Motivate Systems®

Lockout Inspector Administration Guide

Version 1.2

IMPORTANT:

Information in this document is subject to change without notice.

ALL SOFTWARE AND ASSOCIATED MATERIAL DISTRIBUTED BY MOTIVATE SYSTEMS IS PROVIDED “AS IS” WITH NO WARRANTY OR GAURANTEE. MOTIVATE SYSTEMS SHALL NOT BE ACCOUNTABLE FOR ANY MISINTERPETATION OR ERROR RELATED HEREIN.

Product names referenced herein may be trademarks of other companies. Motivate Systems is a registered trademark of Motivate Systems LLC.

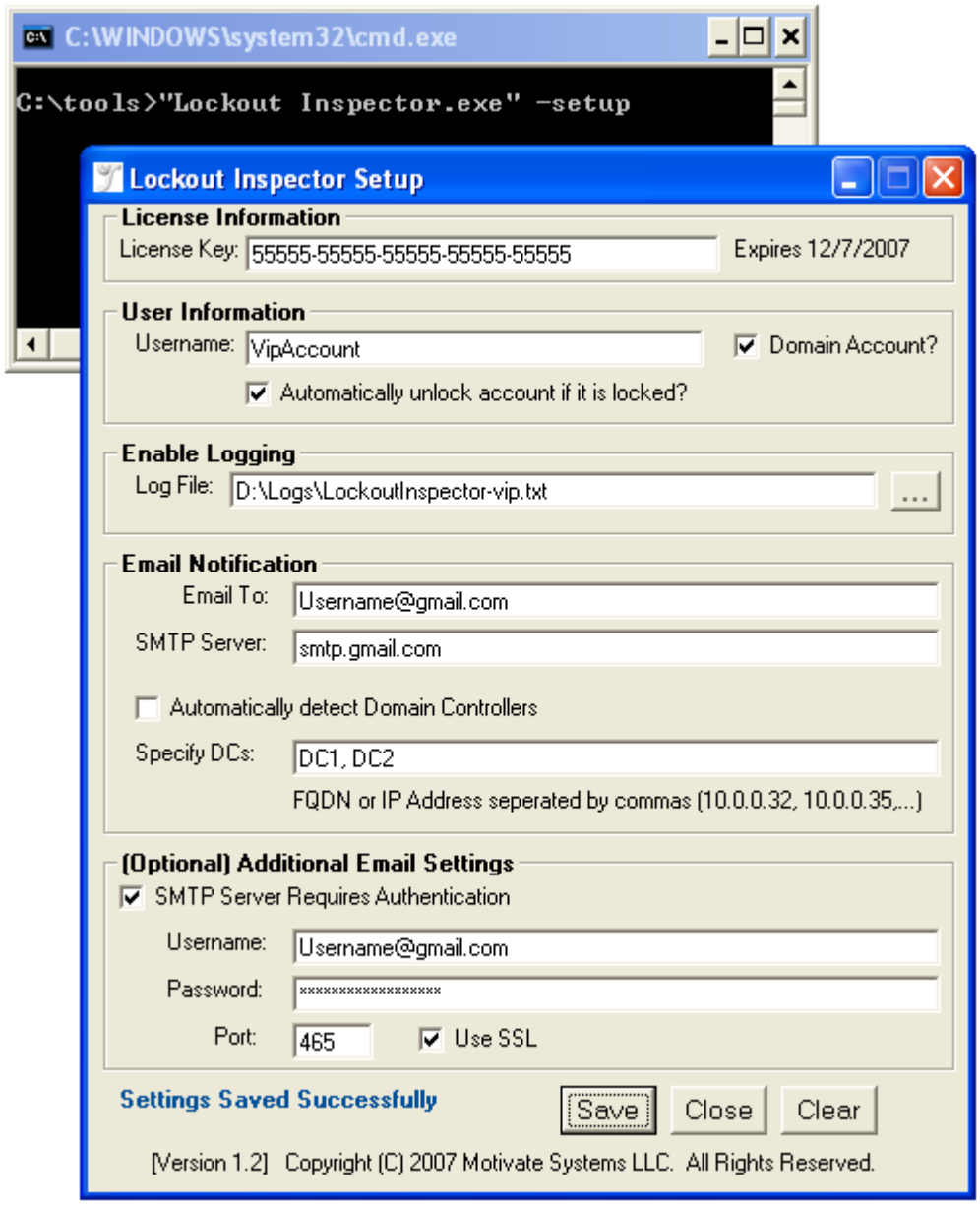
Copyright (C) 2007 by Motivate Systems LLC. All Rights Reserved

Table of Contents

Copyright (C) 2007 by Motivate Systems LLC. All Rights Reserved

I. Entering Setup Mode:

To enter setup mode, simply double click the Setup.bat file or run “Lockout Inspector.exe” from the command line using the –setup flag. For example:



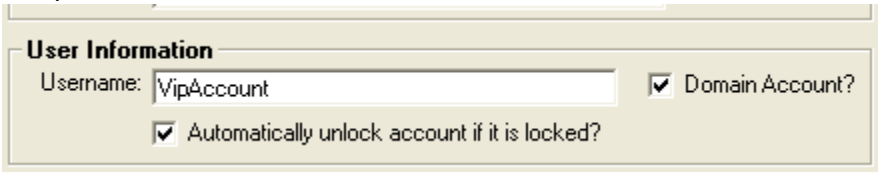
This will launch the Graphical User Interface as shown above. The figure above contains valid settings for all fields (with the exception of a valid license key). A valid license key can be obtained from www.MotivateSystems.com.

Copyright (C) 2007 by Motivate Systems LLC. All Rights Reserved

II. Setting Required Values

License Key
Lockout Inspector provides a fully functional time limited evaluation with no restrictions. After the evaluation period expires, you can continue to use Lockout Inspector by purchasing a license key from www.MotivateSystems.com.

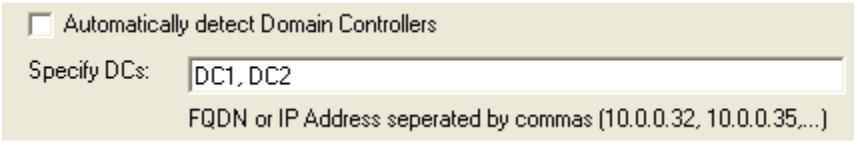
User Information
Enter the username for Lockout Inspector to monitor. This can be a local user account or a domain account. If specifying a domain account, Lockout Inspector is required to run on a computer that is a member of the domain in which the account resides.



To have Lockout Inspector automatically unlock the account, be sure to check this option.

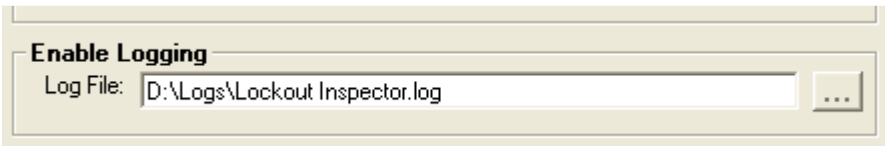
Caution: Use this feature wisely. Lockout policies are set for a reason; to provide a layer of security against brute force attacks against your user account database. Only use this option after you have determined that the source of the lockout is trusted (but currently broken). Use this option as a temporarily workaround until the source can be remedied.

Domain Controller Selection
By default Lockout Inspector will parse the event logs on all Domain Controllers in your domain. If you do not want to parse all DCs, then uncheck the automatic detection setting and specify only the DCs you wish to parse. This is particularly useful when DCs are located at remote sites.



III. Setting Optional Values

Enable Logging
Lockout Inspector will record each time the user account is found locked. To enable logging, specify the file path of the log file. (You must have write permission in the location.)

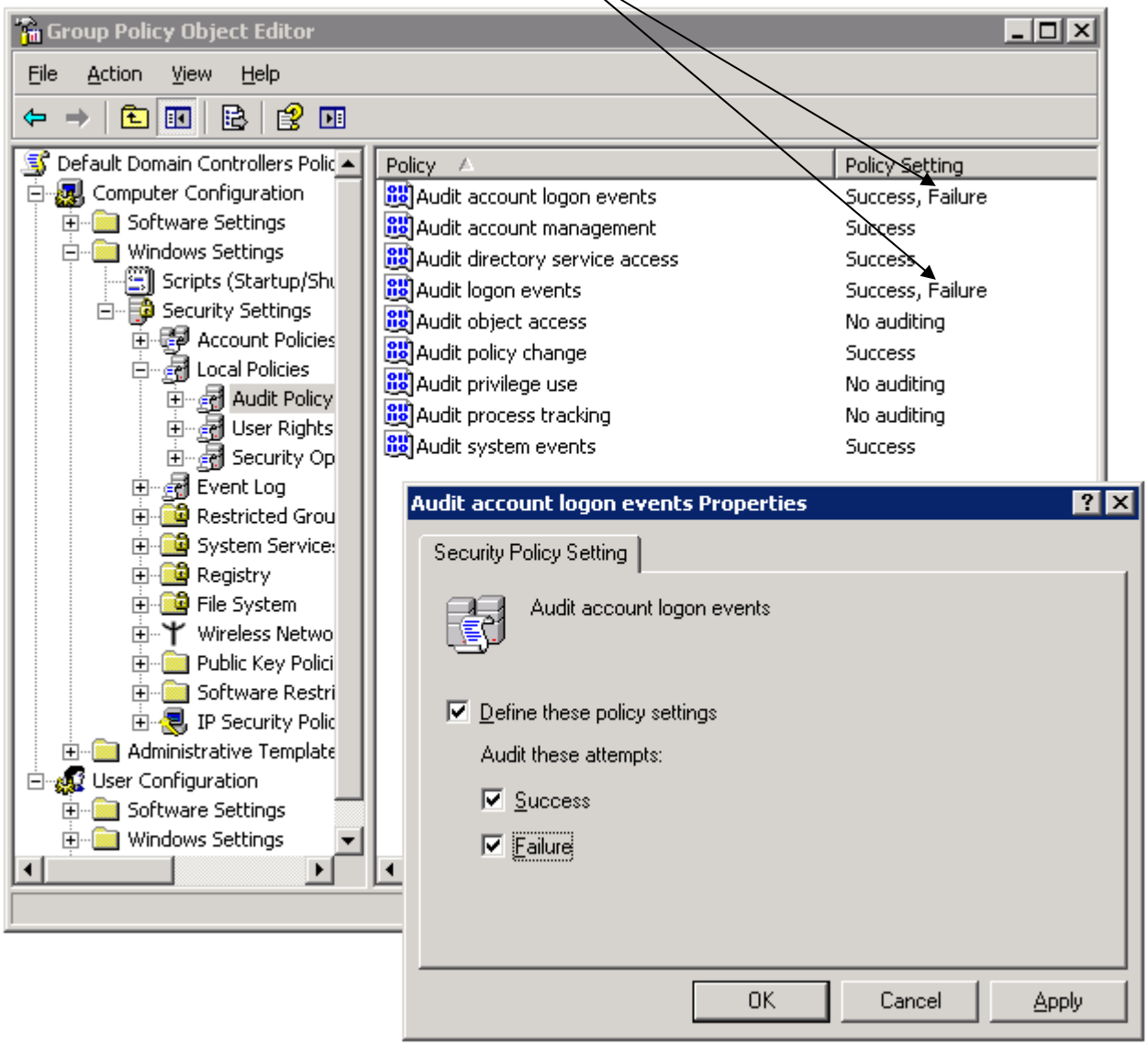


Copyright (C) 2007 by Motivate Systems LLC. All Rights Reserved

Email Notification

To receive alerts by email, enter your email address and a SMTP server. We recommend that you use an internal SMTP server that does not require authentication.

When email notifications have been enabled, Lockout Inspector will send you all recent failed logon events by the user account. In order to receive this information, you must enable auditing for logon event failures. Enable failure auditing for both Audit Account Logon Events and Audit Logon Events. (See the figure below.)



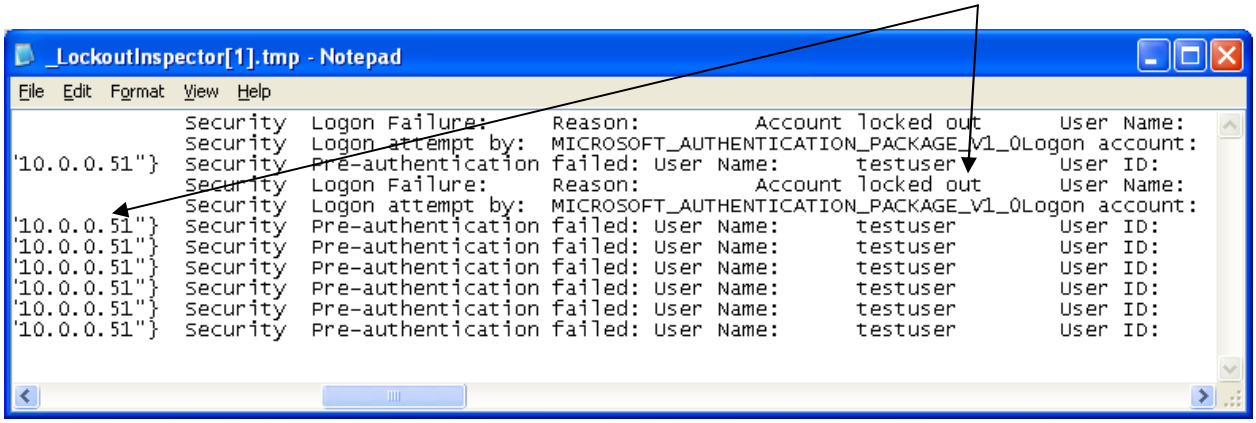
Copyright (C) 2007 by Motivate Systems LLC. All Rights Reserved

IMPORTANT:

- When using Lockout Inspector in a Domain, you must configure the audit policy for the ***Domain Controllers Default Policy.*** (In domain mode, Lockout Inspector parses the event logs on the Domain Controllers.) Launch the Group Policy editor from the Active Directory Users and Computers snap-in.

- When using Lockout Inspector on a standalone computer, click Start->Run then type gpedit.msc. This will launch the ***Local Security Policy*** editor.

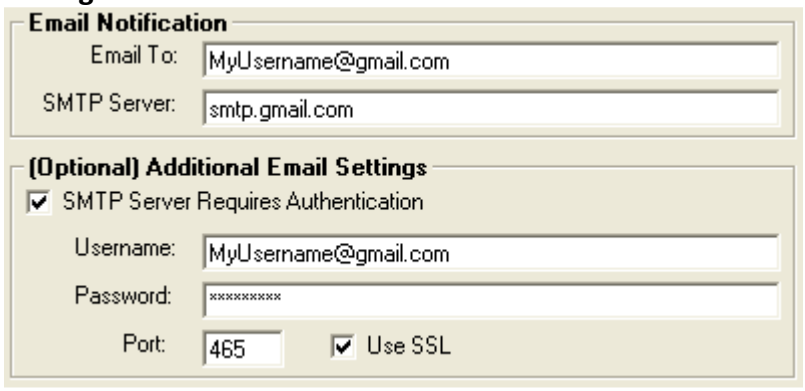
With the appropriate auditing and email notification set, you will receive an attachment by email similar to the figure below. Using this information, you can easily view the IP Address associated with several failed authentication attempts until the account is finally locked out.



Additional Email Options

To use an external SMTP server, the additional email fields may be needed. The following examples show the configuration needed for common external email vendors:

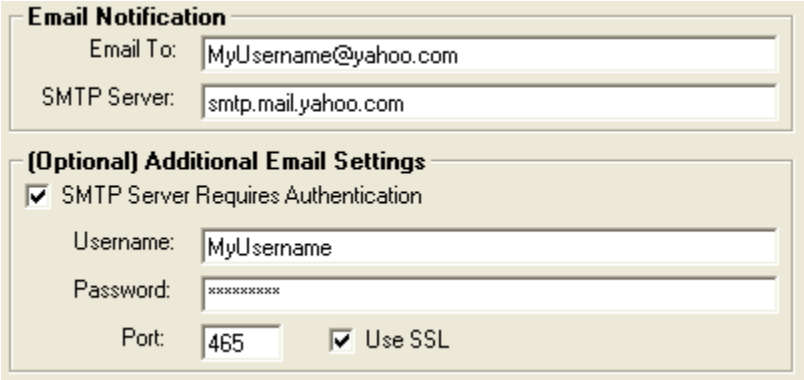
Settings for GMAIL:



Note: Username is your full email address.

Copyright (C) 2007 by Motivate Systems LLC. All Rights Reserved

Settings for Yahoo! Mail

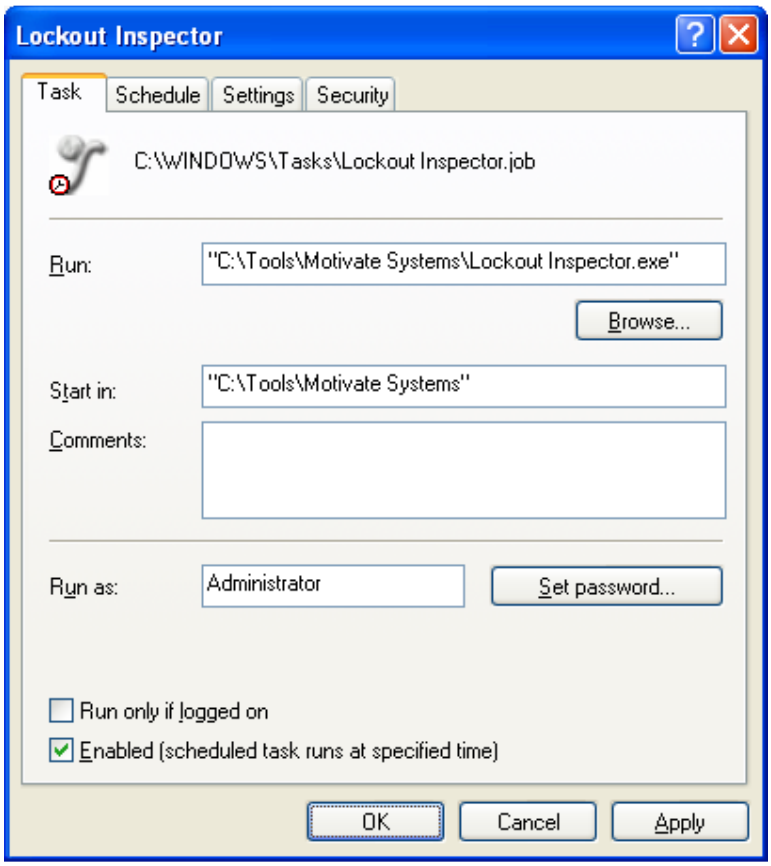


Note: Username is your email address without the "@yahoo.com".

IV. Scheduling

Lockout Inspector utilizes Windows Scheduled Tasks to run at any interval that you specify. After you have configured Lockout Inspector, configure a New Scheduled Task.

Start->Programs->Accessories->System Tools->Scheduled Tasks



IMPORTANT: The account used to run the scheduled task, must have enough rights to unlock the user account in the associated domain.

Copyright (C) 2007 by Motivate Systems LLC. All Rights Reserved

Remove Lockout Inspector using -CleanReg

To remove Lockout Inspector, run “Lockout Inspector.exe” from the command line using the –CleanReg flag. This will remove all applicable entries from your system’s registry.

Copyright (C) 2007 by Motivate Systems LLC. All Rights Reserved