## **GTB DLP Suite**

### **GTB SharePoint Online Discovery**

Reference, Version 15.18.3

GTB Technologies, Inc December 2023

Intellectual property rights	This document is the property of GTB Technologies, Inc. No part of this document shall be reproduced, stored in a retrieval system, translated, transcribed, or transmitted by any means without permission from GTB Technologies. Information contained within this document is confidential and proprietary to GTB Technologies and should not be disclosed to anyone other than the recipients and reviewers of this document. However, in the event of award to GTB Technologies, this information may be disclosed to and will be used on
	behalf of and according to the interests of the client to whom it is addressed.

**Confidentiality Statement** The descriptive materials and related information in this document contain information that is confidential and proprietary to GTB Technologies. This information is submitted with the express understanding that it will be held in strict confidence and will not be disclosed, duplicated, or used, in whole or in part, for any purpose other than evaluation of this document.

Patents Statement	GTB Technologies ha	as pending patent	applications for	this product.
-------------------	---------------------	-------------------	------------------	---------------

Copyright statement	Copyright © GTB Technologies, Inc 2005-2023 www.gttb.com
Contacts	GTB Technologies, Inc. 2054 Vista Parkway, Suite 400 West Palm Beach, FL 33411

Phone: 1 (800) 626-0557 Email: *support@gttb.com* 



### **Contents**

1	Int	roduction	3
	1.1 1.2	Definitions Requirements	3
2	Sh	arePoint with Classic Authentication	4
	2.1	Create a SharePoint Online Service Account	4
	2.2	Add permissions to scan single SharePoint site	2
	2.3	Add permissions to scan all sites	4
	2.4	Install Discovery Server	5
	2.5	Start the SharePoint Online Discovery	6
	2.6	Check scan result	8
	2.7	How to scan all SharePoint sites	9
	2.8	How to scan separate SharePoint files or folders	11
3	Sh	arePoint with Modern Authentication	14
	3.1	Create Application for Modern Authentication	14
	3.2	Add Application credentials	15
	3.3	Install Discovery Server	17
	3.4	Start the SharePoint Online Discovery	18
	3.5	Check scan result	19



# **1** Introduction

This document explains the necessary steps for running the GTB SharePoint Online Discovery.

### 1.1 Definitions

Scanning server – The Windows Server machine which performs the Discovery scan.

#### 1.2 Requirements

 Scanning Server – The GTB Discovery Server installed on any Windows Server. Provide at least 2 CPU cores and 2GB RAM for each.

The Discovery Server scans 1 file per CPU core at a time. The more cores provided, the faster is scanning speed.

SharePoint Online account - Service Account, which has access to the SharePoint Online.



# **2** SharePoint with Classic Authentication

### 2.1 Create a SharePoint Online Service Account

- 1. Open https://admin.microsoft.com/ web page of the Office 365 portal.
- 2. Go to the *Active users* page.
- 3. Click the *Add* button like shown in the Figure below.

	Microsoft 365 admin cent	er	Ø ⊕ ⊕				
=			GTB Tech				
ඛ	Home		Active users				
R	Users						
	Active users						
	Contacts		🐣 Add a user 📃 User templates	🐴 Add multiple u	sers 🛗 Multi-factor authentication 🥻	🖔 Delete a user 🛛 Refresh 🛯 🦓 Reset passw	ord 🛓 Export users \cdots 🍸 Filt
	Guest users						
	Deleted users		Display name ↑		Username	Licenses	Choose columns
ጵ	Groups		O Aleksey Sharaputin	s :	asharaputin@gtbtech.onmicrosoft.com	Exchange Online (Plan 1) , SharePoint (F	Plan 1) , OneDrive fc
	Billing		GTB Demo		Demo@gtbtech.onmicrosoft.com	Exchange Online (Plan 1)	
ß	Setup		info		info140160@gtbtech.onmicrosoft.com	Unlicensed	

4. Type Account Name, Username, and Password in the appropriate fields. Click the Next button.

Add a user	
Basics	Set up the basics
Product licenses	To get started, fill out some basic information about who you're adding as a user.
Optional settings	First name Last name
	SharePoint Scan
O Finish	Display name *
	SharePoint Scan
	Username *
	spscan @ gtbtech.onmicrosoft.com ~
	Password settings
	O Auto-generate password
	Let me create the password
	Password *
	Strong
	Require this user to change their password when they first sign in
	Send password in email upon completion



5. Select *Location* and *License* for SharePoint. Press the *Next* button.



6. Select a Role: User.

Add a user	
Basics	Optional settings
Product licenses     Optional settings	You can choose what role you'd like to assign for this user, and fill in additional profile information.
   Finish	Roles (User: no administration access)
	Profile info



7. Check the details and press the *Finish adding* button.



8. Press the Close button.

Add a user	
Basics     Product licenses	<b>User details</b> Display name: SharePoint Scan Username:spscan@gtbtech.onmicrosoft.com Password: ******* Show
<ul> <li>⊘ Optional settings</li> <li>↓</li> <li>✓ Finish</li> </ul>	Licenses bought None
	SharePoint (Plan 1) Save these user settings as a template? User templates allow you to quickly add similar users in the future by saving a set of shared settings such as domain, password, product licenses, and roles. Review settings for this user template
	Name your template * adduser Add a description (recommended) Example: Template for full-time senior engineers in New York office
	Save as template



### 2.2 Add permissions to scan single SharePoint site

1. Open the *SharePoint Online admin* page and go to the *Active sites* section.

	SharePoint admin cente	r		<u>ૻ</u> ૼૼૼૼૼૼૼૼૼૼૼૼૼૼૼૼૼૼૼૼૼૼૼૼૼૼૼૼૼૼૼૼૻૼઌૼૻૼૼૼૼૼૼ	T CHANNE	
=			Active sites			
ŵ	Home		Use this page to manage all	your sites. Learn more		
	Sites	^	+ Create 🏾 🎭 Permissio	ns 🗸 😤 Hub 🗸 😤 Sharing 📋 Delete		
Ľ	Active sites Deleted sites		Site name $\uparrow$ $\vee$	URL $\vee$	Storage used (G $\vee$	Primary admin $\vee$
<u></u> <u></u> <u></u> <u></u> <u></u> <u></u> <u></u> <u></u> <u></u> <u></u>	Policies	~	09876421109876421	11098764211/sites/09876421109876421109	0.00	A Group owners
٢	Settings		All Company	/sites/allcompany	0.00	A Group owners
55	Content services	~	AIIGTB	/sites/all	0.00	A Group owners
Ģ	Migration		asharaputin	/sites/asharaputin	0.31	ℜ Group owners
	More features		<ul> <li>Communication Site</li> </ul>	/sites/CommunicationSite	0.00	Uzi Yair
_	NOIE learnies		created on Panel	/sites/onPanel	0.00	Uzi Yair
8	OneDrive admin center		DLP Scan	/sites/dlp_scan	0.09	A Group owners
-			dynamic_membership	p/sites/dynamic_membership	0.00	A Group owners
0	Customize navigation		ewrre -	/sites/erwwer	0.00	A Group owners

- 2. Select the site you want to scan.
- 3. Go to the *Permissions* tab, *Additional admins,* and press the *Manage* button.

	SharePoint admin center			$\begin{array}{c} \Phi & \Phi & \Phi & \Phi \\ \hline & & & & & & & & \\ \hline & & & & & & & &$	
=			Active sites		
命	Home		Use this page to manage all your sites. Lea	arn more	DLP Scan
	Sites	^	+ Create 🖇 Permissions 🗸 🖧 Hu	b 🗸 😤 Sharing 📋 Delete	
1	Active sites				General Activity <b>Permissions</b> Policies
	Deleted sites		Site name $\uparrow$ $\checkmark$		
<u>+</u> +	Policies	~	098764211098764211098764211	/sites/09876421109876421109	For info about each role, learn more.
\$	Settings		All Company	/sites/allcompany	Site admins (1)
0.0	Content services	~	AIIGTB	/sites/all	
~	Minneller		asharaputin	/sites/asharaputin	Microsoft 365 Group owners
ري	Migration		Communication Site	/sites/CommunicationSite	Uzi Yair QA@gtbtech.onmicrosoft.com
:	More features	_	created on Panel	/sites/onPanel	Manage
æ	OneDrive admin center		DLP Scan	/sites/dlp_scan	Additional admins
		_	dynamic_membership	/sites/dynamic_membership	None Manage
0	Customize navigation		ewrre	/sites/erwwer	
	Show all		GergeyGarizanScecailGroup!@#\$	/sites/GergeyGarizanScecailGr	Site owners (1)



4. Type Account Name in the search field.

#### Manage additional admins

0 site admins (in addition to the Microsoft 365 Group owners)

Add an adm	Add an admin						
SharePoint Scan							
SS Sh	harePoint Scan						

5. Add and press the **Save** button.

#### Manage additional admins

1 site admin (in addition to the Microsoft 365 Group owners) Add an admin Enter a name or email address Name SharePoint Scan ×



#### 2.3 Add permissions to scan all sites

- 1. Open PowerShell in administration mode.
- 2. Install the SharePoint Online Management Shell.

Install-Module -Name Microsoft.Online.SharePoint.PowerShell

3. Sign in to SP Online in PowerShell.

\$TenantUrl = "Enter the SharePoint admin center URL"

Connect-SPOService -Url \$TenantUrl

4. Get list of all sites.

\$sites = Get-SPOSite -Limit all | foreach { \$\_.URL }

5. Set Administrator user email.

#### \$user = "user@contoso.com"

6. Run the command to add administrator full-access permission to all sites:

echo \$sites | ForEach-Object {Set-SPOUser -Site \$\_-LoginName \$user -IsSiteCollectionAdmin \$true}

Full Access permissions are required if you would like to apply remedial actions like Move/Delete.

赵 Administrator: Wir	ndows PowerShell				-		$\times$
PS C:\sp> \$sites = PS C:\sp> \$user = ' PS C:\sp> echo \$sit	Get-SPOSite   foreach { \$ .URL } "vstovpovoy@gtbtech.onmicrosoft.com" tes   ForEach-Object {Set-SPOUser -	" Site <b>\$_</b>	-LoginName <b>\$user</b>	-IsSiteColle	ectionAd	lmin <b>\$t</b> ı	rue}
Display Name	Login Name	Groups	User Type				
Vladimir Stovpovoy Vladimir Stovpovoy	<pre>vstovpovoy@gtbtech.onmicrosoft.com vstovpovoy@gtbtech.onmicrosoft.com</pre>	{} {}	Member Member				
Vladimir Stovpovoy Vladimir Stovpovoy Vladimir Stovpovov	vstovpovoy@gtbtech.onmicrosoft.com vstovpovoy@gtbtech.onmicrosoft.com vstovpovoy@gtbtech.onmicrosoft.com	$\left\{ \right\}$	Member Member Member				
Vladimir Stovpovoy Vladimir Stovpovoy	vstovpovoy@gtbtech.onmicrosoft.com vstovpovoy@gtbtech.onmicrosoft.com	{} {}	Member Member				
Vladimir Stovpovoy Vladimir Stovpovoy Vladimir Stovpovov	vstovpovoy@gtbtech.onmicrosoft.com vstovpovoy@gtbtech.onmicrosoft.com vstovpovoy@gtbtech.onmicrosoft.com	{} {} {}	Member Member Member				
Vladimir Stovpovoy Vladimir Stovpovoy Vladimir Stovpovoy	vstovpovoy@gtbtech.onmicrosoft.com vstovpovoy@gtbtech.onmicrosoft.com	{} {} {}	Member Member				
Vladimir Stovpovoy Vladimir Stovpovoy Vladimin Stovpovov	vstovpovoy@gtbtech.onmicrosoft.com vstovpovoy@gtbtech.onmicrosoft.com	{} {}	Member Member				
Vladimir Stovpovoy Vladimir Stovpovoy Vladimir Stovpovoy	vstovpovoy@gtbtech.onmicrosoft.com vstovpovoy@gtbtech.onmicrosoft.com	{qa {}	Member Member				
Vladimir Stovpovov	vstovpovoy@gtbtech.onmicrosoft.com	{}	Member				



#### 2.4 Install Discovery Server

- 1. Sign in to the **Central Console** using an account with Administrator privileges.
- 2. Go to the **Help > Download** tab of the GTB Central Console and download the GTB Discovery Server MSI package.

	GTB Central Console		🕼 🗟 🗔 Downloa	ads » Win	dows Endpoint Agents	
$\bigcirc$	Dashboard					
ö	Security Events	>	Windows Endpoint Agents		GTB Endpoint Agent + Networking	165 MB
	Reports		🗯 macOS Endpoint Agents		Endpoint device controls with Discovery + Network Traffic Inspection	v15.7.8-54972
$\overline{\bigcirc}$	GTB DLP Setup	>	🛕 Linux Endpoint Agents			
~	Network Status	>	Name Resolution Helper		GTB Discovery Server	165 MB
G	System	>	Security Manager	<u>+</u>	Discovery Server descution	
8	User Management		Administrative Tools			v15.7.8-54972
×	Maintenance	>	Local links for browsers		Antivirus execution list for Windows OS	
F	Logs	>		=	Antivirus exception list for Windows OS	
1	Help/Downloads	>				
1	Documentation					
	Downloads					

- 3. Install the GTB Discovery Server on any Windows PC where you want to scan from.
- 4. The Discovery Server scans 1 file per CPU core at a time. The more cores provided, the faster is scanning speed.

#### 2.5 Start the SharePoint Online Discovery

- 1. Sign in to the Central Console.
- 2. Go the DLP Setup > Discovery Targets > MS SharePoint tab.

Click the <b>Add</b> button.											
Dashboard     Security Events >	File Shares	🥲 Deploy 🕂 Add	Edit 🛅 Delete								
Image: second secon	MS Exchange     MS SharePoint	ID SCAN SERVER	SHAREPOINT ONLINE	💭 STATUS	<b>O</b> URATION						
Inspector ACL Rules Discovery Targets	Databases		No Discove	ery Scans are avail	able, add a n						
Endpoint Protector IRM Integration	Discover File Shares										
Policy Management Classification											
Detection Engines											

Enter the Scan Name, select the Discovery server, enter the SharePoint URL of the scanned site.
 Press the Add credential icon.

Enter Scan Name		$\left(\times\right)$
ିତ୍ସ MS SharePoint Scan	Scan For / Filters / Remedial Actions     Schedule     Report     Go Advanced	
Designated Scan Server	Select Discovery Server, or download/install a new one	-
Target SharePoint		
SharePoint Online		G
Credential or Cloud Account	Select Credential or create a new one	•
Base URL		₽Ø.
Exclude URL	0	
Incremental Scan		
Scan Images	GTB OCR      External OCR Server URL	
	🕞 Save	ancel



4. Enter service account email and password.

Edit Credential	$(\times)$
Display Name	SPO Scan
Domain\Username or Email address	spscan@gtbtech.onmicrosoft.com
Password	
	B Save Cancel

- 5. Check *SharePoint Online* checkbox.
- 6. Click the Save button.

Enter Scan Name		$\left(\times\right)$
Co MS SharePoint Scan	Scan For / Filters / Remedial Actions Schedule	
		_
Designated Scan Server	(i) Select Discovery Server, or download/install a new one	•
Target SharePoint		
SharePoint Online		Co
Credential or Cloud Account	Select Credential or create a new one	Ŧ
Base URL		ß
C Exclude URL	0	
Incremental Scan		
Scan Images	GTB OCR      External OCR Server URL	
	E Save	ancel

7. Press the *Start* icon to start the SharePoint discovery. The scan should start within a minute.

File Shares	🕼 Depl	oy 🕂 Add	Ce Edit	Delete	2		۲	•	Schedule	A	i
■ MS Exchange ■ MS SharePoint	a D	SCAN SERVER		SHAREPOINT ONLINE		💭 STATUS	TOTAL FILES	TOTAL SIZE, MB	TOTAL SCANNED, MB	REMEDIATIONS	MATC
Databases	0 1	GTBSERVERAM	MAZON 👻								
Cloud Platforms											
Discover File Shares											



#### 2.6 Check scan result

- 1. Sign in to the Central Console.
- 2. Go to the *Security Events > Discovery Scans* page and check the scan results. You should see a new running scan at this tab within few minutes.

(?) Dashboard	C. Local PC D	iscovery 🔀 File Shares	MS Outlook	MS Exchange	MS SharePoint	Databases	G File	Share Monitoring					
Security Events >	2	< < 1 of 1	> >> 🏹 Filters		Delete		Export Stat	istics 👻	Co Exp		*		
Network Inspector Discovery Scans	0	SCAN NAME	SCAN SERVER	START TIME 🔻	END TIME	TOTAL FILES	FILES SCANNED	SCAN SIZE, MB	SCANNED, MB	REMEDIATION	MATCHES	<b>O</b> DURATION	💭 STATUS
Endpoint Protector	310	SharePoint on-premise scan	LoL.gtbtechnologies.com.ua	Oct 02, 2020 01:02:41 PM	Oct 02, 2020 01:02:46 PM	1	1	0.03	0.03	None	1	1m	Completed, 100% done
Cloud Platform													
File Share Audit													
Classification													

3. Each line represents a separate Discovery scan. Double click to see the details.

🚫 GT Dat

#### 2.7 How to scan all SharePoint sites

- 1. Open PowerShell in administration mode.
- 2. Install the SharePoint Online Management Shell.

#### Install-Module -Name Microsoft.Online.SharePoint.PowerShell

- 3. Sign in to SP Online in PowerShell.
- 4. Set Administrator user email.

\$user = "user@contoso.com"

5. Add admin privileges to the service account for SP admin site

Set-SPOUser -Site https://companyname-admin.sharepoint.com/ -LoginName **\$user** - IsSiteCollectionAdmin \$true

2 Windows PowerShell	_		×
PS C:\Users\vstovpovoy> <mark>Set-SPOUser</mark> -Site https://gtbtech-admin.sharepoint.com/ -LoginName \$user -IsSiteCollectionAdr	iin \$t	rue	^
Display Name Login Name Groups User Type			
SharePoint Scan spscan@gtbtech.onmicrosoft.com {} Member			

- 6. Open the GTB Central Console and go the DLP Setup -> Discovery Targets -> MS SharePoint tab.
- 7. Click the Add button.

Dashboard     Security Events >	File Shares	🚱 Deploy 🕒 Add 🗋 Edit	Delete 💈	
Reports	MS Exchange	ID SCAN SERVER	SHAREPOINT ONLINE	
GTB DLP Setup >	Databases			
Discovery Targets Endpoint Protector	Cloud Platforms		No Discove	ry Scans are available, add a n
IRM Integration Policy Management	Discover File Shares			
Classification Detection Engines				
Network Status >				

- 8. Enter the *Scan Name*, select the *Discovery server*, enter the *SharePoint Admin URL* of the scanned site.
- 9. Enter created user credentials into the Username or Email address and password fields.
- 10. Check SharePoint Online checkbox.
- 11. Click the Save button.



Enter Scan Name		$(\times)$
ିତ୍ୱି MS SharePoint Scan	Scan For / Filters / Constructions Schedule	
Designated Scan Server	(i) Select Discovery Server, or download/install a new one	•
Target SharePoint		
SharePoint Online		G
Credential or Cloud Account	() Select Credential or create a new one	-
Co Base URL	0	ম্ব
C Exclude URL	0	
Incremental Scan	0	
Scan Images	(i)         GTB OCR         ▼         External OCR Server URL	
	🗎 Save	Cancel

12. Press the *Start* icon to start the SharePoint discovery. The scan should start within a minute.

File Shares	🕼 Depl	oy 🕂 Add 🎧	, Edit 🔒 Delete	2		۲	•	Schedule	A	i
MS Exchange	0 0	SCAN SERVER	SHAREPOINT ONLINE	💭 STATUS	<b>O</b> DURATION	TOTAL FILES	TOTAL SIZE, MB	TOTAL SCANNED, MB	REMEDIATIONS	матс
Databases	□ 1	GTBSERVERAMAZON	• •							-
Cloud Platforms										
Discover File Shares										

13. Go to the Security Events -> Discovery scans -> MS SharePoint tab and check for scan results.





#### 2.8 How to scan separate SharePoint files or folders

1. Open the SharePoint Online file or folder location that you'd like to scan.

	+ New $\sim$	$\bar{\uparrow}$ Upload $\vee$	Edit in grid view	🖻 Share	Copy link	G Sync		🕞 Add shor	tcut to (
	Documents	> GTB ShareP	oint Test						
	Ď	Name $\vee$		Мос	lified $\vee$	Modifie	d By $\smallsetminus$	Date $\checkmark$	
		<sup>≟'</sup> GTTB		Abou	t a minute ago	Ihor Yesh	chuk		
j	<b>W</b> È	<sup>≥</sup> ' Document.docx		A few	/ seconds ago	Ihor Yesh	chuk		
		Count 2							

2. Highlight the item, click the Show action icon, then Details.

Documents	S GTB SharePoint Te	est	Share		
			Copy link		
۵	Name 🗸		Manage access	lodified By $^{\smallsetminus}$	Date $\checkmark$
<b>e</b>	GTTB	ෂ් හි :	Download	or Yeshchuk	
M	<sup>'</sup> Document.docx		Add shortcut to OneDrive	or Yeshchuk	
	Count		 Delete		
i.	2		Automate >		
			Rename		
			Pin to top		
			Move to		
			Copy to		
			Alert me		
			More >		
			Details		



3. In the pane that appeared find and click the *Copy direct link icon*.

					🔲 GTT	гв ×
	Modified $\checkmark$	Modified By $\vee$	Date 🗠	+ Add cc	Activity	 More details
ę,	Monday at 3:12 AM	Ihor Yeshchuk			This week	
	Monday at 3:12 AM	Ihor Yeshchuk				You created GTTB in GTB SharePoint Test Monday at 3:12 AM
				Co	Type Folder Modified Monday Path C Path Size 152 byte	d at 3:12 AM Team Site > Documents > GTB S Test > GTTB s

- 4. Open the GTB Central Console and go the *DLP Setup -> Discovery Targets -> MS SharePoint* tab.
- 5. Click the **Add** button.

Dashboard     Security Events >	File Shares	🚱 Deploy 🕒 Add 🗋 Edit	Delete ;	2	
.1 Reports	∎⊠ MS Exchange	ID SCAN SERVER	SHAREPOINT	👰 STATUS	
GTB DLP Setup >	S MS SharePoint				
Inspector ACL Rules	Databases		No Discov	verv Scans are avail	able add a n
Endpoint Protector	Cloud Platforms				
IRM Integration	Discover File Shares				
Policy Management Classification					
Detection Engines					
Network Status >					

- 6. Enter the **Scan Name**, select the **Discovery server**, paste **the direct link of the scanned file** that was copied in the step 3.
- 7. Select existing credentials or add a new one.
- 8. Check SharePoint Online checkbox.
- 9. Click the **Save** button.



Enter Scan Name		$(\times$
Co MS SharePoint Scan	Scan For / Filters / Remedial Actions Chedule Content Report	
Designated Scan Server	Select Discovery Server, or download/install a new one	Ŧ
Target SharePoint		
SharePoint Online		G
Credential or Cloud Account	Select Credential or create a new one	•
Co Base URL		ß
Co Exclude URL	0	
Incremental Scan		
Scan Images	① GTB OCR	
	a Save	Cancel

10. Press the Start icon to start the SharePoint discovery. The scan should start within a minute.

File Shares	🧐 Depl	loy 🔶 Add	C Edit	Delete	2			€	•	Schedule	A	i
MS Exchange	0 10	SCAN SERVER		SHAREPOINT ONLINE		💭 STATUS	<b>O</b> DURATION	TOTAL FILES	TOTAL SIZE, MB	TOTAL SCANNED, MB	REMEDIATIONS	МАТС
Databases	0 1	GTBSERVERAN	MAZON 👻									
Cloud Platforms												
Discover File Shares												

11. Go to the Security Events -> Discovery scans -> MS SharePoint tab and check for scan results

( Deshboard	C. Local PC	Discovery 🔀 File Shares	MS Outlook	MS Exchange	MS SharePoint	Databases	G File	Share Monitoring								
Security Events >     All Events	2	4 1 of 1	> > K Filters	-	Delete 💡		Export Stat	stics 💌	Co Es					3	) 🗊	Ō
Network Inspector Discovery Scans	D 10	SCAN NAME	SCAN SERVER	START TIME 👻	END TIME	TOTAL FILES	FILES SCANNED	SCAN SIZE, MB	SCANNED, MB	REMEDIATION	MATCHES		💭 status			
Endpoint Protector	307	SharePoint Online Scan	LoL.gtbtechnologies.com.ua	Oct 02, 2020 11:49:37 AM	Oct 02, 2020 11:52:46 AM	M 138	138	87.39	87.39	None	37	3m	Completed, 100% done			
Cloud Platform File Share Audit Classification																



# 3 SharePoint with Modern Authentication

### 3.1 Create Application for Modern Authentication

- 1. Open URL https://COMPANYNAME.sharepoint.com/\_layouts/15/AppRegNew.aspx
- 2. Click on the Generate button next to Client Id.
- 3. Click on Generate button near Client Secret.
- 4. Note the given Client Id and Client Secret.
- 5. Type the name of the Application in the **Title** field. It could be SPOnline.
- 6. In the App Domain field, enter cloudauth.gttb.com.
- 7. In the Redirect URI field, enter https://cloudauth.gttb.com/callback.php.
- 8. Press Create button.

		Create Cancel
App Information The app's information, including app id, secret, title, hosting url and redirect url.	Client Id: 475:430b-0c6c-489f-9629-99da06ib2a41 Generate	
	Client Secret:	
	dqB8fHxpJ9XTc+ENfTY6iIz1mN4aHqTcP8j Generate	
	Title:	
	SPOscan	
	App Domain: doudauth.gtb.com Example: "www.contoso.com"	
	Redirect URI:	
	https://doudauth.gttb.com/callback.php Example: "https://www.contoso.com/default.aspx"	
		Create Cancel



### 3.2 Add Application credentials

- 1. Sign in to the Central Console.
- 2. Go to the **System > Cloud Accounts**.

GTB Central Console	TB minal Console  (								
<ul> <li>ᢙ Dashboard</li> <li>Output</li> <li>Output&lt;</li></ul>	Endpoint Agent	G Add	Cloud Account						
Reports	DNS		CLOUD PLATFORM	CLOUD ACCOUNT DISPLAY NAME					
GTB DLP Setup >	LDAP Integration	0 1	🏟 Amazon Web Services	\$3					
Network Status	Shadow Location	2	🏟 Amazon Web Services	s3 roort					
Co System >	Emails and Alerts	3	Amazon Web Services	se new root					
Endpoint Agent	SIEM Receiver	4	Amazon Web Services	S3DDDDD					
DNS	DNS Company Name		Microsoft Azure	Azure					
LDAP Integration	E Data and Time	6	<ul> <li>OneDrive</li> </ul>	OneDrive					
Empile and Alerte		7	🝐 Google Drive	google					
SIEM Receiver	Cloud Accounts	8	box Box	Box.com					
Company Name	Security >	9	😻 Dropbox	Dropbox					
Date and Time	SSL Certificates	0 10	ConeDrive	OneD					
Cloud Accounts	0	11	OneDrive for Business	RRogoziansky@gtbtech.onmicrosoft.com					
Security	CC Synchronization	12	CneDrive	one					
SSL Certificates	E Compliance Regulations	13	OneDrive for Business	RRR					
CC Synchronization	Incidents Response	14	Sharepoint	SPO [QA]					
Incidents Response		□ 15	OneDrive for Business	OneFB					

3. Press Add Cloud Account button.

Add Cloud Account				$(\times)$
Enter Display Name (i)	SPO Scan			
How to scan	box	Coogle Drive	ShareFile	ConeDrive for Business
ConeDrive	Microsoft Azure	Amazon S3	SharePoint How to scan	

- 4. Type the **Display Name**.
- 5. Press Add button on the SharePoint card.
- 6. You should see a pop-up as shown below.



Login to account	×
	SharePoint
Enter Account Name	SPO Scan
Enter Site Name	https://gtbtech-admin.sharepoint.com
2FA Client ID	de7a2e0e-0e53-4925-96ae-6113d1266b3b
2FA Client Secret	9J00+6Xgy/tDdtPNcomyDJz0dRhYFIVeGUHi:
How to scan	a Add

- 7. Enter Account Name.
- 8. Enter SharePoint Site Name in the form of https://companyname-admin.sharepoint.com/.
- 9. Enter saved 2FA Client ID and 2FA Client Secret tokens from the previous item.
- 10. Press Add button.
- 11. You should be redirected to the Microsoft site. Sign in to the site as a user with a Site Admin role.

Take a look at item 2.3 to figure out how to assign Site Admin role to the user.



12. In the pop-up window, press Trust It button.





#### 3.3 Install Discovery Server

- 13. Sign in to the Central Console using an account with Administrator privileges.
- Go to the Help > Download tab of the GTB Central Console and download the GTB Discovery Server MSI package.

	GTB Central Console		🍖 🗟 ⊑∏ Download	a 🗟 🔄 Downloads » Windows Endpoint Agents							
$\bigcirc$	Dashboard		-								
:0:	Security Events		📕 Windows Endpoint Agents		GTB Endpoint Agent + Networking	165 MB					
10	Security Events	<i>´</i>	a macOS Endpoint Agents	-	Endpoint device controls with Discovery + Network Traffic Inspection						
.1	Reports			_		v15.7.8-54972					
$\overline{\mathbf{v}}$	GTB DLP Setup	>	🛕 Linux Endpoint Agents								
	Network Status	>	Name Resolution Helper		GTB Discovery Server	165 MB					
Ç <mark>o</mark>	System	>	Security Manager	$\overline{\mathbf{+}}$	Discovery Server description	v15 7 9 54072					
8	User Management		Administrative Tools			¥13.7.0 <sup>-</sup> 34972					
×	Maintenance	>	Local links for browsers		Antivirus exception list for Windows OS						
Ē	Logs	>		=	Antivirus exception list for Windows OS						
?	Help/Downloads	>									
I	Documentation										
	Downloads		-								

- 15. Install the *GTB Discovery Server* on any Windows PC where you want to scan from.
- 16. The Discovery Server scans 1 file per CPU core at a time. The more cores provided, the faster is scanning speed.



#### 3.4 Start the SharePoint Online Discovery

- 1. Sign in to the Central Console.
- 2. Go the DLP Setup > Discovery Targets > MS SharePoint tab.
- 3. Click the Add button.

Dashboard     Security Events >	File Shares	Deploy	🛍 Delete 🥏	
Reports	■ MS Exchange	ID SCAN SERVER	SHAREPOINT	💭 STATUS 🐧 DURATION
GTB DLP Setup >	MS SharePoint			
Inspector ACL Rules	Databases			v Soona ara availabla, add a n
Discovery Targets	Cloud Platforms		NO DISCOVEI	y Scalls ale avaliable, aut a li
Did Interneties				
Policy Management	Discover File Shares			
Classification				
Detection Engines				
Network Status >				

- 4. Enter the Scan Name, select the Discovery server, enter the SharePoint URL of the scanned site. You can specify several URLs to scan. If you want to scan all sites from your SPO specify admin site URL: https://companyname-admin.sharepoint.com.
- 5. Check SharePoint Online checkbox.
- 6. In the Credential or Cloud Account select the Credential or Cloud Account.
- 7. Enter the SharePoint URL of the scanned site

Enter Scan Name		$\propto$
Co MS SharePoint Scan	Scan For / Filters / Remedial Actions Chedule	
Designated Scan Server	Select Discovery Server, or download/install a new one	-
Target SharePoint		
SharePoint Online		Cò
Credential or Cloud Account	Select Credential or create a new one	-
Co Base URL		ß
Co Exclude URL	0	
Incremental Scan	0	
Scan Images	GTB OCR      External OCR Server URL	
	E Save Ca	ancel



- 8. Click the **Save** button.
- 9. Press the *Start* icon to start the SharePoint discovery. The scan should start within a minute.

<b>1</b>	Deploy (	🕂 Add	C Edit	🗎 Delete	\$					[	•	C Schedu	ile 🔒
•	SCAN NAME	E		DESIGNATED SC	AN SERVER	SHAREPOINT ONLINE	💭 STATUS		TOTAL SIZE, MB	FILES SCANNED	SCANNED, MB	REMEDIATIONS	MATCHES
0 1	SPO Scan			GTB_SC.	ANSERVER		-	-	-	-	-	-	-

#### 3.5 Check scan result

- 1. Sign in to the Central Console.
- 2. Go to the *Security Events > Discovery Scans* page and check the scan results. You should see a new running scan at this tab within few minutes.

Dashboard	Local PC D	iscovery 💦 File Shares	MS Outlook	MS Exchange	MS SharePoint	Databases	G File	Share Monitoring					
Security Events >													
All Events	2	C 1 of 1	> > 75 Filters	Υ.	Delete		Export Stat	istics 👻	Co Exp				
Network Inspector													0
Discovery Scans		SCAN NAME	SCAN SERVER	START TIME	END TIME	TOTAL FILES	FILES SCANNED	SCAN SIZE, MB	SCANNED, MB	REMEDIATION	MATCHES	() DURATION	( STATUS
Endpoint Protector	307	SharePoint Online Scan	LoL.gtbtechnologies.com.ua Oct 02, 2020 11:49:37 AM		Oct 02, 2020 11:52:46 AM	138	138	87.39	87.39	None	37	3m	Completed, 100% done
Cloud Platform													
File Share Audit													
Classification													
Reports													

3. Each line represents a separate Discovery scan. Double click to see the details.

If you have any questions, please, email *support@gttb.com* and any of our engineers would be happy to help you.

