EventTracker
Secure. Comply. Succeed.

Agent Direct Log Archiver Configuration Guide

EventTracker
Version 7.x

Publication Date: Sept 10, 2010

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

ABSTRACT

The purpose of this document is to help administrators understand Agent Direct Log Archiver (DLA) and verify all its expected functionality. This document holds good for all versions of EventTracker v7.x versions.

TARGET AUDIENCE

EventTracker administrators who wish to configure Agent DLA.

Table of Contents

Agent DLA

- **What is Agent DLA?**

  Agent DLA is an offline method of archiving events directly into EventTracker data repository.

- **Why is it useful?**

  Transferring events of low priority in real-time impacts the EventTracker Receiver's performance there-by causing high memory/CPU usages, network bandwidth consumption, unnecessary Alerts processing etc.

  Though trivial in significance, those events might contain valuable information, which the administrator might be interested to investigate in later point of time. A work around solution is Agent DLA. As the name suggests, involved parties are remote Agent and Manager side Agent that conduct file transfer business through TCP port 14506.

  Additionally, Agent DLA can also be utilized to transfer other files (backed up log files, .evt, etc). One Agent DLA instance can be configured to transfer files to maximum 5 Manager destinations.

- **How it works?**

  Configure EventTracker Agent to collect and cache events locally, thus reducing the workload of

  EventTracker Receiver, compress to cautiously and frugally use the network bandwidth, encrypt to tamper proof data, and finally transfer to the EventTracker Manager at scheduled intervals, thus automating the entire process.

- **Pros and Cons**

  Advantages prevail over disadvantages. Agent DLA offers multifaceted advantages that include,

  - Dramatic improvement in EventTracker Receiver performance by downsizing the workload
  - Judicious utilization of vital system resources on the EventTracker Manager system
  - Frugal consumption network bandwidth by transmitting compressed, tamper-proof files of negligible size
  - Automated file transfer

  Real-time events may not be available for analysis since file transfer is done offline.

Filter Events

This option helps you to set Agent side filters to filter low priority or insignificant events that being sent to the Manager(s).

1. Double-click **EventTracker Agent Configuration** on the desktop Control Panel.
2. Select the system from the **Select Systems** drop-down list.
3. Click the **Event Filters** tab.

   EventTracker displays the Event Filters tab.

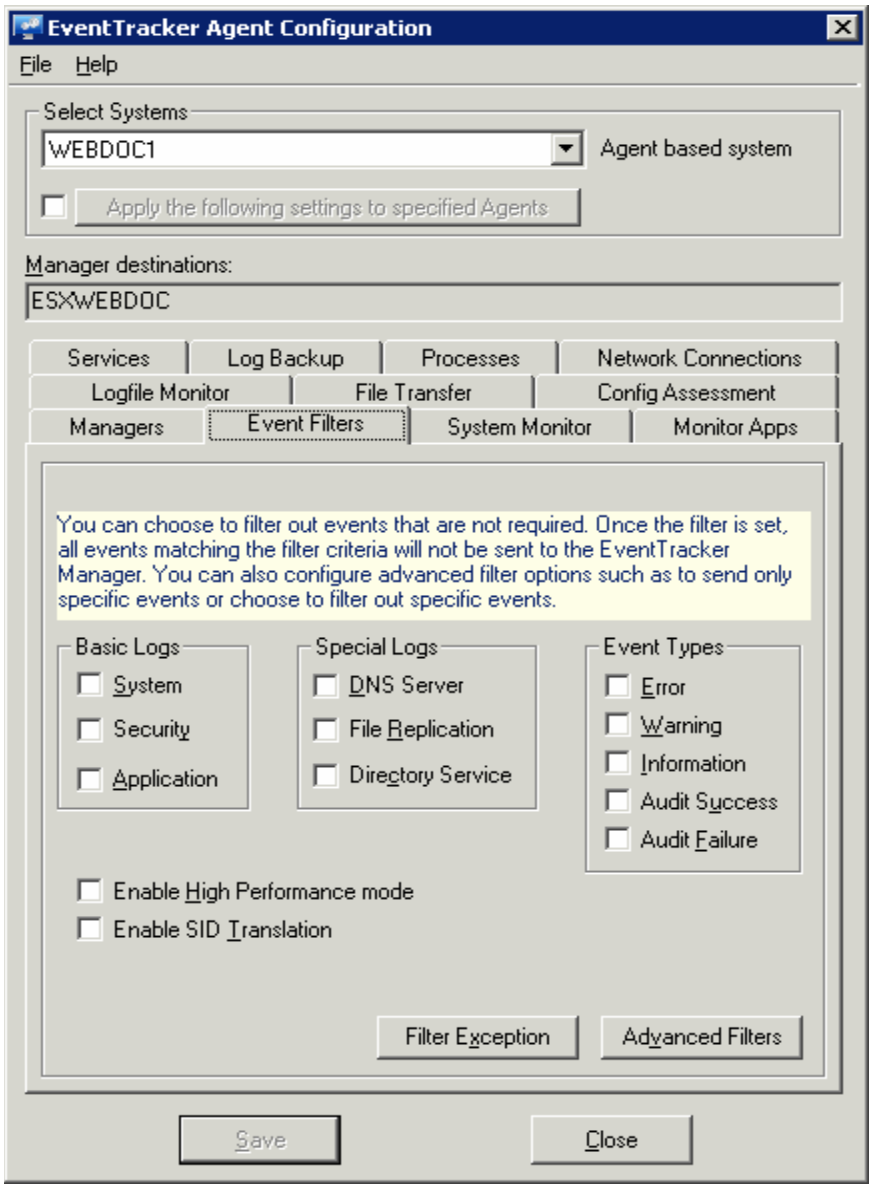


Figure 1

Field	Description
Select Systems	Select a system from the drop-down list for which you want to filter events.
Basic Logs	
System	System log contains events logged by Windows system components. For example, if a driver fails to load during startup, an event is recorded in the system log. Windows predetermines the events that are logged by system components. Availability: All Windows systems
Security	Security log records events such as valid and invalid logon attempts, as well as events related to resource use, such as the creating, opening, or deleting of files. For example, when logon auditing is enabled, an event is recorded in the security log each time a user attempts to log on to the computer. You must be logged on as Administrator or as a member of the Administrators group in order to turn on, use, and specify which events are recorded in the security log. Availability: All Windows systems
Application	Application log contains events logged by programs. For example, a database program may record a file error in the application log. Events that are written to the application log are determined by the developers of the software program. Availability: All Windows systems
Special logs	
DNS Server	DNS server log contains events logged by DNS servers. Availability: DNS servers only
File Replication	File Replication Service log contains domain controller replication events. Availability: Domain Controllers only.
Directory Service	Directory Service log contains Active Directory events. Availability: Domain Controllers only.
Event Types	
Error	A significant problem, such as loss of data or loss of functionality. For example, if a service fails to load during startup, an Error will be logged.
Warning	An event that is not necessarily significant, but may indicate a possible future problem. For example, when disk space is low, a Warning will be logged.

Information	In event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, an Information event will be logged.
Audit Success	An audited security access attempt that succeeds. For example, a user's successful attempt to log on the system will be logged as a Success Audit event.
Audit Failure	An audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt will be logged as a Failure Audit event.
Filter Exception	When you set Filter Exceptions, EventTracker Agent filters all events that matches the filter criteria and forwards only the event(s) that is added to the exception list.
Advanced Filters	When you set Advanced Filters, EventTracker Agent forwards all events that matches the filter criteria to the Manager and filters event(s) that is added to the Advanced Filters list.

4. Select appropriately, for example, Event Types -> Information

   EventTracker displays the Event Filters tab with the newly added filter.

   NOTE:

   The filters are now set and all events of Information Event Type will be filtered out and will not be sent to the EventTracker Manager.

5. Click **Save**, and then click **Close**.

Send Filtered Windows Events to Manager

This option enables you to transfer filtered Windows events at scheduled intervals to the Manager. Windows events that are filtered out by the real time settings are cached for transfer (further filtering is available). This minimizes the EventTracker Receiver service workload and conserves the network bandwidth.

Configure and Associate VCP Port

This option helps you associate VCP port with Agent File Transfer.

1. Log on to EventTracker.
2. Click the **Admin** drop-down list at the upper-right corner.
3. Click the **Manager** hyperlink.

   EventTracker displays the Manager Configuration page.
4. Click the **Syslog / Virtual Collection Point** tab.
5. Click **Add** under Virtual Collection Points and add a VCP port, for example 14515.
6. Click **Save**.
7. Click the **Direct Log Archiver / Netflow Receiver** tab.
8. Select the **Direct log file archiving from external sources** check box.
9. Select a port from the **Associated virtual collection point** drop-down list, for example 14515.
10. Click **Save** on the Manager Configuration page.
11. Click the **Agent Settings** tab.

    Associated virtual collection point is the port that you have configured for Direct Log Archiver.

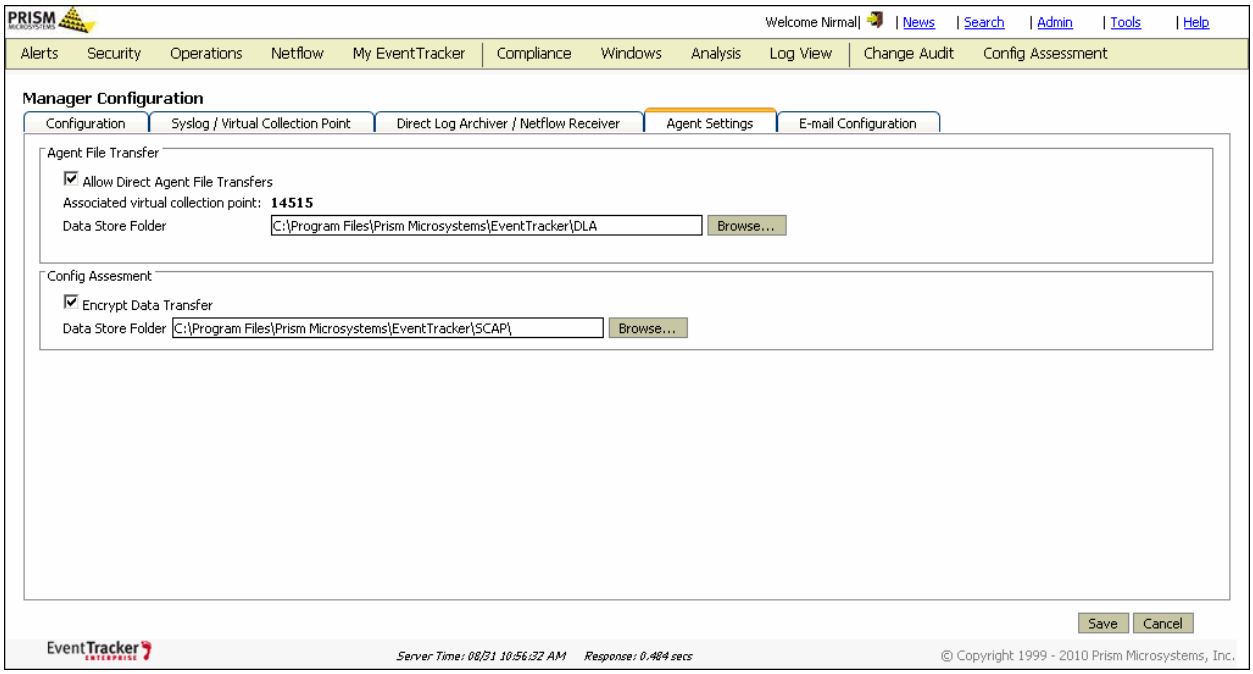


Figure 2

12. Click **Save** on the Manager Configuration page.

Configure EventTracker Windows Agent

This option helps you configure Agent to transfer Windows filtered events and other log files.

1. Open the Agent Configuration window.
2. Select the system from the **Select Systems** drop-down list.
3. Click the **File Transfer** tab.

   EventTracker displays the File Transfer tab.

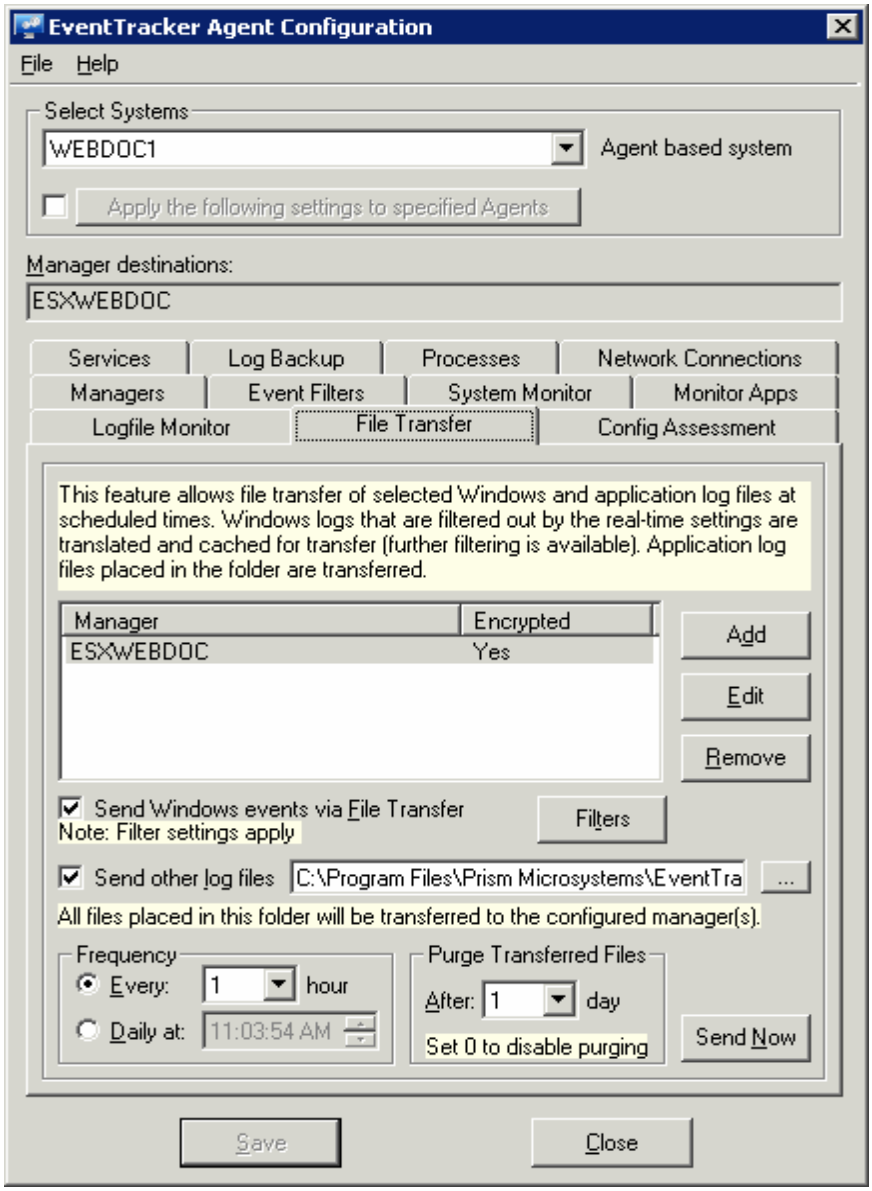
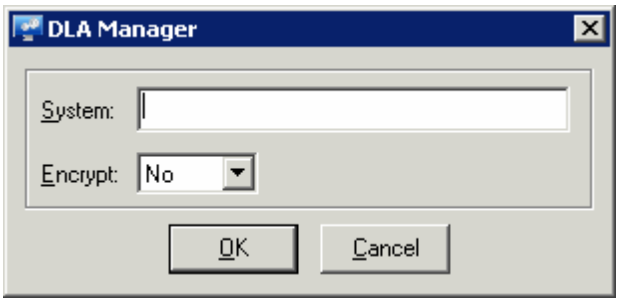
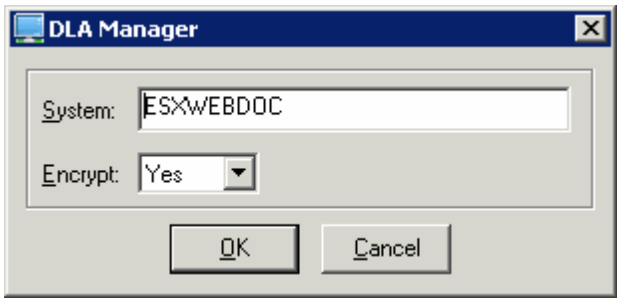
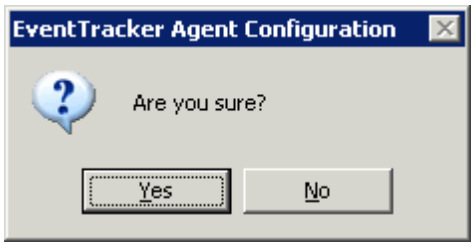


Figure 3

Field	Description
Add	Add destination (EventTracker Manager)  Type the name of the Manager in the **System** field. Select an option from the **Encrypt** drop-down list to encrypt and securely transfer the cached events to the destination. Click **OK**.
Edit	Edit destination. 
Remove	Delete destination. EventTracker displays the confirmation message box. 

Field	Description
Send Windows Events via File Transfer	Select this check box to transfer cached events to the EventTracker Manager (s).
Send other log files	Select this option to transfer application log files and other files.
Frequency	Set the frequency to automate file transfer.
Purge Transferred Files After	Set this option to purge files that are transferred to the Manager after the specified amount of time is elapsed. Setting '0' retains all files.
Send Now	Click this button to override the automated file transfer frequency set and transfer files on demand.

Configure DLA Filters

In the 'Filtering Events' section we have seen how to filter events of Information Event Type. When you enable Agent-DLA all events are cached and transferred to the Manager. But you may not be interested in all events and wish to filter certain events that are insignificant to you. This section explains how to filter cached events.

1. Click **Filters**.

   EventTracker displays the DLA Filters console.

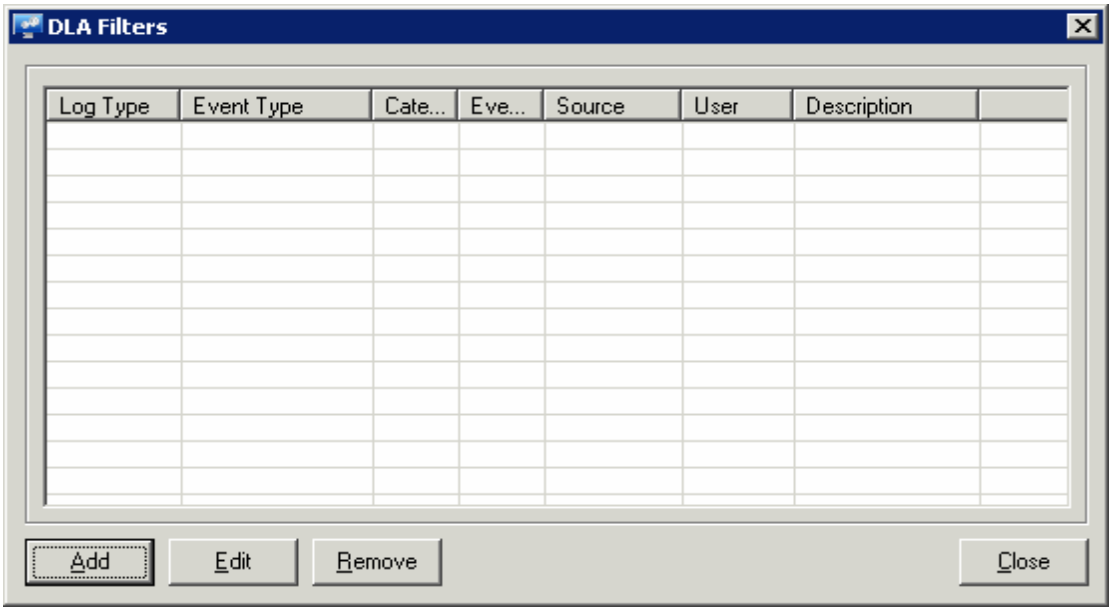


Figure 4

2. Click **Add**.

   EventTracker displays the Event Details window.

3. Enter/select appropriately in the relevant fields.

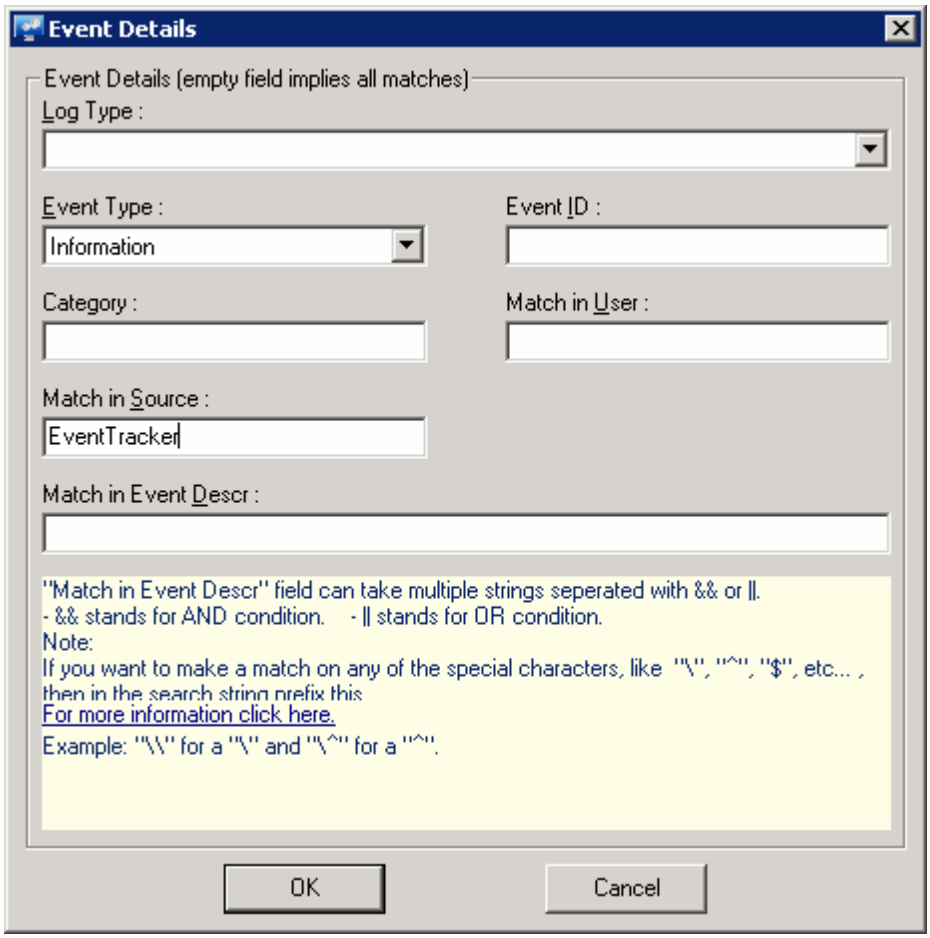


Figure 5

4. Click **OK**.

   EventTracker adds the newly added filter to the filters pool.

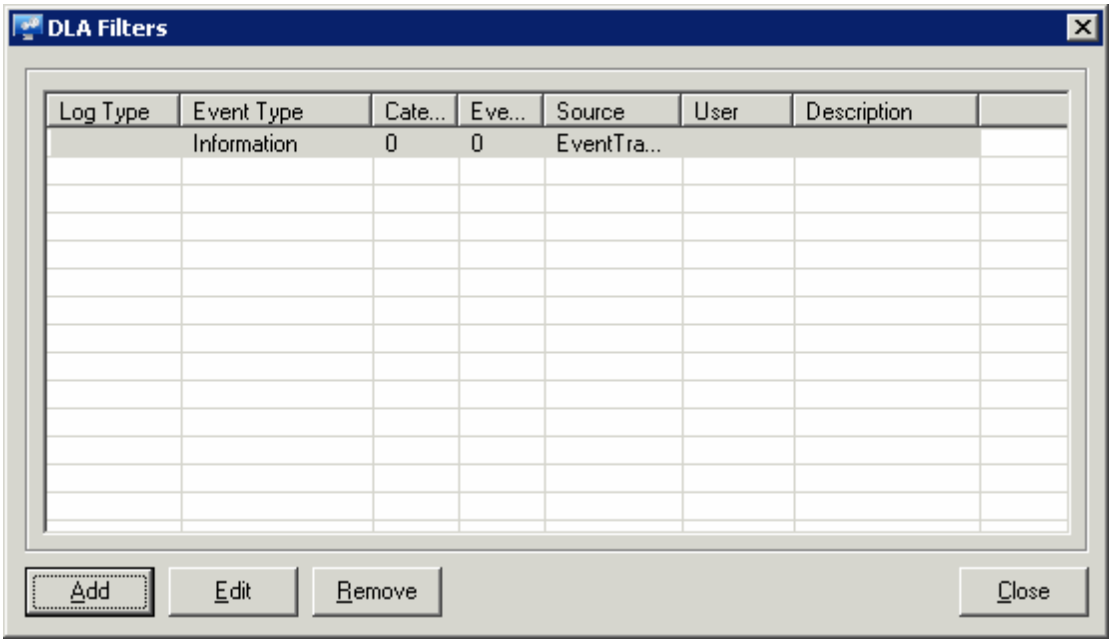


Figure 6

5. Click **Close**.

Verification

Once you are done with the configuration settings, check if .evc files and .cab files are created on the Agent system and DLA instance is created on the Manager system.

EventTracker Agent System

Open the 'DLA' folder under ...\Program Files\Prism Microsystems\EventTracker\Agent. Check if EventTracker Agent service creates '.evc' files. Note that EventTracker Agent service creates .evc files only when the filtered events are available.

Whichever is earlier, either the size of the .evc file reaches 5 MB or the time elapsed is 30 minutes since creating the .evc file, EventTracker Agent service

1. renames the .evc file as Ec2 file
2. compresses the Ec2 file as .CAB file
3. transfers the CAB file to the Manager at the scheduled interval

For example, 1273731788WEBDOC1.evc is renamed and compressed as

1273731788WEBDOC1.ec2EvtFile_Ec2.cab

Had you configured 'Purge Transferred Files' option, EventTracker Agent service moves the files that are transferred to the Manager to the 'DLASentFiles' folder under …\Program Files\Prism Microsystems\EventTracker\Agent\DLA and purges those files at the scheduled interval.

EventTracker Manager System

EventTracker creates a DLA instance with the name of the remote Agent system appended by '-DLA' and transfers filtered events through the DLA channel.

For example, if the name of the remote Agent system is 'WEBDOC1' a DLA instance is created with the same name as 'WEBDOC1-DLA'.

EventTracker System Manager displays the DLA instance under Default systems group.

EventTracker Agent service on the Manager system,

1. receives and dumps the Ec2 CAB files in the 'ETW' folder under …\Program Files\Prism Microsystems\EventTracker\Cache folder.
2. decompresses the CAB files.
3. once the Ec2 files are extracted, discards the CAB files.

EventTracker Archiver service in turn converts the Ec2 files as .mdb files. When the size of the mdb file reaches 50 MB or the time elapsed is 24 hours since creating the mdb file whichever is earlier, compresses the mdb file as CAB file and stores in the …\Program Files\Prism Microsystems\EventTracker\Archives folder.

Through EventVault Configuration, you can also configure EventTracker Archiver to create CAB files at a specified interval.

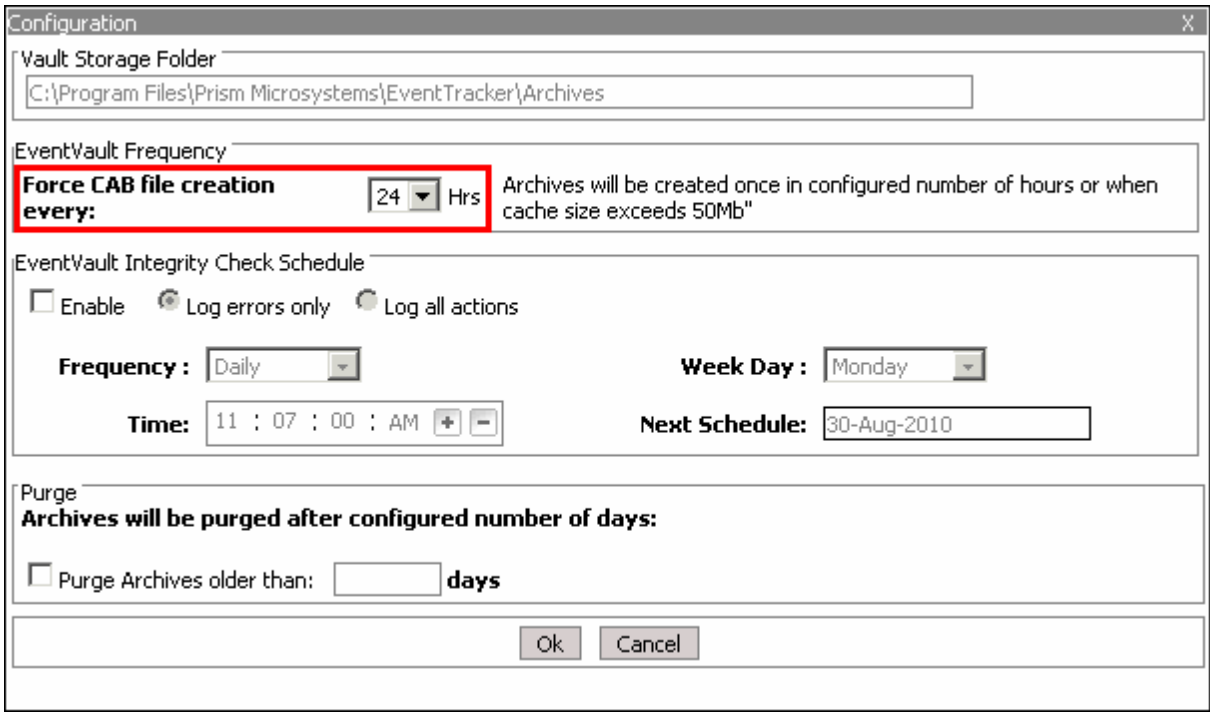


Figure 7

Send Cached events On Demand

This option helps to transfer file on demand by overriding the transfer frequency set.

1. On the EventTracker Agent system, open the Agent Configuration window.
2. Click the **File Transfer** tab.
3. Click **Send Now**.

   EventTracker displays the DLA - Transfer Files window.

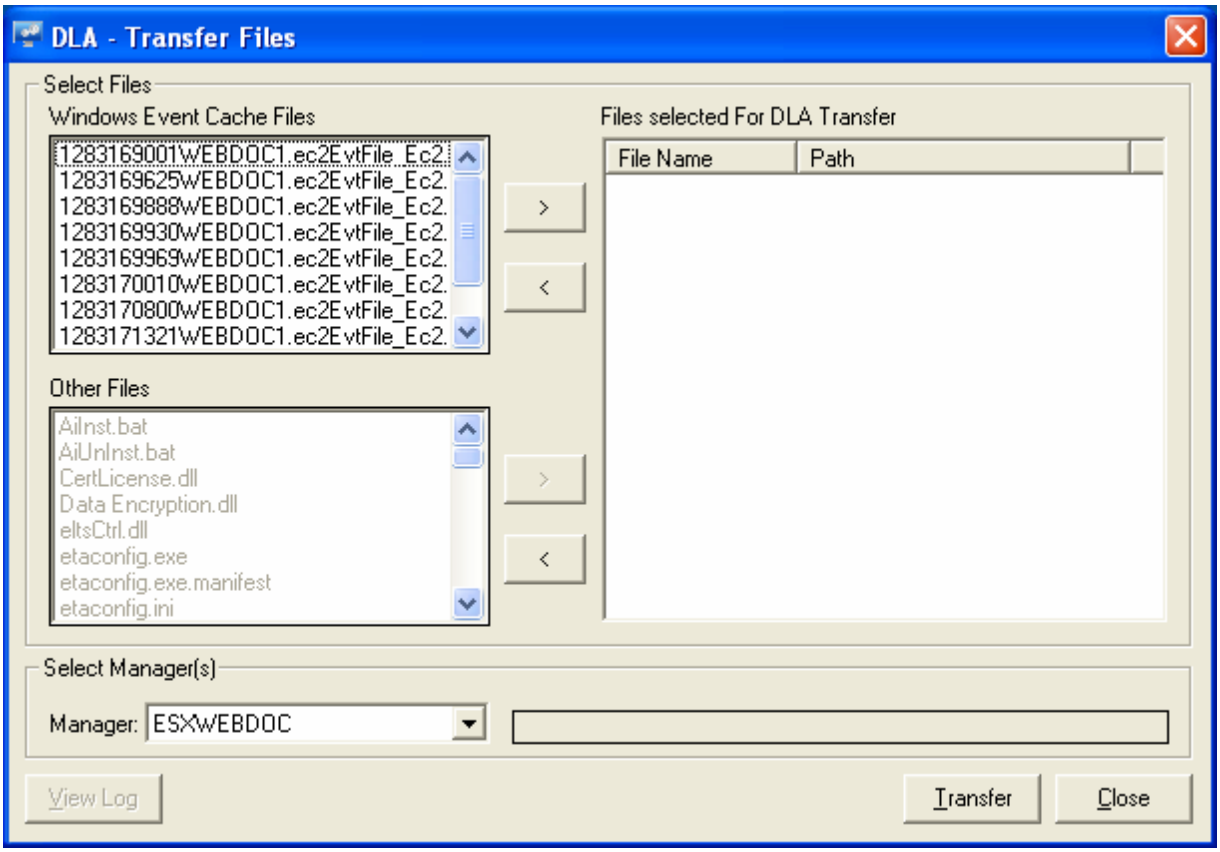


Figure 8

4. Select the CAB files that you wish to transfer from the Windows Event Cache Files list.

5. Click the right arrow button to add the selected file(s) to the Files selected for DLA Transfer list.

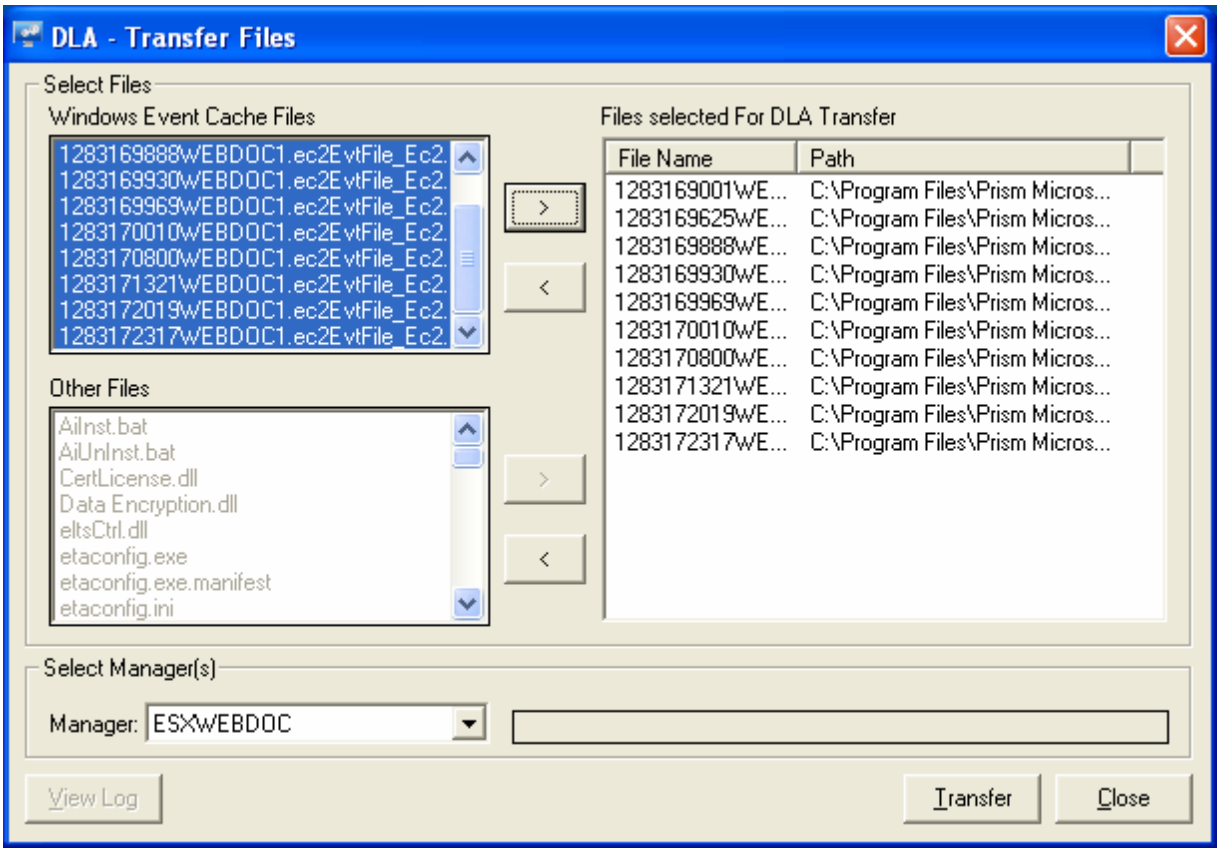


Figure 9

6. Select the destination from the **Manager** drop-down list.

7. Click **Transfer**.

   EventTracker transfers the CAB file(s) to the selected destination.

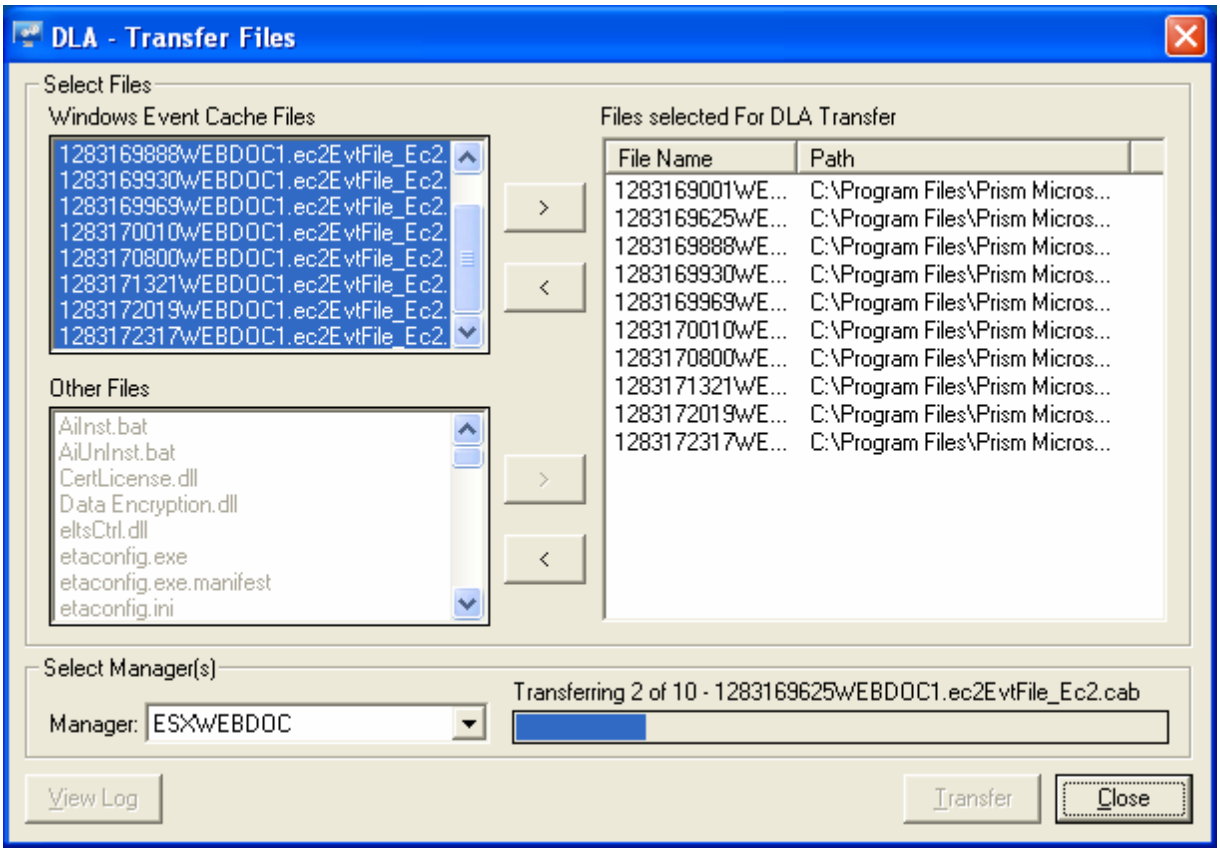


Figure 10

Had you enabled firewall on the Agent system, firewall blocks file transfer and displays the Security Alert.

Figure 11

8. Click **Unblock**.

   Firewall adds the application and the associated port number to the exception list and allows file transfer.

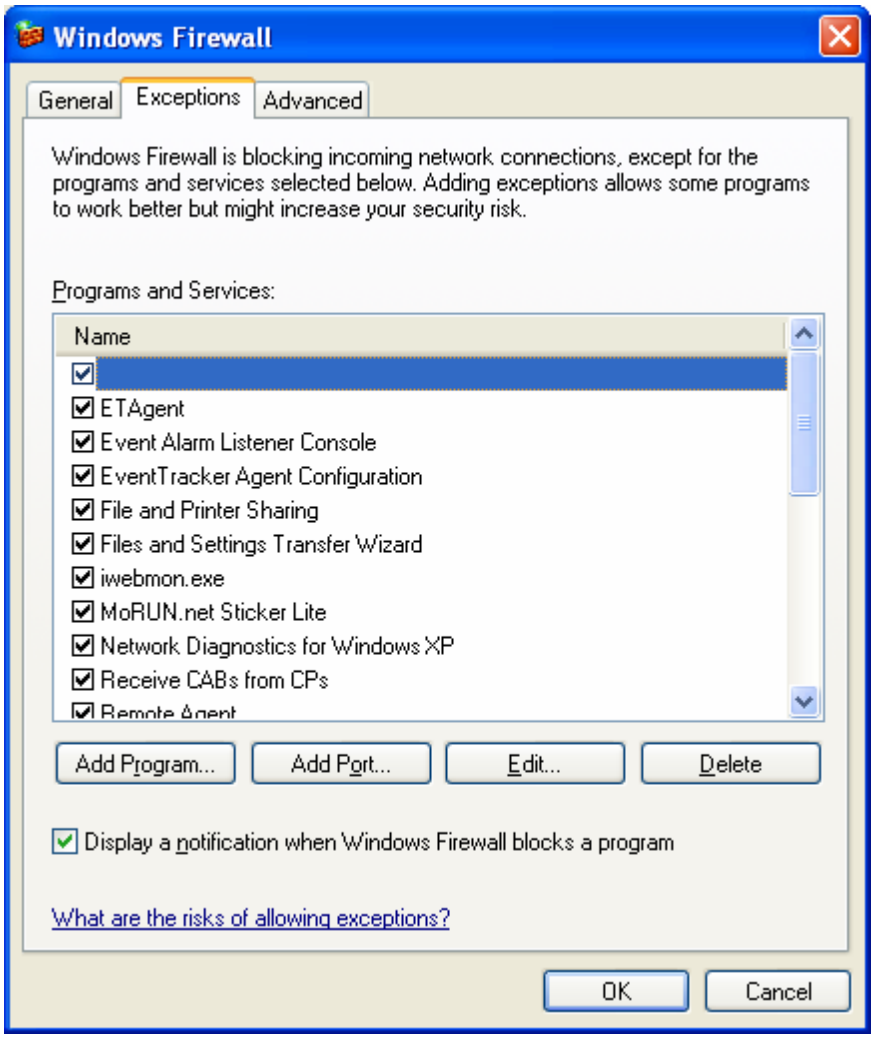


Figure 12

9. Click **Edit** to see the port information.

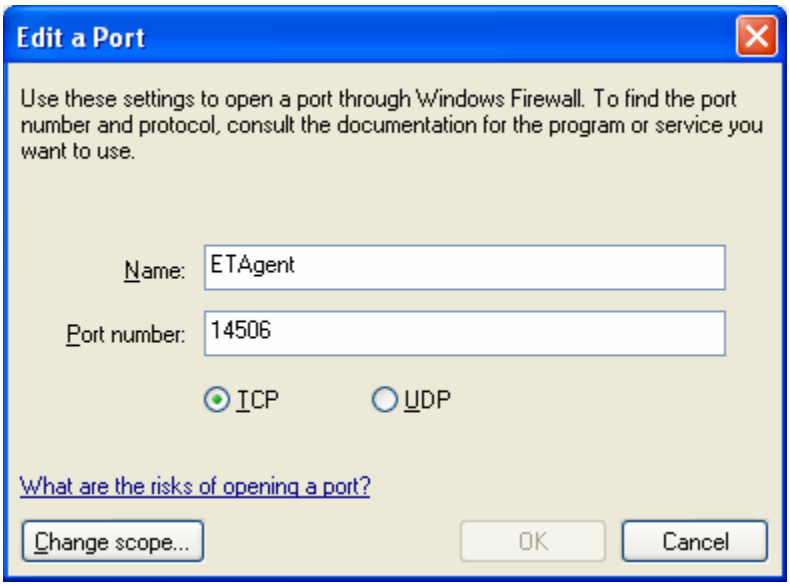


Figure 13

Search Logs for filtered events

This option helps to search events that transferred via file transfer. Cached events that are transferred to Manager will have Event Properties –> Computers as MACHINE NAME-DLA.

To search filtered events transferred via DLA

1. Log on to EventTracker.
2. Click the **Search** hyperlink at the upper-right corner.

   EventTracker displays the Log Search browser.
3. Expand the computer node and click the DLA system.

   (OR)

   Type the name of the DLA system (ex: WEBDOC1-DLA) in the search field and then click **GO**.

   EventTracker Log Search Utility displays the Match Counts graph.

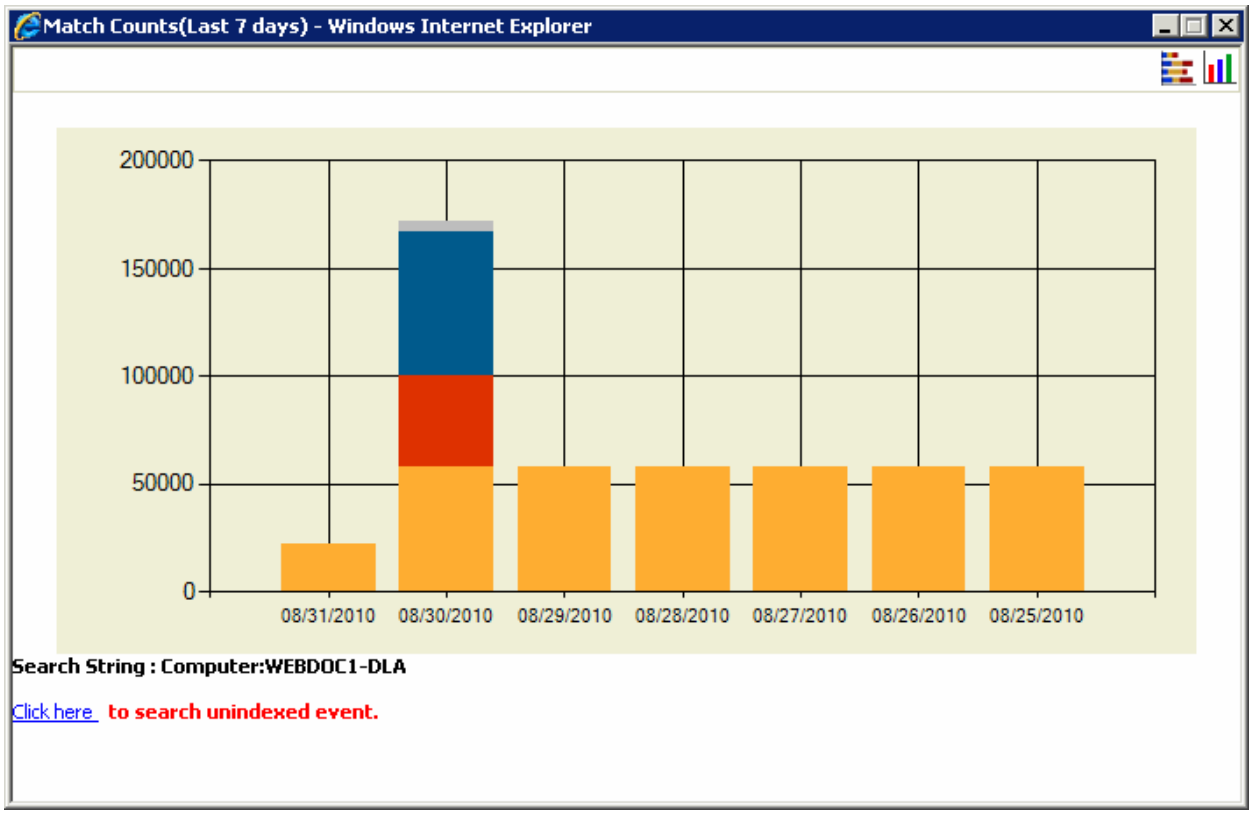


Figure 14

4. Click a disc on a cylinder to view result set for the Search String: Computer:WEBDOC1-DLA.

   It is obvious from the above result set, only the Events that match the filter criteria are sent to the Manager.

Transfer Application Log files and Other Files

This option helps to transfer application log files and other files such as .evt, etc. You can configure Manager DLA to read log files collected from external sources and create CAB files.

Configure Data Storage Folder

This option helps to configure folder to store the log files transferred from the remote Agent computer.

1. Log on to EventTracker.
2. Click the **Admin** menu, click **Manager**, and then click **Agent Settings**.
3. Click **Browse** to select the folder.

   (OR)

   Type the path of the folder in the **Data Storage Folder** field.

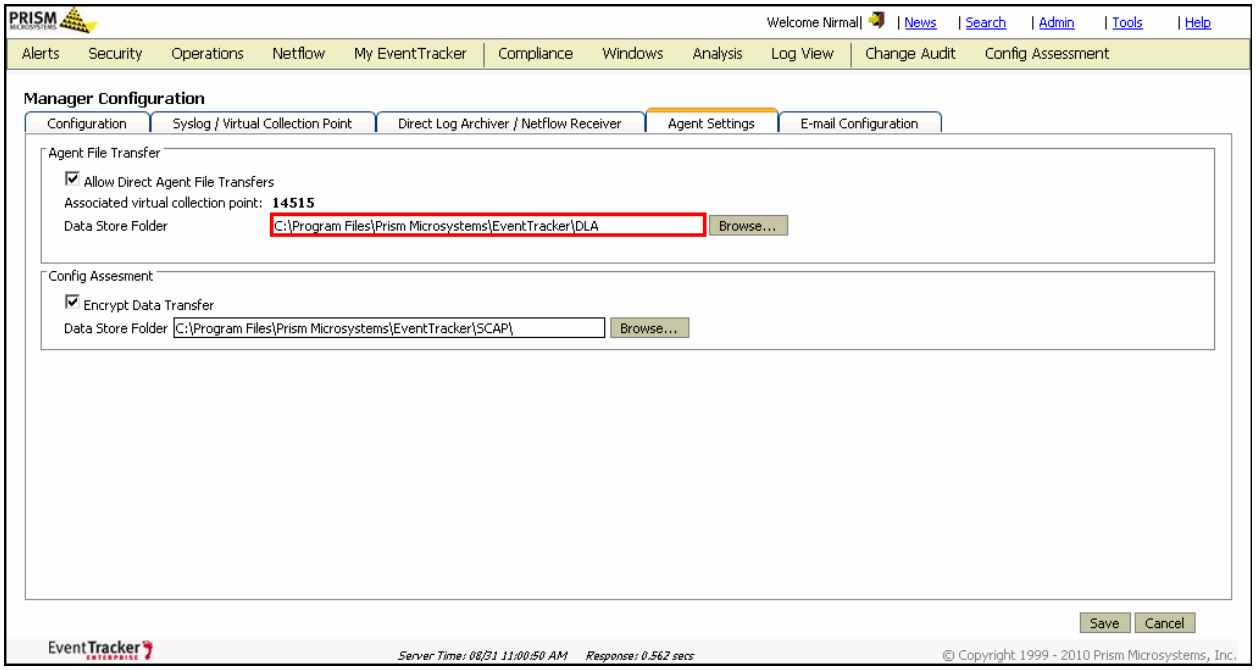


Figure 15

4. Click **Save** on the Manage Configuration page.

Configure EventTracker Windows Agent to transfer files

This option helps to transfer application log files and other files to the Manager.

1. On the Agent system, open the Agent Configuration window.

2. Click the **File Transfer** tab.

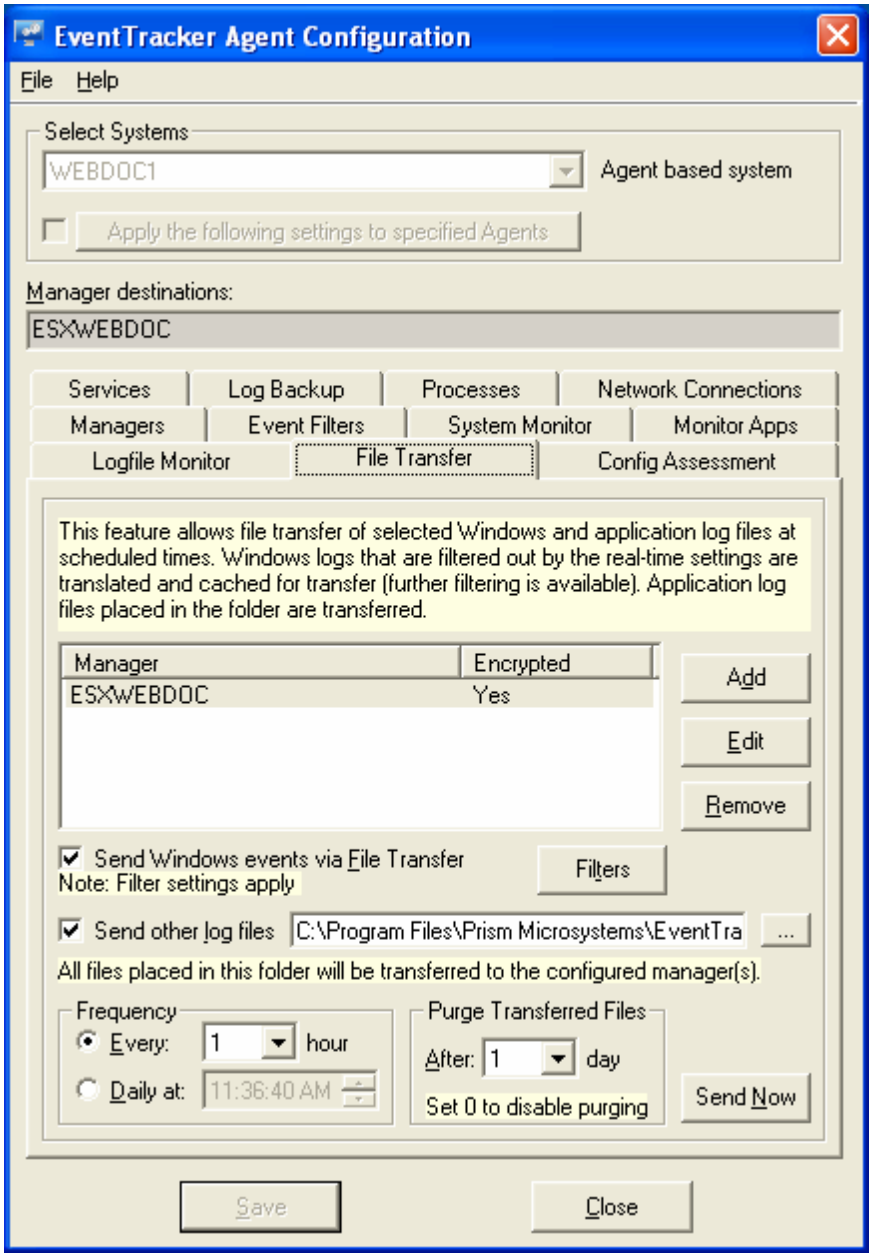


Figure 16

3. Select the **Send other log files** check box, if not selected.

   Default source folder is ...\Program Files\Prism Microsystems\EventTracker\Agent\OtherFiles

4. Click the browse button to select the source folder.

   EventTracker displays the Browse For Folder window.

   Go to the appropriate folder and click **OK**.

   (OR)

   Type the path of the source folder in the text box provided. If the folder exists on a remote system then type the UNC path of the folder.

   EventTracker updates the folder path.

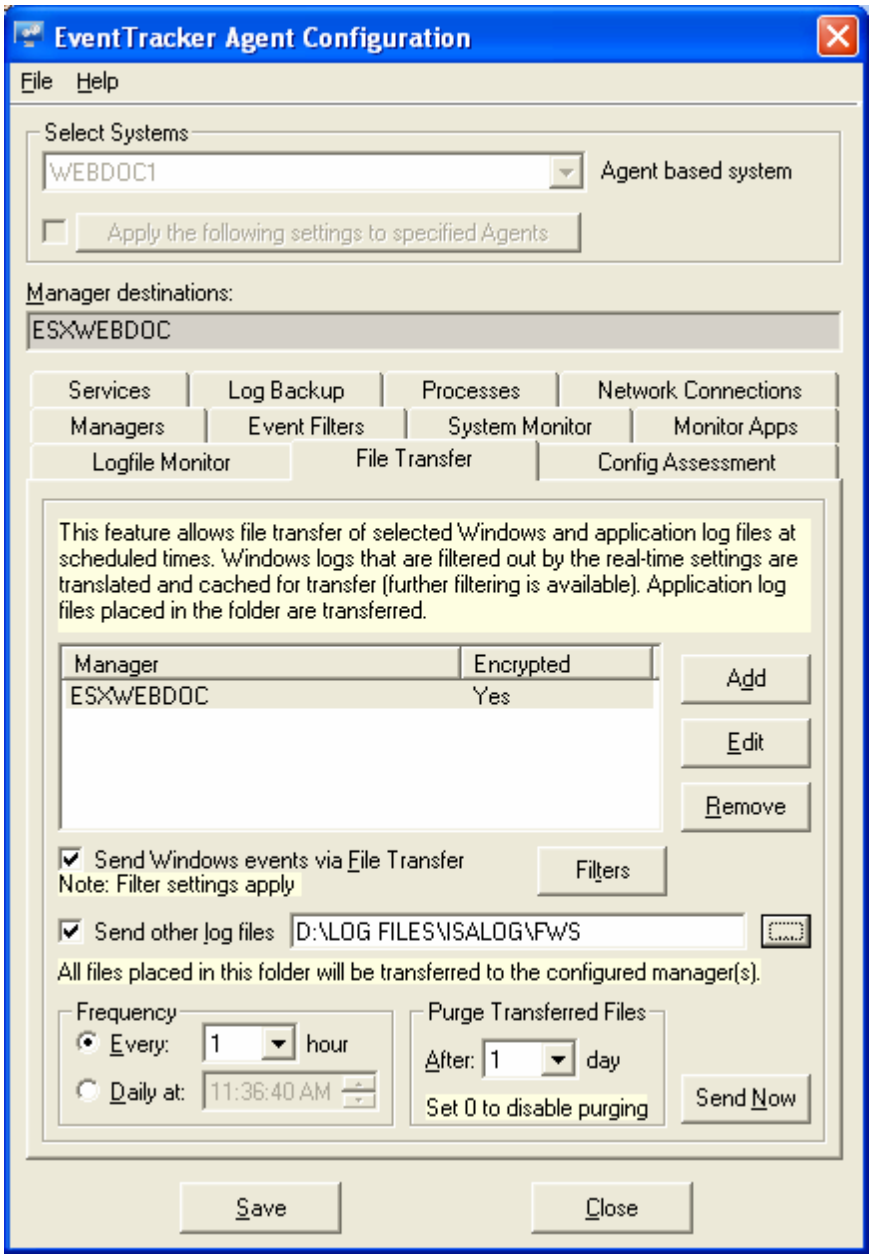


Figure 17

5. Click **Save** to save the settings.

Verification

Once you are done with the configuration settings, check if 'DLASentFiles' folder is created in the source folder (D:\LOGFILES\ISAFWS) on the Agent system.

EventTracker Agent system

EventTracker Agent service,

- compresses log / other files
- creates CAB files
- transfers the CAB files to the Manager.

Open the source folder and check if EventTracker Agent service creates 'DLASentFiles' folder.

Had you configured 'Purge Transferred Files' option, EventTracker Agent service moves the files that are transferred to the Manager to the 'DLASentFiles' folder under the source folder (D:\LOGFILES\ISAFWS) and purges those files at the scheduled interval.

EventTracker Manager system

EventTracker Agent service,

- creates 'DLA' folder under ...\Program Files\Prism Microsystems\EventTracker

  You can also change this 'Data Storage Folder' through Manager Configuration settings.

- creates sub-folder with the name of the remote Agent system

  For example: ...\Program Files\Prism Microsystems\EventTracker\DLA\WEBDOC1, where WEBDOC1 is the name of the remote Agent system

- dumps the log / other files for further processing

Send Files On Demand

1. On the Agent System, open the Agent Configuration window.
2. Click the **File Transfer** tab.
3. Click **Send Now**.

   EventTracker displays the DLA – Transfer Files window

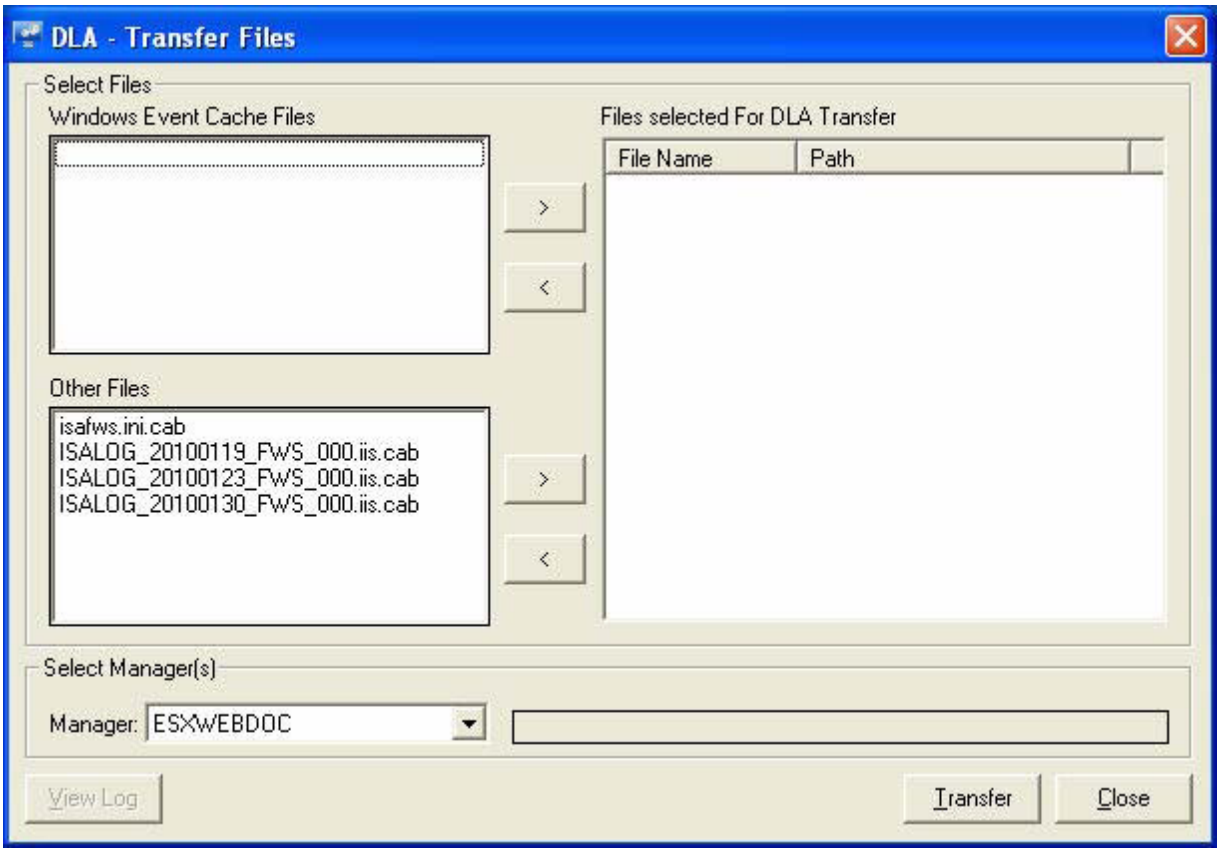


Figure 18

4. Select the files from the **Other Files** list.

   To select multiple files, hold down the CTRL key on your keyboard and click the files names.

5. Click the right arrow button to add the selected files to the Files selected For DLA Transfer list.

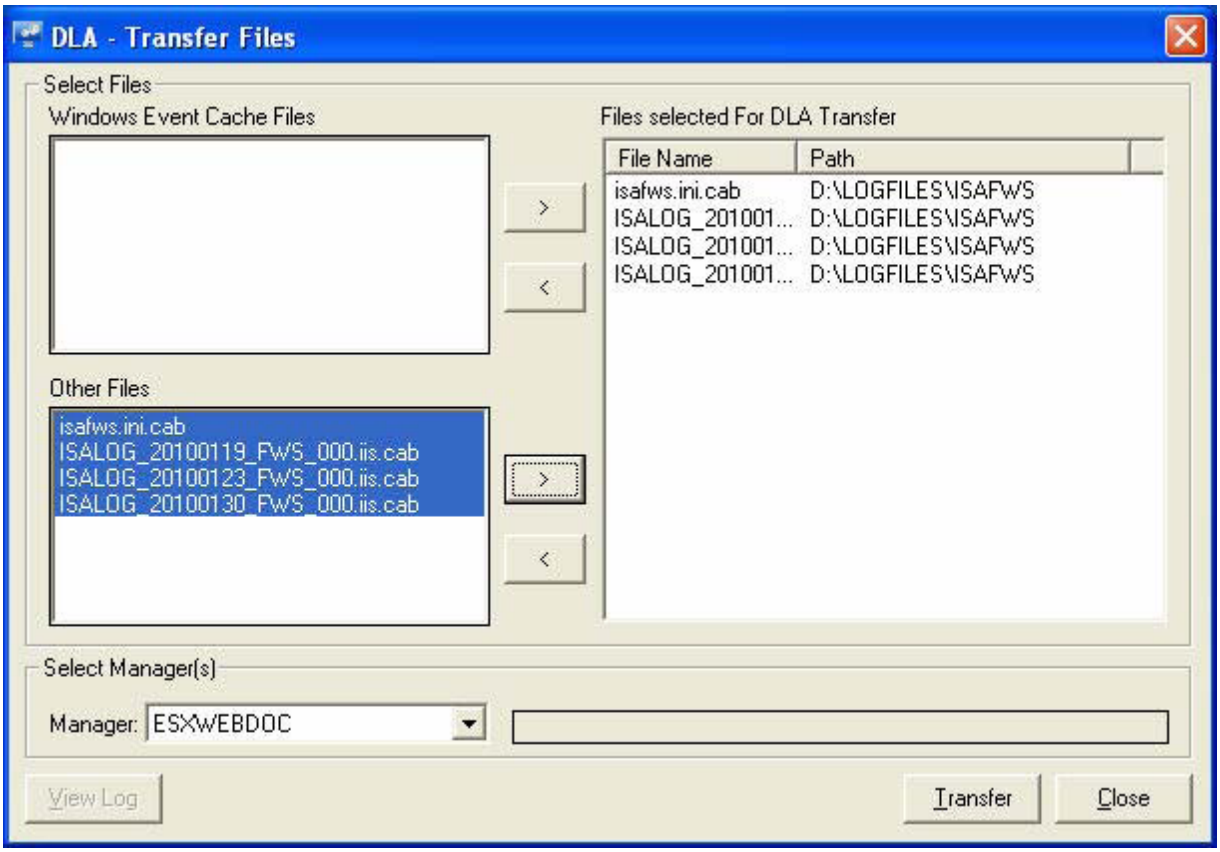


Figure 19

6. Select the destination from the **Manager** drop-down list.

7. Click **Transfer**.

   EventTracker Agent service transfers the selected files to the Manager.

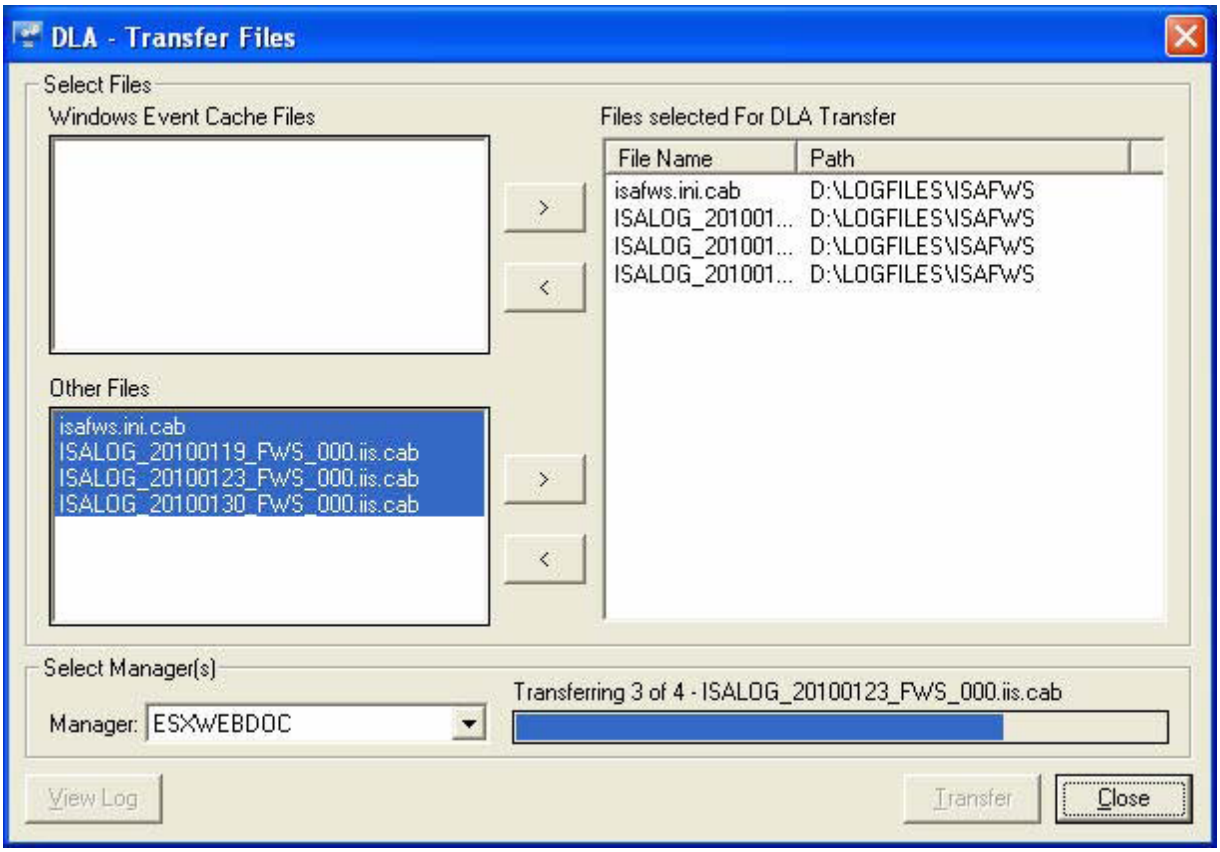

DLA - Transfer Files
Select Files
Windows Event Cache Files
Files selected For DLA Transfer
File Name
Path
isafws.ini.cab
D:\LOGFILES\ISAFWS
ISALOG_201001...
D:\LOGFILES\ISAFWS
ISALOG_201001...
D:\LOGFILES\ISAFWS
ISALOG_201001...
D:\LOGFILES\ISAFWS
Other Files
isafws.ini.cab
ISALOG_20100119_FWS_000.iis.cab
ISALOG_20100123_FWS_000.iis.cab
ISALOG_20100130_FWS_000.iis.cab
Select Manager(s)
Manager:
ESXWEBDOC
Transferring 3 of 4 - ISALOG_20100123_FWS_000.iis.cab
View Log
Transfer
Close

Figure 20

EventTracker Events

Field	Description
Agent DLA File Send Attempt [Event ID: 3279] **EventTracker generates this event on the Agent computer.**	Log Type: Application Event Type: Information (for success), Error (for failure) Event Source: EventTracker Event Category: 2 Event ID: 3279 Description: Agent File Transfer, file send attempt Manager: SIMBI-II File: C:\Program Files\Prism Microsystems\EventTracker\Agent\DLA\1270098659SIMBI-II.ec2 Status: Failed/Success Reason: Descriptive message for failure with error codes etc (applicable only for failures)
Agent DLA File Receive Attempt [Event ID: 2046] **EventTracker generates this event on the Manager computer.**	Log Type: Application Event Type: Information (for success), Error (for failure) Event Source: EventTracker Event Category: 2 Event ID: 2046 Description: Agent File Transfer, file receive attempt Agent: SIMBI-II File: 1270098659SIMBI-II.ec2 Status: Failed/Success Reason: Descriptive message for failure with error codes etc (applicable only for failures)