Integrating Terminal Services Gateway

EventTracker Enterprise
Abstract

The purpose of this document is to help user in monitoring Microsoft Windows Terminal Services Gateway by deploying Windows Agent.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 7.x and later, and Microsoft Windows Server 2008 and later.

Intended audience

Administrators who are assigned the task to monitor and manage Microsoft Windows Terminal Services 2008 and later events using EventTracker.
## Table of Contents

Abstract.................................................................................................................................................. 1  
Scope.................................................................................................................................................. 1  
Intended audience ............................................................................................................................. 1  
Pre-requisite.......................................................................................................................................... 3  
EventTracker Agent configuration ........................................................................................................ 3  
EventTracker Knowledge Pack (KP)....................................................................................................... 7  
  Categories .......................................................................................................................................... 7  
  Reports............................................................................................................................................... 7  
  Alerts.................................................................................................................................................. 8  
  Dashboards........................................................................................................................................ 9  
Import knowledge pack into EventTracker ........................................................................................... 9  
  To import Alerts ............................................................................................................................... 10  
  To import Category .......................................................................................................................... 11  
  To import Tokens ............................................................................................................................. 12  
  To import Flex Reports .................................................................................................................... 13  
  To Configure Flex Dashboard ........................................................................................................... 14  
Verify knowledge pack in EventTracker .............................................................................................. 18  
  Verify Alerts ..................................................................................................................................... 18  
  Verify Categories ............................................................................................................................ 20  
  Verify Tokens ................................................................................................................................... 20  
  Verify Flex Reports .......................................................................................................................... 21  
Sample Reports ................................................................................................................................... 22  
Sample Dashboards............................................................................................................................. 23
Overview

Windows Server® 2008 Terminal Services Gateway (TS Gateway) is a role service that enables authorized remote users to connect to resources on an internal corporate or private network, from any Internet-connected device that can run the Remote Desktop Connection (RDC) client. The network resources can be terminal servers, terminal servers running RemoteApp™ programs, or computers with Remote Desktop enabled.

TS Gateway encapsulates Remote Desktop Protocol (RDP) within RPC, within HTTP over a Secure Sockets Layer (SSL) connection. In this way, TS Gateway helps improve security by establishing an encrypted connection between remote users on the Internet and the internal network resources on which their productivity applications run.

Pre-requisite

Prior to configuring Windows Server 2008 and later and EventTracker 7.x and later, ensure that you meet the following prerequisites:

- Administrative access on EventTracker.
- User should have Administrative rights on Microsoft Windows Terminal Server.

EventTracker Agent configuration

1. Deploy EventTracker Agent in Terminal Services Server, please follow the steps mentioned in How to Install EventTracker and Change Audit.

2. Select the Start > All Programs > Prism Microsystems > EventTracker.

3. In EventTracker Control Panel, double-click EventTracker Agent Configuration.

4. Select Event Filters tab, and then click the Filter Exception button.
Filter Exception window displays.

5. Click the **New** button.
Event Details window displays.

7. Click the **OK** button.
8. **Save** the configuration and **Close** the EventTracker Agent Configuration window.
EventTracker Knowledge Pack (KP)

Once logs are received into EventTracker, Categories and reports can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support Terminal Services Server.

Categories

- **Terminal Services: Connection Broker** - This category based report provides information related to terminal services communication, terminal services farm membership, terminal services session broker configuration, terminal services session broker security group configuration and terminal services session broker server availability.

- **Terminal Services: Desktop Session Host** – This category based report provides information related to remote desktop services availability, remote desktop services client access license availability, remote desktop session host connections, remote desktop session host listener availability, remote desktop session host user configuration and roaming user profile cache availability.

- **Terminal Services: Gateway** - This category based report provides information related to terminal services gateway server availability, terminal services gateway server configuration and terminal services gateway server connections.

- **Terminal Services: Web Access** – This category based report provides information related to terminal services web access configuration.

- **Terminal Services: Licensing** – This category based report provides information related to terminal services client access license availability, terminal services license server activation, terminal services license server database availability, terminal services license server discovery, terminal services license server security group configuration and terminal services per user client access license tracking and reporting.

Reports

- **Terminal Services Gateway-Server configuration failure** - This report provides information related to terminal services gateway server configuration failure details.

- **Terminal Services Gateway- Server configuration success**: This report provides information related to terminal services gateway server configuration success details.
• **Terminal Services Gateway-Server connections failure** - This report provides information related to terminal services gateway server connections failure activity.

• **Terminal Services Gateway-Server connections success** - This report provides information related to terminal services gateway server connections success activity.

• **Terminal Services- Web Access Configuration** - This report provides information related to terminal services web access configuration details.

• **Terminal Services-Desktop session host activity** – This report provides information related to terminal services desktop session host details.

• **Terminal Services-Load balancing** – This report provides information related to terminal services load balancing details.

• **Terminal Services-IP virtualization** – This report provides information related to terminal services ip virtualization details.

• **Terminal Services-Connection and session manager activity** – This report provides information related to terminal services remote and local session manager details.

• **Terminal Services-Session activity**– This report provides information related to session logon and logoff succeeded, session connection and session reconnection details.

• **Terminal Services-User activity**- This report provides information related to user authentication success details.

### Alerts

• **Terminal Services: Desktop session host** - This alert is generated when remote desktop services start failed.

• **Terminal Service: Gateway services** - This alert is generated when terminal service gateway is shutting down.

• **Terminal Services: Licensing** – This alert is generated when terminal services license server cannot issue a terminal services client access license to the client.

• **Terminal Services: User configuration**– This alert is generated when terminal server profile path failed to load and client exceeded the maximum allowed failed logon attempts.
Dashboards

- **Terminal Services: User authentication succeeded** – This dashboard gives us the information about users who authentication is success.

- **Terminal Services: Logon succeeded** – This dashboard gives us the information about connected sessions.

Import knowledge pack into EventTracker

1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**. Click **Import** tab.

![EventTracker Control Panel](image.png)

E-mail: support@EventTracker.com

---

EventTracker: Integrating Terminal Services Gateway
To import Alerts

1. Click Alerts option, and then click the browse button.

2. Locate Terminal Services .isalt file, and then click the Open button.

3. To import alerts, click the Import button.

   EventTracker displays success message.
4. Click **OK**, and then click the **Close** button.

To import Category

1. Click **Category** option, and then click the browse button.

2. Locate Terminal Services `.iscat` file, and then click the **Open** button.
3. To import categories, click the **Import** button.

   EventTracker displays success message.

   ![Figure 9](image)

4. Click **OK**, and then click the **Close** button.

**To import Tokens**

1. Click **Token value** option, and then click the browse button.

   ![Figure 10](image)

2. Locate the Terminal Services.istoken file, and then click the **Open** button.
3. To import tokens, click the **Import** button.

EventTracker displays success message.

![Figure 11](image1.png)

4. Click **OK**, and then click the **Close** button.

To import Flex Reports

1. Click **Reports** option, and then click the browse button.

![Figure 12](image2.png)
2. Locate the Terminal Services.issch file, and then click the Open button.

3. Click the Import button to import the scheduled reports.

   EventTracker displays success message.

   ![Figure 13](image)

4. Click the OK button. Click the Close button.

### To Configure Flex Dashboard

1. Scheduled flex reports (Microsoft DNS: Name resolution successfully) after importing them.
2. During scheduling, please check persist data and select all the columns to persist.

![Figure 14](image)
3. Now, wait for the report to run as per schedule time or run it manually.
4. After generating report, click on Dashboard > Flex.
5. Click on Add Dashboard button and fill Title and Description box and save it.
6. Now, create Dashlet for Microsoft DNS (Top URL usage) by clicking on Configure flex dashlet.

7. Fill WIDGET TITLE (Top URL usage), select DATA SOURCE (Microsoft DNS-Name resolution successfully), select CHART TYPE and select AXIS LABELS [X-AXIS].

![Widget Configuration](image)

Figure 17

8. After selecting and filling all options, click on the TEST button to check the Dashlet. If data are coming properly, then click on CONFIGURE button.
9. After creation of Dashlet for Terminal Services Logon Activity, click on Customize flex dashlet.

10. Select Terminal Services Logon Activity: Top URL usage dashlet and click on ADD button.

11. Now, you can see the Dashlet on Dashboard.
Verify knowledge pack in EventTracker
Verify Alerts

1. Logon to EventTracker Enterprise.
2. Click Admin dropdown, and then click Alert
3. In Search field, type 'Terminal Services', and then click the Go button.
   
   Alert Management page will display all the imported Terminal Services alerts.
4. To activate the imported alerts, select the respective checkbox in the **Active** column.

EventTracker displays message box.

![Message from webpage]

Figure 21

5. Click **OK**, and then click the **Activate Now** button.

**NOTE:**

You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.
Verify Categories

1. Logon to EventTracker Enterprise.
2. Click Admin dropdown, and then click Categories.
3. In Category Tree to view imported categories, scroll down and expand Terminal Services Server group folder to view the imported categories.

Verify Tokens

1. Logon to EventTracker Enterprise.
2. Click the Admin dropdown, and then click Parsing rule.
Verify Flex Reports

1. Logon to EventTracker Enterprise.
2. Click the Reports.
3. Select the Configuration.
4. In the Reports Configuration, select Defined from radio button. EventTracker displays Defined page.
5. In search box enter ‘Terminal Services”. EventTracker displays flex reports of Terminal Services.
Sample Reports

1) Terminal Services: Logon Activity

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>User</th>
<th>Session ID</th>
<th>Source</th>
<th>Network Address</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/24/2015 12:03:54 PM</td>
<td>TS</td>
<td>ALBEVARL\Elmasw</td>
<td>1</td>
<td>LOCAL</td>
<td>10.200.3.36</td>
<td>Session login succeeded</td>
</tr>
<tr>
<td>12/24/2015 12:03:54 PM</td>
<td>TS</td>
<td>ALBEVARL\Ezmedadmin</td>
<td>1</td>
<td>LOCAL</td>
<td>10.200.3.36</td>
<td>Session login succeeded</td>
</tr>
<tr>
<td>12/24/2015 12:03:54 PM</td>
<td>TS</td>
<td>ALBEVARL\Ezmed</td>
<td>1</td>
<td>LOCAL</td>
<td>10.200.3.36</td>
<td>Session login succeeded</td>
</tr>
<tr>
<td>12/24/2015 12:03:54 PM</td>
<td>TS</td>
<td>ALBEVARL\Ezmedadmin</td>
<td>1</td>
<td>LOCAL</td>
<td>10.200.3.36</td>
<td>Session login succeeded</td>
</tr>
<tr>
<td>12/24/2015 12:03:54 PM</td>
<td>TS</td>
<td>ALBEVARL\Elmasw</td>
<td>1</td>
<td>LOCAL</td>
<td>10.200.3.36</td>
<td>Session login succeeded</td>
</tr>
<tr>
<td>12/24/2015 12:03:54 PM</td>
<td>TS</td>
<td>ALBEVARL\Ezmedadmin</td>
<td>1</td>
<td>LOCAL</td>
<td>10.200.3.36</td>
<td>Session login succeeded</td>
</tr>
<tr>
<td>12/24/2015 12:03:54 PM</td>
<td>TS</td>
<td>ALBEVARL\Elmasw</td>
<td>1</td>
<td>LOCAL</td>
<td>10.200.3.36</td>
<td>Session login succeeded</td>
</tr>
<tr>
<td>12/24/2015 12:03:54 PM</td>
<td>TS</td>
<td>ALBEVARL\Ezmedadmin</td>
<td>1</td>
<td>LOCAL</td>
<td>10.200.3.36</td>
<td>Session login succeeded</td>
</tr>
<tr>
<td>12/24/2015 12:03:54 PM</td>
<td>TS</td>
<td>ALBEVARL\Elmasw</td>
<td>1</td>
<td>LOCAL</td>
<td>10.200.3.36</td>
<td>Session login succeeded</td>
</tr>
<tr>
<td>12/24/2015 12:03:54 PM</td>
<td>TS</td>
<td>ALBEVARL\Ezmedadmin</td>
<td>1</td>
<td>LOCAL</td>
<td>10.200.3.36</td>
<td>Session login succeeded</td>
</tr>
</tbody>
</table>
2) Terminal Services: User Activity

![Terminal Services-User activity](image)

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>UserName</th>
<th>Domain Name</th>
<th>Source Network Address</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/24/2015 12:42:45 PM</td>
<td>TS</td>
<td>Deepu</td>
<td>ALBEMARLE</td>
<td>10.200.3.40</td>
<td>User authentication succeeded</td>
</tr>
<tr>
<td>12/24/2015 12:42:55 PM</td>
<td>TS</td>
<td>Anni</td>
<td>ALBEMARLE</td>
<td>10.200.3.41</td>
<td>User authentication succeeded</td>
</tr>
<tr>
<td>12/24/2015 12:43:05 PM</td>
<td>TS</td>
<td>Sophie</td>
<td>ALBEMARLE</td>
<td>10.200.3.38</td>
<td>User authentication succeeded</td>
</tr>
</tbody>
</table>

Figure 27

Sample Dashboards

1. Terminal Services Logon Activity

![Terminal Services Logon Activity](image)

Figure 28