Lepide

CONFIGURATION GUIDE

THE PRINCIPLE OF LEAST PRIVILEGE FOR ACTIVE DIRECTORY

Table of Contents

1. Introduction

The purpose of this document is to detail the minimum rights and privileges required for configuring the Lepide Active Directory component for auditing and the steps which are needed to complete the configuration for a successful setup.

2. Least Privilege Model for Active Directory, Group Policy and Exchange On-Premises

2.1. What's Available with the Least Privilege Model?

a. All AD/GPO/Exchange Modification reports, i.e. States and Changes.

b. Real time alerts and Schedules.

c. Full reporting under Web Console.

d. AD and GPO Backups.

e. AD and GPO State Reports.

f. Lepide Active Directory Cleaner.

g. Lepide User Password Expiration Reminder.

h. All AD/GPO Risk Analysis Reports.

i. Agent-Less Auditing

2.2. What's Not Available with the Least Privilege Model?

a. AD and GPO Restore.

b. Non-Owner Mailbox Auditing under Exchange.

c. Health Monitoring.

d. Automatic Enabling of the Native Auditing from the DCs. (This is a one time process and can be done manually)

e. Automatic Event Log Management of the DCs.

f. Data Discovery and Classification of Exchange Mailboxes.

g. Agent Based Auditing.

2.3. Minimum Rights Required

a. A Domain User Account.

b. This account should have **Db_owner/Db_creator** rights over the SQL databases. An SQL account with the mentioned privileges can also be used.

c. This account should be a member of the **Event Log Readers** group inside AD.

d. This account should be a member of the **Administrators** Group on the Lepide Server.

e. This account should be a member of **Organization Management** group inside AD for Exchange Auditing.

2.4. Setting up the Account Privileges

1. Create a user account in Active Directory and add it under the **Event Log Readers** group.

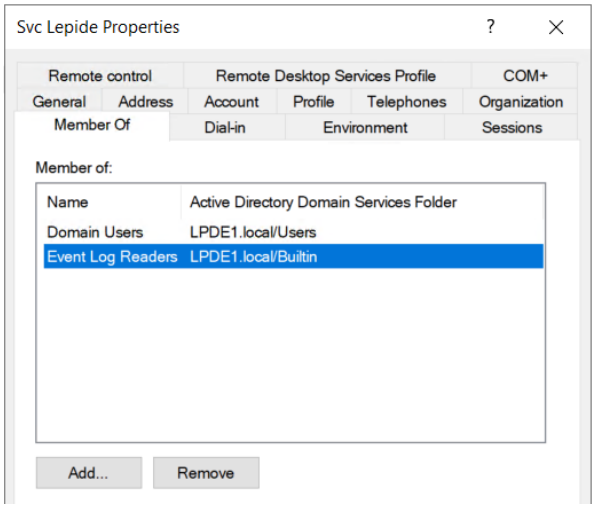

Figure 1: Add User Account in Active Directory

2. Add this user account under the **Local Admin Group** on the Lepide Server. To do this, follow the steps below:

   i. In the **Run** window, type **mmc** and press **Enter**.

   The following screen will be displayed:

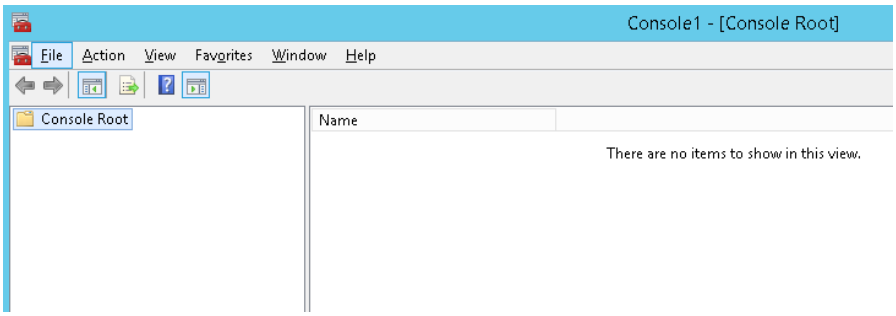

Figure 2: Microsoft Management Console

ii. From the File Menu, choose **Add/Remove Snap-IN**.

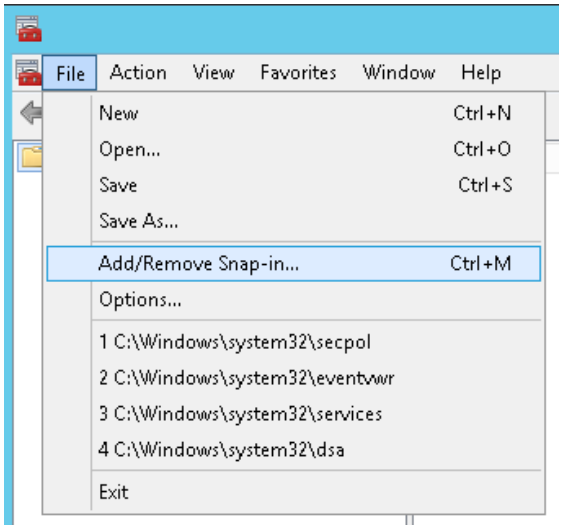

Figure 3: File Menu

The following dialog box is displayed:

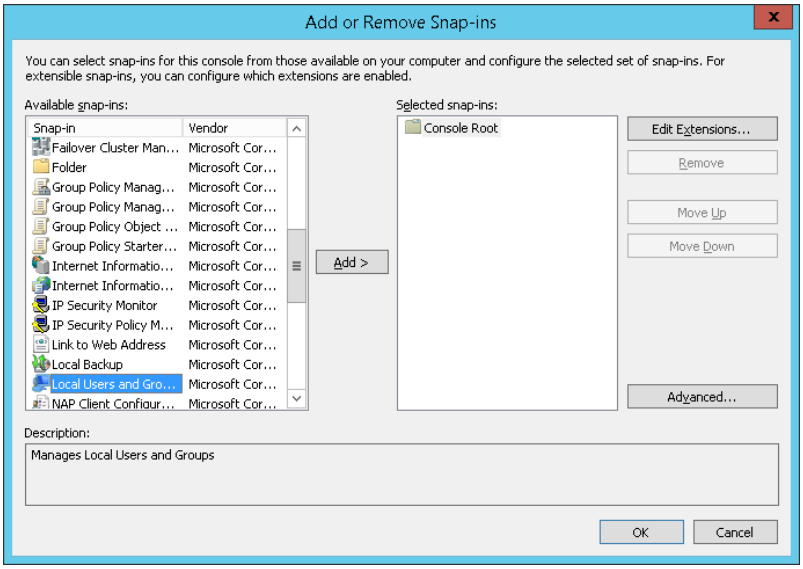

Figure 4: Add or Remove Snap-ins

i. Choose Local Users and Groups

ii. Click **Add**

The following dialog box is displayed:

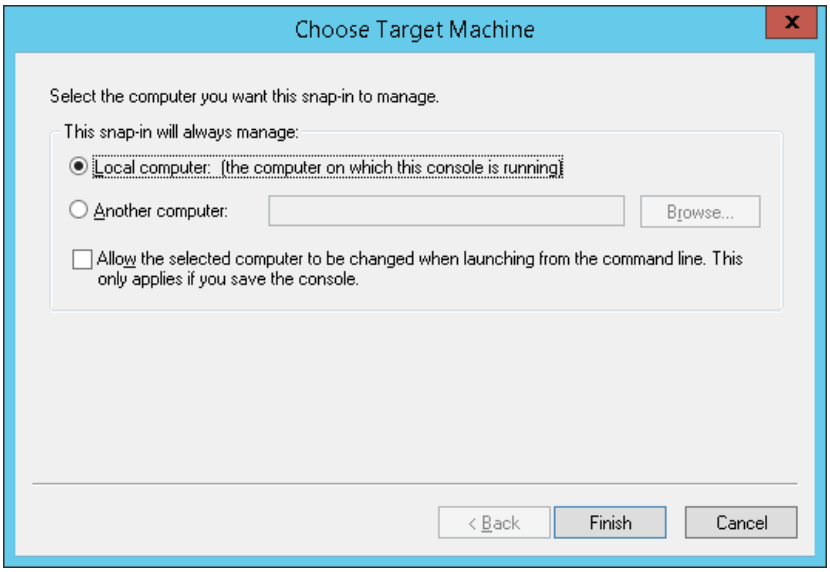

Figure 5: Choose Target Machine

iii. Select **Local computer**

iv. Click **Finish**

v. Click **OK**

1. When the **Choose Target Machine** wizard is closed, the **Local Users and Group** node is added to the console:

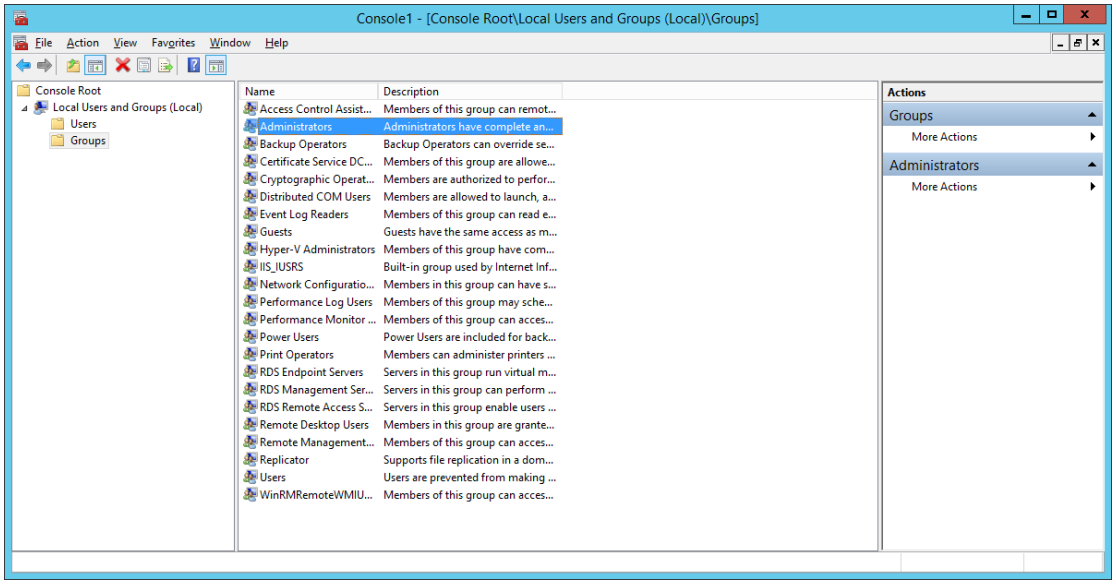

Figure 6: Microsoft Management Console

2. Select **Administrator** from the middle pane and double click.
3. The Administrators Properties dialog box is displayed:

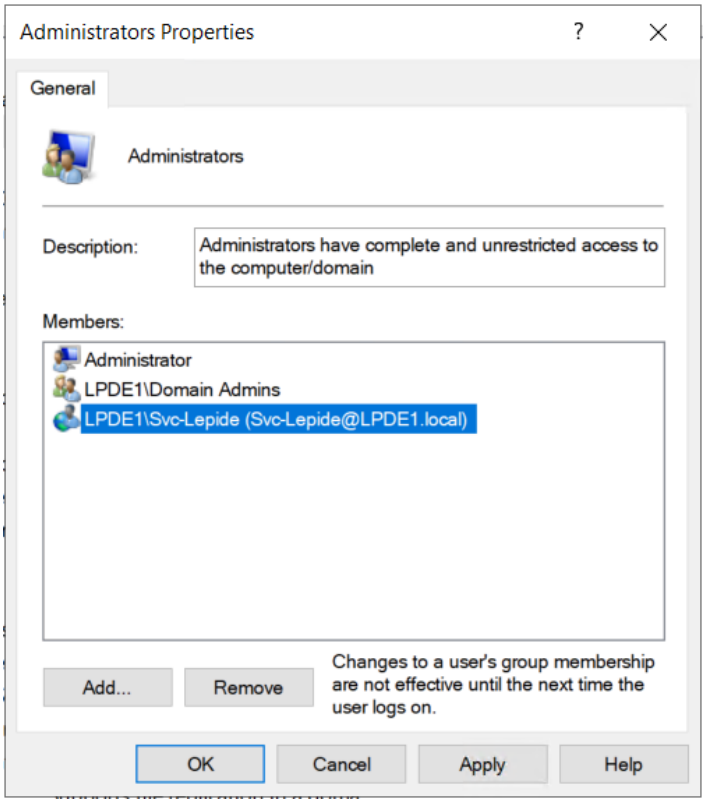

Figure 7: Administrators Properties

4. From the Administrators Properties window, add the newly created user with default access rights.
5. Log in to the Lepide Server using the newly created user credentials.
6. Open **ADSIEdit** and provide access rights to the newly created user using the different naming context of Active Directory.
7. To do this, follow these steps:
    i. From the **Run** window, type **ADSIEDIT.msc** and press **Enter**:
    ii. Right click on the ADSI Edit node and Select **Connect to....**

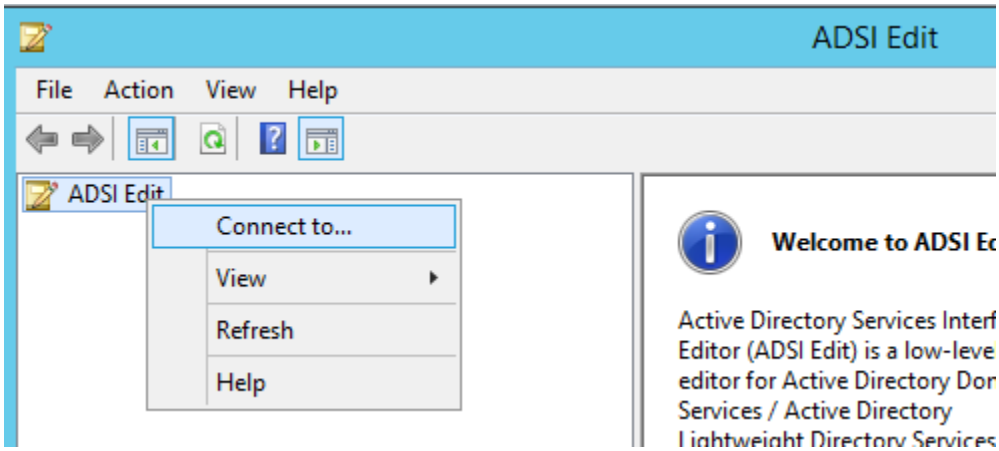

Figure 8: Connect To.. Menu

iii. From the Connection Settings dialog box, select **Default naming context** and click **OK**

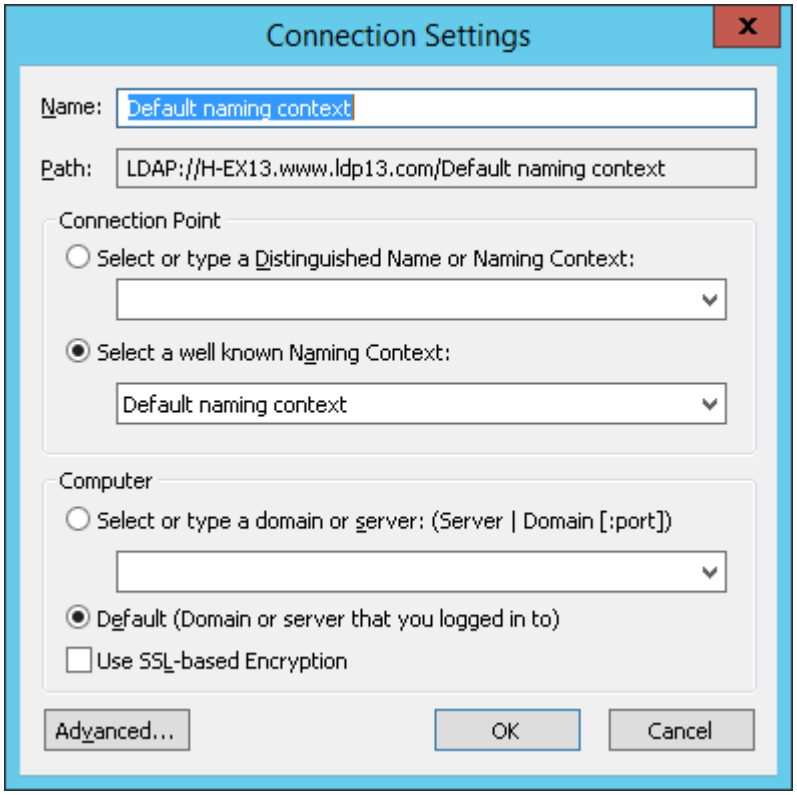

Figure 9: Connection Settings

iv. The **Default Naming context** node will be added to the console.

v. Expand **Default naming context** node and right click on the domain name node as shown below:

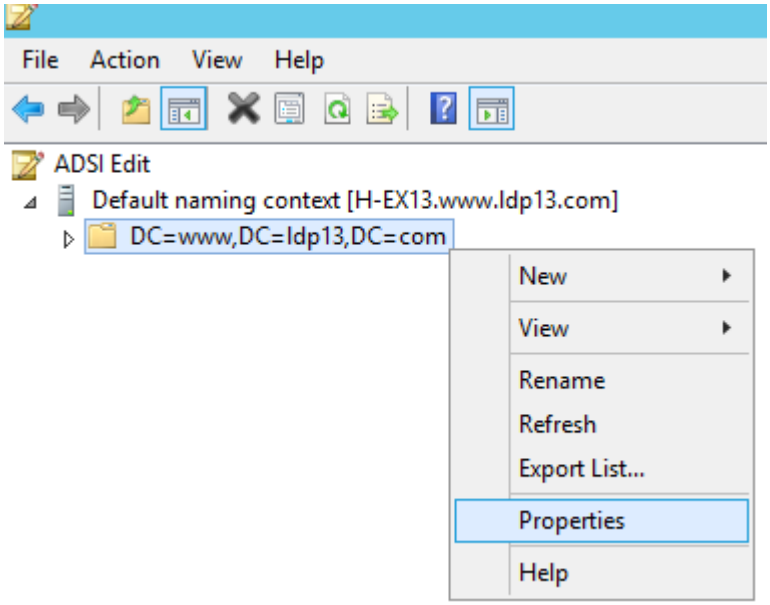

Figure 10: Select Properties

vi. From the Properties window, add the newly created user with default access rights:

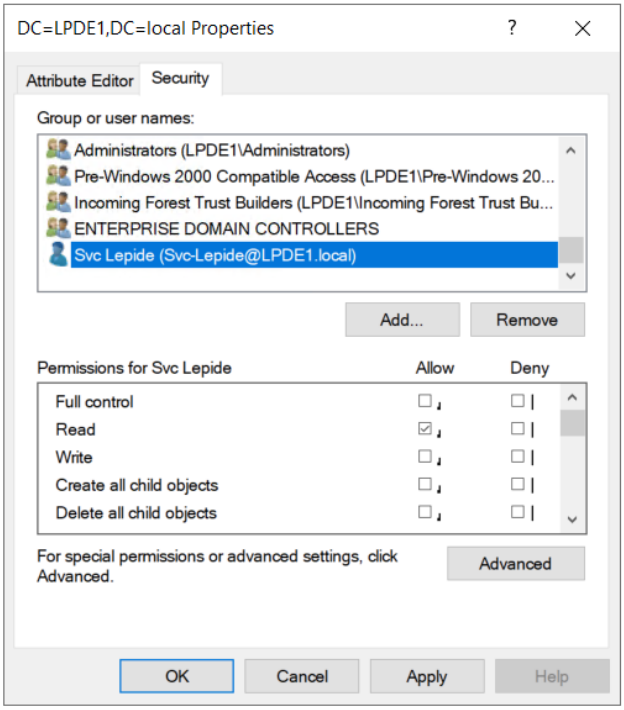

Figure 11: Properties

vii. Repeat the steps above to add another naming context.

Please do not give any permissions to **RootDSE**, as the rights will not be accepted.

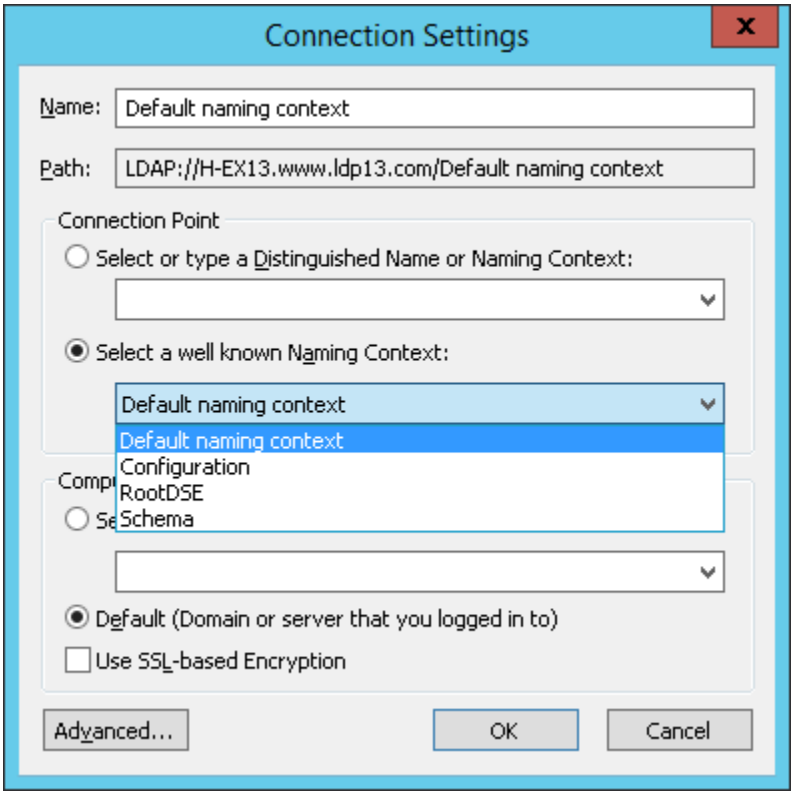

Figure 12: Connection Settings

1. From the Properties dialog box, select **Organization Management**:

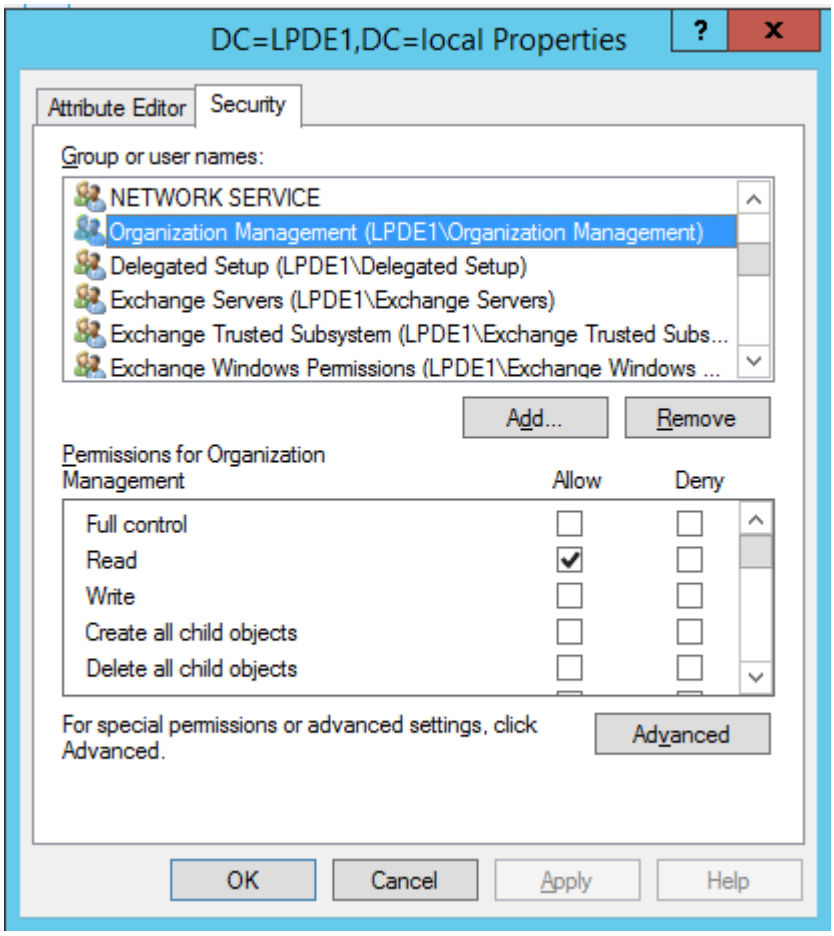

Figure 13: Properties

2. Give **Full Control** access rights to this account on the installation folder (C:\Program Files (x86)\LepideAuditor Suite).
3. Configure the Lepide service with the newly created user.
4. In SQL, create a login by adding the newly created user and selecting **DB Creator** as the role.
5. For Active Directory Cleaner, select Delegation Control for this user account:

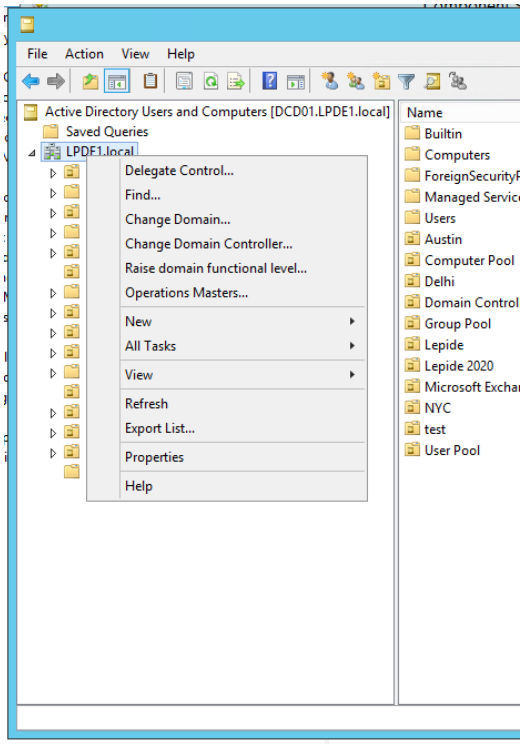

Figure 15: Delegate Control

The Delegation of Control Wizard will start:

Figure 14: Delegation of Control Wizard

6. Click **Next**

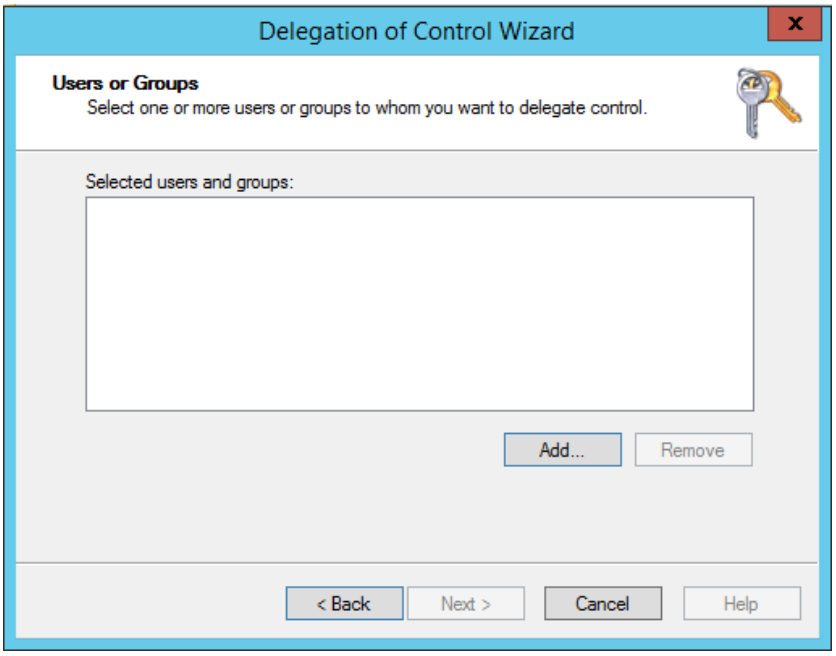

Figure 16: Add User

7. Click **Add** to add a user

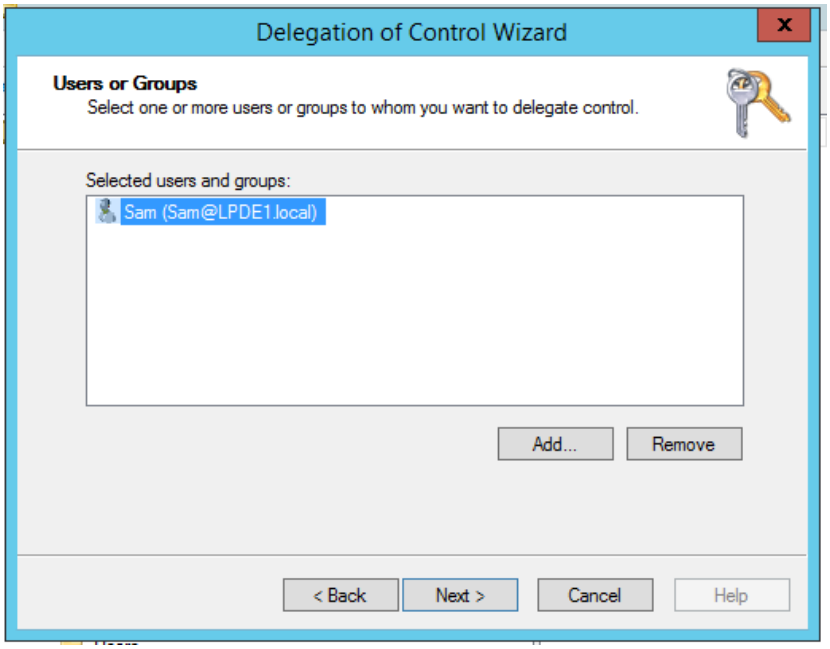

Figure 17: Added User

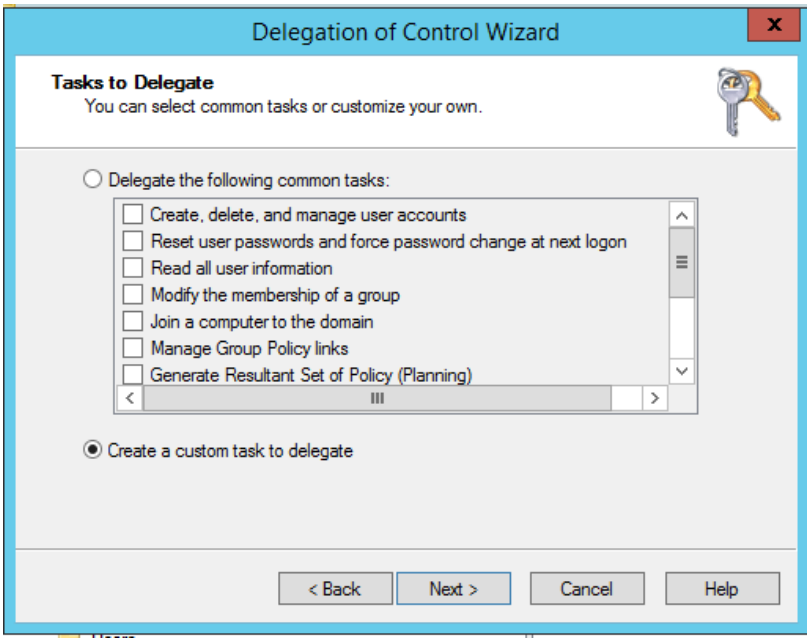

Figure 18: Tasks to Delegate

8. Select **Create a custom task to delegate**
9. Select **User Objects** and **Computer Objects** from the list

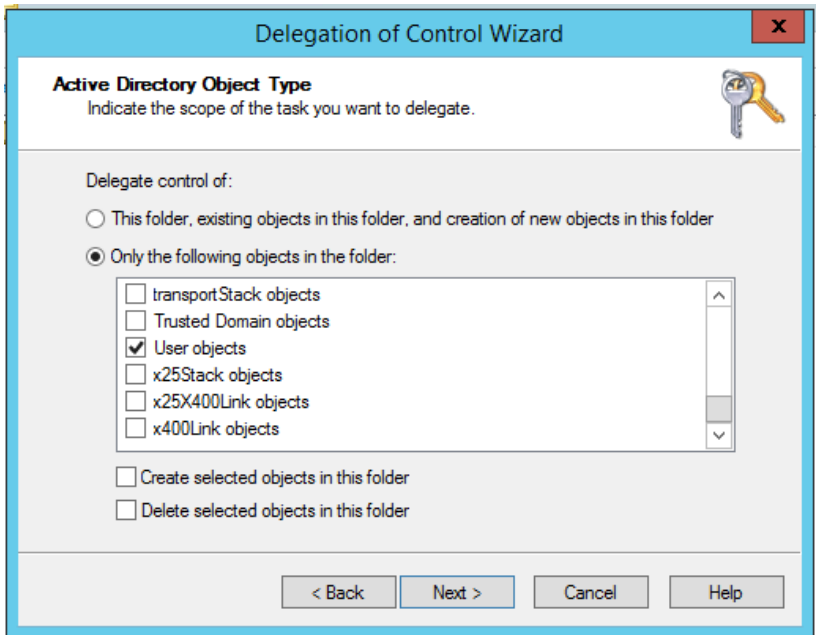

Figure 19: Active Directory Object Type

10. Click **Next**

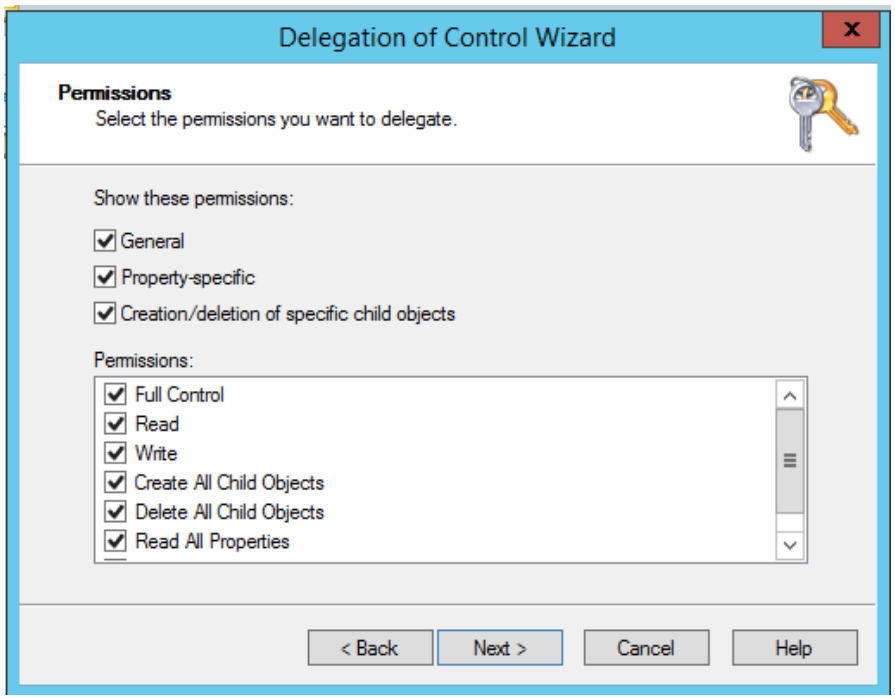

Figure 20: Permissions

11. Select the **Permissions** to delegate
12. Click **Next**

The last step of the Wizard will appear with a summary of delegation of control you have set up:

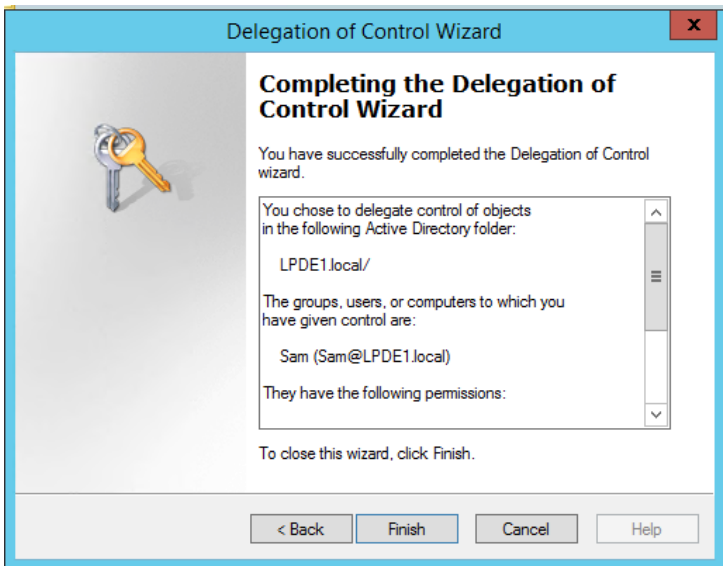

Figure 21: Summary of Delegation of Control

13. Click **Finish**

NOTE:	A new account must be created for using AD Cleaner and then the Lepide server should be logged on with the same account.

3. Support

If you are facing any issues whilst installing, configuring or using the solution, you can connect with our team using the below contact information.

Product Experts

USA/Canada: +1(0)-800-814-0578

UK/Europe: +44 (0) -208-099-5403

Rest of the World: +91 (0) -991-004-9028

Technical Gurus

USA/Canada: +1(0)-800-814-0578

UK/Europe: +44 (0) -208-099-5403

Rest of the World: +91(0)-991-085-4291

Alternatively, visit https://www.lepide.com/contactus.html to chat live with our team. You can also email your queries to the following addresses:

sales@lepide.com

support@lepide.com

To read more about the solution, visit https://www.lepide.com/data-security-platform/.

4. Trademarks

Lepide Data Security Platform, Lepide Data Security Platform App, Lepide Data Security Platform App Server, Lepide Data Security Platform (Web Console), Lepide Data Security Platform Logon/Logoff Audit Module, Lepide Data Security Platform for Active Directory, Lepide Data Security Platform for Group Policy Object, Lepide Data Security Platform for Exchange Server, Lepide Data Security Platform for SQL Server, Lepide Data Security Platform SharePoint, Lepide Object Restore Wizard, Lepide Active Directory Cleaner, Lepide User Password Expiration Reminder, 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.

Microsoft®, Active Directory®, Group Policy Object®, Exchange Server®, Exchange Online®, SharePoint®, and SQL Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

NetApp® is a trademark of NetApp, Inc., registered in the U.S. and/or other countries.