



CornerstoneMFT

Using Events to Thwart Hackers
Quick Start Guide

January 2010

Notices

Thank you for purchasing Cornerstone MFT®.

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 and Cornerstone FTP/MFT Server, WebDrive, DMZedge, and GroupDrive are registered trademarks of South River Technologies, Inc. in the U.S. and other countries. Microsoft, Windows, Windows NT, Windows XP and Windows Vista are registered 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

Please Note: The following instructions will help you to set up Cornerstone MFT to thwart hackers by using Cornerstone MFT *Event Management*. Some screens in this instruction contain options that do not pertain to using event management to thwart hackers. If you need additional information regarding these steps, please see the [Cornerstone MFT User Guide](#). For the purpose of this quick start guide, we will guide you through these options without configuring additional settings. A listing of Frequently Asked Questions (FAQ) is also available at our [Knowledgebase Support Center](#).

Thwarting Hackers using Event Management—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.

Cornerstone MFT *Event Management* can help thwart these attempts by detecting invalid user attempts. Cornerstone MFT 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 Cornerstone MFT *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

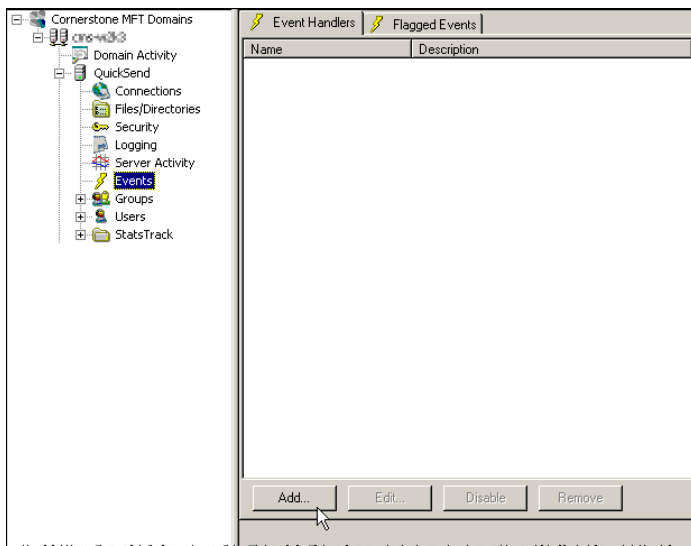
The *Event Management* actions that this quick start guide will help you to configure is just one way that you can use Cornerstone MFT *Event Management* to monitor unauthorized access to the server. Regardless of the event and action configuration for each event, whenever you create new events it is 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

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

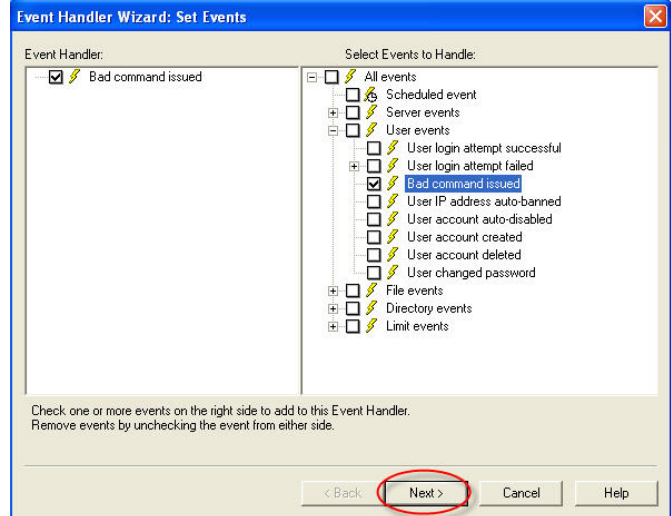
*For more information about specific configuration options available in the *Cornerstone MFT Wizard*, see the [Cornerstone Administrator's User Guide](#) or visit our [Knowledgebase Support Center](#). A complete listing of [SRT Quick Start Guides](#) is also available online.

2. You will use the *Cornerstone MFT Administrator* to configure your *Event Handler*. Select the **server that you would like to modify** from *Cornerstone MFT Domains* tree, and then select **Events**. Click **Add** to add the event. The *Cornerstone MFT 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.



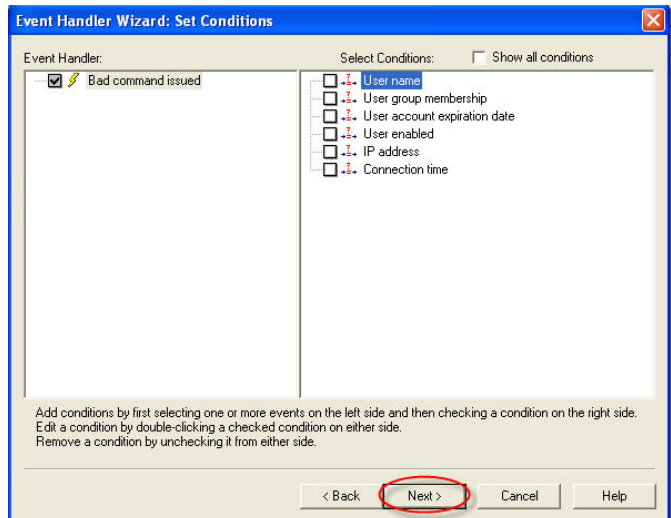
3. Set Events

Select **Bad command issued** using the check box. This option is located on the *Select Events to Handle* menu tree, under *User events, User login attempt failed*. Click **Next**.



4. Set Conditions

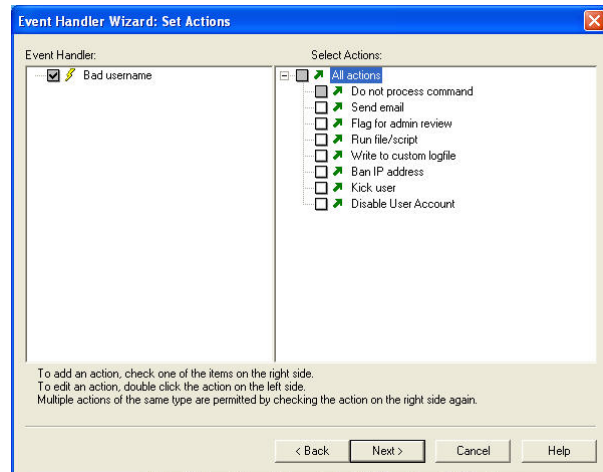
To use this event to thwart hackers you want to capture *all connection attempts*, so do not specify any conditions. Click **Next**.



5. Set Actions

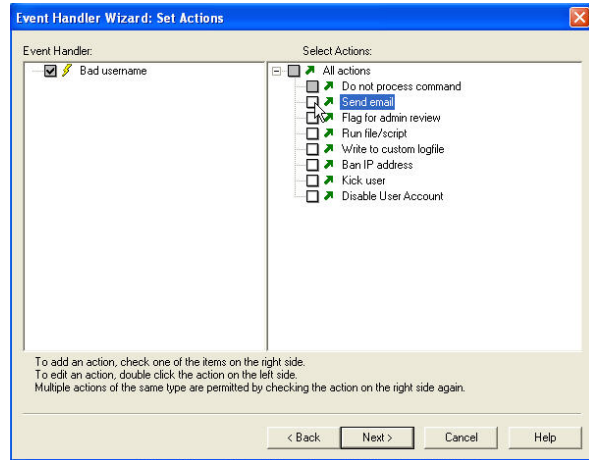
You will set up three separate actions that will occur when a potential hacking attempt is triggered.

- *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.



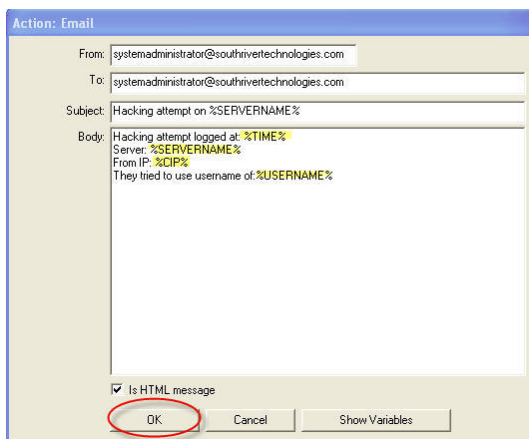
6. *Action: Email*

Select **Send email** using the check box.



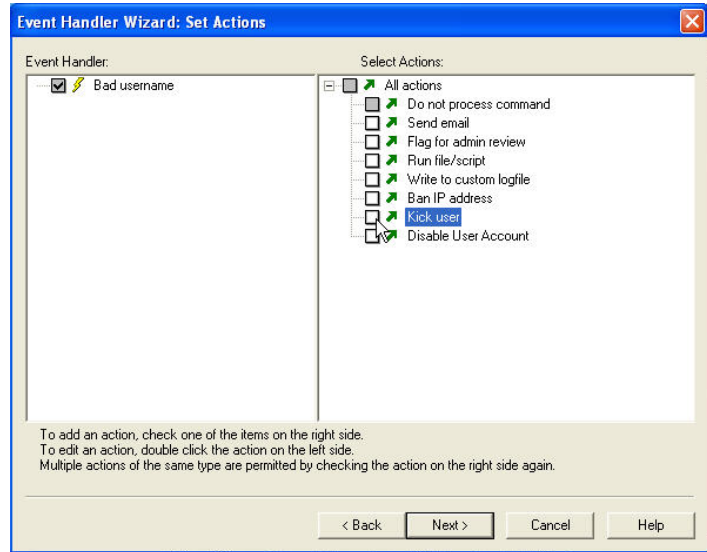
7. Type the **From** and **To email addresses** and **Subject** of the email. In the **Body of the email** it is a good idea to include some details about when the event occurred. We recommend including the **time***, the **server name**, the **IP address of the client**, and the **username** that was 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*, and *username*, use the variables as shown in our example.



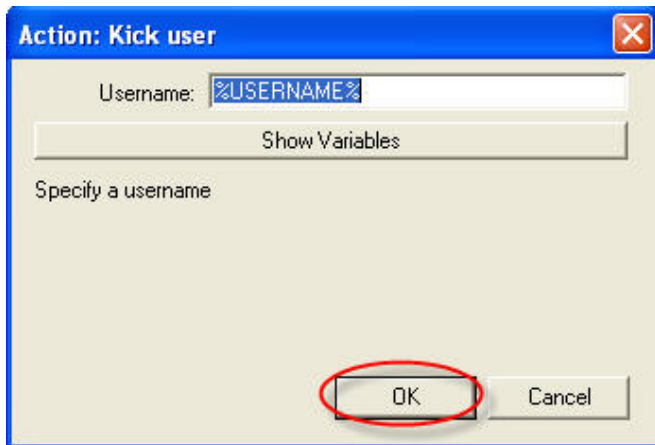
8. Action: Kick User

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



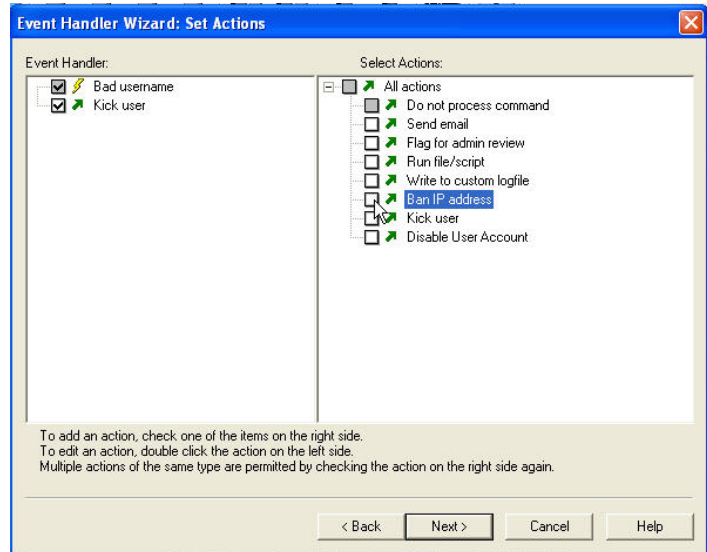
9. The *Kick user* action tells the *Event Manager* to kick this user from the system when the event is triggered.

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



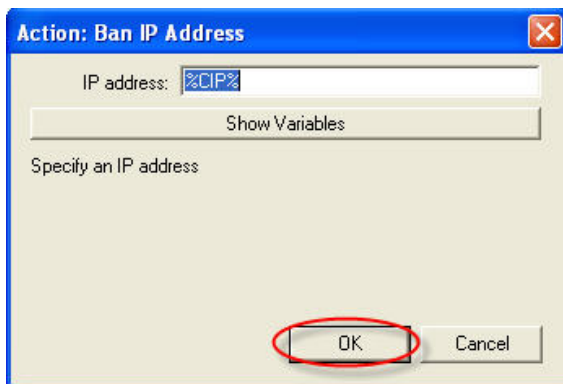
10. Action: Ban IP Address

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

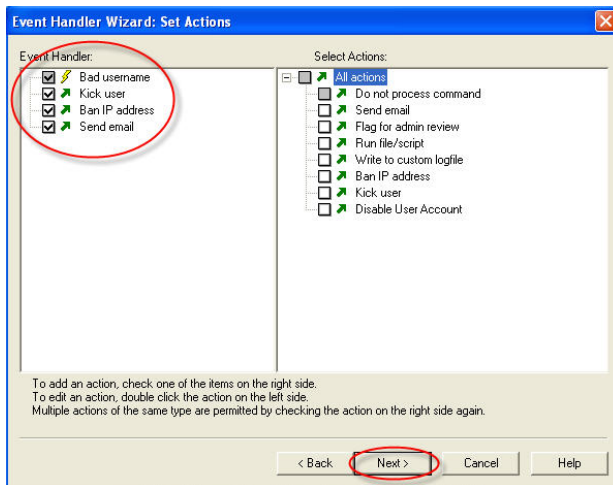


11. The *Ban IP address* action tells the *Event Manager* to add this client IP address to the list of IP addresses that are banned from accessing the server. During this process the *Event Manager* checks to see if the *IP Access Restrictions* feature is enabled at the server level and, if necessary, 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.

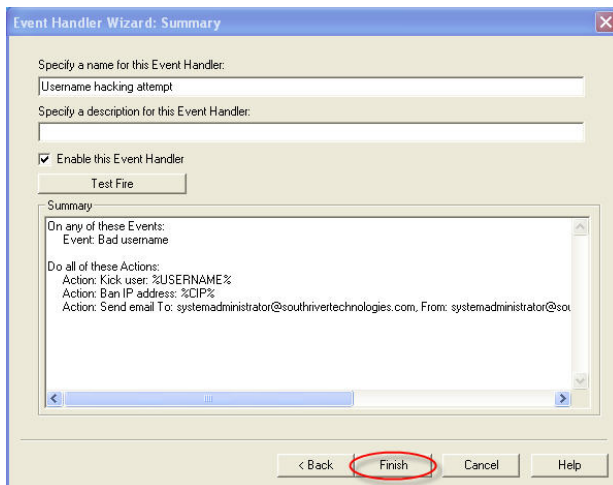
Specify the IP address variable: **%CIP%** and then Click **OK**.



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. The event that you just defined is displayed.

Testing the Event

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

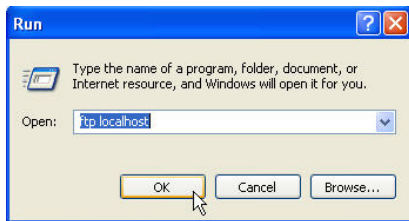
1. O



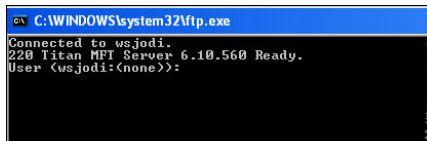
Command Prompt window on the local computer.

2. Type: **ftp localhost**

Click **OK**.

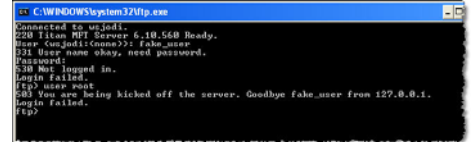


3. The Command Prompt window appears, prompting you to type a user name. Type a **user name that does not exist on the server**. You will then be prompted for your password, type a **fake password**.



4. Try to log on again by typing: **user root**

You will see that you are now kicked off the server.



```

C:\WINDOWS\system32\cmd.exe
Connected to usmjr2.
220 libcom FTP Server 6.10.568 Ready.
User (usmjr2:fake_user): fake_user
331 User name okay, need password.
Password:
530 Not logged in.
Login failed.
ftp> user root
583 You are being kicked off the server. Goodbye fake_user from 127.0.0.1.
Login failed.
ftp>
  
```

5. To test the Ban IP action, quit the current FTP session and then, from the Command Prompt, open a new session by typing: **ftp localhost** You will receive a message indicating that you are now connected to the server and then the connection will be terminated because the server has banned access from your IP address.



```

C:\WINDOWS\system32\cmd.exe
C:\>ftp localhost
Connected to usmjr2.srt.
220 Service ready for new user.
User (usmjr2.srt:(none)): unknown_user
331 User name okay, need password.
Password:
530 Not logged in.
Login failed.
ftp> user root
Connection closed by remote host.
ftp> quit

C:\>ftp localhost
Connected to usmjr2.srt.
Connection closed by remote host.

C:\>_
  
```

6. Launch the *Cornerstone MFT Administrator*. From the *Cornerstone MFT Domains* menu tree, select the **server**, and then select **Connections**. Use the left/right arrows to view the *IP Access* tab. The banned IP Address now shows in the window.
7. To clear this IP Address from the banned list, select **the IP Address** and Click **Delete**.
8. Click **Apply** to apply the change.

About South River Technologies

South River Technologies (SRT) is an innovator in managed file transfer and basic content services 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.

Cornerstone MFT is a registered trademark of South River Technologies, Inc.

© Copyright South River Technologies, 1996-2010. All rights reserved.