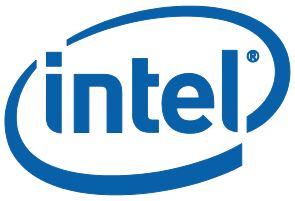

Intel® vPro™ Technology Solution Reference Design

Instant Back to Work

Revision 2.0

November 2011

Document number: 1110

Revision History

Revision	Revision History	Date
1.0	Initial release	September 2011
2.0	Updated to show a test virus, map to a drive and transfer files in the background; also improved KVM support.	November 2011

Contents

Figures

1 Preface

Sometimes a user just can't wait while a virus scan and repair is going on to read important emails. With this solution, a help desk technician can be remotely running a virus scan on a user's Intel® vPro™ technology based PC while the user is reading email on that PC in an Outlook Web Access window. Even if the user's OS is down due to a crippling virus.

This solution boots a lightweight ISO that runs Mozilla Firefox Portable, a web browser, to allow the user to manage their email. Meanwhile, the help desk technician can remotely connect to the PC and run a virus scan on the user's hard drive and even attempt repairs, all while the user has access to their email instead of wasting valuable time.

1.1 Document Scope

This document covers installing required components, using the included ISO Builder utility, and key Intel vPro technology features to remotely deliver the OWA with Virus Scan solution.

1.2 Intended Audience

This document is intended for Information Technology (IT) professionals who create OS images and understand how to manage Intel vPro technology based systems. Readers should have a good working familiarity with Intel vPro technology, OS image creation, and the configuration and use of the Intel® Active Management Technology (Intel® AMT) platform for out-of-band (OOB) management. Readers should also be familiar with the basics of IT infrastructure, especially networked environments and their component technologies.

1.3 Related Documentation and Software

The download site for this and all Use Case Reference Designs:

http://communities.intel.com/docs/DOC-4080

Remote ISO Launcher v1.0

http://communities.intel.com/docs/DOC-5943

Two Stage Boot Process

http://communities.intel.com/docs/DOC-5552

2 Introduction

This document provides instructions on performing a remote virus scan using the ISO Builder utility, the Remote ISO Launcher utility, and Intel vPro technology features. It begins with a high level overview of the process. Next, step-by-step instructions are provided which, if followed exactly, will accomplish this. These step-by-step instructions are designed for use in a lab or test setting and should be adapted and validated to fit with a particular IT deployment.

2.1 Scenario Overview

In this solution a Knowledge Worker has contacted a Service Desk Technician for help with an issue. In troubleshooting the issue, the Technician has determined that the worker's PC may be infected with a virus. Here is where the solution starts.

1. The Technician establishes a connection to the Worker's Intel vPro technology enabled PC (the "managed" PC).
2. A reboot command is issued, causing the managed PC to reboot to a preconfigured ISO image.
3. This image launches Firefox Portable and points to the Worker's web-based email server, allowing the user to access their email or other web based applications.
4. The Technician then remotely runs a virus scan on the Worker's PC and can attempt repairs as well.
5. The Technician can also map a network drive from the Worker's PC to access more tools or to help in repairs.

2.1.1 Network Share for Bootable Image Storage and Delivery

To facilitate the remote reboot of the managed PC, the image is stored on a network location. This location must be accessible from the managed PC. This document outlines creating the share on the Help Desk Console PC. While this location is appropriate for lab scenarios, in a production environment it is best to place the image on the network edge, as close to the managed PC as possible. This may be accomplished by a Distributed File system, or other means. However, placing the image at the network edge is not covered by this document.

NOTE

Another consideration is security. Credentials used by the recovery OS to access this share may be compromised if a user gains access to the recovery. As such, it is recommended to limit the attack surface by creating a special account that has read only access to this share and no others. This way, if the account is compromised, the only files exposed are those on this share.

2.2 Use Case Preparation

Pre-work for this use case includes the following:

1. Create a network share on which to store the bootable image. You will need to create a share drive, a username, and password. This information will be needed in section 3.3.
2. Provide Service Desk Technicians with the tools and training needed to perform the use case. This use case outlines using RealVNC VNC* Viewer Plus and Remote ISO Launcher as the Service Desk tools. Other tools may be used. However, they are beyond the scope of this document.

2.3 Assumptions and Limitations

The detailed steps in this document have the following assumptions

1. All managed systems support KVM Remote Control for optimal control but is not essential for this use case.
2. Intel AMT is set up and configured on the managed systems.
3. The Service Desk Technician has valid Intel AMT credentials needed to access and use IDE Redirection, Serial Over LAN, Remote Control, and KVM Remote Control features.
4. Wired only network connections for the managed system are supported at this time.
5. For Virus Scan to function a non-encrypted hard drive is needed on the managed system. Web Access is not limited by an encrypted hard drive.

2.4 Requirements

Network with DHCP Server	
Development Computer	• Any PC with Microsoft* Windows 7. Used to create the bootable image. For the purpose of the lab, this PC may also be used as the Service Desk Console.
Service Desk Console	• Any PC with Microsoft Windows 7. • Microsoft .NET 4.0 must be installed (required for Remote ISO Launcher application) PC used by the Service Desk technician to remotely control the Knowledge Workers PC in the use case.
Managed Client with Intel vPro technology	• Intel AMT 6.0 or higher for KVM support or Intel AMT 3.0 and higher for SOL support. • Intel Integrated Graphics • Configured for non-TLS, TLS, and Digest credentials. This PC will be scanned for a virus while its user is running OWA during this use case. **Note**: Kerberos credentials are supported but not shown in this document.

3 Preparation and Detailed Steps

This section contains detailed instructions for implementing this solution.

3.1 Set Up ISO Builder

ISO Builder is an application that allows you to create customized bootable image files. Follow the steps below to download, install, and set up ISO Builder, which you will use to create a customized image file in subsequent sections of this document.

3.1.1 Download Required ISO Builder Components

On the Development PC, download the following:

ISO Builder:

http://communities.intel.com/docs/DOC-18972

Extract the ISO_Builder folder to **c:\ISO_builder**.

Note: Create this folder first since subsequent downloads rely on this folder already being in place.

WAIK for Windows 7 Supplement English:

http://www.microsoft.com/download/en/details.aspx?id=5188

Save to: **C:\iso_builder\src\waik_supplement_en-us.iso**

ISO Builder MEI Driver Pack:

http://communities.intel.com/docs/DOC-18972

Save to **C:\iso_builder\src\iso_builder_MEI_drivers.zip**.

ISO Builder LAN Driver Pack:

http://communities.intel.com/docs/DOC-18972

Save to **C:\iso_builder\src\iso_builder_LAN_drivers.zip**.

Two stage boot (used for speeding up the remote boot):

http://communities.intel.com/docs/DOC-5552

Extract the files. Create an **ifast** folder in the **c:\iso_builder\apps\ directory**. Copy the contents of isobuilder folder from the extracted files to the **ifast** folder that you just created.

Outlook Web Access with Virus Scan files

Included with the document is an **OWA_w_Virus_Scan** folder. Copy its contents to **c:\iso_builder\apps\OWA_w_Virus_Scan**.

Available at http://communities.intel.com/docs/DOC-19012

3.1.2 Configure ISO Builder Required Components

You are now ready to run ISO Builder and configure it. Follow instructions below:

1. On the Development PC, launch **iso_builder.vbs**. If prompted, click **Yes** to the User Access Control Message. The following screen is displayed:

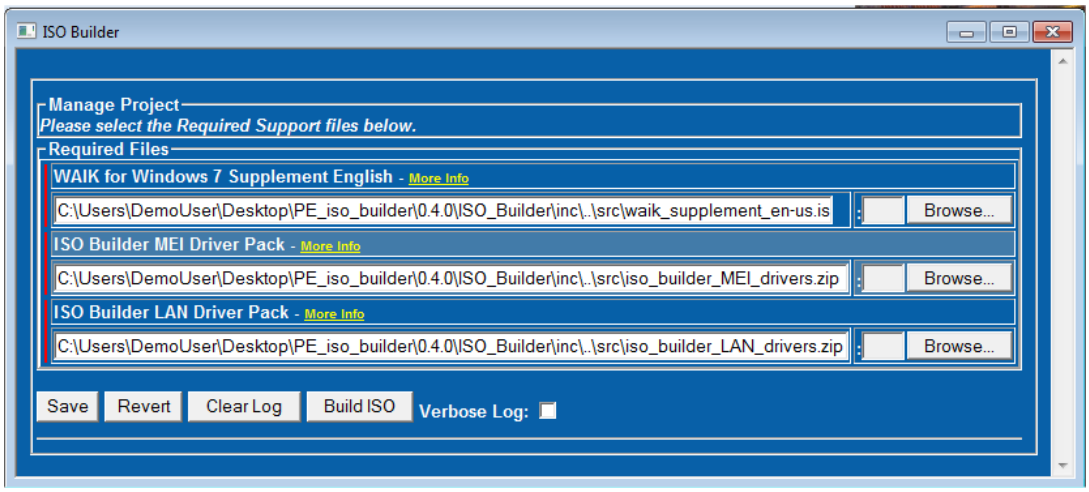

Figure 1: Main ISO Builder Screen

2. If any of the required files are shown with a red line to the left, they cannot be found. Click **Browse** next to each red-lined required file and browse to the location where you placed it in section 3.1.1 above.

3. Once all files are located, more settings options appear, as shown in Figure 2.

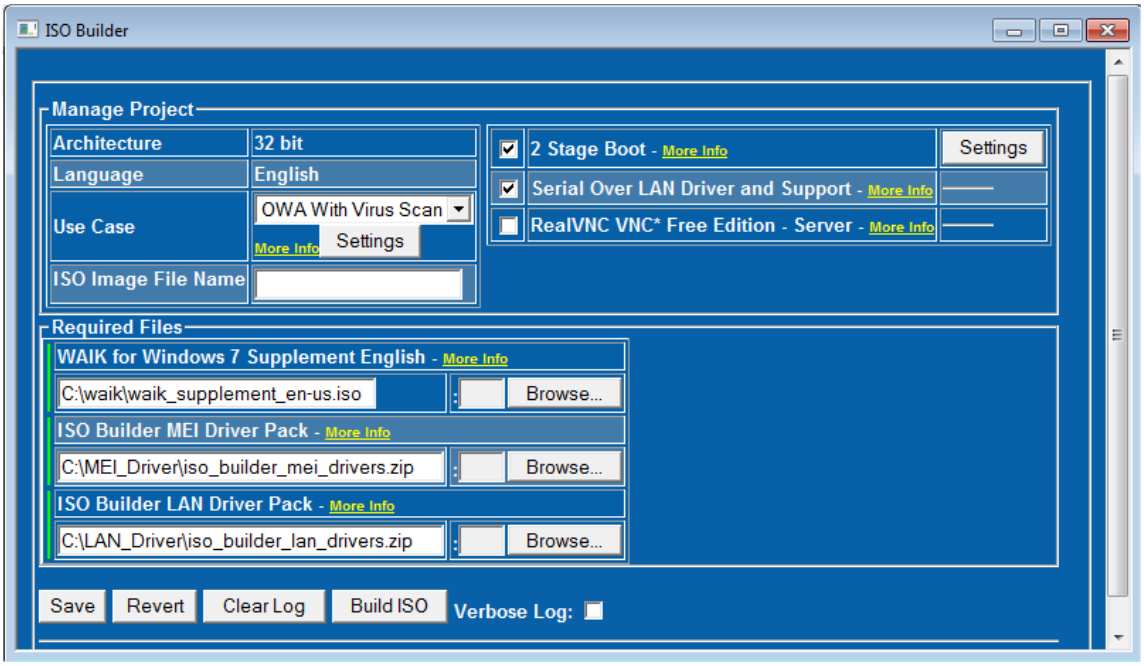

Figure 2: New Settings Displayed

4. Leave **Serial Over LAN Driver and Support** selected.
5. Leave **RealVNC VNC Free Edition** unselected.
6. Proceed to the next section.

3.2 Configure ISO Builder for OWA with Virus Scan

Once the ISO Builder has been set up for general use, it must be configured to work with the OWA with Virus Scan application.

3.2.1 Download and Install Required Components

To setup OWAwVS you need to download and install four packages from the Internet and then assign three of them in the ISO_Builder OWAwVS Settings screen. These packages provide an SSH server (FreeSSHd) for the WinPE ISO as well as an Internet browser (FirefoxPortable). The virus scanner package is McAfee's Virus Command Line Scanner with updated DAT files.

3.2.1.1 Download and Install FreeSSHd

1. On the Development PC, download FreeSSHd.exe from the download section of http://www.freesshd.com/?ctt=download
2. Double click on the downloaded "freeSSHd.exe" to install it on the Development PC. You can uninstall freeSSHd through the Control Panel "uninstall" section.
3. Click Run to run the installer.
4. Click **Next** at the Welcome screen.
5. Choose an installation location or click **Next** to accept default. **NOTE**: *We recommend you install to an easy access location like **C:\freeSSHd** as you will need to navigate to this location later*.
6. Leave **Full Installation** selected and click **Next**
7. In the "Select Start Menu Folder" screen, select **Don't create a Start Menu folder** and click **Next**.
8. In the "Select Additional Tasks" screen, deselect **Create a desktop icon** and click **Next**.
9. In the "Ready to Install" screen, click **Install**..
10. Click **Close** to close the pop up add.
11. Click **Yes** to "Private keys should be created. Should I do it now?".
12. Click **No** to "Do you want to run FreeSSHd as a system service?".
13. Click **Finish** to complete the installation of freeSSHd.

NOTE

You will need to leave freeSSHd as well as the other downloaded components installed on your Development PC as long as you want to build the OWAwVS ISO. FreeSSHd will not be active on your Development PC since you chose not to have the service autostart.

3.2.1.2 Download and Install Firefox Portable

1. On the Development PC, download Firefox Portable from the following website: http://portableapps.com/apps/internet/firefox_portable
2. Double click the executable, FirefoxPortable.exe and click "Next".
3. Choose an easy to access installation location like **C:\FirefoxPortable**.
4. Click "Install" and then "Finish".
5. Once finished, open the folder containing Firefox Portable and double-click on **FirefoxPortable.exe** to launch it. Once it opens, you can exit out. This is required to generate the preference files needed.
6. Firefox Portable can be configured to open to a default Home Page when first opened. It is convenient to make this the webpage for your network e-mail server. This default Home Page is configured in the ISO Builder script and will overwrite any Home Page you configure in Firefox Portable itself.

7. You can however, set other preferences in Firefox Portable in the application. Settings such as network proxy settings and/or e-mail server certificates can be applied to Firefox Portable and they will be transferred to the ISO when built by the ISO Builder.
8. You can apply these changes through Firefox Portable preferences screen just as they would be configured using Firefox. Make your desired configuration changes and exit the application. ISO Builder will include these configurations the next time it builds the OWAwVS ISO.

3.2.1.3 Download and Extract McAfee VirusScan Command Line for Windows

1. On the Development PC, download the latest version of McAfee VirusScan Command Line for Windows 6.0.3. If you are a McAfee customer you may use your Grant number at the following website to download a licensed version: http://www.mcafee.com/us/downloads/downloads.aspx
2. If you are not a McAfee customer you may download an evaluation version of the McAfee VirusScan Command Line for Windows 6.0.3 at the following website: http://www.mcafee.com/apps/downloads/free-evaluations/default.aspx?pc=productcategory&lang=en&plat=platform&ilv=AllVersions&pid=&pg=2&sz=50&srt=description&sd=ASC&segment=false
3. The compressed download file will end with a –l for the licensed version and –e for an evaluation version. The evaluation version will be valid for 30 days. To purchase a licensed version you should call McAfee at (408) 988-3832.
4. Double-click the downloaded zip file and extract its contents. Typically you could do this to your **C:** drive and you would end up with a directory at **C:\vscl-w32-6.0.3-l** containing the CLS files.
5. Download the **avvwin_netware_betadat.zip** from the location below:
   http://www.mcafee.com/apps/mcafee-labs/beta/dat-file-updates.aspx
6. Extract the contents of **avvwin_netware_betadat.zip** to the same directory you created in step 4 and overwrite the existing files.
7. You will need to create a new runtime.dat file for use with the dat-file-updates. Open a command box and navigate to the **C:\vscl-w32-6.0.3-l** directory.
   a) If runtime.dat exists in the directory, type `del runtime.dat` and press 'Enter'.
   b) Type `scan /nc c:` and press 'Enter'.

   This will take a moment to run but an updated runtime.dat file will be created. You can now exit out of the command box.
8. If you want to update to new virus dat-files you should rerun step 7 before building a new ISO.

3.2.2 Configure OWA with Virus Scan

Once you have downloaded all the necessary components, you're ready to configure OWA with Virus Scan.

1. Under **Use Case** select **OWA with Virus Scan** and click **Settings**. The following screen is displayed.

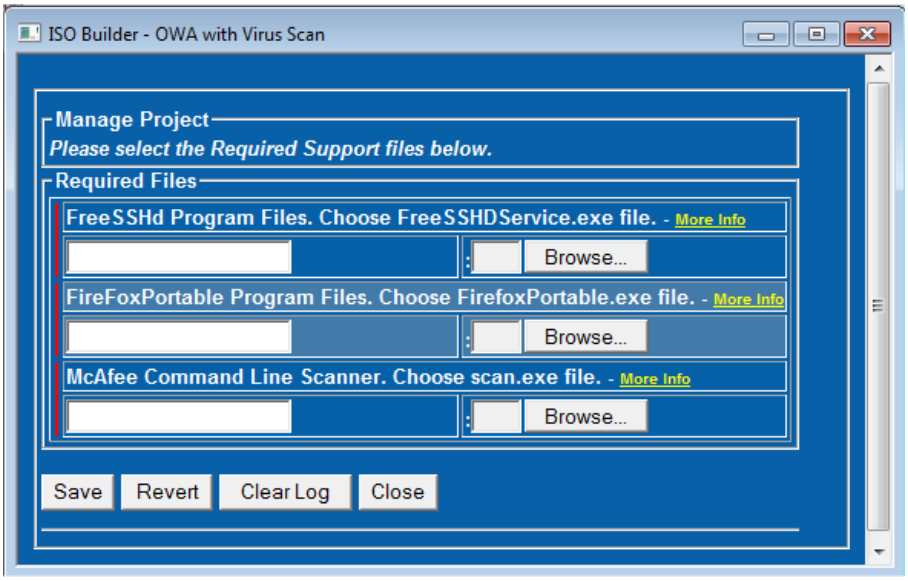

Figure 3: OWA with Virus Scan Settings

2. For each executable in the Required Files section, use the **Browse** button to select the path to its respective program. For example, McAfee Command Line Scanner will be **c:\scan\scan.exe**. The Default Home Page settings pane appears.

3. Enter a Default Home Page for Firefox Portable. This would most likely be the network path to your e-mail server (i.e., http://webmail.yourcompany.com).

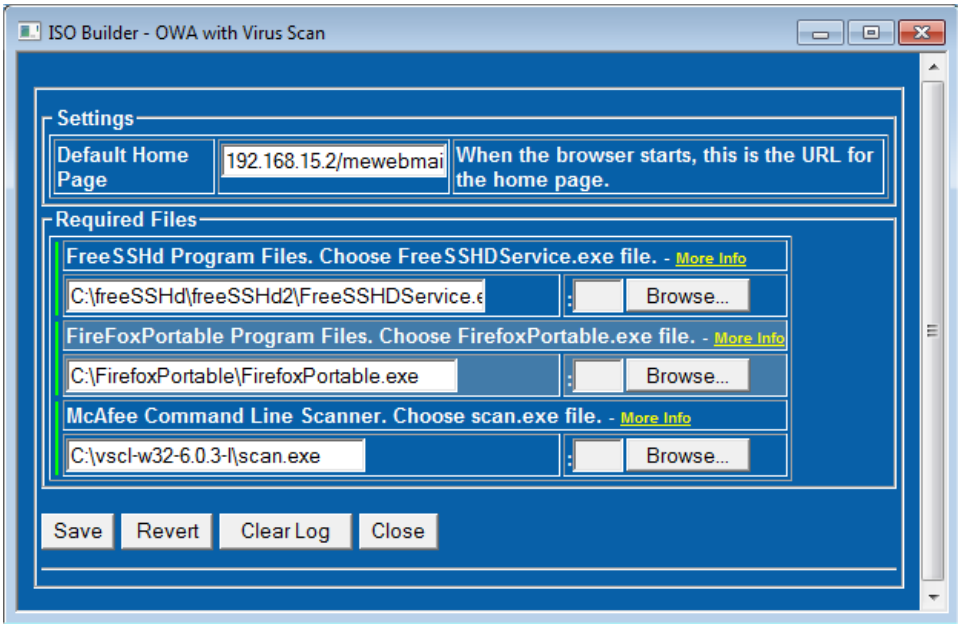

Figure 4: Enter Default Home Page

4. Once all of the files are verified click **Save** and then **Close**.
5. In the ISO Builder main screen, enter a name for the ISO (in this example we use **OWAwVS.iso**).
6. Continue to the next section.

3.3 Configure Two-Stage Boot Process

These steps use the two stage boot process to speed the loading of the OWAwVS ISO. Two stage boot works by using an intermediary boot image. This image is very small and thus, boots quickly. Once this image is loaded, it handles booting of the OWAwVS ISO. The OWAwVS ISO can then be located on the managed PC's hard drive or on a nearby network share. This decreases overall boot time, speeding time to repair.

1. In ISO Builder, select **2 stage boot**.
2. Click **Settings**.
3. Fill in as follows (shown in Figure 5 below).
   - Try Local Hard Drive: **No**
   - Try Network Resource: **Yes**
   - Take input from: **Choose at boot**
   - Download Type: **Share Drive**
   - Username: **<Username you assigned from section 2.2>**
   - Password: **<Password you assigned from section 2.2>**

- Domain: **<IP or name of Service Desk PC>**
- Path: **<IP or name of Service Desk PC>\<sharename from section 2.2>**
- Image: **OWAwVS.iso**

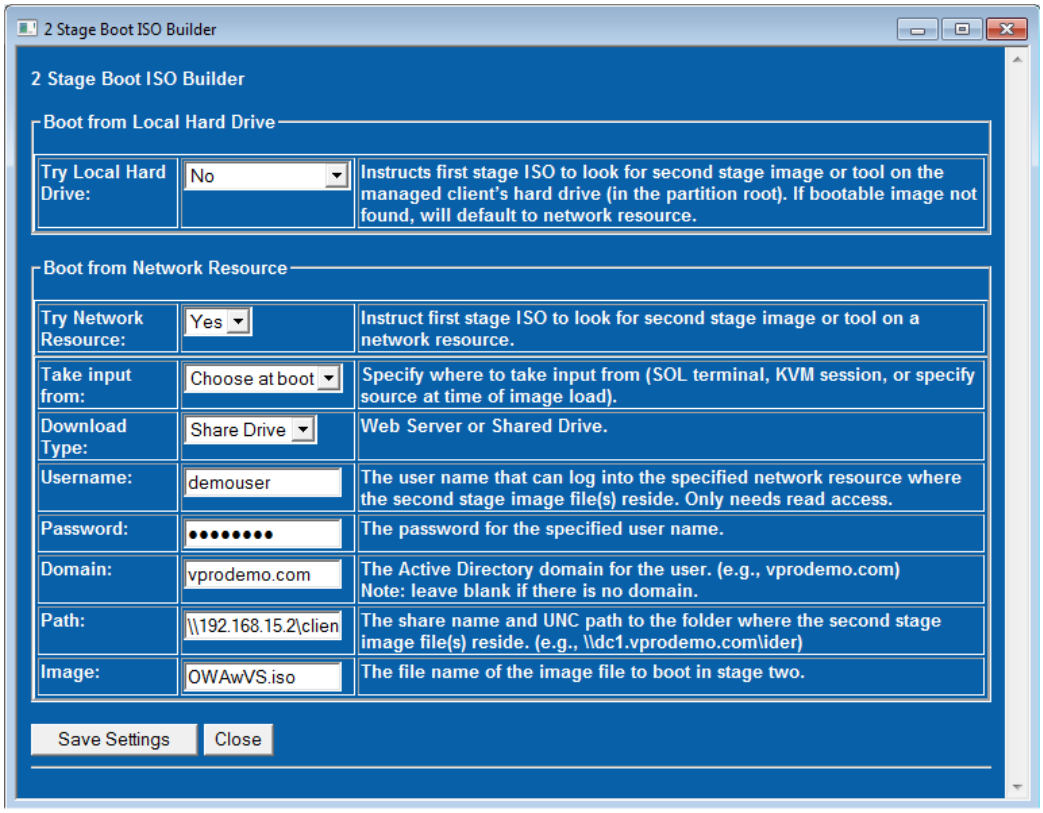

Figure 5: ISO Builder Settings for 2 Stage Boot

4. Click **Save Settings**.
5. Click **Close**.

NOTE

In this procedure, we do not place a local copy of the second-stage OWAwVS.iso file on the managed PC's local hard drive. However, this is an option. If you are interested in more options with using the two-stage boot process, please see the ***Faster Booting Over IDER*** *document, available here:*

http://communities.intel.com/docs/DOC-5552

3.4 Build and Copy the ISO Files

Follow the steps below to build the OWAwVS.iso file, and the first-stage ISO that will launch it as part of the two-stage boot process. You will then copy the files to their required locations.

1. In the main ISO Builder screen, verify that the ISO Image File Name field is set to **OWAwVS.iso** as directed in step5 of section 3.2.2.
2. In ISO Builder, click **Build ISO**. A log is shown at the bottom of the screen. If there is an error, check the log. **NOTE**: *for more detailed messages, select* ***Verbose Log*** *prior to clicking* ***Build ISO***.
3. Upon completion there are now two .iso files, **OWAwVS.iso**, and **ifast_ OWAwVS.iso**, located in the root of ISO Builder directory. **OWAwVS.iso** is your OWA with Virus Scan ISO. **ifast_ OWAwVS.iso** is the first stage boot image that will launch OWAwVS.iso.
4. Copy **OWAwVS.iso** to **c:\OWAwVS** on the Service Desk Console PC.
5. Copy **ifast_OWAwVS.iso** to **c:\ISOs** on the Service Desk PC.

NOTE

The first time through this build process, you will be building both the OWAwVS.iso file and its first-stage ISO, ifast_OWAwVS.iso. However, once both ISOs are created, if you want to modify the OWAwVS.iso file, but not the first-stage ISO, you can deselect ***2-stage boot*** *on the ISO Builder main screen and then simply modify and rebuild OWAwVS.iso.*

3.5 Download and Set Up Remote ISO Launcher (RIL)

On the Service Desk Console PC, do the following:

1. Download Remote ISO Launcher (RIL): http://communities.intel.com/docs/DOC-5943. RIL is used to perform the IDE Redirection process. It also provides automation support. Although not covered, other IDE-R capable software may be used.
2. Extract the RIL files to **c:\RIL**.
3. Launch RIL by double clicking on **c:\RIL\RemoteISOLauncher.exe**.

NOTE

Microsoft's .NET 4.0 must be installed on the PC running RIL. You can obtain.NET 4.0 from Microsoft's website if your PC does not have it installed by default.

4. Click the CD icon.

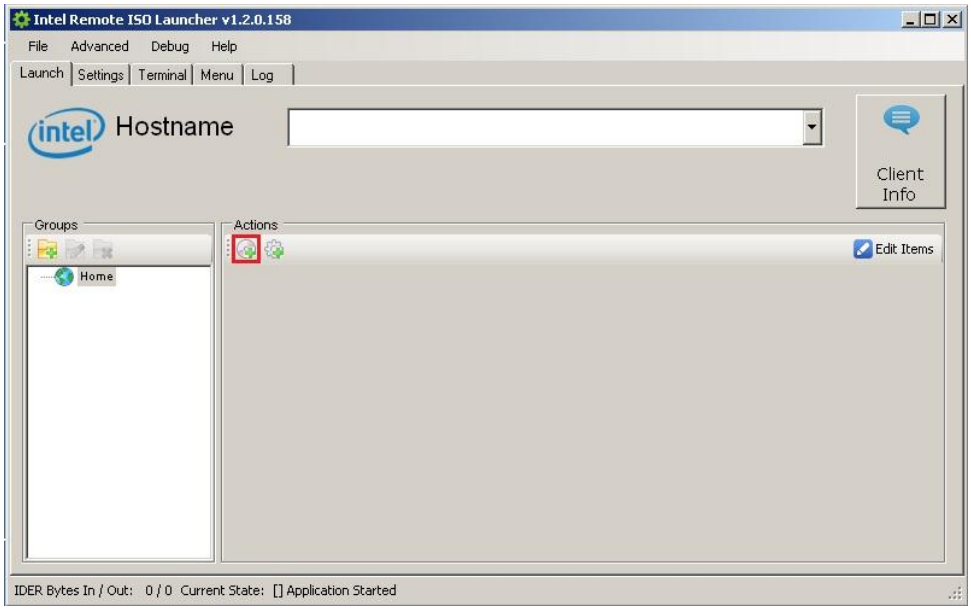

Figure 6: CD Icon on RIL Interface

5. Type in a friendly name "OWAwVS via 2 Stage".
6. Click **Browse**.
7. Select **c:\ISOs\ifast_OWAwVS.iso** from location used in step 0.
8. Click **Open**.
9. Click **Optionally select a color for the button**.
10. Click **Save**.
11. Depending on how your client is provisioned, you may also need to select the **Settings** tab and enter a digest user and password or select TLS.
12. Close RIL, and save settings when prompted.
13. Optionally create a desktop shortcut to **c:\RIL\RemoteISOLauncher.exe**.

3.6 Configure RIL to Launch an SSH Client

In the document example we use "putty.exe" as the SSH client. Putty.exe is included with the ISO Builder application (which you placed on the Development PC in section 3.1.1), in the folder
ISO Builder\apps\sol\src\x86\windows\system32.

1. Place a copy of **putty.exe** in a convenient location on the Service Desk Console PC where RIL is installed (for example, c:\putty\putty.exe). Remember this path.
2. You will need to place a batch file into the RIL Batch folder. This file should be named **start_putty.bat** and should contain the following lines exactly, including quotes:

   ```
   @echo off
   start "" "path to putty.exe from step 1" -ssh itproadmin@%1 -pw P@ssw0rd
   ```

   Be sure to replace *path to putty.exe from step* 1 with the actual path.

3.7 Perform the Remote Virus Scan with OWA

On the Service Desk PC, do the following:

1. In Remote ISO Launcher, enter the IP address for the managed PC.
2. Click **OWAwVS via 2 Stage**. The managed PC will reboot first to the first-stage ISO (ifast_OWAwVS.iso), then to the OWAwVS.iso WinPE image. This may take a minute or two.
3. Once WinPE is booted on the managed client and putty.exe is connected, you can type **vscan** at the default SSH prompt to start a virus scan on the managed client.
4. McAfee virus scanner is located at X:\vscan and can also be run manually. Type **scan /?** for options.
5. Create a network share (to access more tools or to help in repairs) and map it from the managed PC. This network share can be accessed by typing:
   net use Z: \\servername\sharename /user:domainuser password

NOTE

*If you are not using RIL to launch your OWA with Virus Scan ISO then you will need to launch **putty.exe** manually. Use your **start_putty.bat** file and replace %1 with the IP address of the managed client you ran OWAwVS on.*