Hardening Guide for EventTracker Server
Version-9.x
Introduction

The EventTracker solution includes a console component that is installed on a 2008 / 2008 R2 / 2012/2016 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 v9.x console.
# Table of Contents

Introduction ....................................................................................................................................................... 1
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
Secure IIS Web Server ....................................................................................................................................... 4
Secure SQL Server .............................................................................................................................................. 5
Add Windows Firewall Exceptions .................................................................................................................... 5
Check with Vulnerability Scanner ...................................................................................................................... 6
   Security Recommendation for EventTracker v9.0 ........................................................................................ 6
Restrict Email/File Sharing Website access: .................................................................................................... 10

Harden Server – Detailed View ........................................................................................................................... 11
Harden Windows Server .................................................................................................................................. 11
   Apply Group Policies on Windows Server 2012 .......................................................................................... 11
   Apply Group Policies on Win2K8 / 2K8 R2 Enterprise SP1 (Active Directory) ............................................ 20
   Apply Group Policies in a Workgroup on Windows Server 2012 ............................................................. 28
   Apply Group Policies in a Workgroup on Win2K8 / 2K8 R2 .................................................................... 36
Secure IIS Web Server ......................................................................................................................................... 45
Mandatory Requirements ............................................................................................................................... 45
IIS 7, 7.5, 8 and 8.5 on Win 2K8 / 2K8 R2 / 2012/2016 ...................................................................................... 45
Restrict EventTracker website .......................................................................................................................... 69
   Install IP and Domain Restriction in Win2K8, 2K8 R2, 2012, 2016 ............................................................. 69
   Configure IP Address and Domain Restrictions (IIS 7, 7.5, 8 and 8.5) in Win 2K8, Win 2K8 R2, Win 2012,
   Win 2016 ..................................................................................................................................................... 71
Request Filtering in IIS 7, 7.5, 8, 8.5 ................................................................................................................... 73
   To install Request Filtering in Windows 2012/2016 .................................................................................... 73
   To install Request Filtering in Win 2K8 / 2K8 R2/2016 ............................................................................ 74
   To allow/deny access to a specific file name extension ............................................................................. 75
Secure SQL Database Server ............................................................................................................................... 77
SQL Server 2008 / 2008 R2 / 2012/2016 ................................................................................................. 77
SQL Server 2005 .............................................................................................................................................. 80
Disable the SQL Server Services ...................................................................................................................... 81
    SQL Server SA Account ................................................................................................................................ 85
Add Windows Firewall Exceptions .................................................................................................................. 86
EventTracker Settings ...................................................................................................................................... 86
    Secure Agent Configuration and Save as Template .................................................................................... 86
    To Protect the Current Configuration Settings for Local System ................................................................. 86
Secure EventVault Storage .......................................................................................................................... 91
Check with Vulnerability Scanner .................................................................................................................. 95
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 2012/2016 should be carried according to the standard policy. Click the link below to download the GPO and apply the following policies:

Download 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:

Download 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.

Secure IIS Web Server

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

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, 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, Multiple VCP’s can be configured</td>
</tr>
<tr>
<td>14504</td>
<td>EventTracker Active WatchList</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 v9.0

 A golden snapshot of EventTracker v9.0 is available (named Change Policy v9.0). As soon as EventTracker is installed in customer premises, EventTracker v9.0 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] =C:\Program Files (x86)\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 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.
3) Select Change Browser on the toolbar.
   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 1

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. Select **Dashboard** icon and then select the required policy.

![Figure 4](image)

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

![Figure 5](image)

7. Click **Accept icon** and then click **Save icon**.
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.

Restrict Email/File Sharing Website access:

- Though Internet access is required for EventTracker to perform certain functions such as Threat Intel Feeds etc., there are certain accesses that need to be restricted to ensure security.

- Restrict access to personal emails/file sharing website (Gmail, Yahoo, Hotmail, Filezilla, Dropbox, External SharePoint etc.) under the category blocking of URL or Web content filtering service. This secures the system against Data Ex-filtration attempts of the logs stored in the EventTracker instance.

- Apart from this, it is mandatory to block the below sites on the EventTracker Server. Popular categories to be blocked are shown as below:

<table>
<thead>
<tr>
<th>Abortion</th>
<th>Illegal / Questionable</th>
<th>Pornography</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adult / Mature Content</td>
<td>Illegal Drugs</td>
<td>Proxy Avoidance</td>
</tr>
<tr>
<td>Alcohol</td>
<td>Intimate Apparel / Swimsuit</td>
<td>Sex Education</td>
</tr>
<tr>
<td>Alternative Sexuality / Lifestyles</td>
<td>Nudity</td>
<td>Spyware / Malware Sources</td>
</tr>
<tr>
<td>Alternative Spirituality / Occult</td>
<td>Open Image / Media Search</td>
<td>Spyware Effects</td>
</tr>
<tr>
<td>Extreme</td>
<td>Peer-to-Peer (P2P)</td>
<td>Suspicious</td>
</tr>
<tr>
<td>Gambling</td>
<td>Personals / Dating</td>
<td>Tobacco</td>
</tr>
<tr>
<td>Hacking</td>
<td>Phishing</td>
<td>Violence / Hate / Racism</td>
</tr>
</tbody>
</table>

Figure 7
Hardening Guide for EventTracker Server

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

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.

https://downloads.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](image)

**Figure 8**

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.
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.
Figure 13

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

   ![Figure 15](image)

   **Figure 15**

**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**.

![Select GPO dialog box](image)
The Group Policy objects are now linked to the organizational unit.

**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**.

**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.

https://downloads.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.

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

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

3. In the 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.

![Image of Import Progress]

Figure 26: 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.

![Image of Create New OU]

Figure 27: Create New OU
2. Enter the new organizational unit (OU) name, and then click **OK**.
   For example: EventTracker Server

![New Organizational Unit](image)

**Figure 28: 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**.

![Group Policy Management](image)

**Figure 29: 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 30: Select GPO

Figure 31
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.](image-url)
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 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.

   https://downloads.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_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 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)
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.

![App Screen](image-url)

LGPO folder appears on the screen.

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

Figure 37

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

Figure 38
4. Click the **Next >** button.

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

![Figure 39](image)

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

![Figure 40](image)
7. Click the **Install** button.

![LocalGPO Setup](image1)

**Figure 41**

8. Click the **Finish** button.

![LocalGPO Setup](image2)

**Figure 42**
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

![Administrator: LocalGPO Command-line](image)

Figure 43

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.

```powershell
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}

![Figure 44](image)

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**.
2. Select **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 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.
   
   https://downloads.eventtracker.com/support/utils/2008R2SSLFGPOBackup.zip

2. Extract the downloaded file to \\<systemname>\2008R2SSLFGPOBackup.

**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_Complainece_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.

![Microsoft Security Compliance Manager](image)

**Figure 47**

**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**.

- **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**.
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 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.
   - `cscript LocalGPO.wsf /<backup folder path>/\{guid}`
   - Here “guid” is the folder name which got created under GPObackups.
   - Ex: `C:\2008R2SSLFGPOBackup\{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**.

![Figure 57](image1)

![Figure 58](image2)
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 SP1/2012/2016 | OR |
|------------------|--------------------------------------------------------|
| Software and Component | • Internet Information Server (IIS) 7.0 and above. | • Browser, which supports 128-bit encryption |
|                  | • (IE 11 or above/ Firefox 3.5 or above).               |

IIS 7, 7.5, 8 and 8.5 on Win 2K8 / 2K8 R2 / 2012/2016

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.
3 Click the server node.
4 Double click **Server Certificates** icon in the IIS pane.

 Server Certificates pane displays.
5 In the Actions pane, click Create Certificate Request link. Request Certificate dialog box will be opened.
6 Type the system name (FQDN- Fully qualified domain name) as common name in the **Common name** text box.

Example: `mcloon.toons.local`

![Figure 65](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**.
10 Type name and path of the file to save the CSR (Certificate Server Request).

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.

   ![IIS pane](image)

   *Figure 68: IIS pane*

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

![Specify Certificate Authority Response in IIS 7, 7.5](image)
6 Locate the server certificate that has been received from the certificate authority.

Figure 71: Complete Certificate Authority request in IIS 8

Figure 72
7 Click **Open**.

![Figure 73 – Specify Certificate Authority Response](image)

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

![Figure 74 – Complete Certificate Authority request in IIS 7, 7.5](image)
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 76: Certificate appear in the ‘Server Certificates’ list

Step 3: Binding the certificate to the ‘EventTracker’

1. Expand the server node.
2. Expand the Sites node.
3. Click EventTracker.
4. In the Actions pane, click Bindings.

Figure 77: Default Web Site Home- Bindings
Site Bindings dialog box appears on the screen.

![Site Bindings dialog box](image)

Click Add.

Add Site Binding dialog box appears on the screen.

![Add Site Binding dialog box](image)

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.
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**.
Step 4: Configure ‘SSL Settings’

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

1. Expand the Sites node.
2. Click EventTracker.
3. Double-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.

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**.

![Figure 89: Server Manager](image)

3. In the **Server Manger** 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.

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

![Add FTP Site Publishing](image)

**Figure 98**

10 Click the **Next** button. The **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.

**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, 2016**

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 and 8.5) in Win 2K8, Win 2K8 R2, Win 2012, Win 2016

1. Open IIS Manager.
2. Select EventTracker site.
3. In **Features View**, double-click **IP Address and Domain Restrictions**.

4. 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.

Request Filtering in IIS 7, 7.5, 8, 8.5

To install Request Filtering in Windows 2012/2016

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 >**.

![Select server roles](image)

9. On the **Confirm Installation Selections** page, click **Install**.

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

To install Request Filtering in Win 2K8 / 2K8 R2/2016

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 >**.
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**:
   - 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**...
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....

![Figure 110](image)

8. Enter the file name extension that you wish to allow, and then click OK.

Secure SQL Database Server

SQL Server 2008 / 2008 R2 / 2012/2016

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 111: SQL Server 2008 R2 Setup
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 113: 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](image)

   **Figure 114: Run dialog box**

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

   ![Run dialog box](image)

   **Figure 115**

   **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 117

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.

![Figure 120: Services window](image)

**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, 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, Multiple VCP’s can be configured</td>
</tr>
<tr>
<td>14504</td>
<td>EventTracker Active WatchList</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 …ProgramFiles\PrismMicrosystems\EventTracker\RemoteInstaller.

To Protect the Current Configuration Settings for Local System

1. Go to EventTracker Control Panel.
2. Double-click the **EventTracker Agent Configuration**, and then click **File** dropdown.

3. Click the **Security** option.

![Figure 121: Security tab](image)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Agent Configuration Protection**         | **Enable protection for Agent configuration**  
Select this option to protect the configuration settings from being modified by a remote agent system. |
| **Settings can be modified on the following system(s)** | **Local System**  
Select this checkbox to protect the current configuration settings of the local system. Other users cannot modify the settings from their machines. |
Enter IP Address | 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 (,)

Remedial Action | Remedial actions are scripts or EXEs that can be launched at either the agent or Manager side, in response to events.

4. Check the **Enable protection for Agent configuration** option.
5. Click the **OK** button.

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

**To Apply Configuration to Agent System(s)**
1. Go to **EventTracker Control Panel**.
2. Double-click the **EventTracker Agent Configuration**, and then click **File** dropdown.
3. Click the **Load Template** button.

4. Select the **File name** from the file location, and then click the **open** button.
EventTracker loads the selected template configuration.

5. 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.
6. Select a system group from **Select a group** dropdown.

   EventTracker displays the managed systems associated with the selected group.

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

8. 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>
</tbody>
</table>
Apply Only Selected Settings | Select this option to apply only the selected settings made under respective tabs. EventTracker enables the checkboxes. Select appropriately and then click **Apply**.

9. Click the **Apply** button.

   EventTracker displays a warning message.

   ![Message from webpage](image)

   **Figure 126**

   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 button](image)

   10. Click the **Ok** button.

       EventTracker displays confirmation message.

       ![Message from webpage](image)

       **Figure 127**

       **Settings applied successfully.**

       ![OK button](image)

   11. 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.

![Run dialog box](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.

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.
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.

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 may be 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 (service-rsh)( CVE-1999-0651)</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 sylogs 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>
</tbody>
</table>
| **FTP server does not support AUTH command (ftp-generic-0007)** | 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. | 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. |
| **Untrusted TLS/SSL server X.509 certificate (tls-untrusted-ca)** | 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. | Obtain a new certificate signed by trusted certificate authorities, such as Thawte or Verisign. |
| **Guest access allowed to Windows event logs** | Windows event logs have been configured to allow guest access. They contain information about 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. | For each event log listed, find the following registry key:  
`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Eventlog\[logname]`  
Under this key, add a DWORD value named "RestrictGuestAccess" and set it to 1. |
| **Microsoft IIS default installation/welcome page installed (http-iis-default-install-page)** | The IIS default installation or "Welcome" 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. | Replace default page with relevant content page. |
| **TCP timestamp response (generic-tcp-timestamp)** | 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. | 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 "Tcp1323Opt " and set it to 1. |
| General Security Issue | 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. | 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. |

* These vulnerabilities are determined by Vulnerability scanners.