

Terminal Services Gateway

EventTracker v9.2 and above

Abstract

The purpose of this document is to help users to monitor Microsoft Windows **Terminal Services Gateway** by deploying Windows Agent.

Scope

The configuration details in this guide are consistent with **EventTracker** version 9.2 and later, **Terminal Services Gateway**.

Audience

Administrators who want to monitor the **Terminal Services Gateway** using **EventTracker**.

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

This document is for informational purposes only. Netsurion 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 Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion 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 Netsurion, 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.

© 2020 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

- 1. Introduction..... 3
- 2. Pre-requisite 3
- 3. EventTracker Agent configuration 3

1. Introduction

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.

EventTracker gathers and examines acquired logs to identify terminal server configurations, terminal server connections, terminal server desktop host activity. It generates reports for terminal services user session connected, user session disconnected, user authentication success, user authentication failed, and network traffic activity. It displays authentication success and failed with username's, user session connected, and network traffic by systems. It alerts the users when terminal services gateway is shutting down and user authentication fails.

2. Pre-requisite

Prior to configuring Windows Server 2008 and later and EventTracker 9.2 and later, ensure that you meet the following prerequisites.

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

3. 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. Click **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.

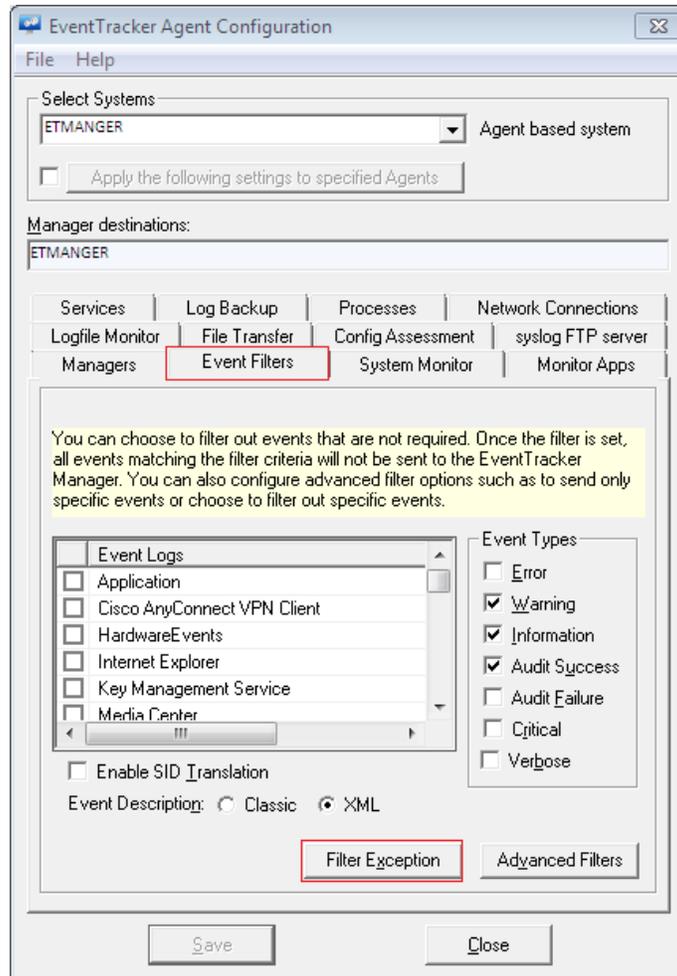


Figure 1

5. Filter Exception window displays. Click **New**.

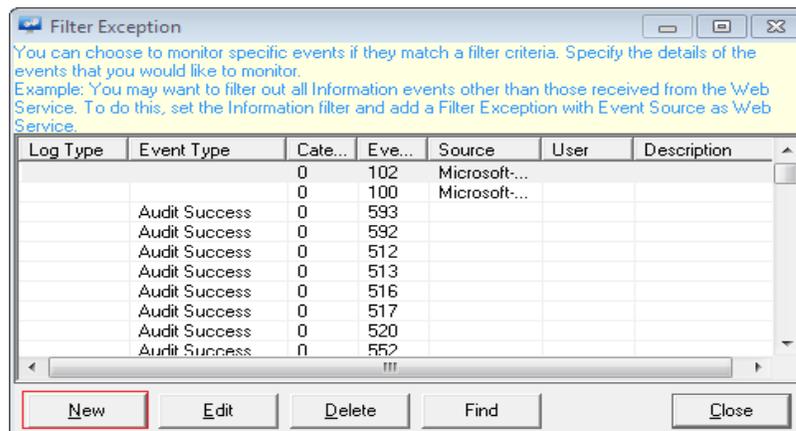
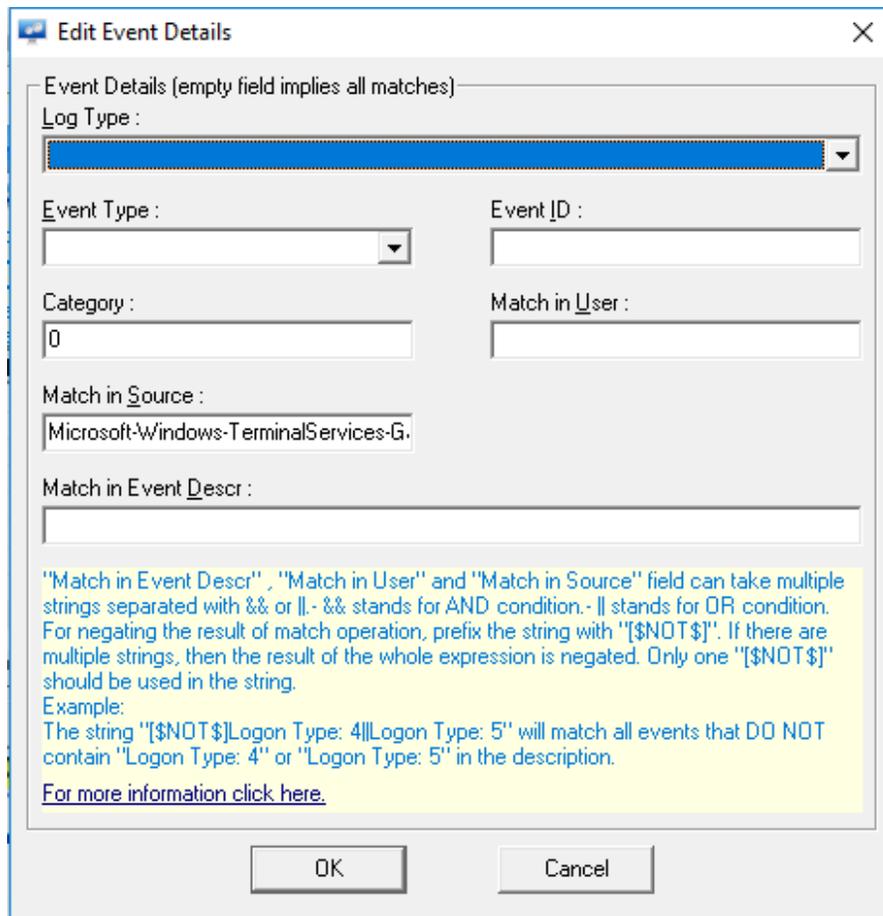


Figure 2

6. Event Details window opens. In **Match in Source** box enter 'Microsoft-Windows-TerminalServices-Gateway'.



Event Details (empty field implies all matches)

Log Type :

Event Type : Event ID :

Category : Match in User :

Match in Source :

Match in Event Descr :

"Match in Event Descr", "Match in User" and "Match in Source" field can take multiple strings separated with && or ||. && stands for AND condition. || stands for OR condition. For negating the result of match operation, prefix the string with "[NOT\$]". If there are multiple strings, then the result of the whole expression is negated. Only one "[NOT\$]" should be used in the string.

Example:
The string "[NOT\$]Logon Type: 4||Logon Type: 5" will match all events that DO NOT contain "Logon Type: 4" or "Logon Type: 5" in the description.

[For more information click here.](#)

OK Cancel

Figure 3

7. Click **OK**.
8. **Save** the configuration and **Close** the EventTracker Agent Configuration window.

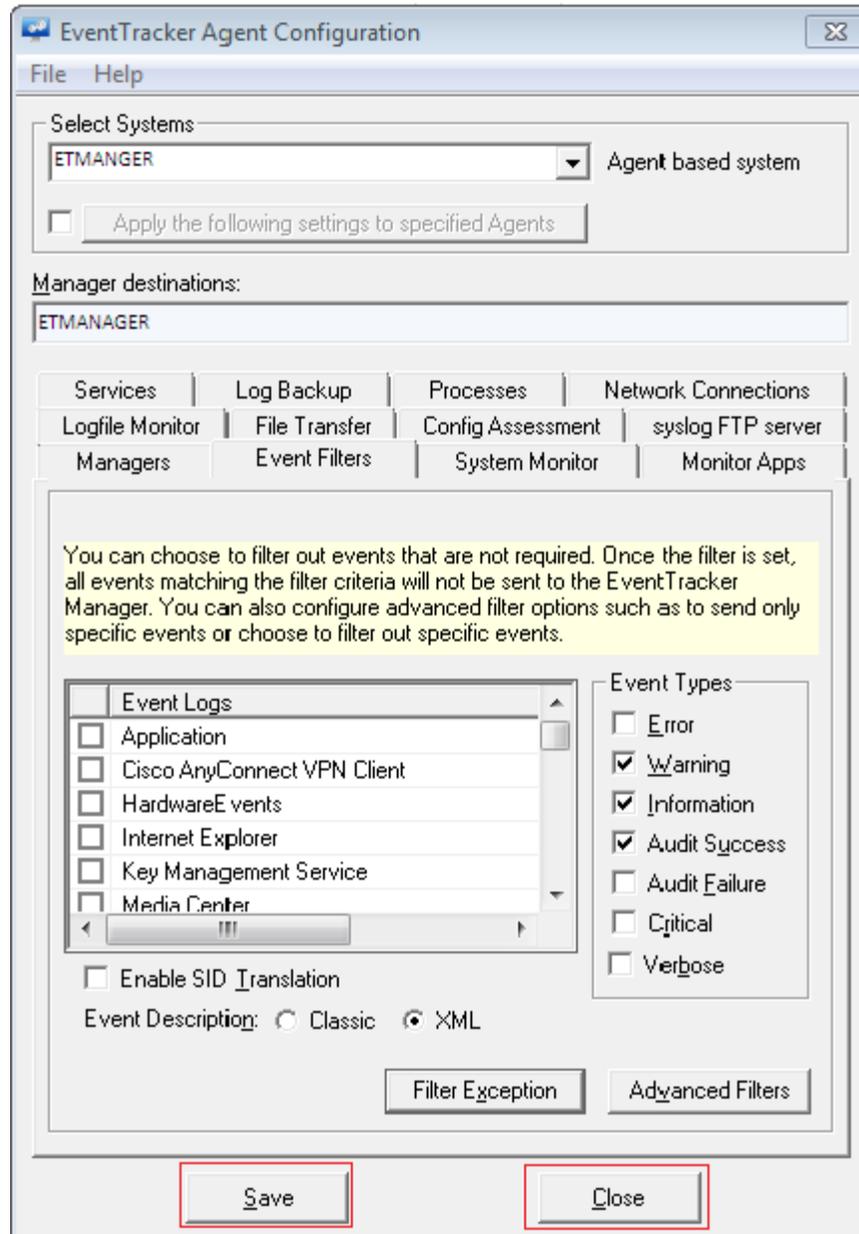


Figure 4