

AppLoader7

Windows Server 2008
Injector Optimization



Protocol Independent
Load Testing

CONTENTS

PREREQUISITES	3
INTRODUCTION.....	3
INJECTOR OPTIMIZATIONS.....	3
GROUP POLICY CONFIGURATIONS	3
<i>Internet Explorer - Disable AutoComplete and HTTP Error Message Pop-Ups.....</i>	<i>3</i>
<i>Internet Explorer - Enable Sending of Non-Encrypted Data (without "Warning" Message).....</i>	<i>5</i>
<i>Internet Explorer - Empty Temporary Internet Files Folder</i>	<i>7</i>
<i>Internet Explorer - Prevent IE "Welcome" Message</i>	<i>9</i>
SERVER MANAGER CONFIGURATIONS.....	10
<i>Internet Explorer - Disable IE Enhanced Security Configuration</i>	<i>10</i>
<i>Allow Remote Desktop Connections to the Injector Server.....</i>	<i>12</i>
<i>Enable "Terminal Services" (known as "Remote Desktop Services" in Windows Server 2008 R2)</i>	<i>13</i>
ADVANCED OPTIMIZATIONS	18
<i>[Optional] Settings for Best Performance.....</i>	<i>18</i>
AFTER MAKING CHANGES	21
CLONING INJECTORS ON VIRTUAL SERVERS	21
UPDATE VSTATION.INI FILE	21

PREREQUISITES

Before proceeding ensure that the following NRG Global products are installed:

- ✓ ScenarioBuilder
- ✓ AppLoader
- ✓ Injector

Note that these applications may all be installed on the same Windows Server or on separate machines.

INTRODUCTION

This document will outline the steps to properly configure Windows Server 2008 for optimal use as an AppLoader Injector.

When working with **Virtual Machines**, we recommend completing the configuration steps outlined in this document and running a typical load test to see how many rUsers your server can handle. Once you are happy with the performance of this prototypical server, clone the server to create additional Injectors. For details and tips on cloning Injectors, please refer to the [Cloning Injectors on Virtual Servers](#) section of this guide.

INJECTOR OPTIMIZATIONS

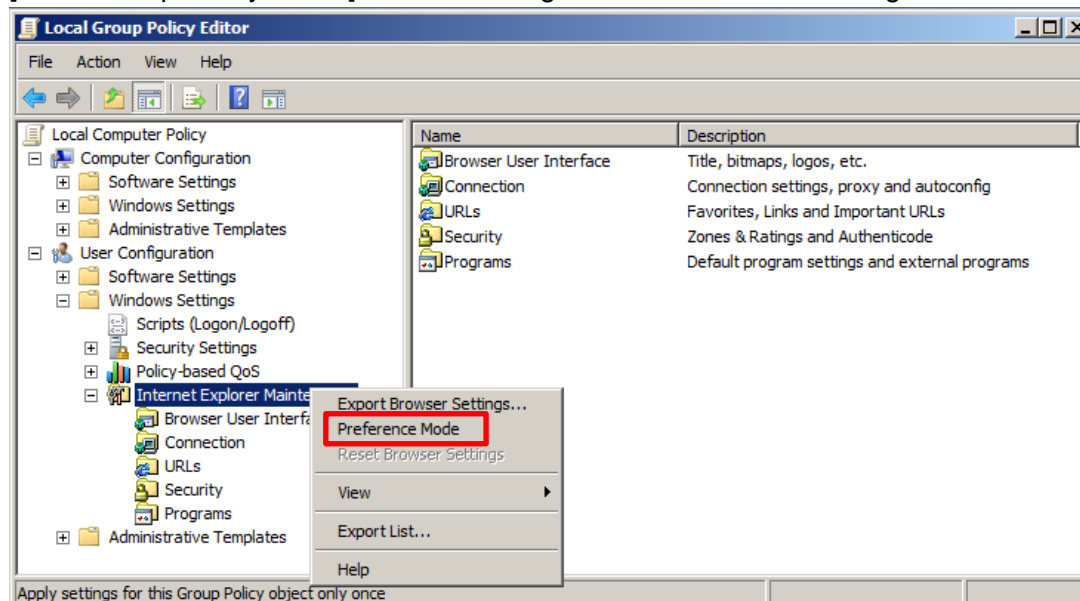
GROUP POLICY CONFIGURATIONS

INTERNET EXPLORER - DISABLE *AUTOCOMplete* AND HTTP ERROR MESSAGE POP-UPS

Go to the Group Policy Object Editor (GPO): Start → Run → type **gpedit.msc**.

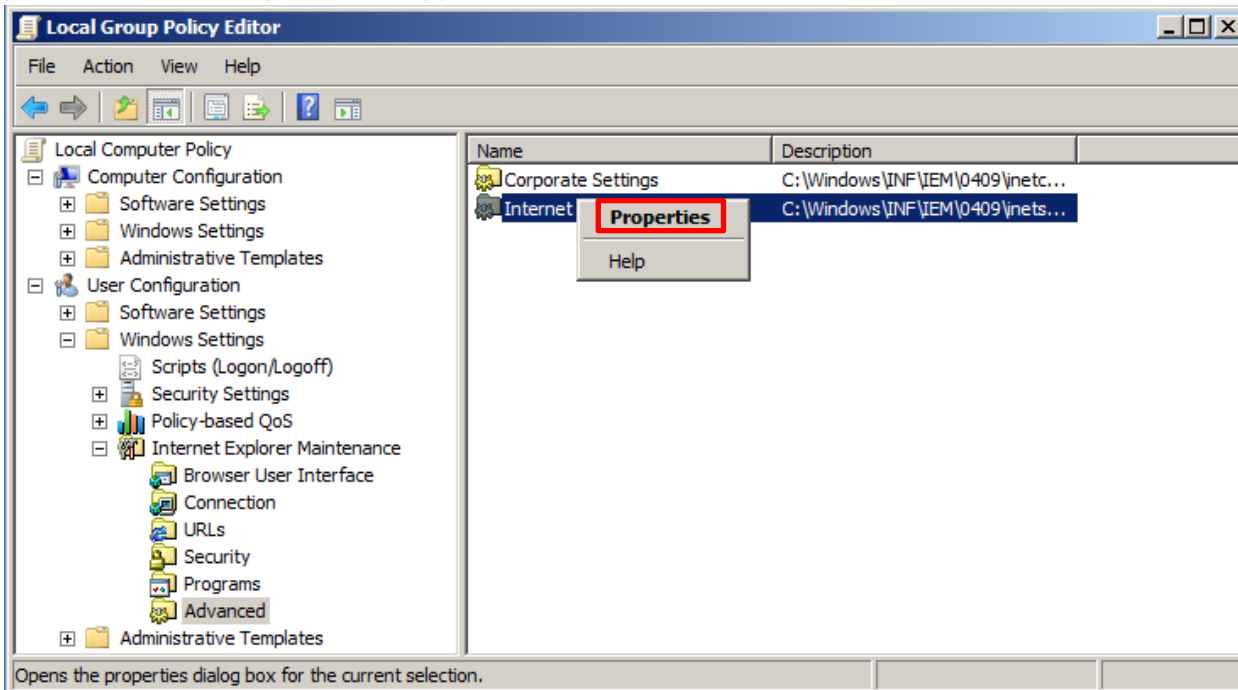
1. Right click on “Internet Explorer Maintenance” and select “Preference Mode”

[Local Group Policy Editor] → User Configuration → Windows Settings → Internet Explorer Maintenance

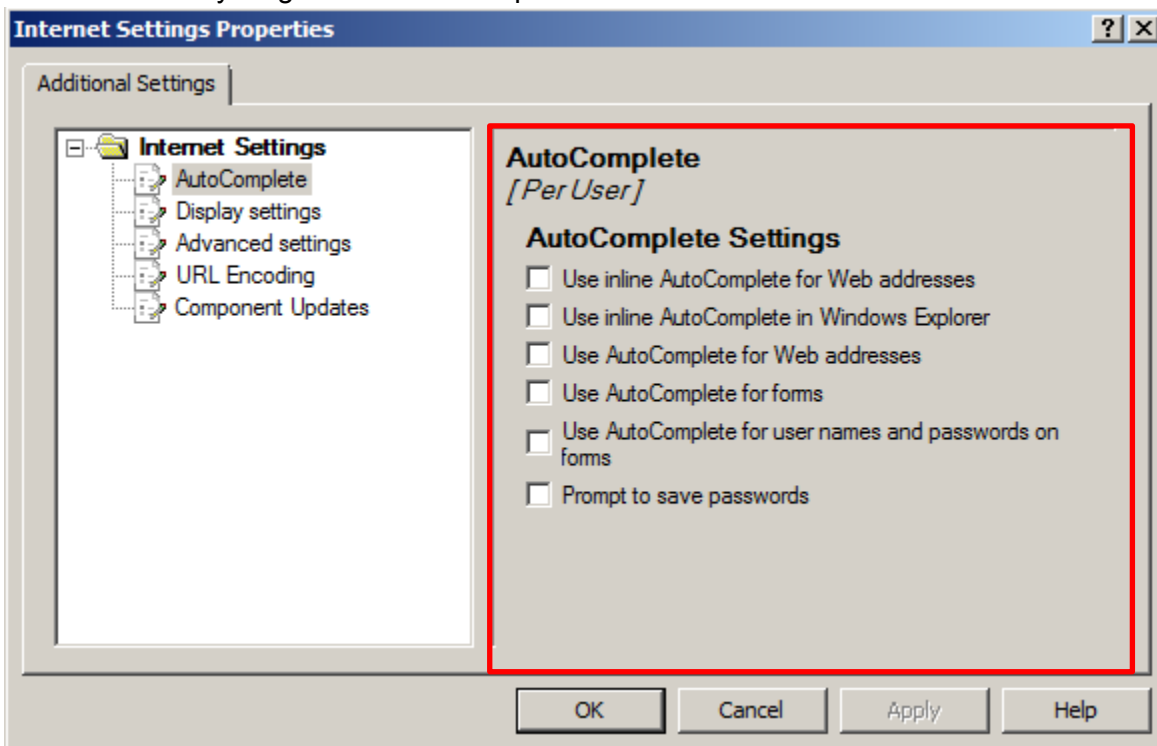


2. Select the “Advanced” folder from the tree hierarchy. In the window to the right, right click the “Internet Settings” and select “Properties”.

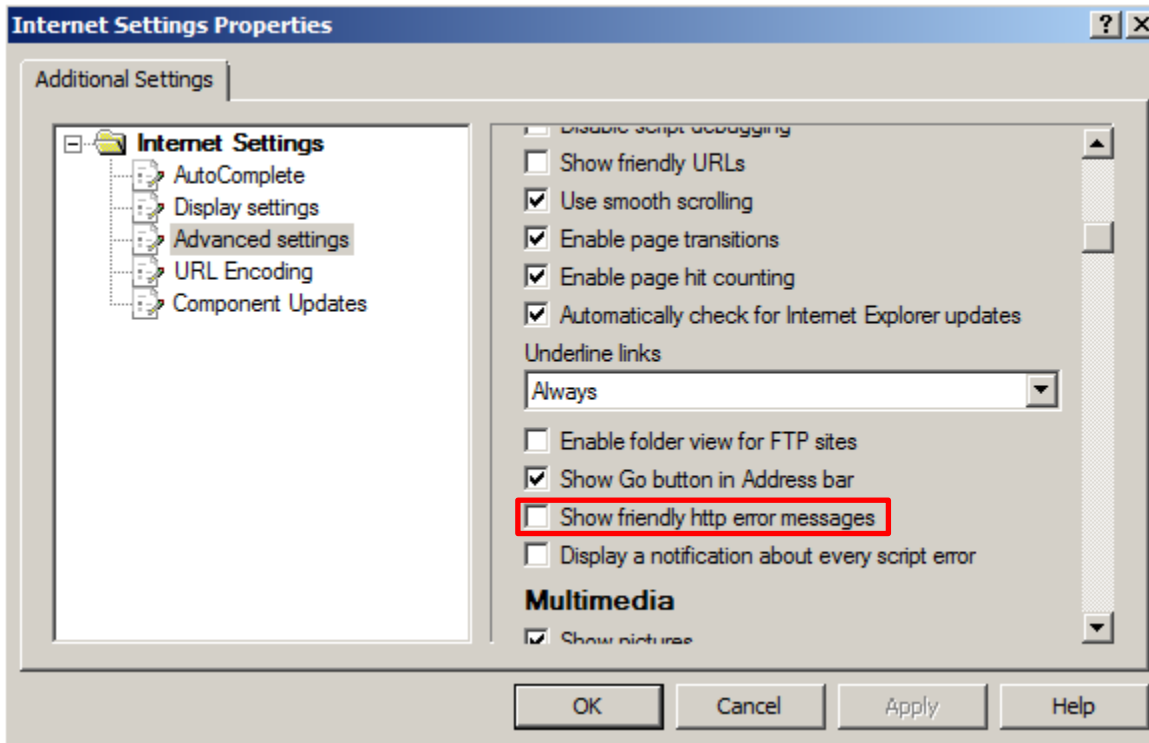
[Local Group Policy Editor]→ UserConfiguration→Internet Explorer Maintenance → Advanced (after clicking on preference mode in previous step)



3. Uncheck everything in the “AutoComplete” section



4. Uncheck “Show friendly http error messages” in “Advanced settings”



5. Click “OK” to save settings and close the windows.

INTERNET EXPLORER - ENABLE SENDING OF NON-ENCRYPTED DATA (WITHOUT “WARNING” MESSAGE)

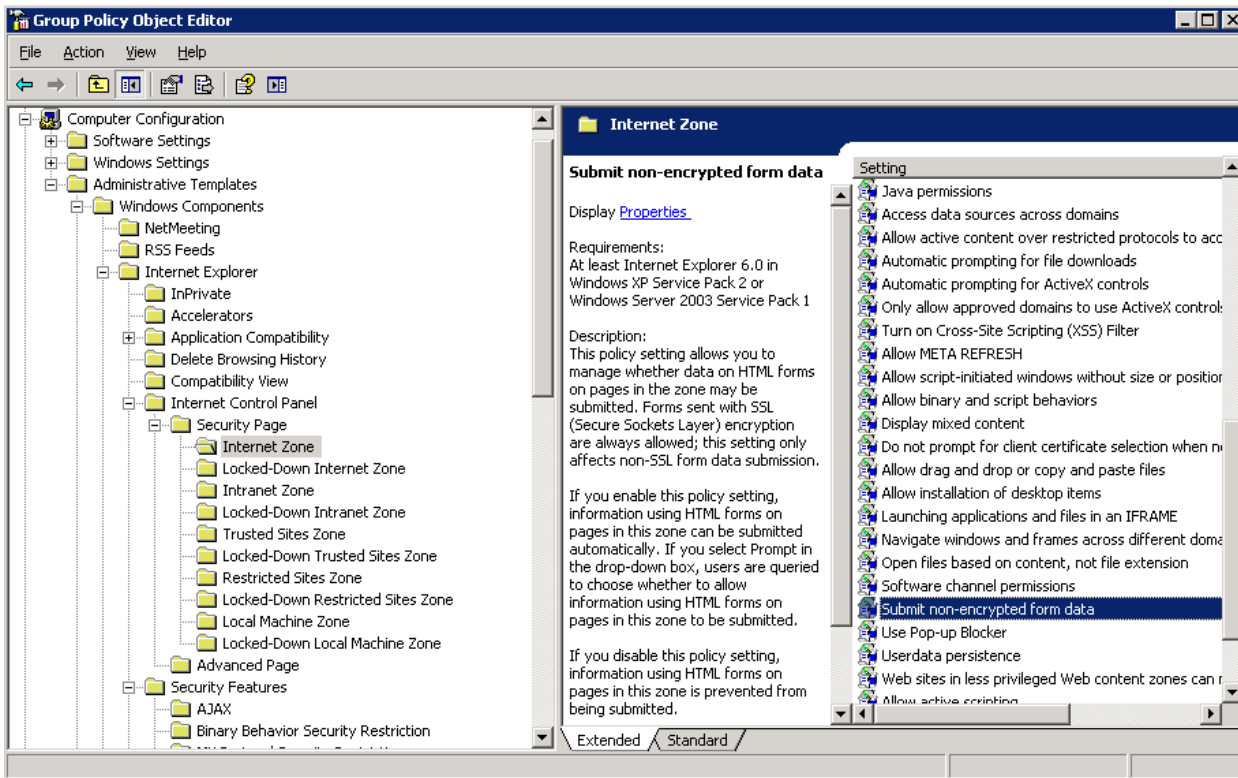
Prevent the following pop-up from occurring in Internet Explorer:



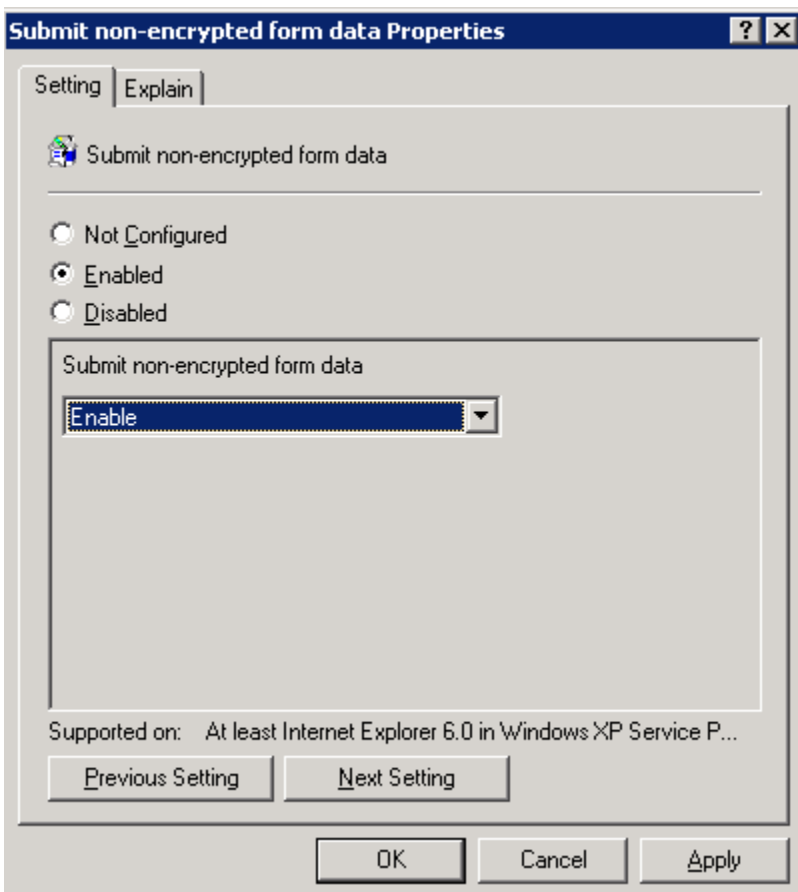
In Group Policy Object Editor, navigate to “Internet Zone” settings and Enable “Submit non-encrypted form data”:

[Group Policy Object Editor] → Computer Configuration → Administrative Templates → Windows Components → Internet Explorer → Internet Control Panel → Internet Zone

In the right pane, right-click “Submit non-encrypted form data”



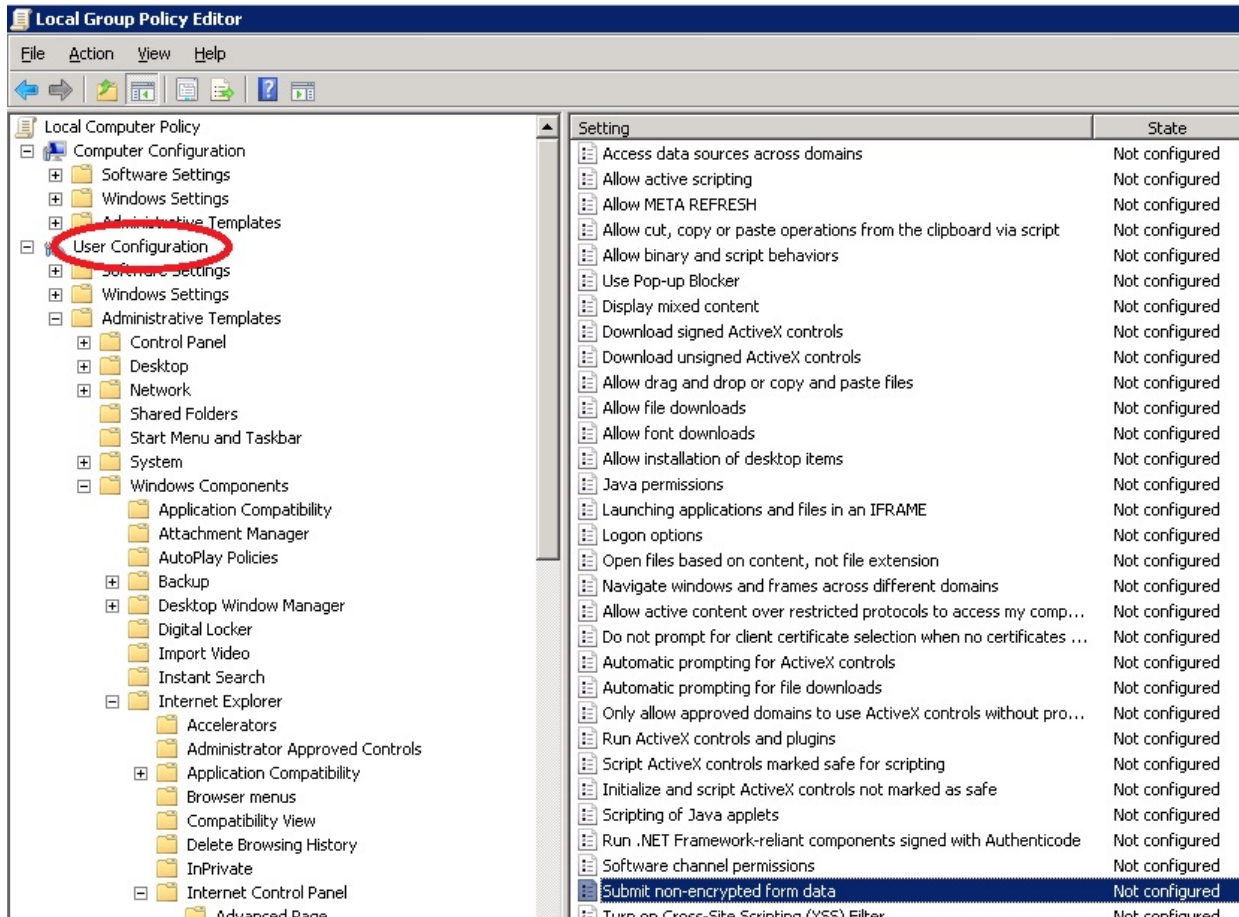
Check “Enabled” and click “Apply”.



Repeat for “User Configuration”

Group Policy Object Editor → User Configuration→ Administrative Templates →
Windows Components→ Internet Explorer→ Internet Control Panel → Internet Zone

In the right pane click “Submit non-encrypted form data”



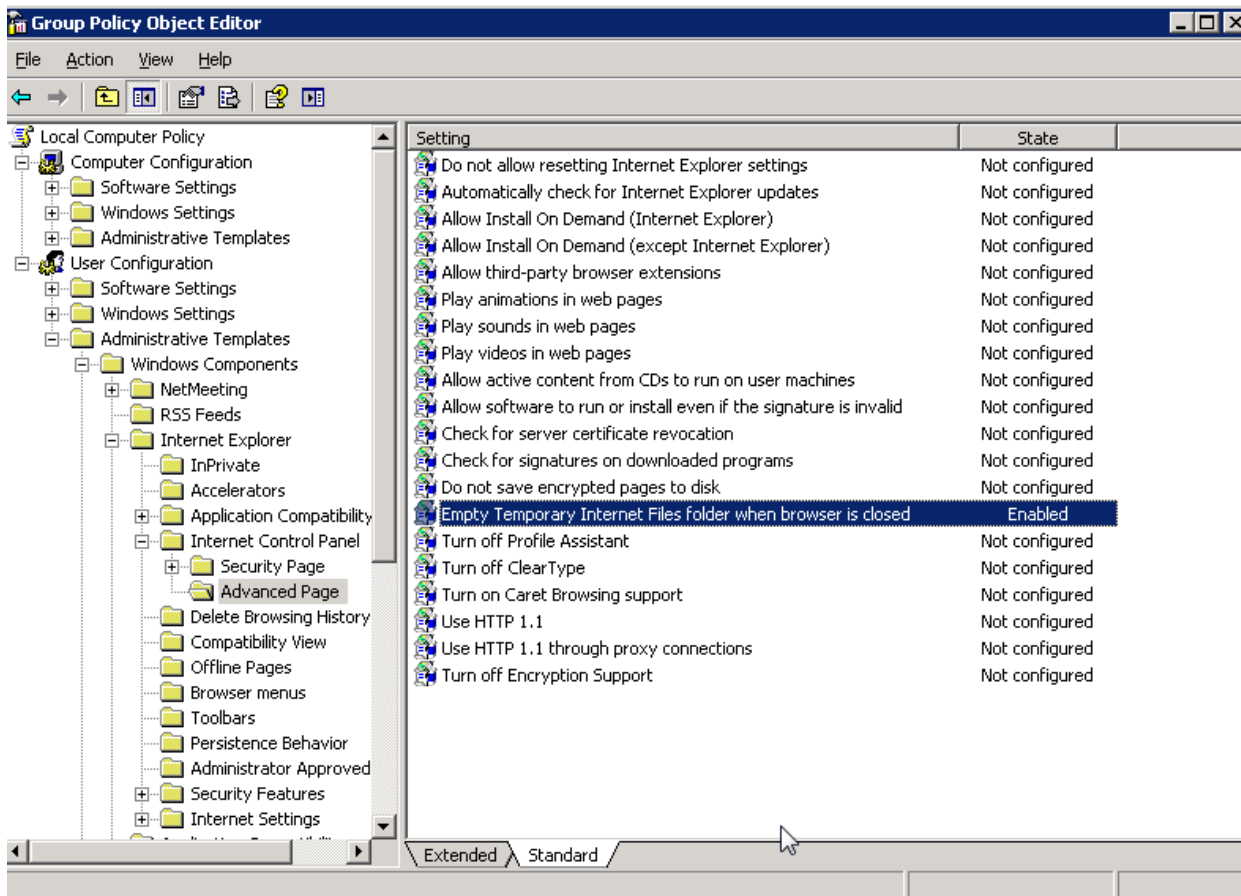
INTERNET EXPLORER - EMPTY TEMPORARY INTERNET FILES FOLDER

Enable “Empty Temporary Internet Files folder when browser is closed” setting in Group Policy Object Editor to clear the browser cache.

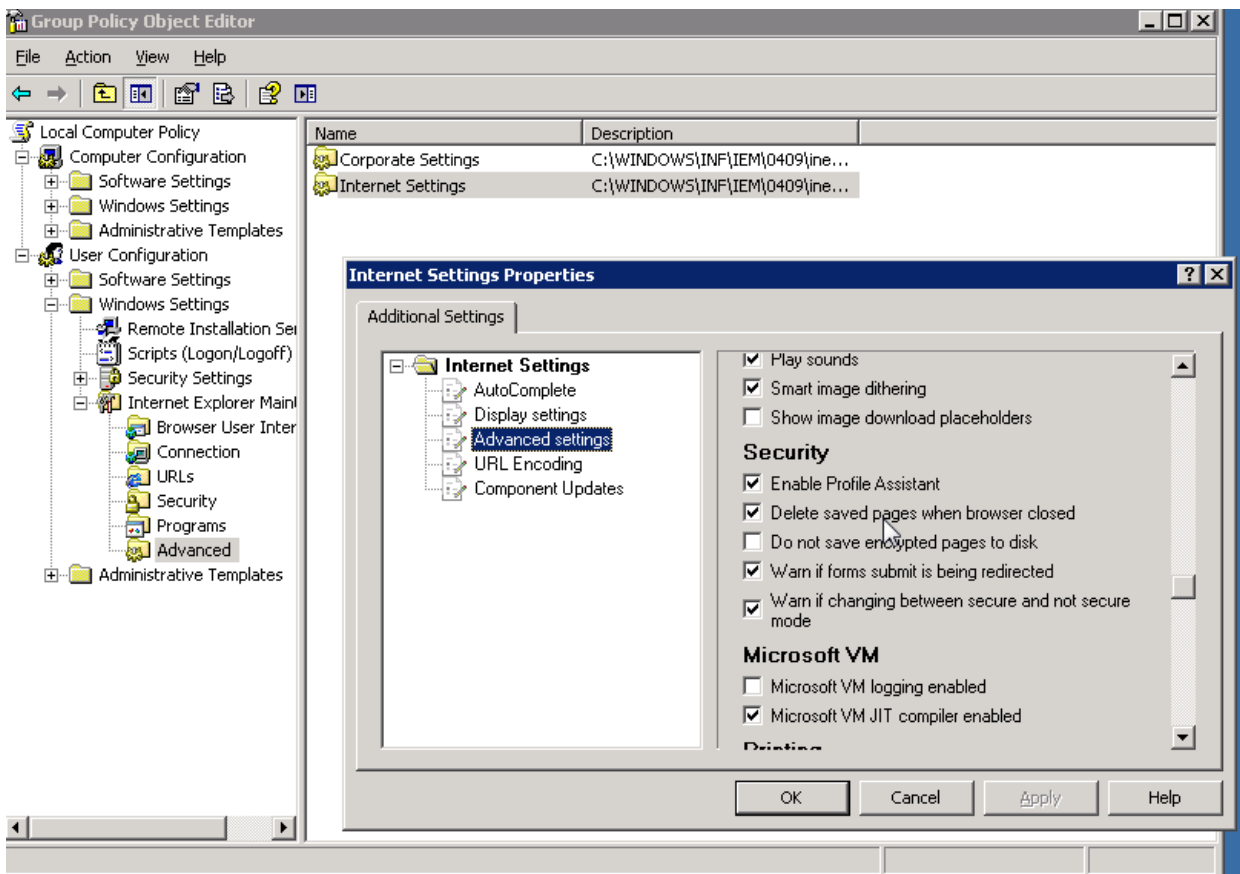
Go to the Group Policy Object Editor (GPO): Start → Run→ type **gpedit.msc**.

From “Administrative Templates” drill down to “Windows Components” → “Internet Explorer” → “Internet Control Panel” → “Advanced Page”.

Double click on “Advanced Page” to bring up the list of settings in the right pane. Find “Empty Temporary Internet Files folder when browser is closed” and right-click on it.



Select "Edit". Check "Delete saved pages when browser closed" in Advanced Settings – Security section:



Click “OK” and close Group Policy Object Editor.

INTERNET EXPLORER - PREVENT IE “WELCOME” MESSAGE

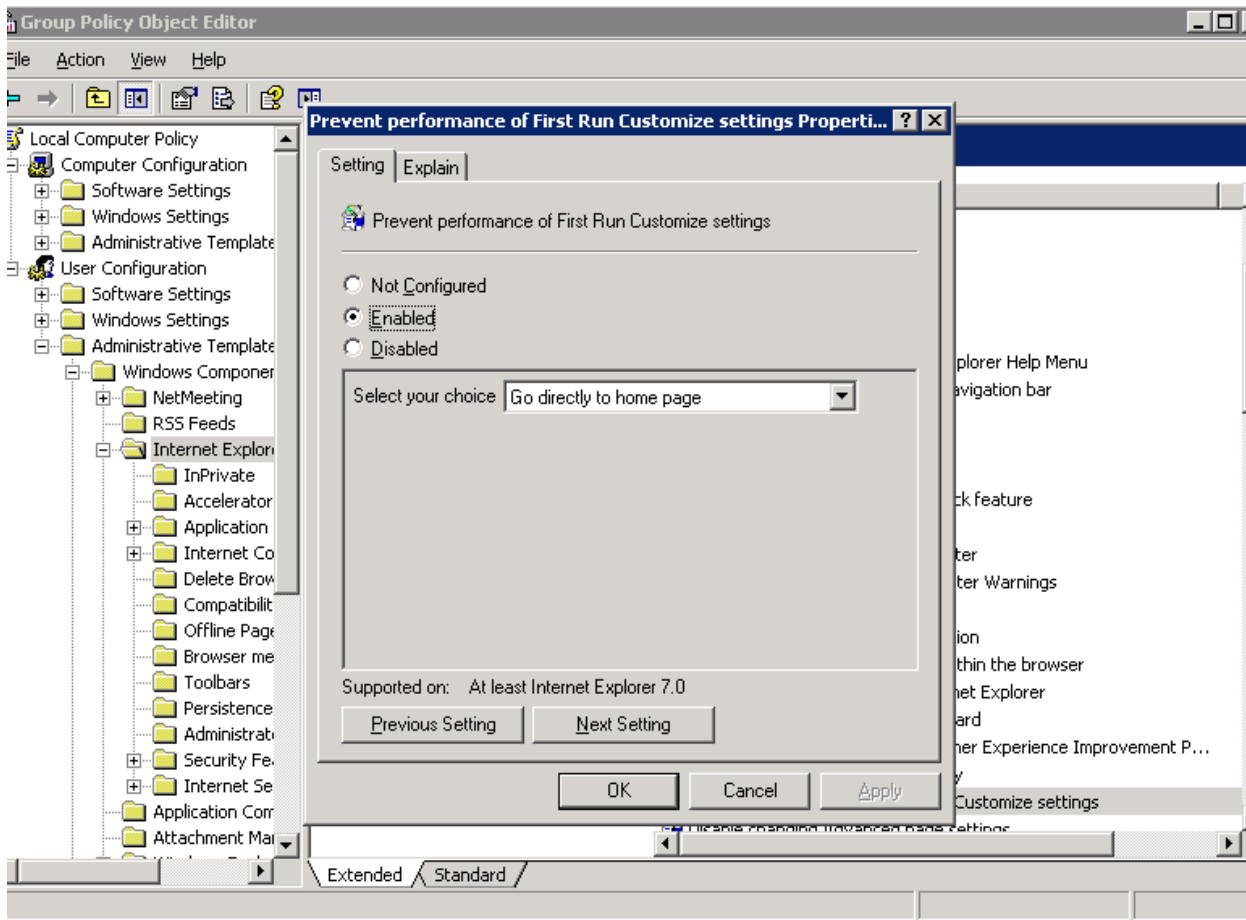
Prevent the following pop-up from occurring when opening Internet Explorer:



Go to the Group Policy Object Editor (GPO): Start → Run → type **gpedit.msc**.

From “Administrative Templates” drill down to “Windows Components” → “Internet Explorer”.

Double click on “Internet Explorer” to bring up the list of settings in the right pane. Find “Prevent Performance of First Run Customize Settings” and right-click on it. Select “Edit” and click “Enabled”. In the “Options” pane choose “Go directly to home page” from the drop down list. Click “Apply”.



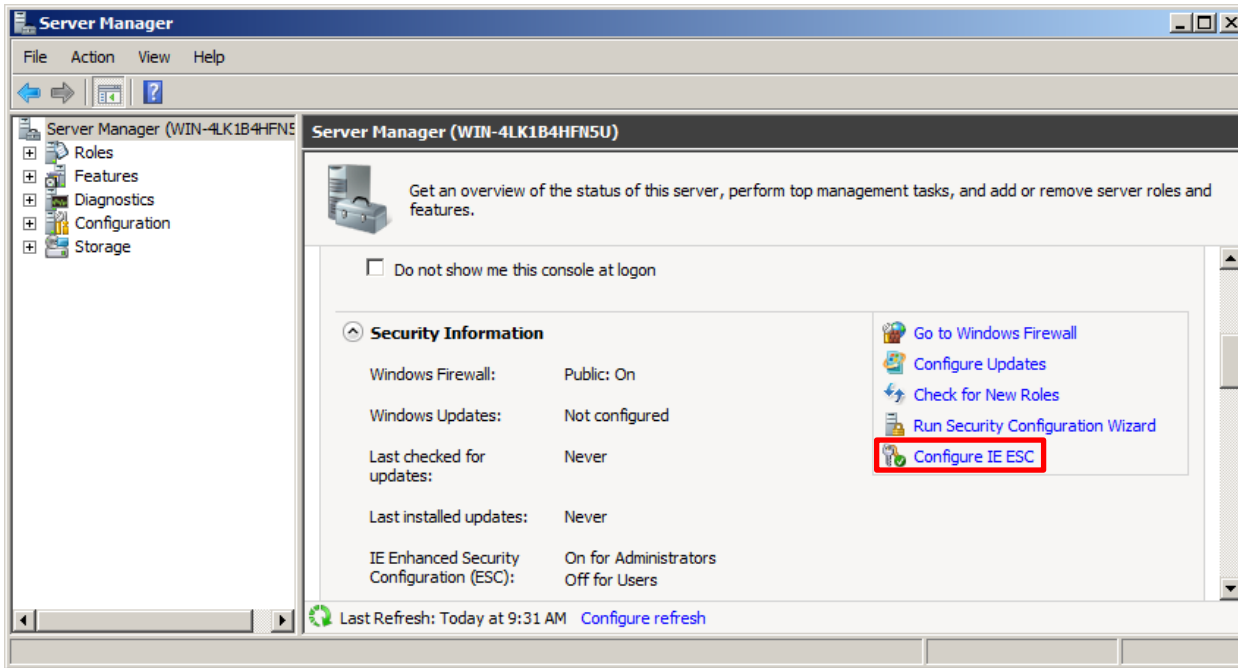
Click “OK” and close Group Policy Object Editor.

SERVER MANAGER CONFIGURATIONS

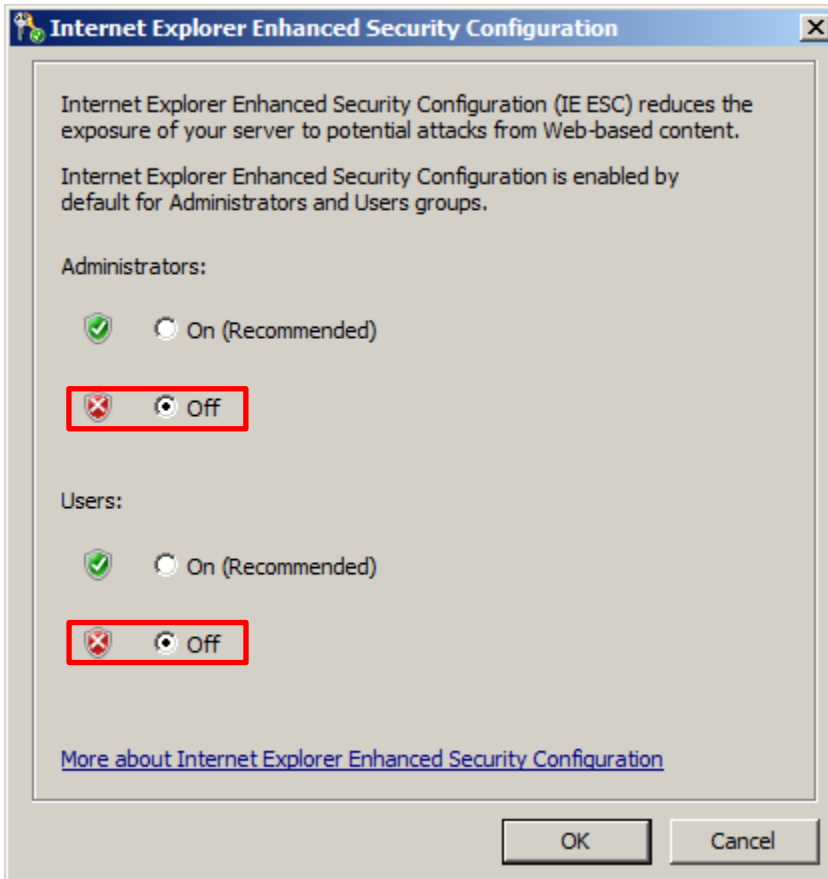
INTERNET EXPLORER - DISABLE IE ENHANCED SECURITY CONFIGURATION

Disable IE “Enhanced Security” to eliminate the majority of Internet Explorer pop-up messages.

Open “Server Manager”: Start → Server Manager (pinned to Start menu) “Security Information” section → Click “Configure IE ESC”



Turn off “Enhanced Security Configuration” for “Administrators” and “Users”

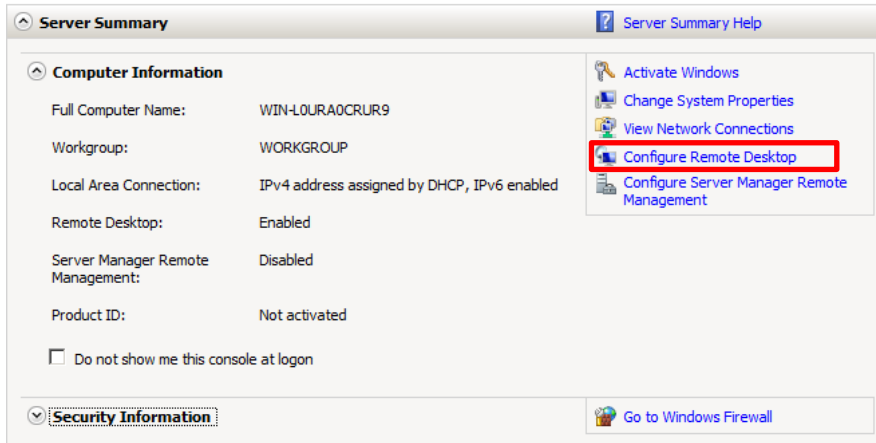


ALLOW REMOTE DESKTOP CONNECTIONS TO THE INJECTOR SERVER

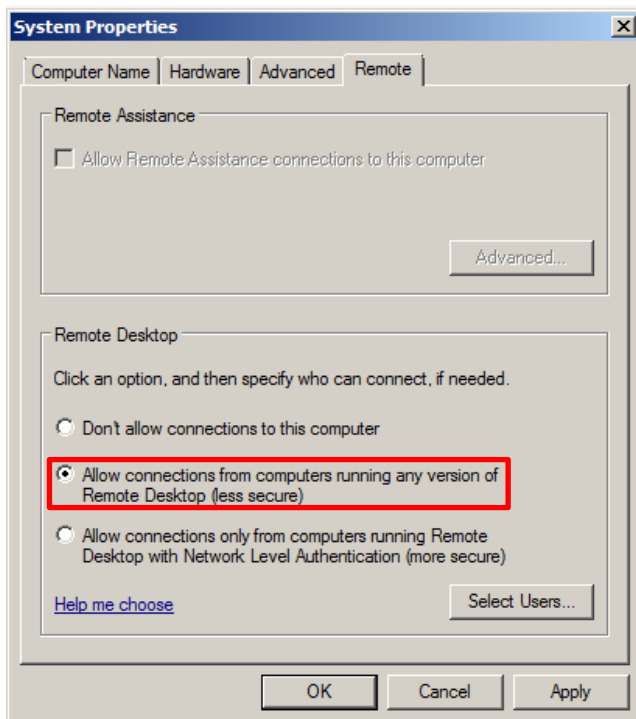
Injectors require that Remote Desktop connections are allowed. Failure to enable this feature will prevent rUsers from starting and logging into Windows.

Open “Server Manager”: Start → Server Manager

Go to the “Server Summary” section → “Configure Remote Desktop”



Click on the radio button “Allow connections from computers running any version of Remote Desktop (less secure).” Then click “Apply” and “OK”

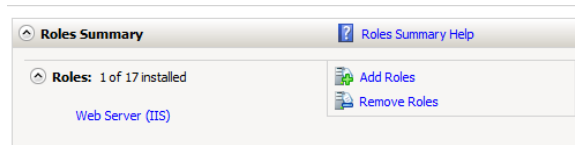


ENABLE “TERMINAL SERVICES” (KNOWN AS “REMOTE DESKTOP SERVICES” IN WINDOWS SERVER 2008 **R2**)

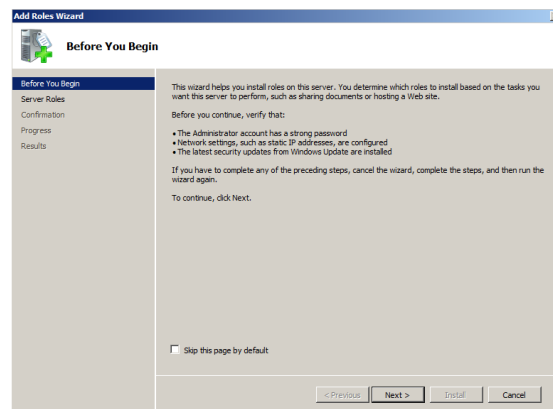
In order for multiple user accounts to login simultaneously on the Injector server, Terminal Services / Remote Desktop Services must be enabled. Terminal Services and Remote Desktop Services provide a 120 day grace period during which no license server is required. During this grace period, your server can accept connections from unlicensed clients without contacting a license server.

To enable Terminal Services / Remote Desktop Services, complete the following steps on your Windows 2008 “Injector” Server:

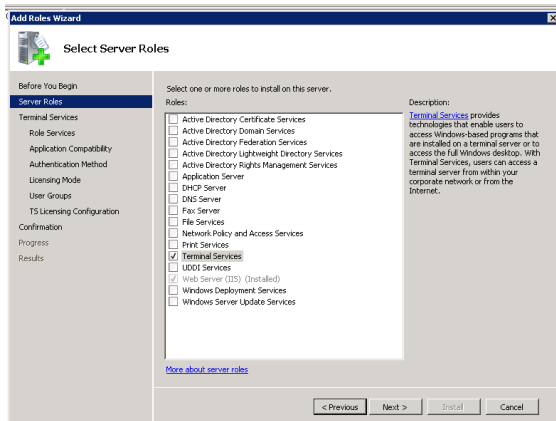
“Server Manager” → “Roles Summary” section → “Add Roles”



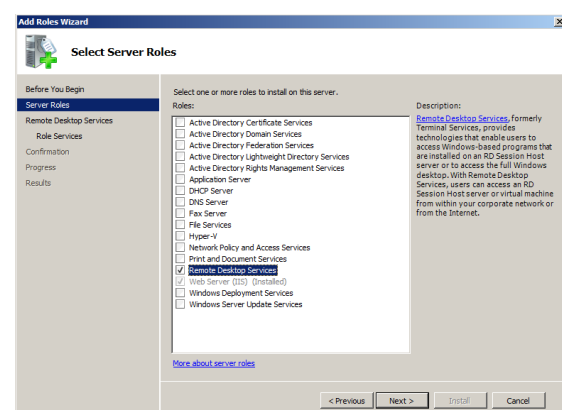
Click “Next”



Click check box for “Terminal Services” (**Server 2008 Standard**); Click “Next”

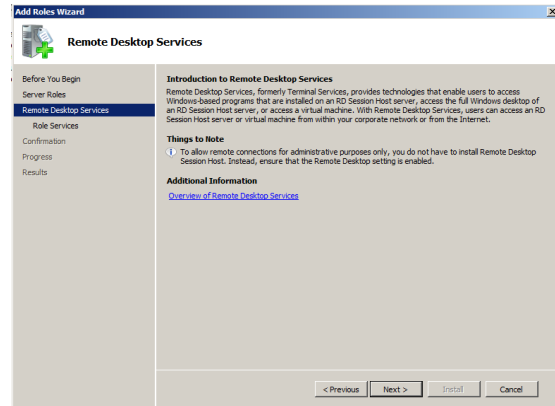
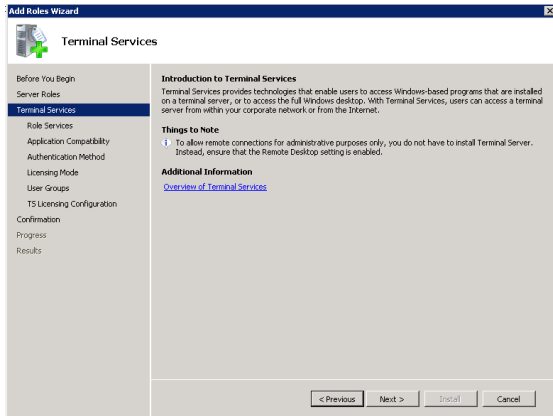


Click check box for “Remote Desktop Services” (**Server 2008 R2**); Click “Next”

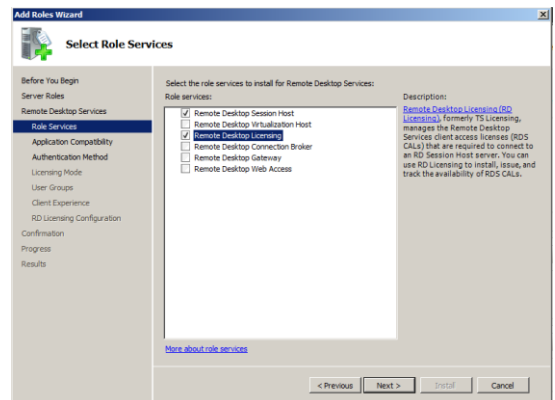
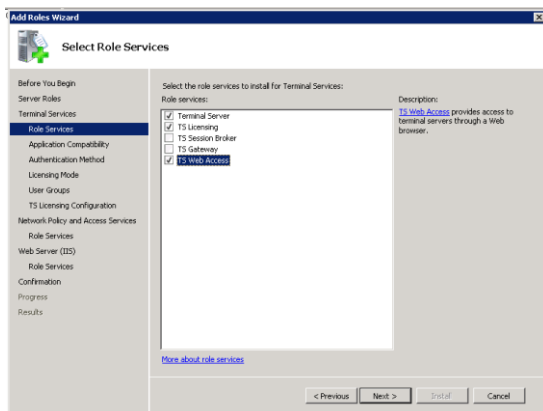




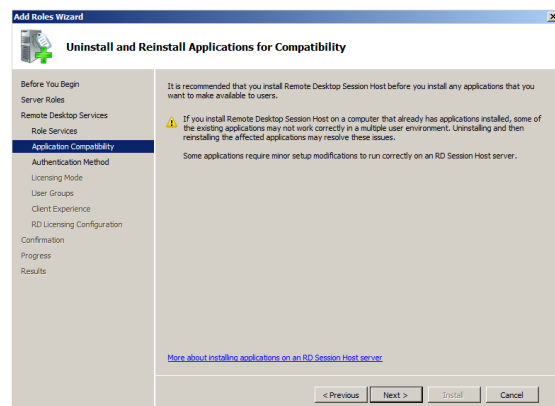
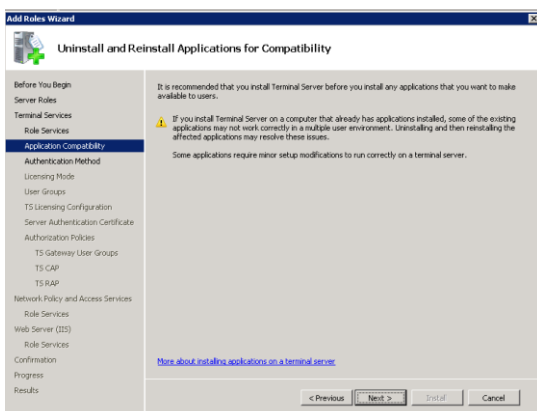
Click “Next”



Click the check boxes next to “Terminal Server”, “TS Licensing” and “TS Web Access”; Click “Next”

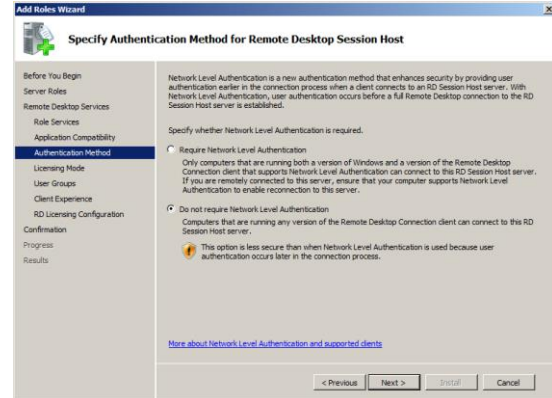
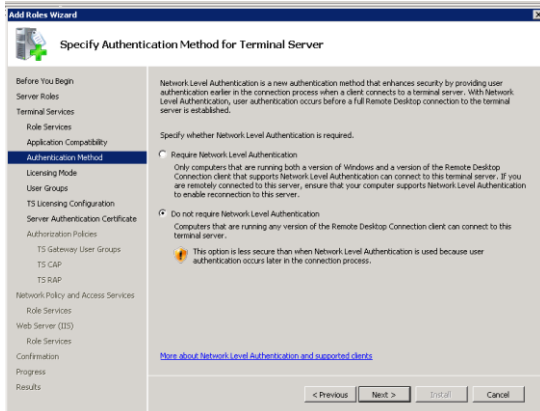


Click “Next”

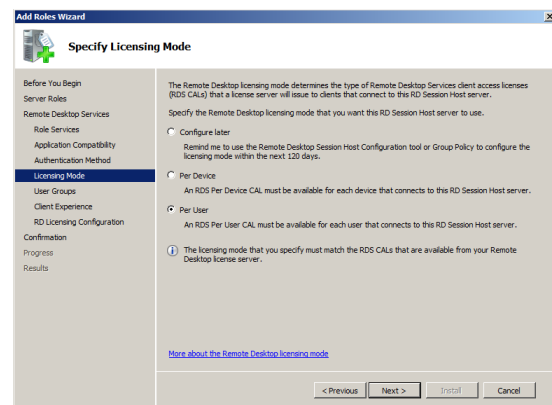
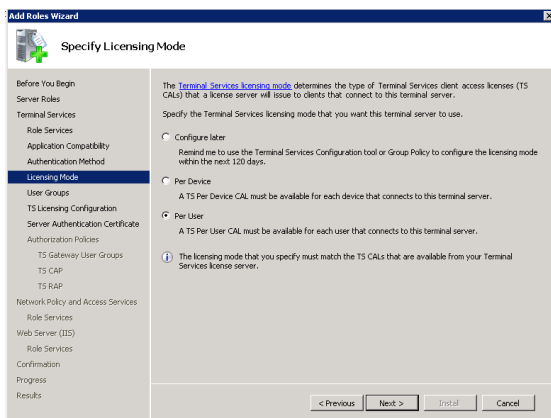




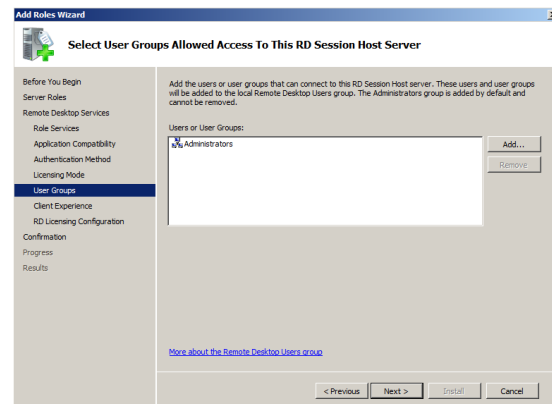
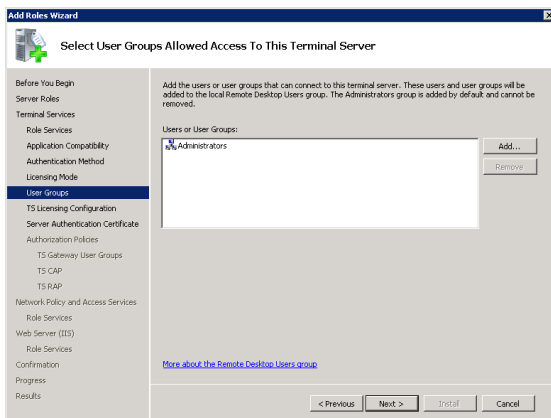
Click the radio button next to “Do not require Network Level Authentication”; Click “Next”



Click the radio button next to “Per User”; Click “Next”



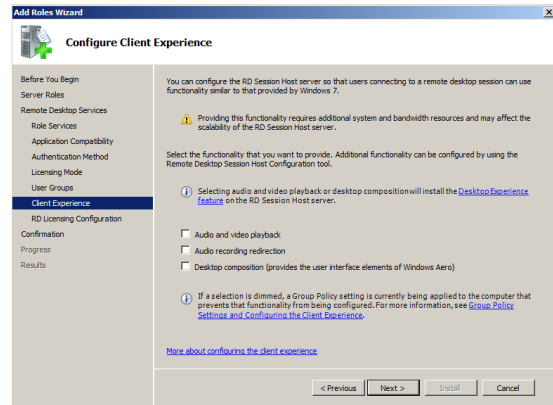
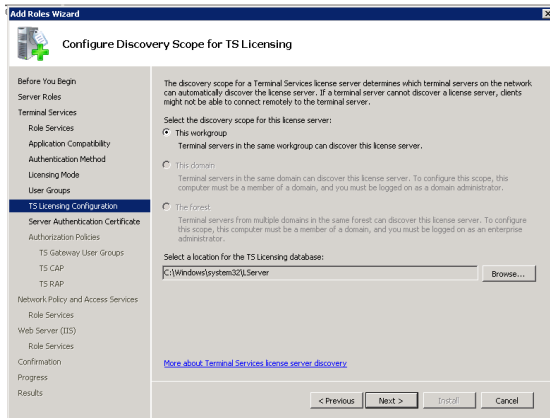
Click “Next”



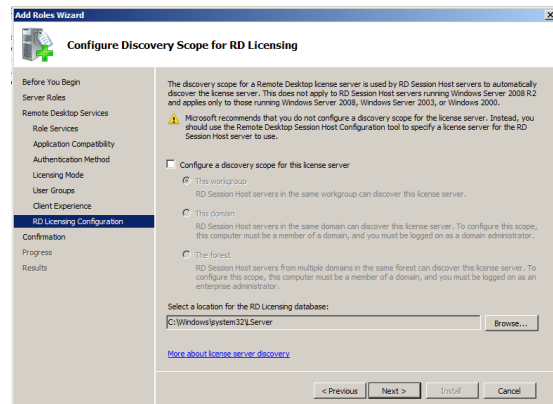
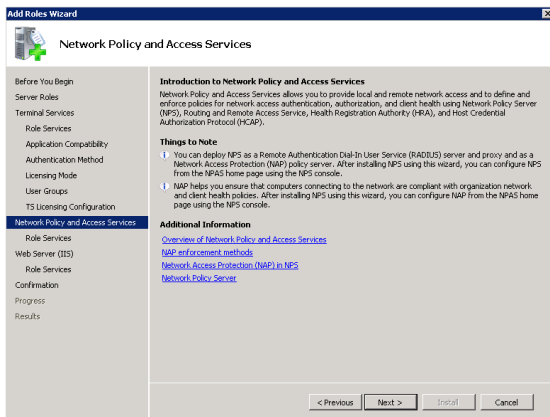
Windows Server 2008 Optimization for AppLoader *Injector*



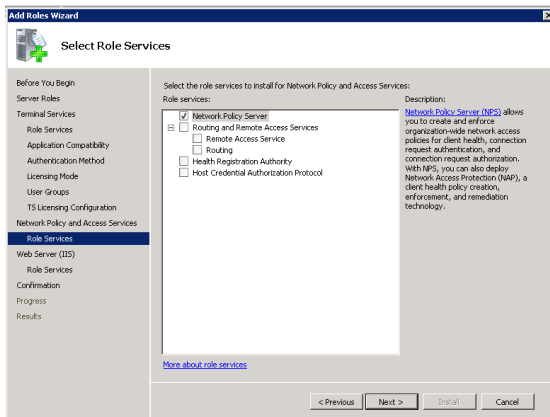
Click “Next”



Click “Next”



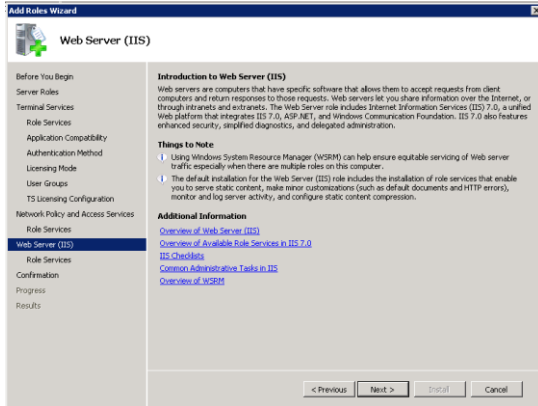
Click “Next”



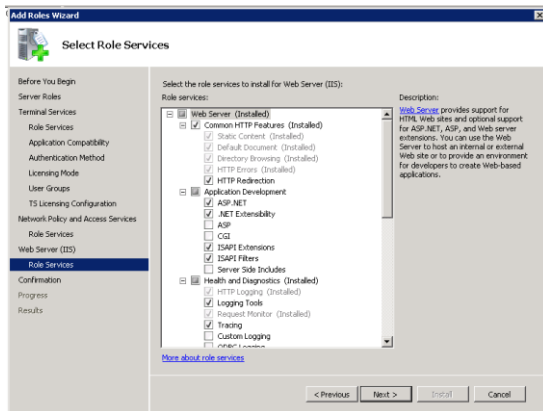
Windows Server 2008 Optimization for AppLoader *Injector*



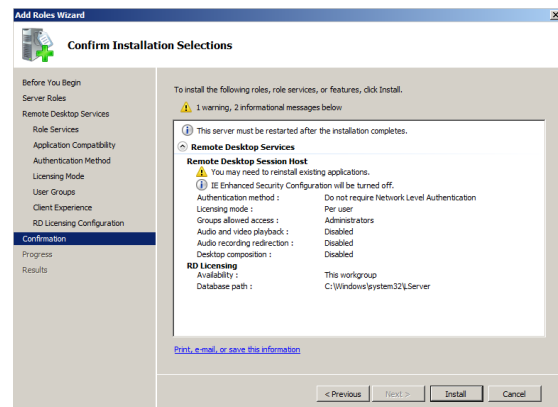
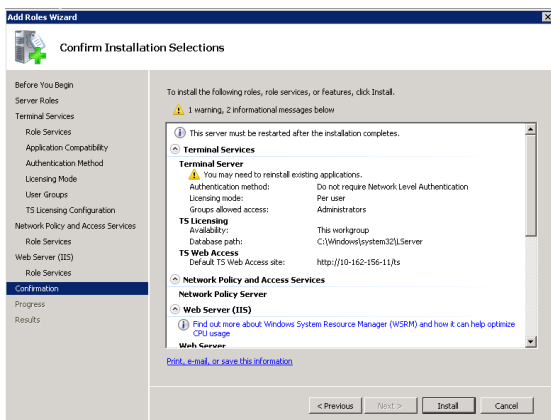
Click “Next”



Click “Next”

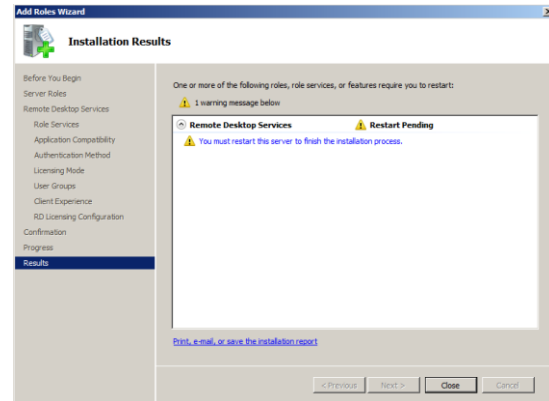
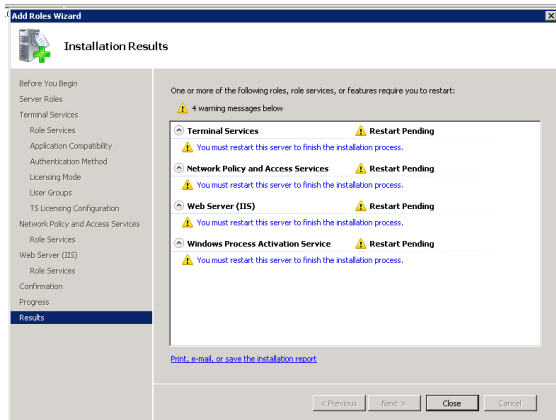


Click “Install”

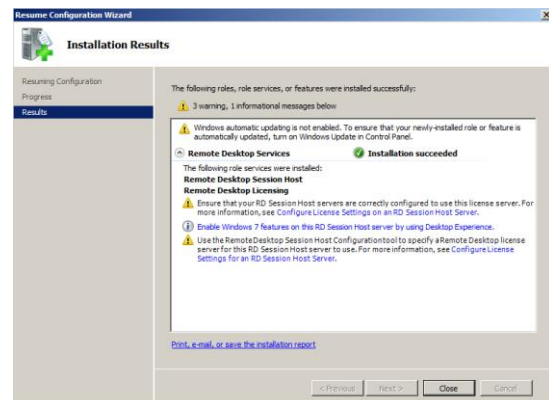
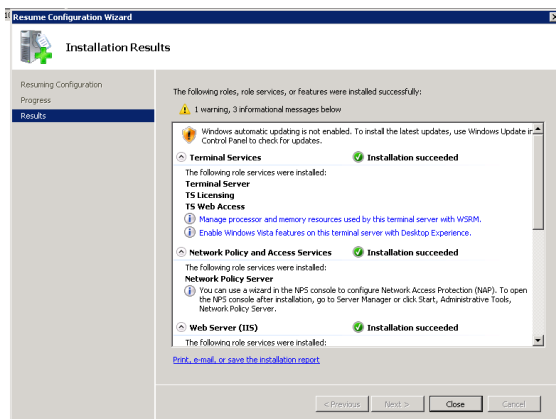




Click “Close” and allow the server to restart. The install will resume after restart.



After you have restarted, the following results will appear:



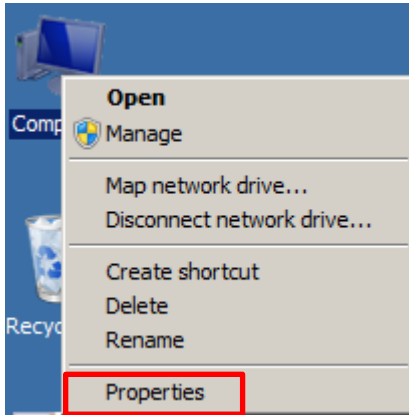
Click “Close”

ADVANCED OPTIMIZATIONS

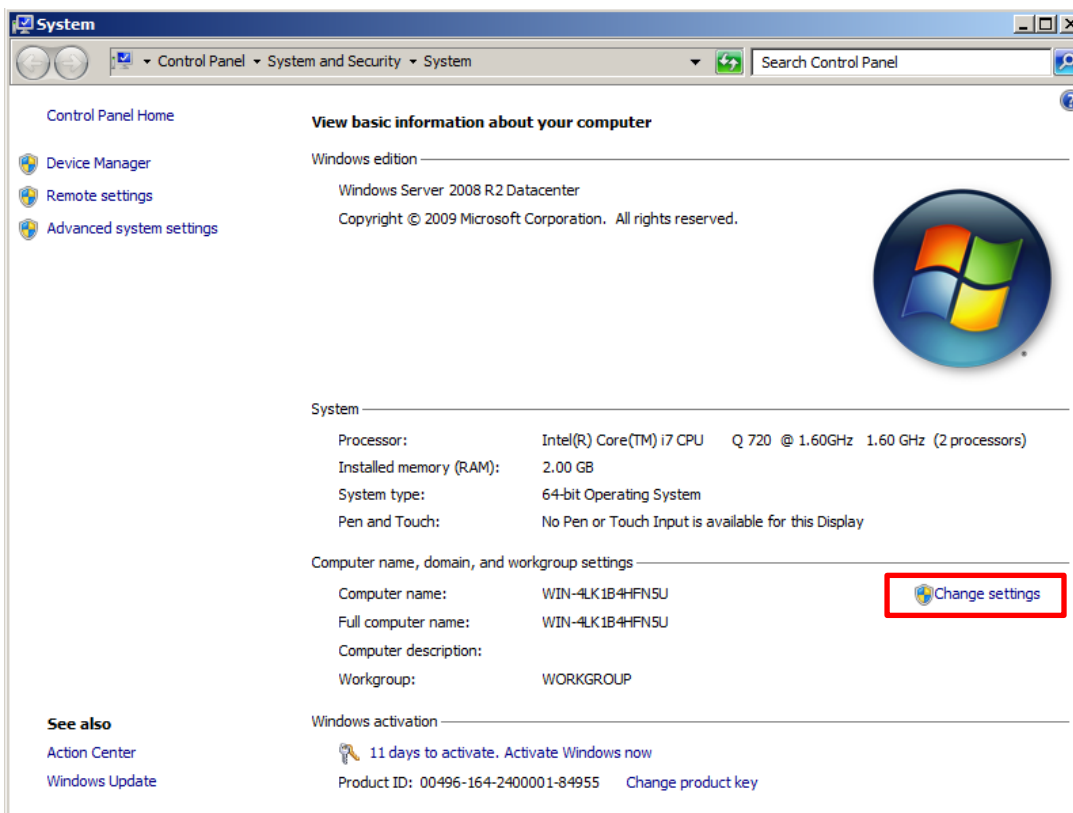
[OPTIONAL] SETTINGS FOR BEST PERFORMANCE AND DISABLING PAGING

Optimizing your server to use more physical memory and less disk I/O and CPU can be a performance enhancer. However, disabling Page Filing on systems with low RAM can cause degradation in performance. ***This step should only be taken by advanced users with a comprehensive understanding of their system's resources.***

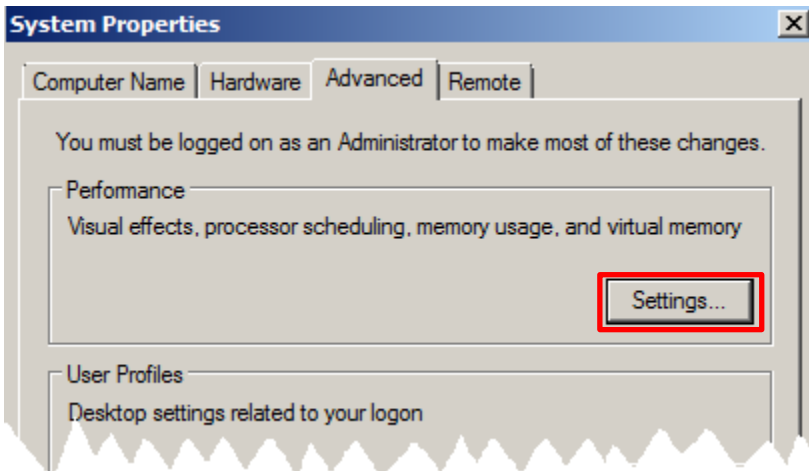
Right click on “Computer”→”Properties”



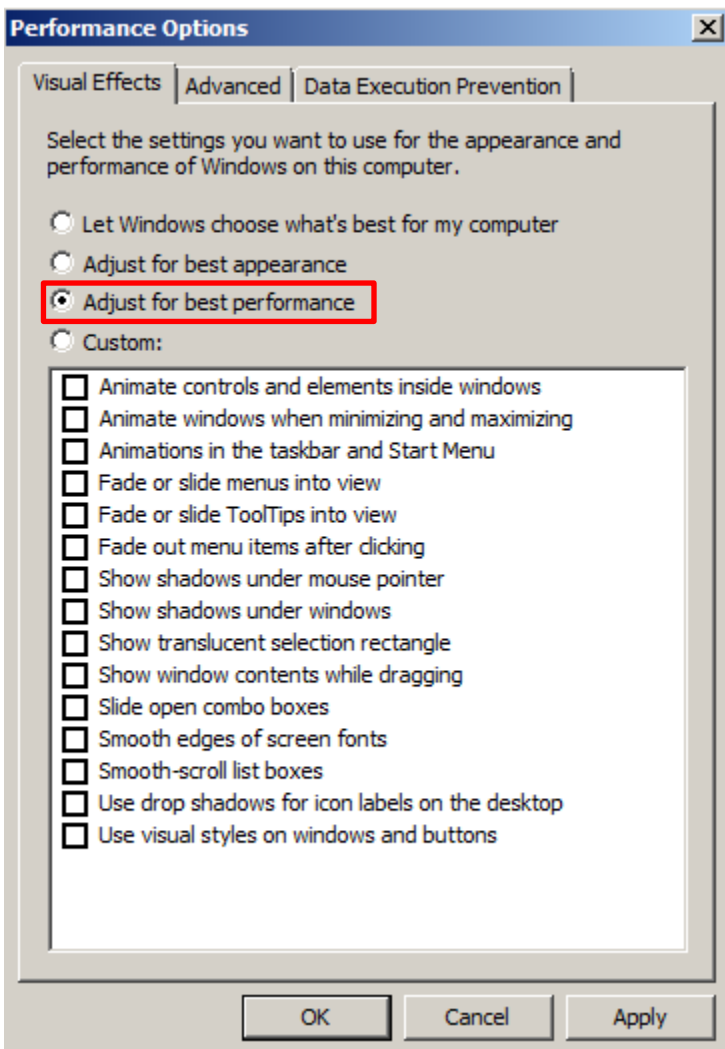
Click on “Change Settings”



Click on “Advanced” tab and click on “Settings” under “Performance”

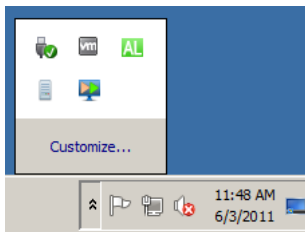


Click on the radio button “Adjust for best performance”.



AFTER MAKING CHANGES

After making any of the recommended configuration changes in this document, you'll need to reboot your Injector server for your changes to take effect. Be sure that the AppLoader process is running on the Controller machine, and the Injector and Vstation processes are running on the Injector machine prior to creating rUsers. The process icons should appear in the Windows taskbar;



CLONING INJECTORS ON VIRTUAL SERVERS

Virtual Servers are a cost effective alternative to expensive physical hardware. Additionally, they offer the flexibility to customize and duplicate configurations with ease. But to fully maximize the benefits of virtual servers, it is imperative that you create the most efficient server possible before cloning. We can't stress enough, the importance of taking the time to optimize your server as outlined in this document and creating and running sample test cases prior to cloning. Once you have optimized your prototypical server, clone away!

UPDATE VSTATION.INI FILE

To register each Injector with the AppLoader Controller you'll need to execute the following steps on each cloned server:

From the Windows Task Manager, look for the **Injector.exe** process. If running, *End Process*.

Browse to Program Files\NrgGlobal\Injector\ and find the **vstation.ini** file. Open with Notepad. Overwrite the following parameters with the Injector IP address and Name (the file will show the IP address and Name of the prototypical server from which you cloned):

```
//vstation's own IP address- this is the ip used to communicate with the Controller
ipaddress=192.168.0.1

//host of the injector
host=Injector1

//alias of the injector to be shown on Controller
alias=Injector1

//location of injector for display on Controller
location=Injector1 - 192.168.0.1

//description of injector
description=Injector Injector1 added via Injector Installer
```

Save and close the vstation.ini file.

From *Start*, open **All Programs>Injector**. Click “Start Injector” and “Register Injector with Controller” (which starts the Injector.exe and checkserver.cmd processes).

Each successfully registered Injector will appear in the ‘Manage Injectors’ window of the AppLoader Controller.