Configure IIS Web Server

Authenticate Clients using Smart Card-v8.3

Publication Date: July 12, 2017
Abstract

The purpose of this document is to help users configure IIS Web Server to authenticate clients using Smart Card. Smart Card can be used for network access, in addition or in alternative to user IDs and passwords, a networked computer equipped with a smart card reader can reliably identify the user.

Audience

EventTracker users who wish to provide additional security and control over user credentials using smart cards.

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
Smart Card.................................................................................................................................................................... 3
Windows 2008 / 2008 R2/ 2012 R2/2016 Server...................................................................................................... 4
  Configure IIS to enable PKI authentication ............................................................................................................ 4
  Steps to setup Smart Card Authentication in IIS once the Web Server has been PKI enabled. ......................... 4
  Enable SSLAlwaysNegoClientCert........................................................................................................................... 8
Apply Smart Card Authenticate Update ..................................................................................................................... 8
Smart Card Settings ..................................................................................................................................................... 8
Execute EventTracker Configuration Utility............................................................................................................. 17
Run updated EventTracker users list....................................................................................................................... 18
Agent Installation Using Smart Card Credentials .................................................................................................... 27
Why to use this update? ........................................................................................................................................... 27
Steps to be followed after applying the Update: ET83U17-001 .................................................................................. 27
**Smart Card**

Interactive logon can be configured to require smart card authentication for greater security.

Smart cards are credit card sized plastic cards that contain integrated circuit chips. Smart cards are used to store user’s certificates and private keys, enabling easy transport of these credentials. Smart cards can perform sophisticated public key cryptography operations, such as digital signing and key exchange.

You can deploy smart cards and smart card readers to provide stronger user authentication and security for a range of security solutions, including logging on over a network, secure Web communication, and secure e-mail.

Smart cards provide tamper-resistant authentication through onboard private key storage and processing. The private key is used in turn to provide other forms of security related to digital signatures and encryption.

**Source:**


**Useful links:**

Windows 2008 / 2008 R2/ 2012 R2/2016 Server

Configure IIS to enable PKI authentication

The steps in this procedure assume that a Secure Sockets Layer (SSL) certificate has already been installed. For more information about adding SSL, please refer to How to – Secure IIS Web Server with SSL.

Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure.

The Web Server will need to be aware of and fully integrated into your Enterprise PKI solution:

- Install Trusted CAs in the Trusted Roots Certificate Stores.
- Configure Certificate Revocation to work with IIS (CRL/OCSP, etc.)

Steps to setup Smart Card Authentication in IIS once the Web Server has been PKI enabled.

   Get the Request signed by a Certificate Authority (CA), most likely you will use your internal Root Certificate Authority (CA) or Intermediate CA.
2. Launch IIS Manager.
For Windows 2012,

- Press **Windows + R** and type “**inetmgr**”.

![Run dialog box](image)

**Figure 2**

- Click **OK**.

3 In IIS, Left Pane select **EventTracker** web site and Double click on **SSL settings** on the Right Pane.

![SSL Settings window](image)

**Figure 3**

**SSL Settings** window displayed.
SSL Settings window displayed.
4 In the SSL Settings section, click Edit.

5 Select the Require Secure Channel (SSL) check box.

6 Select the Require 128-bit encryption check box.

   NOTE:

   In 2008 R2, this option is not available.

7 Under Client Certificates select the Require Client Certificates option.

8 Click Apply in the Action pane.
Enable SSLAlwaysNegoClientCert

Save the following text to a file called "Enable_SSL_Renegotiate.js"

```javascript
var vdirObj=GetObject("IIS://localhost/W3svc/1");
// replace 1 on this line with the number of the web site you wish to configure

WScript.Echo("Value of SSLAlwaysNegoClientCert Before: " + vdirObj.SSLAlwaysNegoClientCert);
vdirObj.Put("SSLAlwaysNegoClientCert", true);
vdirObj.SetInfo();
WScript.Echo("Value of SSLAlwaysNegoClientCert After: " + vdirObj.SSLAlwaysNegoClientCert);
```

Run the following command from an elevated / administrator command prompt:

```
cscript.exe enable_ssl_renegotiate.js
```

Apply Smart Card Authenticate Update

1. Download Smartcard Authentication Update for Appropriate EventTracker version from Update page.
2. Close all EventTracker applications.
3. Apply and run the downloaded update.

Smart Card Settings

To synchronize Smart Card settings with EventTracker, please follow the steps mentioned below.

1) Browse the folder `\InstallDIR\EventTrackerWeb\bin`
2) Double click the **SmartCardSettings.exe** file.

   Smart Card Settings window displays.
EventTracker: Authenticate Clients using Smart Card

Figure 8

3) Enter the **User Domain(s)**: for which the Smart Card is assigned.

   In our example, toons.local.

4) Select and enter appropriate values as described in the table below.

<table>
<thead>
<tr>
<th>Field</th>
<th>Option and description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication Using</strong> - This option is used to know what is embedded in the smart card certificate which can be used for authentication.</td>
<td>Select <strong>Email Address</strong> option.</td>
</tr>
<tr>
<td>Authentication using</td>
<td></td>
</tr>
<tr>
<td>Select, Email Address, UPN, SAMAccountName/Logon Name</td>
<td></td>
</tr>
<tr>
<td>Stored in - Certificate property in which the above mentioned authentication data is stored.</td>
<td>Select <strong>Subject</strong> option.</td>
</tr>
<tr>
<td>Stored in</td>
<td></td>
</tr>
<tr>
<td>Select, Subject, Subject Alternative Name (SAN), Subject</td>
<td></td>
</tr>
</tbody>
</table>
5) If required, enter @ (upn suffix).

NOTE:
The upn suffix is dependent on the entry in Active Directory.

6) Select the Save button.

NOTE:

Authentication Using UPN:

- For DoD customers as per the Common Access Card (CAC) standards, the certificates will have UPN of the user stored in the Subject Alternate Name (SAN) property of the certificate. Hence the smart card settings should be as below.
EventTracker: Authenticate Clients using Smart Card

Figure 9: Sample Certificate

Smart Card Settings for DoD customers is given below. Refer Figure 10.

Figure 10: Smart Settings
When UPN of the user is stored in the **Subject** property of the certificate (as illustrated in the sample certificate – refer Figure 11), the smart card settings should be as in Figure 12.
Authentication Using Email Address:

- For DoD customers as per the Common Access Card (CAC) standards, the certificates will have email address of the user stored in the **Subject** property of the certificate. Hence the smart card settings should be as below.

![Sample Certificate](image)

**Figure 13: Sample Certificate**

- When the email address of the user is stored in the **Subject** property of the certificate (as illustrated in the sample certificate – refer Figure 10), the smart card settings should be as in Figure 14.
Authentication Using Subject Alternative Name:

- For DoD customers as per the Common Access Card (CAC) standards, the certificates will have logon name of the user stored in the **Subject Alternative Name (SAN)** property of the certificate. Hence the smart card settings should be as below.
When the logon name of the user is stored in the **Subject Alternative Name (SAN)** property of the certificate (as illustrated in the sample certificate – refer Figure 15), the smart card settings should be as in Figure 16.
Execute EventTracker Configuration Utility

1) Select the Start button, select Prism Microsystems, and then select EventTracker.

2) Select EventTracker Configuration.

3) Enter the valid user credentials and click the OK button.

4) Login to EventTracker Enterprise.

**NOTE:** Please ensure that EventTracker users accessing via Smart Card should have appropriate non admin user privileges or admin privileges.
Run updated EventTracker users list

This update is required because users listed in Active Directory will be fetched and populated in EventTracker user’s database.

1) Select the Start button, select Prism Microsystems, and then select EventTracker.

2) Select Update Users List.

EventTracker :: Update EventTracker Users list window displays.

3) Select Administrator option for required users and then select the Save button.

NOTE:

- You can assign administrator privilege for users to access EventTracker application after Smart Card Settings are updated.

- In IIS7 and above, when you try to login using the URL, https://server/EventTracker/Login.aspx, logon banner displays. If the user is using the URL https://server/EventTracker/ then logon banner does not display. Hence ‘Login.aspx’ should be enabled in IIS to solve this issue. Please follow the steps given below to configure ‘Login.aspx’ file in IIS.

  a. Login to IIS Manager i.e. click the Start button.
b. In **Search Programs and Files** box, enter ‘inetmgr’ and then press **Enter** key. Internet Information Services (IIS) Manager displays.

c. In **Connections** pane, select local computer, and then select **Sites**.

d. Expand **Site**, and then select **EventTracker** application.

e. In **Features View**, double-click **Default Document**.

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

**Figure 19**

Default Document page displays.
f. In **Actions** pane, click the **Add...** button.

Add Default Document window displays.

g. Enter **Name**: as ‘**Login.aspx**’ and then click the **OK** button.

![Add Default Document](image)

The added document displays in Default Document view.
In IIS6, when you try to login using the URL, https://server/EventTracker/Login.aspx, logon banner displays. If the user is using the URL https://server/EventTracker/ then logon banner does not display. Hence ‘Login.aspx’ should be enabled in IIS to solve this issue. Please follow the steps given below to configure ‘Login.aspx’ file in IIS.

a. Login to IIS Manager i.e. click the Start button.

b. In Search Programs and Files box, enter ‘inetmgr’ and then press Enter key.

Internet Information Services (IIS) Manager displays.

c. In left pane, select Local Computer, select Web Sites, and then select Default Web Site.

d. Right-click EventTracker, and then select Properties.
EventTracker Properties page displays.
EventTracker: Authenticate Clients using Smart Card

Figure 24

e. Select **Documents** tab.

Enable default content page option is enabled by default.
f. Click the **Add**... button.

Add Content Page displays.

g. In **Default content page**: box, enter ‘Login.aspx’ and then click the **OK** button.

Login.aspx page displays as default content page.
h. Click the **Move Up** button.

    Login.aspx page should be the first default content page.
NOTE: After applying the smart card update, if the user tries to login using the smart card authentication and faces any login error, follow the below steps:

- In **Search Programs and Files** box, enter ‘*inetmgr*’ and then press Enter key.

- In left pane, select **Local Computer**, expand **Sites**, expand **EventTracker** site and select **EventTracker** application.

- Go to **Basic Settings** and verify the Application Pool on which EventTracker application is running.

- Close the Basic settings window.

- Now navigate to Application Pool in the left pane. Select the application pool on which EventTracker application is running and change the Managed Pipeline mode to **Classic**.

i. Click **Apply**, and then click the **OK** button.
• Navigate to the root directory, select **ISAPI and CGI Restrictions** click the application pool on which EventTracker application is running and change the Restriction to “**Allowed**”.

Agent Installation Using Smart Card Credentials

Why to use this update?

In the earlier given Smart Card update, it allowed only authentication for EventTracker application. Thus, while installing or deploying agents, the user was required to authenticate using windows credential. To overcome this limitation, a utility has been provided which will now allow the user to deploy agents using their Smart card credentials.

**IMPORTANT**

- The Smart Card user should have proper access rights and permissions on the Remote machine.

- If the Smart card is created for a respective domain and if the user wants to deploy agent in some other domain, he/she should create Domain Trust relationship between the two domains or other multiple domains.

Steps to be followed after applying the Update:
**ET83U17-001**

• Go to the **Install Directory/EventTracker/AdvancedReports** folder.
The following screen gets displayed:
NOTE: Only the windows systems will be listed along with their IP Addresses.

To Install an Agent,

- In the Action field, select Install Agent/Start Poll from the dropdown list.
- Select the Group from the Group Name pane.

All the systems get listed.
• Select the system where you wish to install agent and Change audit.
• Click the checkbox under **Install Agent** and **Install CA** column.

**NOTE:** The change audit column will be displayed only for those users having the license for the same.

• Click **Next**.

---

The Install Option window displays.
NOTE: The Deploy SCAP and Deploy WinSCP options will be available only for licensed version.

- Check the “Install default Remedial Action EXE on this system” option.
- It will display a confirmation message box.
To use custom configuration, click the **Custom configuration** option and select the .ini file.

Select **Yes** and then click the **Install** button.

It will request the user to authenticate using the windows security credential or the Smart card credentials.
• Select Smart Card credentials.

• Enter the smart card credentials and click OK.
The below message gets displayed.

![Request submitted for processing. Check the Installation status screen for updates.](image)

**Figure: 37**

- Click **OK**.
- To view the status of the installation, click the **Installation Status** in the Agent Utility window.

**Figure: 38**

- The Installation Status can be viewed as shown below:

![Installation status](image)

**Figure: 39**

To upgrade an agent,

- In the **Action** field, select **Upgrade** from the dropdown list.
- Select the Group from the **Group Name** pane.

All the systems where agent needs to be upgraded will get listed.

- Select the system and check the options where you wish to upgrade the Agent/Change Audit
- Click **Next**.

![EventTracker: Authenticate Clients using Smart Card](image)

**Figure: 40**

- Check the “**Install default Remedial Action EXE on this system**” option.

It will display a confirmation message box.
• To use custom configuration, click the Custom configuration option and select the .ini file.

• Select Yes and then click the Upgrade button.

It will request the user to authenticate using the windows security credential or the Smart card credentials.

• Select Smart Card credentials.
Enter the smart card credentials and click **OK**.
The below message gets displayed.

![Windows Security dialog box](image)

**Figure: 42**

- Click **OK**.

The Installation Status can be viewed as shown below:
To uninstall an agent,

- In the **Action** field, select **Uninstall agent/Stop poll** from the dropdown list.
- Select the Group from the **Group Name** pane.

All the systems where agent can be uninstalled get listed.

- Select the system and check the options (Agent/Change Audit) which you wish to uninstall.
- Click **Next**.

It will request the user to authenticate using the windows security credential or the Smart card credentials.
EventTracker: Authenticate Clients using Smart Card

- Select Smart Card credentials.

- Enter the smart card credentials and click **OK**.
  The below message gets displayed.

- Click **OK**.
  The Installation Status can be viewed as shown below:
**IMPORTANT NOTE:** If the user gets an error displaying “Copying files to the remote system failed” in the Installation status, as shown in the figure, follow the steps mentioned below:

1. Check the log “Remins.txt” in the Install Directory\EventTracker\RemoteInstaller folder.

2. If the log consists of the **Error:-2146434964**, the user will have to log off the system and log in again with the Smart card credentials and then try deploying the agents.