

# Forcepoint

## Forcepoint Data Visibility

Powered by GetVisibility

Sharepoint Scan Setup

**Forcepoint**

Report

# Table of Contents

**SHAREPOINT SCAN SETUP.....2**  
    SHAREPOINT ONLINE WIZARD: .....2  
    SHAREPOINT ON-PREMISES WIZARD..... 12

# Sharepoint Scan Setup

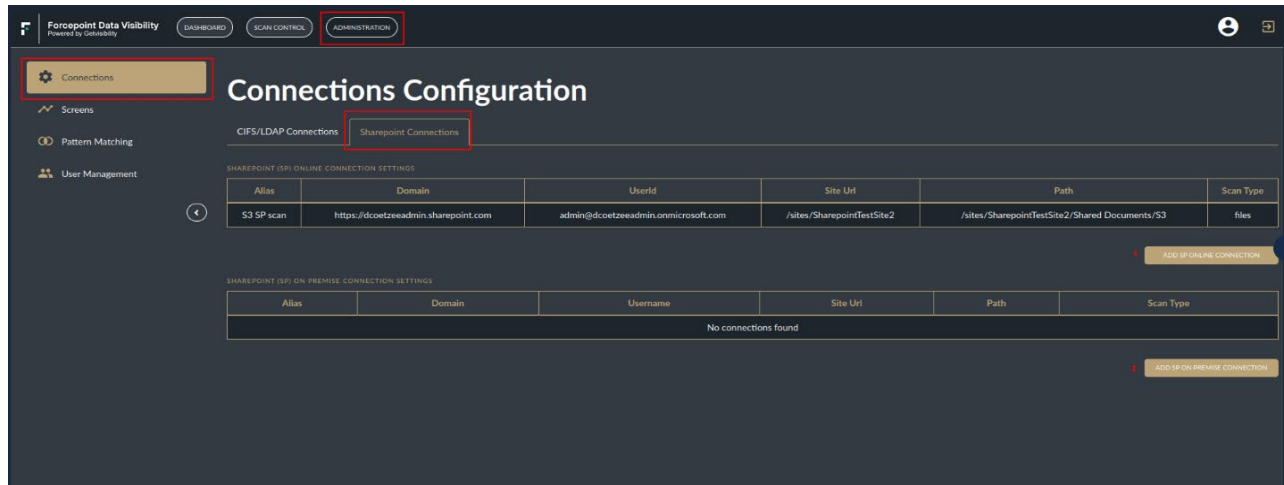


Figure 1: Connection Configuration page

Navigate to **Administration > Connections > Sharepoint Connections**.

1. Sharepoint Online Connection Wizard.
2. Sharepoint On-Premises Connection Wizard.

### Sharepoint Online Wizard:

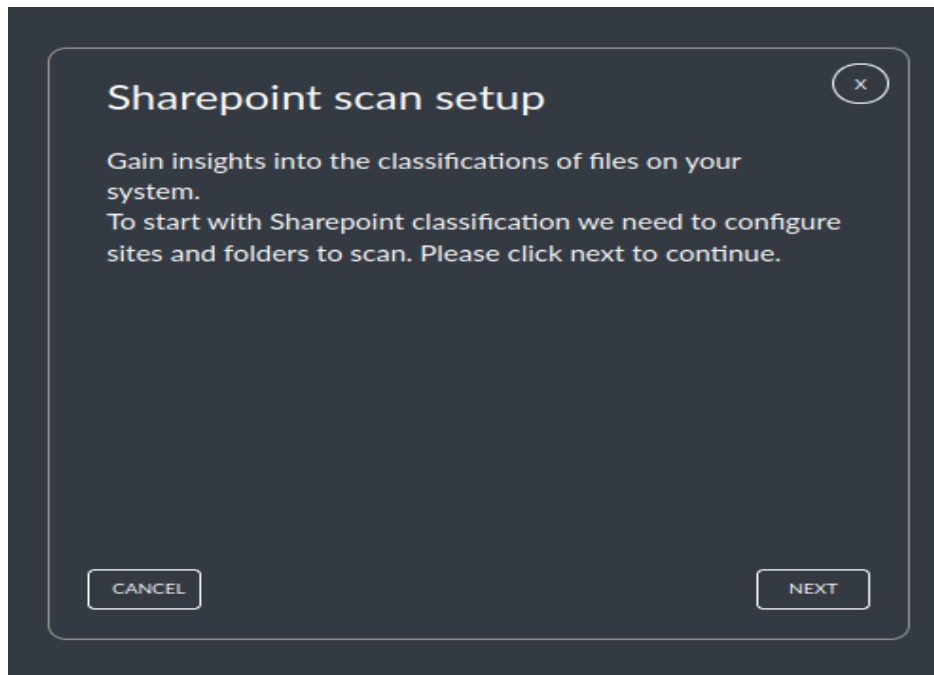


Figure 2: Sharepoint scan setup

3. Select **Next**.

**Step 1 of 4**

### Connection Details X

<b>Domain or FQDN:</b>	<b>1</b>	http://domain.sharepoint.com
<b>Site URL:</b>	<b>2</b>	sites/site
<b>Username:</b>	<b>3</b>	test@domain.sharepoint.com
<i>If you have Application Client ID and Client Secret, please enter below. Otherwise, we will guide you through the process of generating them.</i>		
<b>Application (client) ID:</b>	<b>4</b>	Optional
<b>Client Secret Value:</b>	<b>5</b>	Optional

PREVIOUSNEXT

Figure 3: Connection Details pane

1. The Sharepoint Domain address.
2. The Sharepoint Site URL.
3. A Sharepoint username that has access to the files you wish to scan.
4. Directory ID is used to identify the root folder
5. Application ID is used to link the connectors.
6. Client Secret Value is used to verify the connector.
7. Enter the details that are available. If a connection has not been previously setup, details 4 and 5 will be generated.
8. Select **Next**.

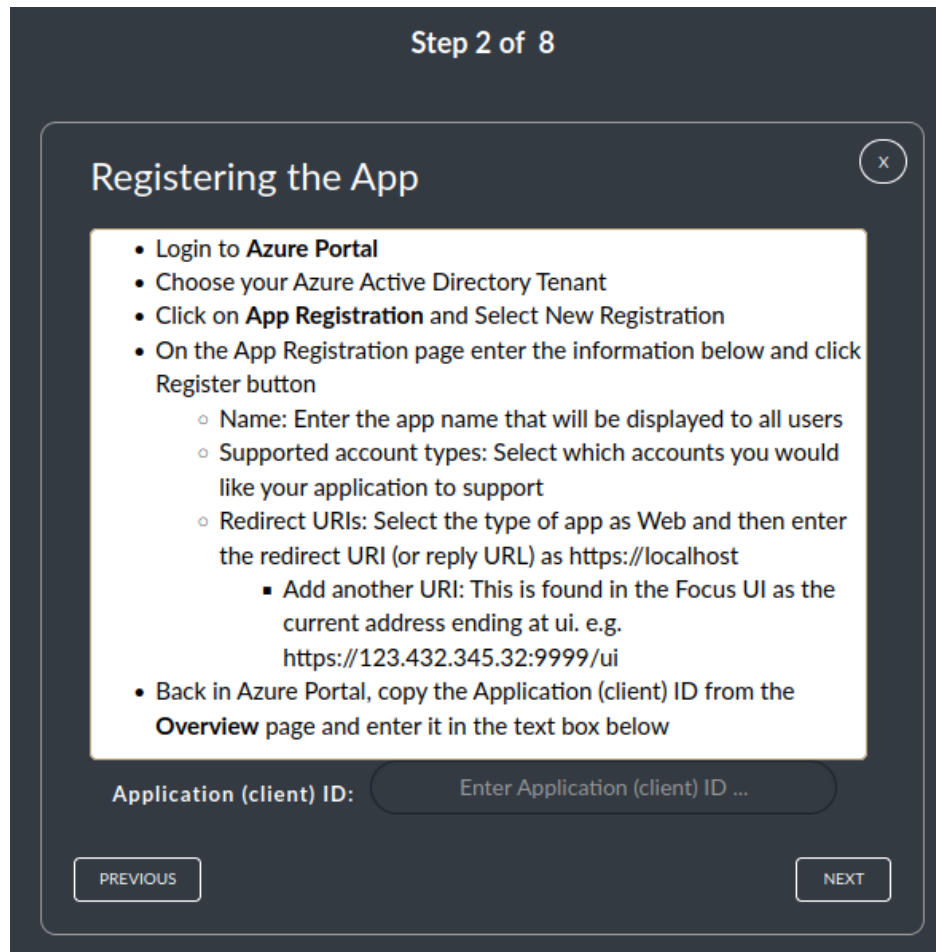


Figure 4: Registering the App

9. Follow the instructions to register the connector and copy the Directory (tenant) and Application (client) IDs.

### 10. Application (client) ID:

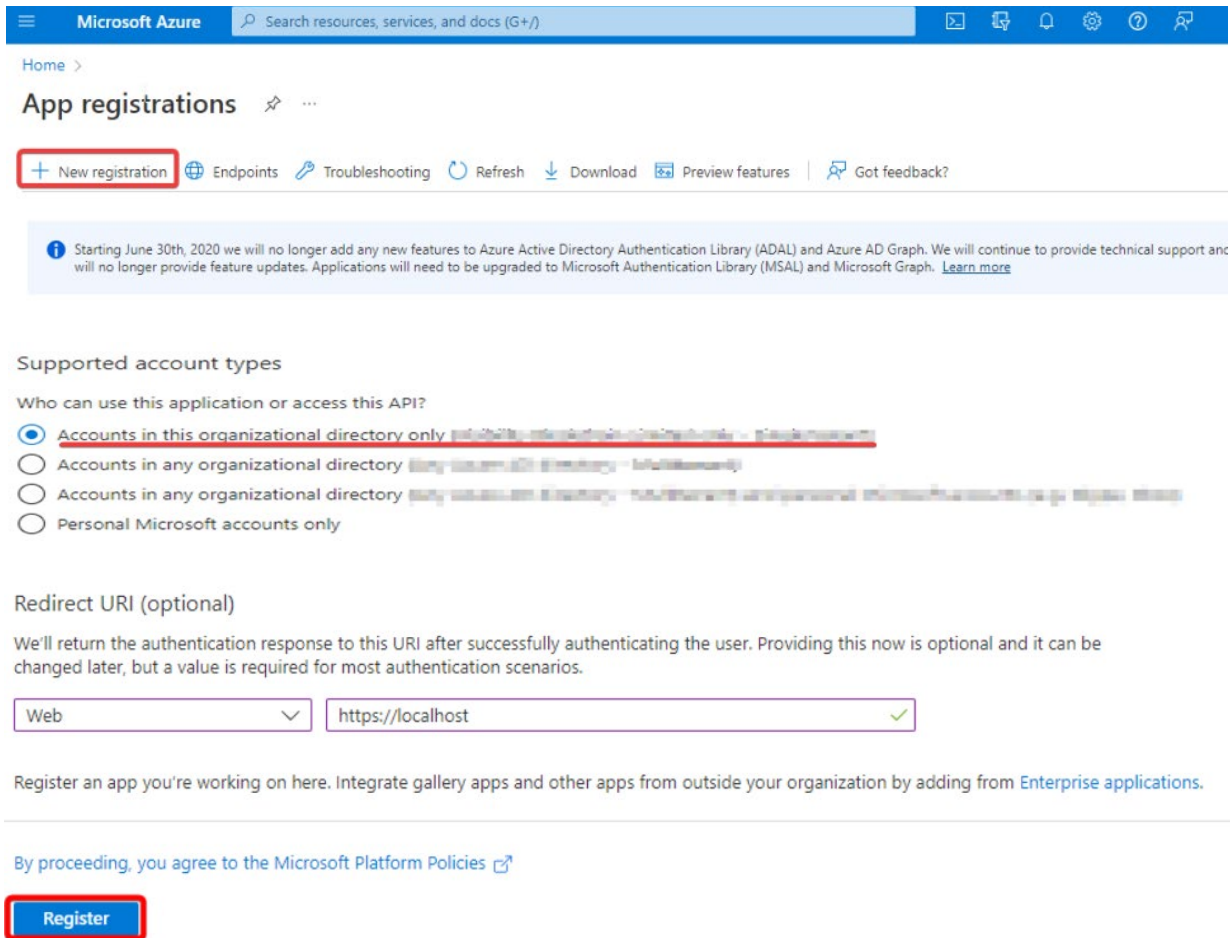


Figure 5: Application ID

### 11. Directory (tenant) ID:

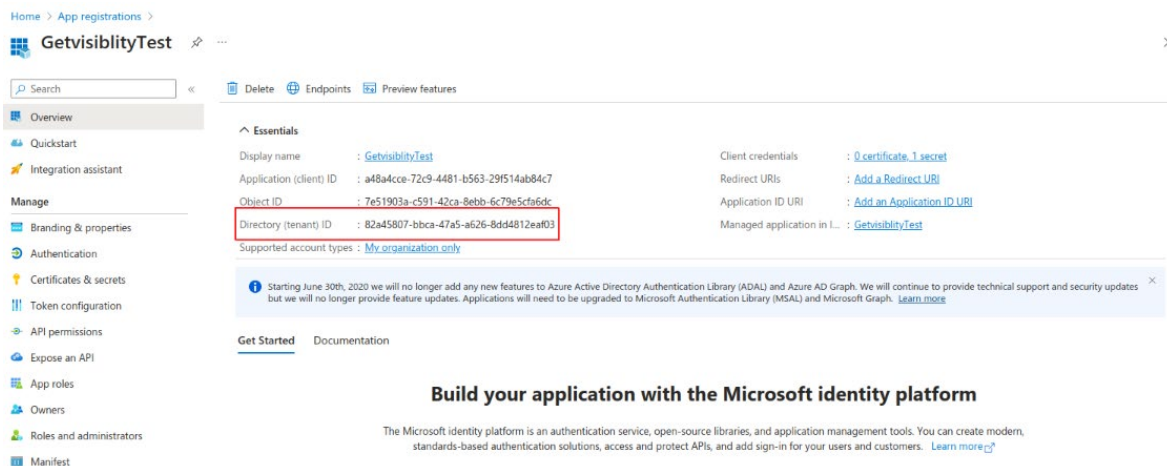


Figure 6: Directory ID

12. Client Secret Value:

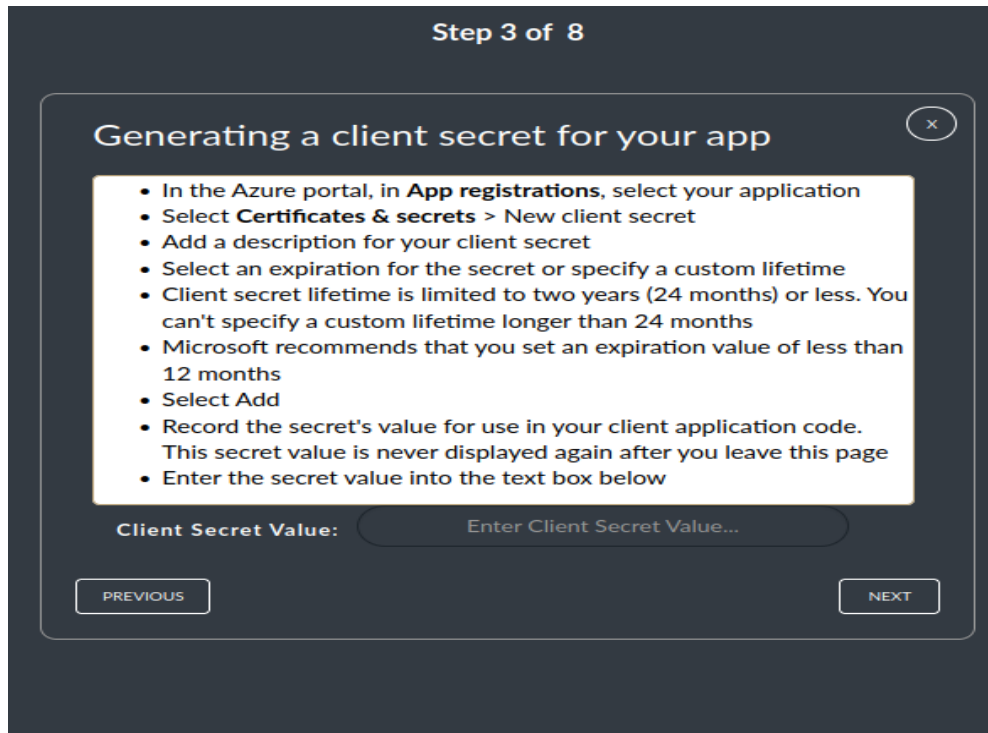


Figure 7: Generating a client secret for your app

13. Follow the instructions:

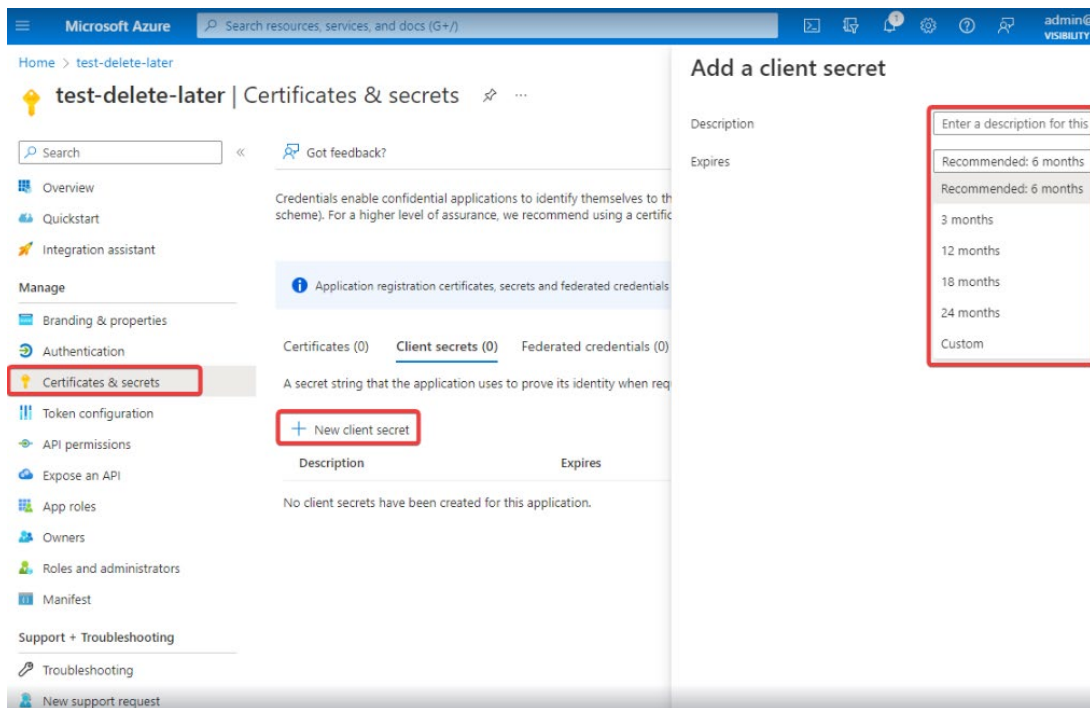


Figure 8: Add a client secret

14. Authenticate Connector:

Users can choose to optionally include sites.manage.all permission here for the tagging functionality.

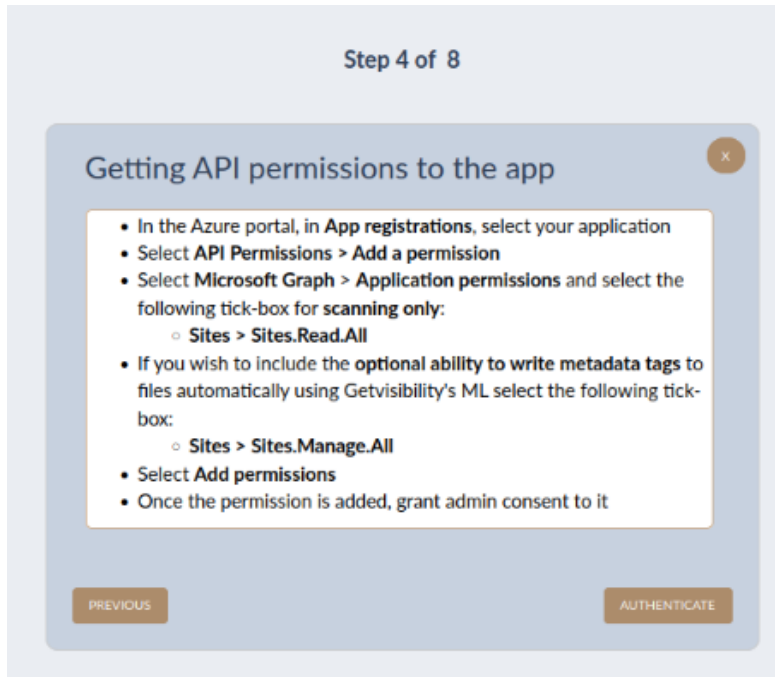
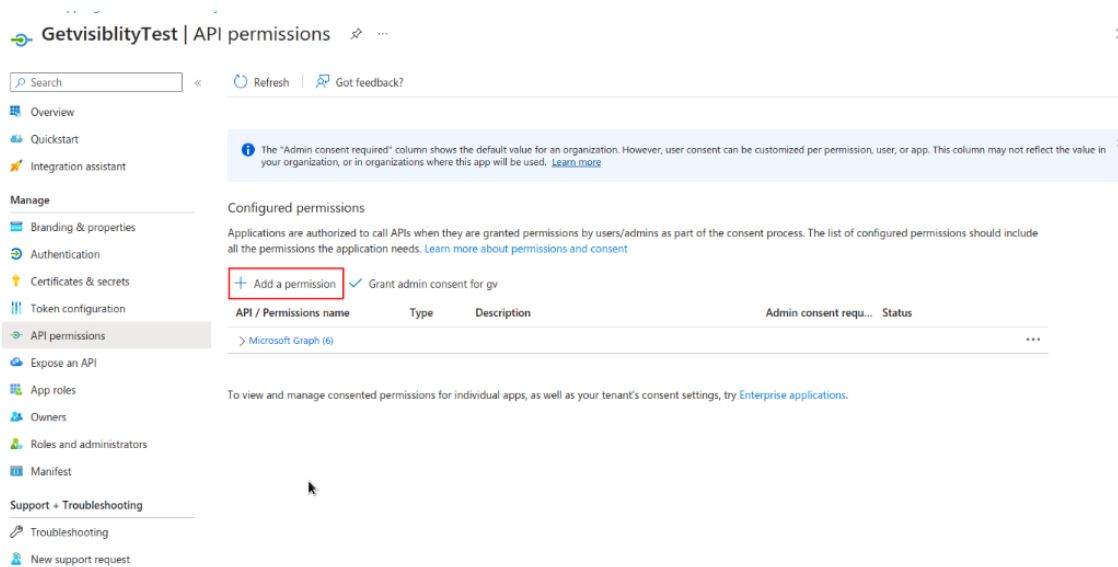


Figure 9: Getting API permission to the app

15. Follow the instructions:






## Request API permissions




Select an API

Microsoft APIs   APIs my organization uses   My APIs


Commonly used Microsoft APIs

**Microsoft Graph**


Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

**Azure Rights Management Services**


Allow validated users to read and write protected content

**Azure Service Management**


Programmatic access to much of the functionality available through the Azure portal

**Dynamics 365 Business Central**


Programmatic access to data and functionality in Dynamics 365 Business Central

**Dynamics CRM**

Access the capabilities of CRM business software and ERP systems

**Intune**

Programmatic access to Intune data

**Office 365 Management APIs**

Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity logs

## Request API permissions



[All APIs](#)

 **Microsoft Graph**  
<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

**Delegated permissions**  
Your application needs to access the API as the signed-in user.

**Application permissions**  
Your application runs as a background service or daemon without a signed-in user.

### Request API permissions

Microsoft Graph  
<https://graph.microsoft.com/> Docs

What type of permissions does your application require?

Delegated permissions  
Your application needs to access the API as the signed-in user.

Application permissions  
Your application runs as a background service or daemon without a signed-in user.

Select permissions expand all

sites

Permission	Admin consent required
Sites (2)	
<input type="checkbox"/> Sites.FullControl.All Have full control of all site collections	Yes
<input checked="" type="checkbox"/> Sites.Manage.All Create, edit, and delete items and lists in all site collections	Yes
<input checked="" type="checkbox"/> Sites.Read.All Read items in all site collections	Yes
<input type="checkbox"/> Sites.ReadWrite.All Read and write items in all site collections	Yes
<input type="checkbox"/> Sites.Selected Access selected site collections	Yes

Figure 10: Request API permissions

16. The details will be populated in the UI:

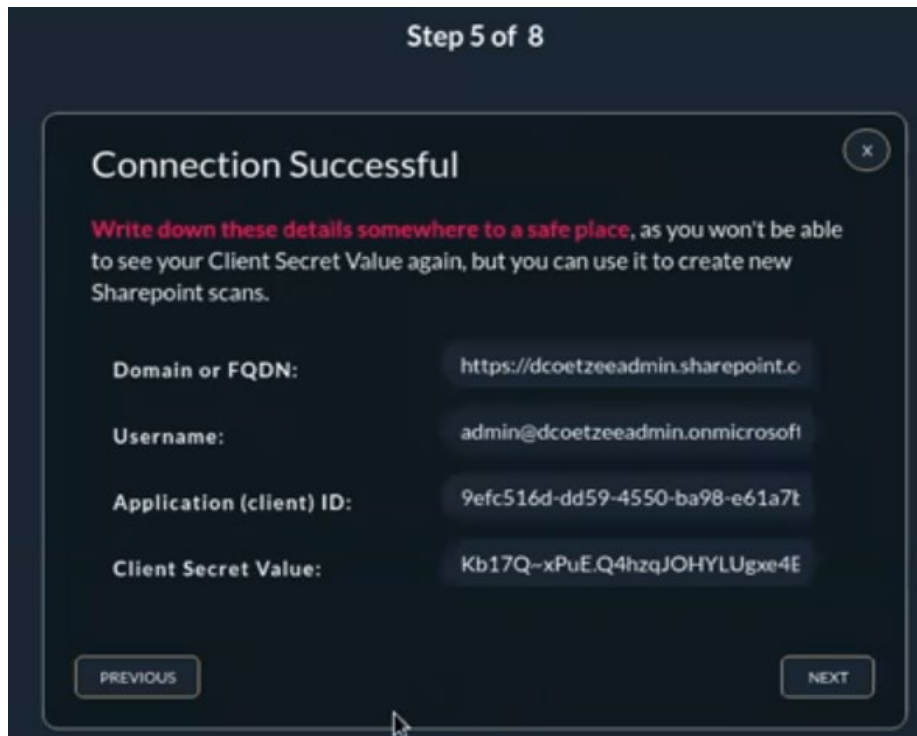


Figure 11: Connection Successful

17. Select the folder to scan:

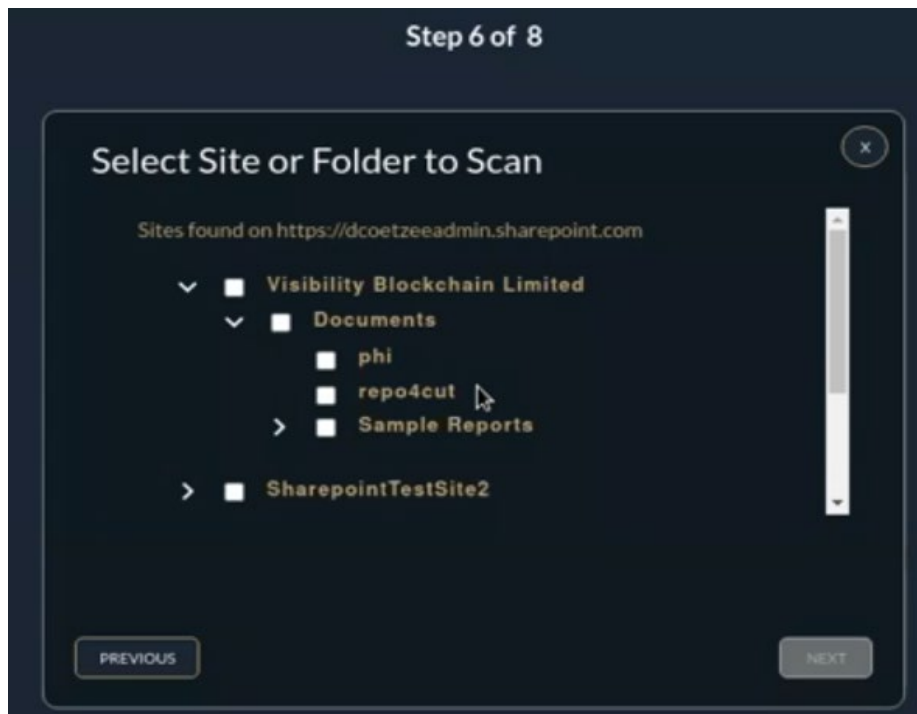


Figure 12: Select site or Folder to Scan

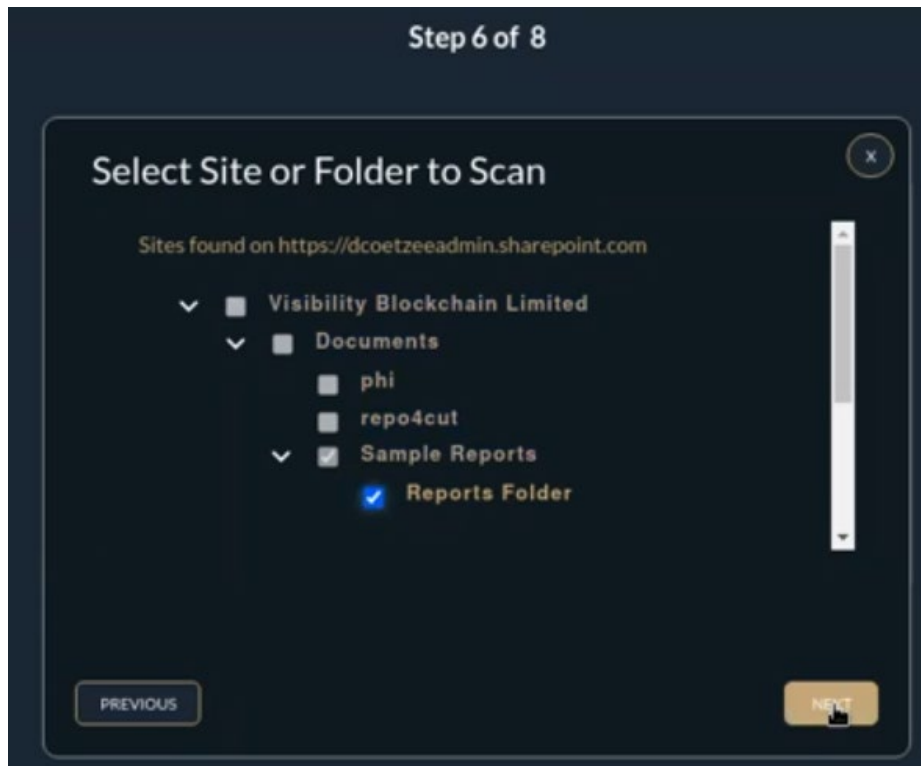


Figure 13: Select site or Folder to Scan

18. Give the connection a name to identify it later:

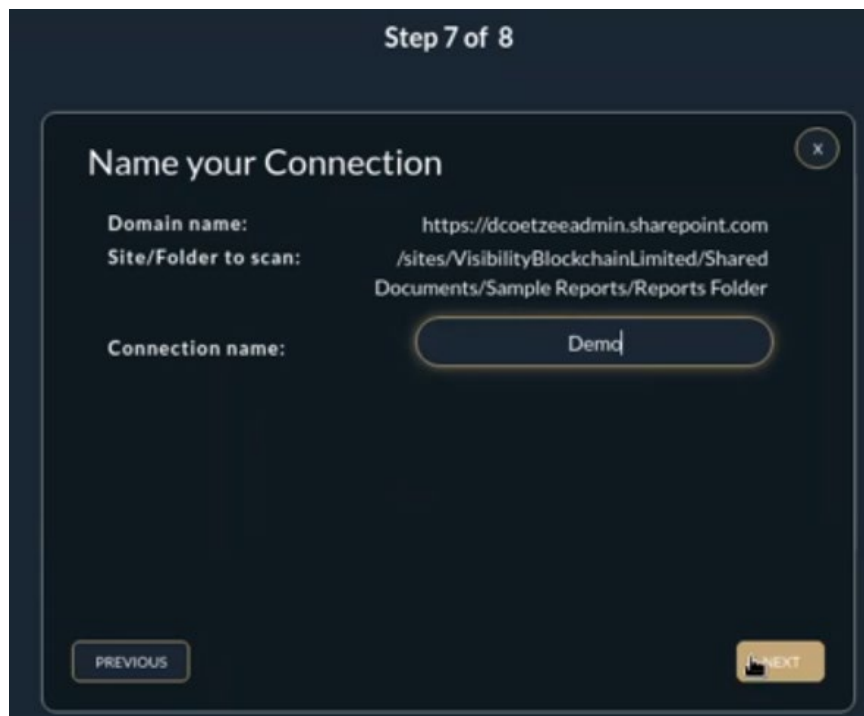


Figure 14: Name your Connection

19. The scan can be saved for later or saved and kicked off immediately.

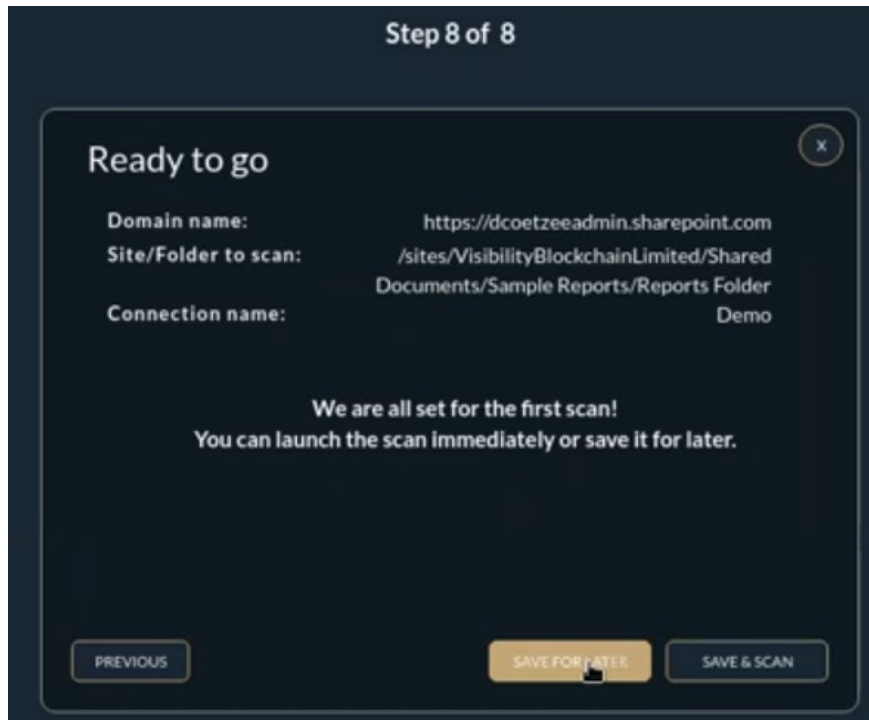


Figure 15: Ready to go

20. The scan is now stored and ready.

### Sharepoint On-Premises Wizard

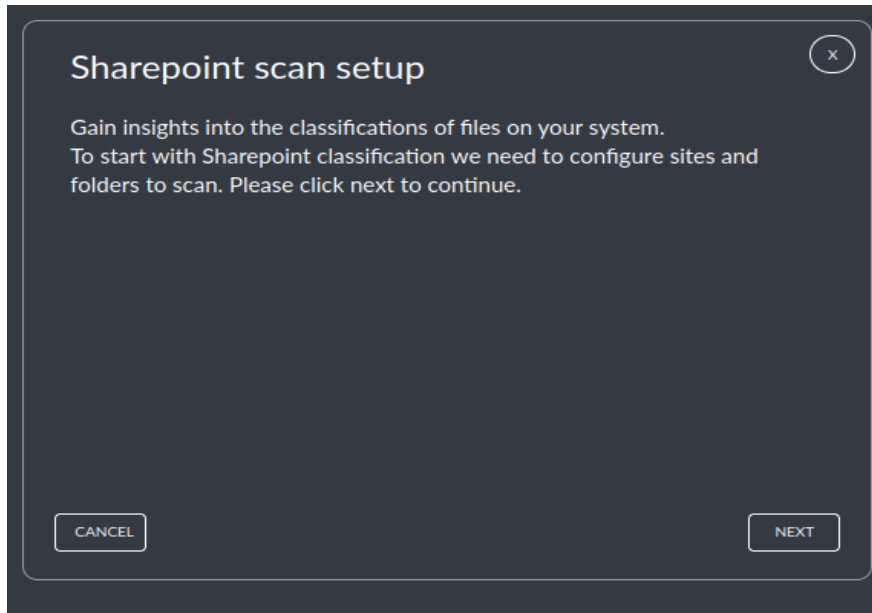


Figure 16: Sharepoint scan setup

21. Select **Next**.

22. Enter credentials:

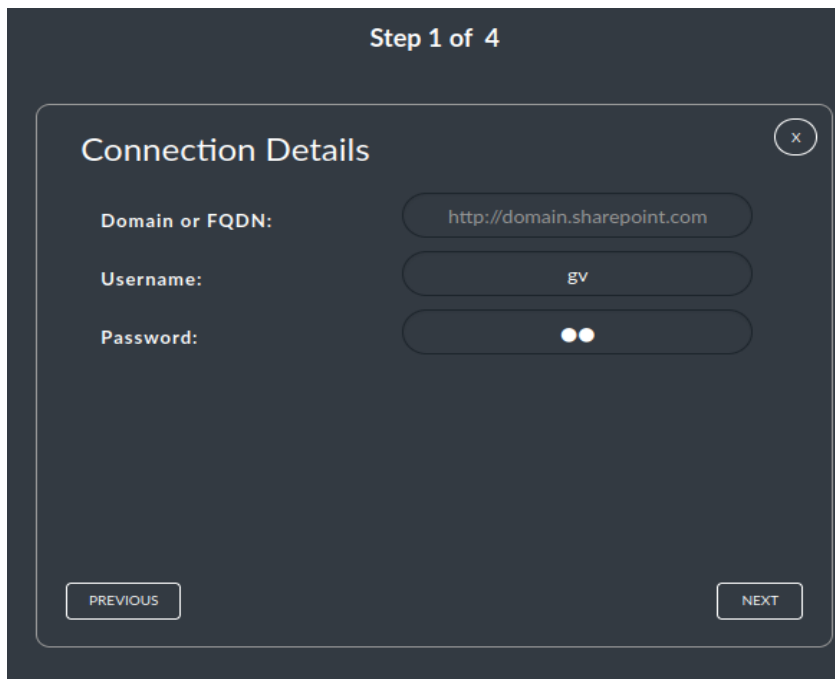


Figure 17: Connection Details

23. Select **Next**.

24. A folder tree of the Sharepoint site is now visible:

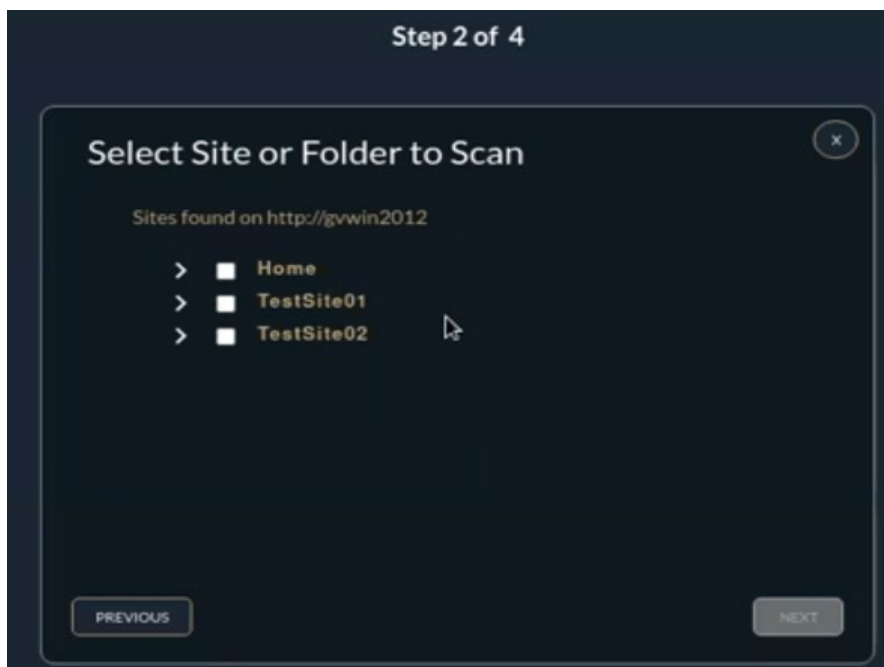


Figure 18: Select Site for Folder to Scan

25. Select folder to scan:

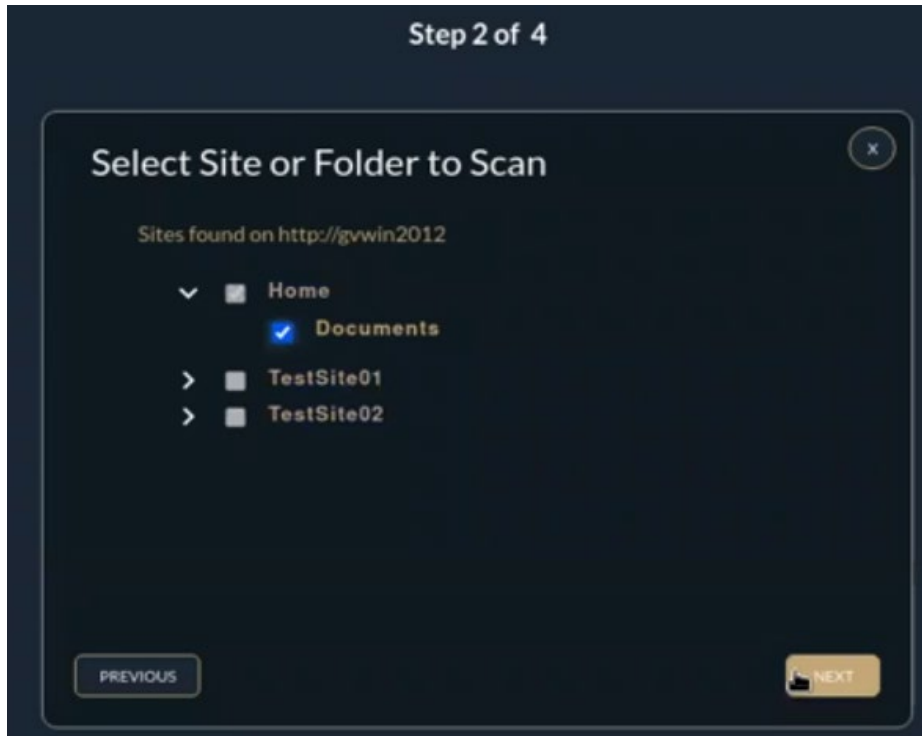


Figure 19: Select Site for Folder to Scan

26. Name the scan to identify it later:

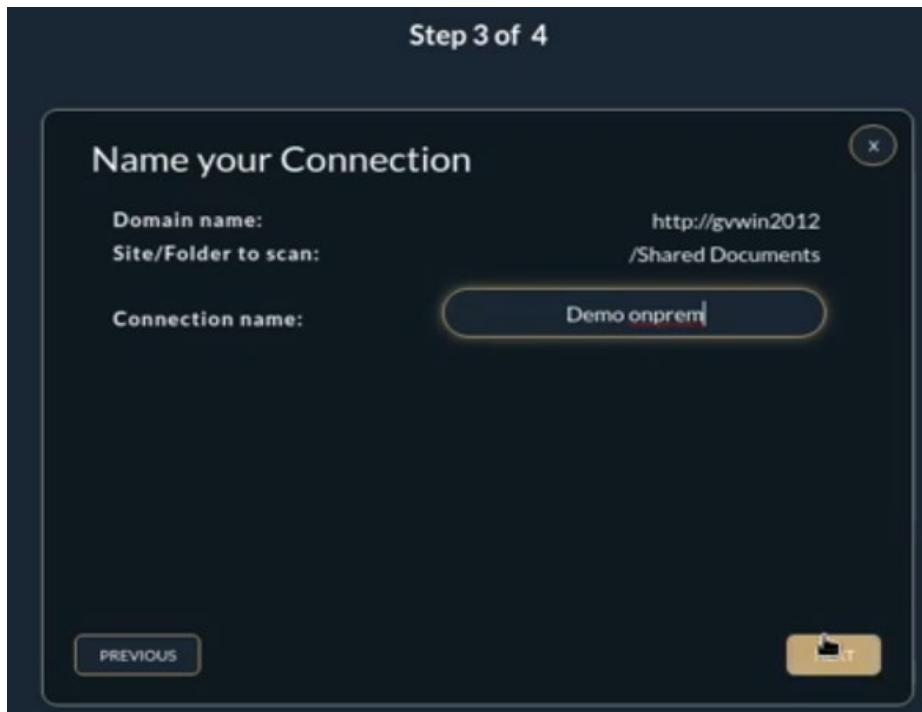


Figure 20: Name your Connection

27. The scan can be saved for later or saved and kicked off immediately:

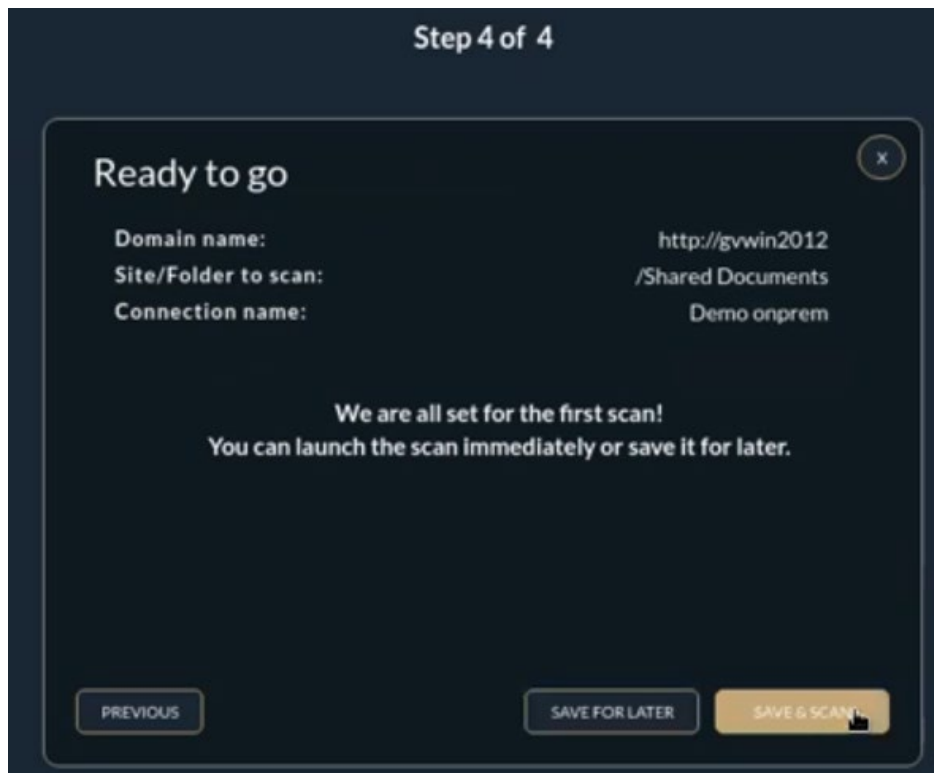


Figure 21: Ready to go





[forcepoint.com/contact](https://forcepoint.com/contact)

## About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly-attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.