Configure IIS Web Server
Authenticate Clients using Smart Card
EventTracker: Authenticate Clients using Smart Card

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.
# Table of Contents

Smart Card ............................................................................................................................................. 3

Windows 2003 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
  - Create IIS Certificate Trust List (CTL)................................................................................................. 7

Windows 2008 / 2008 R2 / 2012 R2 Server ........................................................................................ 13
  - Configure IIS to enable PKI authentication ..................................................................................... 13
  - Steps to setup Smart Card Authentication in IIS once the Web Server has been PKI enabled. .... 13
  - Enable SSLAlwaysNegoClientCert ................................................................................................... 18

Apply Smart Card Authenticate Update................................................................................................ 19

Smart Card Settings............................................................................................................................. 19

Execute EventTracker Configuration Utility ........................................................................................ 28

Run updated EventTracker users list.................................................................................................. 29
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 2003 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 [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. In IIS, right-click EventTracker web site and select Properties on the shortcut menu.
3. Click the Directory Security Tab.
4. In the Secure Communications section, click Edit.
5. Select the Require Secure Channel (SSL) check box.
6. Select the Require 128-bit encryption check box.
7. Under Client Certificates select the Require Client Certificates option.
8 Click **OK**.

9 Click **Apply** and then **OK** on the EventTracker Properties window.

10 Right-click **Default Web site** and select **Properties** on the shortcut menu.

11 Click the **Directory Security** Tab.

12 In the **Secure Communications** section, click **Edit**.

13 Select the **Enable certificate trust list** check box and create a new IIS CTL. Trust only the CA's that have Signed the Smart Card certificates that users will be using to authenticate with.
NOTE:

This option is a Web Site setting. You will not see 'Enable certificate trust list' option setting for EventTracker virtual folder.
Create IIS Certificate Trust List (CTL)

1. Click **New** on the Secure Communications window.

2. Click **Next >**.

![Certificate Trust List Wizard](image-url)
3. Click **Add from File**. Locate and select the file.
4. Click **Open**.
5 Click **Next >**.
6 Type a friendly name and description in the **Friendly name** and **Description** fields respectively.

7 Click **Next >**.
8 Click Finish.

9 Click OK.

10 Click OK on the Secure Communications window.

11 Click Apply and then OK on the Default web site properties window. Close the IIS Manager.
Windows 2008 / 2008 R2/ 2012 R2 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 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**’.

- Click **OK**.

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

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

![Folder View](image)
2) Double click the **SmartCardSettings.exe** file.

   Smart Card Settings window displays.

![Smart Card Settings](image)

**Figure 17**

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>Authentication Using -</td>
<td>Select Email Address option.</td>
</tr>
<tr>
<td>[Select]</td>
<td>Select User Principal Name option.</td>
</tr>
<tr>
<td>[Select]</td>
<td>Select SAMAccountName/Logon name option.</td>
</tr>
<tr>
<td>Authentication using:</td>
<td>Selected options are shown in the table.</td>
</tr>
<tr>
<td>Stored in</td>
<td>Select Subject option.</td>
</tr>
<tr>
<td></td>
<td>Select Subject Alternative Name (SAN) option.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Extract with

Select / enter correct **Delimiter** and specify the **Ordinal Position**:

![Delimiter and Ordinal Position](image)

**RegEx** – Enter an appropriate **Regular Expression** to extract the values stored in Smart Card license details.

![Regular Expression](image)

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.

![Sample Certificate](image)

Figure 18: Sample Certificate

Smart Card Settings for DoD customers is given below. Refer Figure 19.
When UPN of the user is stored in the **Subject** property of the certificate (as illustrated in the sample certificate – refer Figure 20), the smart card settings should be as in Figure 21.
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.
When the email address of the user is stored in the **Subject** property of the certificate (as illustrated in the sample certificate – refer Figure 19), the smart card settings should be as in Figure 23.
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.
EventTracker: Authenticate Clients using Smart Card

Figure 24: Sample Certificate

- 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 24), the smart card settings should be as in Figure 25.

Figure 25: Smart Card Settings
Execute EventTracker Configuration Utility

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

2) Select **EventTracker Configuration**.

![EventTracker Configuration Utility](image)

Figure 26

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](https://server/EventTracker/Login.aspx), logon banner displays. If the user is using the URL [https://server/EventTracker/](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.
EventTracker: Authenticate Clients using Smart Card

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)

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: Authenticate Clients using Smart Card

EventTracker Properties page displays.

Figure 32
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.
i. Click **Apply**, and then click the **OK** button.

**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**’. 