Hardening Guide for EventTracker Server
Introduction

The EventTracker solution includes a console component that is installed on a Windows 2003 / 2008 / 2008 R2 / 2012 server. It is important to harden this server in order to protect it from disruption in service delivery and unauthorized access. This guide describes how to create and maintain a secure environment for the server that runs EventTracker v7.x console.
Table of Contents

Harden Server – Quick View .................................................................................................................. 4
  Harden Windows Server .................................................................................................................. 4
    Apply Group Policies on Windows Server 2012 ........................................................................... 4
    Apply Group Policies on Win2K8 / 2K8 R2 Enterprise SP1 ................................................... 4
    Apply Group Policies on Win2K3 Enterprise SP2 ....................................................................... 4
  Secure IIS Web Server .................................................................................................................. 5
  Secure SQL Server ....................................................................................................................... 5
  Add Windows Firewall Exceptions ................................................................................................. 6
  Check with Vulnerability Scanner ................................................................................................. 6
    Security Recommendation for EventTracker v7.5 ................................................................. 7
    Security Recommendation for EventTracker v7.4 ................................................................. 7

Harden Server – Detailed View ............................................................................................................ 17
  Harden Windows Server ............................................................................................................... 18
    Apply Group Policies on Windows Server 2012 ....................................................................... 18
    Apply Group Policies on Win2K8 / 2K8 R2 Enterprise SP1 (Active Directory) ..................... 27
    Apply Group Policies on Win2K3 Enterprise SP2 (Active Directory) ...................................... 36
    Apply Group Policies in a Workgroup on Windows Server 2012 ........................................... 45
    Apply Group Policies in a Workgroup on Win2K8 / 2K8 R2 ................................................... 55
    Apply Group Policies in a Workgroup on Win2K3 ................................................................. 64
  Secure IIS Web Server ................................................................................................................. 71
    IIS 7, 7.5, 8 on Win 2K8 / 2K8 R2 / 2012 ............................................................................... 72
    IIS 6.0 on Windows Server 2003 Enterprise SP2 ................................................................. 97
  Restrict EventTracker website .................................................................................................... 125
  Install IP and Domain Restriction in Win2K8, 2K8 R2, 2012 .................................................. 125
  Configure IP Address and Domain Restrictions (IIS 7, 7.5, 8) in Win 2K8, Win 2K8 R2, Win 2012 .......................................................................................................................... 127
  Configure IP address and domain name restriction in Win2K3 .................................................. 130
  Request Filtering in IIS 7, 7.5, 8 ............................................................................................... 134
    To install Request Filtering in Windows 2012 ...................................................................... 134
    To install Request Filtering in Win 2K8 / 2K8 R2 ............................................................... 135
    To allow/deny access to a specific file name extension .......................................................... 136
  Install and configure URLScan security tool in IIS 6 ............................................................ 138
    Benefits of URLScan security tool ....................................................................................... 138
    Configure URLScan .............................................................................................................. 138
Secure SQL Database Server ............................................................................................................. 140
  SQL Server 2008 / 2008 R2 / 2012 ............................................................................................. 140
  SQL Server 2005 .......................................................................................................................... 142
Disable the SQL Server Services.................................................................................................. 143
  SQL Server SA Account ........................................................................................................... 147
Add Windows Firewall Exceptions.............................................................................................. 148
EventTracker Settings ................................................................................................................. 149
  Secure Agent Configuration and Save as Template ............................................................... 149
  Secure EventVault Storage ..................................................................................................... 154
Check with Vulnerability Scanner ............................................................................................... 158
Harden Server – Quick View

Harden Windows Server

Microsoft security policies (SSLF- Specialized Security Limited Functionality) should be applied to harden the Windows server. Following policies need to be considered for the hardening process.

Apply Group Policies on Windows Server 2012

Hardening of Windows Server 2012 should be carried according to the standard policy. Click the link below to download the GPO and apply the following policies:

www.eventtracker.com/support/utils/WS2012-GPO.zip

1. WS2012-Domain
2. WS2012-Member-Server
3. WS2012-Web-Server
4. WS2012-Remote Desktop Services
   Click here for the detailed steps to apply the policies.

Apply Group Policies on Win2K8 / 2K8 R2 Enterprise SP1

Hardening of Windows Server 2008 R2 Enterprise SP1 should be carried according to the standard policy. Click the link below to download the GPO and apply the following policies:

www.eventtracker.com/support/utils/WS08R2-SSLF-GPO.zip

1. WS08R2-SSLF-Domain
2. WS08R2-SSLF-Member-Server
3. WS08R2-Web-Server Group Policy
   Click here for the detailed steps to apply the policies.

Apply Group Policies on Win2K3 Enterprise SP2

Hardening of Windows server 2003 Enterprise SP2 should be carried according to the standard policy. Click the link below to download the GPO and apply the following policies:

www.eventtracker.com/support/utils/WS03SP2-SSLF-GPO.zip

1. WS03R2-SSLF-Domain
2. **WS03R2-SSLF-Member-Server**
   Click [here](#) for the detailed steps to apply the policies.

**Secure IIS Web Server**

In the IIS Manager, create a **Certificate request**. Once received, install the certificate.

**NOTE:**

IIS 6 and above are supported.

After certificate installation, bind the certificate to the **Default Web Site**, and then apply **SSL Settings**.

In case of IIS6 on Windows Server 2003,
  a) Configure the Server to Require Clients to Use SSLv3 or TLS.
  b) Configure the Server to Disable Support for Weak Ciphers.
  c) Configure IIS to Return the Fully Qualified Domain Name of the Web Server Instead of its IP Address.

**NOTE:** If FTP server is installed on the EventTracker server to transfer custom logs from remote sources then the password will be sent in clear text, which will be consumed by Direct Log Archiver (DLA) feature. The third party secure ftp server is recommended.

Click [here](#) for the detailed instructions.

In case of IIS 7 Web Server

- Don't place EventTracker server in DMZ network
- Give administrative access only to Authorized users or administrators
- Disable directory Browsing in IIS
- Do not install Internet printing Extension on EventTracker server

**Secure SQL Server**

- While installing SQL server, install only ‘Database Engine Services’. No other services are required.
- Disable (or leave disabled) the following SQL services.
  - Disable the **SQL Server VSS Writer** service.
 Disable the SQL Server Browser service.
 Leave the SQL Active Directory Helper service disabled.

• Only Authorized Administrators and users should be assigned Sysadmin role.
• Recent service packs and critical fixes should be installed for SQL Server and Windows.
• Remove BUILTIN\Administrators group from the SQL Server Logins.

NOTE: Before you remove built in administrators make sure you assign other users sysadmin privileges.

Add Windows Firewall Exceptions

The ports/.exe in use should be added to the firewall exception list. Based on the system capacity, any number of VCP’s can be added. For EventTracker, add the following port numbers/.exe to the firewall exception list:

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Used For</th>
</tr>
</thead>
<tbody>
<tr>
<td>14505 (TCP/UDP)</td>
<td>Windows Receiver</td>
</tr>
<tr>
<td></td>
<td>Multiple VCP’s can be configured</td>
</tr>
<tr>
<td>14502, 14508 (TCP)</td>
<td>Change Audit</td>
</tr>
<tr>
<td>14503 (TCP)</td>
<td>EventTracker Certificate server</td>
</tr>
<tr>
<td>14506 (TCP)</td>
<td>EventTracker Agent</td>
</tr>
<tr>
<td>14507 (TCP)</td>
<td>Collection Master</td>
</tr>
<tr>
<td>443 (TCP)</td>
<td>EventTracker securely access( HTTPS )</td>
</tr>
<tr>
<td>514 (UDP/TCP)</td>
<td>Syslog Receiver</td>
</tr>
<tr>
<td></td>
<td>Multiple VCP’s can be configured</td>
</tr>
</tbody>
</table>

Check with Vulnerability Scanner

The hardened EventTracker system is scanned for vulnerabilities. Click here to read the possibilities and their solutions/configuration changes.
Security Recommendation for EventTracker v7.5

- A golden snapshot of EventTracker v7.5 is available (named Change Policy v7.5). As soon as EventTracker is installed in customer premises, EventTracker v7.5 snapshots has to be taken and compared with the golden snapshot and accept the violations for the first time.

1. Please download the Golden Baseline Policy file.
2. Open the content of this file in notepad and save the file in a desired location with extension ‘.ispol’.
3. Edit the ‘.ispol’ file; enter the correct path of the folder where EventTracker is installed.
   i.e. the command [DefFolder] = F:\Program Files\Prism Microsystems\Common\ has to be replaced with [DefFolder] = \Installdir\Program Files\Prism Microsystems\Common in the entire file.
4. Select Replace All so that the path is updated in the entire document.

To import the policies, kindly follow the steps mentioned in Security Recommendation for EventTracker v7.4.

Security Recommendation for EventTracker v7.4

- A golden snapshot of EventTracker v7.4 is available (named Change Policy v7.4). As soon as EventTracker is installed in customer premises, EventTracker v7.4 snapshots has to be taken and compared with the golden snapshot and accept the violations for the first time.

Please download the Golden Baseline Policy file. Copy the content of this file to notepad and save the file in a desired location with extension ‘.ispol’.

To import the policies, kindly follow the steps given below.

1. Click the Start button, select Prism Microsystems, and then select EventTracker.
2. Select EventTracker Control Panel and then select Change Audit.
   Results Summary Console displays.
   EventTracker - Change Browser displays.
4. Select the Tools menu and then select Configuration Policy Editor.
5. Select the Policy menu and then select Import.
6. Browse the file *.ispol and then select Open.
   Successful message displays.
Figure 1

All the files, folders, registries related to the policy display.

Figure 2

7) Click the **Close** button.

These policies can be viewed and scheduled in EventTracker Web i.e.
1. Login to EventTracker, select the **Change Audit** menu, and then select **Change Policies**.
2. Select the relevant policy to be scheduled.
3. Right-click the policy and then select **Add Scheduled**.

4. Enter the appropriate data and then click **Save**.
5. In **Actions** pane, select **Dashboard** and then select the required policy.

![Figure 5](image_url)

6. To accept all the integrity violations for the first time, select the **Item Name** option.

![Figure 6](image_url)

7. Click **Accept**, and then click **Save**.
To avoid flooding of events when auditing is enabled for a folder, please make sure to grant only necessary permissions to the concerned users.

For example: If users have Read permissions on a particular folder, they may read/download the files many times. As a result the number of events increases. To avoid this kind of a situation, only relevant users should be granted appropriate permission.

For detail information, please refer EventTracker Change Audit User Guide.

As a part of security best practice, server messages need to be parsed before it is passed on to the user. In order to avoid revealing the sensitive server information or private information, it is required to show a generic error messages when an error occurs. To do this, users need to follow the below mentioned steps after EventTracker is installed.

A. Prepare the files to show Custom Error page

1) Create a new folder (Ex: ErrorPages) where EventTracker (i.e. \\
\InstallDIR\EventTracker) is installed.

2) Download and extract the ErrorPages.zip file in this newly created folder and execute the batch file ‘CustomError.bat’.

(To download the zip file, refer ErrorPages.zip)

NOTE:

Please make sure that the Custom Error Pages option is enabled for EventTracker application in IIS pane under Error Pages. Select Edit feature Settings, and then select Custom error pages option.
Figure 7

Run the command prompt as an admin and change the directory to the path where the ‘CustomError.bat’ file is available.

Also please update the ‘applicationhost.config’ file in Windows\System32\inetsrv\config folder with the following code

  <httpErrors lockAttributes="defaultPath" allowAbsolutePathsWhenDelegated="true">

i.e. The line <httpErrors errorMode="Custom"
lockAttributes="allowAbsolutePathsWhenDelegated,defaultPath"> should be replaced with
<httpErrors lockAttributes="defaultPath" allowAbsolutePathsWhenDelegated="true">

3) Enter the command CustomError.bat "<INSTALLDIR>\EventTracker\ErrorPages".

Figure 8
On successful execution of the batch file the following message will shown in the command prompt.

![Command Prompt Screenshot](image9)

**NOTE:**
If the user has already configured a custom error message for EventTracker, the following error message will be thrown as shown below.

![Command Prompt Screenshot](image10)

4) Open IIS, expand **Default Web Site** node, and then select **EventTracker**.

5) In **IIS pane**, select **Error Pages** icon.
   In Error Pages pane, 40 custom error pages display.
Figure 11

6) Launch EventTracker application with URL:

   http://localhost/eventtracker/1=1--
   Or
   https://localhost/eventtracker/1=1--

   The custom error page displays the message “Page not found”.
To configure custom error messages for IIS6.0 manually follow the below mentioned steps:

1. In IIS Manager, double-click the local computer; right-click the Web Sites folder or an individual Web site folder, or a virtual directory, or a file; and then click **Properties**.

   **NOTE:**

   Configuration settings made at the Web Sites level are inherited by all of the Web sites on the server. You can override inheritance by configuring the individual site or site element.

2. Click the **Custom Errors** tab.

3. In the **Error messages for HTTP errors** list, click the HTTP error that you want to change, and then click the **Edit** button.

   **Edit Custom Error Properties** window displays.

   **NOTE:** The following errors are not customizable: 400, 403.9, 411, 414, 500, 500.11, 500.14, 500.15, 501, 503, and 505.

4. In the **Message Type** drop down, select **File** to return a custom error file or **URL** to direct the request to a custom error URL on the local machine.
**NOTE:** If your custom error is an .asp page, you must select URL. If you do not select URL, you risk returning .asp source code to the client.

a. If **File** option is selected, type the path of the file or click **Browse** to navigate to the file. Custom error messages are installed by default to the systemroot\Help\IisHelp\Common folder. The file names are numbers that correspond to the specific HTTP errors; for example, 400.htm, 401-1.htm, and so on.

    (OR)

If **URL** is selected, type the path to the Web site or virtual directory. The URL must be a Web site or a virtual directory on the local machine. In addition, the custom error URL must exist in the application pool that directs the request to the custom error URL. If you store custom error pages in a virtual directory, that virtual directory must run in the same application pool as the rest of your Web site. Otherwise, the worker process cannot serve the custom error page when it is requested.

5. Click **OK**, and then click **OK** again.
Harden Server – Detailed View

Following aspects need to be configured to harden the EventTracker server.

- Harden Windows Server
- Secure IIS Web Server
- Secure SQL Server
- Firewall Settings
- EventTracker Settings
- Check with Vulnerability Scanner
Hardening Guide For EventTracker Server

Harden Windows Server

Apply Group Policies on Windows Server 2012

**Step 1:** Click the link below to download the GPO and extract the contents of zip file onto the system.

http://www.eventtracker.com/support/utils/WS2012-GPO.zip

**Step 2: Create new ‘Group Policy Objects’**

1. Click the **Start** button, select **Administrative Tools**, and then select **Group Policy Management**.
2. In the **Group Policy Management** pane, expand **Domains** node, and then expand ‘local system’ node.
3. Right click **Group Policy Objects**, and then click **New**.
4. Enter the new GPO (Group Policy Object) name as **WS2012-Domain**, and then click **OK**.

![New GPO](figure13.png)

5. Similarly create New GPO for member server, web server and Remote Desktop Services, and name them as **WS2012-Member-Server**, **WS2012-Web-Server** and **WS2012-Remote Desktop Services** respectively.
Step 3: Import Group Policy settings

1. Right click the newly created GPO (For example, **WS2012-Domain**), and click **Import settings**.
   *Import Settings Wizard* dialog box appears on the screen.
2. Click the **Next >** button to start the importing process.
3. In **Backup GPO**, click the **Next >** button.
4. In the **Backup location**, browse the path for backup folder from where the settings are to be imported.
5. Click the **Next >** button.
6. Click the **Next >** button.

![Import Settings Wizard](image)

**Figure 17**

7. In **Source GPO**, select the backed up GPO, and click the **Next >** button.
8. In **Scanning Backup**, once the scanning of settings is complete, click the **Next >** button.
9. In **Migrating References**, click the **Next >** button.
10. Click the **Finish** button.
11. Once the import process is succeeded, click the **OK** button.
Group policy import is now completed for **WS2012-Domain**.

12. Repeat the steps from 1 to 10 to import Group Policy for **WS2012-Member-Server**, **WS2012-Web-Server** and **WS2012-Remote Desktop Services**.

**Step 4: Create new ‘Organizational Unit’**

1. Right click the server computer name, and then click **New Organizational Unit**.
2. Enter the new organizational unit (OU) name, and then click **OK**.

For example: EventTracker Server

![New Organizational Unit](image)

**Step 5: Link the existing GPO to newly created OU**

1. Right click newly created OU – EventTracker Server, and then click **Link an existing GPO**.
2. In the Select GPO dialog box, using Control key select all the three newly created GPO, and then click OK.
The Group Policy objects are now linked to the organizational unit.

**Figure 23**

**Step 6: Link EventTracker Server to newly created OU and reboot the EventTracker server system**

1. Select the **Start** button, select **All Programs**, and then select **Administrative Tools**.
2. Select **Active Directory Users and Computers**.
3. In the **Active Directory Users and Computers** pane, expand **Domains** node, and then click **Computers** node.
4. Right click any EventTracker server system, and then click **Move**.

**Figure 24**

**Move** dialog box will appear on the screen.
5. Select the newly created OU (in this case, select EventTracker Server), and then click OK.

6. In the Active Directory Users and Computers pane, click ‘Organizational Unit’ (in this case, click EventTracker Server).

7. Reboot the EventTracker server system which is linked to the OU.
Apply Group Policies on Win2K8 / 2K8 R2 Enterprise SP1 (Active Directory)

**Step 1:** Click the link below to download the GPO and extract the contents of zip file onto the system.

www.eventtracker.com/support/utils/WS08R2-SSLF-GPO.zip

**Step 2: Create new ‘Group Policy Objects’**

1. Select the **Start** button, select **All Programs**, and then select **Administrative Tools**.
2. Select **Group Policy Management**, expand **Domains** node, and then expand ‘local system’ node.
3. Right click **Group Policy Objects**, and then click **New**.
4. Enter the new GPO (Group Policy Object) name as **WS08R2-SSLF-Domain**, and then click **OK**.

![New GPO](image)

**Figure 27: Create new GPO**

5. Similarly create **New GPO** for member server and web server, and name them as **WS08R2-SSLF-Member-Server** and **WS08R2-Web-Server** respectively.
**Step 3: Import Group Policy settings**

1. Right click the newly created GPO (For example, **WS08R2-SSLF-Domain**), and click **Import settings**.  
   **Import Settings Wizard** dialog box appears on the screen.

2. Click the **Next >** button to start the importing process.

3. In **Backup GPO**, click the **Next >** button.

4. In the **Backup location**, browse the path for backup folder from where the settings are to be imported.
5. Click the **Next >** button.

6. In **Source GPO**, select the backed up GPO, and click the **Next >** button.

7. In **Scanning Backup**, once the scanning of settings is complete, click the **Next >** button.
8. In **Migrating References**, click the **Next >** button.

9. Click the **Finish** button.

10. Once the import process is succeeded, click the **OK** button.

![Import](image)

**Figure 31: Import**

Group policy import is now completed for **WS08R2-SSLF-Domain**.

11. Repeat the steps from 1 to 10 to import Group Policy for **WS08R2-SSLF-Member-Server** and **WS08R2-Web-Server**.

**Step 4: Create new ‘Organizational Unit’**

1. Right click the server computer name, and then click **New Organizational Unit**.
2. Enter the new organizational unit (OU) name, and then click **OK**. For example: EventTracker Server

![Figure 33: Name the new OU](image)

**Figure 33: Name the new OU**

---

**Step 5: Link the existing GPO to newly created OU**

1. Right click newly created OU – EventTracker Server, and then click **Link an existing GPO**.
2. In the **Select GPO** dialog box, using *Control* key select all the three newly created GPO, and then click **OK**.
The Group Policy objects are now linked to the organizational unit.

![Group Policy Management](image)

**Figure 36**

**Step 6: Link EventTracker Server to newly created OU and reboot the EventTracker server system**

1. Select the **Start** button, select **All Programs**, and then select **Administrative Tools**.
2. Select **Active Directory Users and Computers**.
3. In the **Active Directory Users and Computers** pane, expand **Domains** node, and then click **Computers** node.
4. Right click **EventTracker server system**, and then click **Move**.
Move dialog box will appear on the screen.

5. Select the newly created OU (in this case, select EventTracker Server), and then click OK.
6. In the **Active Directory Users and Computers** pane, click ‘organizational unit’ (in this case, click **EventTracker Server**).

   ![Active Directory Users and Computers](image)

   **Figure 39**

   Once linked, EventTracker server name will be displayed under OU.

7. Reboot the EventTracker server system which is linked to the OU.
Apply Group Policies on Win2K3 Enterprise SP2 (Active Directory)

**Step 1:** Click the link below to download the GPO and extract the contents of zip file onto the system.

www.eventtracker.com/support/utils/WS03SP2-SSLF-GPO.zip

**Step 2: Create new ’Group Policy Objects’**

1. Select the **Start** button, select **All Programs**, and then select **Administrative Tools**.
2. Select **Group Policy Management**, expand **Domains** node, and then expand ’local system’ node.
3. Right click **Group Policy Objects**, and then click **New**.
4. Enter the new GPO (Group Policy Object) name as **WS03R2-SSLF-Domain**, and then click **OK**.

![Figure 40](image)

5. Similarly create **New GPO** for member server, and name it as **WS03R2-SSLF-Member-Server**.
Step 3: Import Group Policy settings

1. Right click the newly created GPO (For example, **WS03R2-SSLF-Domain**), and click Import settings.

   **Import Settings Wizard** dialog box appears on the screen.

2. Click the **Next >** button to start the importing process.

3. In **Backup GPO**, click the **Next >** button.

4. In the **Backup location**, browse the path for backup folder from where the settings are to be imported.
5. Click the **Next >** button.

6. In **Source GPO**, select the backed up GPO, and click the **Next >** button.
7. In **Scanning Backup**, once the scanning of settings is complete, click the **Next >** button.
8. In **Migrating References**, click the **Next >** button.
9. Click the **Finish** button.
10. Once the import process is succeeded, click the **OK** button.

![Figure 44](image)

Group policy import is now completed for **WS03R2-SSLF-Domain**.

11. Repeat the steps from 1 to 10 to import Group Policy for **WS03R2-SSLF-Member-Server**.

**Step 4: Create new 'Organizational Unit'**

1. Right click the server computer name, click **New**, and then click **New Organizational Unit**.
2. Enter the new organizational unit (OU) name, and then click **OK**.
   For example: EventTracker Server

![Create New OU](image1.png)

**Figure 45: Create New OU**

For example: EventTracker Server

![Name the new OU](image2.png)

**Figure 46: Name the new OU**

**Step 5: Link the existing GPO to newly created OU**

1. Right click newly created OU – EventTracker Server, and then click **Link an existing GPO**.
2. In the **Select GPO** dialog box, using *Control* key select all the three newly created GPO, and then click **OK**.
The Group Policy objects are now linked to the organizational unit.

![Group Policy Management screenshot](image)

**Figure 49**

**Step 6: Link EventTracker Server to newly created OU and reboot the EventTracker server system**

1. Select the **Start** button, select **All Programs**, and then select **Administrative Tools**.
2. Select **Active Directory Users and Computers**, expand **Domains** node, and then click **Computers** node.
3. Right click **EventTracker server system**, and then click **Move**.
Move dialog box will appear on the screen.
**NOTE:**

The new system moved under OU will be referred as ‘Member server’.

4. Select the newly created OU (in this case, select **EventTracker Server**), and then click **OK**.

5. In the **Active Directory Users and Computers** pane, click ‘organizational unit’ (in this case, click **EventTracker Server**).

6. Reboot the EventTracker server system which is linked to the OU.
Apply Group Policies in a Workgroup on Windows Server 2012

**Step 1: On the workgroup system, download windows server 2012 local security policy backup file**

1. Click the link below to download exported GPO backup.
   www.eventtracker.com/support/utils/WS2012-GPO.zip
2. Extract the downloaded file to \\<systemname>\2012GPOBackup.

**Step 2: On the workgroup system, install the MS Security Compliance Manager (MSCM)**

1. Click the link below to download SCM 3
2. In the webpage, Download SCM 3.0 now!, click the link.
3. Download 'Security_Complianc_Manager_setup.exe', and then click Run as Administrator.
4. Click the Finish button once the installation is completed.

**NOTE:** The installation will be interrupted if the prerequisites (Microsoft Visual C++ 2010 X86 Redistributable, .NET Framework 4, and SQL Express 2012) are not installed on the system. After successful MSCM Installation, Microsoft Security Compliance Manager window appears on the screen.

---

![Microsoft Security Compliance Manager](image.png)

**Figure 53**
Step 3: On the workgroup system, install Local GPO

1. Select the Search button, select Apps, and then select Microsoft Security Compliance Manager.
2. Select LocalGPO.

LGPO folder appears on the screen.

3. Right click LocalGPO, and then click Install.
LocalGPO Setup wizard appears on the screen.

Figure 55

Welcome to the LocalGPO Setup Wizard

The Setup Wizard will install LocalGPO on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Figure 56
4. Click the **Next >** button.
5. Read the license agreement, select ‘**I accept the terms in the License Agreement**’, and then click **Next >**.

![LocalGPO License Agreement](image)

6. Click **LocalGPO** option, if not selected by default, then click the **Next >** button.
7. Click the **Install** button.
8. Click the Finish button.

![Figure 60: LocalGPO Setup](image)

**Step 4: Restoring the Local Security Policy**

Before restoring the Local Group Policy, check the status of default Local Security Policy in the workgroup system.

1. Select the Start button, select Administrative Tools, and then select click Local Security Policy.
3. Click Password Policy, and check the Security Settings.
4. Click Account Lockout Policy, and check the Security Settings.

Now restore the default Local Security Policy in the workgroup system.

1. Select the Start button, select Administrative Tools, and then select LocalGPO.
2. Right click LocalGPO Command-line, and then click Run as administrator.
3. In Administrator: LocalGPO Command-line, type the following command, and then press the Enter button.

```
cscript LocalGPO.wsf /Restore
```
4. Once the default Local Policy is restored, type `Exit` in command line.
5. Restart the workgroup system to refresh the Local Policy.

**Step 5: Importing Security Policy downloaded in step 1**

1. Select the **Start button**, select **Administrative Tools** -> click **LocalGPO** -> right click **LocalGPO Command-line**, and then click **Run as administrator**.
2. In **Administrator: LocalGPO Command-line**, type the following command, and then press the **Enter** button.

   ```cmd
   cscript LocalGPO.wsf /<backup folder path>{guid}
   ```

   Here ‘guid’ is the folder name which was created under GPObackups.

   Ex: `\<systemname>\2012GPOBackup\GPObackups\{713618A7-83F2-46B1-A2CC-9847BB35A4AF}`
3. Restart the computer to refresh the Local Policy.

**Step 6: Verify the applied Security Policy in workgroup system:**

1. Select the Start button, and then select Administrative Tools.
3. Click Password Policy, and check the Security Settings.
4. Click **Account Lockout Policy**, and check the **Security Settings**.
Figure 64
Apply Group Policies in a Workgroup on Win2K8 / 2K8 R2

**Step 1: On the workgroup system, download windows server 2008 R2 / 2012 local security policy backup file**

1. Click the link below to download exported GPO backup.
   www.eventtracker.com/support/utils/2008R2SSLLFGPOBackup.zip
2. Extract the downloaded file to \<systemname>\2008R2SSLLFGPOBackup.

**Step 2: On the workgroup system, install the MS Security Compliance Manager (MSCM)**

1. Click the link below to download SCM 2.5.
2. In the webpage, click the Download SCM 2.5 Now link.
3. Right click 'Security_Complaince_Manager_setup.exe', and then click Run as Administrator.
4. Click the Finish button once the installation is completed.
   **NOTE:** The installation will be interrupted if the prerequisites (Microsoft Visual C++ 2010 X86 Redistributable, .NET Framework 4, and SQL Express 2008) are not installed on the system.

   After successful MSCM Installation, Microsoft Security Compliance Manager window appears on the screen.
Step 3: On the workgroup system, install Local GPO

1. Select the Start button, select All Programs, and then select Microsoft Security Compliance Manager.
2. Select LocalGPO.
LGPO folder appears on the screen.

3. Right click **LocalGPO**, and then click **Install**.

![Figure 66](image)

Figure 66

![Figure 67](image)

Figure 67
LocalGPO Setup wizard appears on the screen.

4. Click the **Next >** button.

5. Read the license agreement, select ‘**I accept the terms in the License Agreement**’, and then click **Next >**.

6. Click **LocalGPO** option, if not selected by default, then click the **Next >** button.
7. Click the **Install** button.

8. Click the **Finish** button.
Step 4: Restoring the Local Security Policy

Before restoring the Local Group Policy, check the status of default Local Security Policy in the workgroup system.

1. Click Start -> All Programs -> Administrative Tools -> click Local Security Policy.
3. Click Password Policy, and check the Security Settings.
4. Click Account Lockout Policy, and check the Security Settings.

Now restore the default Local Security Policy in the workgroup system.

1. Click Start -> All Programs -> click LocalGPO -> right click LocalGPO Command-line, and then click Run as administrator.
2. In Administrator: LocalGPO Command-line, type the following command, and then press the Enter button.

   cscript LocalGPO.wsf /Restore
3. Once the default Local Policy is restored, type **Exit** in command line.

4. Restart the workgroup system to refresh the Local Policy.

**Step 5: Importing Security Policy downloaded in step 1**

1. Click **Start -> All Programs -> click LocalGPO -> right click LocalGPO Command-line**, and then click **Run as administrator**.

2. In **Administrator: LocalGPO Command-line**, type the following command, and then press the **Enter** button.

   ```plaintext
cscript LocalGPO.wsf /<backup folder path>\{guid}
```

   Here ‘**guid**’ is the folder name which got created under GPObackups.

   Ex: **C:\2008R255LFGPOBackup\{95881AD7-2BCD-4FBD-A299-8203899A2B2D}**
3. Restart the computer to refresh the Local Policy.

**Step 6: Verify the applied Security Policy**

**In workgroup system:**

1. Select the **Start** button, select **All Programs**, and then select -> **Administrative Tools**.
2. Click **Local Security Policy**, expand **Account Policies**.
3. Click **Password Policy**, and check the **Security Settings**.
4. Click Account Lockout Policy, and check the Security Settings.
Apply Group Policies in a Workgroup on Win2K3

**Step 1: On the workgroup system, download Windows Server 2003 R2 local security policy backup file**

1. Click the link below to download exported GPO backup.

2. Extract the downloaded zip file to C:\2003SP2SSLLFGPOBackup.

**Step 2: On the workgroup system, install Local GPO**

1. Download LGPOInstaller.zip from below link and extract it.
   [www.eventtracker.com/support/utils/LGPOInstaller.zip](http://www.eventtracker.com/support/utils/LGPOInstaller.zip)

2. Right click on downloaded LocalGPO.msi, and then click Install.

![LocalGPO Setup wizard appears on the screen.](image)
3. Click the Next > button.

4. Read the license agreement, select ‘I accept the terms in the License Agreement’, and then click Next >.

5. Click LocalGPO option, if not selected by default, then click the Next > button.
6. Click the **Install** button.

7. Click the **Finish** button.
Step 3: Restoring the Local Security Policy

Before restoring the Local Group Policy, check the status of default Local Security Policy in the workgroup system.

1. Click **Start** -> **All Programs** -> **Administrative Tools** -> click **Local Security Policy**.
2. In **Local Security Policy** window, expand **Account Policies**.
3. Click **Password Policy**, and check the **Security Settings**.
4. Click **Account Lockout Policy**, and check the **Security Settings**.

Now restore the default Local Security Policy in the workgroup system.

1. Click **Start** -> **All Programs** -> click **LocalGPO** -> right click **LocalGPO Command-line**, and then click **Run as administrator**.
2. In **Administrator: LocalGPO Command-line**, type the following command, and then press **Enter**.

   ```
cscript LocalGPO.wsf /Restore
```
3. Once the default Local Policy is restored, type **Exit** in command line.

4. Restart the workgroup system to refresh the **Local Policy**.

**Step 4: Importing Security Policy downloaded in step 1**

1. Click **Start** -> **All Programs** -> click **LocalGPO** -> right click **LocalGPO Command-line**, and then click **Run as administrator**.

2. In **Administrator: LocalGPO Command-line**, type the following command, and then press the **Enter** button.

   ```
cscript LocalGPO.wsf /<backup folder path>{guid}
   
   Here ‘guid’ is the folder name which got created under GPObackups.
   
   Ex: C:\2003SP2SSLFGPOBackup\{B128F820-6FC7-4395-9F63-F3D22249FF0C}
   ```
3. Restart the computer to refresh the Local Policy.

Step 5: Verify the applied Policy

In workgroup system:

1. Click Start -> All Programs -> Administrative Tools -> click Local Security Policy.
3. Click Password Policy, and check the Security Settings.
4. Click **Account Lockout Policy**, and check the **Security Settings**.

![Account Lockout Policy settings](image)

**Figure 86**

<table>
<thead>
<tr>
<th>Policy</th>
<th>Security Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account lockout duration</td>
<td>15 minutes</td>
</tr>
<tr>
<td>Account lockout threshold</td>
<td>10 invalid logon attempts</td>
</tr>
<tr>
<td>Reset account lockout counter after</td>
<td>10 minutes</td>
</tr>
</tbody>
</table>
Secure IIS Web Server

Secure Sockets Layer (SSL)

The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the internet.

SSL is required to,
- Offer a login or sign in on the site
- Process sensitive data
- Comply with security requirements

Mandatory Requirements

This section describes the mandatory software and component requirements to create SSL digital certificate and secure website hosted on IIS server with SSL digital certificate.

| Operating System | • Windows Server 2008, 2008 R2 Enterprise SP1/2012  
|                  | OR
|                  | • Windows Server 2003 Enterprise SP2
| Software and Component | • Internet Information Server (IIS) 6.0 and above.  
|                      | • Browser, which supports 128-bit encryption  
|                      | (IE 7.0 or above/ Firefox 3.5 or above). |
IIS 7, 7.5, 8 on Win 2K8 / 2K8 R2 / 2012
Step 1: Creating the ‘Certificate Request’

1. Select the **Start** button, select **All Programs**, and then select **Administrative Tools**.  
   **NOTE:** In Windows Server 2012, select the **Start** button, and then select **Administrative Tools**.  
   The screenshot for IIS 8 in Win 2012 may differ but the features and functionality remains the same.

2. Select **Internet Information Services (IIS) Manager**.

![Figure 87: Internet Information Services (IIS) Manager](image-url)
3 Click the server node.
4 Double click **Server Certificates** icon in the IIS pane.

![Figure 90: Server Certificates pane displays.](image)

Server Certificates pane displays.

![Figure 91: Server certificates](image)

5 In the **Actions** pane, click **Create Certificate Request** link.
**Request Certificate** dialog box will be opened.

![Figure 92: Distinguished Name Properties](image)

6. Type the system name (FQDN - Fully qualified domain name) as common name in the **Common name** text box.

   Example: `mcloon.toons.local`

![Figure 93](image)
7. Enter organization and geographical details, and then click **Next**.
8. Leave the default selection in **Cryptographic Service Provider Properties** pane.
9. Set bit length to 2048 from the **Bit length** dropdown, and then click the **Next**.

![Figure 94: Cryptographic Service Provider Properties](image)

10. Type name and path of the file to save the **CSR** (Certificate Server Request).

![Figure 95](image)
11 Click **Finish**.
12 Send this request file to the certificate vendor.

### Step 2: Installing the certificate

**NOTE:** Certificate received from the vendor needs to be copied to the system.

1. Select the **Start** button, select **All Programs**, and then select **Administrative Tools**.
2. Select **Internet Information Services (IIS) Manager**.

   ‘Internet Information Services (IIS) Manager’ window is displayed.

3. Click the server node, and then double click the **Server Certificates** icon in the IIS pane.

   ![Figure 96: IIS pane](image)

4. In the **Actions** pane, click **Complete Certificate Request** hyperlink.
5. In **Complete Certificate Request** dialog box, click the **browse** button.

---

Figure 97: Server Certificates - Complete Certificate Request

Figure 98: Specify Certificate Authority Response in IIS 7, 7.5
6 Locate the server certificate that has been received from the certificate authority.
7 Click **Open**.

![Figure 101](image)

**Figure 101**

8 Type a relevant name in **Friendly name** box to keep track of the certificate on this server.

![Figure 102](image)

**Figure 102 – Complete Certificate Authority request in IIS 7, 7.5**
Figure 103 – Complete Certificate Authority request in IIS 8

9 Click OK.

If successful, the newly installed certificate will be shown in the list. If an error stating ‘the request or private key cannot be found’ occurs, then make sure that the correct certificate is being used and is getting installed on the same server where the CSR (Certificate Server Request) is generated. If these two things are in place then proceed to create a new Certificate Request and reissue/replace the certificate.
Figure 104: Certificate appear in the 'Server Certificates' list

**Step 3: Binding the certificate to the 'Default Web Site'**

1. Expand the server node.
2. Expand the **Sites** node.
3. Click **Default Web Site**.
4. In the **Actions** pane, click **Bindings**.
Figure 105: Default Web Site Home - Bindings

**Site Bindings** dialog box appears on the screen.

![Site Bindings](image)

**Figure 106: Site Bindings**

5. Click **Add**.

Add Site Binding dialog box appears on the screen.
6 Change the **Type** to **https**.

By default, system will select the port number as 443. The default port number can be changed, if required.
7. Select the recently installed SSL certificate.
8 Click **OK**.

The binding for port 443 will be listed.

9 Click **Close**.

Newly added https website is listed under **Browse Web Site**.

![Figure 111: Add Site Binding in IIS 8](image)

![Figure 112](image)
Step 4: Configure ‘SSL Settings’

Configure ‘SSL Settings’ to interact in a specific way with client certificates.

1. Expand the Sites node.
2. Click Default Web Site.
3. Double-click SSL Settings icon.
Figure 114: Click SSL Settings icon

SSL Settings display in the middle pane.
4. Check the **Require SSL** option.
5. In the **Actions** pane, click **Apply**.

After successful SSL settings modification, a message will be displayed in the **Alerts** pane.

![Figure 116](image)

6. Close the **IIS Manager**.

**Step 5: Create FTP service**

NOTE: Follow step 5 and step 6 only if needed to transfer the custom logs from remote server to the EventTracker server.

1. Click the **Start** button, select **All Programs**, and then select **Administrative Tools**.
2. Select **Server Manager**.
3 In the **Server Manager** pane, expand **Roles**.

4 Right click **Web Server (IIS)**, and select **Add Role Services**.

**Server Manager** displays **Add Roles Services** wizard.
5. In the **Roles Services** pane, check **FTP service** option, and then click **Next >**.
6 In the **Confirmation** page, click the **Install** button.

![Figure 121](image)

7 Click the **Close** button once ‘Installation Succeeded’ message appears on the **Results** page.

![Figure 122](image)
Step 6: Create an SSL-enabled FTP Site

1. Select the Start button, select Programs, and then select Administrative Tools.
2. Select Internet Information Services (IIS) Manager.
3. In the Connections pane, select Sites node.
4. Right click Sites node, and then click Add FTP Site.
   (OR)
   Click Add FTP Site in the Actions pane.

Add FTP Site dialog box appears on the screen.

5. In FTP site name, type the site name as 'My New FTP Site', and then locate the physical path of the ftproot folder.
6  Click the **Next** button.
7 Select a local IP address for FTP site from the IP Address drop-down, or type local loopback IP address for the computer by typing "127.0.0.1" in the IP Address box.

8 Keep the default port selection as 21, or the port number can be changed, if required.

9 In the SSL pane, select Allow SSL option, and then click the View button to locate the SSL certificate received by the vendor.

10 Click the Next button. Authentication and Authorization Information page will appear on the screen.

11 In the Authentication pane, check the Basic option.

12 In the Authorization pane, select Specified users from the Allow access to drop-down.

13 Type the user name that is authorized to do FTP access.
   For example: Administrator.

14 Check Read and Write as the Permissions option.
15 Click the **Finish** button.
IIS 6.0 on Windows Server 2003 Enterprise SP2

**Step 1: Create the 'Certificate Request'

1. Select the **Start** button, select **All Programs**, and then select **Control Panel**.
2. Select **Administrative Tools**, and then select **Internet Information Services (IIS) Manager**.

![Image of IIS Manager](image)

**Figure 128: IIS Manager**

3. Expand the highlighted local computer node, expand the **Web Sites** node, and then right click **Default Website**.
4. Click **Properties**.

The **Default Web Site Properties** dialog box will appear on the screen.
5. Click the **Directory Security** tab.
6. Click the **Server Certificate** button.

   *Welcome* screen for **IIS Certificate Wizard** will appear on the screen.
7. Click the **Next >** button.
8. Select **Create a new certificate** option, and then click **Next >**.
9. Select **Prepare the request now, but send it later** option, and then click **Next >**.

![IIS Certificate Wizard](image)

**Figure 134: Place certificate request**

10. In the **Name and Security settings** pane,

   - Type a relevant name for certificate in the **Name** box. Example: TEST
   - Set bit length to 2048 from the **Bit Length** dropdown.
   - Check **Select cryptographic service provider (CSP) for this certificate** option, if required.
11. Click the **Next >** button.

   If **Select cryptographic service provider (CSP) for this certificate** option is selected, then in the next screen select the name of cryptographic provider.

   Select **Microsoft RSA SChannel Cryptographic Provider** as cryptographic provider, and then click the **Next >** button.
12. Type organizational information, and then click the **Next** button.
13. Type the system name (FQDN- Fully Qualified domain name) in **Common name** box as website’s common name, and then click the **Next >** button.

Example: *mcloon.toons.local*

![IIS Certificate Wizard](image)

*Figure 138: Enter a common name for site*

14. Select the country or region from **Country/Region** dropdown,
15. Select state or province from State/Province dropdown.
16. Select city or locality from City/Locality dropdown, and then click the Next > button.
17. Enter a file name for the certificate request, and then click the **Next >** button.

18. Read the **Request File Summary** to verify the provided certificate information, and then click the **Next >** button.

![IIS Certificate Wizard](image)

**Figure 141: Verify provided certificate details**

19. Click the **Finish** button.
Figure 142: Complete the process

20. Send this request file to the certificate vendor.

**Step 2: Install the certificate**

**NOTE:** Certificate received from the vendor needs to be copied to the system.

1. In the **Internet Information Services (IIS) Manager**, right click **Default Websites**, and then click **Properties**.
   
   **Default Web Site Properties** dialog box will appear on the screen.

2. Click the **Directory Security** tab.
3. Click the **Server Certificate** button.

   **Welcome** screen for **IIS Certificate Wizard** will appear on the screen.
4. Click the Next > button.

5. Select **Process the pending request and install the certificate** option, and then click **Next >**.
6. In **Process a Pending Request** pane, browse the certificate file, and then click **Next >**.

![IIS Certificate Wizard](image1)

**Figure 146: Locate the certificate file**

7. By default, the system will select SSL port number as 443 for the website. The default number can be changed, if required, and then click **Next >**.

![IIS Certificate Wizard](image2)

**Figure 147: Website binding to the port number**
8. Read the **Request File Summary** to verify the provided certificate information, and then click the **Next >** button.

![Certificate Summary](image1)

**Figure 148: Certificate Summary**

9. Click the **Finish** button.

![Finish](image2)

**Figure 149: Finish**
The certificate installation process is now completed.

10. Click the **OK** button in **Default Website Properties**.

**Step 3: Configure the SSL settings**

1. In the **Internet Information Services (IIS) Manager**, expand the server node.
2. Expand the **Web Sites** node.
3. Right-click **Default Web Site**, and then click **Properties**.

**Default Web Site Properties** window will appear on the screen.

4. Click the **Directory Security** tab.
5. In the **Secure Communications** pane, click **Edit**.
6 Check the **Require secure channel [SSL]** option, and then check the **Require 128-bit encryption** option.
7 Click **OK**.

**Step 4: Test the SSL enabled default web site**

1 Open the **Internet Explorer**.

2 Type **https://localhost/EventTracker/Login.aspx** in the address field.

   Internet explorer displays the addressed page.
NOTE: If http://localhost/EventTracker/Login.aspx is used in the address field, internet explorer will display server error message.
Step 5: Create FTP service

NOTE: Follow step 5 to transfer custom logs from remote server to EventTracker server only if needed.

1. Select the Start button, select Settings, and then select Control Panel.
2. Double click Add or Remove Programs.
   Add or Remove Programs dialog box will appear.
3. On the left pane, click Add/Remove Windows Components.
   Windows Component Wizard will appear.

4. Double click Application Server.
5 Double click **Internet Information Services (IIS)**.
6  Check **File Transfer Protocol (FTP) Service**, and then click the **OK** button.
7  In the **Application Server** dialog box, click the **OK** button.
8  In the **Windows Component Wizard**, click the **Next >** button.
9  Locate the required file for installation to continue.
10 Click the **Finish** button to complete the Windows Components Wizard.

**Step 6: Configure Windows 2K3/2K8 server to require clients to use SSLv3 or TLS.**

The server accepts clients using TLS or SSLv3, it also accepts clients using SSLv2. SSLv2 is an older implementation of the ‘Secure Sockets Layer’ protocol. It suffers from a number of security flaws allowing attackers to capture and alter information passed between a client and the server.

**NOTE:**

There is no need to do any registry changes in Windows Server 2012.

Follow the instructions given below to disable the PCT 1.0 & SSL 2.0 protocols. Once disabled, IIS will not try to negotiate using the PCT 1.0 & SSL 2.0 protocol.

1. Click the **Start** button, and then click **Run**.
2. Type `regedt32` or type `regedit`, and then click **OK**.
3. In **Registry Editor**, locate the following registry key:
   
   `HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1.0\Server`

4. Click the **Edit** menu, click **New**, and then click **DWORD value**.

   Or

   Right click in right pane, click **New**, and then click **DWORD value**.

5. In the **Name** column, type the value name as ‘Enabled’, and then click outside the name box or press the **Enter** button.
6. Double-click the value name to change the DWORD value to zero.

7. In **Edit DWORD Value** dialog box, type value data as '0', and then click the **OK** button.

---

**Step 7: Configure Windows 2K3/2K8/2K12/2K12R2 server to disable support for 'Weak Ciphers'**

The TLS/SSL server supports cipher suites based on weak algorithms. This may enable an attacker to launch man-in-the-middle attacks and monitor or tamper with sensitive data.

Disable the following keys, if it exists:

- \HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128
- \HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 56/128
- \HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 56/56
- \HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128
- \HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40/128
- HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56 "Enabled"=dword:00000000
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 64/128] "Enabled"=dword:00000000
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128] "Enabled"=dword:00000000
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0
  Create a new key: Server
  Create a new DWORD (32-bit) named Enabled and check the data value is the default 0x00000000 (0)
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0
  Create a new key: Server
  Create a new DWORD (32-bit) named Enabled and check the data value is the default 0x00000000 (0)
  Restart the server.

NOTE:

If the above mentioned entries are not available then you need to create these registry keys manually in the Registry Editor.

To disabled the keys, create the DWORD named "Enabled", and set its data value to 0x0. Follow the steps given below to disable the keys:

1. In Registry Editor, locate the following registry key:
   HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128
2. Click the Edit menu, click New, and then click DWORD value.
   Or
   Right click in right pane, click New, and then click DWORD value.
3. In the **Name** column, type the value name as ‘Enabled’, and then click outside the name box or press the **Enter** button.

   ![Figure 162](image)

   **Figure 162**

   3. In the **Name** column, type the value name as ‘Enabled’, and then click outside the name box or press the **Enter** button.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Default)</td>
<td>REG_SZ</td>
<td>(value not set)</td>
</tr>
<tr>
<td>Enabled</td>
<td>REG_DWORD</td>
<td>0x00000000 (0)</td>
</tr>
</tbody>
</table>

   ![Figure 163](image)

   **Figure 163**

   4. Double-click the value name to change the DWORD value to zero.

   5. In **Edit DWORD Value** dialog box, type value data as ‘0’, and then click the **OK** button.

   ![Figure 164](image)

   **Figure 164**

   NOTE: Using above steps disable the rest of the keys.

**Step 8: Configure IIS to return the ‘Fully Qualified Domain Name’ of the Web Server Instead of its IP Address.**

An incorrectly configured IIS server sometimes leaks its internal IP address in a header field returned after a specially crafted GET or HEAD request. This allows attackers to learn more about the internal network.

Set the UseHostName property. Follow the instructions given below to set the UseHostName property:
1. Click the Start button, and then click Run.
2. Type cmd, and then click OK.
   The command prompt appears on the screen.

![Figure 165](image1)

3. Change to the folder where the Adsutil.vbs file is located. By default, this folder available under C:\Inetpub\AdminScripts.

![Figure 166](image2)

4. Type the following command.
   ```cscript adsutil.vbs set w3svc/1/UseHostName true```

5. Restart the computer.
Restrict EventTracker website

Configuring IP address and domain name restrictions in Internet Information Services (IIS) allows you to permit or deny access to the web server, web sites, folders, or files. Rules can be configured for remote IP addresses or based on the Domain name.

When a remote client that is not permitted access requests a resource i.e. a 403.6 ("Forbidden: IP address of the client has been rejected") or 403.8 ("DNS name of the client is rejected"), HTTP status will be logged by Internet Information Services (IIS).

IP and Domain Restrictions option is not enabled by default when you install Internet Information Services (IIS). You can enable IP and Domain Restrictions option by adding the above Role Service as mentioned below.

Install IP and Domain Restriction in Win2K8, 2K8 R2, 2012

1) Click the Start button.
2) Select Administrative Tools, and then select Server Manager.
3) Select Add Role Services.
4) In ‘Security’, select 'IP and Domain Restrictions', and then select Next.

5) Click the Install button.
Configure IP Address and Domain Restrictions (IIS 7, 7.5, 8) in Win 2K8, Win 2K8 R2, Win 2012

1. Open IIS Manager.
2. Expand Roles node, expand Web Server (IIS) node, and then select Internet Information Services.
3. Expand Default Web Site node, select EventTracker.

Figure 170 in 2K8 R2 machine
4. In **Features View**, double-click **IP Address and Domain Restrictions**.

5. In **Actions** pane, select "**Add Allow Entry**" or "**Add Deny Entry**" to add Allow or Deny entries.
You can specify an IP address or an IP address range or a Domain Name in above dialog boxes.

**NOTE:**
Configuring Allow or Deny restrictions using Domain name require reverse DNS look up every time a request arrives the server. Performing reverse DNS lookups is a potentially expensive operation that can severely degrade the performance of your IIS server.

Configure IP address and domain name restriction in Win2K3

1) Click the **Start** button.
2) Select **Administrative Tools**, and then select **Internet Information Services (IIS) Manager**.
   (OR)
   Select **Run** command prompt, type **inetmgr**, and then select the **OK** button.
   IIS Web Server displays.
3) Expand local computer node, expand **Web Sites** folder, and then expand the **Default Web Site** node.
4) Right-click **EventTracker** and then select **Properties**.
EventTracker Properties window displays.

5) Select **Directory Security** tab.
In IP address and domain name restrictions, select the Edit button. IP Address and Domain Name Restrictions window displays.

7) Select Granted Access or Denied access button and then click the Add button.
8) Select the **Type** of computer (i.e. Single Computer, Group of Computers or Domain name).

9) Enter the **IP address**.

10) Select **DNS Lookup** to enter the DNS name.

11) Click the OK button.
Request Filtering in IIS 7, 7.5, 8

To install Request Filtering in Windows 2012

1. Select the Start button, and then select Administrative Tools.
2. Select Server Manager, select Dashboard, and then select Add Role and Features Wizard.
3. In the Add Roles and Features Wizard, Before You Begin page displays.
4. Select the Next button.
5. On the Select installation type page, select Role-based or feature-based installation, and then select the Next button.
6. On the Select destination server page, select Select a server from the server pool, select your server from Server Pool list, and then choose the Next button.
7. In the Select Server Roles window, expand and select Web Server.
8. Expand and select Security node, and then select Request Filtering, and then click Next >.

10. On the **Results** page, click **Close**.

**To install Request Filtering in Win 2K8 / 2K8 R2**

1. On the taskbar, click **Start**, point to **Administrative Tools**, and then click **Server Manager**.
2. In the **Server Manager** hierarchy pane, expand **Roles**, and then click **Web Server (IIS)**.
3. In the **Web Server (IIS)** pane, scroll to the **Role Services** section, and then click **Add Role Services**.
4. On the **Select Role Services** page of the **Add Role Services Wizard**, select **Request Filtering**, and then click **Next >**.

![Add Role Services](image)

**Figure 181**

5. On the **Confirm Installation Selections** page, click **Install**.
6. On the **Results** page, click **Close**.
To allow/deny access to a specific file name extension

1. Open Internet Information Services (IIS) Manager:
   o If you are using Windows Server 2008 / 2008 R2 / 2012:
     ▪ On the taskbar, click Start, point to Administrative Tools, and then click Internet Information Services (IIS) Manager.
2. In the Connections pane, go to the connection, site, application, or directory for which you want to modify your request filtering settings.
3. In the Home pane, double-click Request Filtering.
4. In the Request Filtering pane, click the File Name Extensions tab.
5. To deny file name extensions in the Actions pane, click Deny File Name Extension...

![Internet Information Services (IIS) Manager](image)

Deny File Name Extension dialog box displays.

6. Enter the file name extension that you wish to block, and then click OK.
For example, to prevent access to files with a file name extension of .inc, you would enter "inc" in the dialog box.

7. To allow file name extensions in Actions pane, click Allow File Name Extension...

8. Enter the file name extension that you wish to allow, and then click OK.
Install and configure URLScan security tool in IIS 6

URLScan is an open source security tool to secure IIS 6.0 only [for IIS 7.0 and above it is in-built]. It is an add-on tool that can be used by Web site administrators.

Benefits of URLScan security tool

- The administrators can control the actions of URLScan and restrict the type of HTTP requests that the server processes.
- An Internet Server API (ISAPI) filter that screens and monitors HTTP requests for Internet Information Server.
- It is used to reduce the exposure of IIS to potential Internet attacks.
- By default, it does not make special accommodations for file name extensions that ASP.NET Web applications use.
- You can change the URLScan configuration to add an extra layer of security for these applications.
- You must disable or enable different file name extensions for application level tracing, XML Web services, and remoting.

Configure URLScan

To configure URLScan to enable standard ASP.NET file name extensions that users are requested to follow these steps:

1. Install the URLScan tool. For information and instructions, visit the following Microsoft Web site:
2. Open the Urlscan.ini file in a text editor (such as Notepad). This file is located in the \System Root\System32\Inetsrv\Urlscan\ folder.
3. In the [AllowExtensions] section, add the following file name extensions:
   - .aspx
4. In the [DenyExtensions] section, add the following file name extensions:
   - .asax
   - .ashx
   - .ascx
   - .config
   - .cs
   - .csproj
   - .dll
   - .licx
5. To turn on application level tracing, add the .axd file name extension to the [AllowExtensions] section. If you do not want to turn on application level tracing, add .axd to the [DenyExtensions] section.

6. To allow Web services, add the .asmx file name extension to the [AllowExtensions] section. If you do not want to allow Web services, add .asmx to the [DenyExtensions] section.

7. To turn on remoting, add the .rem file name extension and the .soap file name extension to the [AllowExtensions] section. If you do not want to turn on remoting, add .rem and .soap to the [DenyExtensions] section.

8. Save and then close the Urlscan.ini file. You must restart IIS for the changes to take effect.

NOTE:

These steps are designed to offer optimal protection, regardless of whether the UseAllowVerbs setting is turned on in URLScan.
Secure SQL Database Server

SQL Server 2008 / 2008 R2 / 2012

Reduce the Surface Area:

To reduce the surface area of SQL Server, apply the following best practices.

1. **Install only the required SQL Server components.**
   While installing SQL Server, do not include ‘Analysis Services’, ‘Integration Services’, and ‘Full-Text’ engine.

2. **Don’t install SQL Server Reporting Services (SSRS) on the same server as the database engine.**
   If SSRS is installed on the same server as the database engine, then web services will open a hole in the security layer.

3. **Install only two features, ‘Database Engine Services’ and ‘Management Tools – Basic’.**

![Figure 185: SQL Server 2008 R2 Setup](image-url)
4. **Disable the following SQL Server services.**
   Disable (or leave disabled) the following services.
   - Disable the **SQL Server VSS Writer** service.
   - Leave the **SQL Server Browser** service disabled.
   - Leave the **SQL Active Directory Helper** service disabled.
   Click [here](#) for the detailed instruction on how to disable the SQL server services.

5. **Make sure that the antivirus is current and configured correctly.**

6. **Install the most recent critical fixes and service packs for both Windows and SQL Server.**
SQL Server 2005

Reduce the Surface Area:

To reduce the surface area of SQL Server, apply the following best practices.

1. **Install only 'Database Engine Services'.**
   
   Do not include Analysis, Reporting, Notification, and Integration services. Also do not opt for Workstation components, Books Online, and development tools option.

![Figure 187: SQL Components](image)

2. **Disable the following SQL Server services.**
   
   Disable (or leave disabled) the following services.
   
   - Disable the SQL Server VSS Writer service.
   - Leave the SQL Active Directory Helper service disabled.
   - Leave the SQL Server Browser service disabled.

   Click [here](#) for the detailed instruction on how to disable the SQL server services.
Disable the SQL Server Services

Follow the steps given below to disable the services,

1. Click **Start** button, and then click **Run**.

![Run dialog box](image1.png)

2. In the **Run** dialog box, type `'Services.msc'`, and then click the **OK** button.

![Run dialog box](image2.png)

**Services** window will appear on the screen.
3. Locate the required service(s) name in the **Name** column. For example: ‘SQL Server VSS Writer’ service.

4. Right click the service to be disabled, and then click **Properties**.
Figure 191

SQL Server VSS Writer Properties (Local Computer) dialog box appears on the screen.
5. Click **Startup type** dropdown, and select ‘**Disabled**’.
6. Click the **Stop** button to stop the service.

7. Click the **Apply** button, and then click the **OK** button.

![Services window](image)

**Figure 194: Services window**

**NOTE:** If remote indexer is enabled in the EventTracker server then,

- ‘SQL server browser’ service should be enabled.
- Need to add ‘sqlbrowser.exe’ & ‘sqlservr.exe’ in firewall exception list.

**SQL Server SA Account**

- Windows Authentication mode is more secure than SQL Authentication. Hence configure SQL Server to use Windows authentication only.
- If Windows Authentication mode is selected during installation, the SA login is disabled by default. If the authentication mode is switched to SQL Server mixed mode after the installation, the SA account is still disabled and must be manually enabled if required.
- If mixed mode authentication needs to be enabled, then
- Disable or Rename SA Account. Do not use this account for SQL server management.
- If there is a need to use SQL Authentication, then enforce a strong password policy.

Add Windows Firewall Exceptions

The ports in use should be added to the firewall exception list. Based on the system capacity, any number of VCP's can be added. For EventTracker, add the following port numbers to the firewall exception list:

<table>
<thead>
<tr>
<th>Port Number/.EXE</th>
<th>Used For</th>
</tr>
</thead>
<tbody>
<tr>
<td>14505(TCP/UDP)</td>
<td>Windows Receiver</td>
</tr>
<tr>
<td></td>
<td>Multiple VCP's can be configured</td>
</tr>
<tr>
<td>14502, 14508 (TCP)</td>
<td>Change Audit</td>
</tr>
<tr>
<td>14503 (TCP)</td>
<td>EventTracker Certificate server</td>
</tr>
<tr>
<td>14506 (TCP)</td>
<td>EventTracker Agent</td>
</tr>
<tr>
<td>14507 (TCP)</td>
<td>Collection Master</td>
</tr>
<tr>
<td>443</td>
<td>EventTracker securely access( HTTPS )</td>
</tr>
<tr>
<td>514 (UDP/TCP)</td>
<td>Syslog Receiver</td>
</tr>
<tr>
<td></td>
<td>Multiple VCP's can be configured</td>
</tr>
</tbody>
</table>
EventTracker Settings

Secure Agent Configuration and Save as Template

The current agent configuration settings on the local system can be protected from being modified by any unauthorized remote system. In this option, either allow only the local system to modify the agent settings or configure up to five IP addresses of remote systems from where the modification of agent configuration is possible.

It is recommended to save the agent configuration settings as a ‘Template’ and apply it to multiple agent systems at once instead of applying them individually.

In order to use the same configuration settings for agent systems, the agent configuration on local system needs to be saved as ‘Template’ first. The template will be saved as .ini file in the default path, which would be ...

To Protect the Current Configuration Settings for Local System

1. Logon to EventTracker Enterprise.
2. Click the Admin dropdown, and then click Windows Agent Config.
3. Click the Security tab.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Agent Configuration Protection</strong></td>
<td></td>
</tr>
<tr>
<td>Enable protection for Agent configuration</td>
<td>Select this option to protect the configuration settings from being modified by a remote agent system.</td>
</tr>
<tr>
<td><strong>Settings can be modified on the following system(s)</strong></td>
<td></td>
</tr>
<tr>
<td>Local System</td>
<td>Select this checkbox to protect the current configuration settings of the local system. Other users cannot modify the settings from their machines.</td>
</tr>
<tr>
<td>Enter IP Address</td>
<td>Select this checkbox to allow the specified remote systems to do the configuration changes in the local system. Type the IP address in the IP Address box. Up to five IP addresses can be configured, separated by comma (,)</td>
</tr>
<tr>
<td>Remedial Action</td>
<td>Remedial actions are scripts or EXEs that can be launched at either the agent or Manager side, in response to events.</td>
</tr>
</tbody>
</table>

4. Check the **Enable protection for Agent configuration** option.

5. Click the **Save** button.

   NOTE: To apply this configuration to the agent systems present in the enterprise, click the **Apply this configuration to agents** button.

**To Save Agent Configuration as Template**

1. In **Windows Agent Config**, make the required configuration changes in **agent configuration** tab(s), and then click the **Save** button.

   EventTracker saves the configuration for the selected system.

2. In order to use the same settings for multiple agent systems, click the **Save as** button to save the setting as template.

   EventTracker displays **Template file location** pop-up window.
3. Enter the template name, and then click the **Save** button.

4. EventTracker saves the agent configuration template in the path specified in **File Location** field.

**To Apply Configuration to Agent System(s)**

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** dropdown, and then click **Windows Agent Config**.
3. Click the **Load Template** button, select the **File name**, and then click the **Load** button.

EventTracker displays the selected template configuration.
4. To apply this configuration to the agent systems present in the enterprise, click the **Apply this configuration to agents** button.

**Apply client configuration across enterprise** dialog box will appear on the screen.
5. Select a system group from **Select a group** dropdown. EventTracker displays the managed systems associated with the selected group.

6. Check the required system options for which the configuration needs to be applied.

7. Select the **Configuration groups** option as per requirement.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Apply Only Modified Settings</strong></td>
<td>EventTracker selects this option by default. Leave the default selection to apply only modified settings.</td>
</tr>
<tr>
<td><strong>Apply All Settings</strong></td>
<td>Select this option to apply all settings including the default and modified settings.</td>
</tr>
<tr>
<td><strong>Apply Only Selected Settings</strong></td>
<td>Select this option to apply only the selected settings made under respective tabs. EventTracker enables the checkboxes. Select appropriately and then click <strong>Apply</strong>.</td>
</tr>
</tbody>
</table>

8. Click the **Apply** button.
EventTracker displays a warning message.

```
Figure 200
```

You have chosen to apply current configuration to specified Agents. This will result in loss of specific Agent configuration done earlier. Do you want to continue?

```
OK Cancel
```

9. Click the **Ok** button.
EventTracker displays confirmation message.

```
Figure 201
```

Settings applied successfully.
10. Click the Ok button.  
The template configuration is loaded successfully on the selected systems.

Secure EventVault Storage

Provide EventVault storage access only to the required EventTracker administrators/users.

1. **Backup purpose:**
   
   Provide the full permission for the user who is responsible to take periodic backup of the data.

2. **Archives stored in UNC (Uniform Naming Convention) path:**
   
   a. Create a service account.
   
   b. Provide full permission to the created service account.
   
   c. Change the following services to run under the created service account.
   
   • EventTracker Scheduler
   
   • EventTracker EventVault
   
   • EventTracker Reporter
   
   • EventTracker Indexer
   
   • Event Correlator (if available)

Change the Service account:

1. Click the Start button, and select Run.

2. Type `services.msc`, and then click the OK button.

![Figure 202](image)

3. In the Services window, search for EventTracker services.
4. Right click the service name, and click **Properties**.

For example: Right click **EventTracker EventVault** service

‘EventTracker EventVault Properties (Local Computer)’ window will be displayed.
5. Click **Log On** tab, and select **This account** option.

![Log On Tab](image)

6. Enter the user credentials and correct password. The user name should be in ‘domain name\user name’ format.
7. Click the **Apply** button.
   Warning message will be displayed on the desktop.

   ![Services Window](image)
   
   Figure 206

8. Click the **OK** button.
9. To run the service with new logon name, stop and start the service.
10. Likewise, for rest of the services, repeat step 4 to step 10 to change the service account.
    The **Log On As** column will display the changed service account name.

   ![Service Details](image)
   
   Figure 207
Check with Vulnerability Scanner

It is a standard practice to scan critical machines for vulnerabilities. The hardened EventTracker system can also be scanned for vulnerabilities. Upon doing so, some of the following vulnerabilities maybe reported.

*The possibilities and their solutions/configuration changes are shown in the below table.

<table>
<thead>
<tr>
<th>Vulnerabilities</th>
<th>Impact</th>
<th>Recommended actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>'rsh' Remote Shell Service Enabled</td>
<td>This is a legacy service often configured to blindly trust some hosts and IPs. The protocol doesn't support encryption or any sort of strong authentication mechanism.</td>
<td>EventTracker uses default port 514 for receiving syslog messages. Configure the firewall to allow incoming connections on port 514 from trusted hosts or use another port for receiving syslog in EventTracker Manager Configuration.</td>
</tr>
<tr>
<td>FTP server does not support AUTH command</td>
<td>By default, FTP clients send user credentials (user ID and password) in clear text to the FTP server. This allows malicious users to intercept the credentials if they can eavesdrop on the connection.</td>
<td>FTP server is installed on the EventTracker server to transfer custom logs from remote sources. • In case of IIS 6, FTP does not support AUTH command. This is by design, use a third party FTP that supports AUTH command and configure FTP over SSL.</td>
</tr>
<tr>
<td>Untrusted TLS/SSL server X.509 certificate</td>
<td>The server's TLS/SSL certificate is signed by a Certification Authority (CA) whose publisher is not known or a trusted one. It could indicate that a TLS/SSL man-in-the-middle is taking place and is eavesdropping on TLS/SSL connections.</td>
<td>Obtain a new certificate signed by trusted certificate authorities, such as Thawte or Verisign.</td>
</tr>
<tr>
<td>Guest access allowed to Windows event logs</td>
<td>Windows event logs have been configured to allow guest access. They contain information about</td>
<td>For each event log listed, find the following registry key: HKEY_LOCAL_MACHINE\System\CurrentCo</td>
</tr>
<tr>
<td>Application, security, and system events taking place on the local machine. These logs can contain sensitive information, therefore only administrators should be allowed to access/read them.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ntrolSet\Services\Event[logname]</strong> Under this key, add a DWORD value named &quot;RestrictGuestAccess&quot; and set it to 1.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Microsoft IIS default installation/welcome page installed (http-iis-default-install-page)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IIS default installation or &quot;Welcome&quot; page is installed on this server. This usually indicates a newly installed server which has not yet been configured properly and not be known about.</td>
</tr>
<tr>
<td>Replace default page with relevant content page.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TCP timestamp response (generic-tcp-timestamp)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The remote host responded with a TCP timestamp. The TCP timestamp response can be used to approximate the remote host's uptime, potentially aiding in further attacks. Additionally, some operating systems can be fingerprinted based on the behavior of their TCP timestamps.</td>
</tr>
<tr>
<td>Disable TCP timestamp responses on Windows. For each event log listed, find the following registry key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters Under this key, add a DWORD value named &quot;Tcp1323Opts&quot; and set it to 1.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>General Security Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Clear text authentication FTP specification primarily provides a means for authenticating user ids and passwords stored in clear text, though there are secure mechanisms to authenticate. User ids and passwords can be stolen by a malicious user if he is able to monitor FTP traffic.</td>
</tr>
<tr>
<td>FTP server is installed on the EventTracker server to transfer custom logs from remote sources. • In case of IIS 6, FTP does not support AUTH command. This is by design, either use a third party FTP that supports AUTH command and configure FTP over SSL or configure FTP server to allow connection from trusted host.</td>
</tr>
</tbody>
</table>

* These vulnerabilities are determined by Vulnerability scanners.