Blue Coat Malware Analysis Appliance v4.2.8

IntelliVM Profile Customization Guide

16 June 2017

Document Revision 1.3

CONTENTS

1. About IntelliVM Profiles

1.1. About this Guide

This manual is intended for malware analysts and researchers who are utilizing the Blue Coat Systems Malware Analysis appliance (MA) solution and are interested in optimizing malware detection via the use of IntelliVM (iVM) profiles. It discusses detailed installation processes for Windows XP and Windows 7; other versions of Windows will follow very similar procedures.

This manual assumes that the reader is well versed in network terminology and operations, and is familiar with malware in general and malware analysis in particular. An understanding of Windows system events and network intrusion techniques is helpful as well.

1.2. System Requirements

The Malware Analysis appliance contains all of the necessary hardware, software, and connectivity needed to analyze malware in isolated or networked environments right out of the box using sophisticated iVM profiles that can be configured to mimic “typical” Windows systems or actual production configurations.

Customizing iVM profiles is accomplished via Remote Desktop connections using built-in or easily accessible open-source tools, connecting to publicly accessible websites for component downloads and updates.

1.3. Help and Support

We strongly recommend that you read this guide thoroughly before installing Malware Analysis appliance and attempting to configure iVM profiles, and that you use it as a reference during installation, configuration, and ongoing usage.

In this guide, you will find instructions on how to install and configure iVM base profiles and how to customize these base images into highly-realistic approximations of production systems used within your organization.

Support

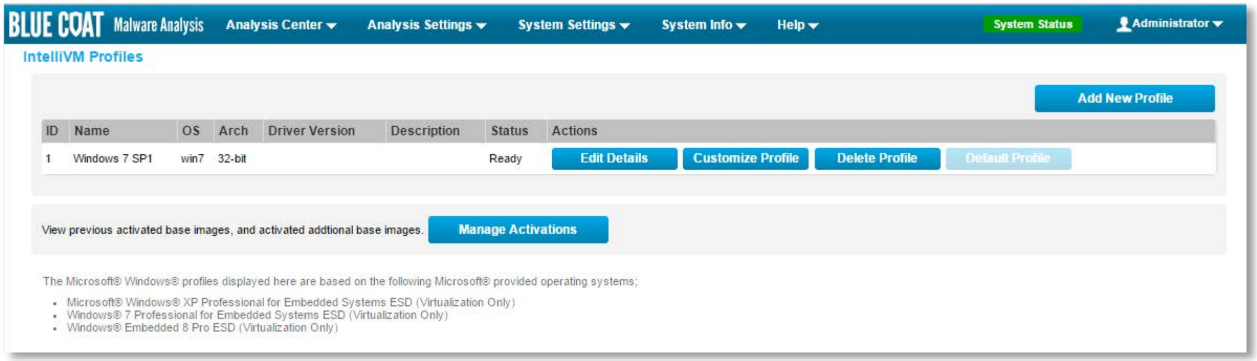
If you encounter any difficulty with the setup or usage of the Malware Analysis appliance in general, or the configuration or usage of iVM profiles in particular, please contact your Symantec sales representative or sales engineer, or visit our Support website at https://support.symantec.com/en_US/contact-support.html.

2. IntelliVM Profiles

2.1. IntelliVM Overview

IntelliVM kernel technology monitors system events for signs of malicious behavior in a virtualized environment. Profiles can be customized to add flexibility to analyze non-traditional malware and to precisely mirror custom environments to detect advanced and targeted threats.

Virtual machines (VMs) are software implementations of computer systems that execute programs just like physical machines, without putting real PCs at risk of malware infection. By using VM profiles to mirror multiple environments, analysts can quickly spot anomalies and differences in behavior that unveil anti-analysis and other advanced malware evasion techniques. VMs can easily be setup to match various Windows XP, Windows 7 (32-bit and 64-bit), and Windows 8 (64-bit) environments – such as patched and unpatched versions running alternate applications, browsers, and plugins – to quickly spot different malicious behaviors on multiple system types. VMs easily revert to a known non-infected state for repeat testing.



IntelliVM Profiles

ID	Name	OS	Arch	Driver Version	Description	Status	Actions
1	Windows 7 SP1	win7	32-bit			Ready	Edit Details Customize Profile Delete Profile Default Profile

View previous activated base images, and activated addtional base images.

The Microsoft® Windows® profiles displayed here are based on the following Microsoft® provided operating systems;

- Microsoft® Windows® XP Professional for Embedded Systems ESD (Virtualization Only)
- Windows® 7 Professional for Embedded Systems ESD (Virtualization Only)
- Windows® Embedded 8 Pro ESD (Virtualization Only)

Figure 1– Available IntelliVM Profiles with Windows 7 set as the Default Profile

2.2. Base Images

Base images include complete Windows operating systems along with a number of preinstalled applications or components used to facilitate malware detection from various file types. Base images do not run directly within Malware Analysis appliance. Instead, they are used to create **profiles** which actually run within the IntelliVM virtual machine framework.

Four (4) base images presently ship with Malware Analysis appliance v4.2.8:

- Windows XP, Service Pack 3 (32-bit)
- Windows 7, Service Pack 1 (32-bit)
- Windows 7, Service Pack 1 (64-bit)
- Windows 8 (64-bit)

Note Base images ship from the factory and can be modified or deleted by the customer. Users cannot add new base images; however they can create an unlimited number of custom profiles derived from the existing base images.

2.3. Profiles

Profiles are ready-to-run encapsulations of base images plus additional customizations designed to replicate particular Windows environments. These customizations include commercial applications, custom applications, additional web browsers, and patches to components including applying Windows Updates to plug security vulnerabilities as they are released by Microsoft Customizing profiles allows the customer to run additional file types through the analysis process with each one running within its own native application.

- **Standard Profiles** – Malware Analysis appliance ships with four (4) standard profiles: **Windows XP SP3**, **Windows 7 SP1 32-bit, Windows 7 SP1 64-bit, and Windows 8 64-bit**

  The preinstalled standard profiles are built from their respective base images.

- **Default Profile** – The profile that runs “automatically” when no particular profile is specified. This profile often represents the most organization’s most prevalent configuration. Only one profile can be the default at a time.

3. Customizing VM Profiles IntelliVM Profiles

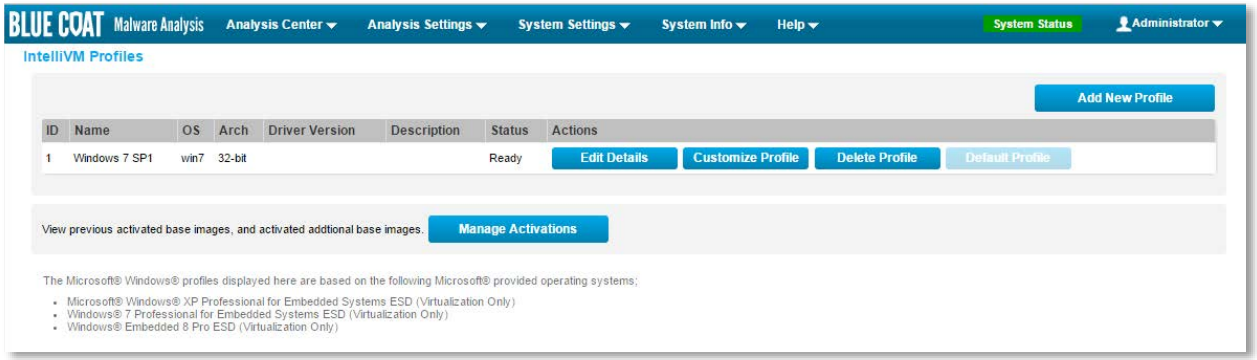
3.1 Build a New Profile

Administrative users can create, modify, or delete VM profiles at any time. Create VM profiles as needed to closely replicate production environments, or to test the behavior of malware across different configurations.

Example: Analysis of potential malicious sample on Sales, Engineering, and Accounting workstations.

Sales Profile	Windows 7 (SP1), Microsoft Office 2010, Internet Explorer 10
Engineering Profile	Windows 7 (SP1), Microsoft Office 2007, Firefox 20
Accounting Profile	Windows XP (SP3), Microsoft Office 2003, Internet Explorer 9

1. Log in to the web interface with Administrator credentials.
2. Select **Analysis Settings > IntelliVM Profiles**. The **IntelliVM Profiles** page is displayed.



IntelliVM Profiles

Add New Profile

ID	Name	OS	Arch	Driver Version	Description	Status	Actions
1	Windows 7 SP1	win7	32-bit			Ready	Edit Details · Customize Profile · Delete Profile · Default Profile

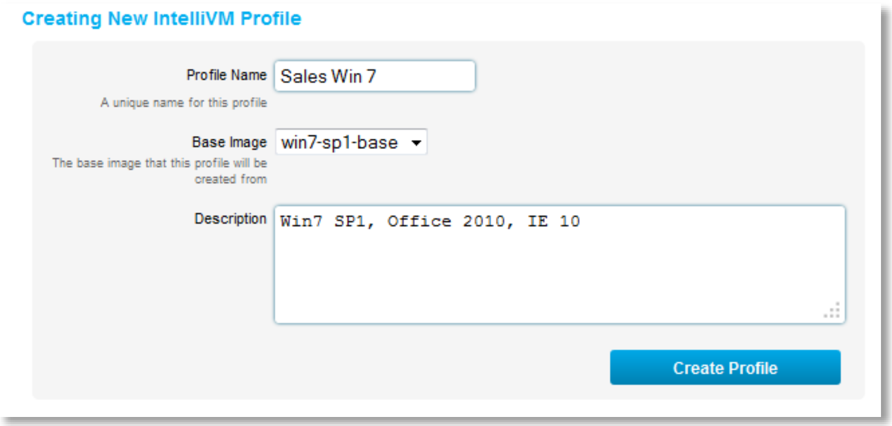
View previous activated base images, and activated addtional base images. Manage Activations

The Microsoft® Windows® profiles displayed here are based on the following Microsoft® provided operating systems:

- Microsoft® Windows® XP Professional for Embedded Systems ESD (Virtualization Only)
- Windows® 7 Professional for Embedded Systems ESD (Virtualization Only)
- Windows® Embedded 8 Pro ESD (Virtualization Only)

Figure 2 - Intelli VM Profiles

3. Click Add New Profile to access the Creating New IntelliVM Profile screen.



Creating New IntelliVM Profile

Profile Name: Sales Win 7
A unique name for this profile

Base Image: win7-sp1-base
The base image that this profile will be created from

Description: Win7 SP1, Office 2010, IE 10

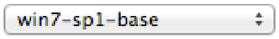
Figure 3 – Creating New IntelliVM Profile

Profile Name Enter a meaningful name for the profile. The name is mandatory.

Example: Sales Win 7

Base Image Select the desired image, the 'starting point' for the new profile. This is mandatory.

Example:

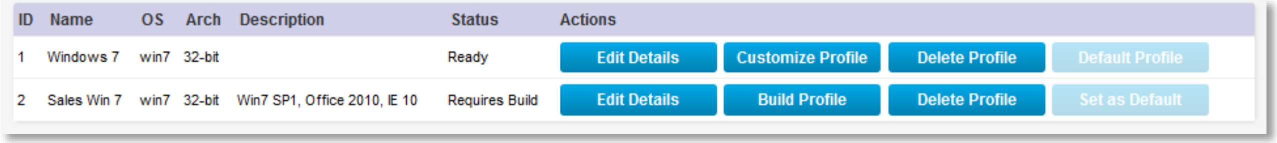


win7-sp1-base

Description List the contents of the profile in as much detail as desired. The description is optional.

Example: Windows 7 (SP1) with Microsoft Office 2010 and Internet Explorer 10

4. Click **Create New Profile** to create the profile after entering all selections. The *IntelliVM Profiles* page is displayed again, with the new profile in the list.

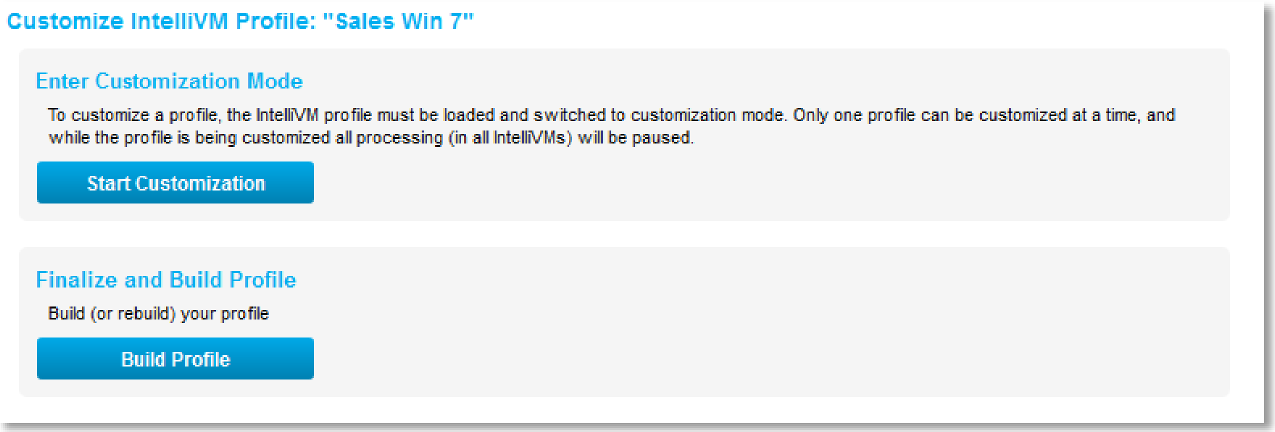


ID	Name	OS	Arch	Description	Status	Actions			
1	Windows 7	win7	32-bit		Ready	Edit Details	Customize Profile	Delete Profile	Default Profile
2	Sales Win 7	win7	32-bit	Win7 SP1, Office 2010, IE 10	Requires Build	Edit Details	Build Profile	Delete Profile	Set as Default

Figure 4 – IntelliVM Profiles List

Note Before a profile has been built, you may click Edit Details to change the base image. After the profile has been built, you cannot change the base image.

5. Click **Build Profile**. The *Customize IntelliVM Profile: [Profile Name]* page is displayed.



Customize IntelliVM Profile: "Sales Win 7"

Enter Customization Mode

To customize a profile, the IntelliVM profile must be loaded and switched to customization mode. Only one profile can be customized at a time, and while the profile is being customized all processing (in all IntelliVMs) will be paused.

Start Customization

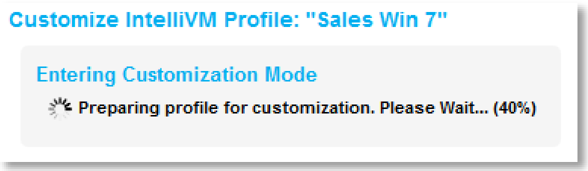
Finalize and Build Profile

Build (or rebuild) your profile

Build Profile

Figure 5 – Customization and Build Page

6. Click **Start Customization**.



Customize IntelliVM Profile: "Sales Win 7"

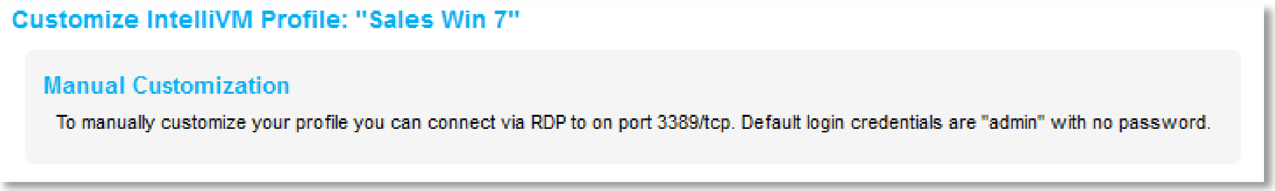
Entering Customization Mode

Preparing profile for customization. Please Wait... (40%)

Figure 6 – Entering Customization Mode

Several minutes will elapse while the profile is prepared for customization.

Caution While you are in customization mode, all processing in all IntelliVMs is suspended.



Customize IntelliVM Profile: "Sales Win 7"

Manual Customization

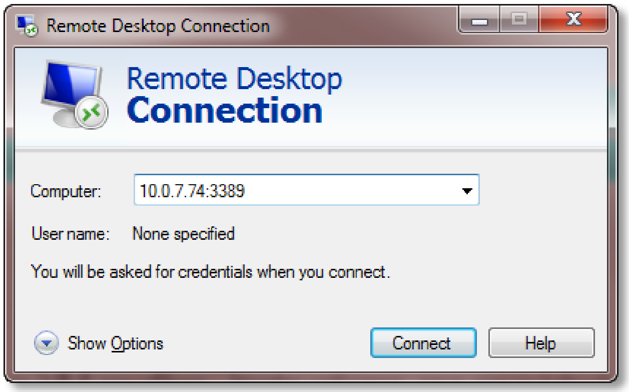
To manually customize your profile you can connect via RDP to on port 3389/tcp. Default login credentials are "admin" with no password.

Figure 7 – Manual Customization Message

When the profile is ready for customization, the following message is displayed: To manually customize your profile you can connect via RDP to on port 3389/tcp. Default login credentials are "admin" with no password.

Note Blue Coat recommends that you not close your browser while customizing a profile.

7. On a Windows workstation, launch Remote Desktop Connection. The **Remote Desktop Connection** dialog is displayed.



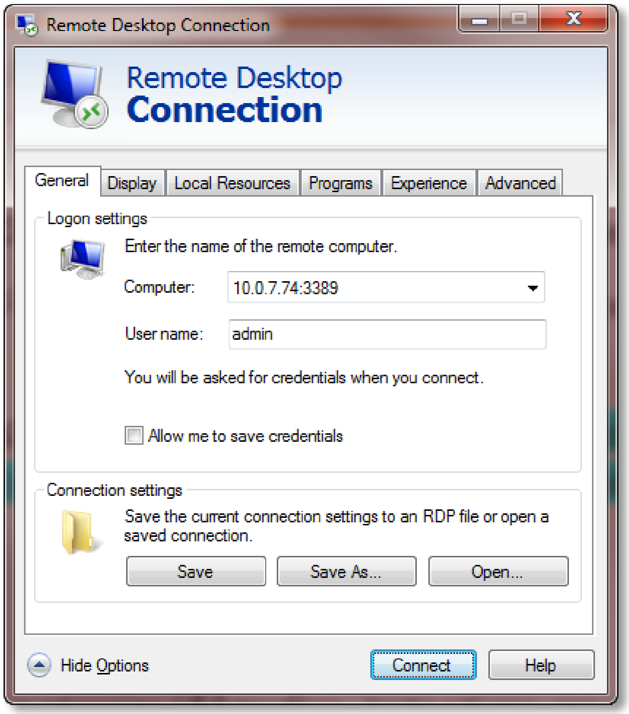
Computer: 10.0.7.74:3389

User name: None specified

You will be asked for credentials when you connect.

Figure 8 – Remote Desktop Connection Dialog

8. Click **Show Options**.



Logon settings

Enter the name of the remote computer.

Computer: 10.0.7.74:3389

User name: admin

You will be asked for credentials when you connect.

□ Allow me to save credentials

Connection settings

Save the current connection settings to an RDP file or open a saved connection.

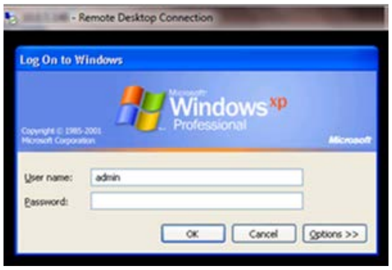
Figure 9 – Expanded Remote Desktop Connection Dialog

- For **Computer**, type the IP address of the Malware Analysis appliance and the port number in the following format: <ip_address>:3389.
- For **User name**, type **admin**.
- Click **Connect**, and then click **OK**. The desktop of the iVM is displayed.

Windows Example

1. Launch **Remote Desktop Connection**
2. Enter the IP address for the Malware Analysis appliance
3. Login to Windows on the Remote Desktop

The virtual Windows Desktop inside of the selected Malware Analysis appliance IntelliVM appears.



User name: admin

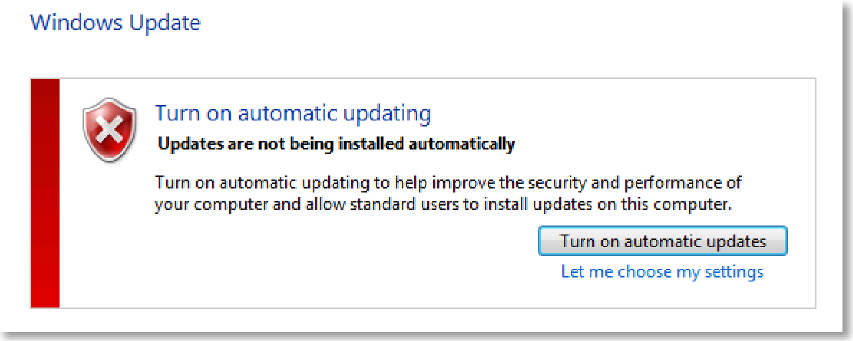
Password:

Remote Desktop Log On to Windows

3.2 Disable Automatic Update Checks

Before adding any customizations, verify that the applications that are already installed on the iVM are not checking for updates automatically. This ensures a consistent, uninterrupted analysis state. Additionally, the device reverts back to its last built state after each analysis. Follow this process:

1 From the Control Panel in the iVM, select **Windows Update** and verify that updates are not being installed automatically.



Windows Update

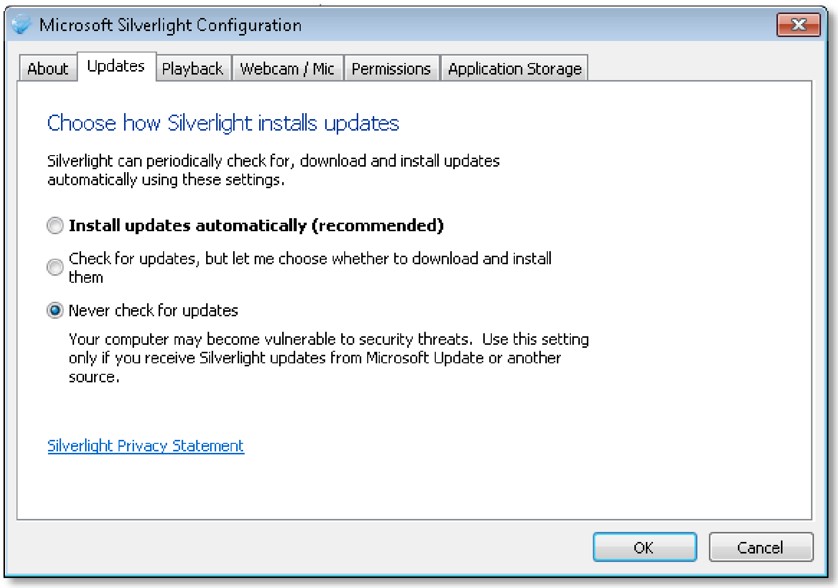
Turn on automatic updating

Updates are not being installed automatically

Turn on automatic updating to help improve the security and performance of your computer and allow standard users to install updates on this computer.

Figure 10 — Windows Update Control

2 Launch the Microsoft Silverlight Configuration dialog.



Microsoft Silverlight Configuration

Choose how Silverlight installs updates

Silverlight can periodically check for, download and install updates automatically using these settings.

○ **Install updates automatically (recommended)**

○ Check for updates, but let me choose whether to download and install them

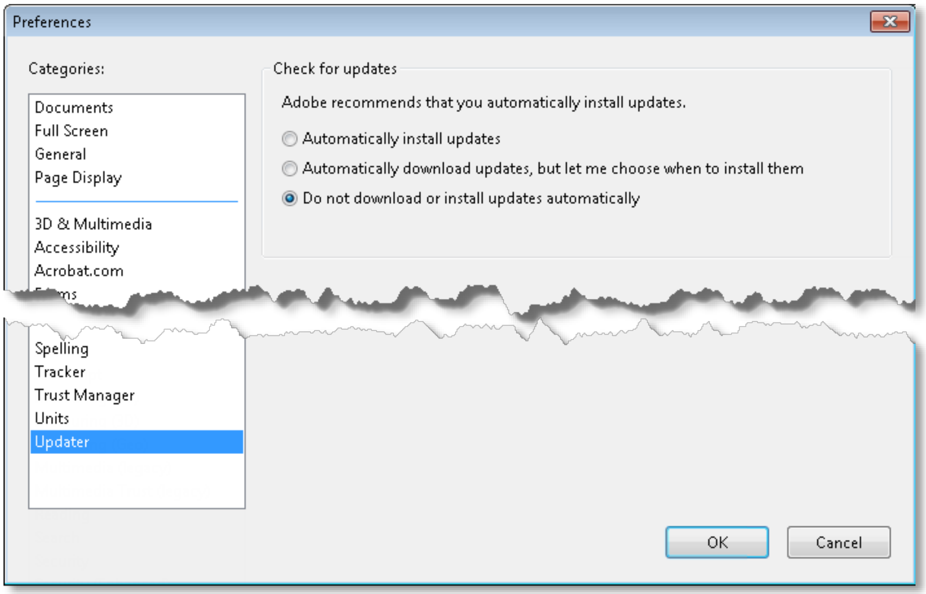
● Never check for updates

Your computer may become vulnerable to security threats. Use this setting only if you receive Silverlight updates from Microsoft Update or another source.

Figure 3 — Silverlight Updates Dialog

3 Click the **Updates** tab, and verify that **Never check for updates** is selected.

4 Launch the Adobe Reader, select **Edit > Preferences**, select **Updater** from the *Categories* list, and verify that **Do not download** or **install updates automatically** is selected.



Preferences

Categories:

Documents
Full Screen
General
Page Display

3D & Multimedia
Accessibility
Acrobat.com
Forms

Spelling
Tracker
Trust Manager
Units
Updater

Check for updates

Adobe recommends that you automatically install updates.

○ Automatically install updates
○ Automatically download updates, but let me choose when to install them
● Do not download or install updates automatically

Figure 4 — Adobe Reader Preferences Dialog

5 For any other non-Microsoft applications that are on the iVM or that you later install, verify that the automatic update checks are disabled.

6 Do you want to further customize the iVM profile?

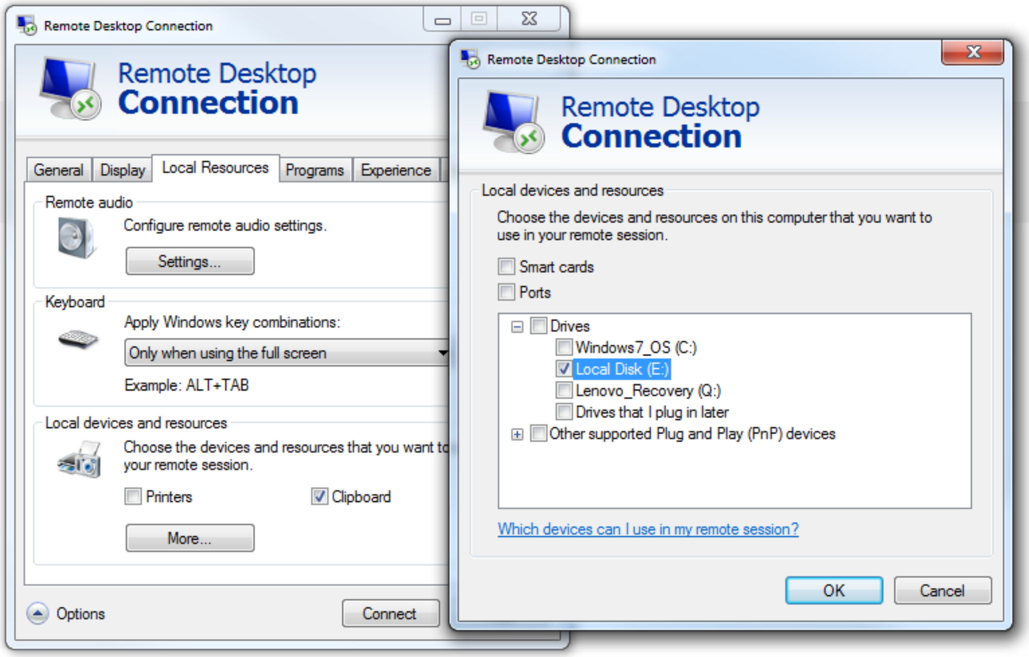
Yes — Continue the procedure.	**No** — Go to Finalize and Build the Profile.

3.3 Application Installation

Note The customer is responsible for obtaining the appropriate licenses for software that is installed on the iVMs. Contact the vendors of the respective software to obtain the proper license type for the iVMs.

To transfer installation files to your iVM, use one of the following methods:

- Use Remote Desktop Sharing. In the Remote Desktop Connection window, go to **Options > Local Resources > More… > Local devices and resources**. Select the location to map.



Remote Desktop Connection

Remote Desktop Connection

General | Display | Local Resources | Programs | Experience

Remote audio

Configure remote audio settings.

Settings...

Keyboard

Apply Windows key combinations:

Only when using the full screen

Example: ALT+TAB

Local devices and resources

Choose the devices and resources that you want to use in your remote session.

☐ Printers ☑ Clipboard

More...

Options Connect

Remote Desktop Connection

Remote Desktop Connection

Local devices and resources

Choose the devices and resources on this computer that you want to use in your remote session.

☐ Smart cards

☐ Ports

- ☐ Drives
  - ☐ Windows7_OS (C:)
  - ☑ Local Disk (E:)
  - ☐ Lenovo_Recovery (Q:)
  - ☐ Drives that I plug in later
- ☐ Other supported Plug and Play (PnP) devices

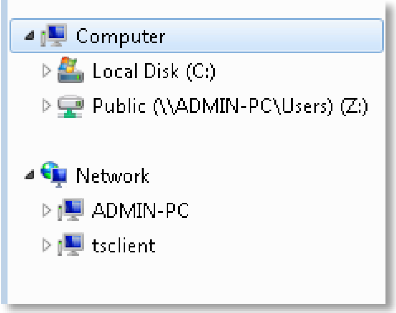
Which devices can I use in my remote session?

OK Cancel

Figure 13 — Network

Copy the files across as required.

- From inside the iVM, map a shared network drive or folder.



- Computer
  - Local Disk (C:)
  - Public (\\ADMIN-PC\Users) (Z:)
- Network
  - ADMIN-PC
  - tsclient

Figure 14 — Network Entities on the iVM

- Connect to the Internet to download software from an Internet resource or vendor site. (This connection is made through the **Backend** interface.)

Note To use a different proxy to access the Internet from inside the iVM, configure that proxy inside the iVM's Windows environment.

- The tsclient entity is the workstation that is accessing the iVM via Remote Desktop.

Install, license, and configure the applications to resemble a typical computing environment at your organization.

Note Your specific remote desktop client will determine which resources are available and the various methods that you can use to add software to a VM profile. Specific procedures are beyond the scope of this guide.

Blue Coat recommends using a shared drive or folder to add software to a VM profile.

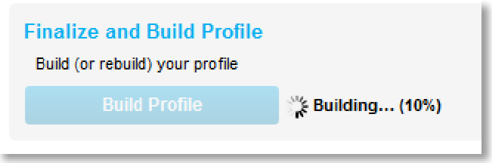
Shutting Down the Remote Connection

Disconnect the connection to the virtual Windows system by clicking Start *and selecting **Disconnect**.*

3.4 Finalize and Build the Profile

When you have finished customizing the profile, you must finalize and build it. Building the profile involves packaging up the base image along with any modifications and additional software, and getting the profile ready to run tasks.

1. Log out of the Remote Desktop session.
2. Return to the *Customize IntelliVM Profile: [Profile Name]* page on the Web interface.
3. Click Build Profile **Build Profile**.



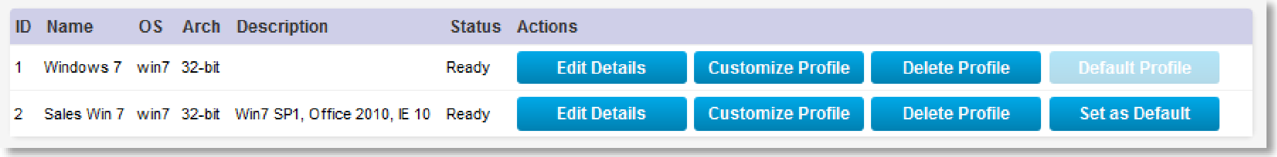
Finalize and Build Profile

Build (or rebuild) your profile

Figure 15 — Profile Building

Several minutes will elapse while the profile is being built.

4. When the profile has finished building, select **Analysis Settings > IntelliVM Profiles** to return to the *IntelliVM Profiles* page.



ID	Name	OS	Arch	Description	Status	Actions			
1	Windows 7	win7	32-bit		Ready	Edit Details	Customize Profile	Delete Profile	Default Profile
2	Sales Win 7	win7	32-bit	Win7 SP1, Office 2010, IE 10	Ready	Edit Details	Customize Profile	Delete Profile	Set as Default

Figure 16 — iVM List

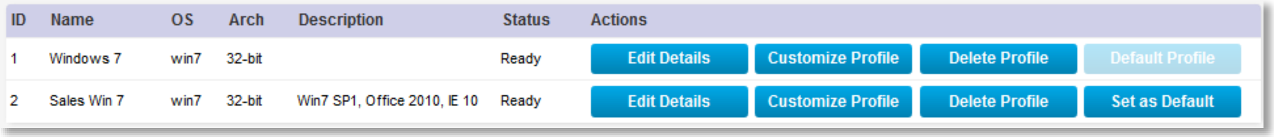
5. The new profile is ready for use. You may begin to send samples to the new profile, or you may select one of the following:
   - **Edit Details** — Return to the *Creating New IntelliVM Profile* page and change the description or name. (You cannot change the base image of an already-built profile.)
   - **Customize Profile** — Click to add further customizations to the iVM profile.
   - **Delete Profile** — Click to delete the profile. This action cannot be undone.
   - **Set as Default** — Click to make this profile your default profile.

3.5 Modifying Profiles

You may modify two aspects of a profile: the iVM itself or the iVM's details.

Note You cannot change the base image of an already-built profile.

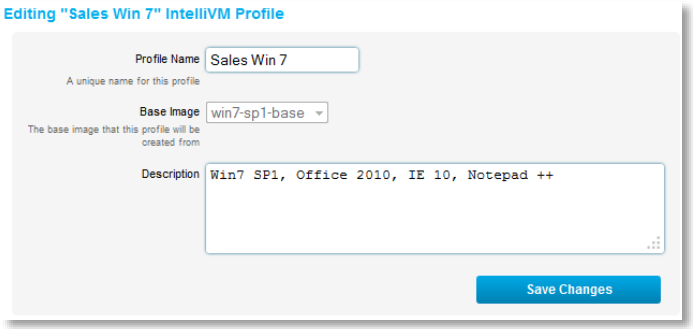
Select **Analysis Settings > IntelliVM Profiles**.



ID	Name	OS	Arch	Description	Status	Actions
1	Windows 7	win7	32-bit		Ready	Edit Details Customize Profile Delete Profile Default Profile
2	Sales Win 7	win7	32-bit	Win7 SP1, Office 2010, IE 10	Ready	Edit Details Customize Profile Delete Profile Set as Default

Figure 17 — iVM List

- To modify the details, click **Edit Details**. Edit either the profile name or its description, and then click **Save Changes**.



Editing "Sales Win 7" IntelliVM Profile

Profile Name: Sales Win 7
A unique name for this profile

Base Image: win7-sp1-base
The base image that this profile will be created from

Description: Win7 SP1, Office 2010, IE 10, Notepad ++

Figure 18 — Editing Details

- To modify a profile, click **Customize Profile**, and then follow the instructions in **steps 0 through □**to access the iVM through Remote Desktop. When you have finished the modifications, you must build the profile again.

3.6 Deleting Profiles

To delete a profile select **Analysis Settings > IntelliVM Profiles**.

Caution Deleting a profile cannot be undone. If you do not intend to deactivate a particular base image, do not delete the last profile that is associated with that image. Deleting a profile that has tasks assigned to it will result in an IVM_Error when that task reaches the top of the queue.

4. Optimizing Profiles

4.1. Standard Profiles

Malware Analysis appliance ships with **base images** for Windows XP SP3 and Windows 7 SP1. Base images are "starting points" for customizing robust malware detection environments. Base images may be enhanced by the customer or the SE.

Base image contents have been specially selected to provide a robust malware testbed. As such, the preinstalled component versions may not necessarily represent the latest versions available from their respective manufacturers.

The standard Malware Analysis appliance IntelliVM base images include:

- Compatibility Pack for the 2007 Office System
- Microsoft Office Excel Viewer
- Microsoft Office Word Viewer 2003
- Microsoft PowerPoint Viewer
- Python 2.7.6
- Windows Internet Explorer 8

Note Due to temporary licensing restrictions, several necessary base image components are unable to ship from the factory preinstalled. We expect this situation to be resolved shortly.

4.2. Enhanced Profiles

Customize profiles to add the flexibility to analyze non-traditional malware, and to closely mirror custom environments to detect advanced and targeted threats. Enhancing the MALWARE ANALYSIS APPLIANCE IntelliVM base images will include adding the following components to the Windows XP SP3 and Windows 7 SP1.

- Adobe Reader
- Adobe Flash
- Microsoft .NET Framework 3.5 SP1
- Microsoft Silverlight
- Java
- Microsoft C++ Redistributable 2010

Note Adding software beyond that which is provided by the base images may require proper third-party licenses.

5. Enhance the Windows XP Profile

The Malware Analysis Appliance comes with the following programs pre-installed. You may update them to the latest version if you wish to.

This section is for your information. All steps are optional.

The examples in this section reflect currently installed versions.

Adding components to base images works the same way as adding software to a physical machine. The process is identical, consisting of downloading software from websites and negotiating installation dialogs.

Step 1: Inside the Windows XP virtual machine on the **Desktop,** press the **Start** button and select **Control Panel**.

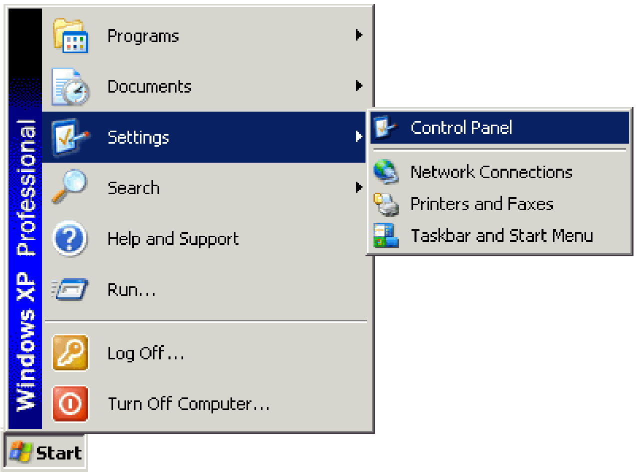


Figure 19 – Windows XP Start Menu

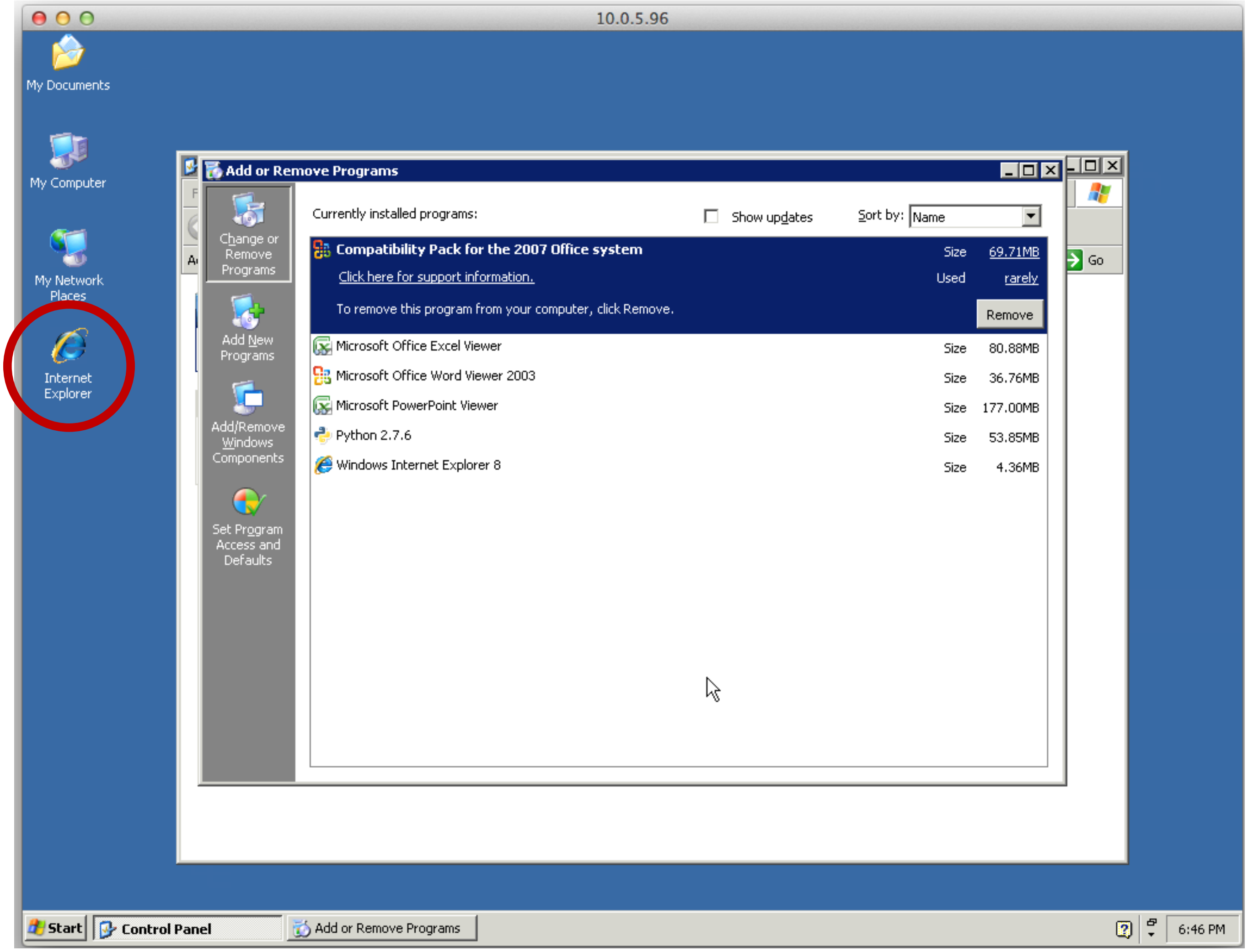
Step 2: Inside the **Control Panel**, click **Add or Remove Programs**.

Step 3: Inside the **Add or Remove Programs** window, confirm that the following programs are currently installed.

- Compatibility Pack for the 2007 Office System
- Microsoft Office Excel Viewer
- Microsoft Office Word Viewer 2003
- Microsoft PowerPoint Viewer
- Python 2.7.6
- Windows Internet Explorer 8

This configuration is the proper starting point for the Windows XP base image enhancement process.

Note Please contact your technical representative if your base image configuration does not closely match Figure 20.



Currently installed programs: □ Show updates Sort by: Name

Program		
Compatibility Pack for the 2007 Office system	Size	69.71MB
Click here for support information.	Used	rarely
To remove this program from your computer, click Remove.		Remove
Microsoft Office Excel Viewer	Size	80.88MB
Microsoft Office Word Viewer 2003	Size	36.76MB
Microsoft PowerPoint Viewer	Size	177.00MB
Python 2.7.6	Size	53.85MB
Windows Internet Explorer 8	Size	4.36MB

Figure 20 – Windows XP Add or Remove Programs displaying starting base image configuration

Step 4: Click the **Internet Explorer** icon on the Windows XP **Desktop** to open the Web browser.

Note *Sections* ***4.1*** *through* ***4.6*** all take place through the Internet Explorer Web browser interface.

6.6 Adobe Reader

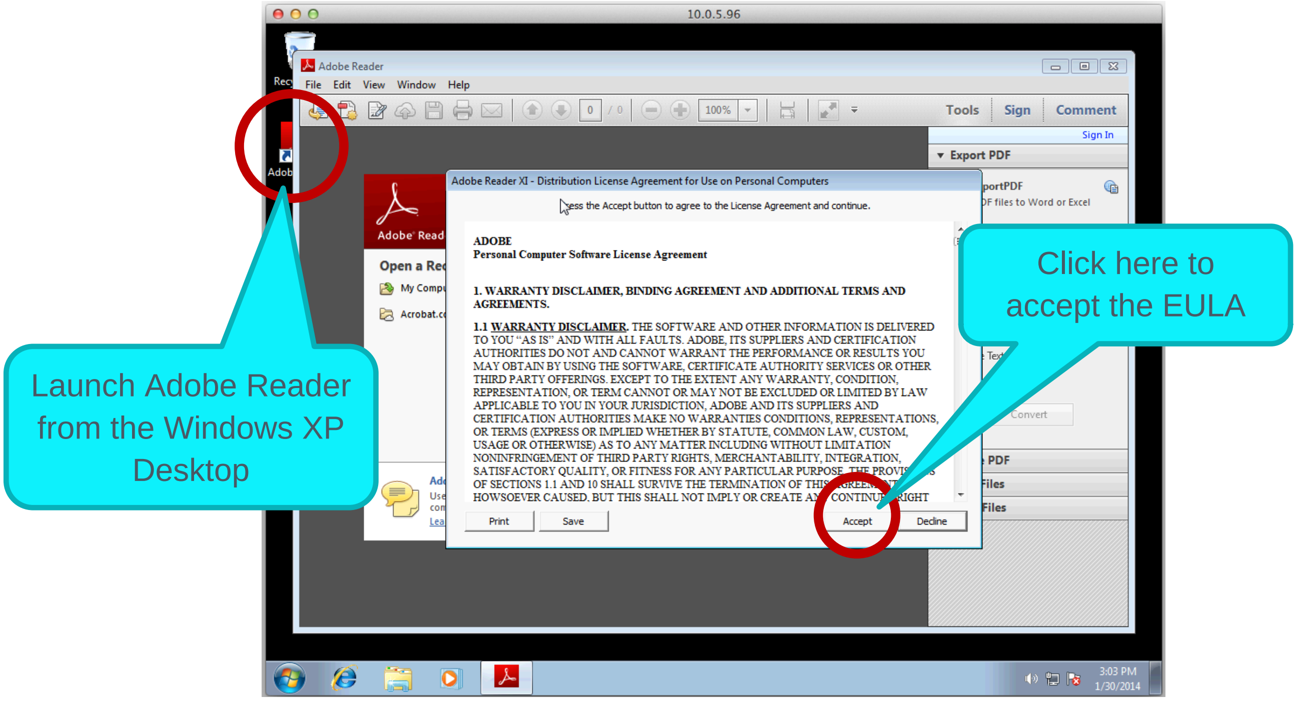
Installing Adobe Reader is optional.

Step 1: Download **Adobe Reader** from the following address and navigate the installer as required; decline the **Optional Offer**, and click **Install Now**.

- http://get.adobe.com/reader/

Step 2: When the installation is complete, run the **Adobe Reader** application from the Desktop and accept the End User License Agreement (EULA). The EULA appears automatically upon the first launch of the application.

Note The IntelliVMs will be unable to utilize Adobe Reader properly until the EULA has been accepted.


10.0.5.96
Adobe Reader
File Edit View Window Help
Tools Sign Comment
Sign In
Export PDF
Launch Adobe Reader from the Windows XP Desktop
Click here to accept the EULA

Adobe Reader XI - Distribution License Agreement for Use on Personal Computers

Press the Accept button to agree to the License Agreement and continue.

ADOBE
Personal Computer Software License Agreement

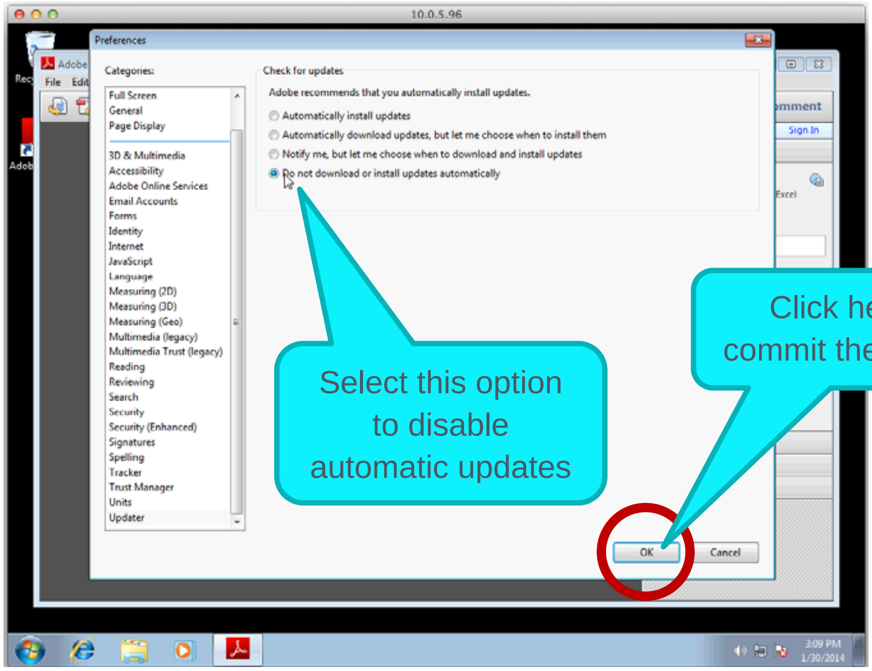
1. WARRANTY DISCLAIMER, BINDING AGREEMENT AND ADDITIONAL TERMS AND AGREEMENTS.

1.1 WARRANTY DISCLAIMER. THE SOFTWARE AND OTHER INFORMATION IS DELIVERED TO YOU "AS IS" AND WITH ALL FAULTS. ADOBE, ITS SUPPLIERS AND CERTIFICATION AUTHORITIES DO NOT AND CANNOT WARRANT THE PERFORMANCE OR RESULTS YOU MAY OBTAIN BY USING THE SOFTWARE, CERTIFICATE AUTHORITY SERVICES OR OTHER THIRD PARTY OFFERINGS. EXCEPT TO THE EXTENT ANY WARRANTY, CONDITION, REPRESENTATION, OR TERM CANNOT OR MAY NOT BE EXCLUDED OR LIMITED BY LAW APPLICABLE TO YOU IN YOUR JURISDICTION, ADOBE AND ITS SUPPLIERS AND CERTIFICATION AUTHORITIES MAKE NO WARRANTIES CONDITIONS, REPRESENTATIONS, OR TERMS (EXPRESS OR IMPLIED WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING WITHOUT LIMITATION NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, INTEGRATION, SATISFACTORY QUALITY, OR FITNESS FOR ANY PARTICULAR PURPOSE. THE PROVISIONS OF SECTIONS 1.1 AND 10 SHALL SURVIVE THE TERMINATION OF THIS AGREEMENT, HOWSOEVER CAUSED, BUT THIS SHALL NOT IMPLY OR CREATE ANY CONTINUING RIGHT

Figure 21 – The Adobe Reader End User License Agreement (EULA)

Step 3: Turn off automatic updates. From the **Edit** menu, select **Preferences**.

Note Updates are valuable for improving security and beneficial for the malware detection process, however it is essential that the MALWARE ANALYSIS APPLIANCE system administrator apply all updates *manually* so as to maintain configuration control over the malware testbed at all times. If components were to be allowed to update themselves automatically at random intervals, then configuration control becomes impractical and the administrator is never quite sure what versions of which components are being used for malware testing.



Check for updates

Adobe recommends that you automatically install updates.

○ Automatically install updates
○ Automatically download updates, but let me choose when to install them
○ Notify me, but let me choose when to download and install updates
● Do not download or install updates automatically

Select this option to disable automatic updates

Click here to commit the change

Figure 22 – Disabling automatic updates from the Preferences screen

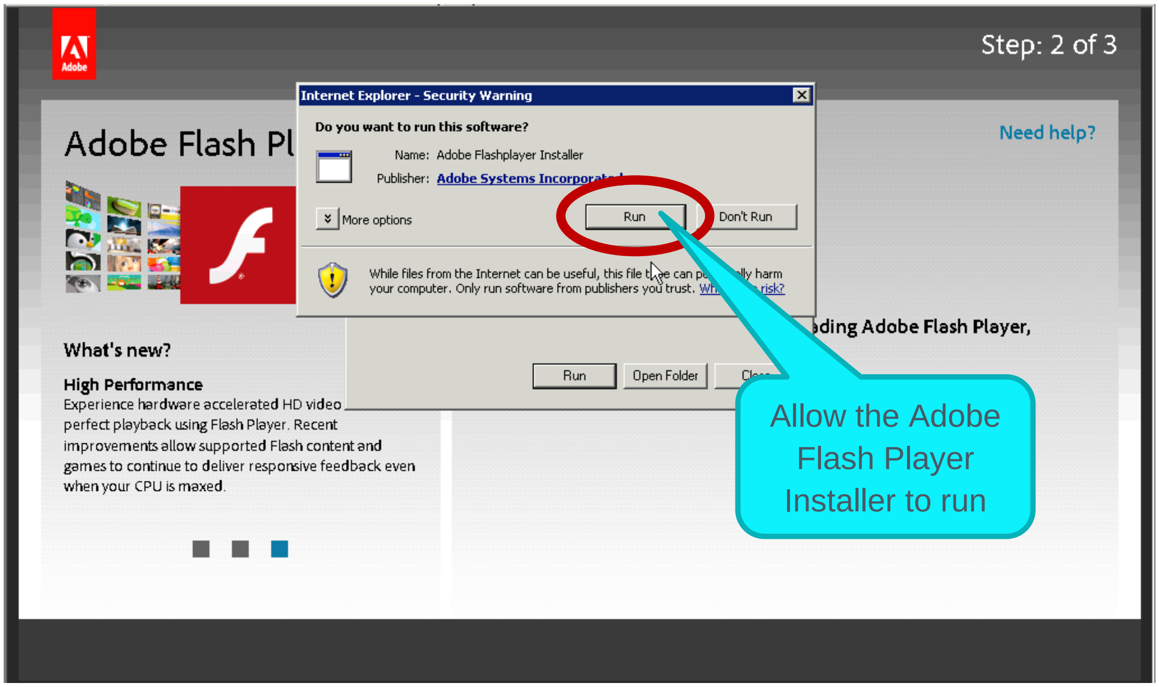
Note Additional Adobe Reader versions: https://get.adobe.com/uk/reader/otherversions/.

6.7 Adobe Flash

Installing Adobe Flash is optional.

Step 1: Download **Adobe Flash** from the following address and navigate the installer as required; ; decline the **Optional Offer**, and click **Install Now**.

http://get.adobe.com/flashplayer/



Internet Explorer - Security Warning

Do you want to run this software?

Name: Adobe Flashplayer Installer

Publisher: Adobe Systems Incorporated

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

…ding Adobe Flash Player,

What's new?

High Performance

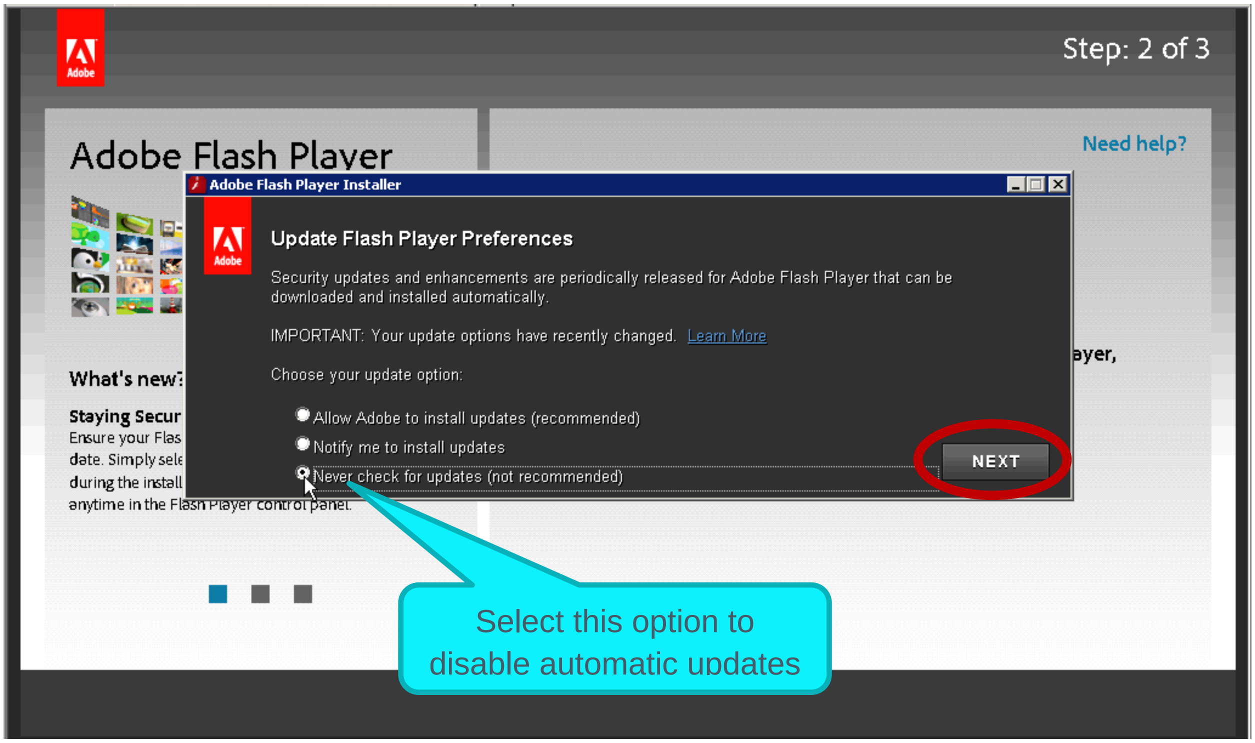
Experience hardware accelerated HD video perfect playback using Flash Player. Recent improvements allow supported Flash content and games to continue to deliver responsive feedback even when your CPU is maxed.

Allow the Adobe Flash Player Installer to run

Figure 23 – Internet Explorer Security Warning

Step 2: If prompted to **Update Flash Play Preferences** during installation, select the following option:

- Never check for updates (not recommended).



Adobe Flash Player Installer

Update Flash Player Preferences

Security updates and enhancements are periodically released for Adobe Flash Player that can be downloaded and installed automatically.

IMPORTANT: Your update options have recently changed. Learn More

Choose your update option:

○ Allow Adobe to install updates (recommended)
○ Notify me to install updates
● Never check for updates (not recommended)

What's new?

Staying Secur…
Ensure your Flas… date. Simply sele… during the install… anytime in the Flash Player control panel.

Select this option to disable automatic updates

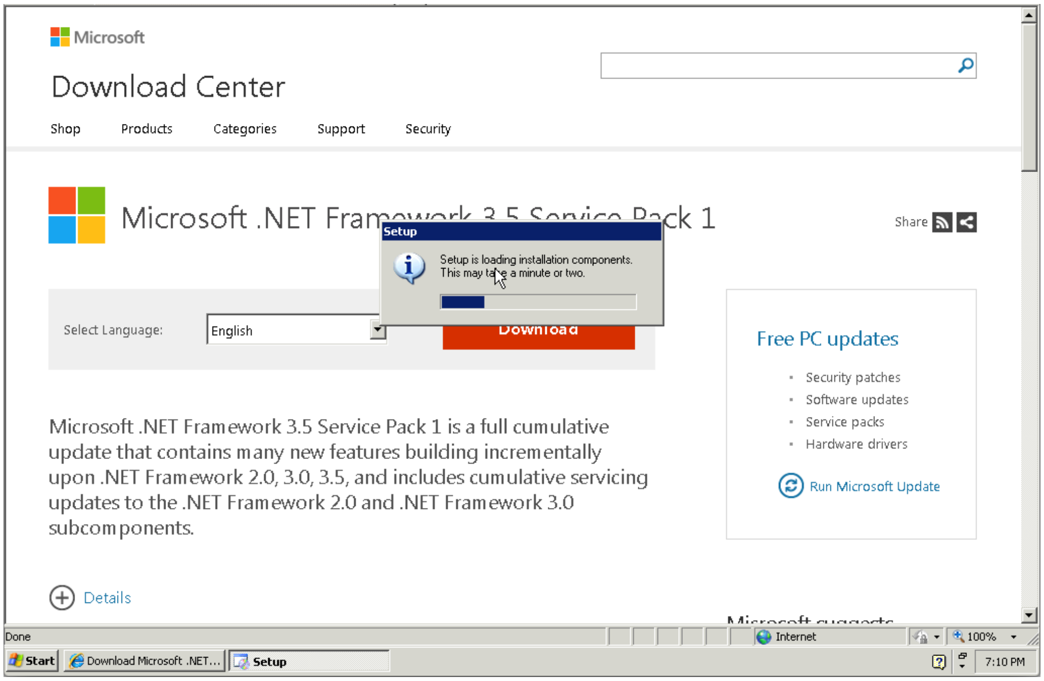
Figure 24 – Update Flash Player Preferences

Note Additional Adobe Flash versions: http://helpx.adobe.com/flash-player/kb/archived-flash-player-versions.html.

6.8 Microsoft .NET Framework 3.5 SP1

Step 1: Download **Microsoft .NET Framework 3.5 SP1** from this address and navigate the installer as required. In Windows 7 .NET is part of the operating system and can be enabled under **Programs and Features**.

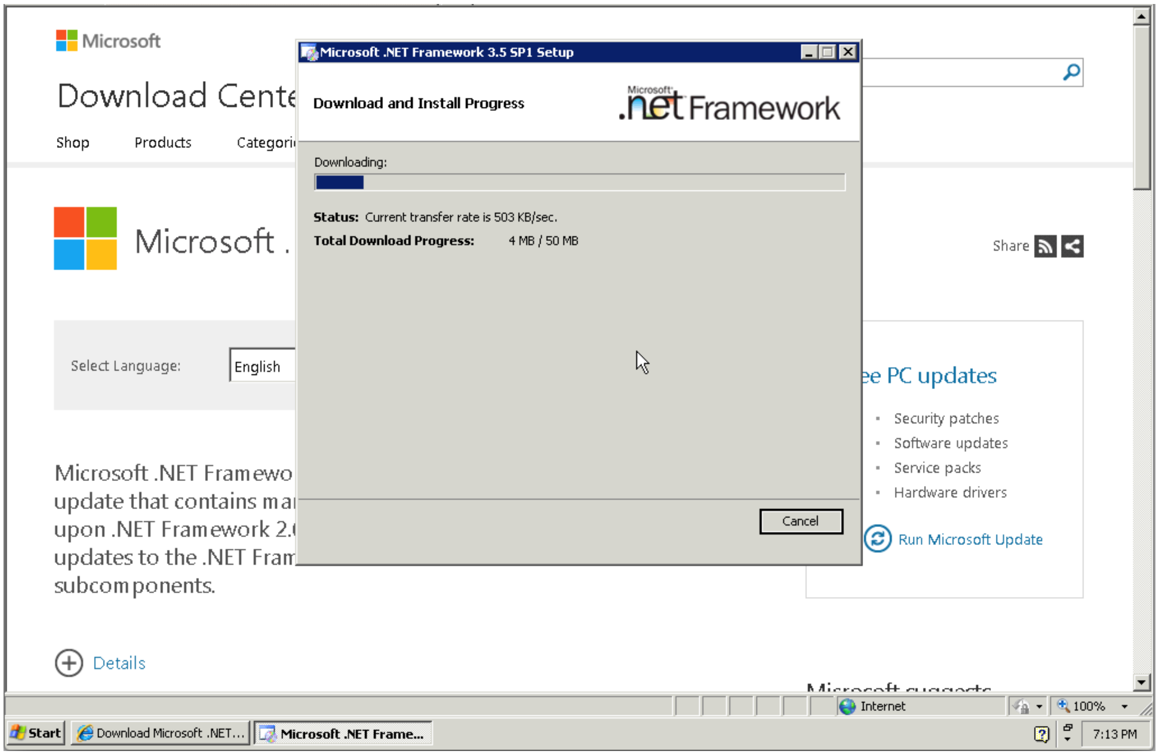
http://www.microsoft.com/en-us/download/details.aspx?id=22 *



Setup is loading installation components. This may take a minute or two.

Microsoft .NET Framework 3.5 Service Pack 1 is a full cumulative update that contains many new features building incrementally upon .NET Framework 2.0, 3.0, 3.5, and includes cumulative servicing updates to the .NET Framework 2.0 and .NET Framework 3.0 subcomponents.

Figure 25 – Installation is proceeding



Microsoft .NET Framework 3.5 SP1 Setup

Download and Install Progress

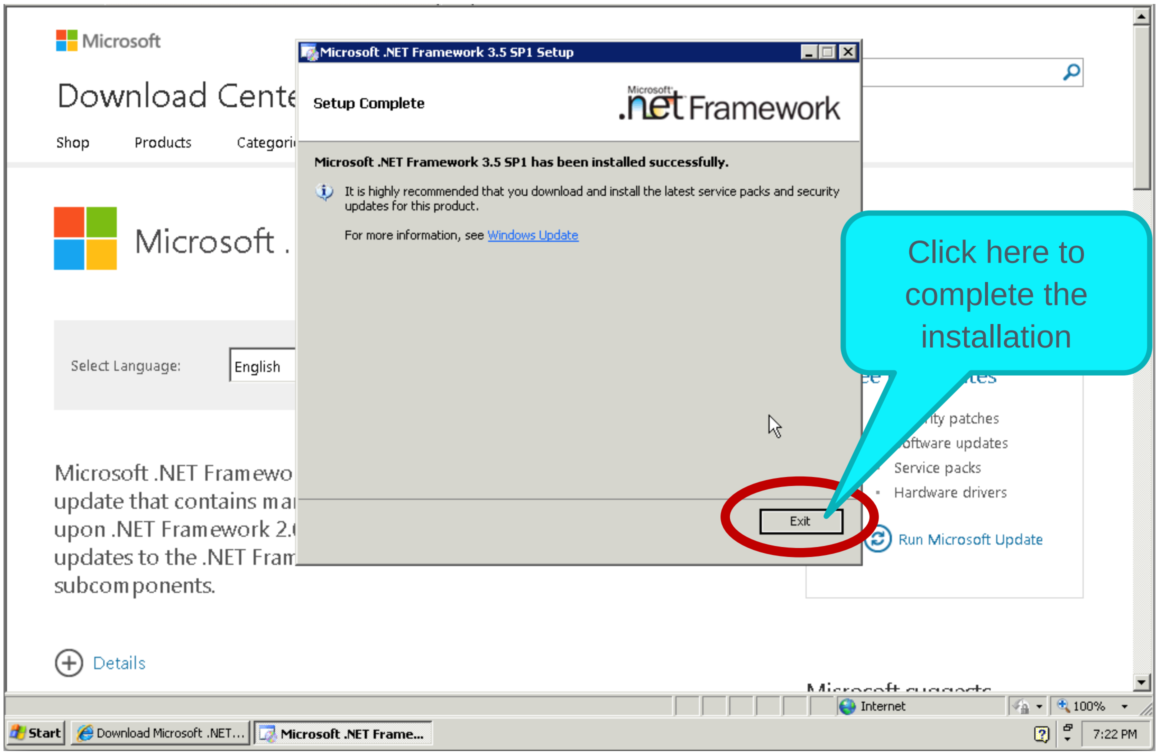
Microsoft .net Framework

Downloading:

Status: Current transfer rate is 503 KB/sec.

Total Download Progress: 4 MB / 50 MB

Figure 26 – Additional components being downloaded and installed



Microsoft .NET Framework 3.5 SP1 Setup

Setup Complete

Microsoft .net Framework

Microsoft .NET Framework 3.5 SP1 has been installed successfully.

It is highly recommended that you download and install the latest service packs and security updates for this product.

For more information, see Windows Update

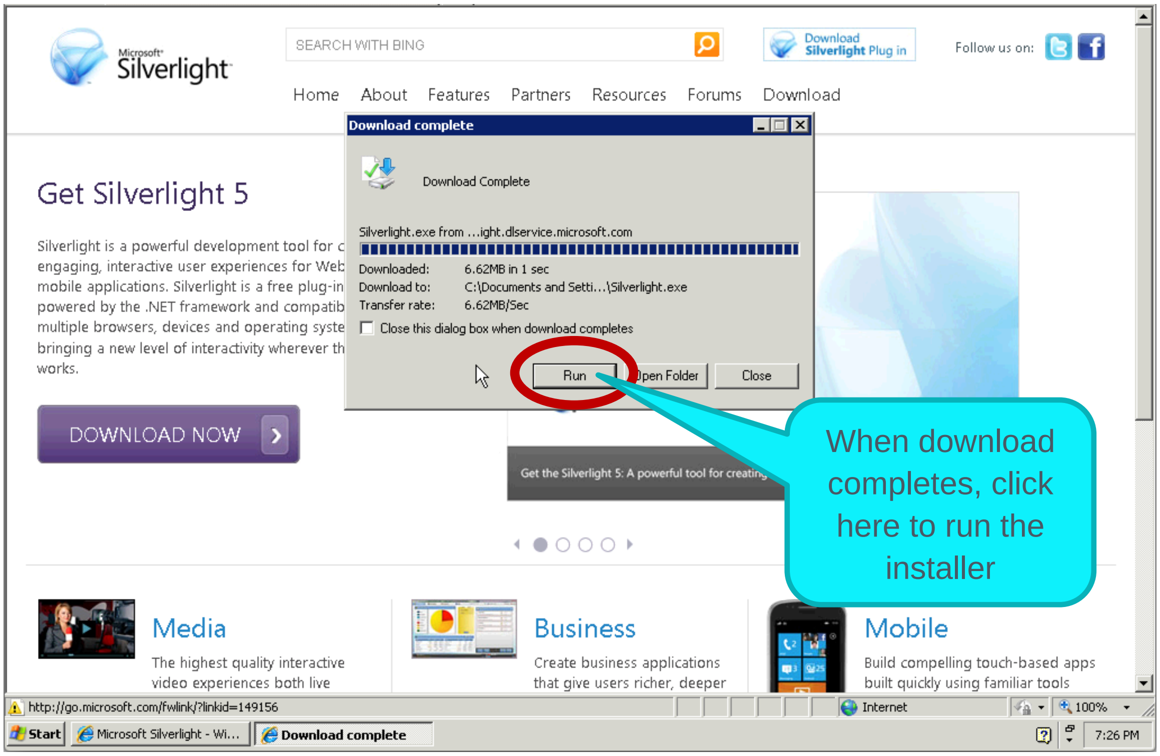
Click here to complete the installation

Figure 27 – Setup Complete

6.9 Microsoft Silverlight

Step 1: Download **Microsoft Silverlight** from this address and navigate the installer as required.

http://www.microsoft.com/silverlight/



Silverlight is a powerful development tool for c engaging, interactive user experiences for Web mobile applications. Silverlight is a free plug-in powered by the .NET framework and compatib multiple browsers, devices and operating syste bringing a new level of interactivity wherever th works.

The highest quality interactive video experiences both live

Create business applications that give users richer, deeper

Build compelling touch-based apps built quickly using familiar tools

http://go.microsoft.com/fwlink/?linkid=149156

Download complete

Download Complete

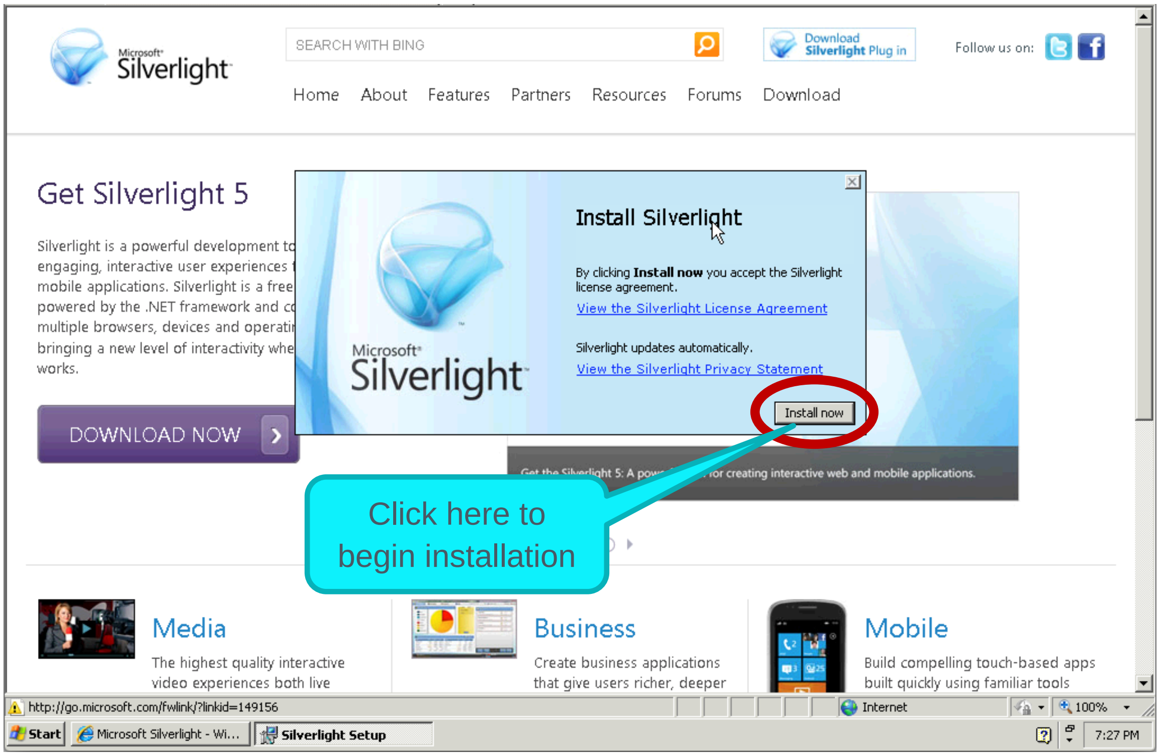
Silverlight.exe from …ight.dlservice.microsoft.com

Downloaded: 6.62MB in 1 sec
Download to: C:\Documents and Setti…\Silverlight.exe
Transfer rate: 6.62MB/Sec

☐ Close this dialog box when download completes

When download completes, click here to run the installer

Figure 28 – Silverlight download complete and ready to run the installer



Get Silverlight 5

Silverlight is a powerful development t[o] engaging, interactive user experiences [f] mobile applications. Silverlight is a free powered by the .NET framework and c[o] multiple browsers, devices and operati[ng] bringing a new level of interactivity whe[re] works.

Install Silverlight

By clicking **Install now** you accept the Silverlight license agreement.

View the Silverlight License Agreement

Silverlight updates automatically.

View the Silverlight Privacy Statement

Get the Silverlight 5: A pow[erful tool f]or creating interactive web and mobile applications.

The highest quality interactive video experiences both live

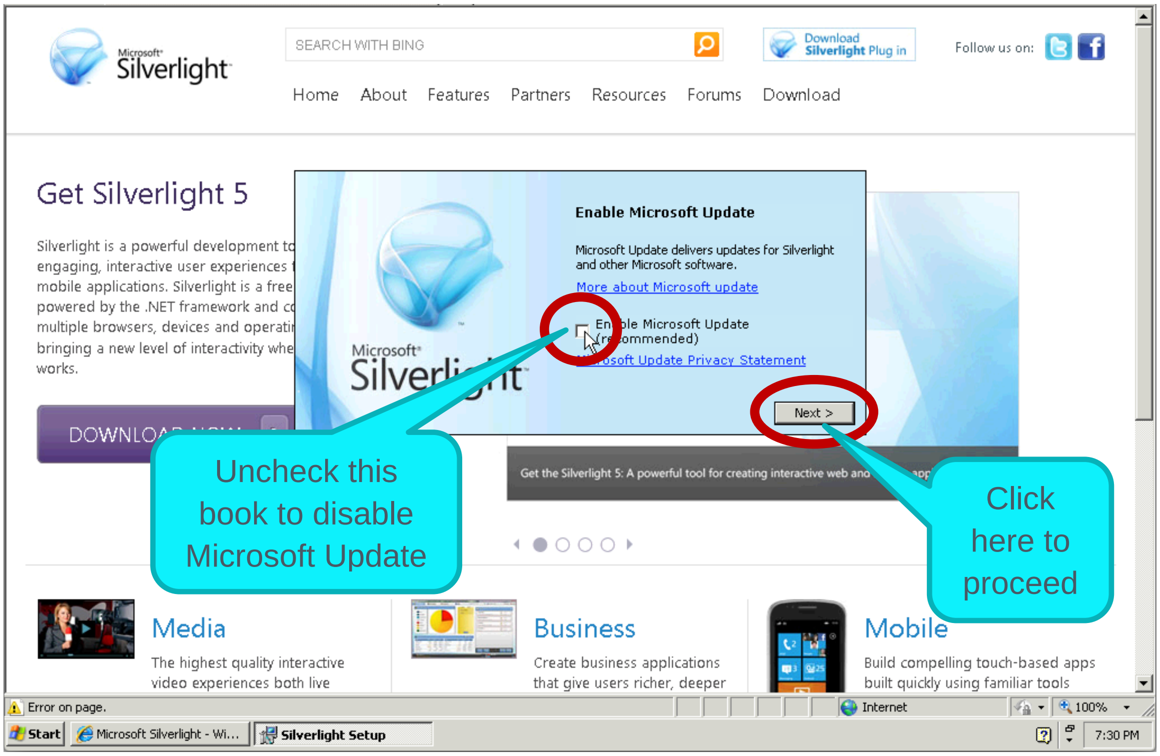
Create business applications that give users richer, deeper

Build compelling touch-based apps built quickly using familiar tools

http://go.microsoft.com/fwlink/?linkid=149156

Click here to begin installation

Figure 29 – Beginning Silverlight installation



Get Silverlight 5

Silverlight is a powerful development t[o] engaging, interactive user experiences [f] mobile applications. Silverlight is a free powered by the .NET framework and c[o] multiple browsers, devices and operati[ng] bringing a new level of interactivity whe[re] works.

Enable Microsoft Update

Microsoft Update delivers updates for Silverlight and other Microsoft software.

More about Microsoft update

□ Enable Microsoft Update (recommended)

Microsoft Update Privacy Statement

Get the Silverlight 5: A powerful tool for creating interactive web and ...

The highest quality interactive video experiences both live

Create business applications that give users richer, deeper

Build compelling touch-based apps built quickly using familiar tools

Error on page.

Uncheck this book to disable Microsoft Update

Click here to proceed

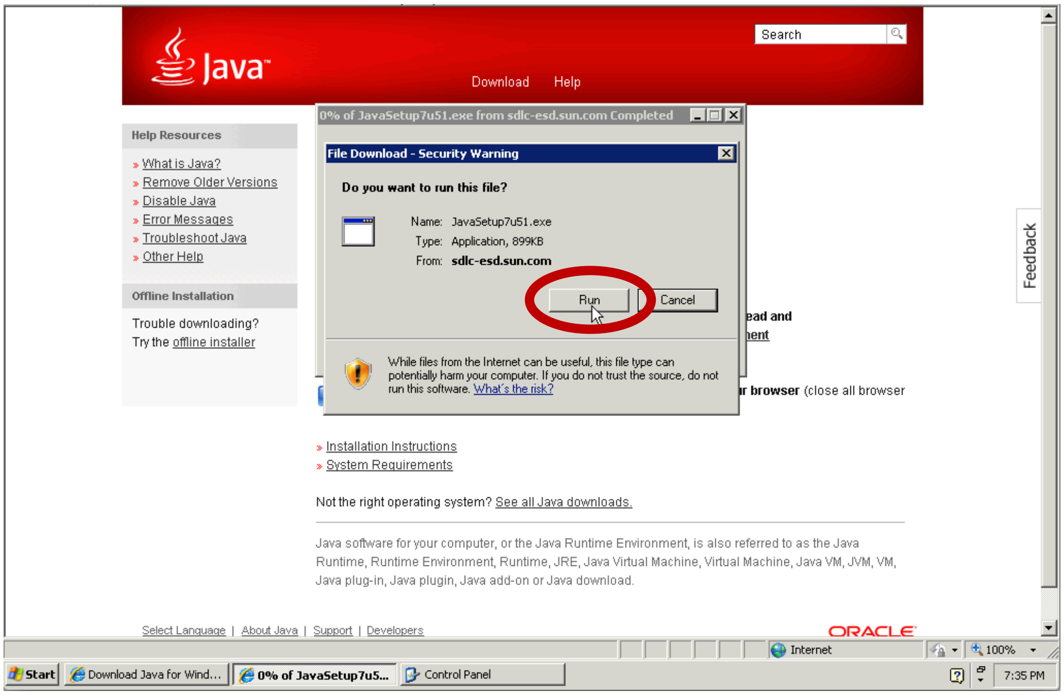
Figure 30 – Disabling Microsoft Update

6.10 Java

Installing Java is optional.

Step 1: Download **Java** from the address below and navigate the installer as required.

http://java.com/en/download/index.jsp



0% of JavaSetup7u51.exe from sdlc-esd.sun.com Completed

File Download - Security Warning

Do you want to run this file?

Name: JavaSetup7u51.exe
Type: Application, 899KB
From: sdlc-esd.sun.com

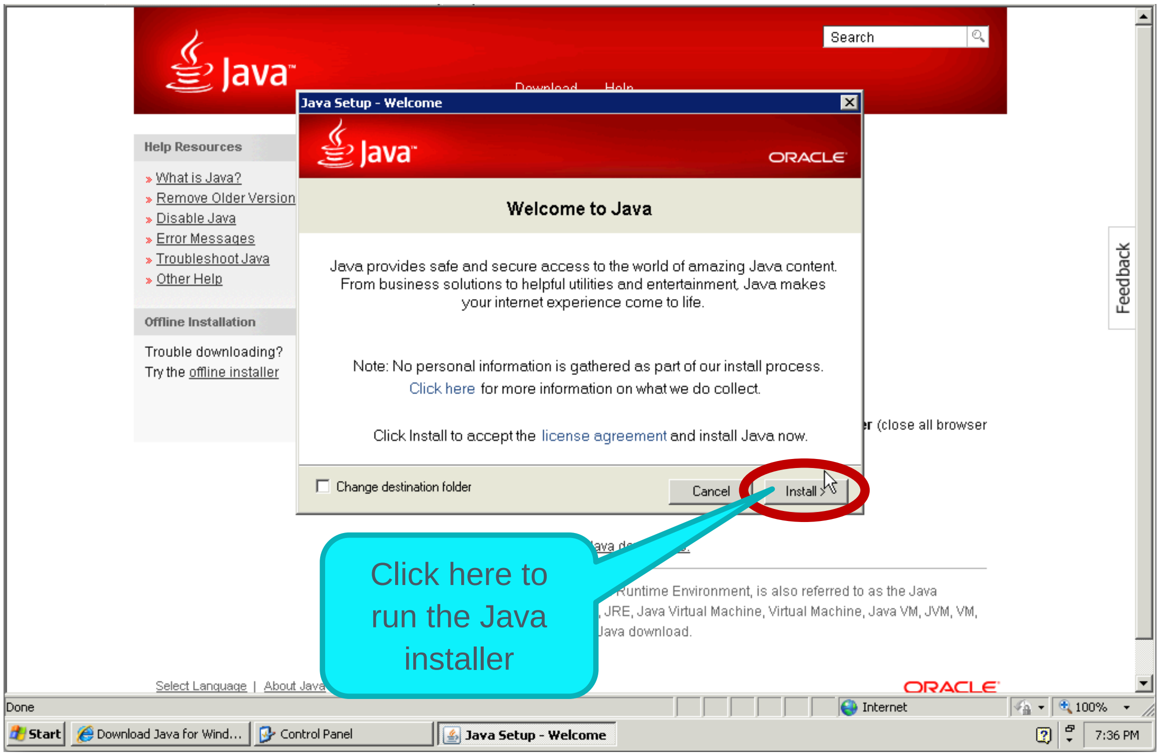
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run this software. What's the risk?

Trouble downloading?
Try the offline installer

Not the right operating system? See all Java downloads.

Java software for your computer, or the Java Runtime Environment, is also referred to as the Java Runtime, Runtime Environment, Runtime, JRE, Java Virtual Machine, Virtual Machine, Java VM, JVM, VM, Java plug-in, Java plugin, Java add-on or Java download.

Figure 31 – File Download Security Warning



Java Setup - Welcome

Welcome to Java

Java provides safe and secure access to the world of amazing Java content. From business solutions to helpful utilities and entertainment, Java makes your internet experience come to life.

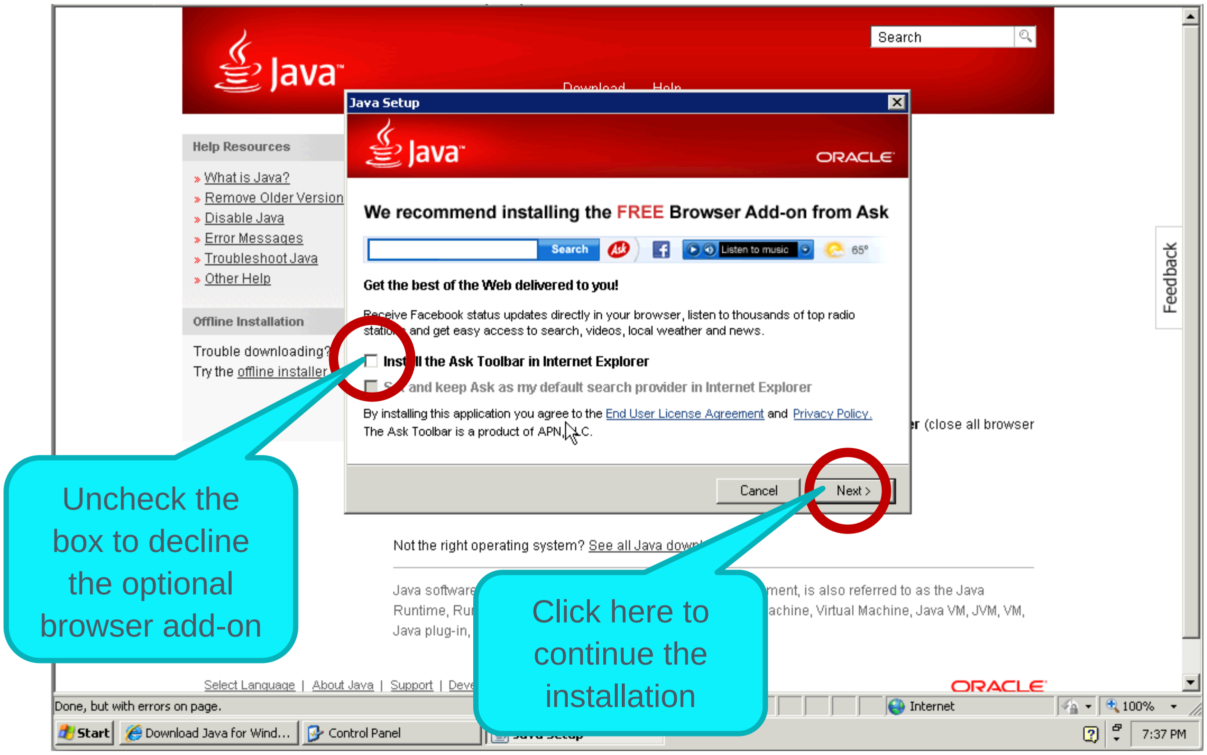
Note: No personal information is gathered as part of our install process. Click here for more information on what we do collect.

Click Install to accept the license agreement and install Java now.

□ Change destination folder

Click here to run the Java installer

Figure 32 – Java Installer Welcome screen



Java Setup

We recommend installing the FREE Browser Add-on from Ask

Get the best of the Web delivered to you!

Receive Facebook status updates directly in your browser, listen to thousands of top radio stations and get easy access to search, videos, local weather and news.

□ Install the Ask Toolbar in Internet Explorer

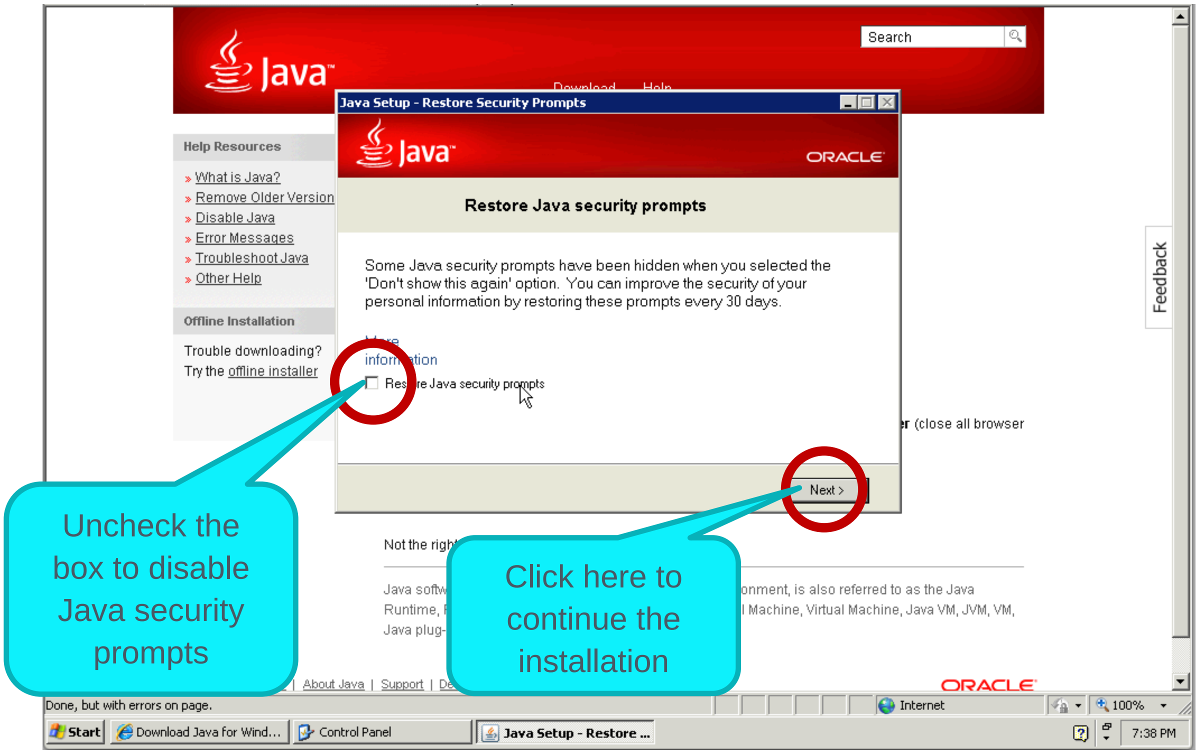
□ Set and keep Ask as my default search provider in Internet Explorer

By installing this application you agree to the End User License Agreement and Privacy Policy.
The Ask Toolbar is a product of APN, LLC.

Uncheck the box to decline the optional browser add-on

Click here to continue the installation

Figure 33 – Decline the Free Brower Add-On



Java Setup - Restore Security Prompts

Restore Java security prompts

Some Java security prompts have been hidden when you selected the 'Don't show this again' option. You can improve the security of your personal information by restoring these prompts every 30 days.

More information

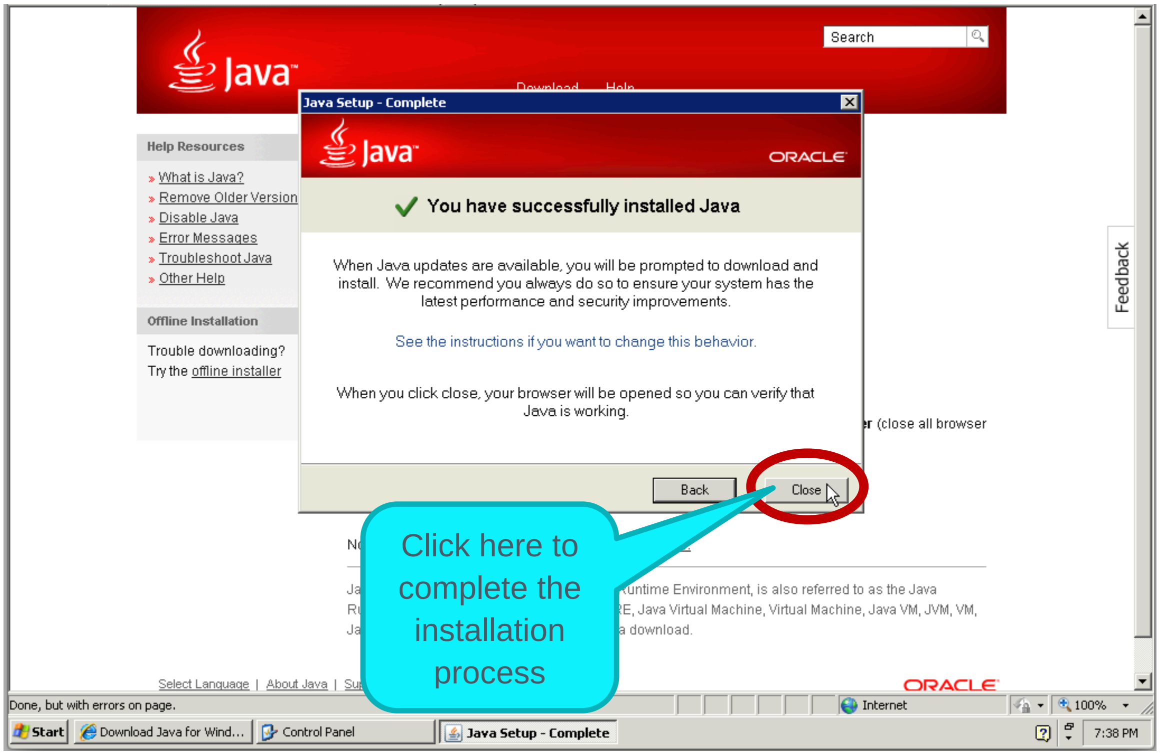
☐ Restore Java security prompts

Next >

Uncheck the box to disable Java security prompts

Click here to continue the installation

Figure 34 – Disable the Java security prompts



Java Setup - Complete

✓ You have successfully installed Java

When Java updates are available, you will be prompted to download and install. We recommend you always do so to ensure your system has the latest performance and security improvements.

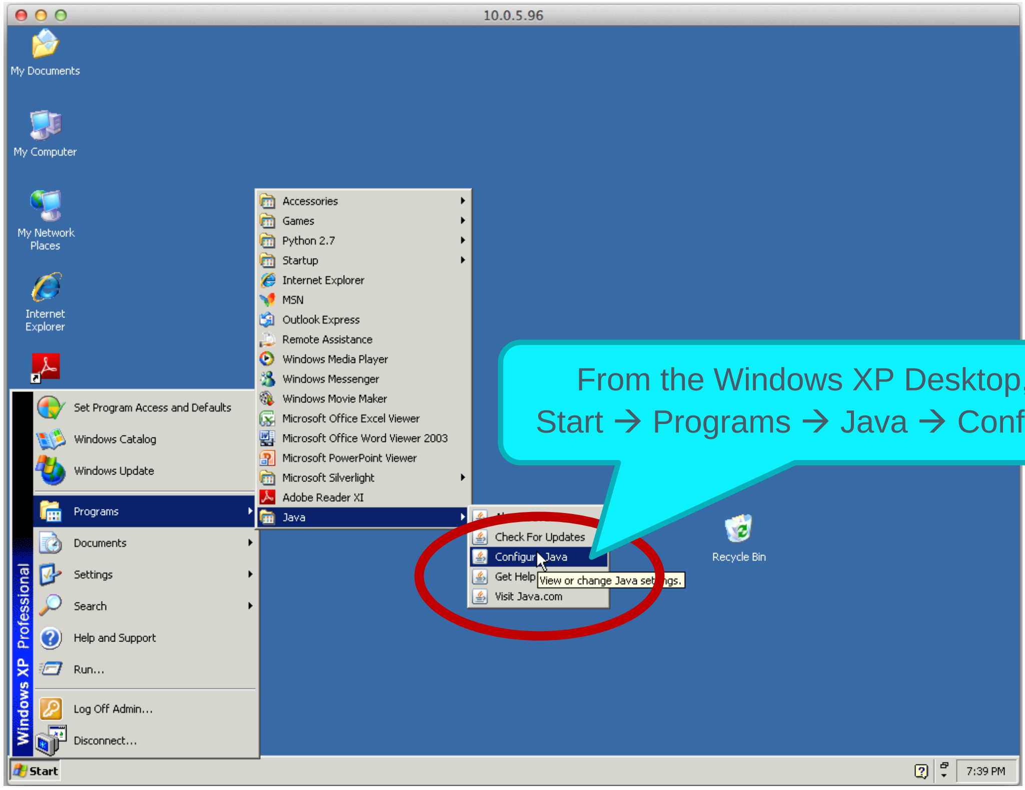
See the instructions if you want to change this behavior.

When you click close, your browser will be opened so you can verify that Java is working.

Back Close

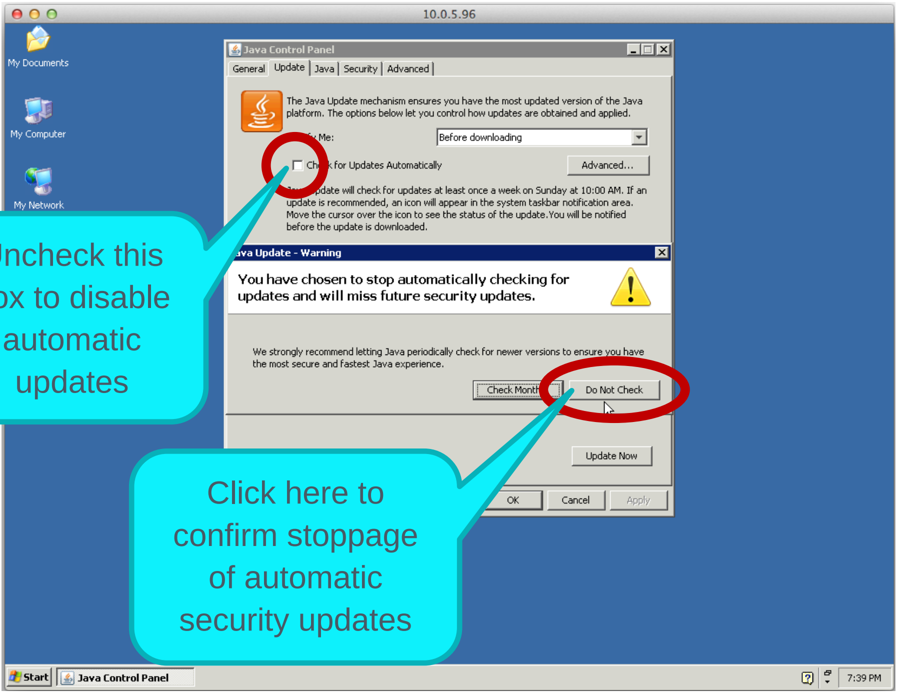
Click here to complete the installation process

Figure 35 – Java installation successful



From the Windows XP Desktop, select: Start → Programs → Java → Configure Java

Figure 36 – Configuring Java



The Java Update mechanism ensures you have the most updated version of the Java platform. The options below let you control how updates are obtained and applied.

Notify Me: Before downloading

□ Check for Updates Automatically

Java Update will check for updates at least once a week on Sunday at 10:00 AM. If an update is recommended, an icon will appear in the system taskbar notification area. Move the cursor over the icon to see the status of the update.You will be notified before the update is downloaded.

Java Update - Warning

You have chosen to stop automatically checking for updates and will miss future security updates.

We strongly recommend letting Java periodically check for newer versions to ensure you have the most secure and fastest Java experience.

Uncheck this box to disable automatic updates

Click here to confirm stoppage of automatic security updates

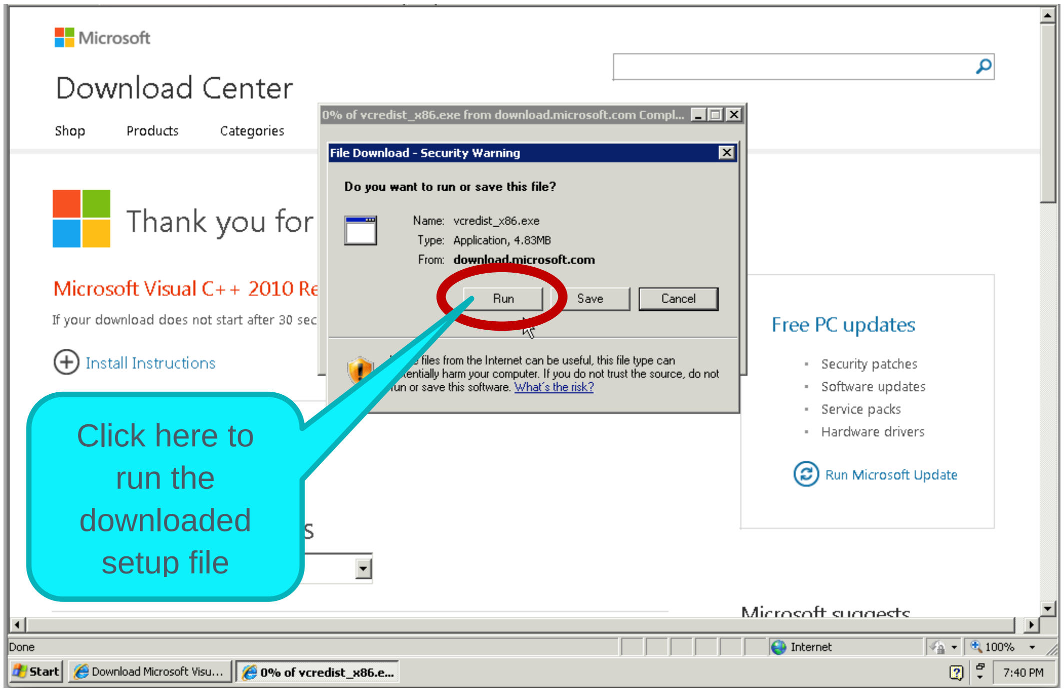
Figure 37 – Disabling Java updates

Note Download older versions from this archive: http://www.oracle.com/technetwork/java/archive-139210.html

6.11 Microsoft Visual C++ Redistributable 2010

Step 1: Download **Microsoft Visual C++ Redistributable 2010** from this address and navigate the installer.

http://www.microsoft.com/en-us/download/details.aspx?id=5555



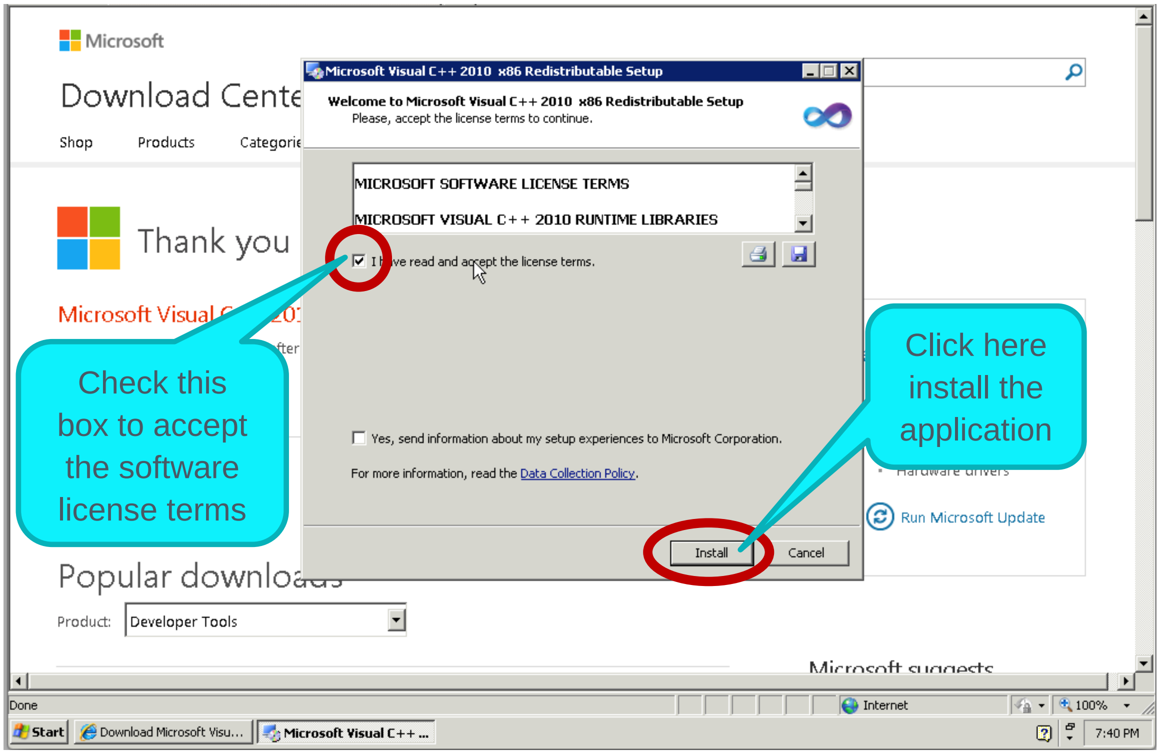
Do you want to run or save this file?

Name: vcredist_x86.exe
Type: Application, 4.83MB
From: **download.microsoft.com**

e files from the Internet can be useful, this file type can tentially harm your computer. If you do not trust the source, do not un or save this software. What's the risk?

Click here to run the downloaded setup file

Figure 38 – File Download Security Warning



Microsoft Visual C++ 2010 x86 Redistributable Setup

Welcome to Microsoft Visual C++ 2010 x86 Redistributable Setup

Please, accept the license terms to continue.

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT VISUAL C++ 2010 RUNTIME LIBRARIES

☑ I have read and accept the license terms.

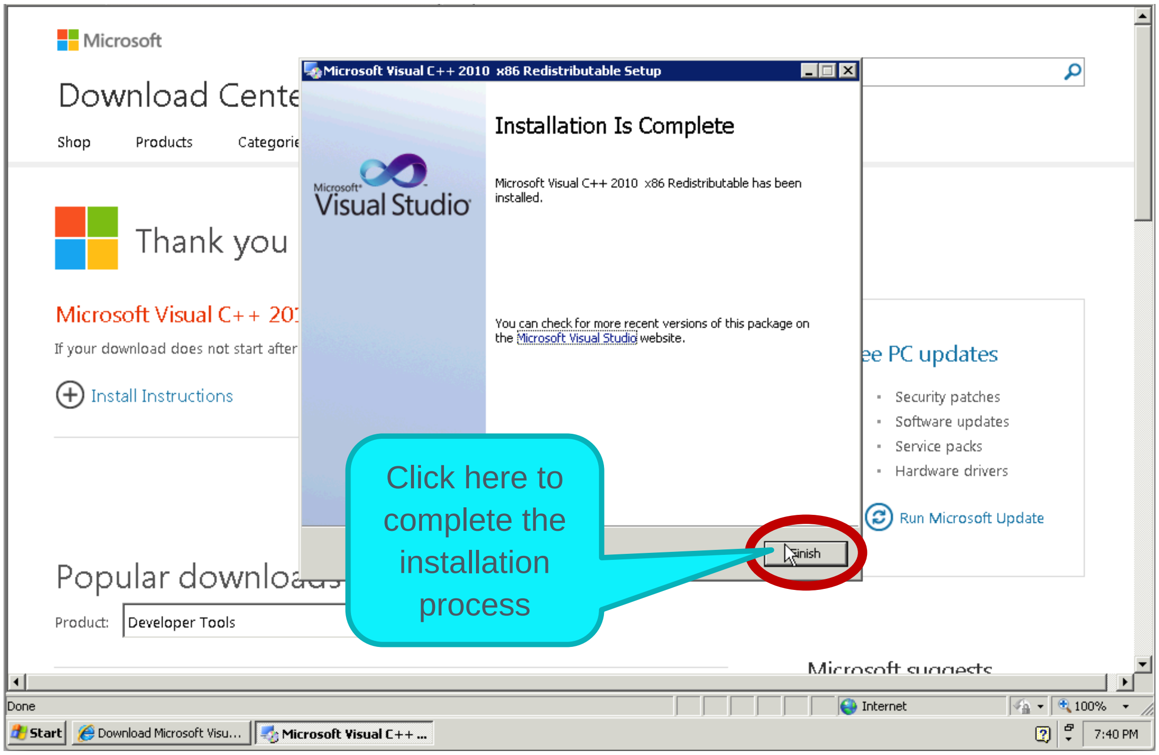
☐ Yes, send information about my setup experiences to Microsoft Corporation.

For more information, read the Data Collection Policy.

Check this box to accept the software license terms

Click here install the application

Figure 39 – Accepting the Microsoft Software License Terms



Microsoft Visual C++ 2010 x86 Redistributable Setup

Installation Is Complete

Microsoft Visual C++ 2010 x86 Redistributable has been installed.

You can check for more recent versions of this package on the Microsoft Visual Studio website.

Click here to complete the installation process

Figure 40 – Installation Complete

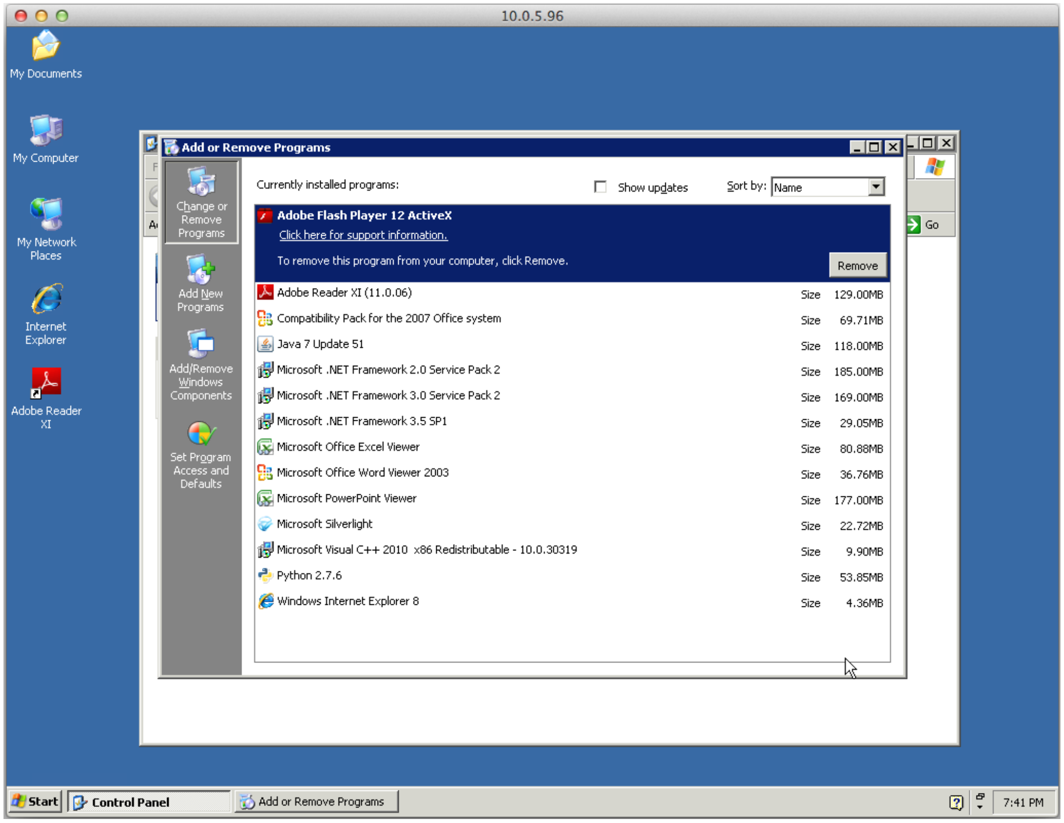
6.12 Final Enhanced Windows XP Profile

Return to the **Add or Remove Programs** window in the Windows XP **Control Panel** (see **Section 5 – Enhancing the Windows XP Profile**, Step 2) and confirm that the following programs are now installed.

- Adobe Flash Player (optional)
- Adobe Reader (optional)
- Compatibility Pack for the 2007 Office System
- Java (optional)
- Microsoft .NET Framework 2.0 Service Pack 2
- Microsoft .NET Framework 3.0 Service Pack 2
- Microsoft .NET Framework 3.5 SP1
- Microsoft Office Excel Viewer
- Microsoft Office Word Viewer 2003
- Microsoft PowerPoint Viewer
- Microsoft Silverlight
- Microsoft Visual C++ 2010 Redistributable
- Python 2.7.6
- Windows Internet Explorer 8

This configuration is the proper ending point for the base profile enhancement process.

Note Please contact your technical representative if your base profile configuration does not closely match Figure 52**.** The versions do not need to be exactly the same as depicted below, as the vendors may post newer versions online.



Currently installed programs: ☐ Show updates Sort by: Name

Adobe Flash Player 12 ActiveX
Click here for support information.
To remove this program from your computer, click Remove. Remove

Adobe Reader XI (11.0.06)	Size	129.00MB
Compatibility Pack for the 2007 Office system	Size	69.71MB
Java 7 Update 51	Size	118.00MB
Microsoft .NET Framework 2.0 Service Pack 2	Size	185.00MB
Microsoft .NET Framework 3.0 Service Pack 2	Size	169.00MB
Microsoft .NET Framework 3.5 SP1	Size	29.05MB
Microsoft Office Excel Viewer	Size	80.88MB
Microsoft Office Word Viewer 2003	Size	36.76MB
Microsoft PowerPoint Viewer	Size	177.00MB
Microsoft Silverlight	Size	22.72MB
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319	Size	9.90MB
Python 2.7.6	Size	53.85MB
Windows Internet Explorer 8	Size	4.36MB

Figure 41 – Ending configuration for the enhanced Windows XP base image

6. Enhance the Windows 7 Profile

The Malware Analysis Appliance comes with the following programs pre-installed. You may update them to the latest version if you wish to.

This section is for your information. All steps are optional.

Microsoft Visual C++ runtime 2010 Redistributable is already included.

Step 1: Inside the Windows 7 virtual machine on the **Desktop**, press the **Start** button and select **Control Panel**.

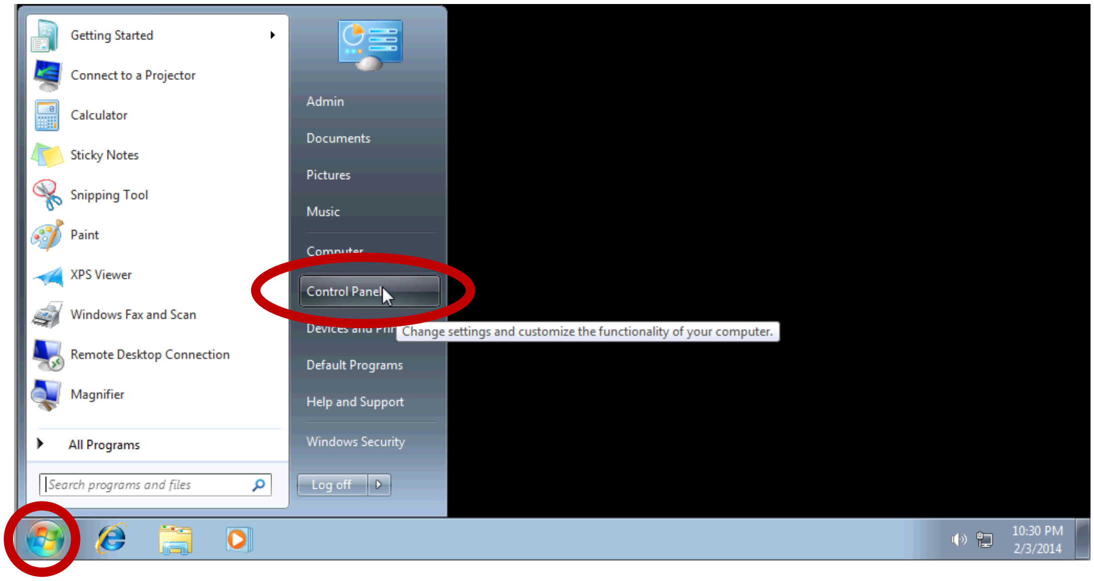


Figure 42 – Windows 7 Start Menu

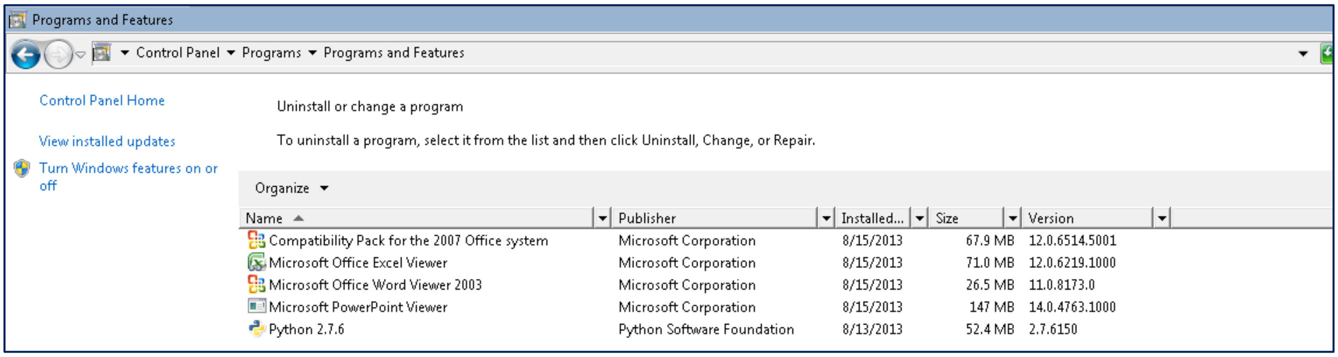
Step 2: Inside the **Control Panel**, click **Programs and Features**.

Step 3: Inside the **Programs and Features** window, confirm that the following programs are currently installed.

- Compatibility Pack for the 2007 Office System
- Microsoft Office Excel Viewer
- Microsoft Office Word Viewer 2003
- Microsoft PowerPoint Viewer
- Python 2.7.6

This configuration is the proper starting point for the Windows 7 base image enhancement process.

Note Please contact your technical representative if your base image configuration does not closely match Figure 43**.**



Programs and Features
Control Panel ▸ Programs ▸ Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Organize ▾

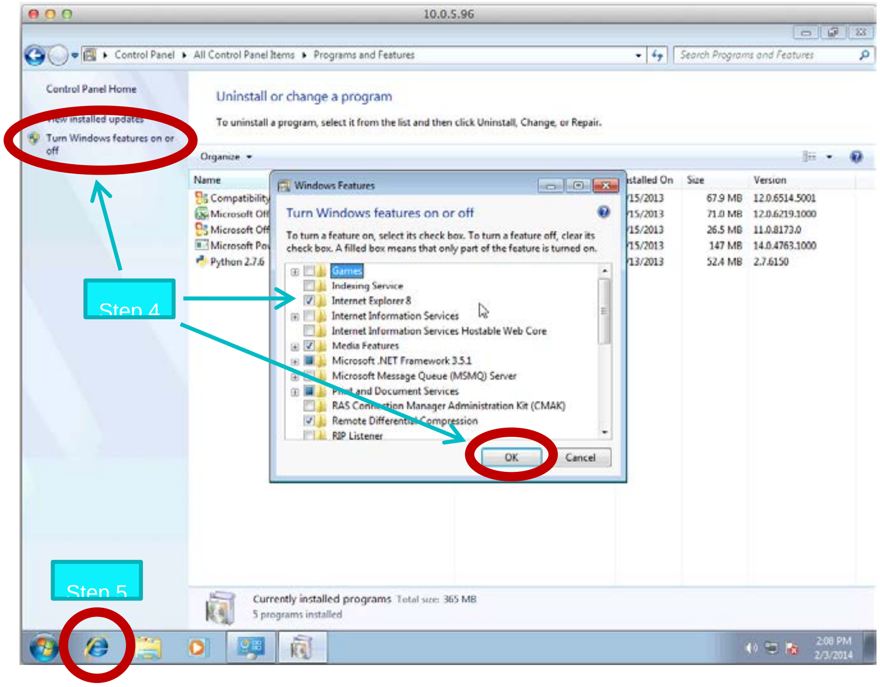
Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed...	Size	Version
Compatibility Pack for the 2007 Office system	Microsoft Corporation	8/15/2013	67.9 MB	12.0.6514.5001
Microsoft Office Excel Viewer	Microsoft Corporation	8/15/2013	71.0 MB	12.0.6219.1000
Microsoft Office Word Viewer 2003	Microsoft Corporation	8/15/2013	26.5 MB	11.0.8173.0
Microsoft PowerPoint Viewer	Microsoft Corporation	8/15/2013	147 MB	14.0.4763.1000
Python 2.7.6	Python Software Foundation	8/13/2013	52.4 MB	2.7.6150

Figure43 – Windows 7 Programs and Features displaying starting base image configuration

Step 4: Verify that **Internet Explorer** is installed and activated by clicking **Turn Windows features on or off**. Click **OK** if you needed to turn Internet Explorer on, or click **Cancel** if it was already activated.



10.0.5.96
Control Panel ▸ All Control Panel Items ▸ Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Organize ▾
Windows Features
Sten 4
Sten 5
OK
Cancel
2:08 PM
2/3/2014

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Installed On	Size	Version
Compatibility	/15/2013	67.9 MB	12.0.6514.5001
Microsoft Off	/15/2013	71.0 MB	12.0.6219.1000
Microsoft Off	/15/2013	26.5 MB	11.0.8173.0
Microsoft Po	/15/2013	147 MB	14.0.4763.1000
Python 2.7.6	/13/2013	52.4 MB	2.7.6150

Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ☐ Games
- ☐ Indexing Service
- ☑ Internet Explorer 8
- ☐ Internet Information Services
- ☐ Internet Information Services Hostable Web Core
- ☑ Media Features
- ■ Microsoft .NET Framework 3.5.1
- ☐ Microsoft Message Queue (MSMQ) Server
- ■ Print and Document Services
- ☐ RAS Connection Manager Administration Kit (CMAK)
- ☑ Remote Differential Compression
- ☐ RIP Listener

Currently installed programs Total size: 365 MB
5 programs installed

Figure 44

Step 5: Click the **Internet Explorer** icon on the Windows 7 **Taskbar** to open the Web browser.

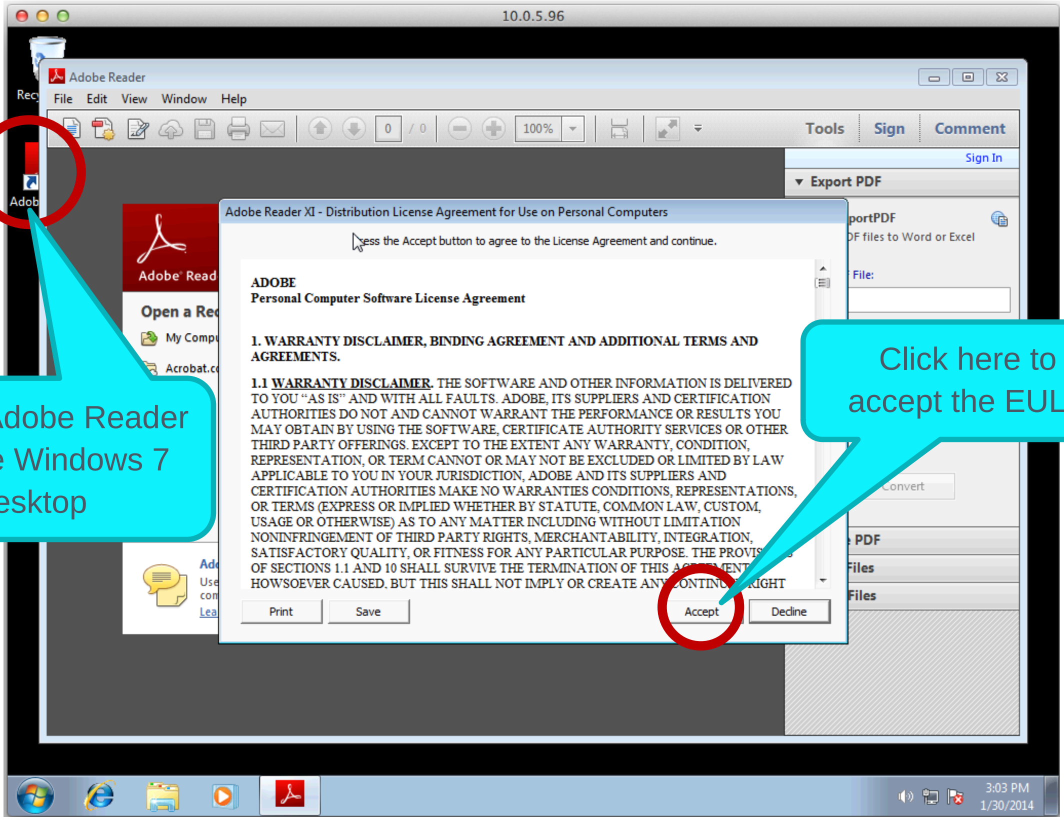
Note **Sections 6.1** through **6.6** all take place through the Internet Explorer Web browser interface.

6.13 Adobe Reader

Installing Adobe Reader is optional.

Step 1: Download **Adobe Reader** from the following address and navigate the installer as required; decline the **Optional Offer**, and click **Install Now**.

http://get.adobe.com/reader/



Adobe Reader XI - Distribution License Agreement for Use on Personal Computers

ess the Accept button to agree to the License Agreement and continue.

ADOBE
Personal Computer Software License Agreement

1. WARRANTY DISCLAIMER, BINDING AGREEMENT AND ADDITIONAL TERMS AND AGREEMENTS.

1.1 WARRANTY DISCLAIMER. THE SOFTWARE AND OTHER INFORMATION IS DELIVERED TO YOU "AS IS" AND WITH ALL FAULTS. ADOBE, ITS SUPPLIERS AND CERTIFICATION AUTHORITIES DO NOT AND CANNOT WARRANT THE PERFORMANCE OR RESULTS YOU MAY OBTAIN BY USING THE SOFTWARE, CERTIFICATE AUTHORITY SERVICES OR OTHER THIRD PARTY OFFERINGS. EXCEPT TO THE EXTENT ANY WARRANTY, CONDITION, REPRESENTATION, OR TERM CANNOT OR MAY NOT BE EXCLUDED OR LIMITED BY LAW APPLICABLE TO YOU IN YOUR JURISDICTION, ADOBE AND ITS SUPPLIERS AND CERTIFICATION AUTHORITIES MAKE NO WARRANTIES CONDITIONS, REPRESENTATIONS, OR TERMS (EXPRESS OR IMPLIED WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING WITHOUT LIMITATION NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, INTEGRATION, SATISFACTORY QUALITY, OR FITNESS FOR ANY PARTICULAR PURPOSE. THE PROVIS OF SECTIONS 1.1 AND 10 SHALL SURVIVE THE TERMINATION OF THIS A ENT HOWSOEVER CAUSED. BUT THIS SHALL NOT IMPLY OR CREATE ANY CONTINU RIGHT

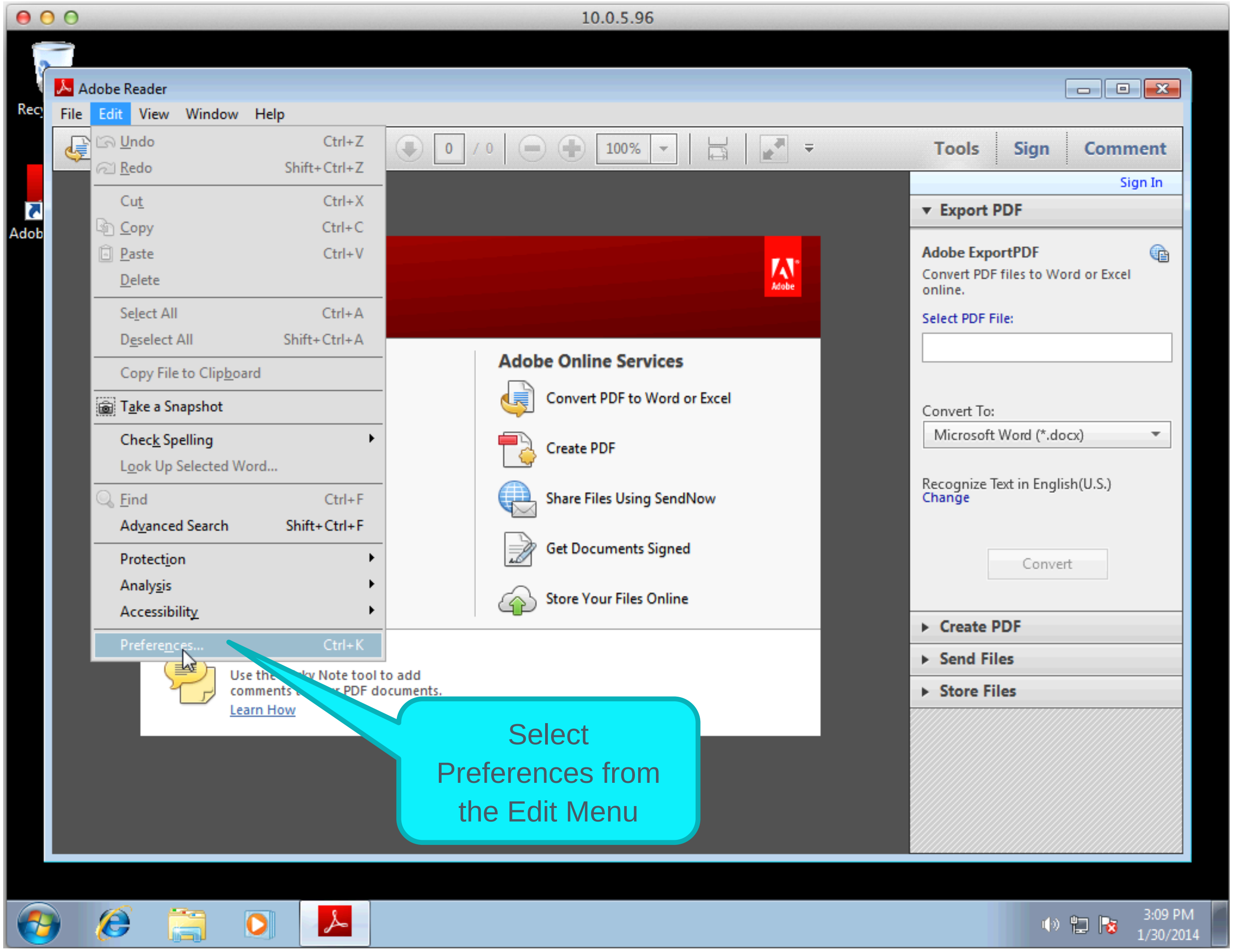
Figure 45 – Accepting the Adobe Reader End User License Agreement

Step 2: When the installation is complete, run the **Adobe Reader** application from the Desktop and accept the End User License Agreement (EULA). The EULA appears automatically upon the first launch of the application.

Note The IntelliVMs will be unable to utilize Adobe Reader properly until the EULA has been accepted.

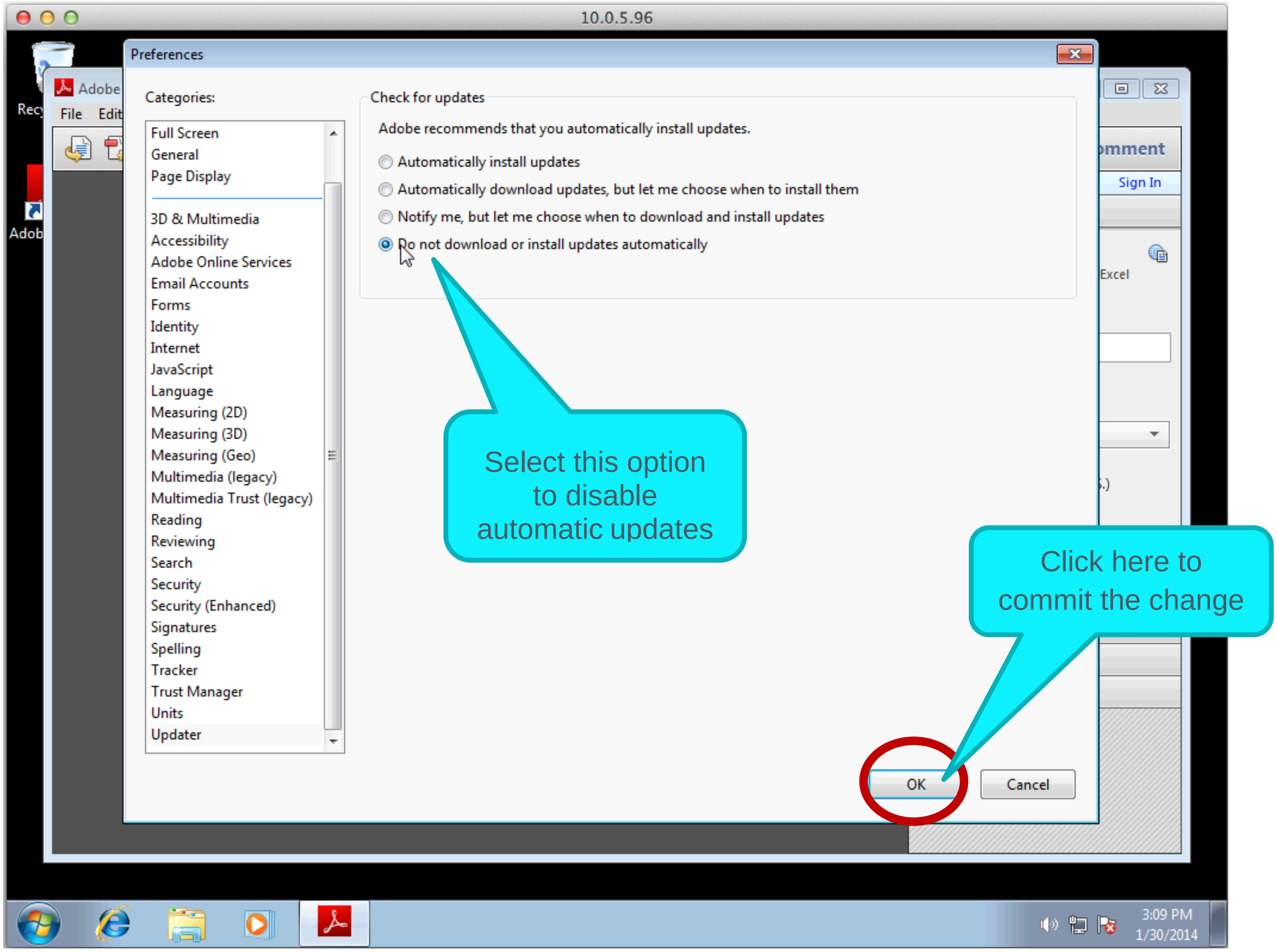
Step 3: Turn off automatic updates. From the **Edit** menu, select **Preferences**.

Note Updates are valuable for improving security and beneficial for the malware detection process, however it is essential that the MALWARE ANALYSIS APPLIANCE system administrator apply all updates *manually* so as to maintain configuration control over the malware testbed at all times. If components were to be allowed to update themselves automatically at random intervals, then configuration control becomes impractical and the administrator is never quite sure what versions of which components are being used for malware testing.



Select Preferences from the Edit Menu

Figure 46 – Opening the Preferences screen



Preferences

Categories:

Check for updates

Adobe recommends that you automatically install updates.

○ Automatically install updates
○ Automatically download updates, but let me choose when to install them
○ Notify me, but let me choose when to download and install updates
● Do not download or install updates automatically

Select this option to disable automatic updates

Click here to commit the change

Figure 47 – Disabling automatic updates from the Preferences screen

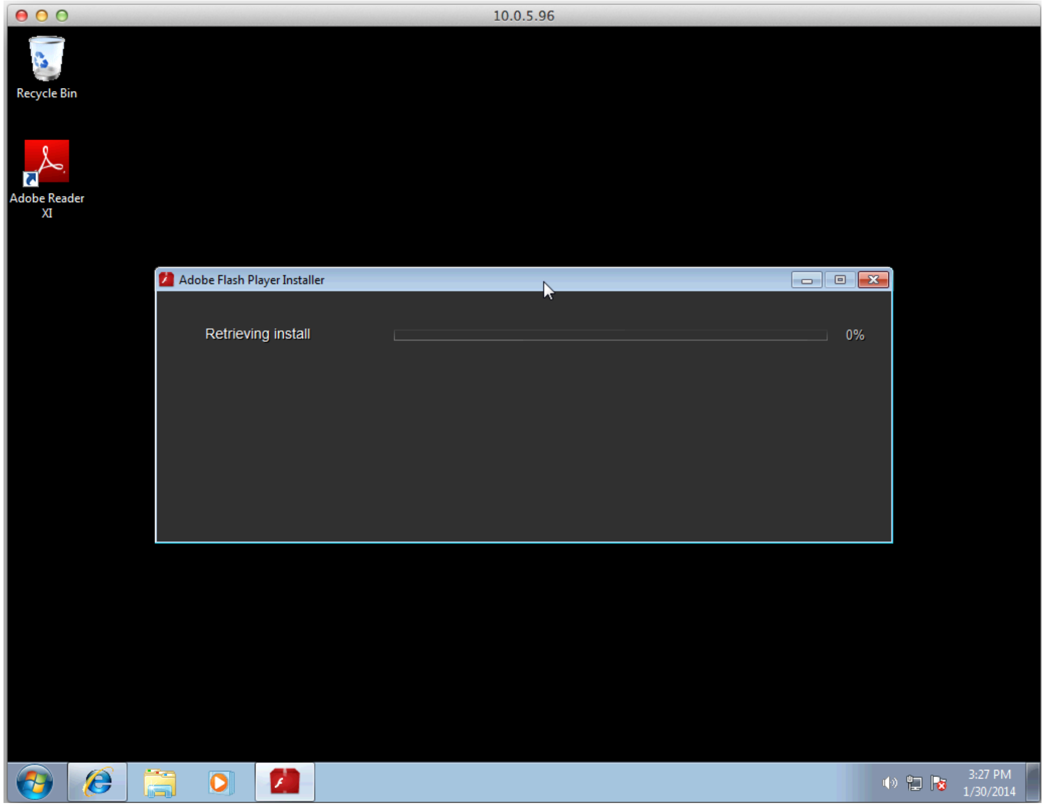
Note Additional Adobe Reader versions: https://get.adobe.com/uk/reader/otherversions/.

6.14 Adobe Flash

Installing Adobe Flash is optional.

Step 1: Download **Adobe Flash** from the following address and navigate the installer as required; decline the **Optional Offer**, and click **Install Now**.

http://get.adobe.com/flashplayer/

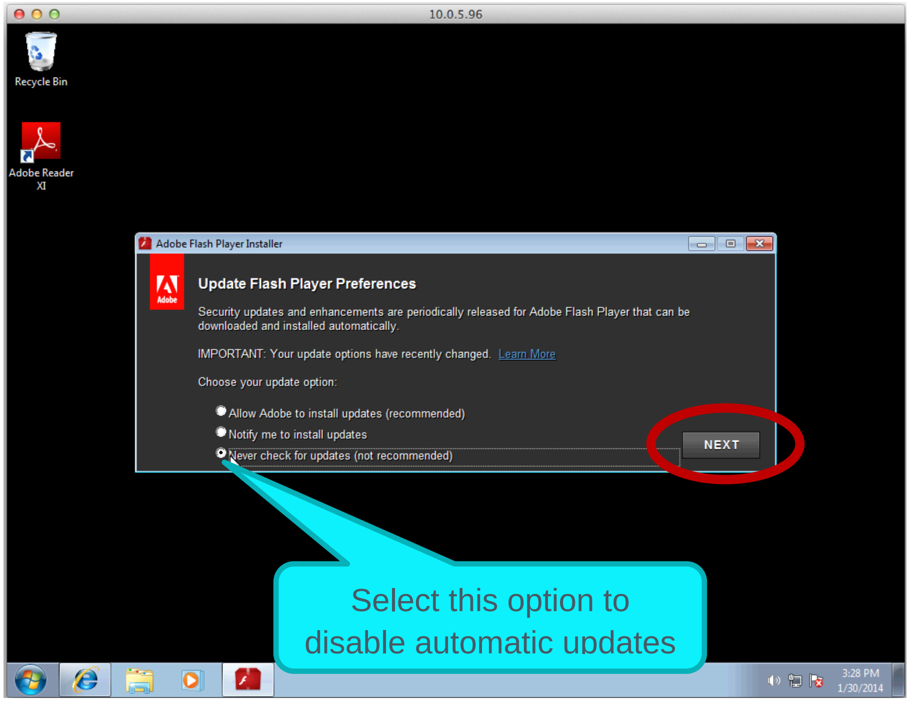


Retrieving install 0%

Figure 48 – Retrieving Adobe Flash Player Installer

Step 2: If prompted to **Update Flash Play Preferences** during installation, select the following option:

- Never check for updates (not recommended).



Update Flash Player Preferences

Security updates and enhancements are periodically released for Adobe Flash Player that can be downloaded and installed automatically.

IMPORTANT: Your update options have recently changed. Learn More

Choose your update option:

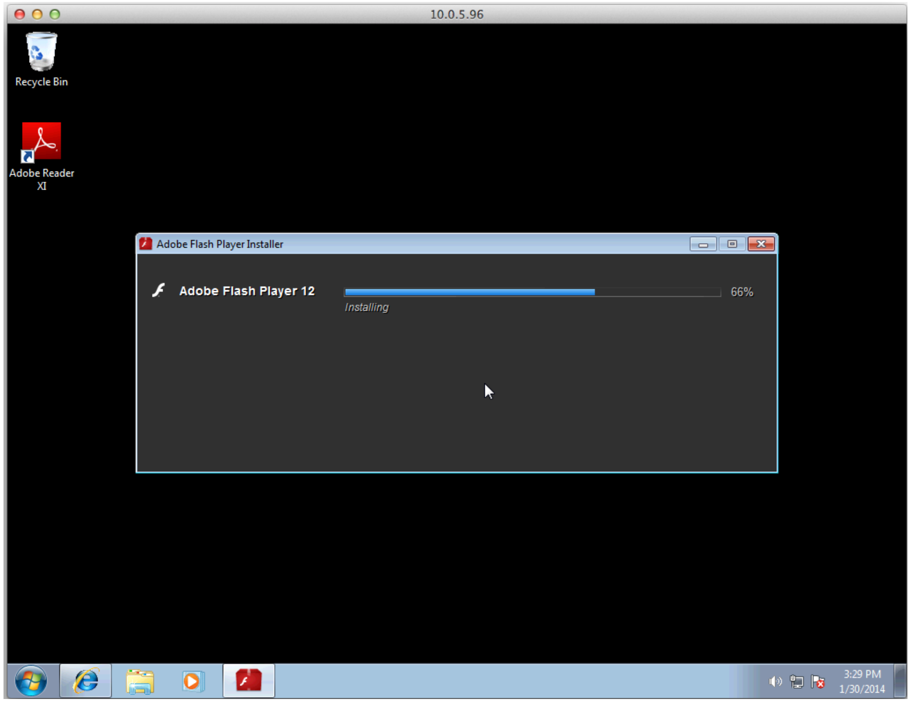
○ Allow Adobe to install updates (recommended)

○ Notify me to install updates

● Never check for updates (not recommended)

Select this option to disable automatic updates

Figure 49 – Update Flash Player Preferences



Adobe Flash Player 12 66%
Installing

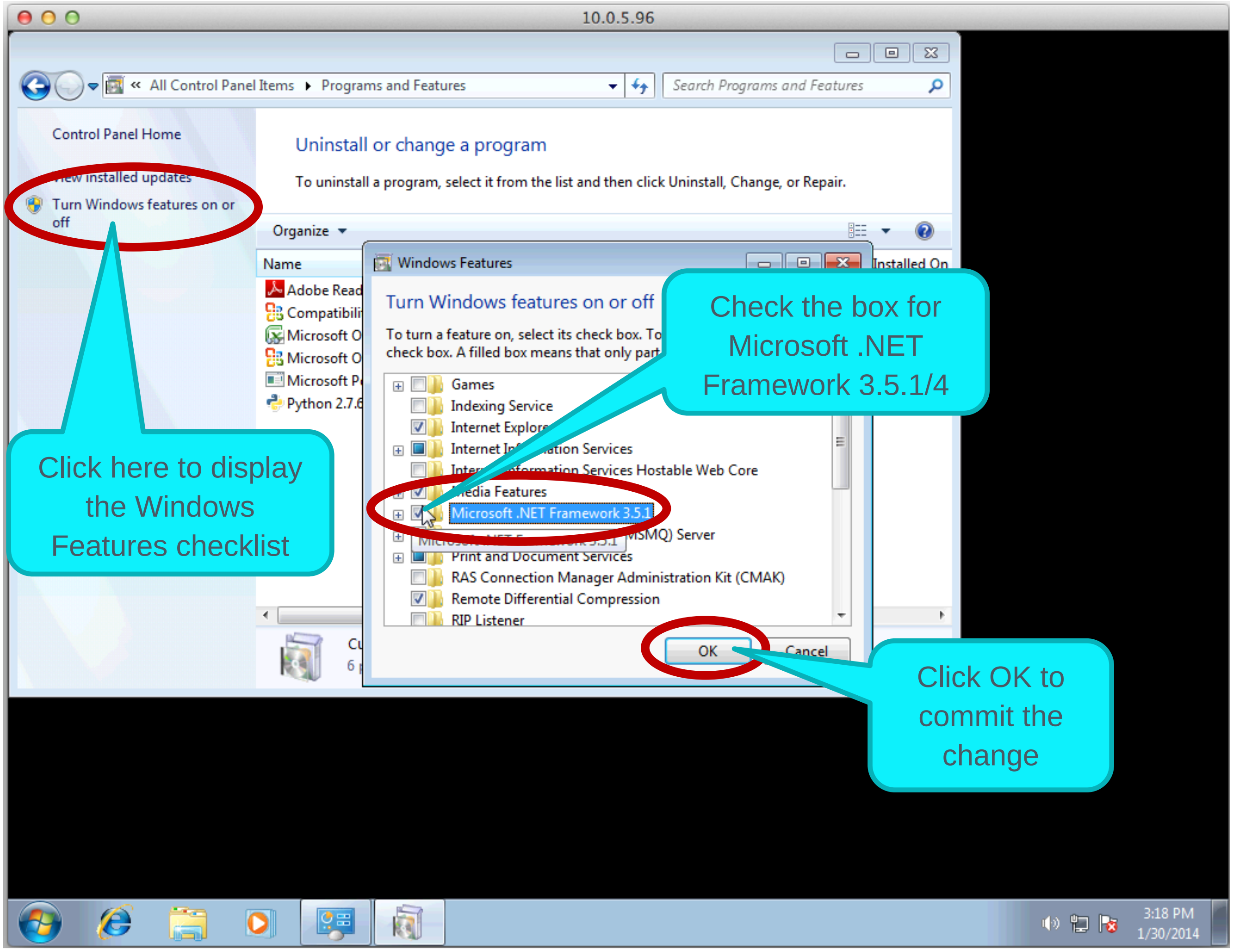
Figure 50 – Installing Adobe Flash Player

Note Additional Adobe Flash versions: http://helpx.adobe.com/flash-player/kb/archived-flash-player-versions.html.

6.15 Microsoft .NET Framework 3.5 SP1

On Windows 7 .NET is part of the operating system and can be enabled under **Programs and Features**.

Note EMET requires .NET 4.5. Install the correct version for your applications.



Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Turn Windows features on or off

To turn a feature on, select its check box. To
check box. A filled box means that only part

- □ Games
- □ Indexing Service
- ☑ Internet Explore
- ■ Internet Information Services
- □ Internet Information Services Hostable Web Core
- ☑ Media Features
- ☑ Microsoft .NET Framework 3.5.1
- MSMQ) Server
- ■ Print and Document Services
- □ RAS Connection Manager Administration Kit (CMAK)
- ☑ Remote Differential Compression
- □ RIP Listener

Click here to display the Windows Features checklist

Check the box for Microsoft .NET Framework 3.5.1/4

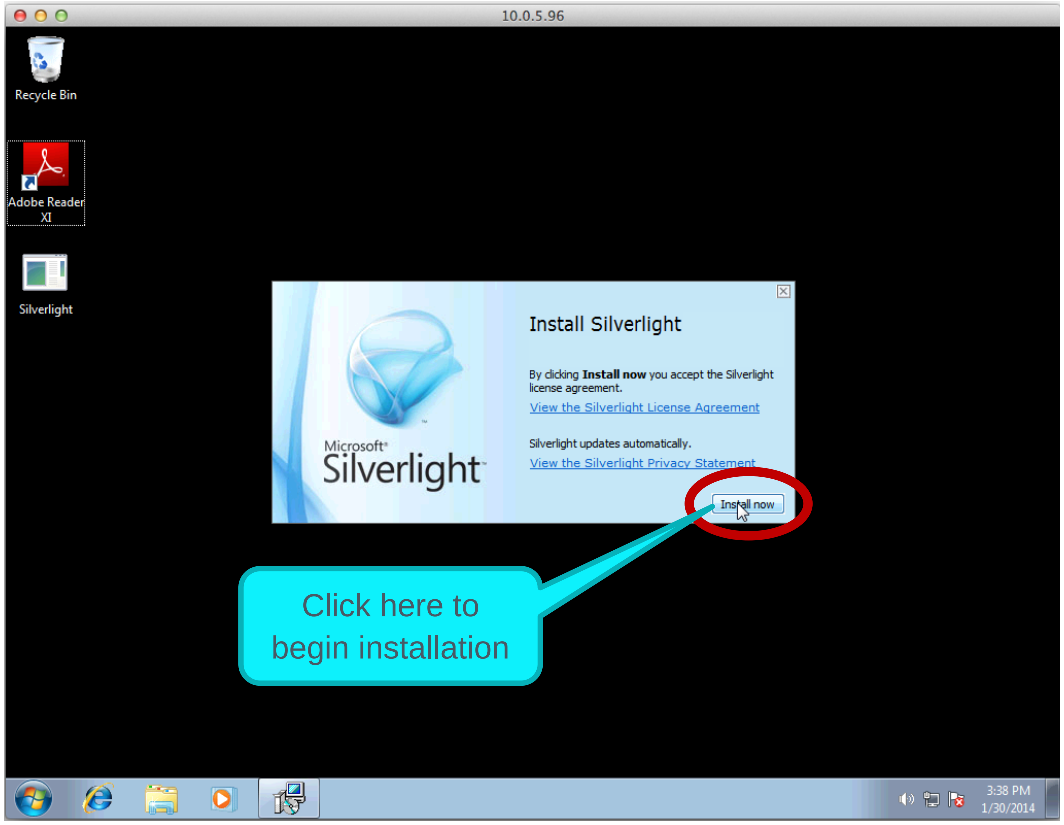
Click OK to commit the change

Figure 51 – Turning on Microsoft .NET Framework 3.5.1 or 4 from the Windows Features checklist

6.16 Microsoft Silverlight

Step 1: Download **Microsoft Silverlight** from this address and navigate the installer as required.

http://www.microsoft.com/silverlight/



Install Silverlight

By clicking **Install now** you accept the Silverlight license agreement.

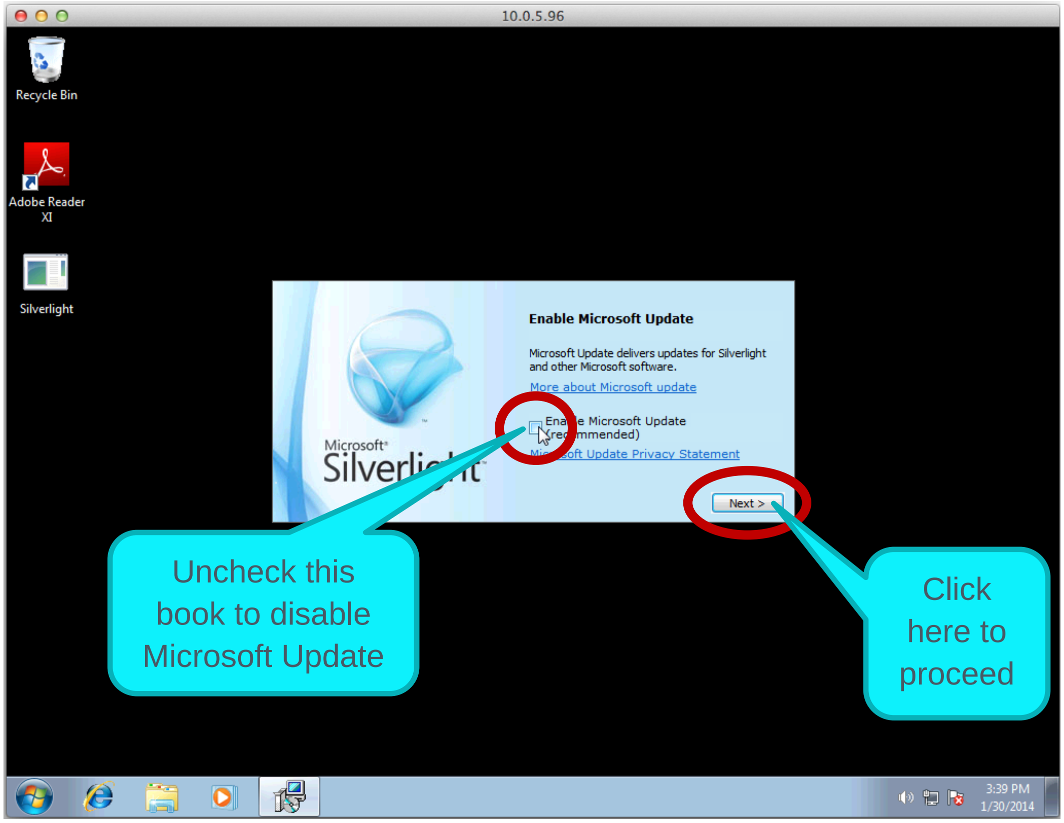
View the Silverlight License Agreement

Silverlight updates automatically.

View the Silverlight Privacy Statement

Click here to begin installation

Figure 52 – Preparing to install Silverlight



10.0.5.96

Enable Microsoft Update

Microsoft Update delivers updates for Silverlight and other Microsoft software.

More about Microsoft update

□ Enable Microsoft Update (recommended)

Microsoft Update Privacy Statement

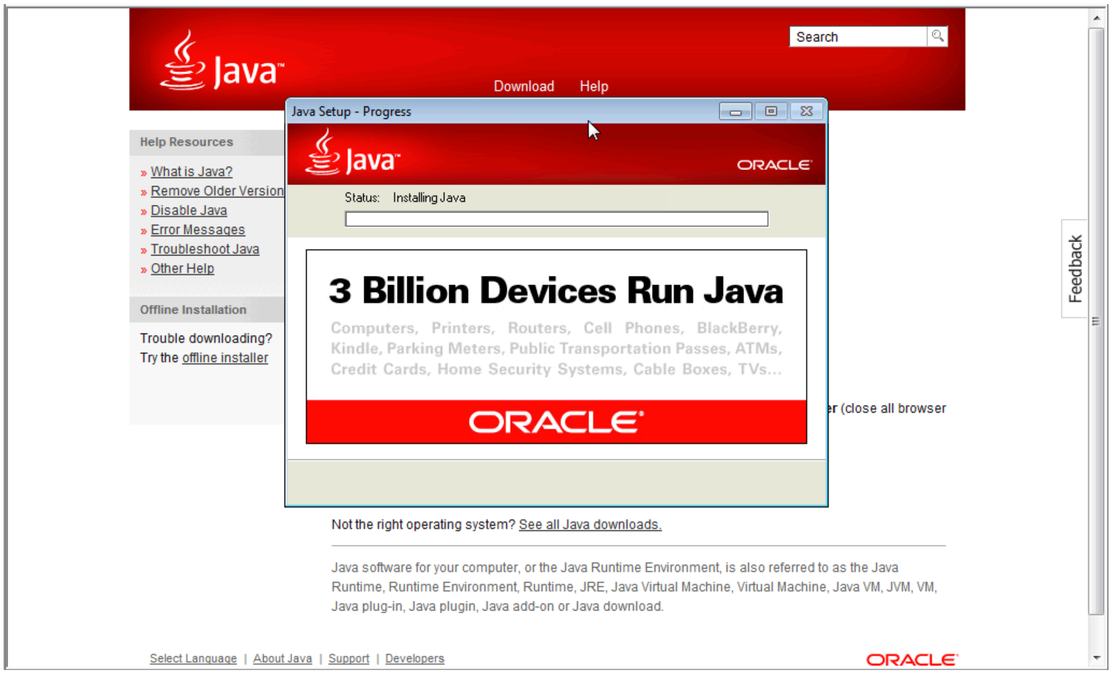
Figure 53 – Disabling automatic Microsoft Updates

6.17 Java

Installing Java is optional.

Step 1: Download **Java** from the address below and navigate to the installer as required.

http://java.com/en/download/index.jsp



Trouble downloading? Try the offline installer

Status: Installing Java

3 Billion Devices Run Java

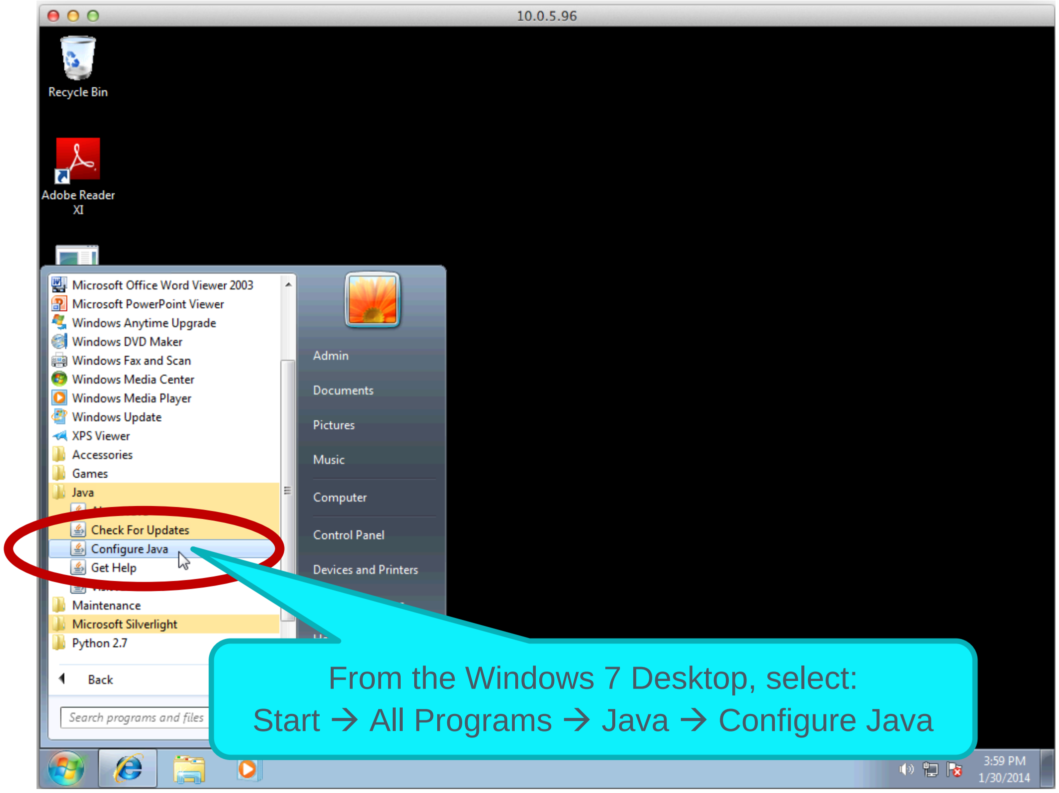
Computers, Printers, Routers, Cell Phones, BlackBerry, Kindle, Parking Meters, Public Transportation Passes, ATMs, Credit Cards, Home Security Systems, Cable Boxes, TVs…

r (close all browser

Not the right operating system? See all Java downloads.

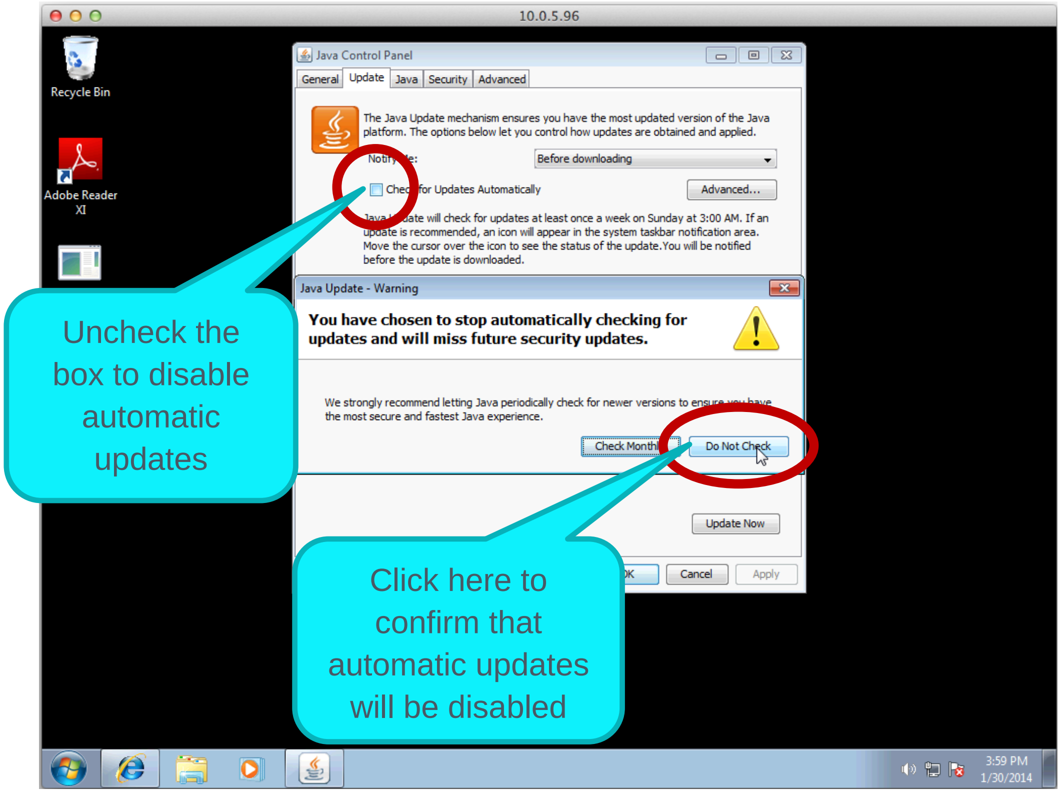
Java software for your computer, or the Java Runtime Environment, is also referred to as the Java Runtime, Java Runtime Environment, Runtime, JRE, Java Virtual Machine, Virtual Machine, Java VM, JVM, VM, Java plug-in, Java plugin, Java add-on or Java download.

Figure 54 – Installing Java



From the Windows 7 Desktop, select:
Start → All Programs → Java → Configure Java

Figure 55 – Configuring Java



The Java Update mechanism ensures you have the most updated version of the Java platform. The options below let you control how updates are obtained and applied.

Notify Me: Before downloading

□ Check for Updates Automatically

Java Update will check for updates at least once a week on Sunday at 3:00 AM. If an update is recommended, an icon will appear in the system taskbar notification area. Move the cursor over the icon to see the status of the update.You will be notified before the update is downloaded.

You have chosen to stop automatically checking for updates and will miss future security updates.

We strongly recommend letting Java periodically check for newer versions to ensure you have the most secure and fastest Java experience.

Uncheck the box to disable automatic updates

Click here to confirm that automatic updates will be disabled

Figure 56 – Disabling automatic Java updates

Note Download older versions from this archive: http://www.oracle.com/technetwork/java/archive-139210.html

6.6 Detect Unknown Exploits with EMET

In the Malware Analysis appliance, the Microsoft® Enhanced Mitigation Experience Toolkit (EMET) detects unknown exploits. For the InteliVM to be able to collect EMET events, EMET must be installed in a Windows 7 or 8 profile, and properly configured. This feature is strongly recommended, but optional.

Note Blue Coat recommends that you first deploy EMET on a new profile to verify that it works as expected.

Step 1: Create a new Windows 7 (or Windows 8) profile. EMET is not supported on Windows XP.

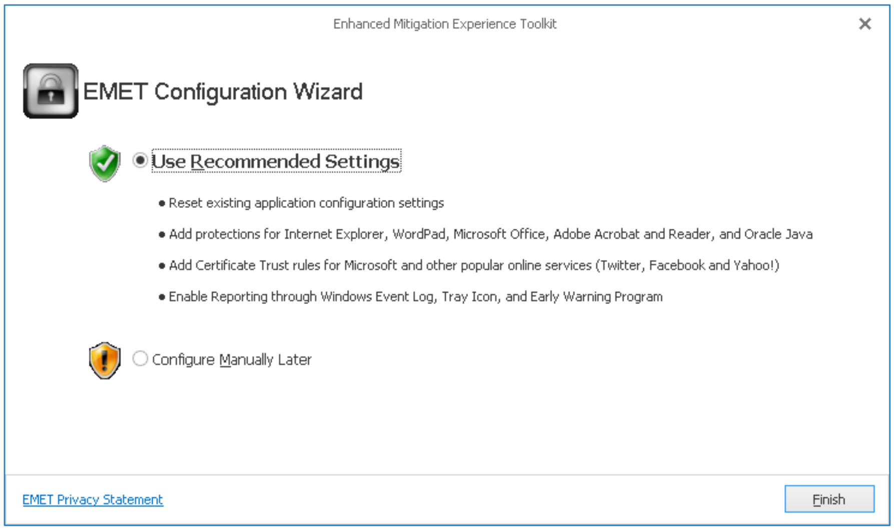
Step 2: Customize the profile, then log on using RDP.

Step 3: Download and install .NET Framework 4.5 on the iVM profile.

Note For EMET to work with Internet Explorer 10 on Windows 8, Microsoft KB 2790907 or a more recent version of the Compatibility Update for Windows 8 must be installed.

Step 4: Download EMET 5.5 and the user-guide PDF from Microsoft at: https://download.microsoft.com/download/8/E/E/8EEFD9FC-46B1-4A8B-9B5D-13B4365F8CA0/EMET%20Setup.msi , and begin the installation.

Step 5: On the *EMET Configuration Wizard* page, select **Use Recommended Settings,** and click **Finish**.



Enhanced Mitigation Experience Toolkit

EMET Configuration Wizard

● Use Recommended Settings

- Reset existing application configuration settings
- Add protections for Internet Explorer, WordPad, Microsoft Office, Adobe Acrobat and Reader, and Oracle Java
- Add Certificate Trust rules for Microsoft and other popular online services (Twitter, Facebook and Yahoo!)
- Enable Reporting through Windows Event Log, Tray Icon, and Early Warning Program

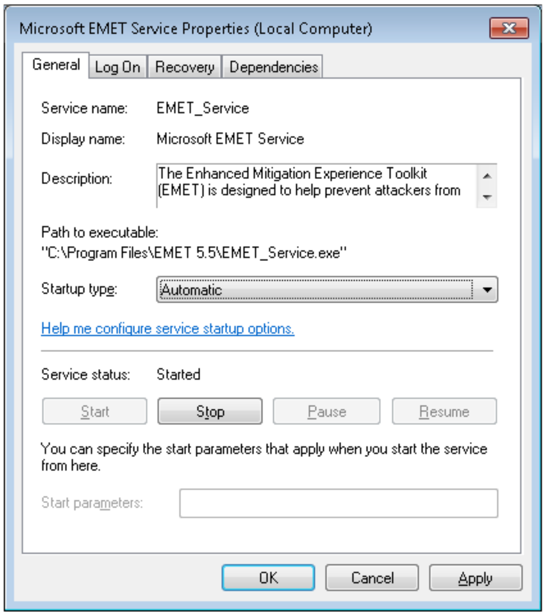
○ Configure Manually Later

Figure 57 – EMET Wizard

Step 6: Configure the EMET service to start automatically with no delay. Follow these steps:

1. Click **Start,** and search for services.msc.
2. Right click the service name, and select **Properties**.

3. Change the **Startup Type** to **Automatic**.



Microsoft EMET Service Properties (Local Computer)

Service name: EMET_Service

Display name: Microsoft EMET Service

Description: The Enhanced Mitigation Experience Toolkit (EMET) is designed to help prevent attackers from

Path to executable:
"C:\Program Files\EMET 5.5\EMET_Service.exe"

Startup type: Automatic

Help me configure service startup options.

Service status: Started

You can specify the start parameters that apply when you start the service from here.

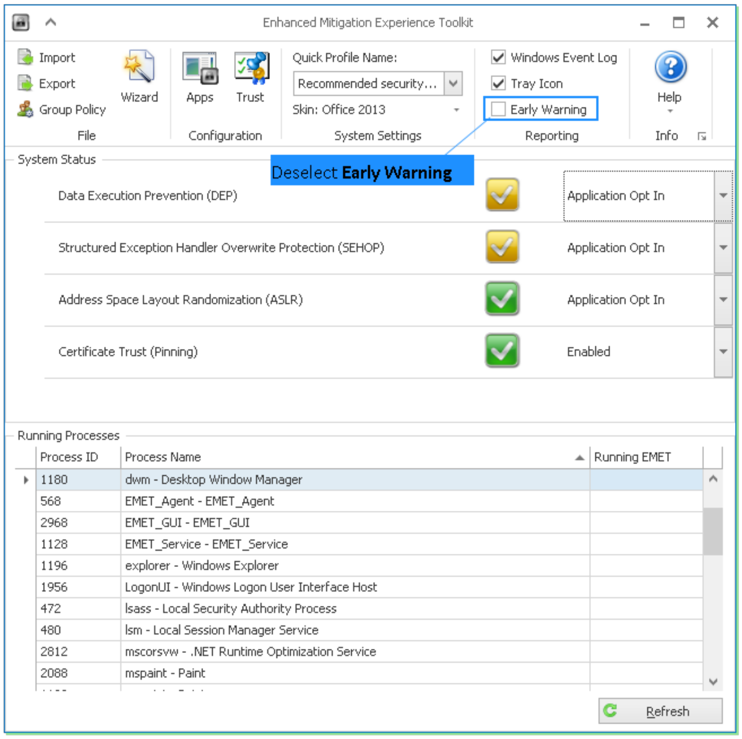
Start parameters:

Figure 58 – Set Startup Type to Automatic

The following optional steps further enhance the EMET configuration.

A: Open the EMET GUI and configure it.

1. Uncheck the **Early Warning option** on the **Enhanced Mitigation Experience Toolkit** window, if you don't want information related to an exploitation attempt to be sent to Microsoft through the standard Windows Error Reporting channel.



Enhanced Mitigation Experience Toolkit

☑ Windows Event Log
☑ Tray Icon
□ Early Warning
Reporting

Deselect **Early Warning**

System Status

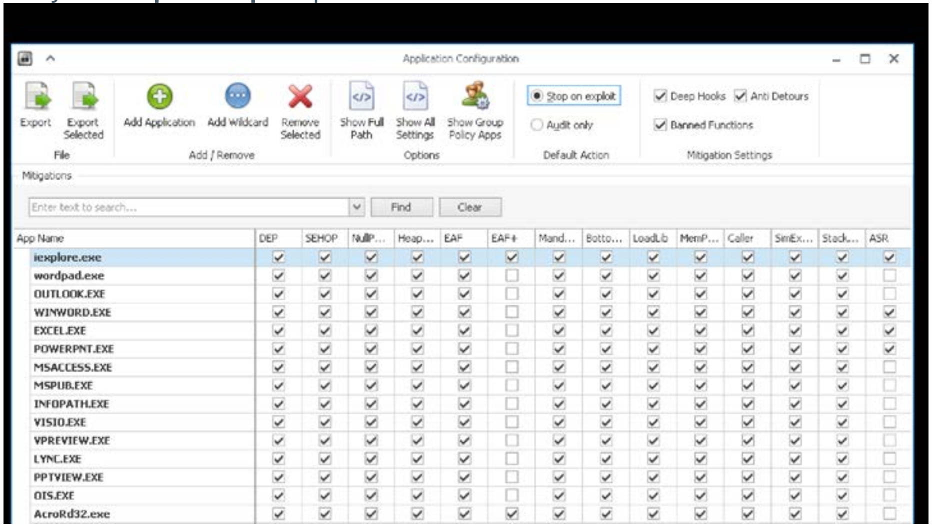
Data Execution Prevention (DEP)	✓	Application Opt In
Structured Exception Handler Overwrite Protection (SEHOP)	✓	Application Opt In
Address Space Layout Randomization (ASLR)	✓	Application Opt In
Certificate Trust (Pinning)	✓	Enabled

Running Processes

Process ID	Process Name	Running EMET
1180	dwm - Desktop Window Manager	
568	EMET_Agent - EMET_Agent	
2968	EMET_GUI - EMET_GUI	
1128	EMET_Service - EMET_Service	
1196	explorer - Windows Explorer	
1956	LogonUI - Windows Logon User Interface Host	
472	lsass - Local Security Authority Process	
480	lsm - Local Session Manager Service	
2812	mscorsvw - .NET Runtime Optimization Service	
2088	mspaint - Paint	

Figure 59 – Deselect Early Warning

2. Click **Apps** in the upper menu bar to open the configuration window.
3. Set your **Stop on Exploit** preference.



Default Action: ● Stop on exploit ○ Audit only

Mitigation Settings: ☑ Deep Hooks ☑ Anti Detours ☑ Banned Functions

Mitigations

Enter text to search...

App Name	DEP	SEHOP	NullP...	Heap...	EAF	EAF+	Mand...	Botto...	LoadLib	MemP...	Caller	SimEx...	Stack...	ASR
iexplore.exe	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
wordpad.exe	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□
OUTLOOK.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□
WINWORD.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	☑
EXCEL.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	☑
POWERPNT.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	☑
MSACCESS.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□
MSPUB.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□
INFOPATH.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□
VISIO.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□
VPREVIEW.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□
LYNC.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□
PPTVIEW.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□
OIS.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□
AcroRd32.exe	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	□

Figure 60 – Configure Stop on exploit

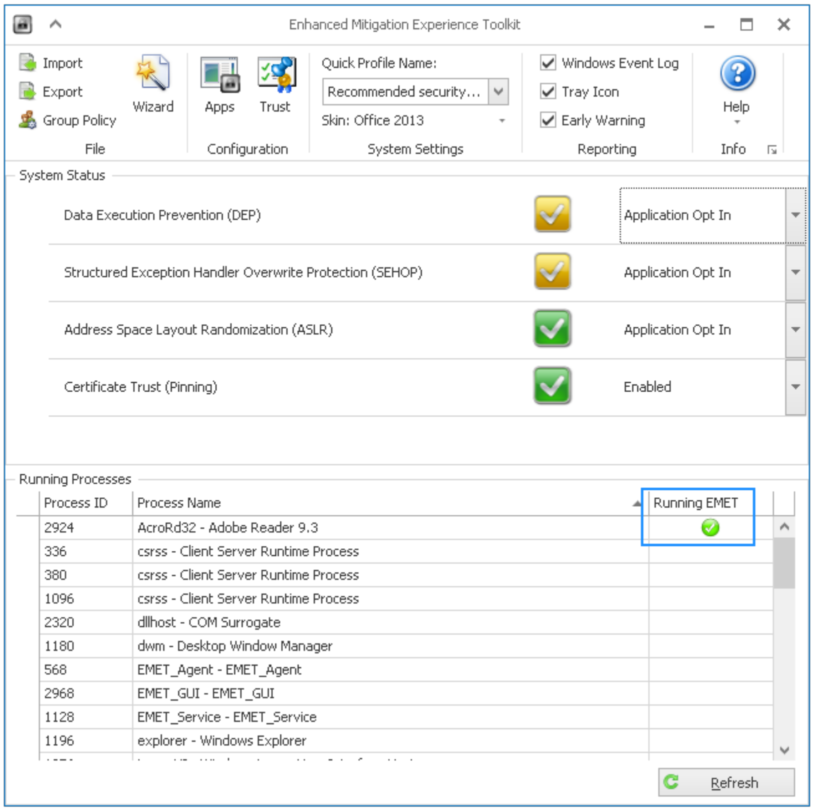
- By default EMET is set to the **Default Action Stop on exploit**. This is the recommended setting for *maximizing detection*. However, this may not give you all the details about the attack, including second stage malware information. Blue Coat recommends maintaining this choice for maximum detection and with simpler configurations.
- For full attack information (and a minimal reduction in exploit detection), select **Audit only**. This will let the exploit continue as long as possible, only observing. This results in significantly more information about consecutive stages of the attack.

4. Remove any applications you don't want to monitor, if necessary. When the **Use Recommended Settings** selection is made during installation, EMET adds and configures a set of popular applications. Click **Remove Selected** when you have highlighted an application in order to remove it.
5. If necessary, add a new application, highlight it in the list, and enable all mitigations for that application (unless otherwise advised).

Note Some mitigations are not compatible with certain applications. Blue Coat recommends referring to the following link to verify your settings, and then to deselect any incompatible mitigations: https://support.microsoft.com/kb/2909257.

6. Click **OK** to return to the EMET Toolkit main window.

B: Start the configured applications, then click **Refresh** in the EMET GUI, and verify you see a green check mark in the **Running EMET** column.



Quick Profile Name: Recommended security...

Skin: Office 2013

☑ Windows Event Log

☑ Tray Icon

☑ Early Warning

System Status

Data Execution Prevention (DEP)	✓	Application Opt In
Structured Exception Handler Overwrite Protection (SEHOP)	✓	Application Opt In
Address Space Layout Randomization (ASLR)	✓	Application Opt In
Certificate Trust (Pinning)	✓	Enabled

Running Processes

Process ID	Process Name	Running EMET
2924	AcroRd32 - Adobe Reader 9.3	✓
336	csrss - Client Server Runtime Process	
380	csrss - Client Server Runtime Process	
1096	csrss - Client Server Runtime Process	
2320	dllhost - COM Surrogate	
1180	dwm - Desktop Window Manager	
568	EMET_Agent - EMET_Agent	
2968	EMET_GUI - EMET_GUI	
1128	EMET_Service - EMET_Service	
1196	explorer - Windows Explorer	

Figure 61 – EMET is running

Step 7: Close all applications, close the remote desktop session, then build the profile.

Step 8: Verify that EMET works by running samples which will trigger EMET. The following MD5 is for reference; Blue Coat is unable to provide the samples, as they are malicisous. They are available on VirusTotal.

- C32AD4D6F6A00C85E6BD152852D5D09F (SimExecFlow, and StackPivot)

6.7 Final Enhanced Windows 7 Profile

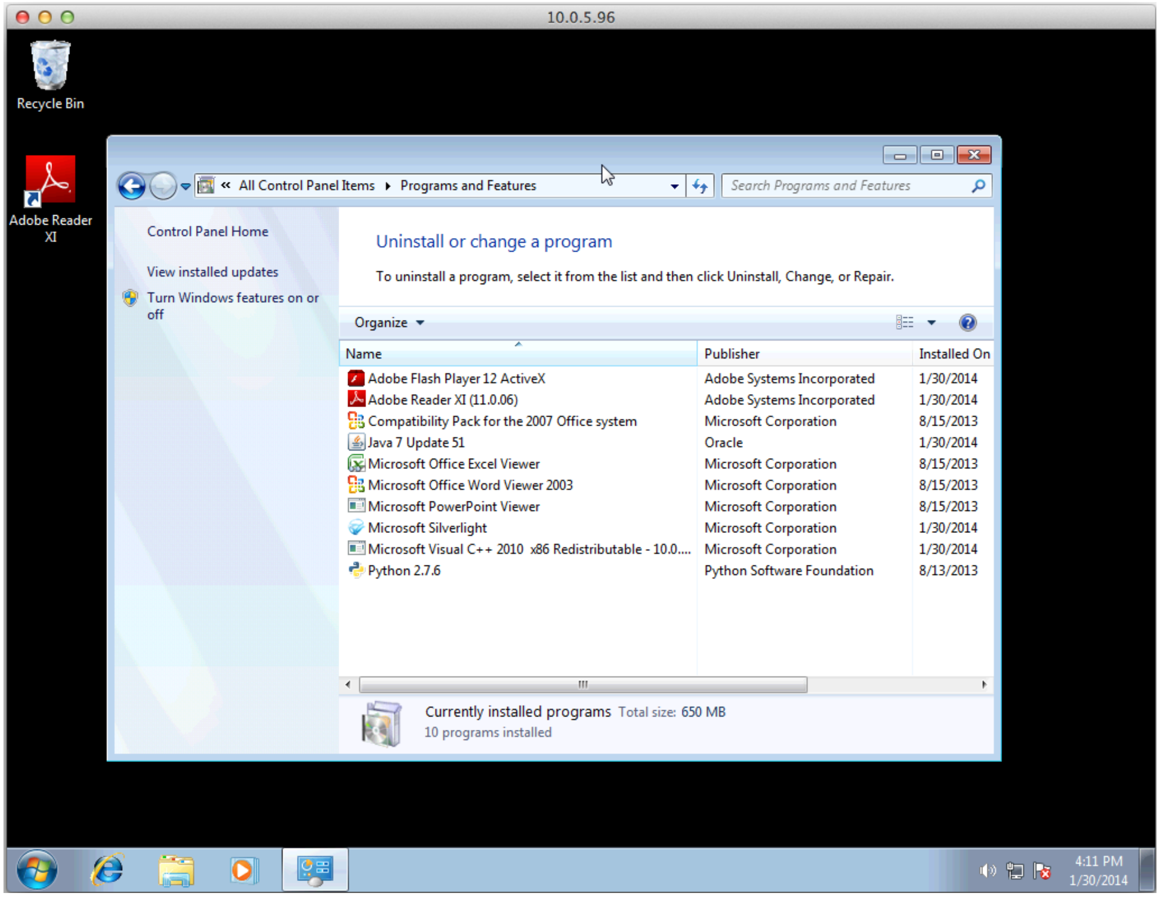
Return to the **Add or Remove Programs** window in the Windows 7 **Control Panel** (see **Section 6 – Enhancing the Windows 7 Profile**, Step 2) and confirm that the following programs are now installed.

- Adobe Flash Player (optional)
- Adobe Reader (optional)
- Compatibility Pack for the 2007 Office System
- Java (optional)
- Microsoft Office Excel Viewer
- Microsoft Office Word Viewer 2003
- Microsoft PowerPoint Viewer
- Microsoft Silverlight
- Python 2.7.6
- EMET 5.5 (strongly recommended, optional)

This configuration is the proper ending point for the base profile enhancement process.

Reminder: Microsoft .NET and Internet Explorer can be viewed from the **Windows Features** checklist in Windows 7.

Note Please contact your technical representative if your base profile configuration does not closely match Figure 62**.** The versions do not need to be exactly the same as depicted below, as the vendors may post newer versions online.


10.0.5.96
Recycle Bin
Adobe Reader XI
« All Control Panel Items ▸ Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Organize ▾
4:11 PM
1/30/2014

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On
Adobe Flash Player 12 ActiveX	Adobe Systems Incorporated	1/30/2014
Adobe Reader XI (11.0.06)	Adobe Systems Incorporated	1/30/2014
Compatibility Pack for the 2007 Office system	Microsoft Corporation	8/15/2013
Java 7 Update 51	Oracle	1/30/2014
Microsoft Office Excel Viewer	Microsoft Corporation	8/15/2013
Microsoft Office Word Viewer 2003	Microsoft Corporation	8/15/2013
Microsoft PowerPoint Viewer	Microsoft Corporation	8/15/2013
Microsoft Silverlight	Microsoft Corporation	1/30/2014
Microsoft Visual C++ 2010 x86 Redistributable - 10.0....	Microsoft Corporation	1/30/2014
Python 2.7.6	Python Software Foundation	8/13/2013

Currently installed programs Total size: 650 MB
10 programs installed

Figure 62 – Verifying the final enhanced Windows 7 base image

7. Enhance the Windows 8 Profile

The Malware Analysis Appliance comes with the following programs pre-installed. You may update them to the latest version if you wish to. User account control is disabled.

This section is for your information. All steps are optional.

Microsoft Visual C++ runtime 2010 Redistributable is already included.

Flash is integrated with Internet Explorer in Windows 8. No separate install is available or required.

Step 1: Inside the Windows 8 virtual machine on the **Desktop**, click **Desktop;** the basic desktop appears.

Step 2: Navigate to the **Control Panel**.

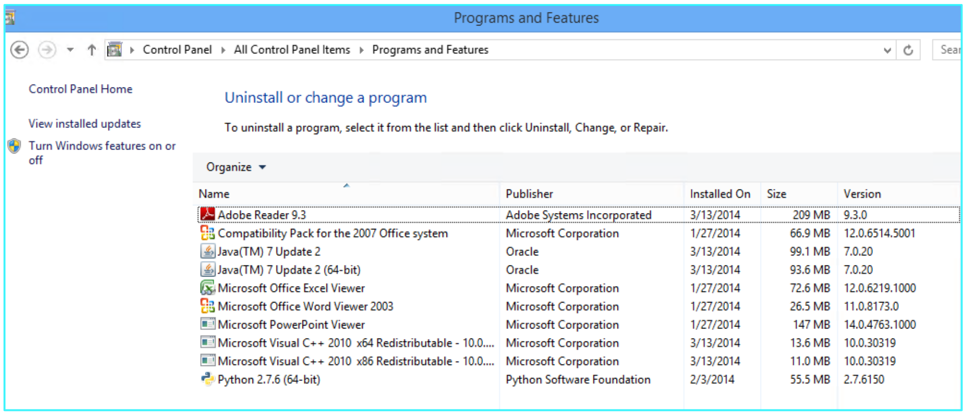
Step 3: Inside the **Control Panel**, click **Programs and Features**.

Step 4: Inside the **Programs and Features** window, confirm that the following programs are currently installed.

- Compatibility Pack for the 2007 Office System
- Microsoft Office Excel Viewer
- Microsoft Office Word Viewer 2003
- Microsoft PowerPoint Viewer
- Python 2.7.6

This configuration is the proper starting point for the Windows 8 base image enhancement process.

Note Please contact your technical representative if your base image configuration does not closely match Figure 63**.**


Programs and Features
Control Panel › All Control Panel Items › Programs and Features
Sear
Control Panel Home
View installed updates
Turn Windows features on or off
Organize ▾

Uninstall or change a program

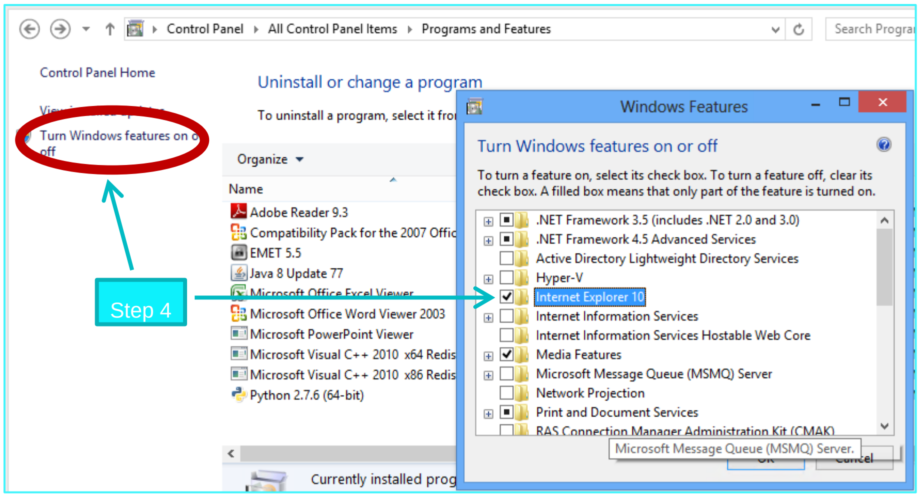
To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On	Size	Version
Adobe Reader 9.3	Adobe Systems Incorporated	3/13/2014	209 MB	9.3.0
Compatibility Pack for the 2007 Office system	Microsoft Corporation	1/27/2014	66.9 MB	12.0.6514.5001
Java(TM) 7 Update 2	Oracle	3/13/2014	99.1 MB	7.0.20
Java(TM) 7 Update 2 (64-bit)	Oracle	3/13/2014	93.6 MB	7.0.20
Microsoft Office Excel Viewer	Microsoft Corporation	1/27/2014	72.6 MB	12.0.6219.1000
Microsoft Office Word Viewer 2003	Microsoft Corporation	1/27/2014	26.5 MB	11.0.8173.0
Microsoft PowerPoint Viewer	Microsoft Corporation	1/27/2014	147 MB	14.0.4763.1000
Microsoft Visual C++ 2010 x64 Redistributable - 10.0....	Microsoft Corporation	3/13/2014	13.6 MB	10.0.30319
Microsoft Visual C++ 2010 x86 Redistributable - 10.0....	Microsoft Corporation	3/13/2014	11.0 MB	10.0.30319
Python 2.7.6 (64-bit)	Python Software Foundation	2/3/2014	55.5 MB	2.7.6150

Figure 63 – Windows 8 Programs and Features displaying starting base image configuration

Step 4: Verify that **Internet Explorer** is installed and activated by clicking **Turn Windows features on or off**.

Click **OK** if you needed to turn Internet Explorer on, or click **Cancel** if it was already activated.



Uninstall or change a program

To uninstall a program, select it fro

Adobe Reader 9.3
Compatibility Pack for the 2007 Offic
EMET 5.5
Java 8 Update 77
Microsoft Office Excel Viewer
Microsoft Office Word Viewer 2003
Microsoft PowerPoint Viewer
Microsoft Visual C++ 2010 x64 Redis
Microsoft Visual C++ 2010 x86 Redis
Python 2.7.6 (64-bit)

Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ■ .NET Framework 3.5 (includes .NET 2.0 and 3.0)
- ■ .NET Framework 4.5 Advanced Services
- □ Active Directory Lightweight Directory Services
- □ Hyper-V
- ☑ Internet Explorer 10
- □ Internet Information Services
- □ Internet Information Services Hostable Web Core
- ☑ Media Features
- □ Microsoft Message Queue (MSMQ) Server
- □ Network Projection
- ■ Print and Document Services
- □ RAS Connection Manager Administration Kit (CMAK)

Microsoft Message Queue (MSMQ) Server.

Figure 64 Verify IE Is Installed

Step 5: Click the **Internet Explorer** icon on the Windows 8 desktop or **Taskbar** to open the Web browser.

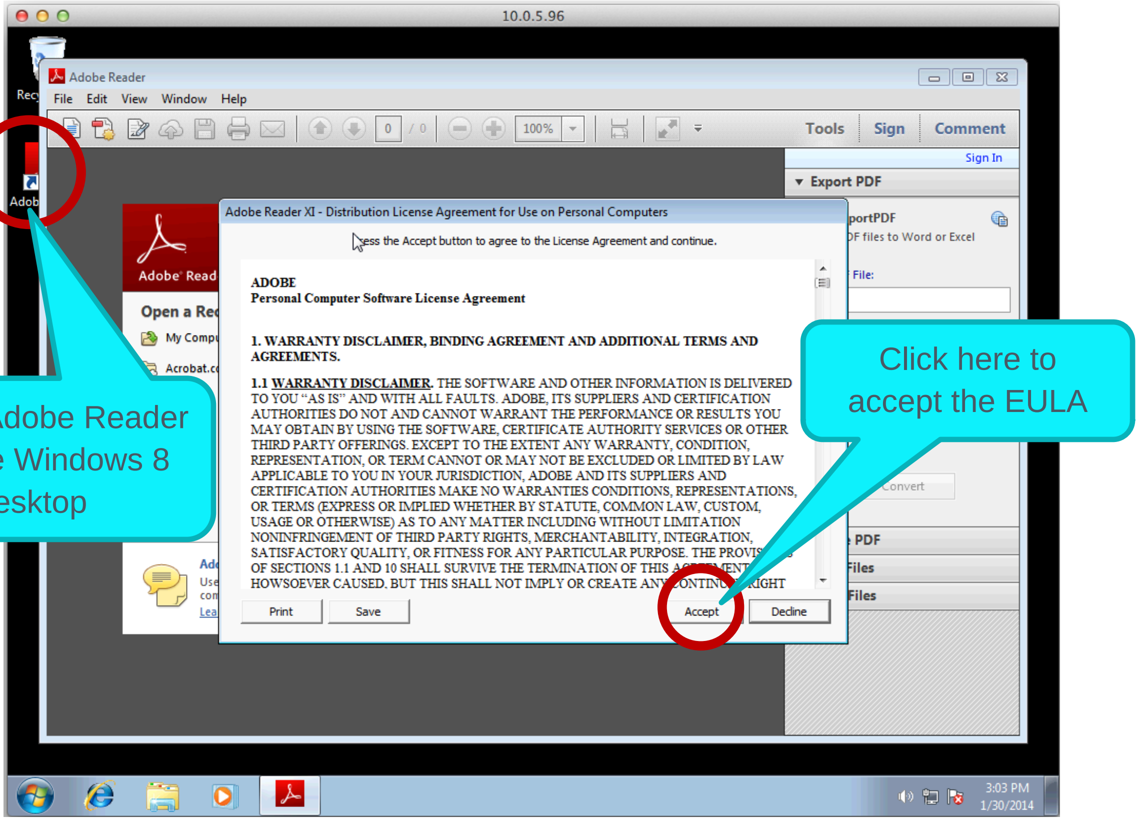
Note **Sections 7.1** through **7.5** all take place through the Internet Explorer Web browser interface.

6.8 Adobe Reader

Installing Adobe Reader is optional.

Step 1: Download **Adobe Reader** from the following address and navigate the installer as required; decline the **Optional Offer**, and click **Install Now**.

http://get.adobe.com/reader/



Adobe Reader XI - Distribution License Agreement for Use on Personal Computers

ess the Accept button to agree to the License Agreement and continue.

ADOBE
Personal Computer Software License Agreement

1. WARRANTY DISCLAIMER, BINDING AGREEMENT AND ADDITIONAL TERMS AND AGREEMENTS.

1.1 WARRANTY DISCLAIMER. THE SOFTWARE AND OTHER INFORMATION IS DELIVERED TO YOU "AS IS" AND WITH ALL FAULTS. ADOBE, ITS SUPPLIERS AND CERTIFICATION AUTHORITIES DO NOT AND CANNOT WARRANT THE PERFORMANCE OR RESULTS YOU MAY OBTAIN BY USING THE SOFTWARE, CERTIFICATE AUTHORITY SERVICES OR OTHER THIRD PARTY OFFERINGS. EXCEPT TO THE EXTENT ANY WARRANTY, CONDITION, REPRESENTATION, OR TERM CANNOT OR MAY NOT BE EXCLUDED OR LIMITED BY LAW APPLICABLE TO YOU IN YOUR JURISDICTION, ADOBE AND ITS SUPPLIERS AND CERTIFICATION AUTHORITIES MAKE NO WARRANTIES CONDITIONS, REPRESENTATIONS, OR TERMS (EXPRESS OR IMPLIED WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING WITHOUT LIMITATION NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, INTEGRATION, SATISFACTORY QUALITY, OR FITNESS FOR ANY PARTICULAR PURPOSE. THE PROVIS OF SECTIONS 1.1 AND 10 SHALL SURVIVE THE TERMINATION OF THIS A ENT HOWSOEVER CAUSED. BUT THIS SHALL NOT IMPLY OR CREATE ANY CONTINU RIGHT

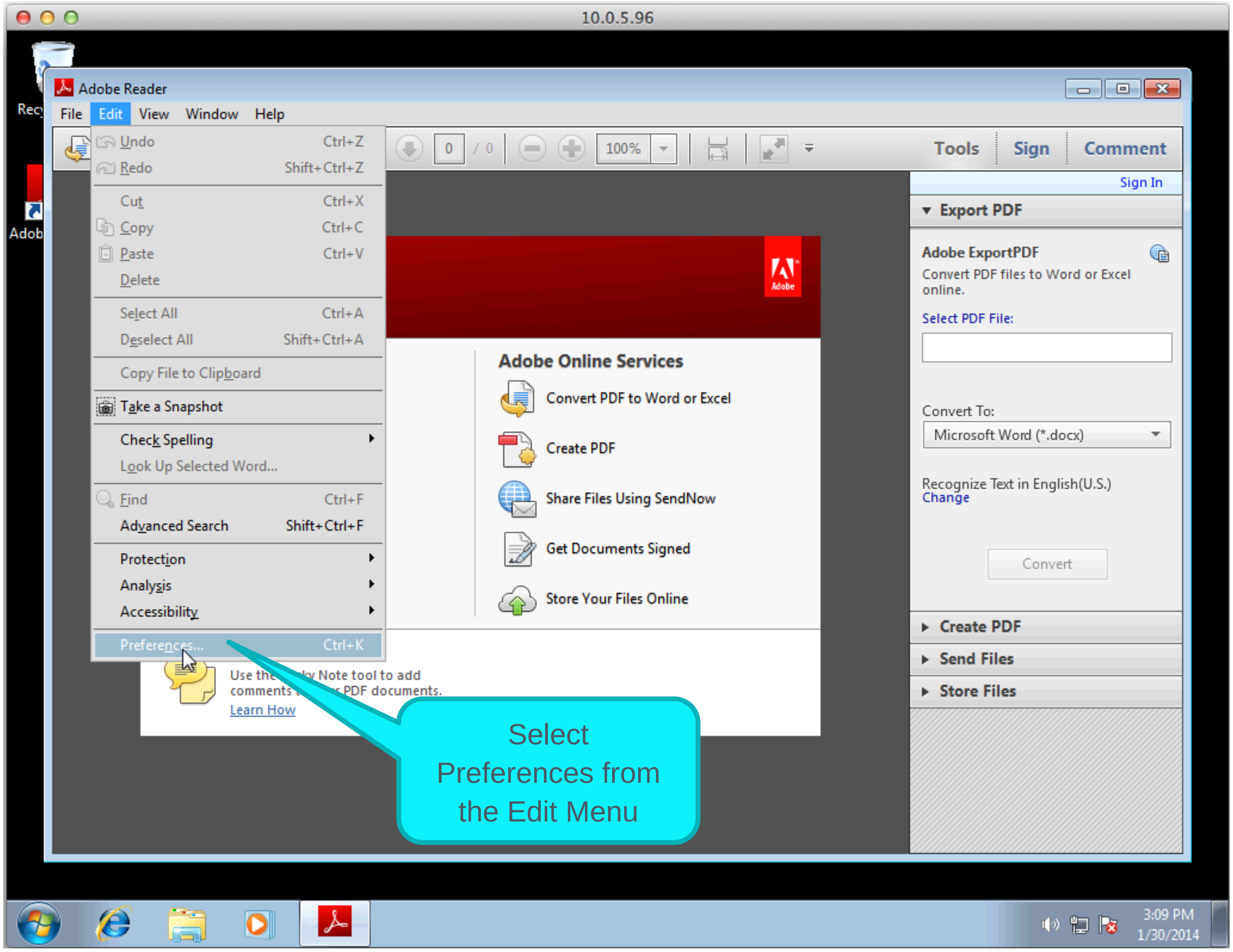
Figure 65 – Accept the Adobe Reader End User License Agreement

Step 2: When the installation is complete, run the **Adobe Reader** application from the Desktop and accept the End User License Agreement (EULA). The EULA appears automatically upon the first launch of the application.

Note The IntelliVMs will be unable to utilize Adobe Reader properly until the EULA has been accepted.

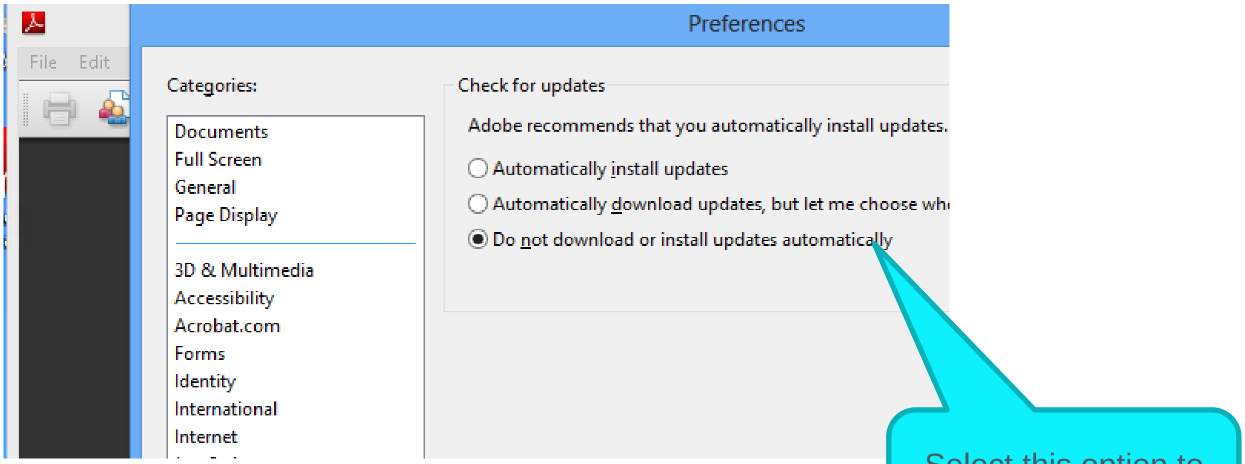
Step 3: Turn off automatic updates. From the **Edit** menu, select **Preferences**.

Note Updates are valuable for improving security and beneficial for the malware detection process, however it is essential that the MALWARE ANALYSIS APPLIANCE system administrator apply all updates *manually* so as to maintain configuration control over the malware testbed at all times. If components were to be allowed to update themselves automatically at random intervals, then configuration control becomes impractical and the administrator is never quite sure what versions of which components are being used for malware testing.



Select Preferences from the Edit Menu

Figure 66 – Opening the Preferences screen



Check for updates

Adobe recommends that you automatically install updates.

○ Automatically install updates

○ Automatically download updates, but let me choose wh

● Do not download or install updates automatically

Select this option to disable automatic updates

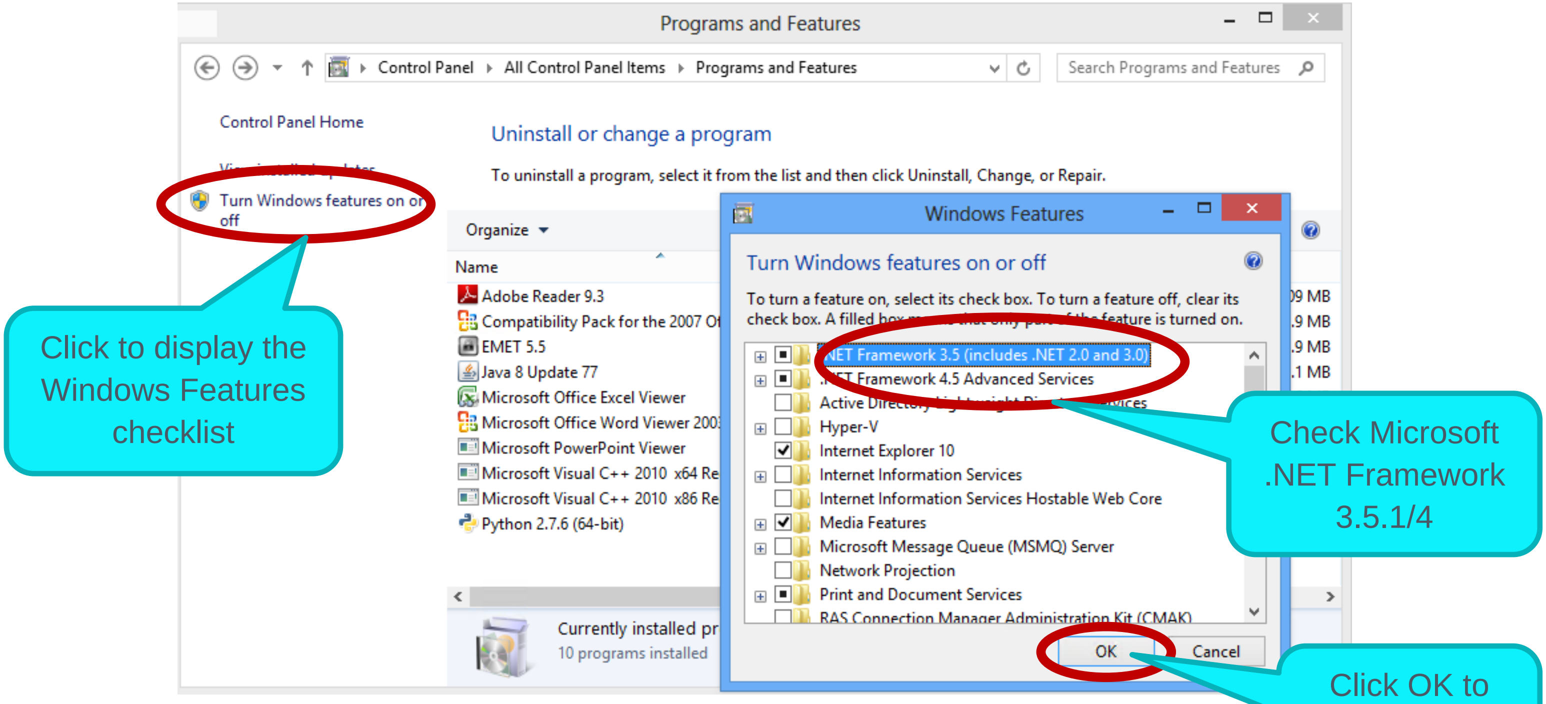
Figure 67 – Disabling automatic updates from the Preferences screen

Note Additional Adobe Reader versions: https://get.adobe.com/uk/reader/otherversions/.

6.9 Microsoft .NET Framework 3.5 SP1

On Windows 8, .NET is part of the operating system and can be enabled under **Programs and Features**.

Note EMET requires .NET 4.5. Install the correct version for your applications.



Programs and Features

Control Panel ▸ All Control Panel Items ▸ Programs and Features

Search Programs and Features

Control Panel Home

View installed updates

Turn Windows features on or off

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Organize ▾

Name

- Adobe Reader 9.3
- Compatibility Pack for the 2007 Of
- EMET 5.5
- Java 8 Update 77
- Microsoft Office Excel Viewer
- Microsoft Office Word Viewer 2003
- Microsoft PowerPoint Viewer
- Microsoft Visual C++ 2010 x64 Re
- Microsoft Visual C++ 2010 x86 Re
- Python 2.7.6 (64-bit)

Currently installed pr
10 programs installed

Windows Features

Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ■ .NET Framework 3.5 (includes .NET 2.0 and 3.0)
- ■ .NET Framework 4.5 Advanced Services
- □ Active Directory Lightweight Directory Services
- □ Hyper-V
- ☑ Internet Explorer 10
- □ Internet Information Services
- □ Internet Information Services Hostable Web Core
- ☑ Media Features
- □ Microsoft Message Queue (MSMQ) Server
- □ Network Projection
- ■ Print and Document Services
- □ RAS Connection Manager Administration Kit (CMAK)

OK Cancel

Click to display the Windows Features checklist

Check Microsoft .NET Framework 3.5.1/4

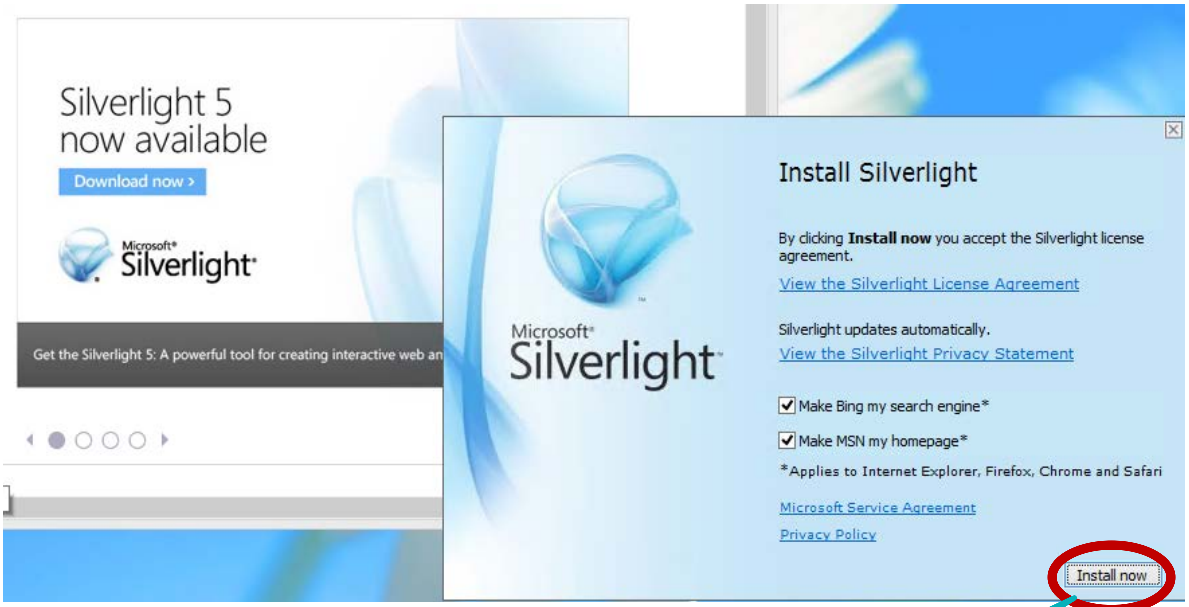
Click OK to commit the change

Figure 68 – Turn on Microsoft .NET Framework 3.5.1 or 4 from the Windows Features checklist

6.10 Microsoft Silverlight

Step 1: Download **Microsoft Silverlight** from this address and navigate the installer as required.

http://www.microsoft.com/silverlight/



Get the Silverlight 5: A powerful tool for creating interactive web an

Install Silverlight

By clicking **Install now** you accept the Silverlight license agreement.

Silverlight updates automatically.

☑ Make Bing my search engine*

☑ Make MSN my homepage*

*Applies to Internet Explorer, Firefox, Chrome and Safari

Figure 69 – Install Silverlight

Click here to begin installation

Important Note

Disable the Silverlight auto update feature. See these documents for details:

- https://www.microsoft.com/getsilverlight/resources/documentation/grouppolicysettings.aspx#AutomaticUpdate (HKEY_LOCAL_MACHINE\Software\Microsoft\Silverlight\UpdateMode = 2)
- https://www.microsoft.com/getsilverlight/resources/documentation/grouppolicysettings.aspx#TrustedApplications (HKEY_LOCAL_MACHINE\Software\Microsoft\Silverlight\AllowInstallOfElevatedTrustApps = 1, HKEY_LOCAL_MACHINE\Software\Microsoft\Silverlight\AllowLaunchOfElevatedTrustApps = 1)

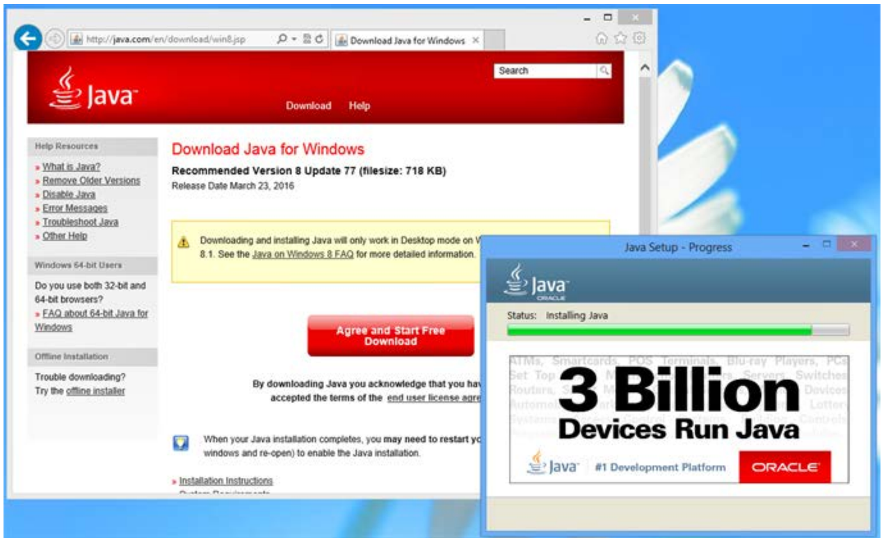
6.11 Java

Installing Java is optional.

Step 1: Download **Java** from the address below and navigate to the installer as required.

http://java.com/en/download/index.jsp

Opt out of the Optional offer, and click **Next.**



Download Java for Windows

Recommended Version 8 Update 77 (filesize: 718 KB)
Release Date March 23, 2016

Downloading and installing Java will only work in Desktop mode on W
8.1. See the Java on Windows 8 FAQ for more detailed information.

Do you use both 32-bit and 64-bit browsers?
FAQ about 64-bit Java for Windows

Trouble downloading?
Try the offline installer

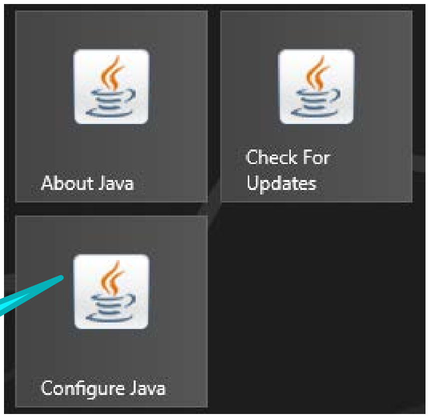
By downloading Java you acknowledge that you hav
accepted the terms of the end user license agre

When your Java installation completes, you may need to restart yo
windows and re-open) to enable the Java installation.

Figure 70 – Installing Java

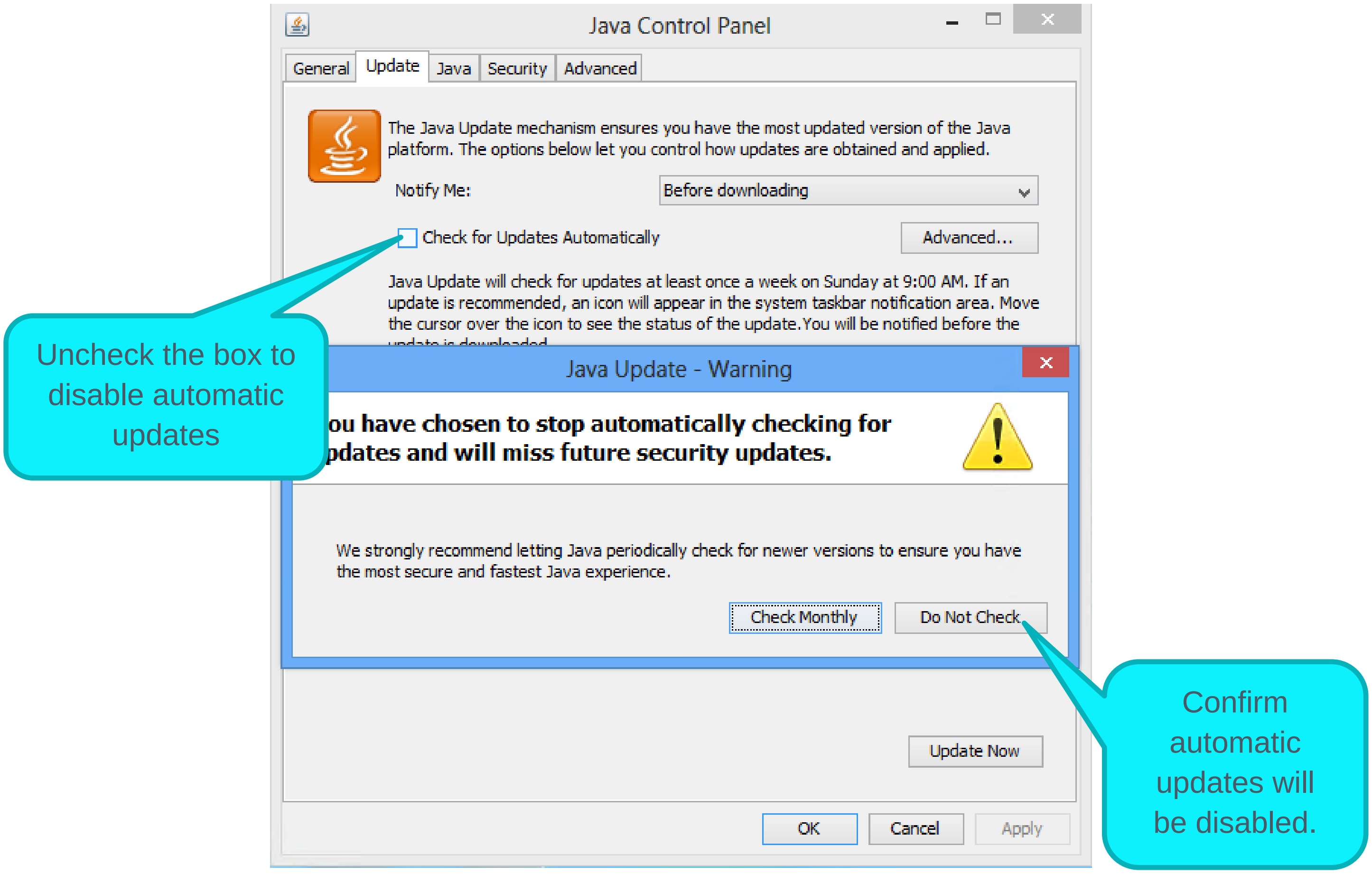
If you see the **Uninstall out-of-date versions** window, click **Uninstall**. The old version of Java will be uninstalled. Click **Next** when required. When the new version has been installed, you will see the **Java Setup – Complete** window. Click **Close**.

Step 2: New Java icons appear on the programs area of the desktop now. Click **Configure Java**.



On the Windows 8 desktop, click Configure Java

Figure 71 – Select Configure Java



The Java Update mechanism ensures you have the most updated version of the Java platform. The options below let you control how updates are obtained and applied.

Notify Me: Before downloading

□ Check for Updates Automatically

Java Update will check for updates at least once a week on Sunday at 9:00 AM. If an update is recommended, an icon will appear in the system taskbar notification area. Move the cursor over the icon to see the status of the update.You will be notified before the update is downloaded.

Java Update - Warning

ou have chosen to stop automatically checking for pdates and will miss future security updates.

We strongly recommend letting Java periodically check for newer versions to ensure you have the most secure and fastest Java experience.

Uncheck the box to disable automatic updates

Confirm automatic updates will be disabled.

Figure 72 – Disabling automatic Java updates

Note Download older versions from this archive: http://www.oracle.com/technetwork/java/archive-139210.html

6.12 Detect Unknown Exploits with EMET

In the Malware Analysis appliance, the Microsoft® Enhanced Mitigation Experience Toolkit (EMET) detects unknown exploits. For the InteliVM to be able to collect EMET events, EMET must be installed in a Windows 7 or 8 profile, and properly configured. This feature is strongly recommended, but optional.

Note Blue Coat recommends that you first deploy EMET on a new profile to verify that it works as expected.

Step 1: Create a new Windows 8 profile. EMET is not supported on Windows XP.

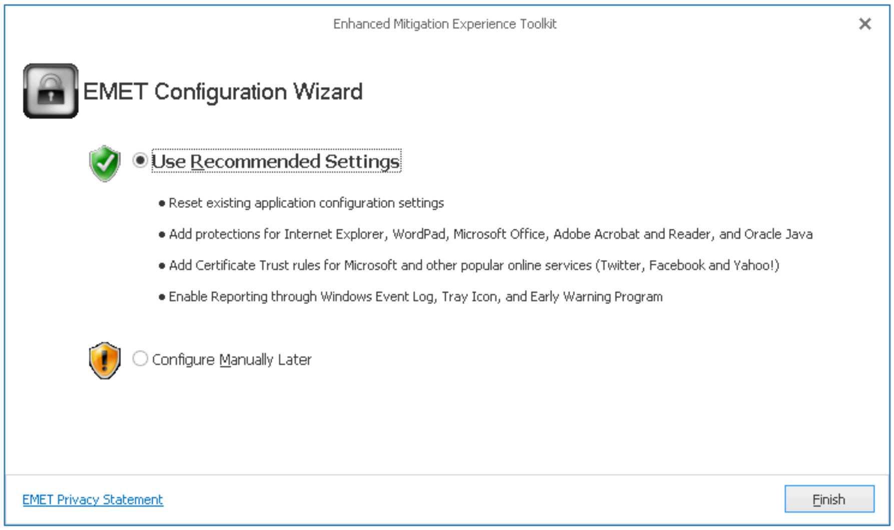
Step 2: Customize the profile, then log on using RDP.

Step 3: Verify the .NET Framework 4.5 in installed on Windows; it is natively installed.

Note For EMET to work with Internet Explorer 10 on Windows 8, Microsoft KB 2790907 or a more recent version of the Compatibility Update for Windows 8 must be installed.

Step 4: Download EMET 5.5 and the user-guide PDF from Microsoft at: https://download.microsoft.com/download/8/E/E/8EEFD9FC-46B1-4A8B-9B5D-13B4365F8CA0/EMET%20Setup.msi , and begin the installation.

Step 5: On the *EMET Configuration Wizard* page, select **Use Recommended Settings,** and click **Finish**.



Enhanced Mitigation Experience Toolkit

EMET Configuration Wizard

● Use Recommended Settings

- Reset existing application configuration settings
- Add protections for Internet Explorer, WordPad, Microsoft Office, Adobe Acrobat and Reader, and Oracle Java
- Add Certificate Trust rules for Microsoft and other popular online services (Twitter, Facebook and Yahoo!)
- Enable Reporting through Windows Event Log, Tray Icon, and Early Warning Program

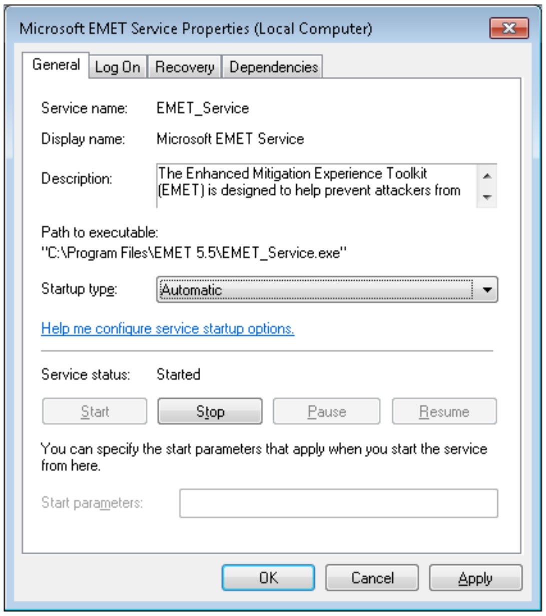
○ Configure Manually Later

Figure 73 – EMET Wizard

Step 6: Configure the EMET service to start automatically with no delay. Follow these steps:

4. Click **Start,** and search for “services.mscaudit only.
5. Right click the service name, and select **Properties**.

6. Change the **Startup Type** to **Automatic**.



Microsoft EMET Service Properties (Local Computer)

Service name: EMET_Service

Display name: Microsoft EMET Service

Description: The Enhanced Mitigation Experience Toolkit (EMET) is designed to help prevent attackers from

Path to executable:
"C:\Program Files\EMET 5.5\EMET_Service.exe"

Startup type: Automatic

Help me configure service startup options.

Service status: Started

You can specify the start parameters that apply when you start the service from here.

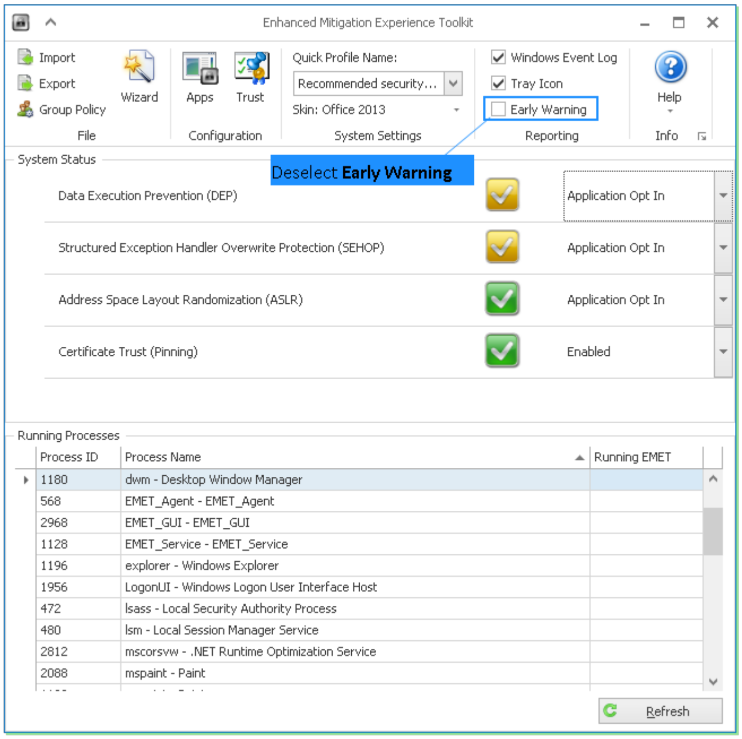
Start parameters:

Figure 74 – Set Startup Type to Automatic

The following optional steps further enhance the EMET configuration.

A: Open the EMET GUI and configure it.

7. Uncheck the Early Warning option on the **Enhanced Mitigation Experience Toolkit** window, if you don't want information related to an exploitation attempt to be sent to Microsoft through the standard Windows Error Reporting channel.



Enhanced Mitigation Experience Toolkit

Quick Profile Name: Recommended security...

Skin: Office 2013

System Settings

☑ Windows Event Log

☑ Tray Icon

□ Early Warning

Reporting

Deselect **Early Warning**

System Status

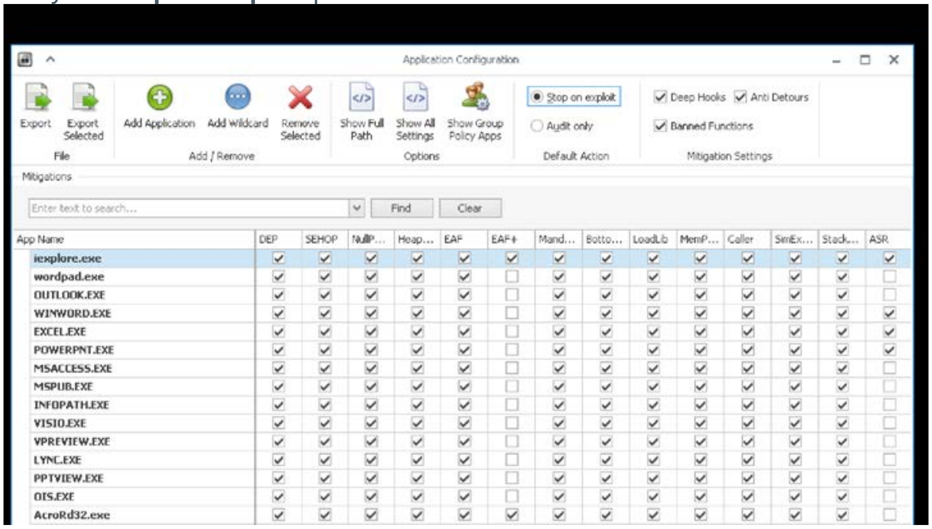
Data Execution Prevention (DEP)	✓	Application Opt In
Structured Exception Handler Overwrite Protection (SEHOP)	✓	Application Opt In
Address Space Layout Randomization (ASLR)	✓	Application Opt In
Certificate Trust (Pinning)	✓	Enabled

Running Processes

Process ID	Process Name	Running EMET
1180	dwm - Desktop Window Manager	
568	EMET_Agent - EMET_Agent	
2968	EMET_GUI - EMET_GUI	
1128	EMET_Service - EMET_Service	
1196	explorer - Windows Explorer	
1956	LogonUI - Windows Logon User Interface Host	
472	lsass - Local Security Authority Process	
480	lsm - Local Session Manager Service	
2812	mscorsvw - .NET Runtime Optimization Service	
2088	mspaint - Paint	

Figure 75 – Deselect Early Warning

8. Click **Apps** in the upper menu bar to open the configuration window.
9. Set your **Stop on Exploit** preference.



● Stop on exploit
○ Audit only

☑ Deep Hooks ☑ Anti Detours
☑ Banned Functions

App Name	DEP	SEHOP	NullP...	Heap...	EAF	EAF+	Mand...	Botto...	LoadLib	MemP...	Caller	SimEx...	Stack...	ASR
iexplore.exe	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
wordpad.exe	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□
OUTLOOK.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□
WINWORD.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	☑
EXCEL.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	☑
POWERPNT.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	☑
MSACCESS.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□
MSPUB.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□
INFOPATH.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□
VISIO.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□
VPREVIEW.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□
LYNC.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□
PPTVIEW.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□
OIS.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□
AcroRd32.exe	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	□

Figure 76 – Configure Stop on exploit

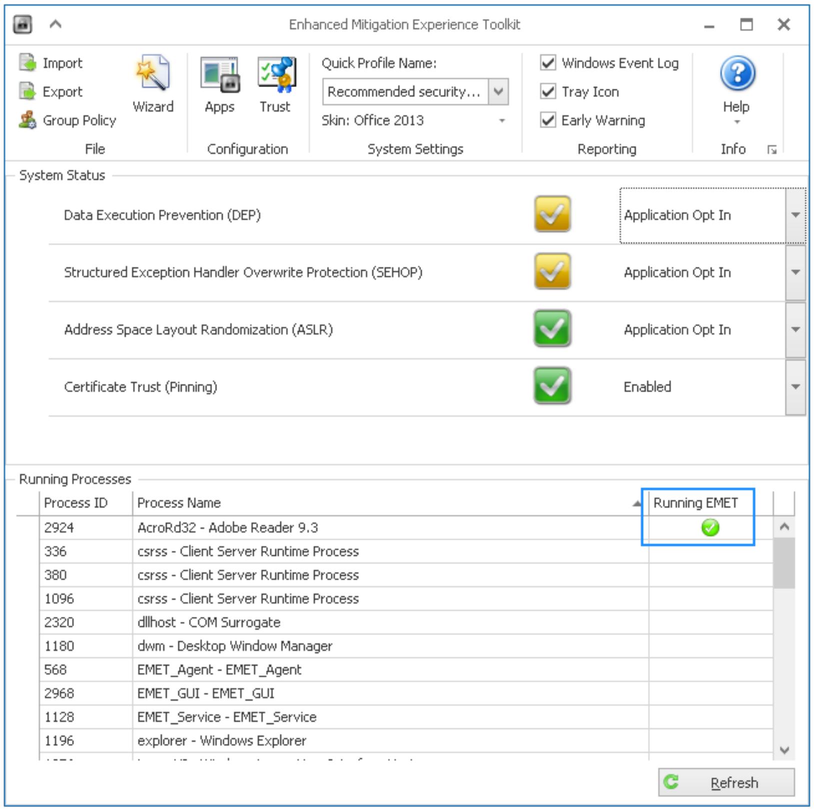
- By default EMET is set to the **Default Action Stop on exploit**. This is the recommended setting for *maximizing detection*. However, this may not give you all the details about the attack, including second stage malware information. Blue Coat recommends maintaining this choice for maximum detection and with simpler configurations.
- For full attack information (and a minimal reduction in exploit detection), select **Audit only**. This will let the exploit continue as long as possible, only observing. This results in significantly more information about consecutive stages of the attack.

10. Remove any applications you don’t want to monitor, if necessary. When the **Use Recommended Settings** selection is made during installation, EMET adds and configures a set of popular applications. Click **Remove Selected** when you have highlighted an application in order to remove it.
11. If necessary, add a new application, highlight it in the list, and enable all mitigations for that application (unless otherwise advised).

Note Some mitigations are not compatible with certain applications. Blue Coat recommends referring to the following link to verify your settings, and then to deselect any incompatible mitigations: https://support.microsoft.com/kb/2909257.

12. Click **OK** to return to the EMET Toolkit main window.

B: Start the configured applications, then click **Refresh** in the EMET GUI, and verify you see a green check mark in the **Running EMET** column.



Quick Profile Name: Recommended security...

Skin: Office 2013

☑ Windows Event Log

☑ Tray Icon

☑ Early Warning

System Status

Data Execution Prevention (DEP)	✓	Application Opt In
Structured Exception Handler Overwrite Protection (SEHOP)	✓	Application Opt In
Address Space Layout Randomization (ASLR)	✓	Application Opt In
Certificate Trust (Pinning)	✓	Enabled

Running Processes

Process ID	Process Name	Running EMET
2924	AcroRd32 - Adobe Reader 9.3	✓
336	csrss - Client Server Runtime Process	
380	csrss - Client Server Runtime Process	
1096	csrss - Client Server Runtime Process	
2320	dllhost - COM Surrogate	
1180	dwm - Desktop Window Manager	
568	EMET_Agent - EMET_Agent	
2968	EMET_GUI - EMET_GUI	
1128	EMET_Service - EMET_Service	
1196	explorer - Windows Explorer	

Figure 77 – EMET is running

Step 7: Close all applications, close the remote desktop session, then build the profile.

Step 8: Verify that EMET works by running samples which will trigger EMET. The following MD5 is for reference; Blue Coat is unable to provide the samples, as they are malicisous. They are available on VirusTotal.

- C32AD4D6F6A00C85E6BD152852D5D09F (SimExecFlow, and StackPivot)

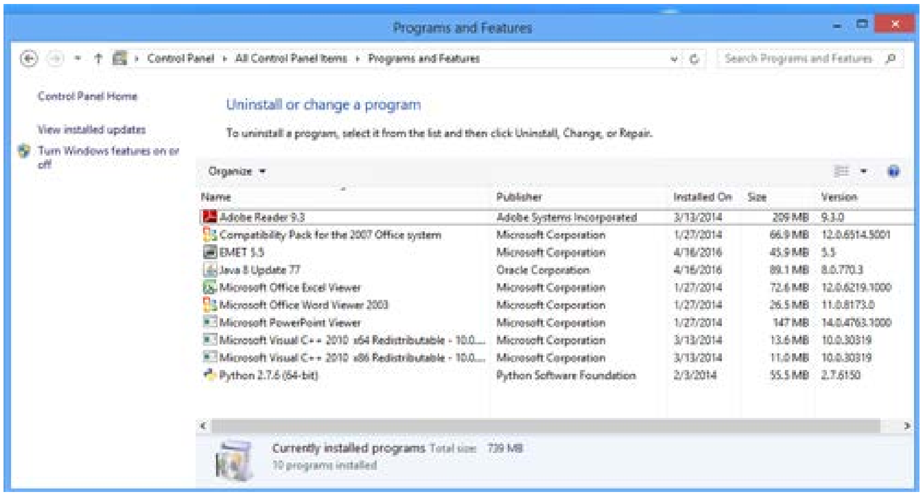
6.13 Final Enhanced Windows 8 Profile

Return to the **Add or Remove Programs** window in the Windows 7 **Control Panel** (see **Section 7 – Enhancing the Windows 8 Profile**, Step 2) and confirm that the following programs are now installed.

- Adobe Flash Player (native in Windows 8)
- Adobe Reader (optional)
- Compatibility Pack for the 2007 Office System
- Microsoft Office Excel Viewer
- Microsoft Office Word Viewer 2003
- Microsoft PowerPoint Viewer
- Microsoft Silverlight
- Python 2.7.6
- EMET 5.5 (strongly recommended, optional)

This configuration is the proper ending point for the base profile enhancement process.

Note Please contact your technical representative if your base profile configuration does not closely match Figure 78**.** The versions do not need to be exactly the same as depicted below, as the vendors may post newer versions online.



Programs and Features
Control Panel › All Control Panel Items › Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Organize ▾

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On	Size	Version
Adobe Reader 9.3	Adobe Systems Incorporated	3/13/2014	209 MB	9.3.0
Compatibility Pack for the 2007 Office system	Microsoft Corporation	1/27/2014	66.9 MB	12.0.6514.5001
EMET 5.5	Microsoft Corporation	4/16/2016	45.9 MB	5.5
Java 8 Update 77	Oracle Corporation	4/16/2016	89.1 MB	8.0.770.3
Microsoft Office Excel Viewer	Microsoft Corporation	1/27/2014	72.6 MB	12.0.6219.1000
Microsoft Office Word Viewer 2003	Microsoft Corporation	1/27/2014	26.5 MB	11.0.8173.0
Microsoft PowerPoint Viewer	Microsoft Corporation	1/27/2014	147 MB	14.0.4763.1000
Microsoft Visual C++ 2010 x64 Redistributable - 10.0....	Microsoft Corporation	3/13/2014	13.6 MB	10.0.30319
Microsoft Visual C++ 2010 x86 Redistributable - 10.0....	Microsoft Corporation	3/13/2014	11.0 MB	10.0.30319
Python 2.7.6 (64-bit)	Python Software Foundation	2/3/2014	55.5 MB	2.7.6150

Currently installed programs Total size: 739 MB
10 programs installed

Figure 78 – Verifying the final enhanced Windows 8 base image

8. Customize an Office 2010 Profile for Malware Detonation

This section explains how to configure a custom Microsoft Office profile such that it detonates in the best possible way. This procedure is specific for Windows 7, but the principles apply to all versions of Windows.

Note: This is a Windows 7 example. Other Windows installations will be similar.

Avoid pitfalls by carefully following the procedures in this section:

- Uninstall all Office Viewer applications.
- Uninstall the Compatibility Pack for the 2007 Office system.
- Start each program at least once to go through the initial configuration.
- Auto-enable macro execution.

Steps Overview

These steps are performed from inside the iVM Profile on the Windows 7 virtual machine, using remote desktop protocol (RDP). Adjust the security settings for each program to maximize the attack surface.

- Step 1: Configure Office
- Step 2: Configure Word
- Step 3: Configure MS Access
- Step 4: Configure Excel
- Step 5: Configure Publisher
- Step 6: Configure PowerPoint
- Step 7: Configure Outlook
- Step 8: Configure Windows Media Player
- Step 9: Configure Internet Explorer (v. 10+)
- Step 10: Configure Enhanced Mitigation Experience Toolkit (EMET)

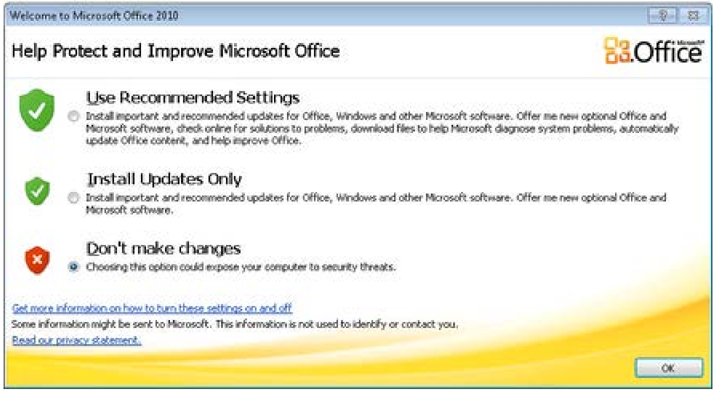
Pre-Requisites

- Office 2010 installed
- EMET 5.5 installed

Step 1: Configure Office

1. Open Microsoft Word. The Activation Wizard begins.
2. Follow the instructions to active Office.

3. Disable changes or updates.



Welcome to Microsoft Office 2010

Help Protect and Improve Microsoft Office

○ Use Recommended Settings
Install important and recommended updates for Office, Windows and other Microsoft software. Offer me new optional Office and Microsoft software, check online for solutions to problems, download files to help Microsoft diagnose system problems, automatically update Office content, and help improve Office.

○ Install Updates Only
Install important and recommended updates for Office, Windows and other Microsoft software. Offer me new optional Office and Microsoft software.

● Don't make changes
Choosing this option could expose your computer to security threats.

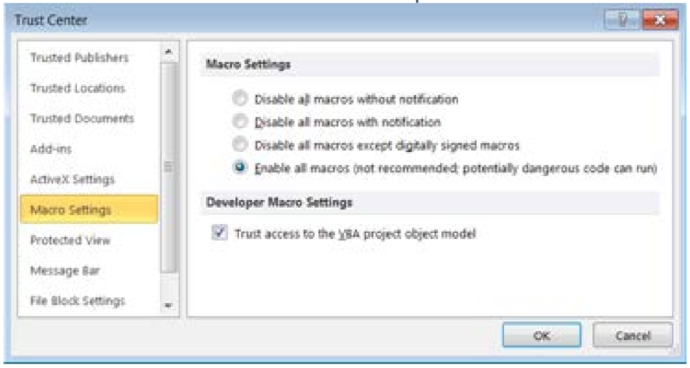
Get more information on how to turn these settings on and off
Some information might be sent to Microsoft. This information is not used to identify or contact you.
Read our privacy statement.

Figure 79 – Don’t Make Changes

4. Close Word.

Step 2: Configure Word

1. Open Word.
2. Navigate to **File > Options > Trust Center > Trust Center Settings**.
3. Enable all macros and VBA developer access.



Trust Center

Macro Settings

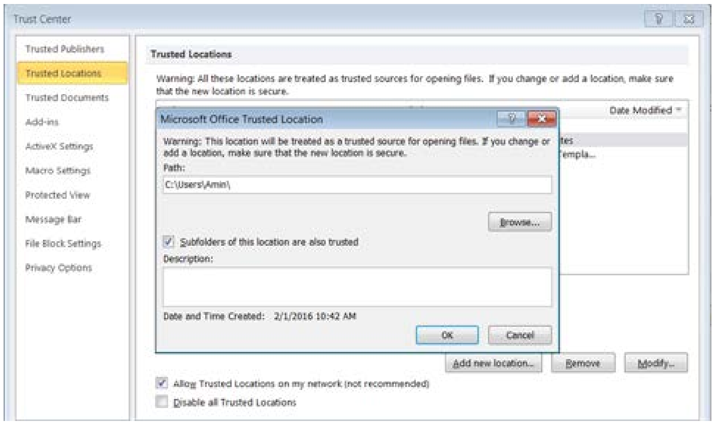
○ Disable all macros without notification
○ Disable all macros with notification
○ Disable all macros except digitally signed macros
● Enable all macros (not recommended; potentially dangerous code can run)

Developer Macro Settings

☑ Trust access to the VBA project object model

Figure 80 – Trust Access

4. On the **Trust Center** window, select **File Block Settings**, and deselect everything.
5. On the Trust Center window, select Trusted Locations, and select Allow Trusted Locations on my network.
    - Add C:\Users\Admin.
    - Check **Subfolders of this location are also trusted**.



Trust Center

Trusted Locations

Warning: All these locations are treated as trusted sources for opening files. If you change or add a location, make sure that the new location is secure.

Microsoft Office Trusted Location

Warning: This location will be treated as a trusted source for opening files. If you change or add a location, make sure that the new location is secure.

Path: C:\Users\Amin\

☑ Subfolders of this location are also trusted

Description:

Date and Time Created: 2/1/2016 10:42 AM

☑ Allow Trusted Locations on my network (not recommended)

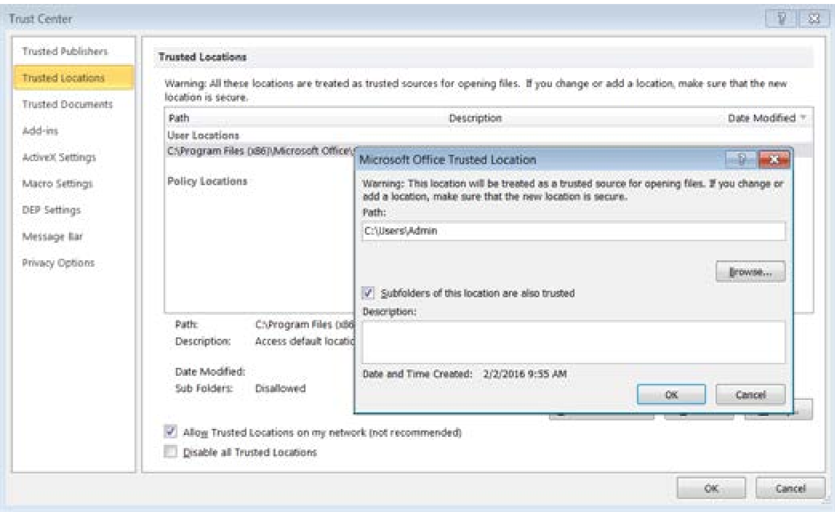
☐ Disable all Trusted Locations

Figure 81 – Subfolders

6. On the **Trust Center** window, select **Protected View**, deselect **Enable Data Execution Prevention mode**, and deselect everything else.
7. On the **Trust Center** window, select **Add-ins**, and deselect **Require Application Add-ins to be signed by Trusted Publisher**.
8. On the **Trust Center** window, select **Trusted Documents**, and check **Allow documents on a network to be trusted**.
9. On the **Trust Center** window, select **Privacy Options**, and deselect **Check Microsoft Office documents that are from or link to suspicious Web sites**.
10. Close Word.

Step 3: Configure MS Access

1. Open Access.
2. Navigate to **File > Options > Trust Center > Trust Center.**
3. Select **ActiveX Settings**, and
   - Tick **Enable all controls without restrictions and without prompting.**
   - Deselect **Safe Mode.**
4. On the **Trust Center** window, select **Macro Settings**, and select **Enable all macros.**
5. On the **Trust Center** window, select **DEP Settings**, and deselect **Enable Data Execution Prevention Mode.**
6. On the **Trust Center** window, select **Trusted Locations.**
   - Add **C:\Users\Admin.**
   - Check **Subfolders of this location are also trusted**.



Warning: All these locations are treated as trusted sources for opening files. If you change or add a location, make sure that the new location is secure.

C:\Program Files (x86)\Microsoft Office\

Path: C:\Program Files (x86

Description: Access default locatio

Date Modified:

Sub Folders: Disallowed

☑ Allow Trusted Locations on my network (not recommended)

□ Disable all Trusted Locations

Warning: This location will be treated as a trusted source for opening files. If you change or add a location, make sure that the new location is secure.

Path:

C:\Users\Admin

☑ Subfolders of this location are also trusted

Description:

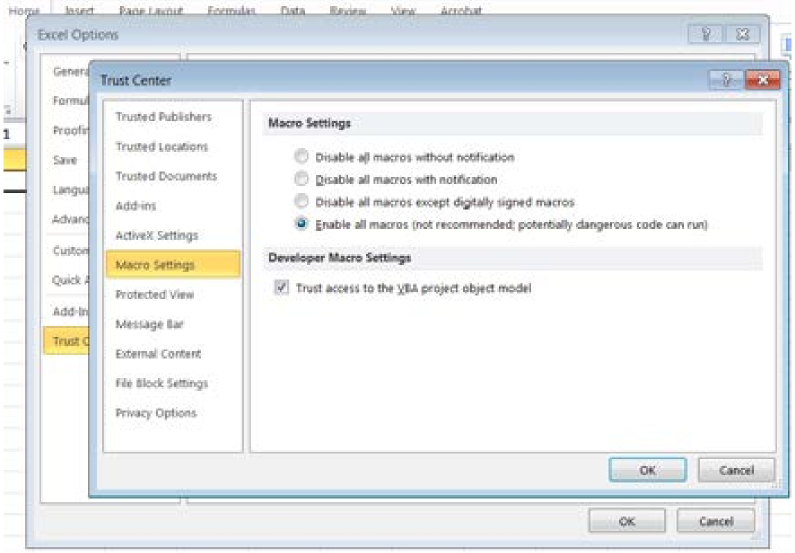
Date and Time Created: 2/2/2016 9:55 AM

Figure 82 – MS Access Subfolders

7. On the **Trust Center** window, select **Add-ins**, and deselect **Require Application Add-ins to be signed by Trusted Publisher**.
8. On the **Trust Center** window, select **Trusted Documents**, and check **Allow documents on a network to be trusted**.
9. On the **Trust Center** window, select **Privacy Options**, and deselect **Check Microsoft Office documents that are from or link to suspicious Web sites**.
10. Close Access.

Step 4: Configure Excel

1. Open Excel.
2. Navigate to **File > Options > Trust Center > Trust Center**.
3. Select **ActiveX Settings**, and
    - Tick **Enable all controls without restrictions and without prompting.**
    - Deselect **Safe Mode.**
4. On the **Trust Center** window, select **Macro Settings**:
    a. Select **Enable all macros**.
    b. Select **Trust access to the VBA project object model**.



Macro Settings

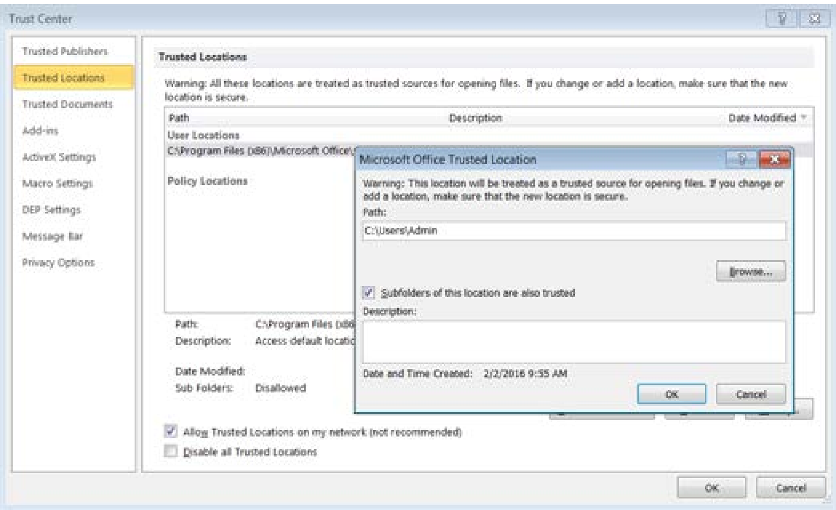
○ Disable all macros without notification
○ Disable all macros with notification
○ Disable all macros except digitally signed macros
● Enable all macros (not recommended; potentially dangerous code can run)

Developer Macro Settings

☑ Trust access to the VBA project object model

Figure 83 – Excel Macro Settings

5. On the **Trust Center** window, select **File Block Settings**, and deselect everything.
6. On the **Trust Center** window, select **Trusted Locations**:
    a. Add **C:\Users\Admin**.
    b. Check **Subfolders of this location are also trusted**.



Trusted Locations

Warning: All these locations are treated as trusted sources for opening files. If you change or add a location, make sure that the new location is secure.

User Locations
C:\Program Files (x86)\Microsoft Office\

Policy Locations

Path: C:\Program Files (x86
Description: Access default locatio
Date Modified:
Sub Folders: Disallowed

☑ Allow Trusted Locations on my network (not recommended)
☐ Disable all Trusted Locations

Microsoft Office Trusted Location

Warning: This location will be treated as a trusted source for opening files. If you change or add a location, make sure that the new location is secure.

Path:
C:\Users\Admin

☑ Subfolders of this location are also trusted

Description:

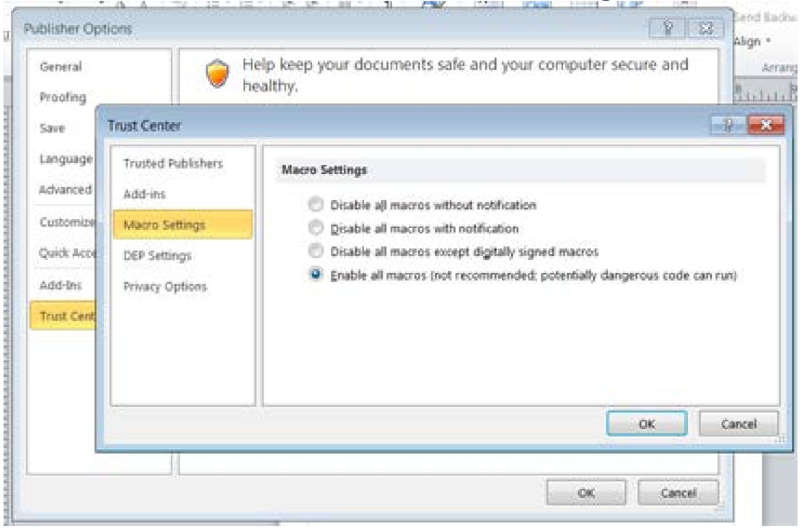
Date and Time Created: 2/2/2016 9:55 AM

Figure 84 – Excel Trusted Locations

7. On the **Trust Center** window, select **Add-ins**, and deselect **Require Application Add-ins to be signed by Trusted Publisher**.
8. On the **Trust Center** window, select **Trusted Documents**, and check **Allow documents on a network to be trusted**.
9. On the **Trust Center** window, select **Privacy Options**, and deselect **Check Microsoft Office documents that are from or link to suspicious Web sites**.
10. On the **Trust Center** window, select **File Block Settings**, and deselect all items in the **File Type** list.
11. Close Excel.

Step 5: Configure Publisher

1. Open Publisher.
2. Navigate to **File > Options > Trust Center > Trust Center**.
3. On the **Trust Center** window, select **Macro Settings**, and select **Enable all macros**.



Macro Settings

○ Disable all macros without notification
○ Disable all macros with notification
○ Disable all macros except digitally signed macros
● Enable all macros (not recommended; potentially dangerous code can run)

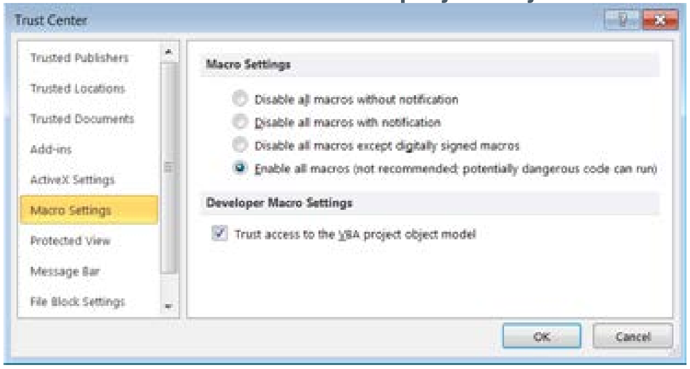
Figure 85 – Publisher Macros

4. On the **Trust Center** window, select **DEP Settings**, and deselect **Enable Data Execution Prevention Mode**.
5. On the **Trust Center** window, select **Add-ins**, and deselect **Require Application Add-ins to be signed by Trusted Publisher**.
6. Close Publisher.

Step 6: Configure PowerPoint

1. Open PowerPoint.
2. Navigate to **File > Options > Trust Center > Trust Center Settings**.
3. On the **Trust Center** window, select **Macro Settings:**

- Select **Enable all macros**.
- Select **Trust access to the VBA project object model**.



Macro Settings

○ Disable all macros without notification

○ Disable all macros with notification

○ Disable all macros except digitally signed macros

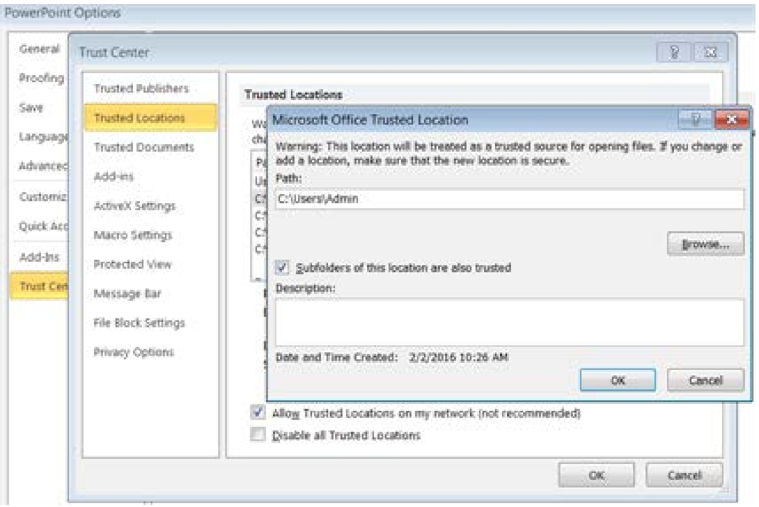
● Enable all macros (not recommended; potentially dangerous code can run)

Developer Macro Settings

☑ Trust access to the VBA project object model

Figure 86 – PowerPoint Macros

4. On the **Trust Center** window, select **Protected View**, and deselect everything.
5. On the **Trust Center** window, select **Trusted Locations**, and select **Allow Trusted Locations on my network.**
   - Add **C:\Users\Admin.**
   - Check **Subfolders of this location are also trusted**.



Microsoft Office Trusted Location

Warning: This location will be treated as a trusted source for opening files. If you change or add a location, make sure that the new location is secure.

Path:

C:\Users\Admin

☑ Subfolders of this location are also trusted

Description:

Date and Time Created: 2/2/2016 10:26 AM

☑ Allow Trusted Locations on my network (not recommended)

☐ Disable all Trusted Locations

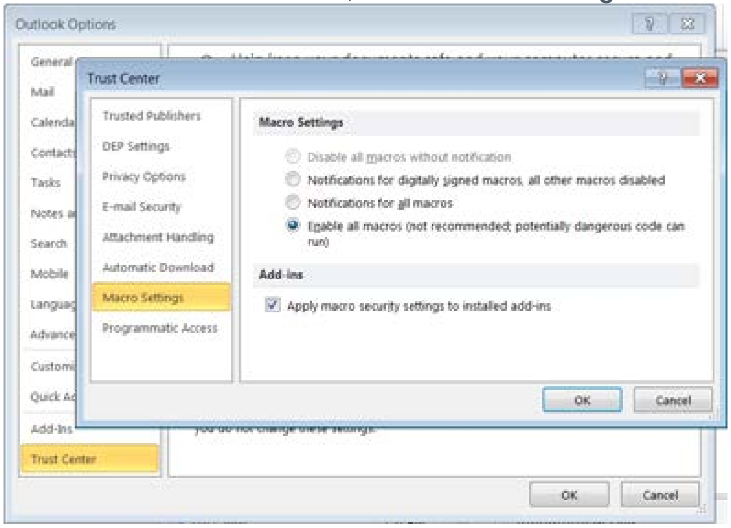
Figure 87 – PowerPoint Subfolders

6. On the **Trust Center** window, select **File Block Settings**, and deselect everything.
7. On the **Trust Center** window, select **Add-ins**, and deselect **Require Application Add-ins to be signed by Trusted Publisher**.
8. On the **Trust Center** window, select **Trusted Documents**, and check **Allow documents on a network to be trusted**.
9. On the **Trust Center** window, select **Privacy Options**, and deselect **Check Microsoft Office documents that are from or link to suspicious Web sites**.
10. Close PowerPoint.

Step 7: Configure Outlook

1. Open Outlook.
2. Proceed through the Startup wizard normally. Set up an email account or not as required.
3. Navigate to **File > Options > Trust Center > Trust Center Settings**.
4. On the **Trust Center** window, select **Automatic Download**, and deselect everything.

5. On the **Trust Center** window, select **Macro Settings**:



Macro Settings

○ Disable all macros without notification
○ Notifications for digitally signed macros, all other macros disabled
○ Notifications for all macros
● Enable all macros (not recommended; potentially dangerous code can run)

Add-ins

☑ Apply macro security settings to installed add-ins

Figure 88 – Excel Macros

- Select **Enable all macros.**
- Select **Apply macros security settings to installed add-ons.**

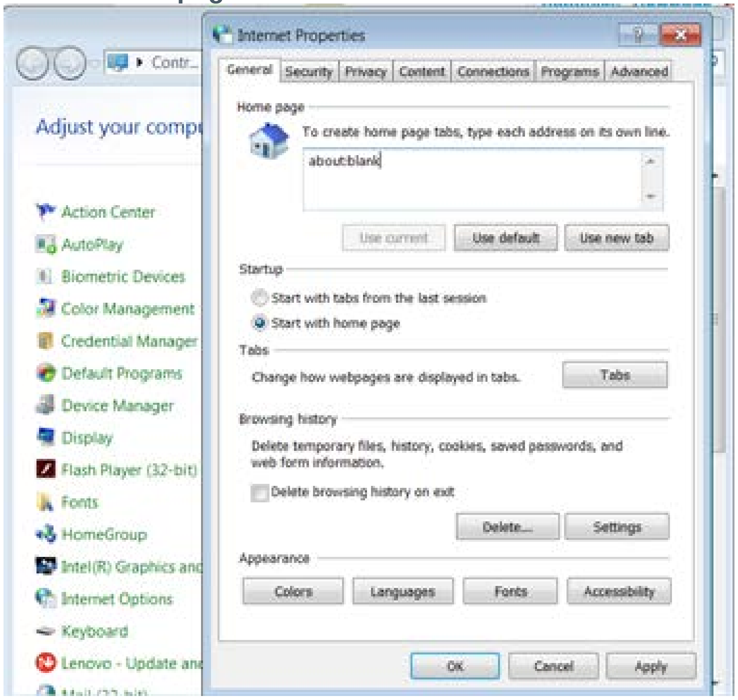
6. On the **Trust Center** window, select **Programmatic Access**, and select **Never warn me about suspicious activity**.
7. On the **Trust Center** window, select **DEP Settings**, and deselect **Enable Data Execution Prevention Mode.**
8. Close Outlook.

Step 8: Configure Windows Media Player

1. Open Windows Media Player.
2. Procced through the Startup wizard normally, using the recommend settings.
3. Close Windows Media Player.

Step 9: Configure Internet Explorer (v. 10+)

1. Open the computer Control Panel, and select **Internet options**.
2. Set the **Home page** to **about:blank**.



Internet Properties

General | Security | Privacy | Content | Connections | Programs | Advanced

Home page

To create home page tabs, type each address on its own line.

about:blank

Startup

○ Start with tabs from the last session

● Start with home page

Tabs

Change how webpages are displayed in tabs.

Browsing history

Delete temporary files, history, cookies, saved passwords, and web form information.

□ Delete browsing history on exit

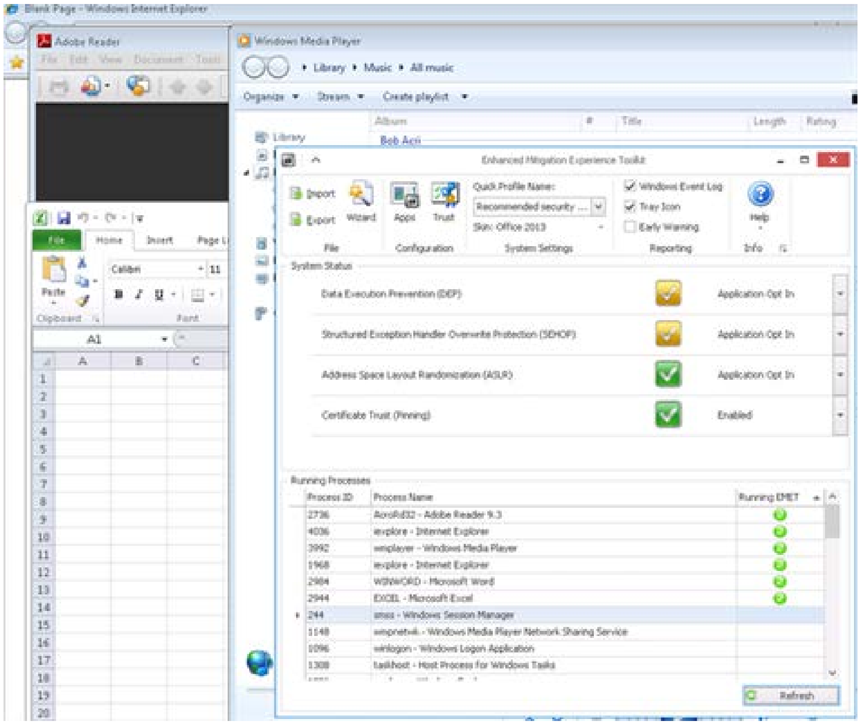
Appearance

Figure 89 – IE Home Page

3. Optional. You may enable items on the **Internet Properties** window. To do so, select **Security > Internet Zone > Settings**. The default settings should be fine.
4. Click **OK** to save your settings, and close the Control Panel.

Step 10: Configure Enhanced Mitigation Experience Toolkit (EMET)

1. Open EMET.
2. From **Apps > Default action > Stop On Exploit**, select from their locations on the hard disk/s:
   - Adobe Acrobat
   - All Office programs (six)
   - Windows Media Player
   - Internet Explorer
3. On the on the **Enhanced Mitigation Experience Toolkit** window, click **Apps** to open the **Application Configuration** window, and enable all metrics for all programs.
4. Close EMET and all other programs.
5. Open EMET.
6. Open two or three programs, and verify each shows as "**Running EMET**" on the EMET window under **Running Processes**.



Quick Profile Name: Recommended security ...

Skin: Office 2013

☑ Windows Event Log

☑ Tray Icon

□ Early Warning

System Status

Data Execution Prevention (DEP)	✓	Application Opt In
Structured Exception Handler Overwrite Protection (SEHOP)	✓	Application Opt In
Address Space Layout Randomization (ASLR)	✓	Application Opt In
Certificate Trust (Pinning)	✓	Enabled

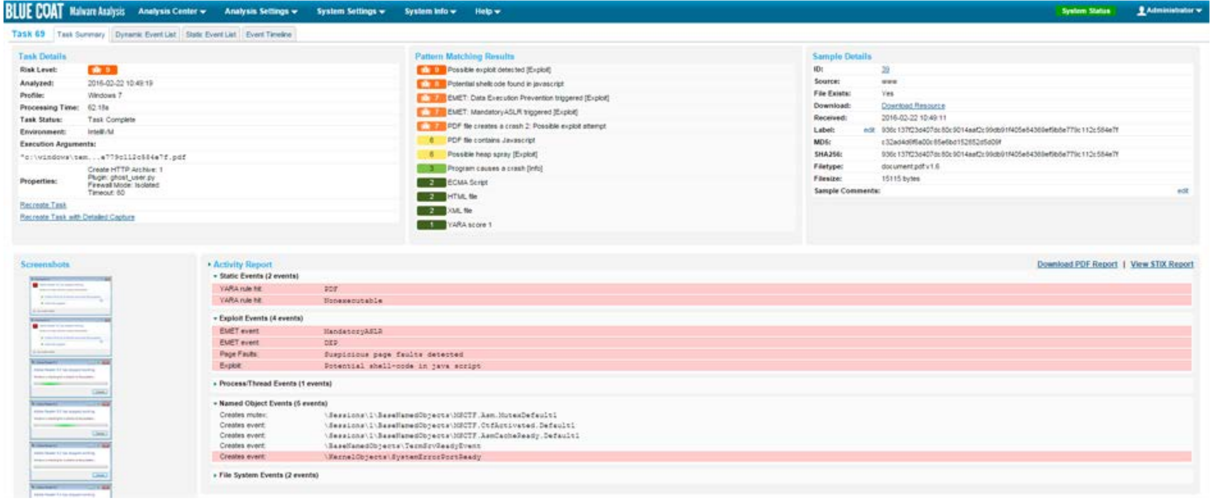
Running Processes

Process ID	Process Name	Running EMET
2736	AcroRd32 - Adobe Reader 9.3	●
4036	iexplore - Internet Explorer	●
3992	wmplayer - Windows Media Player	●
1968	iexplore - Internet Explorer	●
2984	WINWORD - Microsoft Word	●
2944	EXCEL - Microsoft Excel	●
244	smss - Windows Session Manager	
1148	wmpnetwk - Windows Media Player Network Sharing Service	
1096	winlogon - Windows Logon Application	
1308	taskhost - Host Process for Windows Tasks	

Figure 90 – Programs Running EMET

Step 11: *Verify Installations*

1. Finalize and Build the Profile.
2. Verify EMET works:
   - Get sample C32AD4D6F6A00C85E6BD152852D5D09F.
   - Submit the sample to the Malware Analysis appliance.
   - Verify that EMET results are shown in the task results.



Task Details

Risk Level:	9
Analyzed:	2016-02-22 10:49:19
Profile:	Windows 7
Processing Time:	62.18s
Task Status:	Task Complete
Environment:	IntelliVM
Execution Arguments:	
"c:\windows\tem...e779c112c584e7f.pdf	
Properties:	Create HTTP Archive: 1 Plugin: ghost_user.py Firewall Mode: Isolated Timeout: 60

Recreate Task

Recreate Task with Detailed Capture

Pattern Matching Results

9	Possible exploit detected [Exploit]
8	Potential shellcode found in javascript
7	EMET: Data Execution Prevention triggered [Exploit]
7	EMET: MandatoryASLR triggered [Exploit]
7	PDF file creates a crash 2: Possible exploit attempt
6	PDF file contains Javascript
6	Possible heap spray [Exploit]
3	Program causes a crash [Info]
2	ECMA Script
2	HTML file
2	XML file
1	YARA score 1

Sample Details

ID:	39
Source:	www
File Exists:	Yes
Download:	Download Resource
Received:	2016-02-22 10:49:11
Label: edit	936c137f23d407dc80c9014aaf2c99db91f405e84369ef6b6e779c112c584e7f
MD5:	c32ad4d6f6a00c85e6bd152852d5d09f
SHA256:	936c137f23d407dc80c9014aaf2c99db91f405e84369ef6b6e779c112c584e7f
Filetype:	document.pdf.v1.6
Filesize:	15115 bytes
Sample Comments:	edit

Activity Report

- Static Events (2 events)

YARA rule hit:	PDF
YARA rule hit:	Nonexecutable

- Exploit Events (4 events)

EMET event:	MandatoryASLR
EMET event:	DEP
Page Faults:	Suspicious page faults detected
Exploit:	Potential shell-code in java script

- Process/Thread Events (1 events)
- Named Object Events (5 events)

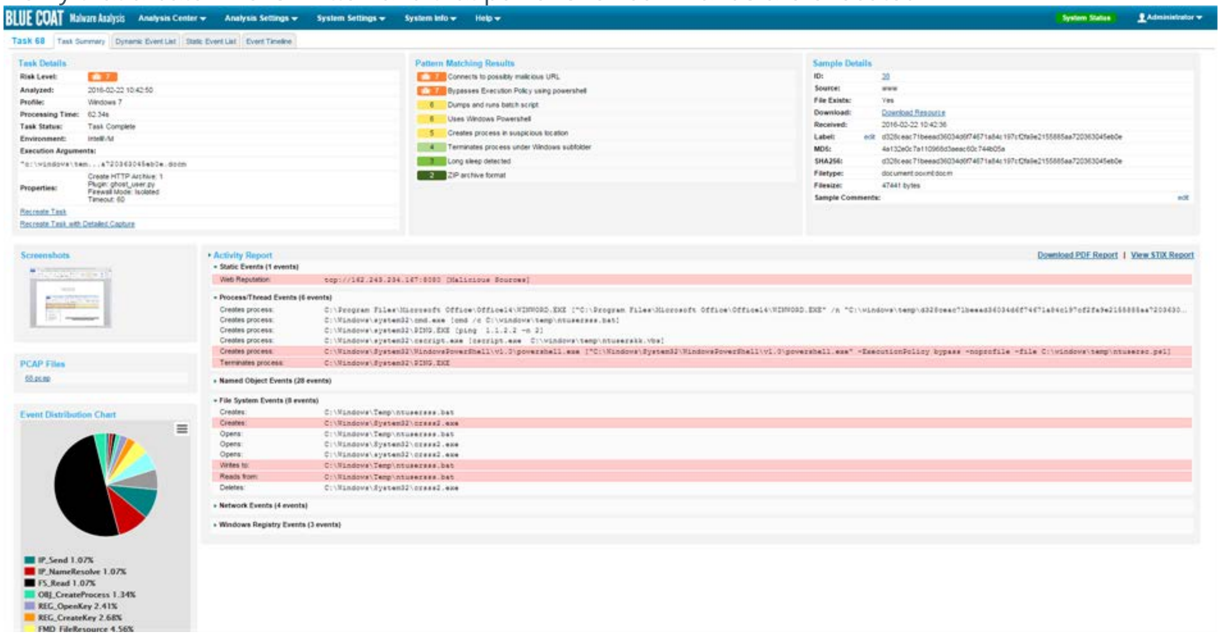
Creates mutex:	\Sessions\1\BaseNamedObjects\MSCTF.Asm.MutexDefault1
Creates event:	\Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1
Creates event:	\Sessions\1\BaseNamedObjects\MSCTF.AsmCacheReady.Default1
Creates event:	\BaseNamedObjects\TermSrvReadyEvent
Creates event:	\KernelObjects\SystemErrorPortReady

- File System Events (2 events)

Figure 91 – Programs Running EMET

3. Verify macros have been enabled, in Word, and elsewhere as required.
   - Get sample 4a132e0c7a110968d3aeac60c744b05a
   - Submit the sample to the Malware Analysis appliance.

- Verify that a batch file is written and that power shell commands are executed.



Task Details

Risk Level:	7
Analyzed:	2016-02-22 10:42:50
Profile:	Windows 7
Processing Time:	62.34s
Task Status:	Task Complete
Environment:	IntelliVM
Execution Arguments:	
"c:\windows\tem...a720363045eb0e.docm	
Properties:	Create HTTP Archive: 1 Plugin: ghost_user.py Firewall Mode: Isolated Timeout: 60

Recreate Task

Recreate Task with Detailed Capture

Pattern Matching Results

7	Connects to possibly malicious URL
7	Bypasses Execution Policy using powershell
6	Dumps and runs batch script
6	Uses Windows Powershell
5	Creates process in suspicious location
4	Terminates process under Windows subfolder
3	Long sleep detected
2	ZIP archive format

Sample Details

ID:	30
Source:	www
File Exists:	Yes
Download:	Download Resource
Received:	2016-02-22 10:42:36
Label: edit	d328ceac71beead36034d6f74671a84c197cf2fa9e2155885aa720363045eb0e
MD5:	4a132e0c7a110968d3eeac60c744b05a
SHA256:	d328ceac71beead36034d6f74671a84c197cf2fa9e2155885aa720363045eb0e
Filetype:	document.ooxml.docm
Filesize:	47441 bytes
Sample Comments:	edit

Screenshots

PCAP Files

68.pcap

Event Distribution Chart

Activity Report

Download PDF Report | View STIX Report

```
▾ Static Events (1 events)
Web Reputation:       tcp://142.243.234.147:8080 [Malicious Sources]

▾ Process/Thread Events (6 events)
Creates process:      C:\Program Files\Microsoft Office\Office14\WINWORD.EXE ["C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /n "C:\windows\temp\d328ceac71beead36034d6f74671a84c197cf2fa9e2155885aa7203630...
Creates process:      C:\Windows\system32\cmd.exe [cmd /c C:\windows\temp\ntuserxss.bat]
Creates process:      C:\Windows\system32\PING.EXE [ping  1.1.2.2 -n 3]
Creates process:      C:\Windows\system32\cscript.exe [cscript.exe  C:\windows\temp\ntuserxkk.vbs]
Creates process:      C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe ["C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ExecutionPolicy bypass -noprofile -file C:\windows\temp\ntuserxc.ps1]
Terminates process:   C:\Windows\System32\PING.EXE

▸ Named Object Events (28 events)

▾ File System Events (8 events)
Creates:              C:\Windows\Temp\ntuserxss.bat
Creates:              C:\Windows\System32\crsss2.exe
Opens:                C:\Windows\Temp\ntuserxss.bat
Opens:                C:\Windows\System32\crsss2.exe
Opens:                C:\Windows\system32\crsss2.exe
Writes to:            C:\Windows\Temp\ntuserxss.bat
Reads from:           C:\Windows\Temp\ntuserxss.bat
Deletes:              C:\Windows\System32\crsss2.exe

▸ Network Events (4 events)

▸ Windows Registry Events (3 events)
```

Figure 92 – Executed Commands

Related Documentation

- Installing EMET; see ***Error! Reference source not found.***.
- Macro configuration in Microsoft Office: https://support.office.com/en-us/article/Enable-or-disable-macros-in-Office-documents-7b4fdd2e-174f-47e2-9611-9efe4f860b12

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE. SYMMANTEC CORPORATION PRODUCTS, TECHNICAL SERVICES, AND ANY OTHER TECHNICAL DATA REFERENCED IN THIS DOCUMENT ARE SUBJECT TO U.S. EXPORT CONTROL AND SANCTIONS LAWS, REGULATIONS AND REQUIREMENTS, AND MAY BE SUBJECT TO EXPORT OR IMPORT REGULATIONS IN OTHER COUNTRIES. YOU AGREE TO COMPLY STRICTLY WITH THESE LAWS, REGULATIONS AND REQUIREMENTS, AND ACKNOWLEDGE THAT YOU HAVE THE RESPONSIBILITY TO OBTAIN ANY LICENSES, PERMITS OR OTHER APPROVALS THAT MAY BE REQUIRED IN ORDER TO EXPORT, RE-EXPORT, TRANSFER IN COUNTRY OR IMPORT AFTER DELIVERY TO YOU.

Symantec Corporation
350 Ellis Street, Mountain View, CA 94043
www.symantec.com