Wyse WSM Reference Architecture and Configuration Guide

(Single site up to 50 users)

Release 1.2

Copyright Notices

End User License Agreement (“License”)

A copy of the Wyse Technology End User License Agreement is included in the software and provided for your reference only. The License at http://www.wyse.com/license as of the purchase date is the controlling licensing agreement. By copying, using, or installing the software or the product, you agree to be bound by those terms.

Trademarks

The Wyse logo and Wyse are trademarks of Wyse Technology Inc. Other product names mentioned herein are for identification purposes only and may be trademarks and/or registered trademarks of their respective companies. Specifications subject to change without notice.

Restricted Rights Legend

You acknowledge that the Software is of U.S. origin. You agree to comply with all applicable international and national laws that apply to the Software, including the U.S. Export Administration Regulations, as well as end-user, end-use and country destination restrictions issued by U.S. and other governments. For additional information on exporting the Software, see http://www.microsoft.com/exporting.

Ordering

For availability, pricing, and ordering information in the United States and Canada, call 1-800-GET-WYSE (1-800-438-9973) or visit us at http://www.wyse.com. In all other countries, contact your sales representative.

Changes

Version	Date	Changes
1.0	4/3/2012	Initial Public Release
1.1	4/23/2012	Updated for SetCache modification settings
1.2	5/11/2012	Added updated info for Dell T110 ii server

Contents

Table of Figures and Tables

1 Introduction

Wyse WSM is the first solution to use OS and application streaming to package and deliver the end user desktop environment to remote client devices, giving IT administrators the control they need to ensure the consistency of desktop software across the enterprise.

Wyse WSM requires very little datacenter infrastructure, operates standalone, or complements existing presentation and VDI solutions, while dramatically reducing the storage space, IT time and expense of delivering and maintaining desktop software throughout an enterprise. By streaming the operating system and applications independently to a stateless client device and running them locally in memory, Wyse WSM enables virtually any Windows application to be run on the client just as it would on a traditional PC. Yet all files and applications reside in the private data center or in the branch router, where they are easier to back up, manage, and maintain.

Because applications are streamed independently of the operating system, Wyse WSM enables standardization of operating system images across the organization and delivers applications based on user roles and responsibilities. Administrators can also easily provision new applications or updates to existing applications without having to modify the operating system image.

Out of the box, the remote client devices contain no local operating system software on the device, but instead use OS and Application Streaming (OAS) to deliver a true PC experience with cloud computing benefits of centralized storage, control, and simplified OS and application maintenance. The true PC OS and applications are literally delivered in real-time over the LAN from Wyse WSM provisioning software in the datacenter cloud.

2 Required Materials

The following materials are required before starting the installation:

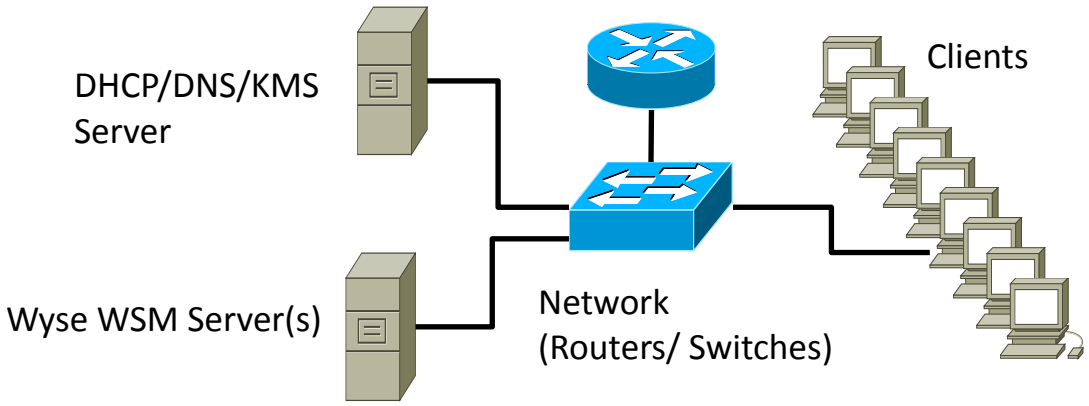
- Windows Server 2008 R2 running DNS, DHCP, and Key Management Services (KMS)
- WSM Deployment Server with (minimum specs)
    - Intel i3-2100 (Dual Core – 3.0 GHz)
    - 8 GB of Memory
    - Intel Q67 or C206 chipset
    - Dual SATA II SSD drives (HDD for up to 25 users)
    - Dual Gigabit Ethernet NICs (single NIC for up to 25 users)
    - Windows 7 Enterprise or Professional (64 bit version)
    - Wyse WSM server image and license (Version 4.01)
- Windows 7 Enterprise or Professional 32 bit ISO image compatible with KMS
- Appropriate applications (such as Office 2010 ISO image compatible with KMS)
- Additional applications which can be site licensed or use an optional license server
- Endpoint devices such as Wyse Z00D
- Required Networking Gear (Routers and Switches)
- Ethernet Cables as needed

3 Preparing the network for WSM deployment

The Wyse WSM reference architecture consists of several components as shown in Figure 1.

- A Management Server – Provides necessary Network services such as Domain Name Service (DNS), Dynamic Host Configuration Protocol (DHCP) and Key Management Service (KMS)
- The Wyse WSM server – Provides the central repository of the streamed OS and Application images. It also stores the system cache files for each streamed client.
- Network Components – Such as switches and routers, needed to connect the streaming client devices to the WSM and Management services as well as the internet.
- Streaming Client Devices – Cloud PC (such as Wyse Z00D or X00m)

Figure 1: Typical Deployment Configuration



The first step is to determine the network information to be used. See Table 1 as a template to fill in this information.

Table 1: Required Network Deployment Information

Domain Name	
IP Subnet for Streaming Clients	
Default Router for Streaming Clients	
DNS server(s) IP address(es)	
Static IP address for WSM server	
Default Router for WSM server	
Active Directory Server Administrator User Name	
Active Directory Server Administrator Password	

If you have not already deployed your management server, see Section 7 on tips for doing so. Make sure that your DNS, DHCP, and Active Directory services are fully functional before proceeding to the next step.

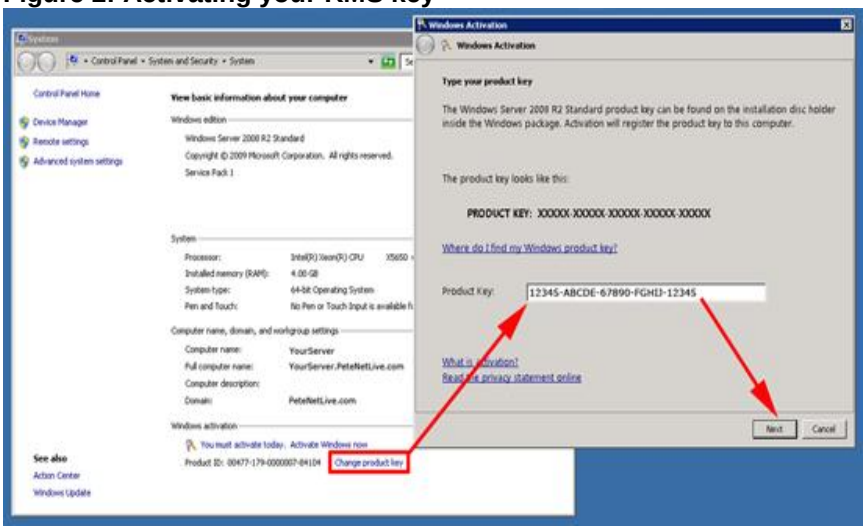
3.1 Configuring Key Management Server (KMS)

The Microsoft Key Management Server must be installed on the network to support the licensing of the individual Windows 7 client desktops. This service allows for each streamed client OS to be automatically activated seamlessly after it is loaded onto the remote device. Since KMS will be used to authenticate the streamed Windows 7 client OS, Microsoft requires that it be installed on a Windows Server 2008 R2 machine. In fact, it is automatically enabled as part of the Windows Server 2008 R2 installation. However, the License Key must be installed before it can authenticate the additional client OS machines.

Log into the Microsoft Volume License Service Center, and retrieve the KMS License Key for "Windows Server 2008 Std/Ent KMS B". To License/Activate Server 2008 R2 **AND** Windows 7 **THIS IS THE ONLY KEY YOU NEED**. You do **NOT** need to add additional keys for Windows 7.

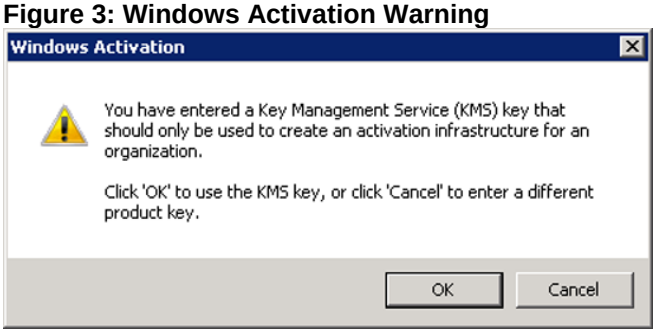
You simply need to change the product key on the server that will be the KMS server, to the new key. Start > Right Click "Computer" > Properties. Select "Change Product Key" > Enter the new KMS Key > Next.

Figure 2: Activating your KMS key



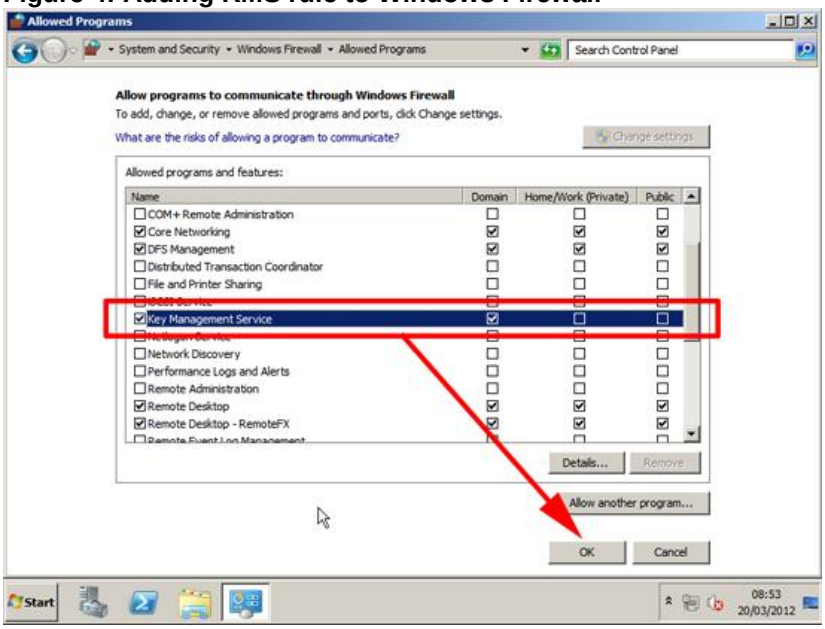
You will receive a warning that you are using a KMS Key > OK. You may now need to activate your copy of Windows with Microsoft, this is done as normal. If you can't get it to work over the internet you can choose to do it over the phone.

Figure 3: Windows Activation Warning



If you are running the Firewall Service on your Windows 2008 R2 server, you will need to enable the rule for the Key Management Service. To allow the service, select Start >Control Panel>System and Security>Windows Firewall>Allow program or feature through Windows Firewall. Scroll down to the Key Management Service and select the check boxes.

Figure 4: Adding KMS rule to Windows Firewall



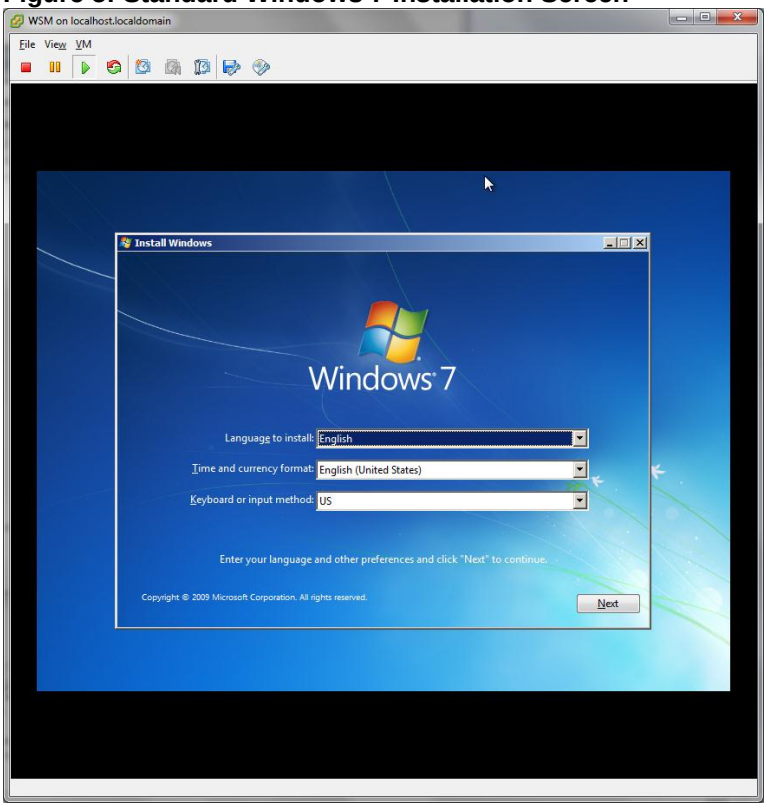
4 Installing WSM Server

Use this section for installation steps for Windows 7 and prepare it for the Wyse WSM server. While you have probably installed Windows many times before, there are some special configuration steps to be completed after the standard installation.

4.1 Loading Windows 7 image

Start installation as if on a standard PC starting with the screen shown in Figure 5.

Figure 5: Standard Windows 7 Installation Screen



After the OS installation is complete, install any required device drivers for the particular server board you are using including network drivers. After installing the updated system drivers, set the static IP address for the NIC interface.

Once the WSM server has network connectivity, use the Microsoft Update Center to install all appropriate updates and patches. This will insure that the WSM server installation is not overwritten by any Microsoft patch or update that might change the NIC interface driver. Since Windows 7 installs Power Management software by default, it is important enable high performance mode as the default mode. Lastly, make sure that the Windows License is applied and is registered with Microsoft.

4.2 Configuring NIC teaming

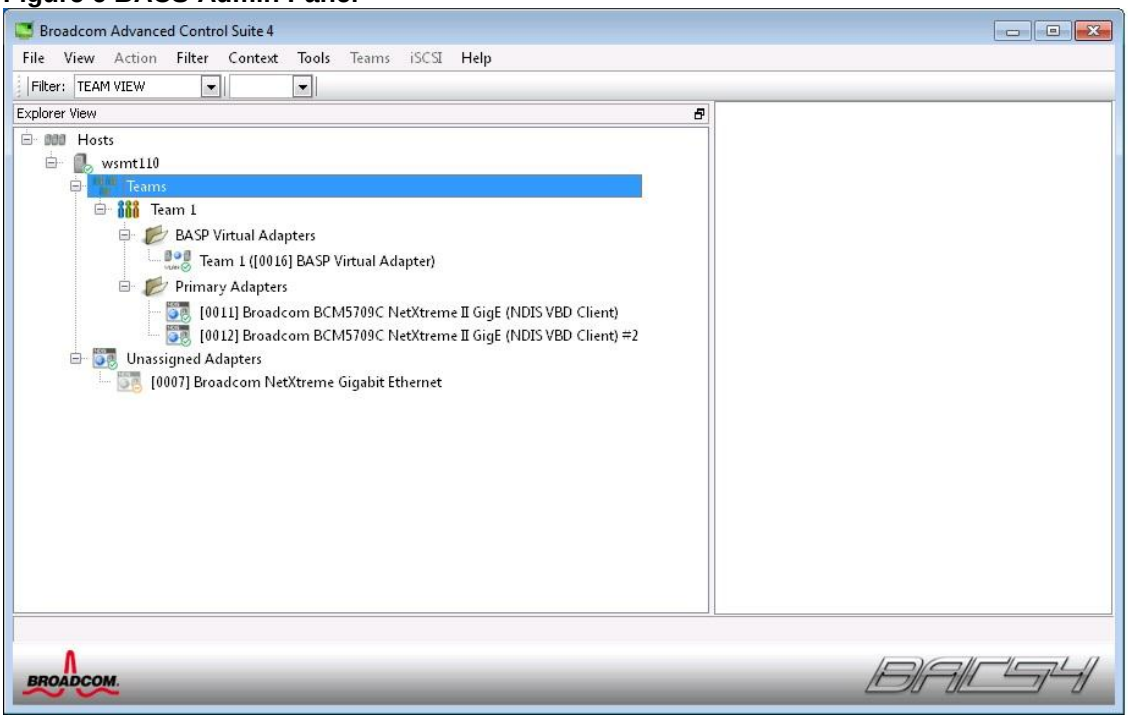
On the Dell T110 ii WSM server platform, there are three Broadcom NICs. For the small server configuration, the onboard NIC will not be used as part of the team, and can be disabled. The NIC teaming software is used to form a 2 Gbps bonded interface by combining the remaining two NICs. This provides more bandwidth for the streaming traffic.

Right click on network icon located on the right side of the task bar at the bottom of the screen. This will open the **Network and Sharing Center** control panel. Click on **Change Adapter Settings**. At this point, you should see your three network adapters, which are normally labeled **Local Area Connection, Local Area Connection 2** and **Local Area Connection 3**. The Intel NIC teaming software will create a fourth interface called **Local Area Connection 4** from these two interfaces. This is a virtual interface. **Once it is created, all new network parameter changes should be made to the team interface.**

In order to create a NIC team, you need to download the Broadcom Advance Control Suite software from: http://www.broadcom.com/support/ethernet_nic/management_applications.php.

Once this is downloaded, right click on the icon and select **Run as Administrator.** After it is installed, you should see a green NIC card icon on the right side of your task bar. You can double click on this icon to launch the BACS software. The BACS organizes the drivers in a tree structure as shown in Figure 6. Next, click on the icon which represents your server's host name.

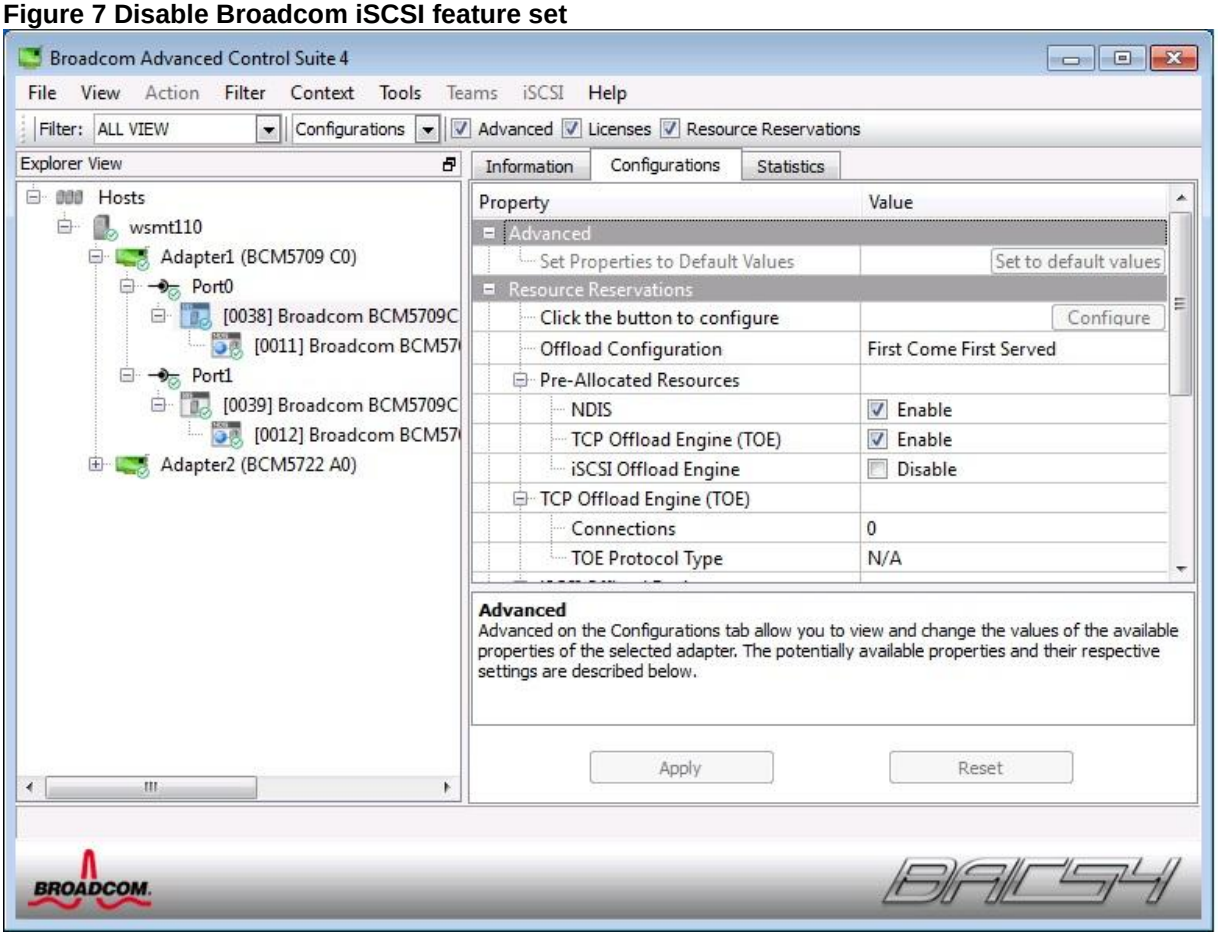
Figure 6 BACS Admin Panel



Before you can create the NIC team, you need to disable the iSCSI feature set from the Broadcom adapters because the iSCSI protocol is not supported on NIC teams.

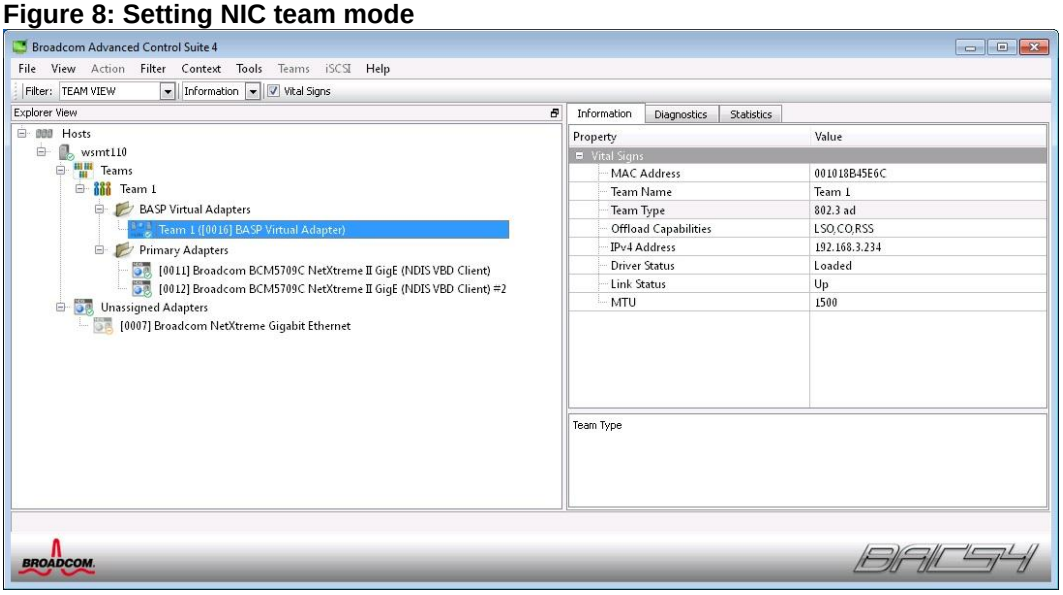
Scroll down to the Broadcom adapters (Primary Adapters) and double click on the first BCM5709 adapter you see. A sub-panel will appear as shown in Figure 7. Click on Resource Reservations and scroll down to the iSCSI Offload Engine. Unselect this feature by clicking in the square.

Figure 7 Disable Broadcom iSCSI feature set



Repeat this procedure for the second Broadcom 5709 adapter. Once you have disabled iSCSI protocol, you can go back and create the NIC Team. Go back to the main panel and select **TEAM VIEW**. You can select the Team menu, and **Create Team**. Select the two Broadcom 5709 adapters and add them to the team. The last item that needs to be changed is the team type. To get proper load balancing, select 802.3ad. This will create an LACP based team. Make sure your upstream is also set to LACP mode.

Figure 8: Setting NIC team mode

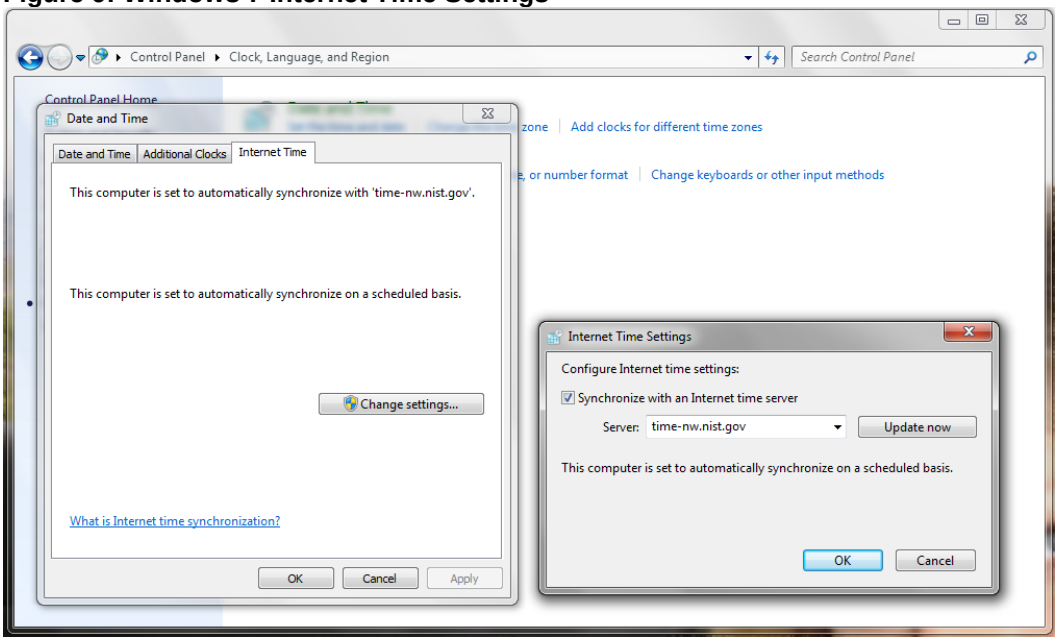


Once the team is created, you can go back to the network control panel and set the IP Address settings on the Team interface.

4.3 Time and NTP settings

The Time and NTP settings for Windows 7 are part of the Control Panel. To access this, select **Control Panel** from the start menu, select **Clock, Language, and Region**, select **Date and Time**, select **Internet Time** tab and click on the **Change Settings** button. Enter the name of the NTP server. Press "OK" then "OK" to exit the **Date and Time** screen.

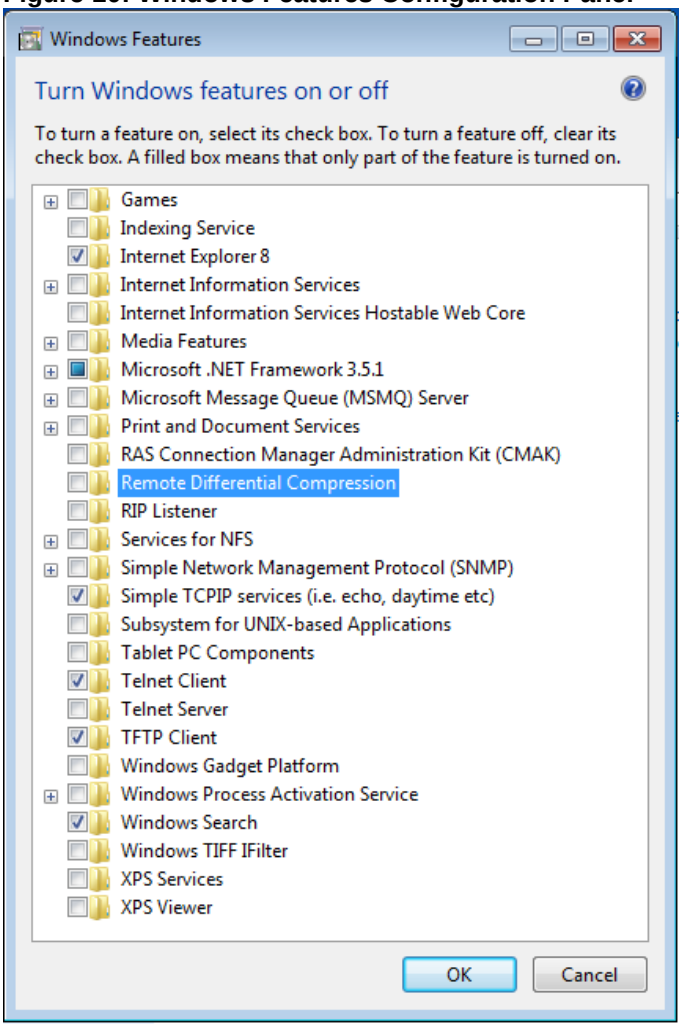
Figure 9: Windows 7 Internet Time Settings



4.4 Optimizing Windows on the WSM server

In order to optimize the Windows 7 OS for WSM operations, certain features need to be turned off and others need to be enabled. A list of features to be turn off are: Media Features, Print and Document Services, Remote Differential Compression, Tablet PC Components, Windows Gadget Platform, XPS Services and XPS Viewer. Also, some optional services should be turned on for troubleshooting purposes: Simple TCPIP services, Telnet Client, TFTP Client. Change these application settings in the Start->Control Panel->Programs->Windows Features screen.

Figure 10: Windows Features Configuration Panel



5 Installing and configuring the WSM software

The installation of WSM server software is in two parts. First, as a prerequisite, the Microsoft SQL Express 2008 software must be installed. Windows 7 is NOT compatible with the 2005 version. Do not use the WSM Prerequisite Application stored in the WSM installation directory. This will cause incompatibilities with Windows 7. After SQL express is installed, the WSM application software can be installed from the pre-mentioned directory.

5.1 Installing Microsoft SQL Express 2008

SQL Express 2008 will need to be installed prior to running the WSM Server Install script. Download the software from Microsoft at:

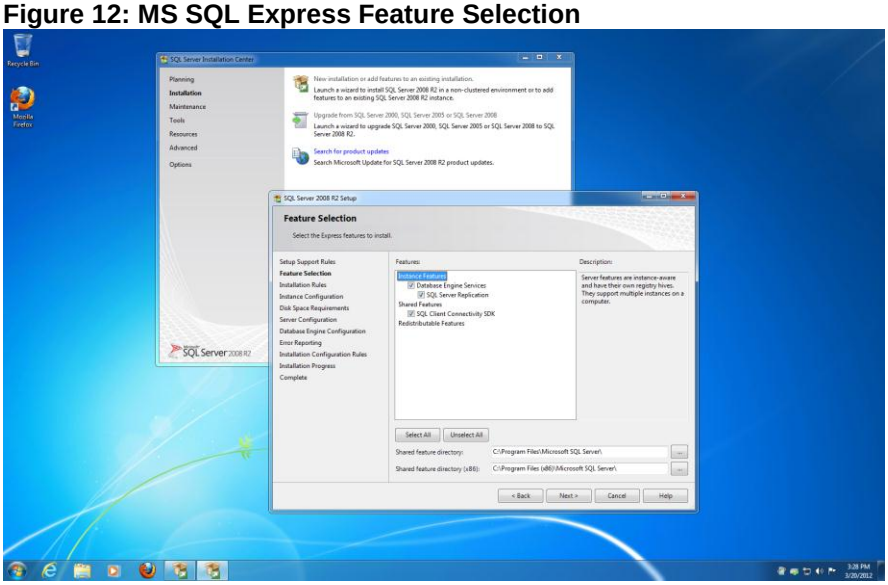
http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=1695

Figure 11: Microsoft SQL Server Download Site

Click on the red box to download the program ***SQLEXPR_x64_ENU.exe***. Once downloaded, it can be executed, by right clicking on its name and selecting **Run as Administrator**. Accept any security warnings that might pop up. The support files will be extracted and the install options page will appear.

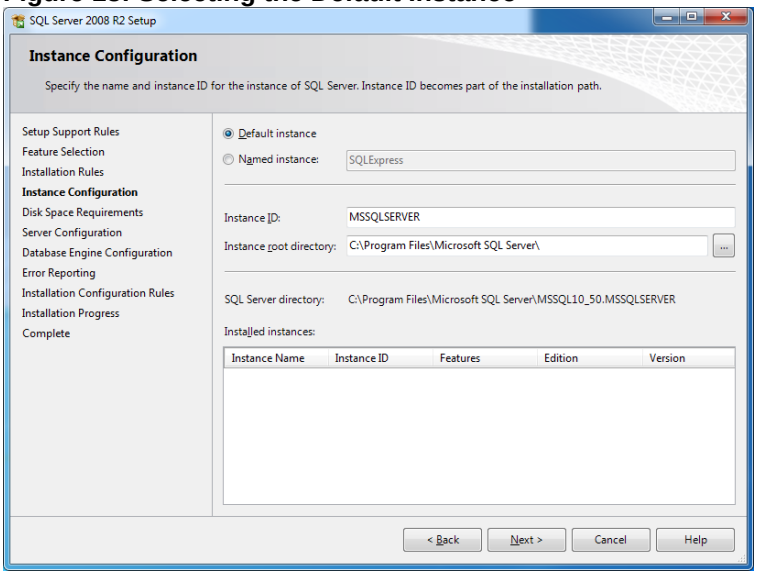
Select New Installation and on the next screen, accept the license agreement. On the **Feature Selection** screen select the defaults by clicking on the ***Next>***.

Figure 12: MS SQL Express Feature Selection



On the **Instance Configuration** screen, to simplify the install, click Default instance (which is not the default). Then click **Next>** to continue to the next screen.

Figure 13: Selecting the Default Instance



On the **Server Configuration Screen**, the default settings are fine, so click **Next>**. On the **Database Engine Configuration** screen select **Mixed Mode** authentication and enter the Systems Administrator (SA) password. It is important to remember this password as it will be needed during the WSM software installation. Click **Next>** to continue.

Figure 14: Setting SQL SA Password

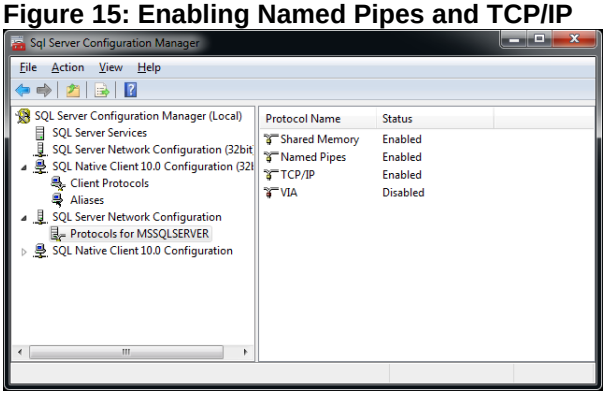
Nothing needs to be changed on the **Error and Reporting** screen, so just click **Next>.** At this point, the software will be installed. When the installation is complete, click **Close**.

5.2 Enabling Named Pipes and TCP/IP connections

The next step is to modify the MS SQL Express Configuration for WSM operation. To do this, from the windows start prompt, select ***START->All Programs->Microsoft SQL Server 2008 R2->Configuration Tools->SQL Server Configuration Manager***. Select ***SQL Server Network Configuration*** and then **Protocols for MSSQLSERVER**.

Make sure that ***Named Pipes*** and ***TCP/IP*** are enabled. By default, they are disabled. Right click on each of them and select ***Enable***. Make sure they are also enabled in ***SQL Native Client 10.0 Configuration***.

Figure 15: Enabling Named Pipes and TCP/IP

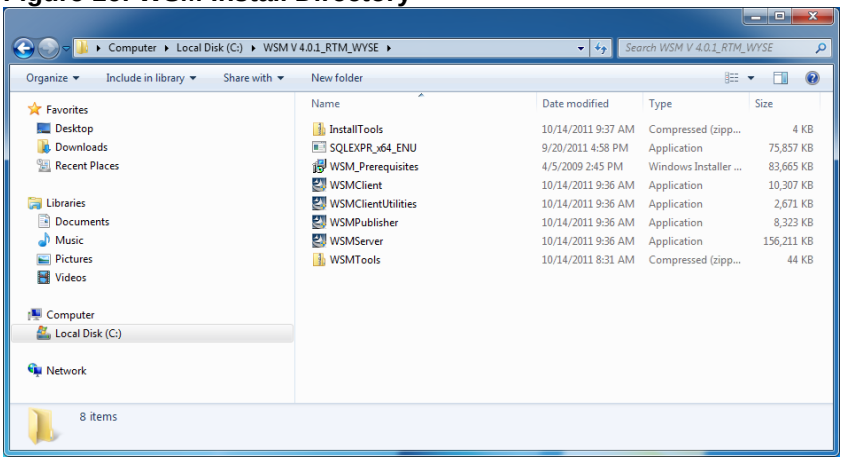


After making these changes, the SQL server will need to be restarted. Click on ***SQL Server Services*** and right click on **SQL Server (MSSQLSERVER)** and select restart.

5.3 Installing the WSM Server Software

The WSM server application is provided in self-extracting ZIP format. Right click on the ZIP file, select **Run as Administrator**, and the software will be installed in the **C:\WSM V 4.0.1_RTM_WYSE directory**. In this location, there will be several subdirectories and executable files.

Figure 16: WSM Install Directory



Right click on **WSMServer** and select **Run as Administrator**. This will start the installation process.

Accept any Windows security Popups. After a few moments, the WSM Server Installation splash screen should appear. Click on **Next>** to continue and accept the License terms as shown in Figure 17.

Figure 17: WSM Server Installation Splash Screen

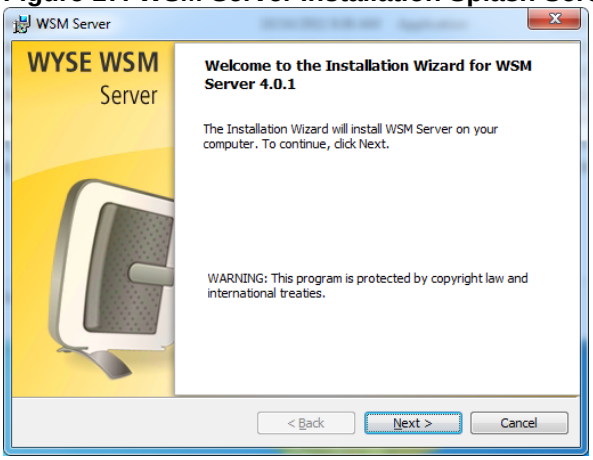
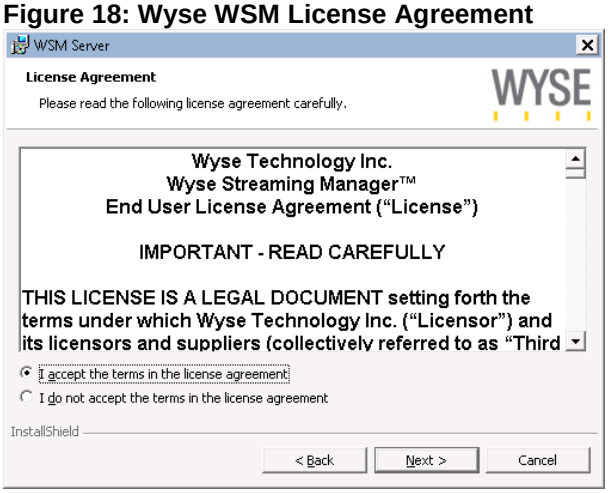


Figure 18: Wyse WSM License Agreement



Click on **This is a new WSM installation** as shown in

Figure 19 and **Typical** on Figure 20.

Figure 19: WSM Server Information

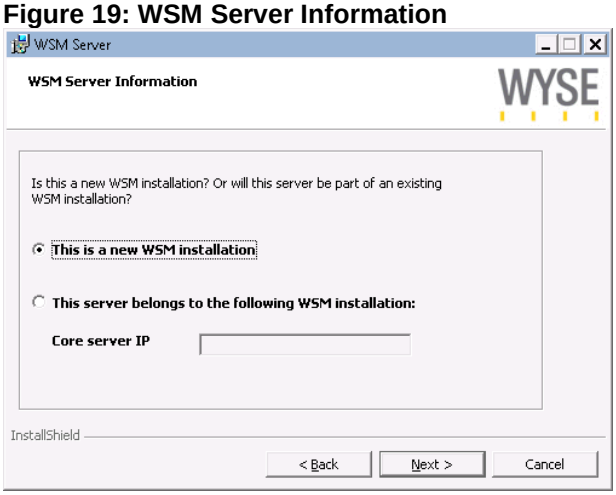
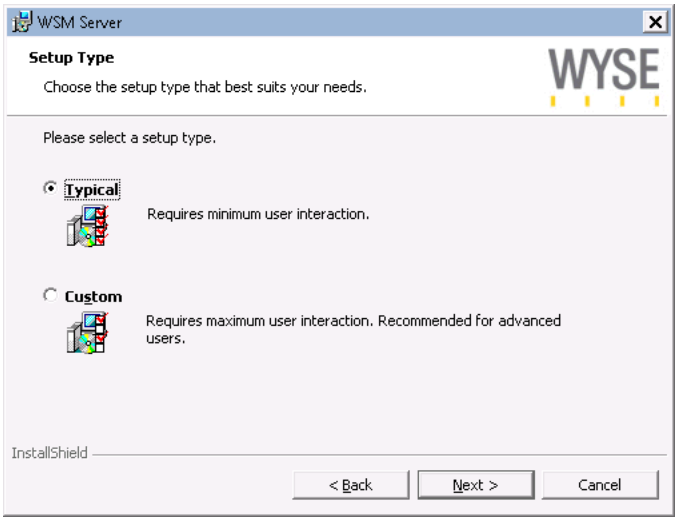
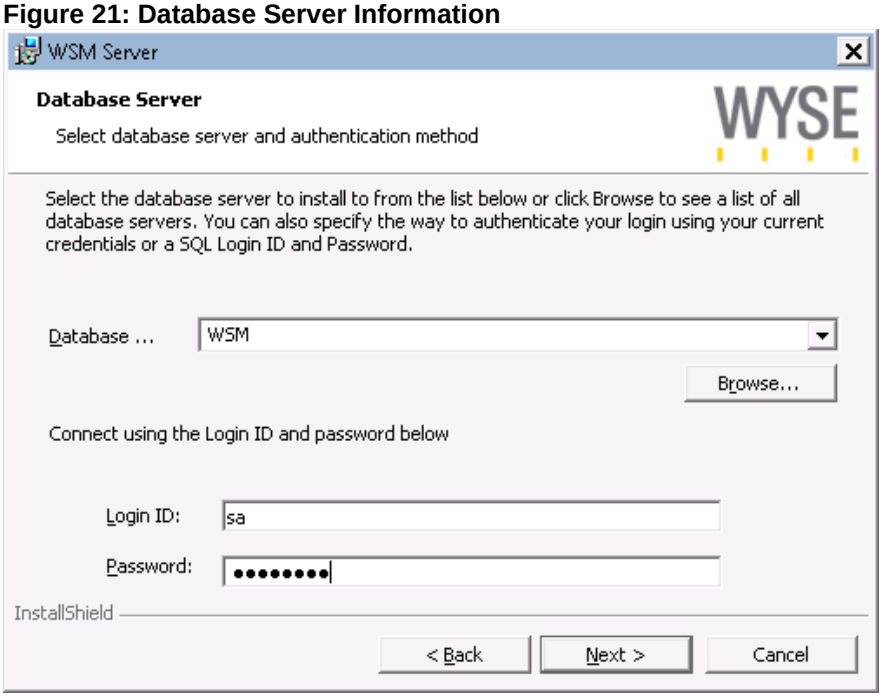


Figure 20: WSM Server Type



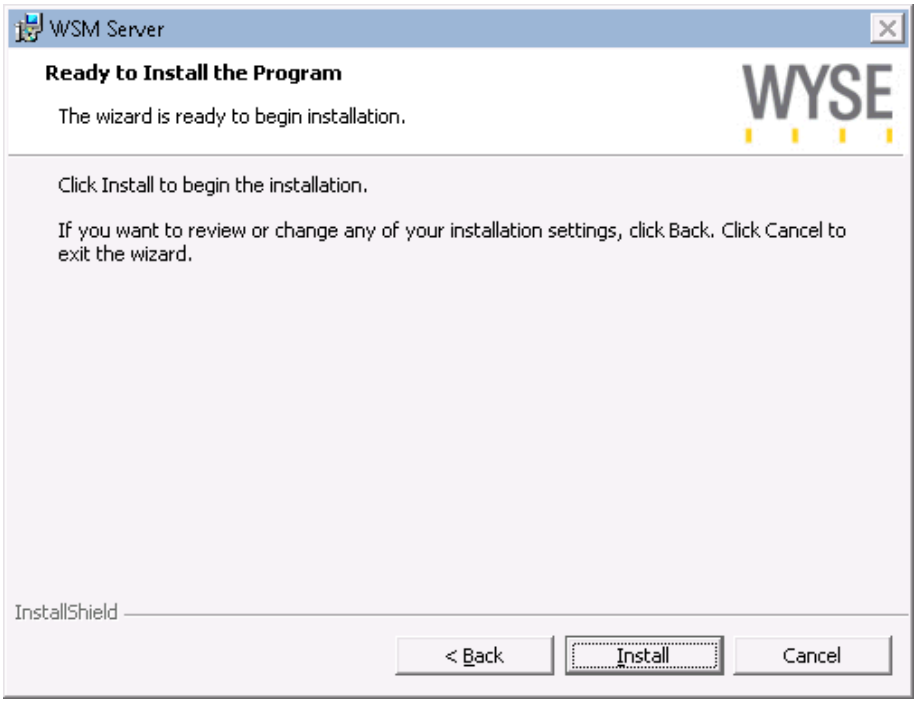
On the **Database Server** screen, the database name should be the same as your WSM server name. Make sure that the **SA** password is the same as you entered in Figure 14 above.

Figure 21: Database Server Information



After checking the information hit **Next>**. The installation should start when you click on **Install**.

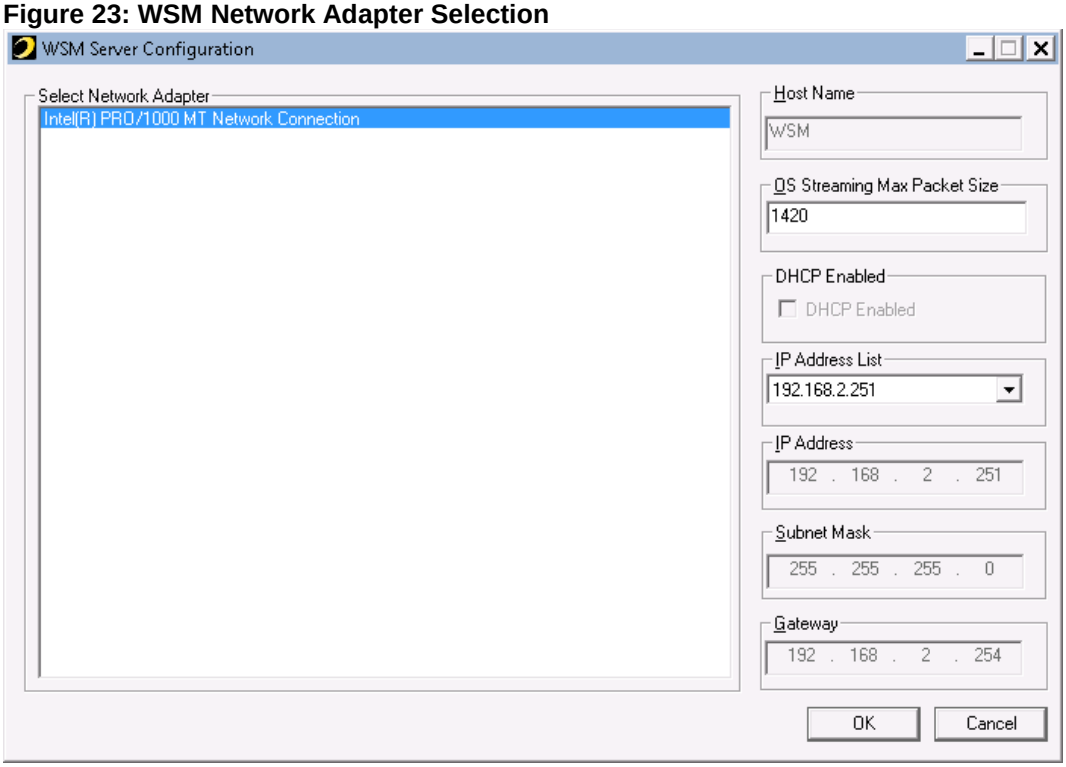
Figure 22: WSM Ready to Install Screen


WSM Server
Ready to Install the Program
The wizard is ready to begin installation.
WYSE
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

During the install, various status messages will appear. You will be asked to select the network adapter as shown on

Figure 23.

Figure 23: WSM Network Adapter Selection

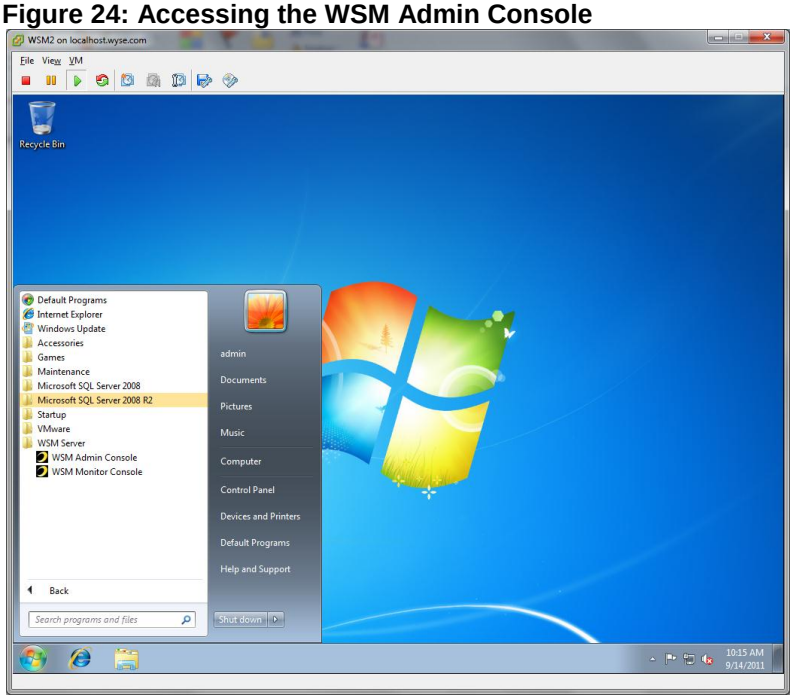


The WSM Installation will be completed after that.

5.4 WSM configuration

To access the WSM Admin Console select **Start->All Programs->WSM Server->WSM Admin Console**.

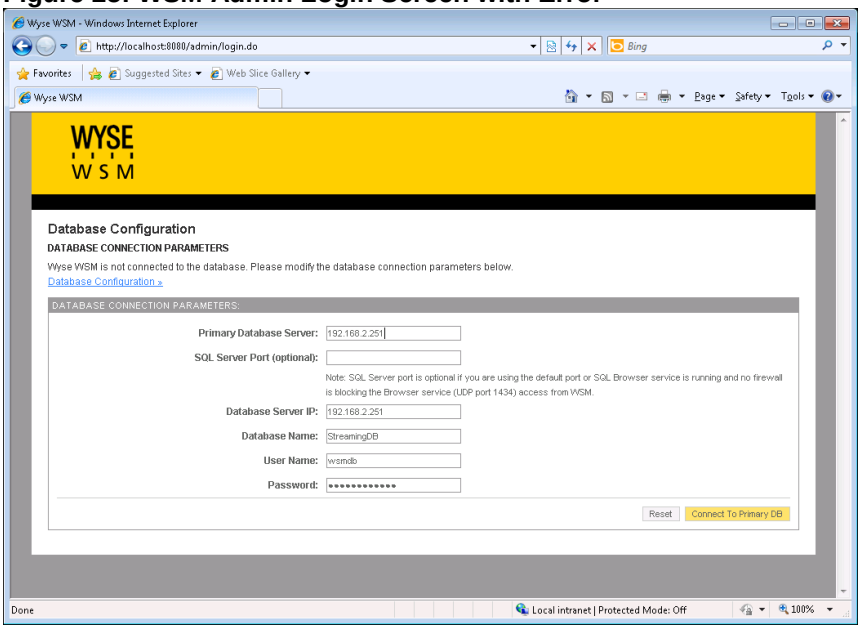
Figure 24: Accessing the WSM Admin Console



If the SQL Express Server Parameters for **TCP/IP** and **Named Pipes** were not set properly as shown on.

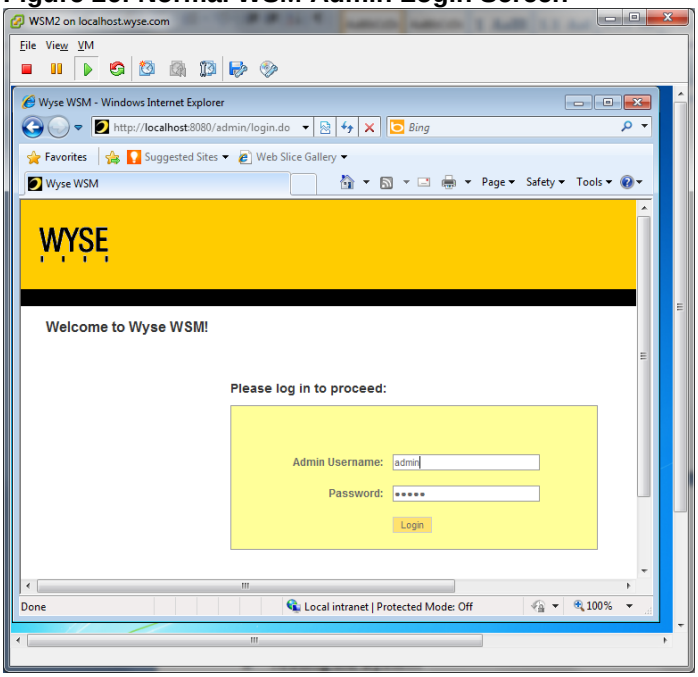
Figure 15, the browser will be redirected to the **Database Configuration** Screen as shown on Figure 25. If this happens, close the browser window, and return to section 5.2.

Figure 25: WSM Admin Login Screen with Error



If the Named Pipes and TCP/IP connections are enabled properly, the browser will be redirected to the normal login screen as shown on Figure 26.

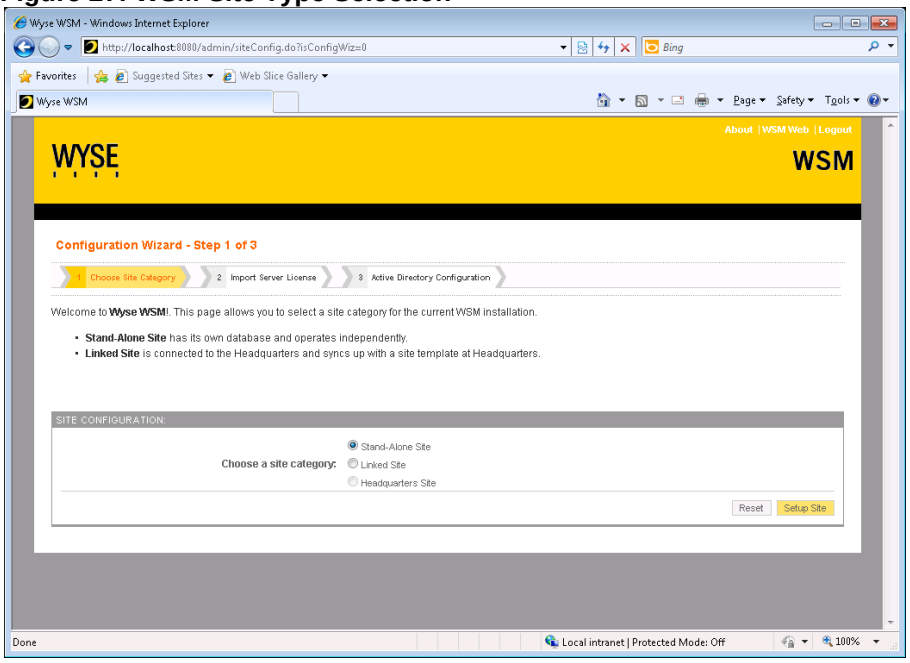
Figure 26: Normal WSM Admin Login Screen



The default username is **admin** and the default password is **admin**.

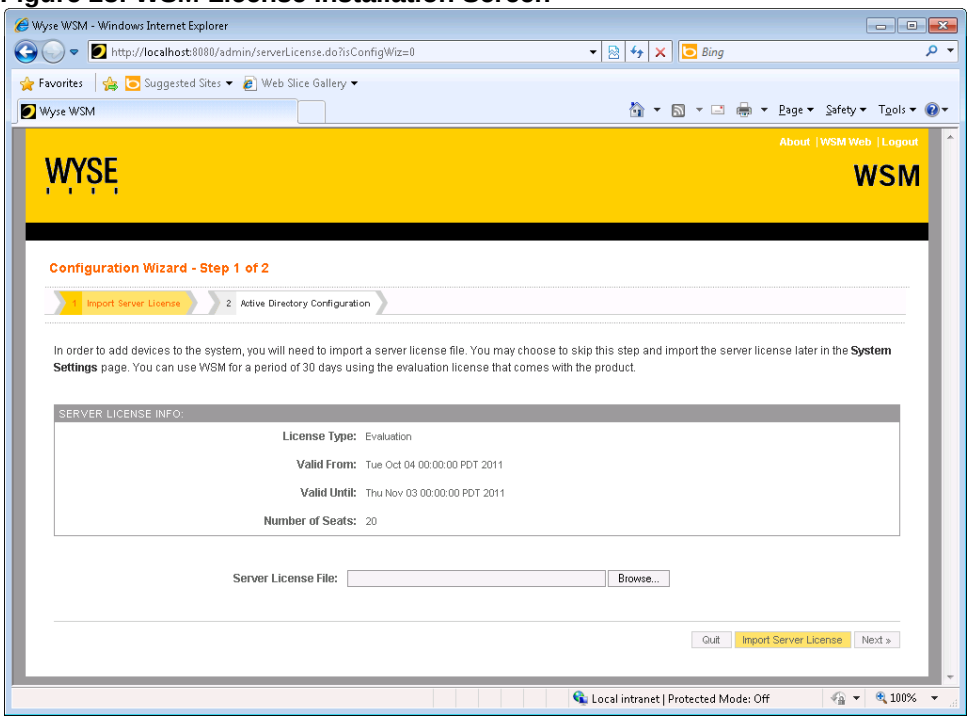
After logging in, you will be directed to the Site Configuration screens starting on Figure 27.

Figure 27: WSM Site Type Selection



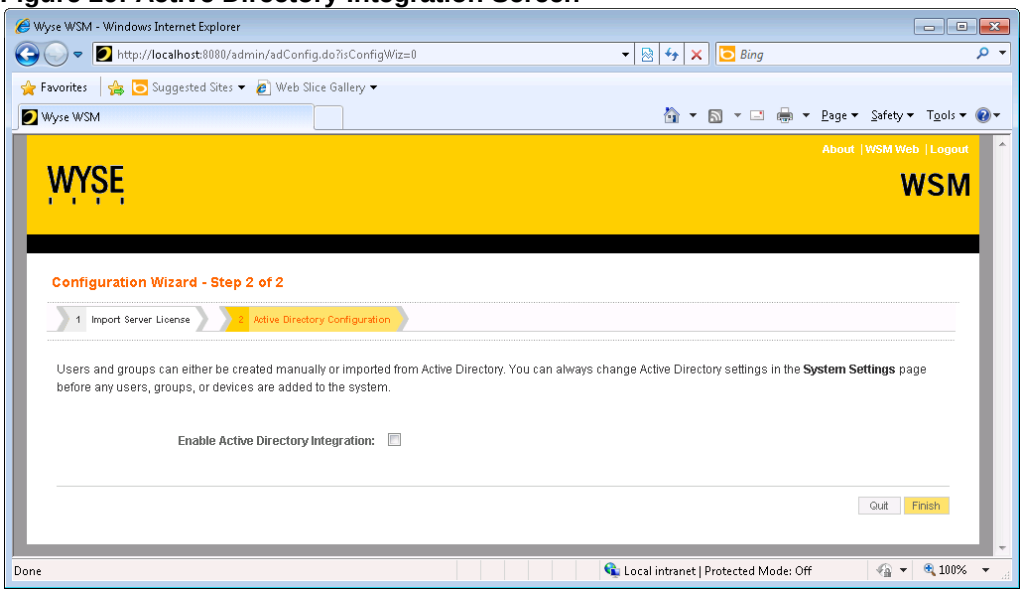
Click on **Setup Site** and you will be directed to the **Step 1 of 2** screen. Click on **Browse**, locate your License file on your desktop and press **Open**.

Figure 28: WSM License Installation Screen



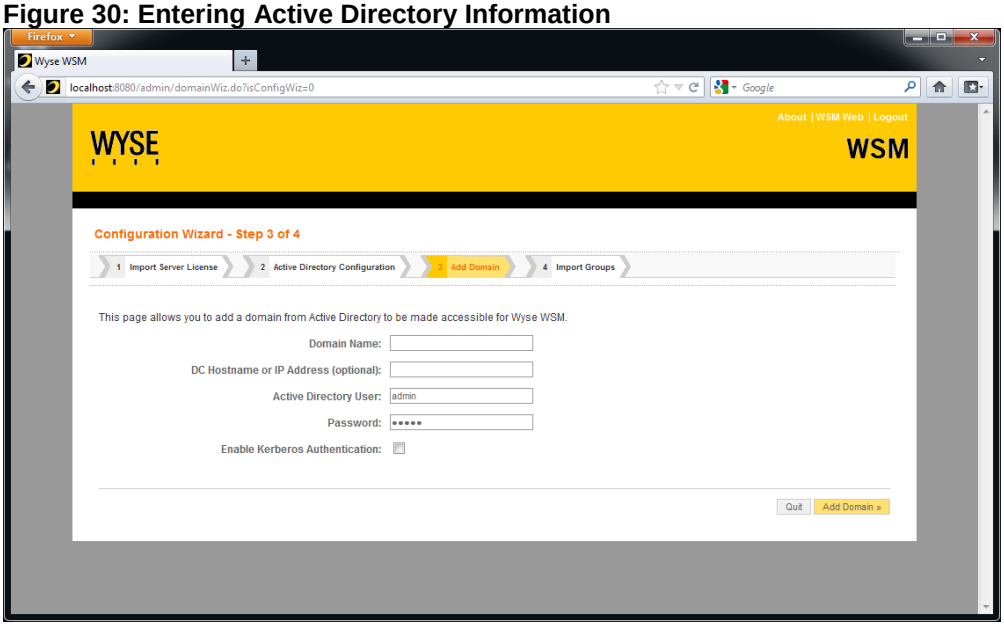
Once the license file is installed, you will be asked if you want to Enable Active Directory integration.

Figure 29: Active Directory Integration Screen



Click on the box to enable the LDAP integration and then click **Next>** when it appears. On the next screen enter the information for your Active Directory Server, and then click **Add Domain**.

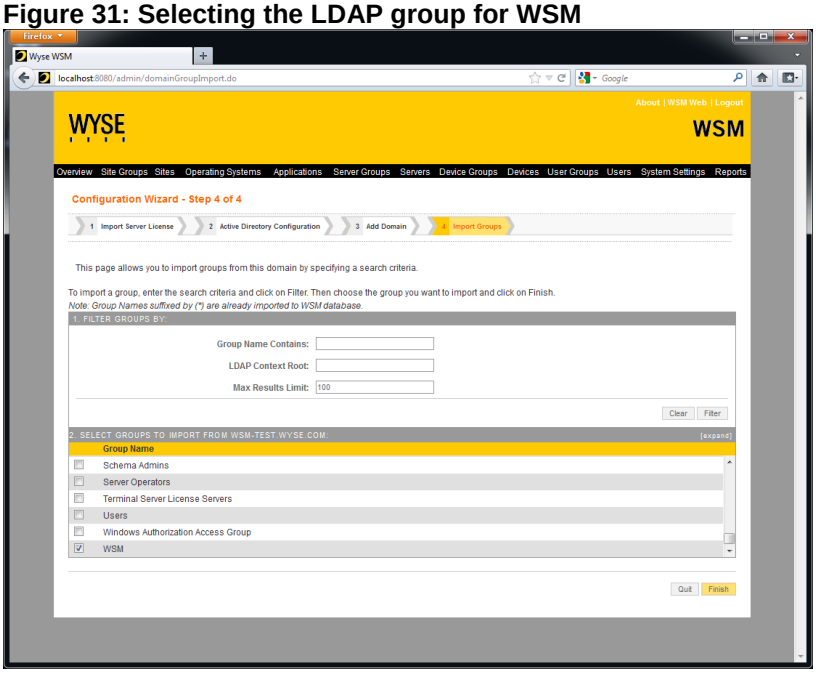
Figure 30: Entering Active Directory Information



On Step 4, you will need to select the specific Organization Area (OA) within your AD database to place the computers that will be added as part of the WSM streaming service. You should select the group that you have created for this purpose. In this example, as shown in

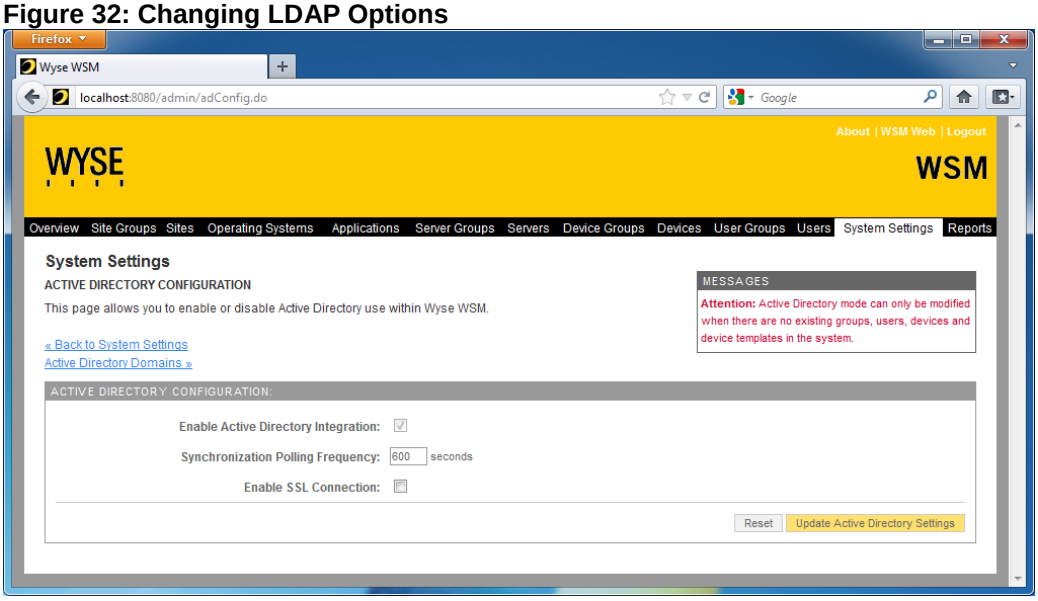
Figure 31, the WSM group was created previously, and is now selected. This will be used for Application Streaming, which will be documented in a future version of this guide. After making the selection, click **Finish**.

Figure 31: Selecting the LDAP group for WSM



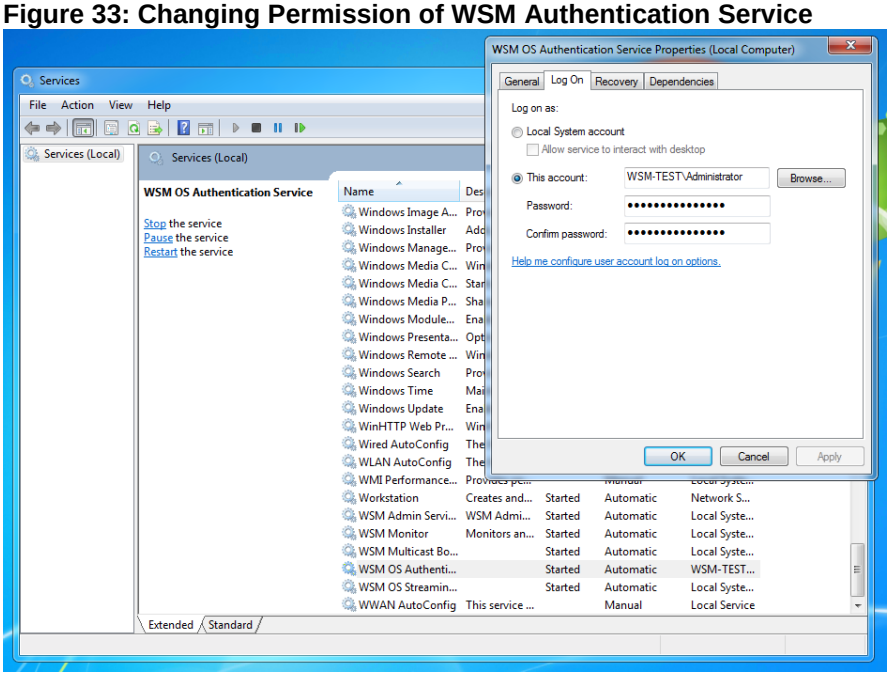
After finishing the initial configuration of WSM, select the **Systems Setting Tab** and then select **Active Directory Configuration**. On this page, you can set the options for the Active Directory interaction. You can enable SSL communications between WSM and AD server.

Figure 32: Changing LDAP Options



If you choose not to enable SSL, then you will need to manually make a change to the **WSM OS Authentication Service** to provide it with the proper permissions to have access to the AD database. From the Windows Start menu, type **Services**. The services application should appear at the top of the start menu. Right click on it and select **Run as administrator**. Scroll through the list of services and towards the bottom you should see **WSM OS Authentication Service**. Right click on it, and select **Properties**. The properties screen should appear as shown on Figure 33. Select the Log On tab and enter the credentials for a user account that has read/write permissions to the AD database.

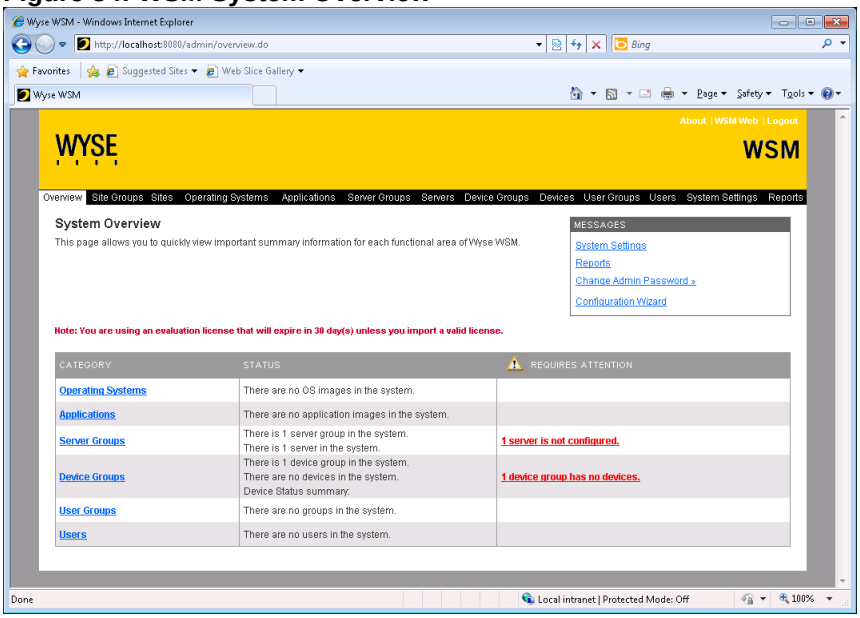
Figure 33: Changing Permission of WSM Authentication Service



You will need to click **OK**. You will need to restart the WSM OS Authentication service for this change to take effect. If the user account or password changes, you will need to manually repeat these steps.

At this point, go back to your WSM Admin console and you should see the System Overview screen as shown in Figure 34. If you have installed your license key, you should not see the red warning as shown.

Figure 34: WSM System Overview



5.5 Modifying the WSM system cache settings

On Windows Operating System, if WSM Streaming server was up for a few days with active or idle streaming sessions, system's available memory will steadily decrease. Server will eventually run out of memory. This was caused by the Windows' file system cache. Since Windows gives priority to the System Cache over application processes, and there is no upper limit on file system cache size on certain Windows systems, running the streaming service for extensive period will end up with a huge file system cache due to the large numbers of file I/O requests made by WSM Streaming service. This problem is not unique to WSM. It applies on any windows services or applications which use heavy file I/O calls. Problem is also more apparent on 64-bit Windows Operating Systems.

Starting on release 4.0.1, Wyse incorporated a subset of MS's Dynamic Cache Service into WSM server to limit the maximum system cache size on 64-bit OS. At this time, there is no workaround for 32-bit versions of Windows.

When WSM Authentication service starts, it launches SetCache64.exe provided that the registry entry **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Wyse\WSM\LS\SkipSetCache** does not exist or is set to 0 (DWORD). If the registry entry exists and is set to any non-zero value, Setcache64 will not run and the cache settings will not be modified.

SetCache64.exe sets the maximum system cache size according to below registry setting: **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Wyse\WSM\MaxSystemCacheMBytes** which represents desired System Cache Size upper limit.

The accepted values are:

0 (default) – Setting the value to 0 will let the system to automatically assign the memory limit based on the amount of available memory. The more memory available, the higher percentage of that memory will be allocated to the System Cache.

Available Memory	Maximum System File Cache Size
<= 2GB	Available Memory * 50%
> 2GB & < 8GB	Available Memory * 75%
>= 8GB	Available Memory * 85%

However, if the Authentication Server is restarted, the amount of available memory at that time may be less than when the server was first started, and therefore, the amount of System Cache memory will also be less.

1-99 - Limit the maximum size of the System File Cache to the specified percentage of currently available memory. The same restriction for setting the value to zero is true here as well. If the Authentication server is restarted and the amount of available memory is less, then the size of the System Cache will also become less.

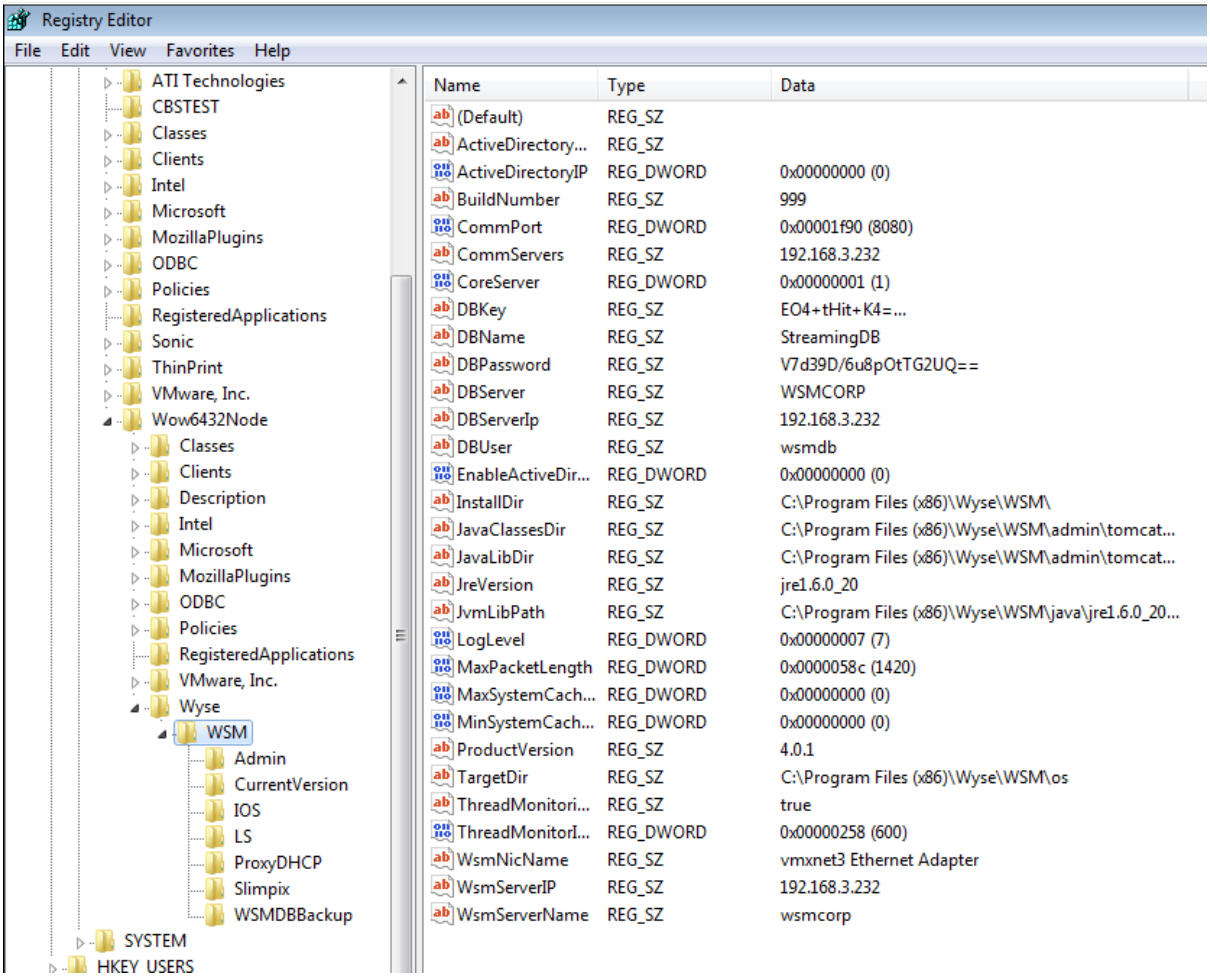
100-199 – These values have no meaning and will be rounded up to 200.

> 200 - Limit the maximum size of the System File Cache to x Mbytes

The maximum system cache file size must be >= 200MB AND <= available ram size minus 300MB. The available ram is the amount of ram after WSM services have been loaded. Setting the value too low will cause performance issues with File I/O. Setting the value too high will take away available memory for programs to load and may cause application errors. The specific value cannot be determined ahead of time. Since every WSM environment and server work load is different, the default setting that Wyse provides is not suitable for all environments. Wyse strongly recommends that you monitor the memory usage of your WSM server and adjust the "MaxSystemCacheMBytes" setting accordingly.

You can use Registry Editor (Regedit) to set these values. To run regedit with administrative permissions, select the **Start** button on the taskbar and type **regedit** in the search window. The Regedit application should appear at the top of the program list. Right click on the name and select **Run as Administrator**. Highlight the menu trees as shown above until you reach the WSM registry folder. On the right side, you will see the list of registry values. Right click **MaxSystemCacheMBytes** and select **Modify**. Click on **Decimal** and enter the value based on the above options.

Figure 35: Setting System Cache Max Value

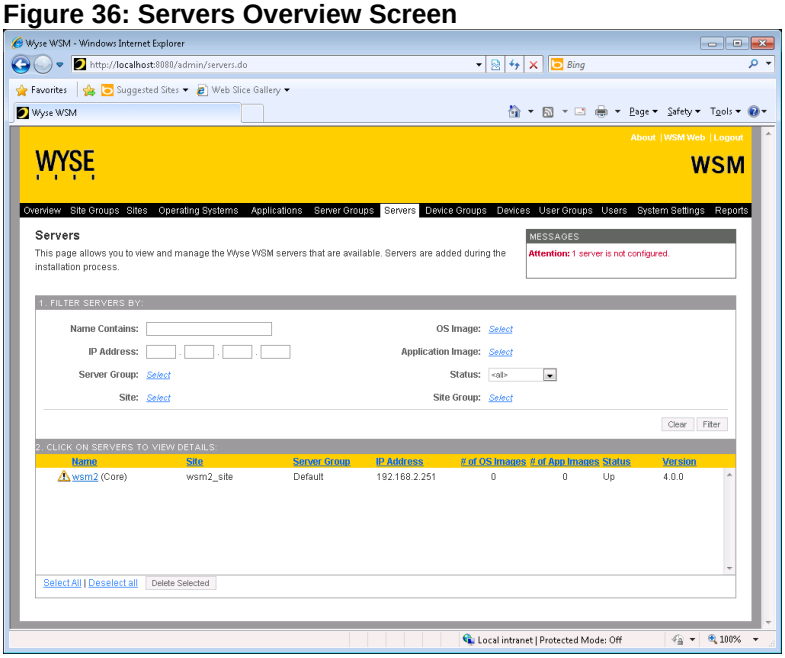


SetCache64 will output messages to the SetCache.log file under "<WSM Server install folder>\log" folder. This log file records the exact value system cache file size was set to.

5.6 Verifying WSM server Installation and Operation

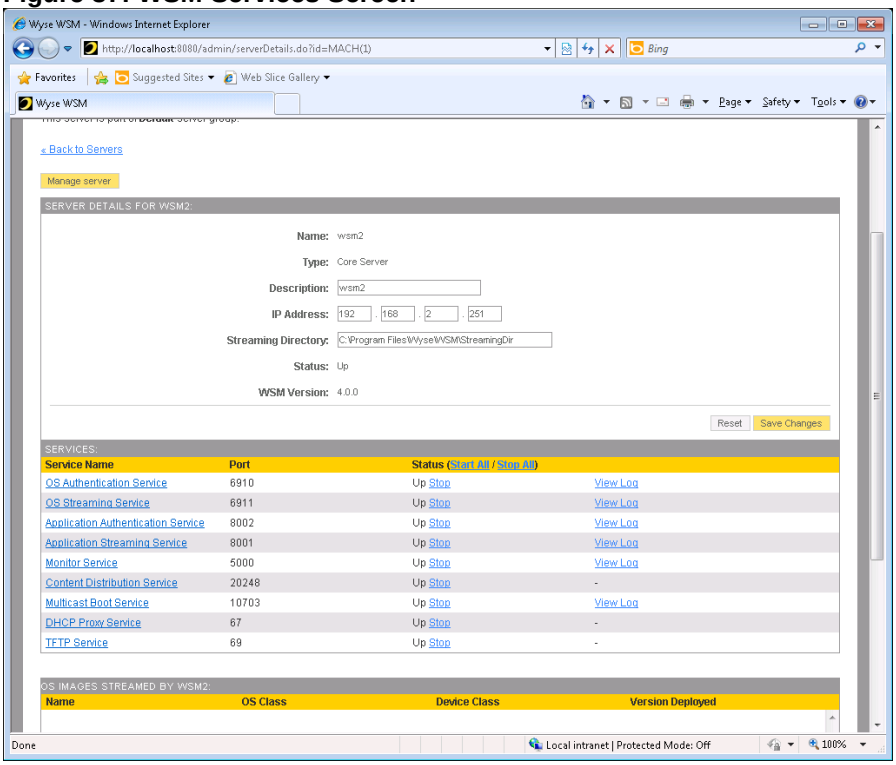
To verify that the WSM software was installed correctly and that it is fully operational, you can click on the Servers tab. You should see a list of the systems running WSM. In this case, it should show only the current machine you are connected to.

Figure 36: Servers Overview Screen



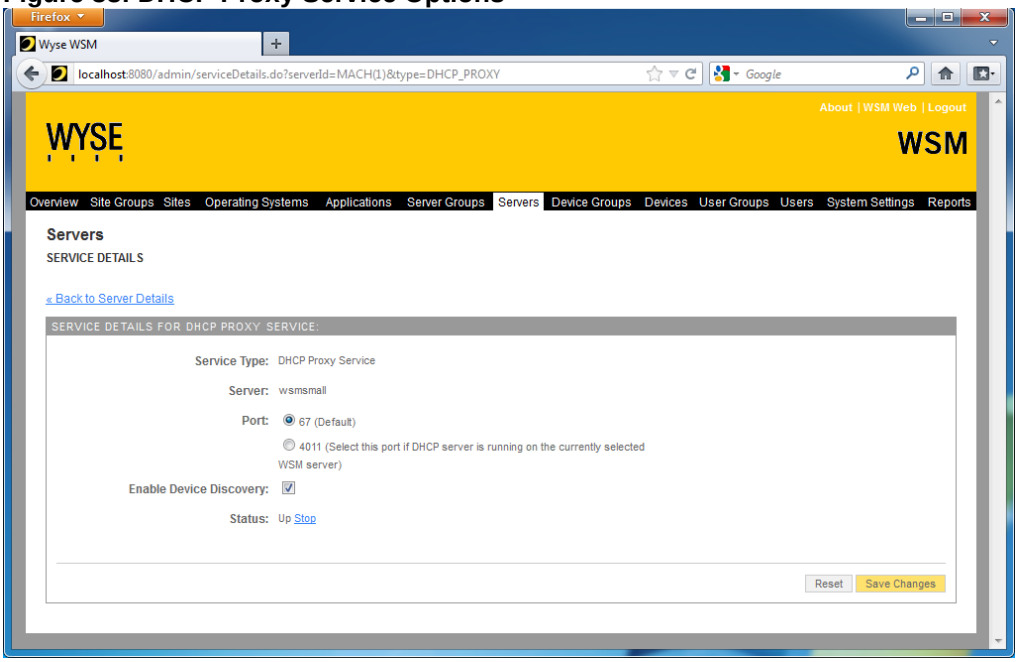
Click on your server name and verify that all the services are running as show in Figure 37.

Figure 37: WSM Services Screen



Click on DHCP Proxy Service and verify that **Enable Device Discovery** option is checked. If not enable it and click **Save Changes**.

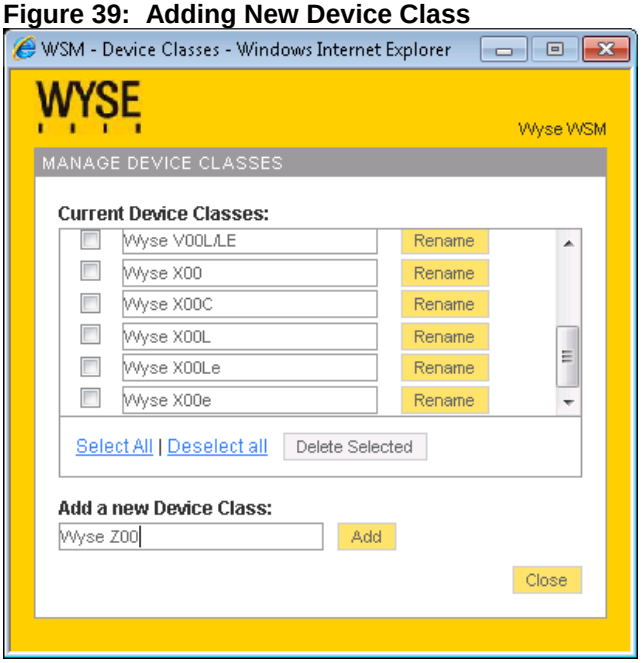
Figure 38: DHCP Proxy Service Options



5.7 Creating New Hardware profile for Streaming Client

You can add a hardware profile for your new streaming client device if it is not already in the WSM database. To do this, click on **Systems Settings** tab on the main screen, and then select **Manage Device Classes**. Look through the list of devices to see if yours is in the list. If not, type the name of the new device class in the **Add a new Device Class** box and click **Add**.

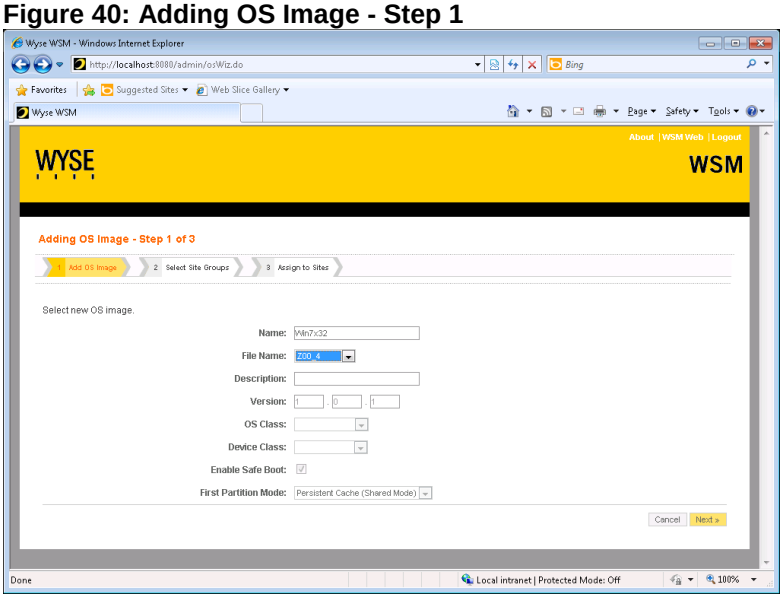
Figure 39: Adding New Device Class



5.8 Adding virtual desktop (Operating system and Applications) to WSM

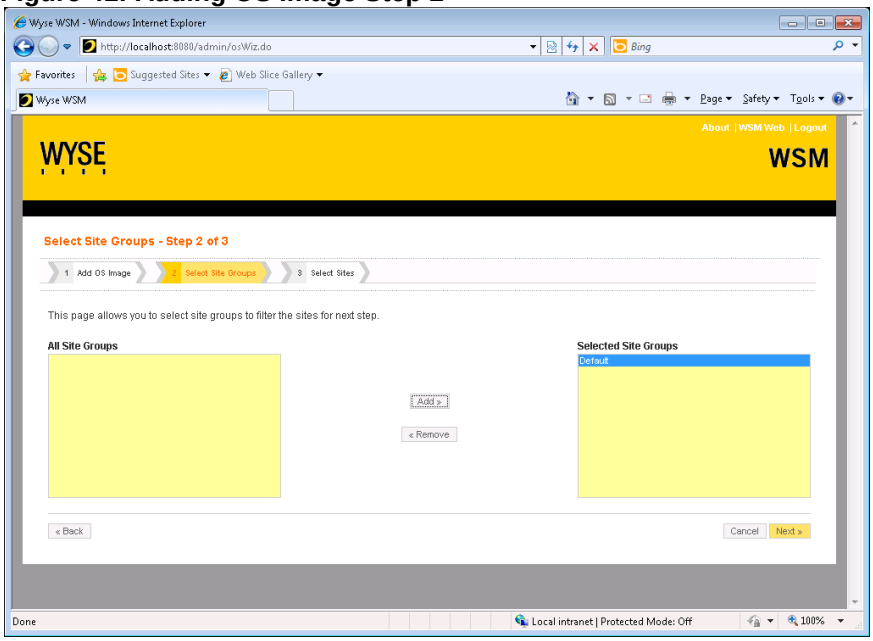
The instructions for building an Operating System image and uploading it to WSM are included in Chapter 6 of the WSM Installation Guide. A summary of the steps is also listed in this guide in Section 6. Once the image has been created and uploaded to the WSM server, it will be available to register into the WSM system. From the main WSM screen, click on **Operating Systems** tab and select **Add OS Image**. On the screen show in Figure 40, type the label you want to assign to this image and select the appropriate file from the pull down **File Name** entry. At this point, you cannot make any other changes on this screen so click on **Next>** to continue.

Figure 40: Adding OS Image - Step 1



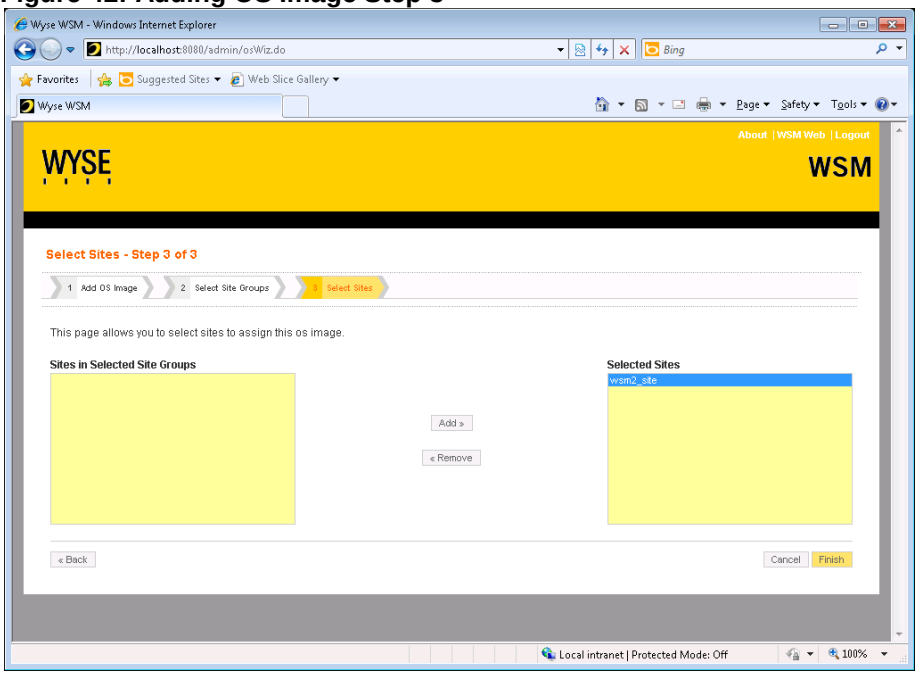
Select the Default Site for this image and click on **Add** and **Next>**.

Figure 41: Adding OS Image Step 2



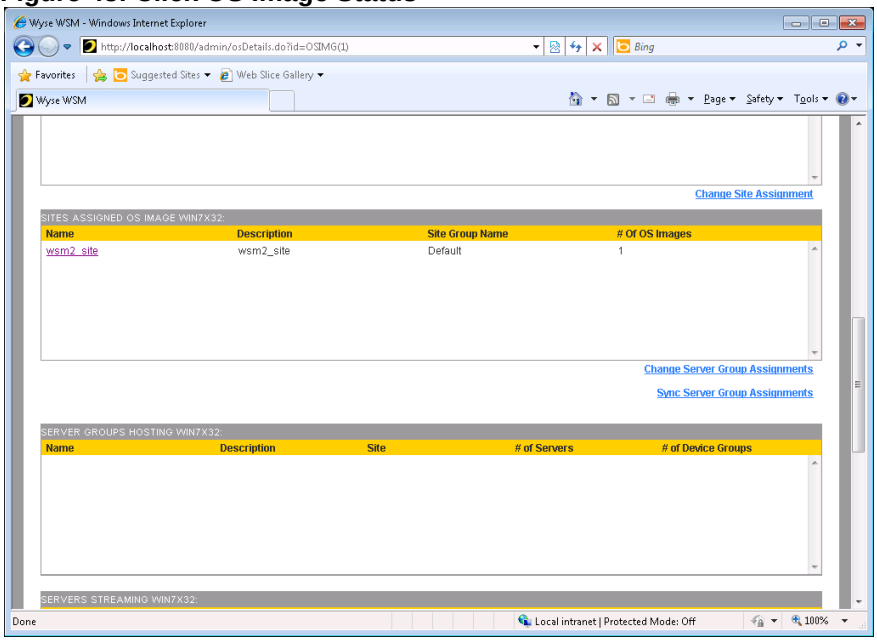
Next, select the Site Group for this image and click **Add** and then **Finish**. Again, there should only be one Site Group to select from.

Figure 42: Adding OS Image Step 3



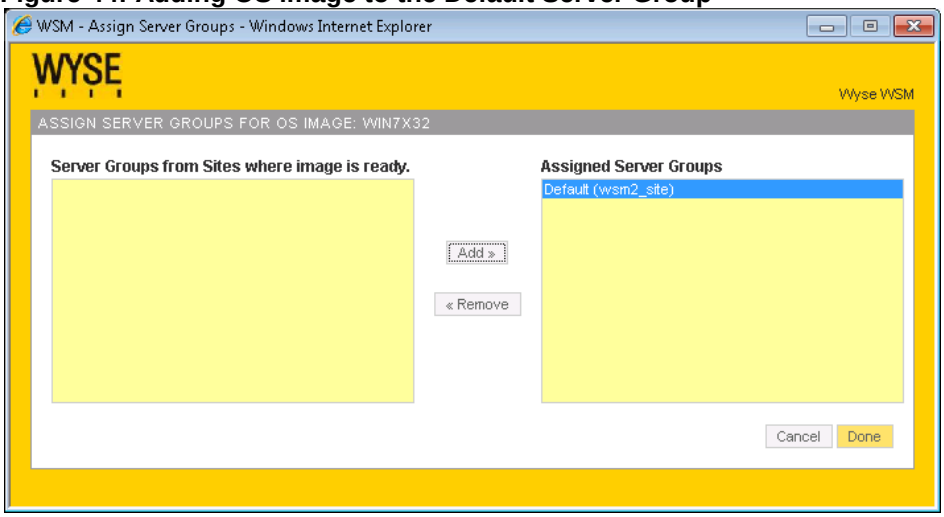
Verify the information you selected, click on the Operating Systems tab on the main screen and select your OS image name. Scroll down as show on Figure 43 and you will notice that no Server Group has been selected. Click **Change Server Group Assignments**.

Figure 43: Click OS Image Status



Select the Default Server Group on Figure 44, click **Add>** and **Done**. This will complete the OS installation into the WSM Database.

Figure 44: Adding OS image to the Default Server Group

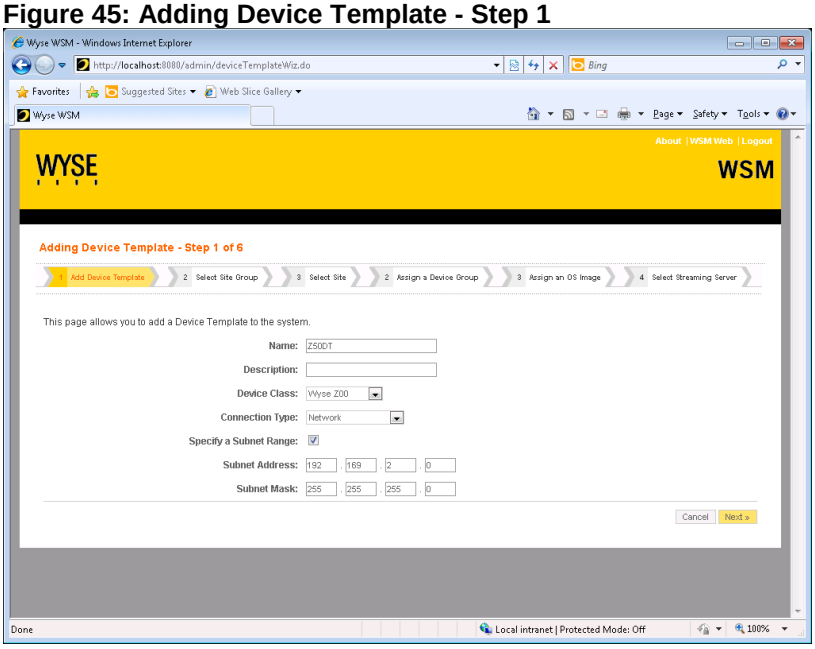


5.9 Creating a Device Template

A Device Template can be created for testing the OS image. This allows you to add device automatically as they turn on. From the main screen, select **Systems Settings** and the **Manage Device Templates**. Then click on **Add Device Template.** Enter the name of the Template as shown in

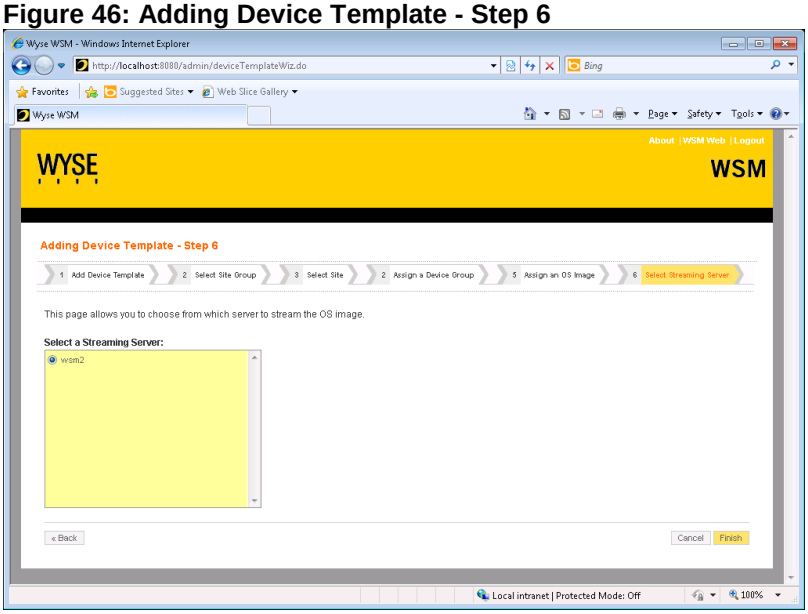
Figure 45. Select the Device Class from the pull down menu item. You can optionally specify the subnet you want by clicking **Specify a Subnet Range** and filling in the subnet information. Lastly, click **Next>** to continue.

Figure 45: Adding Device Template - Step 1



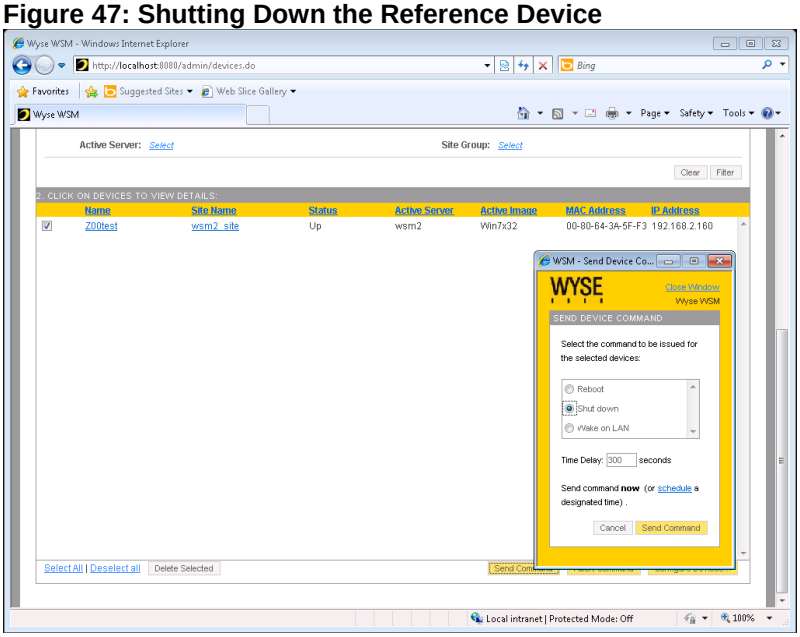
Select the Default Site group by clicking **Next>** on Step 2, the Default Site on Step 3, the default Device group on step 4, the newly created OS Image on Step 5, and finally the default Streaming Server on step 6. This should take you to the screen shown in Figure 46.

Figure 46: Adding Device Template - Step 6



Press **Finish** to complete the template creation. At this point, you should go back to the Operating Systems tab, click on your OS image, and change the **First Partition Boot Mode** to **Private** and click **Save Changes**. This will allow you to boot one device and make any last minute changes to the OS before deploying it to production. After doing this, power on one unit and verify that it gets added to the database by clicking on Devices tab and scrolling down to see if your device gets added to the database as shown in Figure 47. Once it is up and running, you can shut it down remotely by clicking box to the left of the device name and selecting **Send Command** and clicking **Shutdown**.

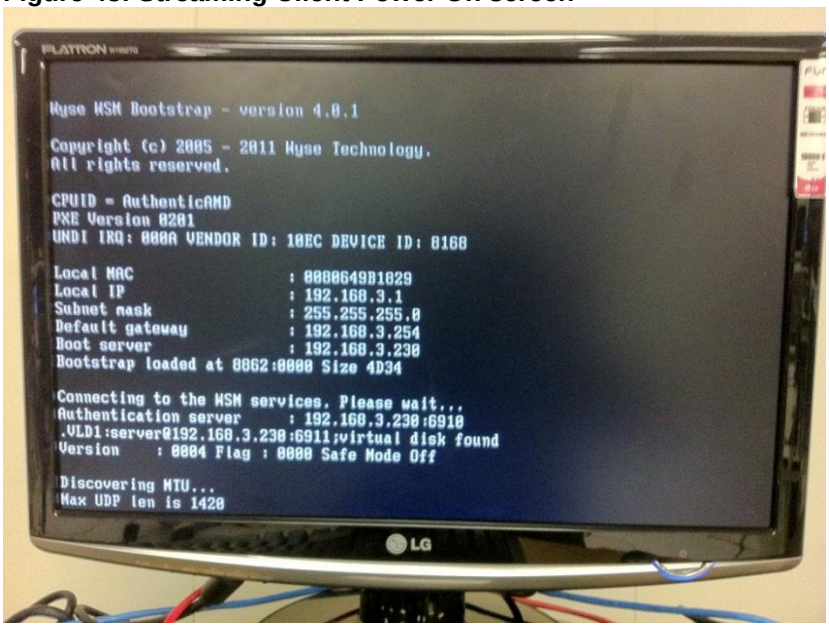
Figure 47: Shutting Down the Reference Device



Before deploying the image, go back and set the **First Partition Boot Mode** back to Persistent or Volatile mode depending on your environment. At this point, the system is up, and you have successfully completed the WSM installation.

An example boot screen on the client device is shown on Figure 48.

Figure 48: Streaming Client Power On screen



You can then go back to the Devices Screen and monitor the power on of the group of test units as shown in Figure 49 through Figure 51.

Figure 49: Monitoring Test Units Power On - Stage 1

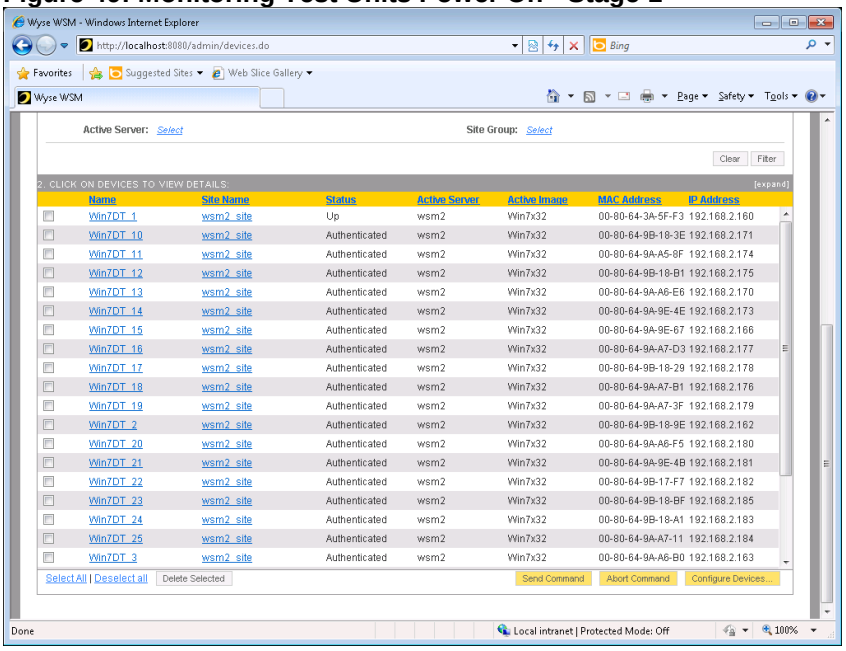


Figure 50: Monitoring Test Units Power On - Stage 2

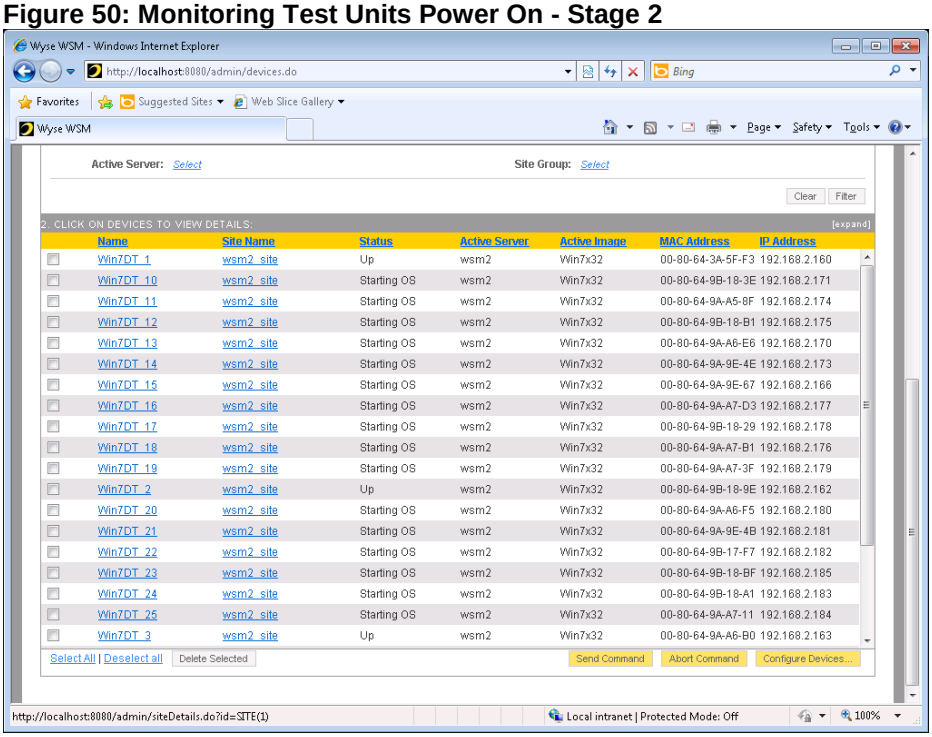
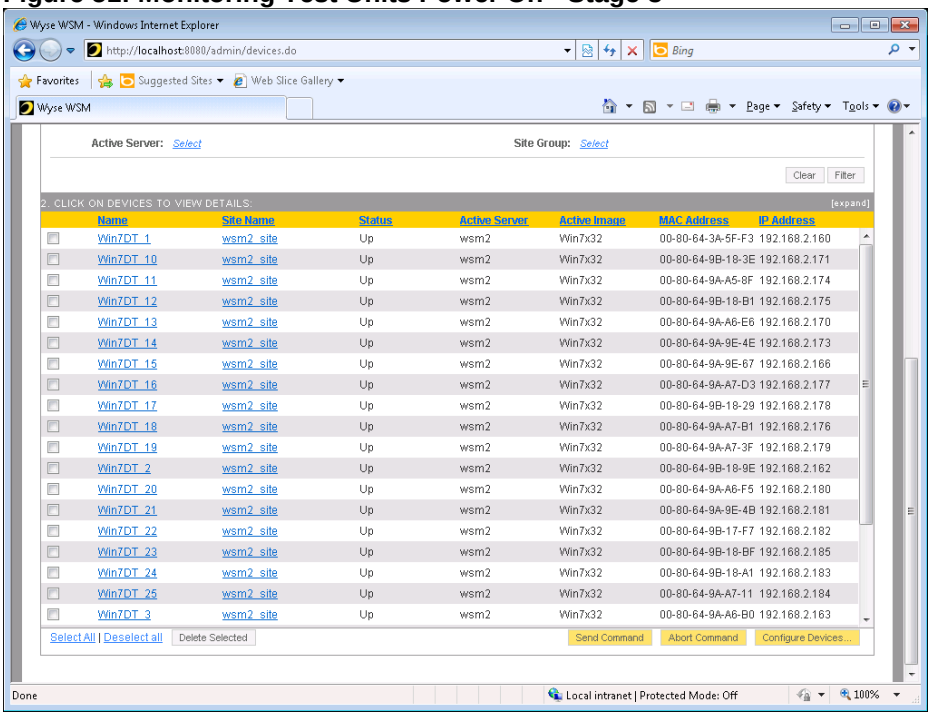


Figure 51: Monitoring Test Units Power On - Stage 3



6 Creating the Streaming Client OS image

WSM Client installation takes place on a Reference Device (PC, Wyse client device, or virtual machine). It will be built using Windows 7 Enterprise or Professional VL Edition operating system and the appropriate device drivers for your streamed clients. The Reference Device must contain all the device drivers for your client environment (the client devices to which you will stream the OS Image—traditional PC, Wyse Cloud PC, or other device). The Reference Device differs from the Streaming Client in one important way. It contains some local storage (HDD or SDD) where the Operating system and applications reside. When the image is captured and uploaded to the WSM server, the OS image will be converted into a Virtual Hard Drive image.

6.1 Installing Windows 7 Volume License Edition

In order to maintain the legality of your Microsoft OS licenses across the various streamed desktop, it is important to use the Volume License (VL) version of Windows 7. This will allow each new streamed desktop OS to authenticate with the Key Management Server which was installed in Section 3.1 above. The client OS must be a 32 bit edition. Windows 64 bit can NOT be streamed from WSM at this time.

Use a USB CD-ROM drive to install the Windows 7 Enterprise or Professional VL Edition operating system (be sure to configure the operating system to meet the needs of all client devices that will boot from it later). When installing the operating system, be sure to boot the Reference Device from the USB CD-ROM drive. If the Reference Device tries to boot from a blank flash drive, you will see a disk error. To ensure the Reference Device boots from the external USB CD-ROM drive, you must set the USB DVD drive to be the first boot device.

For most Wyse thin clients and appliances, you can use the one-time boot menu: Attach the USB CD-ROM drive to the thin client. During boot, press and hold the P key. Select the USB Drive option and press Enter.

For Wyse mobile clients, you can enter and change the BIOS Setup Utility: During boot, press and hold the F2 key. Enter the password **Fireport** (this is case sensitive) and press Enter. Select the Boot Device option and press Enter. Select the USB Drive option and move it to the 1 position by using the + key. Save the BIOS settings and reboot (you can return the original BIOS setup options at a later date if needed).

If you are using a Wyse client device, download and install the client device drivers you need for your specific device class (for example, go to http://www.wyse.com/serviceandsupport/support/downloads.asp, select Z00D under Wyse Cloud PCs in the **Please choose your product** box, click **Search**, click the File Name link for the driver zip, and then use the File Download dialog box to install the drivers).

6.2 Preparing your Reference Device for the WSM Client Software

After you have installed the operating system (and if necessary, the device drivers) on the Reference Device, you will need to make some modifications to image to enhance user experience and improve stability. Perform the same prerequisite steps on the reference device as you did for the WSM server. Make sure to disable the sleep settings in the Power Options Control panel. If your streaming client devices do not have real-time clock chips, you may want to turn on the NTP client as shown in Section 4.3 above. Also, you should also turn off any un-needed windows features using the steps outlined in Section 4.4. Make sure your Reference Device is added into the AD controller, and test the user logon procedure to insure that the roaming profiles are functioning properly.

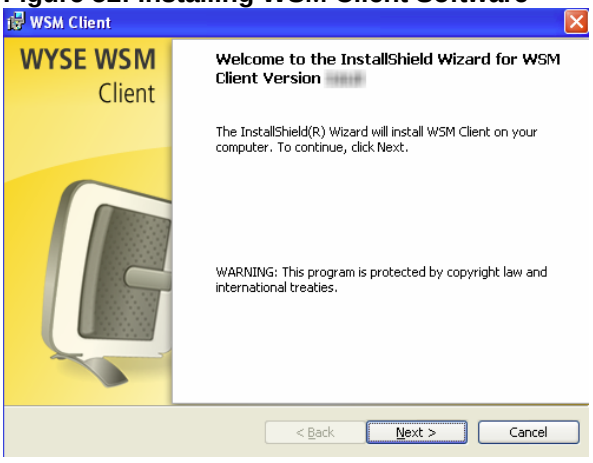
Lastly, a special hotfix from Microsoft is necessary to correct an issue related to a bug that prevents client devices from accepting the streamed OS image from the WSM server. This patch requires that Service Pack 1 be installed prior to the hotfix, and this hotfix is required to be applied before loading the WSM client driver software. You can get this hotfix from the Microsoft website (make sure you download the 32 bit version of the hotfix): http://support.microsoft.com/kb/2550978

6.3 Installing the WSM Client Software

This section provides the detailed procedures you must complete to install the WSM Client. Although you can select custom installation configurations during the installation, it is recommended that you use the default configurations. WSM Client software adds the required drivers and functions for streaming the Client operating system. It also enables application streaming and subscriptions for individual client users. An easy-to-use operating system image creation tool is included in the WSM Client software, which is used to create a base OS Image that can be provisioned to client devices in your WSM environment.

Copy the WSMClient.exe program from your WSM server and place in on the desktop of the reference device. Double-click **WSMClient.exe** and accept the security **User Access Control** pop-up window. This will initiate the Install Shield program. Click **Next>** to open the End User License Agreement window.

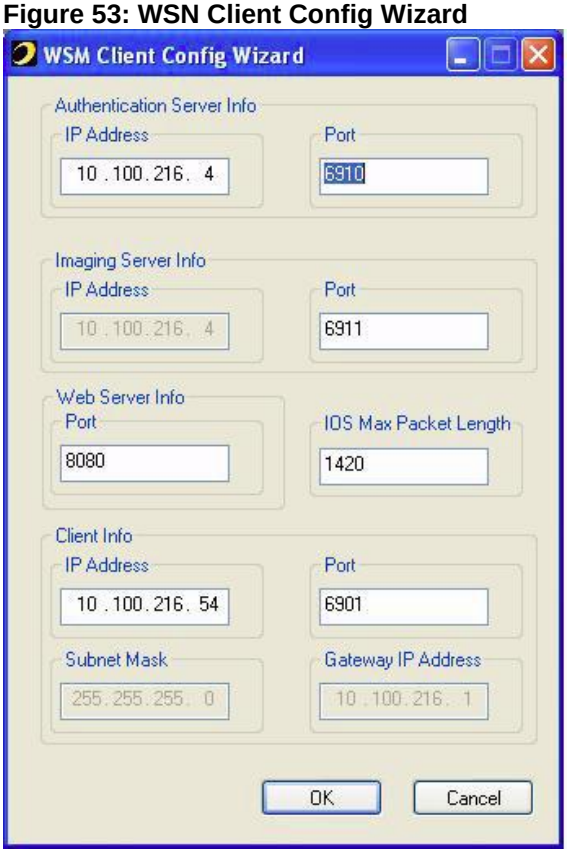
Figure 52: Installing WSM Client Software



After reading the agreement, select the **I accept the terms in the license agreement** option and click **Next>** to open the Customer Information window. Enter the User Name and Organization, and then click **Next>** to open the Destination Folder window. Click **Next>** to accept the default destination. You are ready to install, so click **Install** to begin.

During the installation, the User Account Control pop-up window may appear several times. Accept this pop-up and allow it to automatically install the software and drivers. When the software has finished installing WSM Client Configuration Wizard will appear.

Figure 53: WSN Client Config Wizard



Use the following guidelines to complete the WSM Client Config Wizard:

- Enter the **Authentication Server Info IP Address** to be used by the WSM OS Authentication Service (this address is the same as the Core Server). The **Port** information is automatically filled in with the default value. If the system administrator has changed the port number during the WSM server install, then make sure the **Port** has the same value.
- The **Imaging Server Info IP Address** is a read-only field and is the same as the **Authentication Server IP Address**. It is used by the WSM OS Streaming Service. The **Port** information is automatically filled in with the default value. If the system administrator has changed the port number during the WSM server install, then make user the **Port** has the same value.
- Enter the **Web Server Info Port** address, if necessary. This is the port on which the Web server runs. The **Port** information is automatically filled in with the default value. If the system administrator has changed the port number during the WSM server install, make sure the **Port** has the same value.
- Do not change the **IOS Max Packet Length**. This field was used when either the WSM Client or Server is a version earlier than WSM 3.6.1 (with WSM 3.6.1 or later, the client auto-discovers MTU on boot up).
- The **Client Info IP Address**, **Port**, **Subnet Mask**, and **Gateway IP Address** are automatically set and should not be changed.

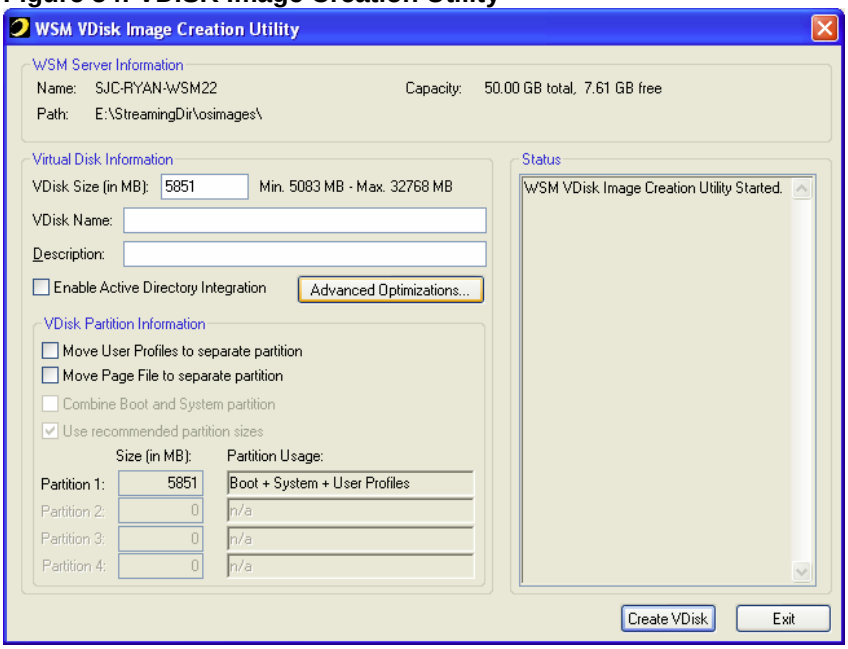
Click **Ok** and then **Finish** completing the installation.

After completing the procedures in this section, restart the system (escape out of the network boot by pressing ESC). You now have the Windows OS Image you need (including the WSM Client software, and if necessary, the device drivers) for your WSM environment on the Reference Device.

6.4 Capturing and uploading the Client OS image

To upload your OS image to the WSM server, locate OSMVDiskImage.exe (the default location is C:\Program Files\Wyse\WSM\os). Right click the OSMVDiskImage.exe and select **Run as Administrator** to open the WSM VDisk Image Creation Utility window.

Figure 54: VDISK Image Creation Utility



Use the following guidelines:

- Enter the **VDisk Size** in MB (the maximum virtual disk size is 32 GB). You may want to increase the size from the default to extend the size of the virtual disk that is assigned to the streaming client. This will provide space for any applications that may be added at a later date or to leave room for application that may be streamed from WSM. The **WSM VDisk Image Creation Utility** will not allow you to create a VDisk that is smaller than this required size.
- Enter a **VDisk Name** and a **Description** for the disk.
- Select the **Enable Active Directory Integration** check box; to integrate WSM Client authentication with Active Directory. This field is used for Application streaming to allow the Windows Login credentials to be used to authenticate the applications that are authorized for the particular user of each streamed client device.
- Clear the **Move User Profiles to a separate partition** check box since you will be using roaming profiles which map the user directory and profiles to an external file server.
- Optionally set the **Move Page File to a separate partition** check box if you want to separate out the page file from the OS image. This will allow you to set the image partition to persistent and the page file partition to volatile independently. Leaving the page file partition set to volatile will make patching the base OS image easier and will also help prevent the page file from becoming fragment during daily use.

Click **Create VDisk** to begin building the virtual disk. After building is complete, the **Done** message appears in the WSM VDisk Image Creation Utility window. Click **Finish** to complete the OS Image capturing process. The system will reboot and finish its process after the restart.

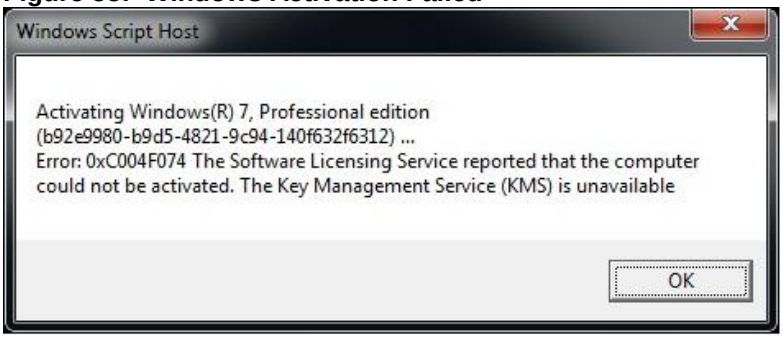
6.5 Testing the newly captured OS image

After the OS image has been captured and uploaded, add it to the WSM database using the instructions in Section 5.8. Make sure to set the image type to **Private Mode** for testing.

Boot a single streaming client and use one of the Active Directory accounts to make sure you can log into the unit. Verify that the user account is using the roaming profile, by opening a windows explorer panel and checking to see if the logical drive from the file server has been mounted for the user account.

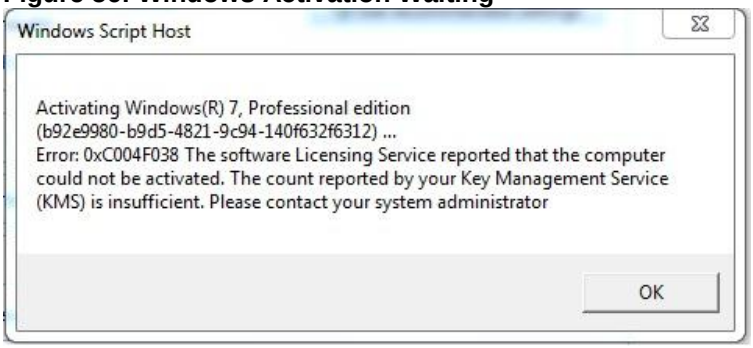
You can activate your Windows OS license with KMS by using a Command Prompt with Administrator privileges and typing the following command: **c:\windows\system32\slmgr /ato**. If your KMS server is not functioning or if your firewall rules are not set properly, you may see the error message shown in Figure 55. Double check both and retry the activation.

Figure 55: Windows Activation Failed



If your Key Management Server is functioning properly, you may still see the error message shown in Figure 56. This message indicates that KMS has not received enough requests to perform the activation. You will receive this message until you have attempted to activate at least 25 clients.

Figure 56: Windows Activation Waiting



If you are operating with less than 25 clients, you can continue to issue the **c:\windows\system32\slmgr /ato** command to bump up your activation count. Once the KMS system as received enough requests, it will start activating the streaming clients and you should see the message shown in Figure 57.

Figure 57: Window Activation Passed

Once you have validated the system, you will need to prepare the boot image for streaming mode by the Rearming process. Because multiple copies of the same image will be deployed (streamed), it is important that each one appear unique on the network. The Rearm process will provide this function. Open a command prompt with administrative privileges and issue the command:

cscript c:\windows\system32\slmgr.vbs –rearm

NOTE: This needs to be the last command issued prior to leaving **Private** mode. Any time you return the image back to private mode for system modification, you will need to rearm the system prior to shutdown.

Shutdown the streaming client, and modify the OS Image type to either **Persistent** or **Volatile** mode in WSM before booting additional clients.

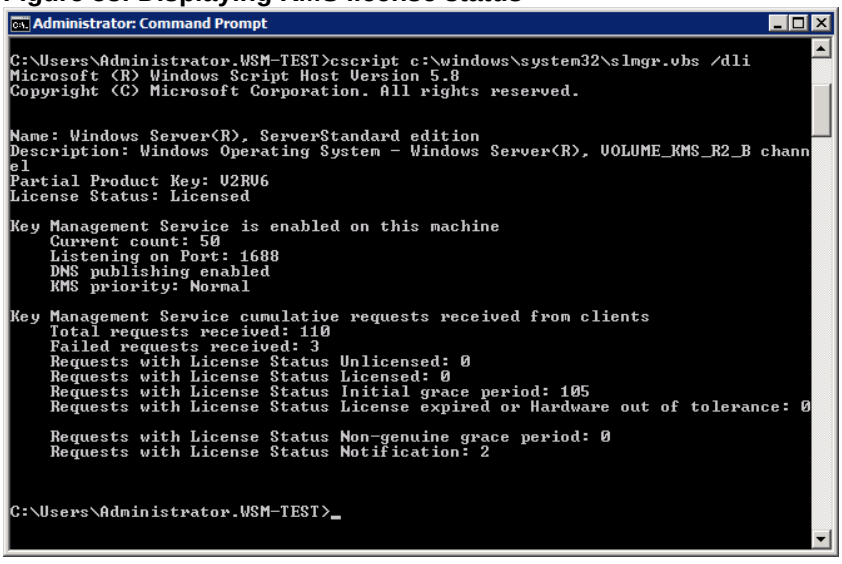
6.5.1 Verifying the KMS activation count

You can also verify the activation count on your KMS server. Using a command prompt on the server providing the KMS service, enter the command**:**

cscript c:\windows\system32\slmgr.vbs /dli.

This command will show the detailed information for KMS service. Look at the **Current count** as shown in Figure 58. This value shows the number of activate licenses.

Figure 58: Displaying KMS license status



7 Installing Management Server

While WSM is usually deployed in an existing network infrastructure, this document will guide the reader through the installation steps for adding the management infrastructure components to support the streaming operations. This document is not intended to be a complete reference guide for installing Windows Server Operating system or the application servers running on it. It is recommended that the reader be familiar with the Microsoft documentation and installation procedures. In this guide, it is assumed that the necessary management components (Active Directory (AD), DNS server, DHCP server, and Key Management Server (KMS)) are installed on the same machine. Since Microsoft AD requires a server OS such as Windows Server 2008 and KMS requires Windows Server 2008 R2 for deploying Windows 7 and Office 2010, the physical server must be 64 bit capable. The server profile (outlined above for the WSM server) can also be used for the Management Server. However, the Management Server and the WSM server must run on two separate machines. If you have an existing AD directory machine, you can skip to section 7.2.1 below.

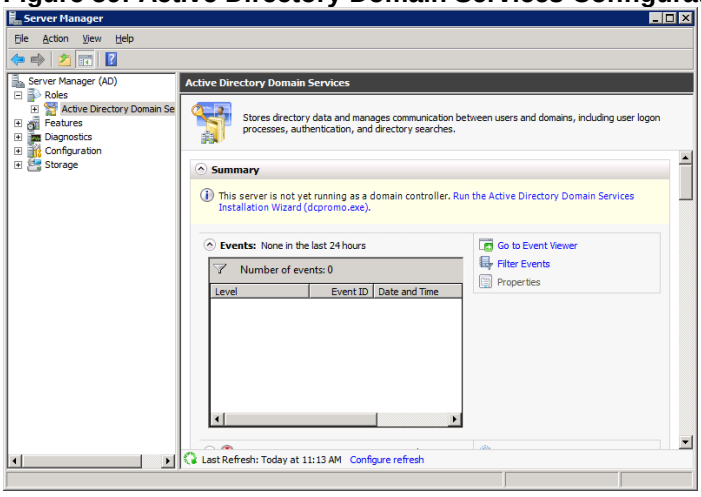
7.1 Installing Windows 2008 R2

As mentioned above, the management server must be 64 bit enabled. This is a requirement to install Microsoft Windows Server 2008 R2 since it runs only on 64 bit enabled hardware. This hardware was outlined in Section 2. Complete the normal installation and apply all required drivers and patches for the particular hardware selected. Since this machine will operate as the KMS host, do NOT activate the license at this time. To simplify the installation, make sure that this machine has a static IP address and will be in the same IP subnet as the client devices.

7.2 Configuring Active Directory

Once you have completed the normal Windows 2008 R2 server installation, open the Server Manager icon which looks like a toolbox sitting next to a tower pc. It should automatically be installed on left part of your toolbar. Once the management panel appears, you can click on the Roles and add the role of *Active Directory Domain Service.* When the Domain service is installed, it will also install the Microsoft .Net Framework. Allow it to continue. Once completed, the system will ask you to run the Active Directory Domain Service Installation Wizard (dcpromo.exe) to configure your Active Directory.

Figure 59: Active Directory Domain Services Configuration Panel



Follow the instructions and create a new Active Directory Forest for this environment. If you are not familiar with Microsoft Active Directory, there are many self-paced courses listed on the internet. There are also several instruction books such as the **Windows Server 2008 Active Directory Resource Kit** available online from retailers such as Amazon.

The DNS service role will also be added to the configuration when the Active Directory Service role is created. This will allow computers to automatically be entered into the AD structure when they are added to the DNS database. WSM will automatically populate the DNS database with the streaming client devices using the names specified within the WSM database. This is why Active Directory integration was enabled as part of the WSM installation.

If you plan to integrate *Active Directory* with WSM *without* SSL, you must ensure that the WSM *OS Authentication Service* is running with the credentials of an *Active Directory* user with privileges to create and manage computer accounts (for example, a member of the *Account Operator* group). In addition, this user must be a member of the local administrators group of the WSM server; otherwise, the OS Authentication service cannot start when being configured to run with the credentials of the *Active Directory* user. For more information about integrating *Active Directory* with WSM *without* SSL, refer to the *Administrators Guide: Wyse WSM™.*

7.2.1 Adding users to the Active Directory

In order to ensure that the client devices function specifically to a particular user, the information for all the system users must be placed into the Active Directory prior to the operating of WSM. Once a user logs onto any of the streamed client devices, the user name will be looked up in the AD and the user will be assigned the appropriate profile. This should include mounting the user's files from the appropriate file server space. It is recommended to store the users files separate from the WSM server. This allows for the network administrator to back up the users files independently from the WSM application files. In addition, if WSM is being used in Volatile Mode, the user's desktop will be wiped clean at each boot up, so storing the user's files on the WSM server would cause them to disappear as well. If WSM is used in Persistent Mode, where the desktop is NOT wiped during each boot up, the hard drive could fill up with those user files.

In order to support this, the user accounts must be set up using a roaming profile. This allows the user to access a remote file share after logon. You can manually put the entries in, or use a scripting tool to batch them together and enter at one time. To accomplish this, the free Solarwinds ***User Input Tool***, available from http://www.solarwinds.com/ was used for this document. A Comma Separated Variable (CSV) file was created in Microsoft Excel then used with this tool to populate the AD. Contact your organization's IT department to see if they already had a tool for batch entry.

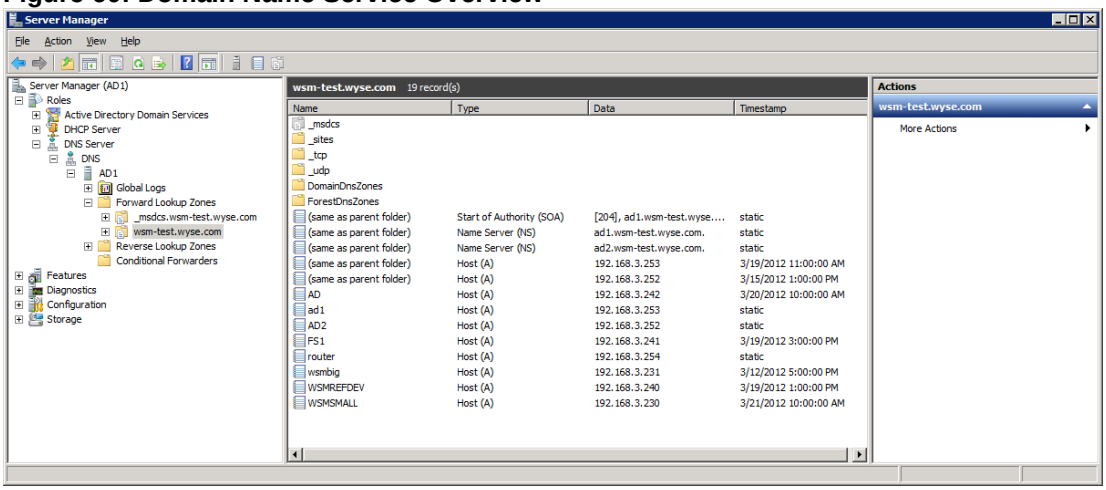
Make sure to set **Password never expires** and clear **User must change password at next login** if you are planning on doing any automated testing of the system, otherwise, the desktops will be stuck waiting for the user to change his password. These fields can easily be changed in bulk by using a third party tool such as AD Infinitum available from http://www.newfawm.com/adi2.htm.

You may need a script to create the user directories on your fileserver. Consult with your IT department on the procedures for doing so.

7.2.2 Configuring DNS Server

While the DNS Server role was added during the Active Directory configuration, you should verify the configuration and make sure both your Forward and Reverse Lookup Zones are constructed properly.

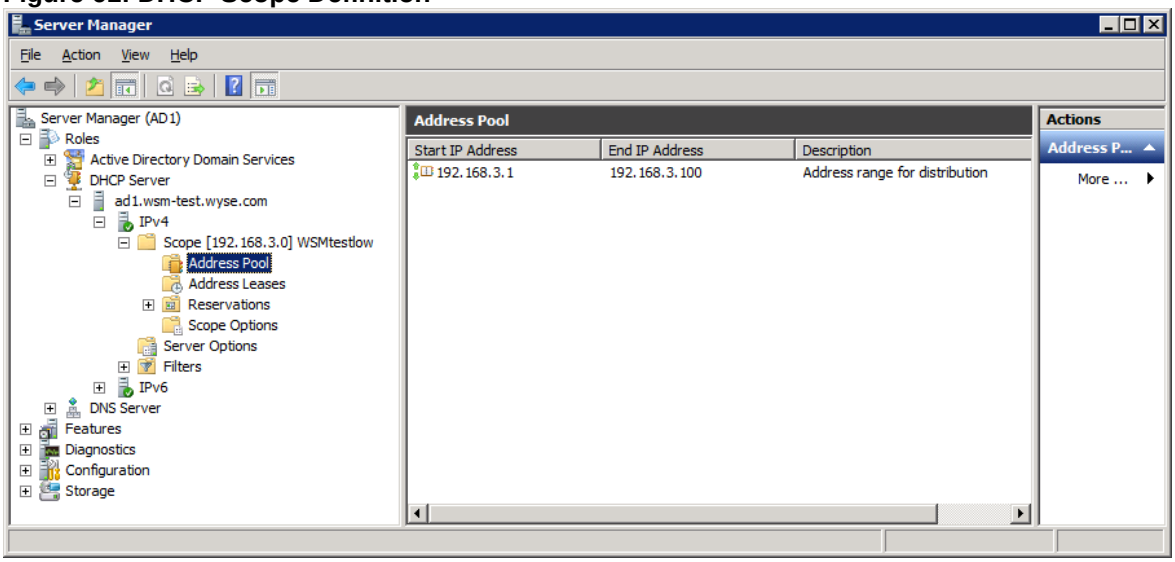
Figure 60: Domain Name Service Overview



7.3 Configuring DHCP Server

The DHCP Server role is not created by default when you enable Active Directory. You will need to enable it and create scope for the streaming client networks. As part of this scope you will need to create an address pool. It is important to specify a range that does not conflict for static IP addresses assigned for servers on that particular subnet. You can also use the **Reservations** to block out certain IP addresses. Make sure the Scope Options contain the Default Router and DNS server definitions for your network configuration.

Figure 61: DHCP Scope Definition



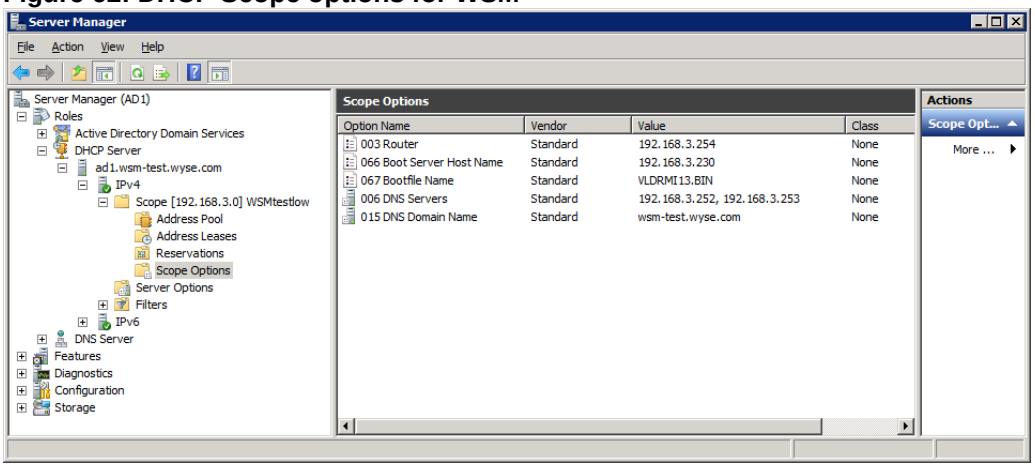
7.3.1 Adding DHCP scope options for remote DHCP and WSM servers

If your WSM server is NOT on the same subnet as your DHCP server and streaming clients, it is necessary to point the streaming clients to the location of the WSM server. This is because the DHCP request made by the streaming clients during the PXE boot phase uses standard IP broadcast packets which do not cross network boundaries.

Add two scope options 66 and 67 as shown in

Figure 62. Option 66 specifies the IP address of the WSM server and Option 67 specifies the boot image. The boot image is actually the pre-boot image that loads prior to the WSM streaming image.

Figure 62: DHCP Scope options for WSM



Appendix A: Test Configuration and Results

This section documents the lab configuration tested as part of this reference architecture and configuration guide. This was a closed environment where all the resources described below were dedicated to the WSM testing. **Wyse recommends up to 50 streaming clients using this configuration for optimal performance**. Using WSM in a production network may yield different results depending on the size of the streamed image, applications running on the desktop, and user operation.

Network equipment

Cisco 3560G-24PS for Corporate Switch
Dell 5548 for Wiring Closet Switch

Management Server (Core services DNS, DHCP, KMS & AD) - Dell Optiplex 755

Intel Core2 Duo E8400 3.0 GHz
4 GB of Memory
80 GB HDD
Windows 2008 Server R2 Standard
Active Directory, DNS, DHCP, and KMS services

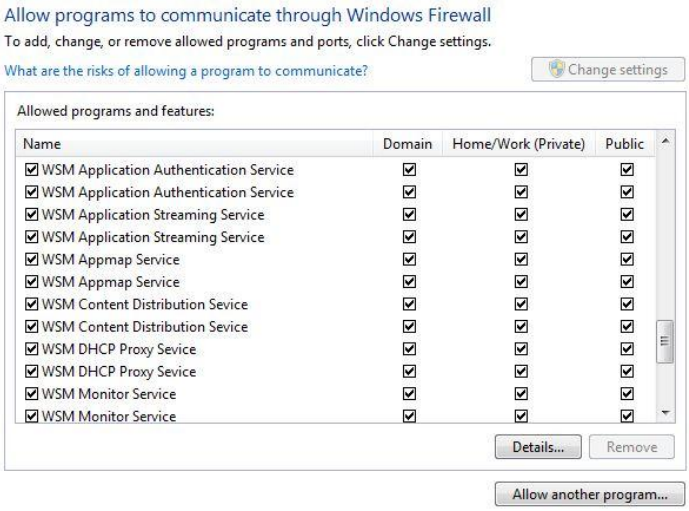
WSM Server

The following server was used for the reference architecture,

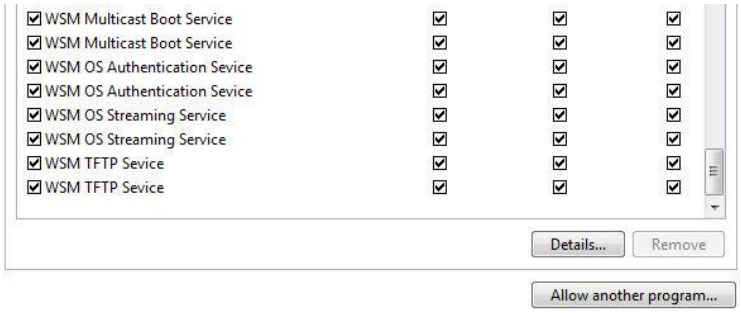
Parameter	Details
Server Model	Dell PowerEdge T110 II
Chassis type	Cabled 6x2.5 hard drives
CPU	Intel Core I3 2100 3.1 GHz, 3M cache, dual core/4T
Memory	8GB memory (2x4GB), 1333MHz
OS	Ordered with no OS. Windows 7 64 bit will be installed as stated above (Section #4.1)
SAS Controller	PERC 200 internal RAID adapter
Hard drives	2 x 300GB 10K SAS 6Gbps 2.5in drives
Network	Broadcom 5709 dual port 1GbE NIC. This adapter is in addition to the onboard 1 GbE NIC port

In our lab test, we also loaded Microsoft Security Essentials available from the website at: http://windows.microsoft.com/en-US/windows/products/security-essentials

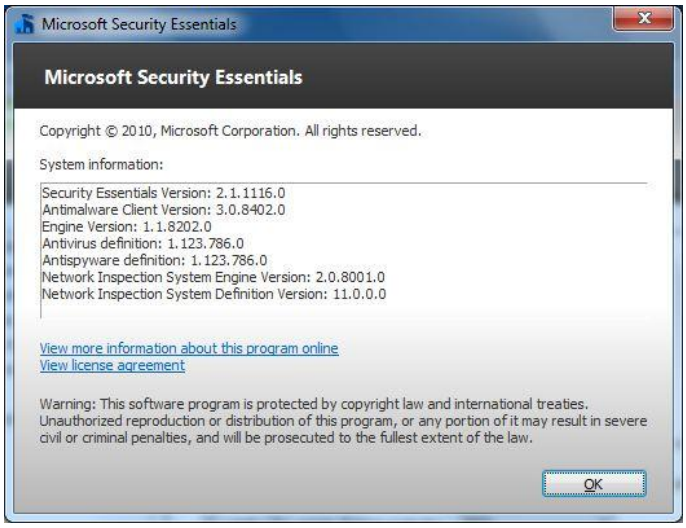
After installing the software, you will need to enable the Windows Firewall filter rules for WSM:



And scroll down to get the remaining services:



You can verify the installation by double clicking on the toolbar icon and select **Help** and **About**.



Streaming Client – Wyse Z00D and Wyse X00M

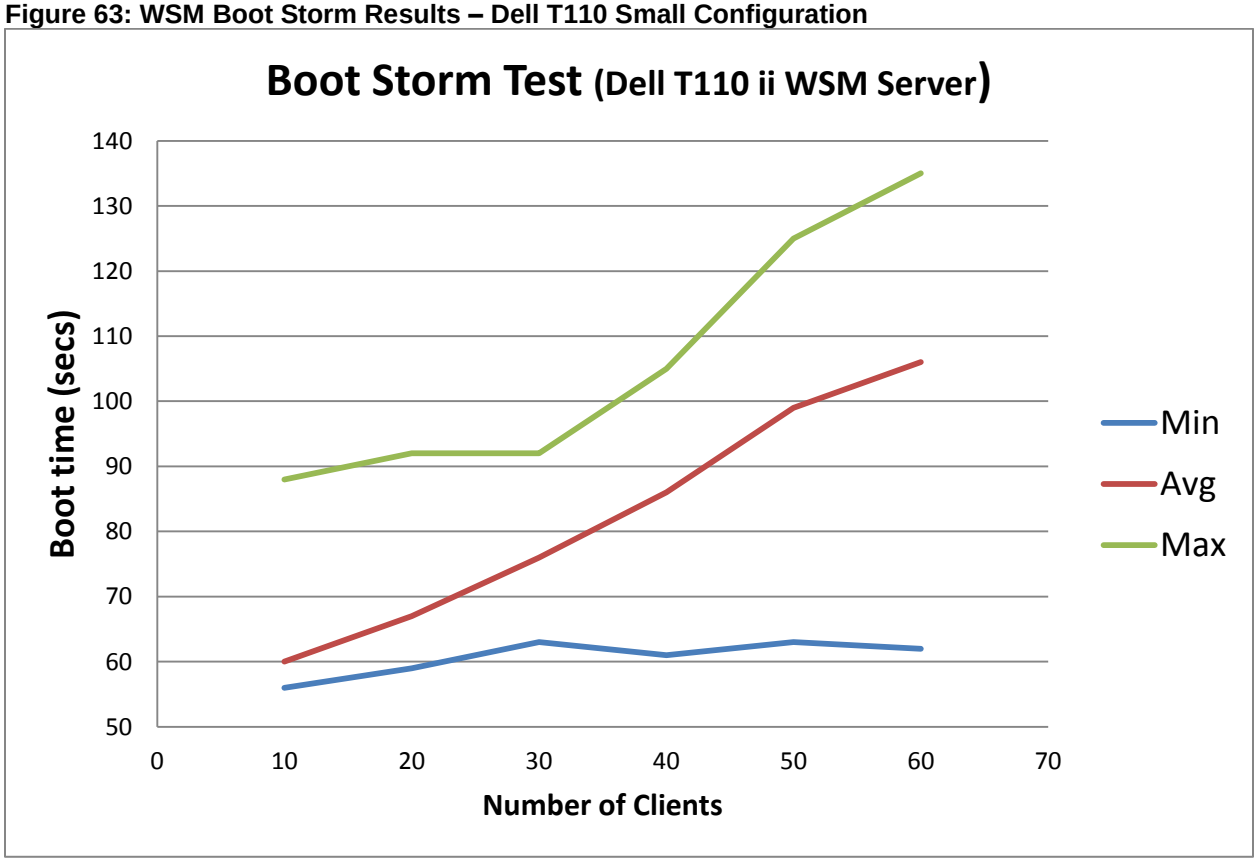
AMD G-T56N Dual Core 1.6 GHz
2 GB of Memory
Windows 7 Professional x32 (streamed from WSM)

VDISK image details – 25 GB

Windows 7 Professional x32 with SP1
Adobe Flash Player 11 ActiveX
Adobe Reader X (10.1.2)
AMD Catalyst Install Manager (Video Driver)
Google Chrome 17.0963.79 m
Google Earth 6.2.1.6014 (beta)
Microsoft .NET Framework Client Profile
Microsoft Visual C++ Studio x86 Redistributable – 10.0.30319
Mozilla Firefox 11.0 (x86 en-US)
Realtek High Definition Audio Driver
Renesas Electronics USB 3.0 Host Controller Driver
Wyse WSM Client

Testing was done with the above equipment using the instructions provided in this document. Streaming client boot storm test results were collected for groups of 10, 20, 30, 40, 50, and 60 simultaneous booting client devices. The times shown in Figure 63 reflect the data collected from the LSLog.txt file located on the WSM server in the **c:/Program Files (x86)/Wyse/WSM/**Log directory. This time does not include the initial DHCP and PXE start times which were approximately 25 seconds collectively and the time for the auto login and remote drive mapping after the boot which accounts for another 15-20 seconds depending on your fileserver and network configuration.

Figure 63: WSM Boot Storm Results – Dell T110 Small Configuration



During the boot storms, data was collected using Perfmon and Task Manager on the WSM server. The resources used during the boot storms were recorded in Figure 64. These were the burst values. Average usage of each of these resources was much less.

Figure 64: WSM Server Resources Used (Burst values)

# of clients	CPU usage (%)	Memory (MB)	Disk Usage (MBps)	Network Usage (Mbps)
10	45	2770	3	970
20	67	3694	4	980
30	57	4278	9	1300
40	58	4355	10	1400
50	73	5682	8	1300
60	90	5960	8	1400

One important data point is that the boot storms present the maximum load on the server from a resource perspective. The times and system resources needed are dependent on the size of the VDISK image. For example, if the vdisk image is in and around 25GB, the performance and usage can be expected as seen above. If the vdisk size increases significantly like 35GB, 40GB etc.., the performance metrics as in the number of clients supported will be smaller. The general rule is as follows,

Number of theoretical maximum clients = 70-75 %(2000/vdisk size in GB)

Example 1:

Vdisk size = 25GB

70 %(2000/25) ~ 50 users

Example 2:

Vdisk size = 35GB

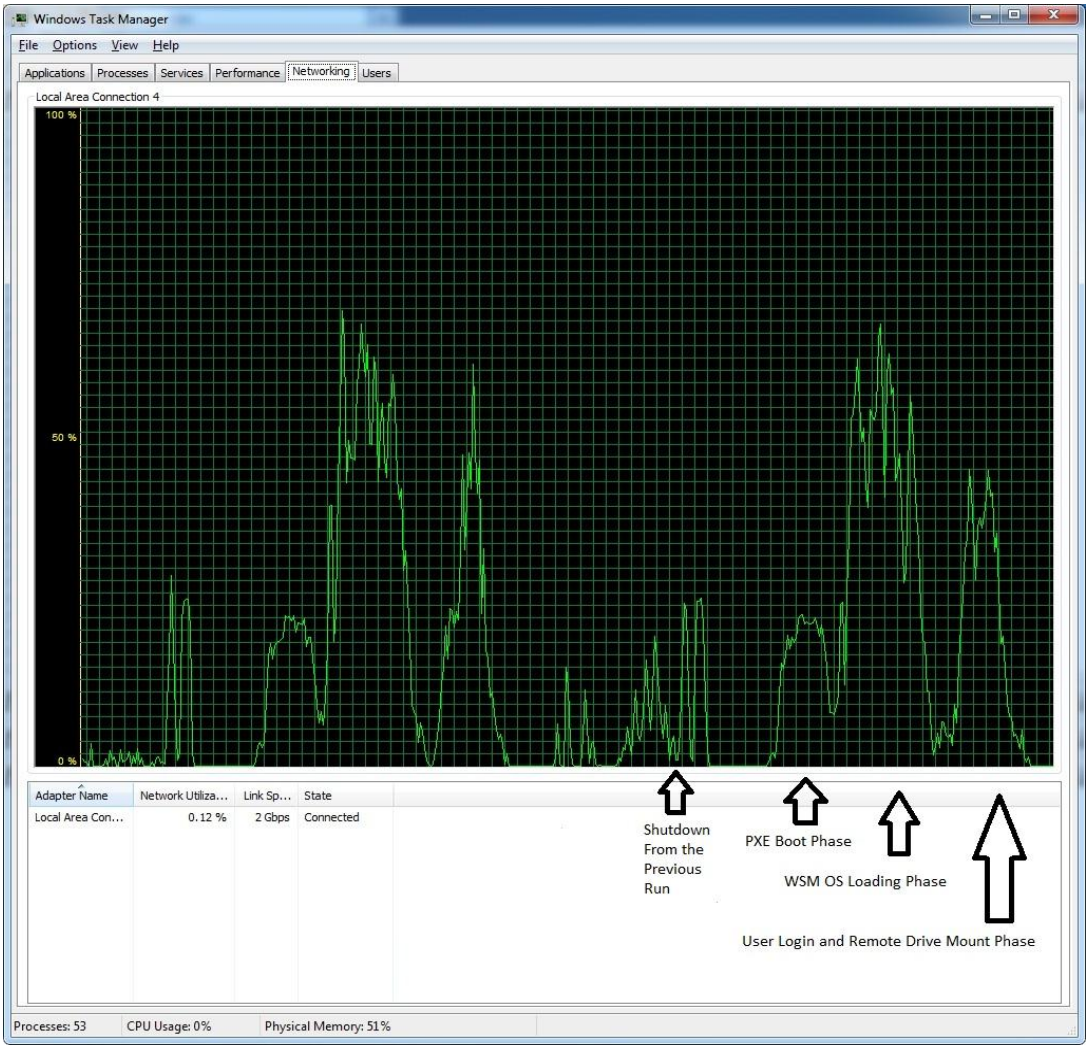
70%(2000/25) ~ 40 users

Please note that the above formula is a general guideline. Other parameters like network limitations will play a factor in optimal performance tuning.

The next phase of testing will include resource utilization during user activity. Application loading and usage will be recorded and presented in a future version.

The network utilization was also recorded from the task manager and recorded for 30 users in Figure 65. Each tick mark in the time domain represents 6 seconds. In this figure, you can see the peaks for the various phases of the booting process. The first set of peaks represents the traffic sent from WSM to tell the streaming clients to shut down and the traffic sent from the clients to close out the open files and disconnect the remotely mounted drives. There is about a 30 second pause while the clients are executing their BIOS commands and waiting for an answer from the DHCP server. The second phase is when the client devices load the pre-booter via PXE boot. The Third Phase is the OS image loading from the WSM server. The last set of peaks show network traffic for the auto login using a user roaming profiles and remote file server mounts for the home directories.

Figure 65: Network Usage during 30 user Boot Storm


Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
Local Area Connection 4
100 %
50 %
0 %
Adapter Name
Network Utiliza...
Link Sp...
State
Local Area Con...
0.12 %
2 Gbps
Connected
Shutdown From the Previous Run
PXE Boot Phase
WSM OS Loading Phase
User Login and Remote Drive Mount Phase
Processes: 53
CPU Usage: 0%
Physical Memory: 51%