Microsoft Enterprise Desktop Virtualization

MED-V Installation and Configuration Manual

MED-V v1 Beta

04.01.09

Contents

Preface

Intended Audience

This Installation and Configuration manual provides background information about MED-V, installing MED-V, how it works and explains how to correctly use the product.

The intended audience is MED-V administrators and IT personnel.

Chapter 1

1. MED-V Overview

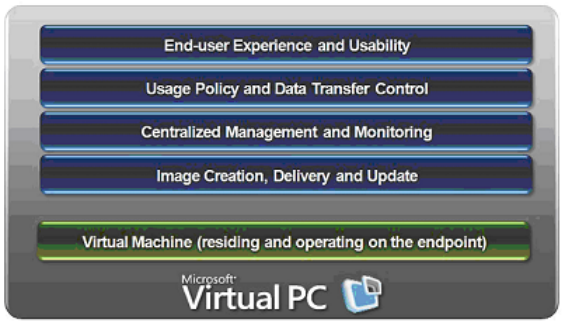
In This Chapter

1.1. Introduction to Microsoft Enterprise Desktop Virtualization (MED-V)

Microsoft® Enterprise Desktop Virtualization (MED-V) enhances deployment and management of Virtual PC images on a Windows® Desktop, while also providing a seamless user experience of a Virtual PC environment, independent of the local desktop configuration and operating system (OS).

MED-V leverages Microsoft Virtual PC to provide an enterprise solution for desktop virtualization. With MED-V, you can easily create, deliver and manage corporate Virtual PC images on any Windows desktop.

MED-V is an integral component of the Microsoft Desktop Optimization Pack, a dynamic solution available to Software Assurance customers, which helps reduce application deployment costs, enables delivery of applications as services, and helps to better manage and control enterprise desktop environments.



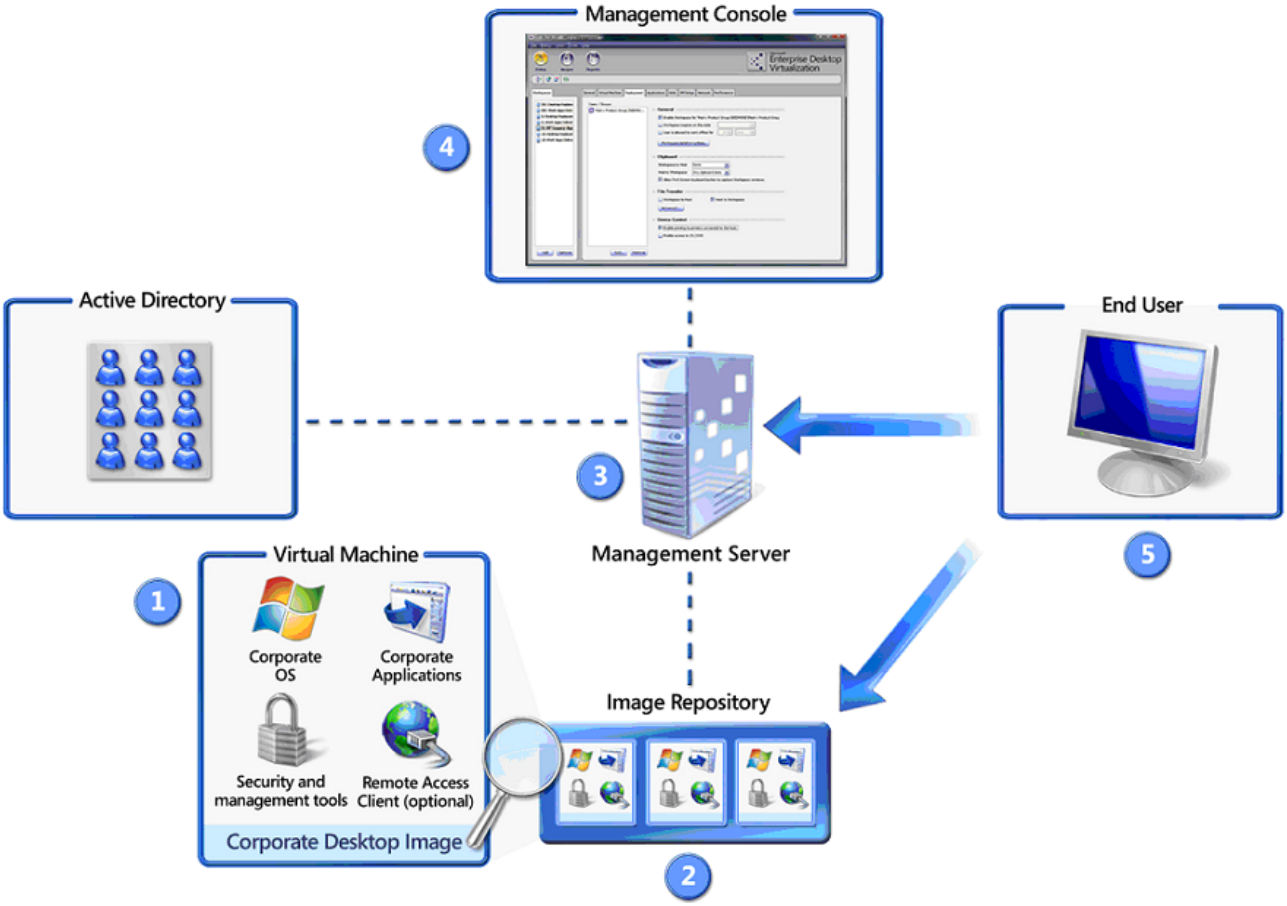
1.1.1. Enable legacy applications and accelerate upgrades to new operating systems

Incompatibility of legacy applications with the new version of Microsoft Windows can often delay enterprise upgrades to the latest version of Windows. Testing and migrating applications can take a while, and users are unable to take advantage of the new capabilities and enhancements offered by the new OS.

By delivering applications in a Virtual PC that runs a previous version of the OS (e.g., Windows XP or Windows 2000), MED-V removes the barriers to OS upgrades, and allows administrators to complete testing and to deal with incompatible applications after the upgrade.

From the user's perspective, these applications are accessible from the standard desktop Start menu and appear side-by-side with native applications – so there is minimal change to the user experience.

1.2. High-level Architecture



The MED-V solution comprises:

- **Administrator-defined "master" virtual machine (1)** - encapsulates a full desktop environment: an OS, applications and optional management and security tools.
- **Image Repository (2) -** stores all virtual images on a standard IIS server and enables virtual images version management, client-authenticated image retrieval, and efficient download (of a new image or an updates) via Trim Transfer technology.
- **Management Server (3)** - associates virtual images from the image repository along with administrator usage policies to Microsoft Active Directory users or groups. The Management Server also aggregates clients' events, and stores them in an external database (MS SQL) for monitoring and reporting purposes.
- A unified **Management Console (4)** - enables administrators to control the Management Server and the Image Repository.
- **End-user Client (5)**

  a. Virtual image life-cycle – Authentication, image retrieval, enforcement of usage policies.

  b. Virtual machine session management - Background start, stop, suspend of the virtual machine.

  c. Single desktop experience - Seamlessly make the applications installed in the virtual machine available through the standard desktop Start menu, and integrate the applications with other applications on the user desktop.

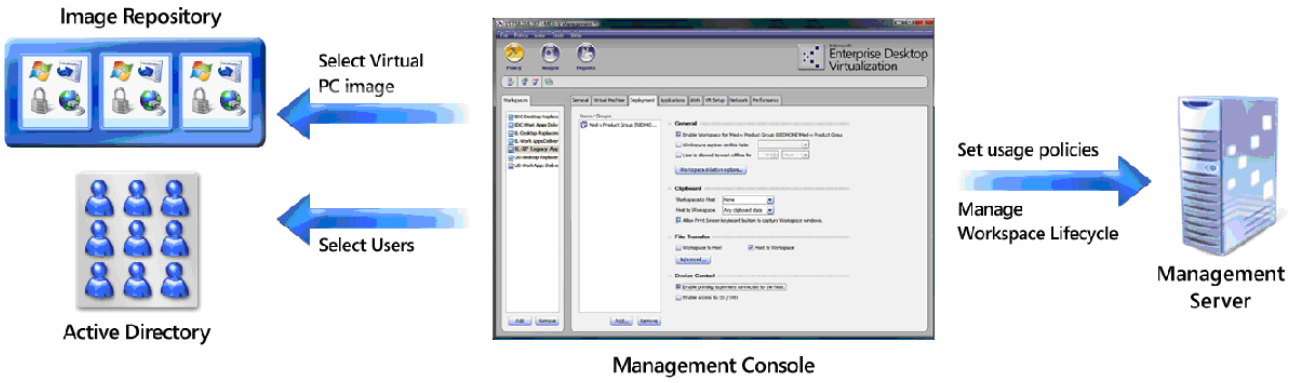
All communication between the client and the servers (Management Server and Image Repository) is carried on top of a standard HTTPs channel.

1.3. Virtual Image Lifecycle Overview

The following describes the typical lifecycle of a MED-V virtual image:

- **Create a virtual image** within Microsoft Virtual PC.
- **Define a MED-V Workspace**

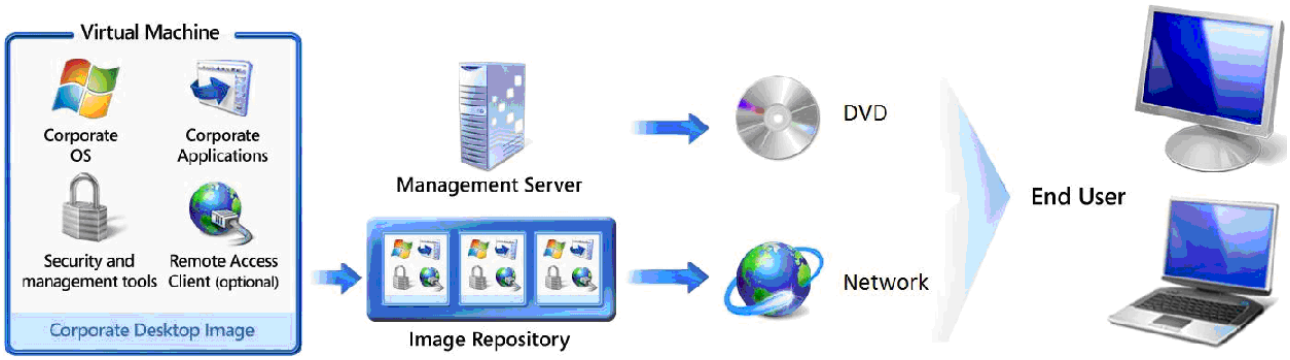
  A Workspace is a virtual image, associated with a set of usage policies and provisioned to specific users:



  - Create a list of applications installed in the virtual image, which are to be made available to end users through their standard desktop Start menu.
  - If applicable, define web sites that should be viewed inside the virtual machine browser, and that are redirected from the host browser to the virtual machine by MED-V client.

- Provision the workspace to Active Directory users and groups.

- **Test the Image** through the MED-V management console, and load it to the MED-V Image Repository.
- **Deploy the MED-V Client via**:
  - **Enterprise software distribution tools**, e.g., System Center Configuration Manager. The MED-V client and Virtual PC software can be deployed as standard MSIs.
  - **Self-install package** - Deliver MED-V "One-click" installation package, which includes MED-V client installation and Virtual PC software, over a self-service website, or by using removable media (e.g., CD, DVD). Installation process is automated, silent and easy for end users.
- **Deliver the virtual image**:



  - **Over the network** - Once the MED-V Client is installed, using any of the previously mentioned methods, the virtual image can be retrieved over the network using standard HTTP/HTTPs tunnel. Trim Transfer technology will accelerate download speed and reduce required bandwidth, as described in a following section.
  - **Using enterprise distribution mechanisms** – Administrators may choose to deliver packaged virtual PC images (created by the MED-V Management Console) using existing systems. The MED-V Client will look for the package in a pre-defined path, and extract the image.
  - **Over a removable media (e.g., DVD)** - When delivering an installation media to the end user, it is possible to add the virtual image to the self-install package. As part of the installation, the virtual image is copied to the local drive.
- **End-users start working** - Users authenticate against the MED-V Management Server and they're ready to work within the virtual machine. After the first online authentication, offline work is also supported, if permitted by the administrator.
- **Manage and update the Workspace** - The Management Console enables administrators to easily update usage policies, provision workspaces to additional users, deprovision existing users, and update the virtual images themselves. All updates are automatically distributed to relevant users when they work online.
- **Monitoring clients** – The MED-V Management Console presents an updated report of all the users. It provides detailed information on all client events, and when there is an error, it and can help the administrator understand the source of the problem remotely, and instruct the user on how to solve it.

Chapter 2

2. Installing MED-V

In This Chapter

2.1. Installing the MED-V Server

2.1.1. MED-V Server Installation Prerequisites

This section describes all the components that must be installed and configured prior to installing the MED-V Server and explains the following tasks:

- Server System Requirements
- Active Directory Requirements
- Installing the Report Database

2.1.1.1. Server System Requirements

The recommended system configuration for use of MED-V is provided in the following table. System performance will be improved when utilizing a system with the recommended system configuration.

Table 1: Recommended System Configuration

Memory	2 GB RAM or greater
Processor	2 GHz or faster
Operating system	Windows Server 2008 Standard/Enterprise Edition x86 & 64 bits
Database	MS SQL Server 2005 Enterprise Edition SP2 MS SQL 2008 Express / Standard / Enterprise editions

2.1.1.2. Active Directory Requirements

When configuring the MED-V Server, if users are not part of the same domain the server belongs to, a trust must be set between the domains.

2.1.1.3. Installing the Report Database

The report database is required for storing all Workspace logs. The log database is then used for generating MED-V reports. For information on reports, refer to Generating Reports.

The SQL server can be installed on the same server as the MED-V server, or on a remote server. If installing on a remote server, refer to Installing SQL Server on a Remote Server.

Installing SQL Server on a Remote Server

To install SQL Server on a remote server:

1. Configure the following on the remote server:
   - Instance name - default instance
   - Authentication mode - mixed mode
   - User - the default user created is 'sa'
   - Password - desired password
   - Collation Settings - default
   - Error in usage report settings - default
2. Install the following files on the MED-V server:
   - Microsoft SQL server native client (Installs the prerequisites for the management objects collection)

     http://download.microsoft.com/download/4/4/D/44DBDE61-B385-4FC2-A67D-48053B8F9FAD/sqlncli.msi
   - Microsoft SQL server management objects collection (includes required dll files)

     http://download.microsoft.com/download/4/4/D/44DBDE61-B385-4FC2-A67D-48053B8F9FAD/SQLServer2005_XMO.msi
   - Feature Pack for Microsoft SQL Server
     http://www.microsoft.com/downloads/details.aspx?FamilyId=D09C1D60-A13C-4479-9B91-9E8B9D835CDC&displaylang=en

2.1.2. Installing and Configuring the MED-V Server

2.1.2.1. Installing the MED-V Server

To install the MED-V server:

1. Install the MED-V Server MSI.

   The MED-V Server MSI is called `MED-V_Server_x.msi`, where x is the version number.

   For example, `MED-V_Server_1.0.65.msi`.

   The **InstallShield Wizard Welcome** screen appears.
2. Click **Next**.

   The **MED-V Server License Agreement** screen appears.
3. Read the license agreement, click **I accept the terms in the license agreement** and then click **Next**.

   The **Destination Folder** screen appears, with the default installation folder displayed.

The default installation folder is `%systemdrive%\Program Files\Microsoft Enterprise Desktop Virtualization\`.

- To change the folder where MED-V should be installed, click **Change...** and browse to an existing folder.

4. Click **Next**.

   The **Ready to Install** screen appears.

5. To continue with the Installation, click **Install**.

   MED-V Server installation starts. This can take several minutes, and the screen may not display text. During installation, several progress screens appear. If an error message appears, follow the instructions provided.

   Upon successful installation, the **Installation Complete** screen appears.

6. Click **Finish** to complete the wizard.

Note: If you are installing the MED-V Server via Microsoft Remote Desktop, use the following syntax: `mstsc/console`. Ensure that your RDP session is directed to the console.

2.1.2.2. Configuring Server Settings

The following server settings can be configured:

- Connections
- Images
- Permissions
- Reports

Configuring Connections

To configure connections:

1. From the Windows Start menu, select **All Programs > MED-V > MED-V Server Configuration Manager**.

   Note: If you selected the **Launch MED-V Server Configuration Manager** check box during the server installation, the MED-V Server Configuration Manager starts automatically once the server installation is complete.

   The MED-V Server Configuration Manager appears.

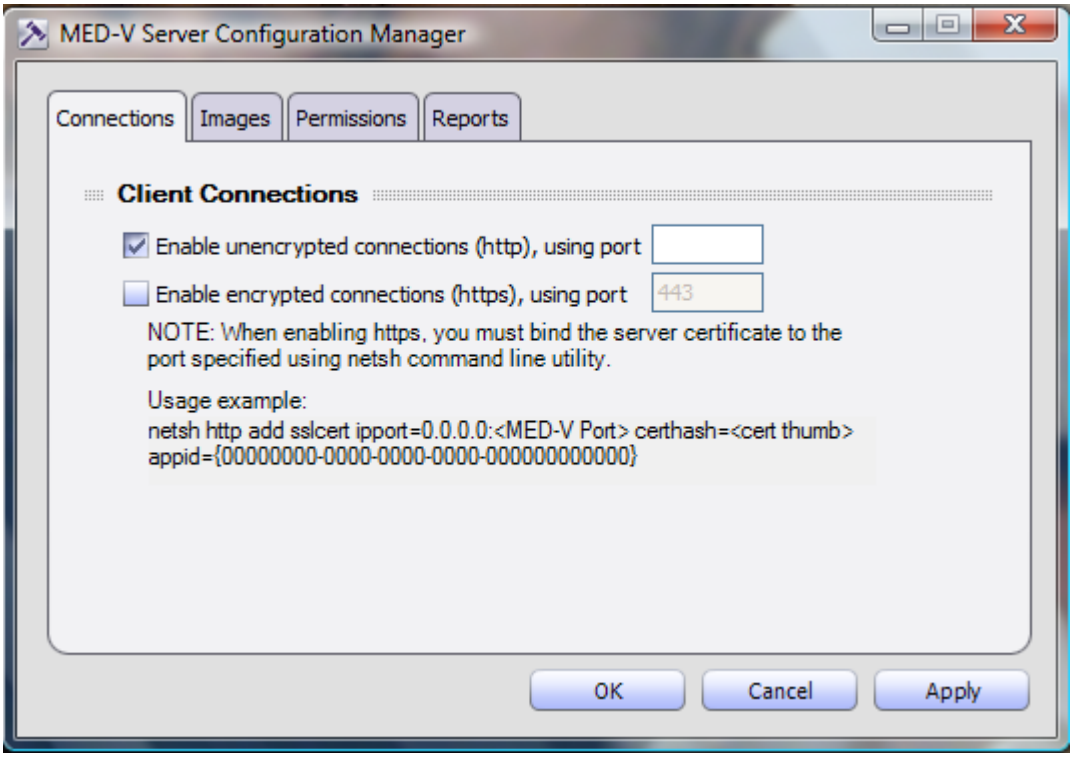


Figure 1: MED-V Server Configuration Manager - Connections Tab

2. In the Connection tab, configure the following client connections settings:
   - **Enable unencrypted connections (http), using port** - Select this check box to enable unencrypted connections using a specified port. In the port box, enter the server port on which to accept unencrypted connections (http).
   - **Enable encrypted connections (https), using port** - Select this check box to enable encrypted connections using a specified port. In the port box, enter the server port on which to accept encrypted connections (https).

     Https is an optional configuration which can be set to ensure secure transactions between the MED-V Server and MED-V Clients. To configure https, you must perform the following procedures:
     - Configure a certificate on the server.
     - Associate the server certificate with the port specified using netsh.
3. Click **OK**.

Configuring Images

To configure images:

1. Click the **Images** tab.

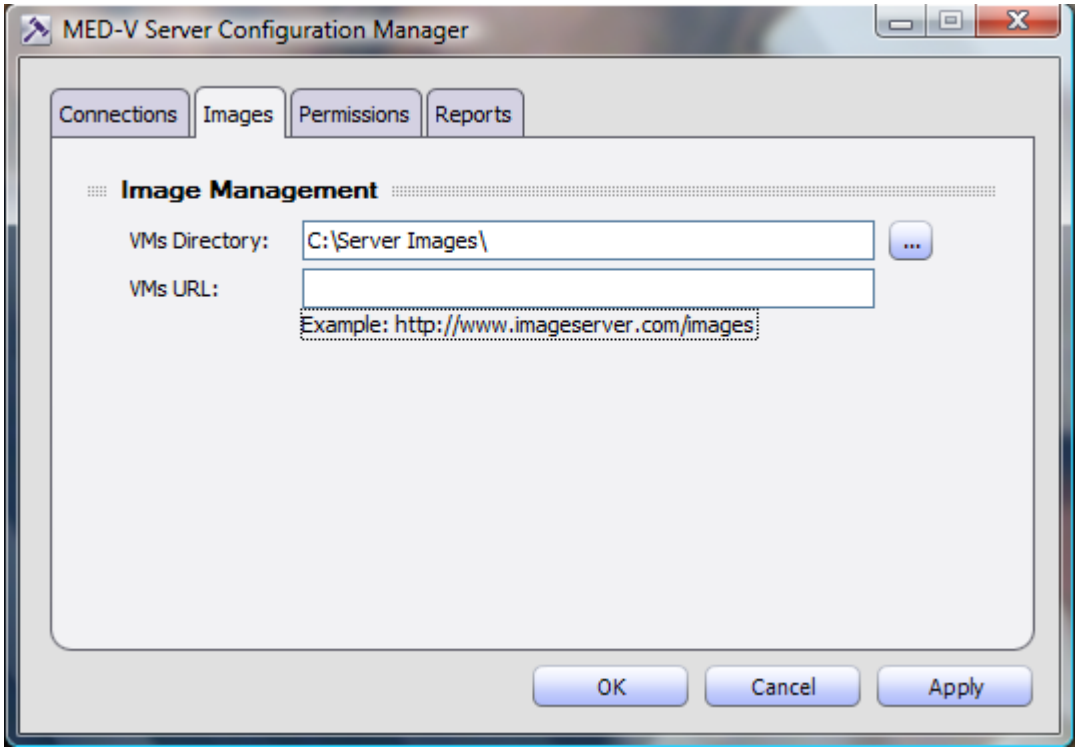


Figure 2: MED-V Server Configuration Manager - Images Tab

2. Configure the following image management settings:
   - **VMS Directory** - The Virtual Machine directory (the directory where the images are stored). This field contains a UNC path to the image directory on the image distribution server that should be accessible from the MED-V server machine.
   - **VMS URL** - The location of the server where the images are stored.

   Note: For details on how to configure an IIS server to serve as an image download server, see Configuring Internet Information Services (IIS).

3. Click **OK**.

Configuring Permissions

To configure permissions:

1. Click the **Permissions** tab.

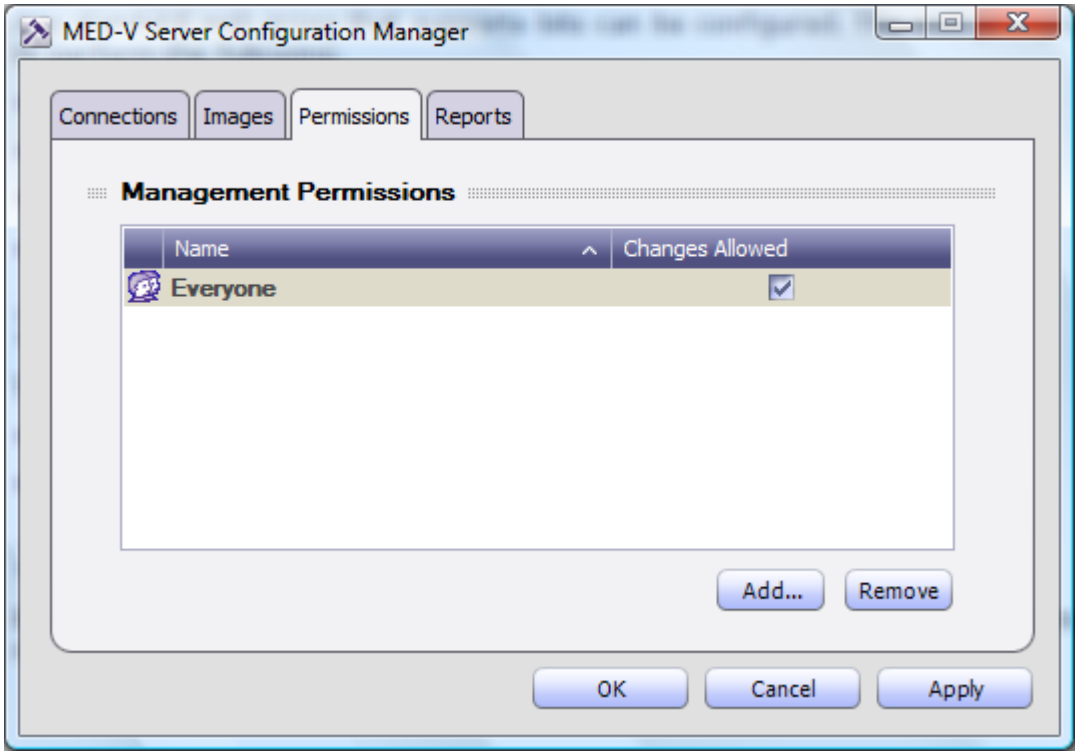


Figure 3: MED-V Server Configuration Manager - Permissions Tab

2. A list of all users who can login is provided. To apply read and write permissions to a user, select the check box next to the user. To apply read-only permissions to a user, clear the check box.
3. To add domain users or groups, click **Add...**.

   The **Enter Users/Groups** dialog box appears.

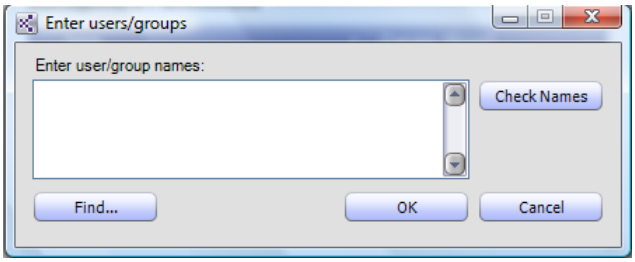


Figure 4: Users/Groups Selection Dialog Box

   a. Select the domain users or groups that you wish to add by doing one of the following:
      - In the **Enter user/group names** field, type a user or group which exists in the domain or as a local user or group on the computer. Then click **Check Names** to resolve it to the full existent name.
      - Click **Find...** to open the standard **Select Users/Groups** dialog box. Then select the domain users or groups you wish to add.

   b. Click **OK**.
4. To remove domain users/groups, select a user/group and click **Remove**.
5. Click **OK**.

Configuring Reports

To configure reports:

1. Click the **Reports** tab.

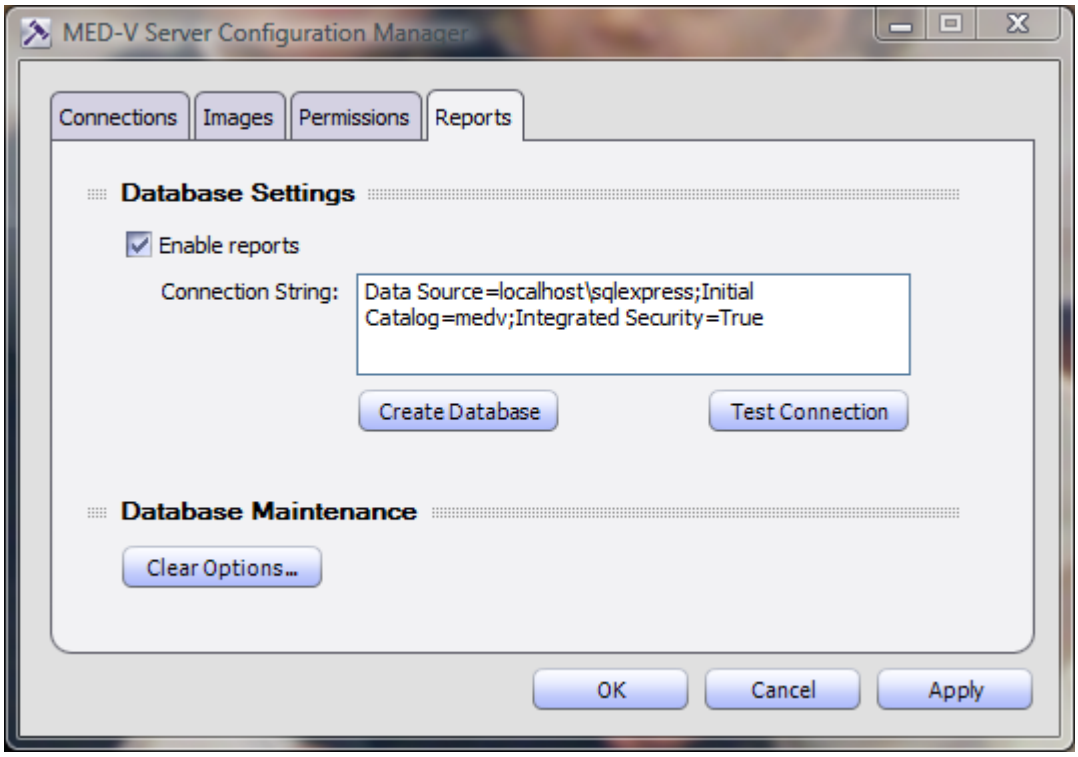


Figure 5: MED-V Server Configuration Manager - Reports Tab

2. To support reports, select **Enable reports**.
3. In the **Connection String** box, enter a connection string for the MSSQL database.
   - When SQL Server is installed on a remote server, use the following connection string:
     `Data Source=<ServerName>;Initial Catalog=<DBName>;uid=sa;pwd=<Password>;`

Note: To connect to SQL Express, use: `Data Source=<ServerName>\sqlexpress`.

4. To create the database, click **Create Database**.
5. To test the connection, click **Test Connection**.
6. To configure database clearing options, click **Clear Options**.

   The **Clear Database Options** dialog box appears.

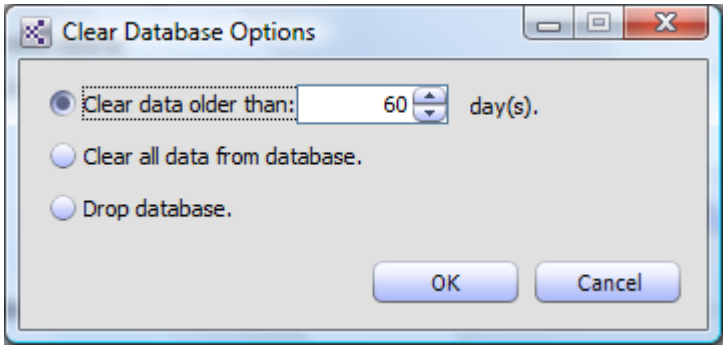


Figure 6: Database Delete Options Dialog Box

a. Choose one of the following options:
   - **Clear data older than** - clear all data older than the number of days specified; in the number box, enter a number of days.
   - **Clear all data from database** - clear all existent data in the database.
   - **Drop database** - delete the database.

b. Click **Delete** to apply changes and close the dialog box.

7. Click **OK** to save the changes or **Cancel** to close the dialog without saving changes.
8. If prompted, restart the MED-V Server service to apply changes to the network settings.

2.2. Installing the MED-V Client and Management

2.2.1. Client Installation Prerequisites

This section describes all the components that must be installed and configured prior to the MED-V Client installation, and explains the following tasks:

- Client System Requirements
- Antivirus/Backup Software Configuration
- Virtual Machine System Requirements
- Installing and Configuring Microsoft Virtual PC 2007

2.2.1.1. Client System Requirements

The recommended system configuration for use of MED-V Client is provided in the following table. System performance will be improved when utilizing a system with the recommended system configuration.

Table 2: Recommended System Configuration

Memory	Minimum: 1 GB Recommended: 2 GB
Free disk space	10 GB
Operating System	Windows XP SP2/3 (Pro, Home), Vista SP1 (Enterprise, Home Basic, Home Premium, Business, Ultimate) 32 bit
Web browser	Microsoft Internet Explorer 7.0
File System	NTFS

Additional Items or Services Required:

Microsoft.NET Framework Version 2.0, 2.0 SP1 (can be downloaded from the Microsoft website).

2.2.1.2. Antivirus/Backup Software Configuration

In order to prevent antivirus activity from affecting the performance of the virtual desktop, it is recommended where possible to exclude the following Virtual Machine file types from any antivirus or backup processing running on the host:

- *.VHD
- *.VUD
- *.VSV
- *.CKM
- *.VMC
- *.INDEX

2.2.1.3. Installing and Configuring Microsoft Virtual PC 2007 SP1

To install Microsoft Virtual PC 2007 SP1:

1. From the Microsoft website, download Virtual PC 2007 SP1.
2. Run the installation file on the host, and follow the wizard.
3. Install Virtual PC 2007 SP1 QFE on the host in elevated mode.

2.2.2. Installing MED-V using the MED-V Client MSI

There are two MED-V components on the client MSI:

- MED-V Client - The MED-V software which must be installed on client machines for running MED-V Workspaces.
- MED-V Management Console - The administrative tools, where administrators can create and maintain images, Workspaces and their policies.

MED-V Management Console and MED-V Client are both installed from the MED-V client MSI; however, MED-V Client can be installed independently without the MED-V Management Console by clearing the **Install the MED-V Management application** check box during the installation.

Note: Do not install MED-V Client using Windows `runas` command.

To install MED-V Client:

1. Login as a user who has local admin rights on the machine.
2. Run the MED-V MSI.

   The MED-V MSI is called `MED-V_x.msi`, where x is the version number.

   For example, `MED-V_1.0.65.msi`.

   The **InstallShield Wizard Welcome** screen appears.

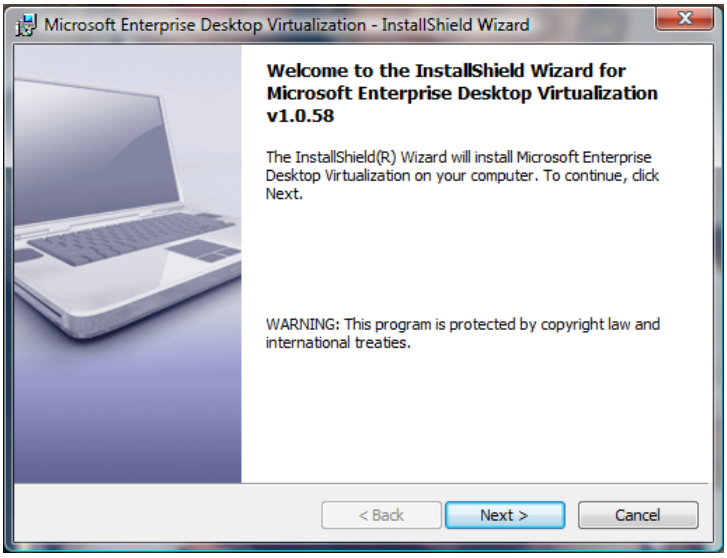


Figure 7: Welcome Screen

3. Click **Next**.

   The **MED-V Client License Agreement** screen appears.

4. Read the license agreement, click **I accept the terms in the license agreement** and then click **Next**.

   The **Destination Folder** screen appears, with the default installation folder displayed.

   The default installation folder is the directory where the OS is installed.

   - To change the folder where MED-V should be installed, click **Change** and browse to an existing folder.

5. Click **Next**.

   The **MED-V Client Settings** screen appears.

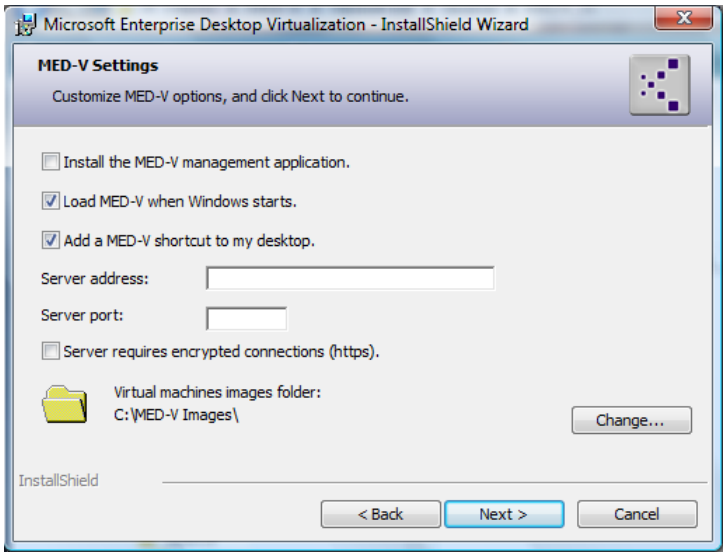


Figure 8: MED-V Settings Screen

6. Select the **Install the MED-V management application** check box to include the management component in the installation.

Note: Administrators should install MED-V Management since it is required for configuring the image and Workspace.

7. Select the **Load MED-V when Windows starts** check box to start MED-V automatically on startup.
8. Select the **Add a MED-V Client shortcut to my desktop** check box to create a MED-V shortcut on your desktop.
9. In the **Server address** field, type the server address.
10. In the **Server port** field, type the server's port.
11. Select the **Server requires encrypted connections (https)** check box to work with https.
12. The default Virtual Machine images folder is displayed. The default installation folder is `%systemdrive%\MED-V Images\`. To change the folder where MED-V should be installed, click **Change** and browse to an existing folder.
13. Click **Next**.

    The **Ready to Install** screen appears.

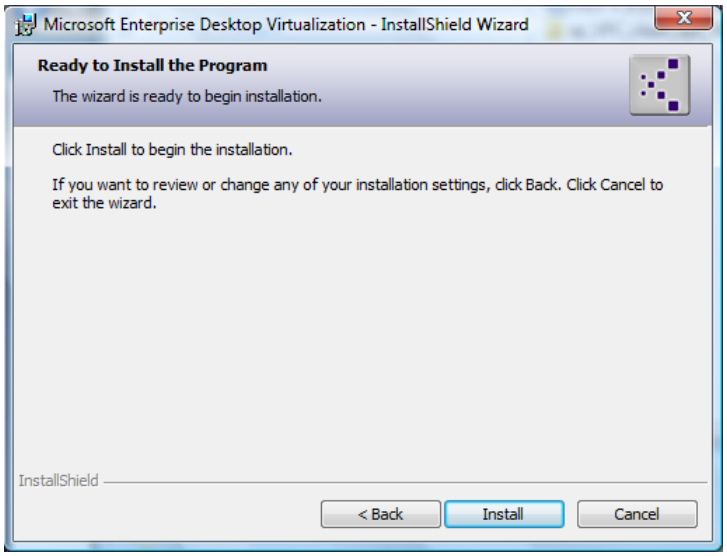


Figure 9: Ready to Install Screen

14. To continue with the installation, click **Install**.

    MED-V Client installation starts. This can take several minutes, and the screen may not display text. During installation, several progress screens appear. If an error message appears, follow the instructions provided.

    Upon successful installation, the **Installation Complete** screen appears.
15. Click **Finish** to quit the wizard.

Chapter 3

3. Configuring a MED-V Image

In This Chapter

This section describes how to configure a MED-V image on a machine on which MED-V Client and MED-V Management are installed, and explains the following tasks:

- Virtual Machine System Requirements
- Creating a VPC Image using Microsoft Virtual PC
- Installing the Workspace MSI
- Running the MED-V Virtual Machine Prerequisites Tool
- Configuring the MED-V Virtual Machine Manual Installation Prerequisites
  - Virtual Machine Settings
  - Image Settings
  - Installing VPC Additions
  - Configuring Printing
- Configuring Sysprep
- Turning off Microsoft Virtual PC

Note: Once the preparations are complete, the machine should not be part of a domain since the join domain procedure should be performed on the client after the deployment, as part of the Workspace setup.

3.1. Virtual Machine System Requirements

The recommended system configuration for use of MED-V Virtual Machine is provided in the following table. System performance will be improved when utilizing a system with the recommended system configuration.

Table 3: Recommended System Configuration

Operating System	Windows XP SP2/SP3 Pro, Windows 2000 SP4
Web browser	Microsoft Internet Explorer 6.0 SP 2, 7.0
File system	NTFS **Note:** Windows XP has a utility that converts FAT to NTFS.

3.2. Creating a VPC Image using Microsoft Virtual VPC

To create a VPC image using Microsoft Virtual PC, follow the VPC documentation in creating a VPC image from your corporate image.

3.3. Installing the Workspace MSI

To install the Workspace image:

1. Start the virtual machine and copy the MED-V Workspace MSI inside.

   The MED-V Workspace MSI is called `MED-V_Workspace_x.msi`, where x is the version number.

   For example, `MED-V_Workspace_1.0.65.msi`.

2. Double-click on the Workspace MSI to install it and follow the wizard.

3.4. Running the MED-V Virtual Machine Prerequisites Tool

Note: The screens in this section refer to a Windows XP image.

The Virtual Machine prerequisites tool is a wizard which automates several of the prerequisites.

Note that although many parameters are configurable in the wizard, the properties required for the proper functioning of MED-V are not configurable.

To run the Virtual Machine prerequisites tool:

1. After the Workspace MSI is installed, from the Windows **Start** menu, select **MED-V > VM Prerequisites Tool**.

   Note: The user running the VM Prerequisites Tool must have local admin rights and must be the only user logged in.

   The **MED-V Virtual Machine Prerequisites Wizard Welcome** screen appears.

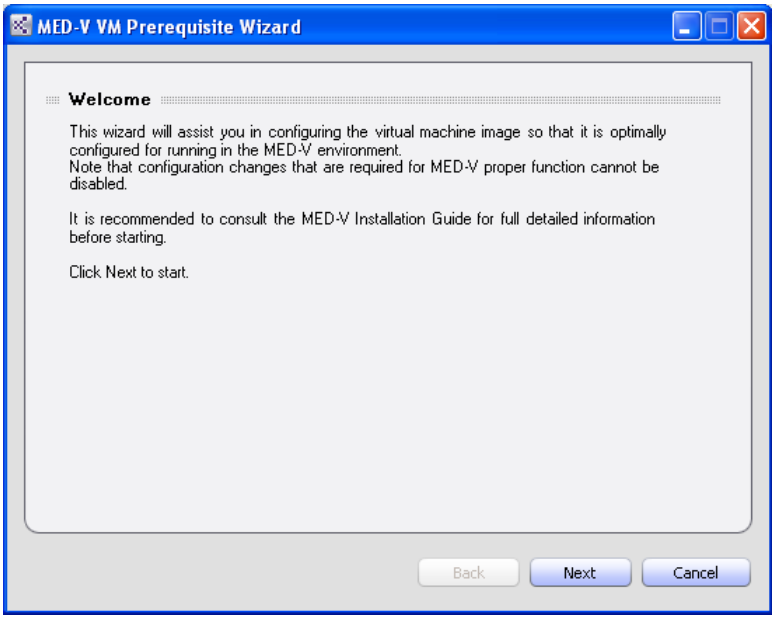


Figure 10: Virtual Machine Prerequisites Tool Welcome Screen

2. Click **Next**.

   The **Windows Settings** screen appears.

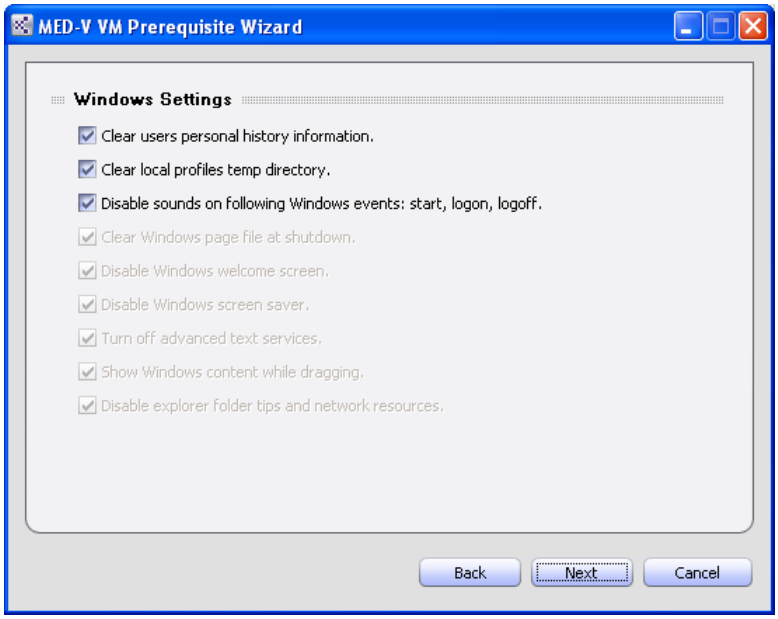


Figure 11: Windows Settings Screen

3. From the following configurable properties, select the ones you wish to set.
   - **Clear users personal history information**
   - **Clear local profiles temp directory**
   - **Disable sounds on following Windows events: start, logon, logoff**
4. Click **Next**.

   The **Internet Explorer Settings** screen appears.

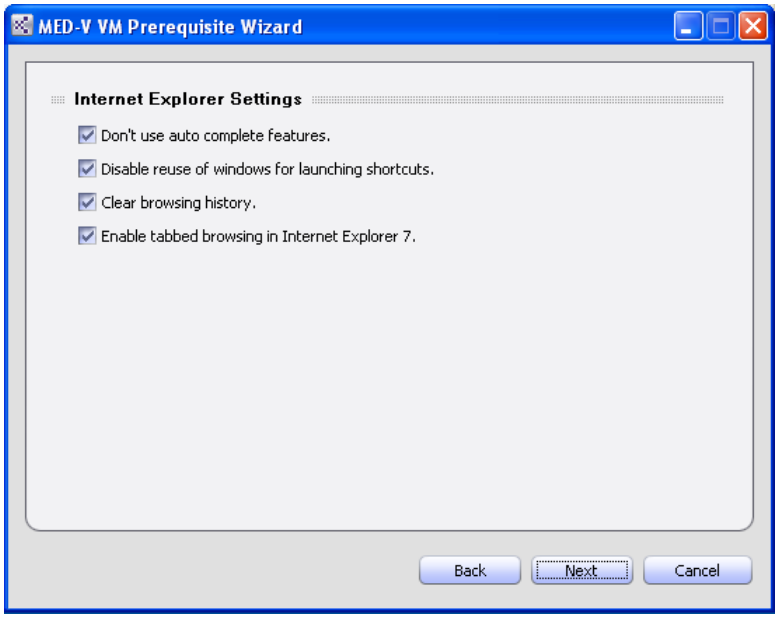


Figure 12: Internet Explorer Settings Screen

5. From the following configurable properties, select the ones you wish to set.
   - **Don't use auto complete features**
   - **Disable reuse of windows for launching shortcuts**
   - **Clear browsing history**
   - **Enable tabbed browsing in Internet Explorer 7**
6. Click **Next**.

   The **Windows Services** screen appears.

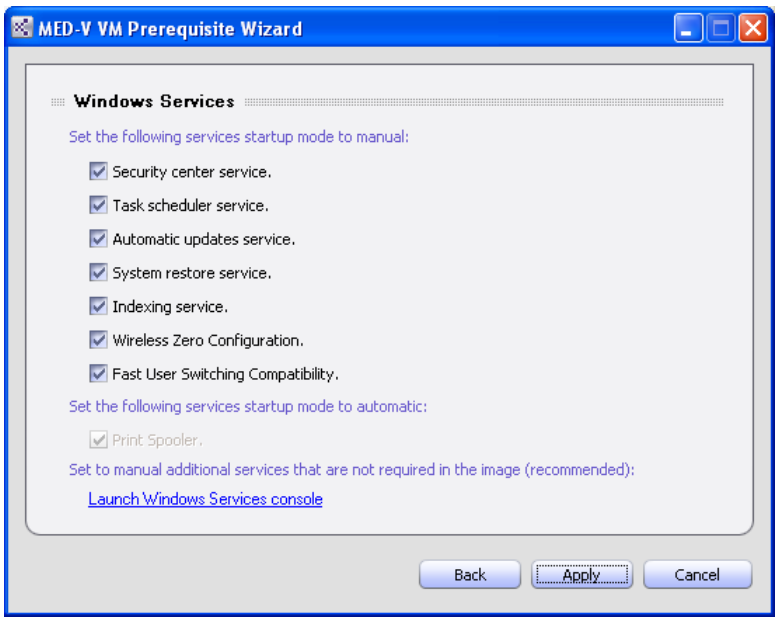


Figure 13: Windows Services Screen

7. From the following configurable properties, select the ones you wish to set.
   - **Security center service**

- **Task scheduler service**
- **Automatic updates service**
- **System restore service**
- **Indexing service**
- **Wireless Zero Configuration**
- **Fast User Switching Compatibility**

8. Click **Apply**.

   The Windows Auto Login screen appears.

Figure 14: Windows Auto Logon Screen

9. To enable Windows Auto Logon, do the following:

   a. Select the **Enable Windows Auto Logon** check box.

   b. Assign a **User name** and **Password**.

10. Click **Apply**.

    A confirmation box appears.

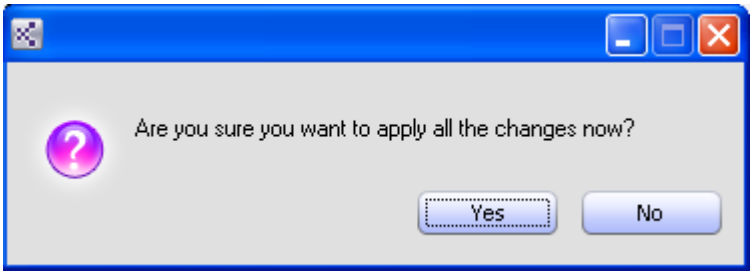


Figure 15: Confirmation Box

11. Click **Yes**.

    The **Summary** screen appears.

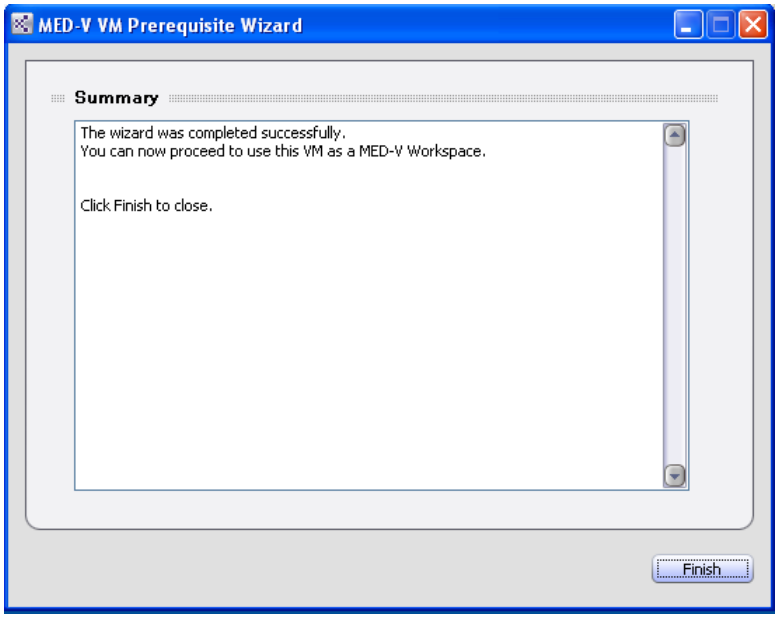


Figure 16: Summary Screen

12. Click **Finish** to quit the wizard.

Note: When a group policy is used, the settings are changed via the prerequisites tool. Verify that the group policy does not overwrite these values.

3.5. Configuring MED-V Virtual Machine Manual Installation Prerequisites

Several of the configurations cannot be configured through the Virtual Machine Prerequisites Tool and must be performed manually.

3.5.1. Virtual Machine Settings

It is recommended to configure the following Virtual Machine settings from the Microsoft Virtual PC console:

- Disable floppy disk drives.
- Disable undo-disks (**Settings** > **undo-disks**).
- Ensure that the image has only one virtual CPU.

3.5.2. Image Settings

Configure the following manual settings inside the image:

- In the **Power Options Properties** window, disable hibernation and sleep.
- Apply the most recent Windows updates.
- In the **Windows Startup and Recovery** dialog, in the **System Failure** section, clear the **Automatically restart** check box.
- Ensure that the image uses a VLK license key.

3.5.3. Installing VPC Additions

To install VPC additions:

- From the **Action** menu, select **Install or Update Virtual Machine Additions**.

3.5.4. Configuring Printing

There are two different ways to configure printing from the Workspace:

- Add a printer to the virtual machine.
- Allow printing with printers that are configured on the host machine.

3.6. Configuring Sysprep

Sysprep is Microsoft's System Preparation Utility for Windows operating system. Sysprep can be used to assign a SID for the machine and for assigning a unique name. It is not recommended to use Sysprep to join a domain, rather use the MED-V join domain script action as described in Script Actions Properties.

To configure Sysprep in a Workspace:

1. Create a directory in the root of the system drive named `Sysprep`.
2. From the Windows installation CD, extract `deploy.cab` to the root of the system drive.

   or

   Download the latest Deployment Tools update from the Microsoft website.
3. Run **Setup Manager** (setupmgr.exe).
4. Follow the Setup Manager wizard.

Once Sysprep is configured and the Workspace is created, Sysprep must be executed.

To execute Sysprep:

1. From the Sysprep folder located in the root of the system drive, run the System Preparation Tool (Sysprep.exe).

   A warning prompt appears.
2. Click **OK**.

   The Sysprep Properties dialog appears.

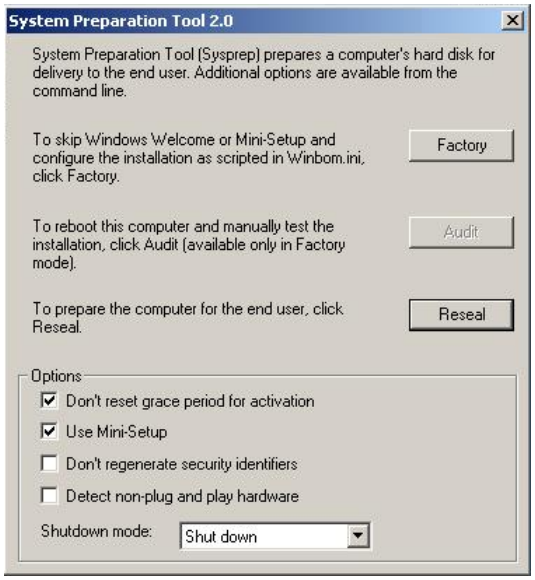


Figure 17: Sysprep Properties Dialog

3. Select the **Don't reset grace period for activation** and **Use Mini-Setup** check boxes.
4. Click **Reseal**.

   A confirmation prompt appears. It lists the options you have already selected.

Figure 18: Sysprep Confirmation Prompt

5. If you are not satisfied with the information listed in the confirmation prompt, click **Cancel** and change the selections.
6. Click **OK** to complete the System Preparation process.

3.7. Turning off Microsoft Virtual PC

Once all the components are installed and configured, close Microsoft Virtual PC and select **Turn Off**.

Chapter 4

4. Opening the MED-V Console

In This Chapter

4.1. Logging In to the MED-V Management Console

To open the MED-V Management Console:

- From the Windows **Start** menu, select **All Programs** > **MED-V** > **MED-V Management**.

  The **Login** window appears.

Figure 19: Login Window

To log in:

1. Type in your domain user credentials in the following format:

   "domain_name\user_name", "password"

   Note: When configuring the server, users with full access as well as users with read-only access are defined. All users must be domain users. The domain username and password is used for MED-V Management login.

2. Click **OK**.

   The **MED-V Management Console** appears.

4.2. MED-V Management Console User Interface

The UI is divided into three sections:

- The **MED-V Management Buttons**, which correspond to the three modules.
  - **Policy** - The Policy module is used to define the Workspaces and their related settings and permissions.
  - **Images** - The Images module is used to manage MED-V Workspace images.
  - **Reports** -The Reports module is used for generating and viewing Workspace reports.
- The **Toolbar** displays shortcuts relevant to the button selected.
- The **Display Pane** displays a module corresponding to the button that is selected.

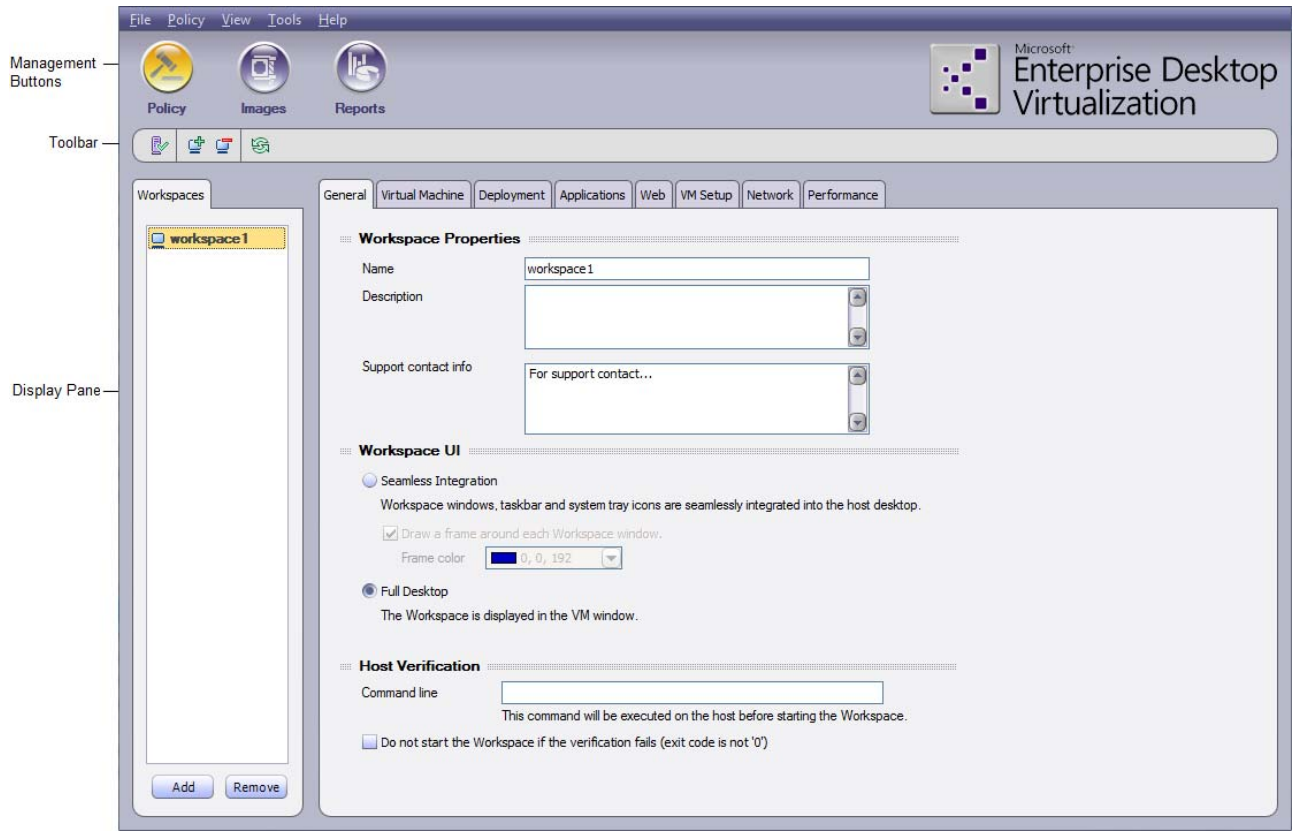


Figure 20: MED-V Management Console

Chapter 5

5. Testing and Deploying a MED-V Image

In This Chapter

The MED-V administrator creates a MED-V image so that it can either be uploaded and then distributed to the client over the web, added to a MED-V package, or downloaded to the client using a third party system. It is recommended to first create a test image and test it on MED-V Client before deploying it.

When creating a MED-V image, it goes through the following three stages:

a. **Local Test Image** - a basic image which can be tested locally.

b. **Local Packed Image** - after the image is tested, the image is packed as it existed prior to testing. No changes from the testing phase itself are included in the packed image.

c. **Packed Image on Server** - the packed image is uploaded to the server.

5.1. Creating a MED-V Test Image

To create a new MED-V test image:

1. Click on the **Images** button.

   The **Images** module appears.

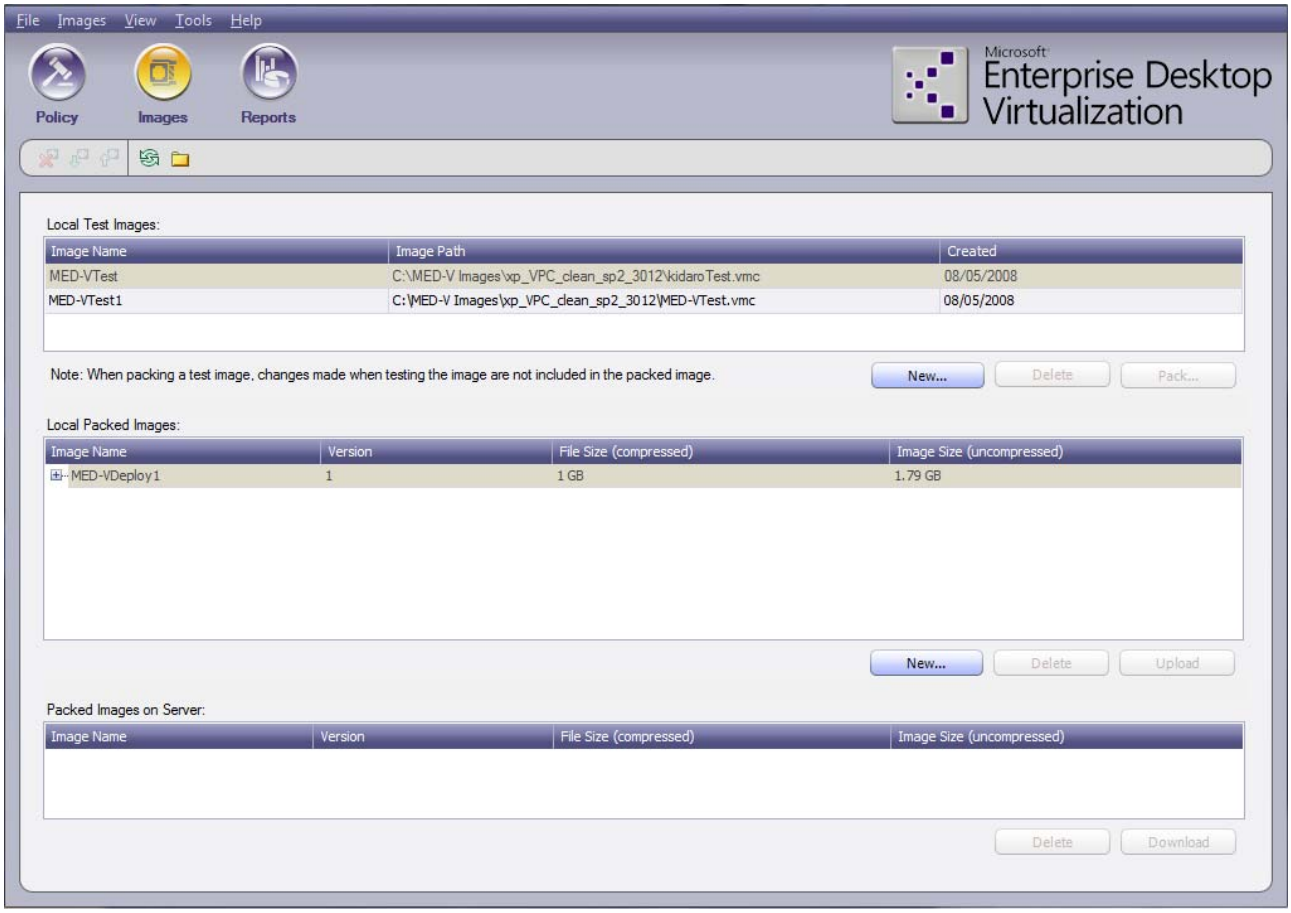


Figure 21: Images Module

- The **Image** module consists of three panes:
  - **Local Test Images** - local unpacked images.
  - **Local Packed Images** - all packed images on the local machine.
  - **Packed Images on Server** - all images which have been packed and uploaded to the server.
- In the Local Packed Images and Packed Images on Server panes, the most recent version of each image is displayed as the parent node. Click on the parent node to view all other existing versions of the image.

2. In the **Local Test Images** pane, click **New**.

   The **Test Image Creation** dialog box appears.

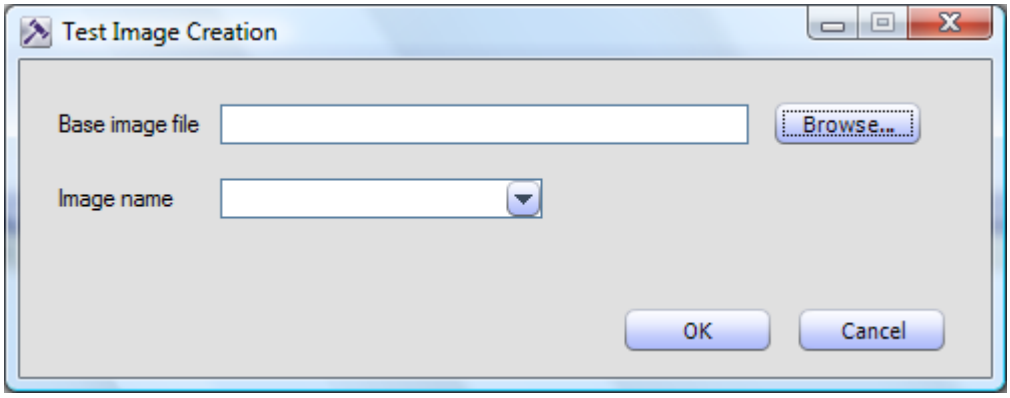


Figure 22: Test Image Creation Dialog Box

3. Select the Virtual Machine image that you wish to configure as a MED-V test image by doing one of the following:
   - In the **Base image file** field, type the full path to the directory where the Microsoft Virtual PC image prepared for MED-V is located.
   - Click **Browse...** to browse to the directory where the Microsoft Virtual PC image prepared for MED-V is located.
4. In the **Image Name** field, type or select the desired name.

   Note: The following characters cannot be included in the image name: space " < > | \ / : * ?

5. Click **OK**.

   A new MED-V test image is created on your host machine with the properties defined in the following table.

   To configure the Workspace image, refer to Configuring a Workspace Policy.

Table 4: Local Test Images Properties

Property	Possible Values/Remarks
Image Name	The name of the test image as it was defined when the administrator created the image.
Image Path	The local path of the test image.
Created	The date the test image was created.

5.2. Testing a MED-V Image from the MED-V Client

Once a MED-V test image is created, use the following procedure to test the image locally.

To test a MED-V Image:

1. Click on the **Policy** button.

   The **Policy** module appears.
2. Assign the MED-V test image to a Workspace by doing the following:
   a. Click the **Virtual Machine** tab.
   b. In the **Assigned Image** field, select the MED-V test image you created. If your test image is not in the list, click **Refresh**.

c. From the toolbar, click Save **changes**.

3. Configure any other Workspace settings you want to test. For detailed information, refer to Configuring a Workspace Policy.
4. Start MED-V Client.

   The **Confirm Running Test** confirmation box appears:

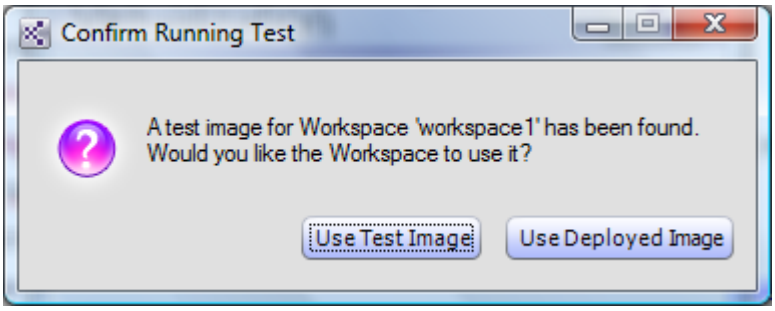


Figure 23: Confirm Running Test Confirmation Box

5. Click **Use Test Image**.
6. Test the Workspace test image.

   For information about starting and running MED-V Client, refer to Running MED-V Client.

Note: While testing an image, do not open VPC and make changes to the image.

Note: When testing an image, no changes are saved to the image between sessions; rather they are saved in a separate, temporary file. This is to ensure that when the image is packed and run on the production environment, it is the original, clean image.

5.3. Packing a MED-V Image

Once an image has been tested it can be packed.

To create a packed image:

1. Click on the **Images** button.

   The **Images** module appears.
2. In the **Local Packed Images** pane, click **New**.

   The **Packed Image Creation** dialog box appears.

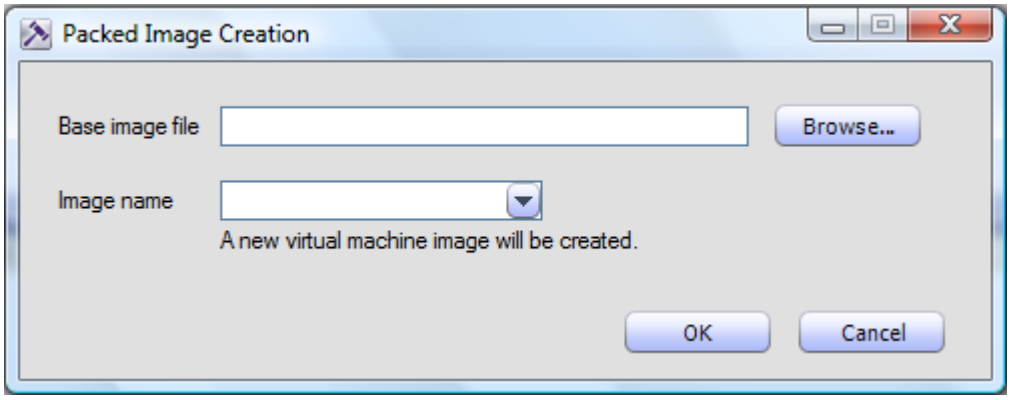


Figure 24: Packed Image Creation Dialog Box

3. Select the Virtual Machine image that you wish to configure as a MED-V image by doing one of the following:
   - In the **Base image file** field, type the full path to the directory where the Microsoft Virtual PC image prepared for MED-V is located.
   - Click **Browse...** to browse to the directory where the Microsoft Virtual PC image prepared for MED-V is located.
4. Specify the name of the new image by doing one of the following:
   - In the **Image Name** field, type the desired name.

     Note: The following characters cannot be included in the image name: space " < > | \ / : * ?

     A new packed image will be created.
   - From the drop-down list, select an existing name.

     A new version of the existing image will be created.
5. Click **OK**.

   A new MED-V packed image is created on your host machine with the properties defined in the following table.

Table 5: Local Packed Images Properties

Property	Possible Values/Remarks
Image Name	The name of the packed image as it was defined when the administrator created the image.
Version	The version of the displayed image. **Note:** All previous versions are kept unless deleted.
File Size (compressed)	The physical compressed size of the image.
Image Size (uncompressed)	The physical uncompressed size of the image.

5.4. Working with Local Packed Images

The following functions can be utilized when working with local packed images:

- Uploading an image to the server
- Downloading an image to the local repository
- Extracting an image for use by the local client
- Deleting an image

To upload an image to the server:

1. In the **Local Packed Images** pane, select the image you created.

   The image appears highlighted.

2. Click **Upload**.

   The image is uploaded to the server. This may take a considerable amount of time.

To download an image:

1. In the **Packed Images on Server** pane, select the image or version of the image you wish to download.

   The image appears highlighted.

2. Click **Download**.

   The image is downloaded to your local machine.

Note: The downloaded image will not appear in the Local Images pane until you refresh the page. Click the Refresh button  to see the downloaded image in the Local Images pane.

A packed image can be unpacked to the local repository by extracting it. It then does not need to be downloaded from the server.

To extract an image:

1. In the **Local Packed Images** pane, select an image.
2. Right-click and from the drop-down menu, select **Extract Image**.

   The image is extracted to the local drive and can now be used by the local client running on the machine.

To delete an image:

1. Click on the image or the version of the image you wish to delete.

   The image appears highlighted.

2. From the **Images** menu, click **Delete**.

   The image is deleted.

5.5. Updating an Image

An existing image can be updated, thereby creating a new version of the image. The new version can then be deployed on client machines, replacing the existing image.

Note: When a new version is deployed on the client, it overwrites the existing image. When updating an image, ensure that no data on the client needs to be saved.

To update an image:

1. Open the existing image in Virtual PC 2007.
2. Make the required changes to the image, updating the image (such as installing new software).
3. Close Virtual PC 2007.
4. Test the image.
5. Once the image is tested, pack it to the local repository using the same name as the existing image.

   Note: If you name the image a different name than the existing version, a new image will be created rather than a new version of the existing image.

6. Upload the new version to the server, or distribute it via a deployment package.

Chapter 6

6. Creating a MED-V Workspace

In This Chapter

A Workspace consists of an image and the Policy, which defines the rules and functionality of the Workspace. Multiple Workspaces can be created, each customized with their own configurations, settings and rules. A user/group or multiple users/groups can be associated with each Workspace, thereby making the Workspace available only for the associated users/groups machines.

6.1. Adding a Workspace

To add a Workspace:

1. Click on the **Policy** button.

   The **Policy** module appears.

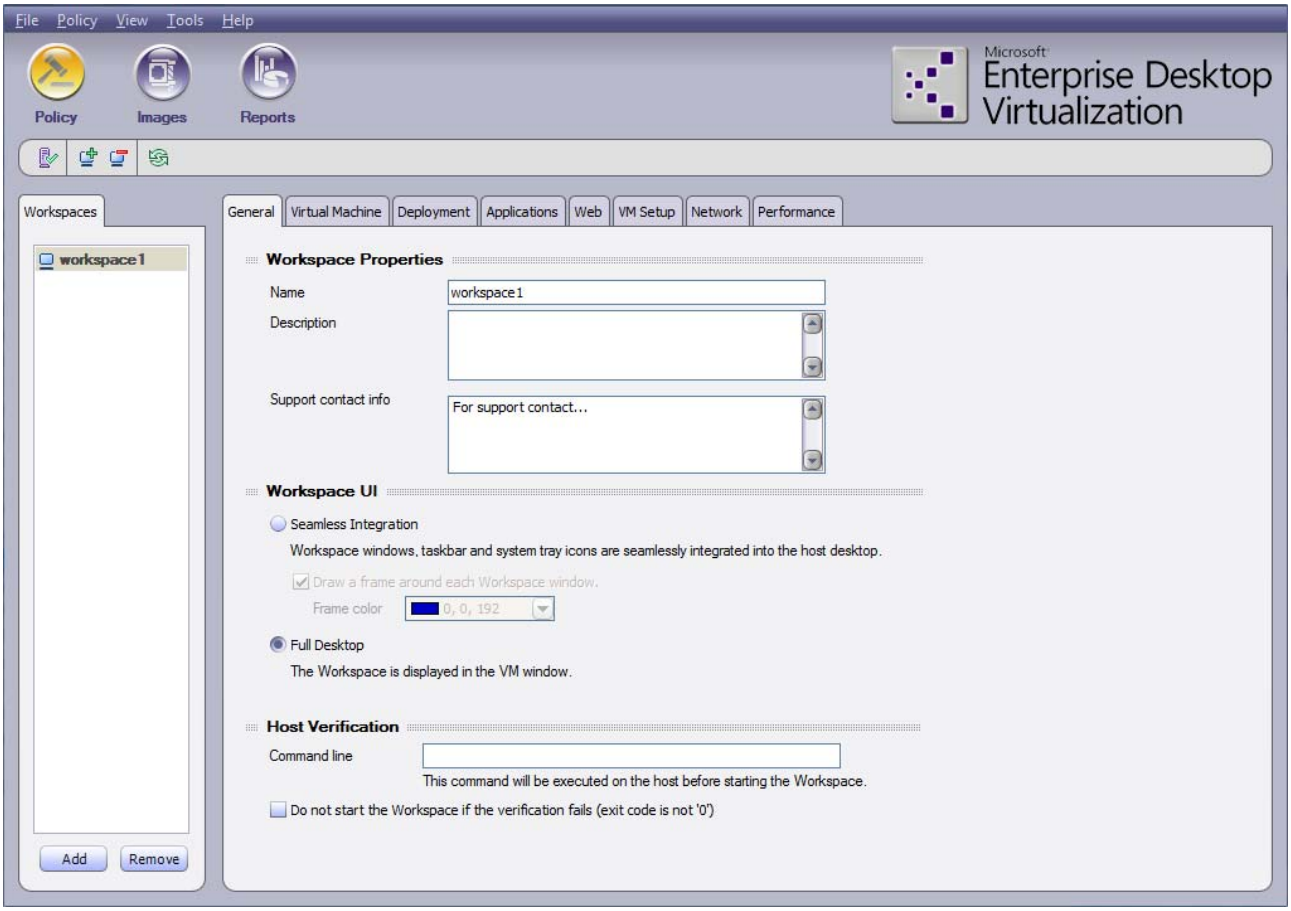


Figure 25: Policy Module

The **Policy** module consists of the **Workspaces** Menu on the left and the **General**, **Virtual Machine, Deployment, Applications**, **Web, VM Setup, Network** and **Performance** tabs.

2. From the **Policy** menu, select **New Workspace**.

   or

   Click **Add**.

   A new Workspace is created.

3. From the **General** tab, in the **Name** field, enter the name of the Workspace.
4. In the **Description** field, enter a description for the Workspace.
5. In the **Support contact info** field, enter the contact information for technical support.

For detailed information on configuring a Workspace, refer to Configuring a Workspace Policy.

6.2. Cloning a Workspace

A Workspace can be cloned so that you can create a Workspace identical to an existing Workspace.

To clone a Workspace:

1. Click on the Workspace you wish to clone.

The Workspace appears highlighted.

2. From the **Policy** menu, select **Clone Workspace**.

   A new Workspace is created with the name <Original Workspace name> - 2.

6.3. Importing a Policy

To import an existing policy:

1. In the Policy module, from the **Policy** menu, select **Import**.

   An Import policy dialog box appears.

2. Browse to the file containing the policy you wish to import.
3. Click **Open**.

   The policy is imported, replacing the existing policy.

6.4. Exporting a Policy

To export policy:

1. In the Policy module, from the **Policy** menu, select **Export**.

   An Export policy dialog box appears.

2. Browse to the directory to which you wish to export the policy.
3. Enter a name for the policy file.
4. Click **Save**.

   The policy is exported.

6.5. Deleting a Workspace

To delete a Workspace:

- In the **Policy** module, while the Workspace pane is in focus, click **Remove**.

Chapter 7

7. Configuring a Workspace Policy

In This Chapter

There are two different types of Workspaces:

- **Persistent** - In a persistent Workspace, all changes and additions the user makes to the Workspace are saved in the Workspace between sessions. Additionally, a persistent Workspace is generally used in a domain environment.
- **Revertible** - In a revertible Workspace, at the completion of each session (i.e. when the Workspace is stopped) the Workspace reverts to its original state during deployment. No changes or additions that the user made are saved on the Workspace between sessions. Additionally, a revertible Workspace cannot be used in a domain environment.

It is important to decide on the type of Workspace you are creating before deploying the Workspace, since it is not recommended to reconfigure the type of Workspace once a policy has been deployed to users.

Note: When configuring a policy, ⚠ this symbol will appear next to mandatory fields which are not filled in. If a mandatory field is not filled in, the symbol will appear on the tab as well.

After configuring policy settings, from the **Policy** menu, select **Commit** to apply and save the settings.

7.1. General Settings

All general settings are configured in the Policy module, from the General tab.

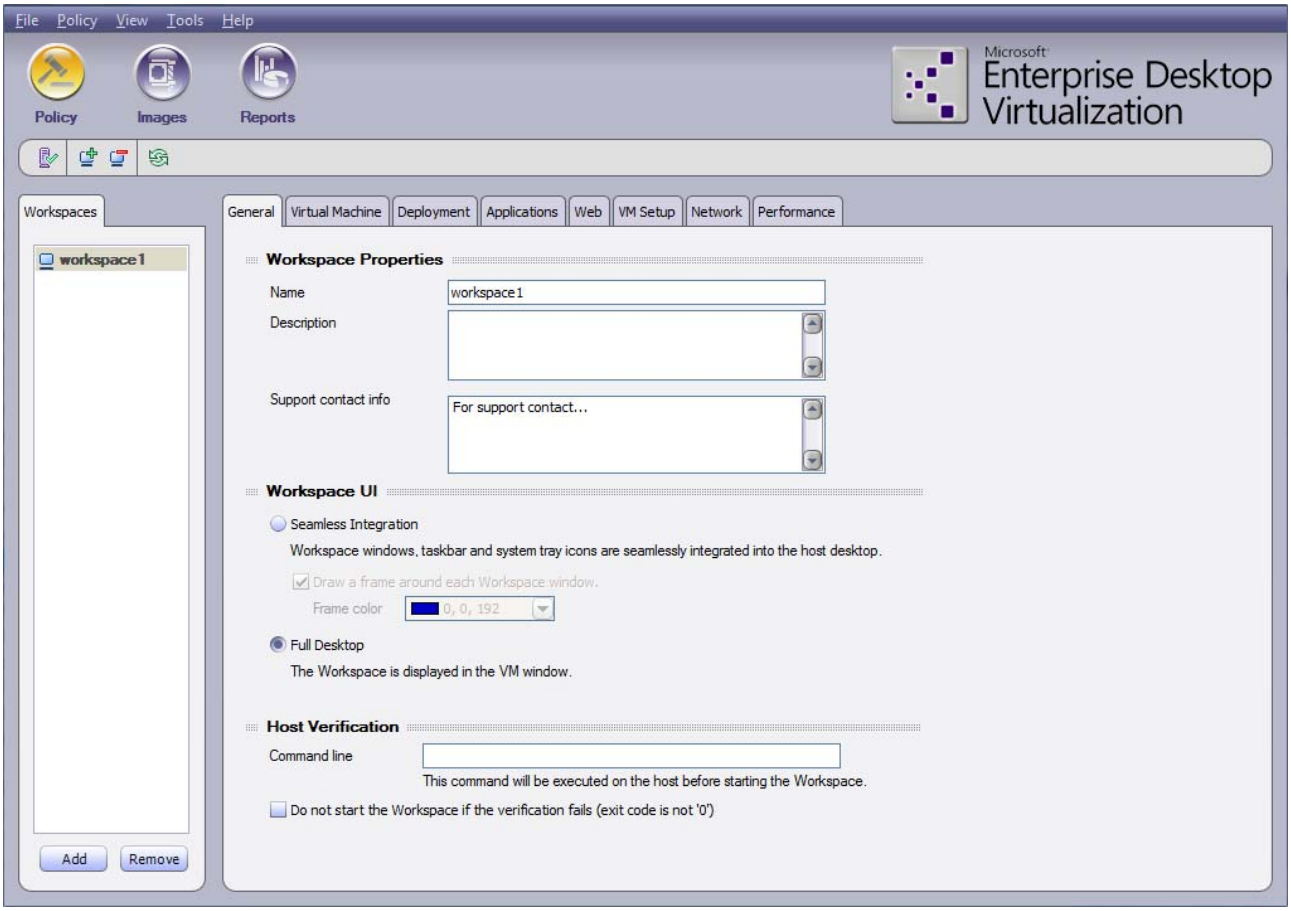


Figure 26: Policy Module

To apply general settings to a Workspace:

1. Click on the Workspace you wish to apply the settings to.

   The selected Workspace appears highlighted.

2. Configure the general properties as described in the following table.

Table 6: General Workspace Properties

Property	Possible Values/Remarks
Workspace Properties	
Name	The name of the Workspace. **Warning:** Do not rename an existing Workspace while it is running on a client machine.
Description	Description of the Workspace which can include the content or status of the Workspace and any other useful information. **Note:** The description is for the purpose of the administrator and has no impact on the policy.
Support Contact Info	The contact information for technical support. The information entered will be displayed in the Support Contact Information screen which can be accessed from the MED-V Client notification area.
Workspace UI	

Property	Possible Values/Remarks
Seamless Integration	Select this option for the Workspace windows, taskbar and system tray icons to integrate seamlessly into the host desktop.
Draw frame around each Workspace window	When using seamless integration, select this option to create a colored border around all applications running within the Workspace and a colored background for all taskbar button icons. In the **Frame color** field, select the color.
Full Desktop	Select this option to display the Workspace as the entire desktop, without integrating with the host.
Host Verification	
Command line	Type a command line to run on the host before starting the Workspace.
Do not start the Workspace if the verification fails (exit code is not '0')	Select this check box if you are using a command line and only want to start the Workspace if the script is completed successfully.

A command line may be run on the host prior to starting the Workspace.

To run a command line before starting a Workspace:

1. In the **Command Line** field, enter a command line.
2. To start the Workspace only if the command line was successful, select the **Do not start the Workspace if the verification fails** check box.

7.2. Virtual Machine Settings

Every Workspace must have a Microsoft Virtual PC image associated with it. Administrators can assign a VPC image as well as set other Virtual Machine properties.

All Virtual Machine settings are configured in the Policy module, from the Virtual Machine Settings tab.

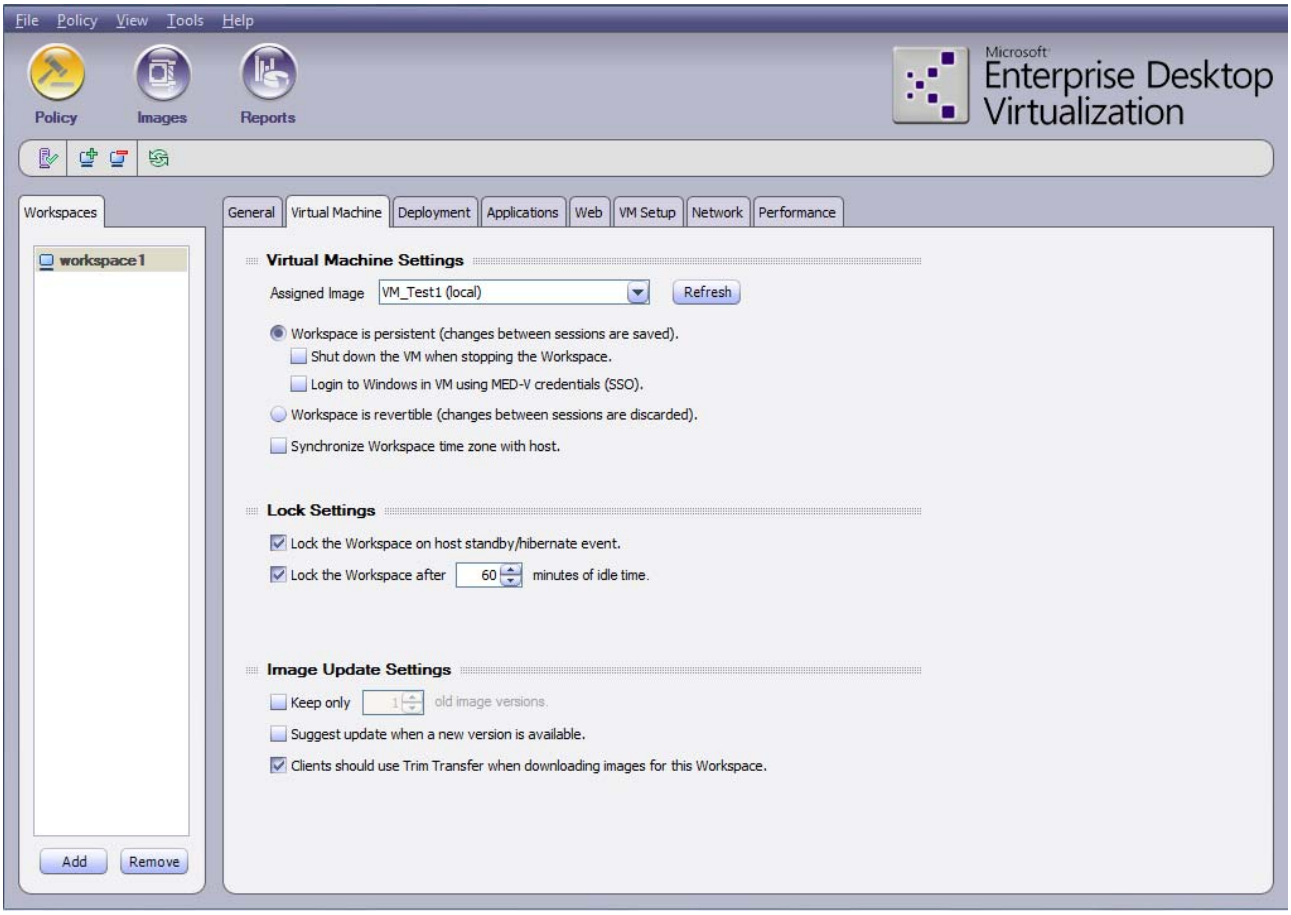


Figure 27: Virtual Machine Pane

To apply Virtual Machine settings to a Workspace:

1. Click on the Workspace you wish to apply the settings to.

   The selected Workspace appears highlighted.

2. Configure the Virtual Machine properties as described in the following table.

Table 7: Virtual Machine Properties

Property	Possible Values / Remarks
Virtual Machine Settings	
Assigned Image	The actual Microsoft Virtual PC image assigned to the Workspace. The menu provides a list of all available Microsoft Virtual PC images. There are three types of images in the Active image list: **Local test images** - Images on the local computer which are not yet packed. These image names are followed by the word test in parenthesis (test) and are for testing purposes only. **Local packed images** - Packed images on the local machine. These images are followed by the word local in parenthesis (local) and cannot be downloaded by clients until the administrator uploads them to the server. A local image can be selected if you are creating a package that will be distributed to the client via removable media (such as USB or DVD).

Property	Possible Values/Remarks
	Packed images on server - Images that are on the server and are available for download by clients. Click **Refresh** to refresh the images list.
Workspace is Persistent	If selected, the Workspace will be a persistent Workspace. In a persistent Workspace, when the Workspace is stopped, changes and additions to the Workspace are saved in the Workspace. For a Domain Workspace, this option must be selected. **Note:** This setting should not be changed once a Workspace is deployed to users.
Shutdown the Virtual Machine when stopping the Workspace	If cleared, at the completion of each session the machine is not shut down but rather takes a snapshot of the Virtual Machine. Upon the initiation of a new session Windows starts from the snapshot (i.e. Widows does not restart and no login is required). **Note:** This property is enabled only if **Workspace is persistent** is selected.
Login to Windows in VM using MED-V credentials (SSO)	Select this check box to login to Windows on the virtual machine using MED-V credentials entered when logging into MED-V Client. **Note:** This property is only enabled when **Workspace is persistent** is selected.
Workspace is Revertible	If selected, the Workspace will be a revertible Workspace. In a revertible Workspace, at the completion of each session (i.e. when the user stops the Workspace) the Workspace reverts to its original state it was in during deployment. No changes or additions that the user made are saved on the Workspace between sessions. **Note:** This setting should not be changed once a Workspace is deployed to users.
Synchronize Workspace time zone with host	Select this check box to synchronize the time zone in the Workspace with the host. The synchronization works differently depending on whether the Workspace is persistent or revertible: • In a persistent Workspace, the time zone first tries to synchronize with the server. If that fails, it synchronizes with the host. • In a revertible directory, it synchronizes with the host.
Lock Settings	
Lock the Workspace on host standby/hibernate event.	Select this check box to automatically lock the Workspace when the host machine goes into standby/hibernate.
Lock the Workspace after	Select this check box to lock the Workspace when the Workspace is idle for a specified period of time. Once selected, the number box is enabled. Enter the number of minutes of idle time before locking the Workspace.

Property	Possible Values/Remarks
	Note: The idle time refers to the Workspace applications (not the host applications).
Deletion Settings	
Keep only	Select this check box to limit the number of old image versions to keep. Once selected, the number box is enabled. Enter the number of old versions to keep.
Suggest update when a new version is available	Select this check box to suggest (but not force) an update when a new version of the image is available.
Clients should use Trim Transfer when downloading images for this Workspace	Select this check box to enable Trim Transfer (see MED-V Trim Transfer™ Technology) when downloading images associated with this Workspace. If this check box is not selected, the full image will be downloaded. **Note:** Trim Transfer requires indexing the hard drive which may take a considerable amount of time. It is recommended to use Trim Transfer when indexing the hard drive is more efficient than downloading the new image version, such as when downloading an image version that is similar to the existing version.

7.3. Deployment Settings

All Workspace permissions are configured in the Policy module, from the Deployment tab.

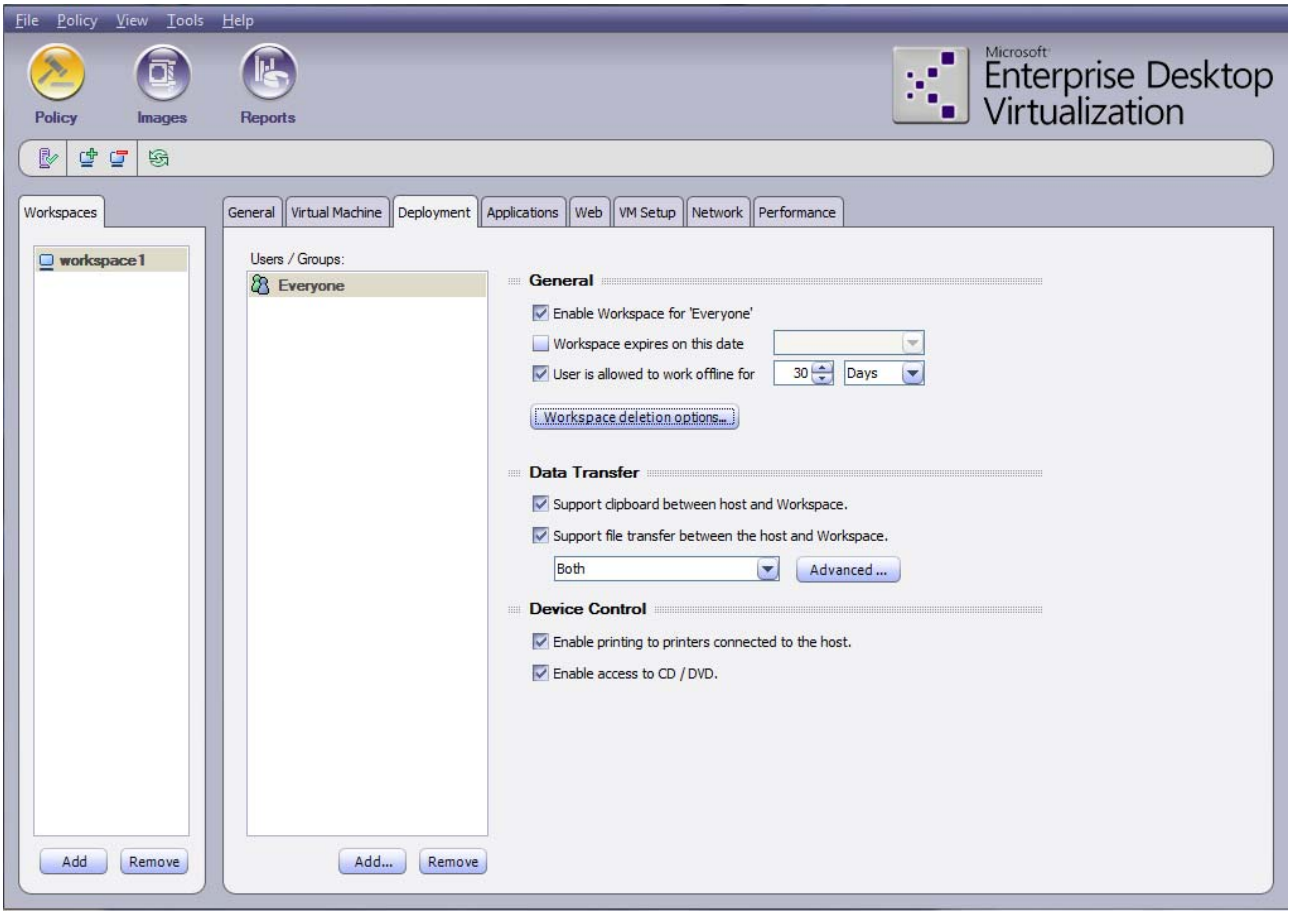


Figure 28: Deployment Pane

In order to allow users to utilize the Workspace, you must first add domain users or groups to the Workspace permissions. You can then set permissions for each user/group.

To add domain users/groups:

1. In the **Users / Groups** window, Click **Add...**

   The **Enter users/groups** dialog box appears.

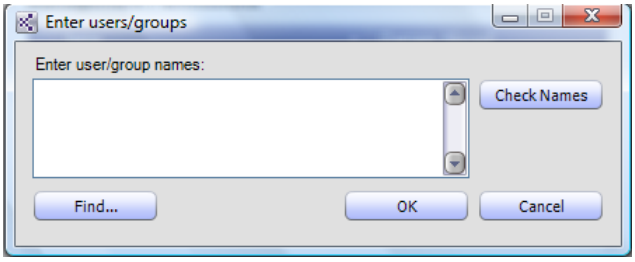


Figure 29: Users/Groups Selection Dialog Box

2. Select the domain users or groups that you want to add by doing one of the following:
   - In the **Enter user/group names** field, type a user or group that exists in the domain or as a local user or group on the computer. Then click **Check Names** to resolve it to the full existent name.

- Click **Browse...** to open the standard **Users/Groups Selection** dialog. Then select the domain users or groups you wish to add.

3. Click **OK**.

   The domain users or groups are added.

Note: Users from trusted domains should be added manually.

Note: It is not recommended to run the Management from a machine that is part of a domain which is not trusted by the domain the server is installed on.

To remove domain users or groups:

1. In the **Users/Groups** window, select the user/group you wish to delete.
2. Click **Remove**.

   The user/group is deleted.

To set permissions for user/group:

1. Click on the user or group to which you are setting the permissions.
2. Configure the Workspace properties as described in the following table.

Table 8: Workspace Deployment Properties

Property	Possible Values/Remarks
General	
Enable Workspace for <user/group>	Select this check box to enable the Workspace for this user/group.
Workspace expires on this date	Select this check box to assign an expiration date for the permissions set for this user/group. Once selected, the date box is enabled. Set the date, and permissions will expire at the end of the date specified.
User is allowed to work offline for	Select this check box to assign a time period in which the policy must be refreshed for this user/group. Once selected, the time period box is enabled. Set the number of days or hours, and at the end of the specified time period the user/group will not be able to connect if the policy is not refreshed.
Workspace deletion options...	Click to set the Workspace deletion options. For detailed information, refer to Workspace Deletion Options.
Data Transfer	
Support clipboard between host and Workspace	Select this check box to enable copying and pasting between the host and the Workspace.
Support file transfer between host and Workspace	Select this check box to enable transferring files between the host and Workspace. Select one of the following options from the **File Transfer** box: • **Both** - Enable transferring files between the host and Workspace. • **Host to Workspace** - Enable transferring files from the host to the

Property	Possible Values/Remarks
	Workspace. • **Workspace to Host** - Enable transferring files from the Workspace to the host. If a user without permissions attempts to transfer files, a user/password window will appear prompting him to enter the credentials of a user with permissions to perform the file transfer.
Advanced	Click to set the advanced file transfer options. For detailed information, refer to Advanced File Transfer Options.
Device Control	
Enable printing to printers connected to the host.	If selected, users can print from the Workspace using the host printer. Note: The printing is performed by the printers which are defined in the host.
Enable access CD/DVD	Select this check box to allow access to a CD/DVD drive from this Workspace.

7.3.1. Multiple Membership

- If a user is part of a group, and permissions are applied to the user as well as to the group he is a part of, all permissions are applied to him.
- If a user is a member of two different groups, the least restrictive permissions are applied.

7.3.2. Workspace Deletion Options

The administrator can set the Workspace deletion options for each user/group so that the Workspace is automatically deleted under certain conditions.

To set Workspace deletion options:

1. From the Deployment pane, click **Workspace deletion options...**.

   The **Workspace Deletion Options** dialog box appears.

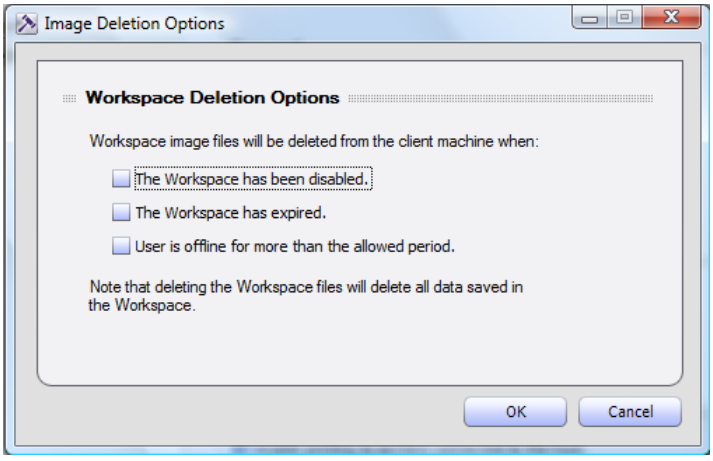


Figure 30: Workspace Deletion Options Dialog Box

2. Select from the following options:

- **The Workspace has been disabled** - If the administrator disables the Workspace, the Workspace is deleted from the user/group machine.
- **The Workspace has expired** - If the Workspace expires according to the date specified, the Workspace is deleted from the user/group machine.
- **User is offline for more than the allowed period** - If the policy is not refreshed in the time period specified since the user was offline; the Workspace is deleted from the user/group machine.

3. Click **OK**.

7.3.3. Advanced File Transfer Options

To set advanced file transfer options:

1. From the Deployment pane, click the **Advanced...** button.

   The **Advanced Workspace to Host** dialog box appears.

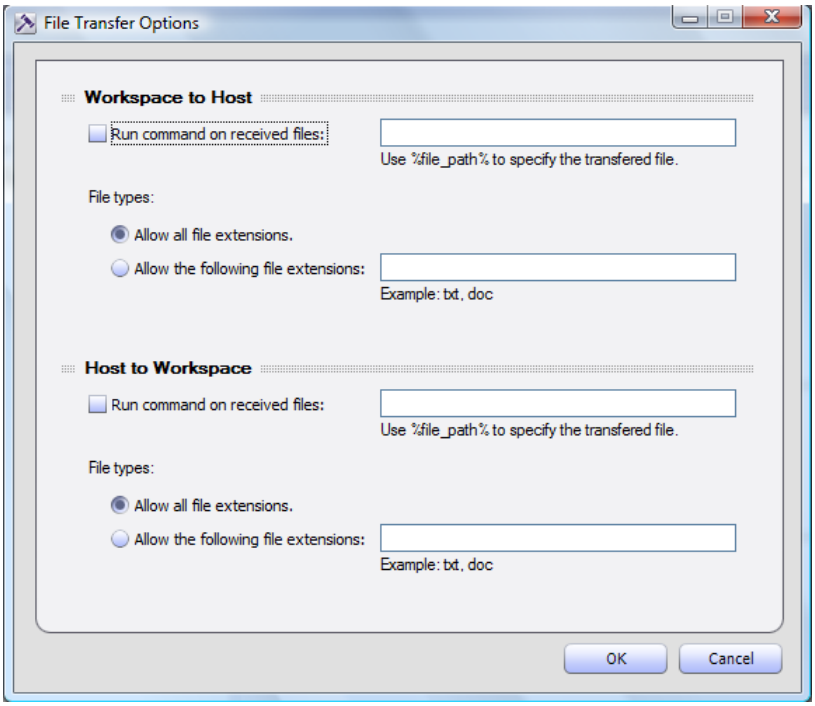


Figure 31: Advanced Workspace to Host Dialog Box

2. Configure the parameters as described in the following table.
3. Click **OK**.

Table 9: Advanced File Transfer Properties

Property	Possible Values/Remarks
Workspace to Host	
Run command on received files	Select this check box to run a command line on all files transferred to the host. In the command line box enter the command line to run on all received files.
File types	• **Allow all file extensions** - click to enable transferring files of any file extension from the Workspace to the host. • **Allow the following file extensions** - click to enable only files with

Property	Possible Values/Remarks
	specified file extensions to be transferred. In the empty field, enter all extensions allowed, separated by commas.
Host to Workspace	
Run command on received files	Select this check box to run a command line on all files transferred to the Workspace. In the command line box, enter the command line to run on all transferred files.
File types	• **Allow all file extensions** - enable transferring files of any file extension. • **Allow the following file extensions** - enable only files with specified file extensions to be transferred from the host to the Workspace. In the empty field, enter all extensions allowed, separated by colons.

7.4. Published Application Settings

Administrators can select applications that can be initiated from within the Workspace the same way they are initiated from the desktop: from the Start menu or from a local host shortcut. Applications selected and defined by the Administrator are called Published Applications.

All published application settings are configured in the Policy module, from the Applications tab.

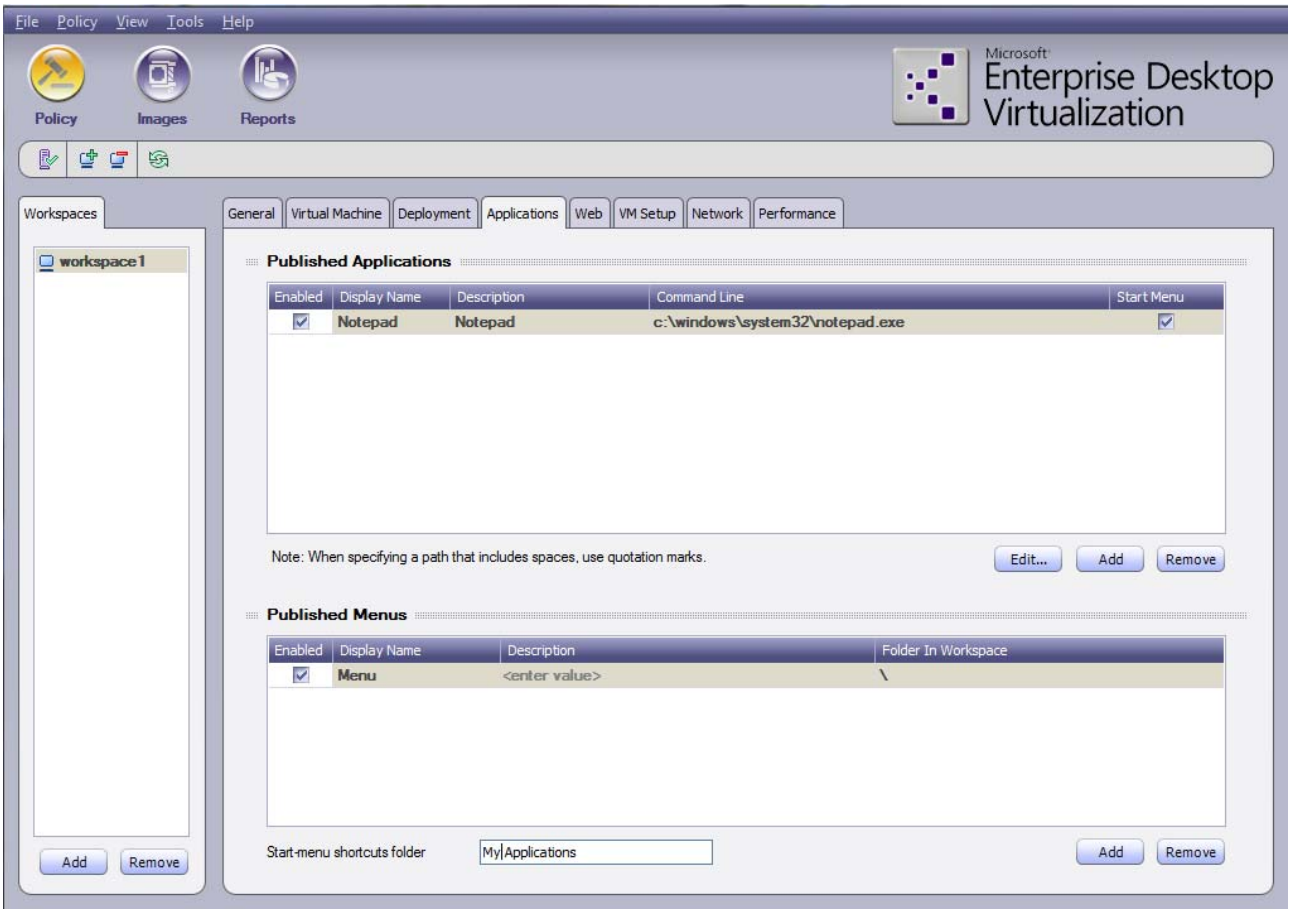


Figure 32: Applications Pane

An application can be published in one of two ways:

- As an application - Select a specific application by typing in the command line for the application. Only the application selected is published.
- As a menu - Select a folder which contains multiple applications. All applications within the folder are published and are displayed as a menu.

7.4.1. Adding a Published Application

To add an application to the Workspace:

1. Click on the Workspace you wish to apply the settings to.

   The selected Workspace appears highlighted.

2. In the **Applications** pane, in the **Published Applications** section, click **Add** to add a new application.

   A new application is added.

3. Configure the application properties as described in the following table.

   The application is added to the **Published Applications** and can be executed from within the Workspace.

Note: If setting Internet Explorer as a published application, make certain that any parameters are not in parentheses to ensure web redirection works properly.

Table 10: Published Application Properties

Property	Possible Values/Remarks
Enabled	Select to enable the published application.
Display Name	The name of the shortcut in the user's Windows Start menu. **Note:** The Display Name is **not** case sensitive.
Description	A description of the published menu.
Command Line	The command with which to execute the application from within the Workspace. The full path is required, and the parameters may be passed to the application in a similar fashion as any other Windows command. In a revertible Workspace, you can map a network drive with MapNetworkDrive syntax: "`MapNetworkDrive <drive> <path>`." For example: "`MapNetworkDrive t: \\tux\data`" To publish Windows file explorer, use the following syntax: "`c:\`" or "`\\tux\largeData`." **Note:** In order to have a name resolution, you need to perform one of the following: ▪ Configure the DNS in the base Workspace image. ▪ Verify the DNS resolution is defined in the host and configure it to use the host DNS.

Property	Possible Values/Remarks
	▪ Use the IP for defining the network drive. **Note:** If the path includes spaces, the entire path must be inside quotation marks. **Note:** The path should not end with a backslash (\).
Start Menu	If selected, a shortcut for the application is created in the user's Windows Start menu.

All published applications appear as shortcuts in the Windows Start menu (**Start** > **All Programs** > **MED-V Applications**).

To remove an application from the Workspace:

1. Click on the Workspace you wish to delete the application from.

   The selected Workspace appears highlighted.

2. In the **Applications** pane, in the **Published Applications** section, select the application you wish to remove.

3. Click **Remove**.

   The application is removed from the list of Published Applications.

7.4.2. Advanced Published Application Settings

Once a published application has been added and configured, the published application can be edited and additional advanced settings can be configured.

To edit a published application with advanced settings:

1. In the Applications pane, add and configure a published application (refer to Adding a Published Application).

2. Select the published application you wish to edit.

   The published application appears highlighted.

3. Click **Edit...**.

   The **Published Application** dialog box appears.

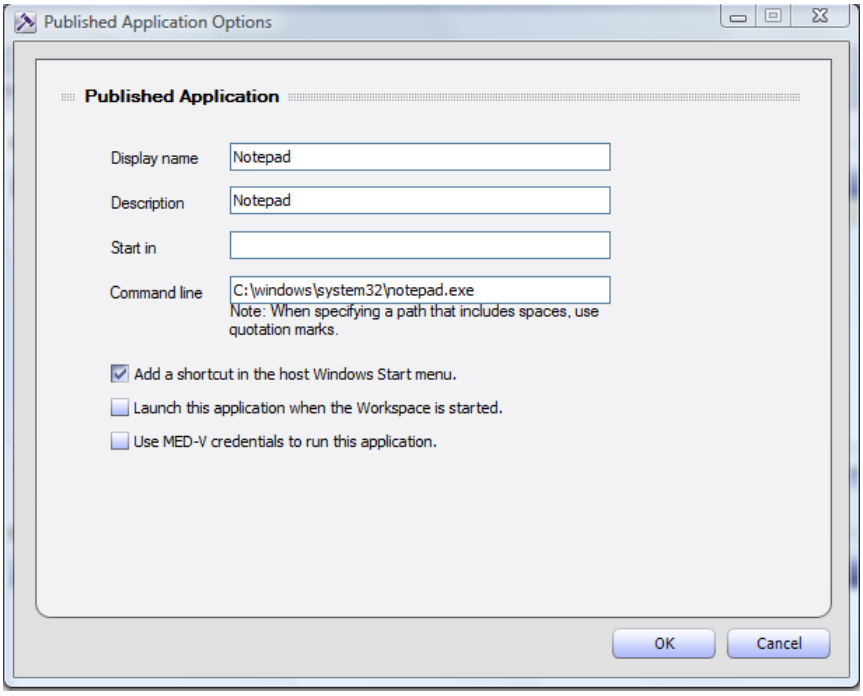


Figure 33: Published Applications Dialog Box

4. Configure the parameters as described in the following table.
5. Click **OK**.

Table 11: Editing Published Application Properties

Property	Possible Values/Remarks
Display name	The name of the shortcut in the user's Windows Start menu. **Note:** The Display Name is **not** case sensitive.
Description	A description of the published menu.
Start in	The directory from which to start the application. **Note:** The path does not need to include quotation marks.
Command line	The command with which to run the application from within the Workspace. The full path is required, and the parameters may be passed to the application in a similar fashion as any other Windows command. In a domain configuration, a shared drive generally exists on the server where all domain machines map to. The directory should be mapped here and if it is a folder which requires user authentication, **Use MED-V credentials to run this application** must be selected. In a revertible Workspace, you can map a network drive with MapNetworkDrive syntax: "`MapNetworkDrive <drive> <path>`." For example: "`MapNetworkDrive t: \\tux\data`" To publish Windows file explorer, use the following syntax: "`c:\`" or "`\\tux\largeData`." **Note:** In order to have a name resolution, you need to perform one

Property	Possible Values/Remarks
	of the following: ▪ Configure the DNS in the base Workspace image. ▪ Verify the DNS resolution is defined in the host and configure it to use the host DNS. ▪ Use the IP for defining the network drive. **Note:** If the path includes spaces, the entire path must be inside quotation marks. **Note:** The path should not end with a backslash (\).
Add a shortcut in the host Windows Start menu	Create a shortcut for the application in the user's Windows Start menu.
Launch this application when the Workspace is started	Run the application automatically when the Workspace starts.
Use MED-V credentials to run this application	Application which request username and password are authenticated using the MED-V credentials. **Note:** ▪ When using SSO, the command line should be: `C:\Windows\Explorer.exe "folder path"` ▪ When not using SSO, the command line should be: `"folder path"`

7.4.3. Adding a Published Menu

To add a menu to the Workspace:

1. Click on the Workspace you wish to apply the settings to.

   The selected Workspace appears highlighted.
2. In the **Applications** pane, in the **Published Menus** section, click **Add** to add a new menu.

   A new menu is added.
3. Configure the menu properties as described in the following table.

   The menu is added to the **Published Menus** and can be run from within the Workspace.

Table 12: Published Menu Properties

Property	Possible Values/Remarks
Enabled	Select this check box to enable the published menu.
Display Name	The name of the shortcut in the user's Windows Start menu.

Property	Possible Values/Remarks
Description	The description, which will appear as a tool-tip when the user's mouse hovers over the shortcut.
Folder in Workspace	Select the folder you wish to publish as a menu containing all the applications within the folder. The text displayed is a relative path from the Programs folder. **Note:** If left blank, all programs on the host will be published as a menu.

All published menus appear as shortcuts in the Windows Start menu (**Start** >**All Programs**> **MED-V Applications**). You can change the name of the shortcut in the **Start-menu shortcuts folder** field.

Note: When configuring two Workspaces, it is recommended to configure a different name for the **Start-menu shortcuts folder**.

To remove a menu from the Workspace:

1. Click on the Workspace you wish to delete the menu from.

   The selected Workspace appears highlighted.

2. In the **Applications** pane, in the **Published Menus** section, select the application you wish to remove.

3. Click **Remove**.

   The menu is removed from the list of Published Menus.

7.4.4. Running a Published Application from a Command Line on the Client

The KidaroRun format enables the administrator to run published applications from any location, such as desktop shortcut, using the following command:

```
"<Install path>\Manager\KidaroCommands.exe" /run "<published application name>" "<workspace name>"
```

Note: The Workspace in which the published application is defined must be running.

7.5. Web Settings

The administrator can set a list of web browsing rules for a Workspace. All sites included in the rules can either be browsed in the Workspace or on the host, as defined by the administrator. All sites not defined within the rules are browsed from the environment in which they were requested. However, you can configure them as a group as well, to be browsed in the Workspace or the host.

The web settings are not a security component but rather for the convenience of the user. The user does not need to open a browser in the Workspace in order to work within the Workspace. He can open a browser on the host and automatically be redirected to the Workspace and vice versa.

Note: Web settings are only applied to Internet Explorer and no other browsers.

All web settings are configured in the Policy module, from the Web tab.

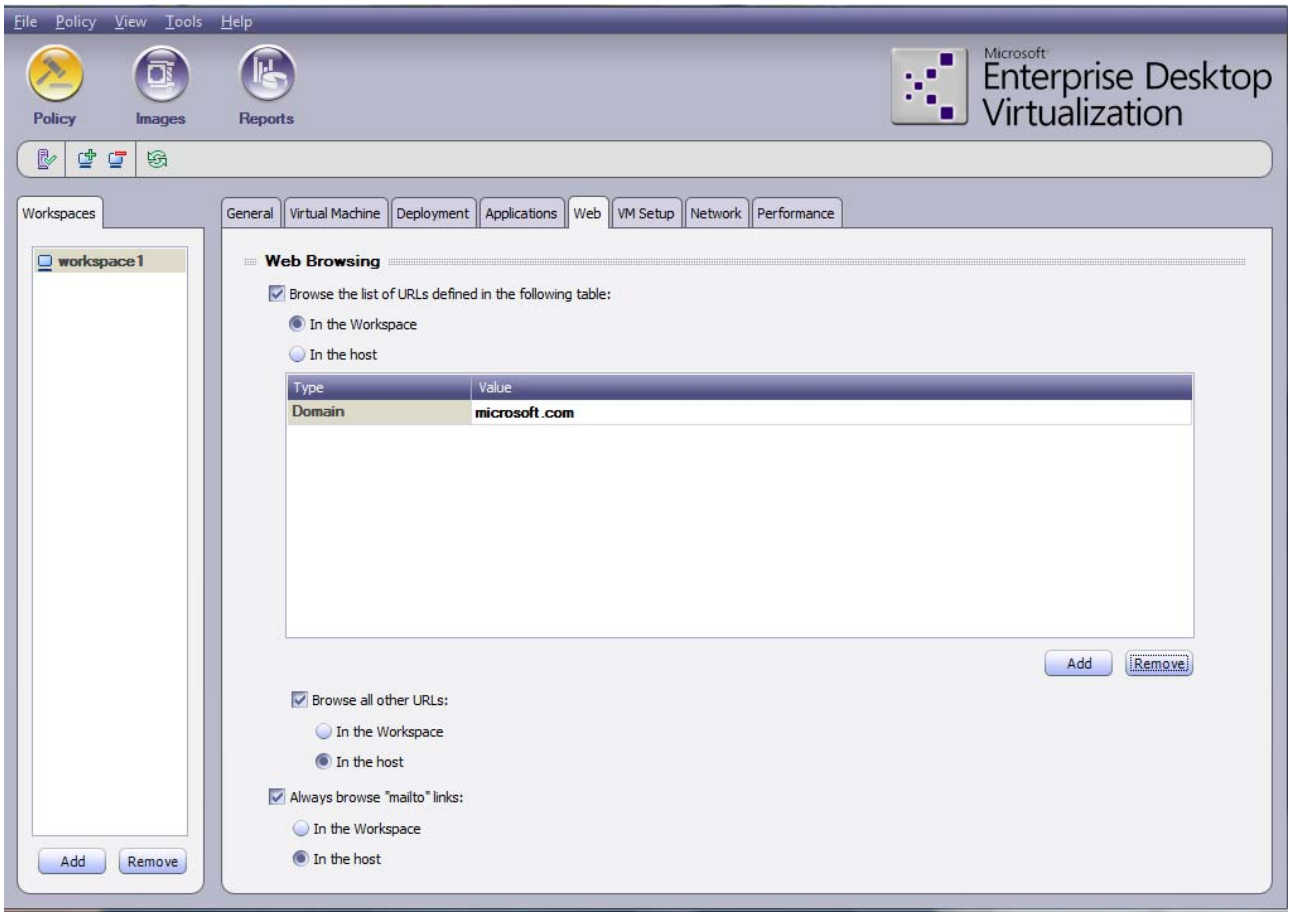


Figure 34: Web Settings

To configure web settings for the Workspace:

1. Click on the Workspace you wish to apply the web settings to.

   The selected Workspace appears highlighted.

2. Select **Browse the list of URLs defined in the following table** to redirect the user to a browser within the Workspace or host, when the user browses to a URL which conforms to the web rules specified.

3. Click one of the following:

   - **In the Workspace** - redirect to a browser in the Workspace.
   - **In the host** - redirect to a browser on the host.

4. Select **Browse the rest of the URLs** to redirect all URLs excluded from the web rules to the host or Workspace.

5. Click one of the following:

   - **In the Workspace** - redirect all other URLs to a browser in the Workspace.
   - **In the host** - redirect all other URLs to a browser on the host.

To add a web rule:

1. Select **Browse the list of URLs defined in the following table** to enable the web browsing rules.
2. Click **Add**.

   A new web rule is added.
3. Configure the web rule properties as described in the following table.

Table 13: Workspace Web Properties

Property	Possible Values/Remarks
Type	• **Domain suffix** - Access to any host address ending with the suffix specified in the **Value** property, is set according to the option set in **Web Browsing**. • **IP Prefix** - Access to any full or partial IP address in the range of the prefix specified in the **Value** property, is set according to the option set in **Web Browsing**. • **All Local Addresses** - Access to all addresses without a '.' are set according to the option set in **Web Browsing**.
Value	• If Domain Suffix is selected in the **Type** property, enter a domain suffix. **Note:** Do not enter "*" before the suffix. **Note:** Domain suffixes support aliases as well. • If IP Prefix is selected in the **Type** property, enter a full or partial IP address.

To delete a web rule:

1. In the **Web** pane, select the web rule you wish to delete.
2. Click **Remove**.

   The web rule is deleted.

7.5.1. Browsing Mail Links

In addition to defining web access rules, you can define one additional property: whether the user can browse mail links. If enabled, when the user clicks a mailto link in the host, the default email software in the Workspace or host is launched.

To browse mail links:

1. Select **Always browse "mailto" links**.
2. Click one of the following:
   - **In the Workspace** - redirect to a browser in the Workspace.
   - **In the host** - redirect to a browser on the host.

   Mailto links are activated.

7.6. VM Setup Settings

The Virtual Machine setup configures the setup performed when the Virtual Machine is run on the client for the first time. The Virtual Machine setup is configured differently for persistent and revertible Workspaces. For a detailed description of persistent and revertible Workspaces, refer to Configuring a Workspace Policy.

All Virtual Machine setup configuration settings are configured in the Policy module, from the VM Setup tab.

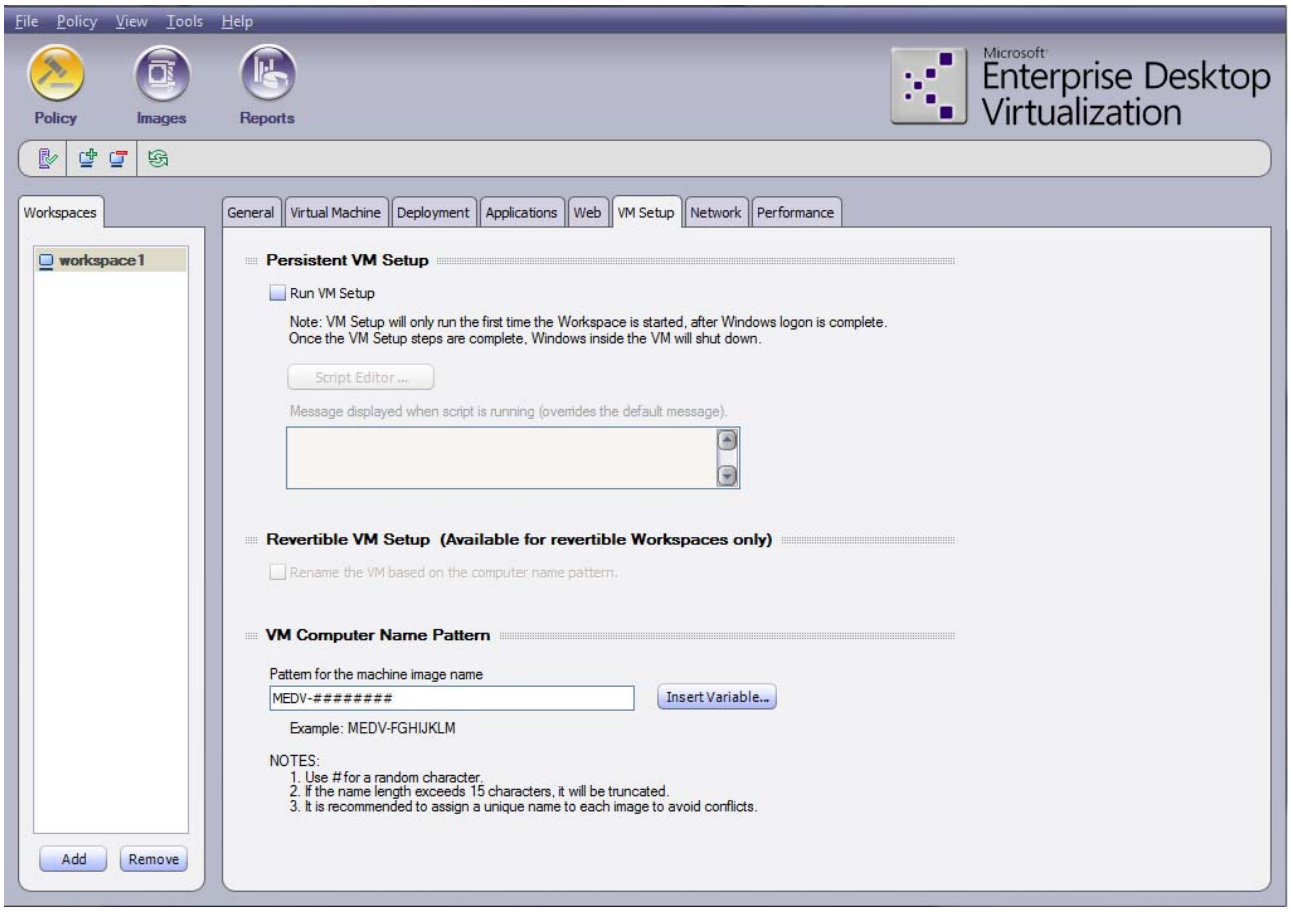


Figure 35: VM Setup Settings

To configure the Virtual Machine setup for a persistent Workspace:

1. Click on a persistent Workspace you wish to apply the settings to.

   The selected Workspace appears highlighted.

2. In the **Persistent VM Setup** section, configure the properties as described in the following table.

Note: The persistent VM setup properties are only enabled for a persistent Workspace.

Table 14: Persistent VM Setup Properties

Property	Possible Values/Remarks
Run VM Setup	Select this check box to run a setup script the first time the Workspace is run.

Property	Possible Values/Remarks
Script Editor...	Click to configure the setup script. For more information, refer to Script Actions Properties. **Note:** This button is only enabled when **Run VM Setup script** is selected.
Message Displayed when script is running	Enter a message to be displayed while the script is running. If left blank, the default message will be displayed. **Note:** This field is only enabled when **Run VM Setup script** is selected.

To configure the Virtual Machine setup for a revertible Workspace:

1. Click on a revertible Workspace you wish to apply the settings to.

   The selected Workspace appears highlighted.

2. In the **Revertible VM Setup** section, configure the properties as described in the following table.

   Note: The revertible VM setup properties are only enabled for a revertible Workspace.

Table 15: Revertible VM Setup Properties

Property	Possible Values/Remarks
Rename the VM based on the computer name pattern	Select this check box to assign a unique name to each computer using the Workspace in order to differentiate between multiple computers using the same Workspace. The machine image names are configured using the VM Computer Name Pattern Properties.

7.6.1. VM Computer Name Pattern Properties

A Virtual Machine computer name pattern can be assigned for both revertible and persistent Workspaces.

- Persistent - In a persistent Workspace administrators can set a computer to be renamed during a setup script.
- Revertible - Administrators can assign a unique name to each revertible Workspace instance to differentiate between multiple computers using the same Workspace.

To assign Virtual Machine computer name pattern to a revertible Workspace:

1. Click on the revertible Workspace you wish to apply the settings to.

   The selected Workspace appears highlighted.

2. In the **Revertible VM Setup** section, select the **Rename the VM based on the computer name pattern** check box (see previous figure).

3. In the **VM Computer Name Pattern** section, enter the pattern to use for naming machine images, using the following:

   - **Constant** - enter free text which will be constant on all computers using the Workspace.
   - **Variable** - enter a variable, by clicking **Insert Variable...** and select from one of the following:

- **User name**
- **Domain name**
- **Host name**
- **Workspace name**
- **Virtual Machine name**

  The variable selected will be specific to the computer using the Workspace. For example, if Domain name is selected, the unique name for each computer will include the computer's domain name.

- **Random characters** - Enter '#' for each random character to include in the pattern. Each computer using the Workspace will have a suffix of the length specified, which is generated randomly.

Note: A revertible VM computer name pattern can only be assigned when the **Rename the VM based on the computer name patters** check box (in the Revertible VM Setup section) is selected.

Note: The computer name has a limit of 15 characters. If the pattern exceeds the limit, it will be truncated.

Note: A unique computer name can only be assigned if it is configured prior to Workspace setup. Changing the name will not affect Workspaces that were already set up.

To assign Virtual Machine computer name pattern to a persistent Workspace:

1. Click on the persistent Workspace you wish to apply the settings to.

   The selected Workspace appears highlighted.

2. In the **Persistent VM Setup** section, click **Script Editor...**.

   The **Script Actions** dialog box appears.

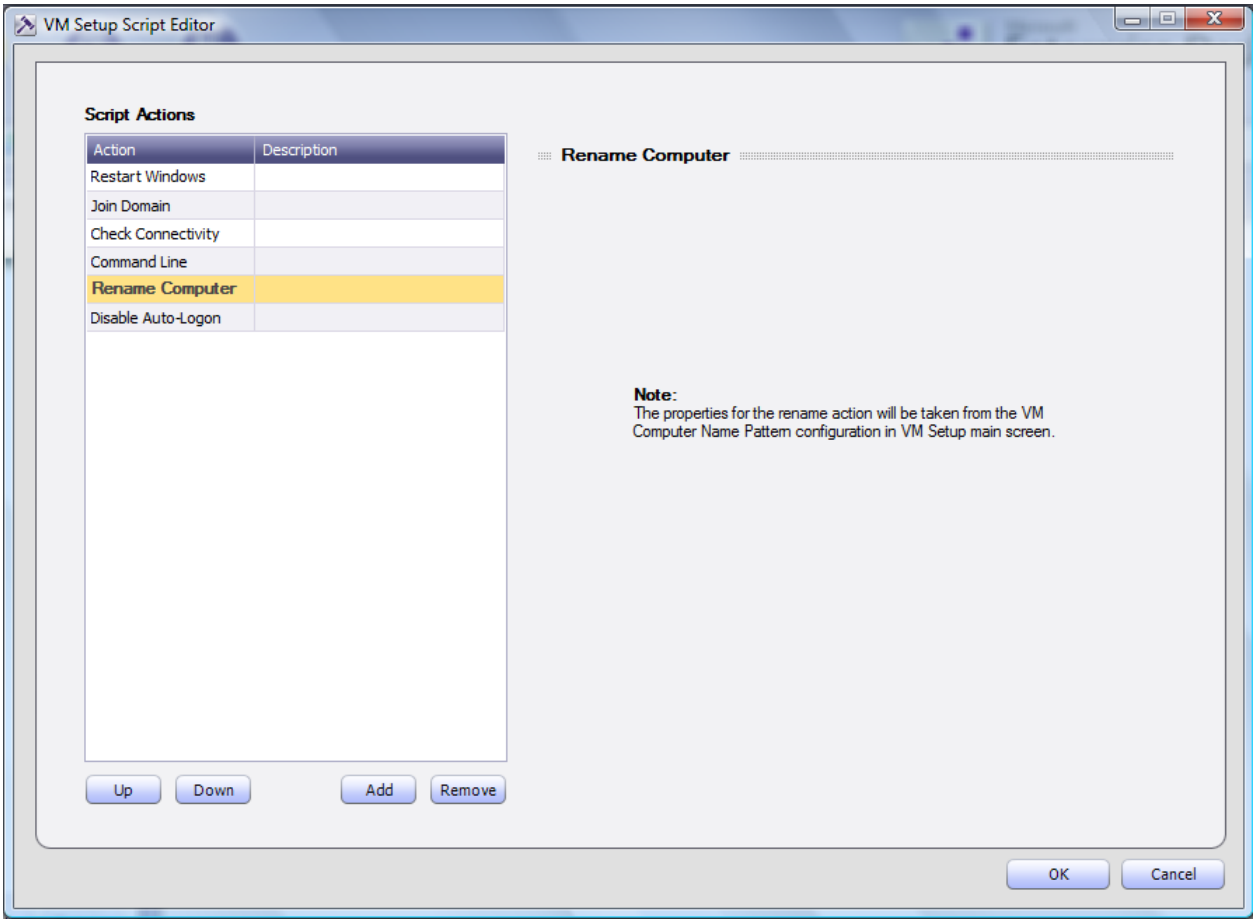


Figure 36: Script Action: Rename Computer

3. Click **Add**; from the popup menu select **Rename Computer**.
4. Click **OK**.

   The Script Actions dialog closes.
5. In the VM setup tab, in the **VM Computer Name Pattern** section, enter the pattern to use for renaming the computer, using the following:
   - **Constant** - enter free text which will be included in the computer name.
   - **Variable** - enter a variable, by clicking **Insert Variable...** and select from one of the following:
     - **User name**
     - **Domain name**
     - **Host name**
     - **Workspace name**
     - **Virtual Machine name**

     The variable selected will be specific to the computer that is being renamed. For example, if Domain name is selected, the computer name will include the computer's domain name.
   - **Random characters** - Enter '#' for each random character to include in the pattern. The computer will have a suffix of the length specified, which is generated randomly.

Note: The computer will only be renamed if it is set as an action in the Script Actions dialog. For detailed information, refer to Script Actions Properties.

Note: The computer name has a limit of 15 characters. If the pattern exceeds the limit, it will be truncated.

7.6.2. Script Actions Properties

The Script Actions editor allows the administrator to create actions to be performed during Workspace setup, as well as to define the order in which they are performed.

The following is a list of actions that can be added to the domain setup script:

- **Restart Windows** - restart Windows.
- **Join Domain** - if joining a domain, include this action and configure the username, password, full qualified domain name, NetBIOS domain name and organization unit (optional).
- **Check Connectivity** - configure a server to connect to, and verify that the Workspace can connect to a network resource (such as the domain server).
- **Command Line** - configure a script in the Workspace and enter a command line that includes the path of the script and the script arguments.
- **Rename Computer** - rename the Virtual Machine computer based on the defined settings.
- **Disable Auto-Logon** - disables Windows Auto-Logon. This action should be added at the end of scripts that add the machine to the domain.

To setup script actions:

1. From the VM Setup tab, click **Script Editor...**.

   The **Script Actions** dialog box appears.

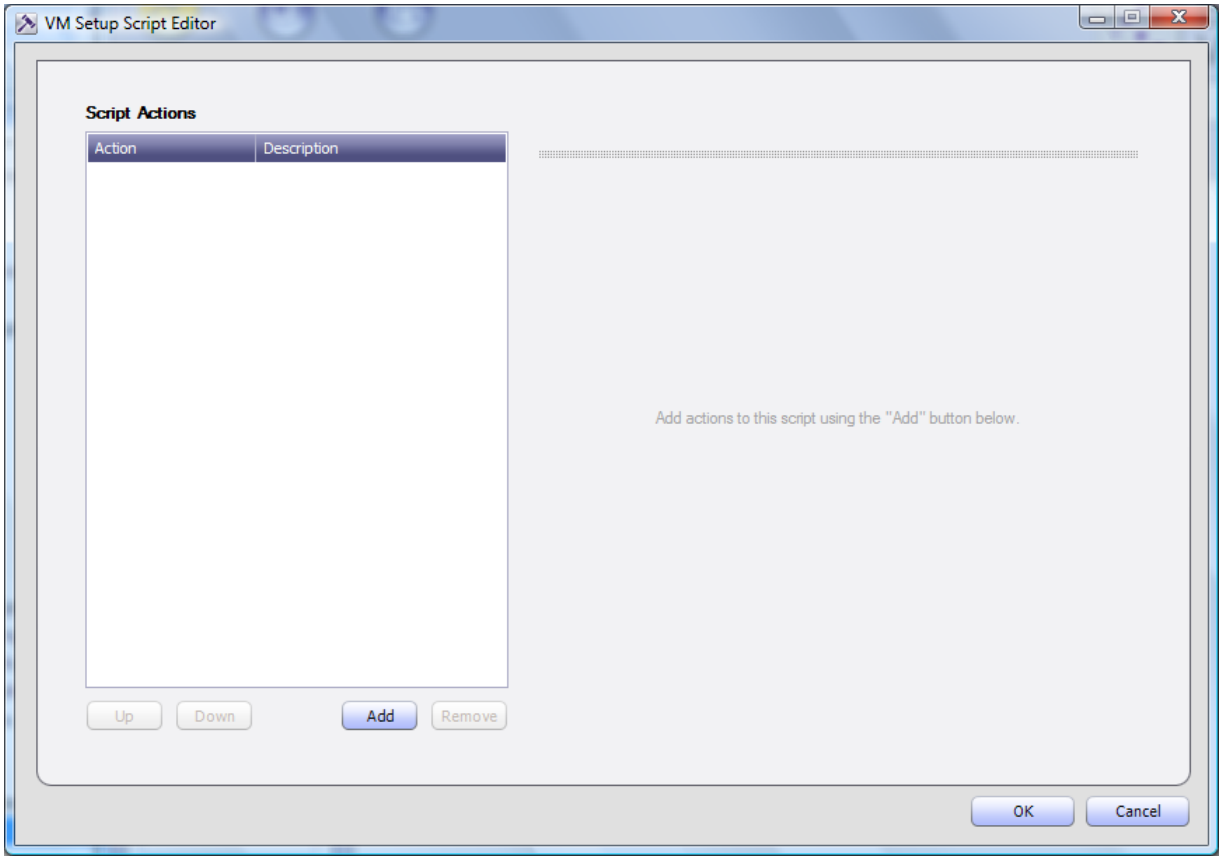


Figure 37: Domain Setup Script Dialog Box

2. Click **Add**, and from the popup menu select the desired actions.
3. Configure the actions as described in the following tables.

Note: Rename Computer is configured in the VM Settings tab. For more information, refer to VM Computer Name Pattern Properties.

Note: To rename computer, Windows must be restarted. It is recommended to add a Restart Windows action following a Rename Computer action.

4. Set the order of the actions, by selecting an action and clicking **Up** or **Down**.
5. Click **OK**.

Note: When running the Join Domain script, in order for the script to work, the user logged into the Workspace Virtual Machine must have local admin rights.

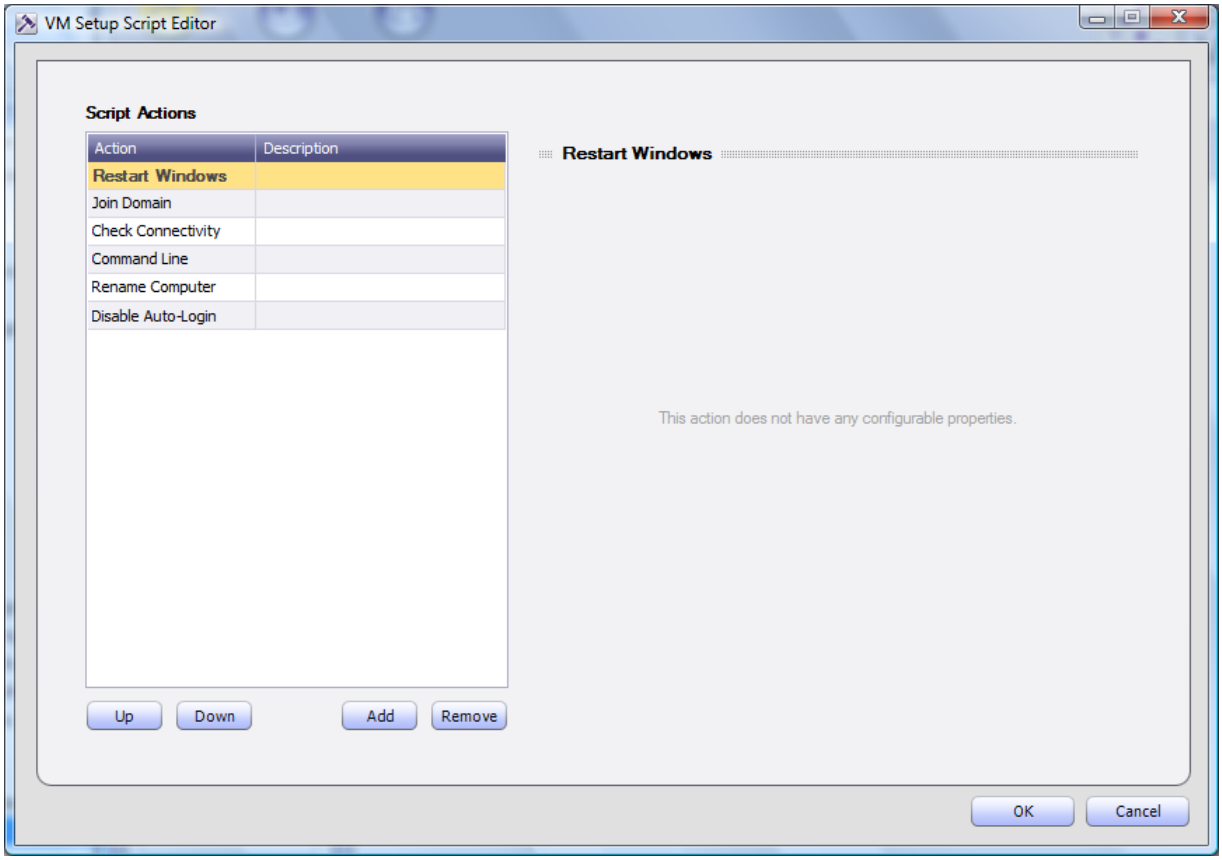


Figure 38: Script Action: Restart Windows

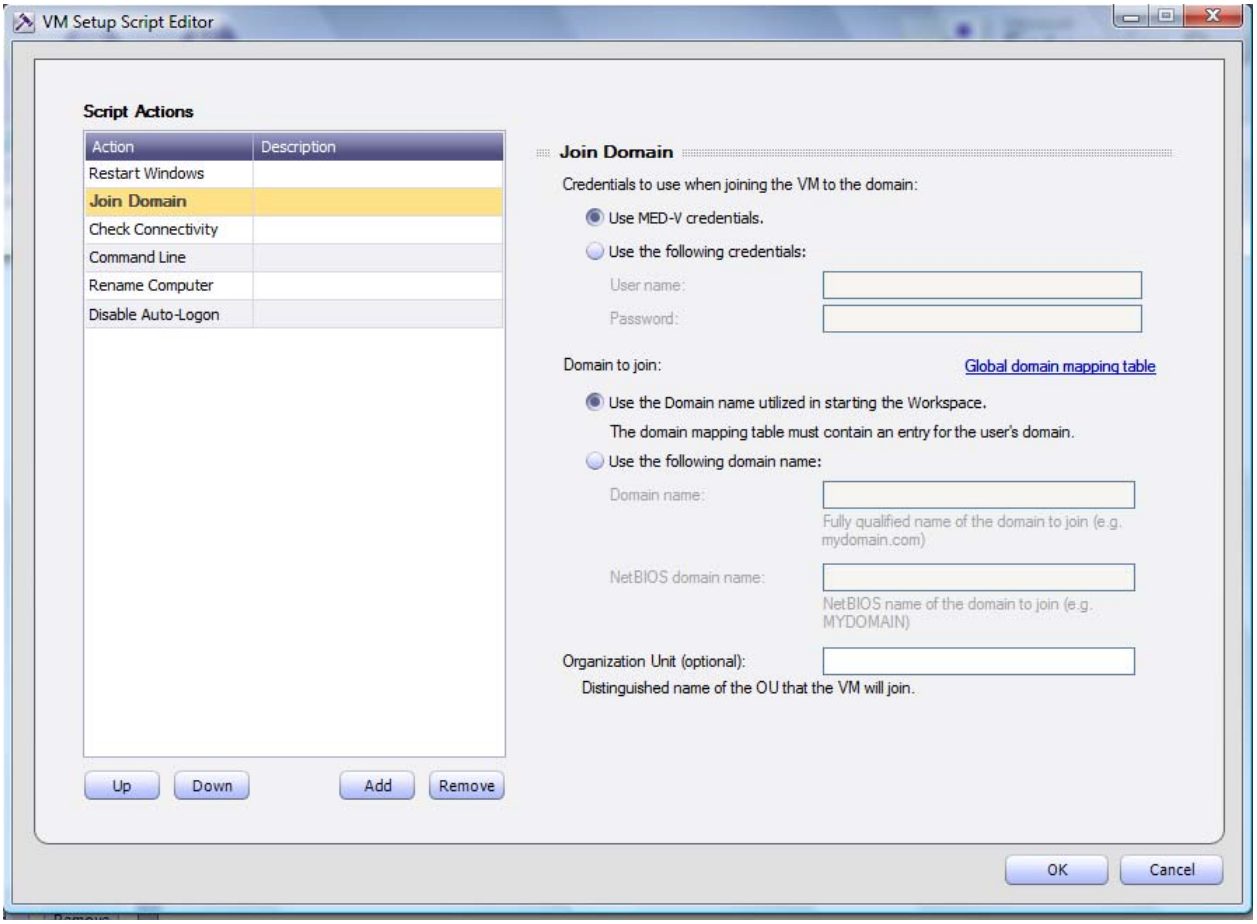


Figure 39: Script Action: Join Domain

Table 16: Join Domain Properties

Property	Possible Values/Remarks
Credentials to use when joining the VM to the domain	Select one of the following credentials to use when joining the VM to the domain: • **Use end-user credentials** - the end-user credentials. • **Use the following credentials** - the credentials specified; enter a user name and password in the corresponding fields.
Domain to join	Select one of the following: • **Use the domain name typed by the end user in the Start Workspace dialog** - join the domain entered by the end user when logging into MED-V Client. To define the mapping from NetBIOS to fully qualified domain names, click **Global domain mapping table**. In the Global domain mapping table, click **Add** and enter a **NetBIOS domain name** and **Fully qualified domain name** • **Use the following domain name** - join the domain specified; enter a domain name and NetBIOS domain name in the corresponding fields.
Organization Unit	An organization unit (OU) may be specified to join the computer to a specific OU. The format must follow an OU distinguished name:

Property	Possible Values/Remarks
	OU=<Organization Unit>,<Domain Controller> (e.g., OU=QATest, DC=il, DC=MED-V, DC=com).

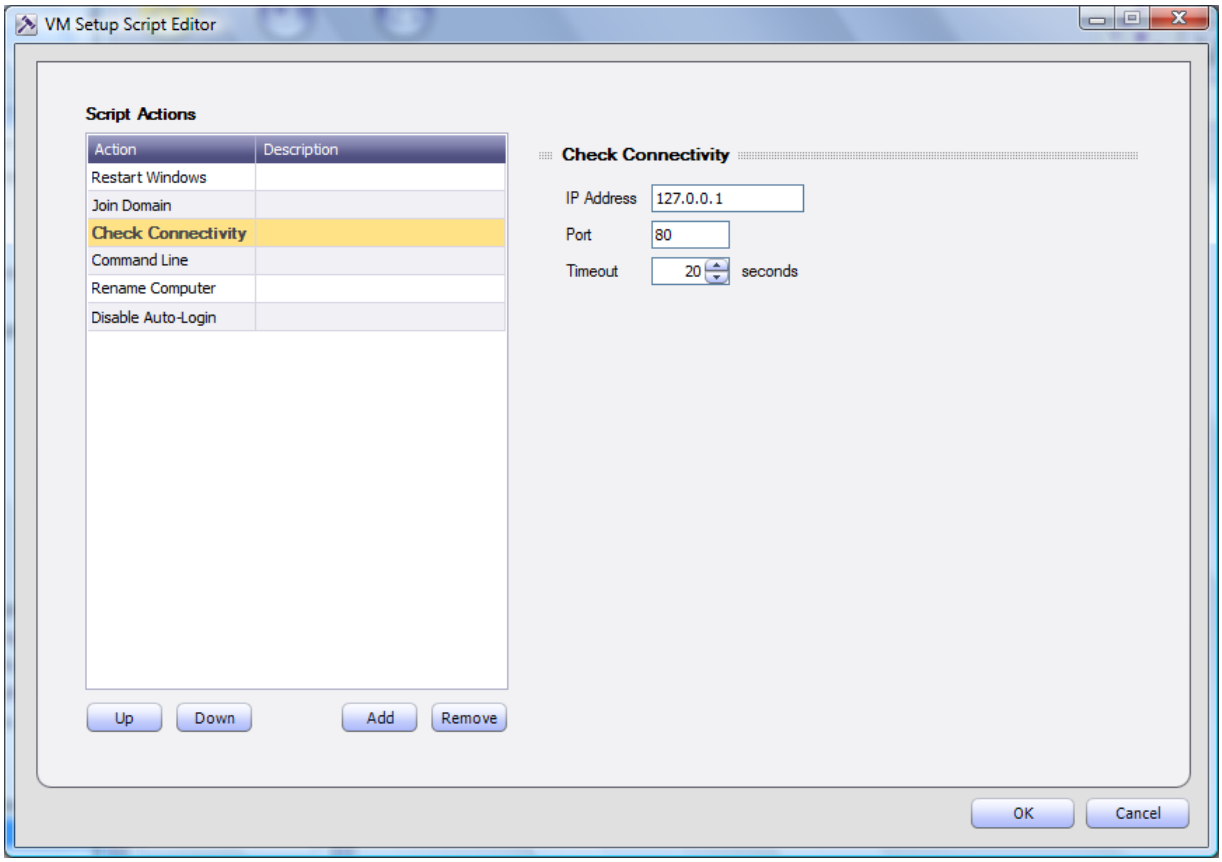


Figure 40: Script Action: Check Connectivity

Table 17: Check Connectivity Properties

Property	Possible Values/Remarks
IP Address	The IP Address of the server that you are verifying connection to.
Port	The port of the server that you are verifying connection to.
Timeout	The number of seconds to wait for a response before timing out.

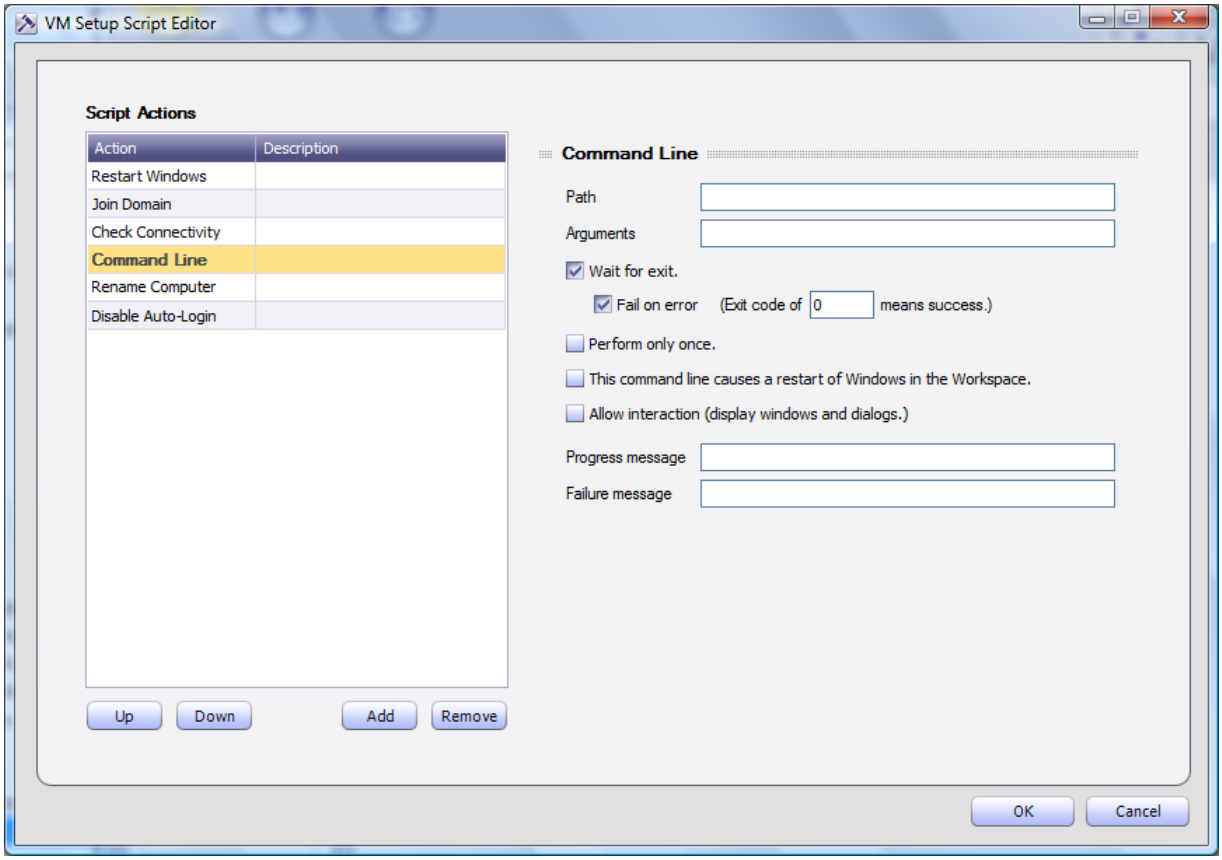


Figure 41: Script Action: Command Line

Table 18: Command Line Properties

Property	Possible Values/Remarks
Path	Configure the path of the command line.
Arguments	Enter any command line arguments.
Wait for exit	Select the check box to wait for a return before continuing with the script actions.
Fail on error	Select this check box to fail if the return is anything but the value specified. Enter the value that will indicate the command as a success. Default: **0**
Perform only once	Select this check box to run only once. If the script fails or is canceled, this command will not be performed again.
This command line causes a restart of Windows in the Workspace	Select this check box if the command line causes a restart after completion.
Allow interaction	Select this check box if the command will require user interaction.
Progress message	Type a message to be displayed to the user while the command is running.
Failure message	Type a message to be displayed to the user if the command fails.

When configuring the Command Line action, several variables can be used as defined in the following table.

Parameter	Value	Description
%KidaroAuthenticatedUser%	An authenticated user name.	MED-V authenticated user name. The user name and password can be used in the join domain VM setup script.
%KidaroAuthenticatedPassword%	An authenticated password.	MED-V authenticated password. The user name and password can be used in the join domain VM setup script.
%KidaroAuthenticatedDomain%	Configured domain.	The domain configured in the MED-V authentication. It can be used on the VM setup scripts.
%DesiredMachineName%	Machine name.	The unique computer name configured in Management. It can be used in the VM Setup script.

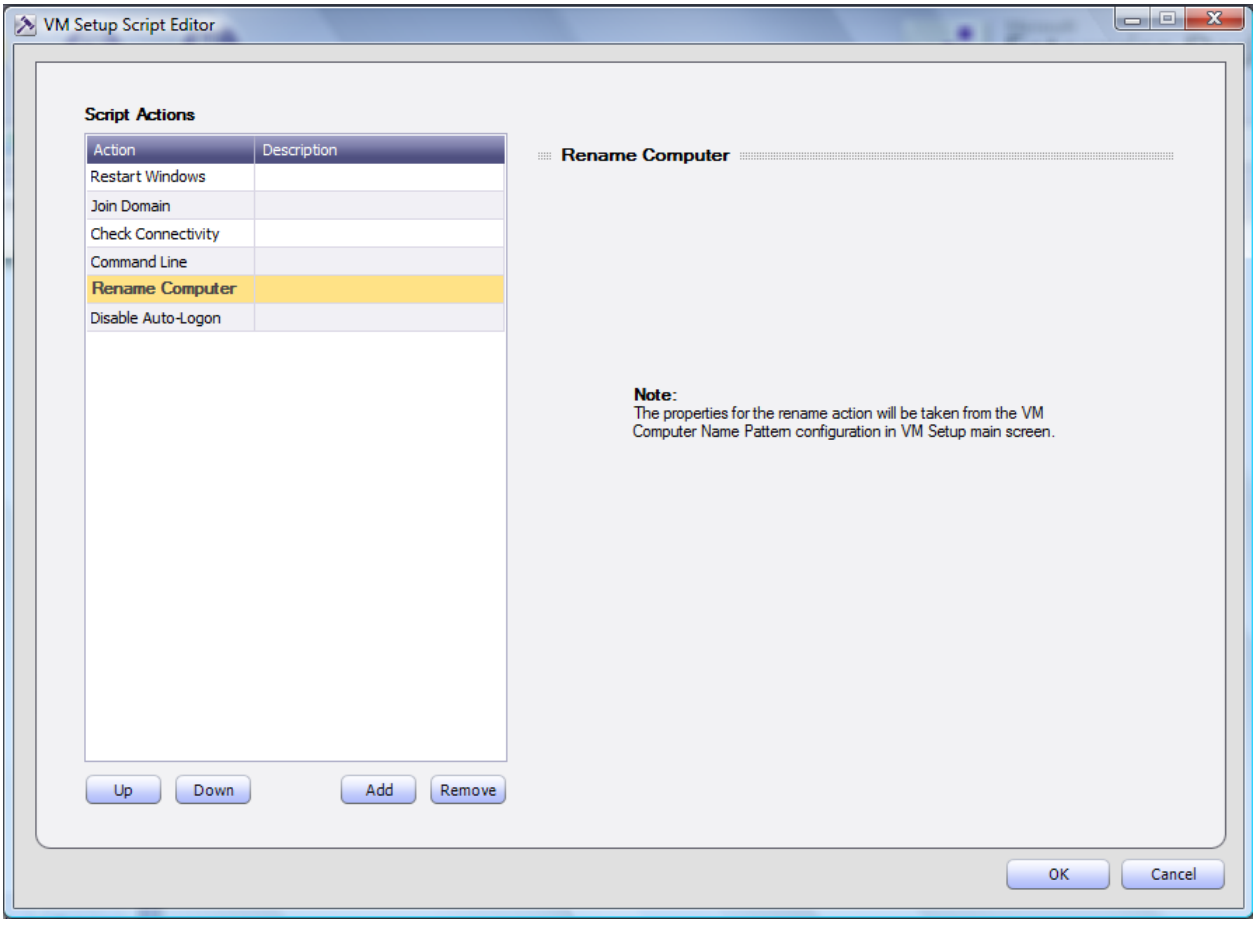


Figure 42: Script Action: Rename Computer

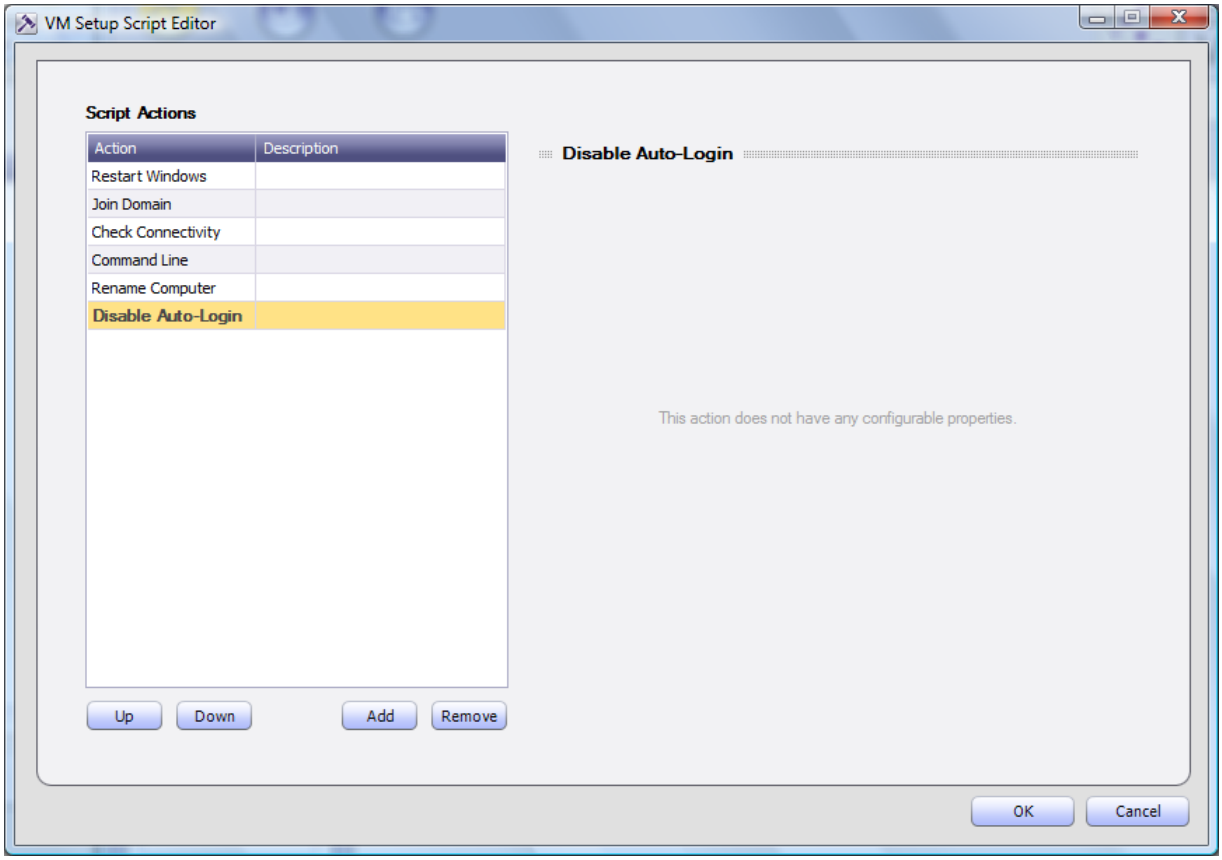


Figure 43: Script Action: Disable Auto-Login

7.7. Network Settings

Administrators can define the network settings for each Workspace.

All network settings are configured in the Policy module, from the Network tab.

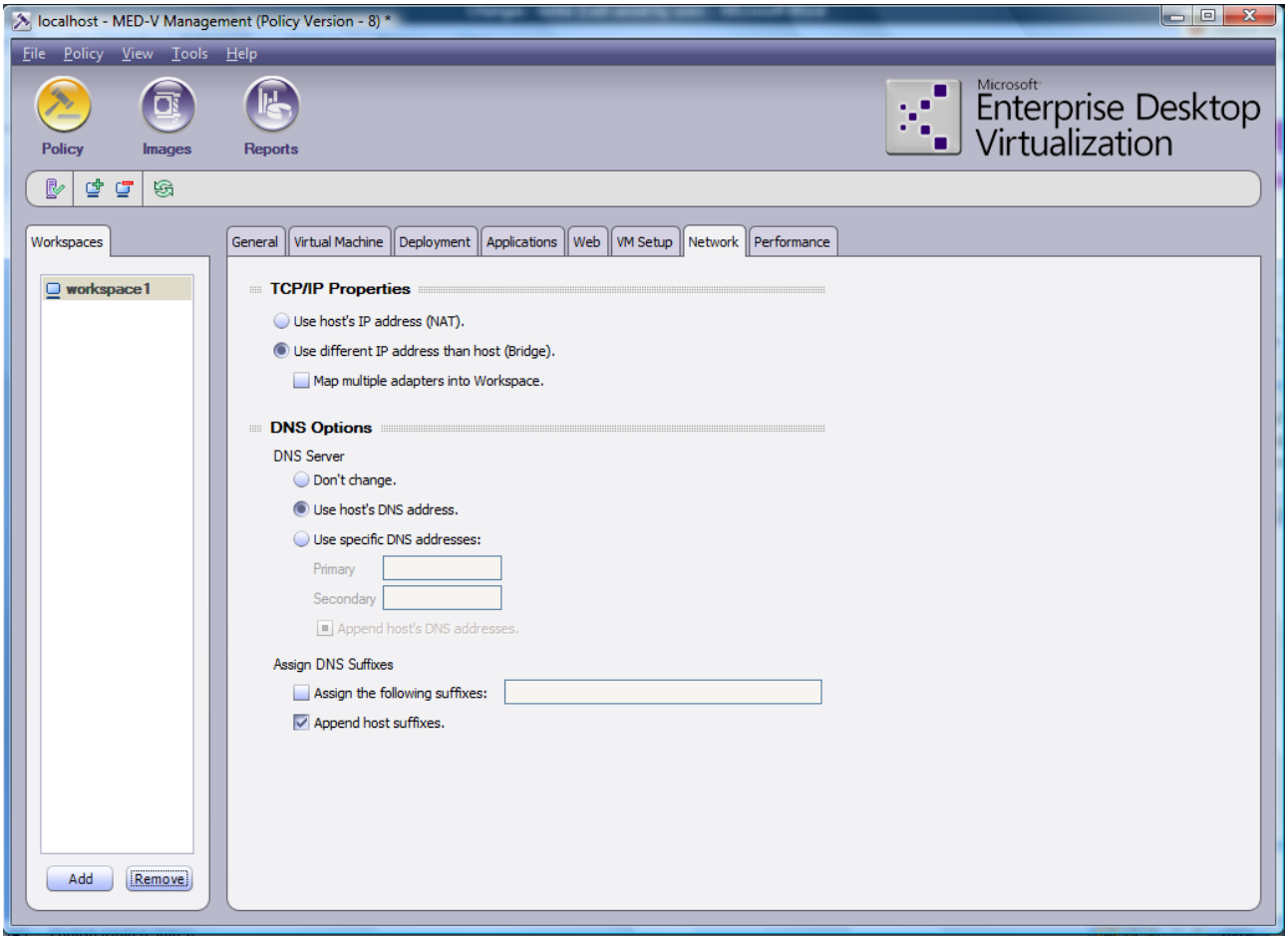


Figure 44: Network Settings

To apply network settings to a Workspace:

1. Click on the Workspace you wish to apply the settings to.

   The selected Workspace appears highlighted.

2. In the **Network** pane, configure the settings as described in the following table.

Table 19: Workspace Network Properties

Property	Possible Values/Remarks
TCP/IP Properties	• **Use host's IP address (NAT)** - The Workspace will use NAT to share the host's IP for outgoing traffic. • **Use different IP address than host (bridge)** - The Workspace will have its own network address, usually obtained via DHCP. Select the **Map multiple adapters into Workspace** check box when the host machine has multiple adapters. It is recommended to use this configuration when the host moves between different networks using different adapters.
DNS Server	• **Don't change** - DNS settings that are set within the Workspace Virtual Machine will not be changed. • **Use Host's DNS address** - Workspace DNS settings will be synchronized to match the host's settings. The DNS synchronization is dynamic. It is synchronized periodically with

Property	Possible Values/Remarks
	the host so that if it is changed on the host, it will change dynamically in the Workspace. • **Use specific DNS addresses** - The Workspace will use a specific DNS, as specified. In the **Primary** and **Secondary** fields, enter the primary and secondary DNS addresses. Select the **Append Host's DNS addresses** check box to append the host to the configured DNS addresses.
Assign DNS Suffixes	• **Assign the following suffixes** - Select this check box to assign specific DNS suffixes; in the box, enter a suffix or multiple suffixes separated by commas. • **Append host suffixes** - Select this check box to append the host suffixes to the DNS address.

7.8. Performance Settings

The following performance setting can be defined for each Workspace:

- Workspace Memory Adjustment

Performance settings are configured in the Policy module, from the Performance tab.

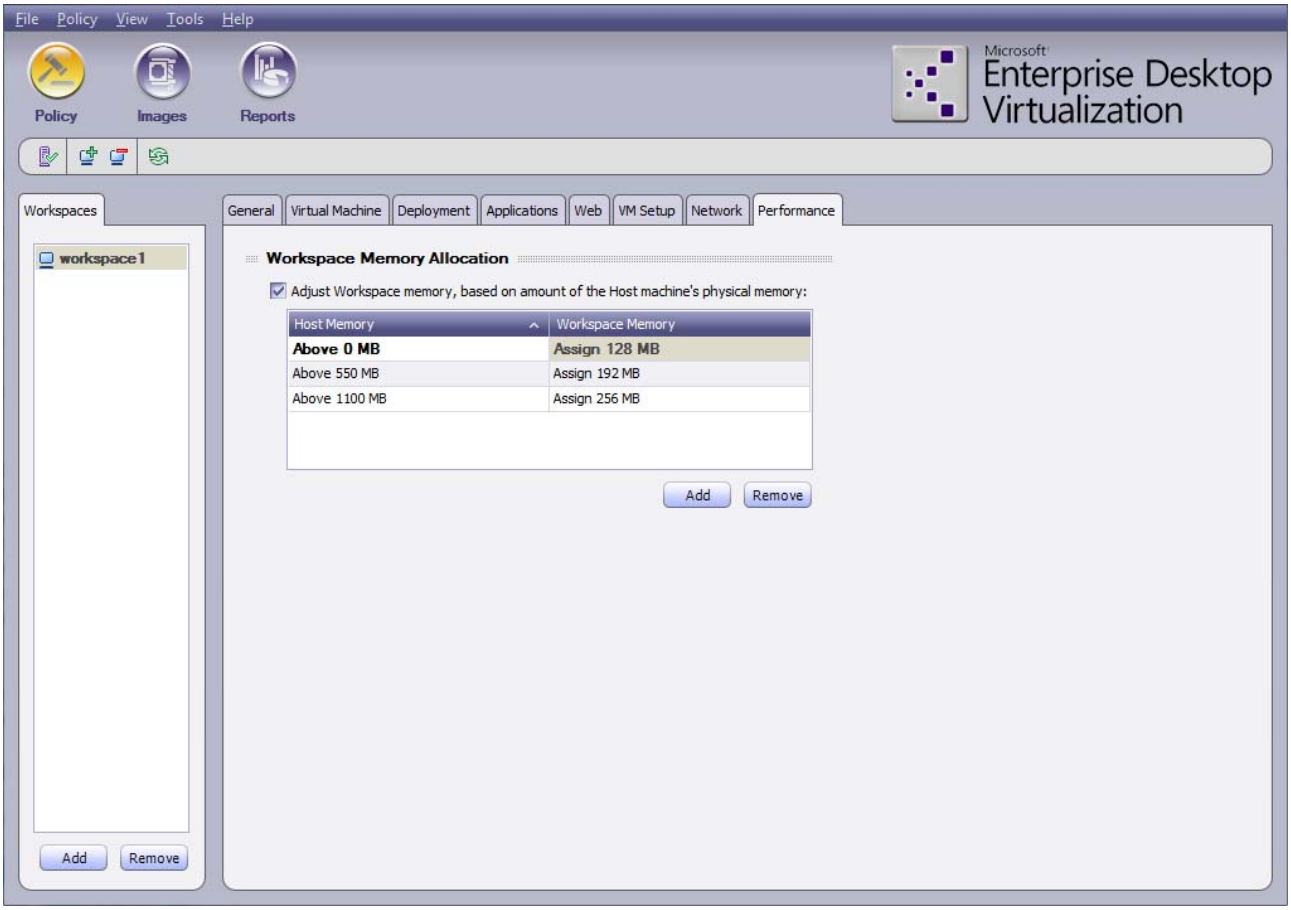


Figure 45: Performance Settings

To apply performance settings to a Workspace:

1. Click on the Workspace you wish to apply the settings to.

   The selected Workspace appears highlighted.

2. Configure the settings as described in the following table.

Table 20: Performance Settings Properties

Property	Possible Values/Remarks
Adjust Workspace memory, based on amount of the Host machine's physical memory	Select this check box and configure the following Workspace properties in the table: • **Host Memory** - Define the common host RAM configuration in your organization based on any numbers of groups you would like to configure. • **Workspace Memory** - Enter the amount of host memory you would like to allocate to the MED-V Workspace.

Chapter 8

8. Deploying MED-V onto the Client

In This Chapter

8.1. Installing MED-V from the Command Line

To install MED-V from the command line:

- From the command line, run the MED-V MSI followed by any of the optional parameters described in the following table.

  The MED-V MSI is called `MED-V_x.msi`, where x is the version number.

  For example, `MED-V_1.0.65.msi`.

Parameter	Value	Description
/quiet		Silent installation
/log <full path to log file>	The full path to the log file.	
INSTALLDIR	The full path to the installation directory.	
VMSFOLDER	The full path to the Virtual Machine folder.	
INSTALL_ADMIN_TOOLS	**1,0** **Default: 0**	Installs MED-V administration tools.
START_AUTOMATICALLY	**1,0** Default: **0**	Automatically starts MED-V Client every time the user logs on to Windows.
SERVER_ADDRESS	host name or IP	

Parameter	Value	Description
SERVER_PORT	port	
SERVER_SSL	**1,0** for **https** or **http**	
START_MEDV	**1**,**0** Default: **1**	Starts MED-V at the completion of the MED-V installation. Note: it is recommended to set START_MEDV=0 in case MED-V is installed by the system (e.g. SCCM)
DESKTOP_SHORTCUT	**1,0** Default: **1**	Creates a shortcut on the Desktop, which starts MED-V Client.
MINIMAL_RAM_REQUIRED	RAM in MB	When installing MED-V, checks if the computer has the minimum amount of RAM specified. If not, installation is aborted.

8.2. Creating a Deployment Package

The deployment package installation provides a method of installing MED-V Client together with all its required prerequisites as well as any settings pre-defined by the administrator.

The Packaging wizard walks you through the creation of a package by creating a folder on your local machine and transferring all the required installation files to the single folder. The contents of the folder can then be moved to multiple removable media drives for distribution.

To create a deployment package:

1. Verify in the Images module, that you have created at least one local packed image.
2. From the **Tools** menu, select **Packaging wizard**.

   The **Packaging wizard** welcome screen appears.

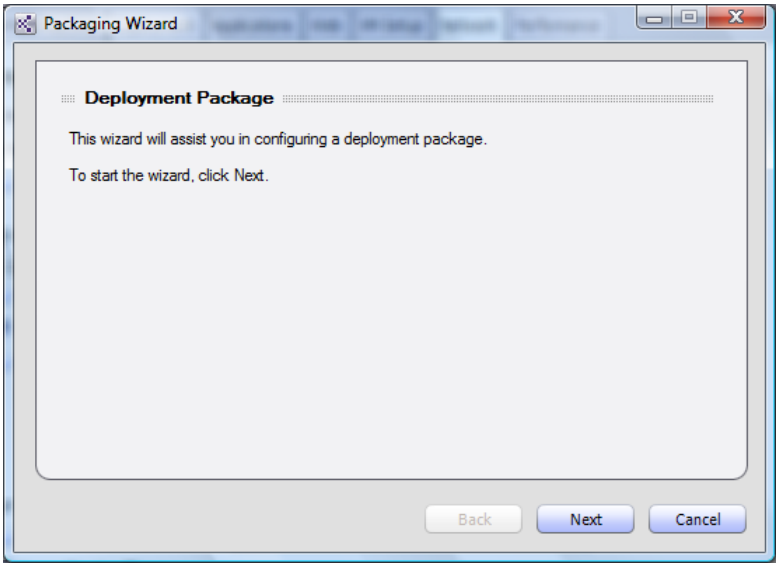


Figure 46: Welcome Screen

3. Click **Next**.

   The **Workspace Image** screen appears.

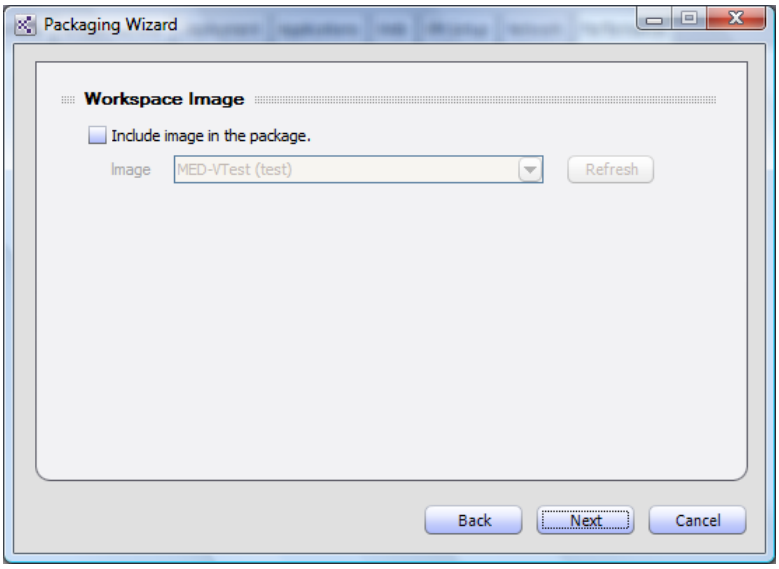


Figure 47: Workspace Image Screen

4. Select the **Include image in the package** check box, to include an image in the package.

   The Image field is enabled.

Note: An image is not required in a MED-V package; the package can be created without an image. In such a case, the image should be uploaded to the server so that it can later be downloaded over the network to the client.

---

5. In the **Image** field, click on the drop-down box to view all available images. Select the image to be copied to the package. Click **Refresh** to refresh the list of available images.
6. Click **Next**.

   The **MED-V Installation Settings** screen appears.

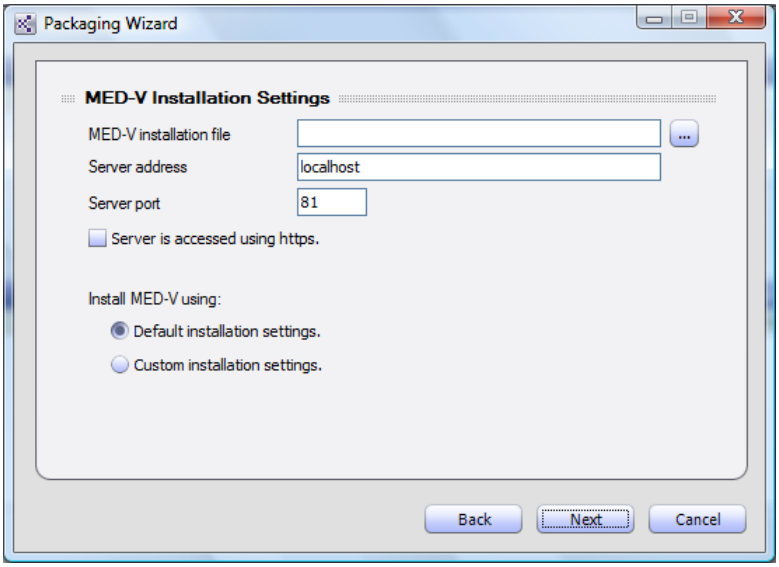


Figure 48: MED-V Installation Settings Screen

7. Select the MED-V installation file by doing one of the following:
   - In the **MED-V installation file** field, type the full path to the directory where the installation file is located.
   - Click **...** to browse to the directory where the installation file is located.

Note: This field is mandatory and the wizard will not continue without a valid file name.

8. In the **Server address** field, type in the Server name or IP address.
9. In the **Server port** field, type the Server port.
10. Select the **Server is accessed using https** check box, to require an https connection to connect to the server.
11. Select **Default installation settings** to continue and leave the default settings.

    Select **Custom installation settings** and then **Next** to set the installation settings in the following screen:

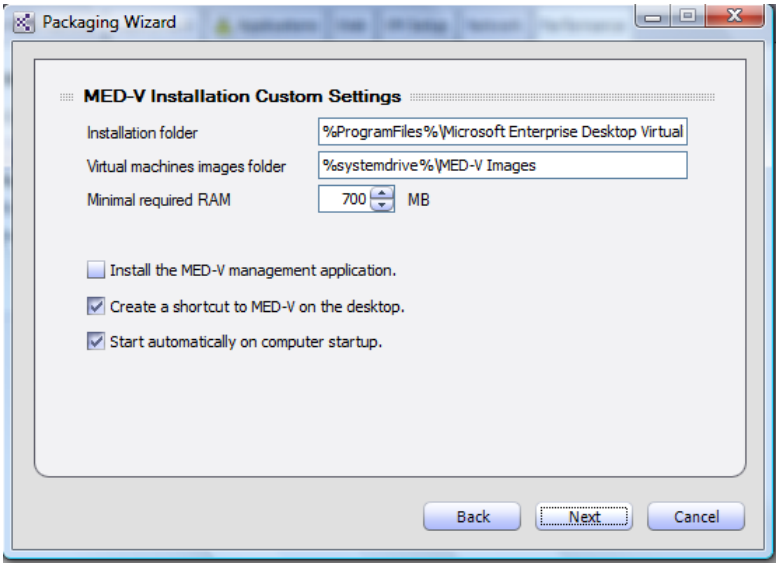


Figure 49: MED-V Installation Custom Settings Screen

a. In the **Installation folder** field, type in the path of the folder where the MED-V files will be installed on the host machine.

Note: It is recommended to use variables in the path rather than constants which might vary from computer to computer.

For example: use `%ProgramFiles%\MED-V` instead of, `c:\MED-V`).

---

b. In the **Virtual machines images folder** field, type the path of the folder where the virtual images files will be installed on the host machine.

c. In the **Minimal required RAM** field, enter the RAM required to install a MED-V package. If the user installing the MED-V package does not have the minimal required RAM, the installation will fail.

d. The following 3 options are enabled or disabled based on the type of package being defined. The first 2 are enabled for a Local package and the last one is enabled for a Portable Workspace package. Select the options you wish from those that are enabled.

- **Install the MED-V management application** - include the MED-V Management Console application in the installation.
- **Create a shortcut to MED-V on the desktop** - create a shortcut to MED-V on the host's desktop.
- **Start automatically on computer startup** - start MED-V automatically on startup.

e. Click **Next**.

The **Additional Installations** screen appears.

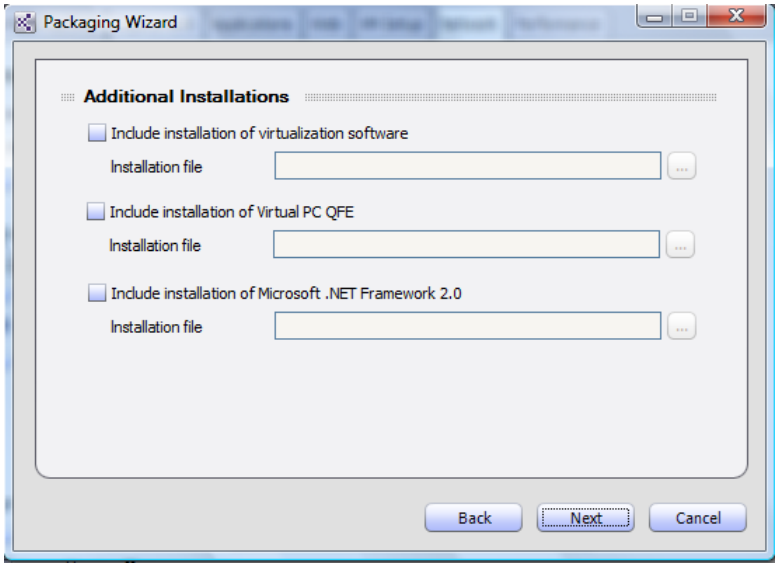


Figure 50: Additional Installations Screen

12. Select the **Include installation of virtualization software** check box to include the Virtual PC installation in the package.

    The **Installation file** field is enabled. Type in the full path of the virtualization software installation file or click **...** to browse to the directory.

13. Select the **Include installation of Virtual PC QFE** check box to include Virtual PC QFE installation in the package.

    The **Installation file** field is enabled. Type the full path of the Virtual PC QFE installation file of click **...** to browse to the directory.

14. Select the **Include installation of Microsoft .NET Framework 2.0** check box to include the Microsoft .NET Framework 2.0 installation in the package.

    The **Installation file** field is enabled. Type in the full path of the Microsoft .NET Framework 2.0 installation file or click **...** to browse to the directory.

15. Click **Next**.

    The **Finalize** screen appears.

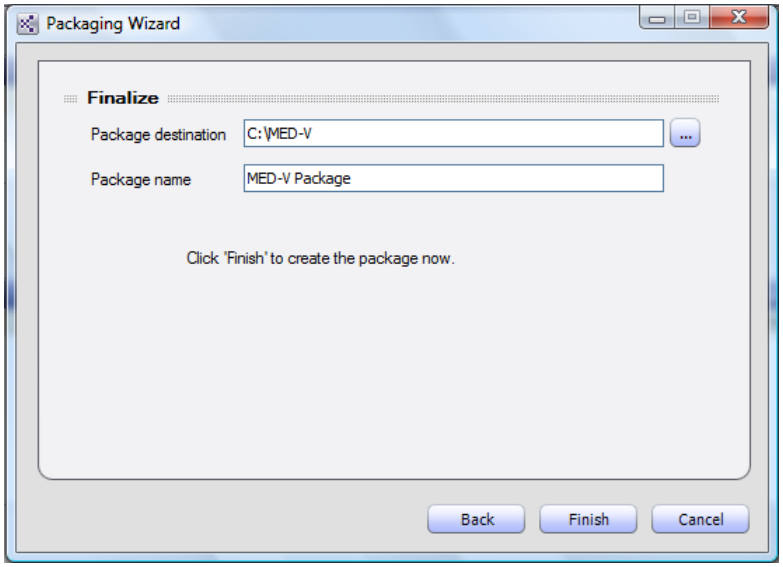


Figure 51: Finalize Screen

16. Select the location where the package should be saved by doing one of the following:
    - In the **Package destination** field, type the full path to the directory where the package should be saved.
    - Click **...** to browse to the directory where the installation files should be saved.

Note: Building the package may consume more space than the actual package size. It is therefore recommended to build the package on the hard drive. Once the package is created, it can then be copied to the USB.

17. In the **Package name** field, type in a name for the package.
18. Click **Finish** to create the package.

    The package is created. This may take several minutes.

    Once the package is created a message appears notifying you that it has been completed successfully.

Note: If your installation location was not removable media, ensure that you copy only the contents of the folder and not the folder itself to the removable media.

Note: The removable media must be large enough so that the package contents consume maximum of 3/4 of the removable media's memory.

Note: When creating the package, up to double the size of the actual package size may be required when the build is complete.

8.3. Installing MED-V from a Deployment Package

To install a deployment package:

1. Do one of the following:
    - Download the MED-V package from the web.
    - Insert the deployment USB or DVD into the host drive.
2. If MED-V doesn't launch automatically, double-click MED-VAutoInstaller.exe.

A dialog appears listing the components that are already installed and those that are currently being installed.

Note: If a version of the Microsoft Virtual PC which is not supported exists on the host machine, a message will appear telling you to uninstall the existing version and run the installer again.

Note: If an older version of MED-V Client exists, it will prompt you asking if you wish to upgrade.

Depending on the components that have been installed, you may need to reboot. If rebooting is necessary, a message appears notifying you that you must reboot.

3. If necessary, reboot the machine.

   Once the installation is complete, MED-V starts and a message appears notifying you that the installation is complete.

4. Login to MED-V using the following user name and password:
   - Type in the domain name and user name followed by the password, of the domain user which is permitted to work with MED-V.
     - Example: "domain_name\user_name", "password"

8.4. Deploying a Workspace Image

Once Administrators have created or updated an image, it can be deployed onto client machines in one of the following ways:

- Web download - The administrator uploads the image to the server and then configures the updated image in the Workspace Policy.

  MED-V Clients which are connected to the MED-V server check for a Policy and Workspace update every fifteen minutes. If there is an updated policy that includes a new image version, the client downloads it.
- Distribution of the image to the client using the corporate deployment system.
- Deploying the image inside the deployment package - Administrators configure the image inside a deployment package. The image is then imported to the host as part of the package installation.

  For details, refer to Installing MED-V from a Deployment Package.

8.4.1. Deploying a Workspace image via the Web

To deploy a Workspace image via the web, the MED-V image must be uploaded to the server. Once it is uploaded, the image is updated on all machines of associated users.

Note: Before uploading an image, verify that a web proxy is not defined in your browser settings and that Windows Update is not currently running.

To upload a packed image to the server:

1. Click on the **Images** button.

   The **Images** module appears.

2. In the **Local Packed Images** pane, select an image.
3. From the toolbar, click **Upload image to server**.

The image is exported and then uploaded to the server. This may take a considerable amount of time.

Images on the server are defined with the properties defined in the following table.

Table 21: Packed Images on Server Properties

Property	Possible Values/Remarks
Image Name	The name of the packed image as it was defined when the administrator created the image.
Version	The version of the displayed image. **Note:** All previous versions are kept unless deleted.
File Size (compressed)	The physical compressed size of the image.
Image Size (uncompressed)	The physical uncompressed size of the image.

You can download an image from the server to your local machine so that you can work on the image.

8.4.2. Configuring Image Pre-Staging

Pre-staging enables deploying an image via the corporate deployment system, such as SCCM, rather than downloading it from the MED-V server. Pre-staging is useful in environments where the corporate system is more effective than the MED-V server.

Note: Image pre-staging only works for the initial image download. It is not supported for image update.

To configure image pre-staging:

1. On the client machine, under the image store directory, create a folder for the pre-staging image.
2. A default registry key is created.

   Note: The registry key name is `PrestagedImagesPath`.

3. When MED-V Client starts, it will look in the specified directory for an image (ckm file and index file). If it finds an image, it will import it. If the image is not located in this path, it will download it from the server.

Chapter 9

9. Running MED-V Client

In This Chapter

9.1. Starting MED-V Client

To start the MED-V Client:

- From the Windows Start menu, select **All Programs** > **MED-V** > **MED-V Client**.

  or

  On the Desktop, double-click the MED-V icon.

9.2. Starting a Workspace

To start a Workspace:

1. From the notification area, right-click on the MED-V icon.
2. From the popup menu, click **Start Workspace**.
   - If there are multiple Workspaces running on the machine, the **Workspace Selection** window appears.

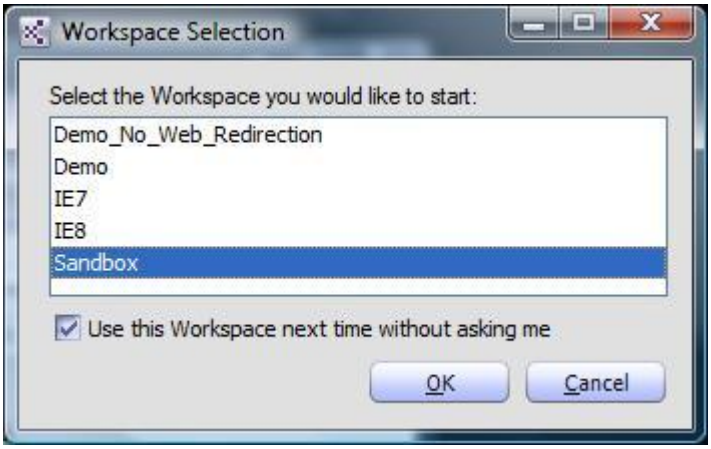


Figure 52: Workspace Selection

a. Select a Workspace.

b. Select the **Use this Workspace next time without asking me** check box, to skip this window the next time the client is started and automatically open the selected Workspace.

c. Click **OK**.

The **Start Workspace Authentication** window appears.

- If there are several Workspaces on the machine, and you have opted to use a specified Workspace, the following window appears:

Figure 53: Workspace Login

- If there is only one Workspace on the machine, the following window appears:

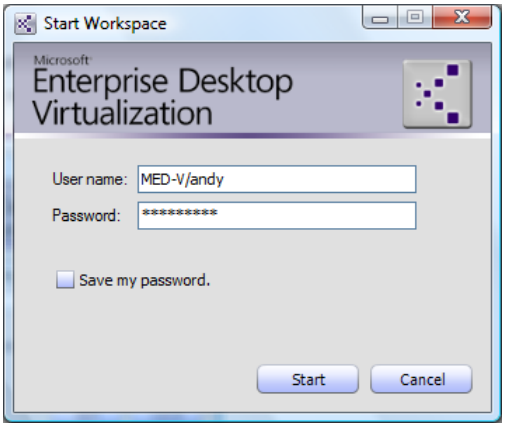


Figure 54: Workspace Login

3. Type in your domain user credentials.

Note: The first time a Workspace is started, the user name should be in the following format: <domain name>\<user name>.

4. Select the **Save my password** check box to save your password between sessions.

Note: In order to enable the save password feature, the `EnableSavePassword` attribute must be set to `True` in the `ClientSettings.xml` file. The file can be found in the **Servers\Configuration Server** folder.

5. Clear the **Start last used Workspace** check box to choose a different Workspace.
6. Click **Start**.

   Several status screens appear depending on the Workspace configuration.

   - If MED-V has not yet been deployed with an image, the following Workspace Download screen appears:

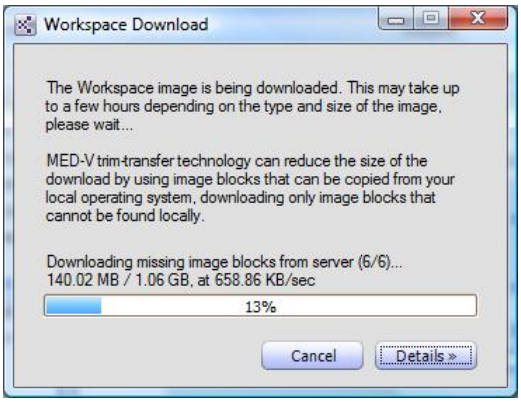


Figure 55: Workspace Download Screen

   - When setting up a persistent Workspace, the following Workspace Setup screen appears:

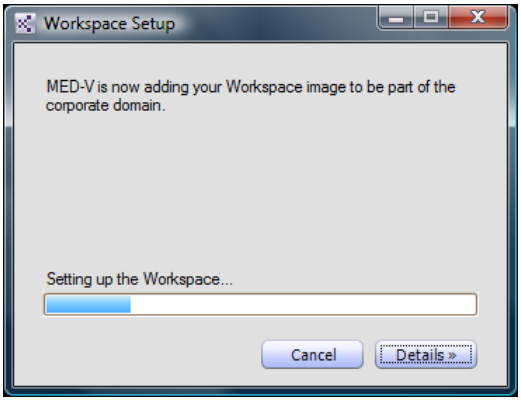


Figure 56: Workspace Setup Screen

The Workspace Start screen appears.

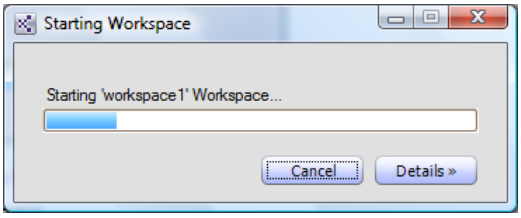


Figure 57: Starting Workspace Screen

9.3. Restarting a Workspace

To restart a Workspace:

1. When the client is running, from the notification area, right-click on the MED-V icon.
2. From the popup menu, click **Restart Workspace**.

   The Workspace is restarted.

   - In a persistent Workspace:

     The Virtual Machine is shutdown and then restarted.
   - In a revertible Workspace:

     The Virtual Machine does not actually shut down, it rather returns to its original state.

9.4. MED-V Settings

To view MED-V settings:

1. From the notification area, right-click the MED-V icon.
2. From the popup menu, click **Settings...**.

   The **Settings** dialog box appears.

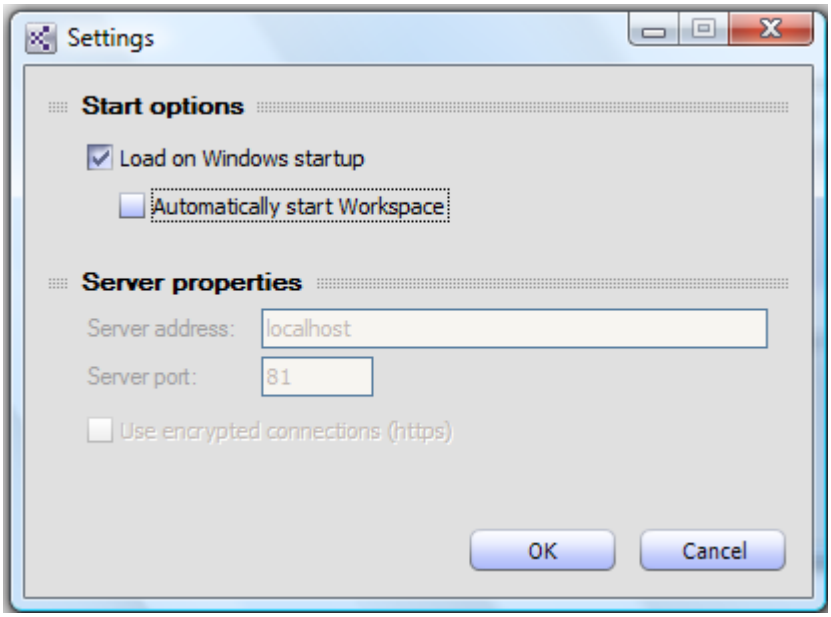


Figure 58: Settings Dialog Box

3. Select **Load on Windows startup** to load MED-V on startup.
4. Select **Automatically start Workspace** to automatically start the Workspace on startup.
5. Configure the server properties described in the following table.

Table 22: Server Settings

Property	Possible Values/Remarks
Server address	The server's DNS name or IP address.
Server port	The server's port.
Use encrypted connections (https)	Select this check box to use encrypted connections.

9.5. About MED-V

To view MED-V general information:

1. From the notification area, right-click the MED-V icon.
2. From the popup menu, click **Help** and then **About...**.

   The **About MED-V** dialog box appears.

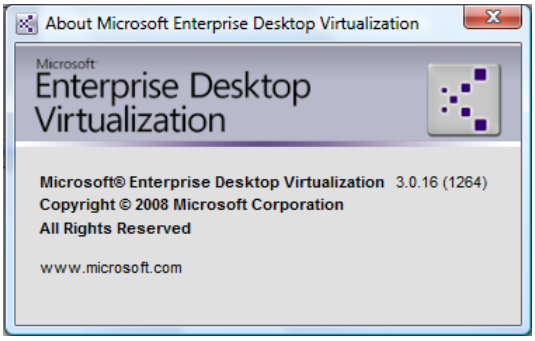


Figure 59: About MED-V Dialog Box

9.6. MED-V Support

To view MED-V support information:

Note: The support contact information only appears if it was configured in MED-V Management.

1. From the notification area, right-click the MED-V icon.
2. From the popup menu, click **Help** and then **Support...**.

   The **Support Contact Information** dialog box appears.

Figure 60: Support Contact Information Dialog Box

9.7. Locking and Unlocking a Workspace

To lock a Workspace that is currently running:

1. From the notification area, right-click on the MED-V icon.
2. From the popup menu, select **Lock Workspace**.

To unlock a Workspace:

1. From the notification area, right-click on the MED-V icon.
2. From the popup menu, select **Unlock Workspace**.

   The **Unlock Workspace** dialog box appears.

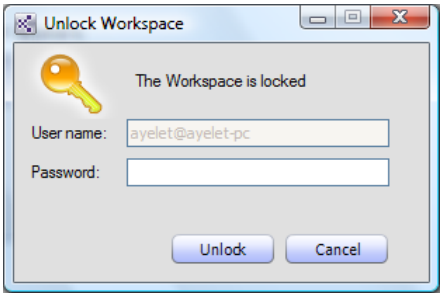


Figure 61: Unlock Workspace Dialog Box

3. Enter your **Password**.
4. Click **Unlock**.

   The Workspace is unlocked.

9.8. MED-V Client Tools

9.8.1. Diagnostics

The diagnostics tool provides all diagnostic information.

To view diagnostics:

1. From the notification area, right-click the MED-V icon.
2. From the popup menu select **Tools** and then **Diagnostics...**.
3. The Diagnostics tool appears.

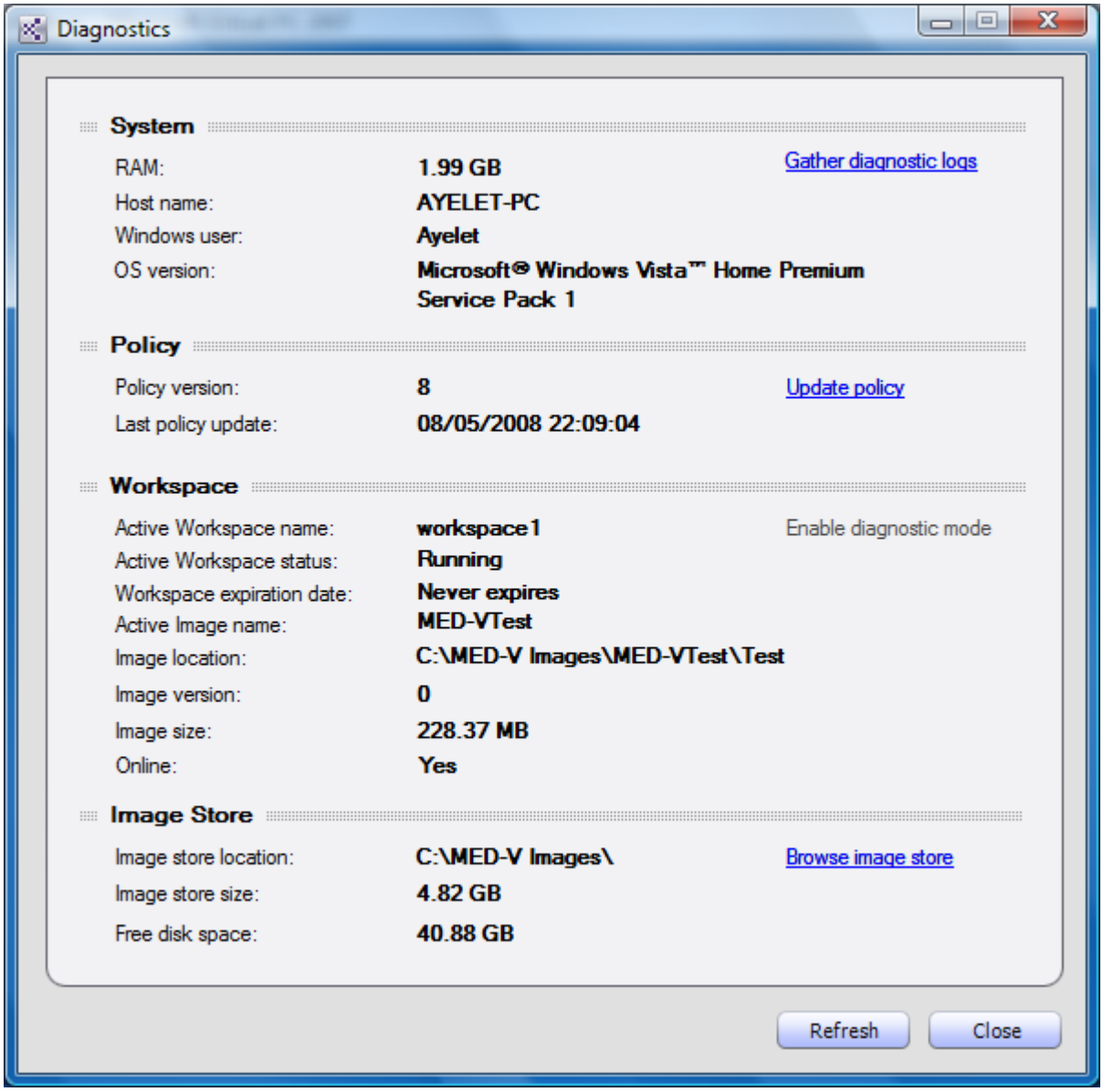


Figure 62: Diagnostics Tool

4. Review all diagnostic information.

The following functions can be performed using the diagnostic tool:

- Gather diagnostic logs - gathers the diagnostic logs and places them on the desktop.
- Update policy - The Workspace policy automatically connects to the MED-V server to refresh the policy every 15 minutes. However, a user may use this option to perform a manual refresh immediately.
- Enable/Disable diagnostic mode - When a Workspace is run in seamless integration mode, it may be difficult to diagnose a problem since you do not see the host or the host interacting with the Workspace. Therefore, you can optionally display the Workspace window, in which you view the entire screen; the host with the Virtual Machine inside. Additionally, this is useful in full desktop mode for viewing VM windows in the Start/Stop Workspace process.
- Browse image store - View all available Workspace images.

9.8.2. File Transfer Tool

The File Transfer Tool can be used to copy files or folders from the Workspace to the host and vice versa.

Note: The File Transfer Tool is only enabled when the Workspace is running.

To copy files or folders from a Workspace that is currently running:

1. From the notification area, right-click the MED-V icon.
2. From the popup menu select **Tools** and then **File Transfer...**.

   The **File Transfer** tool appears.

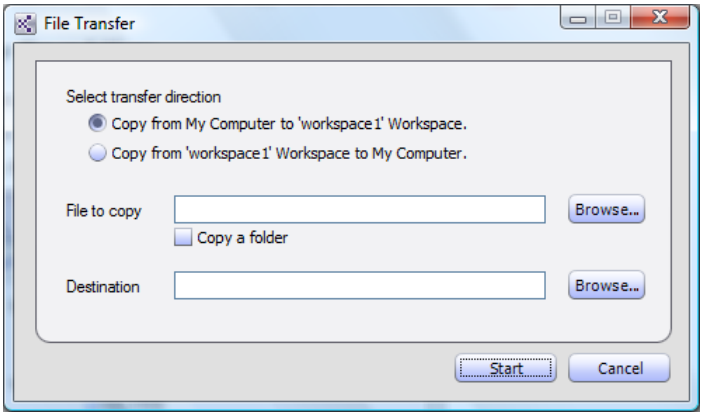


Figure 63: File Transfer Tool

3. In the **Select Transfer direction** field, select the type of transfer to be performed:
   - **Copy from My Computer to 'default workspace' Workspace** - transfer a file or folder from the host to the active Workspace.
   - **Copy from 'default workspace' Workspace to My Computer** - transfer a file or folder from the active Workspace to the host.
4. Select the file or folder you wish to copy by doing one of the following:
   - In the **File to copy** field, type the full path to the directory where the file or folder to copy is located.
   - Click **Browse...** to browse the directory where the file or folder to copy is located.
5. Select the **Copy a folder** check box, if you wish to copy an entire folder.
6. Select the destination to which the file is being transferred by doing one of the following:
   - In the **Destination** field, type the full path of the directory to which the file or folder will be transferred.
   - Click **Browse...** to browse to the directory to which the file or folder will be transferred.
7. Click **Start**.

   The file transfer begins.

9.8.3. Image Downloads

When a new image update is available for a Workspace and the Workspace is active, the user receives a message indicating that a new image is ready for download.

To view available images for download:

1. From the notification area, right-click on the MED-V icon.
2. From the popup menu select **Tools** and then **Image Downloads...**.

   All available image downloads are displayed.

9.9. Stopping a Workspace

To stop a Workspace:

1. From the notification area, right-click on the MED-V icon.
2. From the popup menu, click **Stop Workspace**.

   The Workspace is stopped.

9.10. Exiting MED-V Client

To exit MED-V Client:

1. From the notification area, right-click on the MED-V icon.
2. From the popup menu, select **Exit**.

   MED-V Client exits.

Chapter 10

10. Generating Reports

There are three types of reports that can be created by administrators in MED-V:

- Status - Use the status report to review the current status of all active users and all Workspaces of each user based on a defined period of time. This includes viewing machines that are currently connected to the server, or if they are not currently connected the date and time they were last connected to the server, the status of each machine and other relevant information.
- Activity Log - Use this report to review specific Workspace events in a defined date range.
- Error Log - Use this report to view specific Workspace errors in a defined date range.

The report results can be sorted by any column by clicking the appropriate column name.

The report results can be grouped by dragging a column header to the top of the report. Drag multiple column headers to group one column after another.

10.1. Generating a Status Report

To generate a status report:

1. Click on the **Reports** button.

   The Reports module appears.

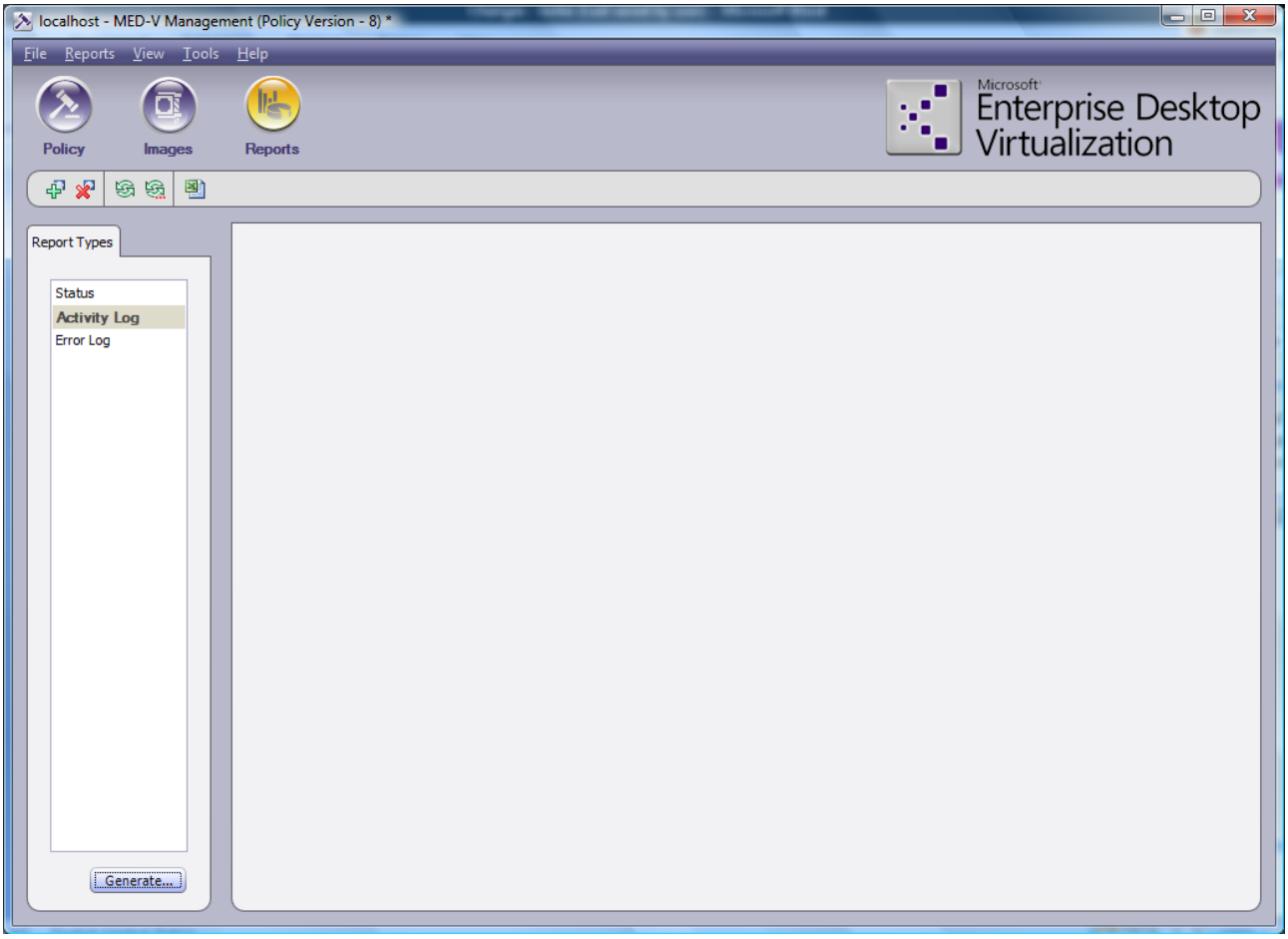


Figure 64: Reports Module

2. In the Report Types menu select **Status** and click **Generate**.

   The Report Parameters dialog box appears.

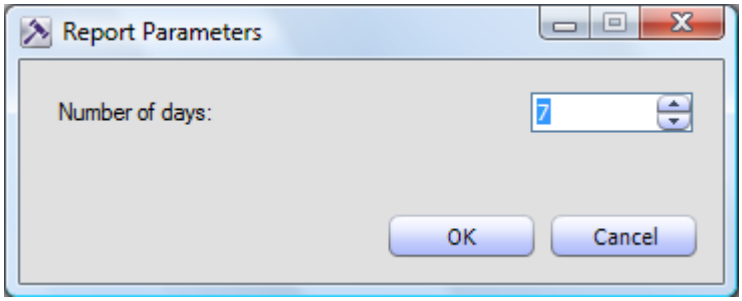


Figure 65: Report Parameters Dialog Box

3. In the **Number of days** field, enter a number or use the arrows to select the number of days to include in the status report.

   A status report is generated. The report parameters are defined in the following table.

Table 23: Client Workspace Properties

Property	Possible Values / Remarks
Time	The date and time the event occurred.

Property	Possible Values/Remarks
	Note: By default the events are displayed in descending date order. However, it can be changed by clicking the **Time Received** column.
User Name	The user who initiated the event. **Note:** If the event occurred before a user logged on, the username is SYSTEM.
Host name	The name of the host computer.
Workspace Name	The name of the Workspace.
Workspace Computer Name	The name of the computer the Workspace is running on.
Online	The current state of the client machine. • **Stopped** • **Started at <date and time the Workspace was started>**
Client Version	The version number of the client.
Policy Version	The policy version that the MED-V Workspace is currently using.
Image Name	The name of the image.
Image Version	The image version that the MED-V Workspace is currently using. **Note:** The Workspace version can be Unknown if it has not yet been downloaded onto a machine.

10.2. Generating an Activity Log Report

To generate an activity log report:

1. Click on the **Reports** button.

   The Reports module appears.

2. In the Report Types menu select **Activity Log** and click **Generate**.

   The Report Parameters dialog box appears.

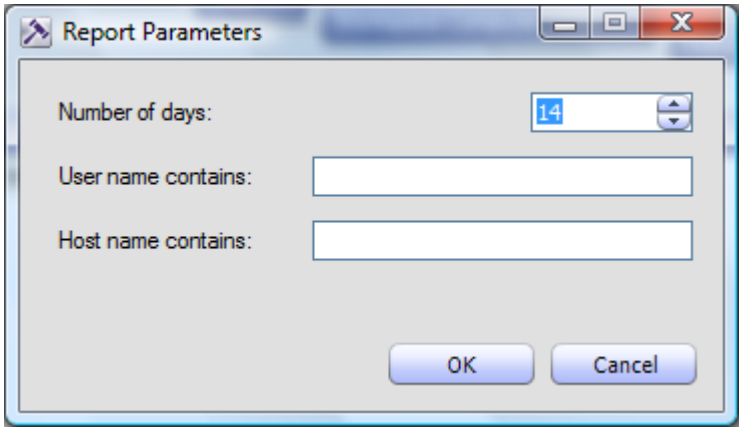


Figure 66: Report Parameters Dialog Box

3. In the Report Parameters dialog box, configure one or more of the following parameters:
   - **Number of days** - the number of days to display in the report.
   - **User name contains** - any event where the user name contains the text entered, is included in the report.
   - **Host name contains** - any event where the host name contains the text entered, is included in the report.

   A report is generated with the events and dates selected. The report parameters are defined in the following table.

Table 24: Activity Log Report Properties

Property	Possible Values/Remarks
Event ID	The event ID.
Severity	**Information**, **Error**, **Warning**
Category	The module that the report is referring to.
Description	A description of the event.
Time Received	The date and time the event was received on the server. **Note:** If the client is working offline the server receives the reports once the client is online. By default the events are displayed in descending date order. However, it can be changed by clicking the **Time Received** column.
Client Time	The date and time the event occurred according to the client clock.
Host name	The name of the host computer.
User Name	The user who initiated the event.
Workspace Name	The name of the Workspace.
Workspace Computer Name	The name of the computer the Workspace is running on.

10.3. Generating an Error Log Report

To generate an error log report:

1. Click on the **Reports** button.

   The Reports module appears.

2. In the Report Types menu select **Error Log** and click **Generate**.

   The Report Parameters dialog box appears.

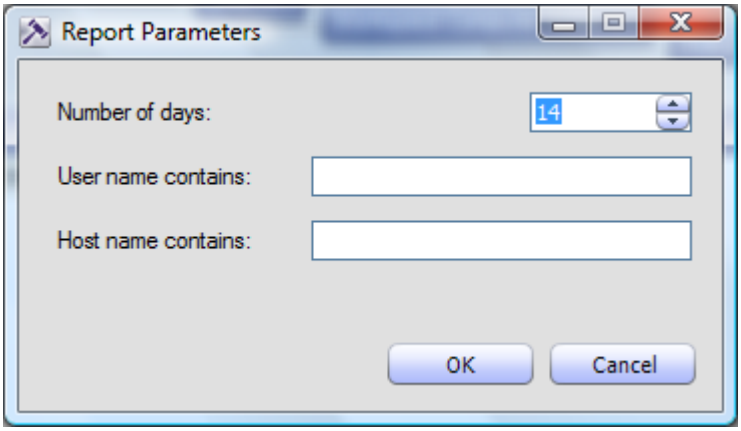


Figure 67: Report Parameters Dialog Box

3. In the Report Parameters dialog box, configure one or more of the following parameters:
   - **Number of days** - the number of days to display in the report.
   - **User name contains** - any event where the user name contains the text entered, is included in the report.
   - **Host name contains** - any event where the host name contains the text entered, is included in the report.

   A report is generated with the events and dates selected. The report parameters are defined in the following table.

Table 25: Activity Log Report Properties

Property	Possible Values/Remarks
Event ID	The event ID.
Category	The module that the report is referring to.
Description	A description of the event.
Time Received	The date and time the event was received on the server. **Note:** If the client is working offline the server receives the reports once the client is online. By default the events are displayed in descending date order. However, it can be changed by clicking the **Time Received** column.
Client Time	The date and time the event occurred according to the client clock.
Host name	The name of the host computer.

Property	Possible Values/Remarks
User Name	The user who initiated the event.
Workspace Name	The name of the Workspace.

10.4. Working with Reports

10.4.1. Refreshing a Report

To refresh an existing report:

1. Select the report you wish to refresh.
2. From the Management toolbar, click  .
   The report is regenerated.

10.4.2. Editing Report Parameters

To edit report parameters:

1. Generate a report.
2. From the Management toolbar, click  .
   The Report Parameters dialog box appears.
3. Configure the parameters and click **OK**.
   The report is regenerated with the new parameters.

10.4.3. Exporting a Report to Excel

To export a report to Excel:

1. Generate a report.
2. From the Management toolbar, click  .
   A Save Report dialog box appears.
3. Enter a name and click **Save**.
   The report is exported to Excel.

10.4.4. Closing a Report

To close a report:

1. Select the report you wish to close.
2. From the Management toolbar, click  .
   The report closes.

Chapter 11

11. Uninstalling MED-V

In This Chapter

11.1. Uninstalling MED-V Client

To uninstall MED-V in Windows XP:

1. If using Windows XP:
   - From the Control Panel, click **Add or Remove Programs**.
2. If using Vista:
   - From the Control Panel, click **Uninstall a Program**.
3. Select **Microsoft Enterprise Desktop Virtualization** and click **Uninstall**.
4. It is recommended to delete the MED-V Virtual Machine folder (default folder is `C:\MED-V Images`).

11.2. Uninstalling MED-V Server

To uninstall the MED-V Server:

1. From the Control Panel, click **Add or Remove Programs**.
2. Select **Microsoft Enterprise Desktop Virtualization (Server)** and click **Uninstall**.

Appendix A

A. Configuring Image Distributions Server

In This Appendix

An image repository is an optional server which is used for image distribution (where administrators upload new images; and client machines check the server every 15 minutes and update their image if a new one is available).

Note: The Image Repository is optional and this section is only relevant if an Image Repository will be used.

Installing Internet Information Services

If IIS is not currently installed on your server, perform the following procedure:

To install IIS on Windows Server 2008:

1. From the Windows Start menu, select **Administrative Tools > Server Manager**.

   The **Server Manager** window appears.

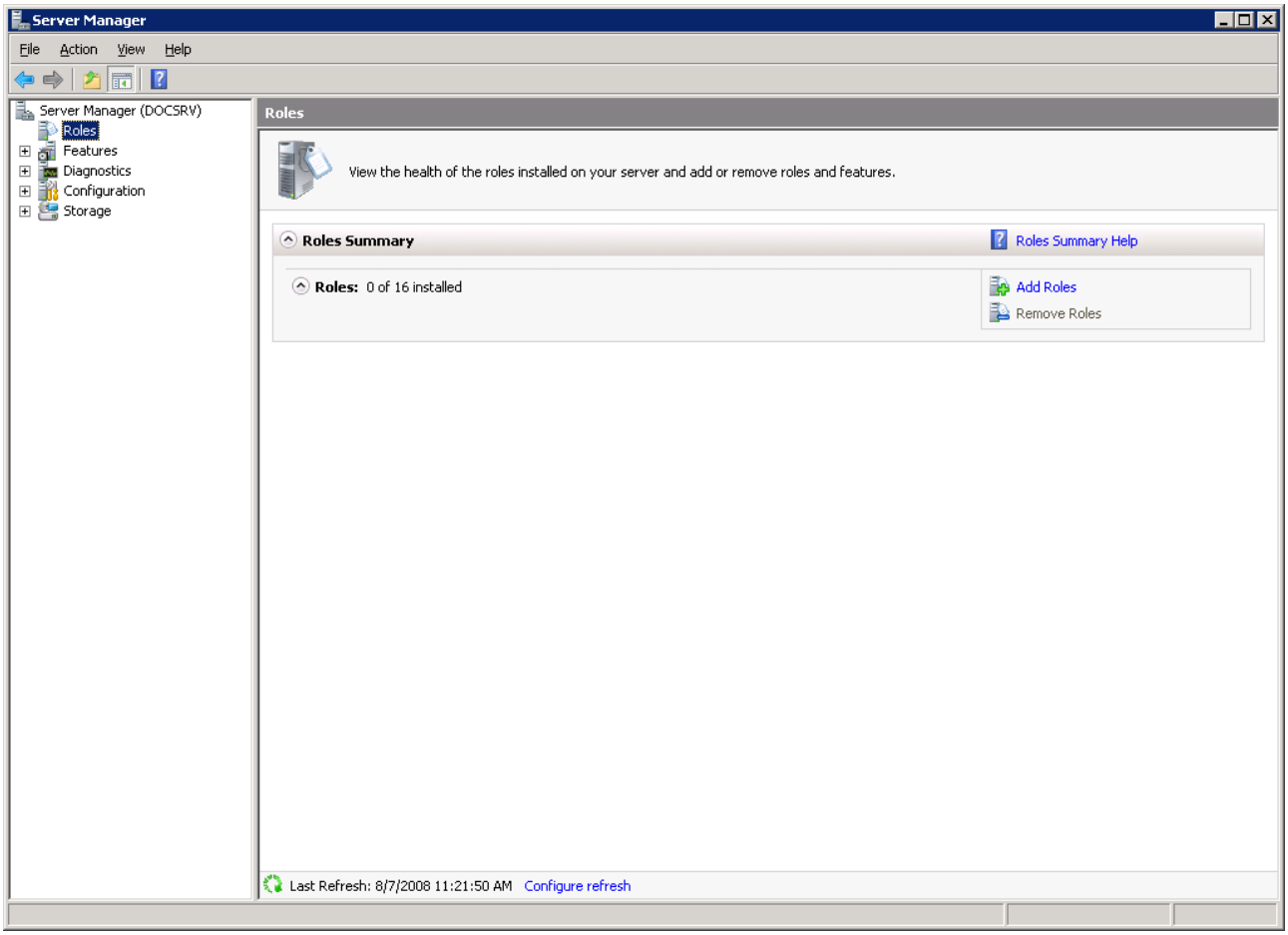


Figure 68: Server Manager Window

2. Click **Roles**. From the **Roles** window, click **Add Roles**.

   The **Add Roles Wizard - Before You Begin** dialog box appears.

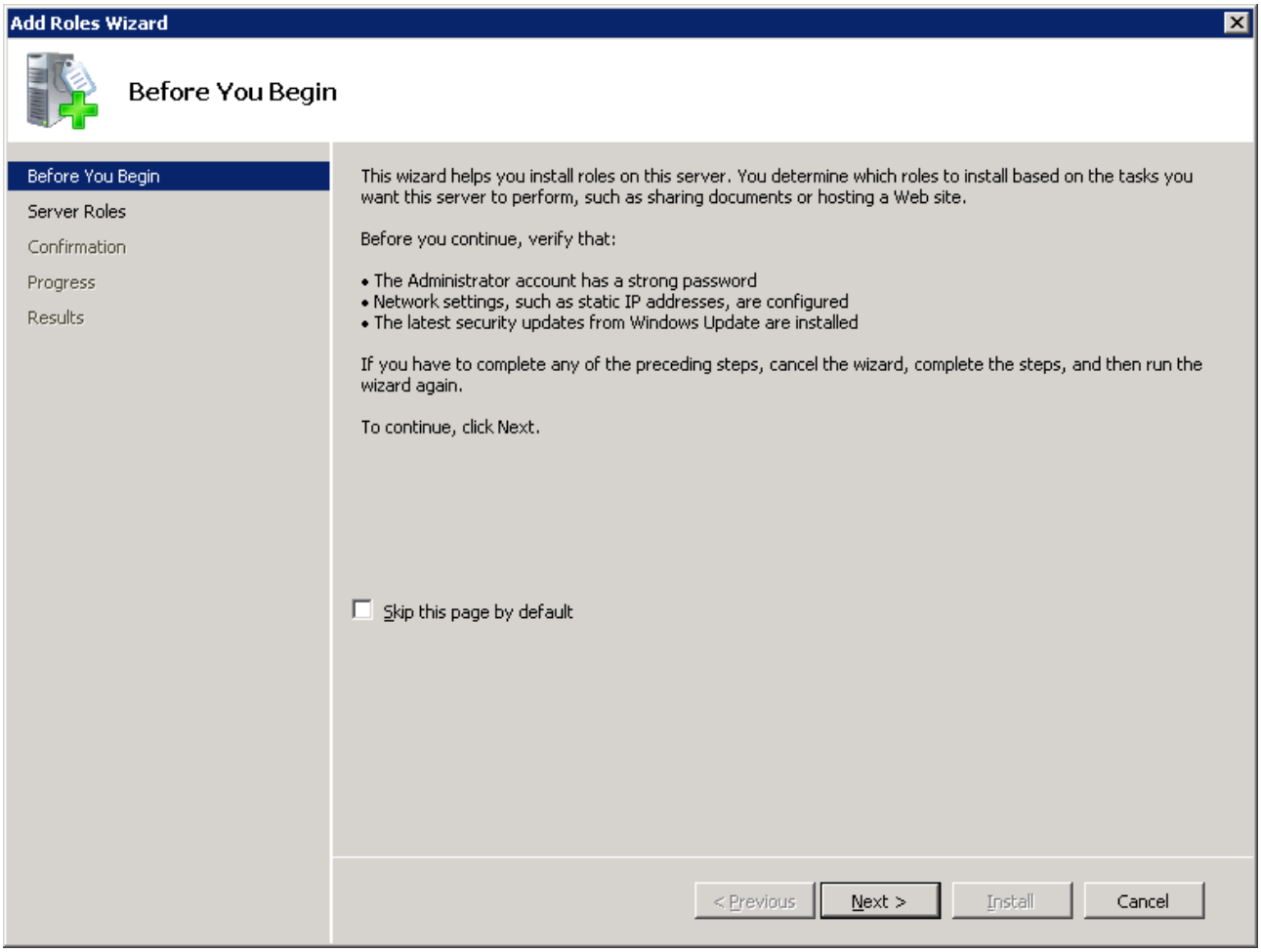


Figure 69: Add Roles Wizard - Before You Begin Dialog Box

3. Click **Next**.

   The **Add Roles Wizard - Select Server Roles** dialog box appears.

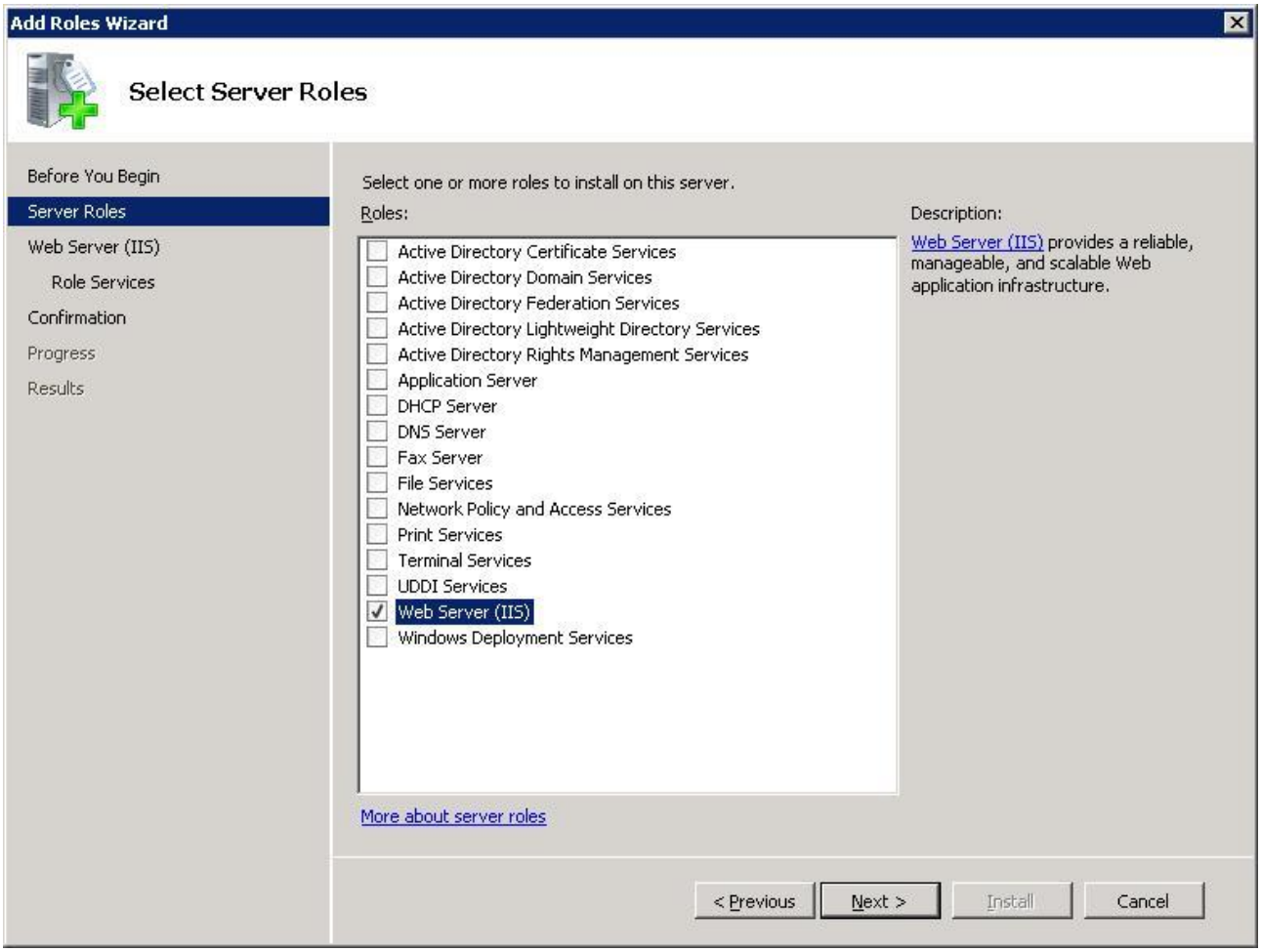


Figure 70: Add Roles Wizard - Select Server Roles Dialog Box

4. Click **Next**.

   The **Add Roles Wizard - Web Server (IIS)** dialog box appears.

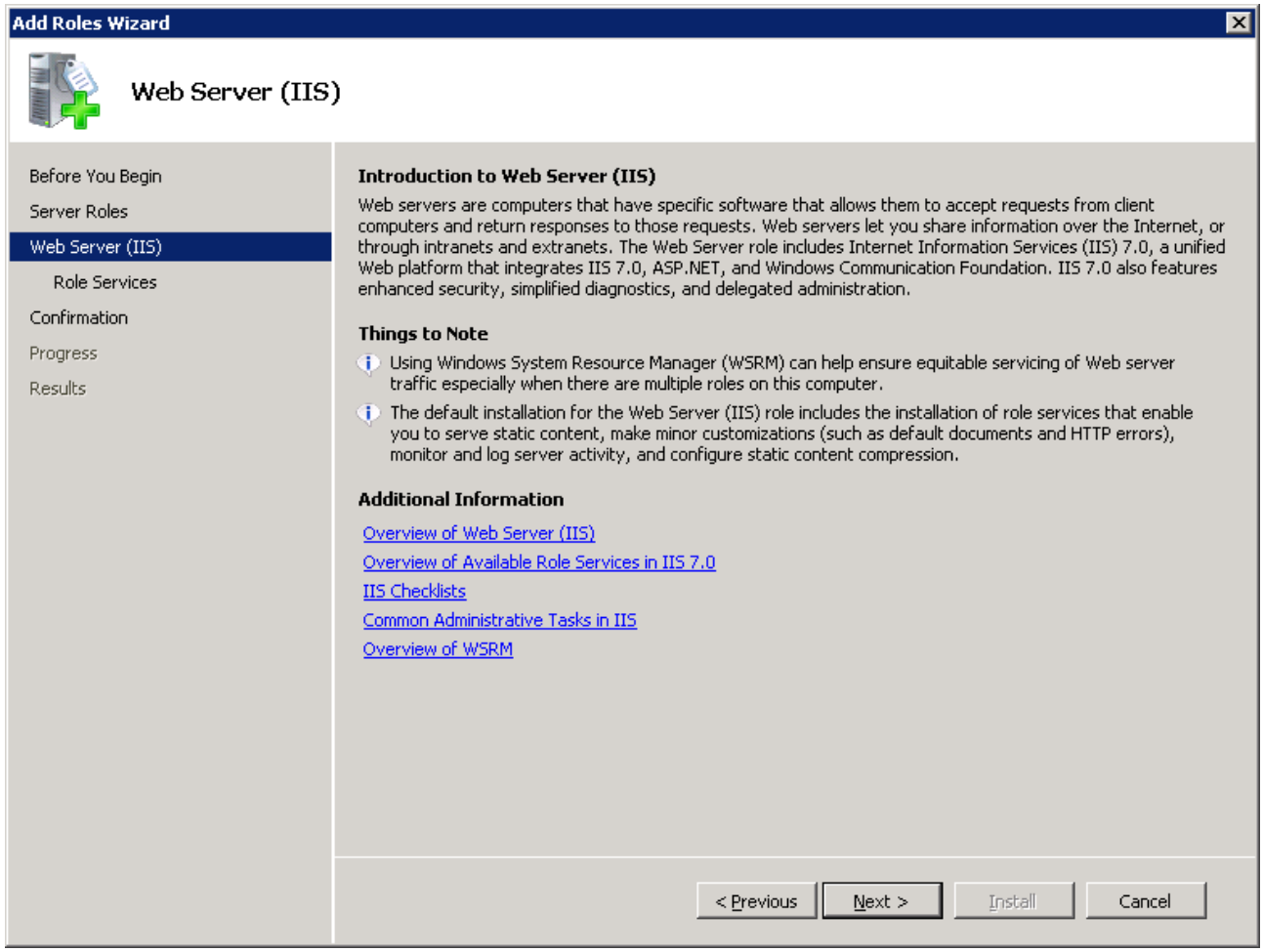


Figure 71: Add Rolls Wizard - Web Server (IIS) Dialog Box

5. Click **Next**.

   The **Add Roles Wizard - Select Role Services** dialog box appears.

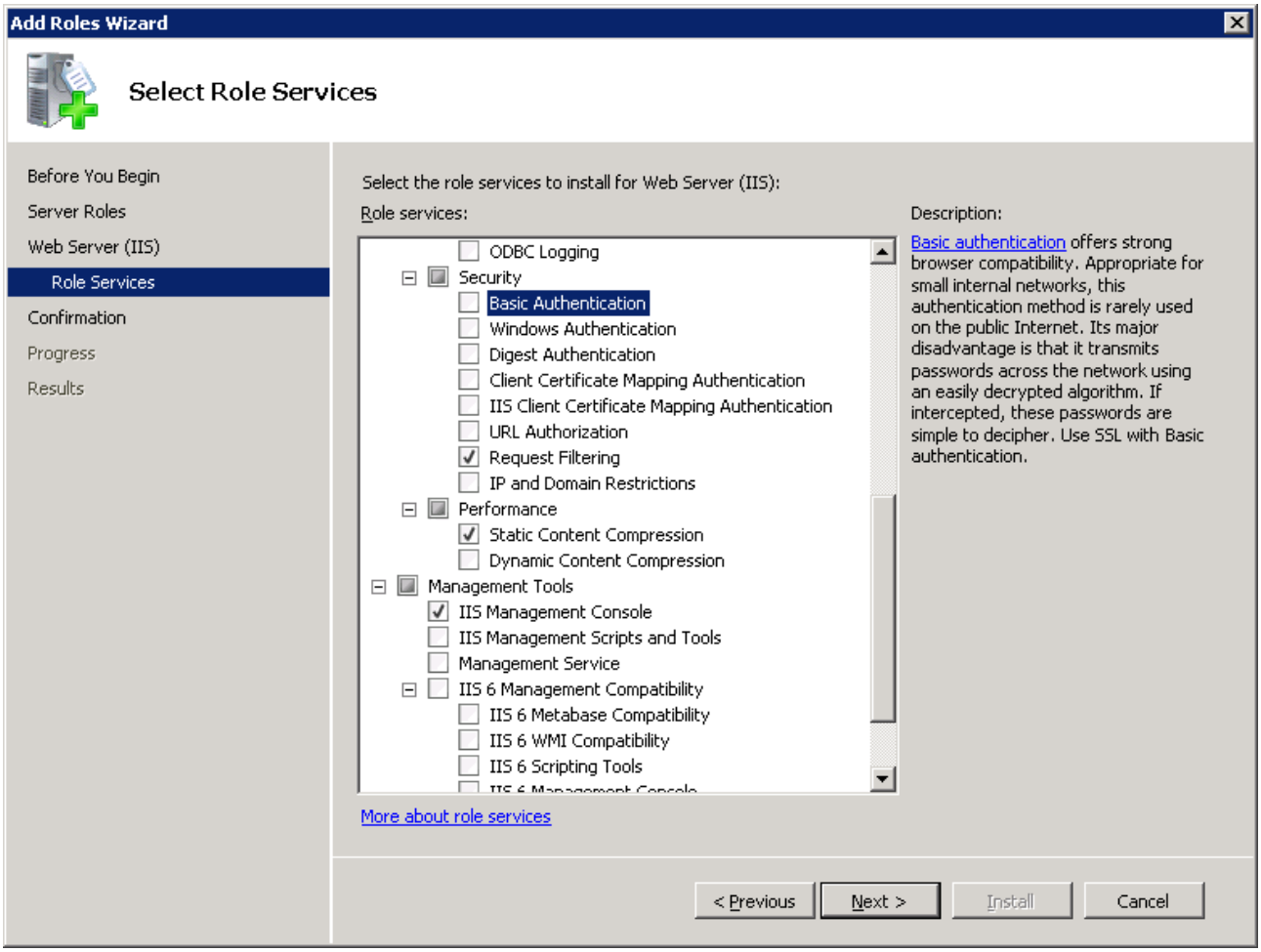


Figure 72: Add Roles Wizard - Select Role Services

6. Select the following supported authentication methods:
   - **Basic Authentication**
   - **Windows Authentication**
   - **Client Certificate Mapping Authentication**
7. Click **Next**.

   The **Add Roles Wizard - Confirm Installation Selections** dialog box appears. It lists the options you have already selected.

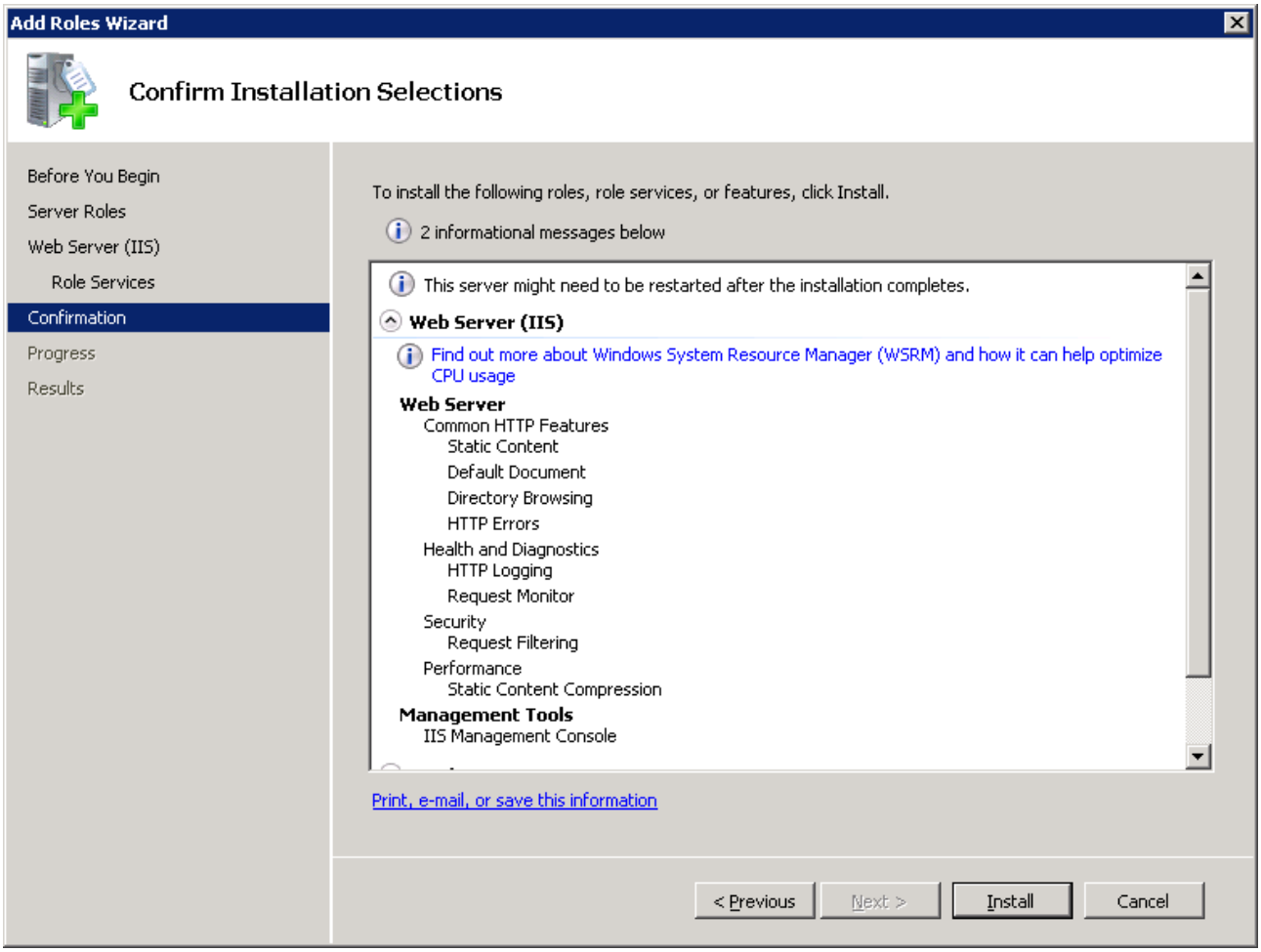


Figure 73: Add Roles Wizard - Confirm Installation Selections Dialog Box

8. If you are not satisfied with the information listed in the Confirm Installation Selections dialog box, do either of the following:
   - To return to a previous screen and change the selections, click **Previous**.

     or
   - To quit the wizard, click **Cancel**.
9. To continue with the installation, click **Install**.

   IIS installation starts. This can take several minutes, and the screen may not display text. During installation, several progress screens appear. If an error message appears, follow the instructions provided.

   Upon successful installation, the **Installation Results** dialog box appears.
10. Click **Close** to quit the wizard.

Adding BITS Server Extensions to IIS

To add BITS server extensions to IIS:

1. From the Windows Start menu, select **Administrative Tools > Server Manager**.

The **Server Manager** window appears.

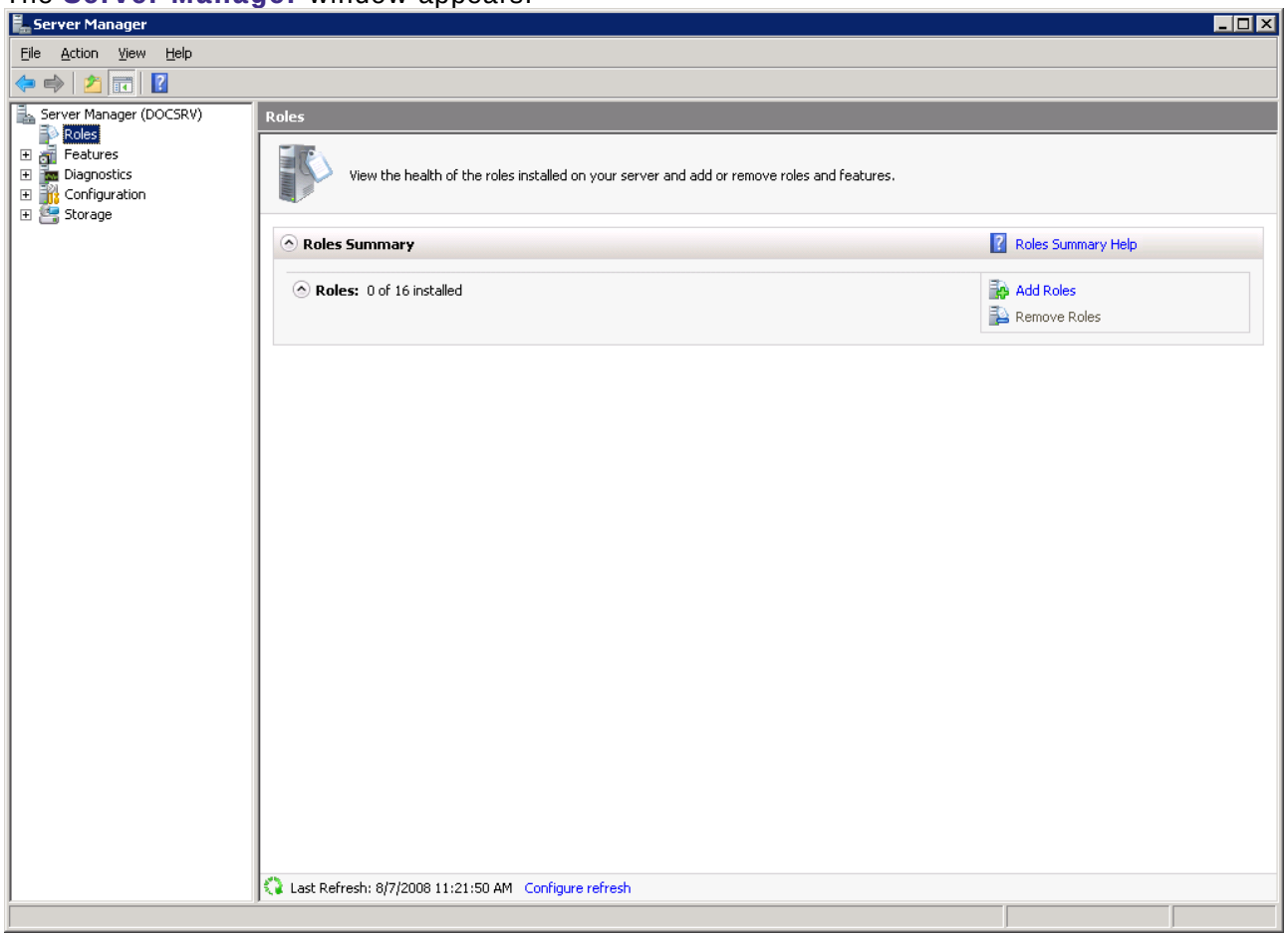


Figure 74 Server Manager Window

2. Click **Features**.

   The **Add Features Wizard - Select Features** dialog box appears.

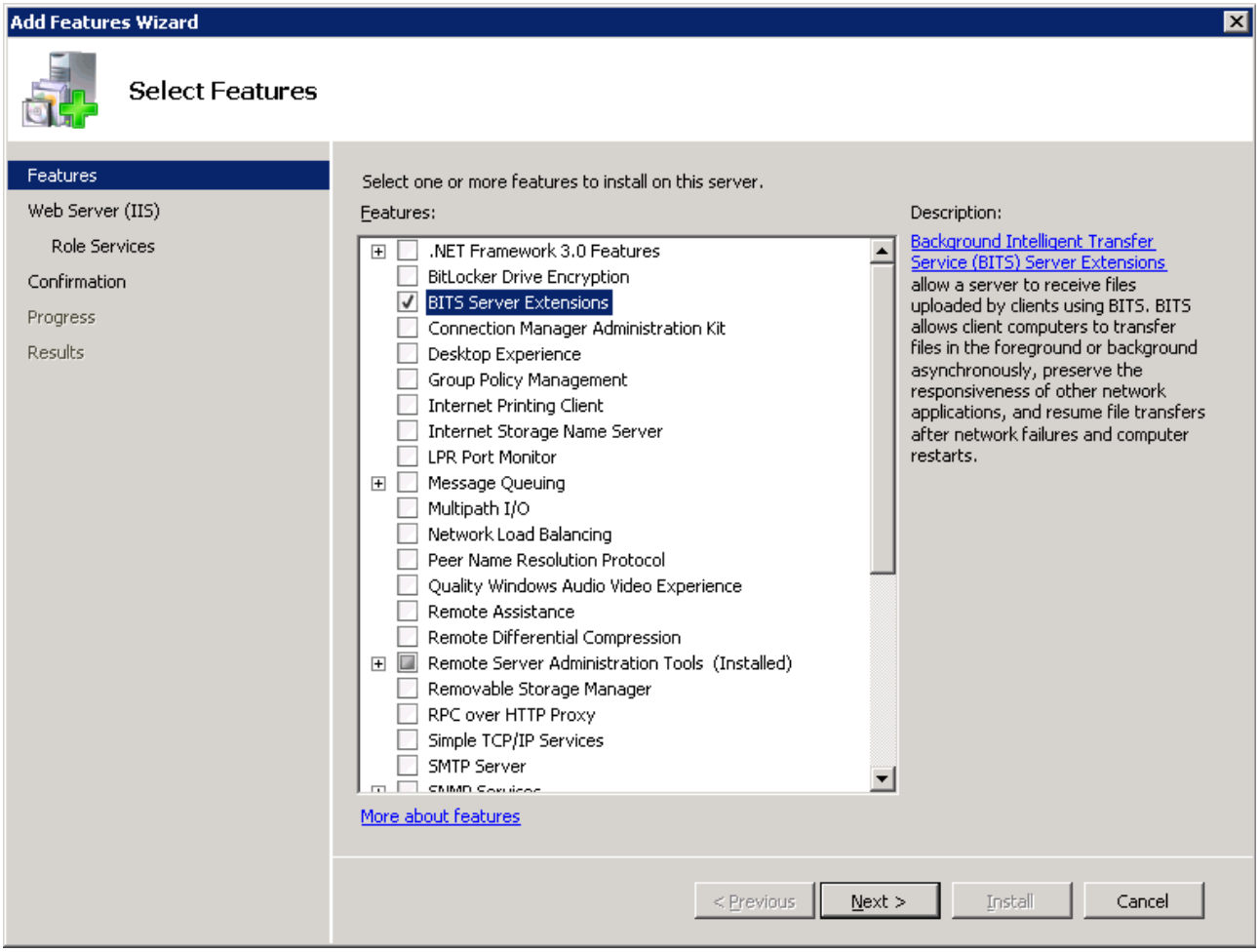


Figure 75: Add Features Wizard - Select Features Dialog Box

3. Select **BITS Server Extensions** and follow the wizard to completion.

Configuring Internet Information Services (IIS)

To configure Internet Information Services:

1. Start the **Internet Information Services (IIS) Manager**.

   The **Internet Information Services (IIS) Manager** appears.

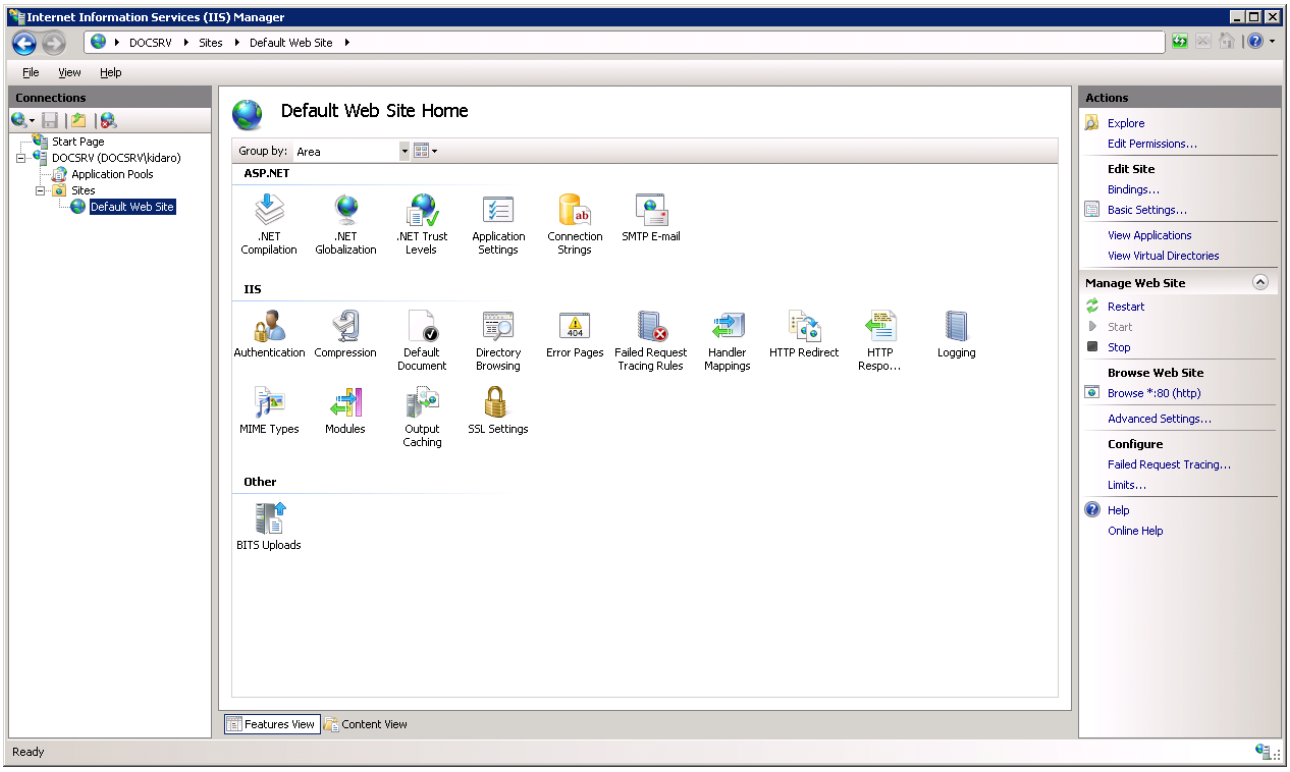


Figure 76: Internet Information Services (IIS) Manager

2. Right-click **Default Web Sites** and from the popup menu, click **Add Virtual Directory**.

   The **Add Virtual Directory** dialog box appears.

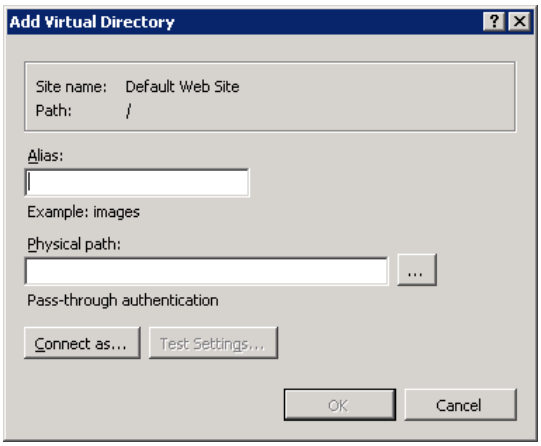


Figure 77: Add Virtual Directory Dialog Box

3. In the **Alias** box, type **MEDVImages**.
4. In the **Physical path** box, type `C:\MED-V Server Images`.Note that you must create this folder first.
5. Click **OK**.
6. From the **Internet Information Services (IIS) Manager**, double-click **BITS Uploads**.

   The **BITS Uploads** window appears.

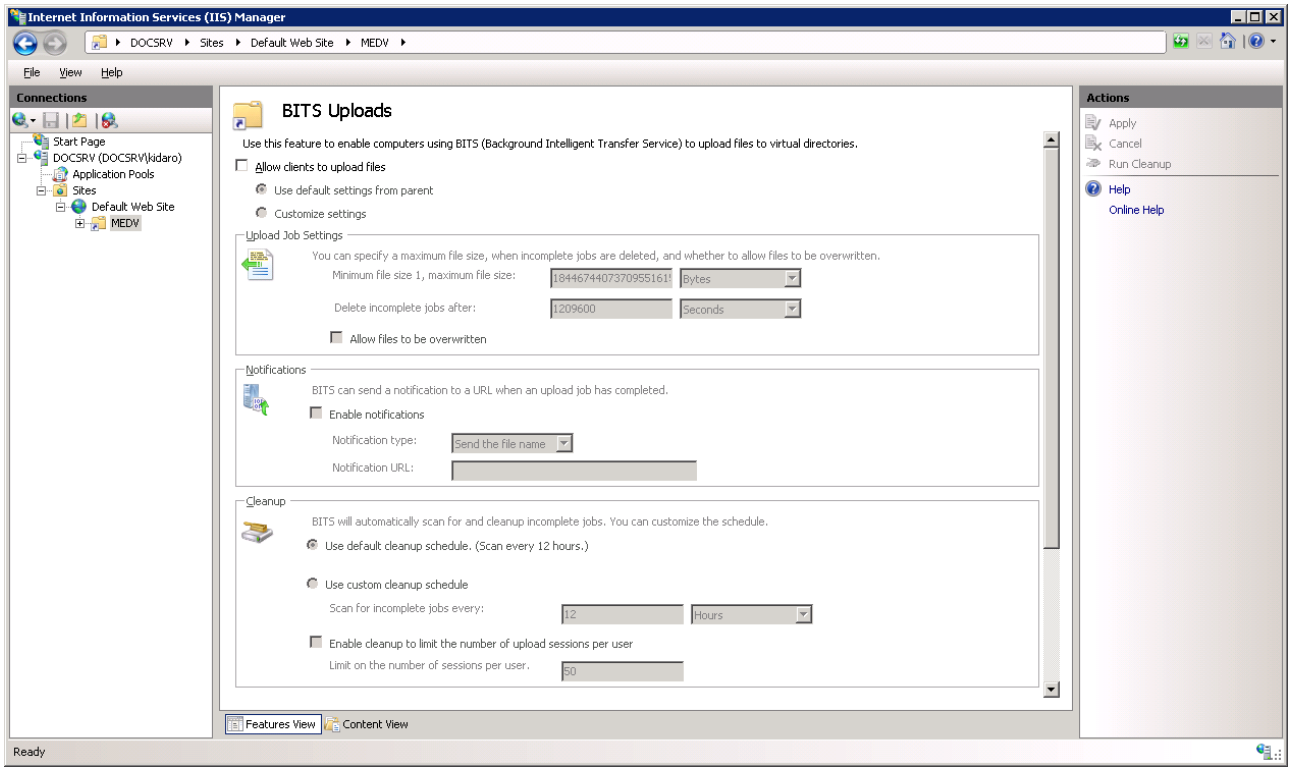


Figure 78: BITS Uploads Window

7. Select the **Allow clients to upload files** check box and click **Apply**.
8. From the **Internet Information Services (IIS) Manager**, click **MIME Types**.

   The **MIME Types** window appears.

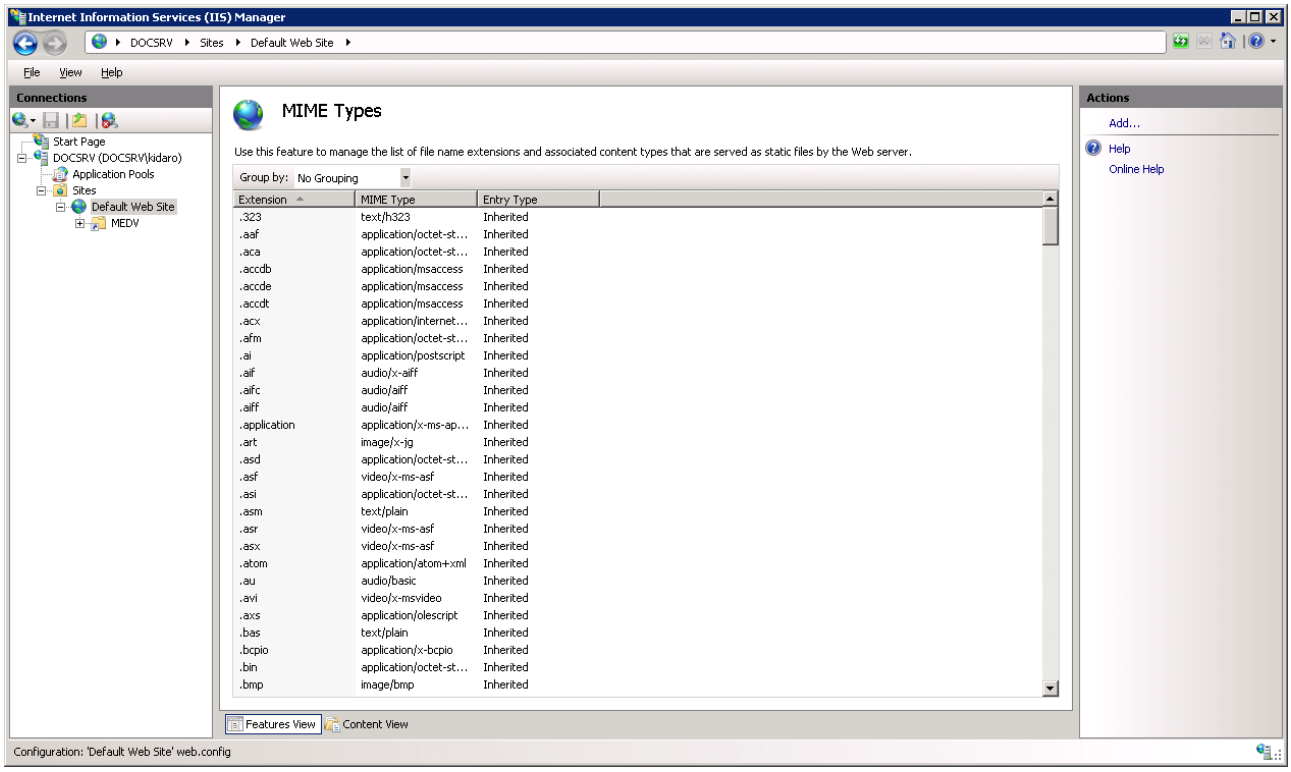


Figure 79: MIME Types Window

9. Add the following MIME types:

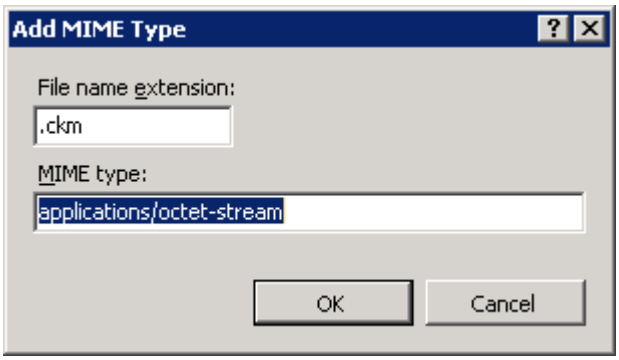


Figure 80: Add MIME Type Dialog Box

- .ckm (application/octet-stream)
- .index (application/octet-stream)

10. From the **Internet Information Services (IIS) Manager**, click **Edit Permissions**.
11. On the MED-V site, select **Security** and **Add read permissions to Everyone**.
12. Restart the IIS Service.

Note: Make sure that the relevant firewall ports are open.

Appendix B

B. Configuring MED-V to Work from Inside a Network or Remotely

To configure MED-V to work from inside a network:

1. Configure a MED-V server and image distribution inside the network.

To configure MED-V to work remotely:

1. Configure a MED-V server and an image distribution server that are accessible from the Internet.
2. If needed, configure a DMZ reverse proxy.
3. Set the authentication method, as described below, in the `ClientSettings.xml` file which can be found in the **Servers\Configuration Server** folder.

To configure MED-V to work both from inside a network and remotely:

1. Configure a MED-V server and image distribution server inside the network.
2. Ensure that the servers are accessible from the Internet.
3. Configure the DNS resolution so that when the client attempts to connect to a server, it automatically connects to the correct server (within the network or over the Internet) based on the client location.
4. If needed, configure a DMZ reverse proxy.
5. Set the authentication method, as described below, in the `ClientSettings.xml` file which can be found in the **Servers\Configuration Server** folder.

When applying new settings, the service must be restarted.

- You can change the IIS authentication scheme to one of the following: BASIC, DIGEST, NTLM, NEGOTIATE. The default is NEGOTIATE, and uses the following entry:

```
<ImageDistribution>
<!-- The authentication used for image download. Basic and digest
authentication should be used only under SSL.-->
   <!-- The line below can be one of the followings: -->
   <!--BG_AUTH_SCHEME>BG_AUTH_SCHEME_BASIC</BG_AUTH_SCHEME-->
   <!--BG_AUTH_SCHEME>BG_AUTH_SCHEME_DIGEST</BG_AUTH_SCHEME-->
   <!--BG_AUTH_SCHEME>BG_AUTH_SCHEME_NTLM</BG_AUTH_SCHEME-->
   <!--BG_AUTH_SCHEME>BG_AUTH_SCHEME_NEGOTIATE</BG_AUTH_SCHEME-->
   <Authentication type="Kidaro.Foundation.Bits.BG_AUTH_SCHEME">
         <BG_AUTH_SCHEME>BG_AUTH_SCHEME_NEGOTIATE</BG_AUTH_SCHEME>
```

```
      </Authentication>
   </ImageDistribution>
```

Appendix C

C. MED-V Trim Transfer™ Technology

MED-V's advanced Trim Transfer de-duplication technology accelerates the download of initial and updated Virtual Machine images over the LAN or WAN, thereby reducing the network bandwidth needed to transport a Workspace Virtual Machine to multiple end-users.

This breakthrough technology uses existing local data to build the Virtual Machine image, leveraging the fact that in many cases, much of the Virtual Machine (e.g., system and application files) already exists on the end-user's disk. For example, if a Virtual Machine containing Microsoft Windows XP is delivered to a client running a local copy of Windows XP, MED-V will automatically remove the redundant Windows XP elements from the transfer. To ensure a valid and functional Workspace, the MED-V Client cryptographically verifies the integrity of local data before it is utilized, guaranteeing that the local blocks of data are absolutely bit-by-bit identical to those in the desired Virtual Machine image. Blocks that do not match are not used.

The process is bandwidth efficient and transparent, and transfers run in the background, utilizing unused network and CPU resources.

When updating to a new image version (e.g., when administrators want to distribute a new application or patch), only the elements that have changed ("deltas") are downloaded, and not the entire Virtual Machine, significantly reducing the required network bandwidth and delivery time.

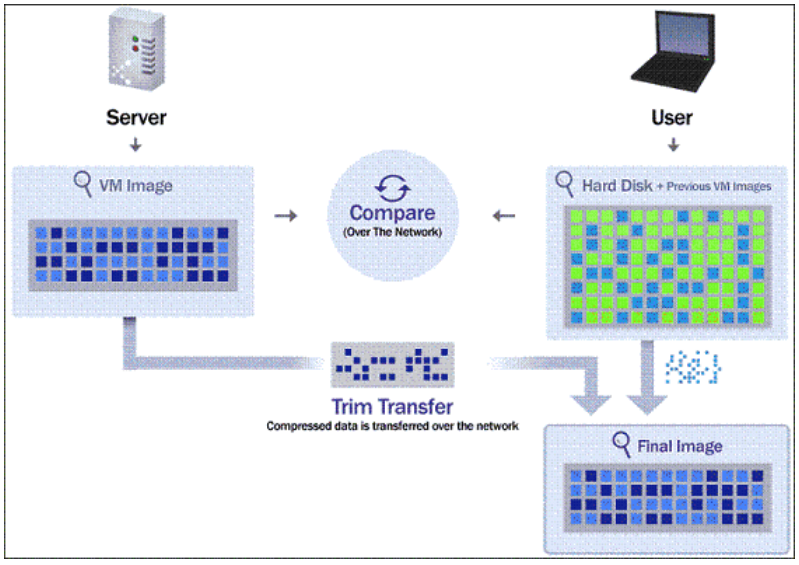


Figure 81: MED-V Trim Transfer™ Technology

You can configure which folders are indexed on the host as part of the Trim Transfer protocol according to the host OS. These setting are configured in the `ClientSettings.xml` file which can be found in the **`Servers\Configuration Server\`** folder.

When applying new settings, the service must be restarted.

```
<HostIndexingXP type="System.String[]">
- <ArrayOfString>
<string>%WINDIR%</string>
<string>%ProgramFiles%\Common Files</string>
<string>%ProgramFiles%\Internet Explorer</string>
<string>%ProgramFiles%\MED-V</string>
<string>%ProgramFiles%\Microsoft Office</string>
<string>%ProgramFiles%\Windows NT</string>
<string>%ProgramFiles%\Messenger</string>
<string>%ProgramFiles%\Adobe</string>
<string>%ProgramFiles%\Outlook Express</string>
</ArrayOfString>
</HostIndexingXP>
- <HostIndexingVista type="System.String[]">
- <ArrayOfString>
<string>%WINDIR%\MSAgent</string>
<string>%WINDIR%\winsxs</string>
<string>%WINDIR%\system</string>
<string>%WINDIR%\system32</string>
<string>%WINDIR%\Microsoft.NET</string>
<string>%WINDIR%\SoftwareDistribution</string>
<string>%WINDIR%\L2Schemas</string>
<string>%WINDIR%\Cursors</string>
<string>%WINDIR%\Boot</string>
<string>%WINDIR%\Help</string>
<string>%WINDIR%\assembly</string>
<string>%WINDIR%\inf</string>
<string>%WINDIR%\fonts</string>
<string>%WINDIR%\Installer</string>
<string>%WINDIR%\IME</string>
<string>%WINDIR%\Resources</string>
<string>%WINDIR%\servicing</string>
<string>%ProgramFiles%\MED-V</string>
<string>%ProgramFiles%\Microsoft Office</string>
</ArrayOfString>
</HostIndexingVista>
```

Glossary

D

Domain

A subnetwork in a LAN, made up of a group of clients and servers under the control of one security database.

G

Guest

The operating system installed in a virtual machine.

H

Host

The operating system instance that is installed on the end user physical device.

I

Image

The virtual machine image file used by Workspaces.

P

Policy

The set of rules, configurations and permissions that define the behavior of MED-V Workspace.

Published Applications

Applications installed on the virtual machine image which are accessible through the Workspace.

V

Virtual image

A file that represents the file system of a virtual machine, and can be delivered to various endpoints independently of their hardware or software.

Virtual PC/Machine

Another instance of an operating system that is running concurrently with the host on the same physical device using virtualization software (e.g., Microsoft Virtual PC).

W

Windows Frame Color

The color given to frames and icon backgrounds of windows, which are running from a Workspace.

Workspace

A set of rules, configurations and permissions which define a secure environment for a specific user or users.

Index

L

M

N

O

P

R

S

T

U

V

W