

2017

Strategies for Thwarting Hackers

Instructions for defending against hacking attempts using Events Management in a Cornerstone MFT Server environment.

QuickStart Guide

© 2017 South River Technologies, Inc.
All Rights Reserved



Thwarting Hacking with Events Management

Unauthorized users or hackers attempting to guess usernames and passwords in order to gain access are some of the most common dangers to servers. Cornerstone MFT Event Management can help thwart them by detecting invalid user attempts. Cornerstone MFT will kick that connection from the server and ban future access from the client IP address.

The following instructions will help you set up a Cornerstone MFT Server to defend against hackers using the built-in Event Management functions. For more support, please refer to our online guide repository here: <http://webdrive.com/product-support/cornerstone-mft/>, or our HelpDesk: <http://srthelpdesk.com>.

Enacting these three actions using the Cornerstone MFT Event Manager will trigger in the event of a hacking attempt and will help protect your server from being compromised:

- **Send Email**
- **Kick User**
- **Ban IP Address**

Event Management Best Practices

The Event Management actions are only a few ways 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 valid users may be banned from the system because of user error.

Configuring the Event Handler

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

You will use the Cornerstone MFT Administrator to configure your Event Handler. Expand the server you would like to modify from the left-hand tree view and select Events. Click Add to add the event. The Cornerstone MFT Event Handler Wizard will launch. The Event Handler Wizard will allow you to add events and conditions and actions for those events.

NOTE: For more information about setting up a new server or specific configuration options available in the Cornerstone MFT Wizard, see the Cornerstone Administrator's User Guide or visit our Knowledgebase Support Center.

1. **Add Events** – In the Event Handler Wizard: Set Events Wizard, expand User Events and check

the “User login attempt failed” option to enable it. Click Next.

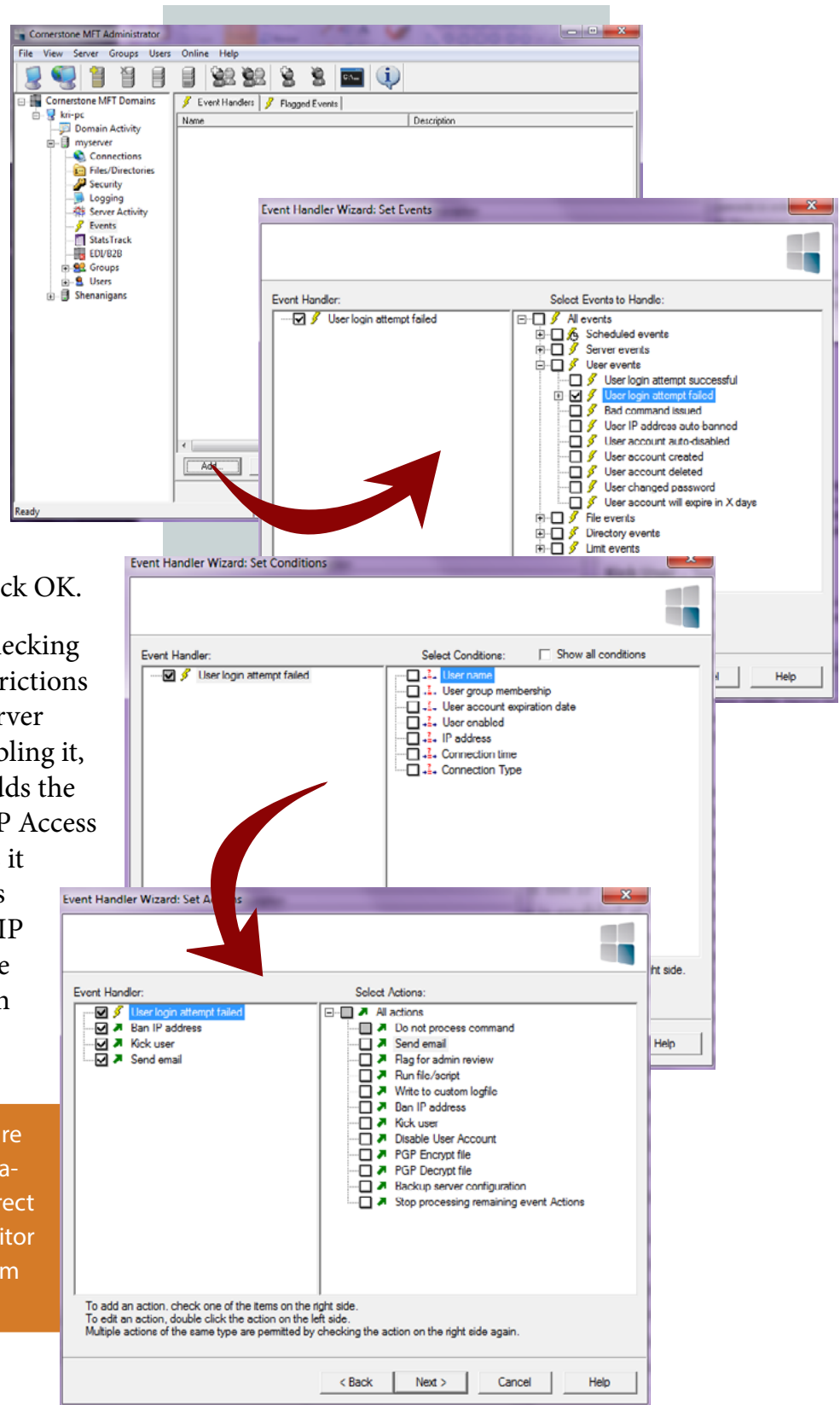
2. **Set Conditions** – To use the “login attempt failed” event to thwart hackers, you want to capture all connection attempts; do not specify any conditions. Click Next.

3. **Set Actions** – Enable the following actions to protect against potential hacking attempts:

- **Kick User** – Terminates the current connection session and prevents the user from issuing another USER command. When you select this, a dialogue box will appear. Keep the default %USERNAME% setting and click OK.
- **Ban IP address** – After checking to see if the IP Access Restrictions feature is enabled at the server level and, if necessary, enabling it, 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. Leave the default %CIP% entry in the dialogue box that appears.

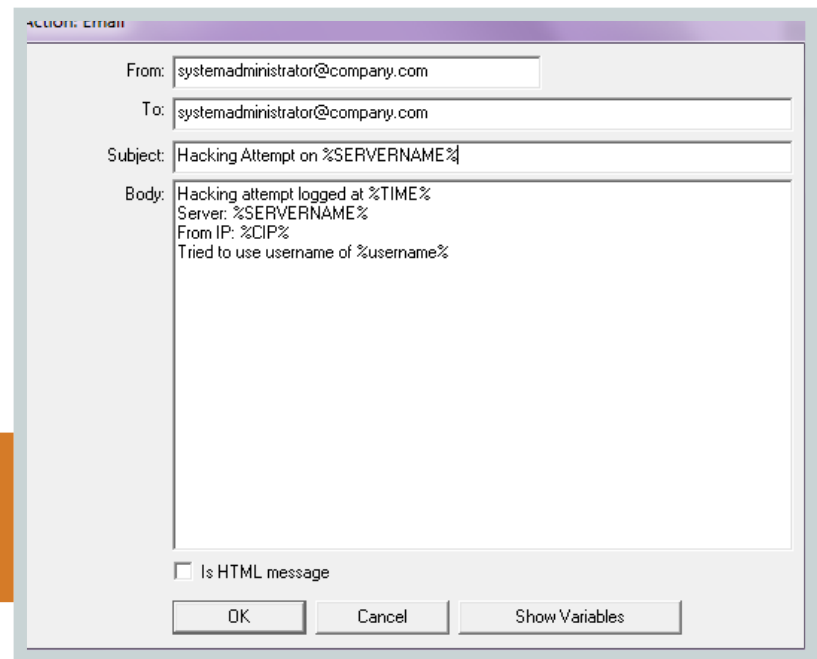
WARNING: Please note that this feature may potentially ban good users permanently if they accidentally enter incorrect information. Take precautions to monitor banned IP addresses closely and inform users.

- **Send Email** – Notifies the



server administrator each time the event is triggered. The server administrator can then double check to make sure a valid user was not banned from the system. Select Send Email and enter the From and To email addresses and the Subject of the email. You may want to include details about when the event occurred in the body of the email. 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.

NOTE: To include the time, server name, IP address, and username, use the variables as shown in our example.



4. Now that you have defined your actions, your Event Handler list should look like our example. Click Next.
5. Type a name for this Event Handler; you may also enter a 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.

The event you just defined should be displayed.

Testing Events

To properly test events, log onto the server using an invalid user name.

1. Open a Run Prompt window on the local computer (Start>Run).
2. Type “ftp localhost” and click OK.
3. The Command Prompt window should appear, prompting you to type a username. Type a username that does not exist on the server. You will then be prompted for your password. Enter a fake password.

NOTE: Cornerstone MFT Server will ask for a password even when a username doesn't exist in the system. This is an added security feature to prevent hackers from fishing for valid usernames.

4. Try to log on again by typing “user root.” You will see that you are now kicked from the server.
5. To test the Ban IP action, quit the current FTP session and, 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. The connection will then be terminated because the server has banned access from your IP address.

- To clear this IP address from the banned list, launch the Cornerstone MFT Administrator. From the Cornerstone left-hand tree view, select the server and Connections. Use the left/right arrows to view the IP Access tab. The banned IP Address now shows in the window. Select the IP Address and Click Delete. Click Apply to apply the change.

System Requirements

Supported Operating Systems

- Windows Server 2012, all editions, 32-bit and 64-bit
- Windows Server 2008-R2, all editions, 32-bit and 64-bit
- Windows Server 2008, all editions, 32-bit and 64-bit

Minimum Hardware Requirements

- 2 GHz Pentium® class processor
- 4GB of RAM is required; 8GB of RAM is recommended
- Minimum 100MB of free disk space for the application
- Minimum SVGA (800x600) resolution display is required to run the Administration console program.

Minimum Software Requirements

- Microsoft .NET Framework v4.0 is required
- Microsoft SQL Server 2005 or later is required
- Microsoft SQL Server Management Studio Express is recommended

Limitations

- Cornerstone MFT server is a multi-threaded, dynamic server solution for the Microsoft Windows operating system. While designed to handle an unlimited number of user connections and servers, like all software, Cornerstone is limited by the resources of the computer; most notably, those limitations imposed by the Windows Sockets (WINSOCK) Library.

About South River Technologies

South River Technologies (SRT) is an innovator in secure file management software. SRT software allows users to securely access, manage, and collaborate on files over the Internet, streamlining business processes to improve productivity. SRT's products enhance customers' existing applications by instantly enabling secure access and collaboration within those applications. More than 90,000 customers in 140 countries use 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. South River Technologies, Cornerstone MFT, Titan FTP Server, WebDrive, and DMZedge Server are registered trademarks of South River Technologies, Inc. in the U.S. and other countries. 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.

Contact Information

South River Technologies, Inc.
1910 Towne Centre Blvd
Suite 250
Annapolis, Maryland 21401
USA

Toll Free: 1-866-861-9483
Main: 443-603-0290
Fax: 410-266-1191
Corporate Web site: www.southrivertech.com
Online Support: www.srthelpdesk.com