



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.

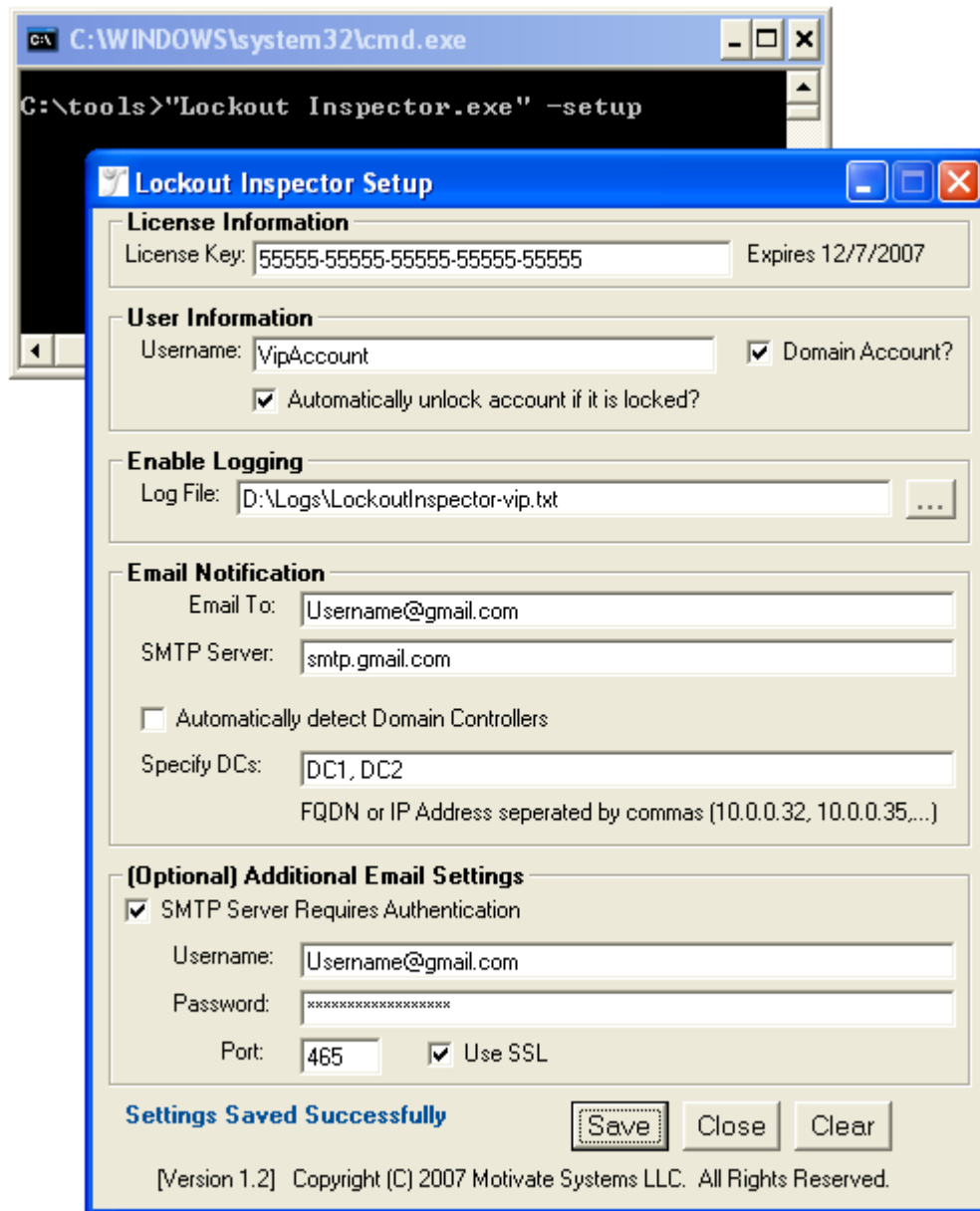
Product names referenced herein may be trademarks of other companies. Motivate Systems is a registered trademark of Motivate Systems LLC.

Table of Contents

- I. Entering Setup Mode**
- II. Setting Required Values**
 - a. License Key
 - b. User Information
 - c. Domain Controller Selection
- III. Setting Optional Values**
 - a. Enable Logging
 - b. Email Notification
- IV. Scheduling**
- V. Removing Lockout Inspector**

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.

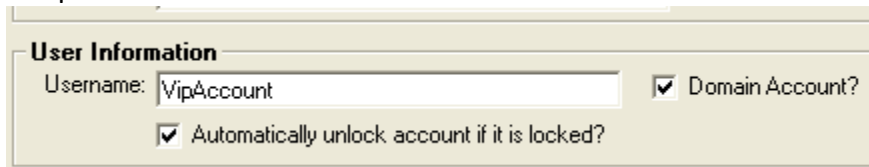
II. Setting Required Values

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.

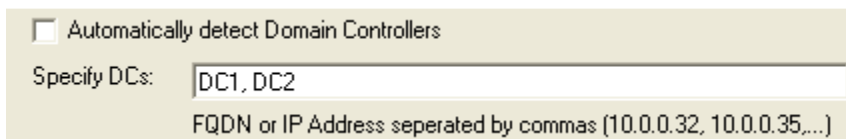
A screenshot of the 'User Information' dialog box. It has a title bar 'User Information'. Inside, there is a 'Username:' label followed by a text box containing 'VipAccount'. To the right of the text box is a checked checkbox labeled 'Domain Account?'. Below the text box is another checked checkbox labeled 'Automatically unlock account if it is locked?'.

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

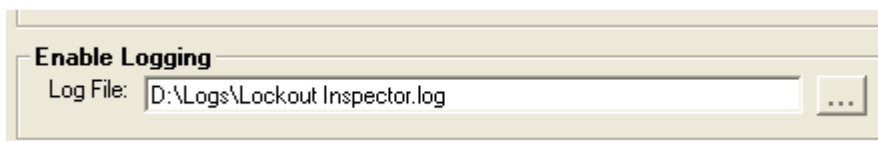
By default Lockout Inspector will parse the event logs on all Domain Controllers in your domain. If you do not want to parse all DCs, then uncheck the automatic detection setting and specify only the DCs you wish to parse. This is particularly useful when DCs are located at remote sites.

A screenshot of the 'Domain Controller Selection' dialog box. It has a title bar. Inside, there is an unchecked checkbox labeled 'Automatically detect Domain Controllers'. Below it is a 'Specify DCs:' label followed by a text box containing 'DC1, DC2'. Below the text box is a small text label: 'FQDN or IP Address seperated by commas (10.0.0.32, 10.0.0.35,...)'.

III. Setting Optional Values

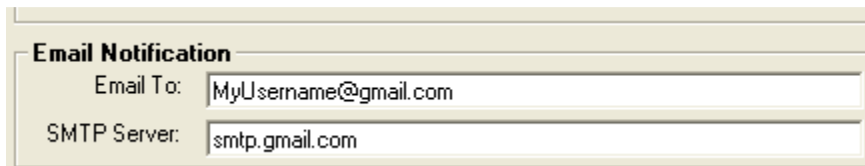
Enable Logging

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.)

A screenshot of the 'Enable Logging' dialog box. It has a title bar 'Enable Logging'. Inside, there is a 'Log File:' label followed by a text box containing 'D:\Logs\Lockout Inspector.log'. To the right of the text box is a button with three dots '...'.

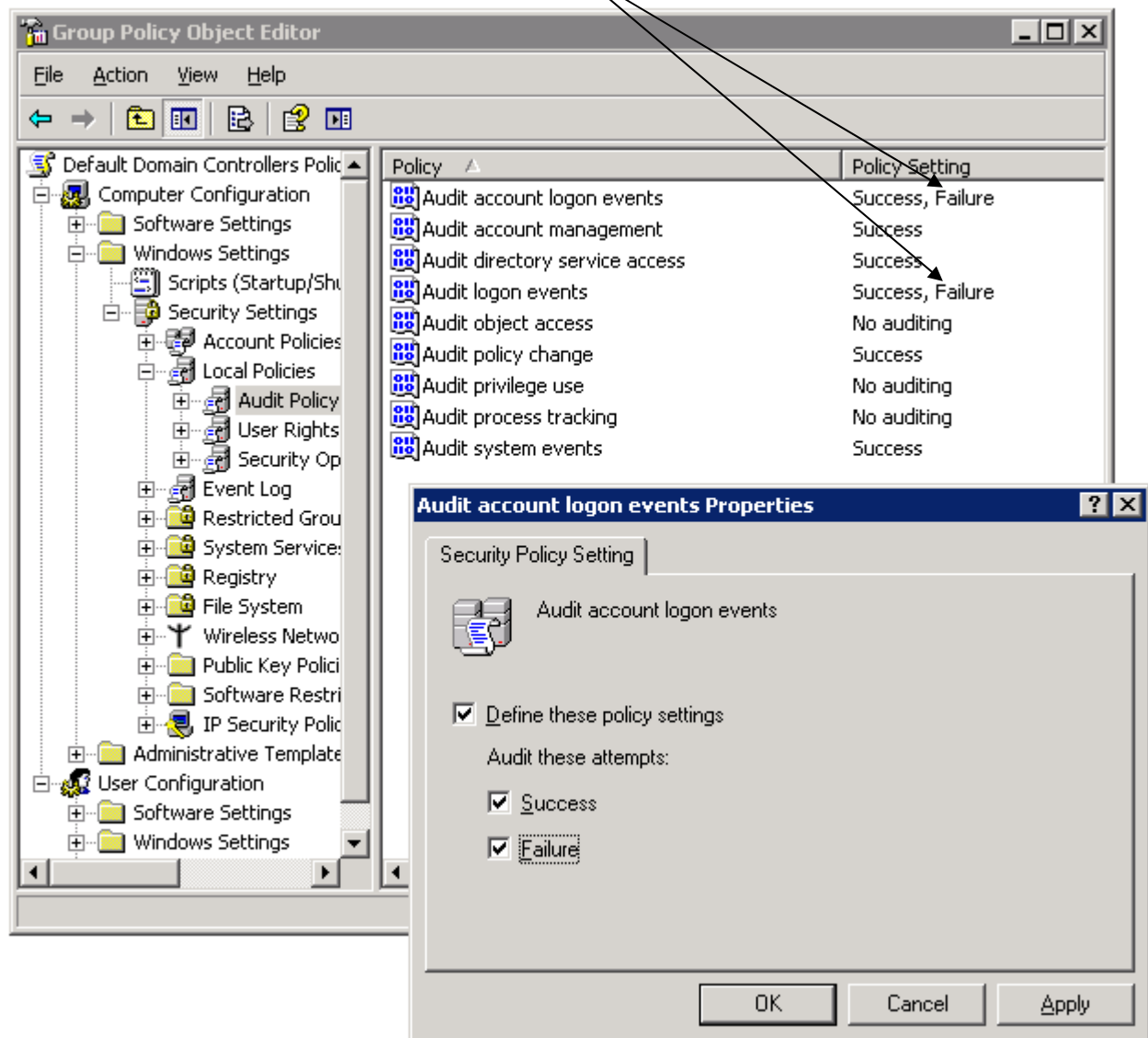
Email Notification

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.



The dialog box titled "Email Notification" contains two input fields. The first field is labeled "Email To:" and contains the text "MyUsername@gmail.com". The second field is labeled "SMTP Server:" and contains the text "smtp.gmail.com".

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.)

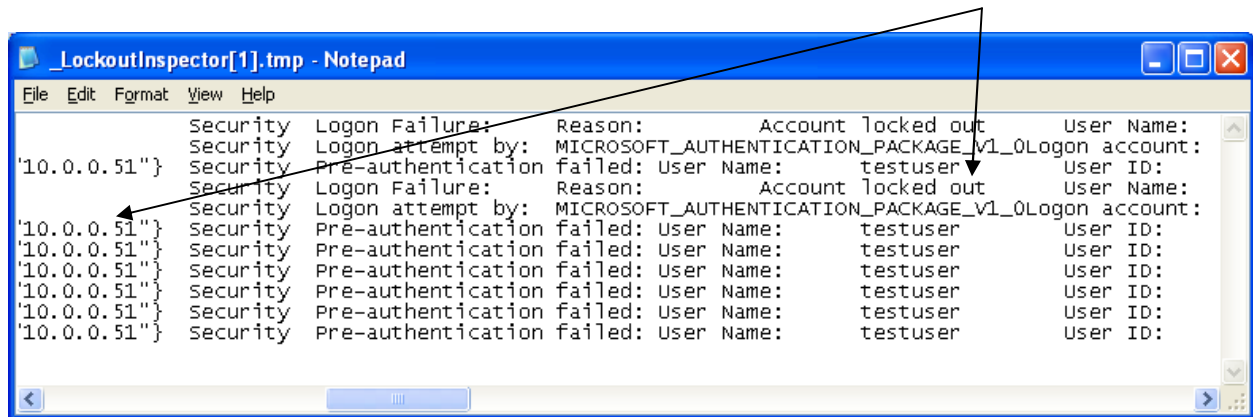


IMPORTANT:

- 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.

- 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:

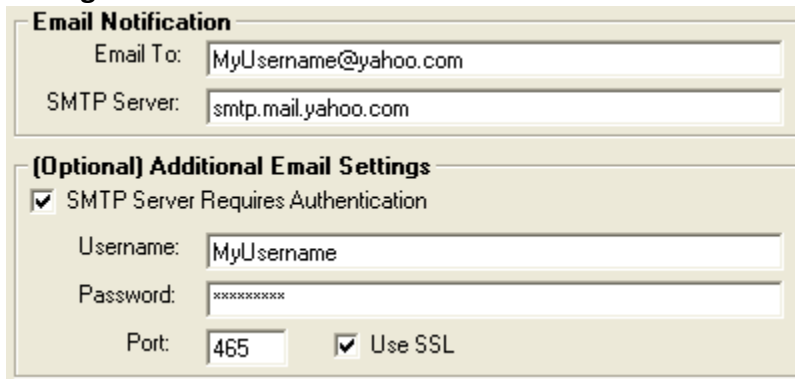
Settings for GMAIL:

Email Notification
Email To:
SMTP Server:

(Optional) Additional Email Settings
☒ SMTP Server Requires Authentication
Username:
Password:
Port: ☒ Use SSL

Note: Username is your full email address.

Settings for Yahoo! Mail



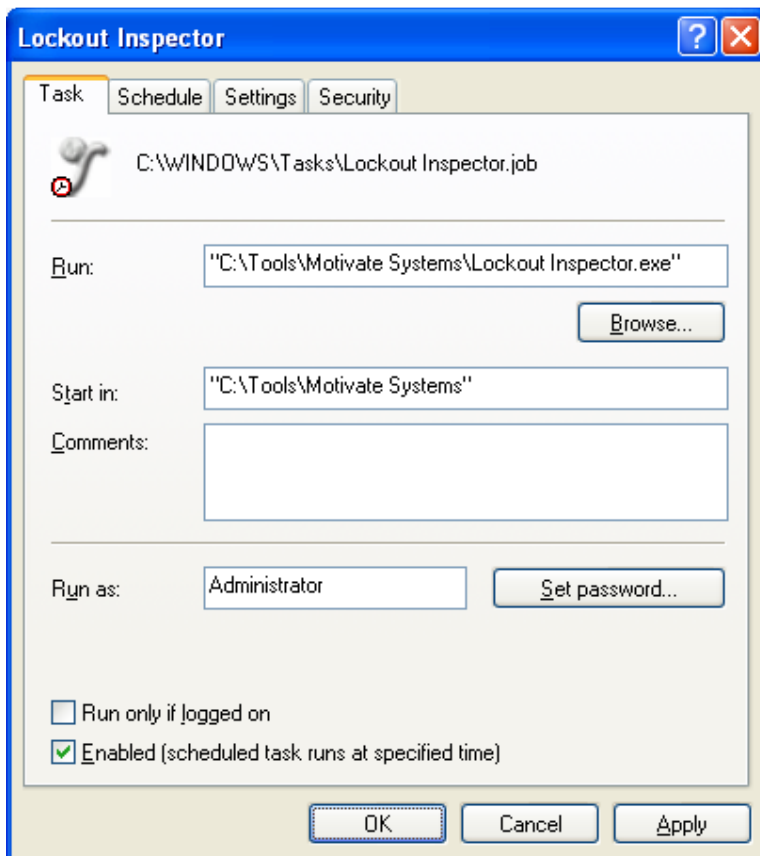
The screenshot shows a settings window titled "Email Notification". It contains two main sections. The first section has two text input fields: "Email To:" with the value "MyUsername@yahoo.com" and "SMTP Server:" with the value "smtp.mail.yahoo.com". The second section is titled "(Optional) Additional Email Settings" and contains four items: a checked checkbox for "SMTP Server Requires Authentication", a "Username:" field with the value "MyUsername", a "Password:" field with the value "*****", and a "Port:" field with the value "465". To the right of the port field is a checked checkbox for "Use SSL".

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



The screenshot shows the "Lockout Inspector" window with the "Schedule" tab selected. The window title bar includes a question mark icon and a close button. The "Task" tab is active, showing a task icon and the path "C:\WINDOWS\Tasks\Lockout Inspector.job". Below this, there are four fields: "Run:" with the value "C:\Tools\Motivate Systems\Lockout Inspector.exe" and a "Browse..." button; "Start in:" with the value "C:\Tools\Motivate Systems"; "Comments:" with an empty text area; and "Run as:" with the value "Administrator" and a "Set password..." button. At the bottom, there are two checkboxes: "Run only if logged on" (unchecked) and "Enabled (scheduled task runs at specified time)" (checked). At the very bottom are three buttons: "OK", "Cancel", and "Apply".

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

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.