Lepide

QUICK START GUIDE

AMAZON S3

Table of Contents

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 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 the Amazon S3 component. For information on installation, please see our Installation and Prerequisites Guide.

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 Prerequisites

The following are prerequisites to add an Amazon S3 component to the Lepide Data Security Platform:

- An S3 bucket needs to be created and the steps to do this can be found here: https://docs.aws.amazon.com/AmazonS3/latest/userguide/creating-bucket.html

3 Access Keys

Access keys are long-term credentials for an AWS Identity and Access Management (IAM) user or the AWS account root user. Access keys consist of two parts: an access key ID (for example, AKIAIOSFODNN7EXAMPLE) and a secret access key (for example, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY). You must use both the access key ID and secret access key together to authenticate your requests.

3.1 How to Manage Access Keys for your AWS Account

Follow these steps to manage access keys for your AWS account. For information about managing access keys for IAM users, see Managing Access Keys for IAM Users in the IAM User Guide.

3.1.1 To create, disable, or delete an access key for your AWS account root user

Use your AWS account email address and password to sign in to the AWS Management Console as the AWS account root user.

NOTE: If you previously signed in to the console with IAM user credentials, your browser might remember this preference and open your account-specific sign-in page. You cannot use the IAM user sign-in page to sign in with your AWS account root user credentials. If you see the IAM user sign-in page, choose **Sign-in using root user credentials** near the bottom of the page to return to the main sign-in page. From there, you can type your AWS account email address and password.

If you previously signed in to the console with IAM user credentials, your browser might remember this preference and open your account-specific sign-in page. You cannot use the IAM user sign-in page to sign in with your AWS account root user credentials. If you see the IAM user sign-in page, choose **Sign-in using root user credentials** near the bottom of the page to return to the main sign-in page. From there, you can type your AWS account email address and password.

1. On the **IAM Dashboard** page, choose your account name in the navigation bar, and then choose **My Security Credentials**.
2. If you see a warning about accessing the security credentials for your AWS account, choose **Continue to Security Credentials**.
3. Expand the Access keys (access key ID and secret access key) section.
4. Choose your preferred action:

To create an access key:

- Choose **Create New Access Key**. Then choose **Download Key File** to save the access key ID and secret access key to a file on your computer. After you close the dialog box, you can't retrieve this secret access key again.

To disable an existing access key

- Choose **Make Inactive** next to the access key that you are disabling. To reenable an inactive access key, choose **Make Active**.

To delete an existing access key

- Before you delete an access key, make sure it's no longer in use. For more information, see Finding unused access keys in the IAM User Guide. You can't recover an access key after deleting it. To delete your access key, choose **Delete** next to the access key that you want to delete.

4 Adding an Amazon S3 Component

The Lepide Data Security Platform tracks the changes inside Amazon S3 and gives detailed reporting on any configuration changes.

To add an Amazon S3 component:

- From the Component Management screen, click on **Cloud Components**:

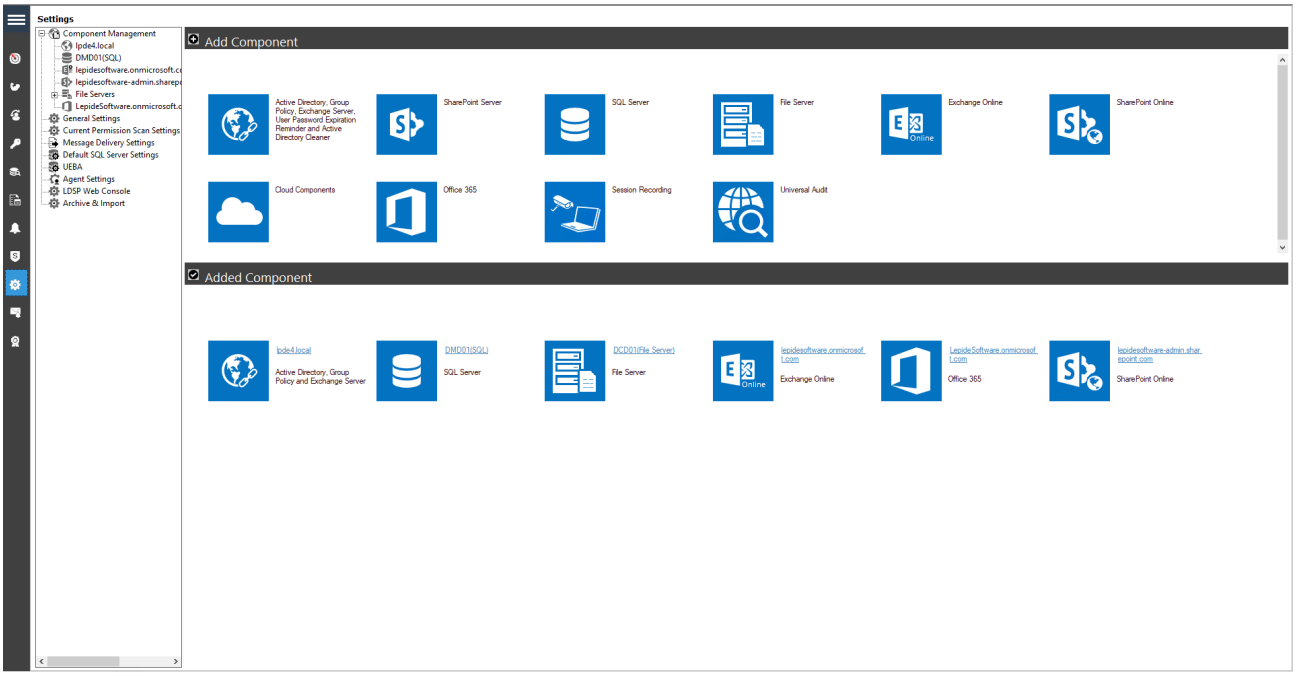

Figure 1: Component Management Screen

- Select Amazon S3 from the components displayed:

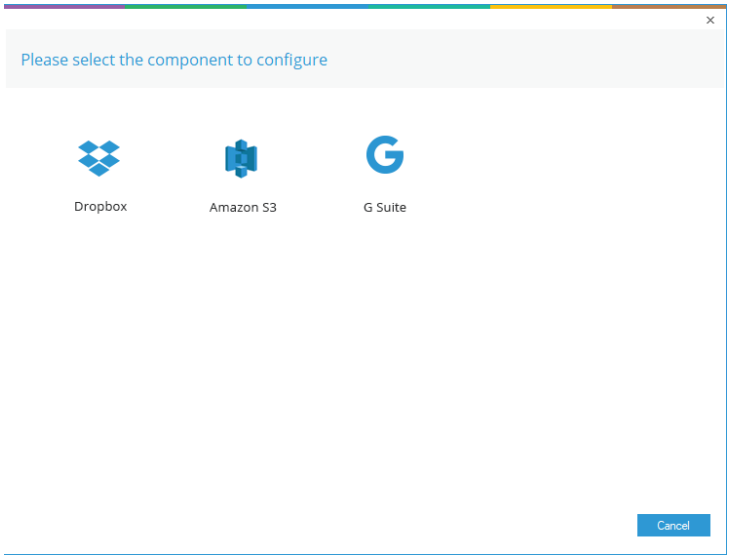

Figure 2: Select the Amazon S3 Component

The Authentication Information dialog box is displayed:

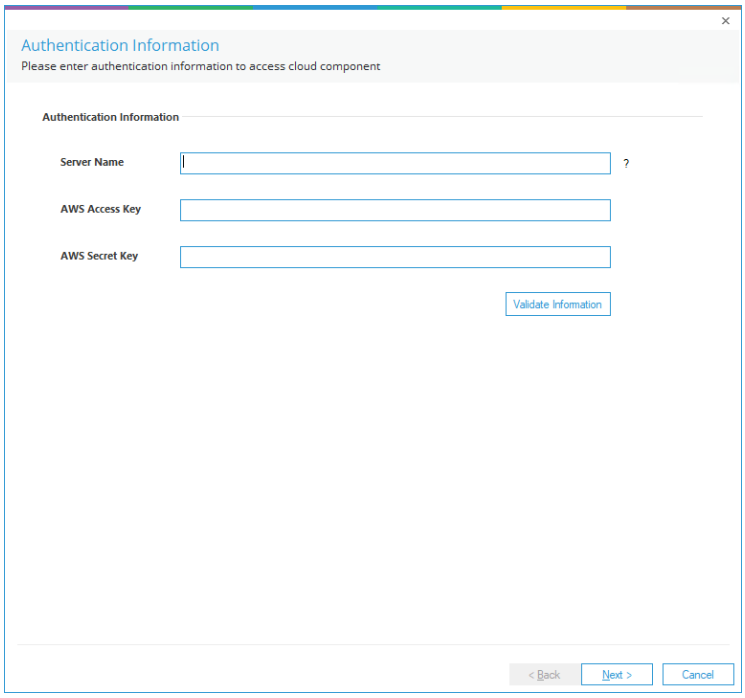

Figure 3: Authentication Information

- Enter the Server Name, the AWS Access Key and the AWS Secret Key

NOTE: The instructions to generate the **AWS Access Key ID** and **AWS Secret Key** are given in Section 3 - Access Keys.

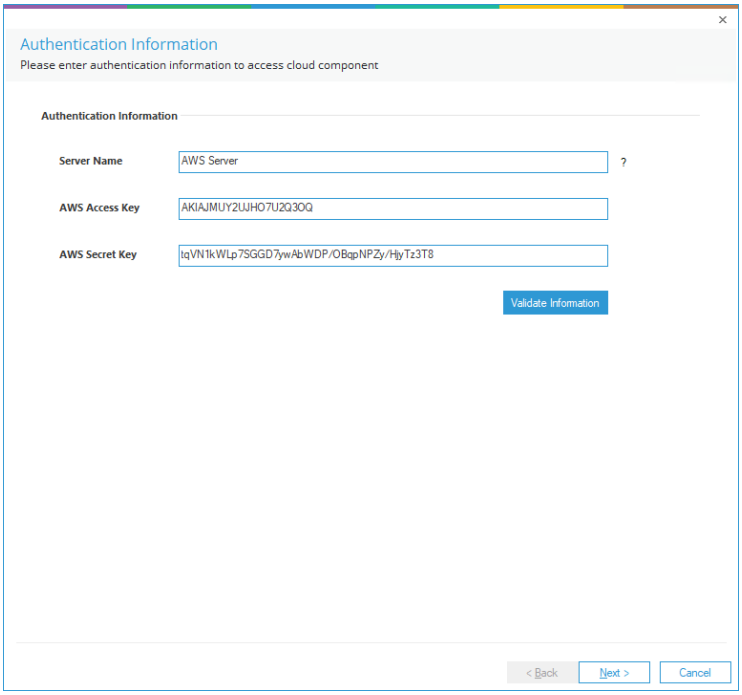

Figure 4: Authentication Information Added

- Click **Validate Information** to validate the information you have entered

- If the information is correct the Information Validated Successfully message box will be displayed:

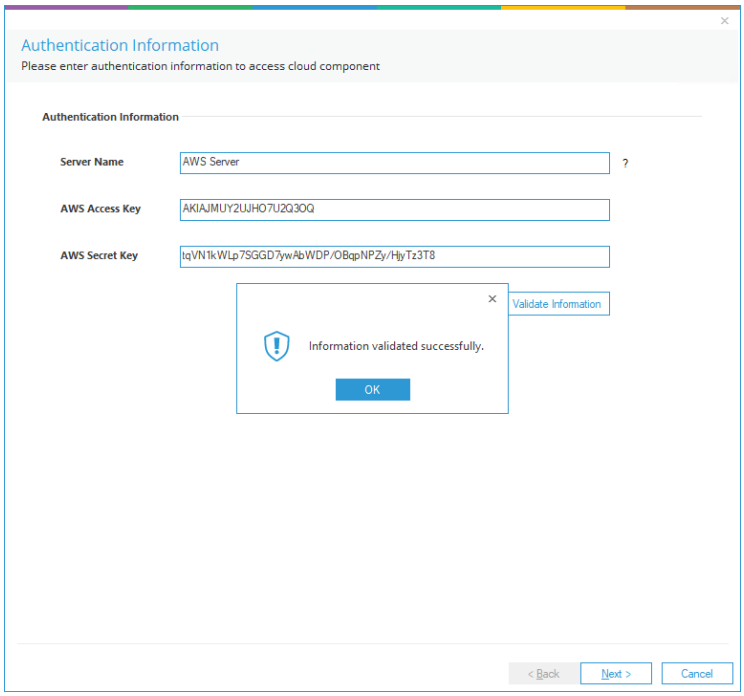

Figure 5: Information Validated Successfully

- Click Ok
- Click **Next**
- The Database Settings dialog box is displayed:

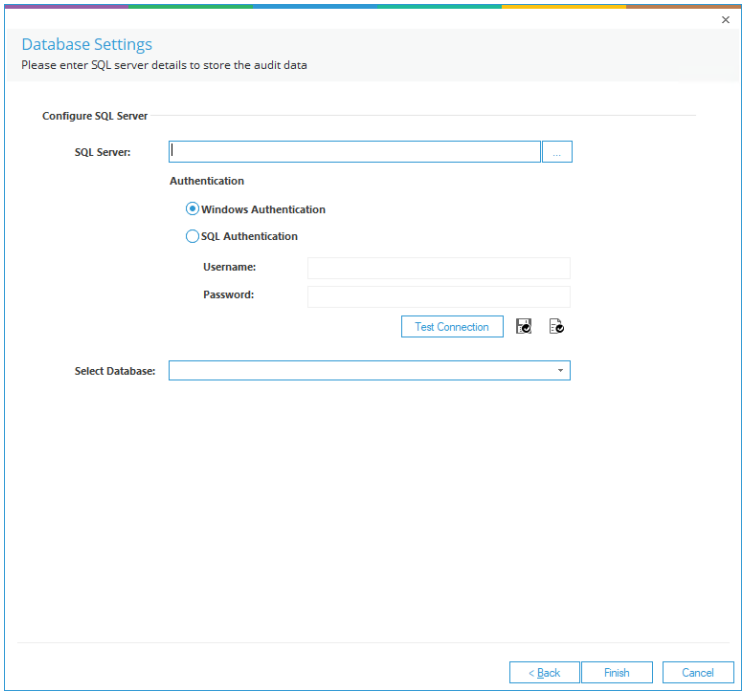

Figure 6: Database Settings

- From this dialog box you can do the following:
- Add the **SQL Server** name. Click the ... icon to select a server
- Select either Windows or SQL Authentication and add a Username and Password for SQL Authentication
- Click **Test Connection** to check that the connection works correctly
- In the **Select Database** box, type in a database name and the Solution will create a database with this name
- Click **Finish**

- A message box will be displayed asking for confirmation to restart the solution:

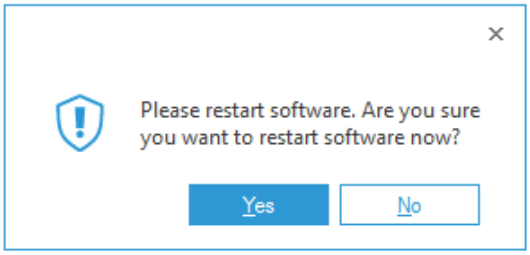

Figure 7: Confirm Restart

- Click **Yes** to restart
- The Amazon S3 Component will be added and displayed on the component management screen:

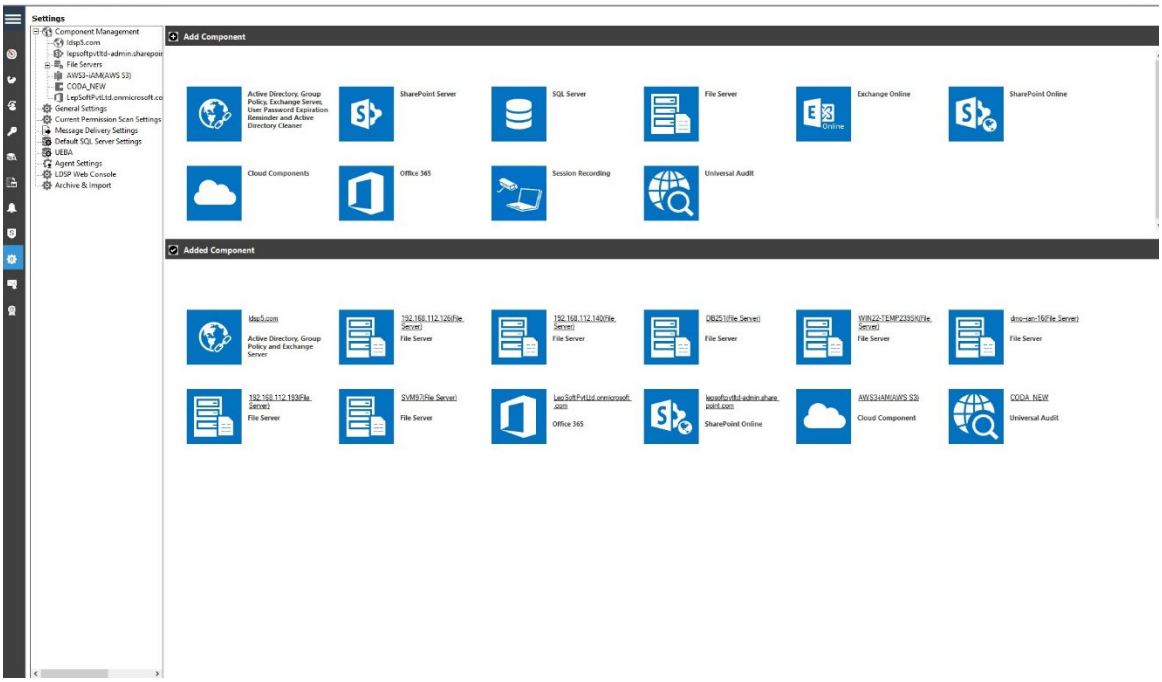

Figure 8: Component Management Screen with Added Cloud Component

5 Viewing the Reports

5.1 All Environment Changes Report

The All Environment Changes Report will show all changes made to the AWS S3 Component.

To run the report:

- Click the Users & Entity behavior icon  to display the States & Behavior screen
- From the tree structure to the left side of the screen select **All Environment Changes**
- Click the **Component Name** filter and select **AWS S3**
- Select a Date Range
- Click Generate Report
- The example below shows the **All Environment Changes Report** with the **AWS S3 filter** applied:

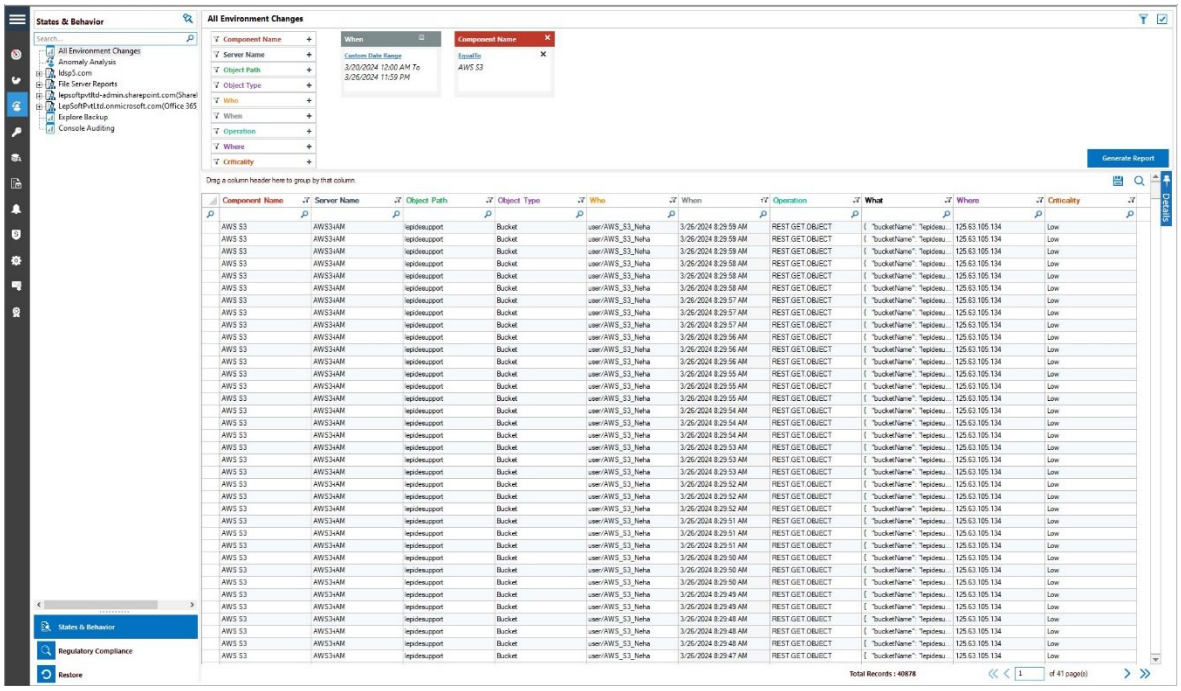

Figure 9: All Environment Changes Report

5.2 The Open AWS S3 Buckets Report

An open AWS S3 bucket is called "open" because anyone can access the data in the bucket without authentication. This can be a major security risk, as anyone can view, download, or even delete the data in the bucket. So, because an open S3 bucket is a potential source of a data breach, it is important to have visibility over all open S3 buckets. This can be achieved by running the **Open AWS S3 Buckets Report**, part of the Lepide Data Security Platform.

5.2.1 Adding a Data Set and Running a Scan

Before the Open AWS S3 Buckets Report can be run, you will need to create a data set and run a Current Permissions Scan to have visibility over the current state of open buckets.

To Add a Data Set:

- Click the Settings icon
- Select Current Permissions Scan Settings from the tree on the left hand side of the screen
- Click the ⊕ icon

The Data Set Information dialog box will be displayed:

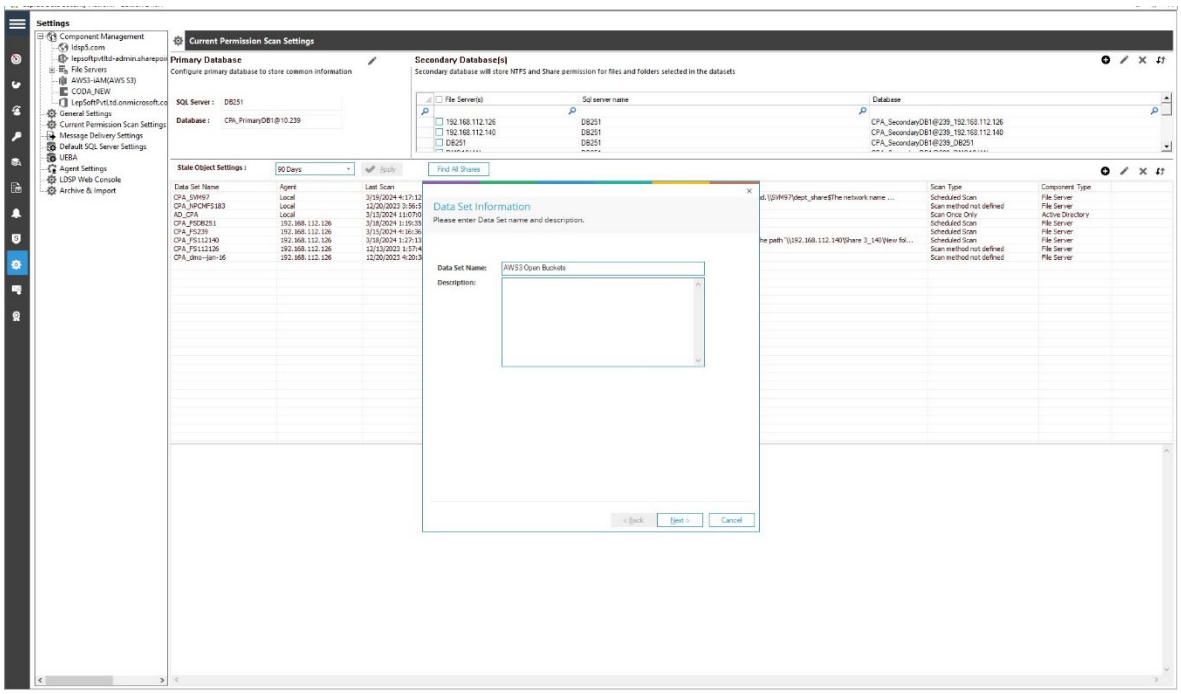

Figure 10: Data Set Information

- Enter a **Data Set Name** and an optional **Description**

- Click **Next**

The Component and Server Information dialog box will be displayed

Enter the following information:

- Component Name
- Server Name
- AWS Access Key
- AWS Secret Key

> **NOTE:** The instructions to generate the **AWS Access Key ID** and **AWS Secret Key** are given in Section 3 - Access Keys.

- Click Validate Information to validate the details which have been entered
- The **Information validated successfully** message box will be displayed:

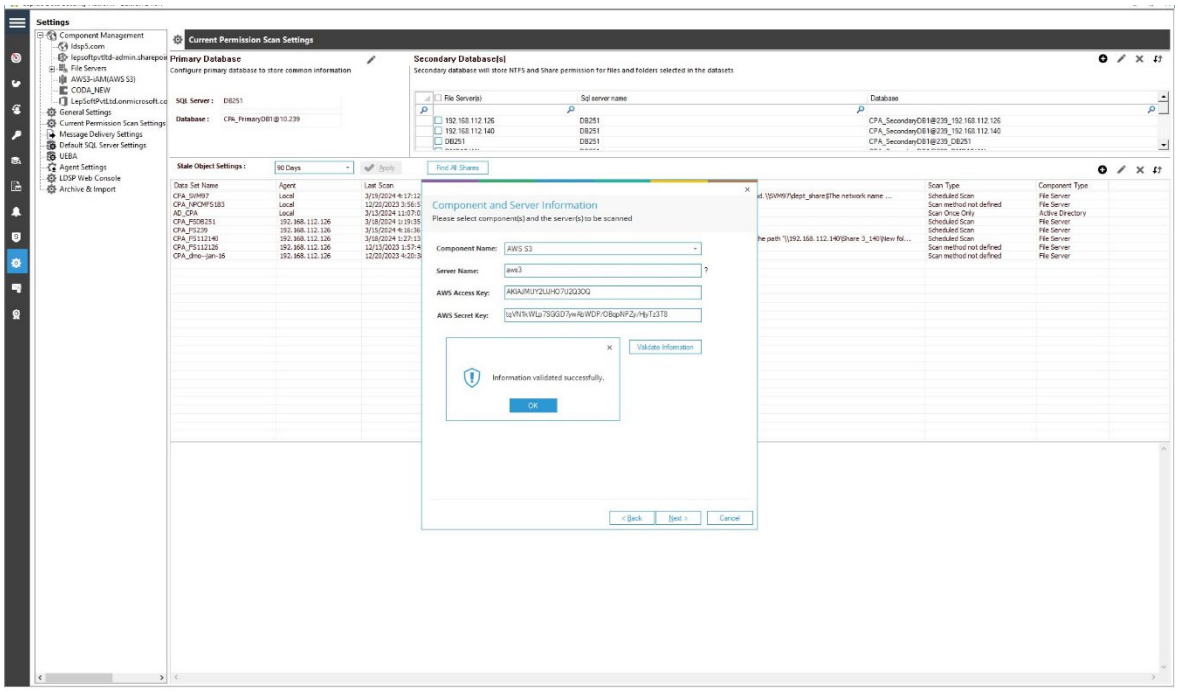

Figure 11: Component and Server Information

- Click **Ok**
- Click **Next**

The Scan Options dialog box will be displayed:

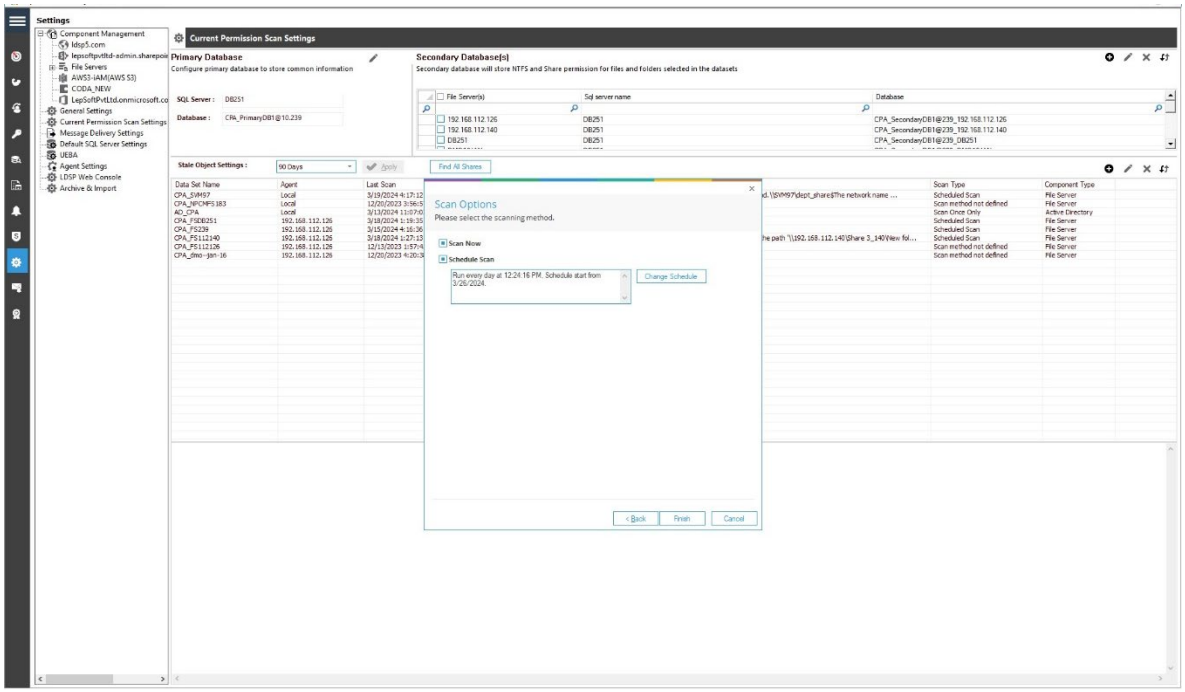

Figure 12: Scan Options

Choose the option you require:

- **Scan Now** to run a scan immediately
- **Schedule Scan** to specify when the scan should be run. Click Change Schedule to set the date and time for running the scan

- Click **Finish**

This will return to the Current Permission Scan Settings screen and the newly added Data Set will be listed:

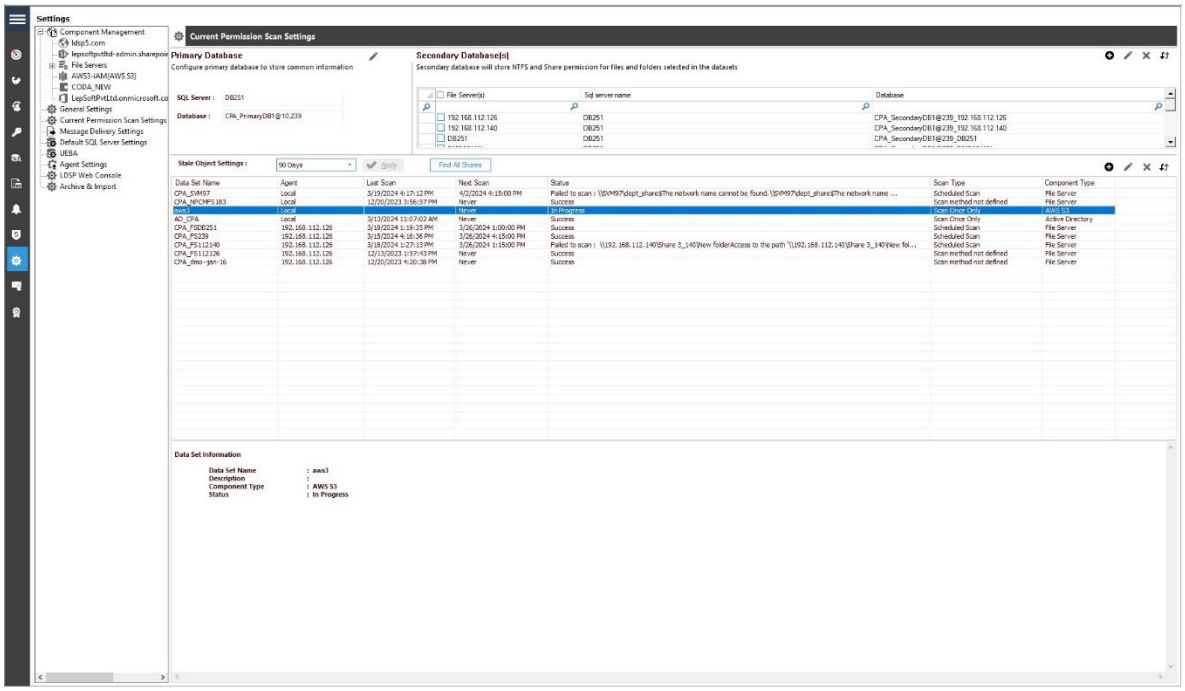

Figure 13: Data Set Added

- If **Scan Now** was selected, the scan will start immediately

Once the scan has run successfully, you can generate the Open AWS S3 Buckets Report

5.2.2 Running the Open AWS S3 Buckets Report

- Click the **Permissions & Privileges** icon  to display the Permissions & Privileges screen
- From the tree structure to the left side of the screen expand **Risk Analysis** and select **Open AWS S3 Buckets**
- Click Generate Report

The example below shows the Open AWS S3 Buckets Report:

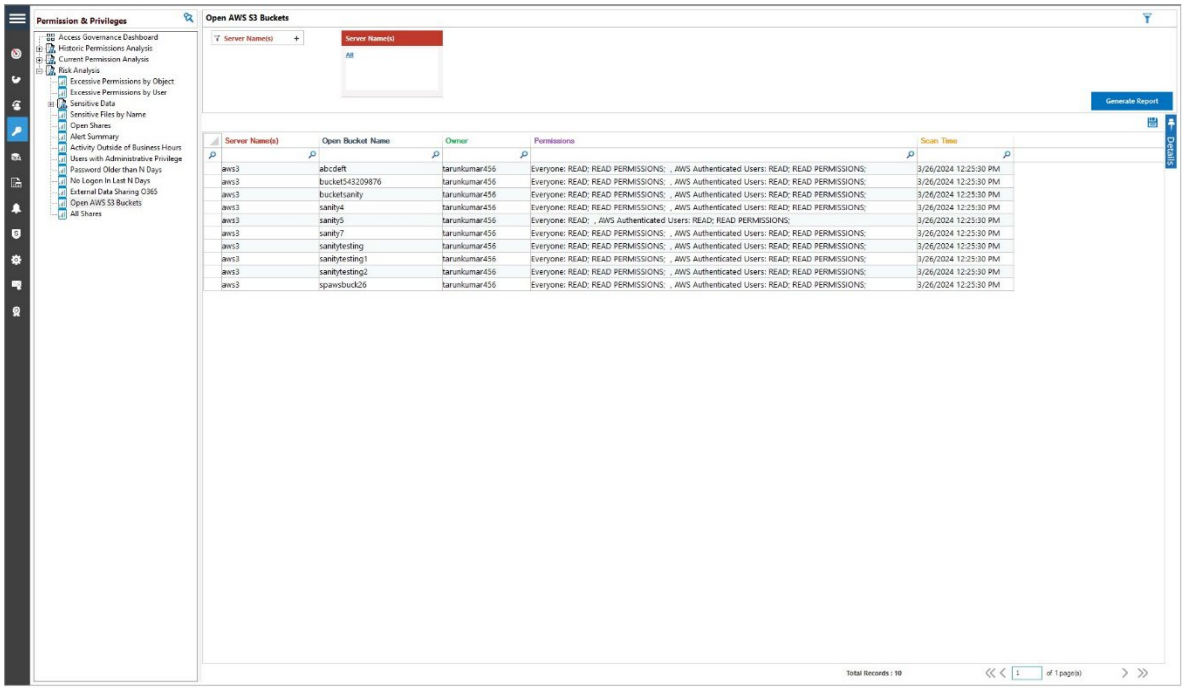

Figure 14: Open AWS S3 Buckets Report

6 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/.

7 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.