# Table of Contents

About this Document .............................................................................................................. 4

**XenClient Enterprise Synchronizer Sizing** ........................................................................... 4
  Understanding VHD Disk Chains ......................................................................................... 4
  Processor Factors .................................................................................................................. 5
  Memory Factors ...................................................................................................................... 6
  Storage Factors ...................................................................................................................... 6
  Network Factors .................................................................................................................... 7
  Synchronizer Sizing Guidelines ............................................................................................ 8

**Windows 7 Best Practices** .................................................................................................. 9
  Improving Performance on Installed Components ............................................................... 9
  Preventing Unnecessary Component Installation ................................................................. 10

**App-V Client and XenClient Enterprise Interoperation** .................................................... 12

**Complex Virtualized Application Requirements and XenClient Enterprise** .................... 13

**Using SCCM with XenClient Enterprise** .......................................................................... 13
  XenClient Enterprise Windows Guests and the SCCM Client .............................................. 14
  Deploying the SCCM Client on XenClient Enterprise Dedicated Images .......................... 14
  Deploying the SCCM Client on XenClient Enterprise Shared Images ............................... 15
  The SCCM Client XenClient Enterprise Synchronizer OS Profile Policy ............................. 16
  Virtual Windows Instances in Active Directory ................................................................. 16
  XenClient Enterprise Hosts, Guest Windows Instances and SCCM Collections ................ 16
  Operating System Updates ................................................................................................. 17
  Application Deployment and Updates via SCCM ................................................................. 17
  Software Inventory ............................................................................................................. 17

**Remote Server Functionality** .......................................................................................... 18
  Personal Virtual Disk (PvD) ................................................................................................. 19
  About XenClient Disk Management Models ....................................................................... 19
  What is PvD? ....................................................................................................................... 19
  How is PvD implemented? ................................................................................................. 20
Copyright © 2014 Citrix All Rights Reserved.
Version: 2.1
Citrix, Inc.
851 West Cypress Creek Road
Fort Lauderdale, FL 33309
United States of America

This document is furnished "AS IS." Citrix, Inc. disclaims all warranties regarding the contents of this document, including, but not limited to, implied warranties of merchantability and fitness for any particular purpose. This document may contain technical or other inaccuracies or typographical errors. Citrix, Inc. reserves the right to revise the information in this document at any time without notice. This document and the software described in this document constitute confidential information of Citrix, Inc. and its licensors, and are furnished under a license from Citrix, Inc.

Citrix Systems, Inc., the Citrix logo, Citrix XenClient, are trademarks of Citrix Systems, Inc. in the United States and other countries. All other products or services mentioned in this document are trademarks or registered trademarks of their respective companies.

Citrix Systems, Inc. acknowledges all trademarks used in this document. Linux is a registered trademark of Linus Torvalds and Ubuntu is registered trademark of Canonical Ltd. Windows is a registered trademarks of Microsoft Corporation. All trademarks are the property of their respective owners.
About this Document

This document provides information about advanced XenClient Enterprise topics. In addition, it also provides an installation FAQ that includes information about common installation problems.

XenClient Enterprise Synchronizer Sizing

There are a number of factors involved in sizing Synchronizer installations, including:

- the number of distinct VMs (virtual machines)
- the number of Client systems and the expected number of VMs each client will run
- the network topology including WAN/LAN speeds
- the type of VMs being utilized and the chosen model for user backups

Each of these factors will impact Synchronizer installation in a number of ways, including:

- processor loading; each server will require a certain amount of processing power to support the registered client population
- memory usage; in general, the more memory a server has, the better it will perform but there are minimum requirements on memory size to support the number of Engine clients.
- storage; the storage needs of a Synchronizer Deployment can vary greatly depending on the deployment model chosen, number of VMs required, number of registered computers, and other factors
- network; part of the design of a Synchronizer installation is calculating bandwidth usage requirements and any limitations that should be applied to the XenClient Enterprise traffic, designing the server structure appropriately and configuring bandwidth management policies

Understanding VHD Disk Chains

VM definitions are made available to each client system. There is one VM for each distinct OS installation; these are personalized for each user when they are deployed to the client systems. VMs consist of:

- meta data describing the VM (OS type, resource allocation, publish history, etc).
- a chain of virtual hard drive (VHD) differencing disks that hold the system disk data. Each time a version of the VM is published a new VHD delta is pushed onto the disk chain to hold the changes for the next version. The bottom disk in the chain is a VHD dynamic disk holding the oldest maintained version of the VM; the Administrator can compress a set of the oldest existing versions into a single dynamic disk to manage the disk space consumed by the VM to manage
disk space consumed by the VM, improve performance, and reduce the bandwidth required to transmit the VM to the endpoint.

- local user backups; the client systems can optionally send backups for each VM deployed to the client back to the server to which it is registered. The user disks are stored as a chain of VHD differencing disks with a VHD dynamic disk at the base. Backups are created based on the backup policy pushing a new, empty VHD onto the top of the disk chain – the latest backup is then represented by the VHD differencing disk that was on the top of the chain before this. Incremental backups are discarded by merging the differences into the VHD dynamic disk at the bottom of the chain (so the bottom always represents the oldest backup).

**Processor Factors**

The processing requirements for a Synchronizer server are:

- creating and updating VMs (Synchronizer server only); the VMs are run under Hyper-V when they are being installed and updated. The Microsoft guidelines for Hyper-V VMs should be followed when calculating the processor requirements for these operations and should take into account the largest number of VMs that will be concurrently updated or published.

- publishing VMs (Synchronizer server only); the publishing process does cause the VM to be run under Hyper-V and also includes processing that is done in the Synchronizer OS instance itself. Since publishing is serialized by the product, it is only necessary to account for one VM at a time being published. The publish process consumes one processor core for the duration of the operation (typically 20-40 minutes per VM).

- deploying VMs (all Synchronizer servers); the server operates as a secure Web server to deploy images and take backups; this processing consumes approximately 3 Xeon class processor cores to saturate a single 1Gb/s link (which translates to around 800Mb/s actual throughput). Synchronizer servers provide this service for Synchronizer Remote Servers and for any Engines registered directly to Synchronizer Central Office Server. Synchronizer Remote Office servers only provide this service to registered endpoints.

- Control Functions (Synchronizer servers only); this component is responsible for managing the database and user interface for the XenClient Enterprise Installation and runs only in Synchronizer Central Server, though it is accessible via Synchronizer Console on Remote Office Servers.
**Memory Factors**

The memory requirements for Synchronizer server include:

- memory required to create and update VMs (Synchronizer Central Server only) – The Microsoft guidelines for Hyper-V VMs should be followed when calculating the memory requirements for these operations and should take into account the largest number of VMs that will be concurrently updated and published.

- publishing VMs (Synchronizer Central Server only); the VM is run on the server system during publish and so enough memory must be free to run the largest VM during publishing. This process is serialized so only one VM will be published at a time.

- Deploying VMs (all Synchronizer Servers); the normal Windows file system cache is heavily utilized when deploying VMs and so the more memory that is available the better the system will run.

The minimum memory size for Synchronizer is 6GB but increasing to 16GB or more will result in improved performance; also, consider memory requirements when rolling up backups (which applies to both central and remote servers).

**Storage Factors**

Each Synchronizer must have enough storage to hold the following:

- Each distinct VM; this includes the base system disk (which can grow to the configured maximum size of the disk) plus any delta disks for intermediate versions. Local retention policies will control the details of how many delta versions should be kept, but best practice is to manage the set of delta disks to keep the following:
  - A base disk that is the basis for the previous deployed version – when a new version has been successfully deployed, the existing versions from the base to the previous deployed version should be merged into a single version using Synchronizer.
  - All of the versions between this and the current deployed version and any version subsequent to this for an updated version under development.

In addition to the size of the disk, each VM is actually stored twice in the system; once uncompressed so it can be manipulated and then also a compressed copy is stored which is what is downloaded to other Remote Office Servers and clients. The compression ratio for these is typically around 50%; when calculating disk space requirements, the total disk space required must be multiplied by 150% to get the actual requirement.

When addressing storage, consider the following:

- All user backups for users registered directly to the server. There is a compressed user backup disk for each VM/User combination (for example, if you have 10 users each of which has 2 VMs
assigned to them then there will be 20 distinct backups. For each user backup, the following will exist:

- A base disk which can be up to the maximum size of the user disk volume. This is the oldest backup in existence.
- A series of delta disks that represent the maximum number of backups.

For example, if the maximum size of a user disk is 30GB and the backup policy indicates user disks should be backed up once per day and the last 7 days of backups are kept, then the following will exist:

- A full backup from 7 days ago which can be up to 30GB (uncompressed) in size
- 6 incremental backups for each of the subsequent days that hold the data modified by the user during each 24-hr period, again stored compressed all of which could theoretically consume approximately 30GB of disk space

When calculating how much disk space is required, a good rule of thumb is that the disks will be compressed by 50%.

**Network Factors**

The network topology has a strong impact on the design of the Synchronizer installation. The following are the most important factors to consider:

- **Slow speed (WAN) connections to remote sites.** The system will perform at its best if Synchronizer Remote Servers are installed at the end of slow speed links as this will mean that VMs are only downloaded once no matter how many clients there are at the remote site AND no backups will be sent over the WAN connection. This results in greatly reduced utilization of the WAN link.

  If it is not feasible to install a Synchronizer Remote Server at every remote location, it is still beneficial to install a server remotely to service a number of sites as this will reduce the load on the outgoing WAN connection from the central data center.

- **Multiple high speed segments.** If the network has multiple separate high speed LAN segments then it makes sense to install a Synchronizer Remote Server on each segment to maximize the number of clients that can be serviced concurrently and minimize the impact on the backbone network. For example, if there is a 10Gb backbone in the central data center and a series of 1Gb LAN segments distributed throughout the organization with small data centers on each segment connected to the backbone then a good implementation strategy would be to install Remote Servers in each satellite data center all connected to the 10Gb backbone and have the Central server in the main data center. This will result in data being distributed to the Remote Servers
very quickly and from there delivered in parallel to all clients on the various slower speed networks.

**Synchronizer Sizing Guidelines**

This section details specific guidelines that can be used to size a Synchronizer installation. It is based on some fundamental assumptions concerning acceptable timeframes for deploying VMs as follows:

- It is often possible to perform an initial deployment of all VMs to all users within a several day time period. This particular operation should only ever be done one time and once all clients have received their VMs, it is only necessary to send updates to those systems. In the future, initial deployments will only be done to small numbers of systems at any given time (as new users are added or existing users are migrated to new hardware to fix h/w failures). It therefore does not make sense to architect the installation to be able to do this one-time operation quickly as it will result in the systems being oversized for normal operation.

- Clearly it must be possible to keep up with the backup policies – so if the policy is to backup all clients every day, it must be possible to transfer the associated data to the Synchronizer servers within the 24hr period.

In addition, there are some assumptions in this document regarding the likely size of VMs and backups:

- A VM will likely be initially around 20GB uncompressed (around 8-10GB compressed) with an absolute maximum size of 50GB uncompressed (20-25GB compressed). A full Windows 7 installation together with Office 2007 Professional is approximately 18GB for example. If we assume weekly updates with a maximum of 4 intermediate versions created, each of which is 1GB, and retaining the last two published versions at most, the estimate of maximum required disk space per VM (including the overhead for storing both uncompressed and compressed) is then:

\[
(50 + 8*1) * 1.5 = \sim 90\text{GB}
\]

- User backups; as stated previously, the size of a user backup can be the full configured size of the disk plus the configured maximum number of incremental snapshots. So, if a user disk is configured to be a maximum of 30GB with daily backups maintained for 7 days and if we assume any given user can modify 1GB of data per day, then the maximum on disk size at the Synchronizer server can be estimated as:

\[
(30 + (6*1)) * 0.5 = \sim 20\text{GB}
\]

With these guidelines in place, it is possible to determine how many Synchronizer servers should be deployed to handle the end client load on the system as follows:
• A Central Server:
  o should have three Xeon class cores for each 1 GB LAN connection plus 1-2 cores for running Synchronizer server processing.
  o should have at least 8GB memory for the Windows instance running the Central Server image plus additional memory for creating, updating and publishing VMs (which should be greater than the largest expected memory size of any individual VM).
  o requires sufficient storage to hold all VMs together with backups for any users directly registered to the server.

• A Remote Server:
  o should have three Xeon class cores for each 1 GB LAN connection.
  o should have at least 8GB memory
  o requires sufficient storage to hold all VMs together with backups for all users that will be registered to the server.

Performance Test Results
The following performance information illustrates expected behaviour when determining the number of XenClient Enterprise clients that can be provisioned with a typical Windows 7 virtual machine within 10 minutes.

This test involved using a typical server running Synchronizer, in this case, a dual quad core (8 CPUs) server with 16 GB of memory and average disk drives. The Windows 7 VM image was approximately 8 GB uncompressed (3+ GB compressed).

**Within 10 minutes, 15 Windows 7 VMs were provisioned, which equates to 90 users in one hour and 2,160 users in one day.**

Windows 7 Best Practices
There are two categorical ways to improve performance on any deployed operating system. One category includes performance improvements of installed components, while the other includes preventing the installation and execution of unnecessary components.

Improving Performance on Installed Components
To improve the performance on installed components:

1. Install Windows Vista/7 with the latest service pack.

Citrix recommends that you install Windows with the latest service pack instead of installing a previously released service pack, then upgrading. For example, install Windows SP2 instead of
installing SP1 then upgrading to SP2.
2. Modify the installer partition table in Windows 7; delete the larger, second partition and
increase the size of the first partition to fill the disk.
4. Run all updates; reboot and repeat until all updates are installed.

Do not install Office Live Add-in and turn off auto-run of Windows Update; disable warning
messages related to Windows Update.
5. Turn off System Restore.
   A. Access the Control Panel > System and Security > System > System Protection screen.
   B. Click Configure.
   C. Select the Turn off system restore checkbox and click OK.

In some cases, disabling Remote Assistance and Remote Desktop is often recommended; Citrix
recommends that these be enabled – they permit an Administrator to remotely debug an OS.
While these abilities hinder performance, they provide a number of benefits.
6. Disable SuperFetch:
   A. Start > services.msc.
   B. Double-click SuperFetch.
   C. Click the Stop button to halt the service.
   D. Change the start-up type to Disabled.
7. Delete the EnableSuperfetch value. To delete the EnableSuperFetch value:
   A. Start > regedit.
   B. HKEY_LOCAL_MACHINE\SYSTEM\CurrentSetControl\Session Manager\Memory
      Management\PrefetchParameters.
   C. Double-click on EnableSuperfetch.
   D. Change the value data field to 0.
8. After disabling SuperFetch and rebooting, delete the contents of c:\windows\prefetch.
9. Run disk cleanup; cleanmgr (specify All Users and keep defaults).
10. Set recycle bin to 100 MB.
11. Turn off scheduled disk defragmenter; start disk defragmenter, configure schedule and uncheck
    the option.

**Preventing Unnecessary Component Installation**

Many installed components, like Sun’s Java or Apple’s Quick Time, install their own updater engines.
These components are not desired when running XenClient Enterprise.

The website appdeploy.com has information on how to customize application installations,
including the removal of unneeded components; each application has its own page of appdeploy.

Many of these installed applications have custom settings that seek to turn off the automatic update
settings of the applications – otherwise, each VM will check for updates and then try to install them,
only to discard the updates at the end of the session. You will update applications in the version on Synchronizer, and then publish that version to distribute the updates to shared VMs.

1. Import the Office 2007 ISO file into the software library. Attach the ISO to the running VM. Install Office 2007 and click customize, run-all-from-my-computer. You can customize it further for your environment.

2. Install Firefox and modify the %program files%\Mozilla Firefox\defaults\pref\firefox.js as follows (the default for these lines is true):

   pref("app.update.enabled", false);
   pref("extensions.update.enabled", false);
   pref("browser.search.update", false);

   For details, See Don’t make firefox go look for updates at:


5. Download the AdbeRdr9x_en_US.exe from the link in the confirmation email and save the file to your desktop.

6. Extract the adobe components using the command AdbeRdr9x_en_US.exe -nos_ne.

7. Download the Adobe Customization Wizard from:


9. Run setup.exe.

10. Install Adobe AIR 1.5 from http://get.adobe.com/air. Use the default values offered.

11. Install both versions (IE and Firefox) of Flash Player. Disable Flash Player’s automatic update.

12. Create or open the C:\WINDOWS\System32\Macromed\Flash\mms.cfg file in a text editor and add the following line: AutoUpdateDisable=1.

13. Save the mms.cfg file with UTF-8 encoding.

   For details, see http://kb2.adobe.com/cps/167/16701594.html.

14. Install latest Sun Java JRE. Create the following registry keys:

   - [HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Java Update\Policy]
   - "EnableJavaUpdate"=dword:0 "NotifyDownload"=dword:0 "NotifyInstall"=dword:0
   - "UpdateSchedule"=dword:0 "Frequency"=dword:0

   For details, see http://www.appdeploy.com/packages/detail.asp?id=1562.
15. Install VPN software. For full Cisco VPN client create an organization profile, for the SSL VPN the default profile should be downloaded with the client.

16. If iTunes is required for your environment, download iTunes from Apple.

17. After installation, disable iTunes update in the Apple Software Update program.

18. Disable iTunes update in the Apple Software Update program.

19. Disable Quick Time updates through its control panel.

20. In the Registry, set HKEY_LOCAL_MACHINE\SOFTWARE\Apple Computer, Inc.\iTunes\Parental Controls\Default\AdminFlags to 0x00000101.


22. Disable the version check by setting the registry value:
   - HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone\DisableVersionCheck to 1

   For details, see the [Skype’s Network Administration Guide](http://www.skype.com/business/).

23. Install your AV/Spyware Engine. Prior to publishing, verify that your AV services are listed in the ‘turn OFF before publishing and ON after NxPrep list’ to prevent extremely long publish cycles.

   For Sophos, do not turn on regular scans. Leave the default integrated scanning of all files opened intact. Run a full app and virus definition update.

Add additional corporate applications......

After all the applications have been installed, re-run Microsoft Update until nothing remains. Also remove all unneeded entries from:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

**App-V Client and XenClient Enterprise Interoperation**

The Microsoft App-V client is deployed as part of the central image in either VM shared or dedicated image mode. Once the virtual image is deployed with the App-V client, the virtual Windows instance is ready to utilize App-V virtual applications as they would on any other physical PC. All of the delivery methods mentioned above work well with XenClient Enterprise. XenClient redirects the locations for the App-V application cache, and virtualized application user preferences, to a location that is outside of the snap-back functionality and controlled through the default VM OS Policy. This means the virtual application and its settings are retained after reboots regardless if the VM image is in shared or dedicated mode. The virtualized application in a VM will operate the same way as it would if loaded on a physical Windows instance.
Complex Virtualized Application Requirements and XenClient Enterprise

In the App-V world, there exists classes of applications that need a device driver deployed locally or require interaction with several applications that need redundant sequencing of applications for the virtualized applications to properly function. XenClient Enterprise provides unique options to help with these issues.

Applications requiring device drivers can be sequenced and delivered, but the device driver can be added to the core VM image and deployed either with the core image or as an update layer. For example, Skype can use a Polycom speaker phone device; however it requires a device driver that is not part of Windows. The Administrator can add the Polycom device driver files to the device driver path in the centralized Windows image and deploy it utilizing the deployment and update capabilities. When the Polycom device is plugged in at the client, the device drivers are available for automatic loading and configuration. Once the App-V Skype instance is launched on the client, it will recognize and utilize the Polycom device.

In the case of a complex application environment, XenClient can deploy and update the non-virtualized applications as part of the centralized images. For example, a law firm has multiple applications that need to tie into a common version of Microsoft Office. Instead of sequencing Office in multiple virtual applications, it can be installed into the central Windows instance. As the virtual Windows image is deployed or updated, the Office version will be local and available to all virtualized applications. Each virtualized application can then take advantage of the local copy, however the Administrator still gets the benefit of only having to update the application in the image once from a single location.

This capability now gives the Administrator a greater level of choices in how they can deploy applications and their dependencies. Instead of having to take the dependency that falls out of App-V’s virtualization capabilities, break it out from the existing MSI, package it into its own MSI and use PCLM to deliver it to any number of desktops, the admin simply adds the component to the centralized Windows image and it is deployed to all the related desktops on the next update. This functionality greatly simplifies this process and extends the value of App-V.

Using SCCM with XenClient Enterprise

In order to understand the proper interactions between the two systems, it is important to understand how the client and its guest Windows instances are recognized. Since XenClient Enterprise is based on the XEN hypervisor, it isn’t recognized by Active Directory or the SCCM console directly. Therefore the management of the core Engine (client) must be performed through Synchronizer while the management of what is placed in the Windows guest instance can be controlled through SCCM.

The following steps will allow you to install a XenClient Windows OS instance from SCCM OSD:

2. Once the image is ready, create the Task Sequence Media following these steps: 
   - Make sure to select Bootable media
   - Select CD/DVD set
   - Select a location to save the ISO file in the Media File line
   - Click **Next**
   - Enable Unknown Computer Support
   - Finish filling in the record according to your company's policy
   - Click **Next**
   - Select the x64 Boot Image as the Media File
   - Select the Distribution Point to get the Boot Image files
3. Click **Next** twice and the Boot Image will be created in the save location.
4. Once created, copy the Boot Image ISO to the FileImport folder in the Synchronizer.
5. In Synchronizer, import the ISO by clicking on Software Library...Import...Fill out the Name of the ISO and select the Boot Image ISO from the drop down list...click **Finish**.
6. Create the VM; be sure to select the SCCM OSD Boot Image ISO as the installation media....
   Installation process.
7. Once the system boots, it will go through the standard SCCM OSD installation process as the physical machines using the corporate image.
8. Once the process is complete, the image is ready to have the SCCM client added and the any finishing touches completed.

**XenClient Enterprise Windows Guests and the SCCM Client**

The SCCM client must be installed on each golden image; however, it is not a requirement to add the client only to a fresh OS installation. Existing Windows images that have been either imported or previously existed in Synchronizer can have the SCCM agent added and deployed.

**Deploying the SCCM Client on XenClient Enterprise Dedicated Images**

In the case of deploying the SCCM client to VMs utilizing dedicated images, the admin is presented with a couple of options. The SCCM client can be added to the golden image itself as long as the image has not been previously deployed, since any changes to the core dedicated image represent a wholesale replacement of the deployed image and resets the targeted system's user state.

In this case, the admin follows the same recommended steps from Microsoft as if they were deploying an image via Ghost or other imaging tools. There are considerations around auto-discovery of Site Codes and ensuring that the proper security keys are made available to the client after the XenClient Enterprise equivalent of SysPrep is run after image deployment. The proper process is as follows:

   - Complete the golden image creation through the Synchronizer Console
• Install the SCCM client per your company’s best practices. It is recommended to use auto site discovery if the VM will be assigned to different sites codes.

• Copy the CCMDelcert.exe and Tranguid.exe tools from the SCCM Client Toolkit (http://www.microsoft.com/downloads/en/details.aspx?FamilyID=61e4e21f-2652-42dd-a04d-b67f0573751d) to c:\Windows\System32

• Install the SCCM client

• Run “CCMDelCert.exe” on the golden image client. This removes the SMS Certificate.

• Run “Tranguid /r” on the golden image client. This will force a new SMS ID to be created.

• Start the Services manager and find the SMS Agent Host service. Stop the service and change the Startup type to “Disabled”

• Open Notepad.exe and add the following lines:
  o sc config "ccmexec" start= auto (please note there is a space between the equal sign and “auto”)
  o net start "ccmexec"

• Save the file as “c:\NxPrepExtend.cmd”, make sure the extension is .cmd and not .cmd.txt by turning off “Hide extension for known file types” in the Tools…Options section for Explorer.

• Once completed, the image is ready for publishing and deployment.

The Administrator may choose not to install the SCCM client into the golden image and opt for a traditional approach to installing the SCCM client. Upon deployment, XenClient Enterprise will present the virtualized Windows instance as a normal Windows instance from SCCMs perspective. Since the dedicated images are not centrally updated and do not synchronize via the snap-back and snap-forward capabilities, the changes to the deployed dedicated image are persistent. This means the standard client deployment methodologies can be applied as outlined in “Tasks for Configuration Manager Client Deployment” from Microsoft TechNet.

**Deploying the SCCM Client on XenClient Enterprise Shared Images**

XenClient Enterprise Shared Images are synchronized with the central image and have the snap-back capability enabled. This presents unique challenges for deploying the SCCM client. In this case, the SCCM client must be added directly to the golden image itself since the any installations after the shared image is deployed will be lost after the next client reboot. There are considerations around auto-discovery of Site Codes and ensuring that the proper security keys are made available to the client after the XenClient Enterprise equivalent of SysPrep is run after image deployment. The proper process is as follows:

• Complete the golden image creation through the Synchronizer Console

• Install the SCCM client per your company’s best practices. It is recommended to use auto site discovery if the VM will be assigned to different sites codes.
- Install the SCCM client
- Run “CCMDelCert.exe” on the golden image client. This removes the SMS Certificate.
- Run “Tranguid /r” on the golden image client. This will force a new SMS ID to be created.
- Start the Services manager and find the SMS Agent Host service. Stop the service and change the Startup type to “Disabled”
- Open Notepad.exe and add the following lines:
  - `sc config "ccmexec" start= auto` (please note there is a space between the equal sign and “auto”)
  - `net start "ccmexec"
- Save the file as “c:\NxPrepExtend.cmd”, make sure the extension is .cmd and not .cmd.txt by turning off “Hide extension for known file types” in the Tools…Options section for Explorer.
- Once completed, the image is ready for publishing and deployment.

**The SCCM Client XenClient Enterprise Synchronizer OS Profile Policy**

When Shared Images are deployed, the SCCM OS Policy must be enabled to ensure any change to the central image does not affect critical SCCM client operation.

**Virtual Windows Instances in Active Directory**

While the Engine and Synchronizer work in concert with Active Directory to assign VM resources, the Engine itself does not actually join the domain. Therefore it is not seen in Active Directory Users and Computers. This is no different than VMware ESX. However, the Windows guests are seen in Active Directory, just as they usually would if they were installed physically.

When Synchronizer performs its preparation and delivery, regardless of whether it is deploying a Dedicated or Shared Image, it will change the name of the computer upon first deployment to the assigned users name combined with a series of numbers that provide a unique name in Active Directory. Once the name is changed, it will automatically be joined to the Windows Domain. This newly deployed name will appear in the Computers OU in Active Directory Users and Computers. This computer object now represents the virtual guest deployed to the VM. It may now be assigned to any OU in Active Directory depending upon organizational and Group Policy requirements.

**XenClient Enterprise Hosts, Guest Windows Instances and SCCM Collections**

SCCM only recognizes Windows OS instances and pulls them into collections. Since XenClient Enterprise Engines are XEN-based systems, they cannot be seen directly inside of SCCM. However, the Windows desktops that are virtual machines with an SCCM client will be seen as part of the SCCM collections. The Engine injects hardware and host information into the HKLM\Software\Citrix\XenClient registry keys.
in each Engine hosted virtual Windows instance. This information can be discovered through a MOF-based extension outlined in the “Hardware Inventory” section below and reported on. It can also be used to form collections by querying the different information surfaced by the virtual machine intermediary resulting in custom collections of Engine hosted virtual machines.

**Operating System Updates**

Operating system updates are performed by two different approaches based on the type of image being used. With Dedicated Images, OS updates are able to be directly delivered to VMs via the SCCM or Windows System Update Server (WSUS) agents.

However, Shared Images do not retain any installed software after the next reboot. This means any updates to the operating system and applications must be performed to the central golden image through the Synchronizer. The process is to launch the golden image in the Synchronizer, then use SCCM and WSUS to perform the updates. The updates will be installed on the golden image, but will be deployed as an update layer through Synchronizer.

**Application Deployment and Updates via SCCM**

Application updates are delivered in the same manner as the OS updates and, once again, are performed by two different approaches based on the type of image being used. With Dedicated Images, application deployments and updates are able to be directly delivered to VMs via the SCCM or WSUS agent.

However, Shared Images do not retain any installed software after the next reboot. This means any updates to the applications must be performed to the central golden image through the Synchronizer. However, application updates can be deployed to the centralized golden image through SCCM. The updates will be installed on the golden image, but will be deployed by the layer update technology in XenClient Enterprise.

**Software Inventory**

Regardless of VM image type deployment, software inventory through SCCM remains unaffected. Custom reports can be created to match the same software in multiple virtual machines on a single host so the real per device/seat licensing requirements are understood. For example, NXTOPHOST1 is hosting two virtual machine instances named “Admin-W7-01” and “Admin-W7-02”. Both instances have Microsoft Office 2010 installed. A custom report can be created to cross-reference the host name with the virtual machines and the software inventory to ensure that IT understands Office is virtually present on the same machine, eliminating any confusion over the number of physical hosts with Office present
Remote Server Functionality

Leveraging Synchronizer remote office server capability allows you to manage all remote servers from your central server. You can gain many key things by using the remote servers such as intelligent caching of downloaded images, efficient use of bandwidth between remote offices, local storage and maintenance of backups, and fast recovery for remote clients. The remote server can be used in WAN or LAN setups. The remote server will require network access to the SQL database as well as the central server. The SQL port 1433 needs to be open for access to the database and port 443 needs to be open for access to the central server. All downloads from the central server are encrypted and compressed. As a user requests an image update, or Engine update they request it from the remote server to which they are registered, the remote server then checks with the central server to begin download of the update. Once the update is downloaded to the remote server it then caches it for the next user.
Personal Virtual Disk (PvD)

This release integrates Personal vDisk technology into the XenClient Enterprise solution. Leveraging this technology, the end user can install apps that persist across reboots without compromising the Administrators ability to update the VM. The implementation of PvD:

- enables computers to retain user-installed applications and desktop settings.
- provides policies to control OS profiles.

About XenClient Disk Management Models

Shared image disk mode enables the Administrator to control applications installed on the user’s virtual machine and also update it. Applications installed by the user disappear across reboots due to snapback that brings back the virtual machine to its pristine state. This disk mode ensures that virtual machines of all users are up-to-date and protected.

With custom image disk mode a user can install and persist applications across reboots. This allows the user to personalize the virtual machine, but at the same time, the user is responsible for keeping the virtual machine up-to-date and in good state.

With the integration of Personal vDisks in XenClient Enterprise, Administrators can update the virtual machine and keep it up-to-date and the same time the user can personalize the virtual machine by installing applications as they persist across reboots.

What is PvD?

With PvD VMs, in addition to the three layers of shared image mode, a new layer called the application VHD is introduced. On this VHD all the user profile changes and apps are stored. The application VHD does not go through a snapback thus the user setting persists across a reboot.

The diagram below provides a high level overview of PvD. For specific disk chaining details refer to the Administration Guide and online Help.

Shared image with Personal vDisks Integration
PvD provides a number of benefits, including:

- support for user-installed drivers and applications.
- elimination of per-boot save/restore change actions.
- elimination of snap forward behaviour, which could lead to loss of user installed applications during updates to the base image.
- support for non-volume licensing, because activation information is preserved and not snapped back.

How is PvD implemented?

XenClient implements PvD functionality in both the Engine and Synchronizer.

The Engine is responsible for creating the PvD disk; when a VM is published, Synchronizer sends an update for the VM, which results in the VM undergoing the NxPrep process. During this time, only updates to the VM are sent to the Engine – this process may take a few minutes, and is dependent on the number of files in the application disk.

Once a PvD VM is created, the disk mode for that VM cannot be changed; if a Shared PvD VM is created, it cannot be switched to a Custom or Shared VM. The decision to create a PvD VM is made when the VM Wizard is initiated – it cannot be changed. You can, however, create a PvD VM from a shared (or custom) VM by cloning it.

The Engine implements PvD in such a way that user applications are retained on the application (referred to as the master) disk. It’s important to note that in general, boot time for PvD-based VMs is similar to shared and custom VMs. In some cases, PvD VMs preparation may take longer to boot than a shared or custom VM.

In the Engine, PvD information is displayed in the Virtual Machine Control Panel: four disk labels are provided (System, User, Local and Master Disks). The image on the following page illustrates PvD-related elements in the Engine:
Synchronizer implements PvD functionality by providing a policy to control user installed applications. Further control is provided by the Snapback feature, which allows the Administrator to reset the VM to a clean state; this process will remove all installed applications and user data.

- Use the Wizard to create a PvD VM.
- Usage mode indicates how the VM is used.
- PvD VMs are labeled in the navigation tree.

Select Snapback Now to manually snapback the disk.
Use Synchronizer’s VM creation Wizard to preserve user installed applications when the VM is restarted. After specifying the VM name, select the appropriate radio button to preserve applications: