LepideAuditor Suite

What's New in Version 16.4.2?

Contents

1. Introduction

This document explains the new additions and enhanced features introduced in the newly released LepideAuditor Suite 16.4.2.

2. New Additions

2.1 Support for SharePoint Server 2016

The new version of LepideAuditor Suite now audits SharePoint Server 2016.

2.2 Account Lockout Reports

The major new addition in the version 16.4.2 is the 'Account Lockout Report.' This report enables you to view the records of all user accounts that are locked out. These records can be filtered down to a granular level as you can see in the below screenshot:

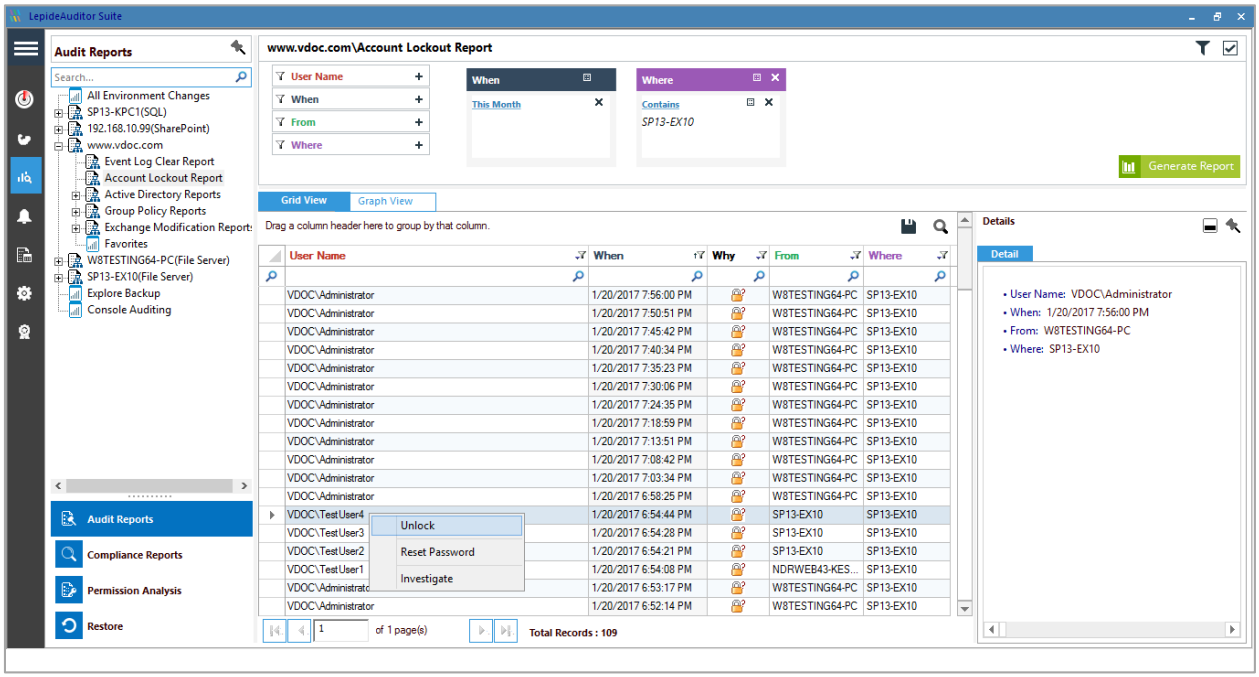

Figure 1: Account Lockout Report

This report allows you to select any particular record of a user account lockout and right click on it to perform any of the following actions:

1. Unlock – This feature lets you unlock the selected user account
2. Reset Password – This feature lets you reset the password of the selected user account. The following dialog box appears on the screen when you click this option

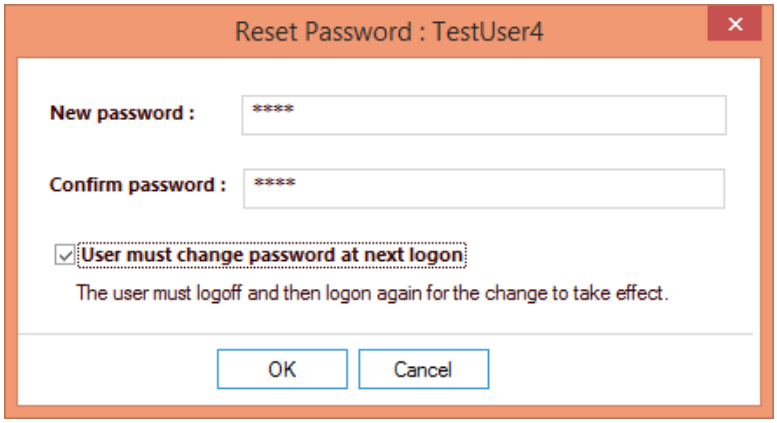

Figure 2: Reset Password

If you want the user to change their already provided password at the next logon, check "User must change password at next logon". If the provided password does not satisfy the conditions set by the previously configured password policies, such as Password History Policy and Password Complexity Policies, the following message box appears on the screen notifying the error:

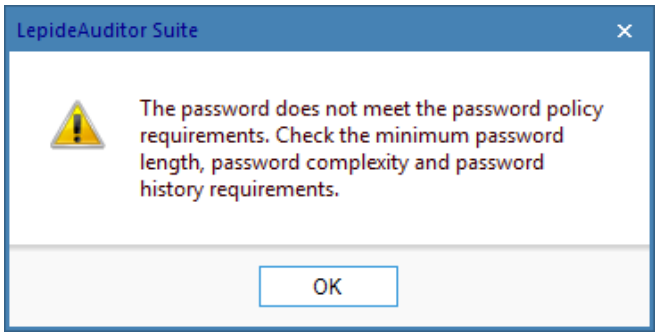

Figure 3: Error while resetting the password

If the password satisfies the conditions of password policies, it will be reset.

3. Investigate – This option allows you to investigate how the selected user account was locked. It checks for the account lockout reasons from COM Objects, Logon Sessions, Mapped Network Drives, Scheduled Tasks and Services.

2.3 Auto-save Scheduled Report on Disk

In addition to sending scheduled repots through email, the new version of LepideAuditor Suite allows you to save the scheduled reports on the selected location periodically, as per the defined schedule. You can also select to send notifications to the required recipients whenever the report is saved on the disk in PDF, MHT or CSV format.

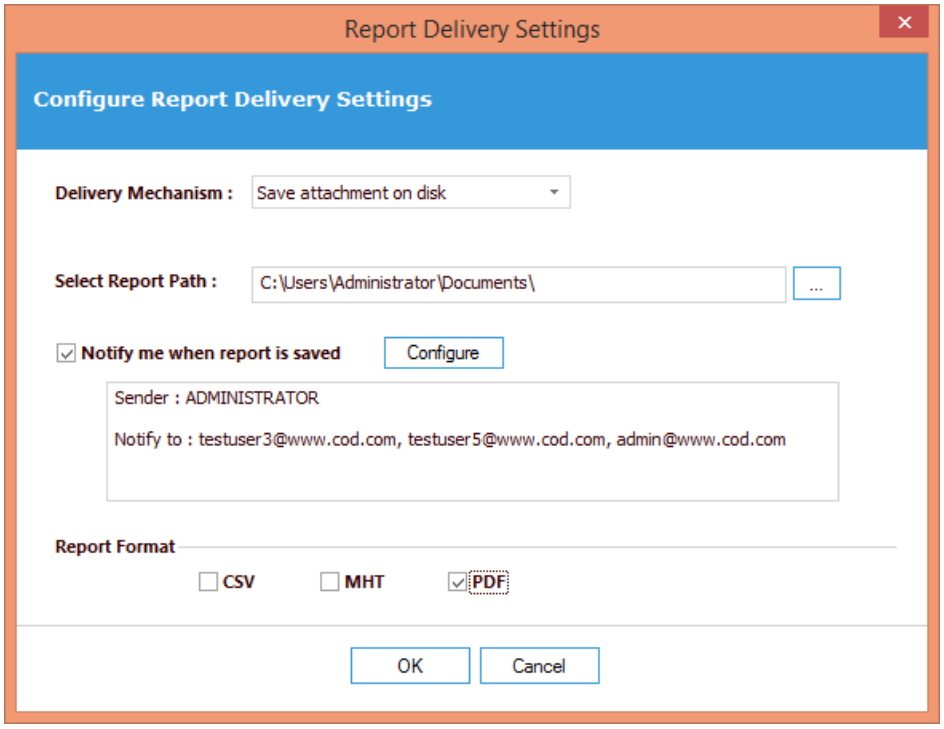

Figure 4: Save the Scheduled Report on disk

We recommend that you save the report at a Shared location, where the selected recipients have required rights to read the files.

2.4 Search Option for Report Names

The "Audit Reports" Tab now provides a search box to let users search the names of Audit Reports and Compliance Reports.

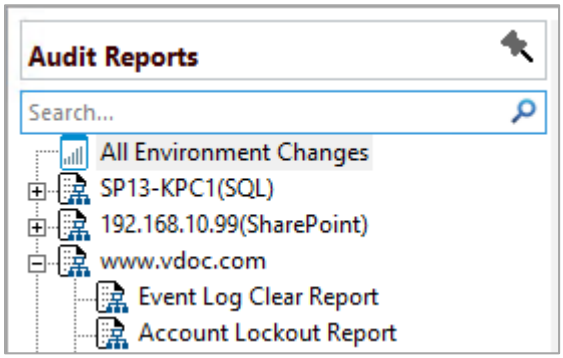

Figure 5: Search Box

This feature allows you to search as you type displaying the search results in real-time when you are typing the keyword.

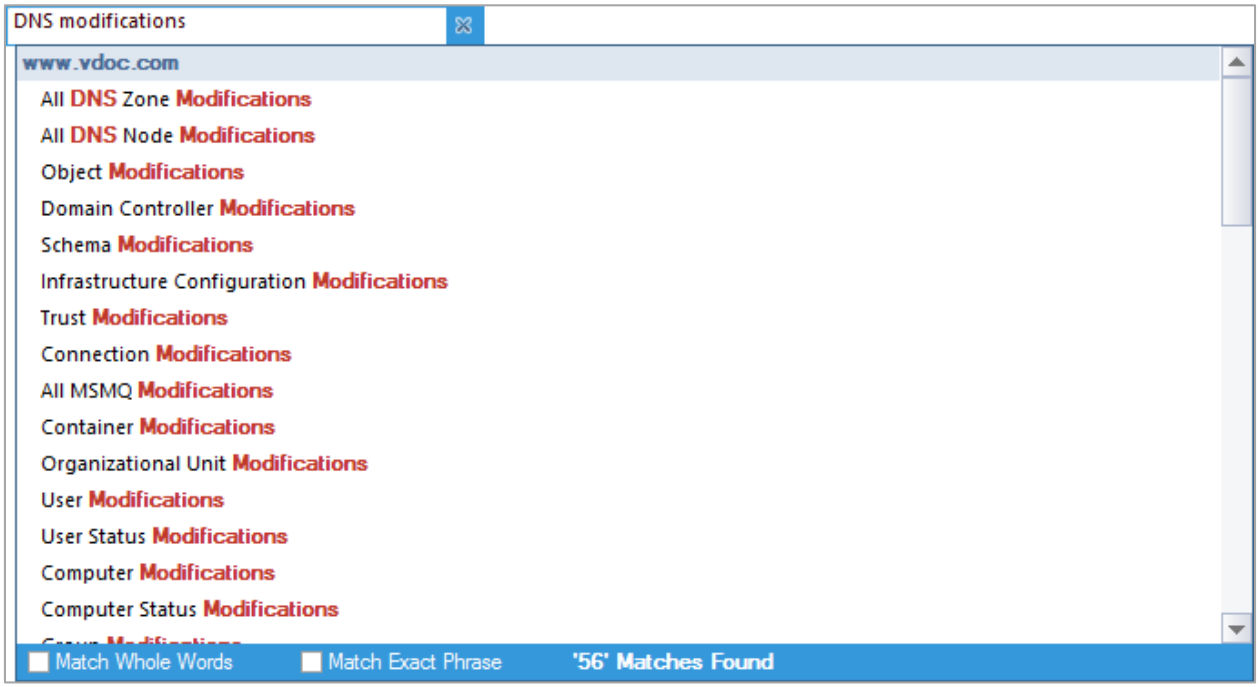

Figure 6: Search Results

2.5 Retention Settings

2.5.1 Retention Settings for Records of Alerts and Scheduled Reports

The records of alerts and scheduled reports will be marked for retention every three hours after their creation whilst the LepideAuditor Suite Service is running or whenever the LepideAuditor Suite Service restarts.

The options for defining the interval after which the records of already sent alerts and schedule reports will be deleted are listed below:

- 7 days
- 15 days
- 30 days
- 60 days
- 90 days

2.5.2 Retention Settings for Backup of State of Active Directory Objects and Group Policy Objects

A complete backup of the state of Active Directory Objects and Group Policy Objects will be marked for retention whenever a further new completed backup is captured by the solution. The available options for defining the intervals are listed below:

- 3 Months

- 1 Year
- 2 Years
- 3 Years
- 4 Years
- 5 Years
- 6 Years
- 7 Years

NOTE: Only complete backup of state of Active Directory Objects and Group Policy Objects will be marked for retention. Their reference backup is not included in the current retention settings.

3. Enhancements

3.1 Monthly Backup of State of Active Directory Objects and Group Policy Objects

In addition to daily and weekly options, the solution now also provides the option to take monthly backups of the state of Active Directory Objects and Group Policy Objects. You can define the preferred day of the month, date and time to take the backup automatically.

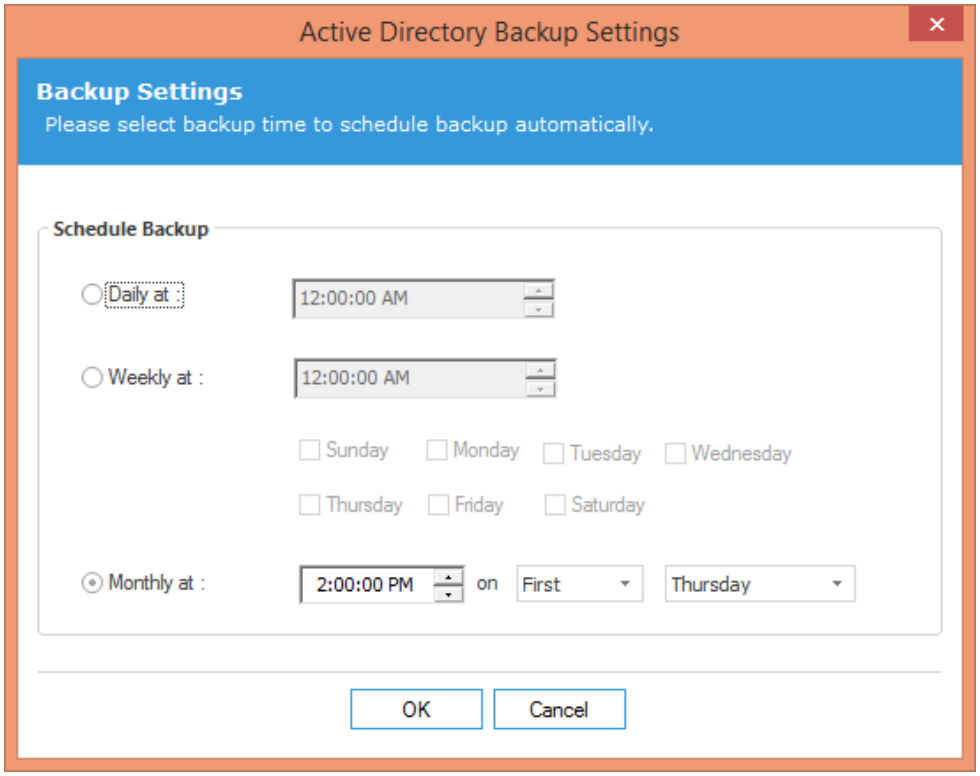

Figure 7: Monthly Backup Option

3.2 Upgraded Group Policy Settings to Enable the Auditing

LepideAuditor Suite now lets you create a new Group Policy at the domain level or at the domain controller level to enable the auditing. You can also select an existing Group Policy to enable the auditing; however, you cannot select the Default Domain Group Policy or the Default Domain Controller Group Policy.

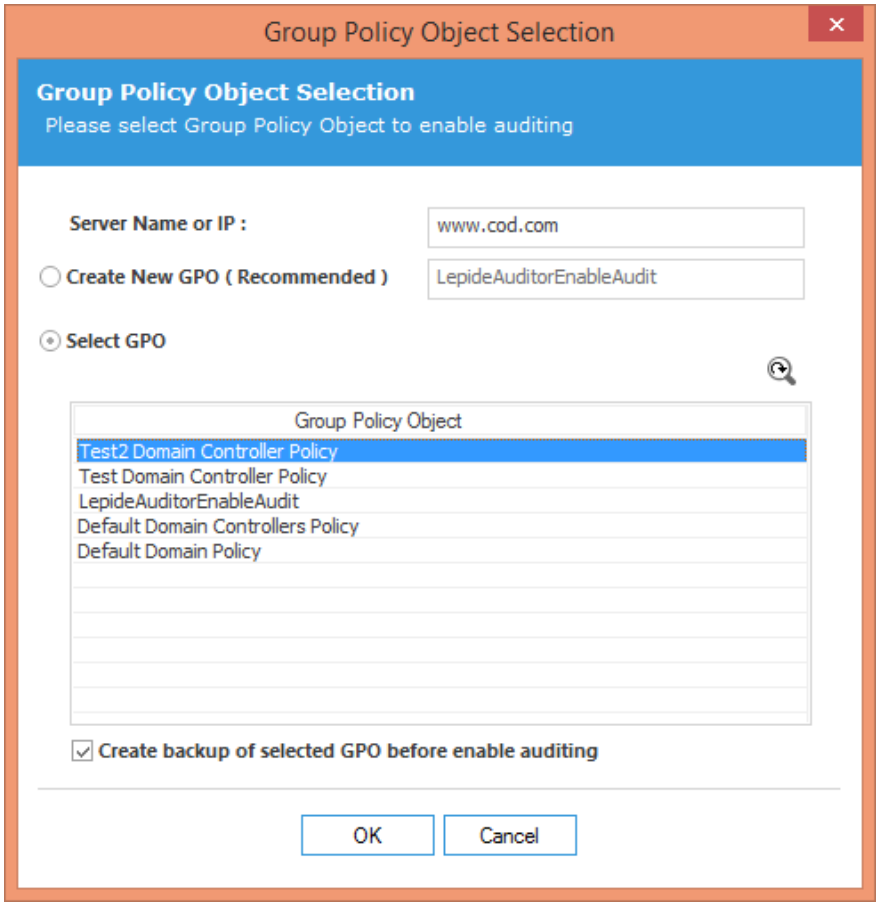

Figure 8: New Options for selecting Group Policies to enable the auditing

When selecting an existing policy, the solution also gives the option to backup the selected Group Policy, which can be used later to revert to that state of Group Policy, which was there before enabling the auditing.

The solution creates a backup of the selected group policy on that server computer, whose IP Address or name has been given in the dialog box, in "%systemdrive%\Windows\Lepide\GPOBKP_24-01-2017 18_13_35\" folder. Here, the "24-01-2017" will be replaced with the date and "18_13_35" will be replaced with the time when you have clicked "OK" to enable auditing using the selected Group Policy.

3.3 Only Agentless SQL Server Auditing

LepideAuditor Suite 16.4.2 now audits SQL Server in agentless mode only. This means no agent will be deployed at SQL Server or installed at the computer where SQL Server is running.

When you are upgrading LepideAuditor Suite to the current version, it automatically uninstalls the agent from SQL Server and requires you to restart the auditing once. If the agent remains installed, the auditing of SQL Server cannot be started. In that case, you have to use "Uninstall Agent" option provided in "Settings" Tab to uninstall the agent.

SQL Server auditing has also been improved with more speed and better accuracy. The removal of auditing agent now does not consume any resource at the server level.

3.4 Updated User Interface of Current Permission Report by User

The "User Interface" of "Current Permission Reports" for shared files or folders has been improved. The simpler interface makes it easier to identify which user has what permissions on selected shared files or folders.

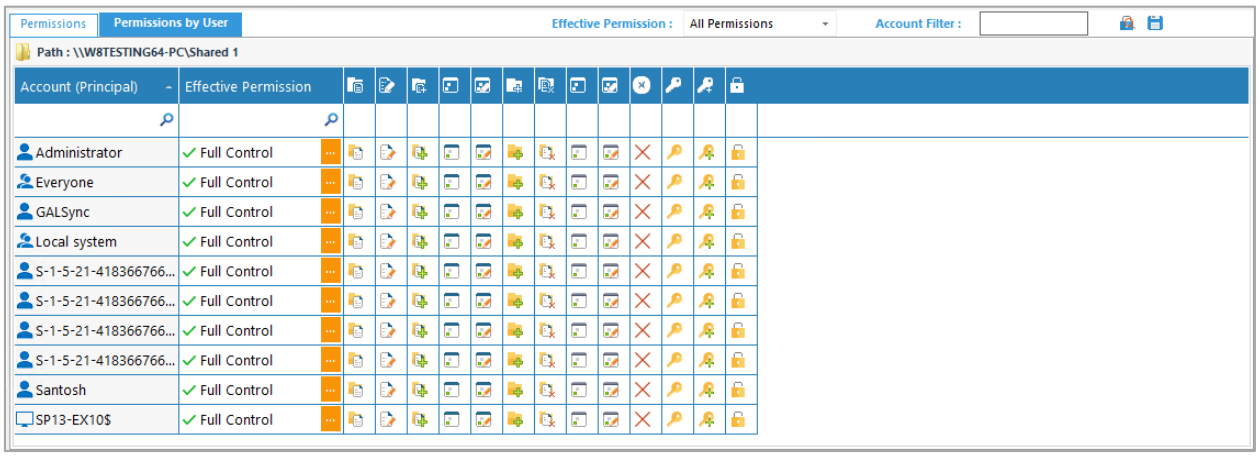

Figure 9: Improved interface of Current Permission Report by Users

3.5 Bug Fixes

Minor bugs fixes offer better functionality.