

Integrate Citrix Access Gateway

Abstract

This guide provides instructions to configure Citrix Access Gateway to transfer logs to EventTracker.

Scope

The configurations detailed in this guide are consistent with **EventTracker** version **7.X and later**.

Audience

Citrix Access Gateway users, who wish to forward event logs to EventTracker Manager and monitor events using EventTracker.

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

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

EventTracker 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 EventTracker, 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.

© 2017 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

- Abstract 1
- Scope 1
- Audience 1
- Overview 3
- Configuring Citrix Access Gateway Event Logging 3
 - To Configure the Remote Server: 3
 - To transfer log files to the remote server 5
 - Configure DLA for Log transfer into EventTracker: 6
 - Configure Freesshd server for log transfer in EventTracker Machine. 6
 - DLA Configuration for log transfer in EventTracker Machine 8

Overview

Citrix NetScaler Gateway is a secure application access solution that provides administrators granular application-level policy and action controls to secure access to applications and data while allowing users to work from anywhere. The solution gives IT administrators a single point of control and tools to help ensure compliance with regulations and the highest levels of information security across and outside the enterprise. At the same time, NetScaler Gateway empowers users with a single point of access—optimized for roles, devices, and networks—to the enterprise applications and data they need. This unique combination of capabilities helps maximize the productivity of today's mobile workforce.

Configuring Citrix Access Gateway Event Logging

You can archive Access Gateway event logs to an external server. You can also manually save and archive the files or can automatically archive the files at scheduled intervals.

To Configure the Remote Server:

1. In the **Access Gateway Management Console**, click **Management**.
2. Under **System Administration**, click **Logging**.

The screenshot displays the 'Networking' configuration page in the Citrix Access Gateway Management Console. The left sidebar shows the 'System Administration' menu with 'Logging' selected. The main panel contains the following configuration details:

Host name: [Redacted]@citrix.net

Network adapters:

Name	IP address	Subnet mask	Adapter Roles			
			Internal	External	Appliance Fallo...	Management
eth0	192.168.2.2	255.255.255.0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Access Gateway Properties:

- Secure port: 443
- Allow ICMP requests
- Enable support access
- Redirect HTTP to HTTPS

Default Gateway:

- Network interface: eth0
- IP address: 192.168.2.1

Figure 1

3. In the Access Gateway Logging panel, under **Remote Server Settings**, set the following options:
 - a. In **Server**, type the IP address or host name of the remote server (EventTracker Machine).
 - b. In **Username**, type the user name.
4. In **Password**, type the user's password.
5. In **Confirm password**, retype the password.
6. In **Transfer protocol**, select one of the following:
 - a. **SCP**. The Secure Copy Protocol (SCP) allows you to transfer files from one computer to another with encryption through the Secure Shell (SSH) protocol.
 - b. **FTP**. The File Transfer Protocol (FTP) allows you to transfer files from one computer to another without encryption.
7. In **Port**, type the port number for the server.
8. In **Remote directory**, type the path of the directory in which you want to store the log files on the remote server.
9. In **Log type**, select one or more types of log file that you want to archive on the remote server: EPA, Info, and Audit.
10. Click **Save**.

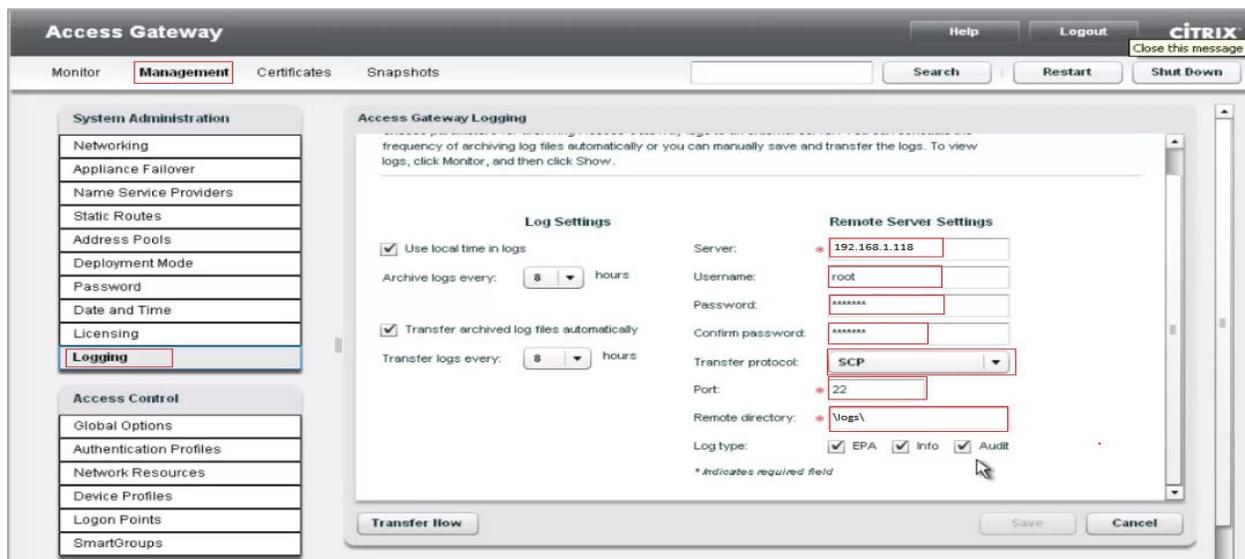


Figure 2

To transfer log files to the remote server

You can transfer log files to the remote server manually or you can schedule automatic archives.

1. In the **Access Gateway Management Console**, click **Management**.
2. Under **System Administration**, click **Logging**.
3. In the Access Gateway Logging panel, under **Log Settings**, set the following options:
 - a. To use the local time in the log files, select the **Use local time in logs** check box.
 - b. To change the scheduled intervals in hours at which log files are archived locally, in **Archive logs every**, select 4 or 8 hours.
 - c. To archive log files automatically, select the **Transfer archived log files automatically** check box and then in **Transfer logs every**, select the frequency with which you want the archived files transferred to the remote server, 4, 8, or 16 hours.
 - d. To manually save and transfer the log files immediately, click **Transfer Now** button.

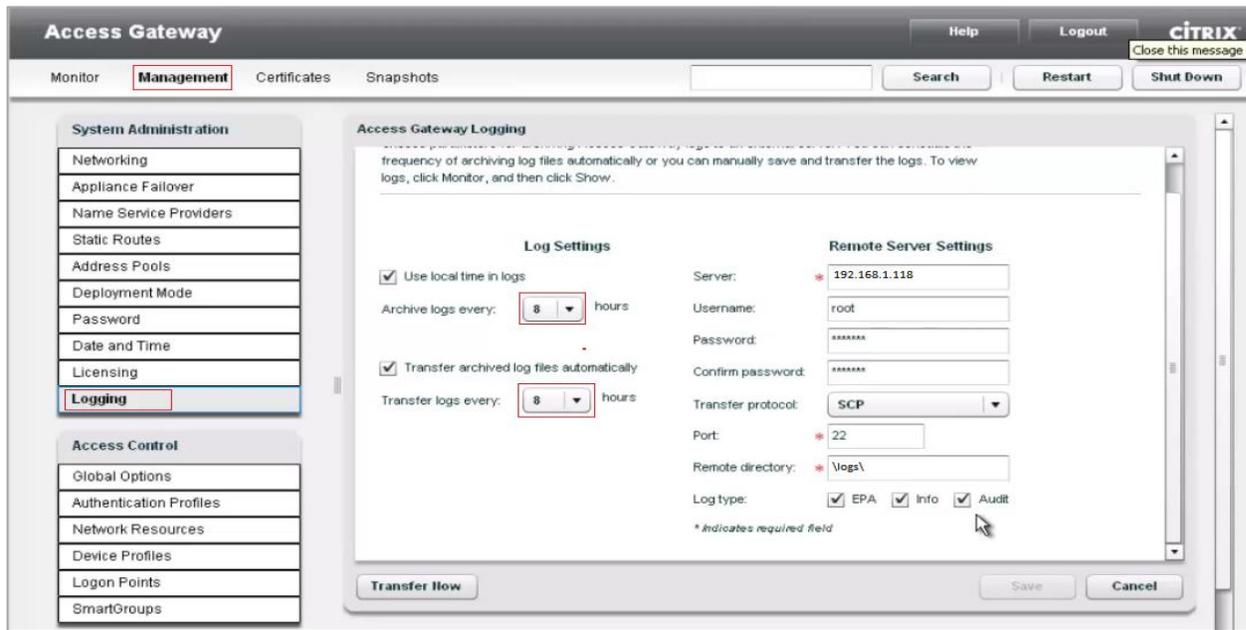


Figure 3

Configure DLA for Log transfer into EventTracker:

Configure Freesshd server for log transfer in EventTracker Machine.

Follow the below mentioned steps for the configuration of log transfer into EventTracker:

1. Download and install [freesshd](#) server in EventTracker Machine.
2. Configure User (e.g root) in freesshd server setting
3. Click the **Add...** button

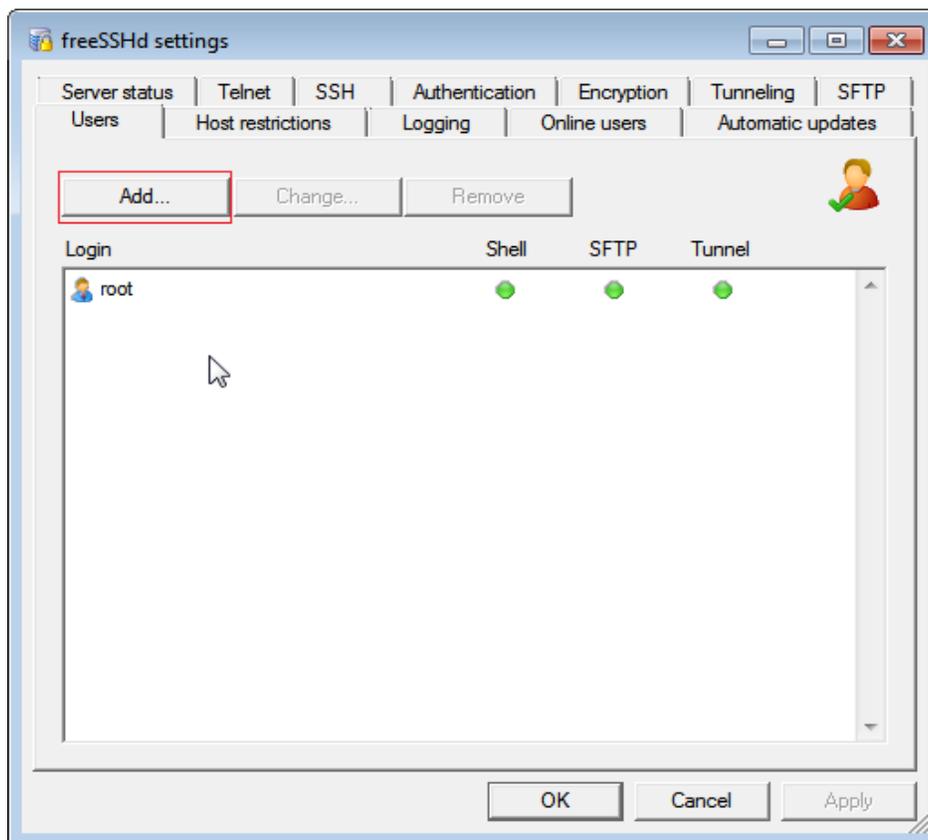


Figure 4

4. Enter the **Login** (e.g root), select the **Authorization** type, and enter the **Password** and select the Option **User can use**.

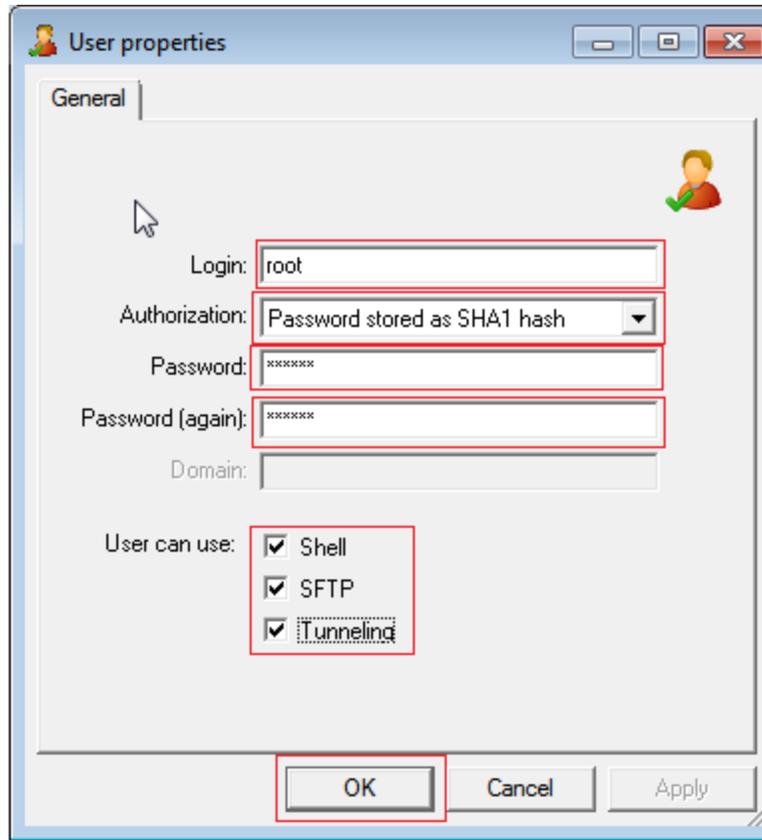


Figure 5

5. Please specify the directory where you want to stored logs by going to **SFTP** tab.

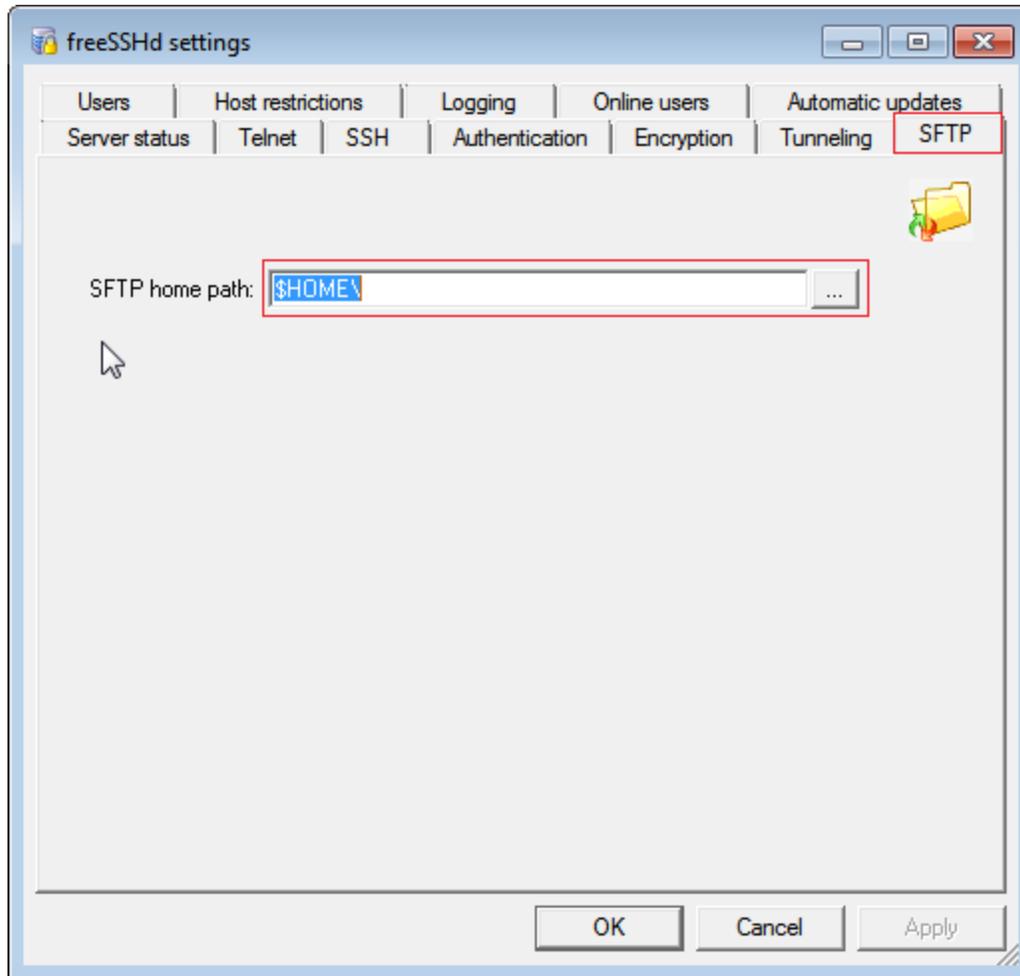


Figure 6

6. Please use Same User and directory for Citrix Access Gateway log transfer configuration.

DLA Configuration for log transfer in EventTracker Machine

1. Login to **EventTracker Enterprise**.
2. Click **Admin** dropdown, and then click **Manager**.
3. Click **Direct Log Archiver** tab.
4. Click **Direct log file archiving from external sources** option.
5. Click the **Add** button.

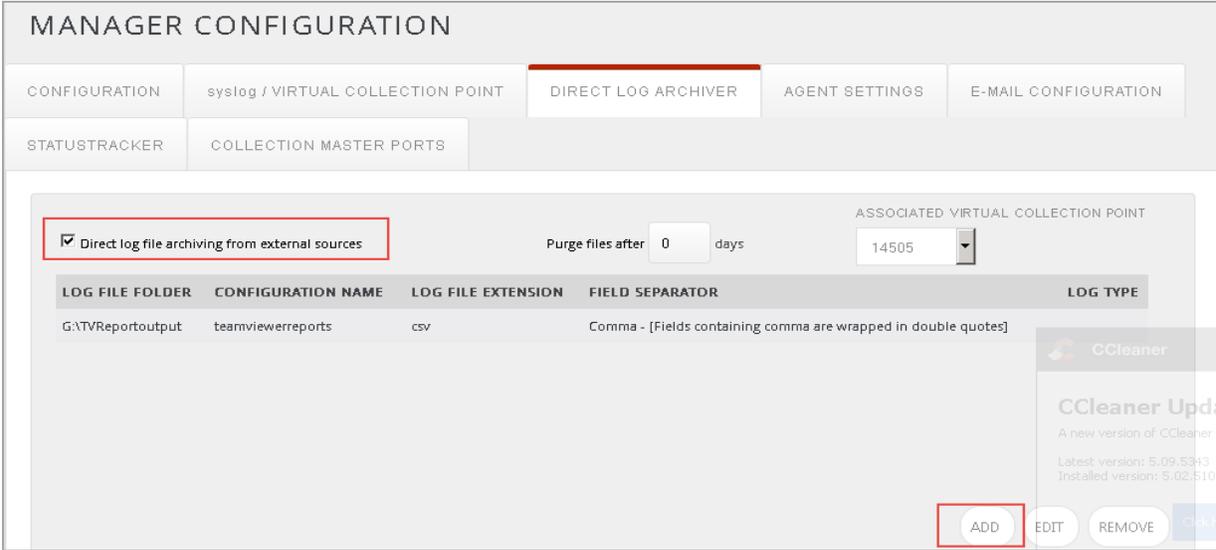


Figure 7

EventTracker displays Direct Archiver Configuration window.

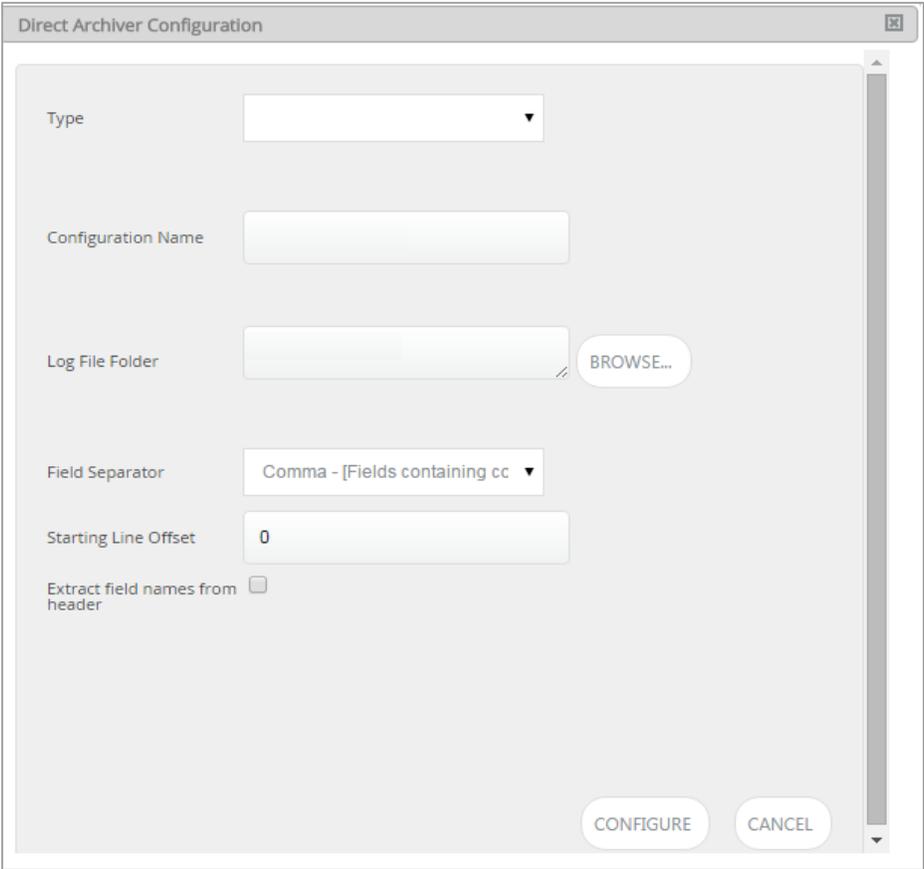


Figure 8

6. In **Type** dropdown, select the type as **Others**.

7. Enter **Logfile Extension** as TXT.
8. Enter **Configuration Name**.
9. Click the **Browse...** button to select the **Log File Folder** path.
(OR)
Type the **Log File Folder** path in the text box.
10. Select **Single Line** Radio Button.
11. In Starting Line Offset let it be zero by default.

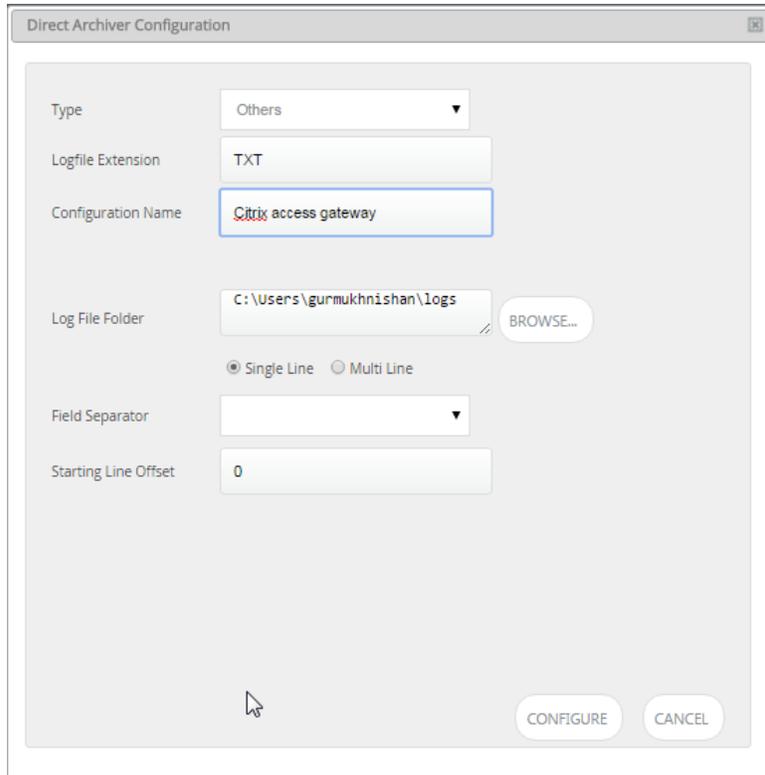
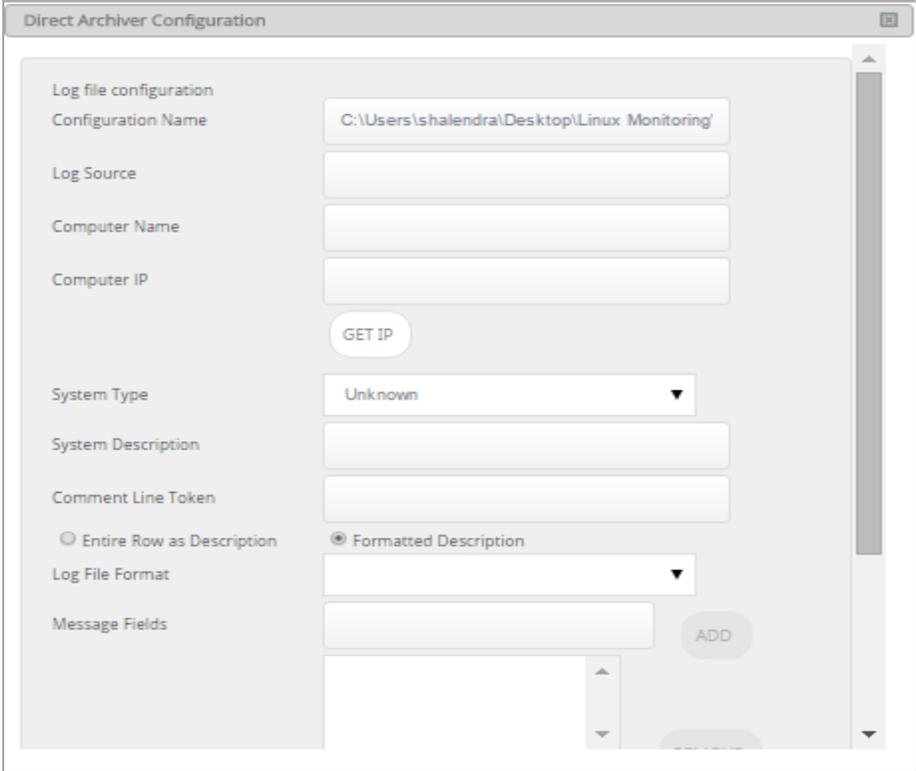


Figure 9

12. Click the **Configure** button.
Logfile configuration pane displays.



The screenshot shows a window titled "Direct Archiver Configuration" with a scrollable content area. The fields and their current values are as follows:

- Configuration Name:** C:\Users\shalendra\Desktop\Linux Monitoring
- Log Source:** (Empty text box)
- Computer Name:** (Empty text box)
- Computer IP:** (Empty text box)
- GET IP:** (Button)
- System Type:** Unknown (Dropdown menu)
- System Description:** (Empty text box)
- Comment Line Token:** (Empty text box)
- Radio Buttons:** Entire Row as Description, Formatted Description
- Log File Format:** (Empty dropdown menu)
- Message Fields:** (Empty text box)
- ADD:** (Button)

Figure 10

13. Enter **Log Source, Computer Name, Computer IP, System Type and System Description.**
14. Leave blank the **Comment Line Token** field.
15. Select **Entire Row as Description** option, if not selected.

The screenshot shows the 'Direct Archiver Configuration' window. The 'Log file configuration' section includes the following fields and values:

- Configuration Name: C:\Users\gurmukhnishan\logs\Citrix access gate
- Log Source: Citrix Access Gateway
- Computer Name: CAG
- Computer IP: 192.168.1.85
- System Type: Win 7
- System Description: OS
- Comment Line Token: (empty)
- Log File Format: (empty)
- Message Fields: (empty)

Additional controls include a 'GET IP' button, radio buttons for 'Entire Row as Description' (selected) and 'Formatted Description', and 'ADD' and 'REMOVE' buttons for the Message Fields list.

Figure 11

16. Click the **Save & Close** button.

The relevant folder is configured in the DLA folder.

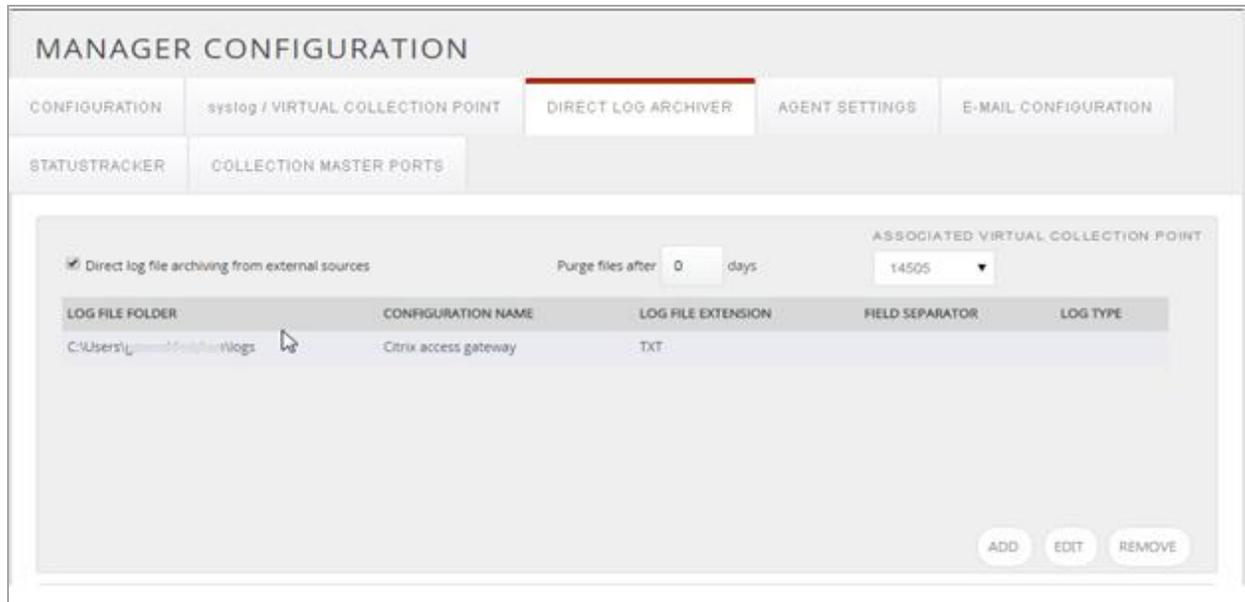


Figure 12

17. Click the **Save** button.

Now Direct Log Archiver (DLA) has been created successfully. Check the logs in search option of EventTracker.

18. Click the **Search** menu, and then select **Advanced Search**.

Advanced Log Search window displays.

19. Select the required systems.

20. In **Custom Criteria** pane, select **Add custom criteria**.

21. In **Search in** drop down, select **Description**.

22. In **Operator** drop down, select **contains**.

23. In **Search for** box, enter **any key word** related to log description like DiskMon, and then click the **Search** button.

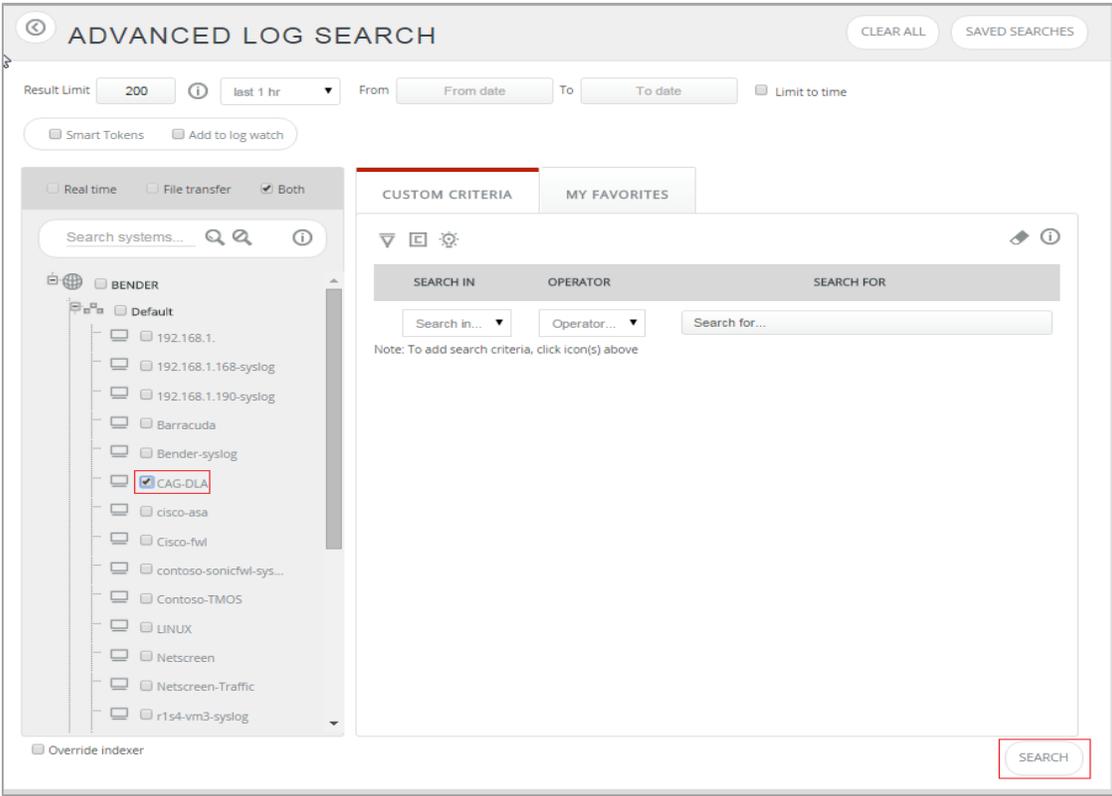


Figure 13

Log Search results display.

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
Collapse all 1:02:39 AM	3230	BENDER / CAG-DLA	SYSTEM	NT AUTHORITY	Citrix Access Gateway
Event Type: Information Log Type: System Category Id: 2	Description: session 201508271031.58 AG: (error): Failed to transfer info_20150825_2000.txt to citrix@10.0.30.56:22: Failure establishing ssh session 201508271032.03 AG: (error): Failed to transfer info_20150825_1600.txt to citrix@10.0.30.56:22: Failure establishing ssh session 201508271032.08 AG: (error): Failed to transfer info_20150825_1200.txt to citrix@10.0.30.56:22: Failure establishing ssh session 201508271032.13 AG: (error): Failed to transfer info_20150825_0800.txt to citrix@10.0.30.56:22: Failure establishing ssh session 201508271032.18 AG: (error): Failed to transfer info_20150825_0400.txt to citrix@10.0.30.56:22: Failure establishing ssh session 201508271032.23 AG: (error): Failed to transfer info_20150825_0000.txt to citrix@10.0.30.56:22: Failure establishing ssh session 201508271032.28 AG: (error): Failed to transfer info_20150824_2000.txt to citrix@10.0.30.56:22: Failure establishing ssh session 201508271032.33 AG: (error): Failed to transfer info_20150824_1600.txt to citrix@10.0.30.56:22: Failure establishing ssh session 201508271032.38 AG: (error): Failed to transfer info_20150824_1200.txt to citrix@10.0.30.56:22: Failure establishing ssh session 201508271032.43 AG: (error): Failed to transfer info_20150824_0800.txt to citrix@10.0.30.56:22: Failure establishing ssh session 201508271032.48 AG: (error): Failed to transfer info_20150824_0400.txt to citrix@10.0.30.56:22: Failure establishing ssh session 201508271032.53 AG: (error): Failed to transfer info_20150824_0000.txt to citrix@10.0.30.56:22: Failure establishing ssh session 201508271032.58 AG: (error): Failed to transfer info_20150823_2000.txt to citrix@10.0.30.56:22: Failure establishing ssh session 201508271033.03 AG: (error): Failed to transfer info_20150823_1600.txt to citrix@10.0.30.56:22: Failure establishing ssh session				

Figure 14