Lepide

Amazon S3.

Quick Start Guide.

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.

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.

3.2 Adding an Amazon S3 Component

An Amazon S3 Component is added from the Web Console Manage Component screen and the steps to do this are as follows:

- From the Web Console Home screen, click the Settings icon (top right of the screen) to display the Admin Console

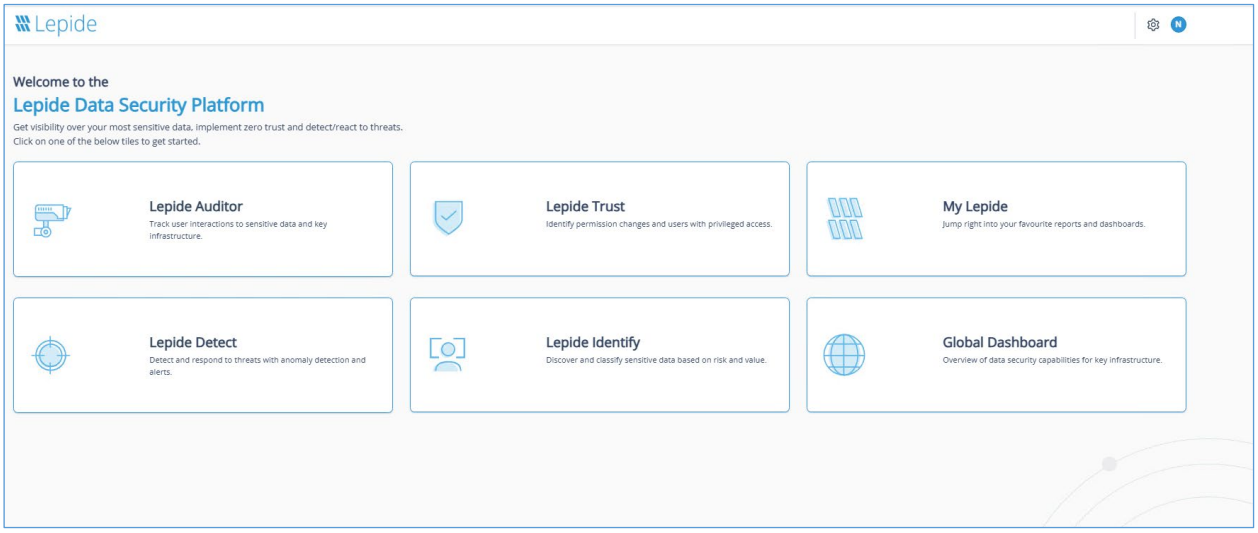

Figure 1: Home Screen

- From here select **Manage Components** from the options on the left-hand side of the screen and the Manage Components screen will be displayed:

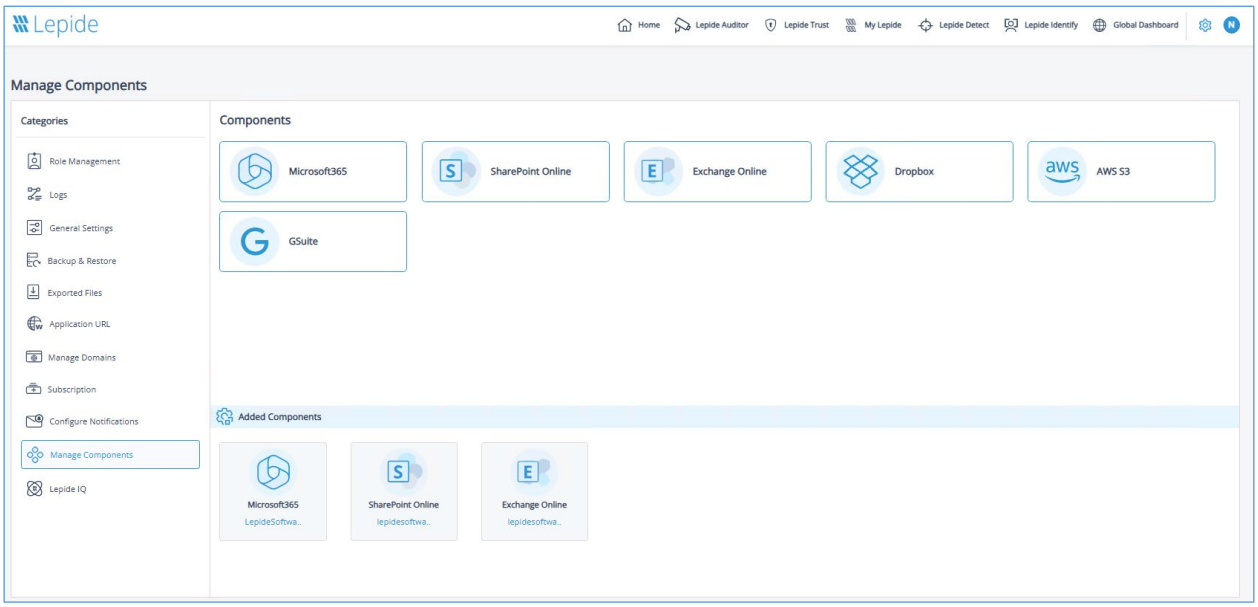

Figure 2: Manage Components

- From the **Components** section, click on the **AWS S3** component and the Add Credential for AWS S3 window is displayed with the Component Credential category selected:

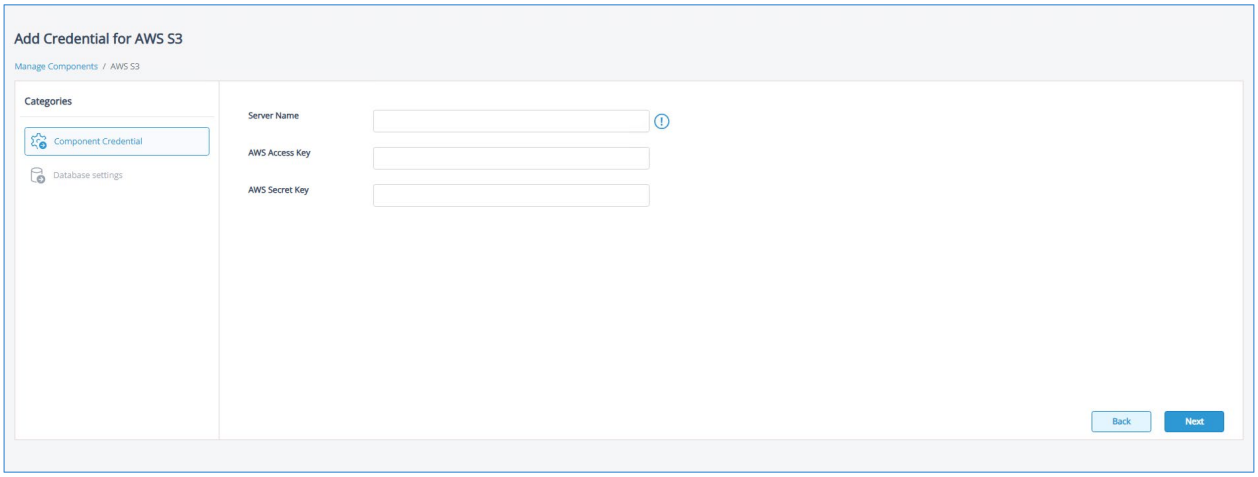

Figure 3: Component Credential

- Add the **Server Name**
- The specified name will appear in the 'Server Name' column for the All Environment Changes Report
- Add the **AWS Access Key** (see section 3.1 of this guide for information on how to create an Access Key)
- Add the **AWS Secret Key (**see section 3.1 of this guide for information on how to create a Secret Access Key)
- Click **Next** to continue

The Database Settings window is displayed.

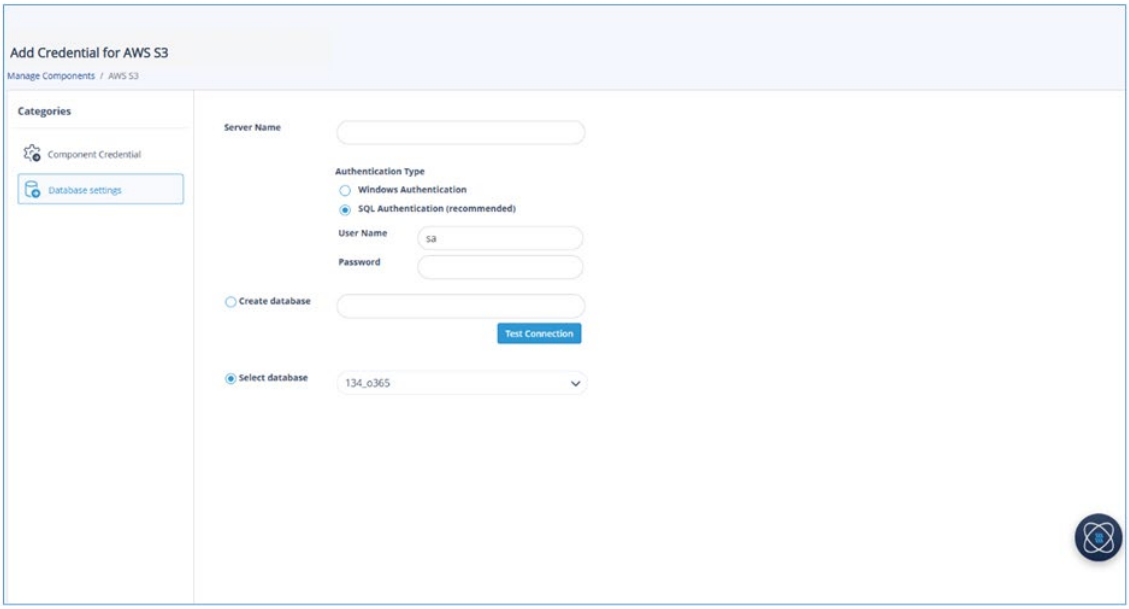

Figure 4: Database Settings

Add the Database Settings as follows:

- **Server Name** – enter the name of the server
- **Authentication Type** – choose from either:
  - Windows Authentication or
  - SQL Authentication – add the User Name and Password
- Select to either Create **database** – enter the database name and click **Test Connection** to test the database connection

  Or
- **Select database** – use the drop-down arrow to select the name of an existing database
- Click **Finish**

The added component will be displayed in the Manage Component window:

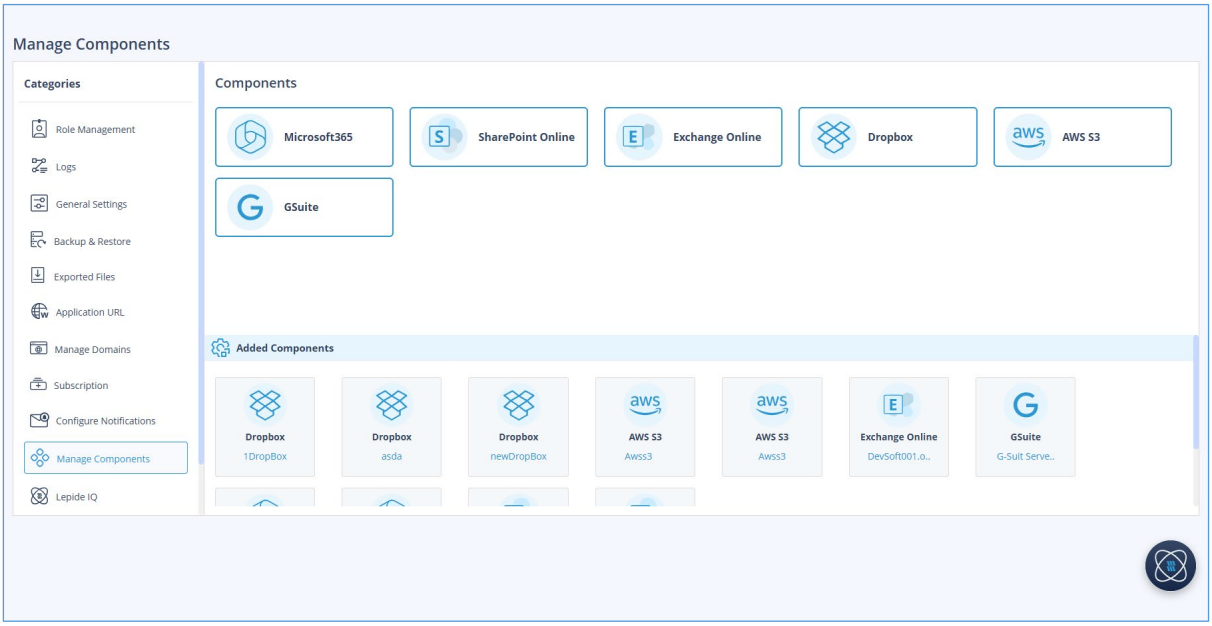

Figure 5: Manage Components

4 Viewing the Reports

4.1 All Environment Changes Report

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

To run the report:

- From the Web Console Home screen, select Lepide Auditor and the Lepide Auditor dashboard screen will be displayed
- From the Lepide **Auditor** menu at the top, select **Reports**

The Lepide Auditor Reports screen will be displayed:

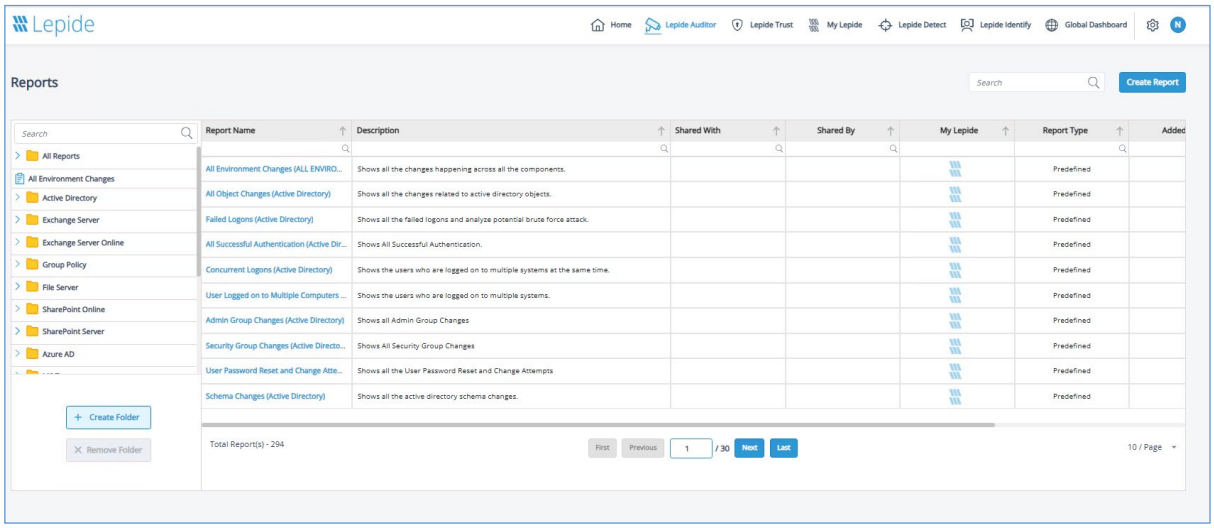

Figure 6: Lepide Auditor Reports

- From here, select the **All Environment Changes Report**:

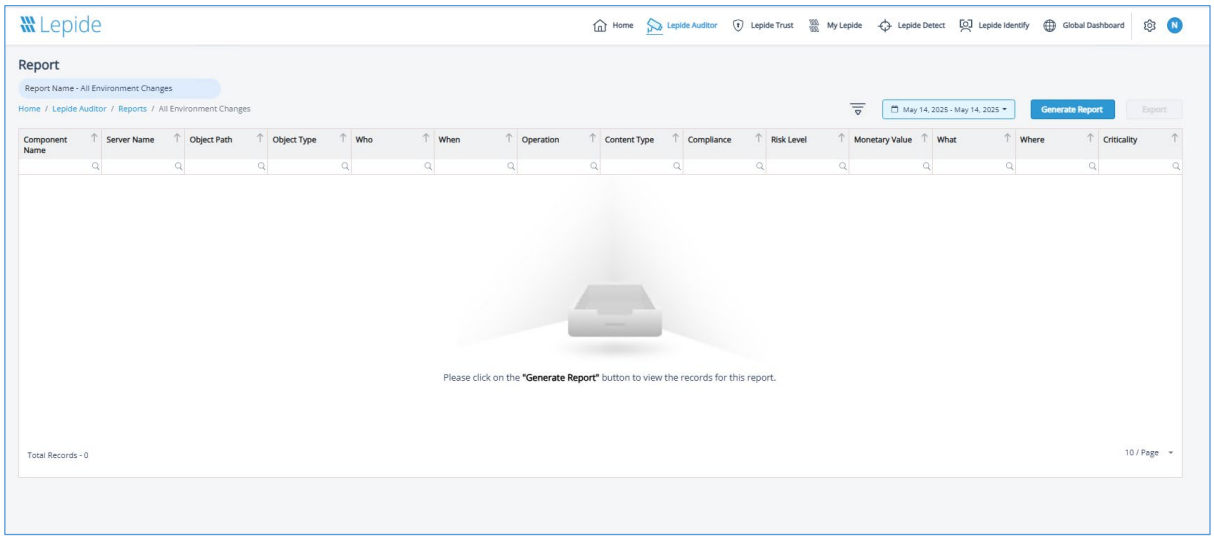

Figure 7: All Environment Changes Report

To apply a filter for AWS S3:

Click the Filter icon: 

- The **Modify Filters** dialog box is displayed

- Click the arrow to display the drop down menu:

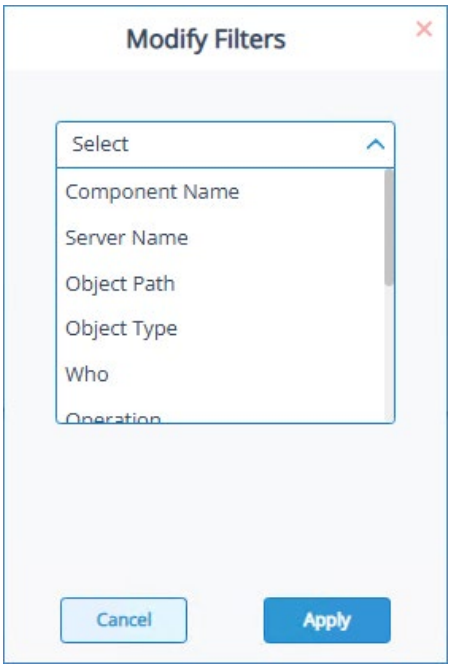

Figure 8: Modify Filters drop down Menu

- Select **Component Name** from the list
- Click the  icon to display a list of components
- Click the arrow next to **Filter Criteria** and select **Equals**

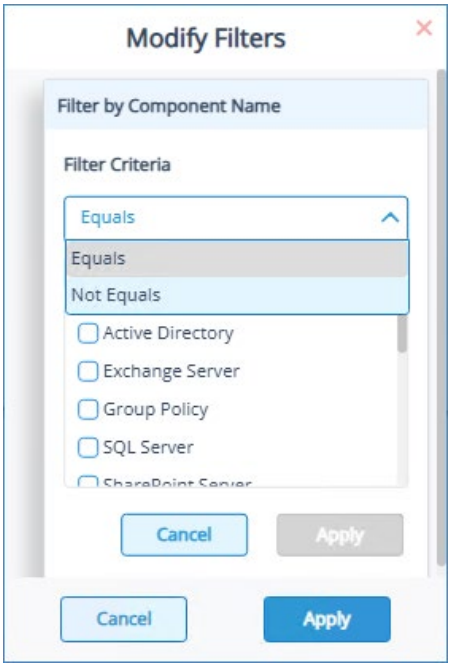

Figure 9: Filter Criteria

- From the list of components, select AWS S3:

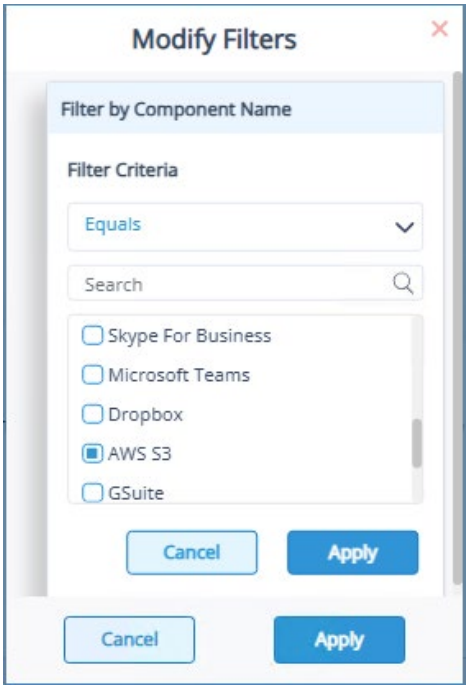

Figure 10: Filter by Component Name

- Click **Apply, Apply** to close the Modify Filter box and go back to the report screen
- Change the time period if required
- Click **Generate** Report

The example below shows the **All Environment Changes Report** with the **AWS S3 filter** applied:

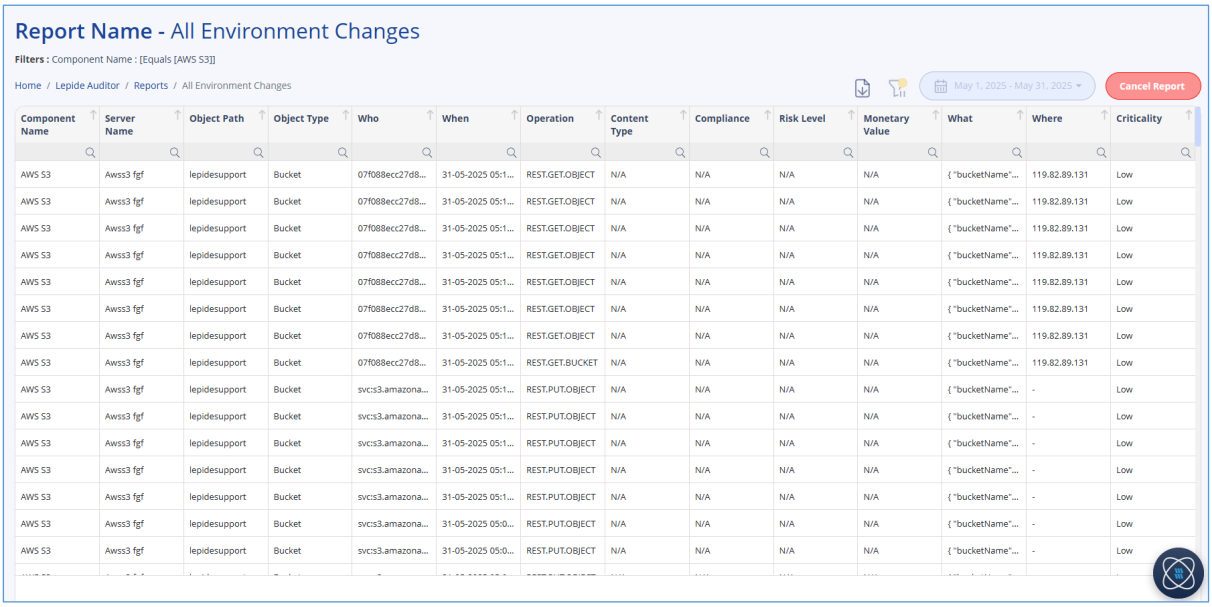

Figure 11: All Environment Changes Report

4.2 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.

4.2.1 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. This is done from the Lepide Main Console, and the steps are as follows:

To Add a Data Set:

- From the icons on the left-hand side of the screen, click the **Settings** icon  and the Settings screen will be displayed:

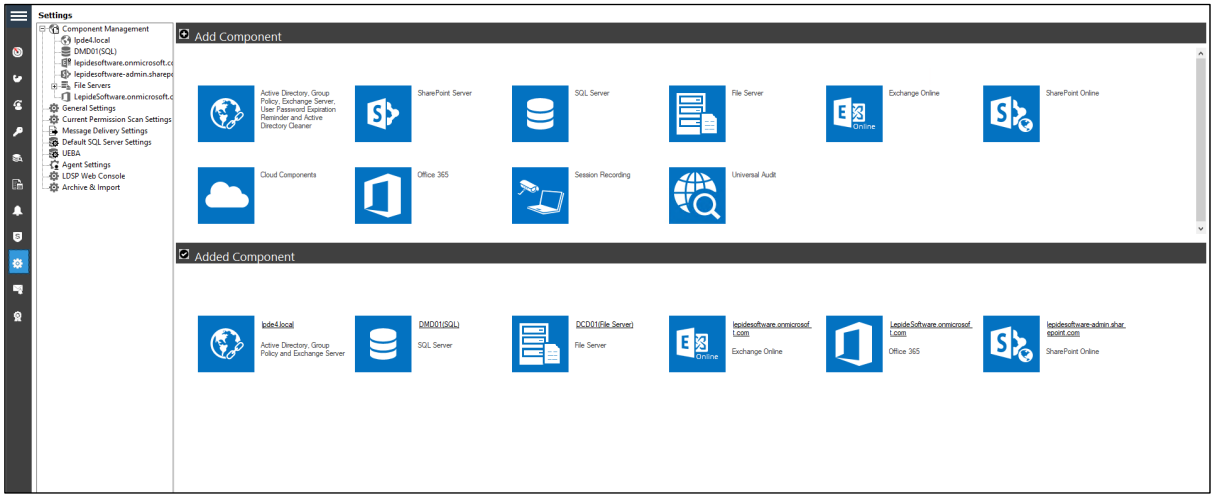

Figure 12: Settings Screen

- 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:

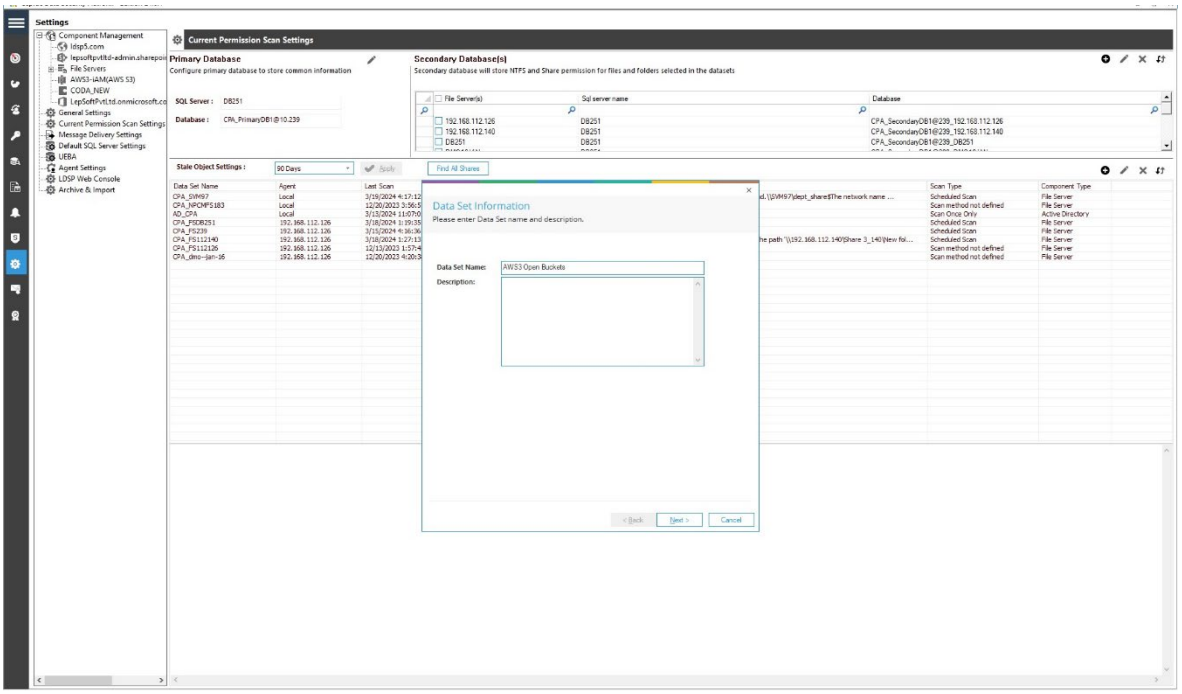

Figure 13: Data Set Information

- 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:

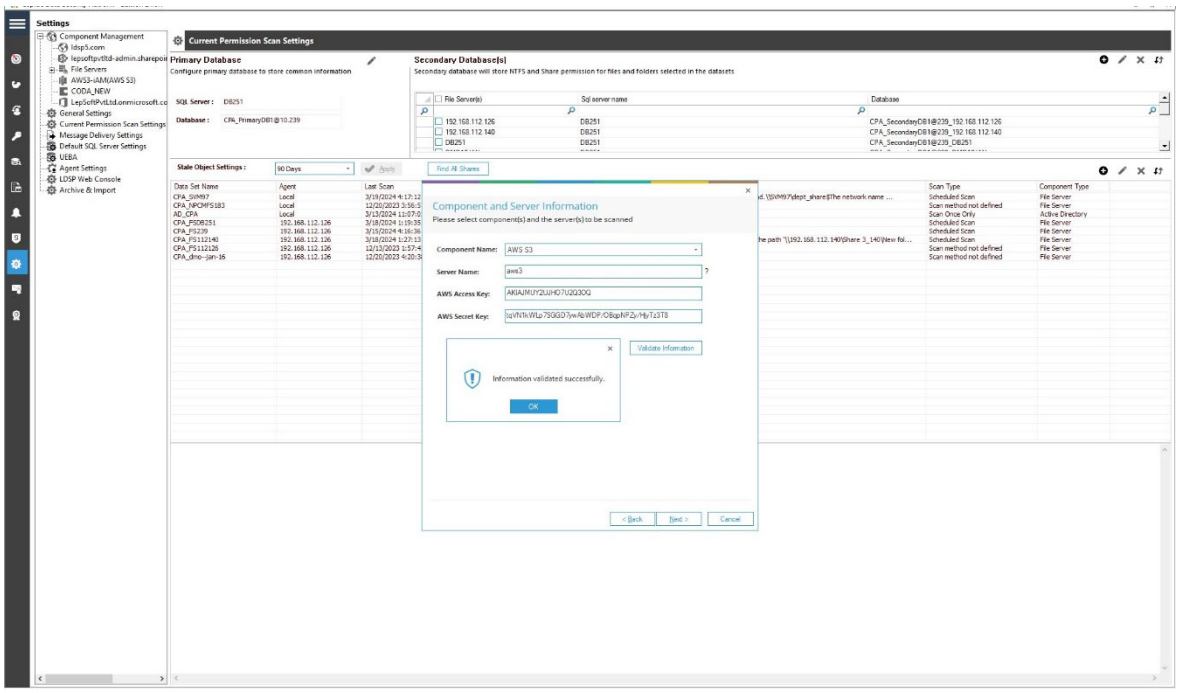

Figure 14: Component and Server Information

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

The Scan Options dialog box will be displayed:

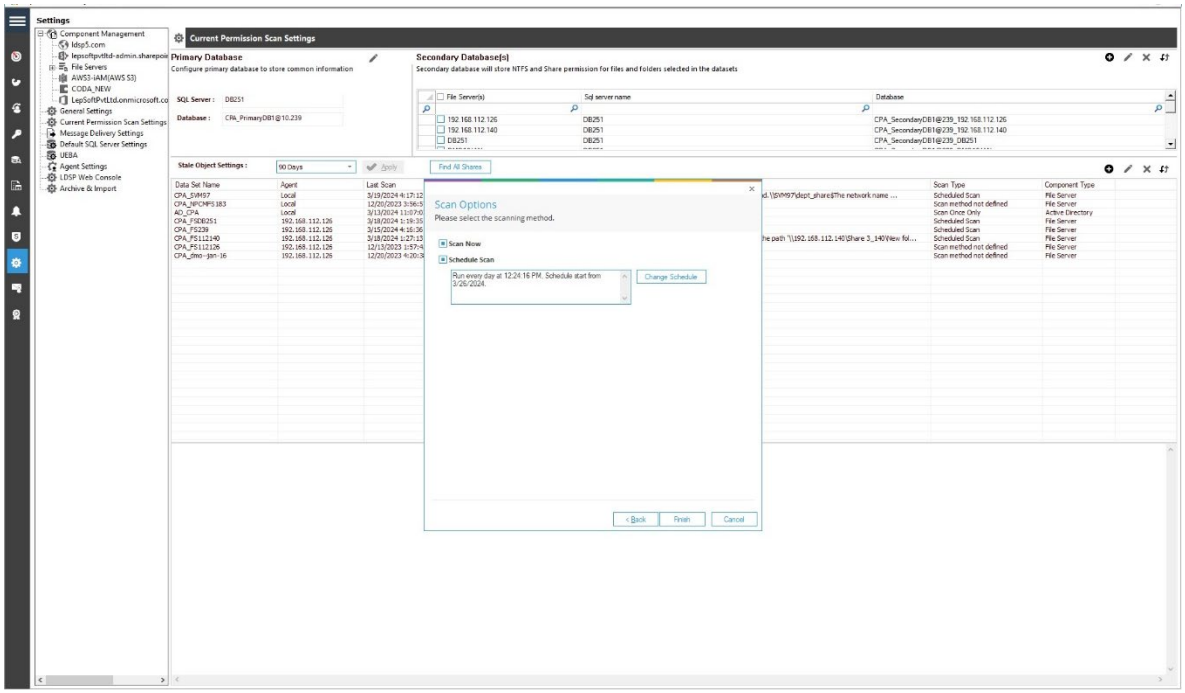

Figure 15: Scan Options

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:

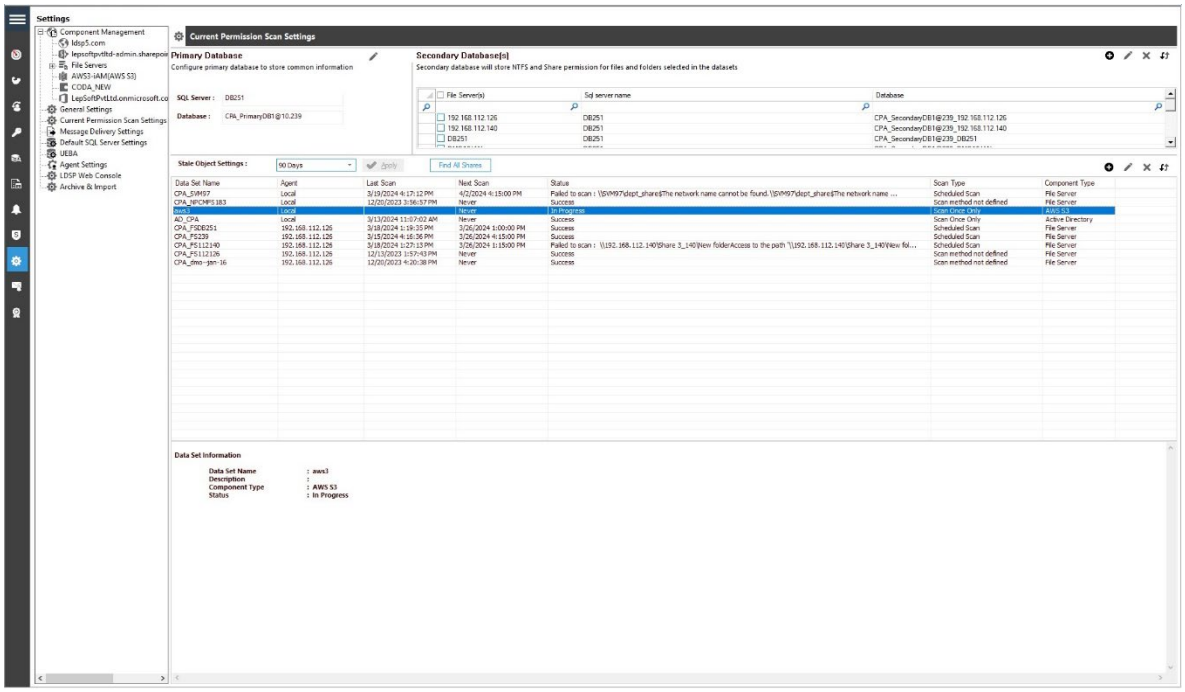

Figure 16: Data Set Added

- 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

4.2.2 Running the Open AWS S3 Buckets Report

- From the Lepide Web Console Home screen, select **Lepide Trust**
- From the Lepide Trust menu, select **Reports**
- Expand **Risk Analysis** from the list of reports on the left-hand side
- Select **Open AWS S3 Buckets**
- Click **Generate Report**

The example below shows the Open AWS S3 Buckets Report:

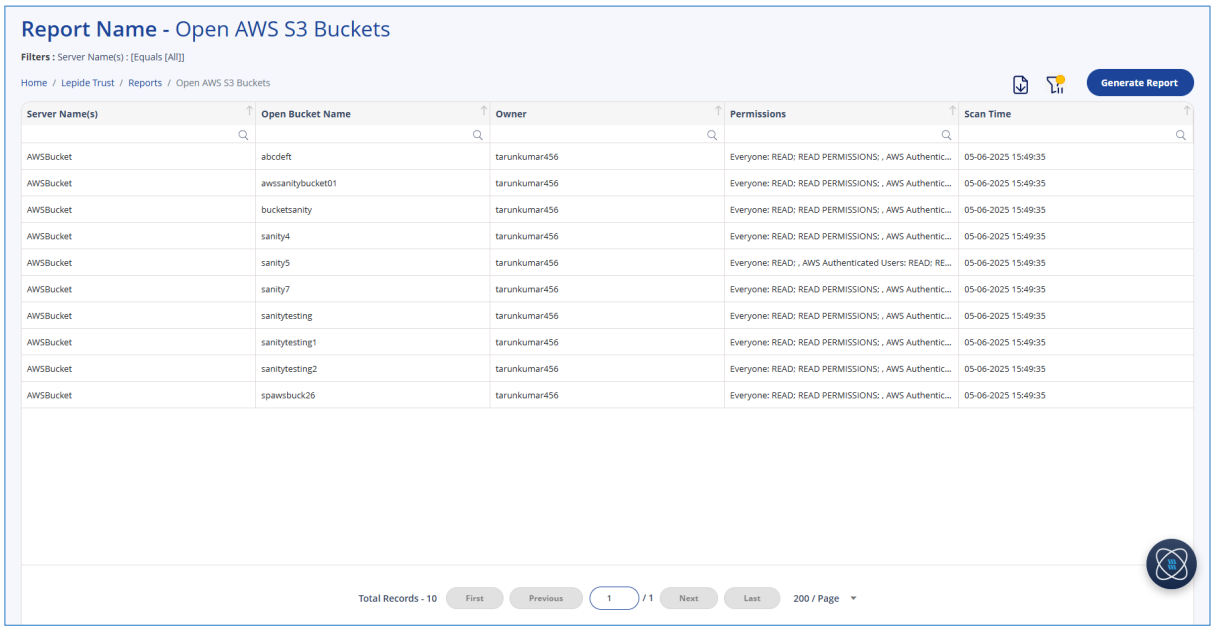

Figure 17: Open AWS S3 Buckets Report

5 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/.

6 Trademarks