Netsurion | EventTracker®

Terminal Services Gateway

EventTracker v9.2 and above

Publication Date: July 2, 2020

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**.

Table of Contents

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.

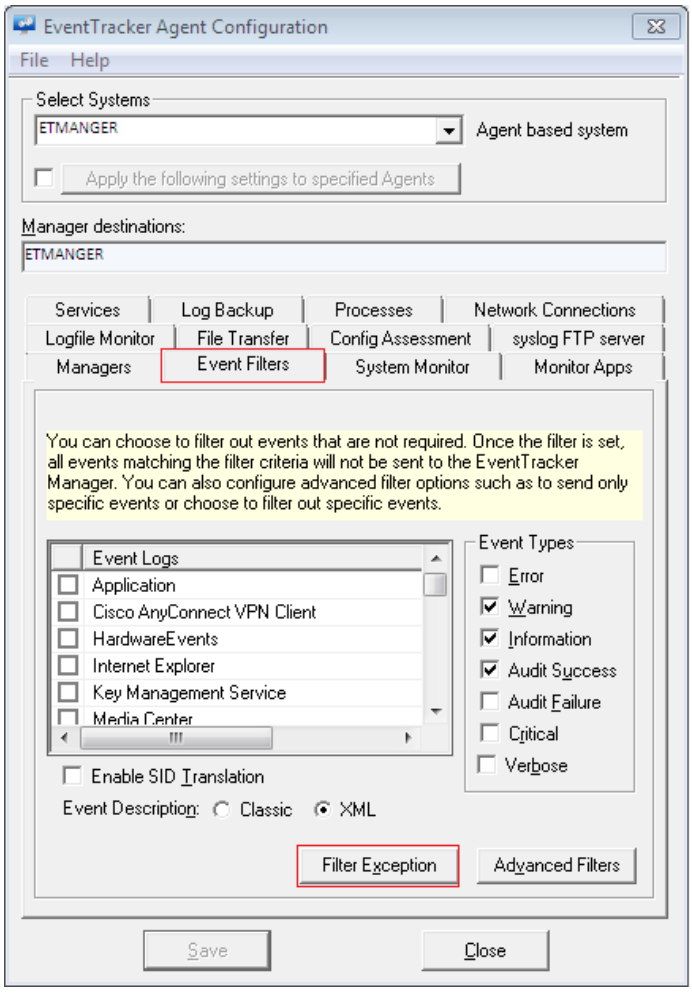

Figure 1

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

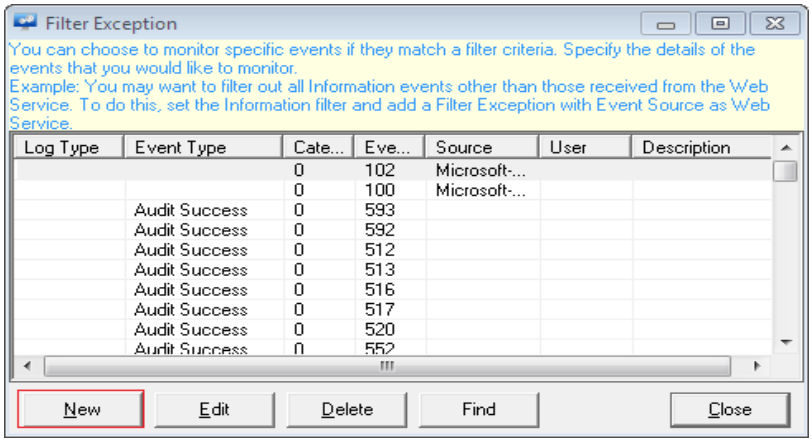

Figure 2

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

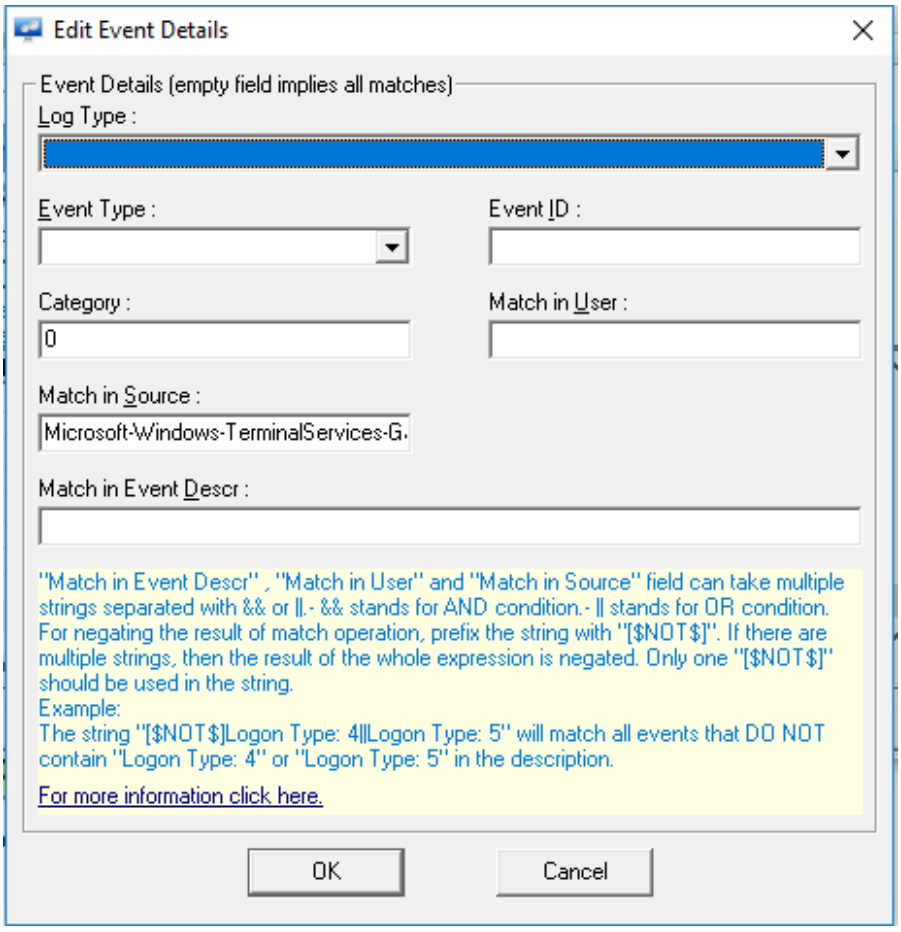

Figure 3

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

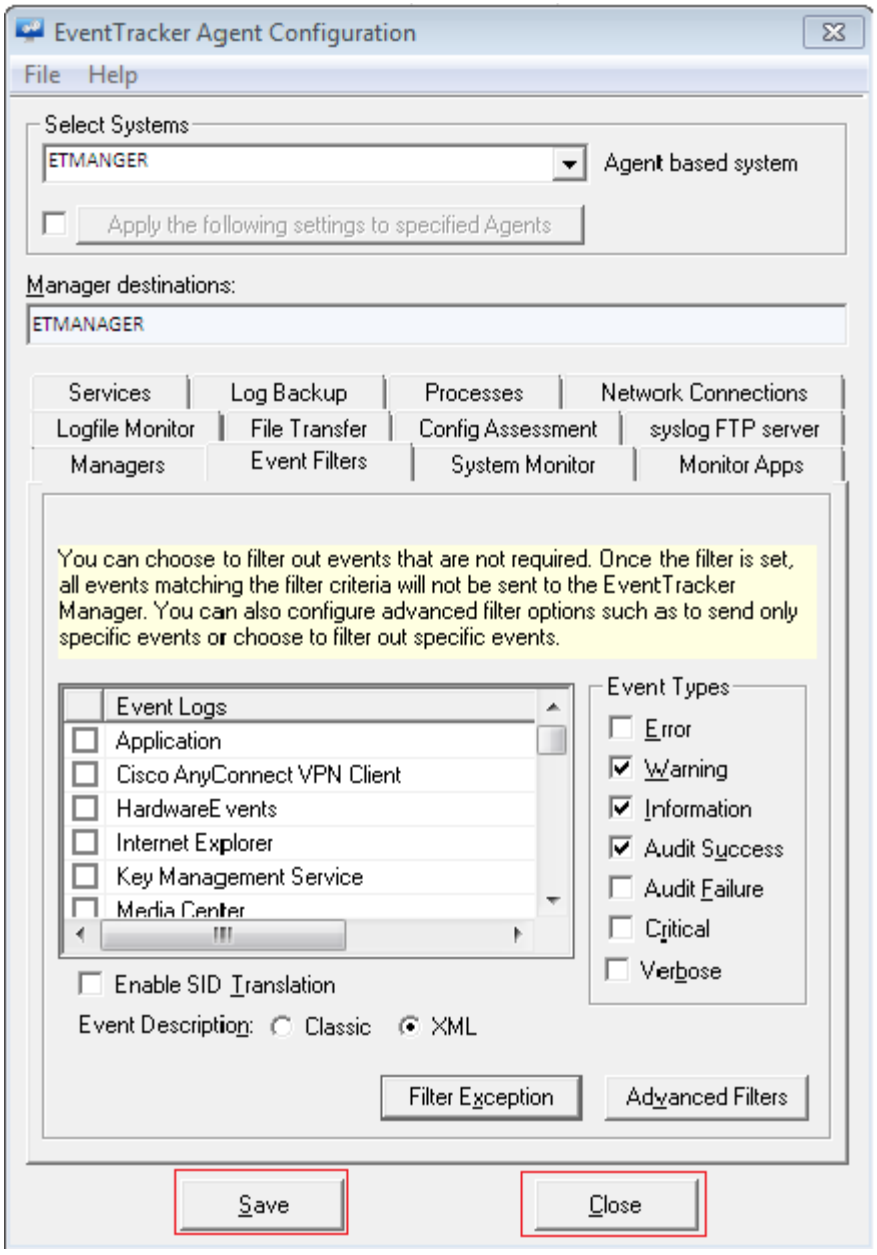
EventTracker Agent Configuration
File Help
Select Systems
ETMANGER
Agent based system
Apply the following settings to specified Agents
Manager destinations:
ETMANAGER
Services
Log Backup
Processes
Network Connections
Logfile Monitor
File Transfer
Config Assessment
syslog FTP server
Managers
Event Filters
System Monitor
Monitor Apps
You can choose to filter out events that are not required. Once the filter is set, all events matching the filter criteria will not be sent to the EventTracker Manager. You can also configure advanced filter options such as to send only specific events or choose to filter out specific events.
Event Logs
Application
Cisco AnyConnect VPN Client
HardwareEvents
Internet Explorer
Key Management Service
Media Center
Event Types
Error
Warning
Information
Audit Success
Audit Failure
Critical
Verbose
Enable SID Translation
Event Description: Classic XML
Filter Exception
Advanced Filters
Save
Close

Figure 4