the BIOS setting** for the computer you are installing the Engine on to boot from USB media. First ensure that the computer's BIOS enables booting from USB media. If the boot order for the USB device is lower than local disk, or if it's not specified, select the boot order menu key, usually F12. ⊙ You can set your computer's boot sequence so that it boots automatically from any installed USB device. In the BIOS>BOOT configuration section, move the USB drive above the local disk in the machine boot order. ⚠ If you arrange the boot order so that the USB drive is the primary boot device, keep in mind that you must remove the USB stick containing the installer before you reboot the next time. **Failure to do so may result in re-installing the Engine!**

Creating a USB Installer

The following instructions assume that you are using the UNetbootin utility to create a USB installer for XenClient Enterprise Engine.

Step	Instructions
1	Open up UNetbootin and select **DiskImage**:

2	**Select** the ISO location:
3	Once you have selected the ISO location, use the **drop-down menu** to select the drive letter of the USB stick on which you are going to create the installer:
4	When you click **OK** you will see the progress of your installer being built. Once the build is complete, click **Exit**.
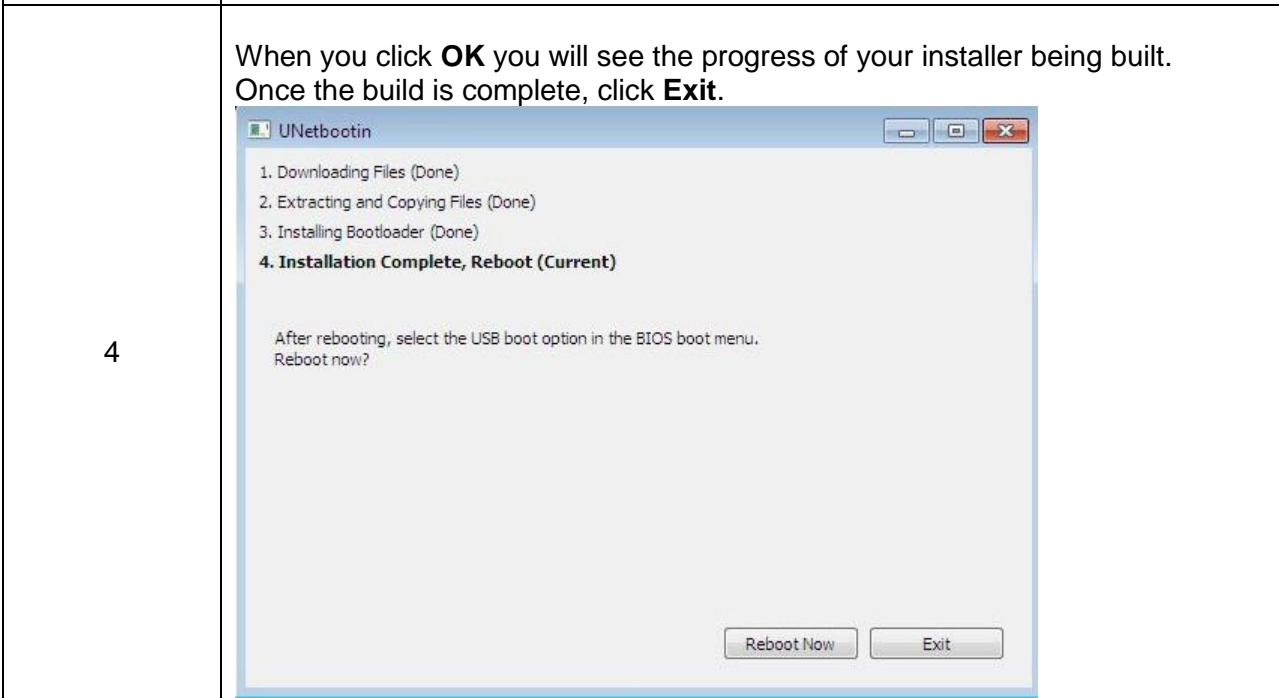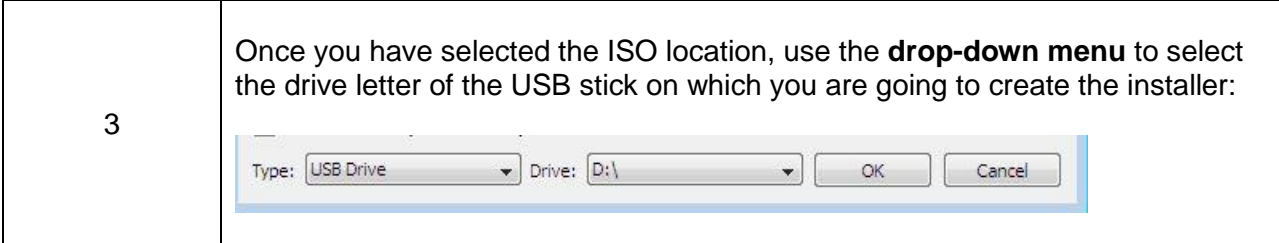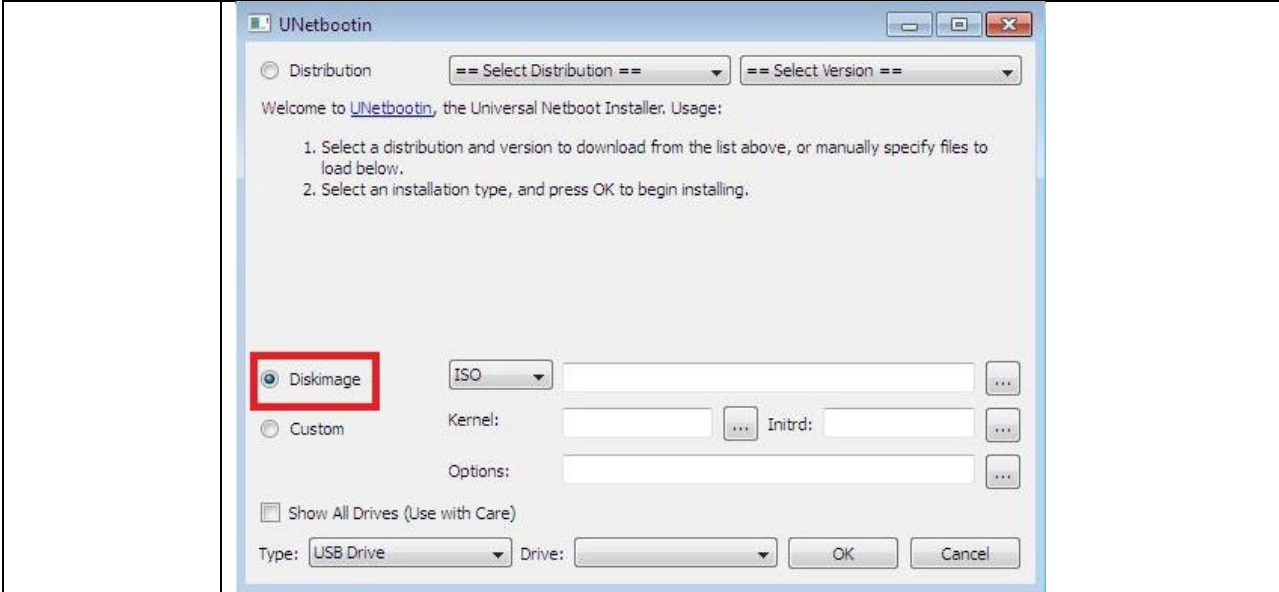
Engine Installation

To boot from the USB drive, the boot order must be modified so that the local disk is below the USB drive upon booting the system. See step 4 in the [Prerequisites](#) section above for instructions on how to do this.

Step	Instructions
1	Shut down the **computer**.
2	Plug the **USB drive** into an available slot.
3	Restart the **computer**.
4	Use the up and down arrow keys to **select a language** (keyboard) for installation and press the **Enter** key.
5	Read and accept the **end user license agreement**. The Engine installer will now scan the computer for previous versions of the Engine.
6	If you are installing over a previous Engine, you have the **choice to upgrade** the version or **replace** the old version, including all user information and XenClient virtual machines. For the purposes of this installation, please remove any old versions of XenClient Engine (if applicable).
7	Use the tab key to select **Entire Disk** (or Stop to end installation) and press **Enter** to install XenClient Engine on the entire disk.
8	Enter the **computer name**, and press the **Enter** key to advance to the next screen. This computer will be identified on XenClient Enterprise Synchronizer primarily with this name. To go back a step, use the Tab key to highlight **Back**, and press **Enter**.
9	Enter the **asset tag** for the computer, and press **Enter**.
10	Use the arrow keys to select whether to use disk encryption. For this installation, please choose the option to **use disk encryption**, and press the **Enter** key to move to the next screen.
11	Your selections are displayed along with a warning that if you continue with a full disk installation, all data on the disk will be erased. If the summary is correct, enter **yes** and press the **Enter** key to install the Engine.
12	The Engine is **installed**, with a progress bar displayed. Once installed, the computer **reboots**.
13	Verify connectivity to the XenClient Enterprise Synchronizer: 1. Open the XenClient Engine **Control Panel**. 2. Locate the **Wired** and **Wireless** networking Control Panel. 3. In the **Related Tasks** section of the Control Panel (located in the left

	panel of the interface), select **Test**.
	4. In the **Test Your Network Connection** screen, enter the **IP address** of the management server.
	5. Click **OK** to test the connection.

Engine Registration

XenClient Enterprise Engine supports the following registration models:

- Register this computer with a Synchronizer and assign a user
- Register this computer with a Synchronizer on behalf of another user
- Register this computer without a user
- Set a local username and password - If the Engine will not have access to a server, or, if registration is not desirable, one can take ownership by creating a local username and password to enable login and lock features.

For the purposes of this installation, we will register the computer to a Synchronizer and assign it a user.

Step	Instructions
1	From the Launcher screen of the XenClient Enterprise Engine, click the **Registration icon** in the lower left portion of the UI:
2	In the Registration Wizard screen, select the **Register this computer and assign a user** radio button. Click **Next**.
3	Enter the **server name** and specify the **username** and **password** for the user.
4	Any VMs assigned to that user should begin to download and install on the XenClient Engine.

Mounting PV drivers

Paravirtualized (PV) drivers are used to accelerate the audio, USB device handling, keyboard, mouse, and graphics for Windows-based virtual machines.

To install PV drivers once the Windows installation has completed:

Step	Instructions
1	In the Launcher screen of the XenClient Enterprise Engine, select the **virtual machine icon** to display configuration options. ⓘ Placing the cursor on a virtual machine icon displays a list of control options.
2	Select the **Tool** icon to display the virtual machine control panel.
3	In the lower left portion of the control panel, select **Mount Paravirtualized Drivers** in the Related Tasks portion of the interface. ⓘ The virtual machine must be running when mounting PV drivers. Click the **OK** button in the popup box.
4	Access the Windows virtual machine (click the **VM** icon, or use hot keys **Ctrl+Up** arrow).
5	In the Windows VM, click **Computer** from the Start menu where a new CD drive will appear, labeled **XenClient Drivers**. ⓘ It may take a few seconds to display the XenClient Drivers label.
6	Double click the **XenClient Drivers CD drive** icon, then select the **PV drivers executable file** (.exe file) to start the XenClient PV Drivers installation.
7	Follow the steps in the installation wizard to install the PV drivers.
8	Restart the virtual machine once the installation is complete; from the Launcher screen, select the start option (you may have to stop the VM prior to restart).
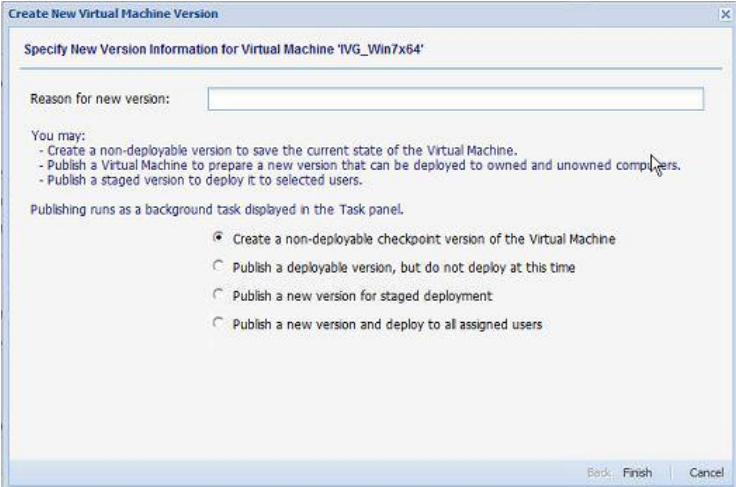
Provisioning a User

When provisioning a new user, a local or AD user must first be created. See section, Creating Users to learn about this process. A VM must then be published (or republished) and assigned to that user. The sections below describe how to do this in XenClient Synchronizer.

Publishing a Virtual Machine

Publishing a virtual machine makes it available to users that have been assigned that VM. Publishing makes a VM a virtual ready-to-run desktop. You can publish a new VM or republish an updated existing VM. See section

When you first publish a new VM, it has no assigned users, and it must be created and published before you can assign users to it.

Step	Instructions
1	Click **Virtual Machines** in the navigation panel and select the VM to publish.
2	In the Actions panel, click **Version/Publish.**
3	The **Create New Virtual Machine Version** window appears. Enter a **reason** for the publish. The reason is displayed in the list of versions for the VM. Select the type of publish: **Non-deployable** - use this to save an interim check point while working. The VM can be returned to this point if later changes are not satisfactory. **Deployable** (but not deployed) - this is a version that is ready for use,
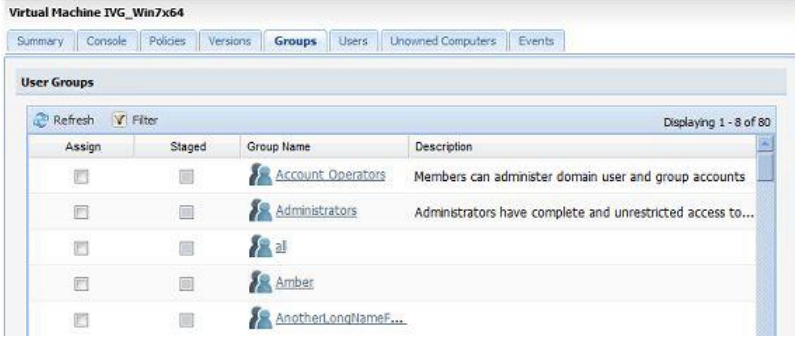
	but is not automatically distributed to assigned users. Use this to test a version before releasing it to users. It can be later deployed using the Deploy action on the version of the VM.
	• **Staged** - this is a version that is deployed to selected users. Use this to release a version to selected users. Click here for details.
	• **Deployed** - this is the version to be distributed to assigned users (assigned the green bar)
	A diagnostics package is created in the event of a failure during publish. To create a diagnostics package in any event, fill the diagnostics checkbox (applicable for all types except non-deployable publishes).
	Click **Finish**.
	The newly created VM is published. Next, assign users to this VM. See the next section, Assigning a User for how to do this.

Assigning a User

Once a virtual machine has been published in a deployable version, it is ready to be assigned to one or more users. Once assigned, when the user's Engine contacts Synchronizer, it downloads any updates to the user's assigned virtual machines.

If a virtual machine is assigned to a group, it is assigned to all users in that group.

To assign a VM to user(s):

Step	Instructions
1	Click **Virtual Machines** in the navigation panel and find the virtual machine to assign.
2	Click on the **Users** or **Groups** tab (depending on if you want to assign the VM to a user or a group). Fill the checkbox of each Group or User you want to assign the virtual machine. Users or groups already assigned to that VM already have a checkbox.

Step	Instructions
3	After you make your changes, click **Save**. The current **published and deployable** version or **staged** version of that virtual machine is sent to the selected users or all members of a selected group.

Patching & Updating
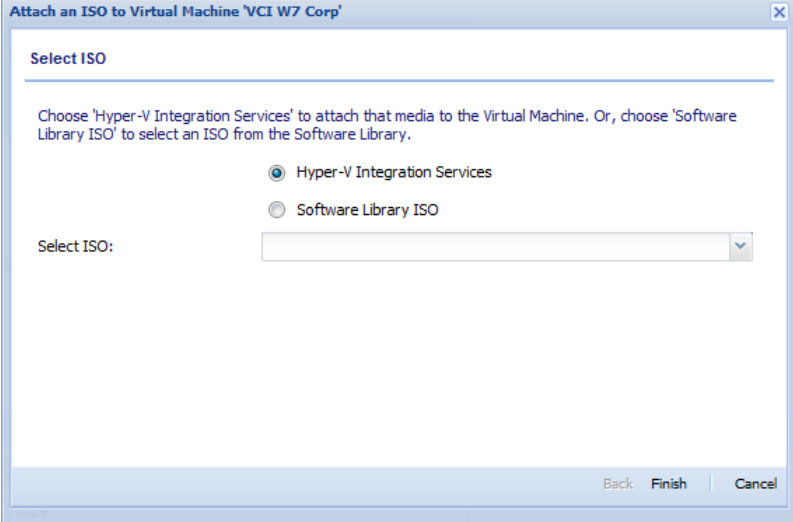
Attach ISOs

You can attach an ISO file to a virtual machine. An ISO file is a single-file image of a CD/DVD installation or data disk. Attaching an ISO file to a virtual machine creates a virtual CD/DVD drive within the virtual machine. Once the Attach ISO action has taken place, proceed with accessing the virtual CD/DVD drive as you would normally. Installing software from an ISO file is the same as any installation of software to a VM base image.

The VM does not have to be running when you attach an ISO file. However, if the ISO includes an autorun file, the VM needs to be running with a user logged on to automatically start the autorun file.

An attached ISO is listed on the virtual machine's Summary tab. You can only attach one ISO file to a virtual machine at a time.

Step	Instructions
1	Click **Virtual Machines** in the navigation panel, and select the virtual machine you want to attach an ISO file to.
2	In the Actions Panel, click the **Attach ISO** action.

Step	Instructions
3	The **Attach ISO Wizard** screen appears: Click **Software Library ISO**, and then **select the ISO** from the drop-down list.
4	Click **Finish**. The ISO can now be accessed as a virtual CD/DVD drive from the VM in the Console.
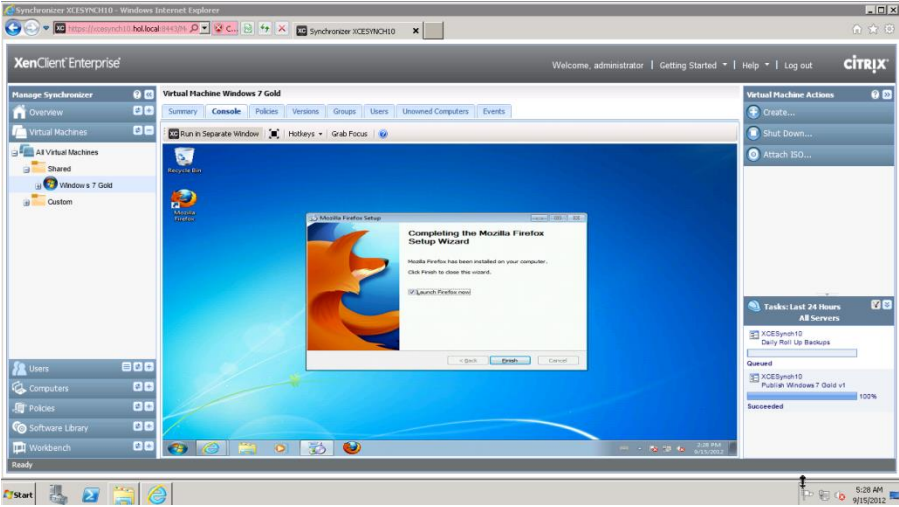
Update a Virtual Machine

To update an existing VM, make any updates needed and then publish it to make the new version available to assigned users. When the user's computer next contacts Synchronizer, it downloads the updated VM. When that VM is next started, the updated version is used.

Add Hyper-V Integration Services (HIS) to the VM to get additional services when running the VM in the Console window. For example, HIS provides a virtual mouse for VMs running in the Console. See section Install Hyper-V Integration Services for how to install HIS on the virtual machine.

To update a VM:

Step	Instructions
1	Click **Virtual Machines** in the navigation panel and select the VM to update.
2	In the Actions panel, click **Start.**

3	Click the **Console** tab. You should see the VM starting up.	
4	Log in to the VM and perform an update such as installing a new application. Recommendations include installing Mozilla Firefox, Google Chrome, or Microsoft Office. 	
5	After the update has been made, click **Shutdown** in the Actions panel.	
6	Make sure that the VM has been completely shut down and is selected. In the Actions panel, click **Version/Publish.**	
6	The **Create New Virtual Machine Version** window appears.	

Create New Virtual Machine Version

Specify New Version Information for Virtual Machine 'IVG_Win7x64'

Reason for new version: [   ]

You may:
- Create a non-deployable version to save the current state of the Virtual Machine.
- Publish a Virtual Machine to prepare a new version that can be deployed to owned and unowned computers.
- Publish a staged version to deploy it to selected users.

Publishing runs as a background task displayed in the Task panel.

○ Create a non-deployable checkpoint version of the Virtual Machine
○ Publish a deployable version, but do not deploy at this time
○ Publish a new version for staged deployment
○ Publish a new version and deploy to all assigned users

Back   Finish   Cancel

Enter a **reason** for the new version of the VM, which will be published The reason is displayed in the list of versions for the VM. A new version of the VM will be published.

Select the type of publish (Non-deployable, Deployable, Staged, Deployed)

If this VM has a staged version, Synchronizer asks what to do with the users currently using the staged version.
- Fill the first checkbox to move staged users and groups to the current published version.

A diagnostics package is created in the event of a failure during publish. To create a diagnostics package in any event**,** fill the checkbox for all types except non-deployable publishes.

Click **Finish**.
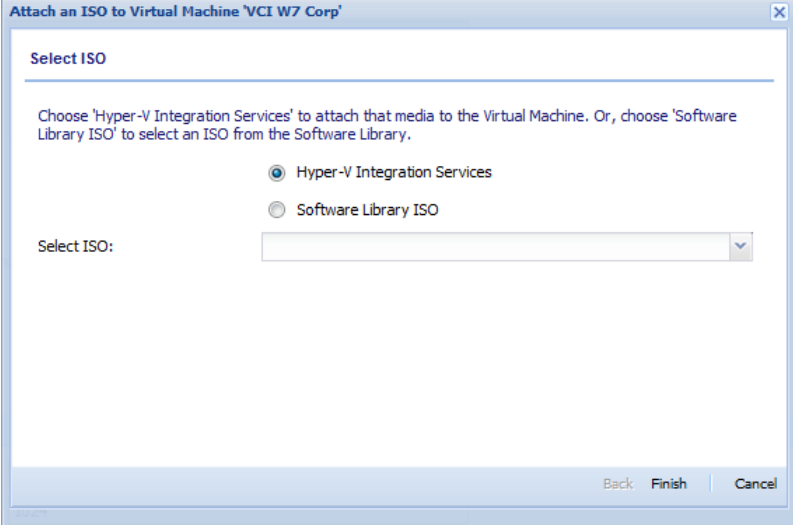
The newly created version is published. It is downloaded to assigned users the next time they contact the Synchronizer. See section Check for Updates if you would like to immediately update the VM.

Install Hyper-V Integration Services

To provide additional services such as a (virtual) mouse for virtual machines running in the Console, install Hyper-V Integration Services (HIS) on a virtual machine. To simplify this task, Synchronizer offers the ISO for Hyper-V Integration Services to attach to the VM.

ⓘ This functionality is specific to Windows XP and Vista VMs only.

Step	Instructions

1	Follow steps 1-2 in section Attach ISOs to start the **Attach ISO** screen.

2	The **Attach ISO Wizard** screen appears:
	
	Attach an ISO to Virtual Machine 'VCI W7 Corp'
	
	Select ISO
	
	Choose 'Hyper-V Integration Services' to attach that media to the Virtual Machine. Or, choose 'Software Library ISO' to select an ISO from the Software Library.
	
	    ◉ Hyper-V Integration Services
	    ○ Software Library ISO
	
	Select ISO: [_____ ▼]
	
	Back Finish
		Cancel
		
		Click the **Hyper-V Integration Services** radio button.

3	Click **Finish**. The Synchronizer will now install Hyper-V Integration Services on the VM.

Check for Updates

Step	Instructions
1	Go to the **Launcher** screen of XenClient Enterprise Engine and click on the **Activity Center** icon (the flag).
2	Click on **Check for Updates**
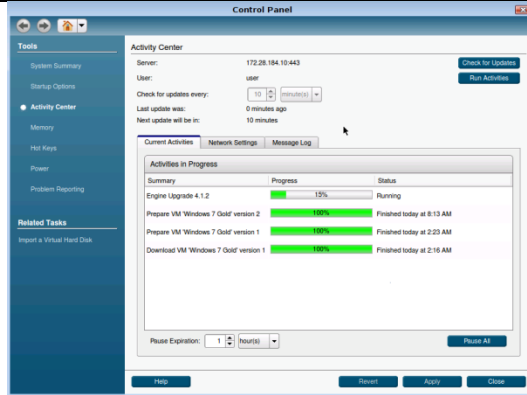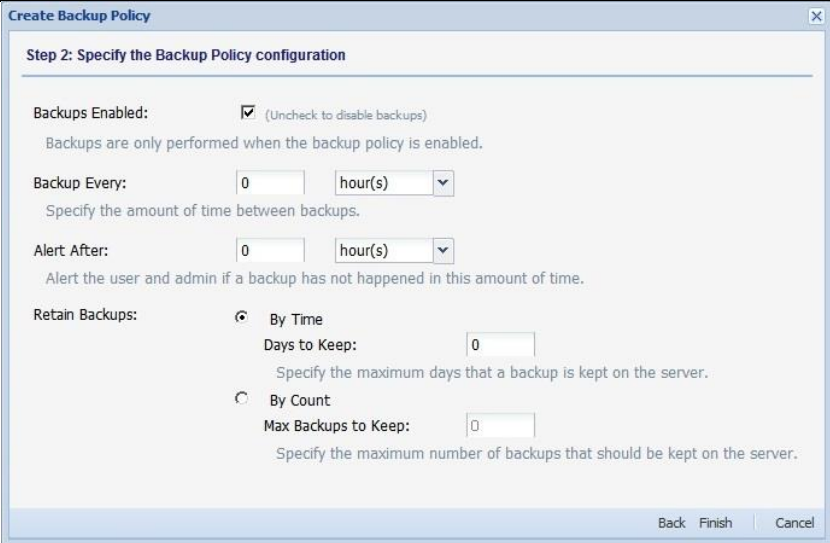
The Engine will check for updates from the XenClient Enterprise Synchronizer that it is registered to. Any new updates or policy changes will be pushed down to the Engine.

Backup & Recovery

Setting the Backup Policy

Before performing a backup for a VM, a backup policy must be defined and assigned to it. See the steps below for how to set the backup policy.

Step	Instructions
1	Follow steps 1-3 in section Creating a Policy to start the policy wizard for a new **Backup Policy**.
2	Select the **Backups Enabled** checkbox to enable backups. Specify the **interval between backups**; enter a value for the amount of time and use the dropdown menu to select the time format (days or hours). Indicate the **interval until an alert** is sent if a backup has not happened. Enter a value for the amount of time, and use the dropdown menu to choose the time format (days or hours). Determine a format for retaining backups on the Synchronizer. Select **By Time** or **By Count**, then enter a value for the period a backup is kept or the maximum number of backups to keep on the Synchronizer.

	Click **Finish**.
3	The backup policy appears in the list of backup policies under **Policies** in the navigation panel.
4	Click **Virtual Machines** in the navigation panel, and select the virtual machine you want the new backup policy to apply to.
5	Click on the **Policies** tab.
6	Click on the dropdown box for the VM's **Backup** policy and choose the new backup policy.
7	Click **Save** in the upper right portion of the workspace to apply the changes.

Backing up a VM

After setting the backup policy for a VM, back up of a VM can either be done based upon the interval set in the backup policy or backed up immediately. See the steps below for instructions on how to immediately back up a VM in XenClient.

Step	Instructions
1	See section Setting the Backup Policy to ensure that the backup policy for a VM has been set.
2	Click on the **Control Panel** icon (see below) in the **Launcher** screen of the XenClient Enterprise Engine.
3	Click on the **Virtual Machines** category.

4	Select the VM that you wish to back up.The **Virtual Machine Configuration** screen appears. Click **Backup Now** to back up the VM.
5	A popup message, **Snapshot successfully completed**, should appear. Click **OK** to close the popup dialog box.
6	Go back to the **Launcher** screen and click on the Activity Center icon (the flag). Verify that the XenClient Engine is uploading the backup by looking at the **Current Activities** tab.

Restoring a VM

The user data from a VM can be restored from the latest backup on Synchronizer. Restoration restores the whole user disk and replaces the VM. A user disk can be restored either onto the same computer or onto a different computer.

   • If a user's computer is lost or stops working properly, their VM is restored to a new computer.
   • If all or some of a user's data becomes corrupt or accidentally lost, their VM is restored to the same computer.

See the steps below for instructions on how to restore a VM to the same computer. See section, *Restoring a Virtual Machine from Backup* in the XenClient Enterprise 4.5 Administration Guide for more information on how to restore a VM from a backup.

Step	Instructions
1	Ensure that the data to be restored for a VM is available as backup. See section Backing up a VM for to ensure that a VM has been backed up.
2	Click **Users** in the navigation panel in the XenClient Enterprise Synchronizer and select the user for the VM to restore.

3	If the latest backup (top one on the list) will be restored, continue with step 4.
	
	If a backup from a previous date is needed, set the restore point to the correct backup:
	
	   1. Fill the **Restore Point** checkbox of the backup to use; any earlier backup dates are also filled in.
	   2. Click **Save**.
	
	The selected backup will be restored. If there are later backups existing,
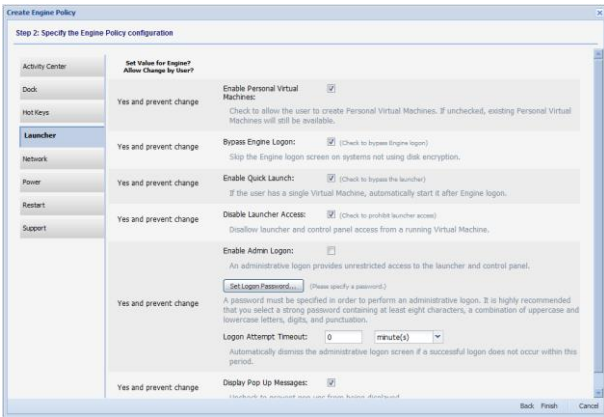
	backup processing will be suspended for this virtual machine.
4	Shutdown the VM to be restored.
5	**Unassign** the VM from the user. The virtual machine is removed when the computer next contacts Synchronizer.
6	Assign the virtual machine to the user. See section Assigning a User for information on how to assign a VM to a user. The virtual machine, including the user's restored data is downloaded and prepared for use when the Engine next contacts the Synchronizer.

User Experience

Hiding the Hypervisor

This functionality only works on a XenClient Enterprise Engine that does not have disk encryption enabled.

Step	Instructions
1	Ensure that you have a single VM installed and running on an instance of **XenClient Enterprise Engine** without disk encryption enabled.
2	Follow steps 1-3 in section Creating a Policy to start the policy wizard for a new **Engine Policy**.
3	Click on the **Launcher** tab in the **Create Engine Policy** wizard. Fill in the checkboxes for **Bypass Engine Logon**, **Enable Quick Launch** and **Disable Launcher Access**. Leave the rest of the configuration fields to their default settings.

	Click **Finish**.
4	Click **Users** in the navigation panel, and select the user you want the new engine policy to apply to.
5	Click on the **Policies** tab.
6	Fill in the checkbox for **Override default policy ["DefaultPolicyName"].** Click on the dropdown box for the user's **Engine** policy and choose the new engine policy.
7	Click **Save** in the upper right portion of the workspace to apply the changes.
8	See section Check for Updates to immediately enforce the new Engine policy on the **XenClient Enterprise Engine**. The Engine may need to be restarted for the new policies to take effect.
9	After the Engine has been restarted, confirm that the Engine automatically boots into a single VM with no **Launcher** screen shown. Also, you should not be able to switch between the VM and the **Launcher** screen.

In-Guest Controls

Virtual Machine Toggling

Step	Instructions
1	Ensure that you have multiple VMs installed and running on **XenClient Enterprise Engine**.
2	Press the **Ctrl + Down Arrow** keys simultaneously. The **Launcher** screen of the XenClient Enterprise Engine should appear, showing your VMs.
3	Press the **Ctrl + Up Arrow** keys simultaneously. The last running (active) VM should appear.
4	Press the **Ctrl + Right** or **Ctrl + Left Arrow** keys simultaneously. XenClient should toggle back and forth between the different VMs that are running on the Engine.

Step	Instructions
5	See **Hot Keys** tab in **Languages and Keyboards** in the **Control Panel** of XenClient Enterprise Engine for more keyboard shortcuts.

Network Connection

Step	Instructions
1	Ensure that you have the **XenClient Enterprise Engine** installed and has a working network connection. For these purposes, we recommend using a wireless network connection.
2	Click on the **Network Configuration** icon (Ethernet cable or Wireless icon) in the **Launcher** screen of XenClient Enterprise Engine.
3	Click on the **Disable** button to stop network connectivity. Click **Yes** on the popup box to confirm the action.
4	The **Network Configuation** icon should look like a red Ethernet cable to signify loss of network connectivity.
5	Switch to a VM and confirm that you can still run your desktop (VM) without network connectivity.
6	Click on the **Network Configuration** icon again. Click on **Enable** under Wireless to re-enable the network connection.

Policy Management

Policies control various aspects of how a virtual machine, a XenClient Enterprise Engine, or a XenClient Enterprise Synchronizer performs. Policies are defined in the XenClient Enterprise Synchronizer, and then assigned to VMs, Engines, or Synchronizers. Only one type of each policy can be assigned to a VM, Engine or Synchronizer at a time. If you create and assign a policy, it goes into effect immediately. VMs assigned to that policy receive it and change their behavior to conform to the policy at the next contact with the Synchronizer.

Some behaviors only act at virtual machine start up or shut down.

If an organization wants to change its policies in the Synchronizer, it can either:
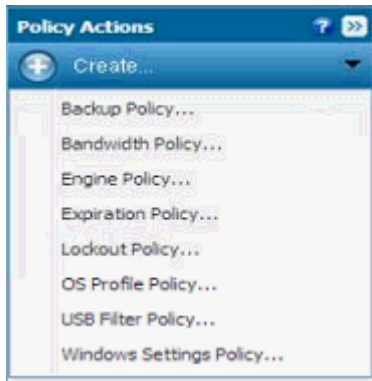
- Assign a different policy - original policy remains the same; new policy affects all VMs to which it is assigned.
- Modify the policy definition - changes policy definition, affecting all VMs currently assigned to that policy.

There are nine different policy types:

Policy	Description
Administrator Role	Allows an administrator to assign privileges based on an assigned role.
Backup	Provides policies that control the bandwidth, including options for setting upload and download throttling.
Bandwidth	Sets the bandwidth policy for an IP or subnet (max bandwidth, time period, etc.).
Engine	Defines aspects of the behavior of the XenClient Enterprise Engine (rather than a virtual machine).
Expiration	Describes how long after initial use a virtual machine expires.
Lockout	Describes how long the computer can be out of contact with the Synchronizer before locking users out of the virtual machine.
OS Profile	Describes a set of rules for the operating system for describing special handling for applications, services, or other settings.
USB Filter	Describes what types of USB devices can be used on the virtual machine.
Windows Setting	Defines Windows-related policies, like logon parameters.

Creating a Policy

Before a policy can be set, it must be created. Define a policy using the below steps:
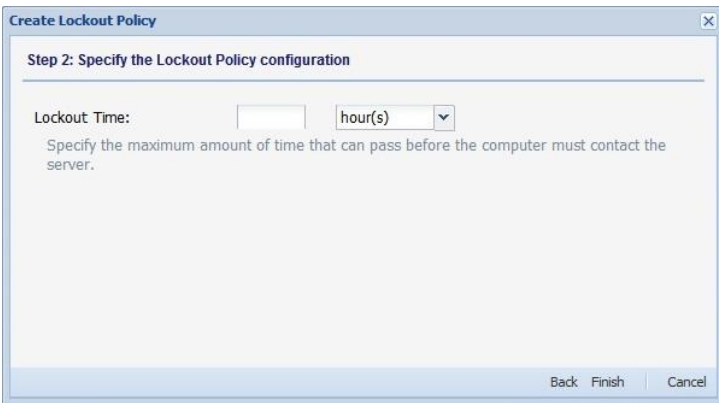
Step	Instructions
1	Click **Policies** in the navigation panel.
2	In the Actions Panel, click on **Create** and select a policy from the dropdown box.
3	All policies have the same first step in the Policy Wizard process. Enter the **Name** and **Description** for the policy. Click **Next** to continue with the policy

	wizard for the selected policy type.
4	Click **Finish** once the wizard for the selected policy has been completed.
5	The new policy appears in the list of policies for the respective policy type under **Policies** in the navigation panel.
6	For Virtual Machine policies, click **Virtual Machines** in the navigation panel, and select the virtual machine you want the new policy to apply to.
7	Click on the **Policies** tab.
8	Click on the dropdown box for the respective policy type for the VM and choose the new policy.
9	Click **Save** in the upper right portion of the workspace to apply the changes.

Lockout Policy

Lockout policies describe how long the computer can be out of contact with the Synchronizer before locking users out of the VM. This is often used to help IT maintain the security and management of computers by ensuring that users periodically connect to the Synchronizer.

See the steps below for instructions on how to define and enforce a Lockout policy.

Step	Instructions
1	Follow steps 1-3 in section Creating a Policy to start the policy wizard for a new **Lockout Policy**.
2	Specify the **length of time** a computer can go without contacting the server. Select the units (hours or days) and the number of those units. For these purposes, we recommend using **1 hour** as the lockout time. Click **Finish**.
3	Follow steps 5-9 in section Creating a Policy to assign the policy to the VM you want the new lockout policy to apply to.

4	See section <u>Check for Updates</u> to immediately enforce the new lockout policy on the VM in the XenClient Enterprise Engine. We recommend that you disable the network connection for the duration of the lockout time (to prevent the VM from contacting the Synchronizer). See section <u>Network Connection</u> on how to do this.
5	Verify that the VM is **locked out** once the lockout time passes. Reset the Lockout policy for the VM and check for an update on the Engine to unlock the VM.

USB Filter Policy

USB Filter policies may be enforced to prevent users from using unauthorized USB devices on specific VMs. This is useful for when organizations want to lockdown a VM and ensure that no corporate data is leaked through the USB devices.

See the steps below for instructions on how to define an USB Filter policy.

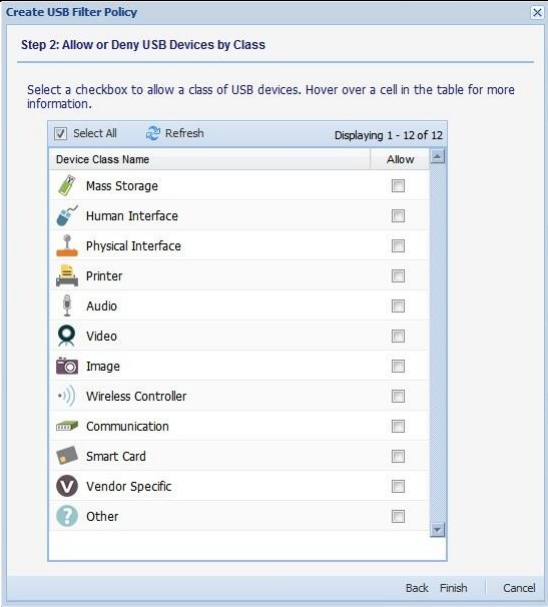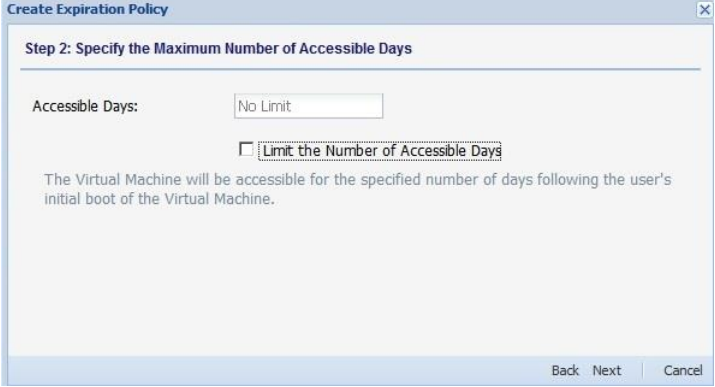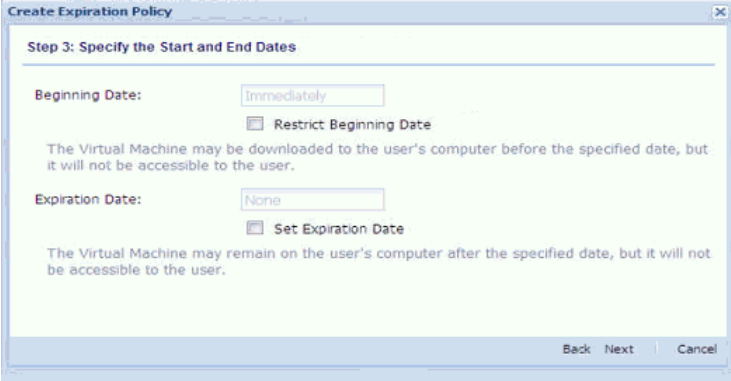| Step	Instructions
1	Insert a USB device into a computer running **XenClient Enterprise Engine**. We recommend using a USB memory stick.
2	Click on the **Control Panel** icon (see below) in the **Launcher** screen of the XenClient Enterprise Engine.
3	Click on the **Devices** category. Then select **Devices Manager.** Choose the VM you wish to use the USB device in under the respective dropdown box under **Assignment.** Click **Apply** to immediately apply the changes and click **Close**. The USB device should appear in the VM (typically under My Computer).
4	Follow steps 1-3 in section <u>Creating a Policy</u> to start the policy wizard for a new **USB Filter Policy**.
5	Click the corresponding checkbox for device types that are allowable on a VM. Hover over any of the device classes for a brief description. For these purposes, **do not** fill the checkbox for the USB device type that you inserted into the computer.

Click **Finish**.

6	Follow steps 5-9 in section <u>Creating a Policy</u> to assign the policy to the VM you want the new USB filter policy to apply to. For these purposes choose the VM using the USB device.
7	See section <u>Check for Updates</u> to immediately enforce the new USB policy on the VM in the XenClient Enterprise Engine.
8	Verify that the USB device disappears from the VM and that a message, **Removing USB device due to a policy change** appears in the Engine. Reset the USB filter policy (to the original policy) to use the USB device again. The USB device should reappear in the VM.
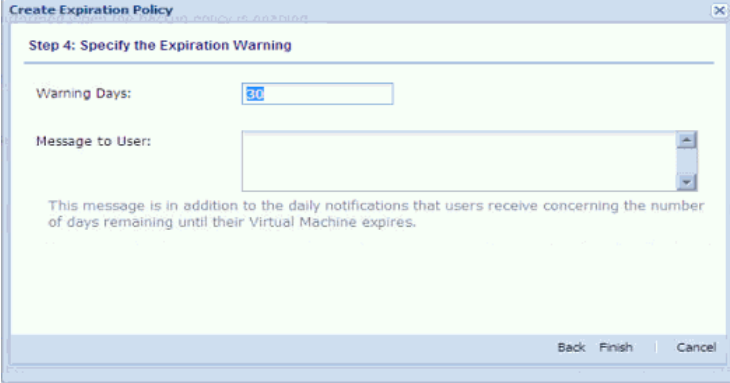
Expiration Policy

Expiration policies limit VM use to a number of days from first use. These policies are most useful for a contingent workforce of temporary workers or contractors who only need access to a VM for a specified amount of time.

See the steps below for instructions on how to define an expiration policy.

Step	Instructions
1	Follow steps 1-3 in section <u>Creating a Policy</u> to start the policy wizard for a new **Expiration Policy**.
2	You can fill the checkbox to limit the number of accessible days and specify the number of days to gives access to a VM. For these purposes, we recommend that you **do not** fill the checkbox or specify the number of accessible days.

	Click **Next**.
3	The Start and End Date screen appears in the wizard. You can fill one or both checkboxes to restrict by start date and/or end date. For each checkbox filled, select a date for the **beginning** or **expiration date**. The virtual machine is disabled before the beginning date and after the expiration date. For these purposes, we recommend filling in the **Set Expiration Date** checkbox and choosing an expiration date in the past (before today's date). **Do not** fill in the checkbox for **Restrict Beginning Date**. Click **Next**.
4	The Warning screen appears in the wizard.

Enter how many **days** before expiration to warn the user, and the **warning message** sent to the user. For these purposes, leave this screen as-is.

Click **Finish**.

Step	Instructions
5	Follow steps 5-9 in section Creating a Policy to assign the policy to the VM you want the new Expiration policy to apply to.
6	See section Check for Updates to immediately enforce the new Expiration policy on the VM in the XenClient Enterprise Engine.
7	Verify that the VM expires. Access to the VM should be disabled and it should show a status of **Expired.** The VM may need to be shut down or restarted before expiring. Reset the Expiration policy (to the original policy) to gain access to the VM again.
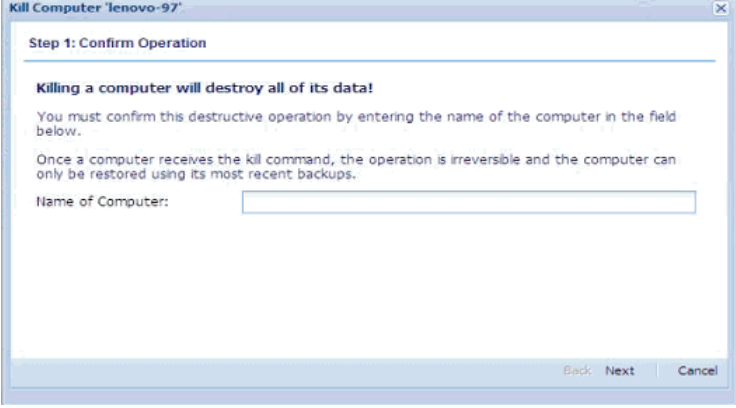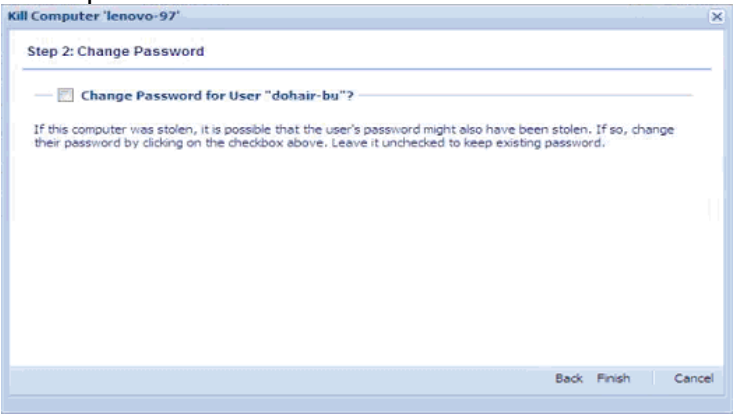
Remote Wipe/Kill

Remote wipe/kill severs the relationship between the user and the computer and erases the computer's hard disk. It instructs the computer to remove any virtual machines, virtual applications, policies, user data, and the XenClient Enterprise Engine from the computer. This is used most often when a computer has been lost or stolen.

⚠ **Do this last!!!! Remote Wipe/Kill will completely wipe the computer you are using.**

See the steps below for instructions on how to perform a remote wipe/kill

Step	Instructions
1	Click **Computers** in the navigation panel, and select the computer to kill.
2	Click on the **Kill** action.
3	The **Kill confirmation** pop-up appears.

	Kill Computer 'lenovo-97' ✕ **Step 1: Confirm Operation** **Killing a computer will destroy all of its data!** You must confirm this destructive operation by entering the name of the computer in the field below. Once a computer receives the kill command, the operation is irreversible and the computer can only be restored using its most recent backups. Name of Computer: [_____] Back Next Cancel Enter the **name** of the computer to be killed and click **Next**.

4	The second screen of the confirmation offers the option of changing a local user's password:
	
	Kill Computer 'lenovo-97' ✕
	
	Step 2: Change Password
	
	   ☐ **Change Password for User "dohair-bu"?**
	
	If this computer was stolen, it is possible that the user's password might also have been stolen. If so, change their password by clicking on the checkbox above. Leave it unchecked to keep existing password.
	
	                                                                Back Finish Cancel
	
	Fill the checkbox to change a local user's password.
	
	ⓘ This option will not affect a domain user. Reset a domain user's password through Active Directory.

5	If the local user's password was changed, fields appear for the new password. Enter and confirm the **new password**. Click **Finish**.
6	The computer's Summary tab is updated to display a status of **Kill - Queued**. At this point, you can click the **Cancel Kill** action to avoid the Kill action. In that case, the **Kill** action is canceled and not sent to the computer, and the computer can continue to be used. If not cancelled, when the XenClient Enterprise Engine next contacts the Synchronizer, it is sent the command to delete the virtual machines, user data, and XenClient Enterprise Engine. See section Check for Updates to immediately connect to the Synchronizer. Its status is updated to **Kill - Secured**, and the computer is moved to the **Lost or Stolen Computer** folder.

	If the user's password was changed, the new password must be entered when the user next logs in.
	The Synchronizer will not register a computer listed in the **Lost or Stolen Computer** folder. If recovered, the computer can use the **Recycle** action to be available for use.