Secure IIS Web Server with SSL
Abstract

The purpose of this document is to help users to

- Install and configure Secure Socket Layer (SSL)
- Secure the IIS Web server with SSL

It is supported for all EventTracker Enterprise v8.x versions.

NOTE: From v8.0 onwards, EventTracker is not supporting Windows 2003 (Operating System) and IIS 6.

Audience

The document holds good for EventTracker Users and Administrators who wish to access EventTracker via a secured layer.

The information contained in this document represents the current view of EventTracker on the issues discussed as of the date of publication. Because EventTracker must respond to changing market conditions, it should not be interpreted to be a commitment on the part of EventTracker, and EventTracker cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. EventTracker MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.

EventTracker may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from EventTracker, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2017 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
# Table of Contents

Abstract .................................................................................................................................................................... 1
Audience .................................................................................................................................................................. 1

Secure IIS Web Server with SSL .......................................................................................................................... 3
Secure Sockets Layer (SSL) ...................................................................................................................................... 3
Mandatory Requirements ....................................................................................................................................... 3
Operating System ................................................................................................................................................ 3
Software and Components .................................................................................................................................. 3

Windows Server 2012/2016 Enterprise ..................................................................................................................... 3
Install Active Directory Certificate Services (AD CS) in Win 2012 ........................................................................ 4
Configure Active Directory Certificate Services (AD CS) in Win 2012 ................................................................. 18
Create a certificate request in Win 2012 ................................................................................................................ 30
  Get Pending Request Accepted by the Certificate Authority (CA) in Win 2012 .................................................... 37
Complete the certificate request in Win 2012 ......................................................................................................... 41
Bind the certificate to ‘Default Web Site’ in Win 2012 ........................................................................................... 48
Configure ‘SSL Settings’ in Win 2012 .................................................................................................................... 52

Windows Server 2K8/2K8 R2 Enterprise .................................................................................................................. 53
Install and configure the Certificate Authority (CA) in Win 2K8 / 2K8 R2 ............................................................ 54
Create Certificate Request in Win 2K8 / 2K8 R2 .................................................................................................... 67
  Get Pending Request Accepted by the Certificate Authority (CA) in Win 2K8 / 2K8 R2 ........................................... 73
Install the Certificate in Win 2K8 / 2K8 R2 ............................................................................................................... 78
Bind the Certificate to the Default Web Site in Win 2K8 / 2K8 R2 ................................................................. 82
  EventTracker 8.0 and above .............................................................................................................................. 82
Test the SSL Enabled Default Web Site in Win 2K8 / 2K8 R2 ................................................................................. 85
Configure SSL Settings in Win 2K8 / 2K8 R2 ........................................................................................................ 86
Secure IIS Web Server with SSL

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.

Source: [http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci343029,00.html](http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci343029,00.html)

You need SSL if you,

- Offer a login or sign in on your site
- Process sensitive data
- Need to comply with security requirements

Mandatory Requirements

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

Operating System

- Windows 2008 / 2008 R2 Server
- Windows 2012 Server
- Windows 2016 Server

Software and Components

- Active Directory and Domain Controller.
- Internet Information Server (IIS) 7.0 and above.
- Browser, which supports 128-bit encryption (IE 11 or above).

Windows Server 2012/2016 Enterprise

Windows Server 2012 uses Internet Information Services (IIS) 8.0 and 8.5.

Windows Server 2016 uses Internet Information Services (IIS) 10.

Summary:

- Install and configure the Certificate Authority (CA)
- Create the Certificate Request
- Get the Pending Request Accepted by the Certificate Authority
- Install the Certificate
Secure IIS Web Server with SSL

- Bind the Certificate to the Default Web Site
- Test the SSL enabled Default Web Site
- Configure SSL Settings

Install Active Directory Certificate Services (AD CS) in Win 2012

1. Select the Start button, select Administrative Tools, and then select Server Manager.

Server Manager displays. The Dashboard is displayed by default.

![Server Manager Dashboard](Figure 1)

2. Select Add Roles and Features.

   Add Roles and Features Wizard displays.

3. In the Before You Begin page, select the Next > button.
4. On the **Select installation type** page, select **Role-based or feature-based installation**, and then select the **Next >** button.
5. On the **Select destination server** page, select **Select a server from the server pool**, select a server from **Server Pool** list, and then select the **Next >** button.
6. On Select server roles page, select Active Directory Certificate Services option and then select the Next> button.
Add Features that are required for Active Directory Certificate Services window displays.
7. Verify the required features and then select the **Add Features** button.

Select server roles window displays.
8. **Select the** Next > **button.**

Select features page displays.
9. Select the **Next >** button.

   Active Directory Certificate Services page display.
10. Select the **Next >** button.

11. In **Select role services** page, select the **Certificate Authority** (if not selected) and **Certification Authority Web Enrollment** option.
Add features that are required for Certificate Authority Web Enrollment window displays.
12. Select the **Add features** button.

The selected role services are enabled.
13. Select the **Next >** button.

Confirm installation selections window displays.
14. Select the **Restart the destination server automatically if required** option and then select the **Install** button.

A successful message displays.
The installation of Active Directory Certificate Services is complete but is yet to be configured.
Configure Active Directory Certificate Services (AD CS) in Win 2012

The server manager displays a notification that AD CS is not yet configured.

1. **Click on the notification and continue to configure AD CS.**

   AD CS Configuration window displays to enter credentials:

   ![Figure 14](image)

   **Figure 14**

2. **Select the Next > button.**

   Role Services page displays.
3. Select role services **Certification Authority, Certification Authority Web Enrollment** option and then select the **Next >** button.
4. **Select the Next > button.**

   Setup Type page displays to specify Certification Authority.
By default, Standalone CA option is selected as Setup Type.

15. Select the **Next >** button.

CA Type page displays. By default, Root CA is selected as CA Type.
16. Select the **Next >** button.

Private Key page displays.

By default, Create a new private key option is selected.
17. Select the **Next >** button.

Cryptography for CA page displays.

By default, RSA#Microsoft Software Key Storage Provider is selected as Cryptographic provider and Key character length is 2048.
18. In **Select the hash algorithm for signing certificates issues by this CA**: list, select **SHA1**.

19. Select the **Next >** button.

CA Name page displays.
20. Type a distinctive common name and distinctive name in the **Common name for this CA:** and **Distinguished name suffix:** fields respectively or leave as it is.

21. Select the **Next >** button.

Validity Period page displays.
22. Set the **Specify the validity period** and then select the **Next >** button.

CA Database page displays.
23. If required, change the path of **Certificate database location:** and **Certificate database log location:** or leave it as it is.

24. Select the **Next >** button.
25. Crosscheck the configuration settings, and then select the **Configure** button.

A message stating ‘Configuration succeeded’ displays.
26. Select the Close button.

Server Manager displays the newly installed Role Services.

27. Restart the server.
Create a certificate request in Win 2012

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

![Figure 26](image)

2. Select the server node.
3. In IIS pane, double click **Server Certificates** icon.

![Server Certificates page displays.](image-url)

Figure 27

Server Certificates page displays.

Figure 28
4. In **Actions** pane, select **Create Certificate Request** link.

Request Certificate window displays.
5. In **Distinguished Name Properties** page, type the system name (FQDN - Fully qualified domain name) as common name in the **Common name** text box.

Example: mcloon.toons.local
6. Enter organization and geographical details, and then select the **Next** button. Cryptographic Service Provider Properties page displays.
Secure IIS Web Server with SSL

Figure 32

Microsoft RSA SChannel Cryptographic Provider is selected by default as Cryptographic service provider.

7. In **Bit length**: dropdown, set the bit length to 2048, and then select the **Next** button.

File Name page displays.
8. In **Specify a file name for the certificate request:**, type name and path of the file to save the **CSR** (Certificate Server Request).

9. Select the **Finish** button.

   Send this request file to the certificate vendor.
Get Pending Request Accepted by the Certificate Authority (CA) in Win 2012

Now you have a pending certificate request, and it needs to be accepted by the CA.

1. Open Internet explorer.
2. Type `http://server/certsrv` in the Address field.
   Here “server” is the name of the server for which you are creating the certificate.
   Example: elcwin2k8 or localhost

![Figure 34](image1)

3. Click the **Request a certificate** hyperlink.

![Figure 35](image2)

4. Click the **advanced certificate request** hyperlink.
5. Click the **Submit a certificate request by using a Base64-encoded CMC or PKCS #10 file, or submit a renewal request using a base64-encoded PKCS #7 file** hyperlink.

6. In **Saved Request**: box; enter the content of the certreq.txt file.

7. In **Certificate Template**: drop-down, select **Web Server**.
8. Click the **Submit >** button.
   Once you click Submit, the certificate is issued to you.

9. Select **Base 64 encoded** option.

10. Click **Download certificate** hyperlink.
11. To save the certificate on local drive, click the **Save** button.

Complete the certificate request in Win 2012

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

1. Select the Start button, select Administrative Tools, and then select Internet Information Services (IIS) Manager.
   ‘Internet Information Services (IIS) Manager’ window is displayed.
2. Click the server node.
3. In IIS pane, double click the Server Certificates icon.

5. In **Complete Certificate Request** window, click the browse button to specify **File name containing the certification authority’s response**.
Secure IIS Web Server with SSL

Complete Certificate Request

Specify Certificate Authority Response

Complete a previously created certificate request by retrieving the file that contains the certificate authority’s response.

File name containing the certification authority’s response:

Friendly name:

Select a certificate store for the new certificate:

Personal

6. Locate the server certificate that has been received from the certificate authority and then click Open.
Figure 45

Specify Certificate Authority Response page displays.
7. Type a relevant name in **Friendly name:** box to keep track of the certificate on this server and then 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.
Bind the certificate to ‘Default Web Site’ in Win 2012

1. Expand the server node, expand the Sites node, and then select Default Web Site node.

2. In the Actions pane, select Bindings....

![Figure 49: Site Bindings window displays.](image)
3. Select the **Add**... **button**.

Add Site Binding window displays.

4. In **Type**: drop down, select **https**.
By default, system will select the port number as 443. The default port number can be changed, if required.

5. In **SSL certificate**: drop down, select the recently installed SSL certificate, and then select the **OK** button.

The binding for port number 443 is listed.
6. Select the **Close** button.

The newly added https website is listed in Actions pane under Browse Website.
Configure ‘SSL Settings’ in Win 2012

1. To configure ‘SSL Settings’ to interact in a specific way with client certificates, expand the Sites node, and then select Default Web Site node.
2. In IIS pane, double-click SSL Settings icon.

Figure 56
SSL Settings page display.
3. Select **Require SSL** option.
4. In **Actions** pane, select the **Apply** button.
   
   After successful SSL settings modification, a message will be displayed in the **Actions** pane.
5. Close the **IIS Manager**.

**Windows Server 2K8/2K8 R2 Enterprise**

Windows Server 2K8 uses Internet Information Services (IIS) 7.0 and 7.5

**Summary:**
- Installing and configuring the Certificate Authority (CA)
- Creating the Certificate Request
- Getting the Pending Request Accepted by the Certificate Authority
- Installing the Certificate
- Binding the Certificate to the Default Web Site
- Testing the SSL enabled Default Web Site
- Configuring SSL Settings
Install and configure the Certificate Authority (CA) in Win 2K8 / 2K8 R2

1. Select the Start button, select Settings, and then select Control Panel.
2. Select Programs and Features, and then select Turn Windows Features on or off.

Server Manager displays.

3. Select Roles node, and then select Add Roles.
Add Roles Wizard displays.

4. Select the **Next >** button.
Select Server Roles page display.

**Figure 62**

5. Select **Active Directory Certificate Services** option and then select the **Next >** button.

**Figure 63**
Secure IIS Web Server with SSL

Introduction to Active Directory Certificate Services page displays.

Figure 64

6. Select the **Next >** button.
7. Select **Certificate Authority** (if not selected), **Certification Authority Web Enrollment** option, and then select the **Next >** button.

Figure 65
Specify Setup Type page displays.

By default, **Enterprise** option is selected as **Setup Type**.

![Add Roles Wizard]

Specify CA Type page displays.

By default, **Root CA** is selected as **CA Type**.

8. Select the **Next >** button.

Specify CA Type page displays.

By default, **Root CA** is selected as **CA Type**.
9. Select the **Next >** button.
   
   Set Up Private Key page displays.
   
   By default, **Create a new private key** option is selected.
10. Select the **Next >** button.
By default, RSA#Microsoft Software Key Storage Provider is selected as Cryptographic Service Provider (CSP) and Key character length as 2048. Leave as it is.

11. In **Select the hash algorithm for signing certificates issued by this CA**: list, select the Hash Algorithm as sha1.

![Configure Cryptography for CA](image)

**Figure 70**

12. Select the **Next >** button.

Configure CA Name page displays.
13. Type a distinctive common name and distinctive name in the **Common name for this CA:** and **Distinguished name suffix:** fields respectively or leave as it is.

14. Select the **Next >** button.

Set Validity Period page displays.
15. In Select validity period for the certificate generated for this CA:, set validity period and then select the Next > button.

Configure Certificate Database page displays.
16. If required, change the path of **Certificate database location:** and **Certificate database log location:**; select the **Browse** button and specify the path of the folder.

17. Select the **Next >** button.

Confirm Installation Selections page display.

18. Crosscheck the configuration settings, and then select the **Install** button.

Installation Progress is displays.
After successful installation, installation results are displayed.
19. Select the **Close** button.

Server Manager displays the newly installed Role Services.

![Figure 77](image.png)

20. Restart the server.
Create Certificate Request in Win 2K8 / 2K8 R2

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

   Internet Information Services (IIS) Manager is displayed.

3. Click the server node.
4. Double-click **Server Certificates** icon.
5. In **Actions** pane, click **Create Certificate Request** link.

![Figure 81](image1)

Request Certificate window displays.

![Figure 82](image2)
6. Enter/select appropriate data in the relevant fields.

7. Select the **Next** button.
Leave the default Cryptographic service provider as it is. Increase the Bit length if desired. Higher is more secure but slower.

8. Select the **Next** button.

   File Name page displays.

   ![Figure 85](image)

9. Type name and path of the file or browse the location of the file to save the Certificate Request.
10. Select the **Finish** button.

Open the certreq.txt file in the Notepad.
Get Pending Request Accepted by the Certificate Authority (CA) in Win 2K8 / 2K8 R2

Now you have a pending certificate request, and it needs to be accepted by the CA.

1. Open the Internet explorer.
2. Type `http://server/certsrv` in the Address field.
   Here “server’ is the name of the server you are creating the certificate. Example: elcwin2k8.

   ![Image of Internet Explorer](image)
   
   **Figure 88**

3. Click the Request a certificate hyperlink.
4. Click the **advanced certificate request** hyperlink.
5. Click the **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file** hyperlink.

Submit a Certificate Request or Renewal Request page displays.

![Submit a Certificate Request or Renewal Request](image)

**Figure 91**

6. In the **Saved Request:** box, insert the content of the `certreq.txt` file.

7. In **Certificate Template:** drop-down, select **Web Server**.
8. Click the **Submit >** button.
   Once you click Submit, the certificate is issued to you.

9. Select **Base 64 encoded** option.

10. Click **Download certificate**.
11. Select the Save button.

Save the certificate on your local drive.

![Figure 94](image1)

12. Select the Save button.

![Figure 95](image2)

Install the Certificate in Win 2K8 / 2K8 R2

1. Select the **Start** button, select **Programs**, and then select **Administrative Tools**.
2. Select **Internet Information Services (IIS) Manager**.
3. Select the server node.
4. In **IIS** pane, double-click **Server Certificates** icon. 
   **Server Certificates** page displays.

![Figure 96](image)

5. In **Actions** pane, click **Complete Certificate Request**....
   Complete Certificate Request window displays.
6. Click the **Browse** button and select the server certificate that you received from the CA.
7. Click **Open**.

8. Type any **Friendly name** to keep track of the certificate on this server.
9. Click OK.

If successful, you will see your newly installed certificate in the list.

If you receive an error stating that the request or private key cannot be found, make sure you are using the correct certificate and that you are installing it to the same server that you generated the CSR on. If you are sure of those two things, you may just need to create a new Certificate Request and reissue/replace the certificate.
Bind the Certificate to the Default Web Site in Win 2K8 / 2K8 R2
EventTracker 8.0 and above

1. Expand the server node, expand the Sites node.
2. Select the EventTracker node.
3. In Actions pane, select Bindings....

![Figure 103](image)

Site Bindings window displays.

![Figure 104](image)

4. Select the Add... button.
Add Site Binding window displays.

**Figure 105**

5. In **Type** drop down, select **https**.

**Figure 106**

6. In **SSL certificate**: dropdown, select the certificate that is just installed.

**Figure 107**
7. Click **OK**.

The binding for port 443 is listed.

![Site Bindings](image)

Fig. 108

8. Click **Close**.

The newly added https web site is listed under Browse Web Site pane.

For **EventTracker 8.0 and above**, refer the figure below:

![EventTracker Home](image)

Fig. 111
Test the SSL Enabled Default Web Site in Win 2K8 / 2K8 R2

1. Open the Internet Explorer.
2. Type http://localhost/EventTracker/Login.aspx in the Address field.
   Internet Explorer displays the Security Alert.

   ![Security Alert](image)

   Figure 112

3. Click OK.

   Internet Explorer displays an error page because the self-signed certificate was issued by your machine, not a trusted Certificate Authority (CA). Internet Explorer will trust the certificate if you add it to the list of Trusted Root Certification Authorities in the certificates store on the local machine or in Group Policy for the domain.

   ![Error Page](image)

   Figure 113
4. Click **Continue to this website (not recommended)**.

    Internet Explorer displays the Security Alert.

    ![Security Alert Image]

    **Figure 114**

5. Click **OK**.

    Internet Explorer displays the Login page.

**Configure SSL Settings in Win 2K8 / 2K8 R2**

**For EventTracker 8.0 and above,**

Configure SSL settings if you want your site to require SSL, or to interact in a specific way with client certificates.

1. Expand the **Sites** node, and then select **EventTracker** node.
2. Double-click **SSL Settings**.
3. Select **Require SSL** option and click the **Require** option.
4. In **Actions** pane, select **Apply**.

A successful message displays.