



QUICK START GUIDE

MICROSOFT 365

Table of Contents

1	Introduction.....	4
2	Exchange Online	4
2.1	Prerequisites.....	4
2.2	Steps to Register an App and Generate the Client ID and Secret Key for Exchange Online Auditing	4
2.3	Assigning the Role to the Application	5
2.4	Permissions for Auditing, DDC, & CPA.....	5
2.4.1	Permissions for Auditing	5
2.4.2	Permissions for Data Discovery & Classification	6
2.4.3	Permissions for Current Permissions Analysis.....	6
2.5	Install the Exchange Online Management Module	6
2.6	Generate a ThumbPrint.....	7
2.7	How to Install a Certificate for DDC and FSA Agent	8
2.8	Adding an Exchange Online Component	8
2.9	Viewing the Reports	16
3	Office 365 Component.....	18
3.1	Prerequisites.....	18
3.2	OneDrive	18
3.2.1	Steps to Register an App and Generate the Client ID and Secret Key for OneDrive Auditing	18
3.2.2	Steps to Generate the Client ID and Secret Key for OneDrive Data Discovery & Classification	20
3.2.3	Steps to Generate the Client ID and Secret Key for OneDrive Current Permissions Analysis.....	21
3.3	Azure.....	22
3.3.1	Steps to Register an App and Generate the Client ID and Secret Key for Azure Auditing	22
3.4	Teams	23
3.4.1	Steps to Register an App and Generate the Client ID and Secret Key for Teams Auditing	23
3.5	Skype for Business	24
3.5.1	Steps to Register an App and Generate the Client ID and Secret Key for Skype for Business Auditing	24



- 3.6 Adding Azure Active Directory, OneDrive for Business, Skype for Business & Microsoft Teams..... 25
- 3.7 Viewing the Reports 29
- 4 SharePoint Online..... 30
 - 4.1 Prerequisites..... 30
 - 4.2 Steps to Register an App and Generate the Client ID and Secret Key for SharePoint Online Auditing. 31
 - 4.3 Steps to Generate the Client ID and Secret Key for SharePoint Online Data Discovery & Classification 32
 - 4.4 Steps to Generate the Client ID and Secret Key for SharePoint Online Current Permissions Analysis. 34
 - 4.5 Adding a SharePoint Online Component 35
 - 4.6 Viewing the Reports 42
- 5 Support 44
- 6 Trademarks 44

1 Introduction

The Lepide Data Security Platform performs comprehensive auditing and reporting on critical changes on Microsoft 365 components. The components supported for Microsoft 365 are: Exchange Online, SharePoint Online, Azure Active Directory, OneDrive for Business, Skype for Business and Microsoft Teams.

This guide takes you through the process of standard configuration of the Lepide Data Security Platform for Microsoft 365 Components. 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 Exchange Online

2.1 Prerequisites

The following are prerequisites to add an Exchange Online component to the Lepide Data Security Platform:

- The Lepide Server and Agent's Machine need to be logged in with Admin User
- The Lepide Server and Agent's Machine are required to be Remote signed
- Dot Net Framework 4.6.2 Developer Pack is required on the Lepide Server and Agent's Machine.
- Tls 1.2 is required for the Lepide Server and Agent's Machine

2.2 Steps to Register an App and Generate the Client ID and Secret Key for Exchange Online Auditing

1. Log into the Microsoft 365 account through Global Admin
2. Select **Azure Active Directory Account** through the Admin Center
3. Click on **App Registration** and follow the steps below to generate Client ID and Secret Key:
 - Select **New Registration** and provide a valid name for the registration and select supported account type
 - Click on **Register Account** and client ID will be displayed which the user can copy for future reference
 - For the given Client ID generated in the Azure Account Dashboard, click on **Certificates and**



Secrets

- Click on **Add New Client Secret** (with expiry period) and a Secret ID will be generated which the user can copy for future reference

2.3 Assigning the Role to the Application

1. Go to Azure Active Directory Dashboard and select the tab **Roles and Administrators**
2. Under Roles and Administrators select **Global Reader** and double click on it to Add assignments In Add Assignments go to Select Member(s) and select the newly created Application.
3. Then the Assignment Type will be eligible. Unlock permanently eligible and selection assignment duration and click **Assign**
4. Under Roles and Administrators assign **Exchange Administrator** by following above steps.

NOTE:**Global Reader:**

This Is required for providing permission to the Application so that it can read different audit log events by using different technologies.

Exchange Administrator:

This is required for providing permission to the Application so that it can manage all aspects of Exchange Online so that we can Read Mailbox Audit Logs by using Exchange Online PowerShell.

2.4 Permissions for Auditing, DDC, & CPA

2.4.1 Permissions for Auditing

For Office 365 Exchange Online (Delegated And Application)

Exchange.ManageAsApp Application Exchange Online

Graph Api (Delegated and Application)

User.Read Application Graph API

MailboxSetting.Read Application Graph API

Office365 Management APIs

ActivityFeed.Read	Delegated	Management API
ActivityFeed.Read	Application	Management API

2.4.2 Permissions for Data Discovery & Classification

Graph Api (Delegated and Application)

MailboxSettings.ReadWrite	Application	Graph API
User.ReadWrite.All	Application	Graph API
Directory.ReadWrite.All	Application	Graph API
Mail.ReadWrite	Application	Graph API
Calendars.ReadWrite	Application	Graph API
Contacts.ReadWrite	Application	Graph API
Tasks.ReadWrite.All	Application	Graph API

2.4.3 Permissions for Current Permissions Analysis

For Office 365 Exchange Online (Delegated And Application)

Exchange.ManageAsApp	Application	Exchange Online
----------------------	-------------	-----------------

2.5 Install the Exchange Online Management Module

1. Open Windows PowerShell by run as Administrator

NOTE: Run the following commands firstly in Windows PowerShell(x86) then in Windows PowerShell

2. To Ensure that you have Nuget Package installed run the below command.
 - Get-Module -ListAvailable -Name NuGet
3. If you don't have a NuGet Package then to install the module run the below command
 - Install-Module -Name NuGet -Force
4. To Ensure that you have a version of PowerShellGet and PackageManagement newer than 1.0.0.1 installed, run the command below:

Get-Module PowerShellGet, PackageManagement -ListAvailable

5. If you have an older version of PowerShellGet and PackageManagement then to install the latest version, run the command below:

Install-Module PowerShellGet -Force -AllowClobber

6. To install the Exchange Online PowerShell module run the command below:

Install-Module -Name ExchangeOnlineManagement -RequiredVersion 3.1.0 -Force

2.6 Generate a ThumbPrint

The steps to install the Exchange Online PowerShell module are as follows:

- A. Open Windows PowerShell, run as Administrator
- B. To ensure that you have a version of PowerShellGet and PackageManagement newer than 1.0.0.1 installed, run the command below:
Get-Module PowerShellGet, PackageManagement -ListAvailable
- C. If you have an older version of PowerShellGet and PackageManagement then to install the latest version, run the command below:
"Install-Module PowerShellGet -Force -AllowClobber"
- D. To install the ExchangeOnline PowerShell module run the command below:
"Install-Module -Name ExchangeOnlineManagement"

The steps to create a certificate for your domain name are as follows:

- A. Run the following PowerShell commands:
 - a. `$mycert = New-SelfSignedCertificate -DnsName "YourDomainName.com" -CertStoreLocation "cert:\LocalMachine\My"-NotAfter (Get-Date).AddYears(NumberOfYears) -KeySpec KeyExchange -FriendlyName "scriptfile"`
Note: "scriptfile" should be the User Defined Name for the certificate
 - b. `$mycert | Select-Object -Property Subject,Thumbprint,NotBefore,NotAfter`
Note: User should copy Thumbprint value as it is required for Login Information
 - c. `$mycert | Export-Certificate -FilePath "C:\temp\scriptfile.cer"`
Note: FilePath should ends with a (.cer) file type
 - d. `$mycert | Export-PfxCertificate -FilePath "C:\temp\scriptfile.pfx" -Password $(ConvertTo-SecureString -String "Password value" -AsPlainText -Force)`
Note: Password value is the User Defined Password Value for certificate
- B. Install the Certificate in the "trusted root certification Authorities Store" of Agent's System Machine

- a. Open the certificates of .cer and .pfx as filetype (generated in the above steps)
- b. Install the certificates with "local machine" as the store location option
- c. In case of a (.pfx) certificate, enter the "password value" mentioned in the above step
- d. Choose the "windows can automatically select a certificate store" as an option for the "Certificate Store" path

The steps to upload the certificate for your client application are as follows:

In the App registrations tab for the client application:

- A. Select Certificates & secrets, Certificates
- B. Click on **Upload certificate** and select the certificate file to upload
- C. Click **Add**. Once the certificate is uploaded, the thumbprint, start date and expiration values are displayed

NOTE: The User should copy the Client ID and ThumbPrint as this will be needed for Login Information

2.7 How to Install a Certificate for DDC and FSA Agent

The Certificate should be installed in the **'Trusted Root Certification Authorities Store'** of the Agent's System Machine

1. Open the certificates of .cer and .pfx as filetype (generated in the above steps).
2. Install the certificates with **'local machine'** as the store location option
3. In the case of a (.pfx) certificate enter the **'password value'** mentioned in the above step
4. Choose the 'windows can automatically select a certificate Store' as the option for 'Certificate Store' path

2.8 Adding an Exchange Online Component

The Lepide Data Security Platform tracks the changes inside Exchange Online and gives detailed reporting on any configuration changes, for example Mailbox Modifications, Exchange Group Modifications, etc.

To add an Exchange online component:

- From the Component Management screen, click on **Exchange Online**:

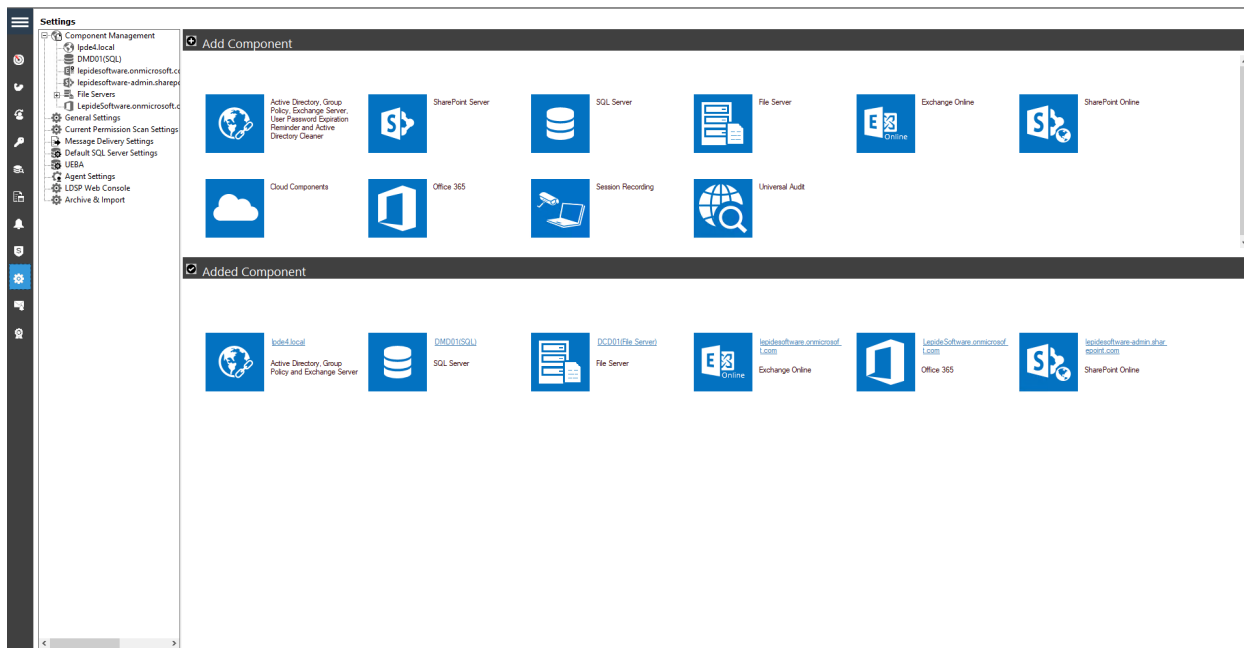


Figure 1: Component Management Screen

The Global Administrator App Credentials dialog box appears:

Global Administrator App Credentials

Please provide the global administrator app Client ID and Secret Value Key.

Tenant Name

Enter like: Your domain name.onmicrosoft.com

Subscription Type ?

Client ID

Secret Key

ThumbPrint ?

< Back Next > Cancel

Figure 2: App Credentials

- Enter the Tenant Name, choose the Subscription Type and enter the Client ID, Secret Key and ThumbPrint

NOTE: The instructions to generate the **Client ID** and **Secret Key** are given in Section 2.2. The instructions to generate the **ThumbPrint** are given in Section 2.6 - Generate a ThumbPrint

- Click **Next**
- The Add Mailboxes to Audit dialog box is displayed:

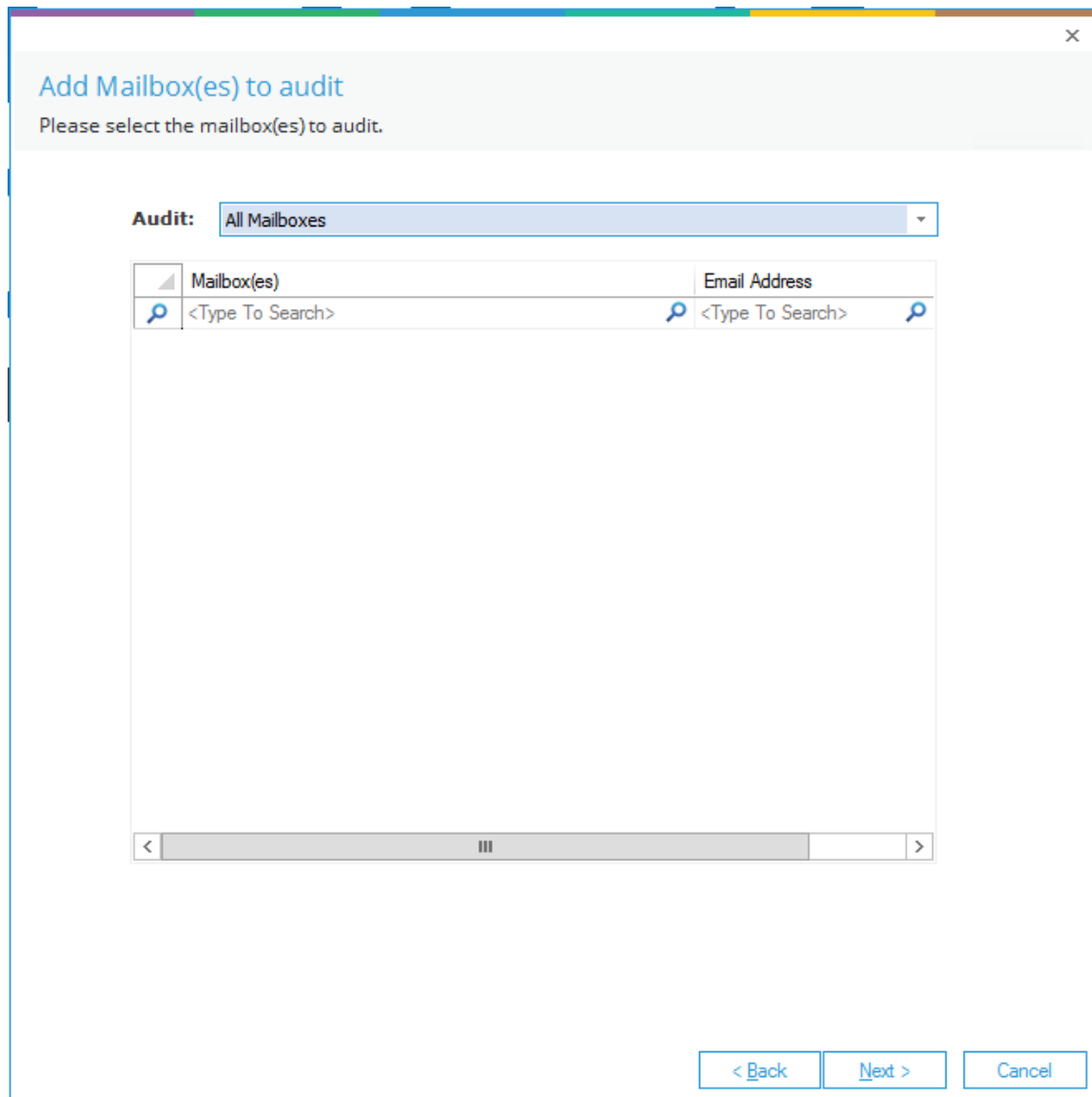


Figure 3: Add Mailboxes to Audit

- Select the Mailboxes you would like to audit. The options are:
 - All Mailboxes – this is the default option
 - Selected Only
 - All but Excluding Selected
- To audit specific mailboxes, choose **Selected Only** from the drop-down list and the mailboxes are displayed with checkboxes to select those to be **included** in auditing:

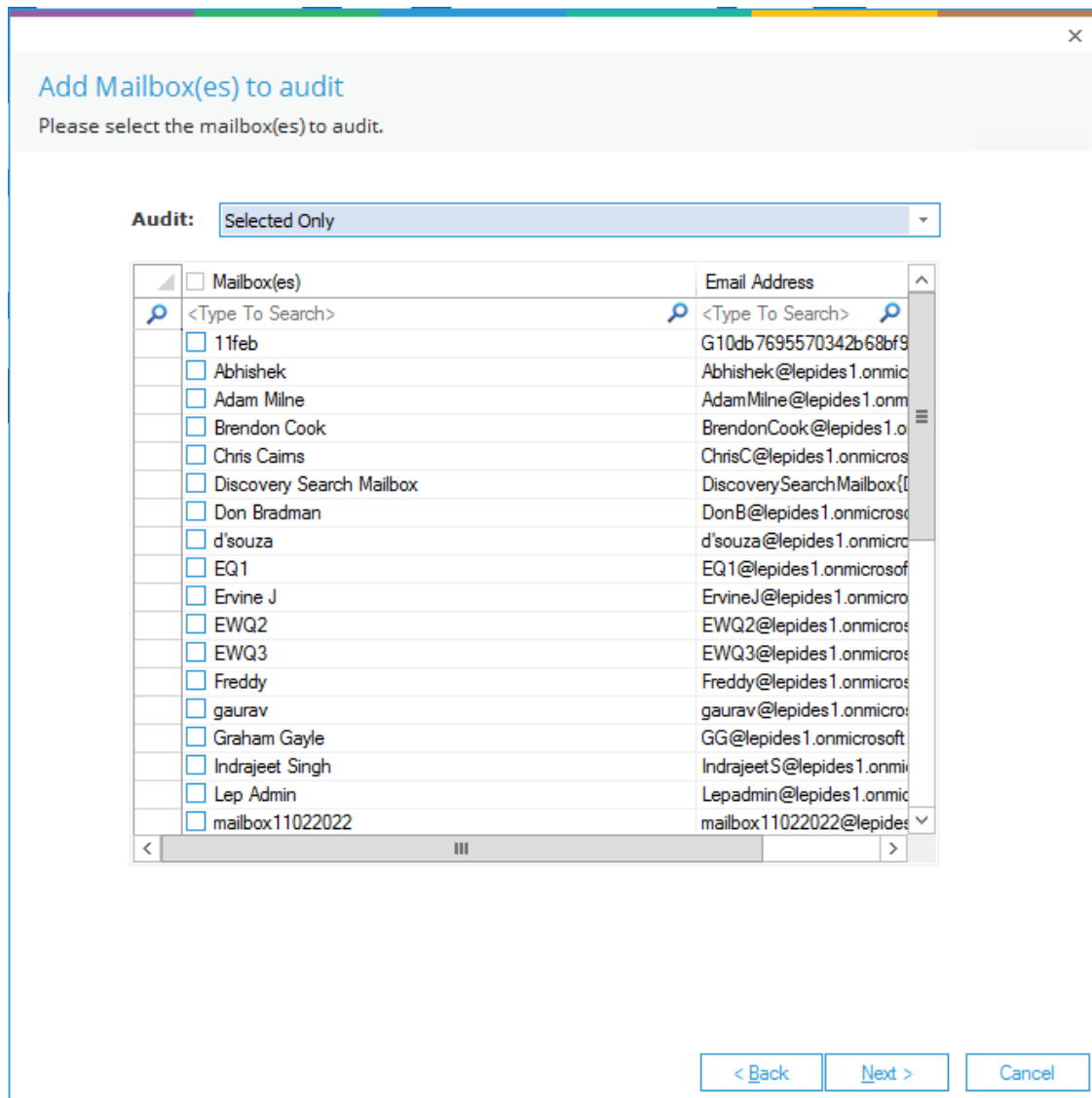


Figure 4: Add Selected Mailboxes to Audit

- To audit all **except** specific mailboxes, choose **All but Excluding Selected** from the drop-down list and the checked mailboxes will be **excluded** from auditing.
- Click **Next**
- The Add Objects to Audit dialog box is displayed:

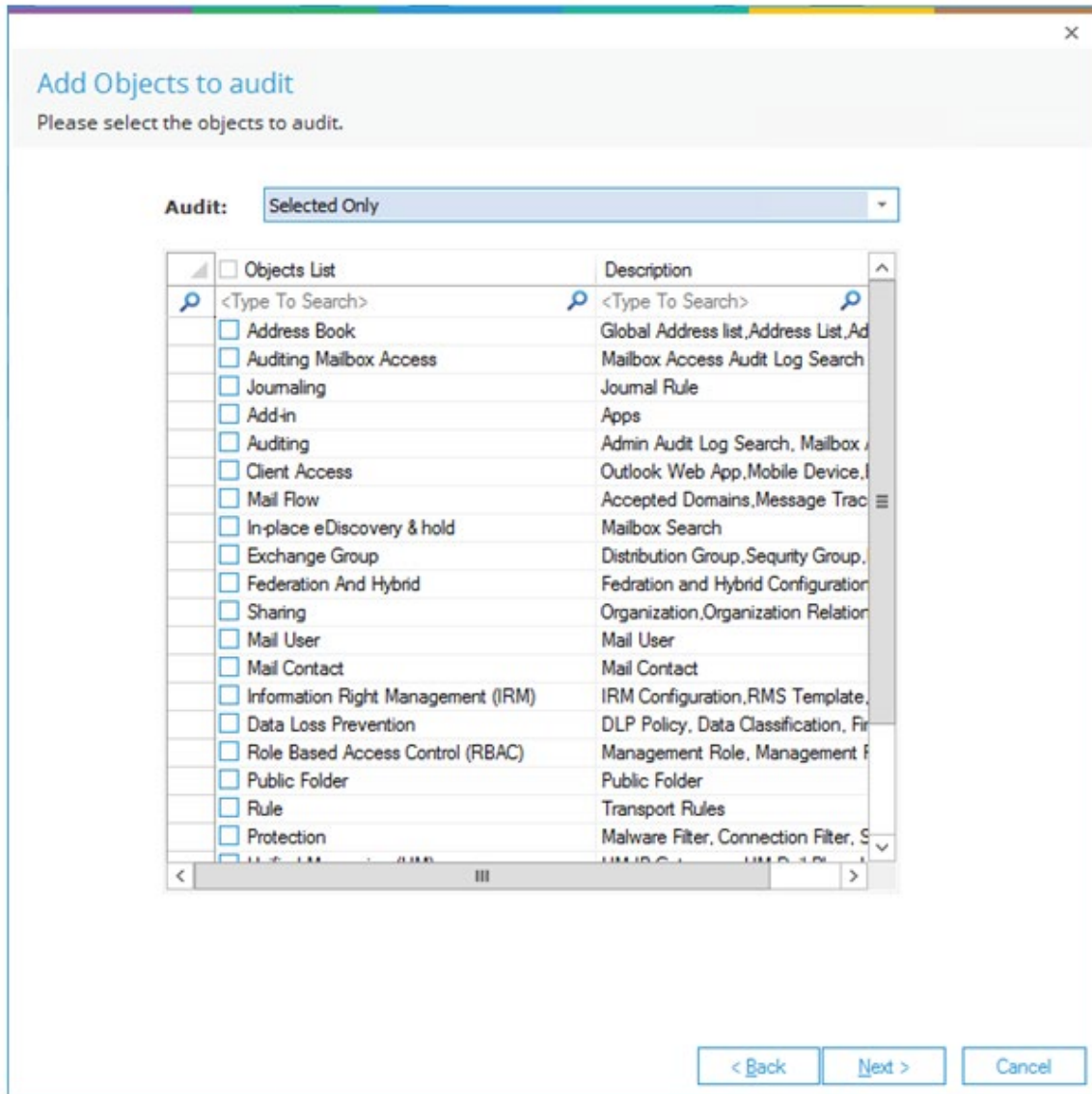


Figure 5: Add Objects to Audit

- Select the Objects you would like to audit. The options are:
 - All Objects – this is the default option
 - Selected Only
 - All but Excluding Selected
- To audit specific objects, choose **Selected Only** from the drop-down list and the objects are displayed with checkboxes to select those to be **included** in auditing:
- To audit all **except** specific objects, choose **All but Excluding Selected** from the drop-down list and the checked objects will be **excluded** from auditing.
- Click **Next**
- The Database Settings dialog box is displayed:

Database Settings
Please provide SQL server details to store the audit data

Configure SQL Server

SQL Server: 192.168.40.238

Authentication

Windows Authentication

SQL Authentication

User Name: sa

Password:

Test Connection

Select Database: Lepide_Exch_Online

Collect Changes Every: 5 Minutes.

< Back Next > Cancel

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
 - In the **Select Database** box, type in a name and the Solution will create a database with this name
 - Collect **Changes Every**: Set the frequency to collect the changes from the M365 portal. The minimum is 5 minutes

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

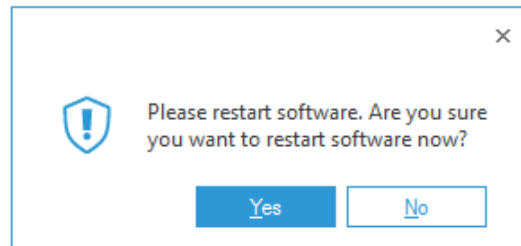



Figure 7: Confirm Restart

- Click **Yes** to restart

2.9 Viewing the Reports

Exchange Online reports are available from the States & Behavior screen.

- Click the Users & Entity behavior icon  to display the States & Behavior screen
- From the tree structure to the left side of the screen expand Exchange Online.
- There will be a separate Node for Exchange Online for the tenant which has been added. Expand this Node
- The example below shows the All Modifications in Exchange Online Report:

States & Behavior

kpvt.onmicrosoft.com(Exchange Online)/All Modifications in Exchange Online

Object Name When

Object Class Who Modified Operation When What Where

Grid View Graph View

Drag a column header here to group by that column.

Object Name	Object Class	Who Modified	Operation	When	What	Where
uwp_a0178055-26a8-48ce...	Unified Group	taun@kpvt.onmicrosoft.com	Deleted	11/6/2019 4:06:30 PM	Unified Group Deleted :	BM1PFR0101MB1316 (15.20...
zz_25c9f68-ab8-4386-839...	Unified Group	taun@kpvt.onmicrosoft.com	Deleted	11/6/2019 4:06:20 PM	Unified Group Deleted :	BM1PFR0101MB1316 (15.20...
wee_86c9f3ac-0e01-4396-...	Unified Group	taun@kpvt.onmicrosoft.com	Deleted	11/6/2019 4:06:01 PM	Unified Group Deleted :	BM1PFR0101MB1316 (15.20...
Test1	Role Group	taun@kpvt.onmicrosoft.com	Created	11/5/2019 5:19:36 PM	Role Group Created : Attr	BM1PFR0101MB1316 (15.20...
ApplicationImpersonation-Ta...	Management Role Assigm.	taun@kpvt.onmicrosoft.com	Created	11/5/2019 3:14:50 PM	Management Role Assigm.	BM1PFR0101MB1316 (15.20...
996_724e7c1-4c2e-414a-9...	Unified Group	taun@kpvt.onmicrosoft.com	Deleted	11/4/2019 2:52:18 PM	Unified Group Deleted :	BM1PFR0101MB1316 (15.20...
NewDL001	Distribution Group	taun@kpvt.onmicrosoft.com	Deleted	11/4/2019 2:51:56 PM	Distribution Group Deleted	BM1PFR0101MB1316 (15.20...
ISLAND_c624925ad19-4...	Unified Group	taun@kpvt.onmicrosoft.com	Deleted	11/4/2019 2:51:43 PM	Unified Group Deleted :	BM1PFR0101MB1316 (15.20...
Mailbox16	Mailbox	taun@kpvt.onmicrosoft.com	Permissions Modified	11/4/2019 2:48:31 PM	Mailbox Permissions Modifie	BM1PFR0101MB1316 (15.20...
Mailbox167	Mailbox	taun@kpvt.onmicrosoft.com	Permissions Modified	11/4/2019 2:32:56 PM	Mailbox Permissions Modifie	BM1PFR0101MB1316 (15.20...
Mailbox158	Mailbox	taun@kpvt.onmicrosoft.com	Permissions Modified	11/4/2019 2:32:39 PM	Mailbox Permissions Modifie	BM1PFR0101MB1316 (15.20...
Mailbox15	Mailbox	taun@kpvt.onmicrosoft.com	Permissions Modified	11/4/2019 12:57:53 PM	Mailbox Permissions Modifie	BM1PFR0101MB1316 (15.20...
Mailbox139	Mailbox	taun@kpvt.onmicrosoft.com	Permissions Modified	11/4/2019 11:52:36 AM	Mailbox Permissions Modifie	BM1PFR0101MB1316 (15.20...
License2	Mailbox	taun@kpvt.onmicrosoft.com	Permissions Modified	11/4/2019 11:52:21 AM	Mailbox Permissions Modifie	BM1PFR0101MB1316 (15.20...
ApplicationImpersonation-Ta...	Management Role Assigm.	taun@kpvt.onmicrosoft.com	Created	11/4/2019 11:14:02 AM	Management Role Assigm.	BM1PFR0101MB1316 (15.20...
Sales	Mailbox	taun@kpvt.onmicrosoft.com	Deleted	10/31/2019 2:48:05 PM	Mailbox Deleted :	BM1PFR0101MB1316 (15.20...
Nick Jonas	Mailbox	taun@kpvt.onmicrosoft.com	Deleted	10/31/2019 2:48:01 PM	Mailbox Deleted :	BM1PFR0101MB1316 (15.20...
Marketing	Mailbox	taun@kpvt.onmicrosoft.com	Deleted	10/31/2019 2:47:56 PM	Mailbox Deleted :	BM1PFR0101MB1316 (15.20...
3633	Mailbox	taun@kpvt.onmicrosoft.com	Deleted	10/31/2019 2:47:48 PM	Mailbox Deleted :	BM1PFR0101MB1316 (15.20...
GAZ	Mailbox	taun@kpvt.onmicrosoft.com	Deleted	10/31/2019 2:47:44 PM	Mailbox Deleted :	BM1PFR0101MB1316 (15.20...
ApplicationImpersonation-Ta...	Management Role Assigm.	taun@kpvt.onmicrosoft.com	Created	10/30/2019 12:48:13 PM	Management Role Assigm.	BM1PFR0101MB1316 (15.20...
ApplicationImpersonation-Ta...	Management Role Assigm.	taun@kpvt.onmicrosoft.com	Created	10/29/2019 3:15:04 PM	Management Role Assigm.	BM1PFR0101MB1316 (15.20...
NewDL002	Dynamic Distribution Group	taun@kpvt.onmicrosoft.com	Properties Modified	10/25/2019 4:25:59 PM	Dynamic Distribution Group	BM1PFR0101MB1316 (15.20...
NewDL002	Dynamic Distribution Group	taun@kpvt.onmicrosoft.com	Created	10/25/2019 4:25:58 PM	Dynamic Distribution Group	BM1PFR0101MB1316 (15.20...
NewDL001	Distribution Group	taun@kpvt.onmicrosoft.com	Owner Modified	10/25/2019 4:25:42 PM	Distribution Group Owner M.	BM1PFR0101MB1316 (15.20...
NewDL001	Distribution Group	taun@kpvt.onmicrosoft.com	Created	10/25/2019 4:25:42 PM	Distribution Group Created	BM1PFR0101MB1316 (15.20...
Mailbox130	Mailbox	taun@kpvt.onmicrosoft.com	Permissions Modified	10/25/2019 1:24:16 PM	Mailbox Permissions Modifie	BM1PFR0101MB1316 (15.20...
Mailbox123	Mailbox	taun@kpvt.onmicrosoft.com	Permissions Modified	10/25/2019 1:24:03 PM	Mailbox Permissions Modifie	BM1PFR0101MB1316 (15.20...
Mailbox11	Mailbox	taun@kpvt.onmicrosoft.com	Permissions Modified	10/25/2019 1:23:51 PM	Mailbox Permissions Modifie	BM1PFR0101MB1316 (15.20...
zz_25c9f68-ab8-4386-839...	Unified Group	gaaran@kpvt.onmicrosoft.c...	Properties Modified	10/24/2019 2:13:05 PM	Unified Group Properties Mo	BM1PFR0101MB3027 (15.20...
8f4d1315-5d93-4621-9872b...	Addin	gaaran@kpvt.onmicrosoft.c...	Created	10/24/2019 12:44:15 PM	Addin Created : Attribute	BM1PFR0101MB3027 (15.20...

States & Behavior

Regulatory Compliance

Figure 8: All Modifications in Exchange Online Report

3 Office 365 Component

3.1 Prerequisites

- To add OneDrive, Azure, Teams or Skype for Business components to the Lepide Data Security Platform for Auditing, an app must be registered on the Microsoft 365 portal.
- Login to the Office 365 Tenant needs to be done by a User with a Global Administrator account. This is because if the user does not have global admin rights then they will not be able to grant admin consent permissions to the Tenant.
- Without Global Admin rights, the Grant permission option in Microsoft will be grayed out.

3.2 OneDrive

3.2.1 Steps to Register an App and Generate the Client ID and Secret Key for OneDrive Auditing

1. Log onto the Microsoft 365 Admin Center
2. Select **Azure Active Directory** from the Admin Center
3. Click on **App Registration** and follow the steps below to generate Client ID and Secret Key:
 - Select **New Registration** and provide a valid name for the registration.
 - Click on **Register Account** and the Client ID will be displayed which the user can copy for future use
 - For the given Client ID generated in the Azure Account Dashboard, click on **Certificates and Secrets**.
 - Click on **Add New Client Secret** and a **Secret Value** will be generated which the user can copy for future use.

NOTE: Copy the Client ID and Secret value for adding an Office 365 component for OneDrive

4. Click on the API permission tab for the given Client ID and select **Add a Permission**
5. Select Microsoft API's and API's my organization uses as follows:
Microsoft 365 Graph API's, Office 365 Management API's and select permission type(s) as detailed below:

Microsoft Graph API's

AuditLog.Read.All Delegated

AuditLog.Read.All Application

Office 365 Management API's

ActivityFeed.Read Application

ActivityFeed.ReadDlp Application

NOTE: Every permission change required must be granted admin consent

6. Now add the components with Client ID and Secret Key

3.2.2 Steps to Generate the Client ID and Secret Key for OneDrive Data Discovery & Classification

Modern Authentication for OneDrive for Business

1. Log into the office 365 account through SharePoint Administrator / Global Administrator
2. Go to https://<Tenant>-admin.sharepoint.com/_layouts/15/appregnew.aspx
3. Click the two **Generate** buttons to generate a **Client ID** and a **Secret Key** and set the following options:
 - Title: Enter a name for the app
 - App Domain: www.localhost.com
 - Redirect URL: <https://www.localhost.com/>

NOTE: Save the retrieved Client ID and Secret Key. They are the credentials you are using and allow read or update actions to be performed on your OneDrive for Business environment.

4. Go to https://<Tenant>-admin.sharepoint.com/_layouts/15/appinv.aspx
5. Enter the generated **Client ID** in the **App Id** field and click **Lookup**
6. In the App's Permission Request XML field, enter the code below to grant appropriate access:

```
<AppPermissionRequests AllowAppOnlyPolicy="true">  
<AppPermissionRequest Scope="http://sharepoint/content/tenant" Right="FullControl" />  
<AppPermissionRequest Scope="http://sharepoint/social/tenant" Right="Read" />  
</AppPermissionRequests>
```

7. Click **Create**
8. You will now be prompted to trust the add-in for all the permissions that it requires
9. Click **Trust It** to grant the requested access
10. Now, Create a profile in Data Discovery & Classification and Classify it

3.2.3 Steps to Generate the Client ID and Secret Key for OneDrive Current Permissions Analysis

Modern Authentication for OneDrive for Business

1. Log into the office 365 account through SharePoint Administrator / Global Administrator.
2. Go to https://<Tenant>-admin.sharepoint.com/_layouts/15/appregnew.aspx
3. Click the two **Generate** buttons to generate a **Client ID** and a **Secret Key**
4. Specify the following options:
 - Title: Enter a name for the app
 - App Domain: www.localhost.com
 - Redirect URL: <https://www.localhost.com/>

NOTE: Save the retrieved Client ID and Secret Key. They are the credentials you are using and allow read or update actions to be performed on your OneDrive for Business environment.

5. Go to https://<Tenant>-admin.sharepoint.com/_layouts/15/appinv.aspx
6. Enter the generated **Client ID** in the **App Id** field and click **Lookup**
7. In the App's Permission Request XML field, enter the below code to grant appropriate access:

```
<AppPermissionRequests AllowAppOnlyPolicy="true">  
<AppPermissionRequest Scope="http://sharepoint/content/tenant" Right="FullControl" />  
<AppPermissionRequest Scope="http://sharepoint/social/tenant" Right="Read" />  
</AppPermissionRequests>
```

8. Click **Create**
9. You will be prompted to trust the add-in for all the permissions that it requires
10. Click **Trust It** to grant the requested access
11. Now, Create a dataset in Current permission scan settings and Scan it

3.3 Azure

3.3.1 Steps to Register an App and Generate the Client ID and Secret Key for Azure Auditing

1. Log onto the Microsoft 365 Admin Center
2. Select **Azure Active Directory** from the Admin Center
3. Click on **App Registration** and follow the steps below to generate Client ID and Secret Key:
 - Select **New Registration** and provide a valid name for the registration.
 - Click on **Register Account** and the Client ID will be displayed which the user can copy for future use
 - For the given Client Id generated in the Azure Account Dashboard, click on **Certificates and Secrets**.
 - Click on **Add New Client Secret** and a **Secret Value** will be generated which the user can copy for future use.

NOTE: Copy the Client ID and Secret value for adding Office 365 component for Azure

4. Click on the API permission tab for the given Client ID and select **Add a Permission**
5. Select Microsoft API's and API's my organization uses as follows:
 - Microsoft Graph API's**

Sites.Read.All	Delegated
----------------	-----------
 - Office 365 Management API's**

ActivityFeed.Read	Delegated
ActivityFeed.Read	Application
ActivityFeed.ReadDlp	Delegated
ActivityFeed.ReadDlp	Application
6. Now add the components with Client ID and Secret Key

3.4 Teams

3.4.1 Steps to Register an App and Generate the Client ID and Secret Key for Teams Auditing

1. Log onto the Microsoft 365 Admin Center
2. Select **Azure Active Directory** from the Admin Center
3. Click on **App Registration** and follow the steps below to generate Client ID and Secret Key:
 - Select **New Registration** and provide a valid name for the registration.
 - Click on **Register Account** and the Client ID will be displayed which the user can copy for future use
 - For the given Client Id generated in the Azure Account Dashboard, click on **Certificates and Secrets**.
 - Click on **Add New Client Secret** and a **Secret Value** will be generated which the user can copy for future use.

NOTE: Copy the Client ID and Secret value for adding Office 365 component for Teams

4. Click on the API permission tab for the given Client ID and select **Add a Permission**
5. Select Microsoft API's and API's my organization uses as follows:
 - Microsoft Graph API's**

Sites.Read.All	Delegated
----------------	-----------
 - Office 365 Management API's**

ActivityFeed.Read	Delegated
ActivityFeed.Read	Application
ActivityFeed.ReadDlp	Delegated
ActivityFeed.ReadDlp	Application
6. Now add the components with Client ID and Secret Key

3.5 Skype for Business

3.5.1 Steps to Register an App and Generate the Client ID and Secret Key for Skype for Business Auditing

1. Log onto the Microsoft 365 Admin Center
2. Select **Azure Active Directory** from the Admin Center
3. Click on **App Registration** and follow the steps below to generate Client ID and Secret Key:
 - Select **New Registration** and provide a valid name for the registration.
 - Click on **Register Account** and the Client ID will be displayed which the user can copy for future use
 - For the given Client Id generated in the Azure Account Dashboard, click on **Certificates and Secrets**.
 - Click on **Add New Client Secret** and a **Secret Value** will be generated which the user can copy for future use.

NOTE: Copy the Client ID and Secret value for adding Office 365 component for Skype

4. Click on the API permission tab for the given Client ID and select **Add a Permission**
5. Select Microsoft API's and API's my organization uses as follows:
 - Microsoft Graph API's**

Sites.Read.All	Delegated
----------------	-----------
 - Office 365 Management API's**

ActivityFeed.Read	Delegated
ActivityFeed.Read	Application
ActivityFeed.ReadDlp	Delegated
ActivityFeed.ReadDlp	Application
6. Now add the components with Client ID and Secret Key

3.6 Adding Azure Active Directory, OneDrive for Business, Skype for Business & Microsoft Teams

The Lepide Data Security Platform audits the changes inside Azure AD, OneDrive, Skype for Business and MS Teams and all these components can be added in one go under the component name Office 365.

NOTE: We can audit azure file storage if synced with an on-premise file server

1. From the Component Management screen, click on **Office 365** to add your Tenant.

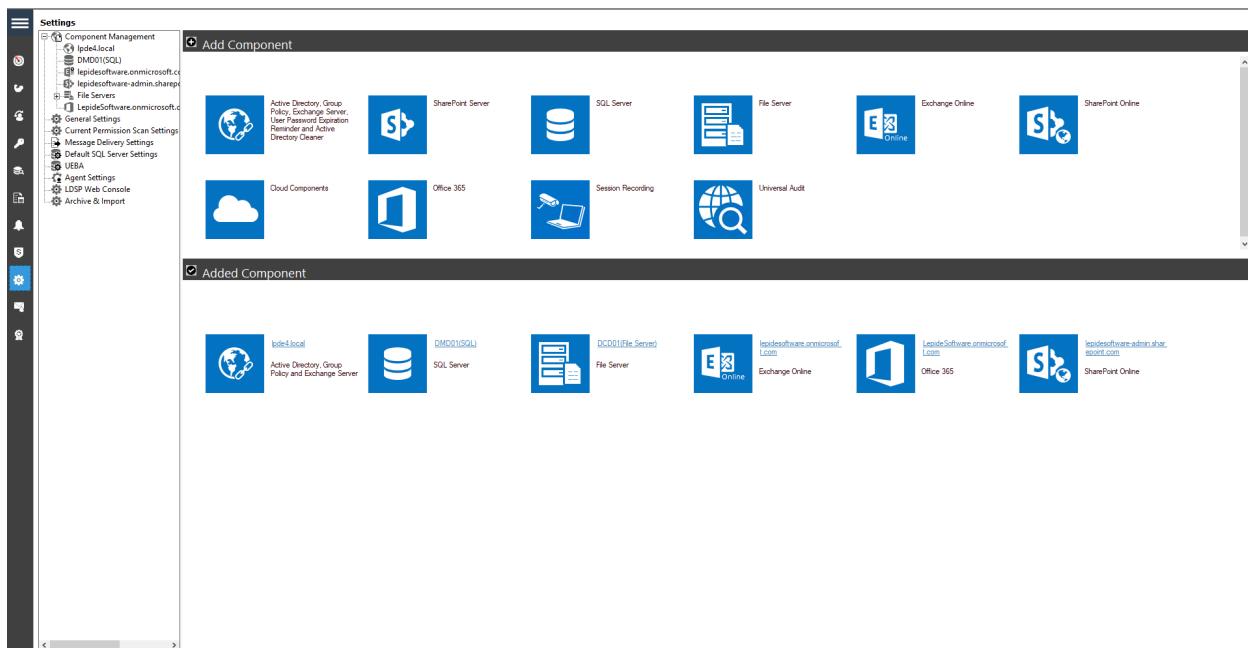


Figure 9: Component Management Screen

The Global Administrator App Credentials dialog box appears:

Global Administrator App Credentials
Please provide the global administrator app Client ID and Secret Value Key.

Tenant Name
Enter like: Your domain name.onmicrosoft.com

Subscription Type ?

Client ID

Secret Key

< Back Next > Cancel

Figure 10: App Credentials

2. Enter the Tenant Name, choose the Subscription Type and enter the Client ID and Secret Key.
3. The instructions to generate the Client ID and Secret Key are given in Sections 3.2 to 3.5 of this guide
4. Close this dialog box once finished and click **Next**

The Components dialog box is displayed:

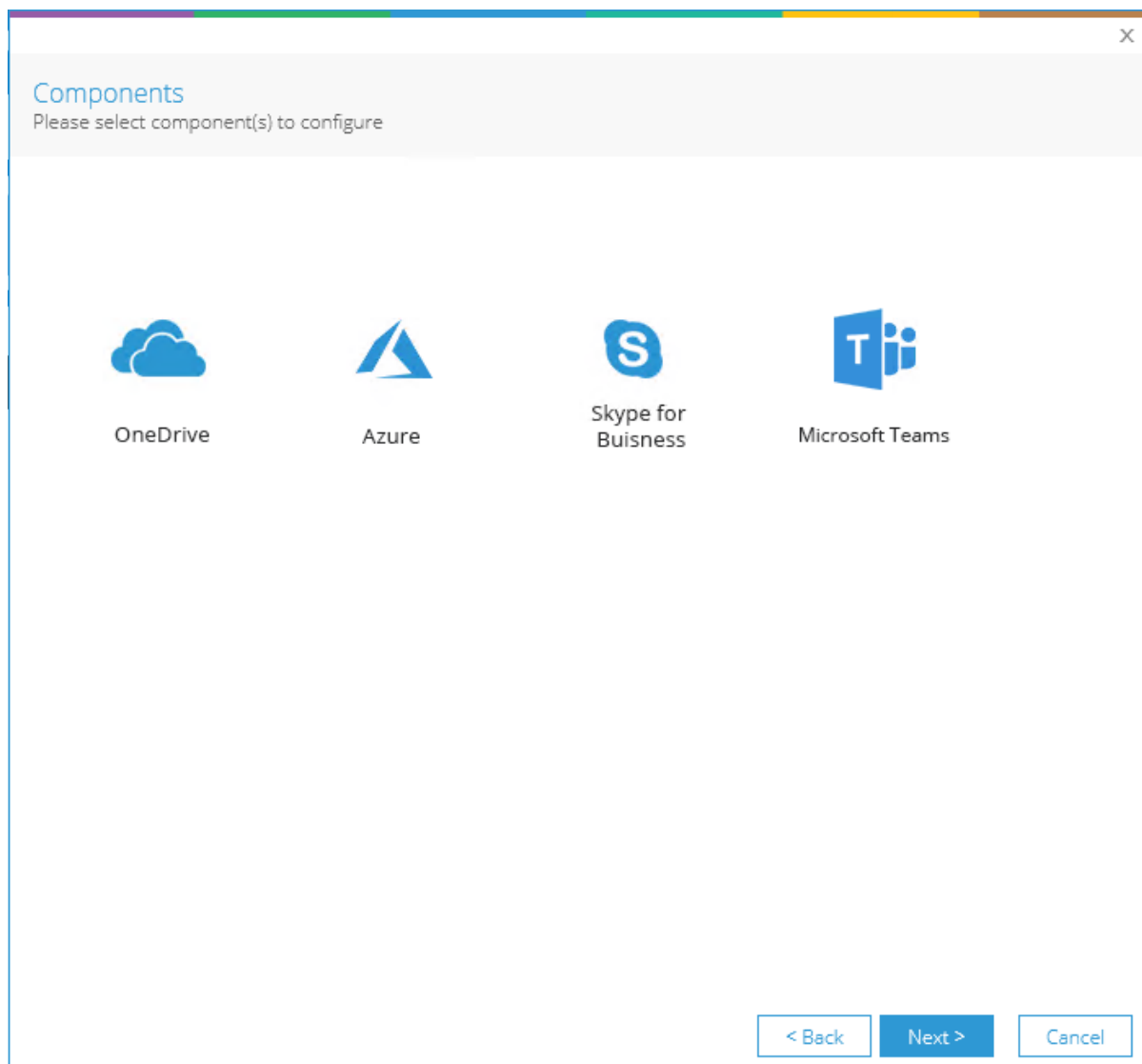


Figure 11: Components

5. Select the components you would like to audit. You can add any one or more components as required.
6. Click **Next**

Database Settings

Please enter SQL server details to store the audit data

Configure SQL Server

SQL Server: 192.168.40.238

Authentication

Windows Authentication

SQL Authentication (recommended)

User Name: sa


Password: ●●●●●●

Test Connection

Select Database: Lepide_0365

< Back Next > Cancel

Figure 12: Database Settings

7. The database settings dialog box is displayed:
8. From this dialog box you can do the following:
 - Add the SQL Server name. Click the  icon to select a server
 - In the Select Database box, type in a name and the Solution will create a database with this name
9. Click **Finish**

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

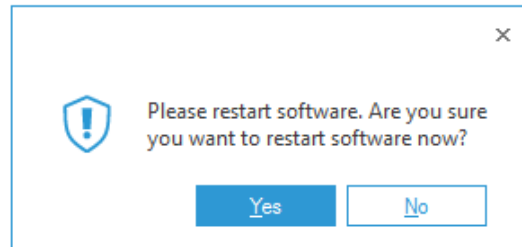



Figure 13: Confirm Restart

11. Click **Yes** to restart

3.7 Viewing the Reports

- Click the Users & Entity behavior icon  to display the States & Behavior screen
- The All-Environment Changes Report holds all the changes for these components
- From the tree structure to the left side of the screen click on **All Environment Changes**.
- The example below shows the All Environment Changes Report:

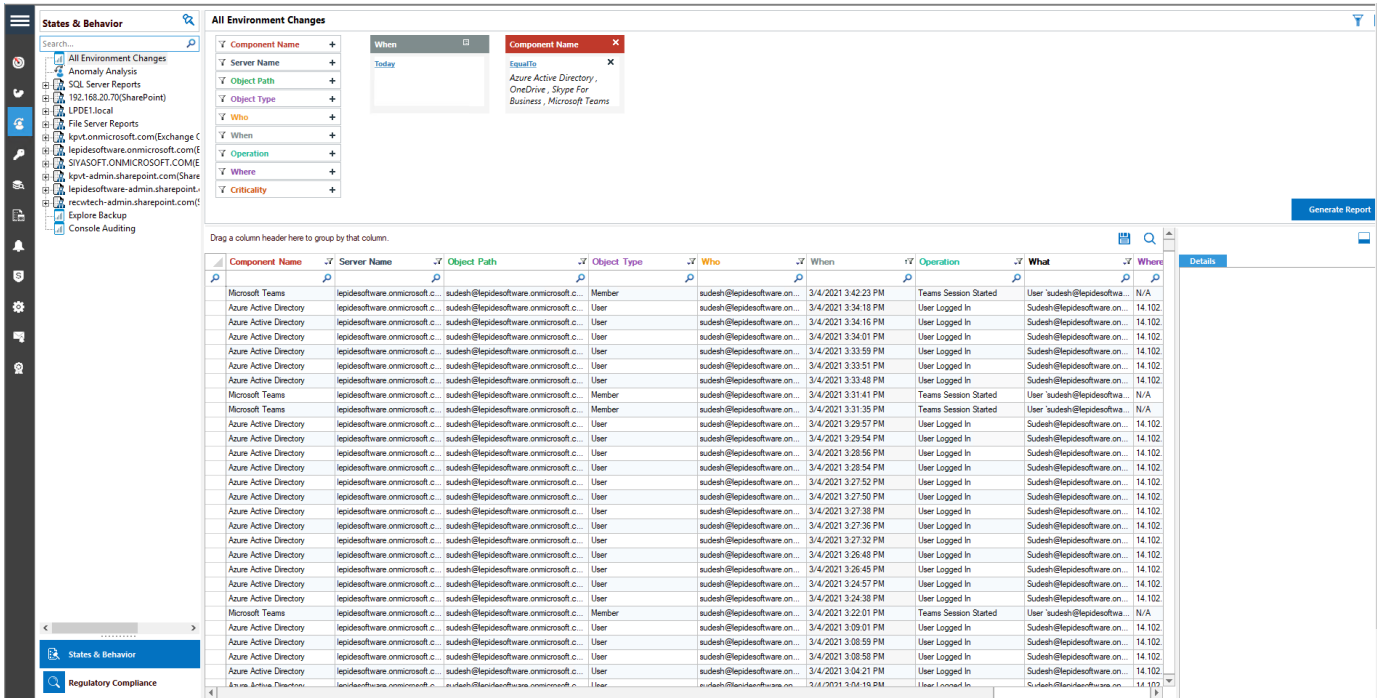


Figure 14: All Environment Changes Report

4 SharePoint Online

4.1 Prerequisites

- To add SharePoint Online to the Lepide Data Security Platform for Auditing, an app must be registered on the Microsoft 365 portal.
- Login to the Office 365 Tenant needs to be done by a User with a Global Administrator account. This is because if the user does not have global admin rights then they will not be able to grant admin consent permissions to the Tenant.
- Without Global Admin rights, the Grant permission option in Microsoft will be grayed out.

4.2 Steps to Register an App and Generate the Client ID and Secret Key for SharePoint Online Auditing

Log onto the Microsoft 365 Admin Center

1. Select **Azure Active Directory** from the Admin Center
2. Click on **App Registration** and follow the steps below to generate Client ID and Secret Key:
 - Select **New Registration** and provide a valid name for the registration.
 - Click on **Register Account** and the Client ID will be displayed which the user can copy for future use
 - For the given Client Id generated in the Azure Account Dashboard, click on **Certificates and Secrets**.
 - Click on **Add New Client Secret** and a **Secret Value** will be generated which the user can copy for future use.

NOTE: Copy the Client ID and Secret value for adding a SharePoint Online component.

3. Click on the API permission tab for the given Client ID and select **Add a Permission** Microsoft 365 Graph API's, Office 365 Management API's and select permission type(s) as detailed below:

Microsoft Graph API's

Sites.Read.All	Delegated
----------------	-----------

Office 365 Management API's

ActivityFeed.Read	Delegated
ActivityFeed.Read	Application
ActivityFeed.ReadDlp	Delegated
ActivityFeed.ReadDlp	Application

NOTE: Every permission change required must be granted admin consent

4. Now add the components with Client ID and Secret Key

4.3 Steps to Generate the Client ID and Secret Key for SharePoint Online Data Discovery & Classification

Modern Authentication for SharePoint Online

1. Log into the Office 365 account through SharePoint Administrator / Global Administrator
2. Go to https://<Tenant>-admin.sharepoint.com/_layouts/15/appregnew.aspx
3. Click the two **Generate** buttons to generate a **Client ID** and a **Secret Key** and set the following options:
 - Title: Enter a name for the app
 - App Domain: www.localhost.com
 - Redirect URL: <https://www.localhost.com/>

NOTE: Save the retrieved Client ID and Secret Key. They are the credentials you are using and allow read or update actions to be performed on your SharePoint Online for Data Discovery and Classification.

4. Go to https://<Tenant>-admin.sharepoint.com/_layouts/15/appinv.aspx
5. Enter the generated **Client ID** in the **App Id** field and click **Lookup**
6. In the App's Permission Request XML field, enter the code below to grant appropriate access:

```
<AppPermissionRequests AllowAppOnlyPolicy="true">  
<AppPermissionRequest Scope="http://sharepoint/content/tenant" Right="FullControl" />  
</AppPermissionRequests>
```

7. You will now be prompted to trust the add-in for all the permissions that it requires
8. Click **Trust It** to grant the requested access

Please run the command below at SharePoint Online Management Shell:

```
function Enable-SPDisableCustomAppAuthentication {  
    Write-Host "Please specify sharepoint organisation name." -ForegroundColor Green  
    Write-Host "For example if your sharepoint site is https://contoso.sharepoint.com value should be  
    contoso: " -ForegroundColor Green -NoNewline  
    $orgName = Read-Host  
    $orgName = $contosh
```



```
Write-Verbose "Connecting to: https://contoso-admin.sharepoint.com" -Verbose
Connect-SPOService -Url "https://contosh-admin.sharepoint.com"
Set-SPOTenant -DisableCustomAppAuthentication $false
}
Enable-SPDisableCustomAppAuthentication
```

Please run the command below:

```
Set-SPOTenant -DisableCustomAppAuthentication $false
```

The permissions given to the Client ID are as follows:

Scope: <http://sharepoint/content/tenant> Full Control

Full control is required here as **Read permission** is required to read the file and content, **Write permission** is required to be able to add the tags and the **Manage permission** is required to be able to manage both the added and existing tags on the file. By using the Full Control permission, all these options are available.

Now, Create a profile in Data Discovery & Classification and Classify it

4.4 Steps to Generate the Client ID and Secret Key for SharePoint Online Current Permissions Analysis

Modern Authentication for OneDrive for Business

1. Log into the office 365 account through SharePoint Administrator / Global Administrator.
2. Go to https://<Tenant>-admin.sharepoint.com/_layouts/15/appregnew.aspx
3. Click the two **Generate** buttons to generate a **Client ID** and a **Secret Key**
4. Specify the following options:
 - Title: Enter a name for the app
 - App Domain: www.localhost.com
 - Redirect URL: <https://www.localhost.com/>

NOTE: Save the retrieved Client ID and Secret Key. They are the credentials you are using and allow read or update actions to be performed on your SharePoint Online for Current Permission Analysis.

5. Go to https://<Tenant>-admin.sharepoint.com/_layouts/15/appinv.aspx
6. Enter the generated **Client ID** in the **App Id** field and click **Lookup**
7. In the App's Permission Request XML field, enter the code below to grant appropriate access:
<AppPermissionRequests AllowAppOnlyPolicy="true">
<AppPermissionRequest Scope="http://sharepoint/content/tenant" Right="FullControl" />
</AppPermissionRequests>
11. You will now be prompted to trust the add-in for all the permissions that it requires
12. Click **Trust It** to grant the requested access

Please run the command below at SharePoint Online Management Shell:

```
function Enable-SPDisableCustomAppAuthentication {  
    Write-Host "Please specify sharepoint organisation name." -ForegroundColor Green  
    Write-Host "For example if your sharepoint site is https://contoso.sharepoint.com value should be  
    contoso:" -ForegroundColor Green -NoNewline  
    $orgName = Read-Host  
    $orgName = $contosh
```

```
Write-Verbose "Connecting to: https://contoso-admin.sharepoint.com" -Verbose  
Connect-SPOService -Url "https://contosh-admin.sharepoint.com"
```

- Set-SPOTenant
- Now, Create a dataset in Current permission scan settings and Scan it

4.5 Adding a SharePoint Online Component

The Lepide Data Security Platform tracks the changes inside SharePoint Online and gives detailed reporting on any configuration changes. For example, Document Modifications, SharePoint Group Modifications, etc.

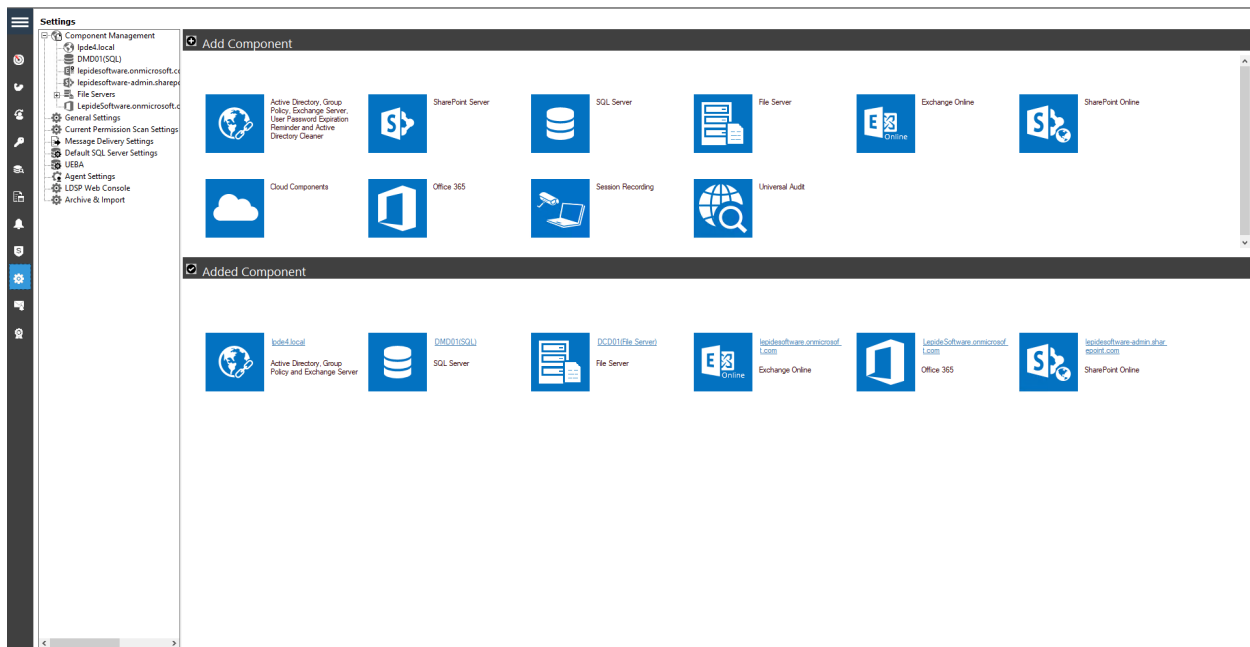


Figure 15: Component Management Screen

- From the Component Management screen click on **SharePoint Online**.

The Global Administrator App Credentials dialog box is displayed:

Global Administrator App Credentials
Please provide the global administrator app Client ID and Secret Value Key.

Central Admin URL ?

NOTE: Please add the Central Admin URL correctly. Use format "https://domainName-admin.sharepoint.com" Enter like: Your domain name.onmicrosoft.com

Tenant Name

Client ID

Secret Key

< Back Next > Cancel

Figure 16: App Credentials

- Enter the Central Admin URL, Tenant Name and the Client ID and Secret Key.
- The instructions to generate the Client ID and Secret Key are given in Section 4.2 to 4.4 of this guide
- **Close** this dialog box once finished and click **Next**

The Add Objects to Audit dialog box is displayed:

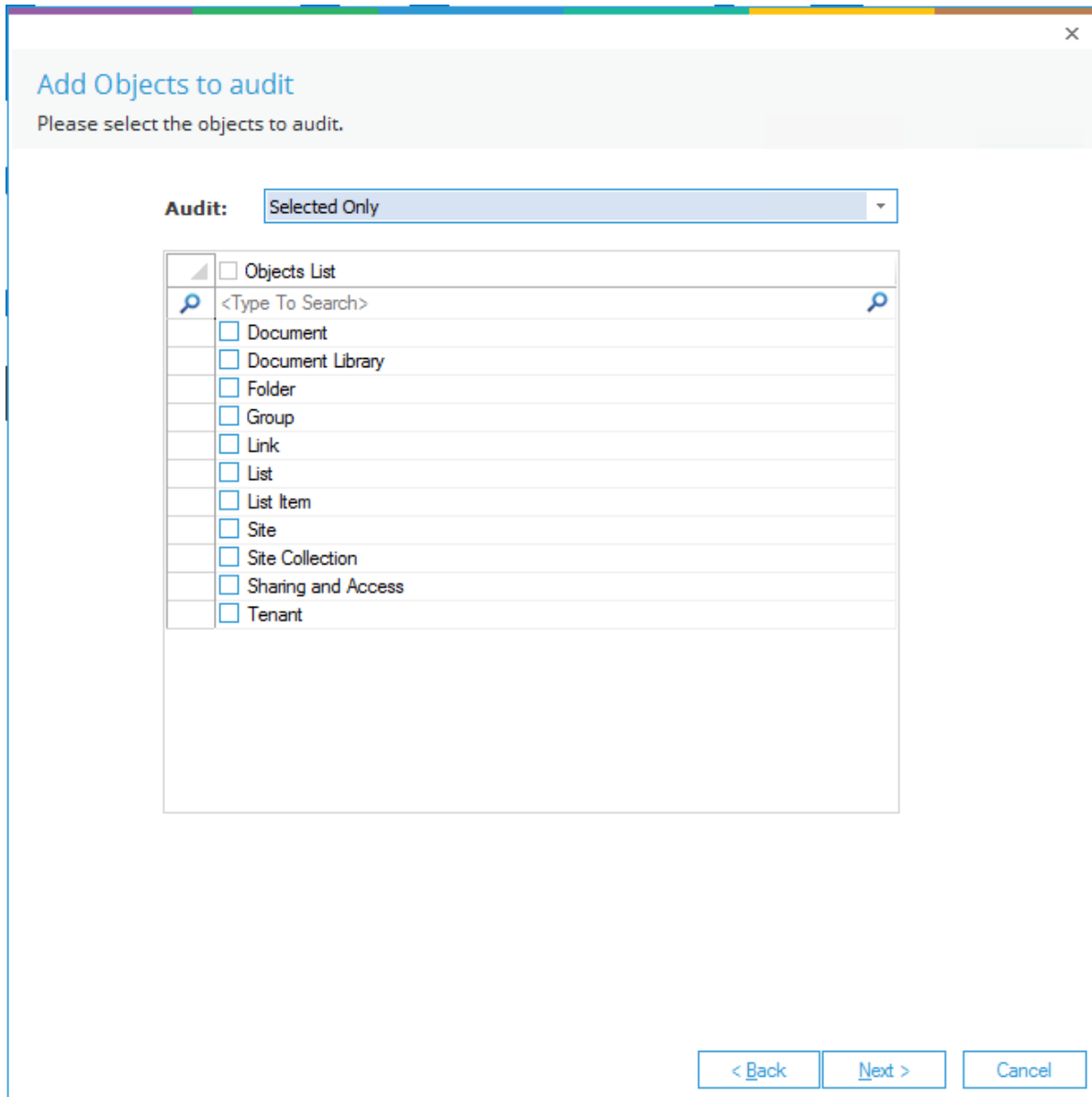


Figure 17: Add Objects to Audit

- Select the Objects you would like to audit. The options are:
 - All Objects – this is the default option
 - Selected Only

- All but Excluding Selected
 - To audit specific objects, choose **Selected Only** from the drop-down list and the objects are displayed with checkboxes to select those to be **included** in auditing:
 - To audit all **except** specific objects, choose **All but Excluding Selected** from the drop-down list and the checked objects will be **excluded** from auditing.

- Click **Next**

The Add Operations dialog box is displayed:

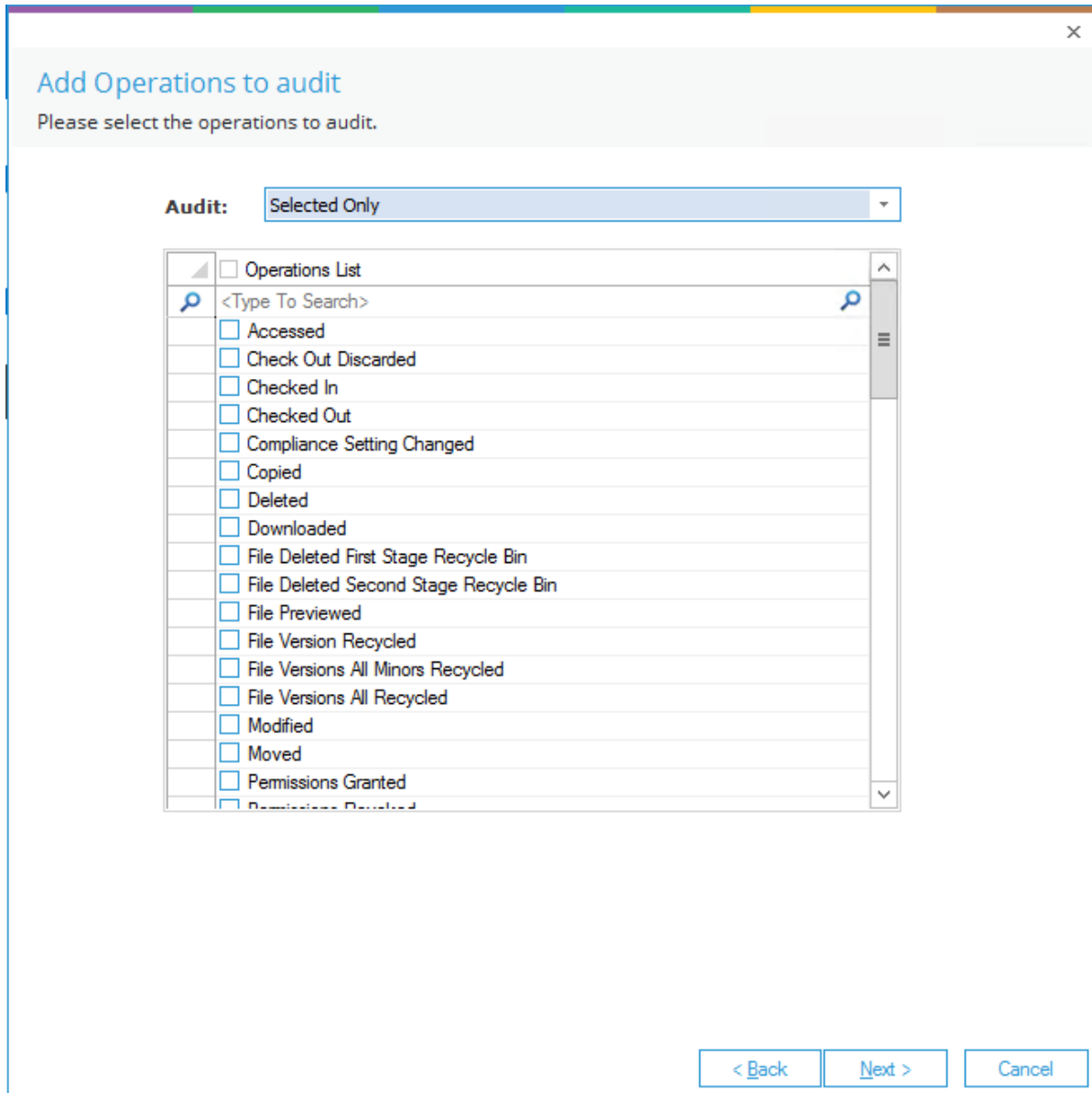


Figure 18: Add Operations to Audit

- Select the Operations you would like to audit. The options are:
 - All – this is the default option
 - Selected Only
 - All but Excluding Selected
 - To audit specific operations, choose **Selected Only** from the drop-down list and the operations are displayed with checkboxes to select those to be **included** in auditing:
 - To audit all **except** specific operations, choose **All but Excluding Selected** from the drop-down list and the checked operations will be **excluded** from auditing.
- Click **Next**

The Database Settings dialog box is displayed:

Database Settings
Please enter SQL server details to store the audit data

Configure SQL Server

SQL Server: 192.168.40.238

Authentication

Windows Authentication

SQL Authentication

User Name: sa

Password: ••••••••

Test Connection

Select Database: Lepide_SP_Online

< Back Next > Cancel

Figure 19: Database Settings

- From this dialog box you can do the following:
 - Add the **SQL Server** name. Click the icon to select a server
 - In the **Select Database** box, type in a 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:

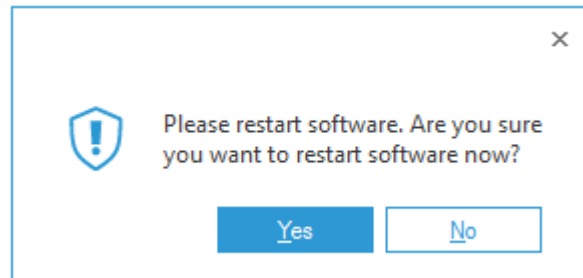



Figure 20: Confirm Restart

- Click **Yes** to restart

4.6 Viewing the Reports

- Click the Users & Entity behavior icon  to display the States & Behavior screen
- From the tree structure to the left side of the screen expand SharePoint Online.
- There will be a separate Node for SharePoint Online for the tenant which has been added. Expand this Node
- The example below shows the All Modifications in SharePoint Online Report:

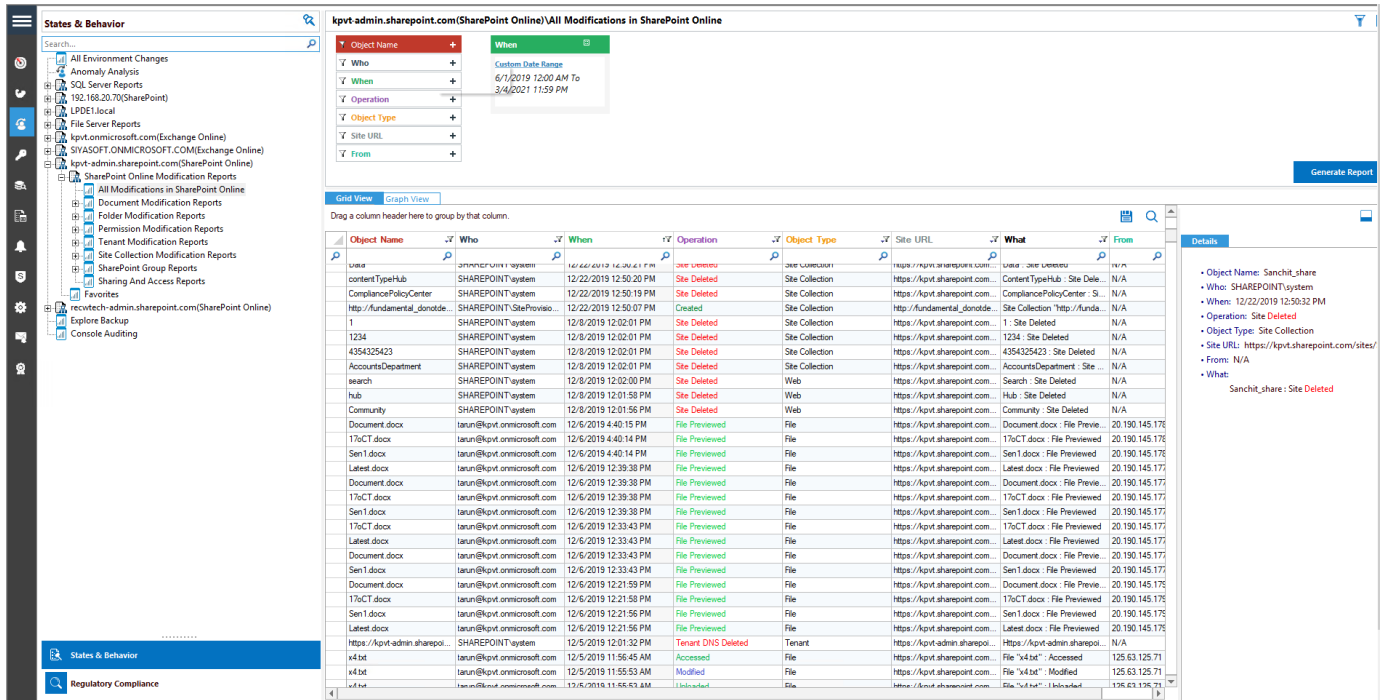


Figure 21: All Modifications in SharePoint Online Report

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

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.

