



**GroupDrive**

**GroupDrive Collaboration Server  
Using Events to Thwart Hackers  
Quick Start Guide**

**February 2010**

## Notices

Copyright 2010 South River Technologies, Inc. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement, OEM, or reseller agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of South River Technologies, Inc.

South River Technologies<sup>®</sup>, GroupDrive Collaboration Server<sup>®</sup>, Cornerstone MFT<sup>™</sup>, Titan FTP Server<sup>®</sup>, DMZedge Server<sup>™</sup>, and WebDrive<sup>®</sup> are trademarks of South River Technologies, Inc. in the U.S. and other countries. Microsoft, Windows, Windows NT, Windows XP, and Windows Vista are trademarks of Microsoft Corporation, Inc. The names of other actual companies and products mentioned herein may be the trademarks of their respective owners. Any information in this document about compatible products or services should not be construed in any way to suggest SRT endorsement of that product or service.

South River Technologies, Inc.  
2635 Riva Road  
Suite 100  
Annapolis, Maryland 21401  
USA  
Telephone: 410-266-0667  
Fax: 410-266-1191  
[www.southrivertech.com](http://www.southrivertech.com)

**Please Note:** This quick start guide will help you to configure events in GroupDrive Collaboration Server to help you to thwart hackers. If you need assistance configuring options that are not included in this quick start guide, the [GroupDrive Server Administrator User's Guide](#) is available online. A listing of Frequently Asked Questions (FAQ) is also available at our [Knowledgebase Support Center](#) and a complete listing of SRT [Quick Start Guides](#) is available online.

## Using Event Management to Thwart Hackers—Overview

One of the most common server problems involves unauthorized users or hackers attempting to guess user names and passwords in order to gain access to the server.

GroupDrive Collaboration Server *Event Management* can help thwart these attempts by detecting invalid user attempts. GroupDrive will kick that connection from the server and ban future access from the client IP address.

This quick start guide will help you to set up three separate actions using the GroupDrive Collaboration Server *Event Manager* that will help protect your server from being compromised. These actions will occur when a hacking attempt is triggered.

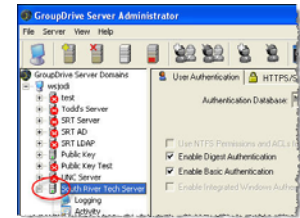
- *Send Email* – An *Email* action allows the server administrator to be notified each time the event is triggered. It is a very good idea to send an email notification so that the server administrator can double check to make sure that a valid user was not banned from the system.
- *Kick User* – A *Kick User* action terminates the current connection session and prevents the user from issuing another USER command.
- *Ban IP Address* – A *Ban IP Address* action prevents future connections to the server from the same client IP address.

### Event Management Best Practices

The *Event Management* actions that this quick start guide will help you to configure is just one way that you can use GroupDrive Collaboration Server *Event Management* to monitor unauthorized access to the server. Regardless of the event and action configuration for each event, whenever you create new events it is a good idea to send an email notification to the system administrator, especially if you have defined an action that bans someone from accessing the system. Although rare, on occasion a valid user may misspell their user name or some other error may occur that causes a valid user to be banned from the system.

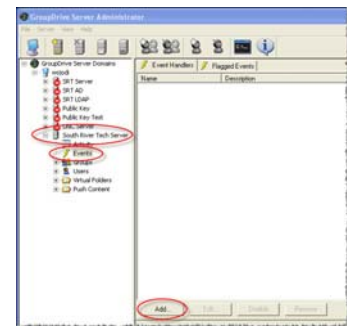
## Configuring the Event Handler

- Once you have created your server using the GroupDrive **New Server Wizard**\*, the server starts and appears in the main GroupDrive Administrator window. A green icon appears to indicate that the server is running.



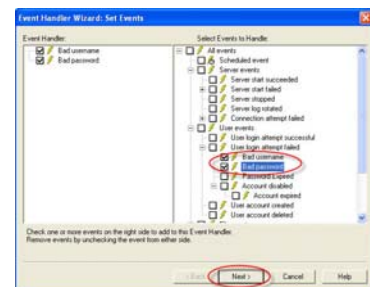
\*For more information about specific configuration options available in the GroupDrive **New Server Wizard**, see the [GroupDrive Administrator's User Guide](#) or visit our [Knowledgebase Support Center](#). A complete listing of [SRT Quick Start Guides](#) is also available online.

- You will use the GroupDrive Server Administrator to configure your Event Handler. Select the server that you would like to modify from the **GroupDrive Server Domains** tree, and then select **Events**. Click **Add** to add the event. The GroupDrive **Event Handler Wizard** will launch. The **Event Handler Wizard** will allow you to **Set Events**, **Set Conditions** for the events that you select, and then **Set Actions** for those events.



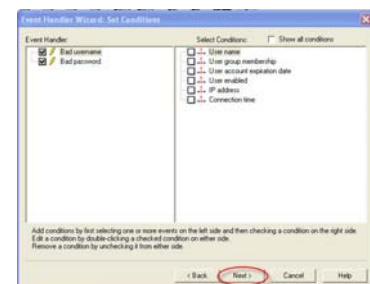
### 3. Set Events

Select **Bad username** and **Bad password**. This option is located on the **Select Events to Handle** menu tree, under **User events > User login attempt failed**. Click **Next**.



### 4. Set Conditions

To use this event to thwart hackers you want to capture all connection attempts, so do not specify any conditions. Click **Next**.



## 5. Set Actions

You will set up three separate actions that will occur when a potential hacking attempt is triggered.

**Send email**—An email action notifies the server administrator each time the event is triggered. We recommend that you use the **Send email** option so that the server administrator can verify that a *valid user* is not banned from the system.

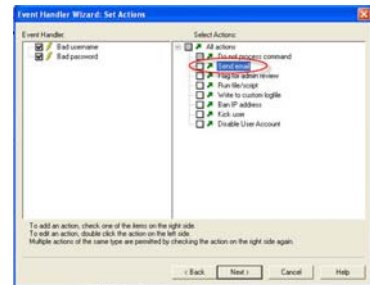


**Kick User**—The **Kick User** action terminates the current connection session and prevents the user from issuing another user command.

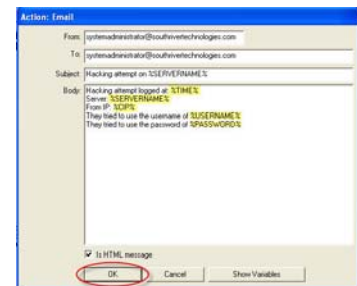
**Ban IP address**—The **Ban IP address** action prevents any future connections from the same client IP address.

## 6. Action: Email

Select **Send email** using the check box. The **Action:Email** window will appear.



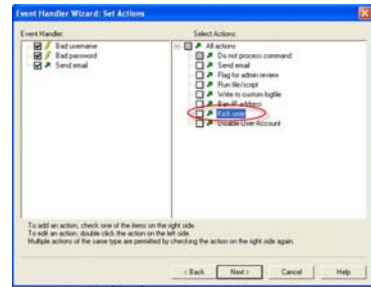
7. Type the **From:** and **To:** email addresses and **Subject** of the email. In the **Body** of the email it is a good idea to include some details about when the event occurred. We recommend including the **time**, the **server name**, the **IP address** of the client, the **username** and the **password\*** that was used during the hack attempt. If the message is HTML, select the HTML Message check box. Click **OK**.



\*To include the **time**, **server name**, **IP address**, **username**, and **password**, use the variables as shown in our example.

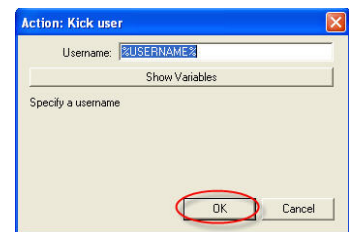
## 8. Action: Kick User

Select **Kick user** using the check box.



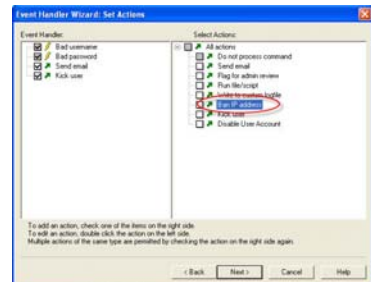
## 9. The **Kick user** action tells the **Event Manager** to **kick this user from the system** when the event is triggered.

Specify the **%USERNAME%** variable so that the Event Manager will only kick the user name that was used during the hack attempt. Click **OK**.



## 10. Action: Ban IP Address

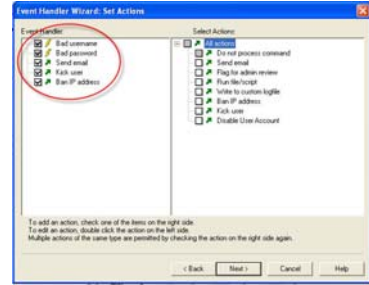
Select **Ban IP address** using the check box.



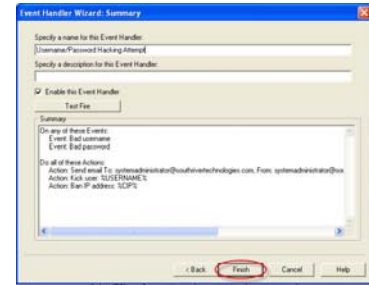
## 11. The **Ban IP address** action tells the **Event Manager** to add this client IP address to the list of IP addresses that are banned from accessing the server. During this process the **Event Manager** checks to see if the **IP Access Restrictions** feature is enabled at the server level and, if necessary, enables it at the server level. The **Event Manager** then adds the current IP address to the **IP Access Restrictions** list and marks it as banned. No connections will be accepted from this IP address in the future. Specify the IP address variable: **%CIP%** and then Click **OK**.



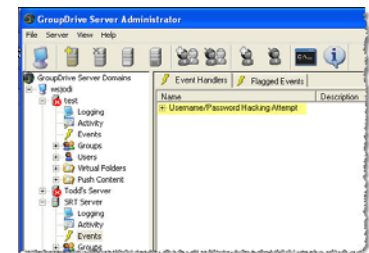
12. Now that you have defined your actions, your **Event Handler** list should look like our example. Click **Next**.



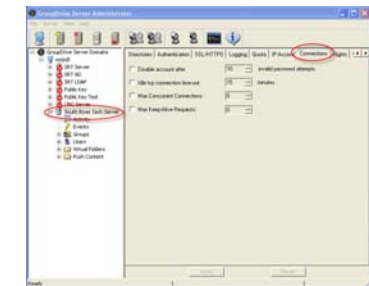
13. Type a **name** for this **Event Handler** and type an optional description. This Event Handler is enabled by default. You may *Test Fire* this Event Handler now; however, since you do not have a valid client IP address or user name, the test will not be 100% accurate. Click **Finish**.



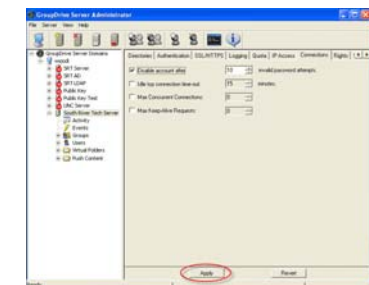
14. **Stop** and then **Start** the Server. The event that you just defined is displayed.



15. You will now need to enable the **Disable account** option and select the number of password attempts that you will allow. Select the **Server** from the *GroupDrive Server Domains tree*. Use the right/left arrows to select the **Connections** tab.



16. Select **Disable account after** using the check box. Use the up/down arrows if you would like to change the number of allowed attempts. Click **Apply** to apply the changes.



You are now finished with the steps for creating this Event Handler. The next step is to test the event.

## Test the Event

To properly test the event, you will logon to the server using an invalid user name.

1. Right-click on the **server** and select **Launch Browser**. The GroupDrive Logon screen will appear.



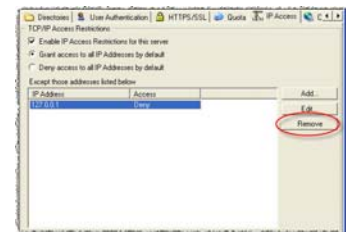
2. **Logon** to GroupDrive using a user name and password that **does not exist** on the server.



3. GroupDrive will issue a warning that the username or password was incorrect. The number of logon attempts is configurable and defaults to ten attempts. Attempt to logon ten times or the number of attempts that you configured on the server.



4. Launch the *GroupDrive Sever Administrator*. From the *GroupDrive Server Domains* menu tree, select the **Server**. In the tab pane, use the left/right arrows to view the **IP Access** tab. The banned IP Address now shows in the window.\*



\*To remove this banned address, click **Remove**, and then click **Apply**.

## About South River Technologies

South River Technologies (SRT) is an innovator in managed file transfer and document collaboration software. SRT's software seamlessly integrates access to remote files into the desktop applications that users rely on, creating an instantly familiar interface for collaborating, sharing, and accessing files. SRT's enterprise class server products are built using industry standard encryption, highly granular security configuration controls, and technologies to reduce the risk of network intrusions. Over 60,000 customers, including more than 70 colleges and universities, government agencies such as NASA and FAA and other blue chip companies in more than 110 countries rely on SRT's software to make remote file access and collaboration more efficient for their customers, partners, and distributed workforce. For more information, please visit [www.southrivertech.com](http://www.southrivertech.com).