



CONFIGURATION GUIDE

# NASUNI FILE SERVER QUICK START GUIDE

# Table of Contents

1	Introduction .....	3
2	Requirements and Prerequisites .....	3
2.1	Basic System Requirements.....	3
2.2	Supported Servers for Auditing .....	4
2.3	Supported Protocols.....	4
3	Nasuni .....	4
3.1	Prerequisites to Audit Nasuni.....	4
3.2	Service Rights.....	5
3.3	Local System Rights .....	5
3.4	Add Nasuni.....	5
3.5	Editing the Nasuni Credentials .....	13
4	Support.....	15
5	Trademarks.....	15

# 1 Introduction

The Lepide Data Security Platform provides a comprehensive way to provide visibility across Active Directory, Group Policy, Exchange on-premises, M365, SharePoint, SQL Server, Windows File Server, NetApp Filer, EMC Isilon, Nasuni and every platform which can provide an integration with Syslogs and RestAPI.

This guide takes you through the process of standard configuration of the Lepide Data Security Platform for Nasuni.

If you have any questions at any point in the process, you can contact our Support Team. The contact details are listed at the end of this document.

## 2 Requirements and Prerequisites

Before you start installing the Lepide Data Security Platform for File Server, make sure that your computer meets the following requirements:

### 2.1 Basic System Requirements

- Required Processor
  - Minimum dual-core processor
  - Recommended quad-core processor
- Required RAM
  - Minimum 4 GB RAM
  - Recommended 8 GB RAM
- Required free disk space
  - Minimum 1 GB
  - Recommended 2 GB
- Any of the following 32-bit or 64-bit Windows Operating Systems.
  - Windows Server OS: 2016, 2019 and 2022 (latest)
- Any of the following SQL Servers (local or network hosted) for storing auditing logs:
  - Any SQL Server above and including SQL Server 2016 (standard or enterprise)
    - .NET Framework 4.6.2 developer pack and above

## 2.2 Supported Servers for Auditing

Audited Servers	Supported Versions
Nasuni	NMC 23.3.6 or above

## 2.3 Supported Protocols

- UDP - User Datagram Protocol

# 3 Nasuni

## 3.1 Prerequisites to Audit Nasuni

- Pre-requisite to audit Nasuni:
  - Login to Nasuni NMC and Enter the Credentials
  - Click on the Filer Navbar tab and then click on Syslog Export Setting on the left navigation bar
  - Select the Particular filer and then click the Edit Filer Button
  - After clicking on the Edit Filer Button, the Filer Syslog Export Settings Wizard Will Open. Enter the Server IP and Port where you need to send the Syslog Forwarding and then click on Save Setting.
  - Do not use port 0 or port 514. Port 514 is already reserved for another component.
  - Make sure your NMC and Filer have an internet connection for creating a volume or changing the port for syslog forwarding.

**NOTE:** Auditing for all events, **except Denied Events**, is captured in our environment.

## 3.2 Service Rights

- Nasuni users can access the Nasuni APIs whether as a native user or domain user which is created in Nasuni. However, a native user cannot access the shared folder.
- Requirement to get Permission Changes: if a volume is created, ensure that the volume is created in NTFS Exclusive Mode because if you need to check the auditing for permission and owner changes, it should only be done in NTFS Exclusive Mode.

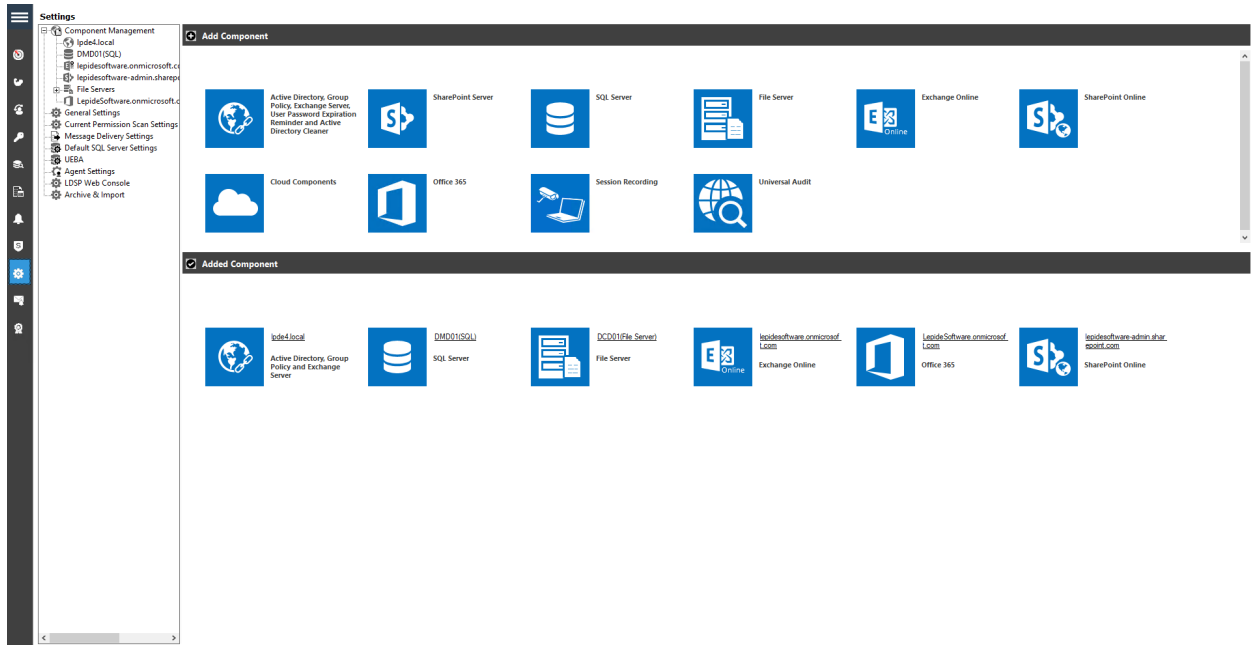
## 3.3 Local System Rights

- To run Lepide after installation, you can select any of the following:
  - A local system administrator (for permission and property changes in auditing)
  - A member of the domain admins group
- The user should have the following permissions on the local computer where the software is installed:
  - Full access permission to the drive on which the operating system is installed
  - Read/Write permissions in the registry

## 3.4 Add Nasuni

After you have installed the Solution and configured the Lepide service to run with administrative credentials, you can add a Nasuni File Server for auditing.

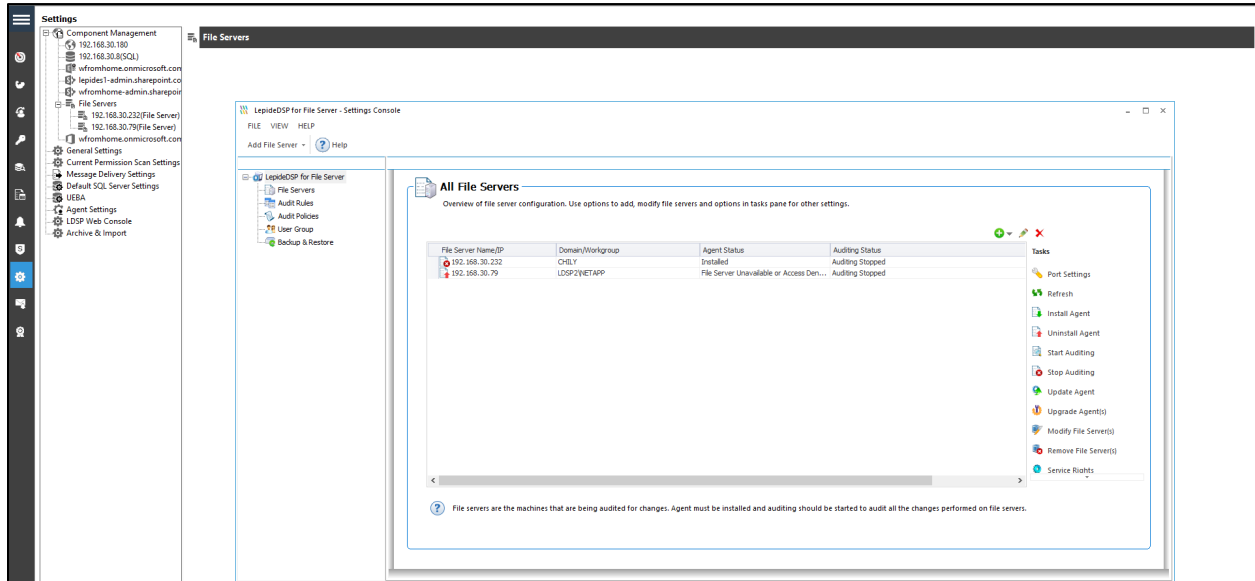





**Figure 1: Component Management Window**

1. From the Component Management window, under the **Add Component** section, click on the **File Server** icon to add this component to the solution.

The File Server Settings Console dialog box is displayed:

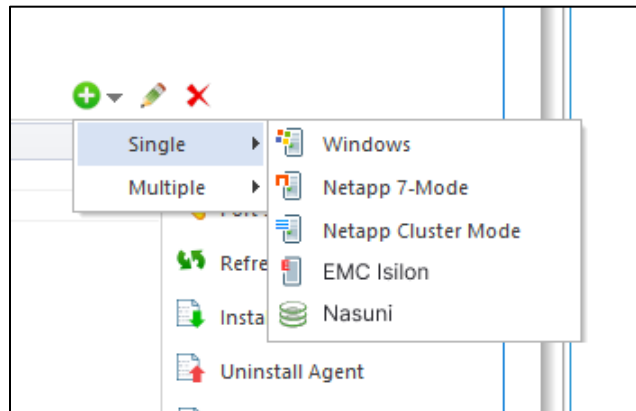


**Figure 2: File Server Console**

Here, you can click **Add File Server** icon  on the toolbar to add either of the following file servers:

- Windows File Server
- NetApp Filer
- EMC Isilon
- Nasuni

2. Click the **Add File Server** icon,  select **Single** then select **Nasuni**.



*Figure 3: Option to Add Nasuni File Server*

3. The **Add File Server** wizard starts:

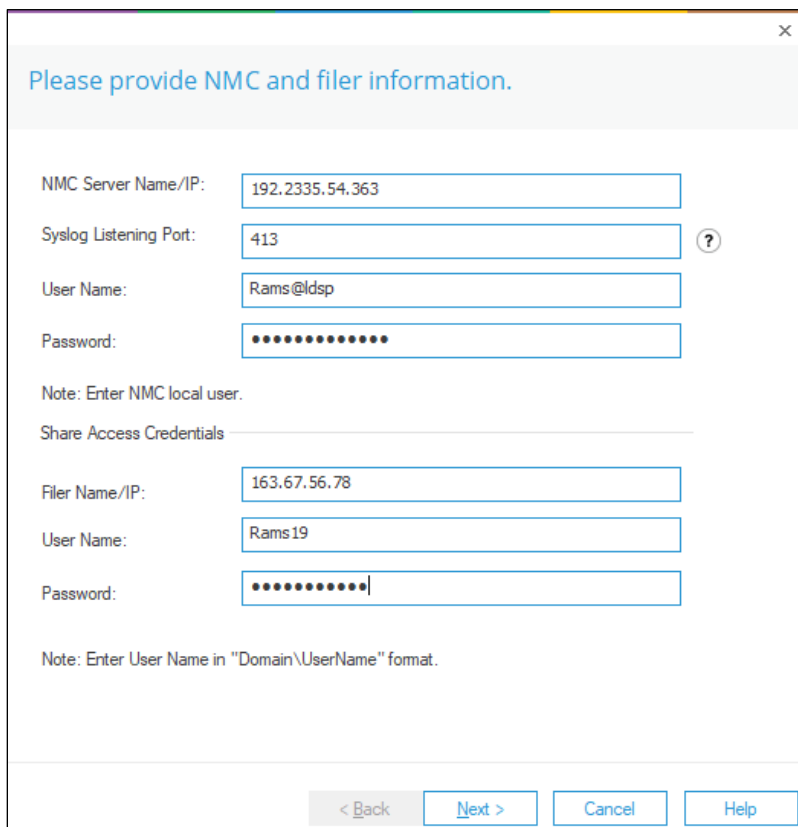


The screenshot shows a configuration window with the following elements:

- Title:** Please provide NMC and filer information.
- Fields:**
  - NMC Server Name/IP:
  - Syslog Listening Port:  (with a help icon)
  - User Name:
  - Password:
  - Share Access Credentials:
  - Filer Name/IP:
  - User Name:
  - Password:
- Notes:**
  - Note: Enter NMC local user.
  - Note: Enter User Name in "Domain\UserName" format.
- Buttons:** < Back, Next >, Cancel, Help

**Figure 4: NMC and Filer Information**

4. Add all the details for the NMC file server.
  - a. Add the NMC Name/IP, the Syslog Listing Port, the User Name and Password
  - b. Add the Share Access Filer Name/IP, User Name and Password



The screenshot shows a configuration window titled "Please provide NMC and filer information." with a close button (X) in the top right corner. The window is divided into two main sections: "NMC Server Information" and "Share Access Credentials".

**NMC Server Information:**

- NMC Server Name/IP: 192.2335.54.363
- Syslog Listening Port: 413 (with a help icon ?)
- User Name: Rams@ldsp
- Password: [Redacted]
- Note: Enter NMC local user.

**Share Access Credentials:**

- Filer Name/IP: 163.67.56.78
- User Name: Rams19
- Password: [Redacted]
- Note: Enter User Name in "Domain\UserName" format.

At the bottom of the window, there are four buttons: "< Back" (disabled), "Next >" (active), "Cancel", and "Help".

**Figure 5: NMC and Filer Information Completed**

5. Click **Next** to go to the next step, to provide the details of SQL Server to create a database for storing auditing logs.

Please Provide SQL Server information

Server Name :

Windows Authentication  SQL Server Authentication (Recommended)

User Name :

Password :

**Note :** Windows authentication credentials only applicable for insert data from file Server Directly

**Database Option :**

Create Database

Select Database

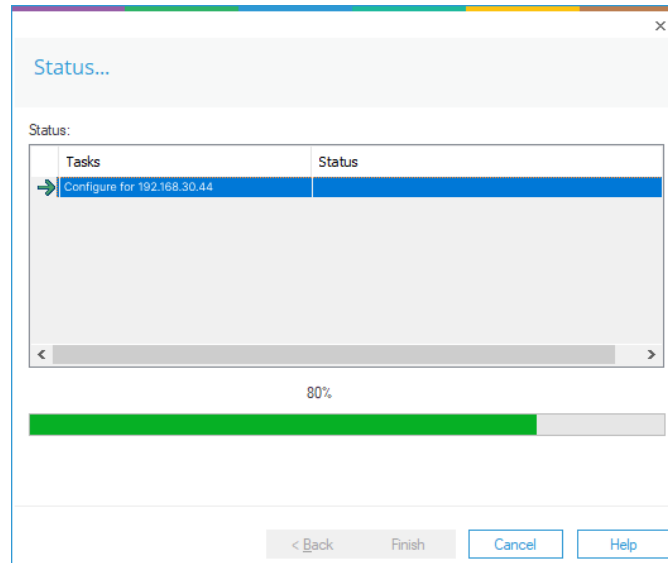
**Note :** If you do not have SQL Server installed then click this link to download SQL Express edition.  
<https://www.microsoft.com/en-in/education/products/microsoft-365>

< Back

**Figure 6: SQL Server Details to add Nasuni**

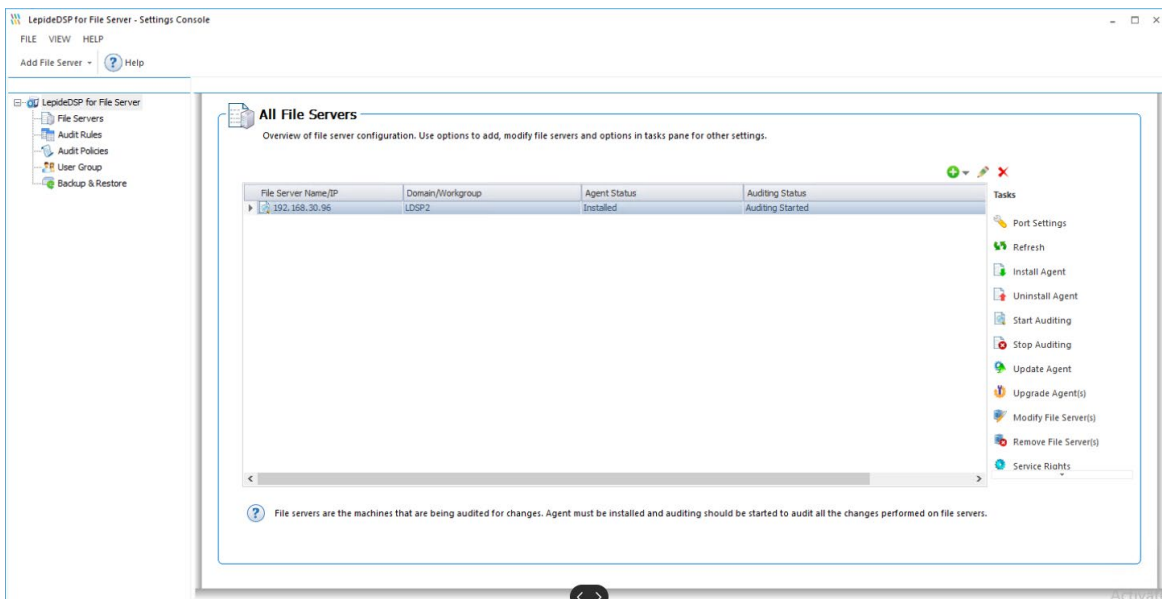
6. Enter the **Server Name** or click Browse to select the desired SQL Server.
7. There are two authentication options available:
  - **Windows Authentication:** This mode can be selected if SQL Server is installed on the same computer where the solution is installed.
  - **SQL Server Authentication:** Select this mode if SQL Server is installed on a remote or local computer. We recommend that this option is selected.
  - Provide the username and password of a SQL user, who has sufficient rights to create the database.
8. Enter a database name in the database name field to create a new database. You can also select an existing database created earlier by Lepide or another application.
9. Click **Next**

The Status dialog box is displayed:



**Figure 7: Status**

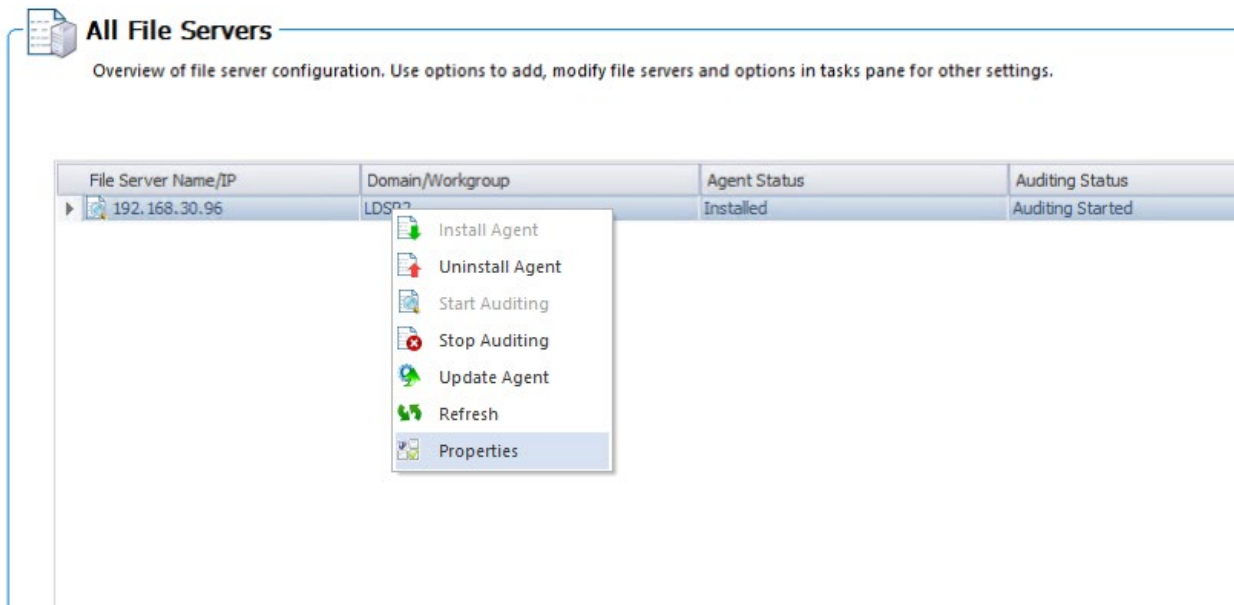
10. Once complete, click **Finish**
11. You will return to the Settings Console and the File Server will be listed with Auditing started:



**Figure 8: Settings Console with File Server Installed**

## 3.5 Editing the Nasuni Credentials

- To make changes to the credentials, right click on the File Server name and choose **Properties**



**Figure 9: Properties Menu**

The Properties dialog box will be displayed:

Specify the credentials which will be used to logon to the following file server.

File Server : 192.154.43.32

Domain/Workgroup : LDSP2

Agent Status: Installed

Audit Status: Auditing Started

Port : 413

User Name : Rams@ldsp

Password : \*\*\*\*\*

**Share Access Credentials**

User Name : Rams19

Password : \*\*\*\*\*

OK Cancel

**Figure 10: Properties**

- Make changes as required and click **OK** when finished

## 4 Support

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

### 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](mailto:sales@Lepide.com)

[support@Lepide.com](mailto:support@Lepide.com)

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

## 5 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.