LEPIDE SOFTWARE

Configuration Guide

This document explains the steps to configure LepideAuditor Suite.

LepideAuditor Suite
A Complete Solution to monitor and audit the Active Directory, Group Policy Objects, Exchange Server, SharePoint Server, and SQL Server

LepideAuditor Suite

Copyright

LepideAuditor Suite, LepideAuditor App, LepideAuditor App Server, LepideAuditor Suite (Web Console), LepideAuditor Logon/Logoff Audit Module, any and all components, any and all accompanying software, files, data and materials, this Configuration Guide, and other documentation are copyright of Lepide Software Private Limited, with all rights reserved under the copyright laws. This user guide cannot be reproduced in any form without the prior written permission of Lepide Software Private Limited. No Patent Liability is assumed, however, with respect to the use of the information contained herein.

Warranty Disclaimers and Liability Limitation

LepideAuditor Suite, LepideAuditor App, LepideAuditor App Server, LepideAuditor Suite (Web Console), LepideAuditor Logon/Logoff Audit Module, any and all components, any and all accompanying software, files, data and materials, are distributed and provided AS IS and with no warranties of any kind, whether expressed or implied. In particular, there is no warranty for any harm, destruction, impairment caused to the system where these are installed. You acknowledge that good data processing procedure dictates that any program, listed above, must be thoroughly tested with non-critical data before there is any reliance on it, and you hereby assume the entire risk of all use of the copies of LepideAuditor Suite and the above listed accompanying programs covered by this License. This disclaimer of warranty constitutes an essential part of this License.

In addition, in no event does Lepide Software Private Limited authorize you or anyone else to use LepideAuditor Suite and the above listed accompanying programs in applications or systems where LepideAuditor Suite and the above listed accompanying programs' failure to perform can reasonably be expected to result in a significant physical injury, or in loss of life. Any such use is entirely at your own risk, and you agree to hold Lepide Software Private Limited harmless from any and all claims or losses relating to such unauthorized use.

Trademarks

LepideAuditor Suite, LAS, LepideAuditor App, LepideAuditor App Server, LepideAuditor Suite (Web Console), LepideAuditor Logon/Logoff Audit Module, LepideAuditor for Active Directory, LAAD, LepideAuditor for Group Policy Object, LAGPO, LepideAuditor for Exchange Server, LAES, LepideAuditor for SQL Server, LASS, LepideAuditor SharePoint, LASP, Lepide Object

Restore Wizard, Lepide Active Directory Cleaner, LADC, Lepide User Password Expiration Reminder, LUPER, and LiveFeed are registered trademarks of Lepide Software Pvt Ltd.

All other brand names, product names, logos, registered marks, service marks and trademarks (except above of Lepide Software Pvt. Ltd.) appearing in this document are the sole property of their respective owners. These are purely used for informational purposes only. We have compiled a list of such trademarks but it may be possible that few of them are not listed here.

Windows XP®, Windows 7®, Windows 8®, Windows 8.1®, Windows 10®, Windows 2000 Server®, Windows 2000 Advanced Server®, Windows Server 2003®, Windows Server 2003 R2®, Windows Server 2008®, Windows Server 2008 R2®, Windows Server 2012®, Exchange Server 2003®, Exchange Server 2007®, Exchange Server 2010®, Exchange Server 2013®, SharePoint Server®, SharePoint Server 2010®, SharePoint Foundation 2010®, SharePoint Server 2013® SharePoint Foundation 2013®, SQL Server 2005®, SQL Server 2008®, SQL Server 2008 R2®, SQL Server 2012®, SQL Server 2014®, SQL Server 2016®, SQL Server 2005 Express Edition®, SQL Server 2008 Express® SQL Server 2008 R2 Express®, SQL Server 2012 Express®, SQL Server 2014 Express® .NET Framework 4.0, .NET Framework 2.0, Windows PowerShell® are registered trademarks of Microsoft Corporation.

Intel and Pentium are registered trademarks of Intel Corporation.

Contact Information

Email: sales@lepide.com

Website: http://www.lepide.com

Table of Contents

1. Introduction

Welcome to the Configuration Guide of LepideAuditor Suite.

This software is a comprehensive solution providing all round audit information and control regarding **Active Directory, Group Policy Objects, Exchange Servers, SharePoint Servers, and SQL Servers.**

In this configuration guide, we have covered the most essential steps to be followed for first time usage of LepideAuditor Suite Software. If you want to view the dedicated Configuration Guides for each component, then click the following links.

1. Configuration Guide for Active Directory, Group Policy, and Exchange Server
    a. Configuration Guide for Active Directory Cleaner
    b. Configuration Guide for User Password Expiration Reminder
    c. Configuration Guide for Enabling Auditing
    d. Configuration Guide for Non-Owner Mailbox Access Auditing
    e. Configuration Guide for Logon/Logoff Audit Module
2. Configuration Guide for SharePoint Server
3. Configuration Guide for SQL Server
4. Configuration Guide for LepideAuditor App

2. System Requirements

Before you start installing LepideAuditor Suite, make sure that your computer meets the following requirements.

2.1 Basic System Requirements

- Dual Core Processor or higher Processor
- Minimum 4 GB RAM
- Required free disk space
    - Minimum 1 GB
    - Recommended 2 GB
- .NET Framework 4.0 or later
- Group Policy for Windows Server 2003
- Any of the following SQL Servers (local or network hosted) for storing auditing logs:

  - SQL Server 2005
  - SQL Server 2008
  - SQL Server 2008 R2
  - SQL Server 2012
  - SQL Server 2014
  - SQL Server 2016
  - SQL Server 2005 Express Edition
  - SQL Server 2008 Express
  - SQL Server 2008 R2 Express
  - SQL Server 2012 Express
  - SQL Server 2014 Express
- Any of the following 32 bit or 64 bit Windows Operating Systems.
  - Windows XP
  - Windows 7
  - Windows 8
  - Windows 8.1
  - Windows 10
  - Windows Server 2003
  - Windows Server 2003 R2
  - Windows Server 2008
  - Windows Server 2008 R2
  - Windows Server 2012
  - Windows Server 2012 R2

2.2 Supported Windows Servers

Any of the following Windows Servers.

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

2.3 Supported Exchange Servers

- Exchange Server 2003
- Exchange Server 2007
- Exchange Server 2010
- Exchange Server 2013

2.4 Supported SharePoint Servers

- SharePoint Server 2010
- SharePoint Foundation 2010
- SharePoint Server 2013
- SharePoint Foundation 2013

2.5 Supported SQL Servers for Auditing

- SQL Server 2005
- SQL Server 2008
- SQL Server 2008 R2
- SQL Server 2012
- SQL Server 2014

2.6 Prerequisites for Windows Server 2003 /R2

Following are the prerequisites to audit Windows Server 2003 and Windows Server 2003 R2 (both 32-bit and 64-bit versions)

- .NET Framework 2.0
- Windows PowerShell 2.0
- GPMC.MSC
- Hotfix of http://support2.microsoft.com/hotfix/KBHotfix.aspx?kbnum=941084&kbln=en-us for Windows Server 2003

2.7 Prerequisites for Domain Auditing

Following are the prerequisites for auditing a domain's Active Directory, Group Policy, and Exchange Server.

- Event Viewer of domain controller(s) and main domain, to be audited, should be accessible.

2.8 Prerequisites for Group Policy Auditing

- Windows PowerShell 2.0 should be installed on server with agent.
- .NET Framework 4.0 should be installed both on server to be monitored and machine where software is installed.
- GPMC should be installed on the machine where software is installed.
- Following are the prerequisites for agentless Group Policy Auditing
  - Software should be installed on client machine.
  - Windows PowerShell 2.0 for client machine

2.9 Prerequisites for Health Monitoring

- WMI Services should be up and running.
- Hotfix of http://support2.microsoft.com/hotfix/KBHotfix.aspx?kbnum=941084&kbln=en-us for Windows Server 2003

2.10 Prerequisites for SharePoint & SQL Server

Following are the prerequisites for auditing SharePoint Server (any version) and SQL Server (any version)

- Microsoft System CLR Types for SQL Server 2012
- Microsoft SQL Server 2012 Management Objects Setup
- .NET Framework 4.0 should be installed both on server to be monitored and machine where software is installed.

2.11 Prerequisites for Web Console

Following are the prerequisites for LepideAuditor Suite (Web Console)

- .NET Framework 4.0 or later for installing LepideAuditor Suite (Web Console)
- Web Browser is required to open Web Console.
  - Internet Explorer 8 or later
  - Mozilla Firefox 20.0 or later
  - Apple Safari 4.0 or later
  - Google Chrome

3. User Rights

To install and work with LAS, you need to have appropriate rights over the system where it will be installed. Also, you need to have appropriate rights to access Active Directory, Exchange Server, SQL Server and SharePoint Server.

3.1 Service Rights

To run LepideAuditor Suite Service, the local system administrator rights are required. If you want to run the service using other user, then the selected user should be member of Domain Admins group.

3.2 Local System Rights

User should have following permissions on local computer on which software is installed:

- Full access permission over drive in which Operating System is installed
- Read/Write permissions in the registry

Steps to assign these permissions are:

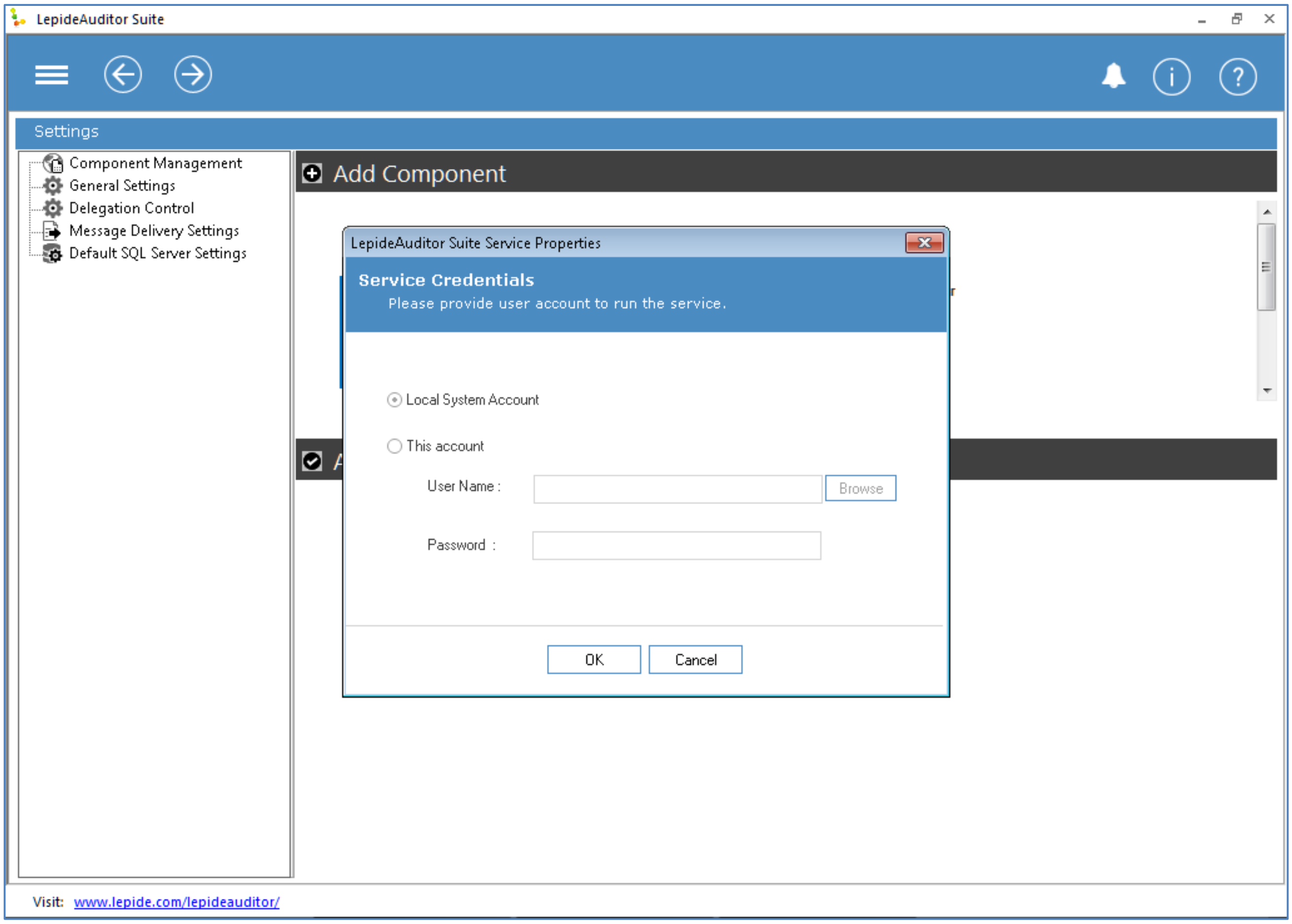
1. Go to Control Panel and select "User Accounts".
2. Select the user and select Change Account Type.
3. Make User as Administrator.
4. Click "Save".

NOTE:

1. Steps mentioned above may vary depending on the Windows version installed on the system.
2. If the User Account does not exist on the system, create a new User Account with Administrative rights.

4. Configure Service Credentials

You can configure this option to select the User Account with which you want to create and run the Windows Service of LepideAuditor Suite. This setting will appear at the Welcome Screen when you are installing the software for the very first time.



LepideAuditor Suite Service Properties

Service Credentials

Please provide user account to run the service.

● Local System Account

○ This account

User Name :

Password :

Figure 1: Configure the credentials

Follow the steps below to configure this option.

1. It contains the following two options.

   A. **Local Account:** Select this option to install and run the LepideAuditor Suite service using the local system account.

   B. **This account:** Select this option to install and run the LepideAuditor Suite service using the provided user account.

2. Select "This Account" for installing and running the service with a customized account.

NOTE: Right click on "Component Management" node in "Settings" tab to access the option to configure the service credentials.

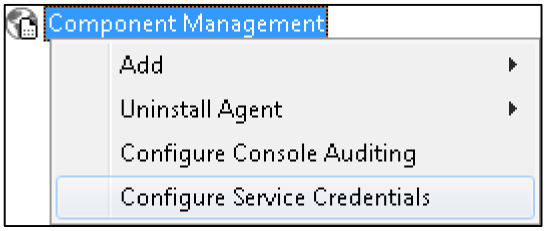
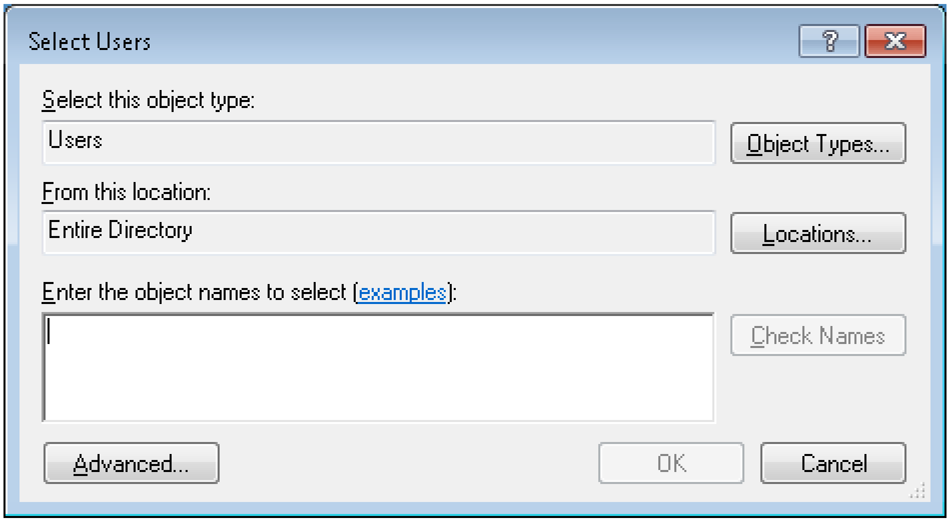


Figure 2: Option to access Service Credentials

3. You can click "Browse" to select a user account from Active Directory.



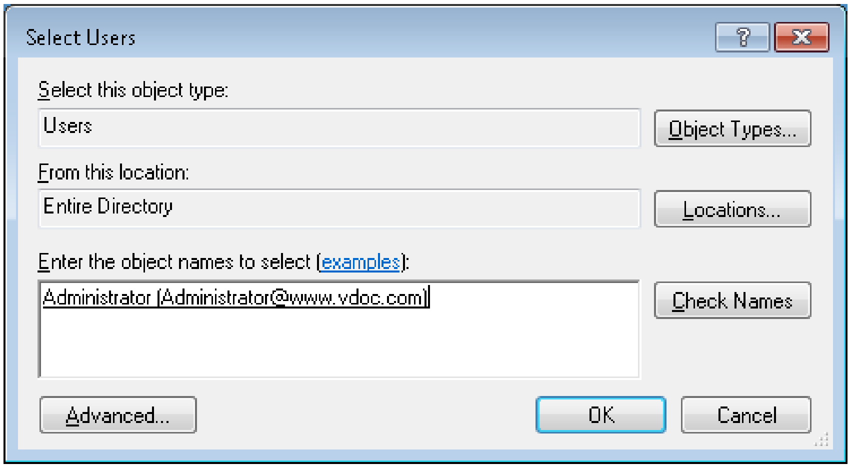
Select this object type: Users

From this location: Entire Directory

Enter the object names to select (examples):

Figure 3: Select User from Active Directory

4. You can type a username and click "Check Names" to verify. Once verified, the username will have an underline.



Select this object type: Users

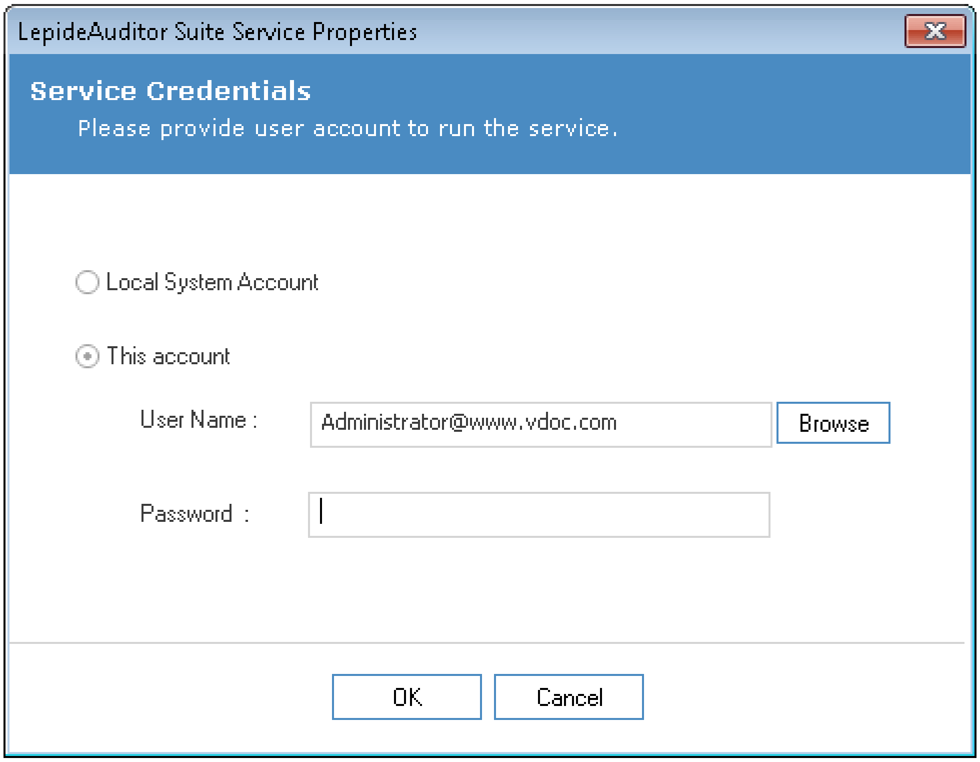
From this location: Entire Directory

Enter the object names to select (examples): Administrator (Administrator@www.vdoc.com)

Figure 4: Selected a user

NOTE: The selected user should be a member of "Domain Admins" group.

5. Click "OK" to save the selection. It takes you back to the previous dialog box.



LepideAuditor Suite Service Properties

Service Credentials

Please provide user account to run the service.

○ Local System Account

● This account

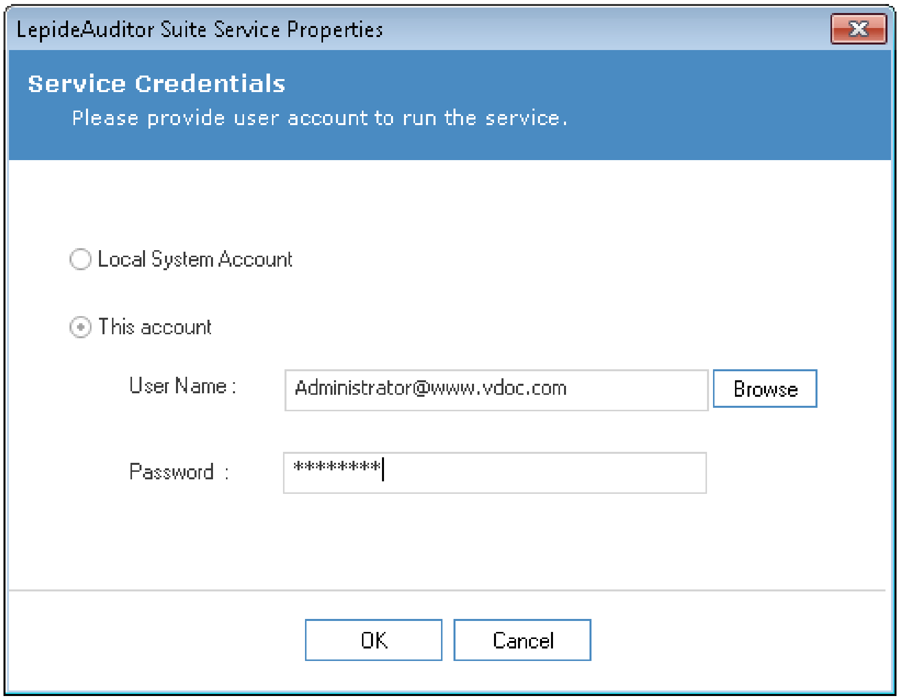
User Name : Administrator@www.vdoc.com

Password :

Figure 5: Selected a user

You can manually enter the username in the same format.

6. Enter the password for the selected user.



LepideAuditor Suite Service Properties

Service Credentials

Please provide user account to run the service.

○ Local System Account

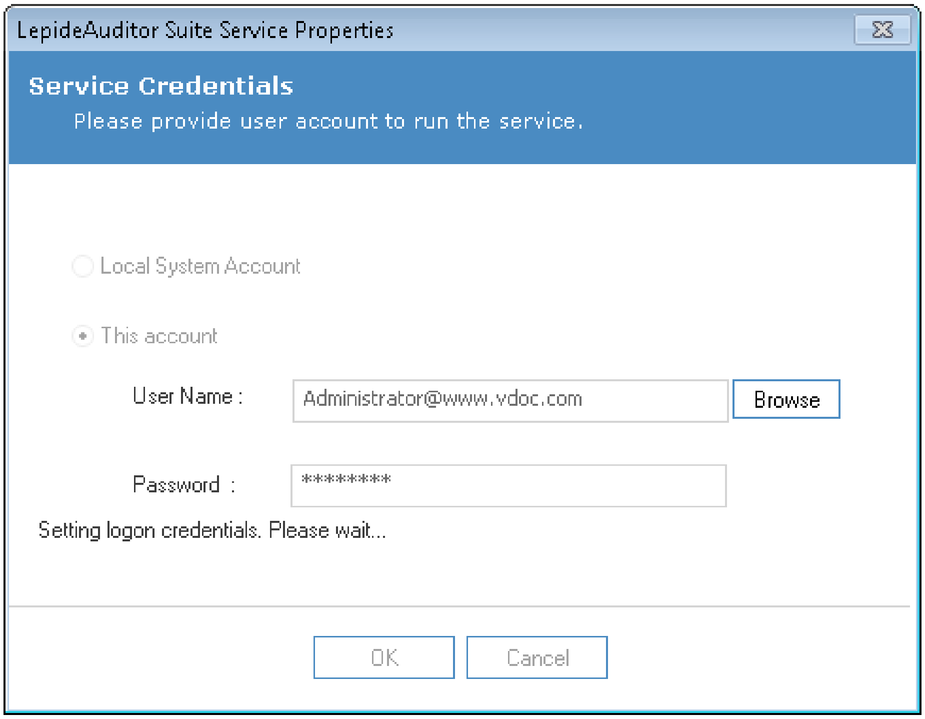
● This account

User Name : Administrator@www.vdoc.com

Password : *********

Figure 6: Entered the Login Credentials

7. Click "OK". The software processes the request to configure the service.



LepideAuditor Suite Service Properties
Service Credentials
Please provide user account to run the service.

○ Local System Account

● This account

User Name : Administrator@www.vdoc.com

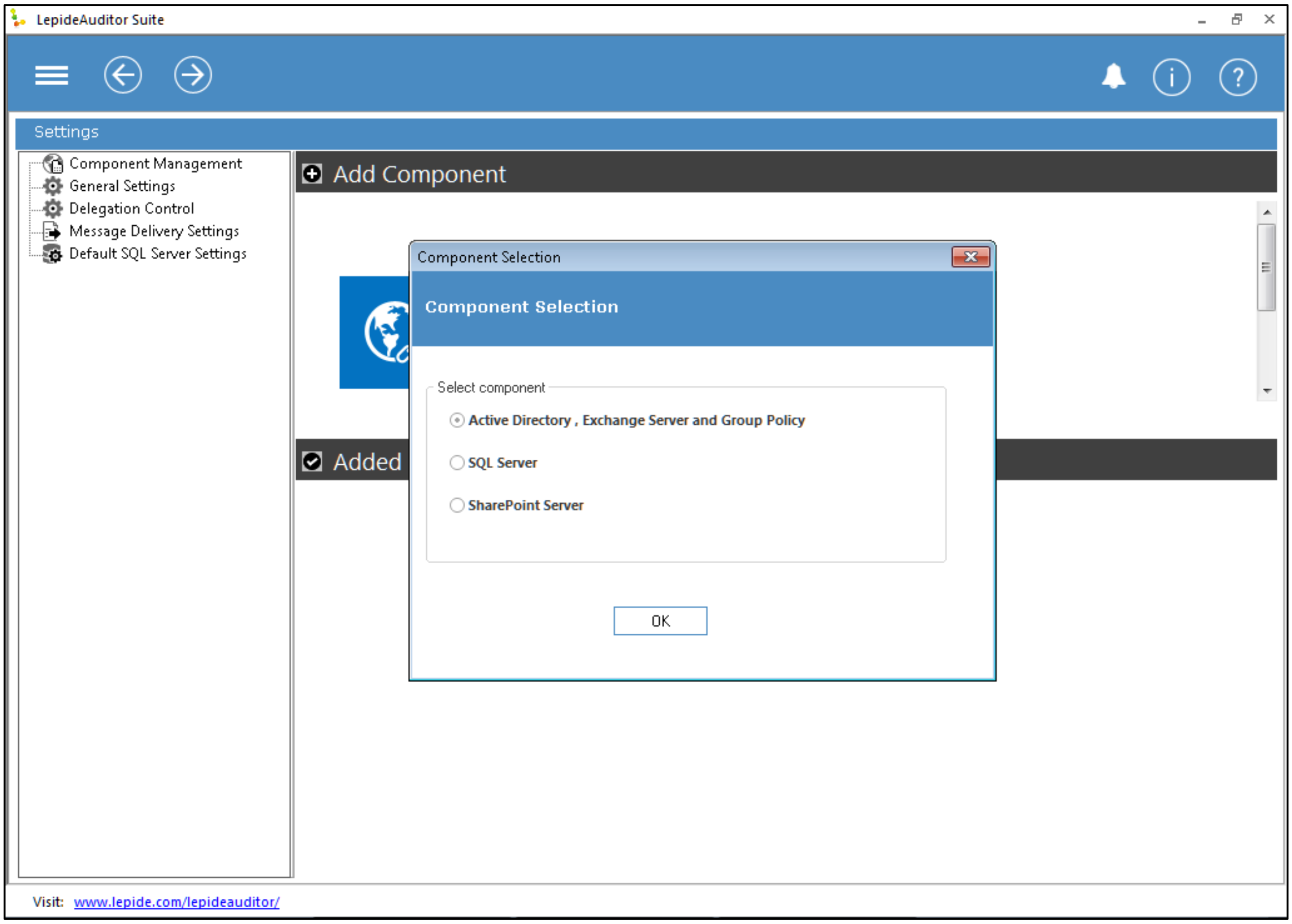
Password : *********

Setting logon credentials. Please wait...

Figure 7: Processing the Service Configuration

Once done, the dialog box will disappear.

After configuring the credentials, "Component Selection" dialog box appears.



Component Selection

Component Selection

Select component

● Active Directory , Exchange Server and Group Policy

○ SQL Server

○ SharePoint Server

OK

Figure 8: Select Component

Select the type of component and add it for auditing.

5. Settings

It is the centralized control panel of the software, which allows you to perform all required settings to configure and use the software. Its settings are divided into the following categories, each of which has a node in the left panel.

- Component Management
    - Domain Settings
        - Active Directory
        - Group Policy Objects
        - Exchange Server
        - User Password Expiration Reminder
        - Active Directory Cleaner
    - SharePoint Server Settings
    - SQL Server Settings
- General Settings
- Delegation Control
- Delivery Message Settings
    - App Profile Management
    - Email Configuration
- Default SQL Server Settings

For basic configuration and software usage, these three sections have been dealt in detail here.

5.1 Component Management

This section allows you to manage domains. You can add/remove/modify the added server components, and configure/install/uninstall their auditing agents from here. If no component is added, you will receive the option to add component and to uninstall agent from any domain, SQL Server, or SharePoint Server without adding it.

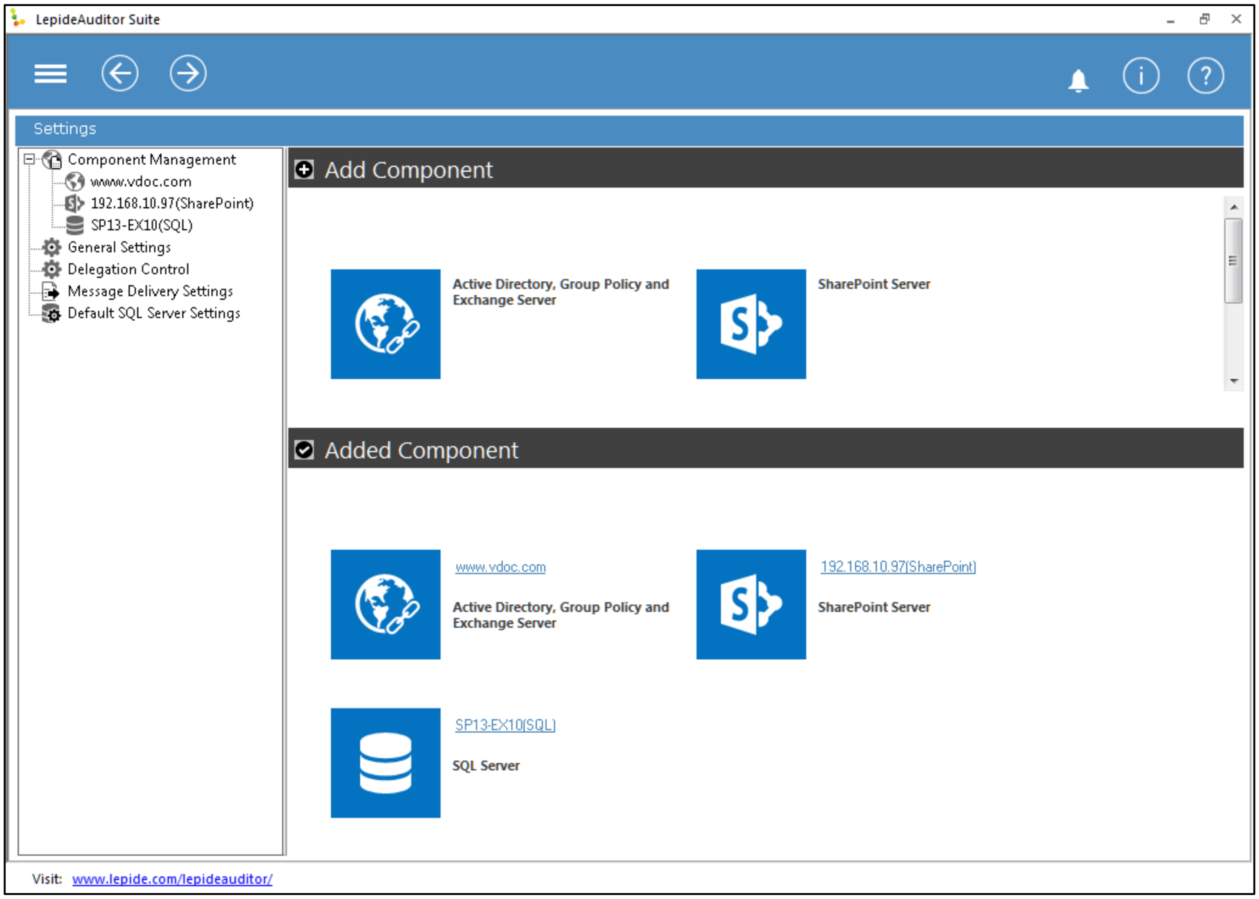

LepideAuditor Suite
Settings
Component Management
www.vdoc.com
192.168.10.97(SharePoint)
SP13-EX10(SQL)
General Settings
Delegation Control
Message Delivery Settings
Default SQL Server Settings
Add Component
Active Directory, Group Policy and Exchange Server
SharePoint Server
Added Component
www.vdoc.com
Active Directory, Group Policy and Exchange Server
192.168.10.97(SharePoint)
SharePoint Server
SP13-EX10(SQL)
SQL Server
Visit: www.lepide.com/lepideauditor/

Figure 9: Component Management

This tab's interface is divided into two sections - "Add Component" that lets you add new component and "Added Component" that lets you manage already added components.

The steps to manage the different components are discussed in three different guides. Click the links below to know more about them.

1) Configuration Guide for Active Directory, Group Policy, and Exchange Server
2) Configuration Guide for SharePoint Server
3) Configuration Guide for SQL Server

In Component Management, you can perform the following operations.

5.1.1 Add Component

You can click any button "Active Directory, Group Policy and Exchange Server", "SharePoint Server", or "SQL Server" in "Add Component" section to add a new component. Alternatively, you can right click on root node of "Component Management" and go to "Add" sub-menu to access the options to add component. The procedure is exactly same as explained above.

5.1.2 Remove Component

Right click on the node of component below "Component Management" and click "Remove" option to remove it. You can also click the component and click "Remove" link in "Actions" pane.

5.1.3 Modify Component Properties

You can modify the properties and customize the auditing of added components such as domain (Active Directory, Group Policy, and Exchange Server), SharePoint Server, and SQL Server.

5.1.4 Manage Auditing Agent

The agentless auditing is available for domain (Active Directory, Group Policy, and Exchange Server) and SQL Server. However, the agent is required to audit SQL Server, Non-Owner Mailbox Access of Exchange and logon/logoff events of domain.

You can perform the following tasks to manage the agents.

- Switch between Agentless and Agent-based auditing (to and fro)
- Uninstall Agent
- Reinstall Agent

Uninstalling the agent serves two purposes:

1. Uninstall agent from selective DCs in a domain, which you do not want to audit anymore.
2. Uninstall agent manually over a DC whose domain has been already removed from the audit list.

5.1.5 Manage Health Monitoring

You can enable or disable the health monitoring of domain and SQL Server.

5.1.6 Console Auditing Settings

Console Auditing lets you audit the user actions performed on the console of LepideAuditor Suite. A separate report named "Console Auditing" has been added in "Audit Reports" Tab. You have to configure the Console Auditing Setting in Component Management in order to enable the auditing of console.

Follow the steps below to configure the Console Auditing Settings.

1. Right click on "Component Management" node in "Settings" Tab.

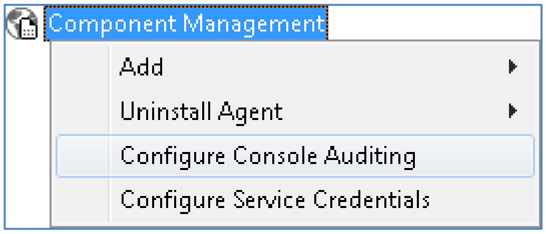


Figure 10: Option to access Console Auditing

2. Click "Console Auditing" to access the following dialog box.

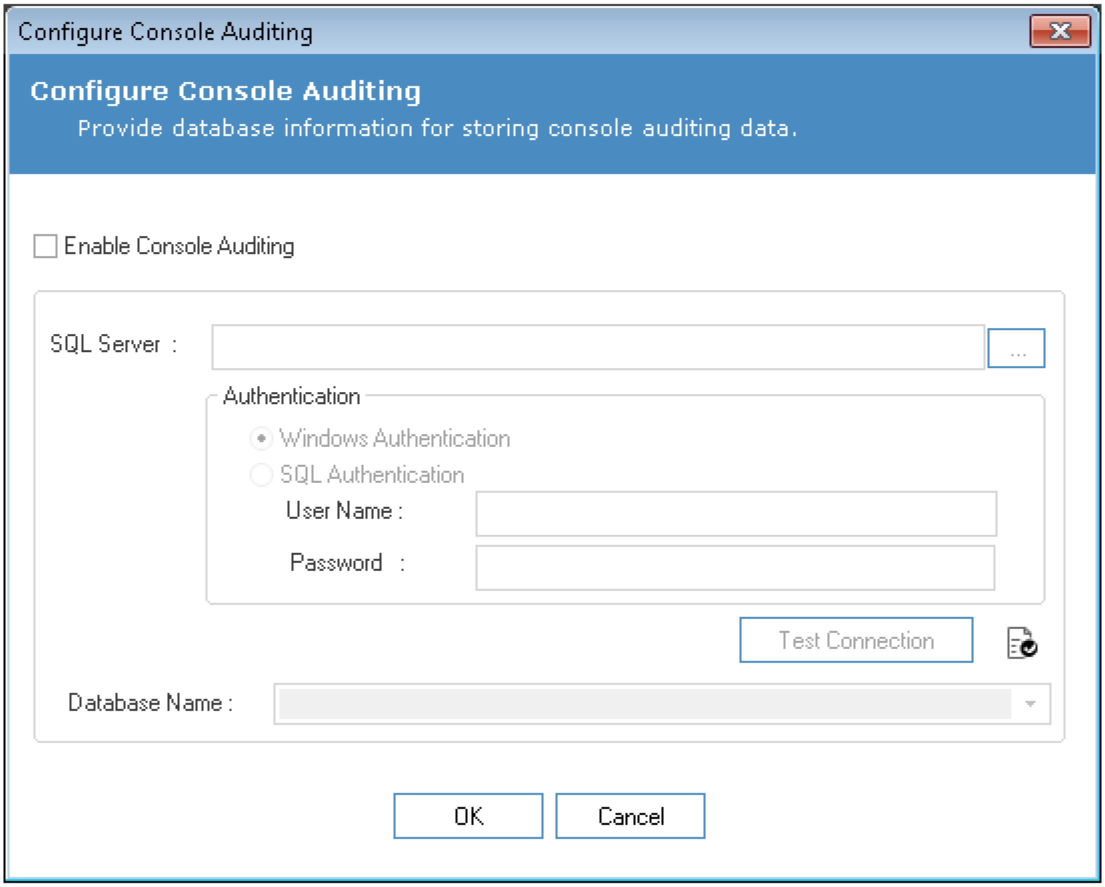
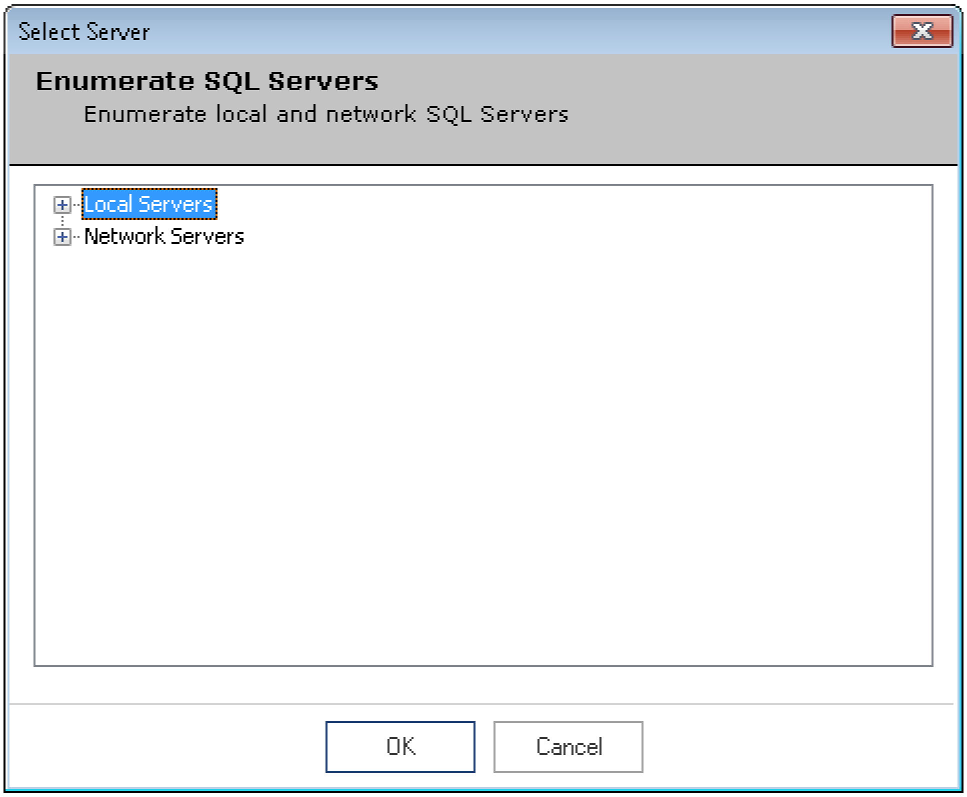

Configure Console Auditing
Configure Console Auditing
Provide database information for storing console auditing data.
□ Enable Console Auditing
SQL Server :
...
Authentication
● Windows Authentication
○ SQL Authentication
User Name :
Password :
Test Connection
Database Name :
OK
Cancel

Figure 11: Console Auditing Settings

3. Check the box of "Enable Console Auditing". It enables the following section containing the database settings.

NOTE: You can click icon to load the SQL Server Settings from "Default SQL Server Settings".

4. The software lets you connect to a local or networked SQL Server. You can either enter the name of SQL Server manually in the text box or click ... to enumerate all SQL Servers in a list and select the desired one in the following box.



Select Server

Enumerate SQL Servers

Enumerate local and network SQL Servers

Figure 12: Select an SQL Server

5. Click ⊞ icon to expand the listings for local and network servers. You can click ⊟ icon to collapse the list.

6. Select a server and click "OK" to go back to the "SQL Server Settings" box, which now shows the selected SQL Server.

7. You have to select any of the following authentication types.

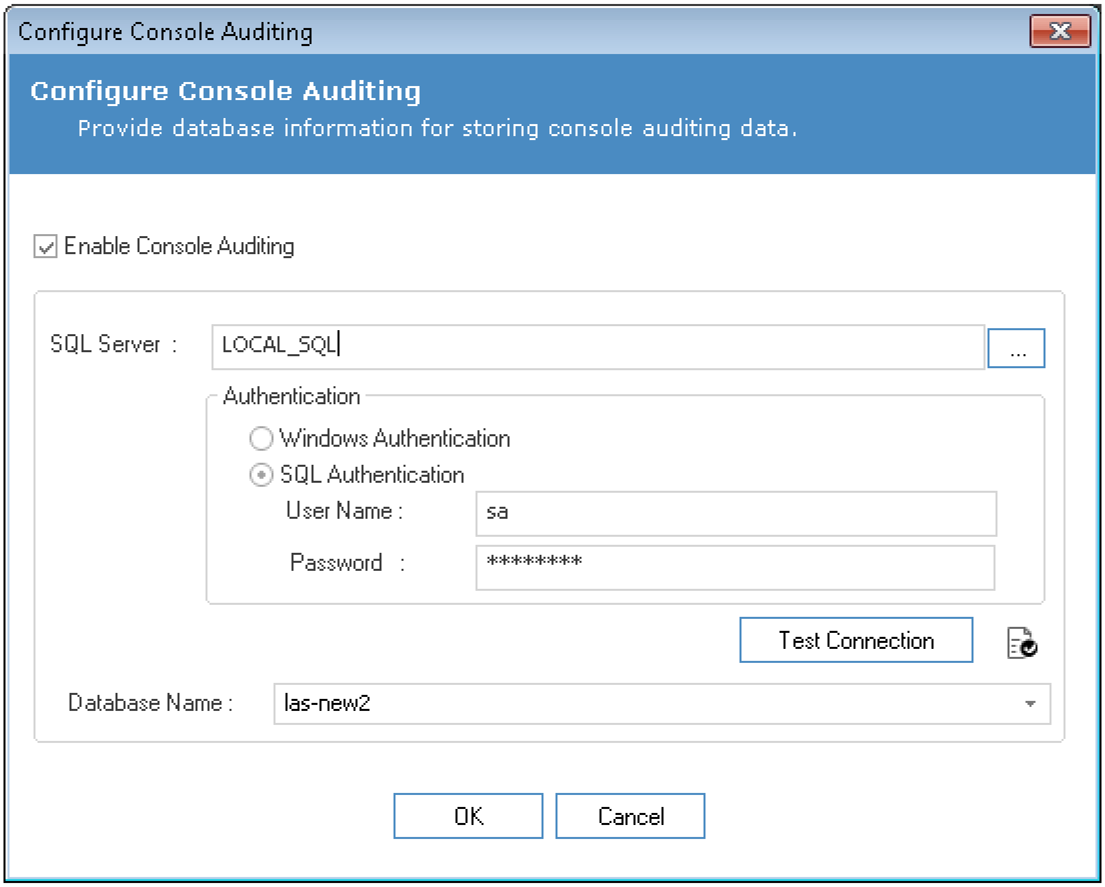
   A. **Windows Authentication:** It lets the software login at SQL Server using the credentials of that user with which you are logged into the computer currently.

   B. **SQL Server Authentication:** It lets you provide the username and password of an SQL Server user.

It is recommended to use the SQL Server Authentication

8. You have to provide a database name in the text box saying "Database". If you are reinstalling the software, then you can reuse the earlier database.

9. Following is a snapshot of the dialog box containing the sample details, where we have selected to login with SQL Server Authentication mode.



Configure Console Auditing

Configure Console Auditing

Provide database information for storing console auditing data.

☑ Enable Console Auditing

SQL Server : LOCAL_SQL

Authentication

○ Windows Authentication

● SQL Authentication

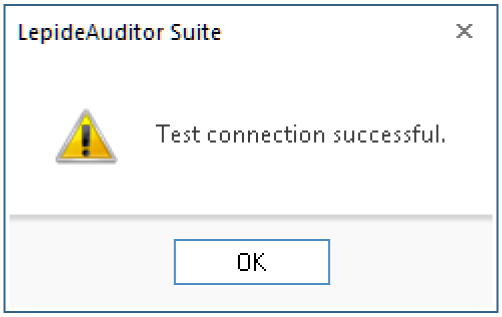
User Name : sa

Password : *********

Database Name : las-new2

Figure 13: Sample Details

10. Click Test Connection to test the connection between the software and the selected SQL Server using the provided details. It either displays an error if failed to connect or shows the following message confirming the successful connection.



LepideAuditor Suite

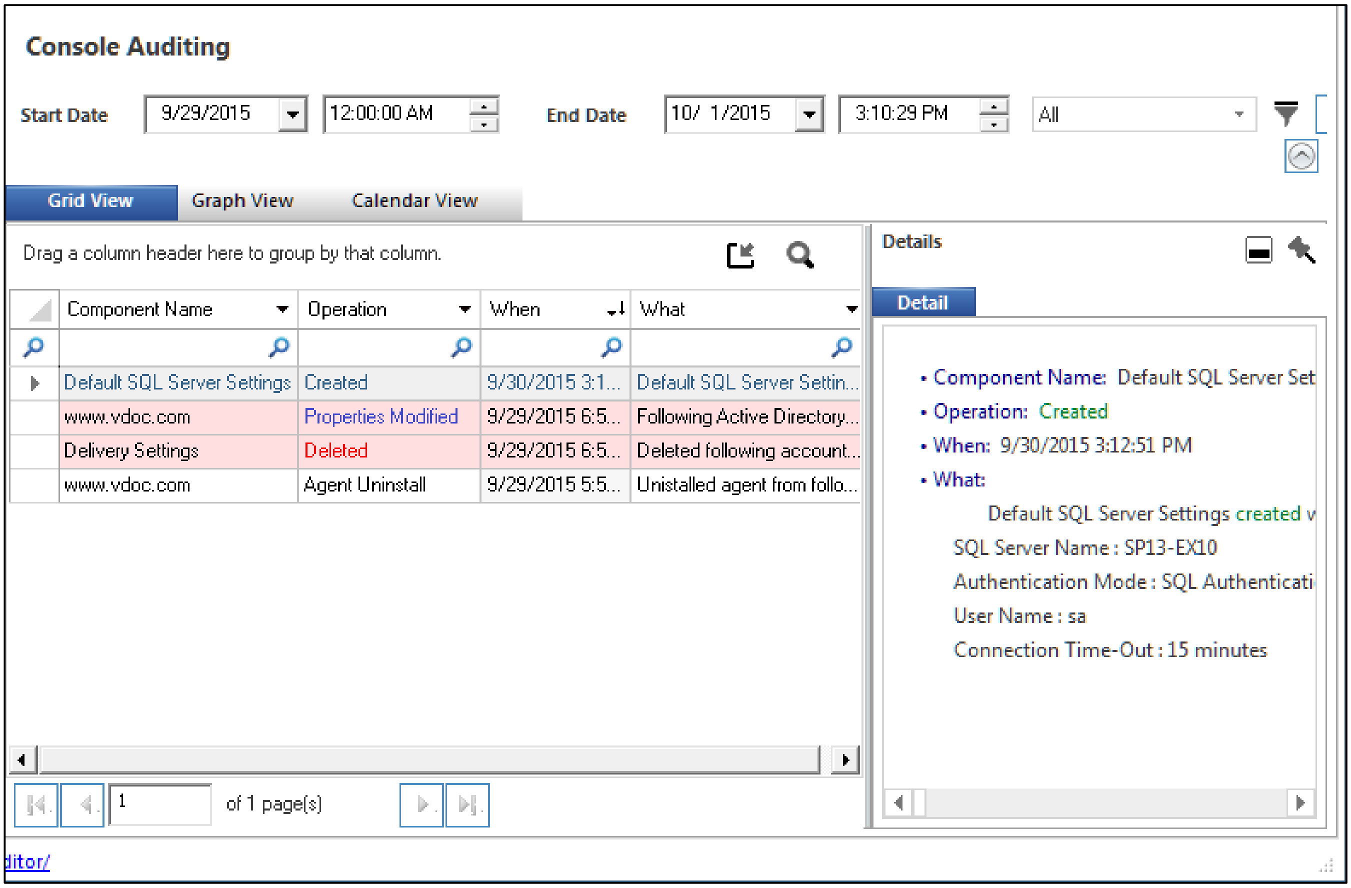
Test connection successful.

Figure 14: The connection to SQL Server is successful.

11. Enter the name of database. You can use the same database, which has been used earlier to save the auditing logs of server components.

12. Click "OK" to save the settings.

Console Auditing is enabled once you perform the above steps to configure its settings. Now, you can go to "Audit Reports" section to view the Console Auditing Report.



Console Auditing

Start Date: 9/29/2015 12:00:00 AM
End Date: 10/ 1/2015 3:10:29 PM
All

Drag a column header here to group by that column.

	Component Name	Operation	When	What
▶	Default SQL Server Settings	Created	9/30/2015 3:1...	Default SQL Server Settin...
	www.vdoc.com	Properties Modified	9/29/2015 6:5...	Following Active Directory...
	Delivery Settings	Deleted	9/29/2015 6:5...	Deleted following account...
	www.vdoc.com	Agent Uninstall	9/29/2015 5:5...	Unistalled agent from follo...

1 of 1 page(s)

- Component Name: Default SQL Server Set
- Operation: Created
- When: 9/30/2015 3:12:51 PM
- What:

  Default SQL Server Settings created v

  SQL Server Name : SP13-EX10

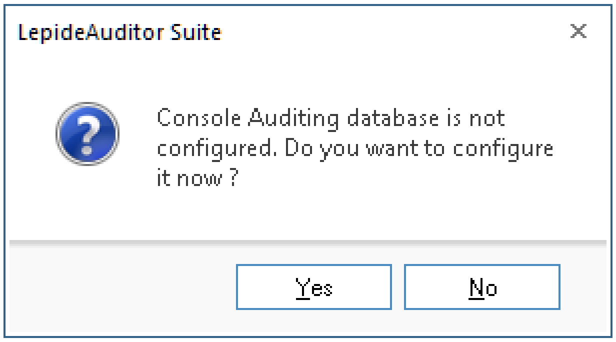
  Authentication Mode : SQL Authenticati

  User Name : sa

  Connection Time-Out : 15 minutes

Figure 15: Report of Console Auditing

If the Console Auditing Settings are not configured, then you will receive the following error message while trying to generate "Console Auditing" Report.

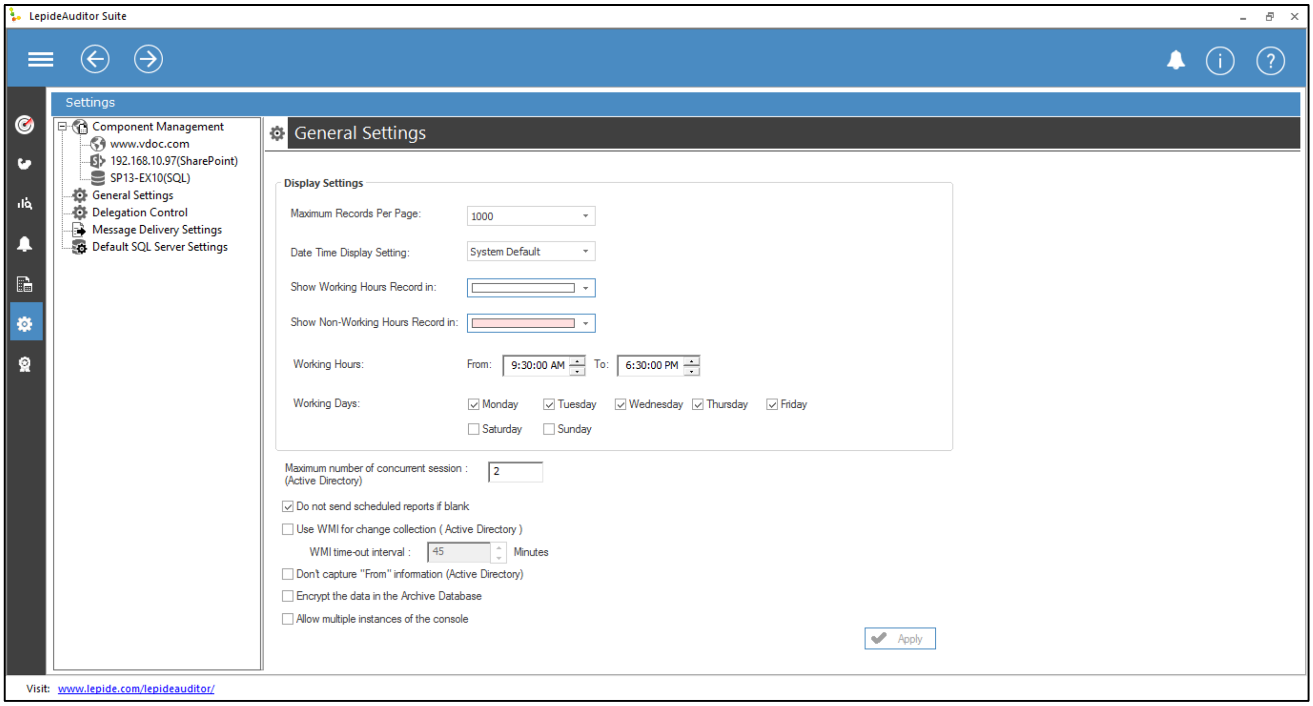


Console Auditing database is not configured. Do you want to configure it now ?

Figure 16: Console Auditing is not configured

5.2 General Settings

LepideAuditor Suite provides extended reports and entire audit details. You can configure reports settings to get the reports displayed as per your personal preferences.



Display Settings

Maximum Records Per Page: 1000

Date Time Display Setting: System Default

Show Working Hours Record in: ⬜

Show Non-Working Hours Record in: 🟥

Working Hours: From: 9:30:00 AM To: 6:30:00 PM

Working Days: ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday □ Saturday □ Sunday

Maximum number of concurrent session : (Active Directory) 2

☑ Do not send scheduled reports if blank

□ Use WMI for change collection (Active Directory)

WMI time-out interval : 45 Minutes

□ Dont capture "From" information (Active Directory)

□ Encrypt the data in the Archive Database

□ Allow multiple instances of the console

Figure 17: General Settings

General Settings is divided into two sections:

5.2.1 Display Settings

Here, you can select how many records will be displayed in a page and decide whether to send the blank reports via email or not.

i. **Maximum Records per Page:** Select the maximum number of records that you wish to be displayed in each report page.

ii. **Date/Time Format:** Specify the date and time format from the available options in the dropdown list.

iii. **Show working hours record in:** Select the preferred color to get the reports in working hours displayed in that particular color.

iv. **Show non-working hours record in:** Select the preferred color to get the reports in non-working hours displayed in that particular color.

v. **Working and Non-Working Hours:** Here, you can define the working hours on a daily basis and working days. Once working and non-working hours/days are configured separately, you can view the audit reports as per working and non-working hours.

5.2.2 Other Settings

This section contains the following settings.

1. **Maximum number of concurrent session (Active Directory):** Here, concurrent sessions mean the number of domain controllers that can be audited collectively by LepideAuditor Suite at a time.

   You can increase or decrease the number of domain controllers to be audited at a time.

2. **Do not send scheduled reports, if blank:** Select this checkbox if you do not want scheduled report recipients to receive blank report mails without any data.

3. **Use WMI for Change Collection (Active Directory):** Check this option to enable the usage of WMI in collecting the Active Directory logs. You can define the WMI time out-interval as well. You have to uncheck this option to disable the usage of WMI.

4. **Don't capture "From" information (Active Directory):** You can check this option to disable the capturing of "From" field while auditing Active Directory.

   Unchecking this option enables the capturing of this particular field in Active Directory auditing logs.

5. **Encrypt the data in the Archive Database:** You can enable this option to enhance the security of logs stored in archive database.

6. **Allow multiple instances of the console:** Check this option to use the multiple instances of LepideAuditor Suite at a given point of time.

   If you want to run only one instance of Auditor Suite at any time, then please uncheck this option.

NOTE: Changes in settings in each section can be individually applied.

5.3 Delegation Control

Web Console of LepideAuditor Suite lets the domain users access the audit reports from anywhere in a domain's local network. The user has to provide the login credentials to access the report. "Delegation Control" lets the administrator to create accounts for the domain users to access Web Reports and select what reports they can access.

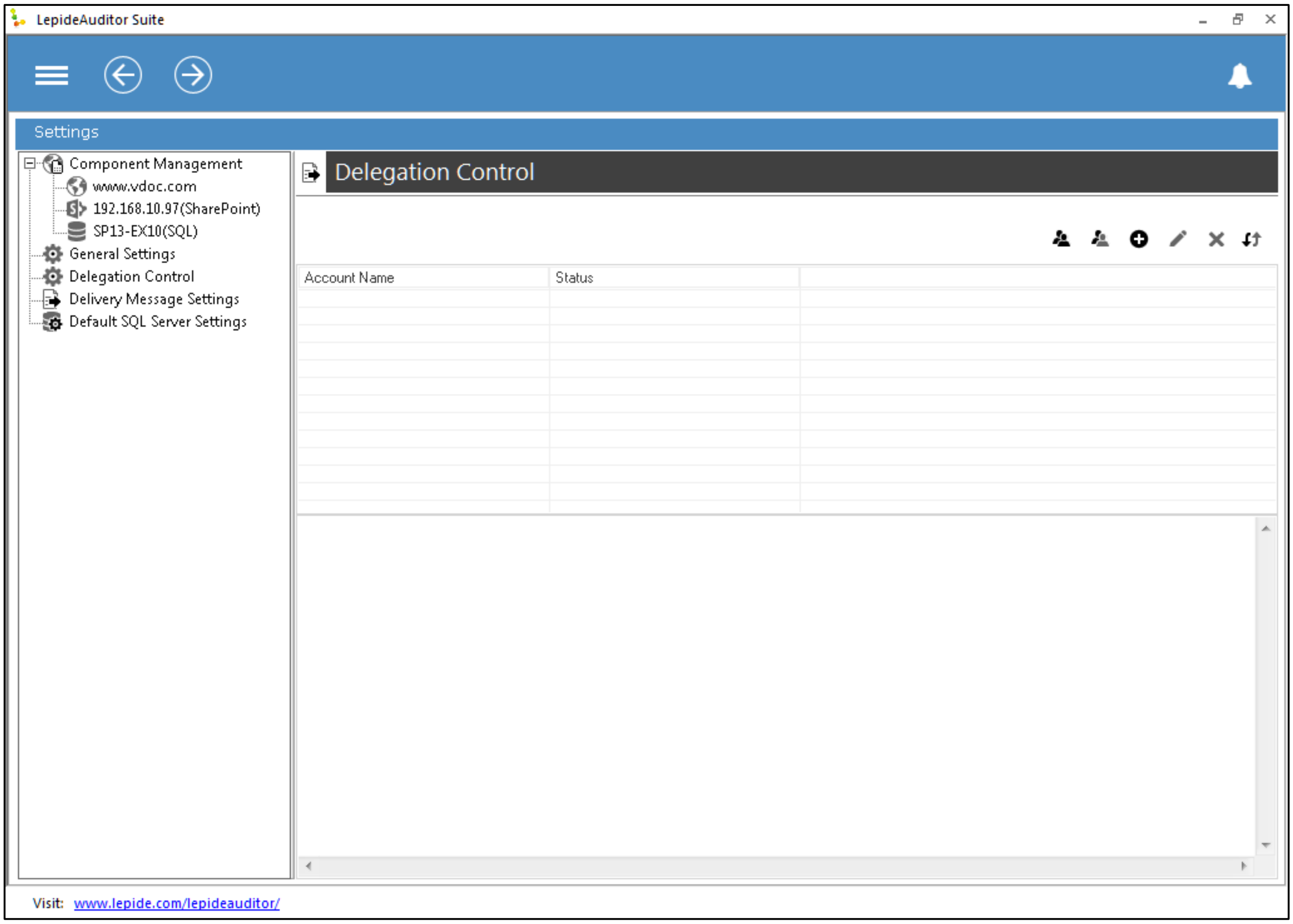


Figure 18: Delegation Control Settings

Here, Administrator can add, edit, delete, enable, and disable the user accounts, using which domain users can access Web Report Console.

Follow the below steps to add a new delegation account.

1. Click ⊕ icon to create a new account. It shows the following wizard.

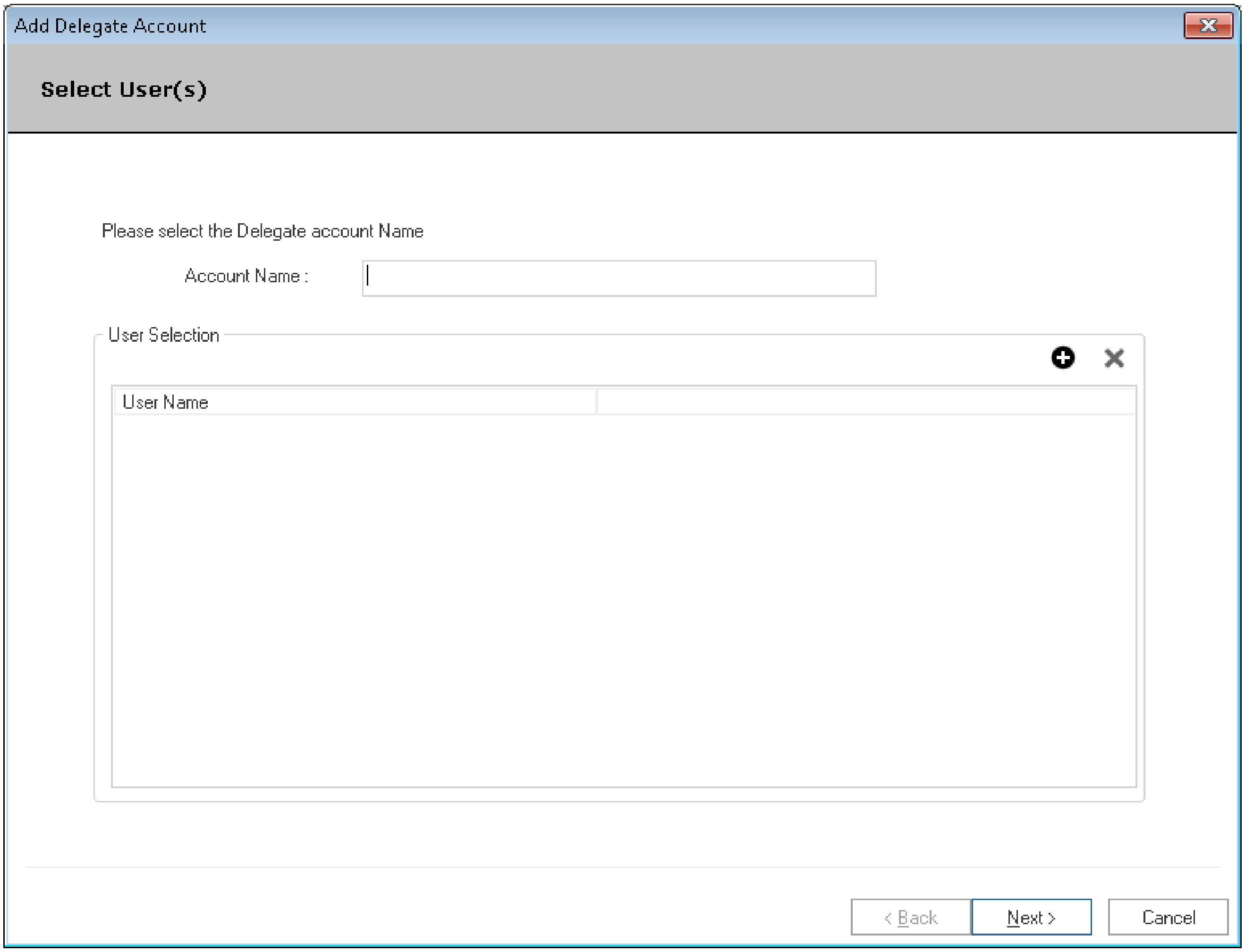


Figure 19: Add Delegate User Account wizard

2. Enter the account name in the textbox.
3. Click ⊕ to add the user(s) who can use this account to login at Web Report Console. It shows the following dialog box.

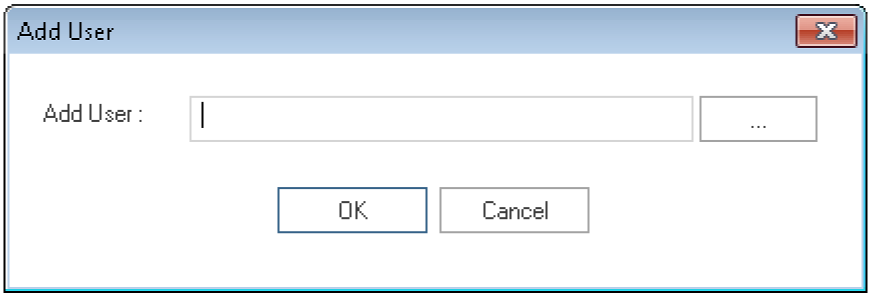
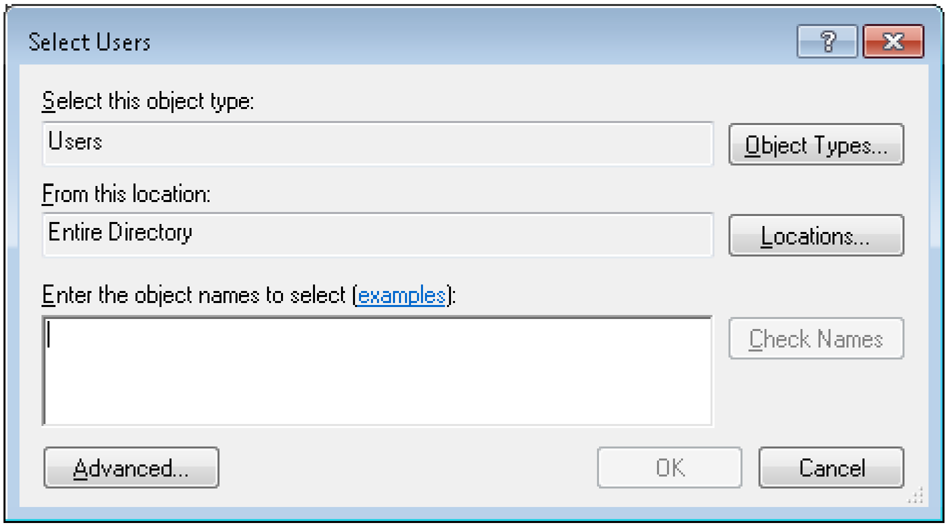


Figure 20: Dialog box to add the users

4. Click ... button to select the users from the domain's Active Directory. It shows the following dialog box.



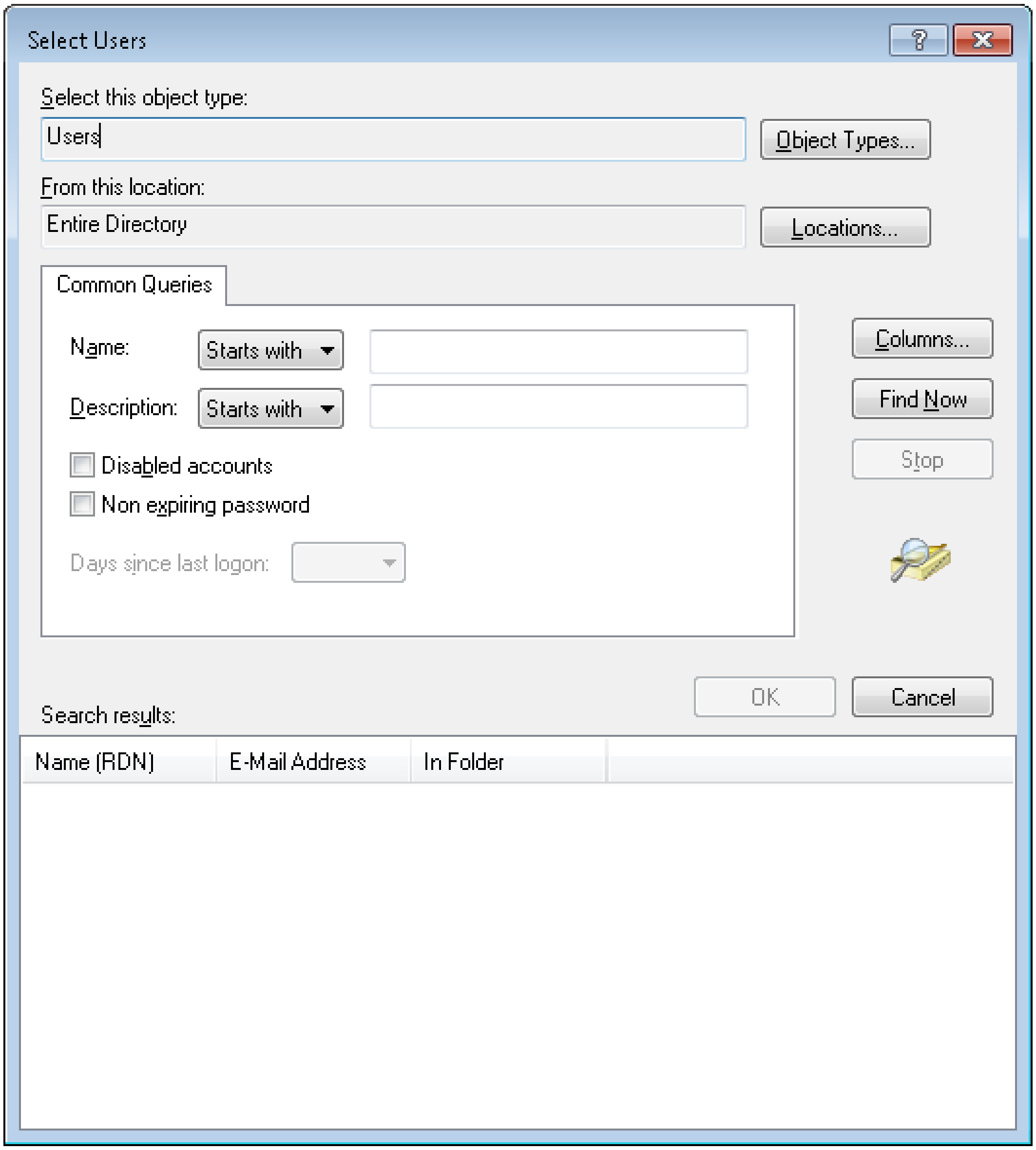
Select this object type: Users

From this location: Entire Directory

Figure 21: Dialog box to select the users from Active Directory

5. Enter the name of user to be added. You can type multiple usernames separated with ; (semicolon).

6. You can also click "Advanced". It shows the options to find the Active directory and select what has can be added to create delegation account.

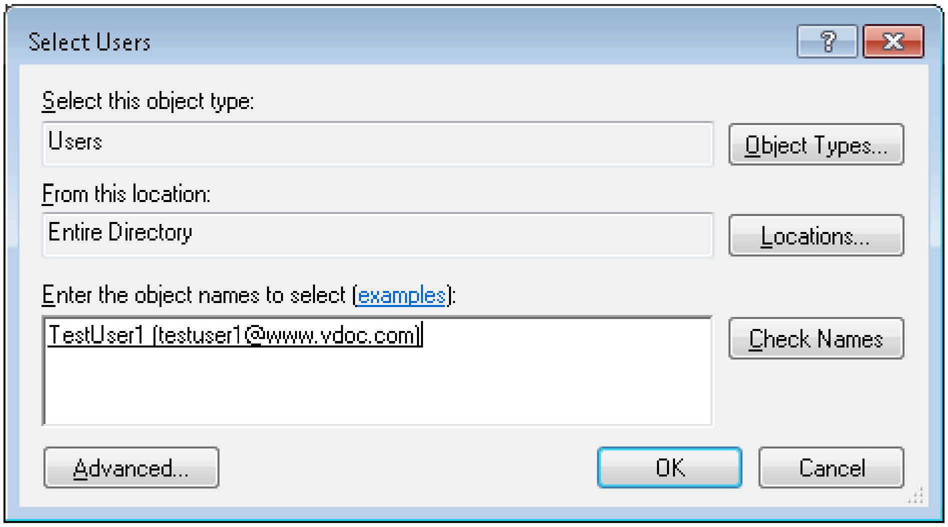


Select this object type: Users

From this location: Entire Directory

Figure 22: Dialog box to find and select the users from Active Directory

7. Click "Check Names" to validate the entered username(s).



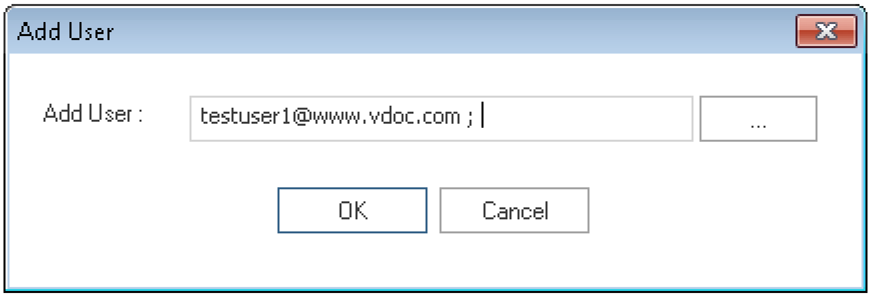
Select this object type: Users

From this location: Entire Directory

Enter the object names to select (examples): TestUser1 (testuser1@www.vdoc.com)

Figure 23: Dialog box to select the users from Active Directory

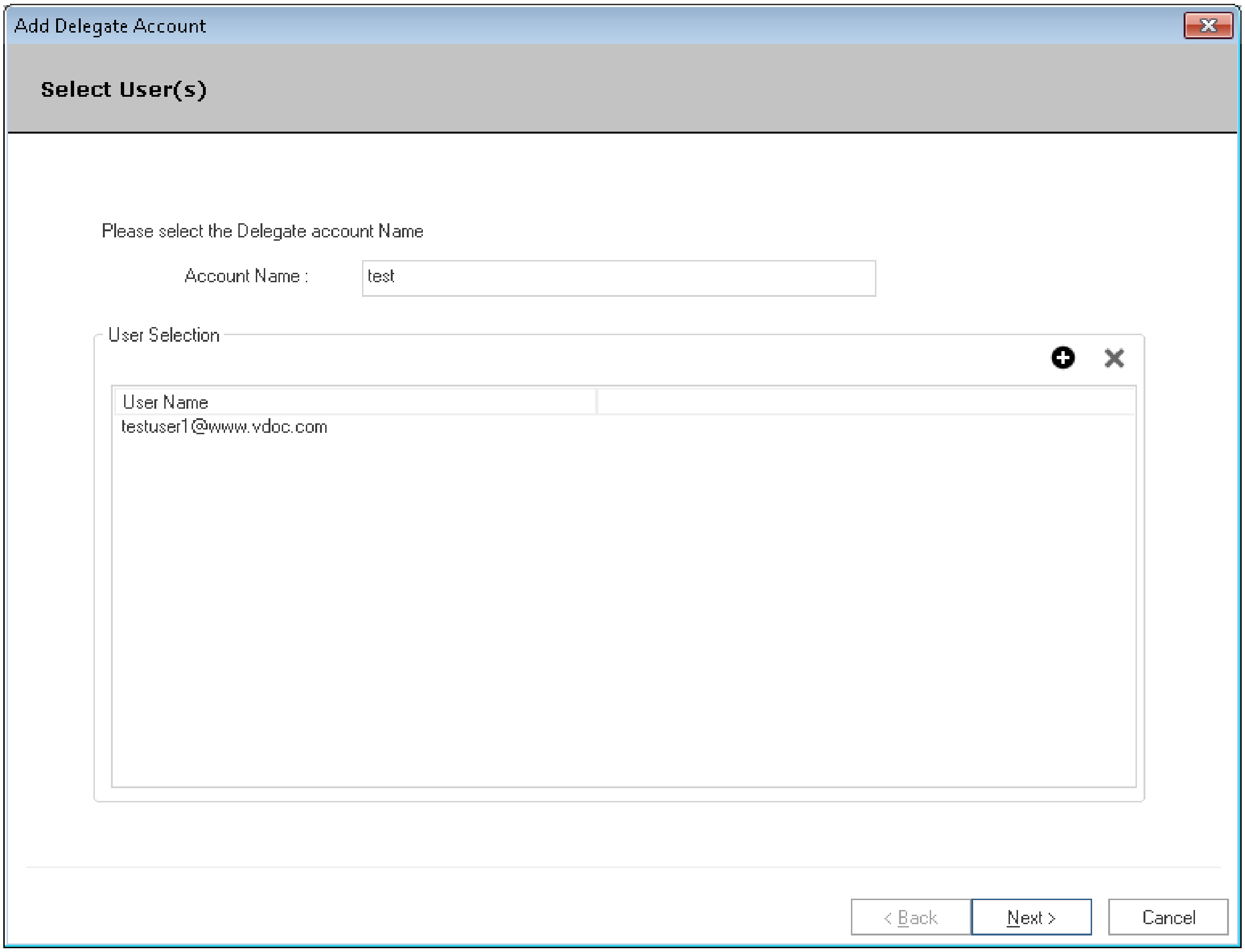
8. Click "OK" once you have added the required users. It takes you back to "Add Users" dialog box that now shows selected AD user.



Add User : testuser1@www.vdoc.com ;

Figure 24: Showing the user to be added

9. Click "OK". It adds the selected user in the list and takes you back to "Add Delegate Account" wizard.



Please select the Delegate account Name

Account Name : test

User Selection

User Name
testuser1@www.vdoc.com

Figure 25: Listing the added users

You can follow the above steps to add more user for this new delegate account.

10. You can select any added user here in the list and click ✖ icon to remove the user.

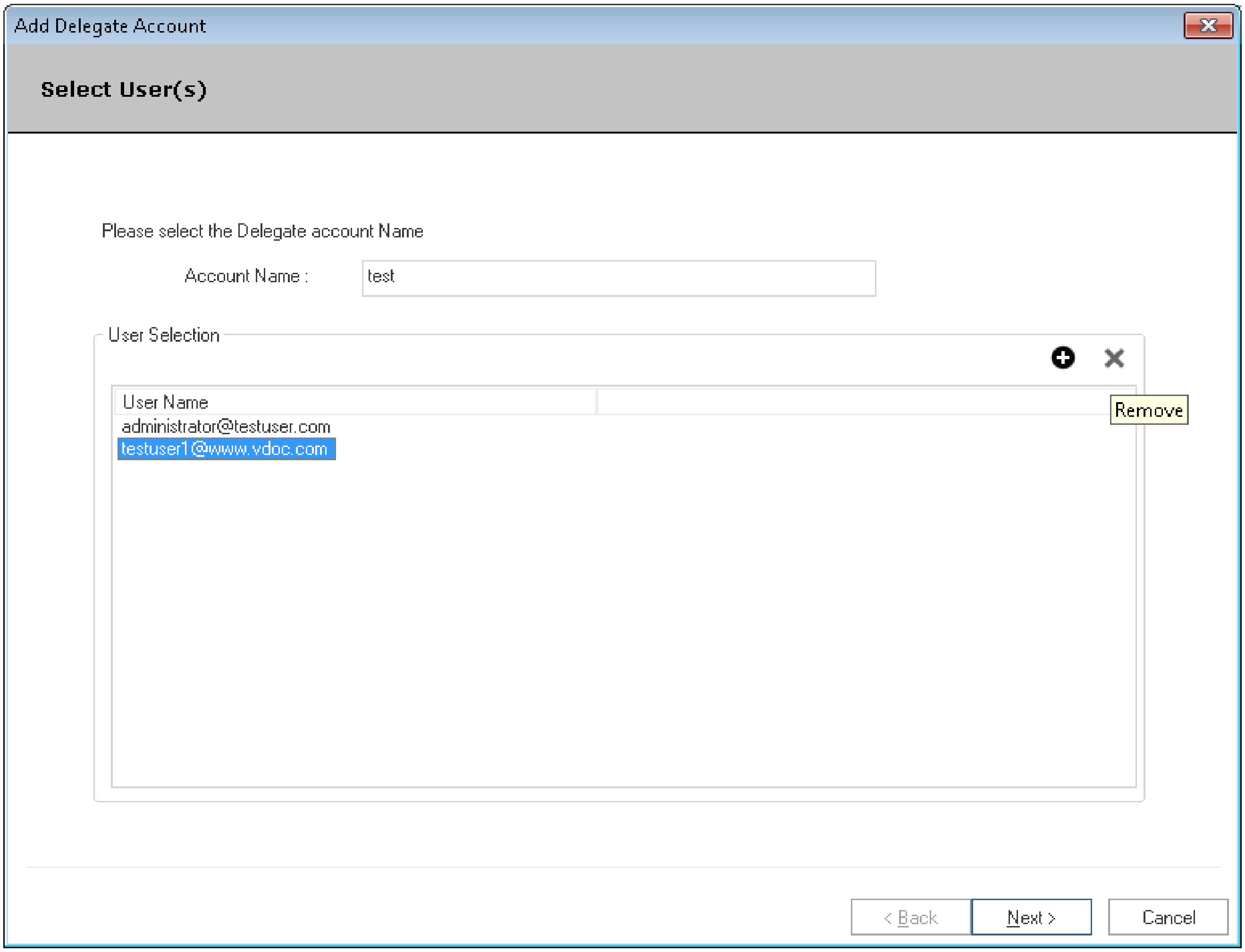
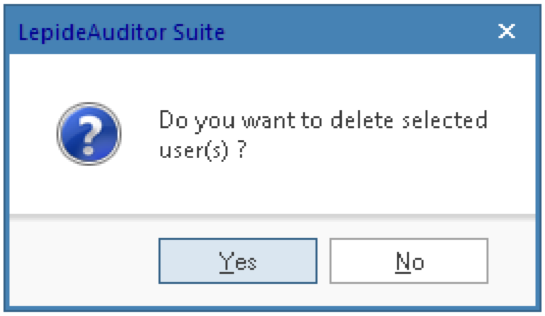


Figure 26: Option to remove the user

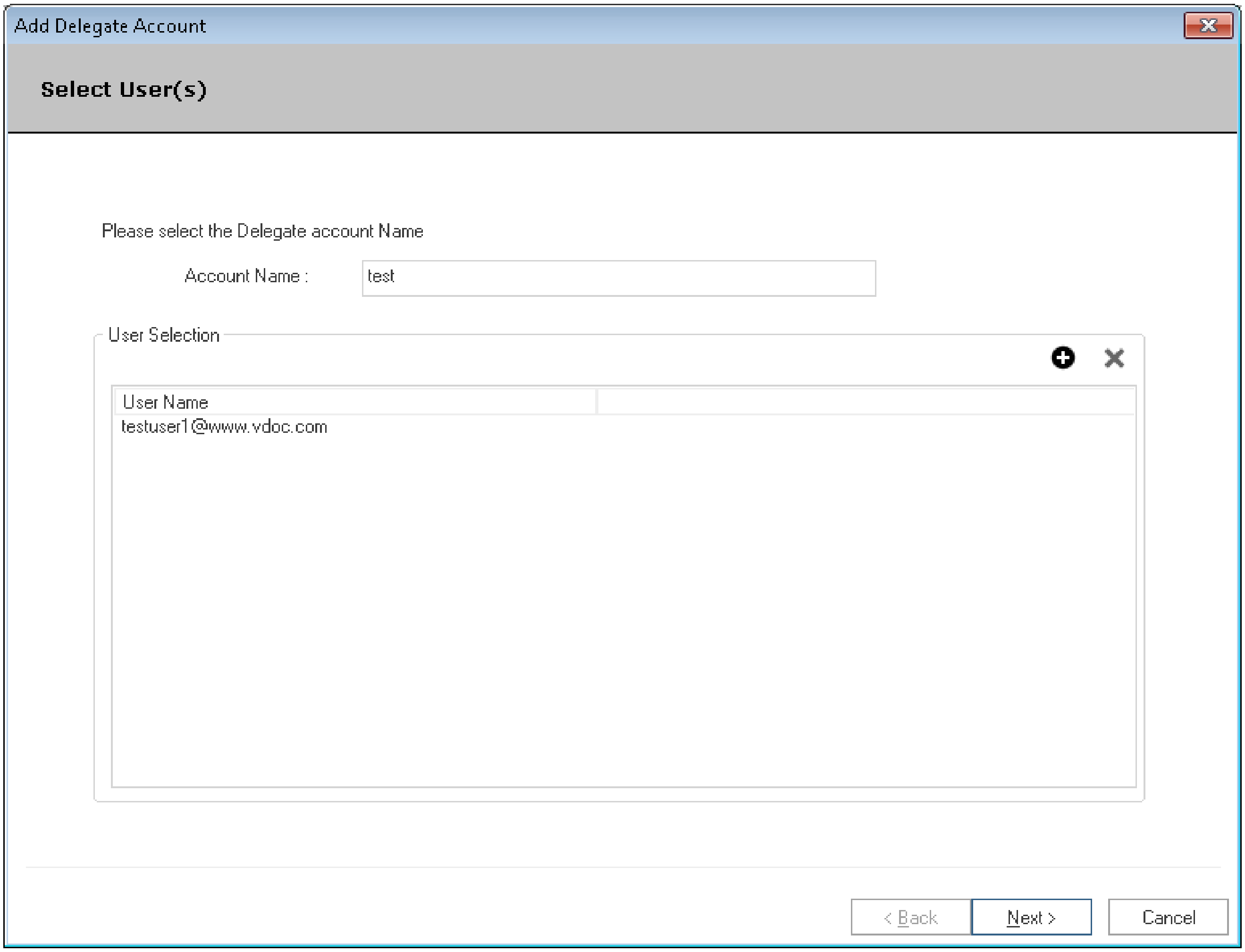
11. Clicking ✖ shows the warning message.



Do you want to delete selected user(s) ?

Figure 27: Warning before deleting user from the list

12. Click "Yes" to delete the user from list. Once clicked, it takes you back to earlier wizard, which confirms that user deleted successfully.



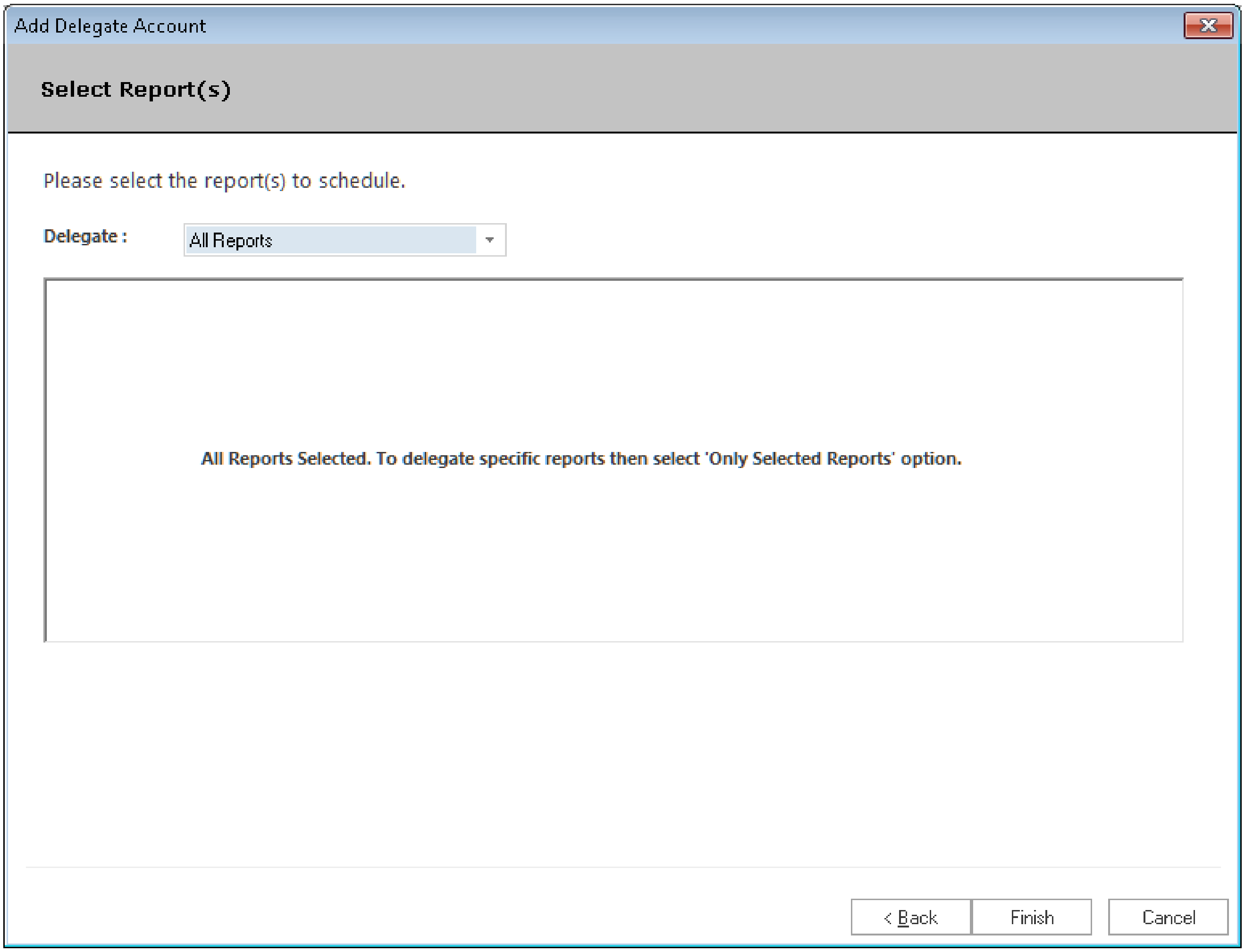
Please select the Delegate account Name

Account Name : test

User Name	
testuser1@www.vdoc.com	

Figure 28: Listing the added users

13. Click "Next" to proceed ahead. The next step gives you the option to select the reports for which you want to authorize the account.



Select Report(s)

Please select the report(s) to schedule.

Delegate : All Reports

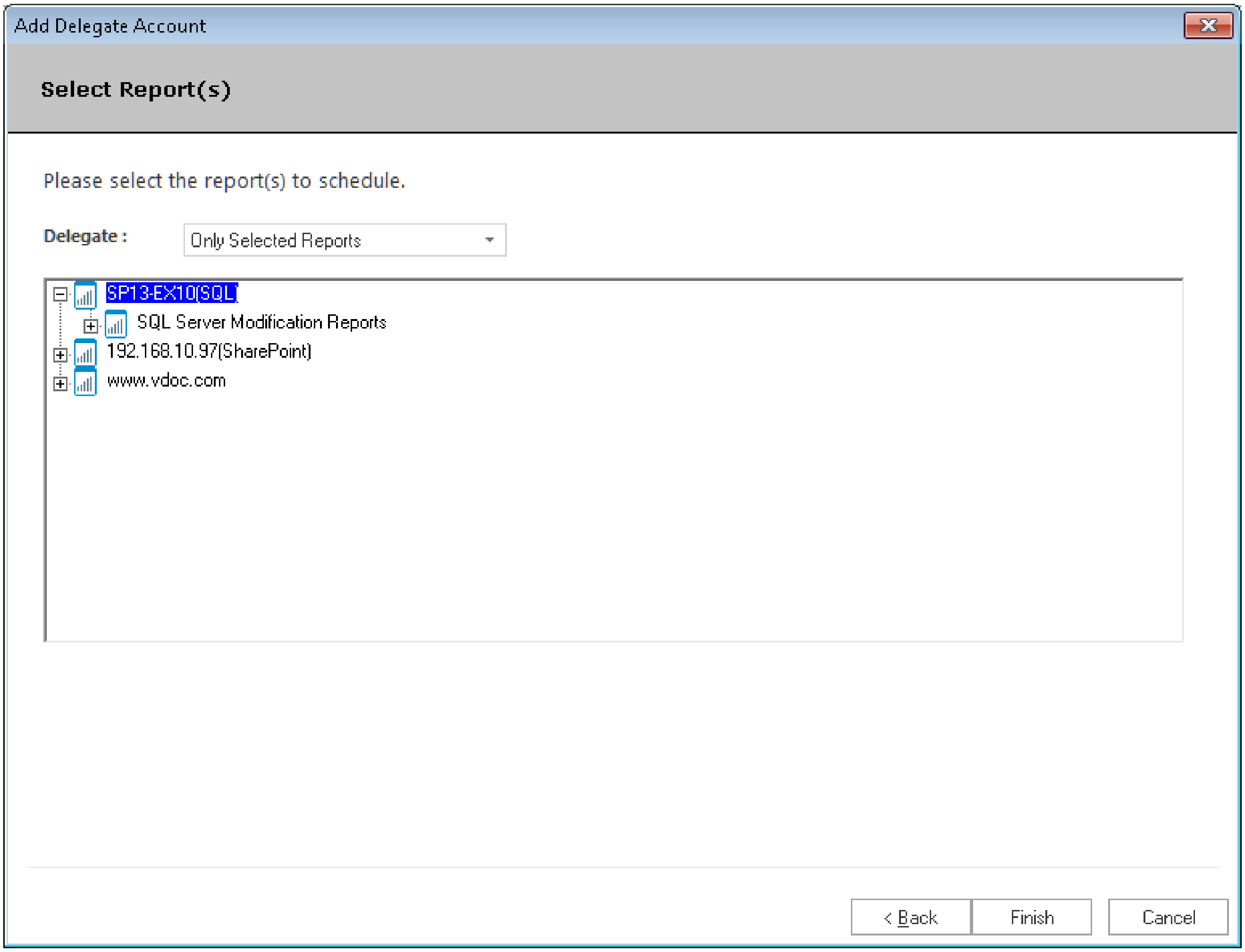
All Reports Selected. To delegate specific reports then select 'Only Selected Reports' option.

Figure 29: Step to select the reports for the account

14. Delegate" drop-down menu has the following options.

    A. **All Reports:** Select this option to authorize the new account access all audit reports.

B. **Only Selected Reports:** Select this option to choose what reports the new account can access and what cannot.



Add Delegate Account

Select Report(s)

Please select the report(s) to schedule.

Delegate : Only Selected Reports

Figure 30: Select the reports for which account will be authorized

15. Select the reports, which are divided into three different categories.

A. **SQL Server:** It shows the auditing reports for SQL Server.

B. **SharePoint:** It shows the auditing reports for SharePoint Server.

C. **Domain:** It shows the reports for domain. It is further divided into the following categories.

I. **Active Directory Reports:** It shows the following reports of Active Directory.

a. Active Directory Modification Reports

b. Active Directory Security Reports

c. Active Directory Custom Report

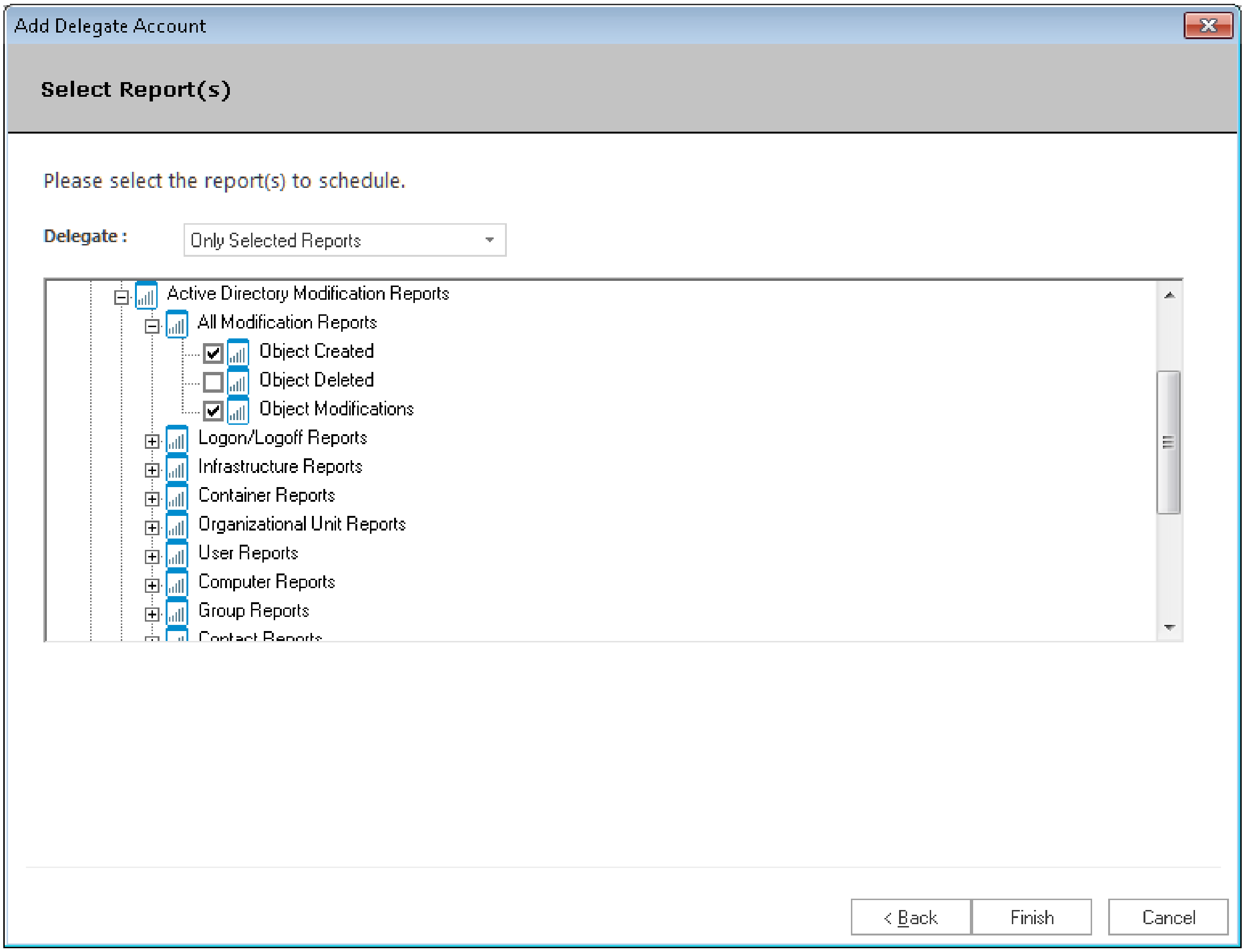
II. **Group Policy Reports:** It shows the following reports of Group Policy.

a. Group Policy Modification Reports

b. Group Policy Custom Reports

III. **Exchange Server Reports:** It shows the auditing reports of Exchange Server.

16. Select the reports for which you want to provide access to the delegation account.



Add Delegate Account

Select Report(s)

Please select the report(s) to schedule.

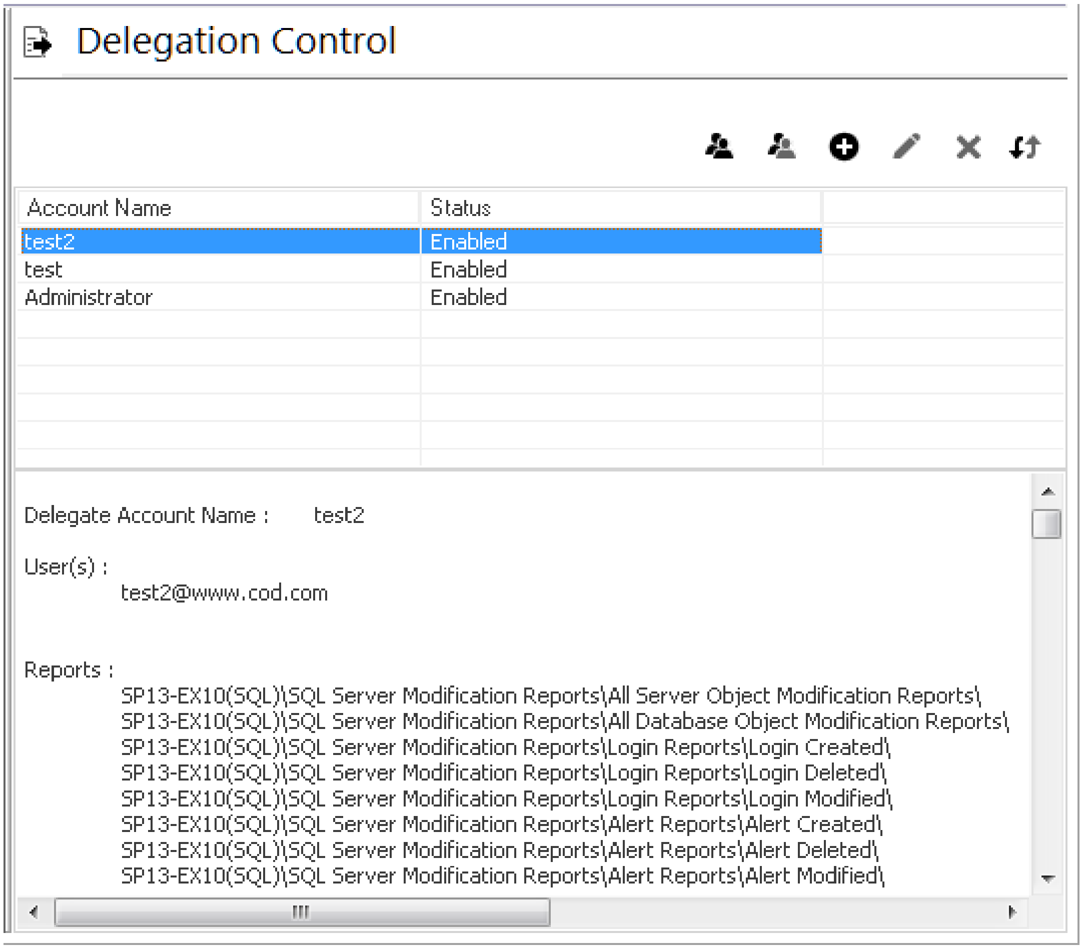
Delegate : Only Selected Reports

- Active Directory Modification Reports
  - All Modification Reports
    - ☑ Object Created
    - □ Object Deleted
    - ☑ Object Modifications
  - Logon/Logoff Reports
  - Infrastructure Reports
  - Container Reports
  - Organizational Unit Reports
  - User Reports
  - Computer Reports
  - Group Reports
  - Contact Reports

Figure 31: Displaying Selected Reports

17. Click "Finish" to create the account.

You can follow the above steps to create multiple accounts. Delegate Control displays all created account in the list.



Delegation Control

Account Name	Status
test2	Enabled
test	Enabled
Administrator	Enabled

Delegate Account Name : test2

User(s) :
test2@www.cod.com

Reports :
SP13-EX10(SQL)\SQL Server Modification Reports\All Server Object Modification Reports\
SP13-EX10(SQL)\SQL Server Modification Reports\All Database Object Modification Reports\
SP13-EX10(SQL)\SQL Server Modification Reports\Login Reports\Login Created\
SP13-EX10(SQL)\SQL Server Modification Reports\Login Reports\Login Deleted\
SP13-EX10(SQL)\SQL Server Modification Reports\Login Reports\Login Modified\
SP13-EX10(SQL)\SQL Server Modification Reports\Alert Reports\Alert Created\
SP13-EX10(SQL)\SQL Server Modification Reports\Alert Reports\Alert Deleted\
SP13-EX10(SQL)\SQL Server Modification Reports\Alert Reports\Alert Modified\

Figure 32: Displaying the added accounts

Following are the other options available in "Delegation Control".

✕ Use this icon to remove an added delegation account

✎ Use this icon to modify details in a delegation account. Just select the account from the list and click this icon. Change the required values and click "OK" to apply the changes.

⇅ Use this icon to refresh changes and display the latest changes in the Delegation Account list, if any.

👤 Use this icon to disable an existing delegation account.

👤 Use this icon to enable an existing delegation account.

5.4 Message Delivery Settings

This setting allows you to define the medium of sending delivery notifications like auditing alerts' messages, health monitoring alerts' messages, and scheduled reports.

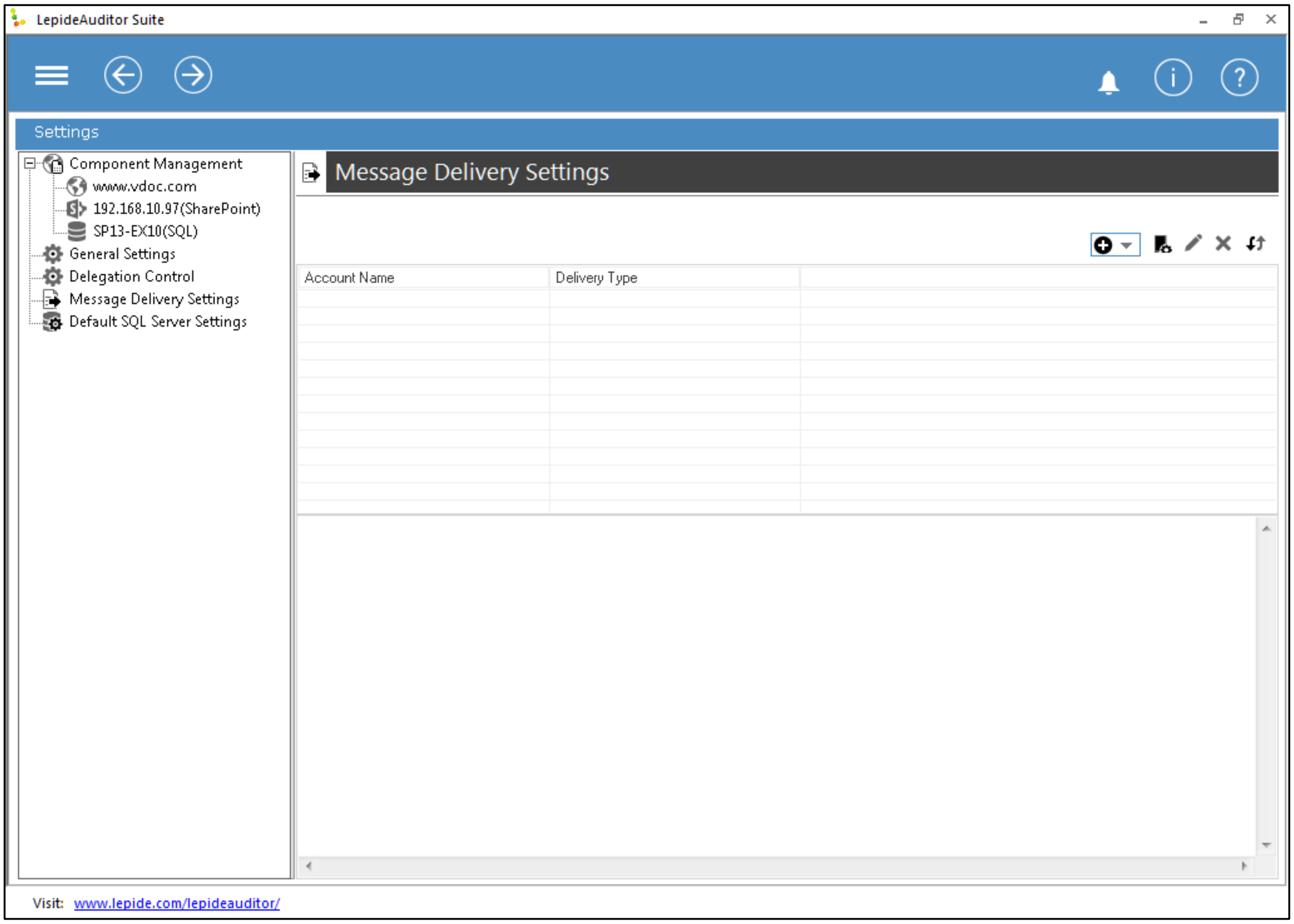

LepideAuditor Suite
Settings
Component Management
www.vdoc.com
192.168.10.97(SharePoint)
SP13-EX10(SQL)
General Settings
Delegation Control
Message Delivery Settings
Default SQL Server Settings
Message Delivery Settings
Account Name
Delivery Type
Visit: www.lepide.com/lepideauditor/

Figure 33: Message Delivery Settings

There are two methods to send the delivery notifications.

1. Email Account
2. Mobile App Account

5.4.1 Email Account

The software lets you add email accounts, modify existing accounts and remove email accounts. The added email account(s) are used to send real-time alerts and scheduled reports.

To add an email account, click on the ⊕▾ button and select "Add Email Account" option.

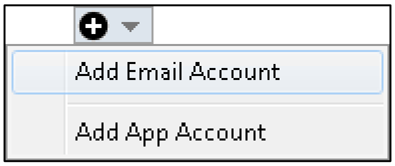
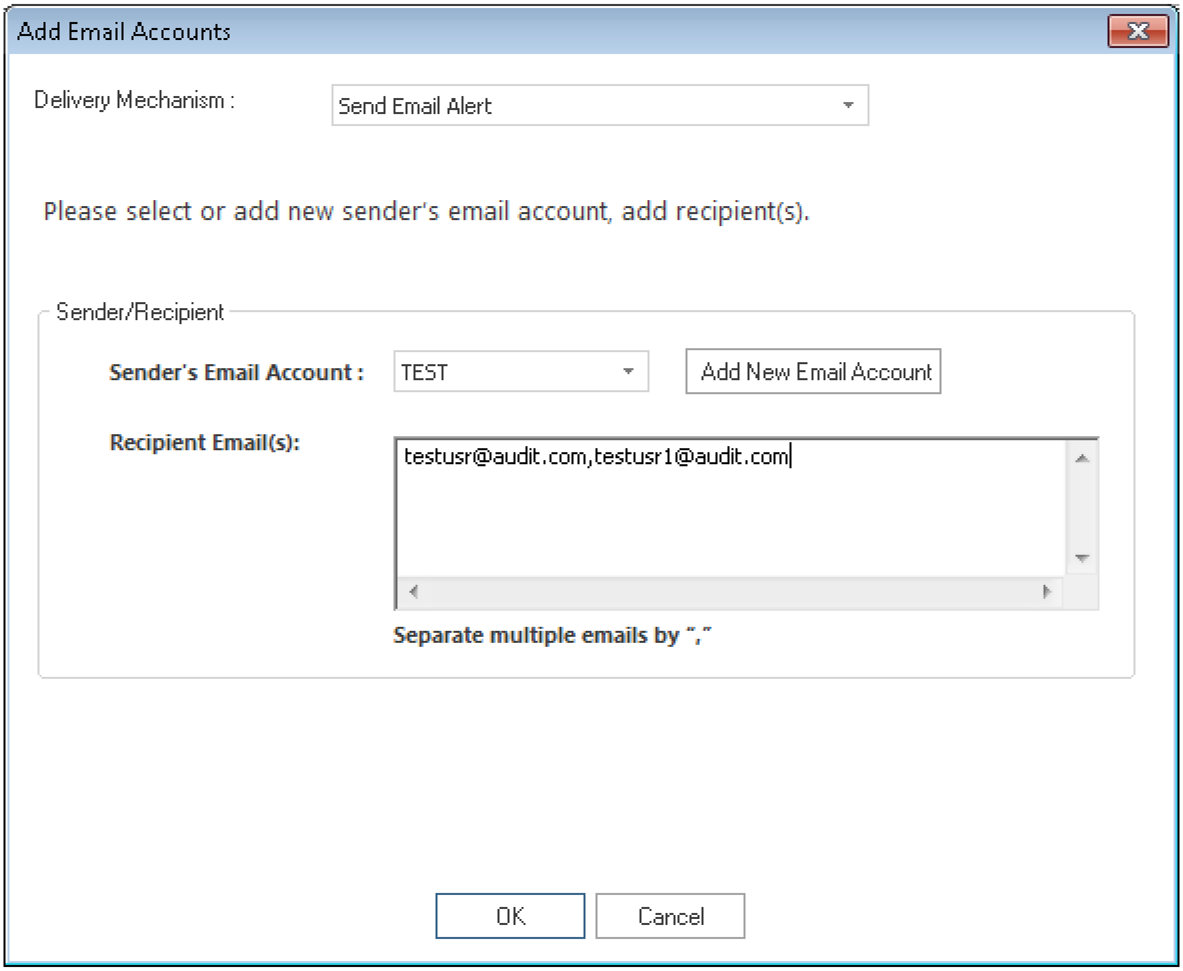


Figure 34: Option to add an email account

Following wizard will open up. Populate the required fields as described below.


Add Email Accounts

Delivery Mechanism : Send Email Alert

Please select or add new sender's email account, add recipient(s).

Sender/Recipient

Sender's Email Account : TEST

Recipient Email(s): testusr@audit.com,testusr1@audit.com

Separate multiple emails by ","

Figure 35: Add Email Account

Enter the following details:

1. **Display Name:** Provide a name that will be used as the profile name.
2. **Sender's Email ID:** Enter the email address that will be used to send emails.
3. **Logon Name:** Enter the login name for your email address. This name will be used by the software to login on the provided Email Server on your behalf.
4. **Password**: Provide the required password for the provided logon name.
5. **Server Name:** Enter the server name or IP Address of your email ID. The software will use this value to find out the email server and ping it.
6. **Port:** Enter the port number for SMTP connection (the default port number is 25).The software will try to connect to the SMTP Server at this port.
7. **Requires a secure connection (SSL)**: Check this box if you want the software to connect to your email server using SSL.
8. **Send Test Email**: Use this option to send a test mail to check the authenticity of the details provided here. It is **recommended** to perform this step before moving ahead.

Thus, the following email account will be added in software under "Delivery Message Settings". This email account will be used to send emails. You can add more email accounts for using different account for different purposes.

Other available options in this section are:

✕ Use this icon to remove an added email account

✎ Use this icon to modify details in an existing email account. Just select the account from the list and click on this button. Change the required values and click the "OK" button to make changes.

⇅ Use this icon to refresh changes and display the latest changes in the Email Account list, if any.

5.4.2 App Account

An App Account will send the delivery notifications to Mobile Application of LepideAuditor Suite.

Software lets you add app accounts, modify and remove existing. The added email account(s) are used to send real-time alerts and scheduled reports.

To add an email account, click on the ⊕▾ button and select "Add Email Account" option.

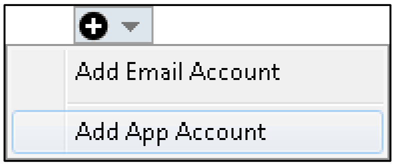
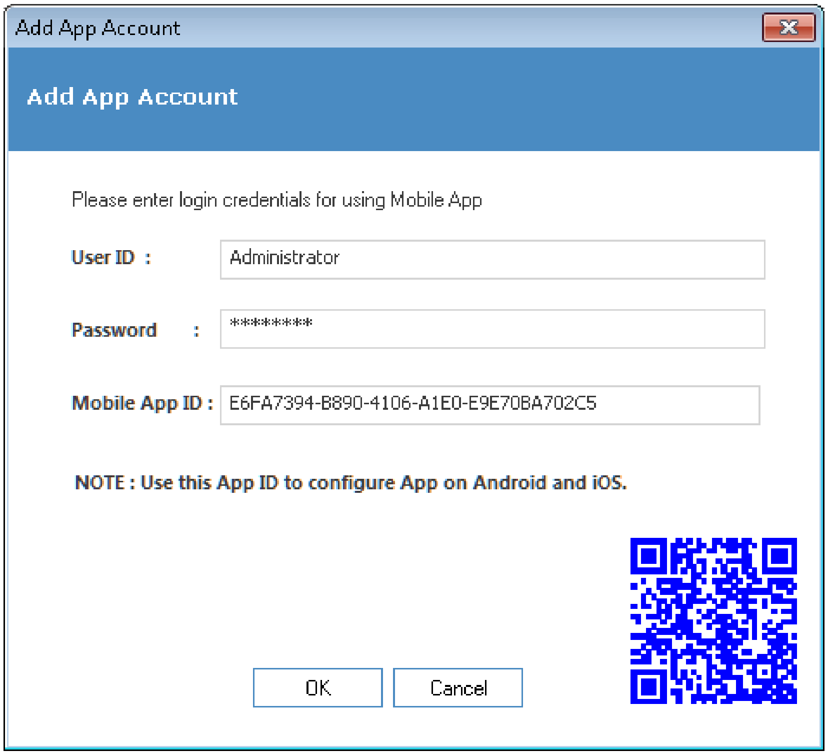


Figure 36: Option to add an App Account

Following wizard will open up. Populate the required fields as described below.



Please enter login credentials for using Mobile App

User ID : Administrator

Password : *********

Mobile App ID : E6FA7394-B890-4106-A1E0-E9E70BA702C5

NOTE : Use this App ID to configure App on Android and iOS.

Figure 37: Dialog box to add an App Account

Enter the following details:

1. **User ID:** Provide a user ID with which you will create a profile in Mobile Application.

2. **Password:** Enter the password for the user ID with which you will login in Mobile Application.

3. **Mobile App ID:** Note down the Application ID and use it to create the profile in mobile application.

Click “OK”. Thus, the following email account will be added in software under “Delivery Message Settings”. This app account will be used to send notifications to the installed mobile application “LepideAuditor App”. You can add more app accounts for using on different applications of different phones. However, one account should be used for only one application.

Other available options in this section are:

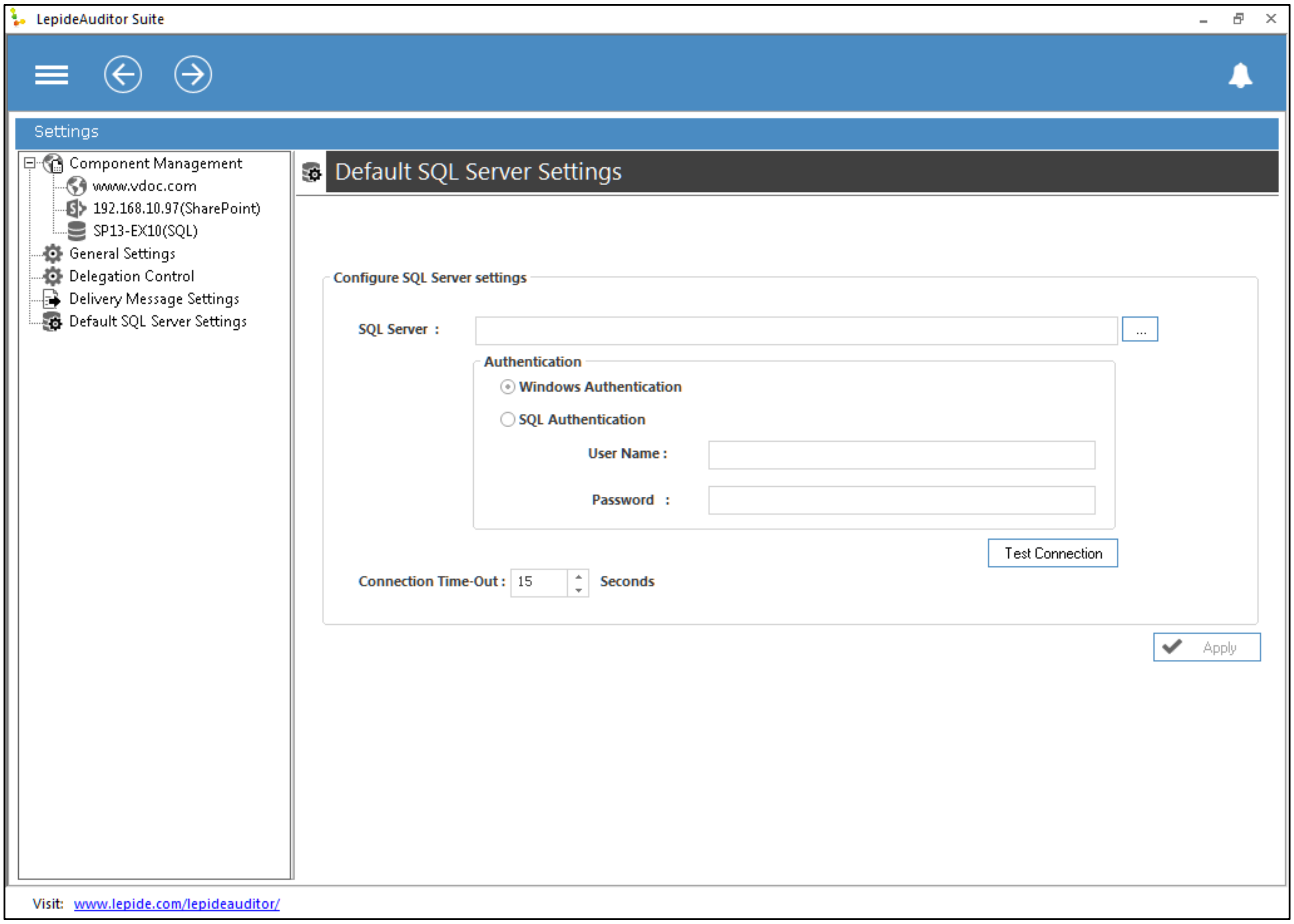
✕ Use this icon to remove an added App account

✎ Use this icon to modify details in an existing App account. Just select the account from the list and click on this button. Change the required values and click the "OK" button to make changes.

⇅ Use this icon to refresh changes and display the latest changes in the App Account list, if any.

5.5 Default SQL Settings

This setting lets you configure the default SQL Server for storing logs for software.



Default SQL Server Settings

Configure SQL Server settings

SQL Server :

Authentication

● Windows Authentication

○ SQL Authentication

User Name :

Password :

Connection Time-Out : 15 Seconds

Figure 38: Default SQL Server Settings

Follow the steps below to configure this setting,

1. Software lets you connect to a local or networked SQL Server. You can either enter the name of SQL Server manually in the text box or click [...] to enumerate all SQL Servers in a list and select the desired one in the following box.

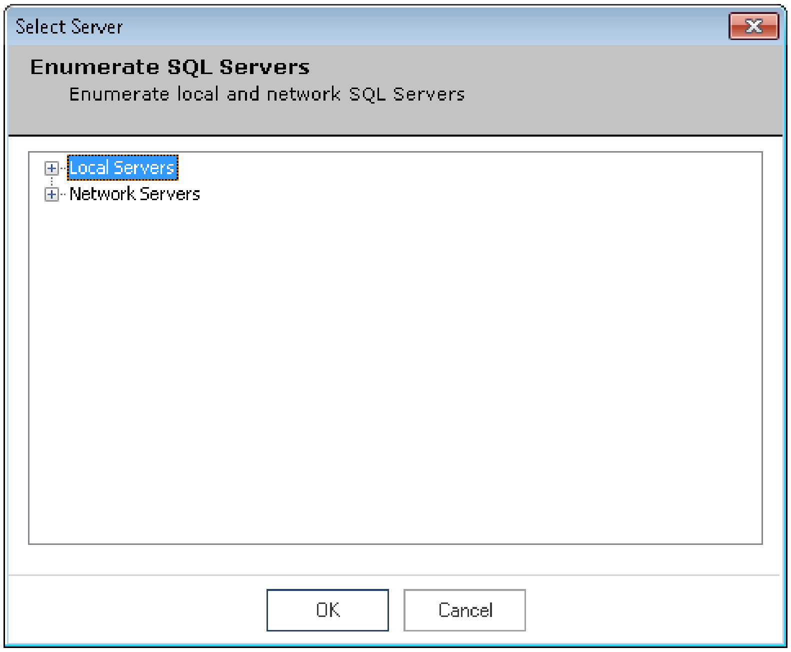


Figure 39: Select a SQL Server

2. Click ⊞ icon to expand the listings for local and network servers. You can click ⊟ icon to collapse the list.

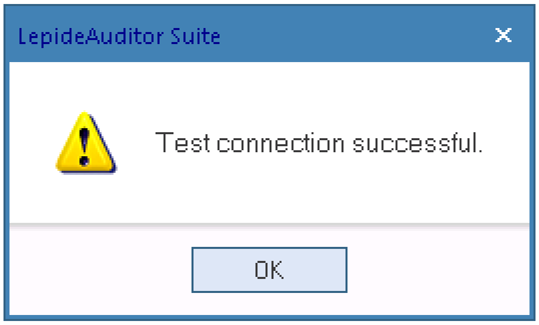
3. Select a server and click "OK" button. This will take you back the "SQL Server Settings" box, which will now show the selected SQL Server.

4. You've to select any of the following authentication types.

   a. **Windows Authentication:** It will let the software login at SQL Server using the credentials of that user with which you're logged in at the computer currently.

   b. **SQL Server Authentication:** It will let you provide the username and password of a SQL Server user.

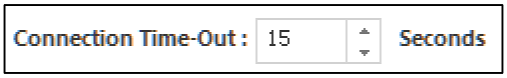
5. Click Test Connection to test the connection between the software and the selected SQL Server with the provided details. This will either display an error if failed to connect or shows the following message confirming the successful connection.



Test connection successful.

Figure 40: Tested the connection

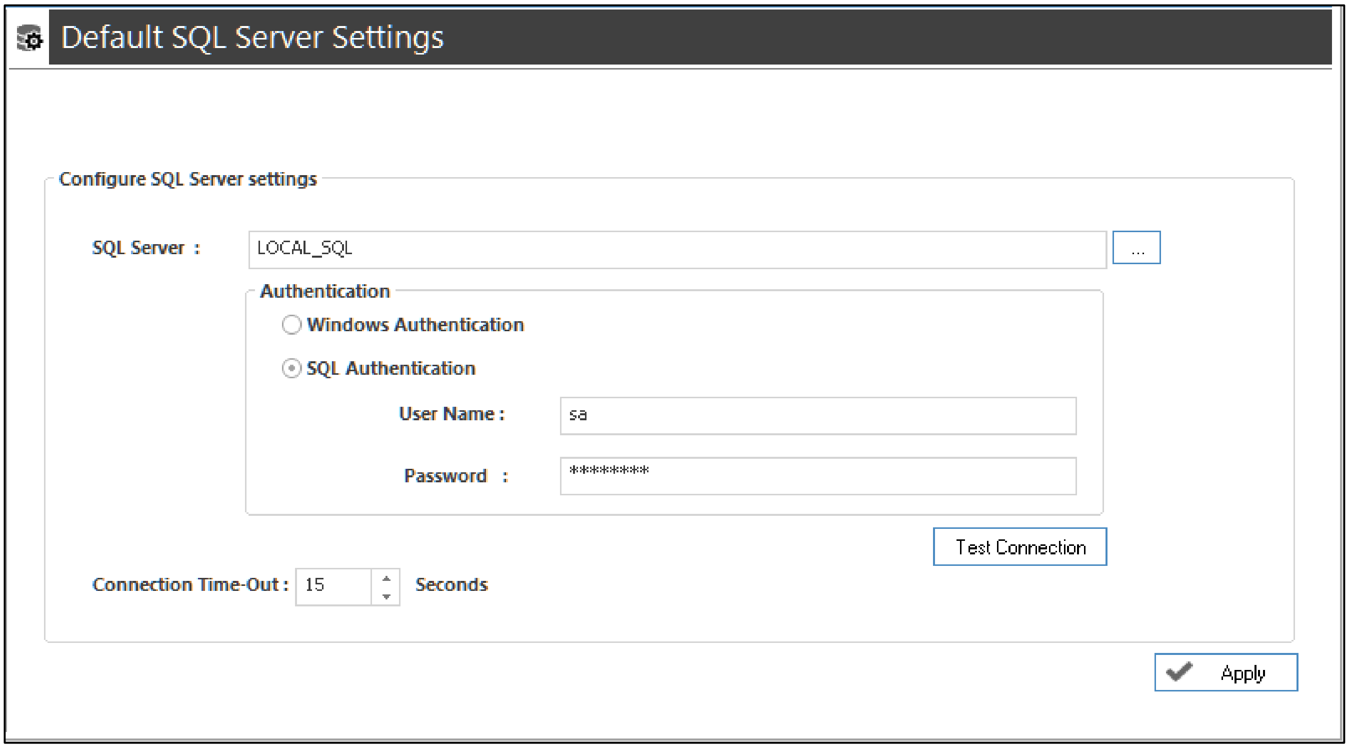
6. Bottom section deals with the connectivity timeout period between the software and SQL Server. You can use its buttons to increase/decrease the values or provide a manual value for it.



Connection Time-Out : 15 Seconds

Figure 41: Connection time-out setting

7. Following is a snapshot of the dialog box containing the sample details, where we've selected to login with SQL Server Authentication mode.



Default SQL Server Settings

Configure SQL Server settings

SQL Server : LOCAL_SQL

Authentication

○ Windows Authentication

● SQL Authentication

User Name : sa

Password : *********

Connection Time-Out : 15 Seconds

Figure 42: Default SQL Server

5.5.1 Using the Default SQL Server Settings

At a screen where you have to provide the details of SQL Server for storing or retrieving auditing logs, you will receive either anyone or both of the following buttons.

1. : Click it to save the current Database Settings as the default SQL Server, which will be displayed as default in "SQL Server Settings".

2. : Click it to load the Database Settings from the default SQL Server configured in "SQL Server Settings".

Thus, you can perform the basic settings required for preliminary software usage following the above-mentioned steps.

6. Conclusion

After following the above mentioned steps, you will start receiving audit reports and see dashboard details. In order to create alerts and schedule reports for accessing complete software features, check the software help manual: http://www.lepide.com/lepideauditor/

Thus, LepideAuditor Suite can be easily configured and used to audit Active Directory, Group Policy Objects, Exchange Servers, SharePoint and SQL Servers. Real-time auditing, Dashboard reports in graphical format and LiveFeed add a definite edge to this application. Moreover, email alerts, scheduled reports and options to restore AD state make it a one-stop solution for all Auditing purposes.

To read more about the software visit: http://www.lepide.com/lepideauditor/

For software related queries, you can contact us at:

Helpline: +1-800-814-0578

For support or any other queries, drop a mail at:

For General Queries:	contact@lepide.com
For Sales:	sales@lepide.com
For Technical Support:	support@lepide.com