Configure Cloud Applications To Use with API-Based Data Protection

For supported software information, click here.

Versa API-based data protection (API-DP) secures SaaS and IaaS applications using APIs provided by cloud services. To use API-based data protection, you register with the SaaS and IaaS applications and then use OAuth 2.0 to obtain access to the information. Real-time objects and objects at rest are scanned, and policy-based control is enforced. Real-time information relating to the various objects is sent as events (such as file upload and user login activity) to Versa services running in the cloud. Data associated with different objects is scanned, analyzed, and categorized by processing the object data through various types of security policy, including data loss prevention (DLP), cloud access security broker (CASB), and malware sandboxing. Scheduled jobs can scan objects periodically. Vulnerable data can be redacted, encrypted, quarantined, and deleted.

To use API-based data protection, you create an API data protection policy to identify any policy violations, and then you configure an API connection and instance for a supported cloud application. You can use Versa API-based data protection with the following SaaS and IaaS cloud applications. This article describes how to configure these cloud applications so that you can use them with Versa API-based data protection.

Application Type	Data at Rest	Event-Based	Shared Links
SaaS Applications			
Asana	Workspaces, projects, milestones, tasks, subtasks, comments, messages, attachments	Yes	Yes	NA
Box	Files, folders	Yes	Yes	Yes
Cisco Webex Teams	Files, messages	No	Yes	NA
Citrix ShareFile	Files, folders	Yes	Yes	Yes
Confluence	Pages, blogs, comments, attachments	Yes	Yes	NA
Dropbox	Files, folders	Yes	Yes	Yes
Egnyte	Files, folders	Yes	Yes	Yes

Application Type	Data at Rest	Event-Based	Shared Links
Bitbucket	Repository, branch, files	Yes	NA
Bitbucket	Project, branch, files	Yes	NA
Gmail	Email content, attachments	Yes	NA
Google Drive	Files, folders	Yes	Yes
Jira	Projects, issues, issue descriptions, comments, attachments	Yes	NA
Microsoft OneDrive	Files, folders	Yes	Yes
Microsoft Outlook	Email content, attachments	Yes	NA
Microsoft SharePoint	Files, folders	Yes	Yes
Microsoft Teams	Messages in channel and direct messaging, attachments handled by Microsoft SharePoint	Yes	NA
Microsoft Yammer	Networks, communities, storylines, posts, comments, replies	Yes	NA
Notion	Pages, database, bookmark, bulleted list item, callout, code, equation, file, headings, image, numbered list item, paragraph, PDF, quote, toggle blocks	Yes	NA
Salesforce	Salesforce files, libraries, account attachments, contact attachments, chatter attachments (posts and comments)	Yes	NA
ServiceNow	Service Now and attachments	Yes	NA
Slack	Workspace, channels, messages, files	Yes	NA
Trello	Workspaces, boards, lists, cards, comments, attachments	Yes	NA

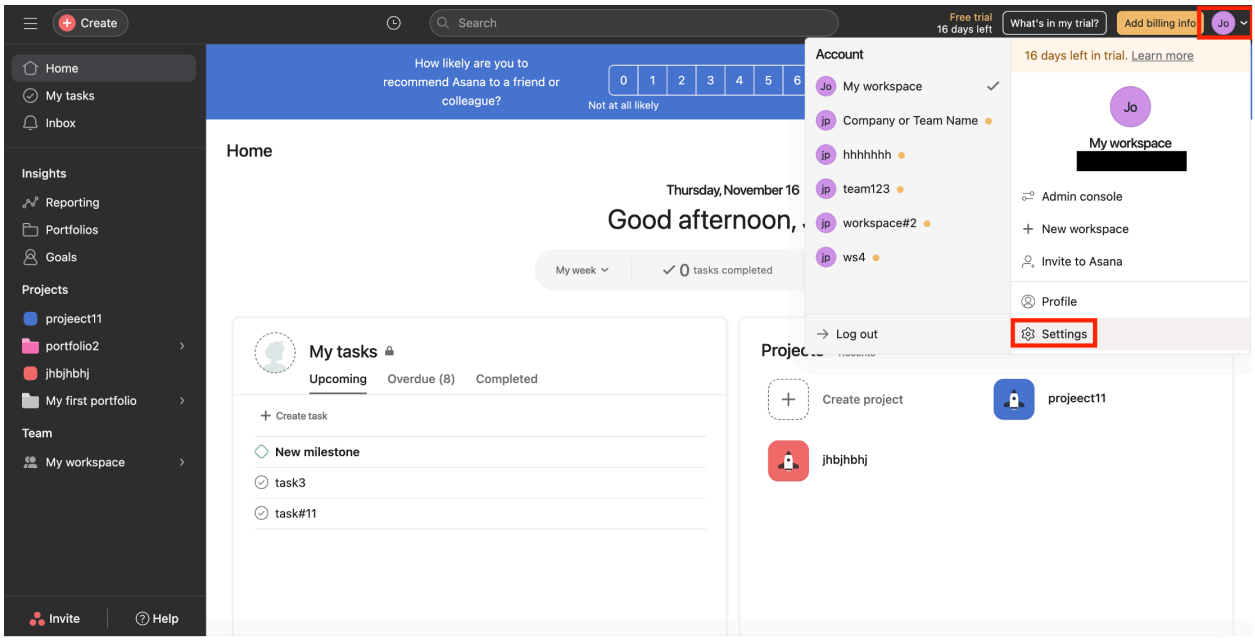
Application Type	Data at Rest	Event-Based	Shared Links
Workplace from Meta	Groups, posts, chat, files, events, knowledge library, notes, comments	Yes	NA
Zendesk	Content, attachment	Yes	NA
Zoom	Messages and transcript	No	NA
IaaS Applications			
Amazon Web Services	S3 buckets, files, folders	Yes	No
Google Cloud Platform	Buckets, files, folders	Yes	No
Microsoft Azure	Storage accounts, containers, files	Yes	Yes
Oracle Cloud Infrastructure	Regions, compartments, buckets, objects	Yes	NA

Asana API-Based Data Protection

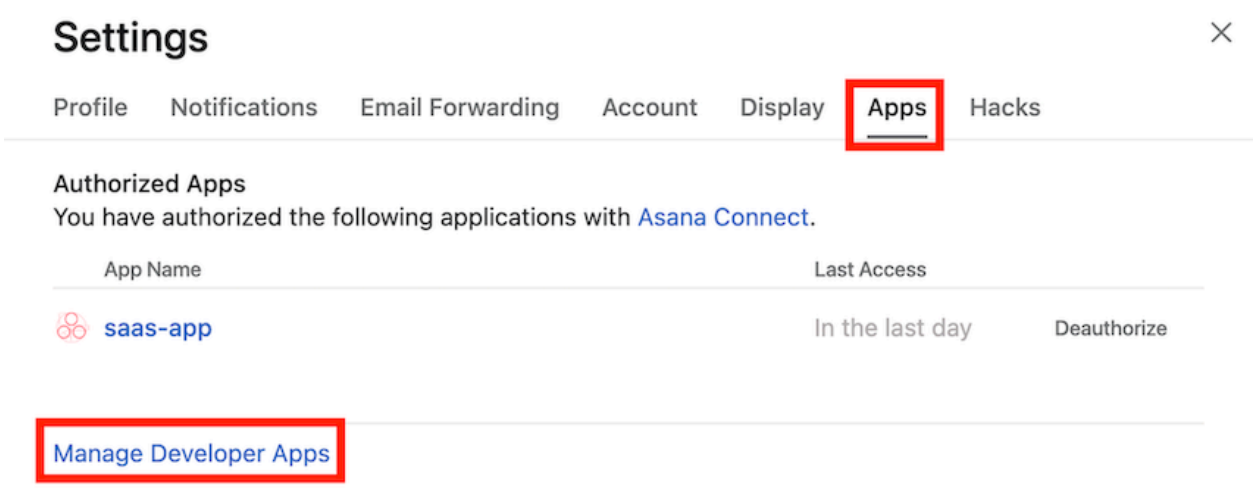
This section describes how to configure the Asana Application for API-based data protection.

Create the Asana Application for API-Based Data Protection

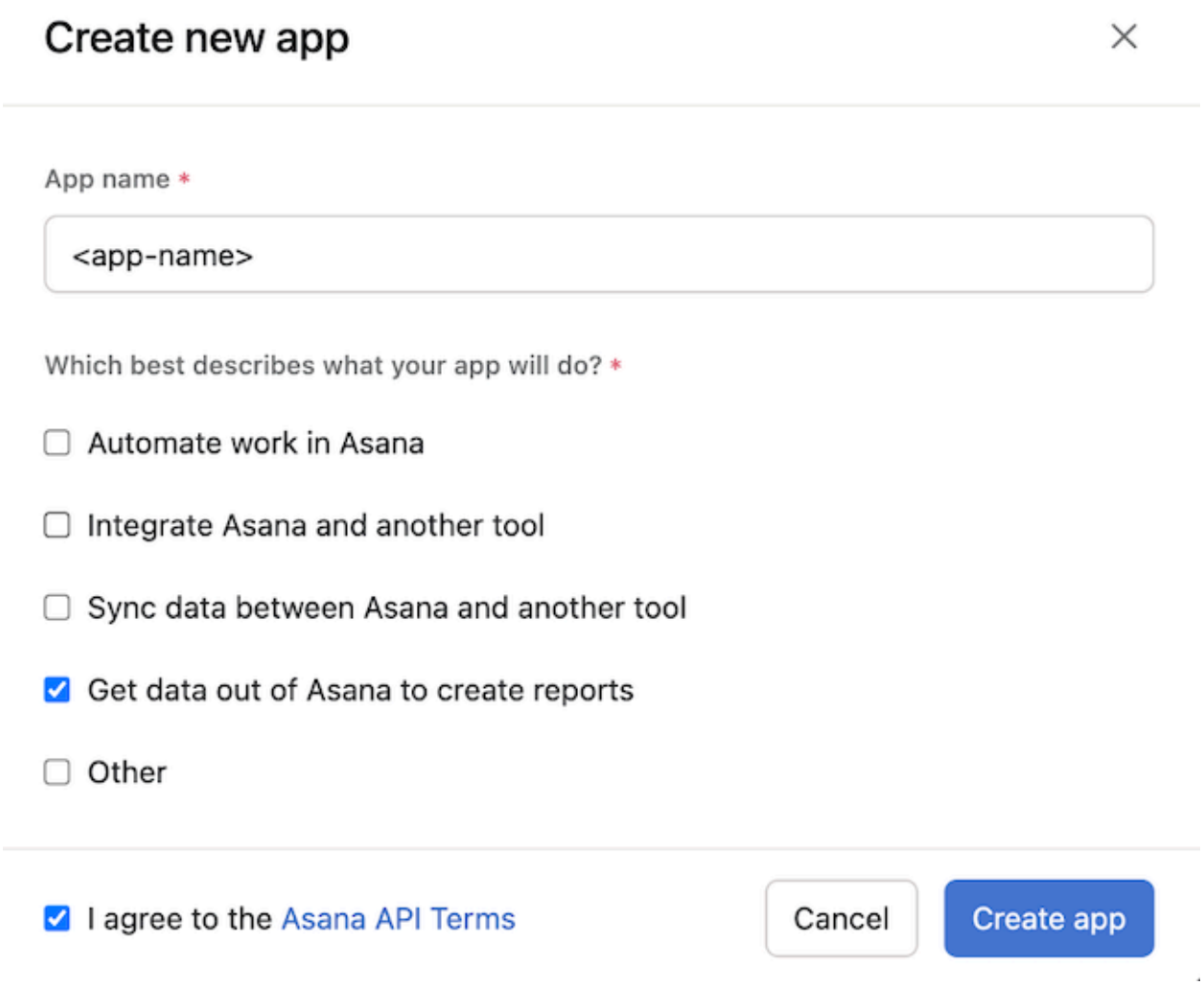
1. Log in with admin credentials at https://app.asana.com/-/login. Go to the dropdown menu on the top right corner and then click on “Settings”.



2. Click “Apps” at the top bar of the settings window then click;“Manage Developer Apps”.



3. Click Create New App in the new window. Enter the name, check the use cases, and agree to the terms and conditions.

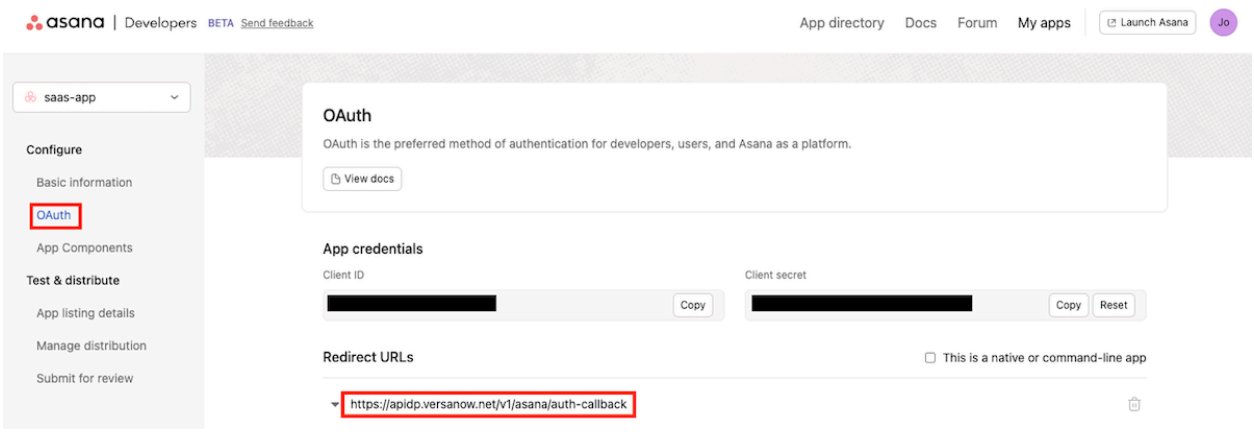


4. Click Create App.

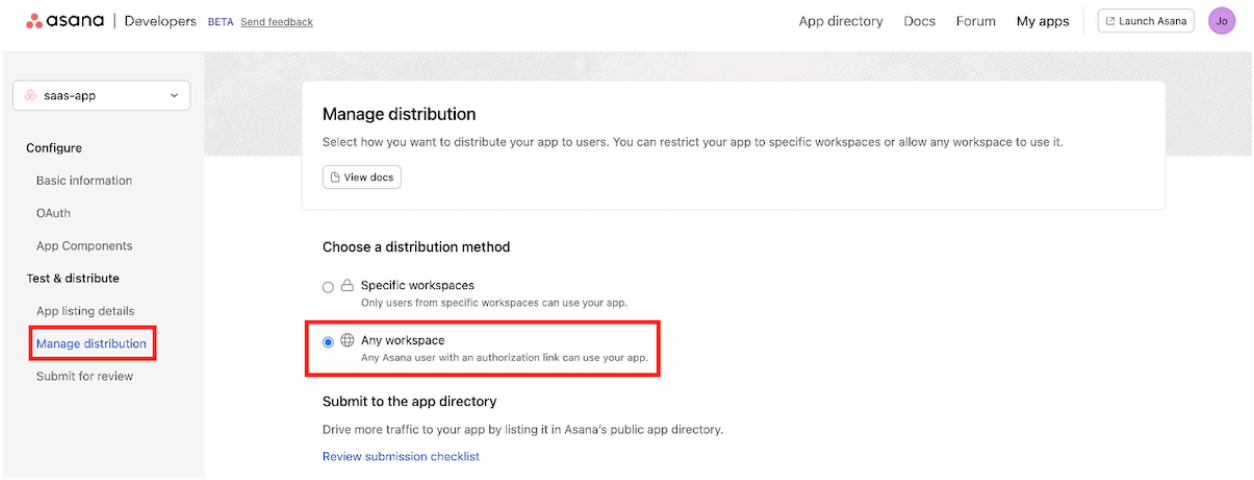
Configure the Asana Application for API-Based Data Protection

1. In the application window at https://app.asana.com/0/my-apps/<app-client-id>/settings, select OAuth in the left menu bar, and then configure the callback URL in the Redirect URLs field.

Updated: Wed, 23 Oct 2024 08:39:56 GMT



2. Select Manage Distribution, = and then click Any Workspace.

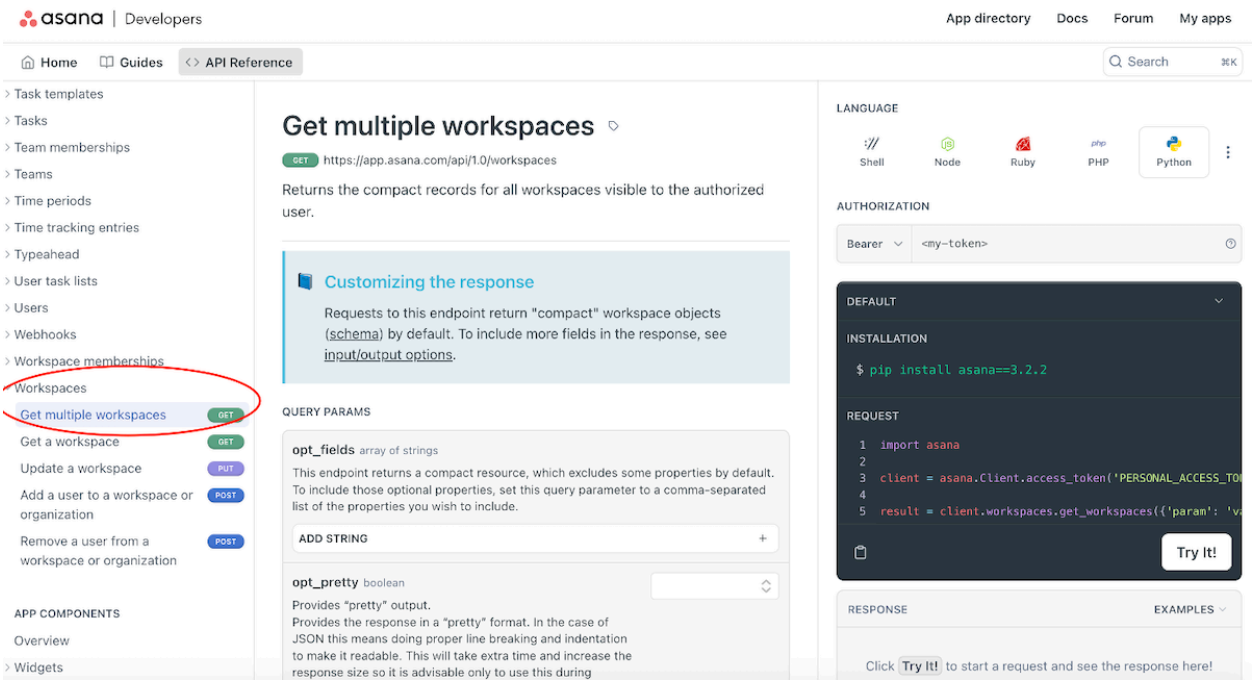


Configure Asana Webhooks Manually

Webhooks are automatically established and managed, but you can manage them manually.

To configure webhooks manually:

1. Obtain the resource ID of interest by going to https://developers.asana.com/reference/rest-api-reference. Select the desired resource on the right, and then select Get Multiple for the resource. You need to use a valid access token.



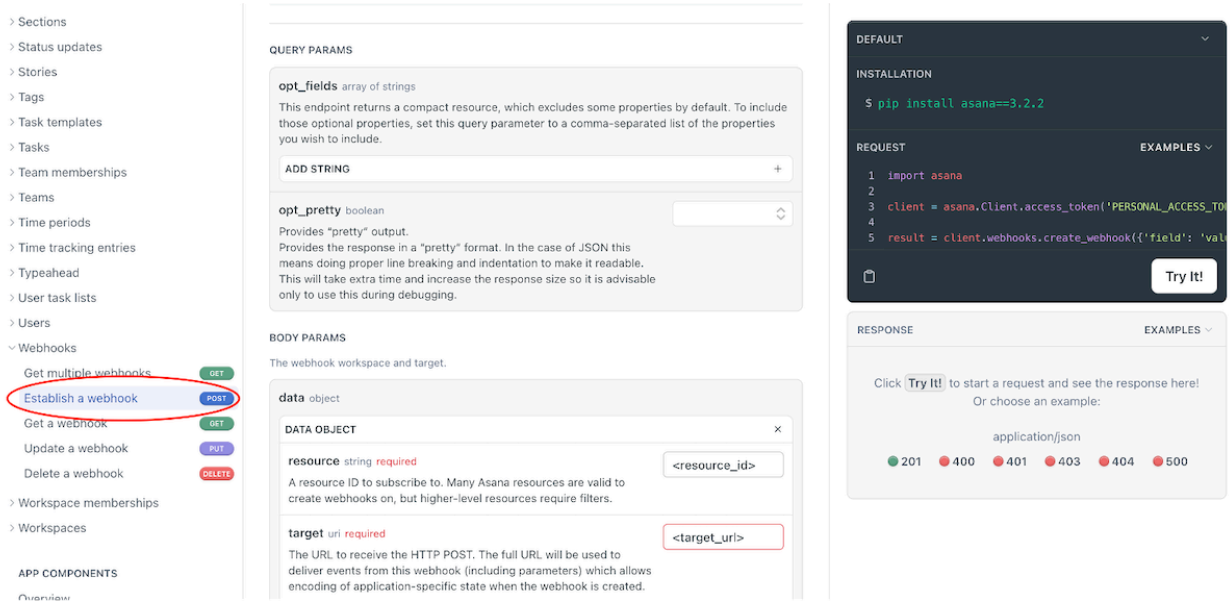
It is often necessary to start with parent resources to locate a specific resource identifier. The organizational level is as follows:

Workspace
- Projects
  - Section
    - Tasks
      - Subtasks
    - Milestones
      - Subtasks
    - Attachments

- Users
  - Section
    - Tasks
      - Subtasks
    - Milestones
      - Subtasks
    - Attachments

If the parent ID is unknown, you can trace backward up the tree to find a resource ID. You need to find the token only for the workspace IDs.

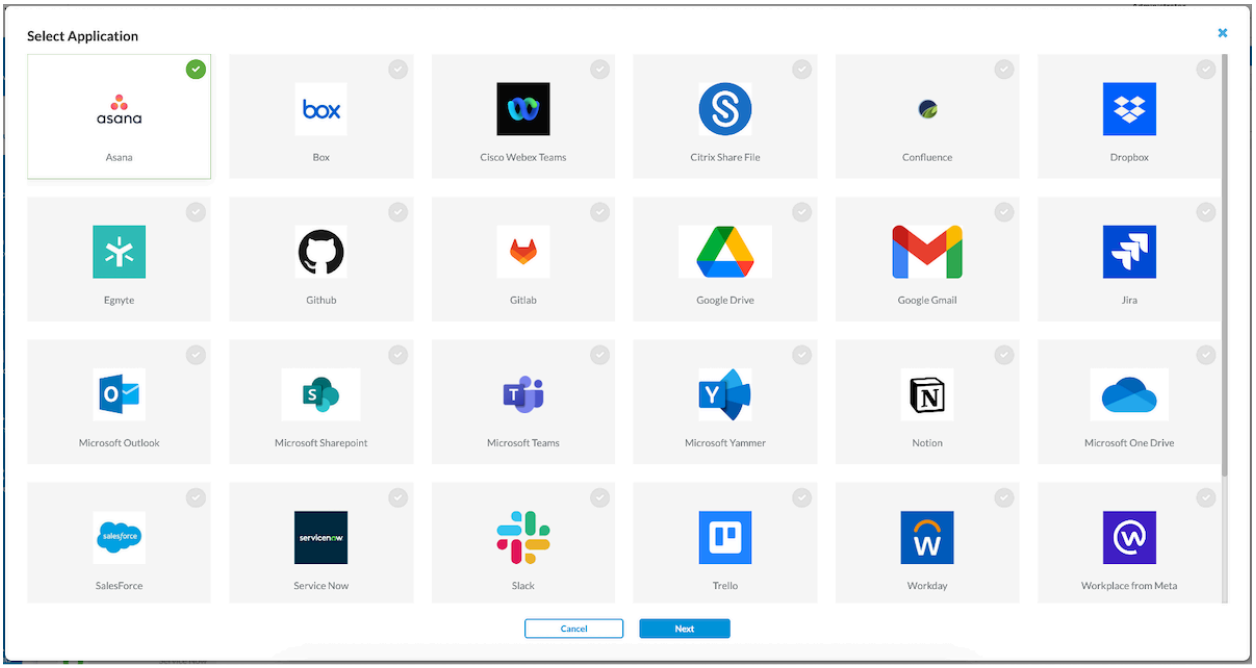
2. Using the ID of the resource, establish a webhook on https://developers.asana.com/reference/createwebhook. To do this, enter the resource ID and target URL under “Body params->data” and then clicking “Try it!”. Larger resources, such as workspaces, may need filtering into their sub-resources; that is, Workspace filtered into its projects.



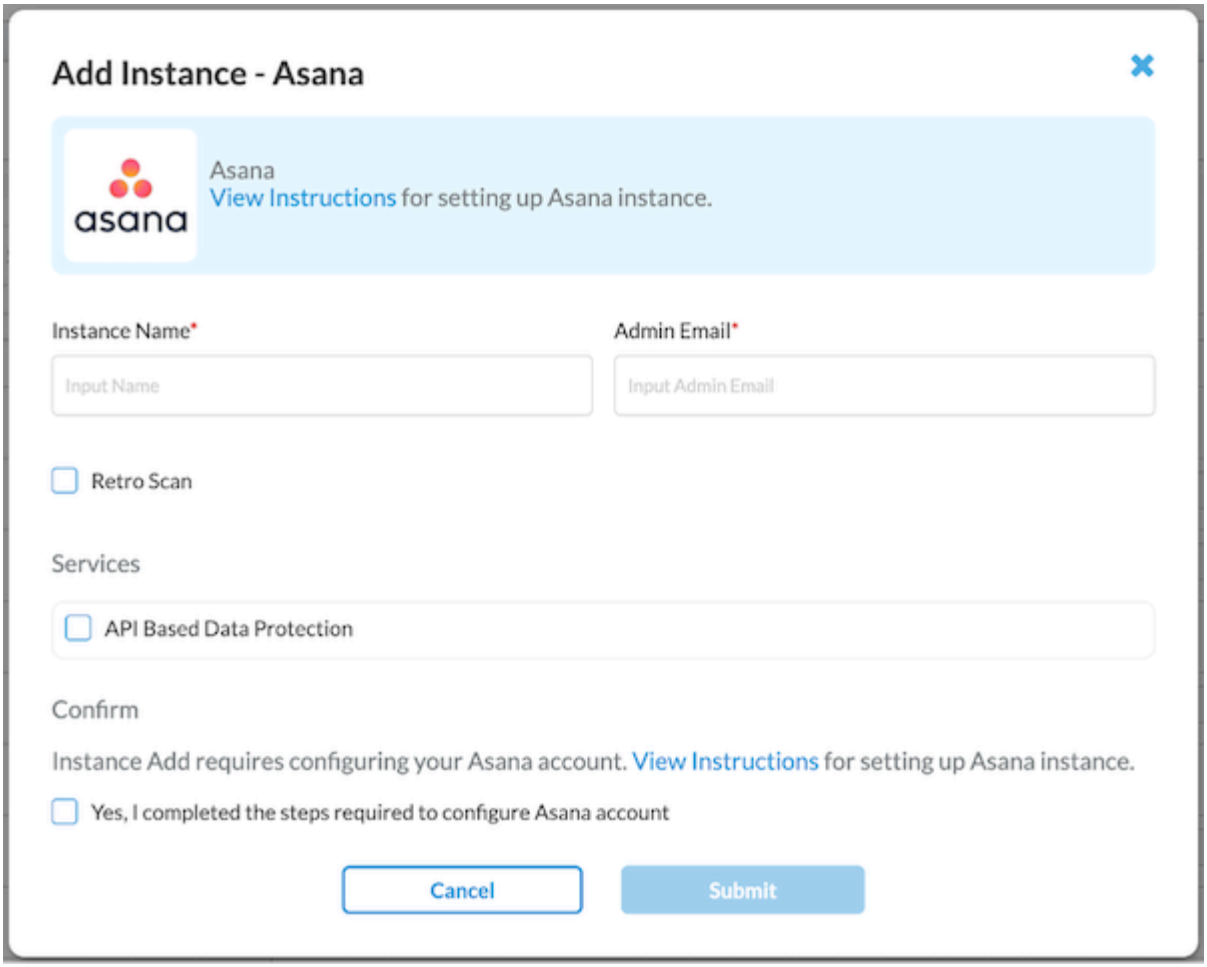
Configure an Asana Connector

To configure an Asana connector:

1. In the Versa Concerto portal, select a tenant under Tenants in the left menu bar.
2. Navigate to Configure > Advanced Security > API Based Data Protection > Connectors.
3. Click Add and select Asana, and then click Next.



4. Specify the Instance name and Admin email, then select the required services.



Field	Description
Instance Name (Required)	Enter the name of the instance.
Admin Email (Required)	Enter the email address of the Asana administrator account.
Retro Scan	Select to scan and protect all the files and objects that are present on Asana at the time of connector creation.
Services	Select the services for which this instance will be used.

Field	Description
	◦ API Based Data protection: Scan and protect content
Confirm	Select to indicate that the steps mentioned in the previous section to configure the Asana account have been followed.

5. Click Submit.

After adding the instance, click “Grant Access” to start the OAuth 2.0 process of granting access to the Versa API-DP cloud. This will open a login prompt for the Asana account. Use administrator credentials to log in and grant access. Webhooks for existing workspaces will be automatically established during this OAuth process.

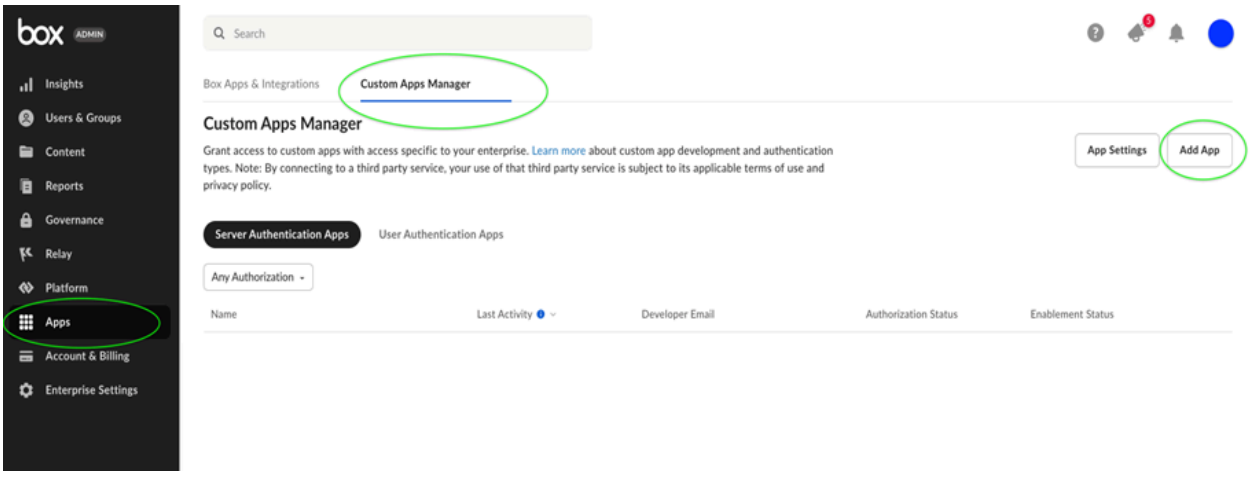
Box API-Based Data Protection

This section describes how to configure the Box application for API-based data protection.

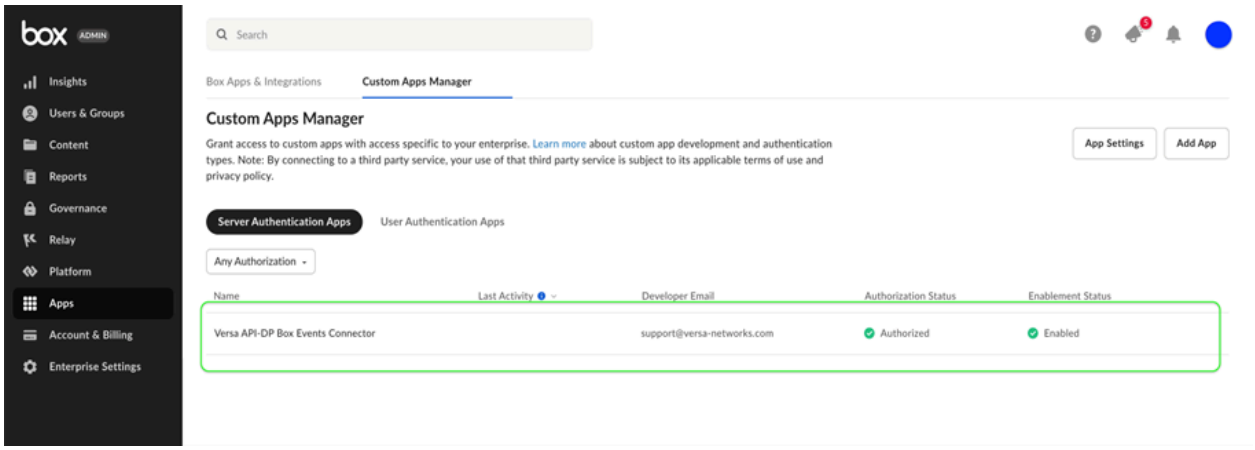
Configure Box for API-Based Data Protection

To configure a new instance for Box:

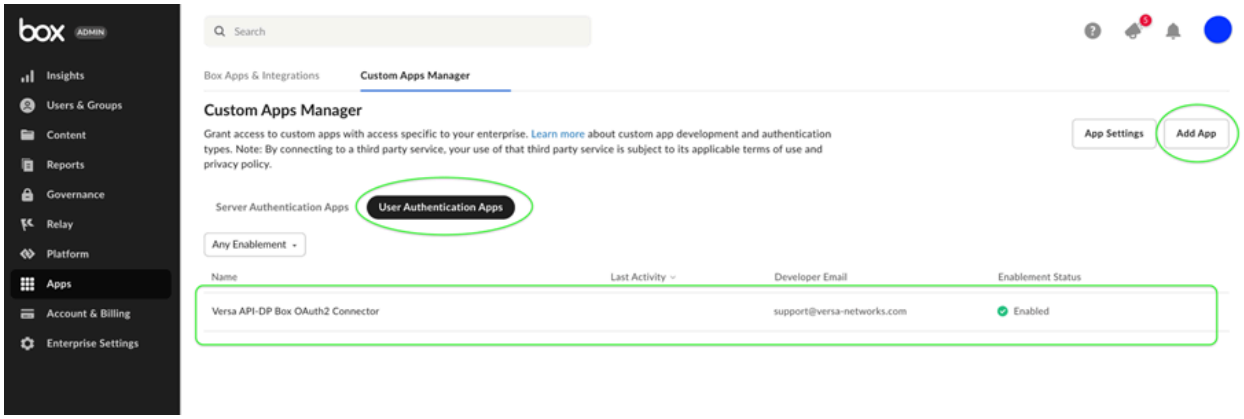
1. Login to Box as an administrator and navigate to Admin Console.
2. Click Apps in the left menu bar.
3. Select Custom App Manager tab and click Add App.



4. Enter client ID 6b86gkdkodpctqqatwy4r2ernpizzukk. Click Next and Authorize.
5. In the Server Authentication Apps tab, Versa API-DP Box OAuth2 Connector entry displays.



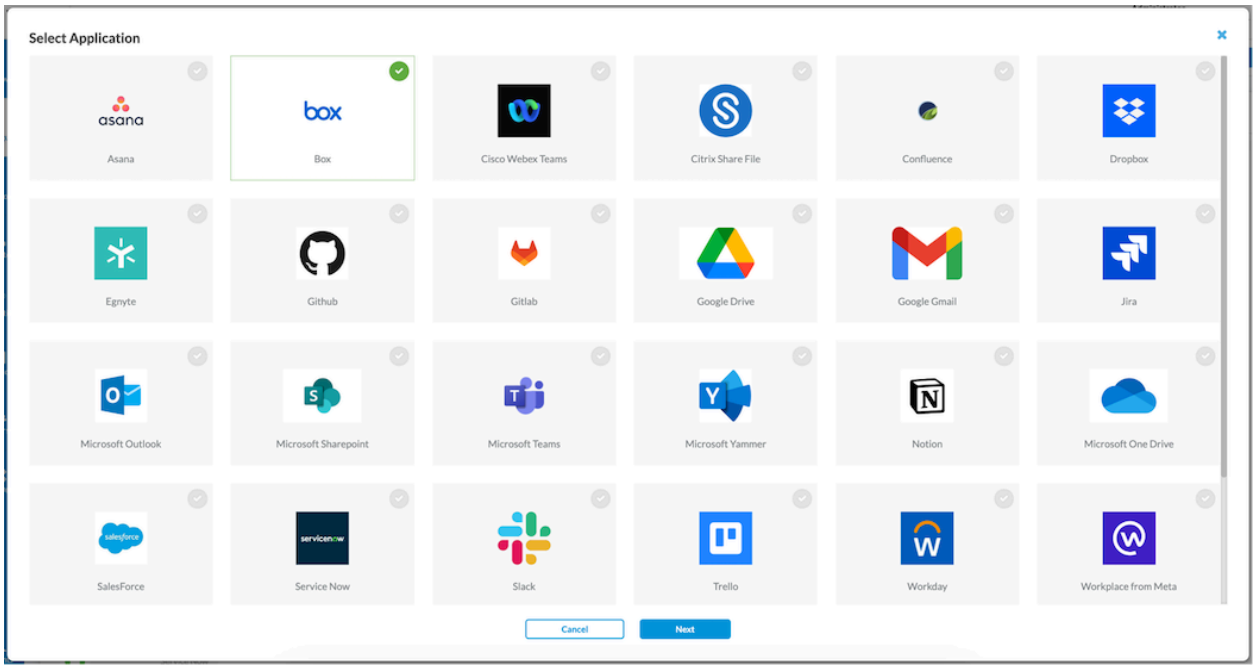
6. Select User Authentication Apps tab and click Add App.
7. Enter client ID uzzgjqd7b6hjhvxk05l3d40s8evcxirr. Click Next and Authorize.
8. In the User Authentication Apps tab, Versa API-DP Box OAuth2 Connector entry displays.



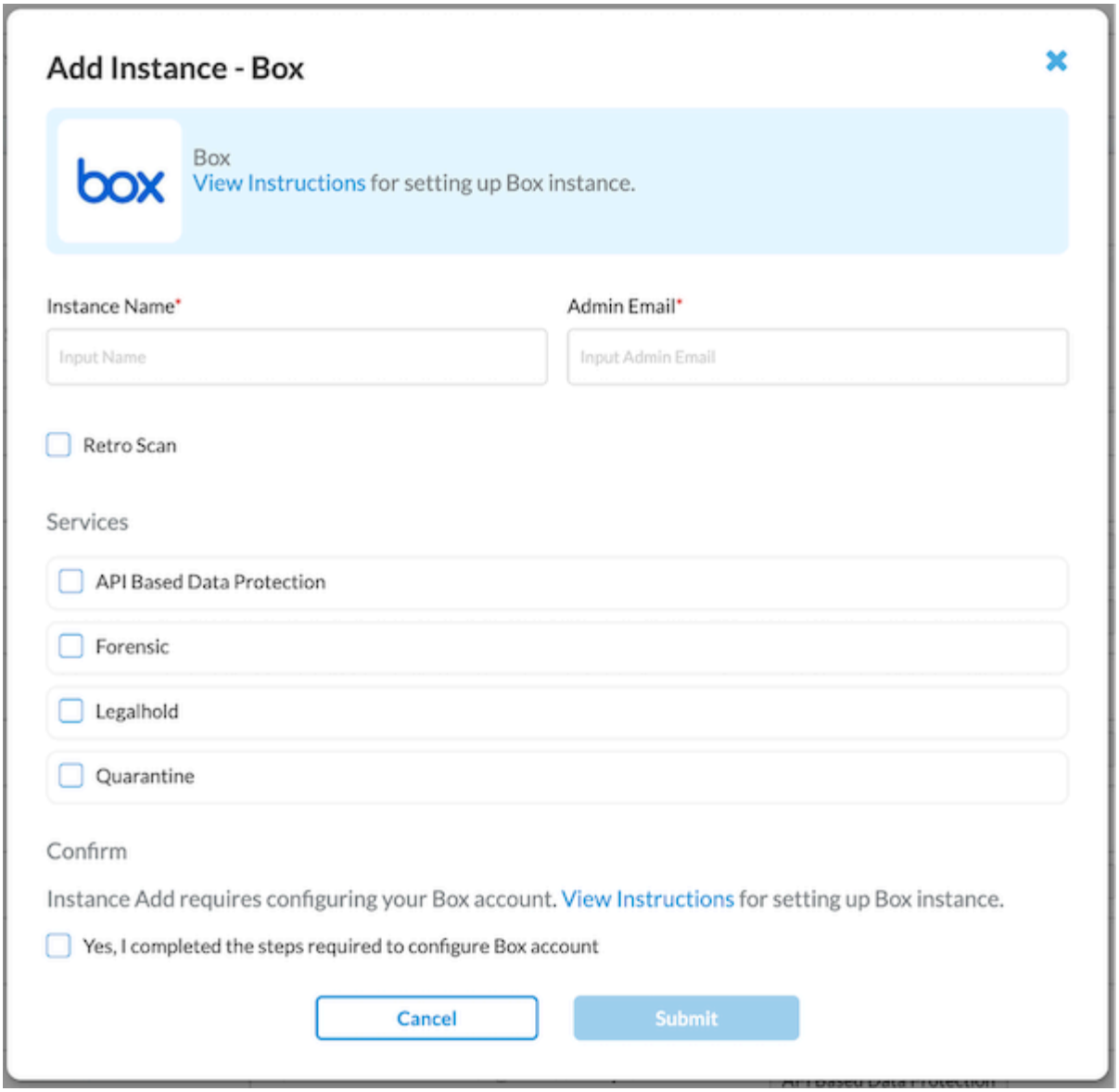
Configure a Box Connector

To configure a connector for Box:

1. Navigate to "Configure" > “Advanced Security” > “API Based Data Protection” > “Connectors”.
2. Select the SaaS tab, select Box, then click the ✚ Add icon.



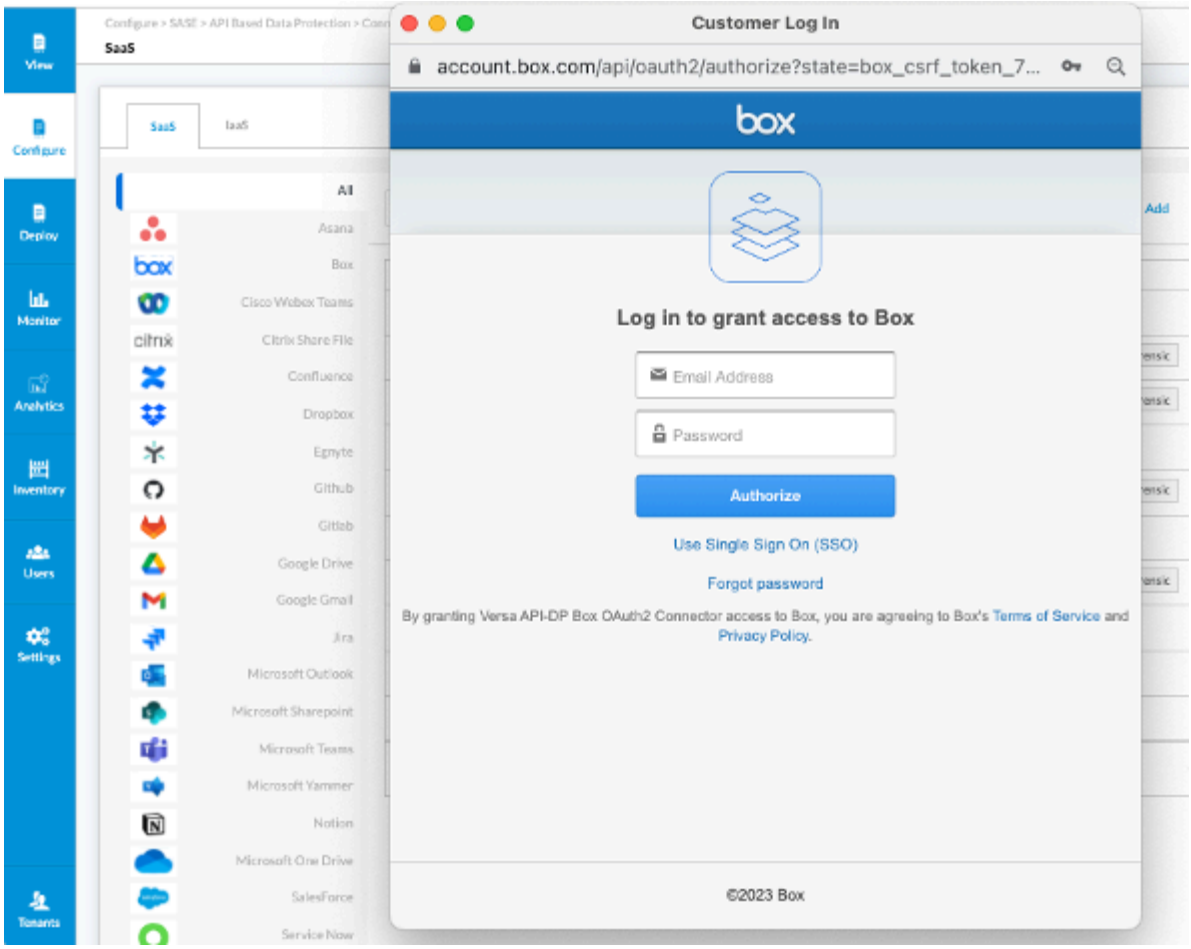
3. In the Add Instance window, enter information for the following fields.



Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email (Required)	Enter an email address of the Box administrator account.
Retro Scan	Click to scan and protect all the files that are present on Box at the time of connector creation.
Services	Select the services to use for the instance.

Field	Description
	◦ API-Based Data Protection—Scan and protect content. ◦ Forensic—Use this instance for forensics. ◦ Legal Hold—Use this instance for legal hold. ◦ Quarantine—Use this instance for quarantine files.
Confirm	Click to confirm that the steps required to configure the Box account are complete.

4. Click Submit. The new instance is added to the Box application and displayed in the Connectors > SaaS screen.
5. After adding the instance, select Grant Access to the new instance to start the OAuth2 process of granting access to the Versa API data protection cloud. This will open login prompt for the Box account.



6. Use the Administrator credentials to login. The next screen shows the permissions that the Versa service will require to scan and monitor the Box account. Click “Grant Access to Box”.

Cisco Webex Teams API-Based Data Protection

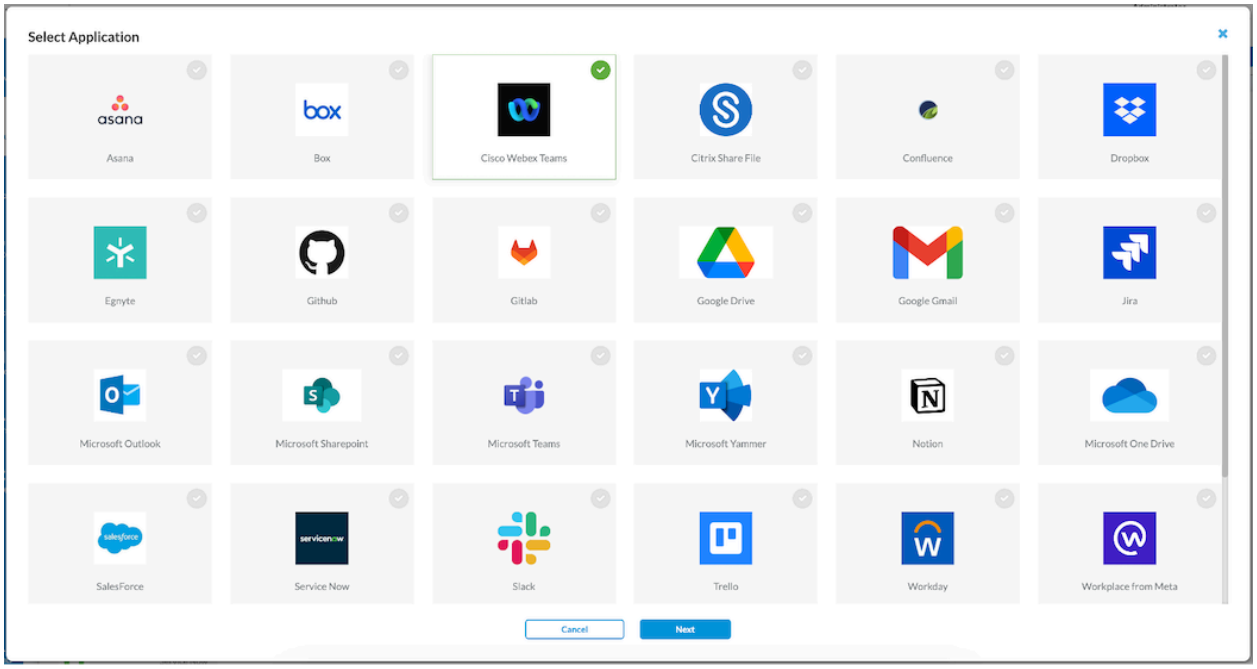
This section describes how to configure the Cisco Webex Teams application for API -baseddata protection.

Configure Cisco Webex Teams for API-Based Data Protection

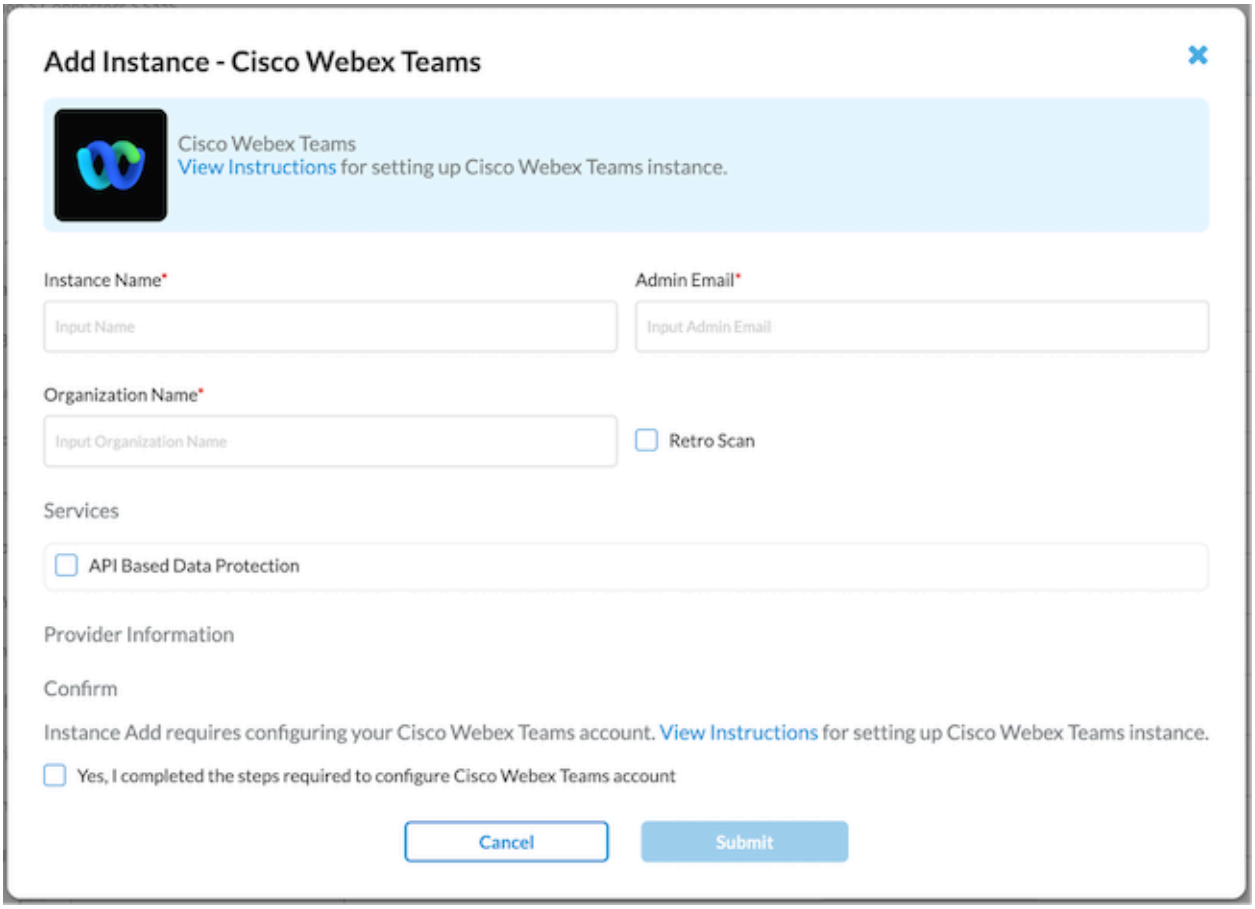
For Cisco Webex, no configuration is required.

Configure a Cisco Webex Connector

1. Navigate to "Configure" > “Advanced Security” > “API Based Data Protection” > “Connectors”.
2. Select the SaaS tab, select Cisco Webex Team, then click the + Add icon.



3. In the Add Instance window, enter information for the following fields.



Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email (Required)	Enter the email address of the Cisco Webex administrator account.
Retro Scan	Click to scan and protect all the files that are present on Webex at the time of connector creation.
Services	Select the services to use for the instance. ◦ API-Based Data Protection—Scan and protect content
Confirm	Click to confirm that the steps required to configure the Cisco Webex account are complete.

4. Click Submit.

5. After adding the instance, select Grant Access to the new instance to start the OAuth2 process of granting access to the Versa API data protection cloud. This will open login prompt for the Cisco Webex Teams account. Use the administrator credentials to log in and grant access.

Citrix ShareFile API-Based Data Protection

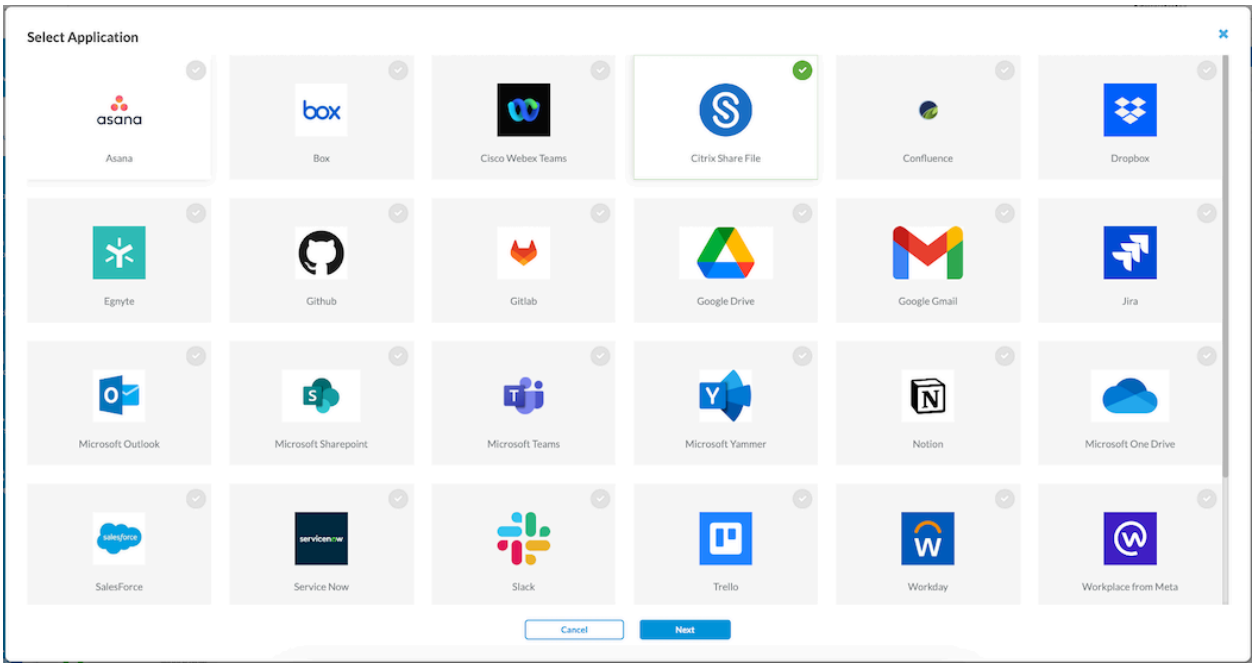
This section describes how to configure the Citrix ShareFile application for API-based data protection.

Configure Citrix ShareFile for API-Based Data Protection

For Citrix ShareFile, no configuration is required.

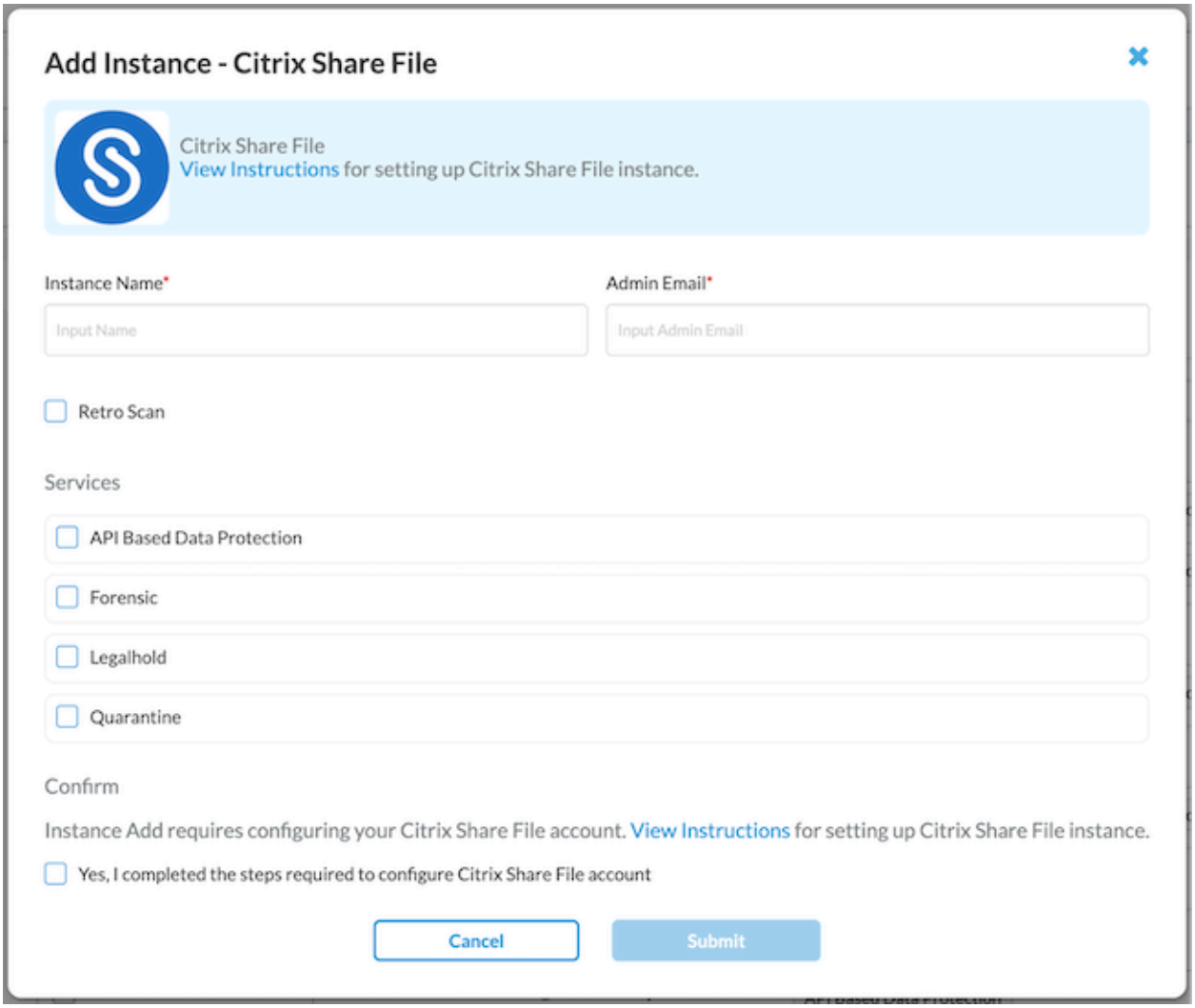
Configure a Citrix ShareFile Connector

1. Navigate to "Configure" > “Advanced Security” > “API Based Data Protection” > “Connectors”.
2. Click the + Add icon, select Citrix ShareFile, then click Next.



3. In the Add Instance window, enter information for the following fields.

Updated: Wed, 23 Oct 2024 08:39:56 GMT



Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email (Required)	Enter an email address of the Citrix ShareFile administrator account.
Retro Scan	Click to scan and protect all the files that are present on Citrix ShareFile at the time of connector creation.
Services	Select the services to use for the instance. ◦ API-Based Data Protection—Scan and protect content ◦ Forensic—Use this instance for forensics

Field	Description
	◦ Legal Hold—Use this instance for legal hold ◦ Quarantine—Use this instance for quarantine files
Confirm	Click to confirm that the steps required to configure the Citrix ShareFile account are complete.

4. Click Submit.
5. After the instance is added, select Grant Access to start the OAuth2 process of granting access to the Versa API data protection cloud. This will open a login prompt for the Citrix ShareFile account. Use the administrator credentials to log in and grant access.

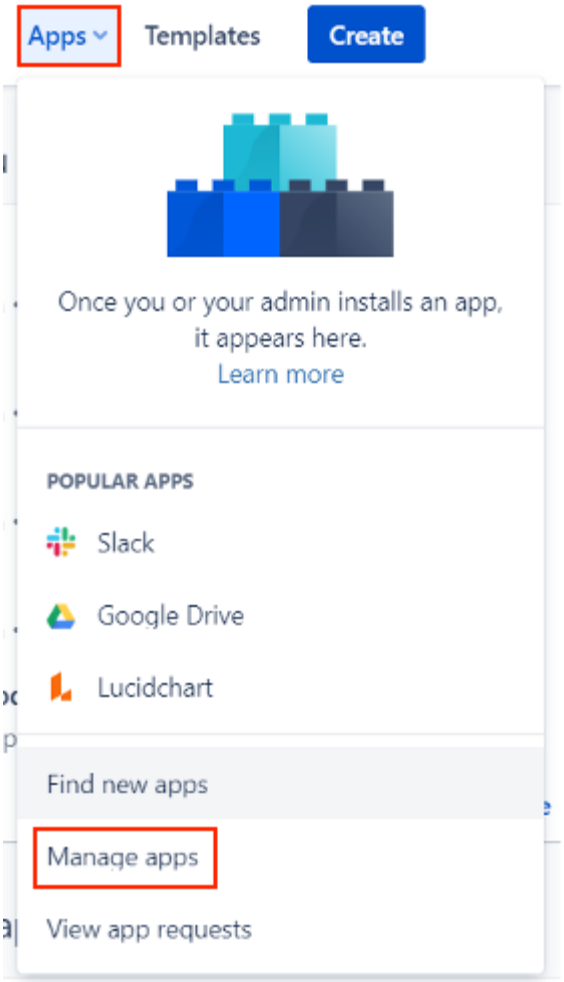
Confluence API-Based Data Protection

This section describes how to configure the Confluence application for API-based data protection.

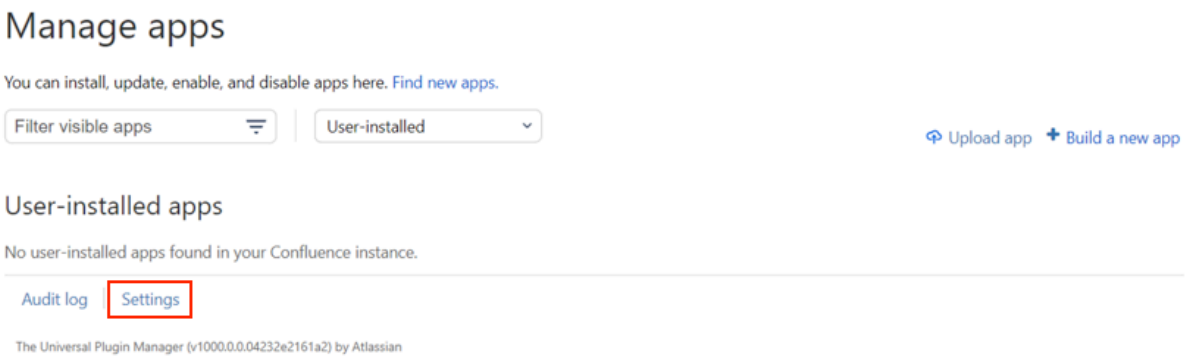
Configure Confluence for API-Based Data Protection

To configure Confluence for API-based data protection:

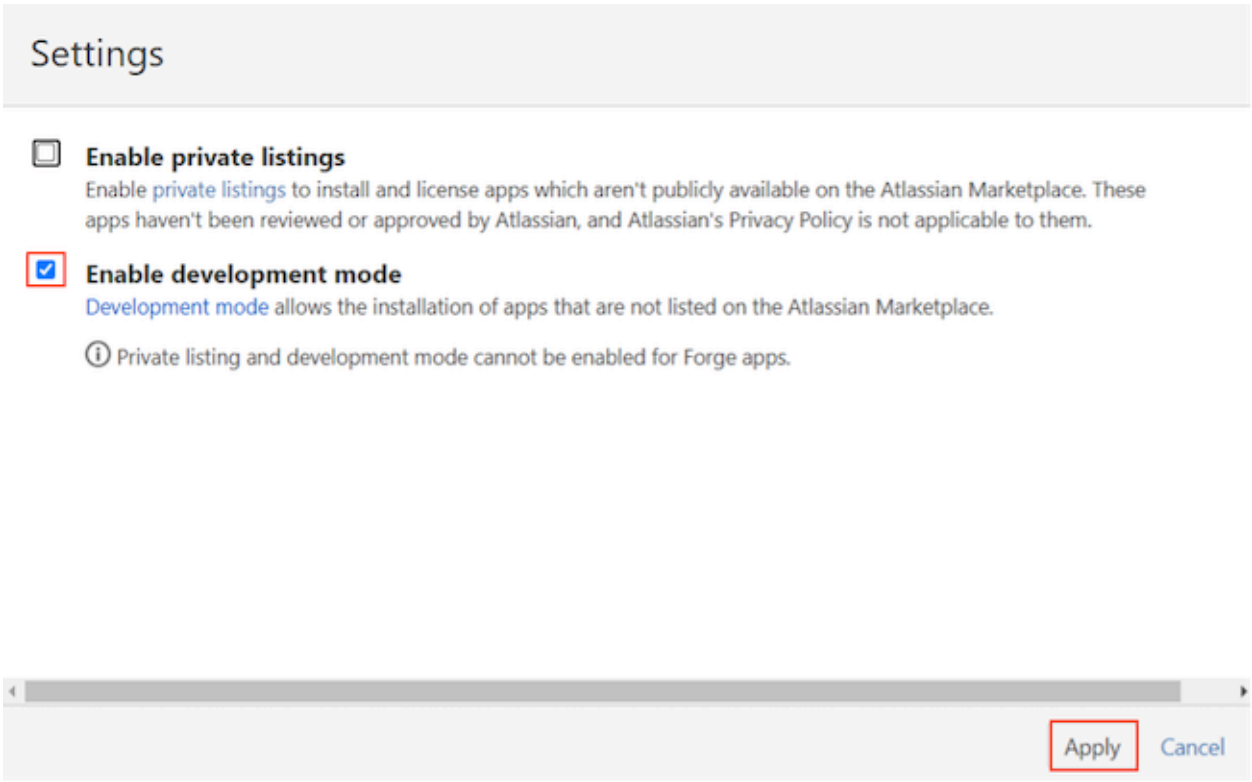
1. Go to atlassian.com and navigate to Confluence.
2. In the Confluence site, click on "Apps" on the top-nav bar and then select "Manage apps" from the dropdown.



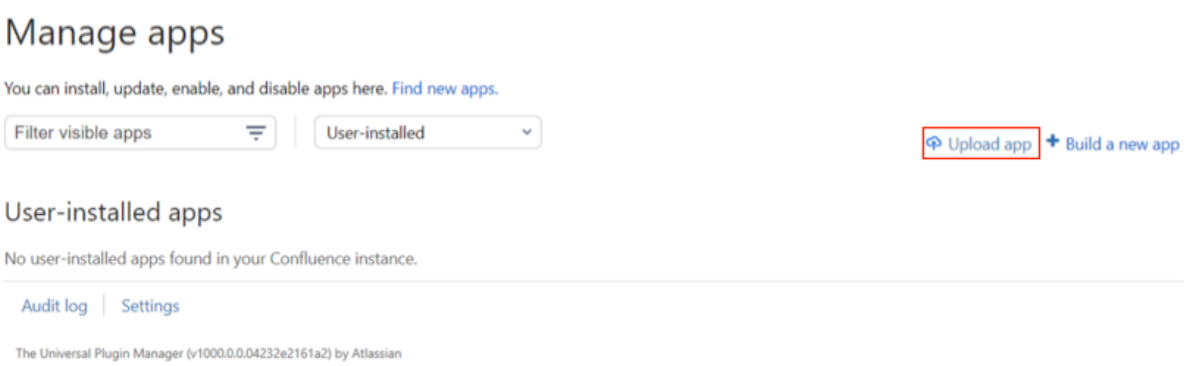
3. Click Settings under User-installed apps.



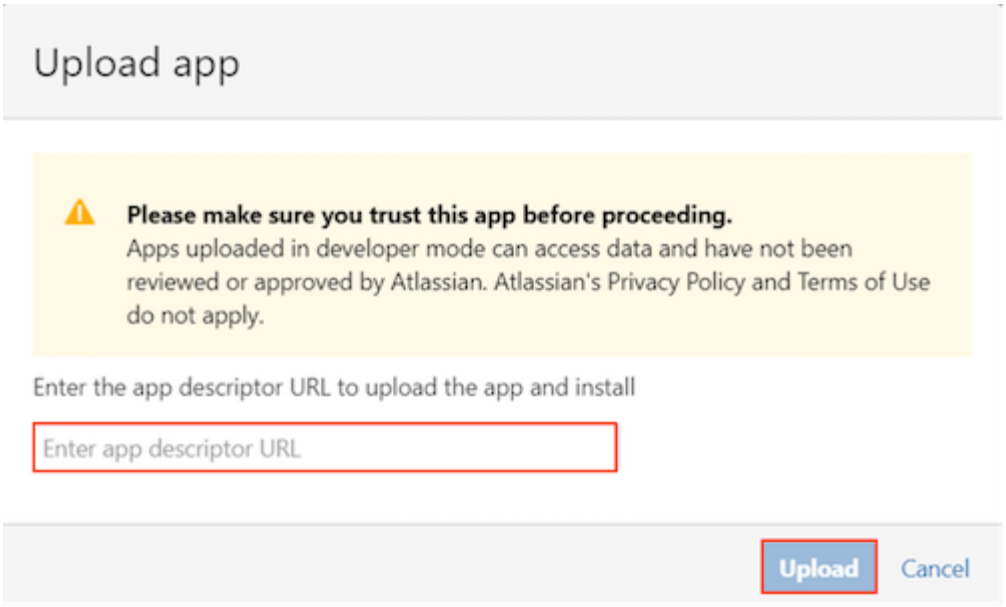
4. Select "Enable development mode," then click "Apply."



5. In the "Manage apps" page, click the "Upload app" button.



6. In the "Upload app" popup window, enter https://apidp.versanow.net/v1/confluence/webhook-app-descriptor.json, then click "Upload".

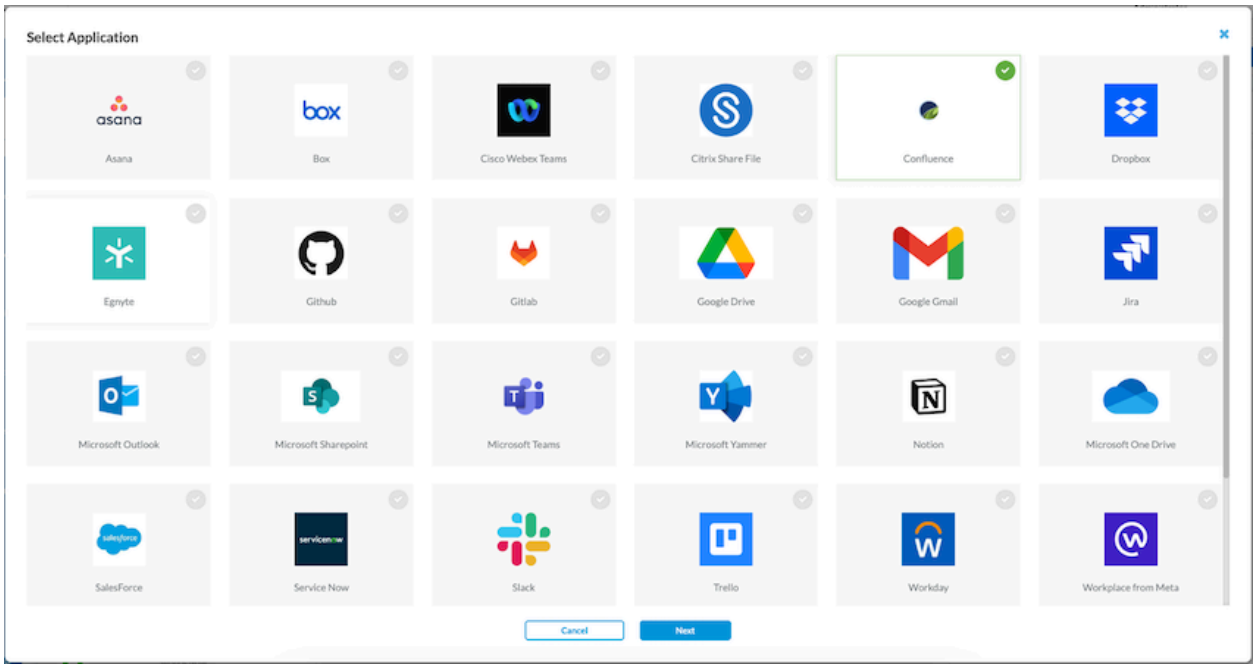


7. After initiating the installation process, allow some time for the application to be installed and configured. Once completed, the process is finished.

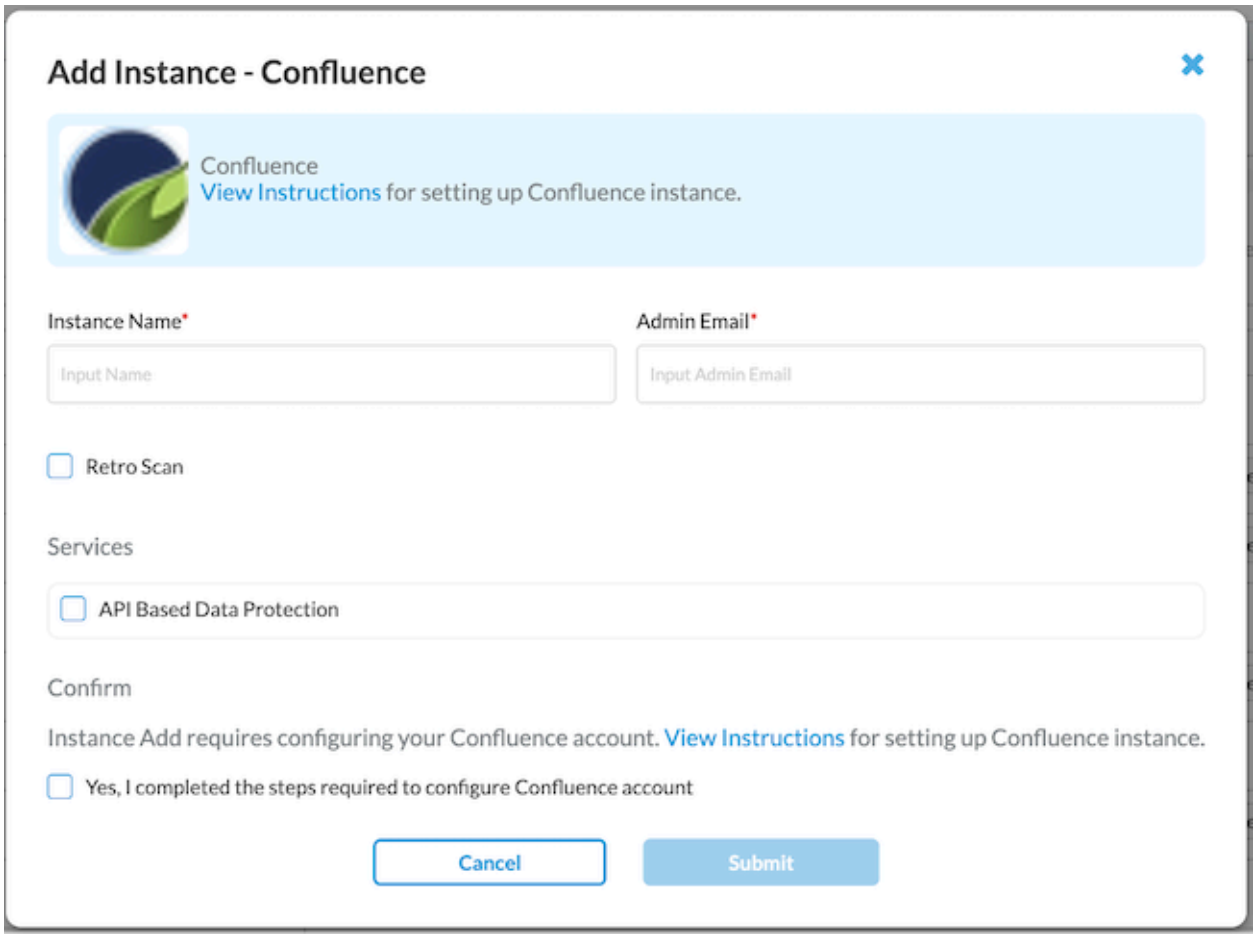
Configure a Confluence Connector

To configure a Confluence connector:

1. Navigate to "Configure" > “Advanced Security” > “API Based Data Protection” > “Connectors”.
2. Click the + Add icon, select Confluence, then click Next.



3. In the Add Instance window, enter information for the following fields.



Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email (Required)	Enter an email address of the Confluence administrator account.
Retro Scan	Click to scan and protect all the files that are present on Confluence at the time of connector creation.
Services	Select the services to use for the instance. ◦ API-Based Data Protection—Scan and protect content
Confirm	Click to confirm that the steps required to configure the Confluence account are complete.

4. Click Submit.
5. After the instance is added, select Grant Access to start the OAuth2 process of granting access to the Versa API data protection cloud. This will open a login prompt for the Confluence account. Use the administrator credentials to log in and grant access

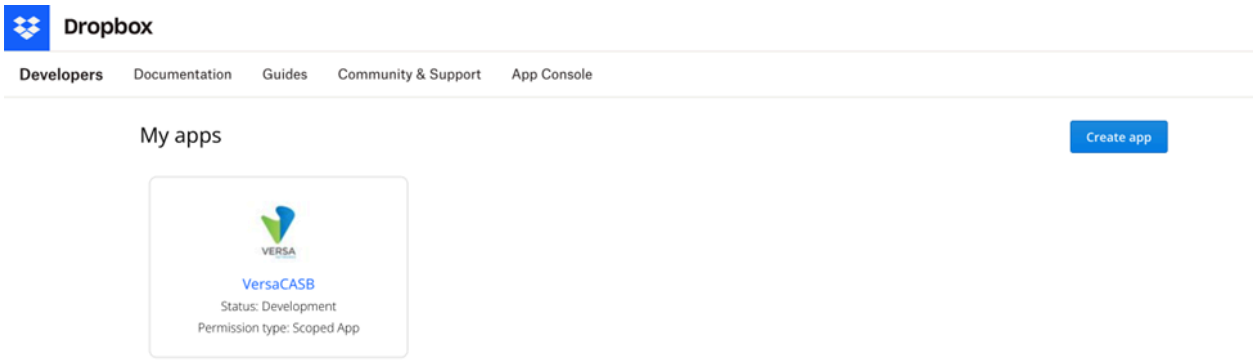
Dropbox API-Based Data Protection

This section describse how to configure the Confluence application for API-based data protection.

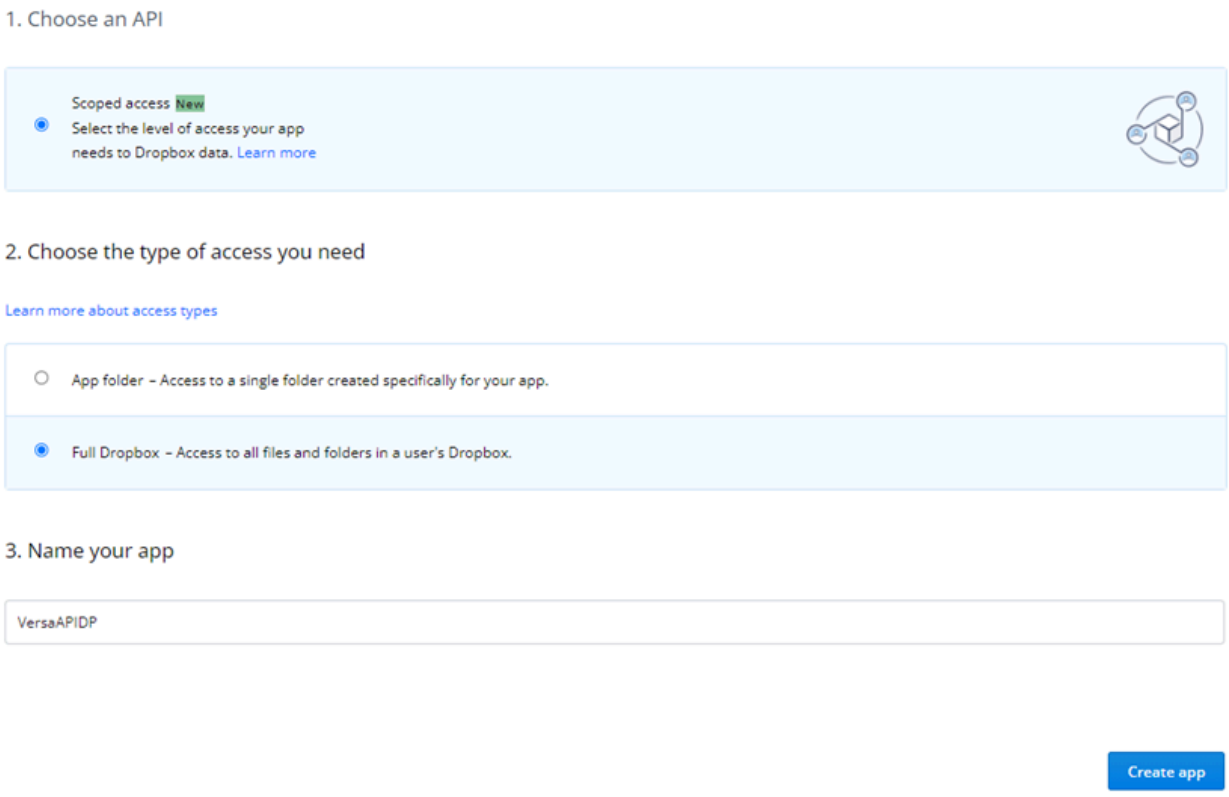
Configure Dropbox for API-Based Data Protection

To configure a new instance for Dropbox:

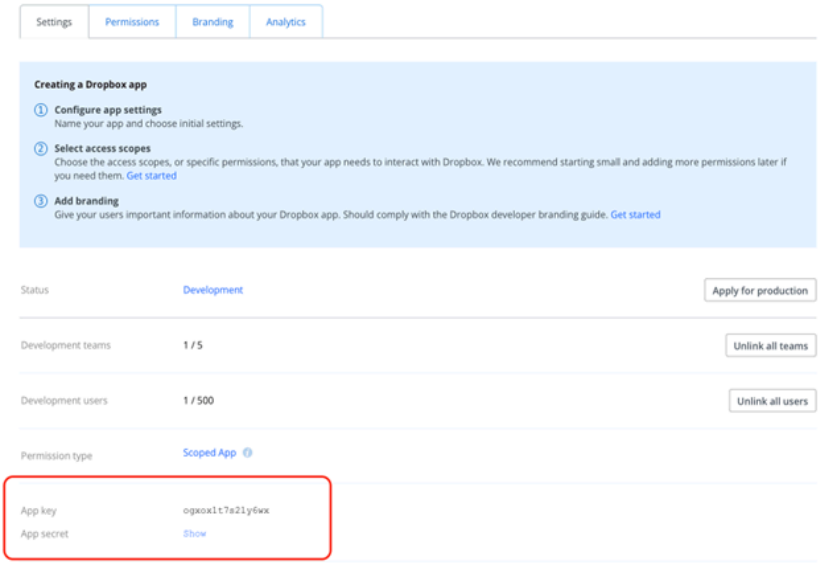
1. Login to https://www.dropbox.com/developers and navigate to App Console.
2. On the right hand side of the page, click Create app to create an application like the “VersaCASB” example shown below.



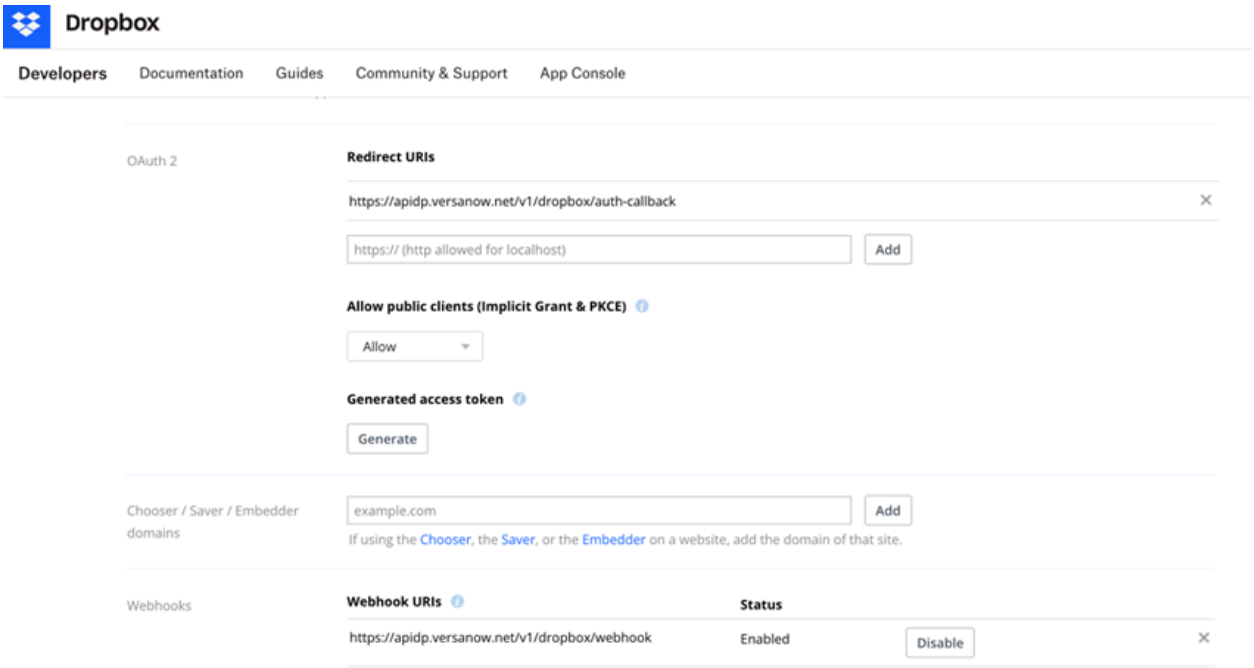
3. Fill and select all the corresponding fields depending on the scope of access you want to give, the file access level you want, and the name of the application you would like to have.



4. Click Create app.
5. Once the application is created, you can click on the application to visit the settings page that contains all relevant information regarding the OAUth 2.0 flow. You can access the app key and secret, as shown below highlighted in red.

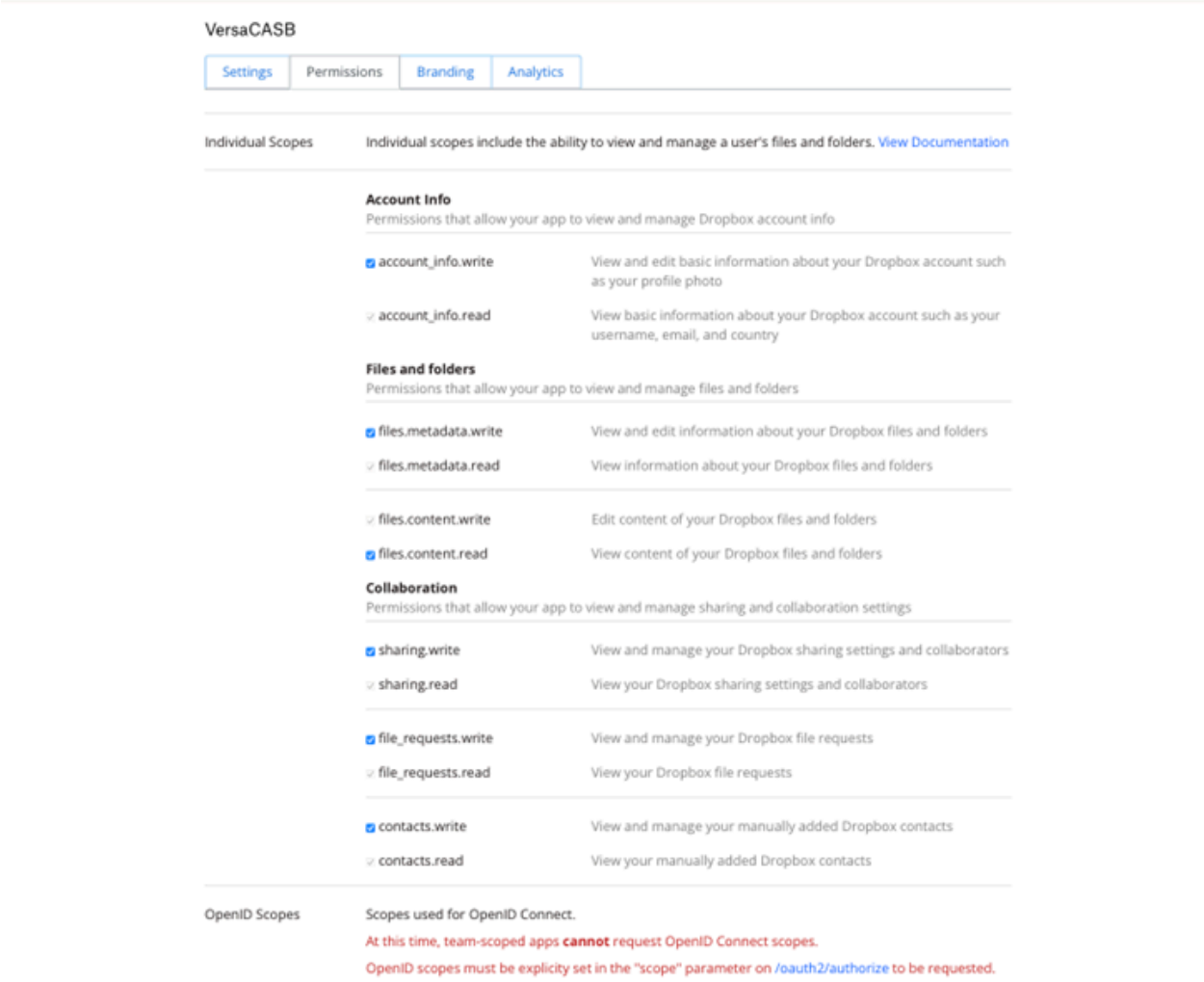


6. In the Dropbox Developers tab, enter the following information.



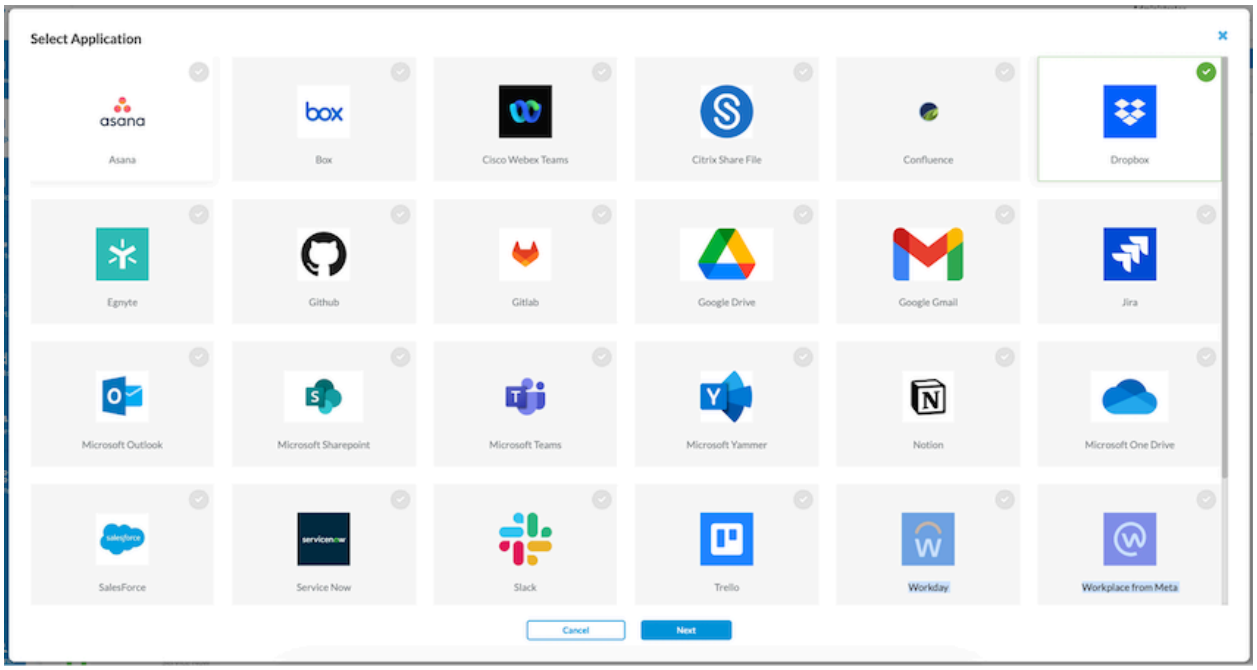
Field	Description
Redirect URIs	Enter https://apidp.versanow.net/v1/dropbox/auth-callback
Webhook URIs	Enter https://apidp.versanow.net/v1/dropbox/webhook

7. Click Permissions tab to manage specific scopes. Select the options as displayed in the following screen.

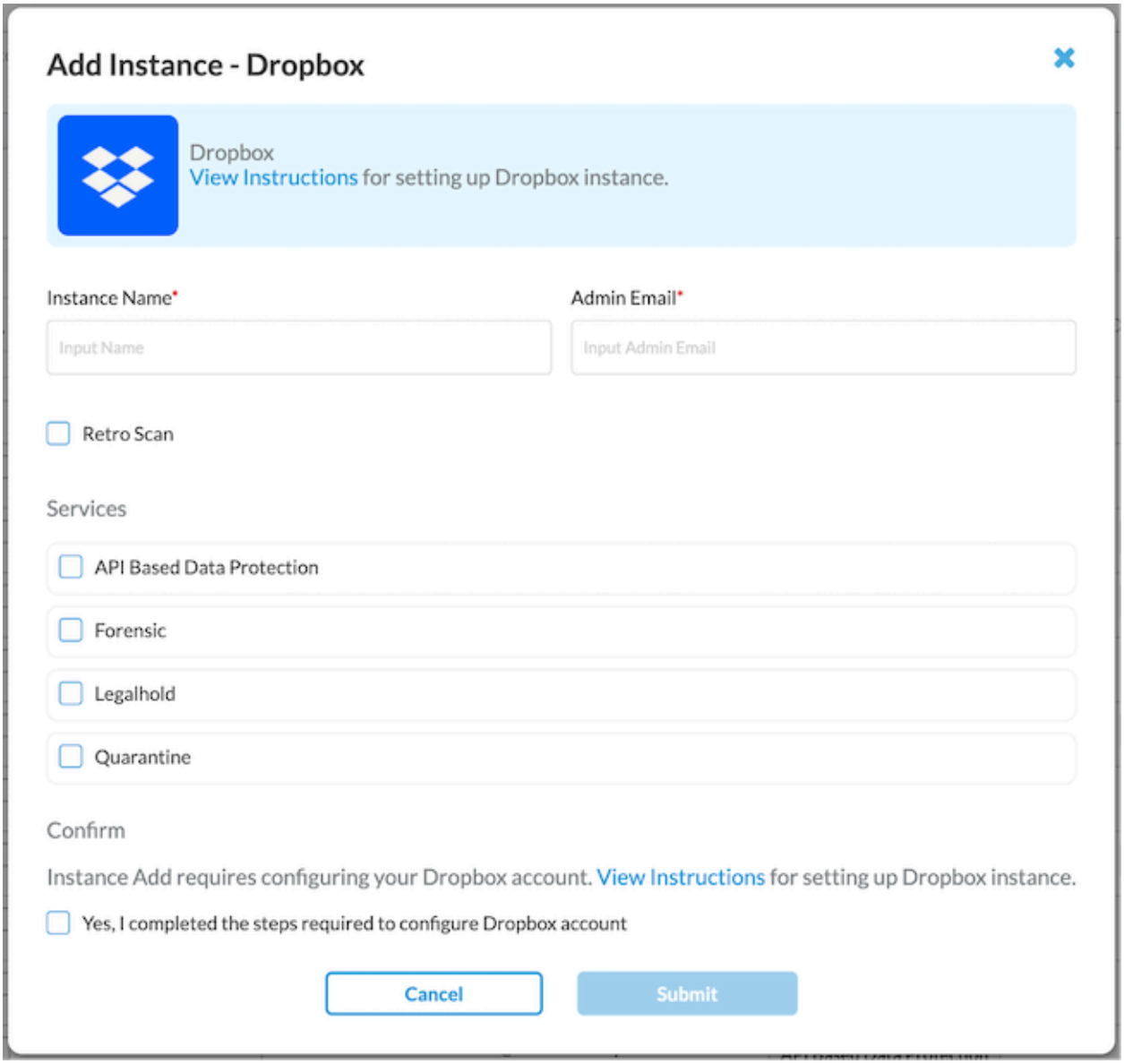


Configure a Dropbox Connector

1. Navigate to "Configure" > “Advanced Security” > “API Based Data Protection” > “Connectors”.
2. Click the ✚ Add icon, select Confluence, then click Next.



3. In the Add Instance window, enter information for the following fields.



Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email (Required)	Enter an email address of the Dropbox administrator account.
Retro Scan	Scan and protect all the files that are present on Dropbox at the time of connector creation.
Services	Select the services to use for the instance.

Field	Description
	◦ API-Based Data Protection—Scan and protect content. ◦ Forensic: Use this instance for Forensics. ◦ Legal hold: Use this instance for Legal hold. ◦ Quarantine—Use this instance for quarantine files.
Confirm	Click to confirm that the steps required to configure the Dropbox account are complete.

4. Click Submit.
5. After the instance is added, select Grant Access to start the OAuth2 process of granting access to the Versa API data protection cloud. Use Dropbox Administrator credentials to log in and grant access.

Egnyte API-Based Data Protection

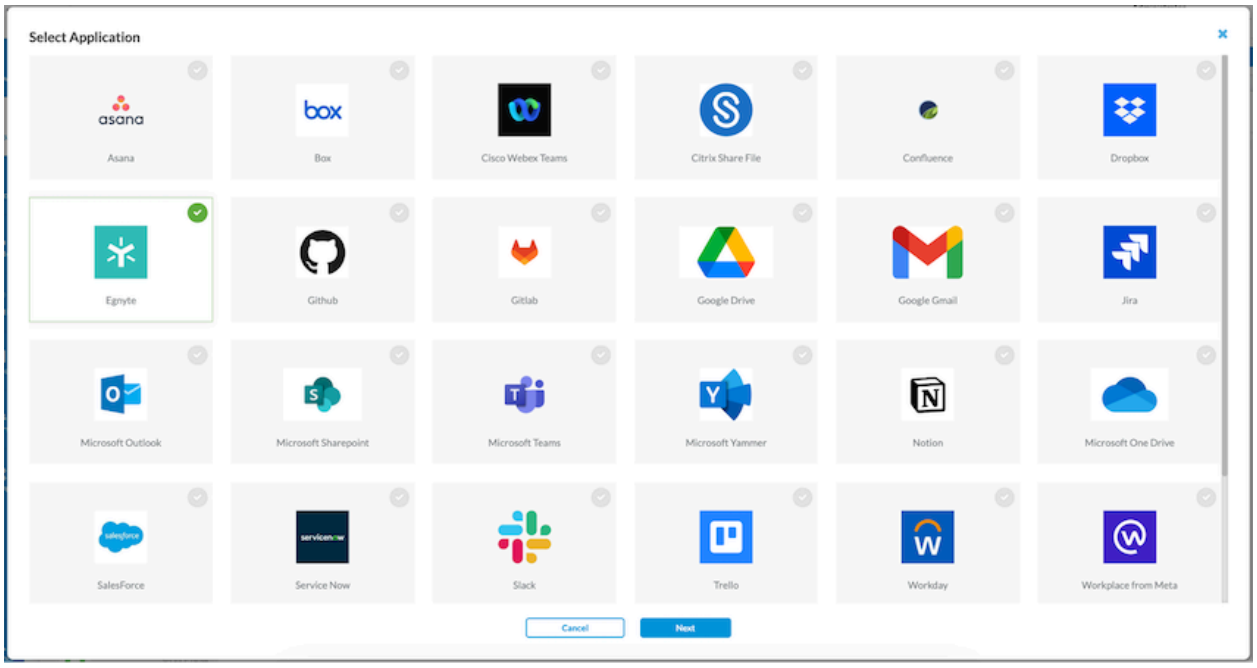
This section describes how to configure the Confluence application for API-based data protection.

Configure Egnyte for API-Based Data Protection

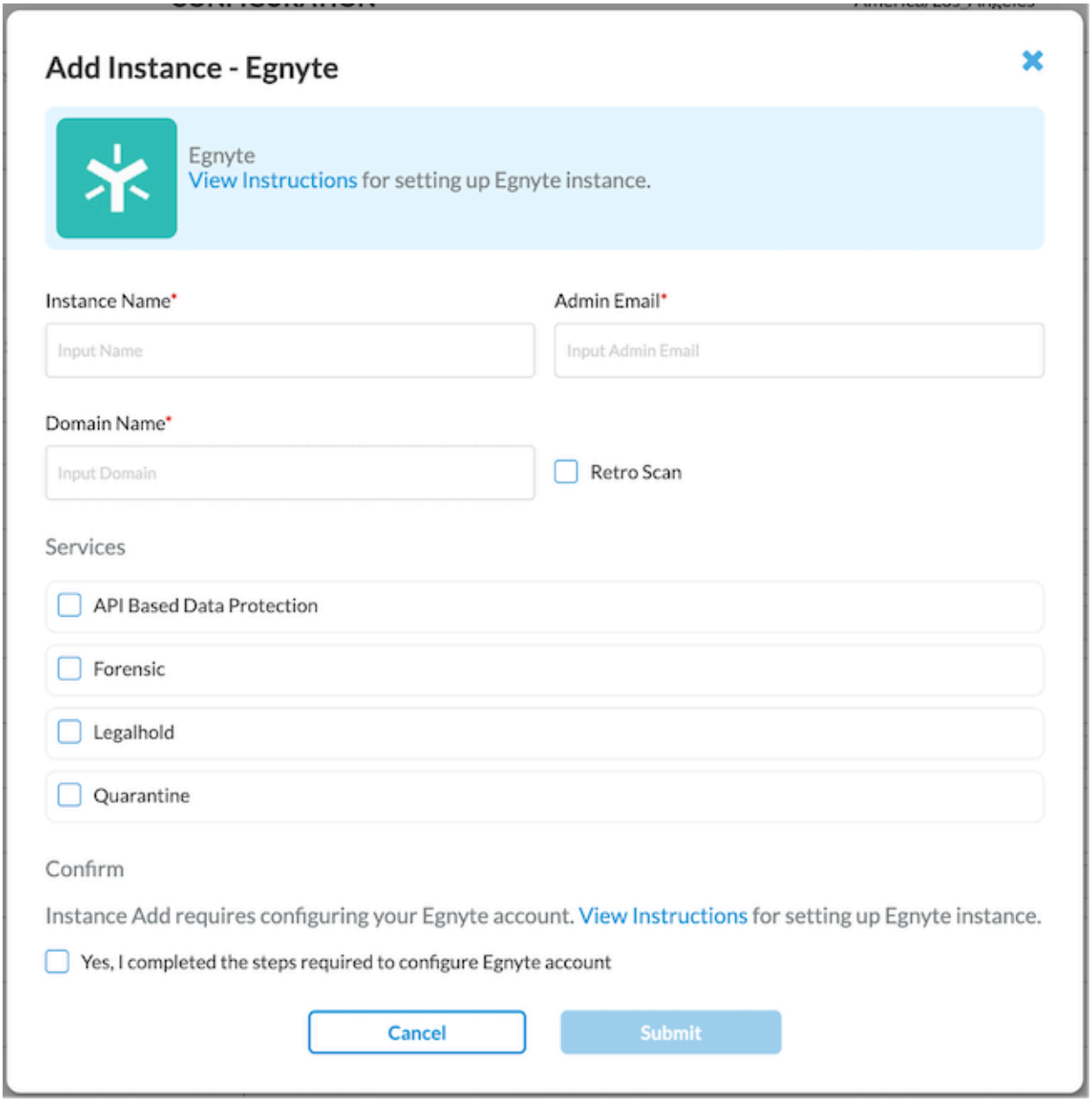
For Egnyte, no configuration is required at https://www.egnyte.com.

Configure an Egnyte Connector

1. Navigate to "Configure" > “Advanced Security” > “API Based Data Protection” > “Connectors”.
2. Click the + Add icon, select Egnyte, then click Next.



3. In the Add Instance window, enter information for the following fields.



Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email (Required)	Enter an email address of the Egnyte administrator account.
Domain Name (Required)	Enter the name prefix used in Egnyte domain name.
Services	Select the services to use for the instance.

Field	Description
	◦ API-Based Data Protection—Scan and protect content. ◦ Forensic—Use this instance for forensics. ◦ Legal hold: Use this instance for Legal hold. ◦ Quarantine—Use this instance for quarantine files.
Confirm	Click to confirm that the steps required to configure the Egnyte account are complete.

4. Click Submit.
5. After the instance is added, select Grant Access to start the OAuth2 process of granting access to the Versa API data protection cloud. Use Egnyte Administrator credentials to log in and grant access.

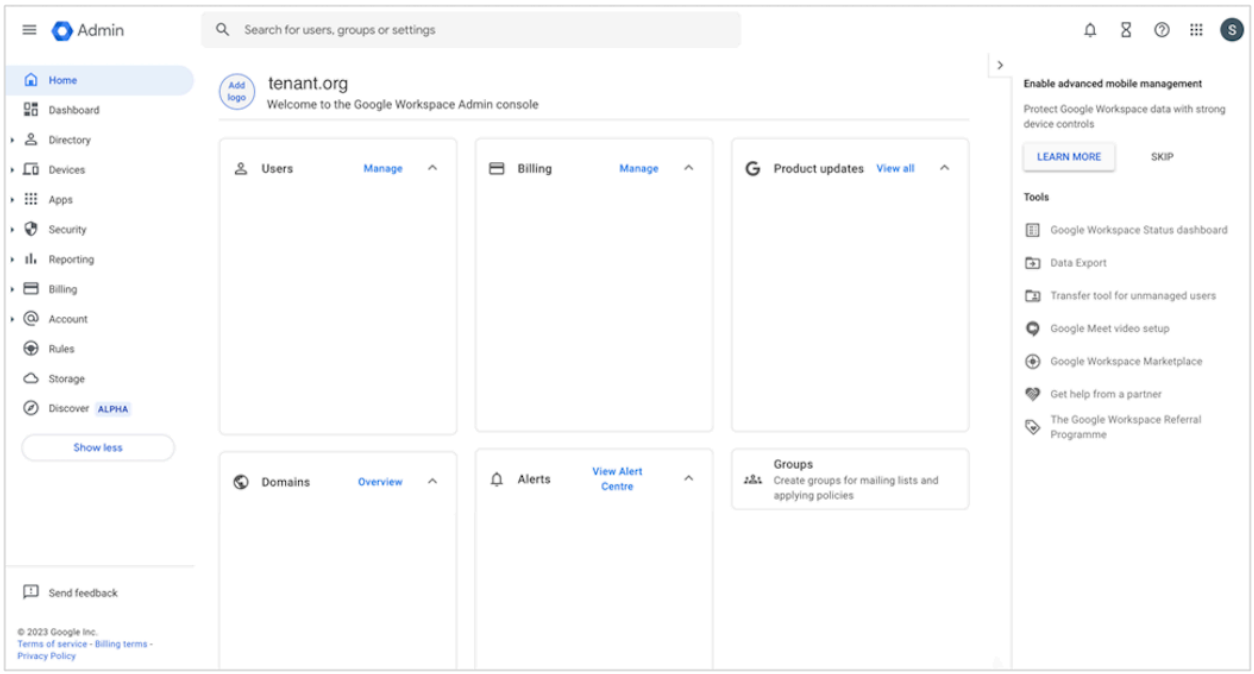
Google Drive API-Based Data Protection

This section describes how to configure the Google Drive application for API-based data protection.

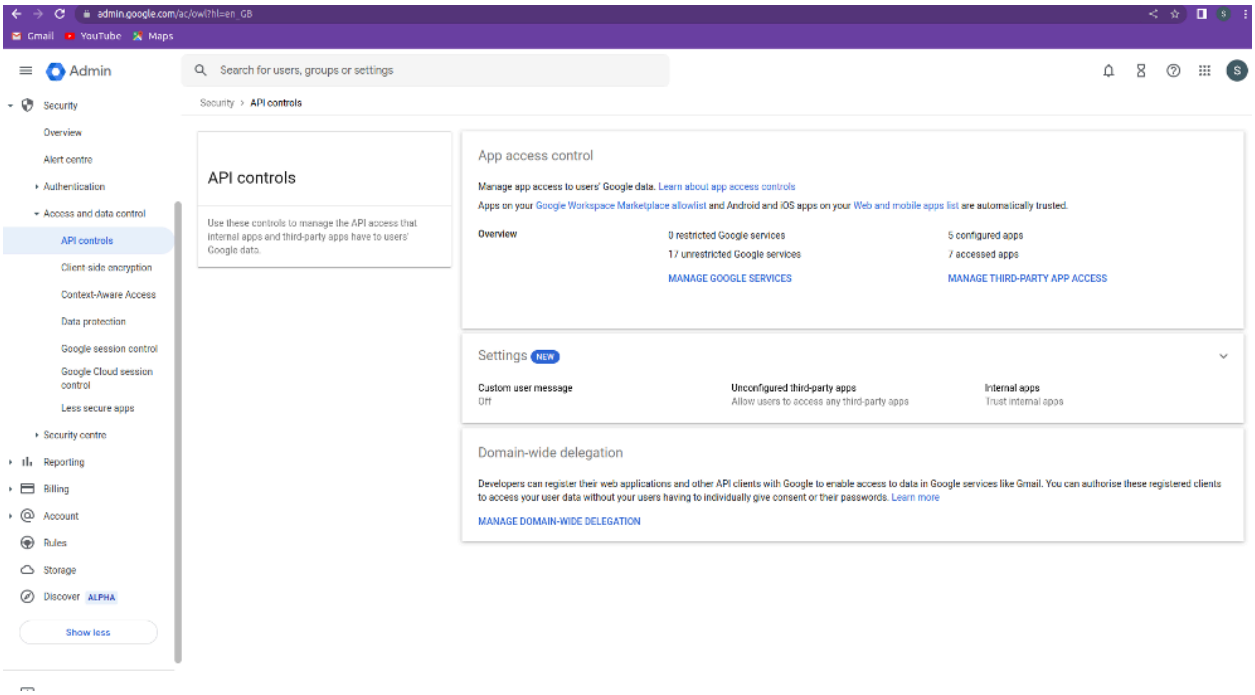
Configure Google Drive for API-Based Data Protection

To configure a new instance for Google Drive:

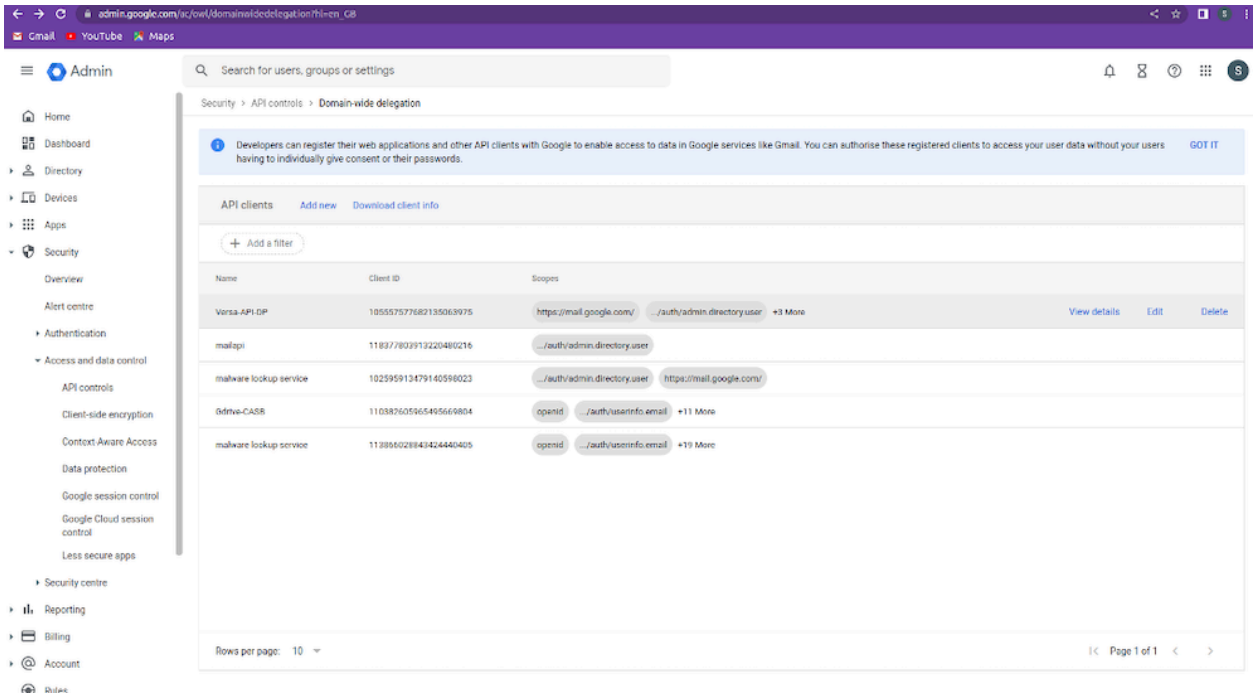
1. Log in to the admin console using administrator credentials.



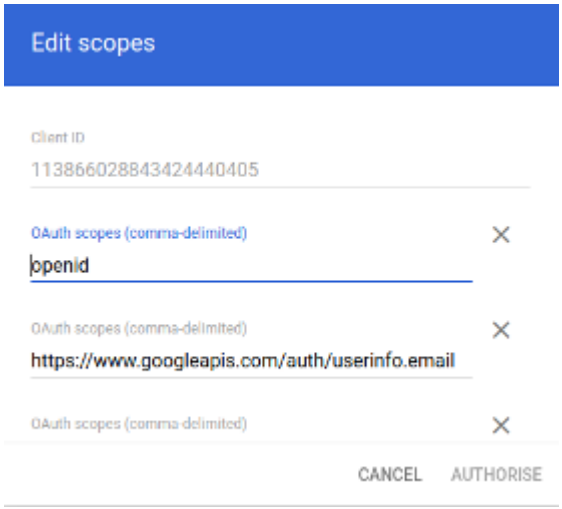
2. Select Security > Access and Data Control > API controls in the left menu bar, and then click Manage Domain-wide Delegation.



3. In the Domain-wide Delegation pane, click Add New.



4. Enter information for the following fields.



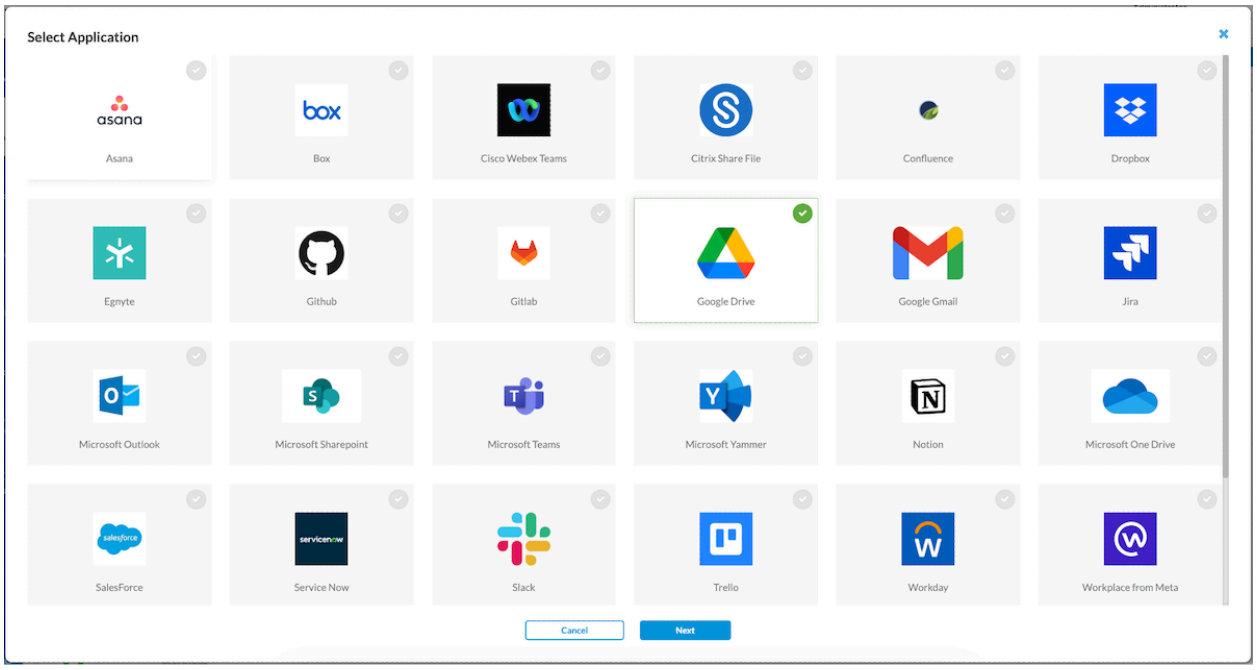
Field	Description
Client ID	Add client ID 113866028843424440405.
Scopes	Add the following scopes; ◦ https://www.googleapis.com/auth/admin.datatransfer ◦ https://www.googleapis.com/auth/

Field	Description
	admin.directory.domain.readonly ◦ https://www.googleapis.com/auth/admin.directory.group ◦ https://www.googleapis.com/auth/admin.directory.group.member ◦ https://www.googleapis.com/auth/admin.directory.group.member.readonly ◦ https://www.googleapis.com/auth/admin.directory.group.readonly ◦ https://www.googleapis.com/auth/admin.directory.user ◦ https://www.googleapis.com/auth/admin.directory.user.readonly ◦ https://www.googleapis.com/auth/admin.directory.user.security ◦ https://www.googleapis.com/auth/admin.reports.audit.readonly ◦ https://www.googleapis.com/auth/cloud-platform ◦ https://www.googleapis.com/auth/drive ◦ https://www.googleapis.com/auth/drive.appdata ◦ https://www.googleapis.com/auth/drive.file ◦ https://www.googleapis.com/auth/drive.metadata ◦ https://www.googleapis.com/auth/drive.metadata.readonly ◦ https://www.googleapis.com/auth/drive.photos.readonly ◦ https://www.googleapis.com/auth/drive.readonly ◦ https://www.googleapis.com/auth/userinfo.email ◦ https://www.googleapis.com/auth/userinfo.profile ◦ openid

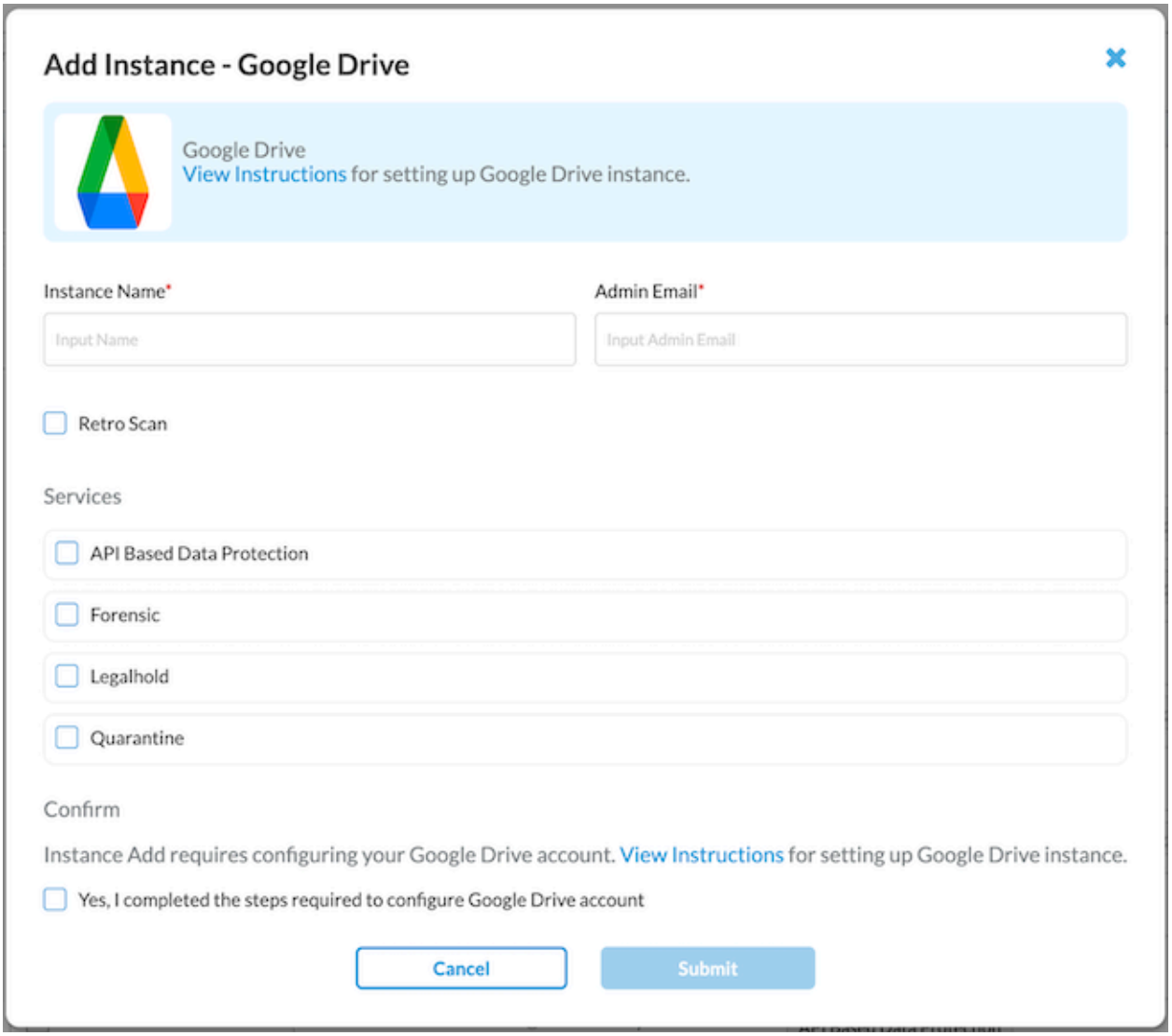
5. Click Authorize.

Configure a Google Drive Connector

1. Navigate to "Configure" > “Advanced Security” > “API Based Data Protection” > “Connectors”.
2. Click the + Add icon, select Google Drive, then click Next.



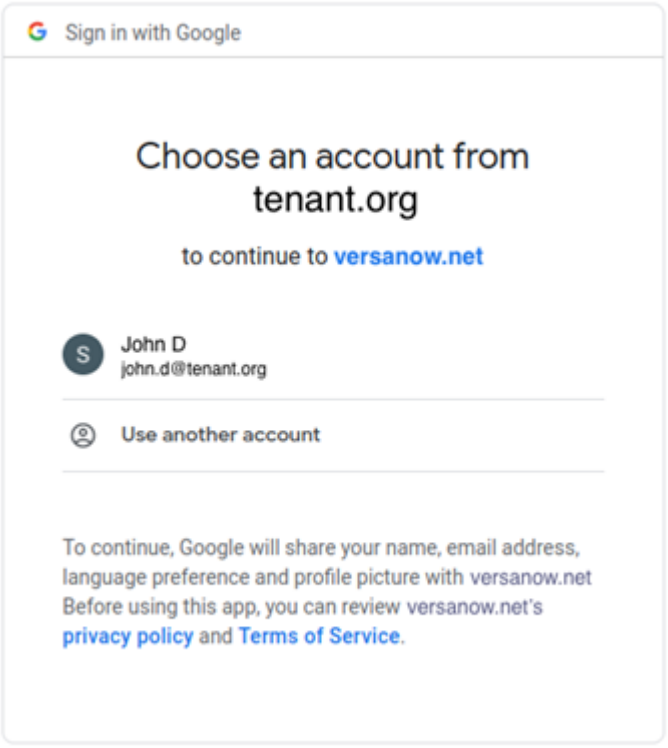
3. In the Add Instance window, enter information for the following fields.



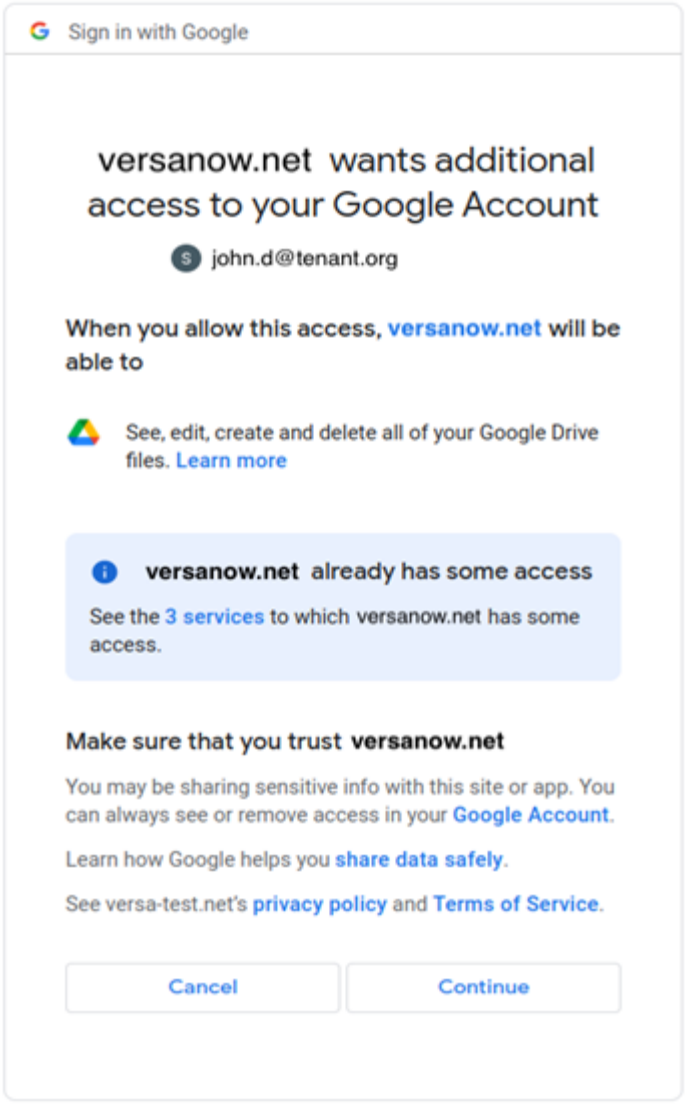
Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email	Enter the email address of the Google administrator account.
Retro Scan	Click to scan and protect all the files that are present on Google Drive at the time of connector creation.
Services	Select the services to use for the instance. ◦ API-Based Data Protection—Scan and protect content.

Field	Description
	◦ Forensic—Use this instance for forensics. ◦ Legal Hold—Use this instance for legal hold. ◦ Quarantine—Use this instance for quarantine files.
Confirm	Click to confirm that the steps required to configure the Google Drive account are complete.

4. Click Submit.
5. After adding the instance, select Grant Access to start the OAuth2 process of granting access to the Versa API data protection cloud. This will open a login prompt for the Google account.



6. Use Google Drive Administrator credentials to log in. The next screen will show the permissions that the Versa service will require to scan and monitor the Google Drive account. Click Accept to grant access to the Google Drive account.



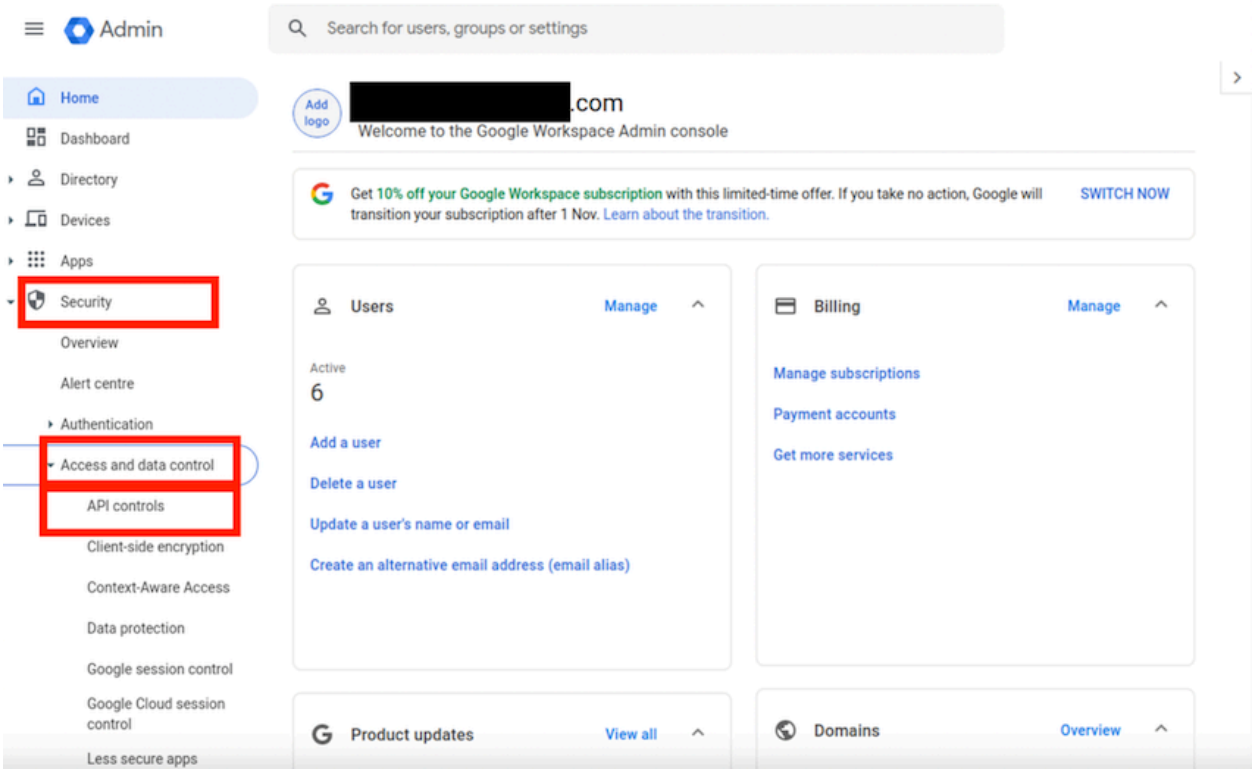
Gmail API-Based Data Protection

This section describes how to configure the Google Gmail application for API-based data protection.

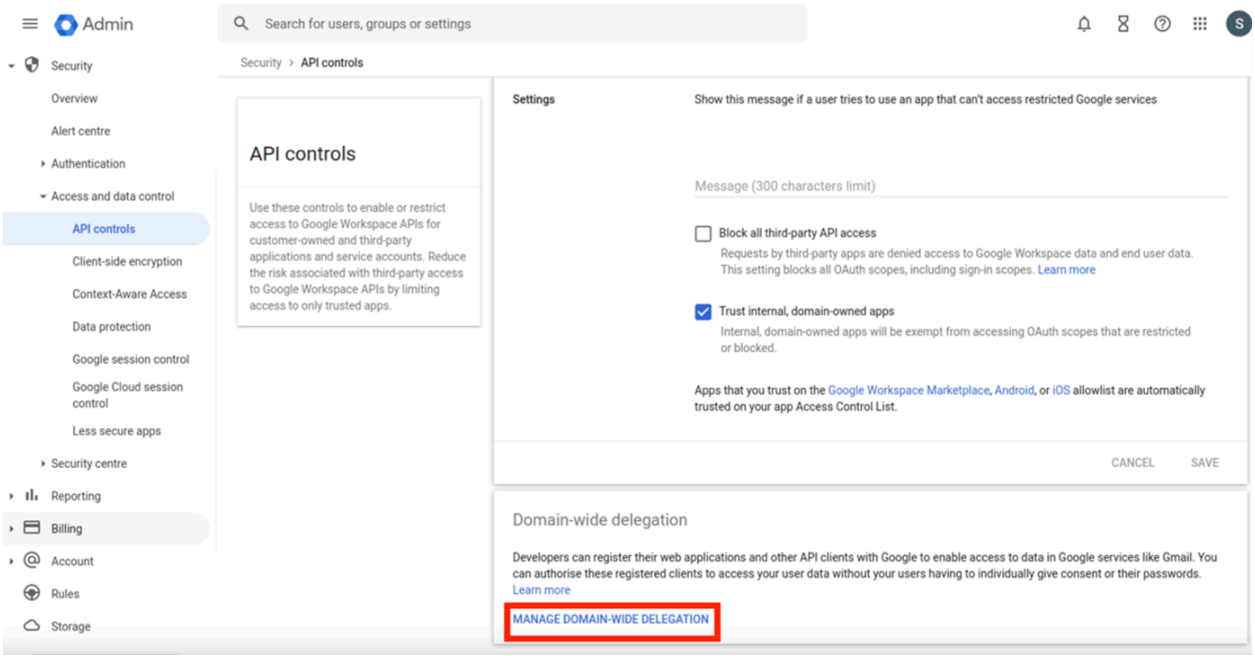
Configure Gmail for API-Based Data Protection

To configure a new instance for Gmail:

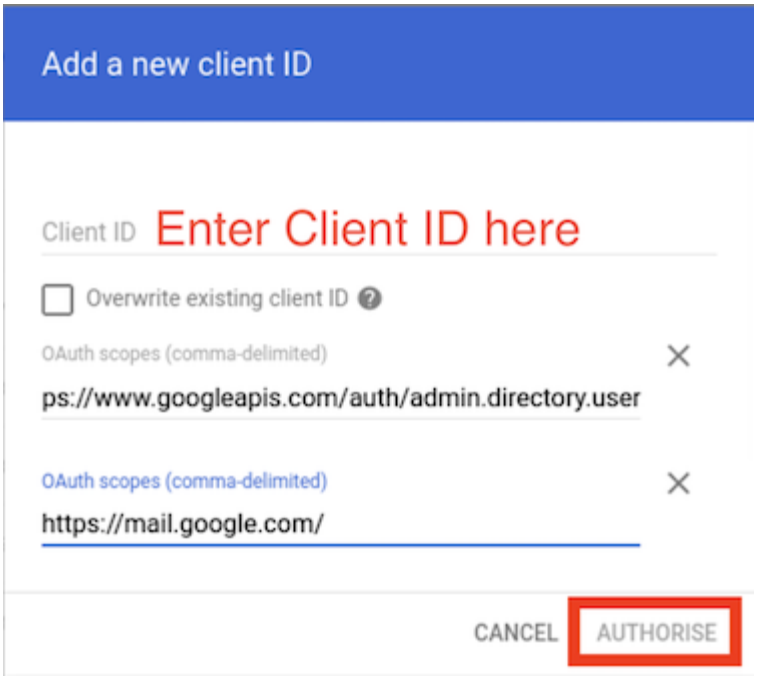
1. Login to https://admin.google.com as an administrator.
2. Click Security > Access and data control > API controls in the left menu bar.



3. In the Domain-wide Delegation section, click Manage Domain-wide Delegation.



4. In the API Clients Label, click Add New and enter information for the following fields.



Field	Description
Client ID	Enter the client ID 105557577682135063975.
OAuth Scopes	Enter two OAuth scopes: ◦ https://mail.google.com/ ◦ https://www.googleapis.com/auth/admin.directory.user

5. Click Authorize.

Configure a Gmail Connector

1. Under API-Based Data Protection, select Application > Gmail.
2. In the Add Instance window, enter information for the following fields.

Field	Description
Instance Name (Required)	Enter a name for the instance.
Google Directory Admin Email (Required)	Enter an email address of the Google Directory administrator account.
Google Mail Admin Email (Required)	Enter an email address of the Google Mail

Field	Description
	administrator account.
Services	Select the services to use for the instance. ◦ API-Based Data Protection—Scan and protect content.
Confirm	Click to confirm that the steps required to configure the Google Gmail account are complete.

3. Click Submit.
4. After the instance is added, select Grant Access to start the OAuth2 process of granting access to the Versa API data protection cloud. Use Google Administrator credentials to log in and grant access.

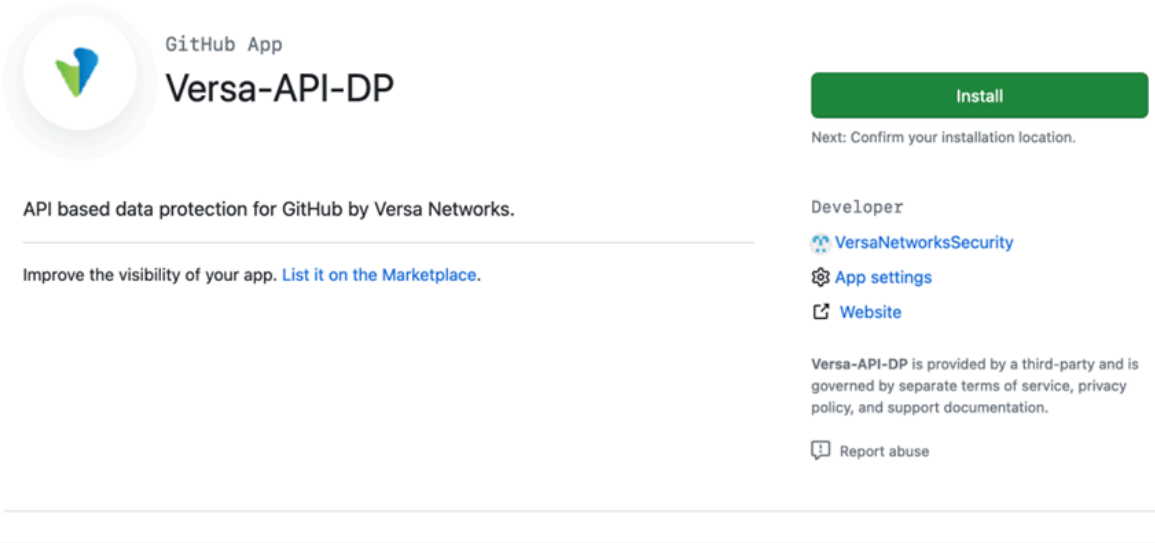
GitHub API-Based Data Protection

This section describes how to configure the GitHub application for API-based data protection.

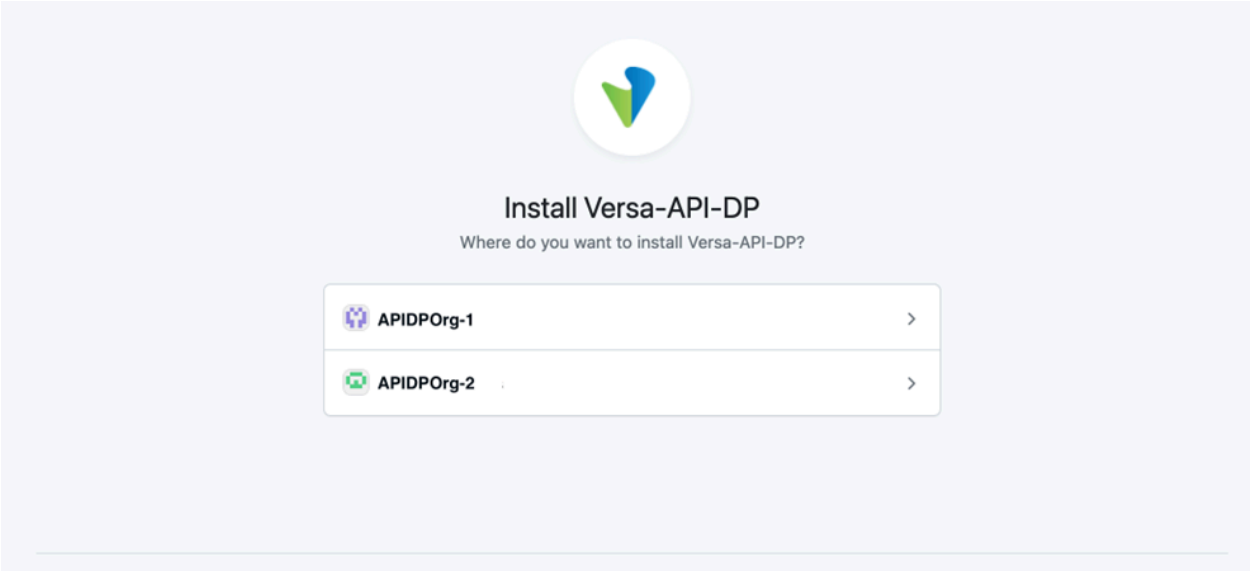
Configure GitHub for API-Based Data Protection

To configure a new instance for GitHub:

1. Browse to https://github.com/apps/saas-github
2. Click Install.



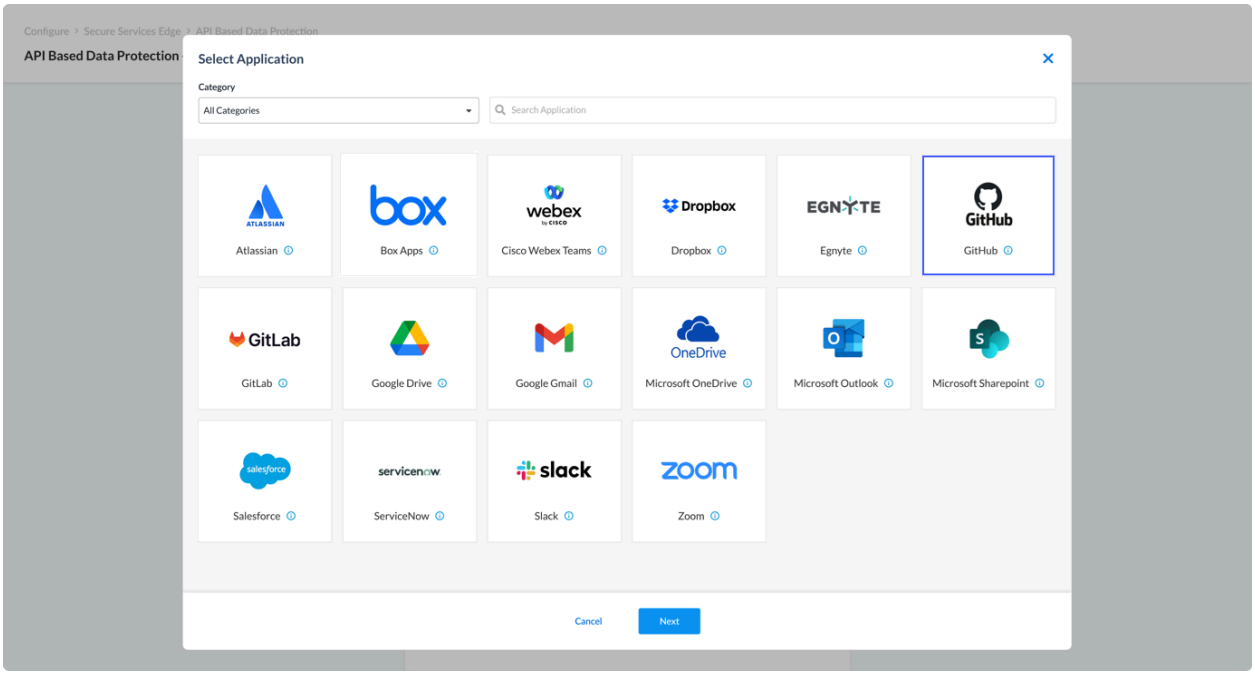
3. Select the user, team, or organization to install GitHub.



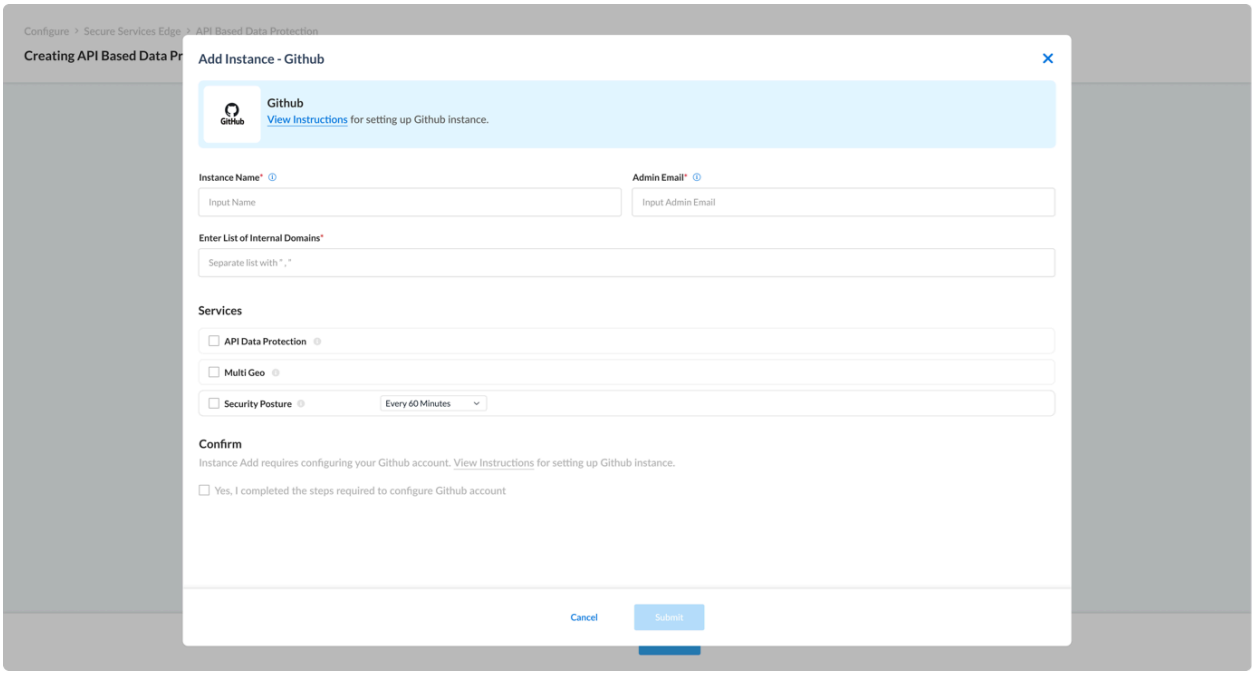
4. Grant permission to all or selected repository and click Install.

Configure a GitHub Connector

1. Under API-Based Data Protection, select Application > GitHub.



2. In the Add Instance window, enter information for the following fields.



Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email (Required)	Enter an email address of the GitHub administrator account.
Services	Select the services to use for the instance. ◦ API-Based Data Protection—Scan and protect content. ◦ Multi Geo—Use this instance for multpile geographical areas. ◦ Security Posture—Use this instance for security posture.
Confirm	Click to confirm that the steps required to configure the GitHub account are complete.

3. Click Submit.
4. After the instance is added, select Grant Access to start the OAuth2 process of granting access to the Versa API data protection cloud. Use GitHub Administrator credentials to log in and grant access.

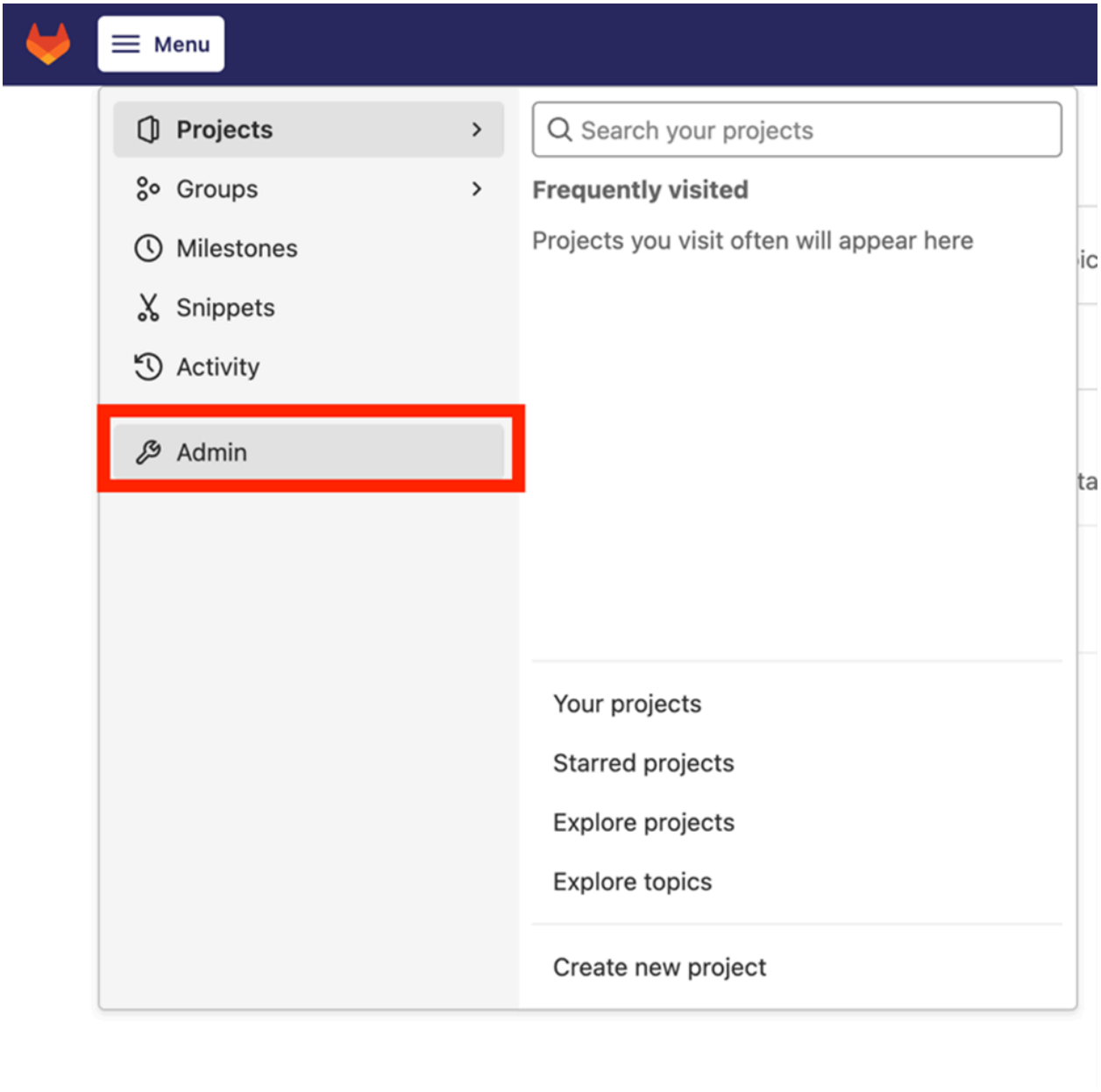
GitLab API-Based Data Protection

This section describes how to configure the GitLab application for API-based data protection.

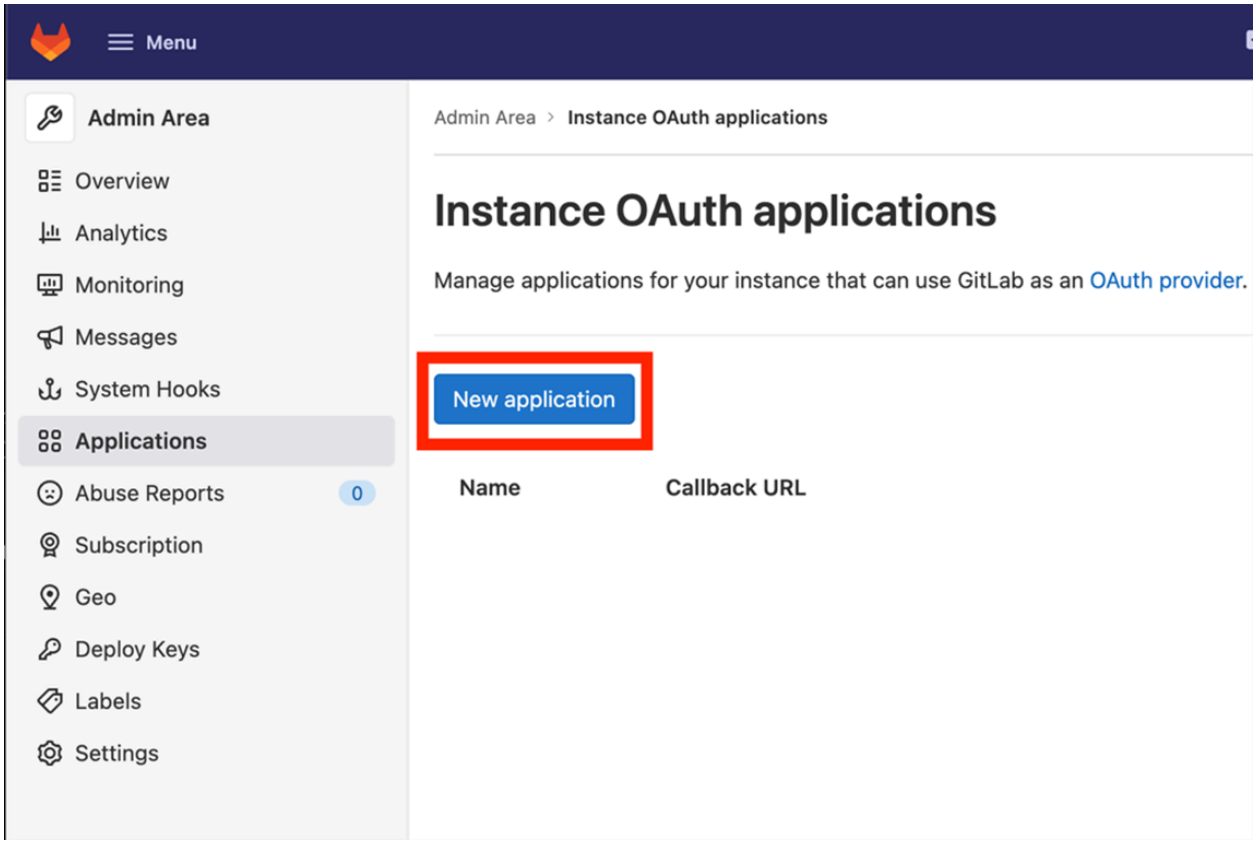
Configure GitLab for API-Based Data Protection

To configure a new instance for GitLab:

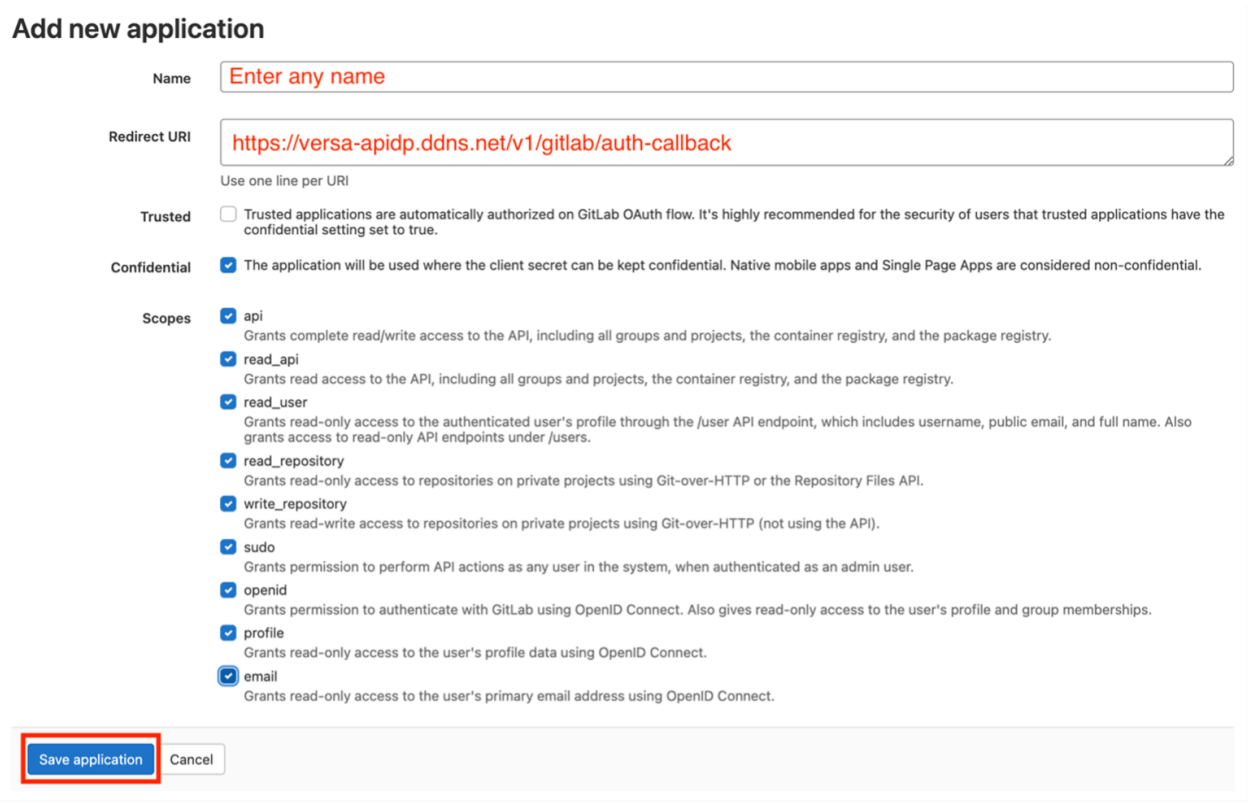
1. Login to GitLab as an administrator.
2. Click the Menu icon and select Admin.



3. In the Admin Area menu bar, select Applications, and then click New Application.

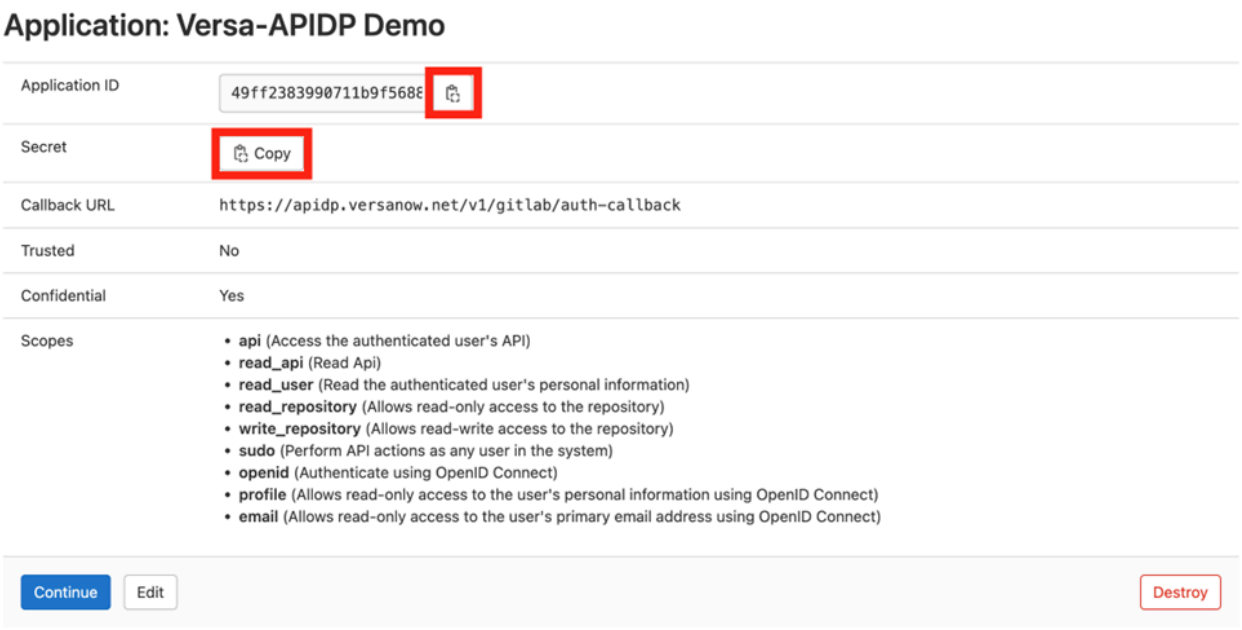


4. In the Add New Application popup, enter information for the following fields and then click Save Application.



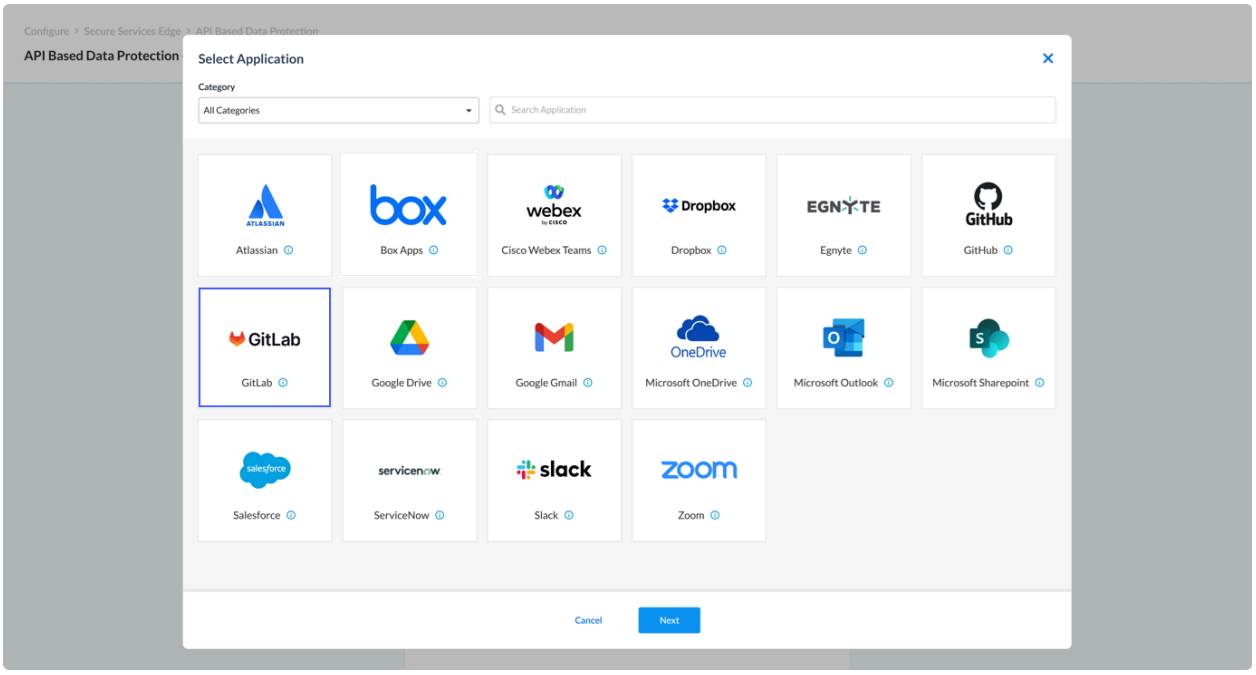
Field	Description
Name	Enter a name for the application.
Redirect URI	Enter the redirect URI https://apidp.versanow.net/v1/gitlab/auth-callback.
Trusted	NA
Confidential	Select confidential.
Scopes	Click the checkbox to select all scopes.

5. Note down the application ID and click Copy icon to copy the secret value. Save this information to use while creating GitLab connector.

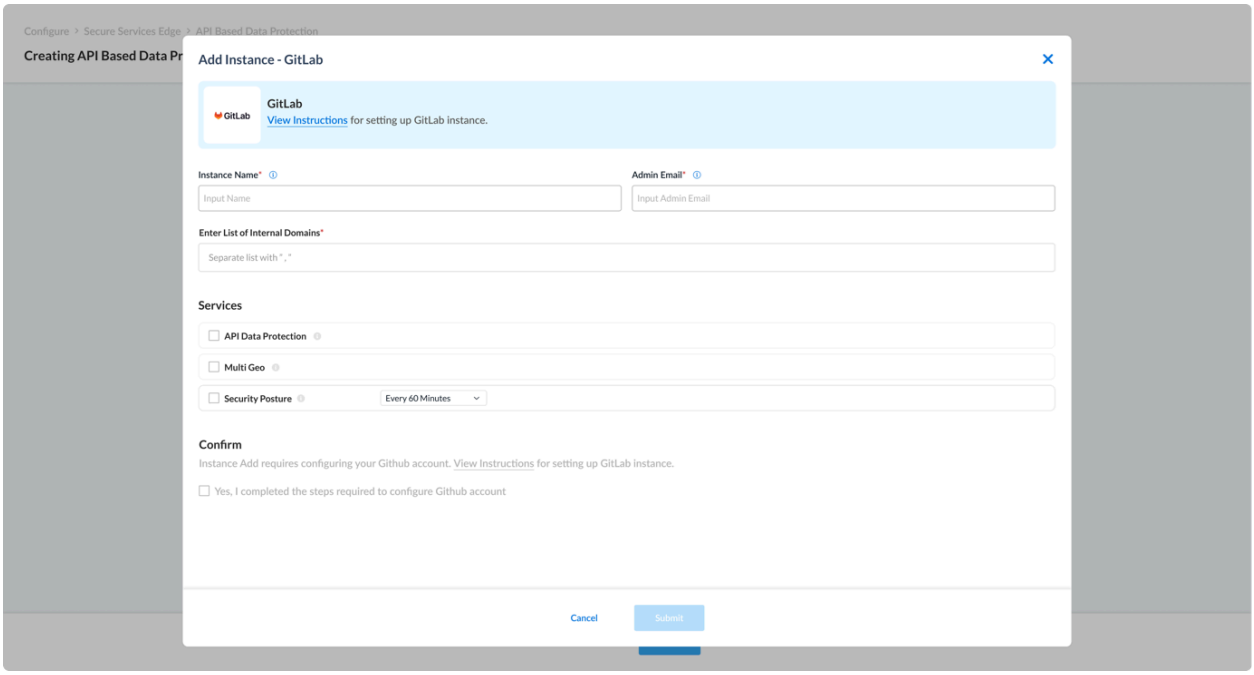


Configure a GitLab Connector

1. Under API-Based Data Protection, select Application > GitLab.



2. In the Add Instance window, enter information for the following fields.



Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email (Required)	Enter an email address of the Cisco Webex administrator account.
Domain Name (Required)	Enter the domain name of the GitLab instance. For example, gitlab.companyname.com)
Services	Select the services to use for the instance. ◦ API-Based Data Protection—Scan and protect content. ◦ Multi Geo—Use this instance for multiple geographic locations. ◦ Security Posture—Use this instance for security posture.
Confirm	Click to confirm that the steps required to configure the GitLab account are complete.

3. Click Submit.
4. After the instance is added, select Grant Access to start the OAuth2 process of granting access to the Versa API data protection cloud. Use GitLab Administrator credentials to log in and grant access.

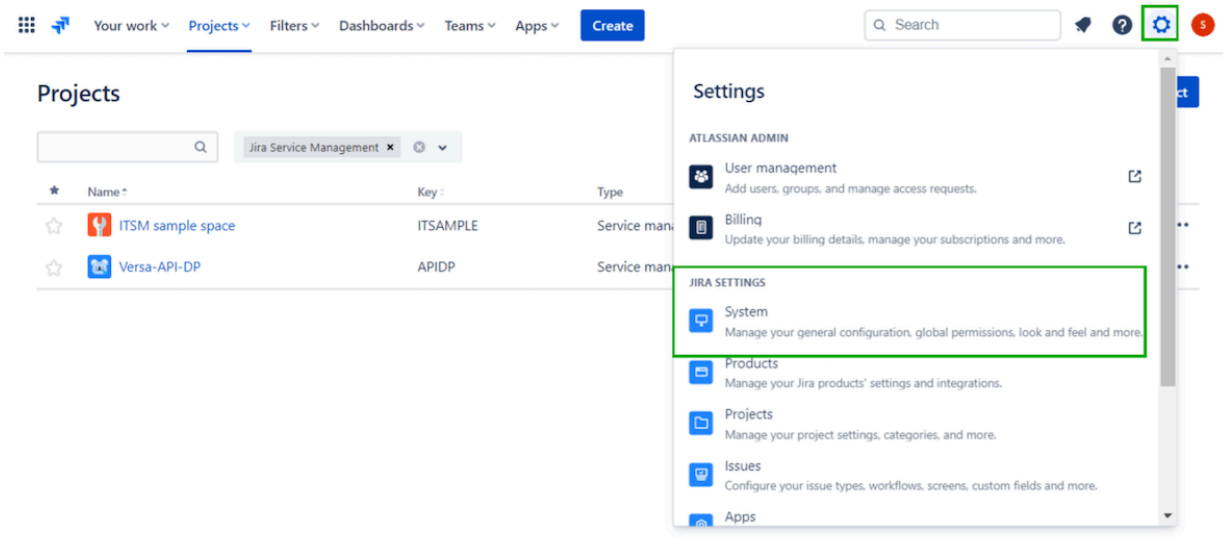
Jira API-Based Data Protection

This section describes how to configure the Jira application for API-based data protection.

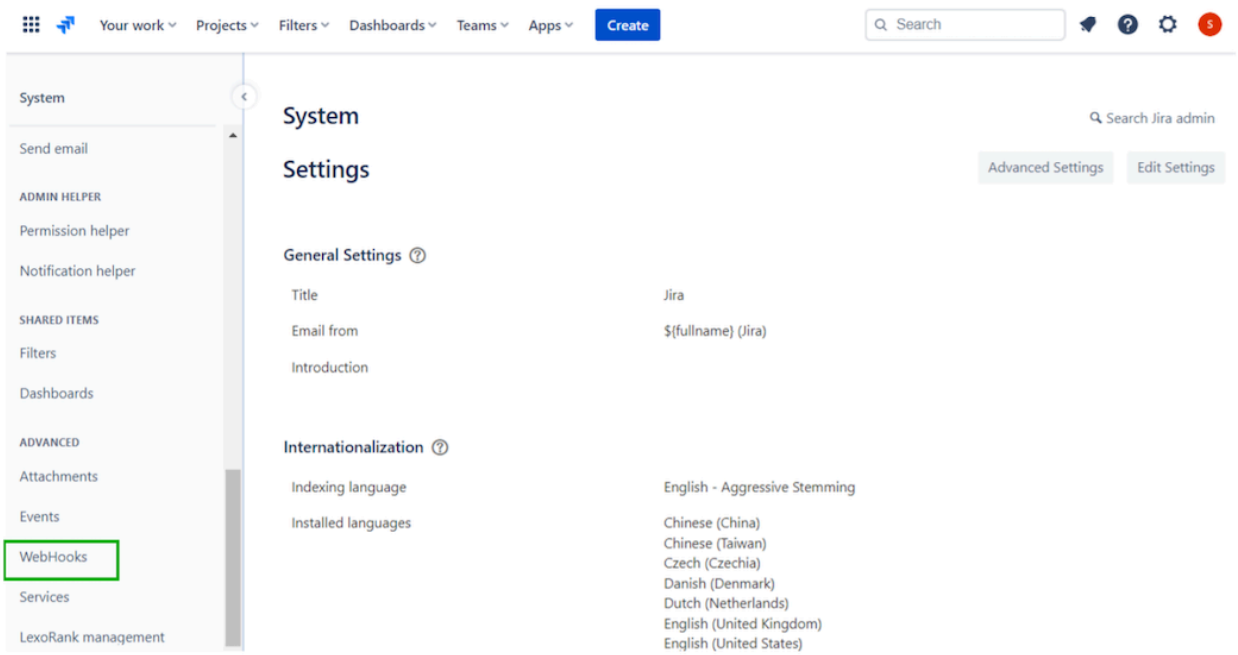
Configure Jira for API-Based Data Protection

To configure Jira for API-based data protection:

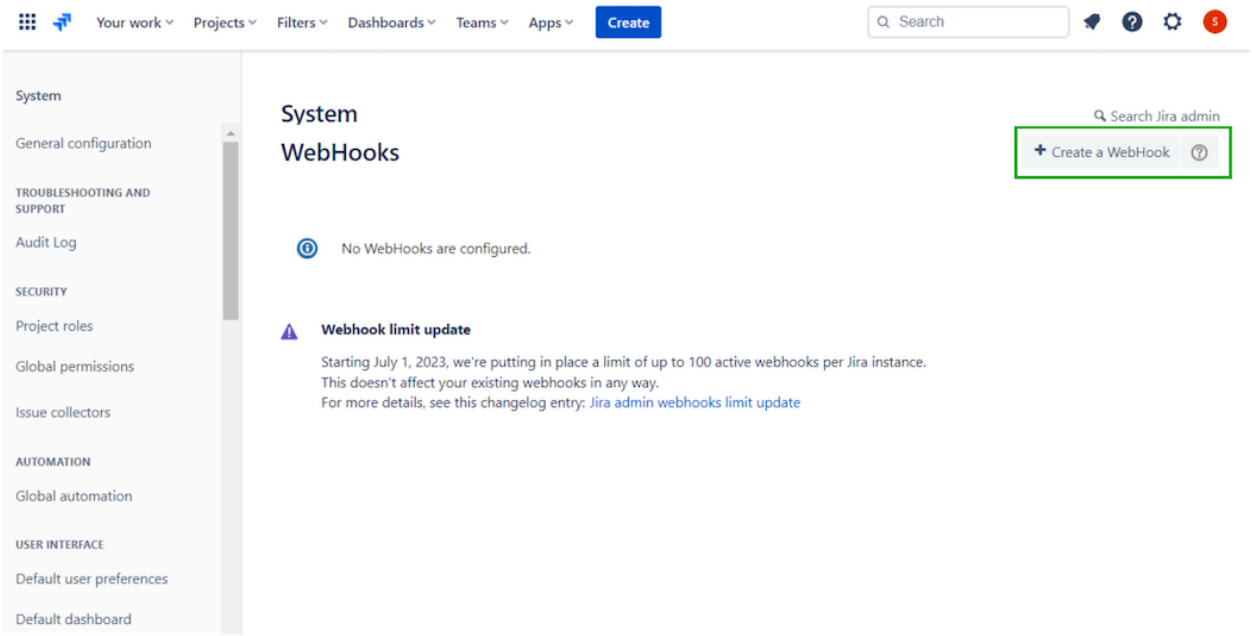
1. Login with administrator credentials at http://atlassian.com and navigate to any Jira product. Click on the Gear icon in the screen's upper-right corner and select "System" under "JIRA SETTINGS."



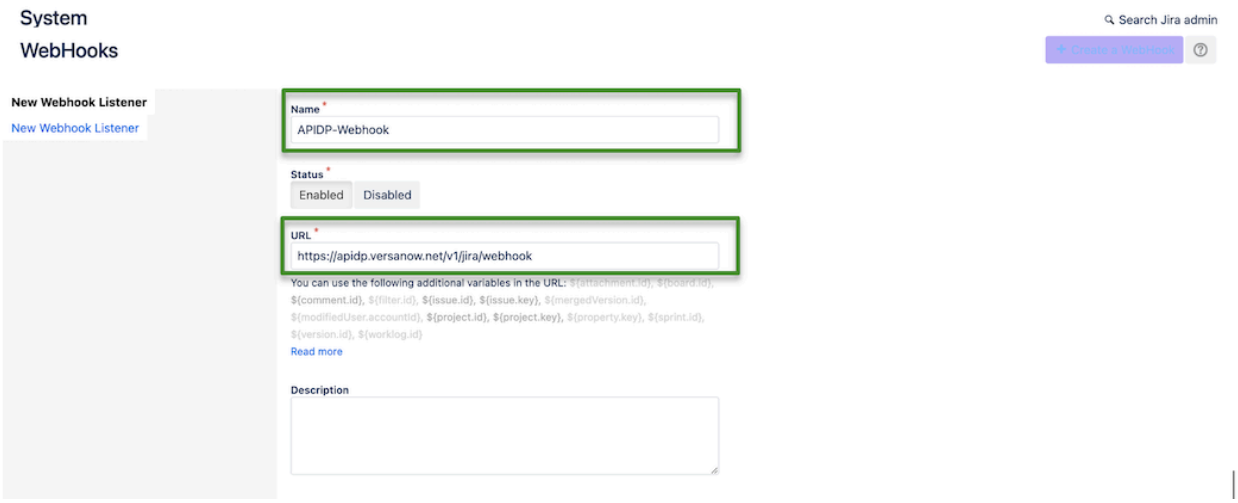
2. In the left menu bar under Advanced, click WebHooks.



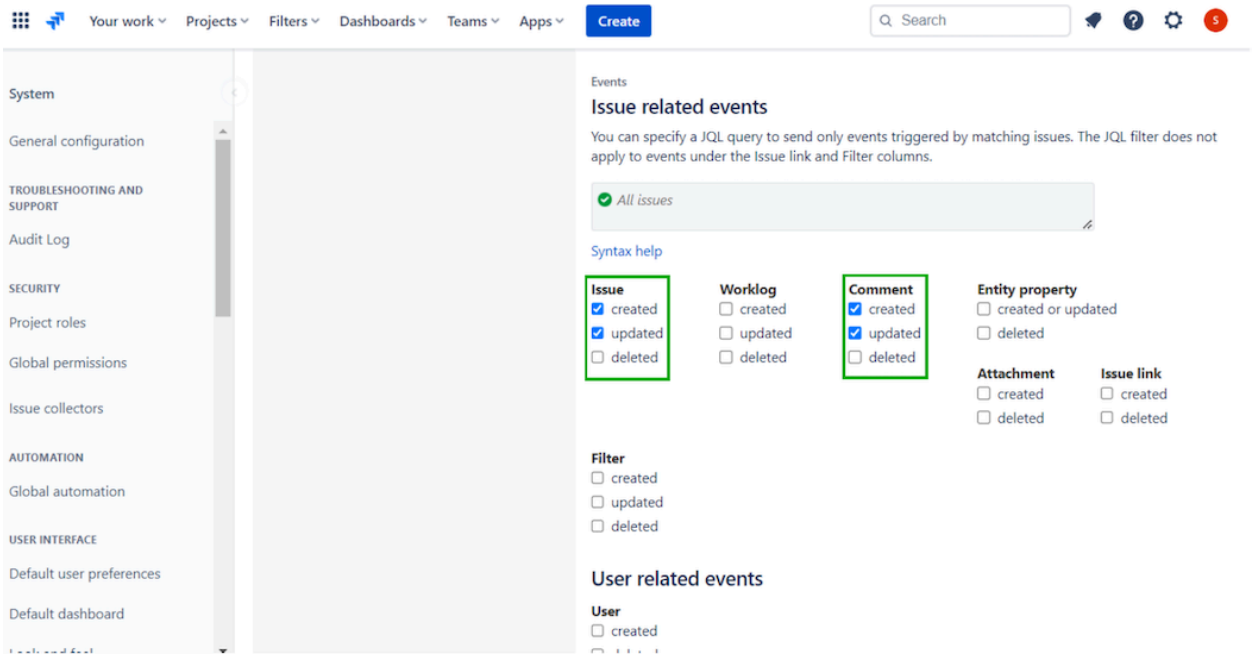
3. Click + Create a WebHook in the upper-right corner.



4. Enter a name for the webhook and enter the endpoint URL https://apidp.versanow.net/v1/jira/webhook under the URL.

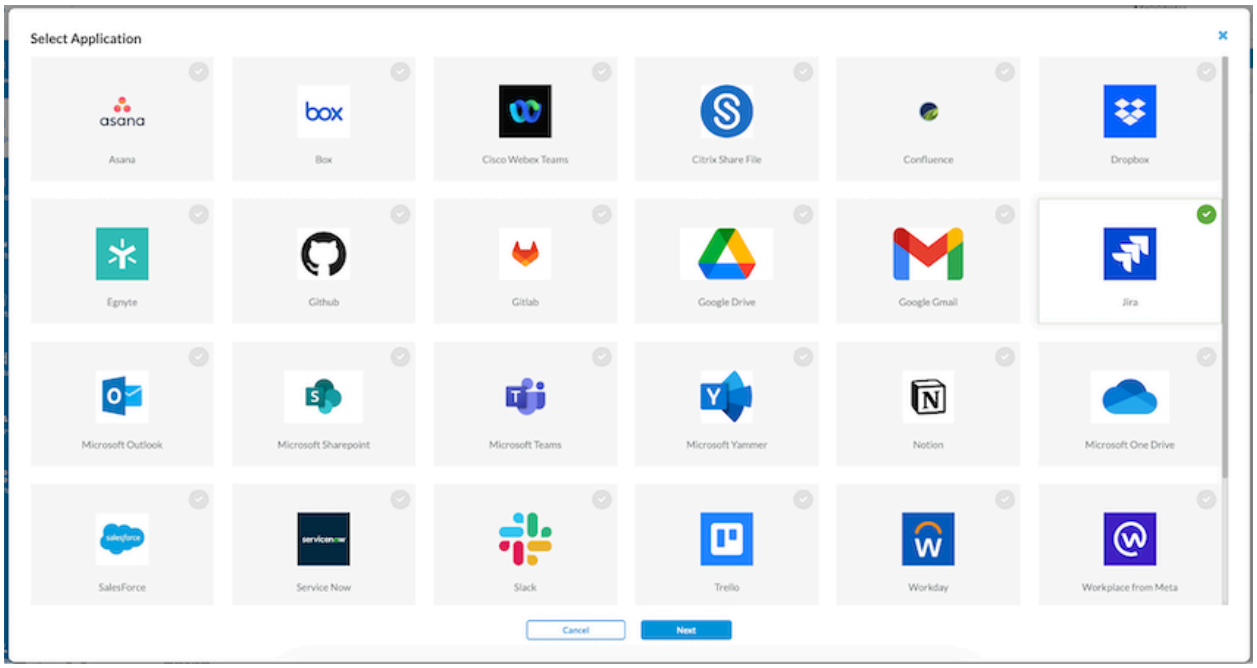


5. Select the events that trigger the webhook and click Create at the bottom of the screen.

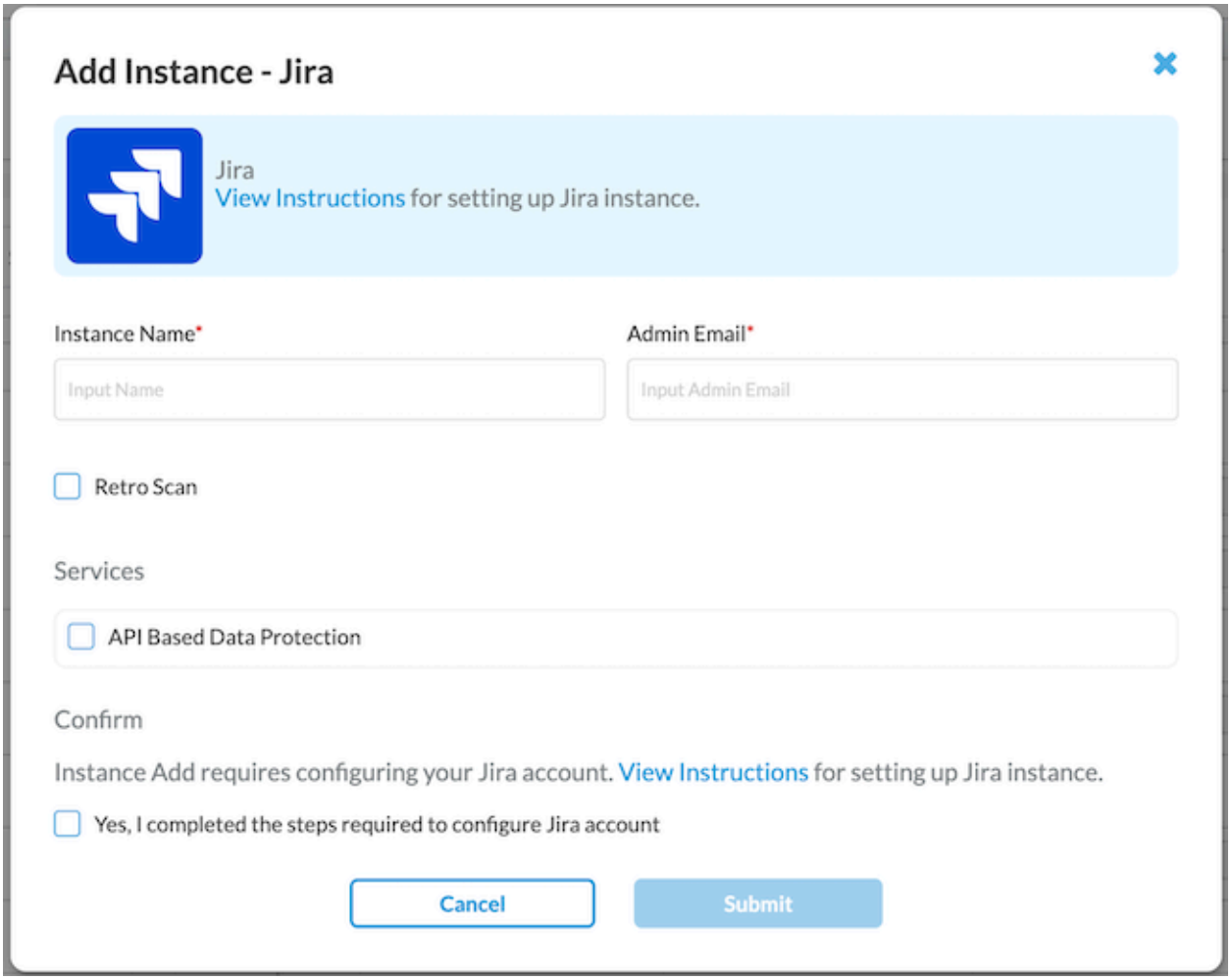


Configure a Jira Connector

1. Navigate to Configure > Advanced Security > API Based Data Protection > Connectors.
2. Click the + Add icon, select Jira, then click Next.



3. In the Add Instance window, enter information for the following fields.



Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email	Enter the email address of the Jira administrator account.
Retro Scan	Click to scan and protect all the files that are present on Jira at the time of connector creation.
Services	Select the services to use for the instance. ◦ API-Based Data Protection—Scan and protect content.
Confirm	Click to confirm that the steps required to configure the Jira account are complete.

4. After adding the instance, click “Grant Access” to start the OAuth 2.0 process of granting access to the Versa API-DP cloud. This will open a login prompt for the Jira account. Use administrator credentials to log in and grant access.

Microsoft Outlook API-Based Data Protection

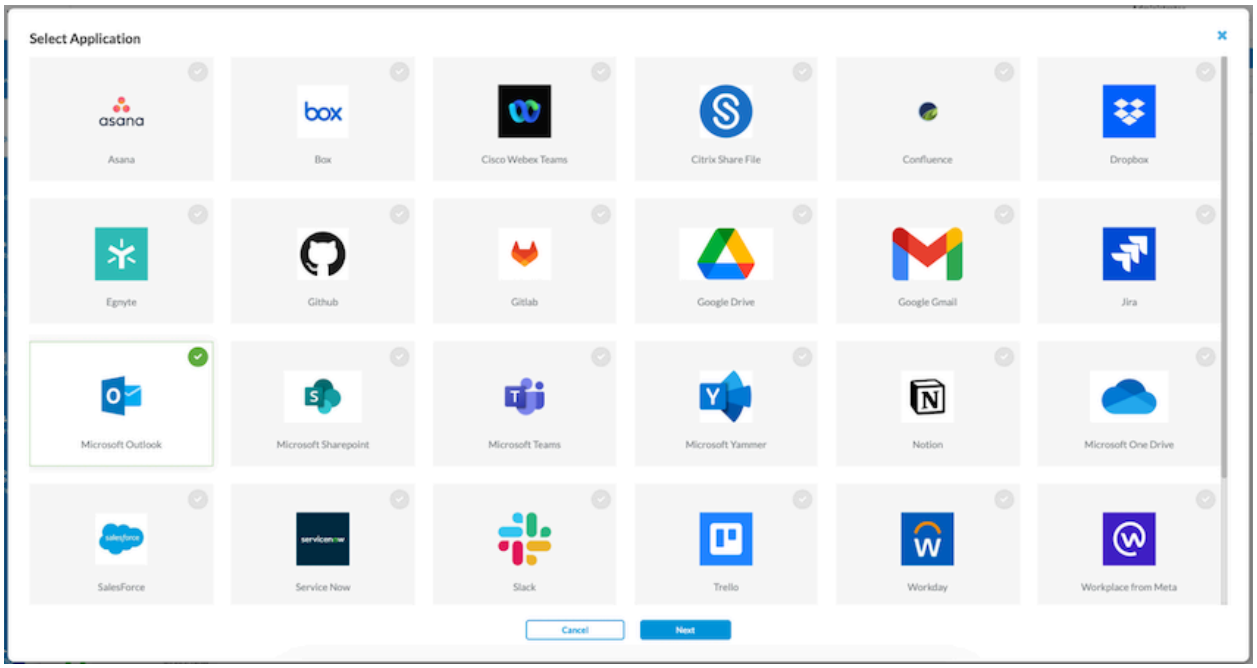
This section describes how to configure the Microsoft Outlook application for API-based data protection.

Configure Microsoft Outlook for API-Based Data Protection

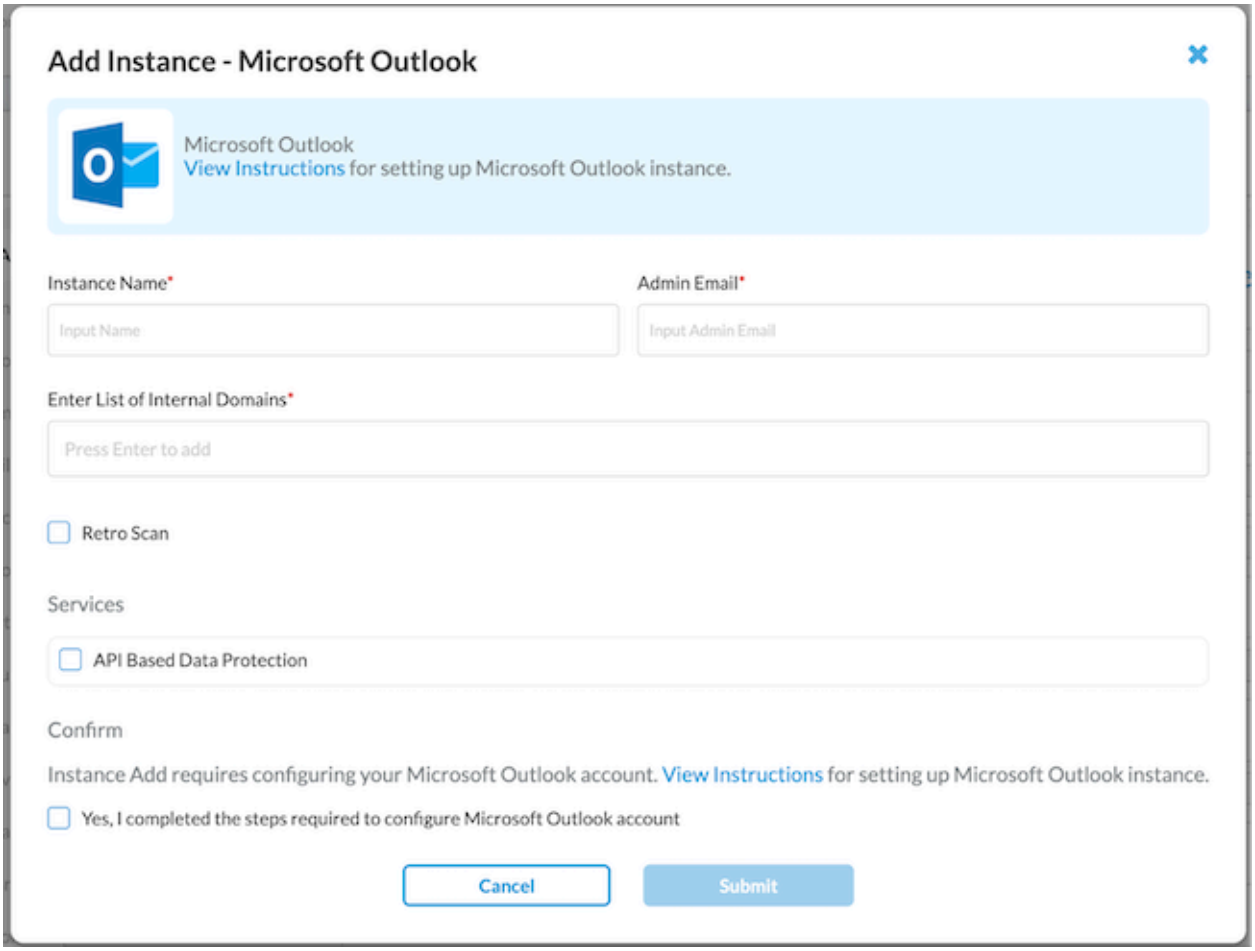
For Microsoft Outlook, no configuration is required.

Configure a Microsoft Outlook Connector

1. Navigate to "Configure" > “Advanced Security” > “API Based Data Protection” > “Connectors”.
2. Click the ✚Add icon, select Jira, then click Next.



3. In the Add Instance window, enter information for the following fields.



Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email (Required)	Enter the email address of the Microsoft Outlook administrator account.
Enter List of Internal Domains	Enter the domains configured for the organization.
Retro Scan	Click to scan and protect all the messages and attachments that are present on Microsoft Outlook at the time of connector creation.
Services	Select the services to use for the instance. ◦ API-Based Data Protection—Scan and protect content.
Confirm	Click to confirm that the steps required to configure the Microsoft Outlook account are complete.

4. Click Submit.
5. After the instance is added, select Grant Access to start the OAuth2 process of granting access to the Versa API data protection cloud. This will open a login prompt for the Microsoft account. Use Microsoft Administrator credentials to log in and grant access.

Microsoft OneDrive API-Based Data Protection

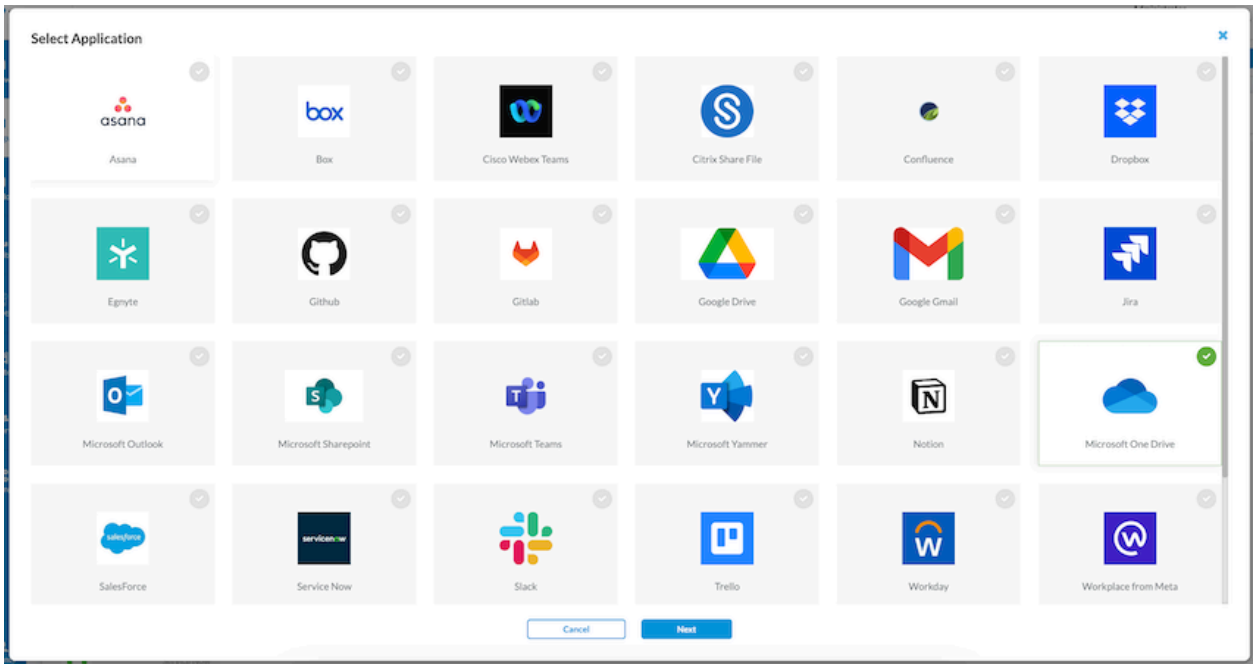
This section describes how to configure the Microsoft OneDrive application for API-based data protection.

Configure Microsoft OneDrive for API-Based Data Protection

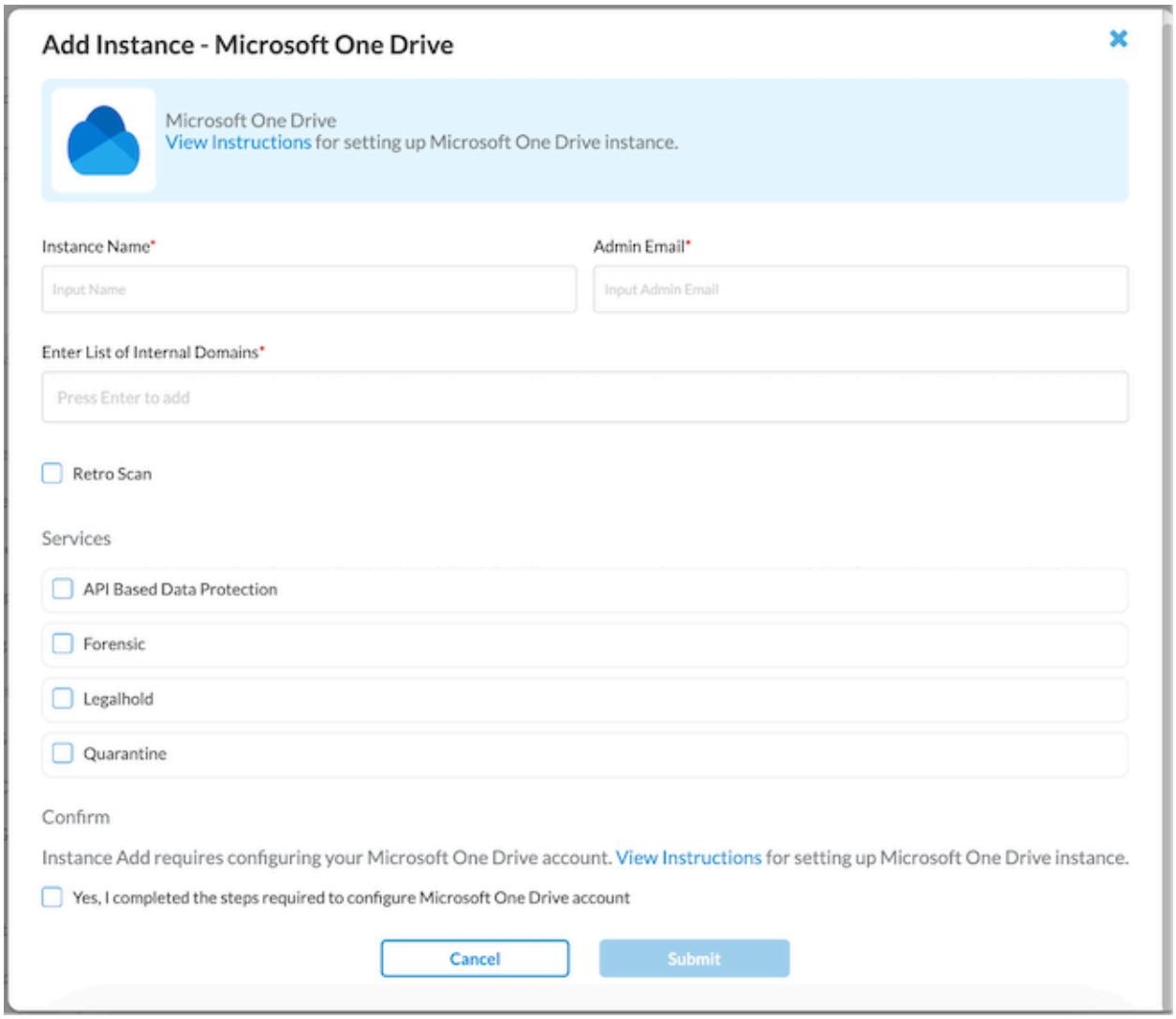
For Microsoft OneDrive, no configuration is required.

Configure a Microsoft OneDrive Connector

1. Navigate to "Configure" > “Advanced Security” > “API Based Data Protection” > “Connectors”.
2. Click the + Add icon, select Jira, then click Next.



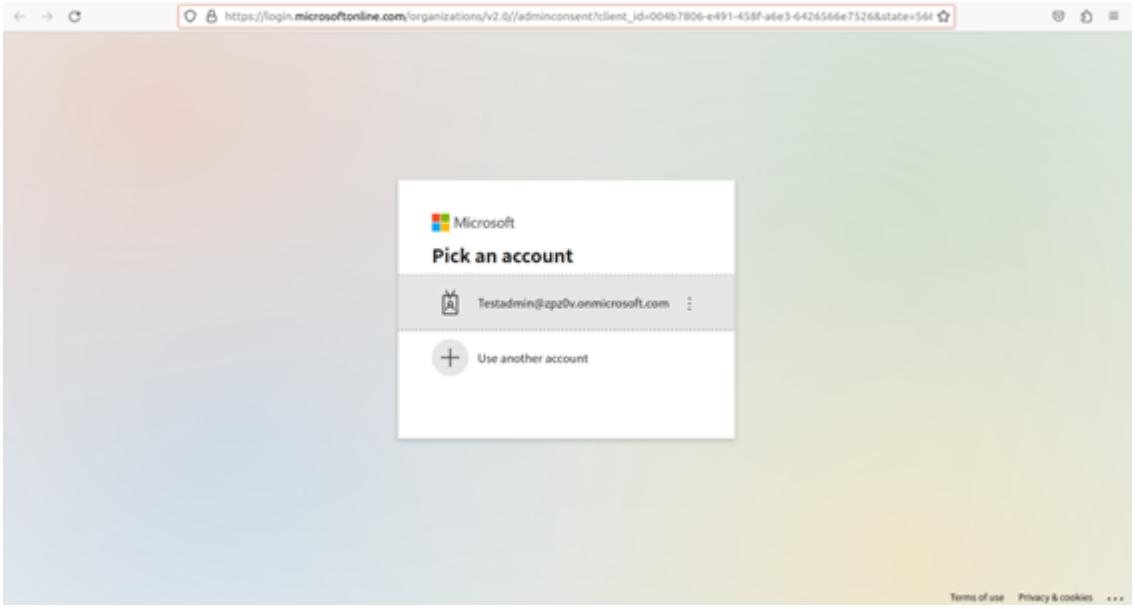
3. In the Add Instance window, enter information for the following fields.



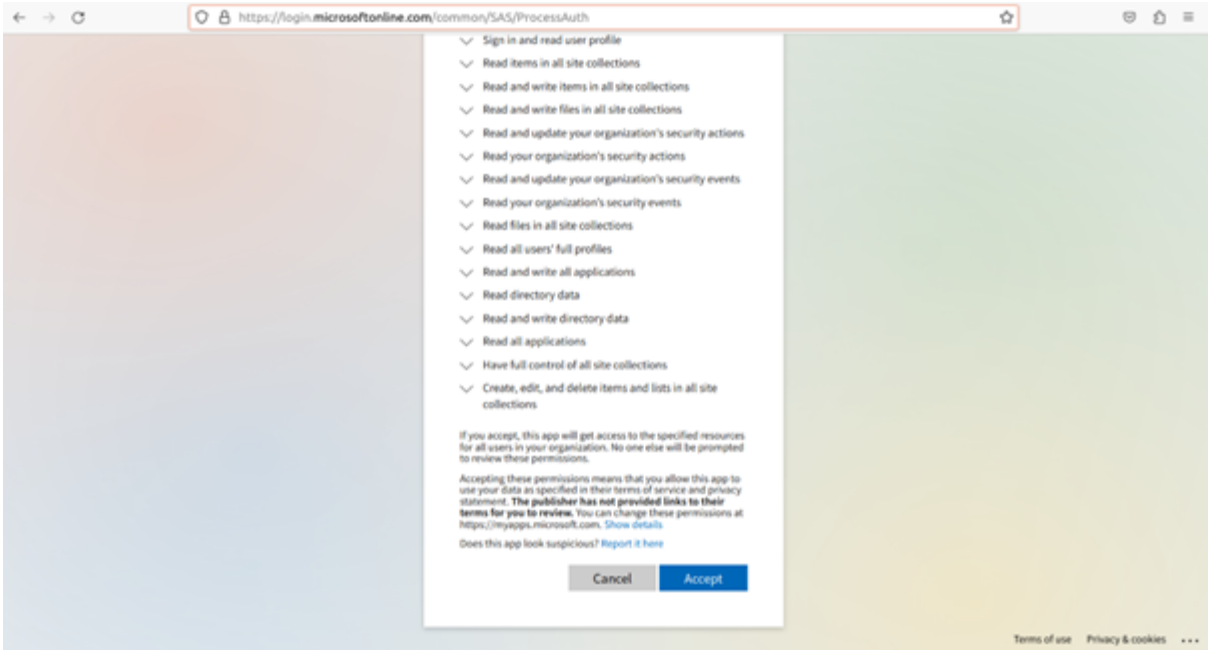
Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email (Required)	Enter an email address of the Microsoft OneDrive administrator account.
Enter List of Internal Domains	Enter domains configured for the organization.
Retro Scan	Click to scan and protect all the files that are present on Microsoft OneDrive at the time of connector creation.
Services	Select the services to use for the instance. ◦ API-Based Data Protection—Scan and protect

Field	Description
	content. ◦ Forensic: Use this instance for Forensics. ◦ Legal Hold—Use this instance for legal hold. ◦ Quarantine—Use this instance for quarantine files. ◦ Security Posture—Use this instance to access security risk and manage application's security posture..
Confirm	Click to confirm that the steps required to configure the Microsoft OneDrive account are complete.

4. Click Submit.
5. After adding the instance, select Grant Access to start the OAuth2 process of granting access to the Versa API data protection cloud. This will open the login prompt for the Microsoft account.



6. Use Microsoft OneDrive Administrator credentials to log in. The next screen will show the permissions that the Versa service will require to scan and monitor the OneDrive account. Click Accept to grant access to Microsoft OneDrive account.



Microsoft SharePoint API-Based Data Protection

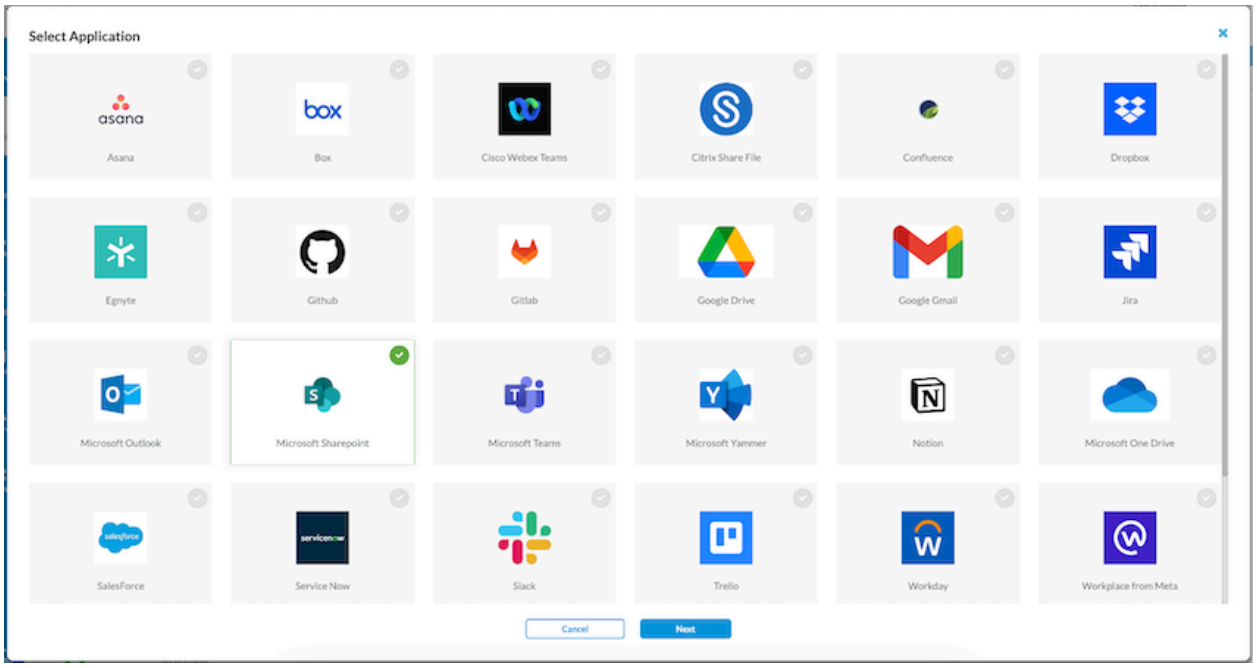
This section describes how to configure the Microsoft SharePoint application for API-based data protection.

Configure Microsoft SharePoint for API-Based Data Protection

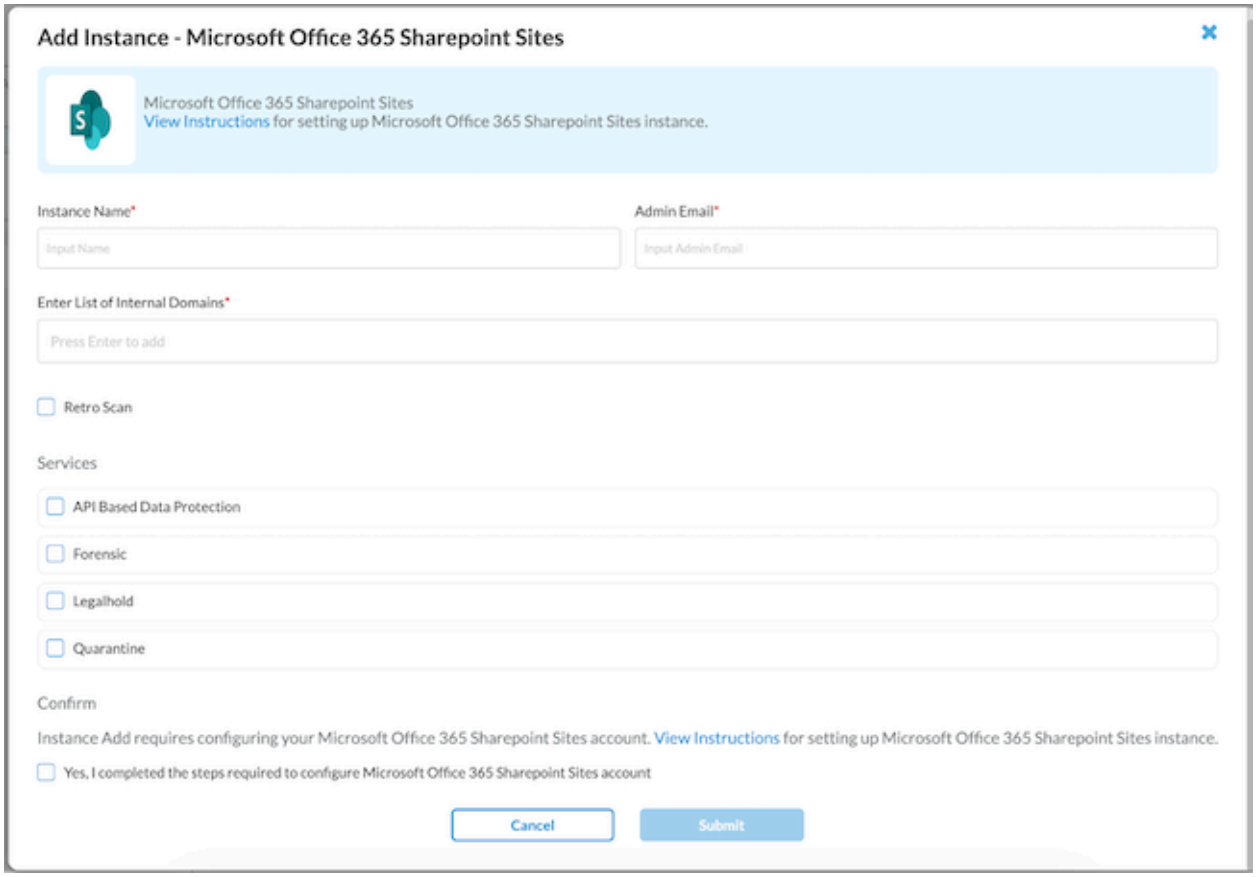
For Microsoft SharePoint, no configuration is required.

Configure a Microsoft SharePoint Connector

1. Navigate to "Configure" > “Advanced Security” > “API Based Data Protection” > “Connectors”.
2. Click the + Add icon, select Jira, then click Next.

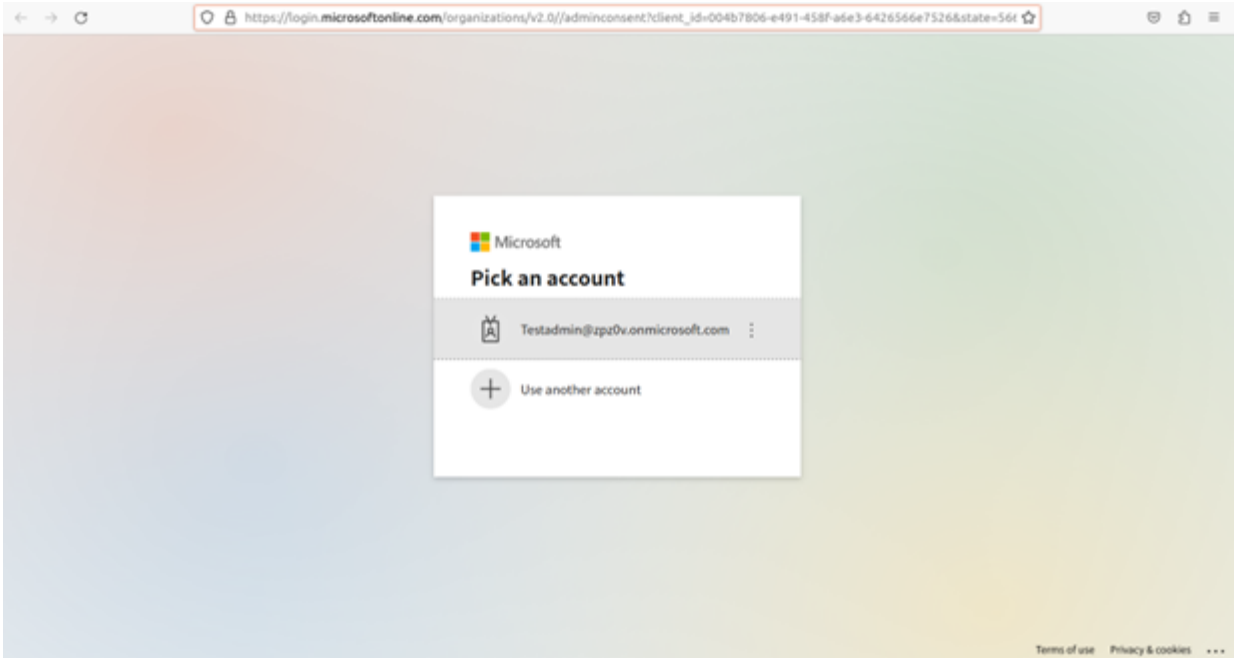


3. In the Add Instance window, enter information for the following fields.

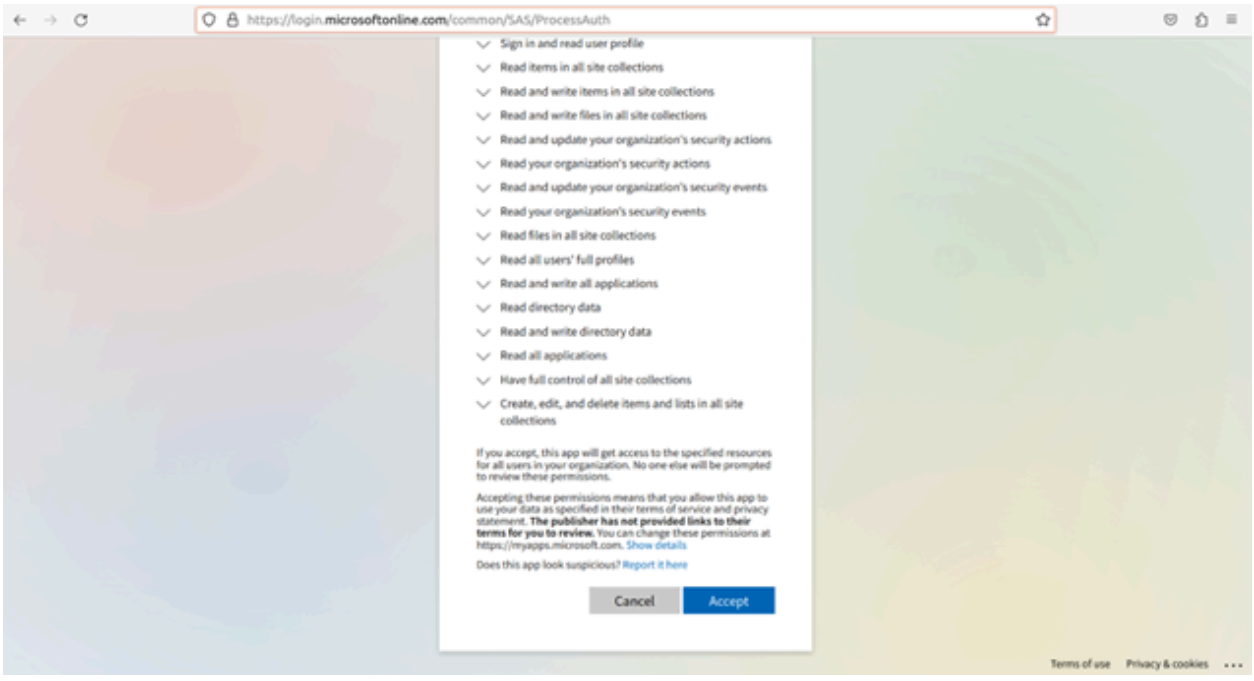


Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email (Required)	Enter an email address of the Microsoft SharePoint administrator account.
Enter List of Internal Domains (Required)	Enter domains configured for the organization.
Retro Scan	Click to scan and protect all the files that are present on Microsoft SharePoint at the time of connector creation.
Services	Select the services to use for the instance. ◦ API Based Data Protection—Scan and protect content. ◦ Forensic—Use this instance for forensics. ◦ Legal Hold—Use this instance for legal hold. ◦ Quarantine—Use this instance for quarantine files.
Confirm	Click to confirm that the steps required to configure the Microsoft SharePoint account are complete.

4. Click Submit.
5. After adding the instance, select Grant Access to start the OAuth2 process of granting access to the Versa API data protection cloud. This will open login prompt for Microsoft account.



6. Use Microsoft SharePoint Administrator credentials to log in. The next screen will show the permissions that the Versa service will require to scan and monitor the Microsoft SharePoint account. Click Accept to grant access to Microsoft SharePoint account.



Microsoft Teams API-Based Data Protection

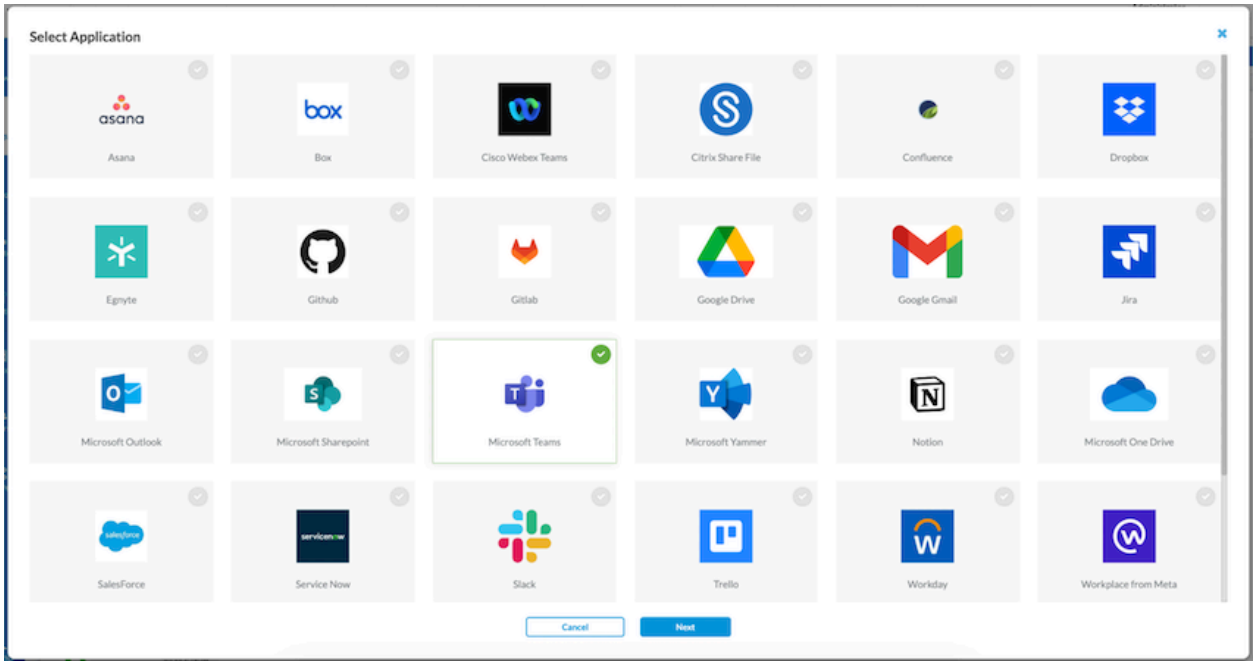
This section describes how to configure the Microsoft Teams application for API-based data protection.

Configure Microsoft Teams for API-Based Data Protection

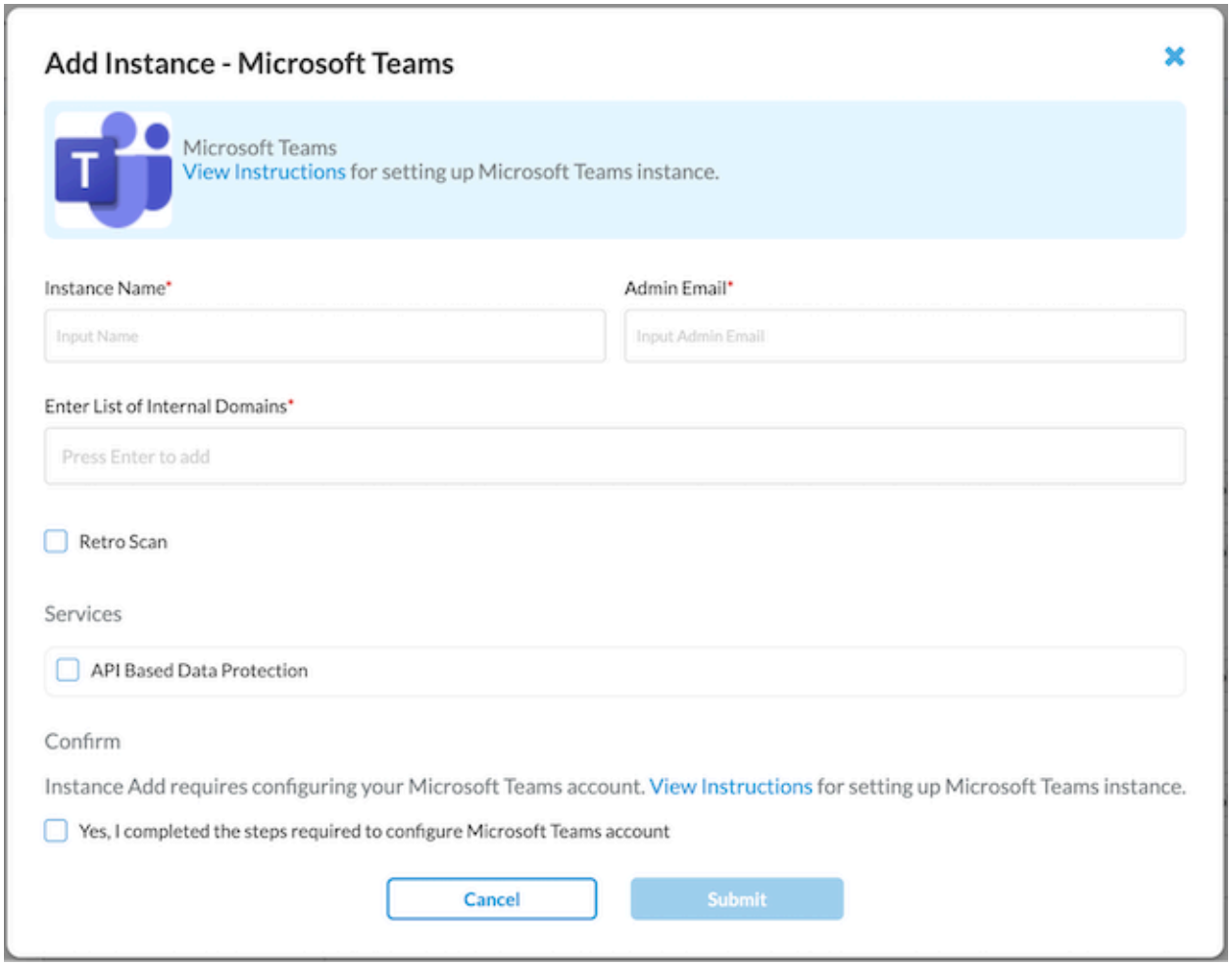
For Microsoft Teams, no configuration is required.

Configure a Microsoft Teams Connector

1. Navigate to "Configure" > “Advanced Security” > “API Based Data Protection” > “Connectors”.
2. Click the + Add icon, select Jira, then click Next.



3. In the Add Instance window, enter information for the following fields.



Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email (Required)	Enter an email address of the Microsoft Teams administrator account.
Enter List of Internal Domains (Required)	Enter domains configured for the organization.
Retro Scan	Click to scan and protect all the files that are present on Microsoft Teams at the time of connector creation.
Services	Select the services to use for the instance. ◦ API-Based Data Protection—Scan and protect content.
Confirm	Click to confirm that the steps required to configure the Microsoft Teams account are complete.

4. Click Submit.
5. After adding the instance, select Grant Access to start the OAuth2 process of granting access to the Versa API data protection cloud. This will open a login prompt for the Microsoft account. Use Microsoft Teams Administrator credentials to log in and grant access.

Microsoft Yammer API-Based Data Protection

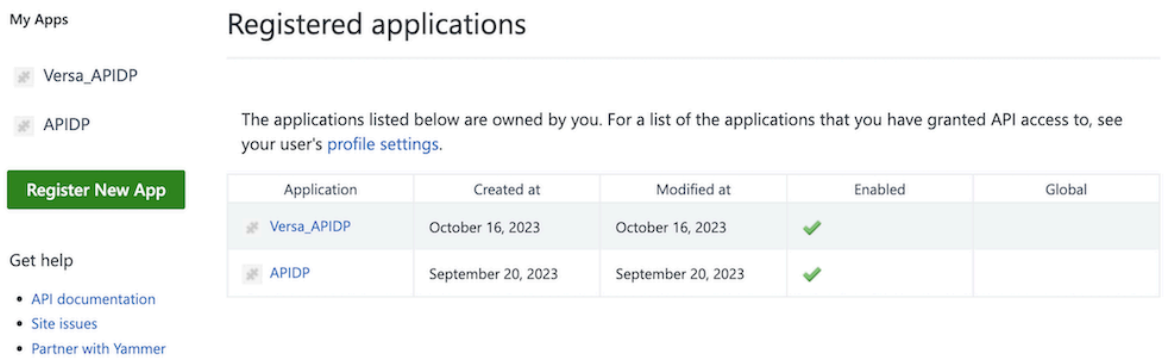
This section describes how to configure the Microsoft Yammer application for API-based data protection.

Configure Microsoft Yammer for API-Based Data Protection

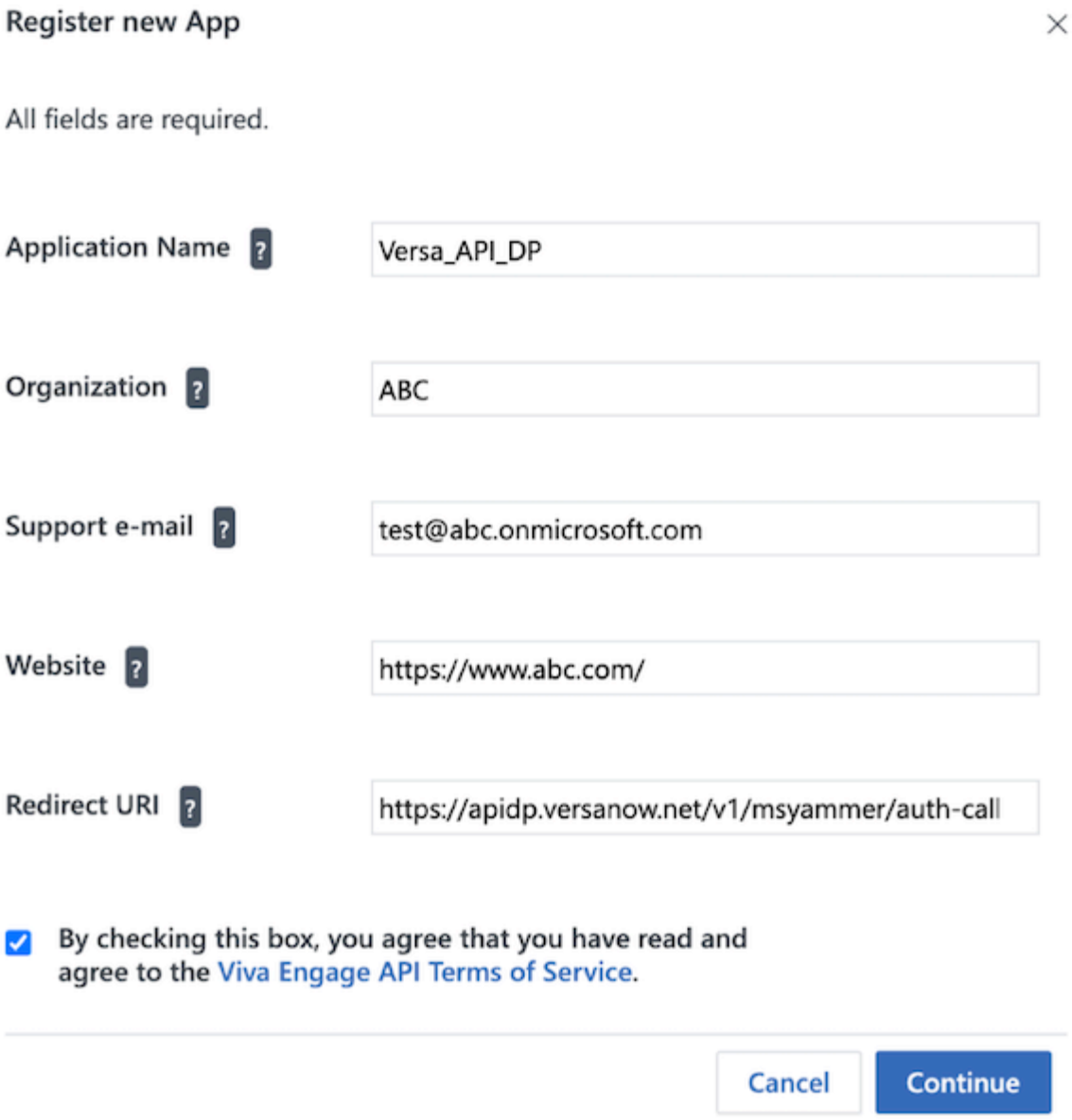
Note: Create a new user with administrator privileges and an application to track all activity. The new admin should be added to all communities over the network to monitor them. The new admin should never unfollow any user.

To configure Microsoft Yammer for API-based data protection:

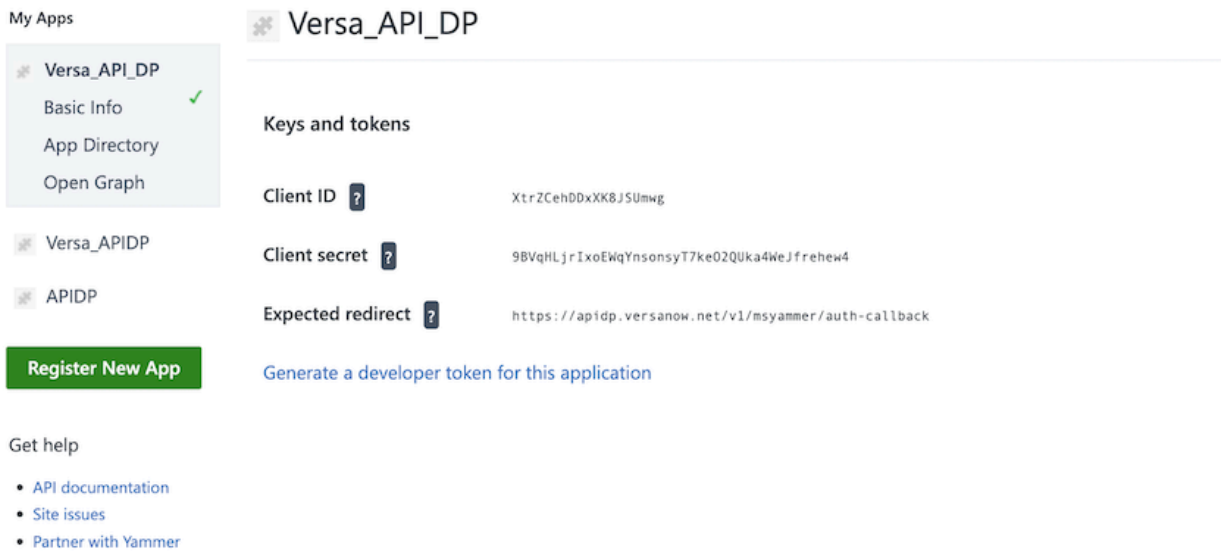
1. Login with administrator credentials at https://www.yammer.com/client_applications.
2. Click “Register New App” under “My Apps.”



3. Enter information in all the fields, agree to the terms and conditions, then click Continue.

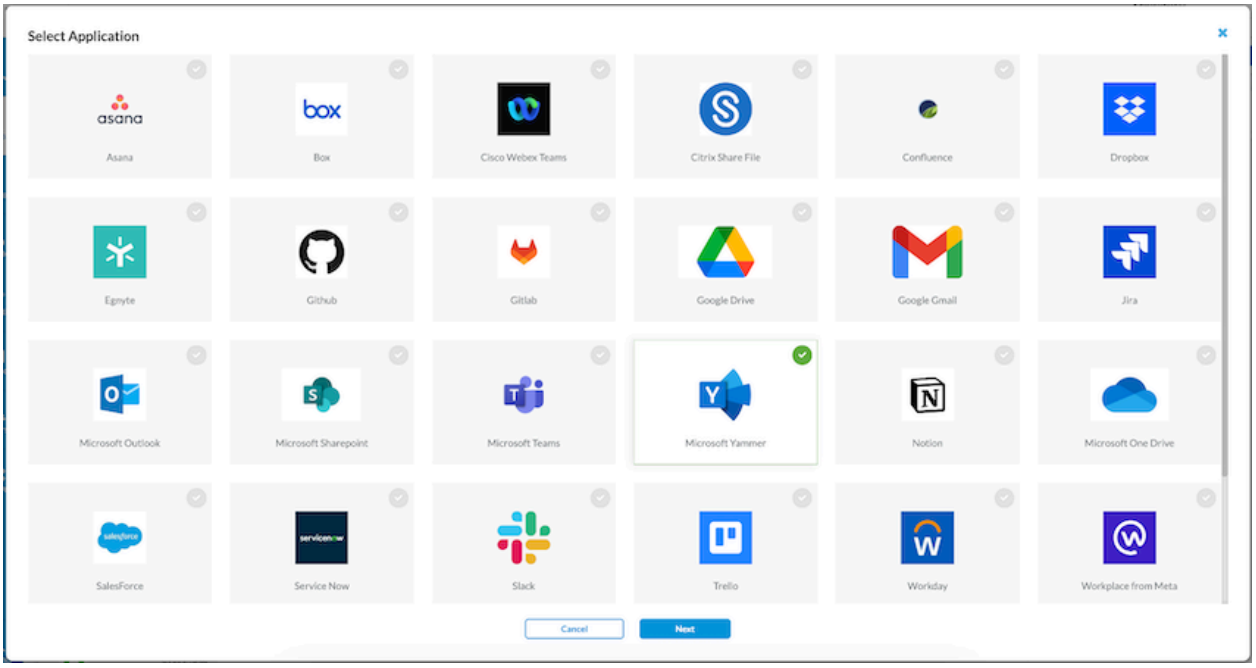


4. The application is created, and key and tokens are ready.

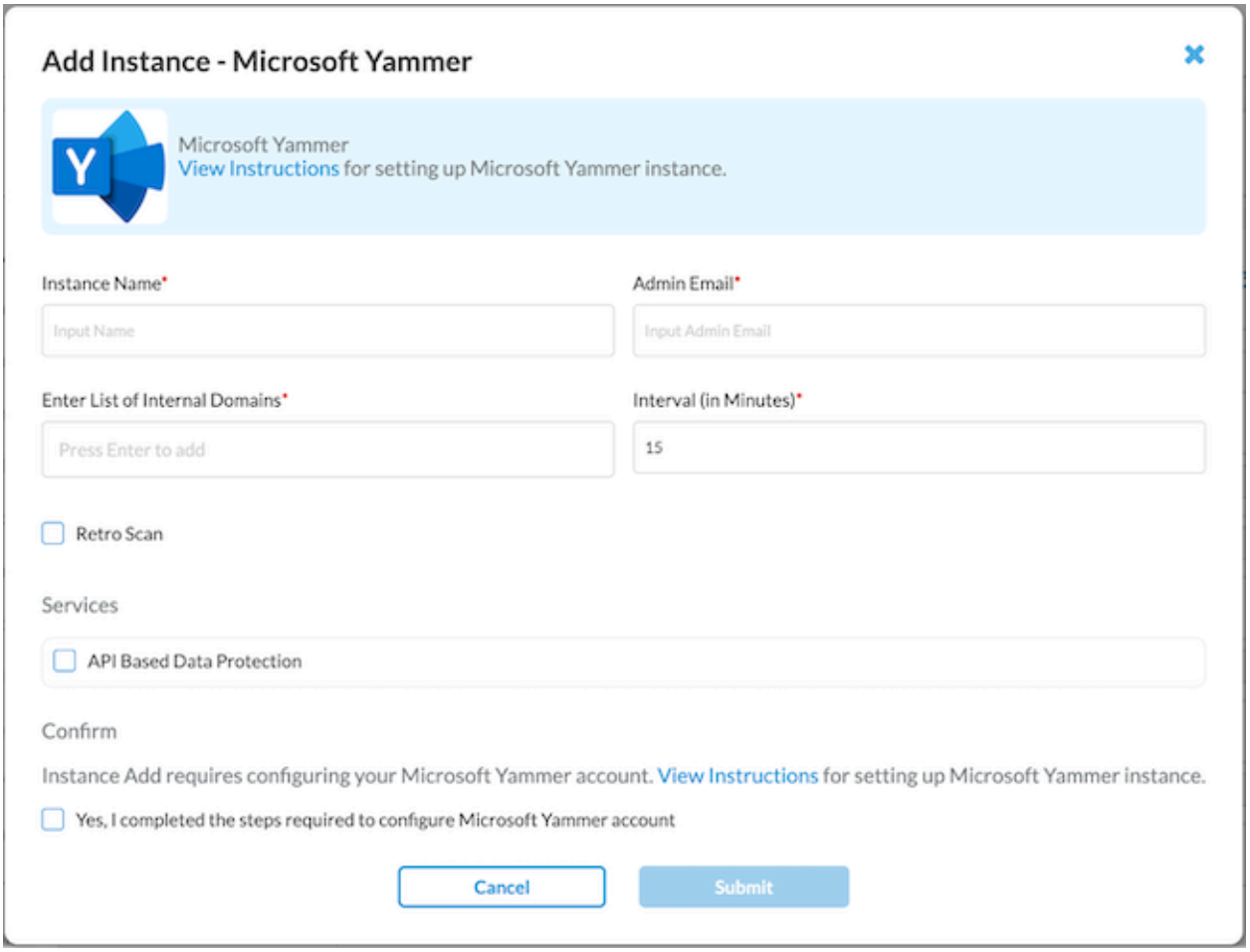


Configure a Microsoft Yammer Connector

1. Navigate to "Configure" > “Advanced Security” > “API Based Data Protection” > “Connectors”.
2. Click the ✚ Add icon, select Microsoft Yammer, then click Next.



3. In the Add Instance window, enter information for the following fields.



Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email (Required)	Enter an email address of the Microsoft Yammer administrator account.
Enter List of Internal Domains (Required)	Enter domains configured for the organization.
Interval (in minutes) (Required)	Enter the Interval time in minutes to register for polling.
Retro Scan	Click to scan and protect all the files that are present on Microsoft Yammer at the time of connector creation.
Services	Select the services to use for the instance. ◦ API-Based Data Protection—Scan and protect

Field	Description
	content.
Confirm	Click to confirm that the steps required to configure the Microsoft Yammer account are complete.

4. After adding the instance, click “Grant Access” to start the OAuth 2.0 process of granting access to the Versa API-DP cloud. This will open a login prompt for the Viva Engage (Yammer) account. Use administrator credentials to log in and grant access.

Notion API-Based Data Protection

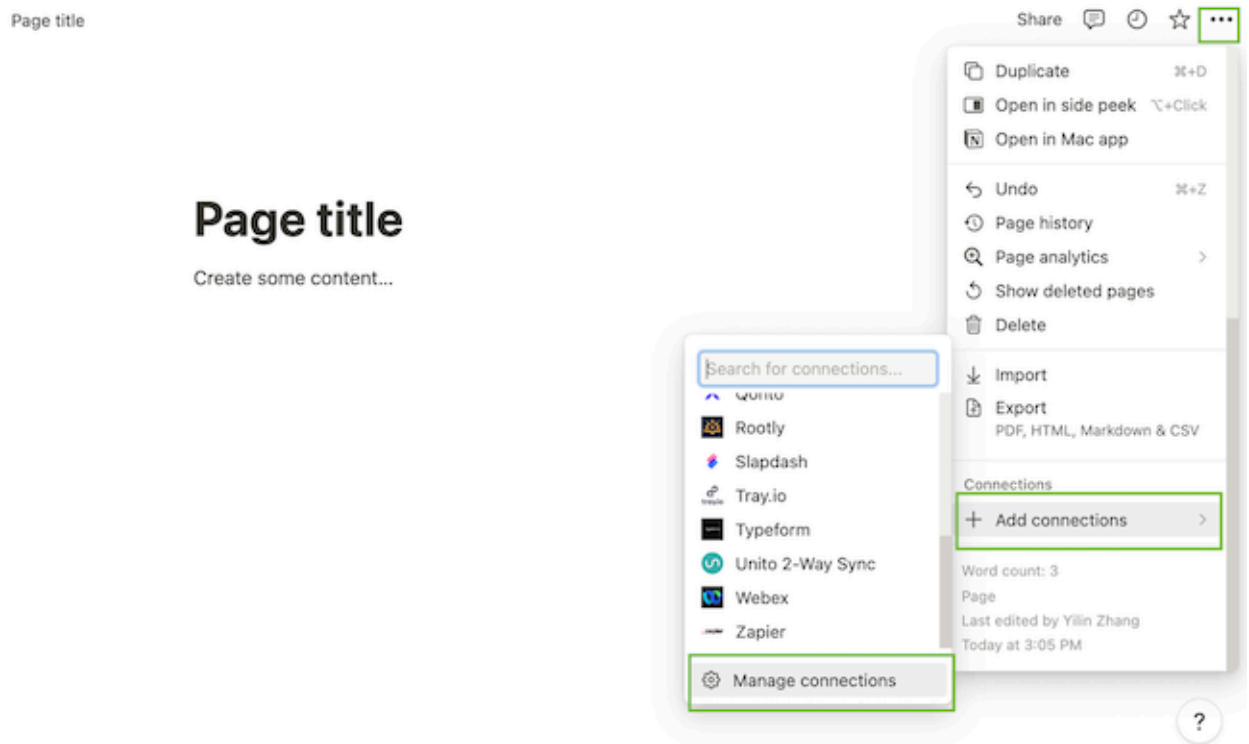
This section describes how to configure the Notion application for API-based data protection.

Configure Notion for API-Based Data Protection

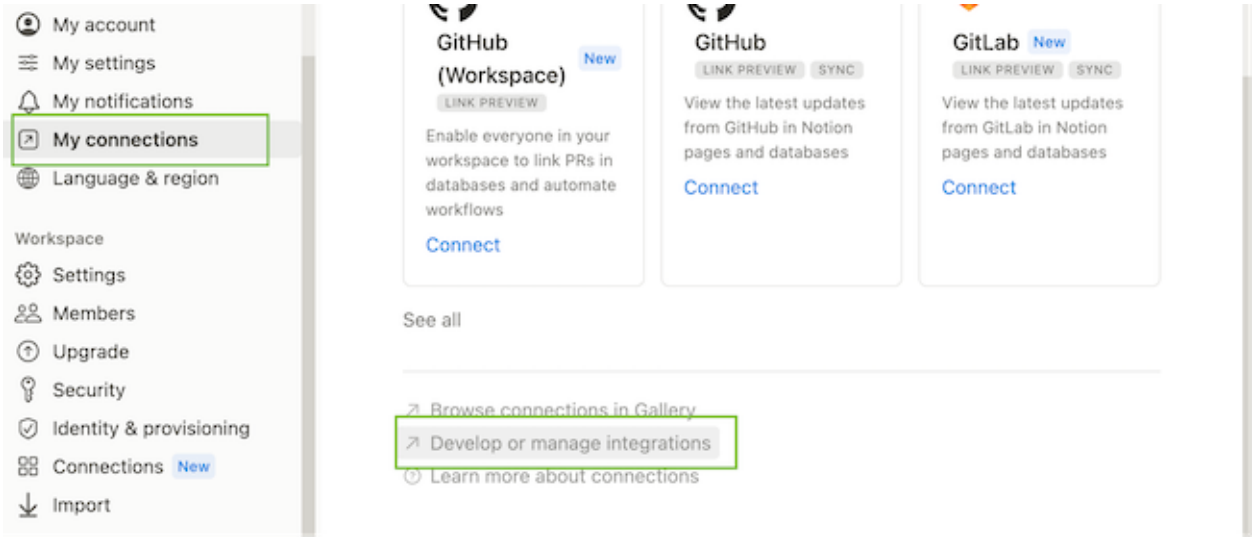
For Notion, no configuration is required at the Cisco Webex account.

To create a new integration:

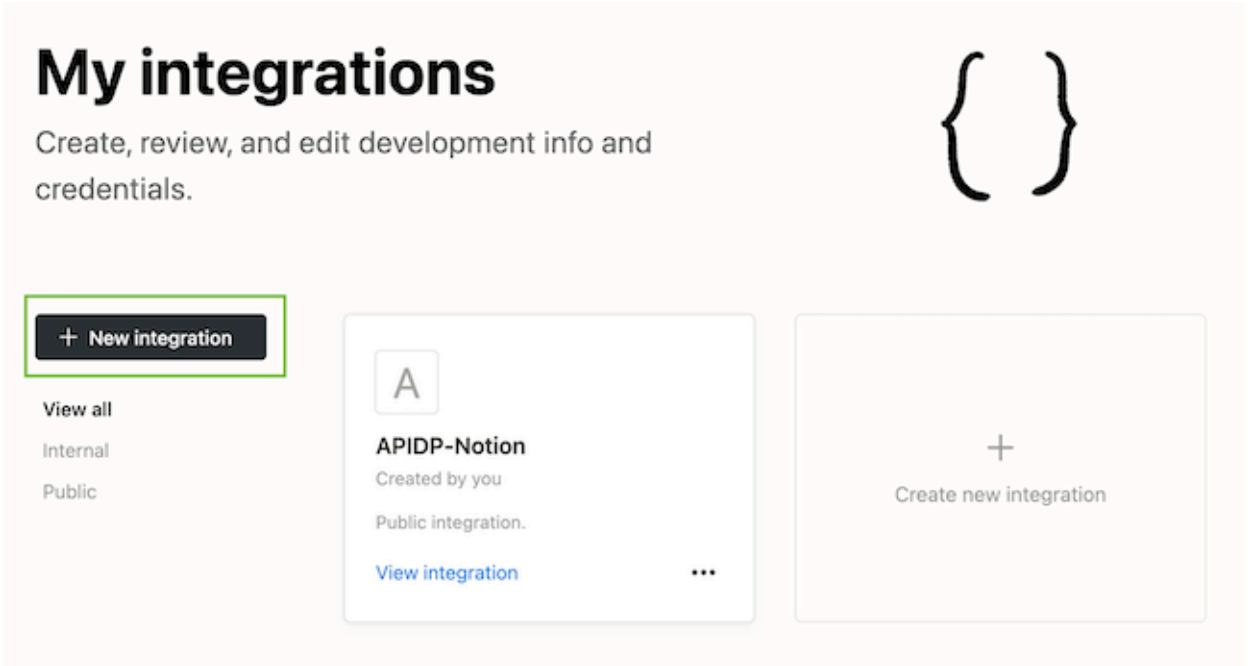
1. Select elipses in the right corner -> Add connections -> Manage connections.

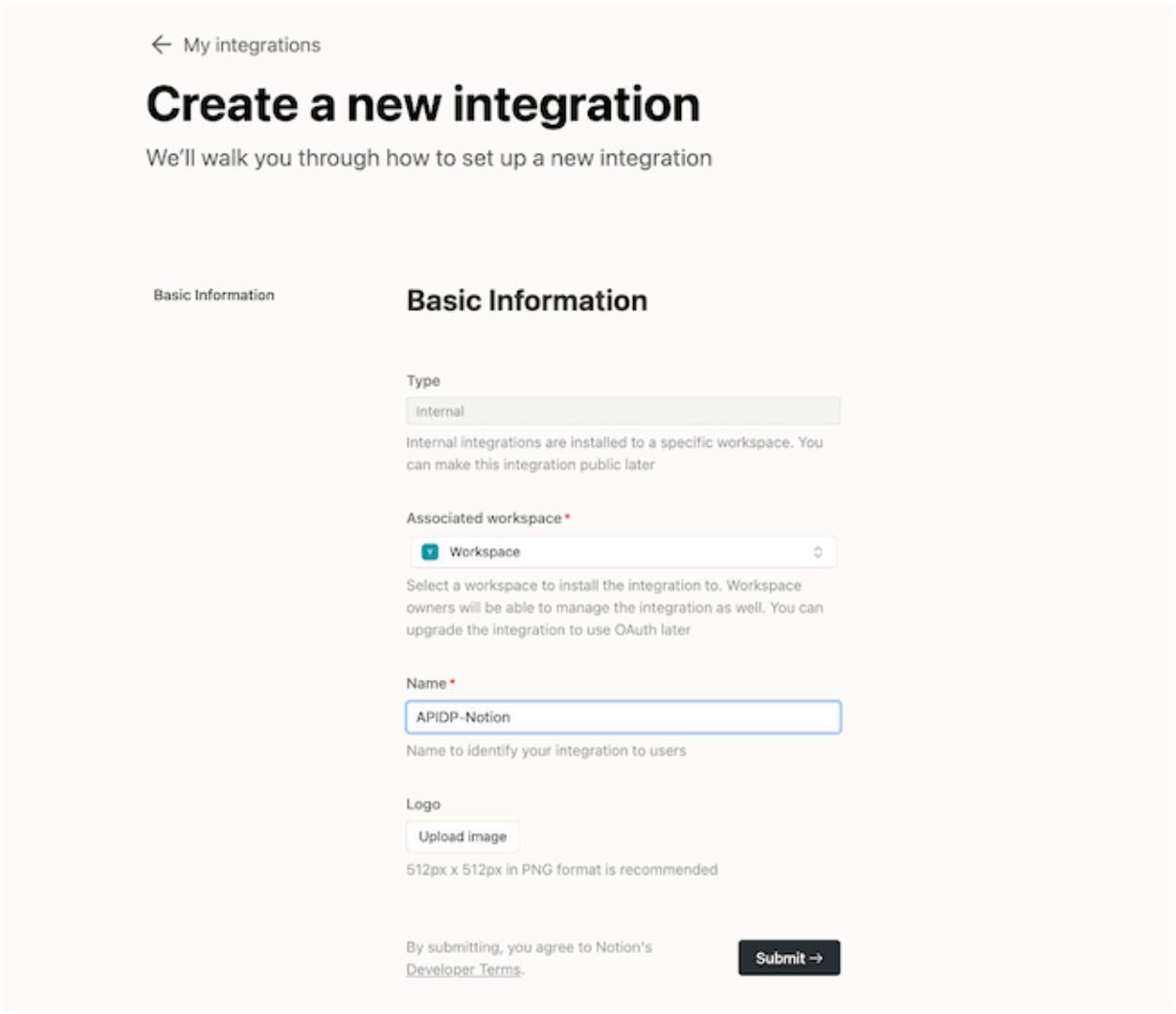


2. Under My connections -> Develop or manage integrations.

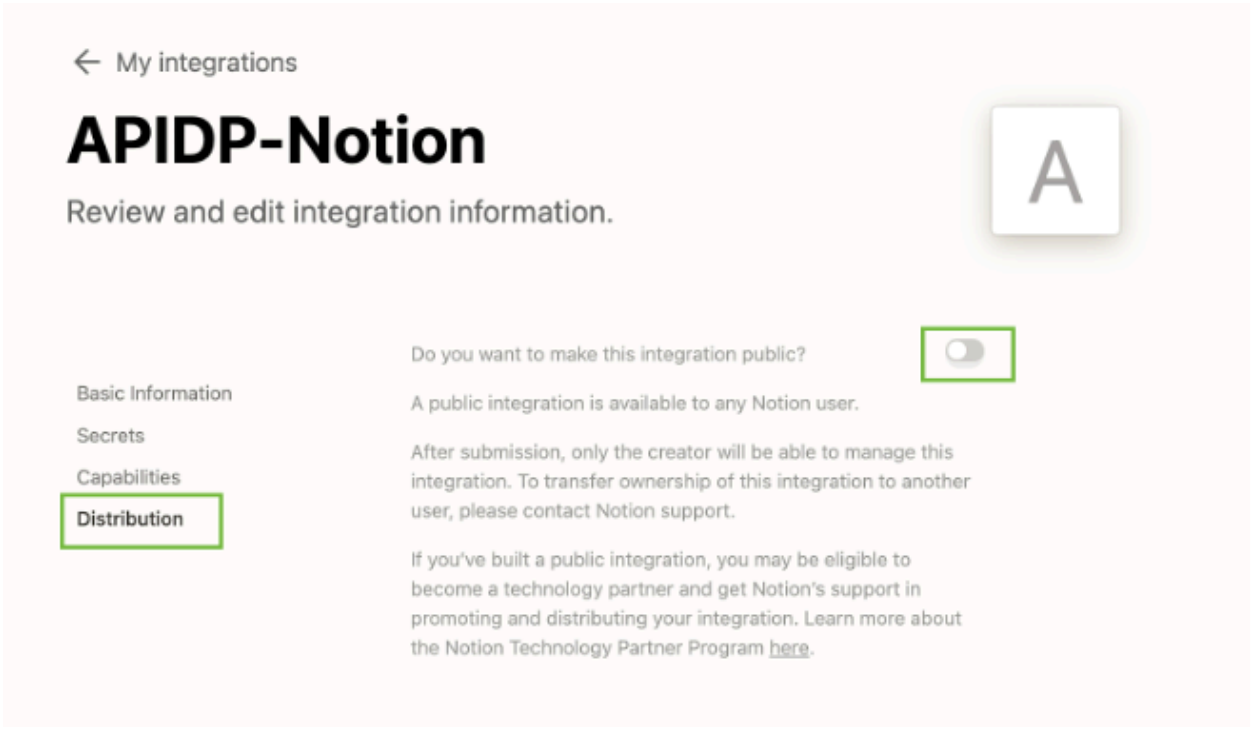


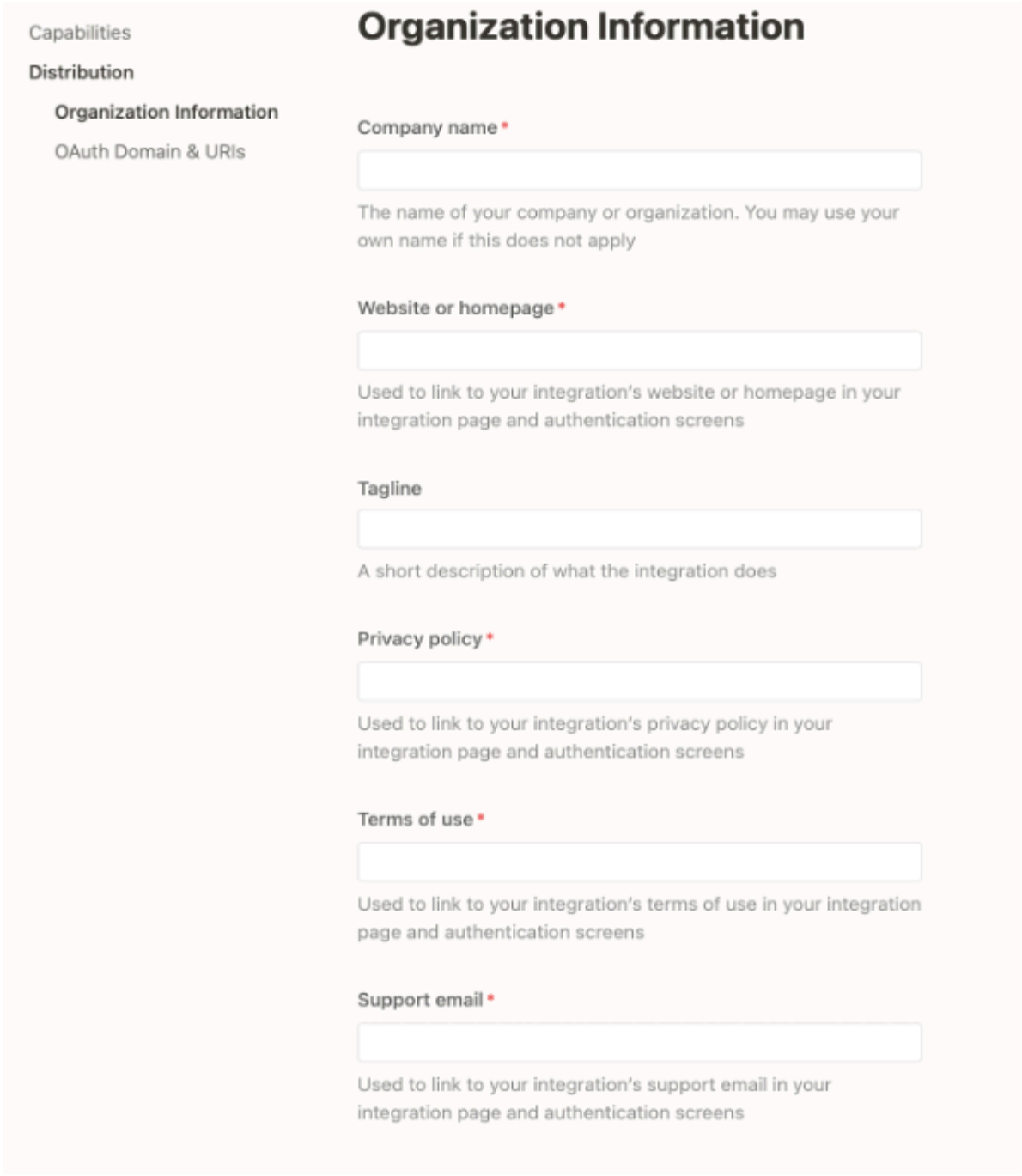
3. Add new integration and put name for the integration.



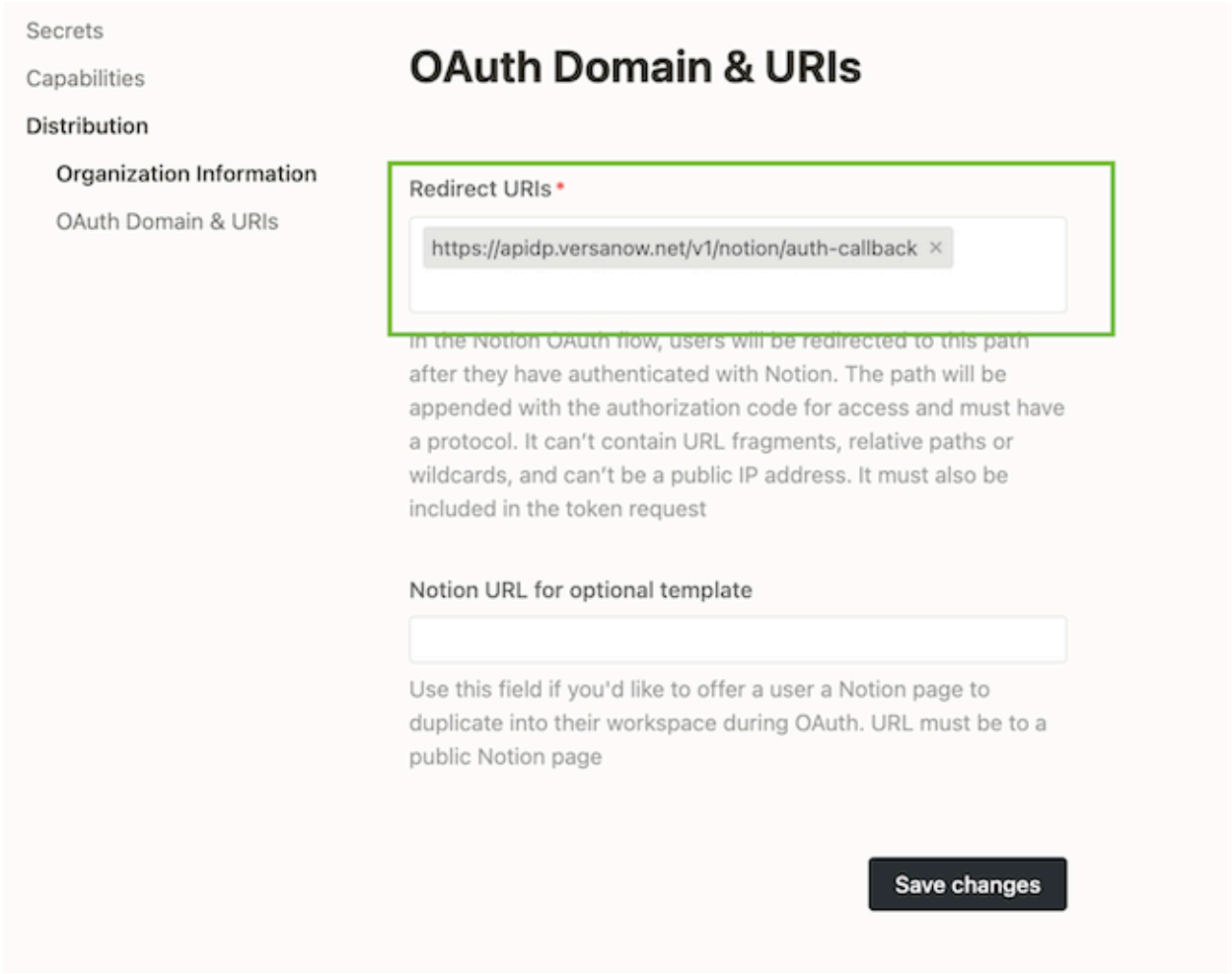


4. Make it public. After submitting the new integration, change it from a private integration to a public integration so that all accounts can access it. Under Distribution, make the integration public and provide basic information.

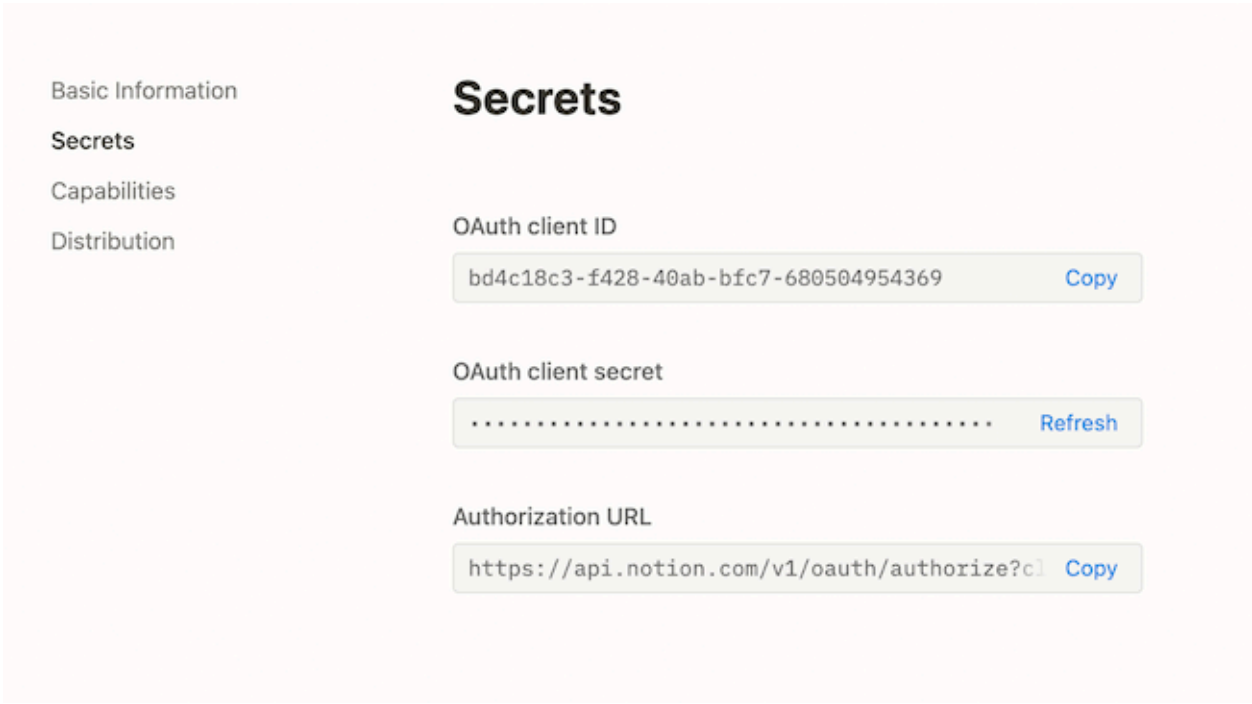




5. Under OAuth Domain & URIs, set redirect URI.



6. Client-id and secret is under secrets.

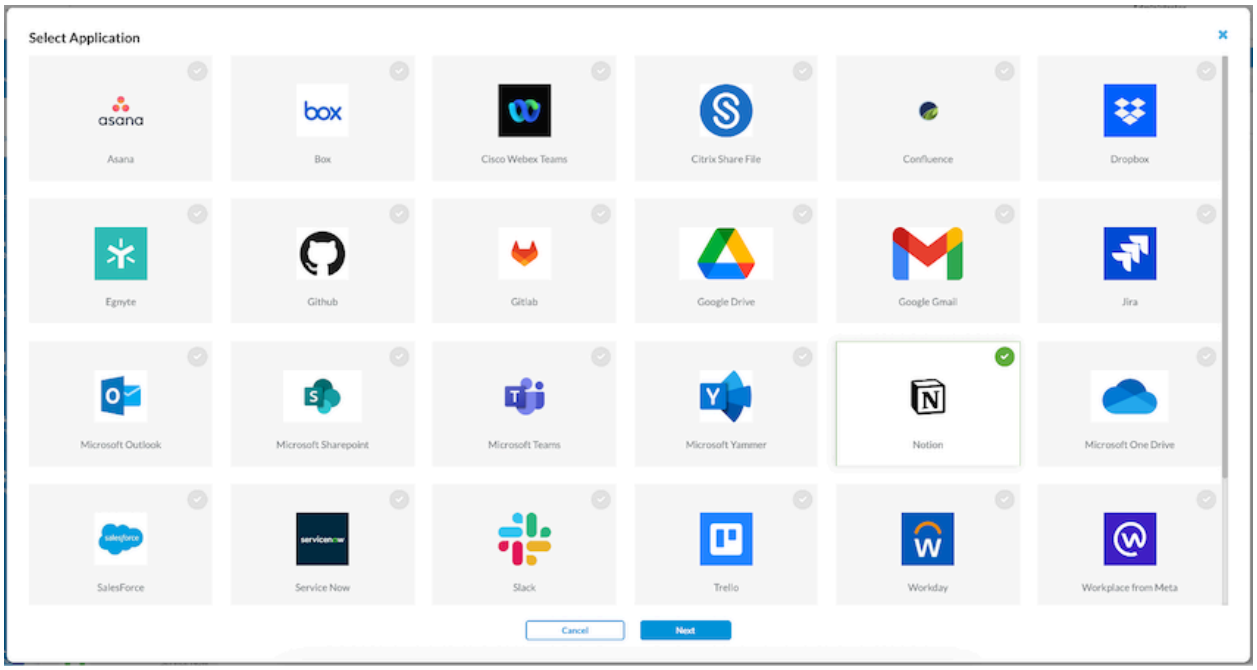


Note: A newly added page/database does not automatically connect to the integration. It needs to be manually added to integration.

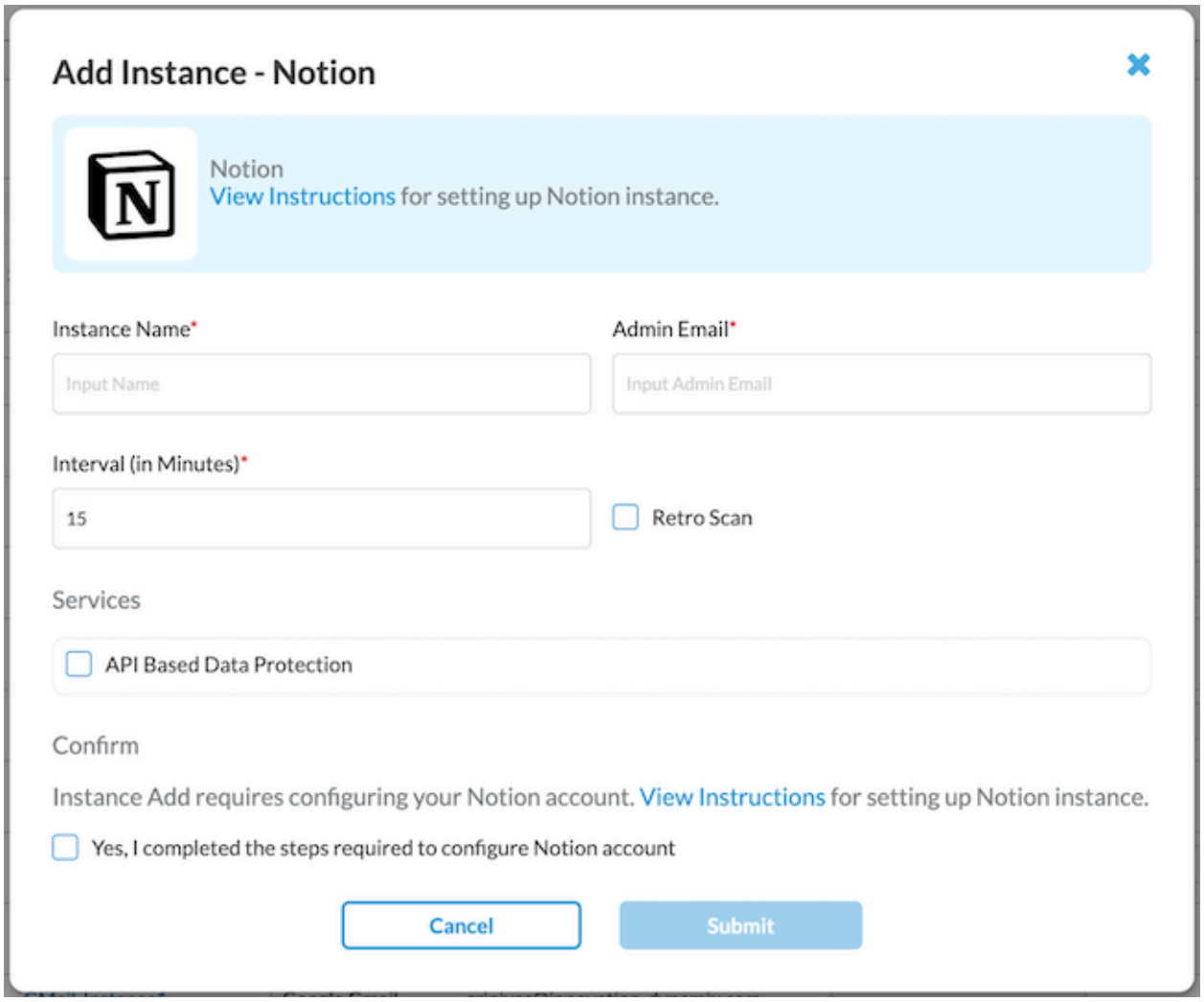
Configure a Notion Connector

To configure a Notion connector:

1. Navigate to "Configure" > “Advanced Security” > “API Based Data Protection” > “Connectors”.
2. Click the + Add icon, select Notion, then click Next.



3. In the Add Instance window, enter information for the following fields.



Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email (Required)	Enter an email address of the Notion administrator account.
Interval (in minutes) (Required)	Enter the Interval time in minutes to register for polling.
Retro Scan	Click to scan and protect all the files that are present on Notion at the time of connector creation.
Services	Select the services to use for the instance. ◦ API-Based Data Protection—Scan and protect content.
Confirm	Click to confirm that the steps required to configure the Notion account are complete.

4. After adding the instance, click “Grant Access” to start the OAuth 2.0 process of granting access to the Versa API-DP cloud. This will open a login prompt for the Notion account. Use administrator credentials to log in and grant access.

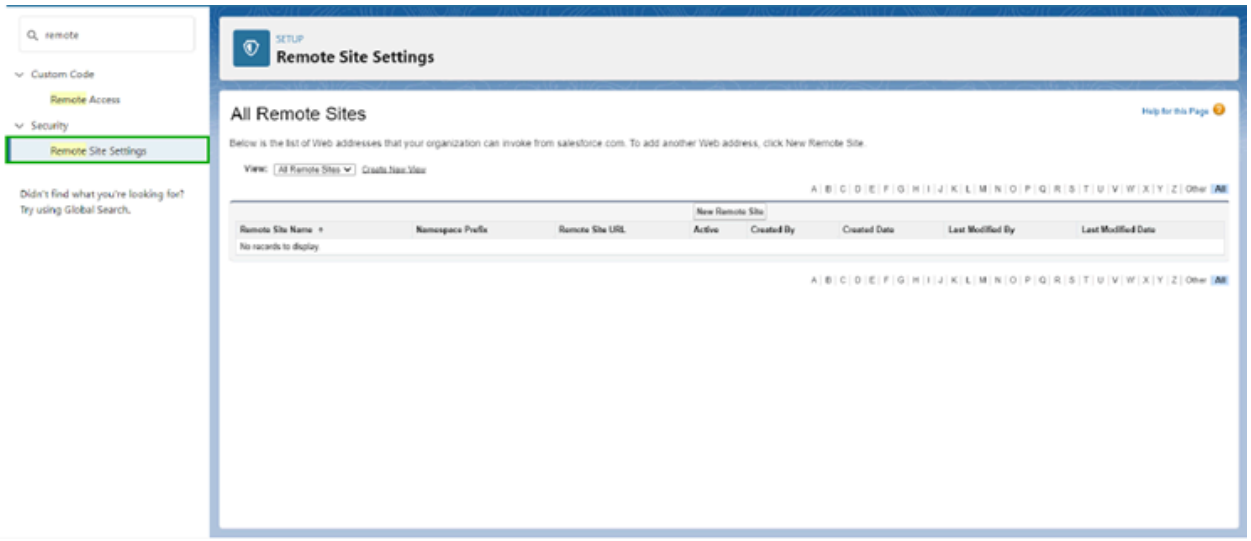
Salesforce API-Based Data Protection

This section describes how to configure the Salesforce application for API-based data protection.

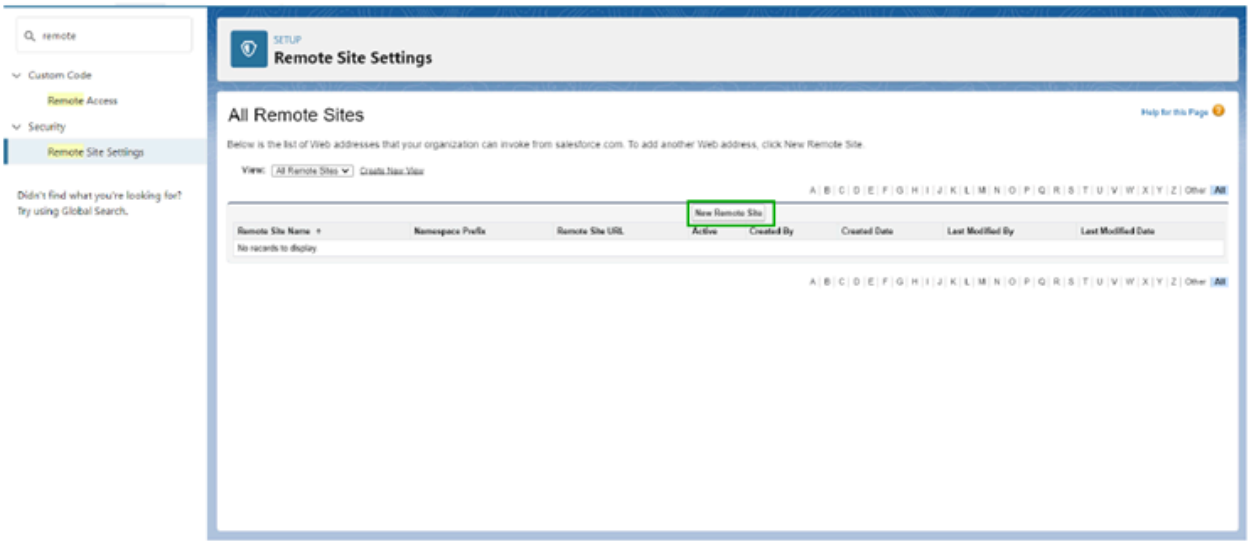
Configure Salesforce for API-Based Data Protection

To configure a new instance for Salesforce:

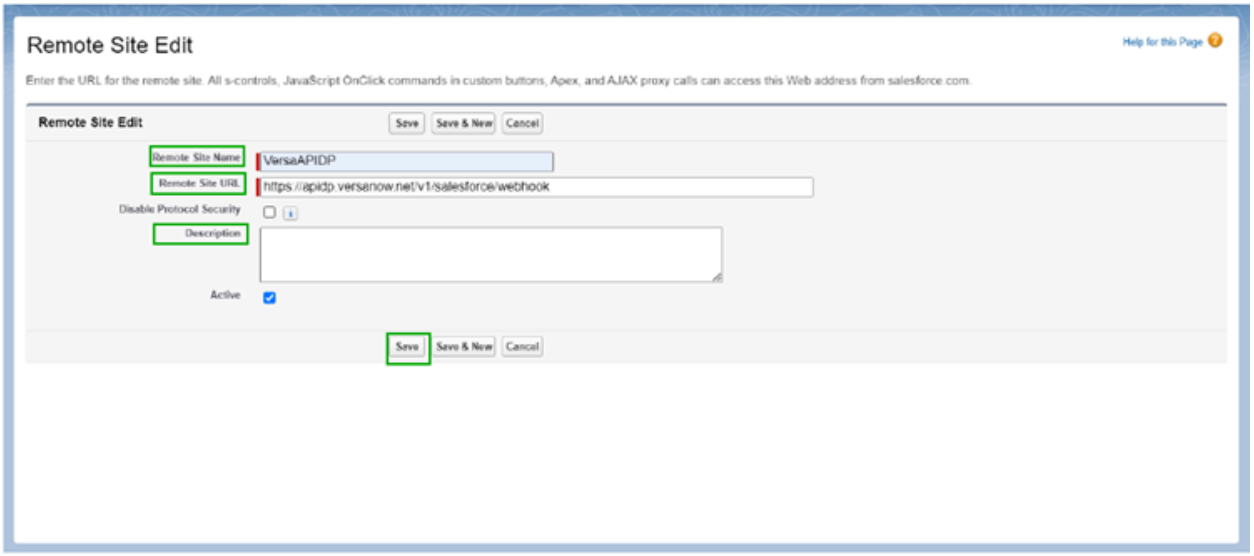
1. Go to Setup page, search for Remote Site Settings in the quick find box, and then select Remote Site Settings.



2. To create a new remote site, click New Remote Site.



3. In the Remote Site edit window, enter information for the following fields.

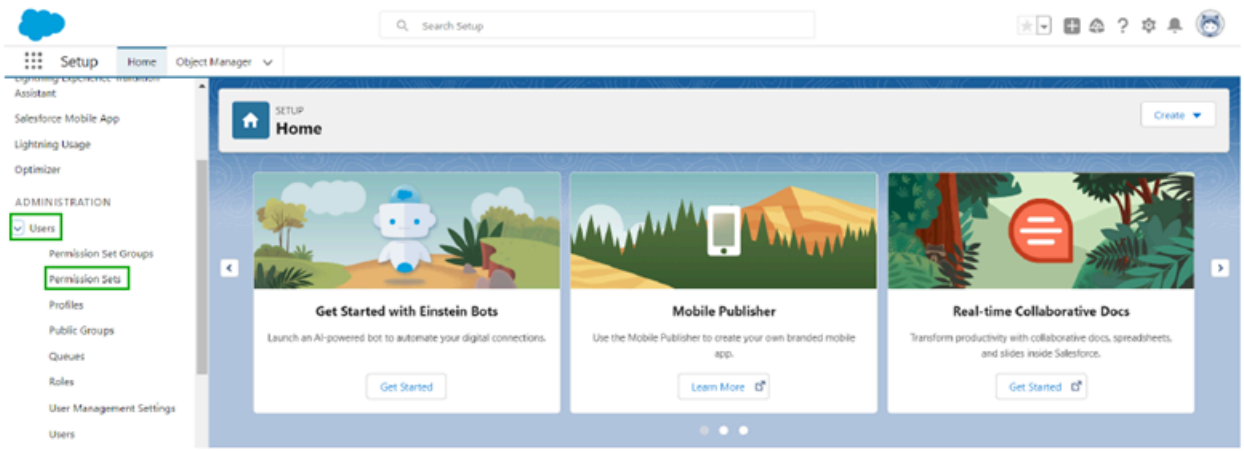


Field	Description
Remote Site Name (Required)	Enter a name for the remote site.
Remote Site URL (Required)	Enter URL of the endpoint.
Description	Enter a description.

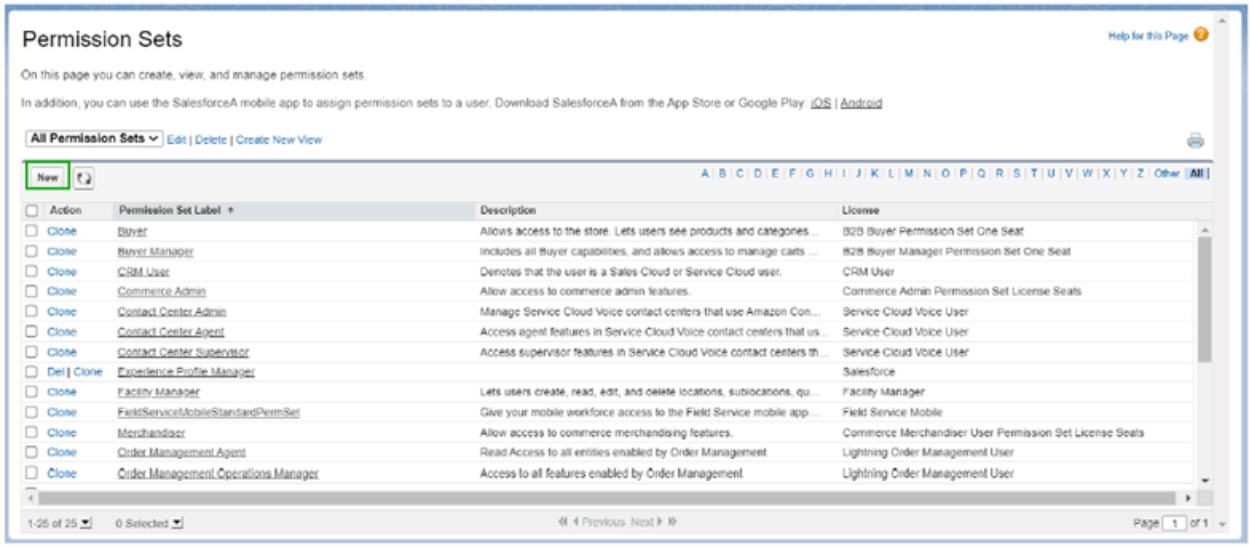
4. Click Save.

To enable listing private files of all users in the organization (optional):

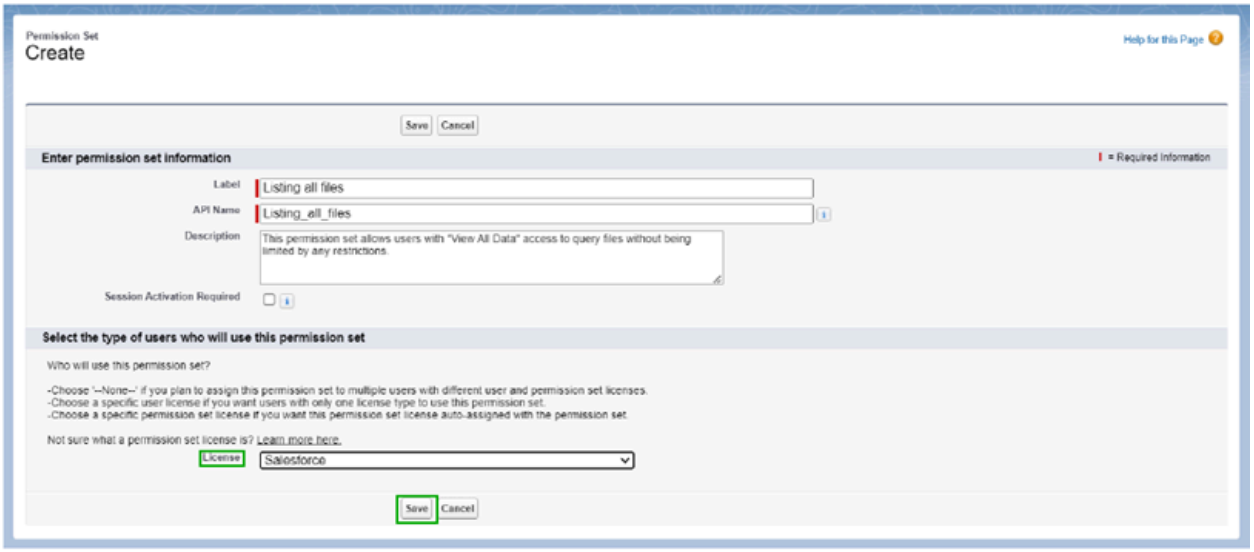
1. Log in to login.salesforce.com as an administrator.
2. Go to Setup, and select Administration > Users > Permission Sets, and then click Create.



3. In the Permission Sets page, click New.

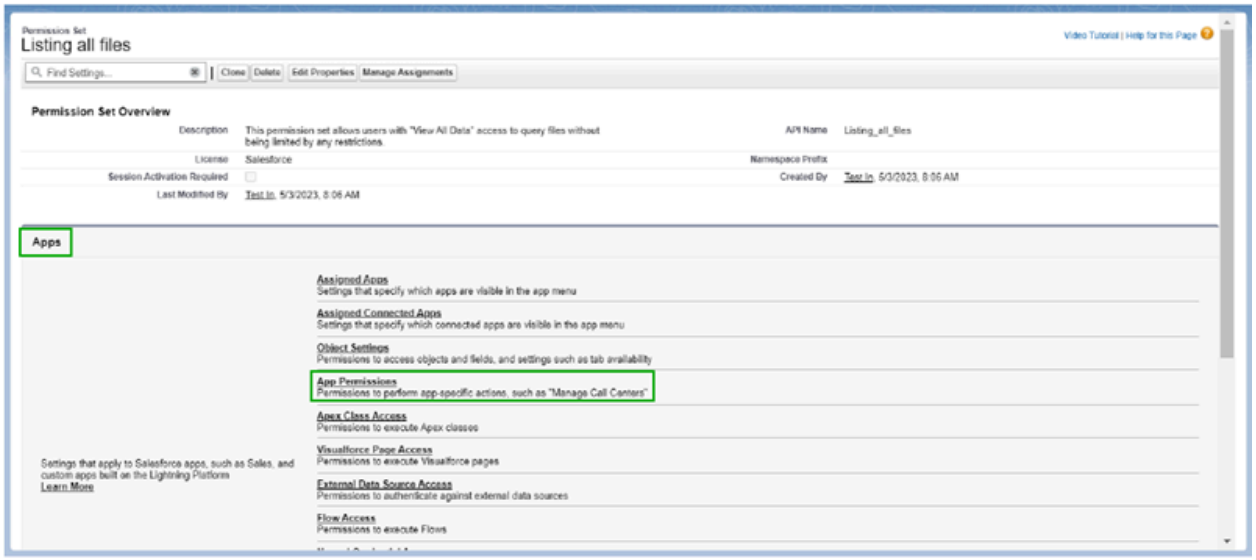


4. In the Permission Sets Create page, enter information for the following fields.

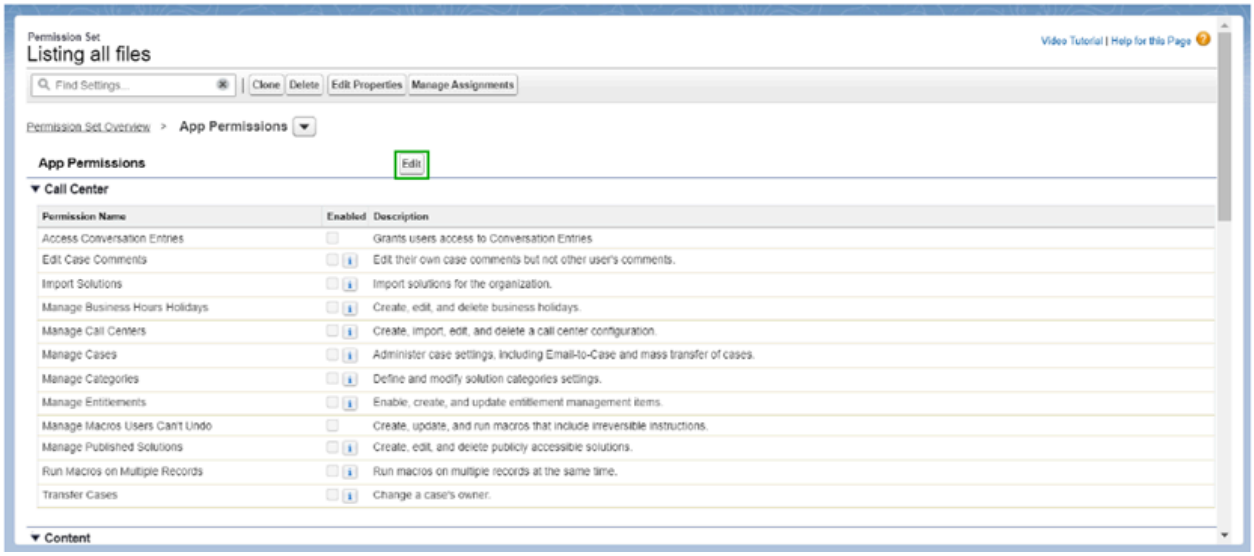


Field	Description
Label	Enter the label information for the permission set.
API Name	Enter a name for the permission set.
Description	Enter a description.
License	Select Salesforce from the license drop-down list.

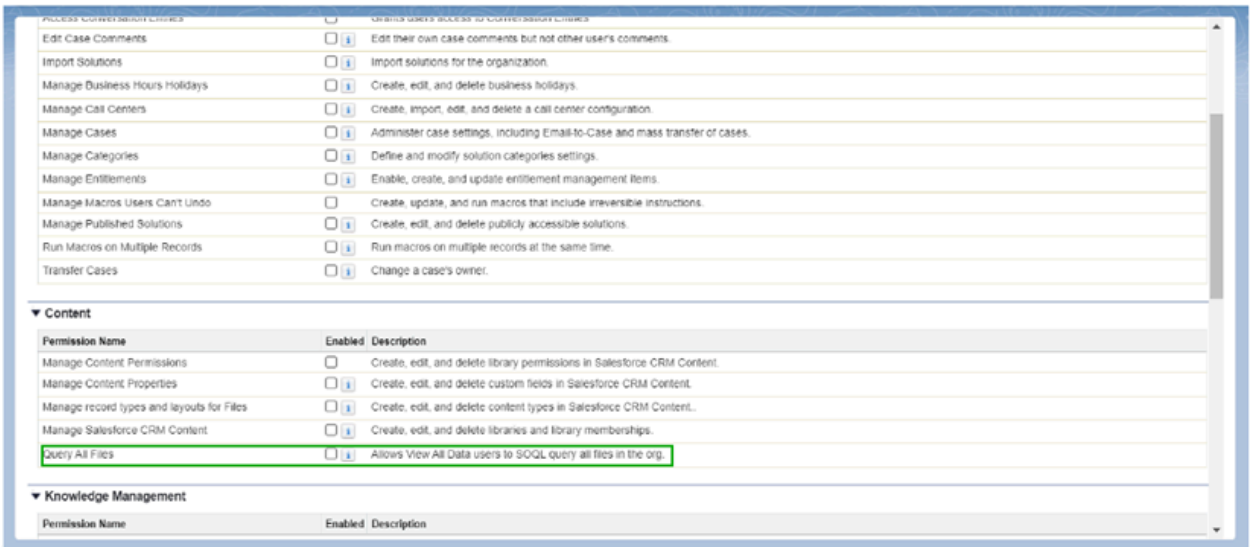
5. Click Save.
6. In the Permission Set Listing all files page, select App Permissions in the Apps section.



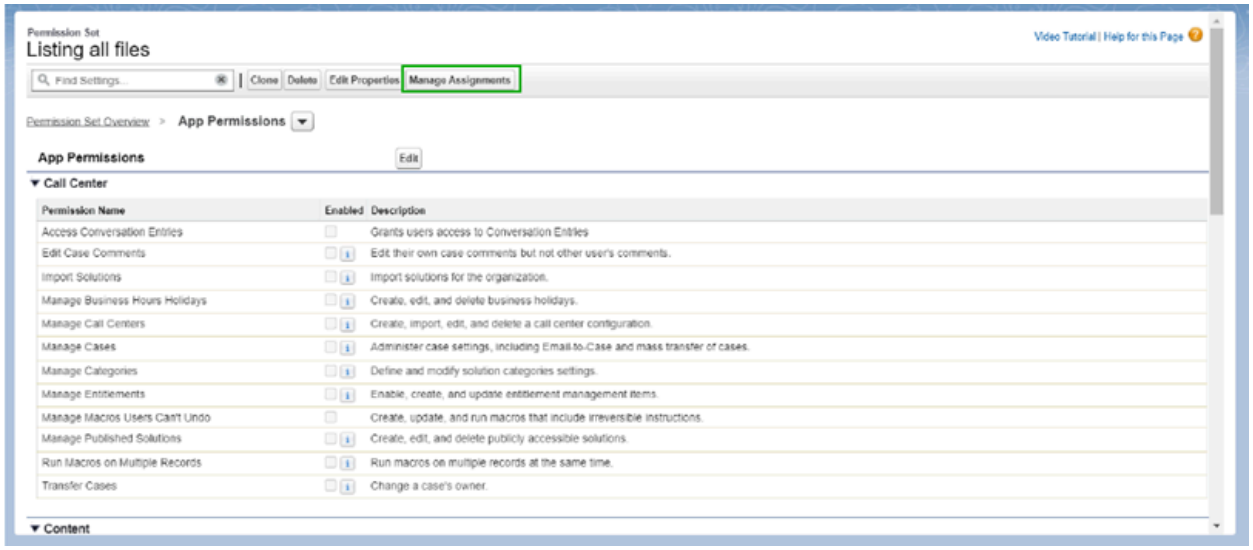
7. Click Edit next to App Permissions label.



8. Select Query All Files checkbox in the Content section.



9. Click Save and confirm permission changes.
10. Click Manage Assignments tab, and then add assignments.



11. Select user (admin), and click Assign.

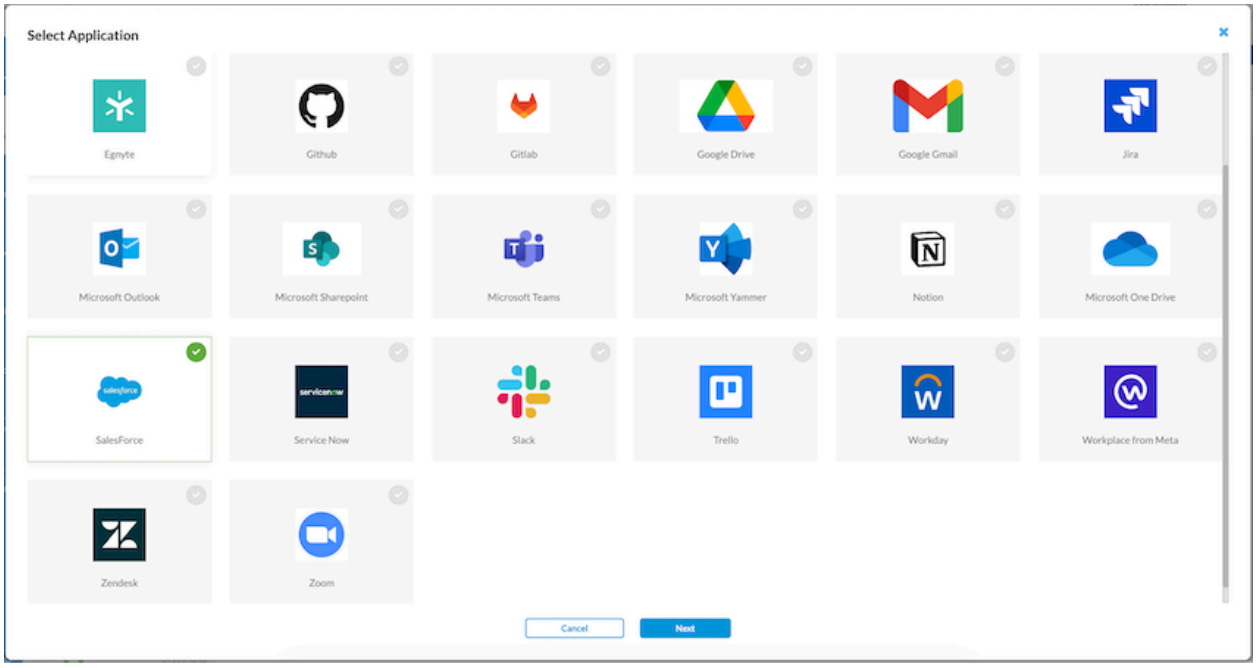
To Install the package with Apex Classes and Triggers:

1. Install the package.
   - To install the package in the production environment, click https://login.salesforce.com/packaging/installPackage.apexp?p0=04tDn000000AtV5&isdtp=p1
   - To install the package in the Sandbox environment, click https://test.salesforce.com/packaging/installPackage.apexp?p0=04tDn000000AtV5&isdtp=p1
2. Log in as an administrator.
3. Install users based on the user's requirements.

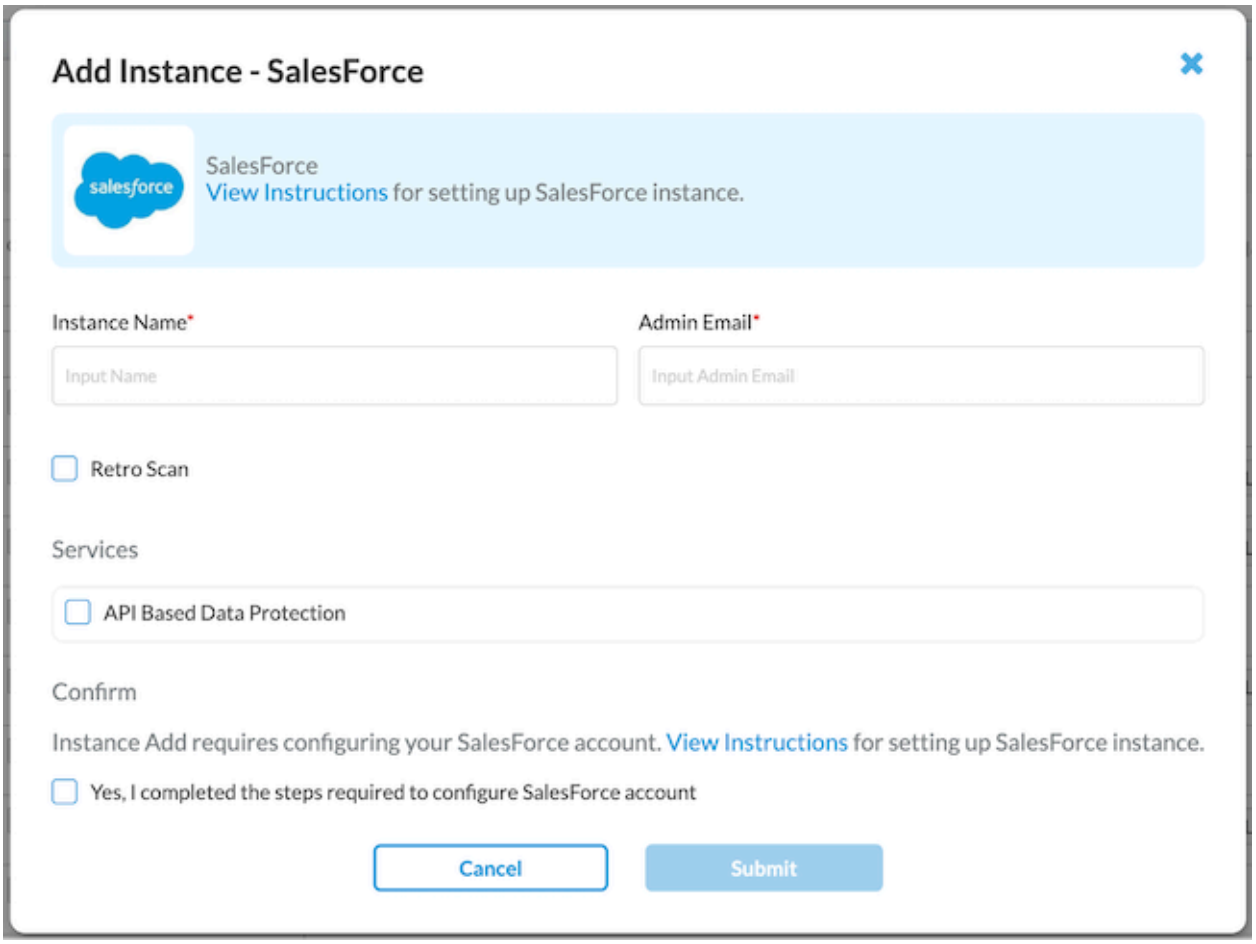
4. Click Install and wait for the installation to complete.
5. Click Done.

Configure a Salesforce Connector

1. Navigate to "Configure" > “Advanced Security” > “API Based Data Protection” > “Connectors”.
2. Click the + Add icon, select Salesforce, then click Next.



3. In the Add Instance window, enter information for the following fields.



Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email (Required)	Enter an email address of the Salesforce administrator account.
Retro Scan	Click to scan and protect all the files that are present on Salesforce at the time of connector creation.
Services	Select the services to use for the instance. ◦ API-Based Data Protection—Scan and protect content.
Confirm	Click to confirm that the steps required to configure the Salesforce account are complete.

4. Click Submit.
5. After adding the instance, select Grant Access to start the OAuth2 process of granting access to the Versa API

data protection cloud. This will open a login prompt for the Salesforce account. Use Salesforce Administrator credentials to log in and grant access.

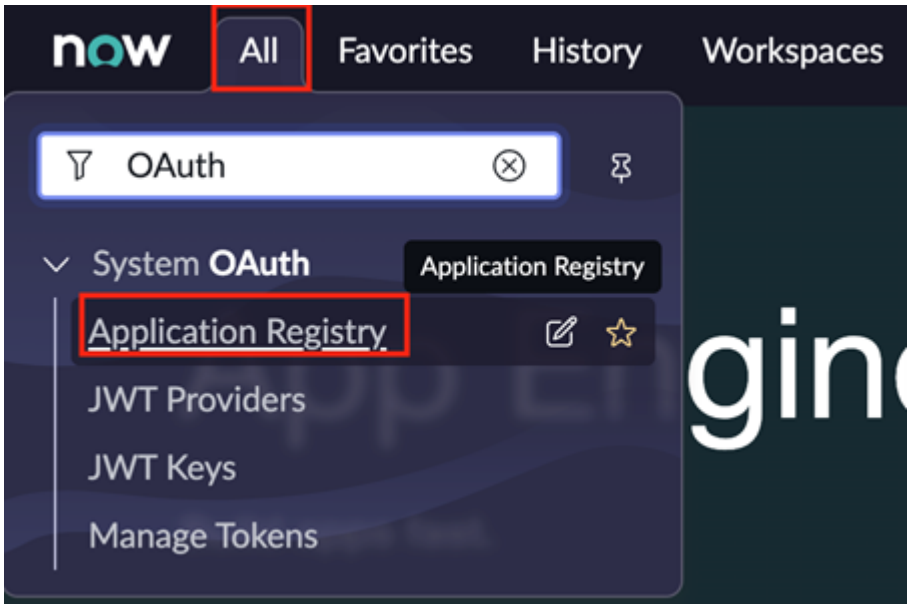
ServiceNow API-Based Data Protection

This section describes how to configure the ServiceNow application for API-based data protection.

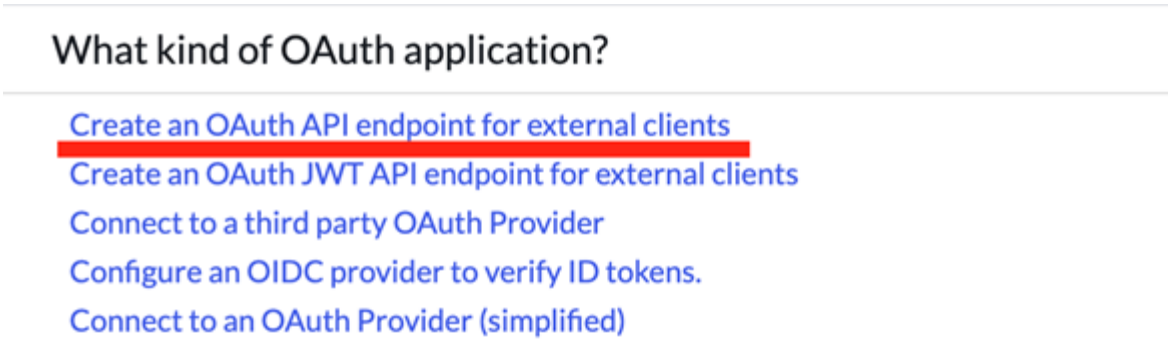
Configure ServiceNow for API-Based Data Protection

To configure a new instance for ServiceNow:

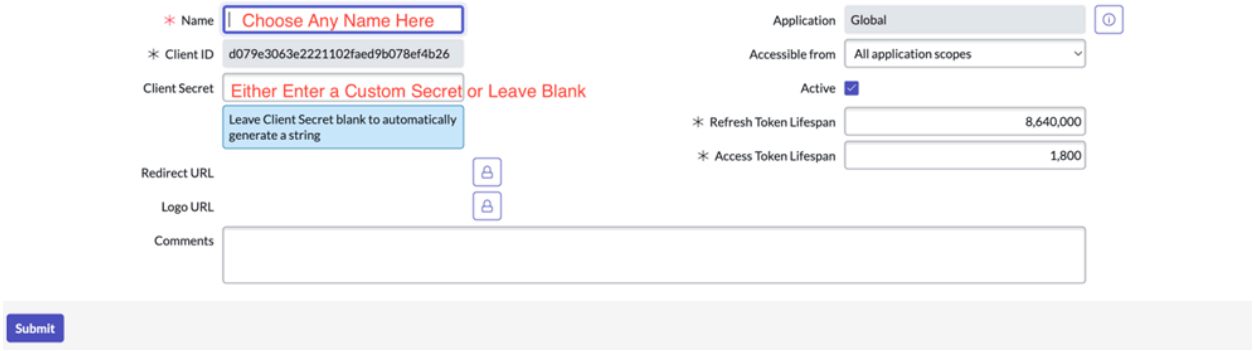
1. Log in to ServiceNow as an administrator.
2. In the All tab, search for OAuth and select Application Registry in System OAuth.



3. To create a new OAuth app, select New on the top-right corner of the page.
4. Select Create an OAuth API endpoint for external clients.

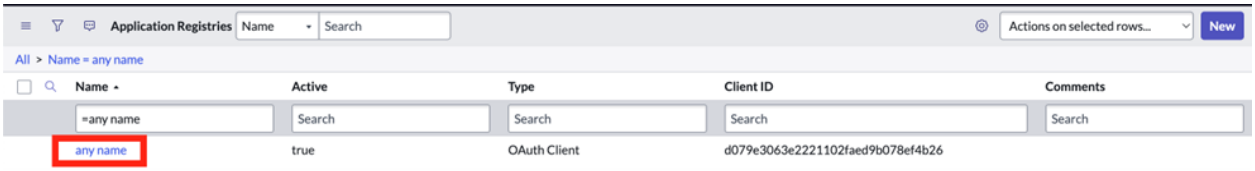


5. Enter information for the following fields.

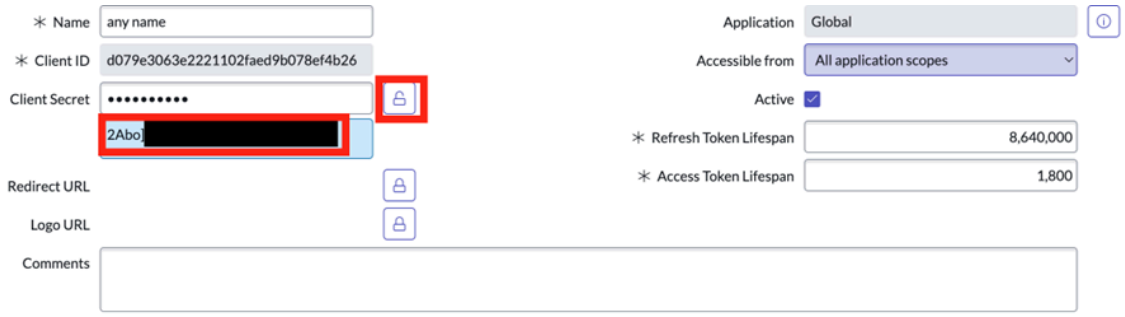


Field	Description
Name	Enter a name for the OAuth app.
Client Secret	Enter a custom password or leave blank for ServiceNow to create a password.

6. Click Submit.
7. Select the new app created.

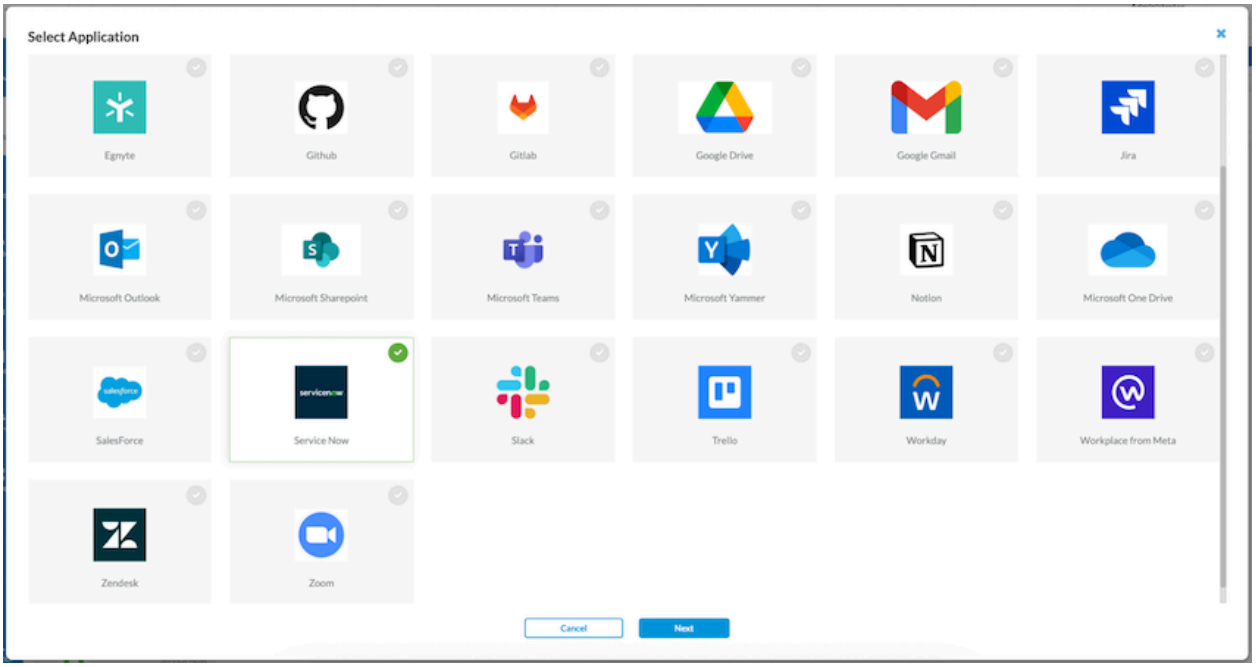


8. Click the lock icon near the client secret option. A blue text block displays that contains the client secret. Copy and store the client ID and client secret.

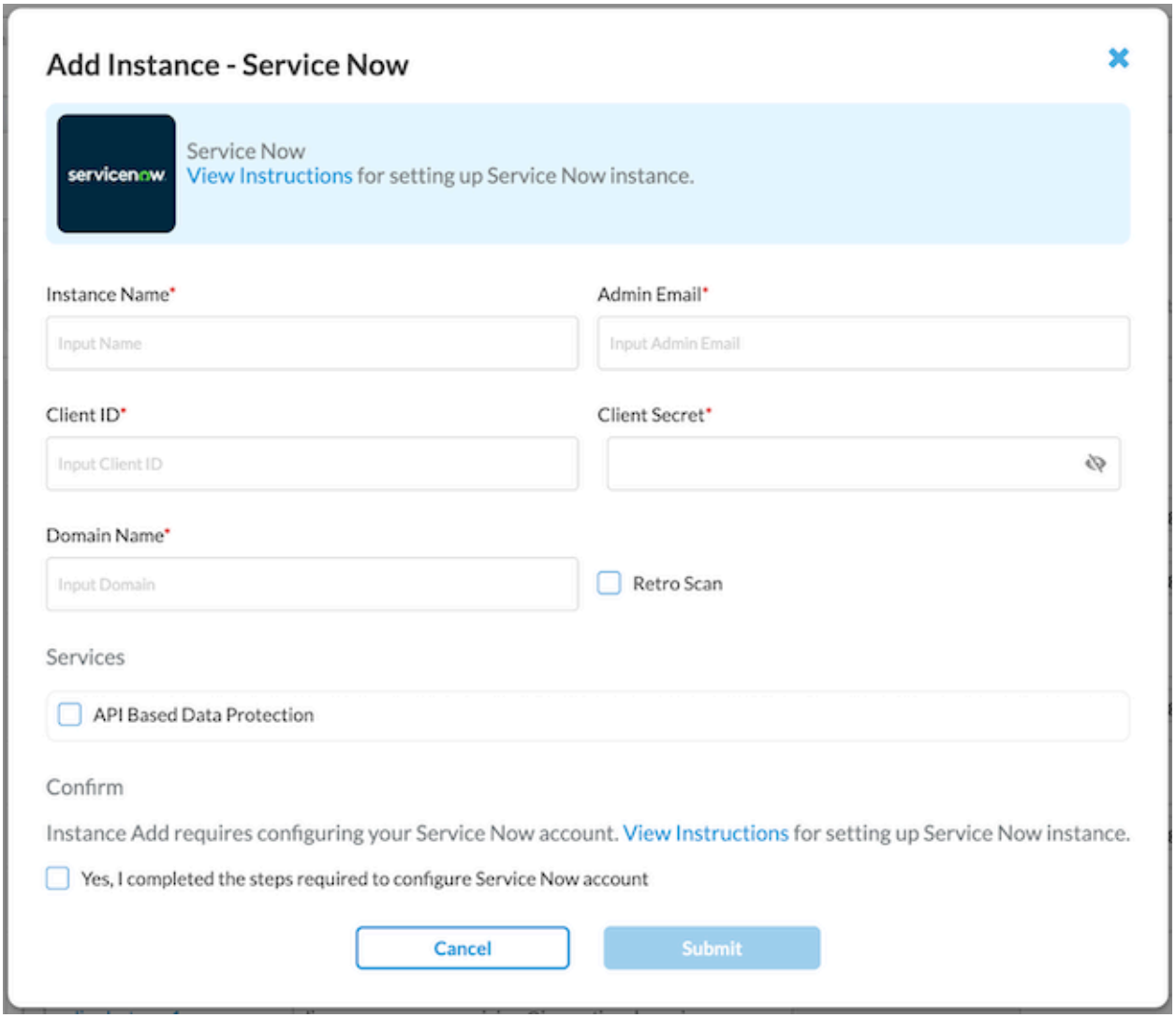


Configure a ServiceNow Connector

1. Navigate to "Configure" > “Advanced Security” > “API Based Data Protection” > “Connectors”.
2. Click the + Add icon, select ServiceNow, then click Next.



3. In the Add Instance window, enter information for the following fields.



Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email (Required)	Enter the email address of the ServiceNow administrator account.
Client ID (Required)	Client ID of the OAuth app created.
Client Secret (Required)	Client secret of the OAuth app created.
Domain Name (Required)	Enter the subdomain of the instance. For example, *companyname*.servicenow.com
Retro Scan	Click to scan and protect all the files and other objects that are present on ServiceNow at the time of connector creation.

Field	Description
Services	Select the services to use for the instance. ◦ API-Based Data Protection—Scan and protect content.
Confirm	Click to confirm that the steps required to configure the ServiceNow account are complete.

4. Click Submit.
5. After adding the instance, select Grant Access to start the OAuth2 process of granting access to the Versa API data protection cloud. This will open a login prompt for the ServiceNow account. Use ServiceNow Administrator credentials to log in and grant access.

Slack API-Based Data Protection

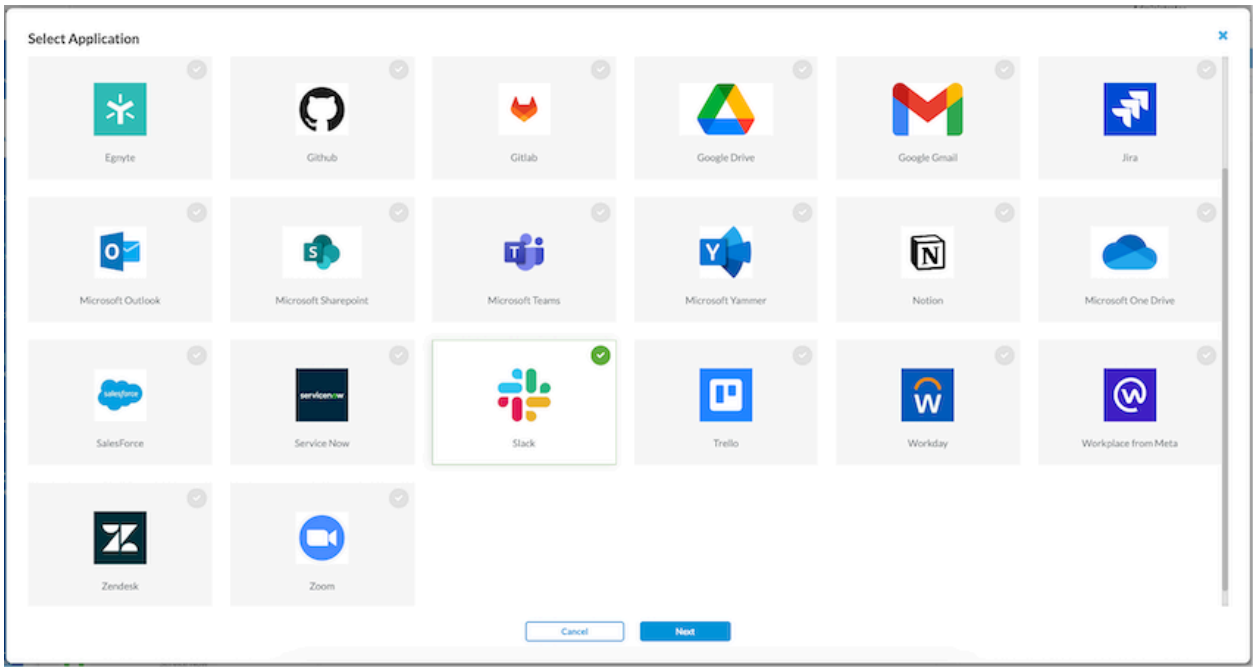
This section describes how to configure the Slack application for API-based data protection.

Configure Slack for API-Based Data Protection

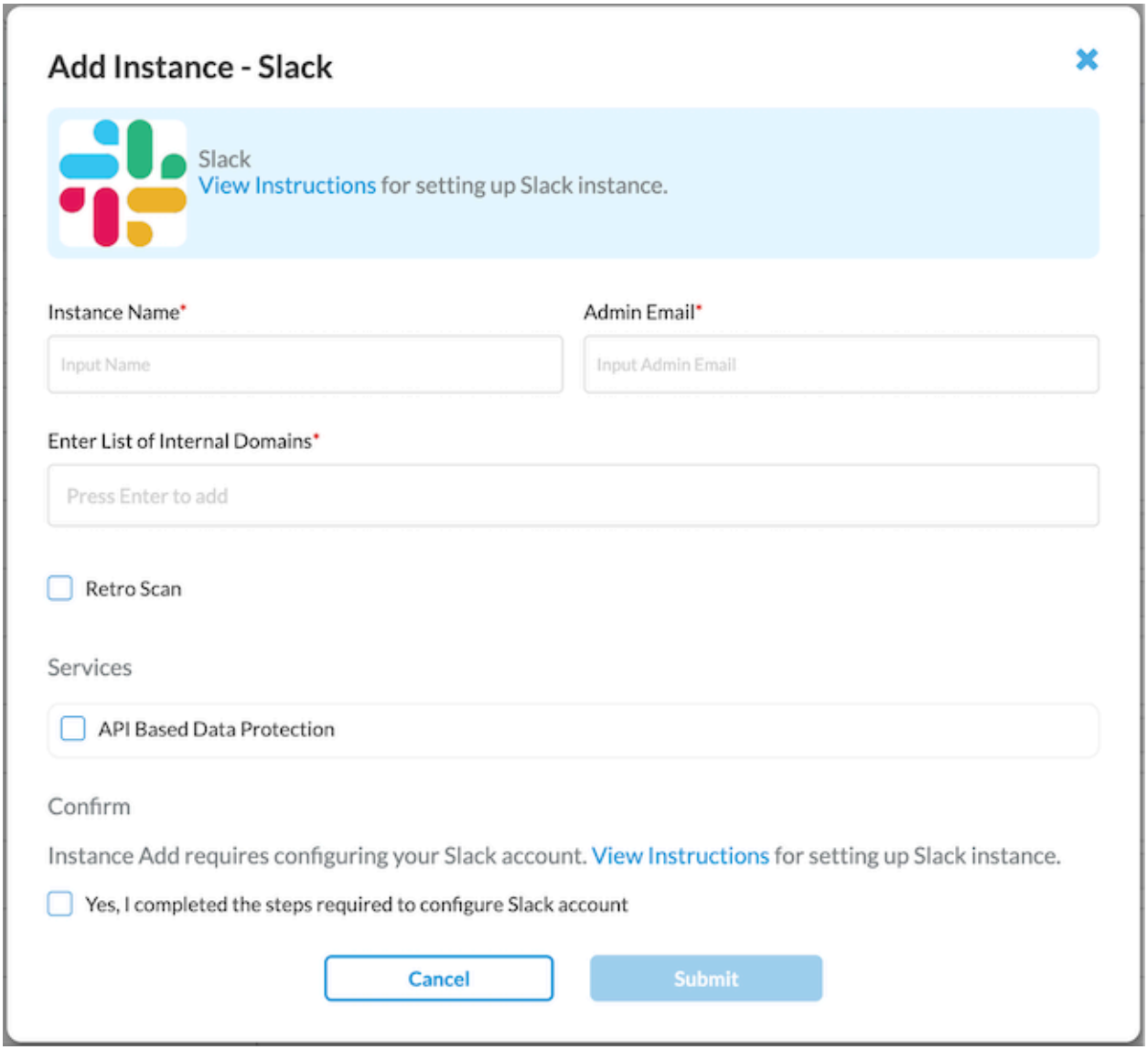
For Slack, no configuration is required.

Configure a Slack Connector

1. Navigate to "Configure" > “Advanced Security” > “API Based Data Protection” > “Connectors”.
2. Click the + Add icon, select ServiceNow, then click Next.



3. In the Add Instance window, enter information for the following fields.



Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email (Required)	Enter the email address of the Slack administrator account.
Enter List of Internal Domains (Required)	Enter domains configured for the organization.
Retro Scan	Click to scan and protect all the files and other objects that are present on Slack at the time of connector creation.

Field	Description
Services	Select the services to use for the instance. ◦ API-Based Data Protection—Scan and protect content.
Confirm	Click to confirm that the steps required to configure the Slack account are complete.

4. Click Submit.
5. After adding the instance, select Grant Access to start the OAuth2 process of granting access to the Versa API data protection cloud. This will open a login prompt for the Slack account. Use Slack Administrator credentials to log in and grant access.

Trello API-Based Data Protection

This section describes how to configure the Trello application for API-based data protection.

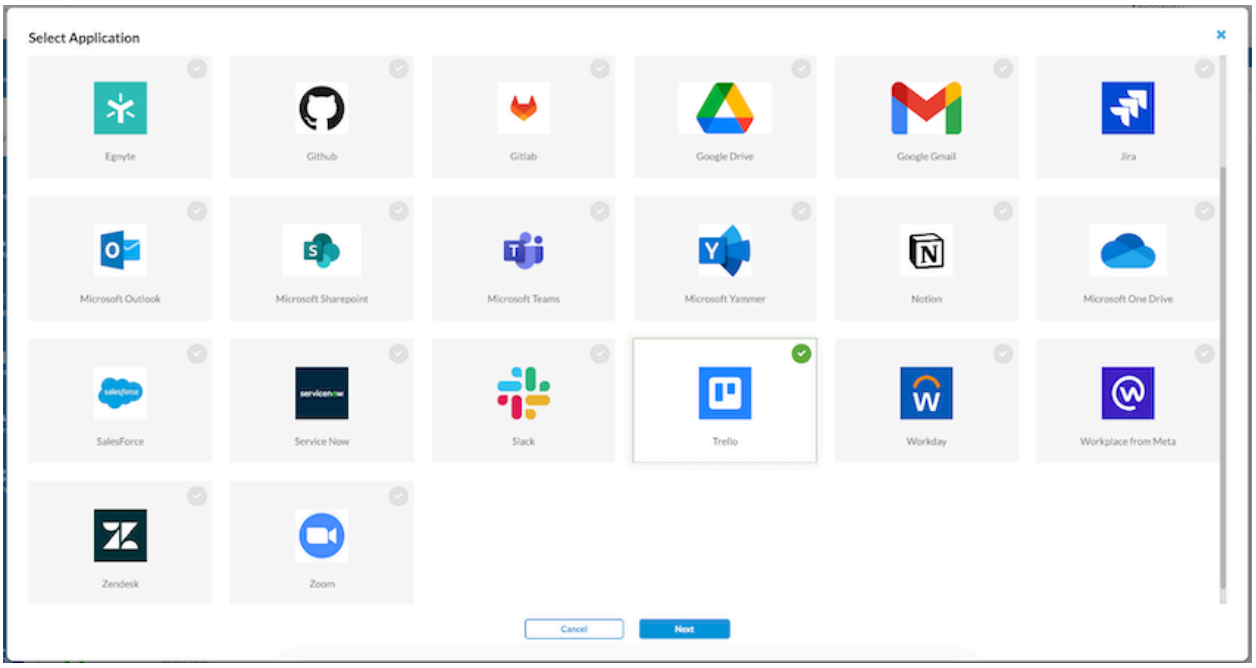
Configure Trello for API-Based Data Protection

For Trello, no configuration is required.

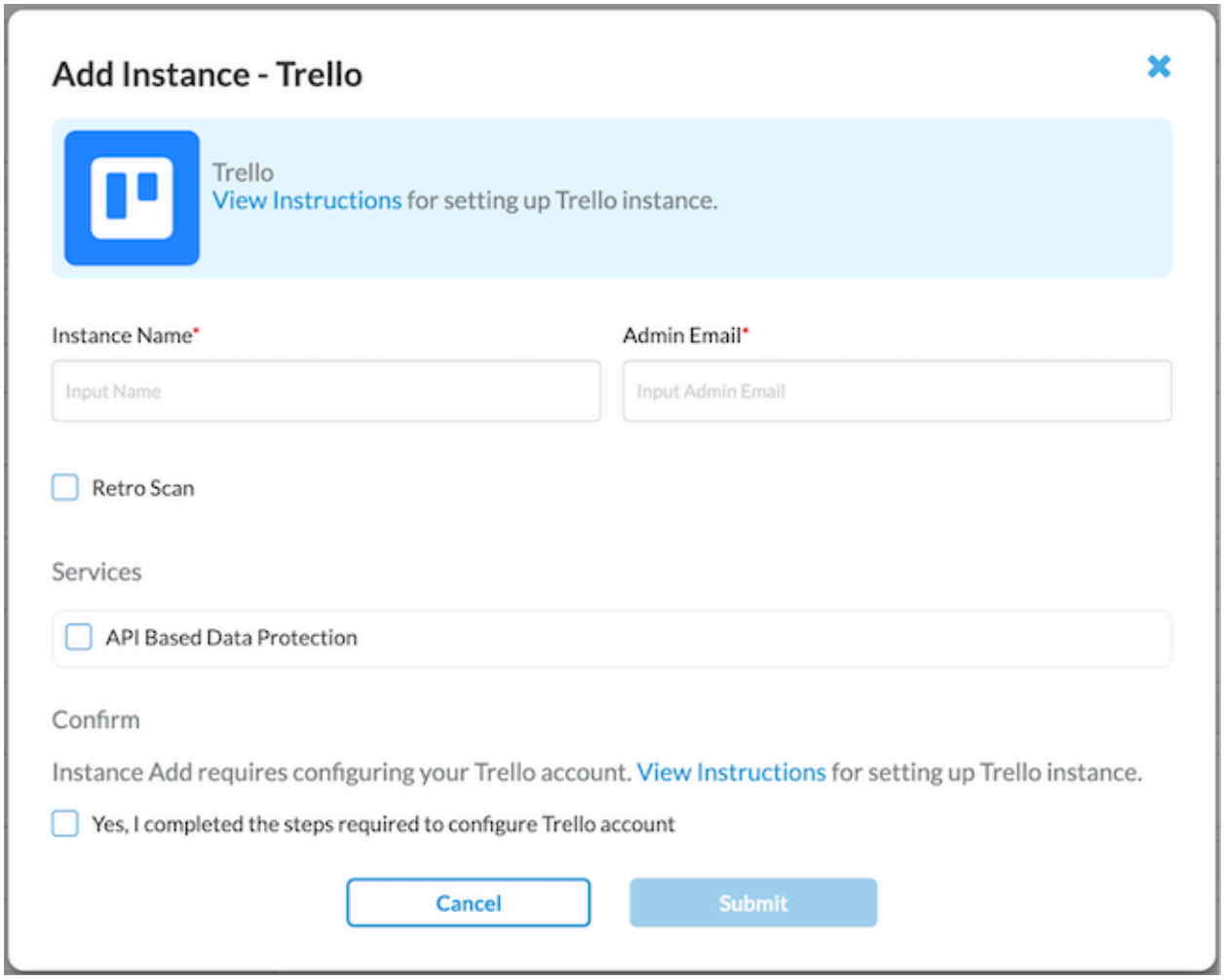
Configure a Trello Connector

To configure a Trello connector:

1. Navigate to "Configure" > “Advanced Security” > “API Based Data Protection” > “Connectors”.
2. Click the + Add icon, select ServiceNow, then click Next.



3. In the Add Instance window, enter information for the following fields.



Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email (Required)	Enter the email address of the Trello administrator account.
Retro Scan	Click to scan and protect all the files and other objects that are present on Trello at the time of connector creation.
Services	Select the services to use for the instance. ◦ API-Based Data Protection—Scan and protect content.
Confirm	Click to confirm that the steps required to configure the Trello account are complete.

4. Click Submit.
5. After adding the instance, click “Grant Access” to start the OAuth 2.0 process of granting access to the Versa API-DP cloud. This will open a login prompt for the Trello account. Use administrator credentials to log in and grant access.

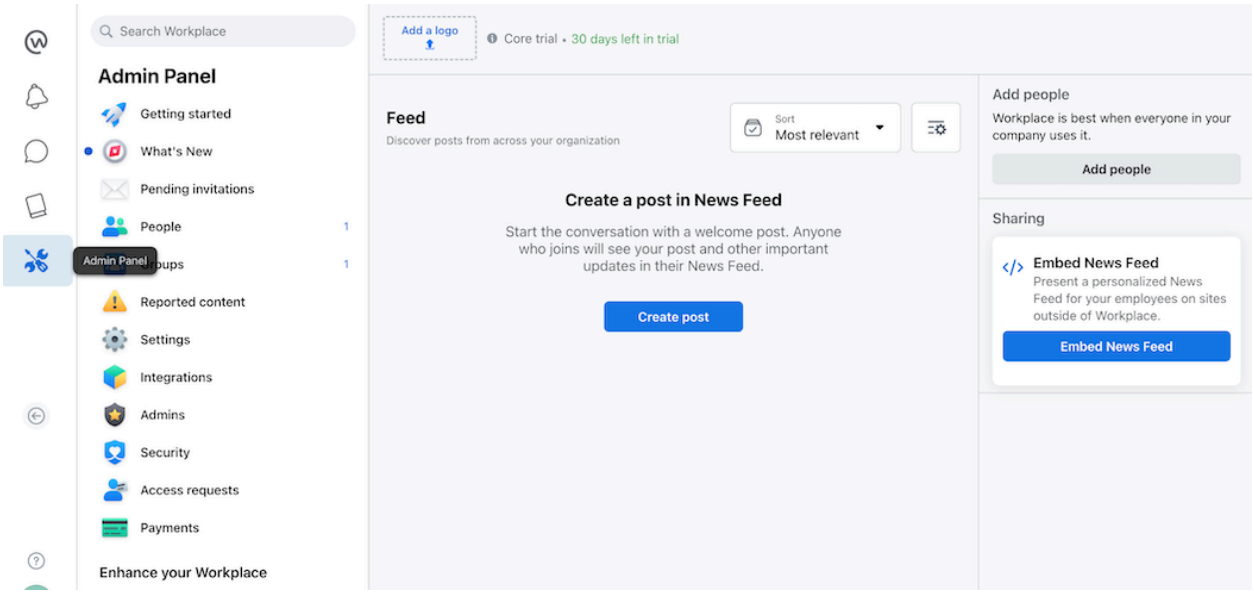
Workplace from Meta API-Based Data Protection

This section describes how to configure the Workplace from Meta application for API-based data protection.

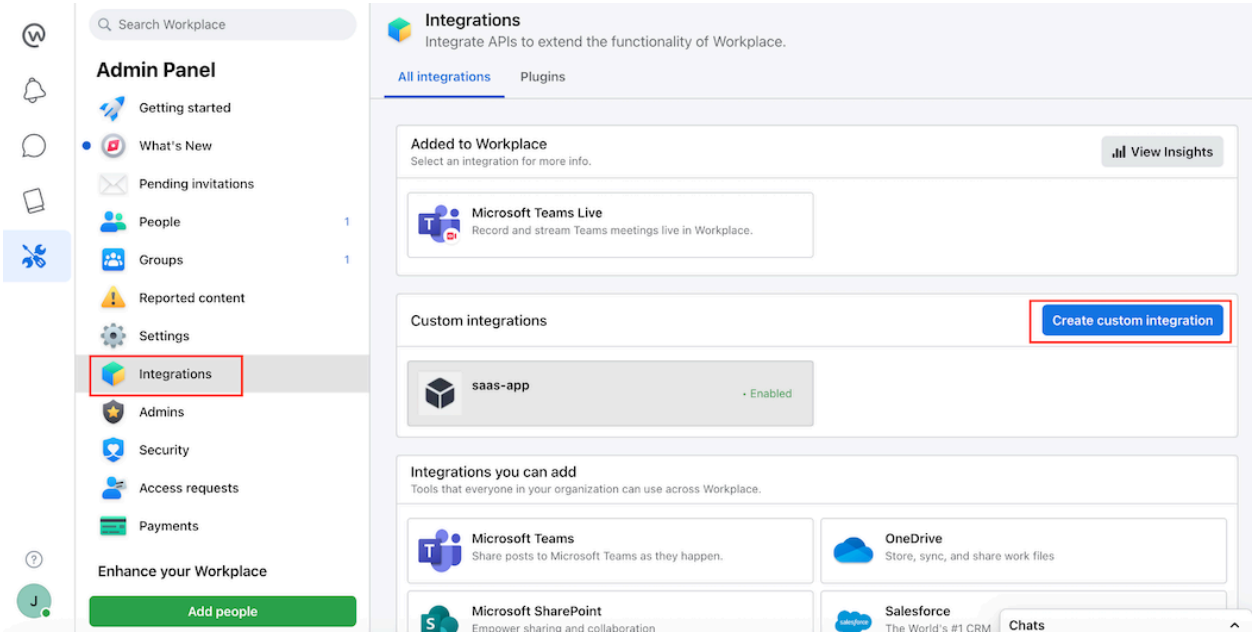
Configure a Workplace Custom Integration

To configure a Workplace custom integration:

1. Login with admin credentials at https://www.workplace.com/.
2. Click Admin Panel in the left menu bar.

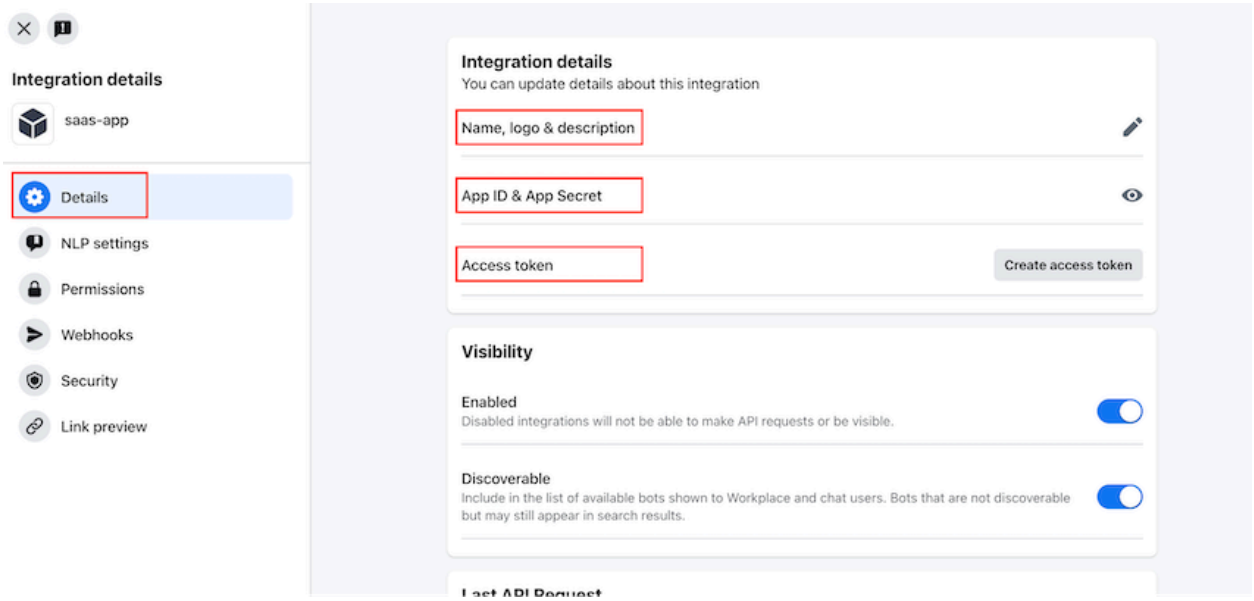


3. Click Integrations under the Admin Panel, then click Create custom integration in the main pane. Specify a name and a description, then click Create to create the custom integration.



4. In the custom integration you created, access the App ID, Client ID, and access token from “Details” in the left menu bar.

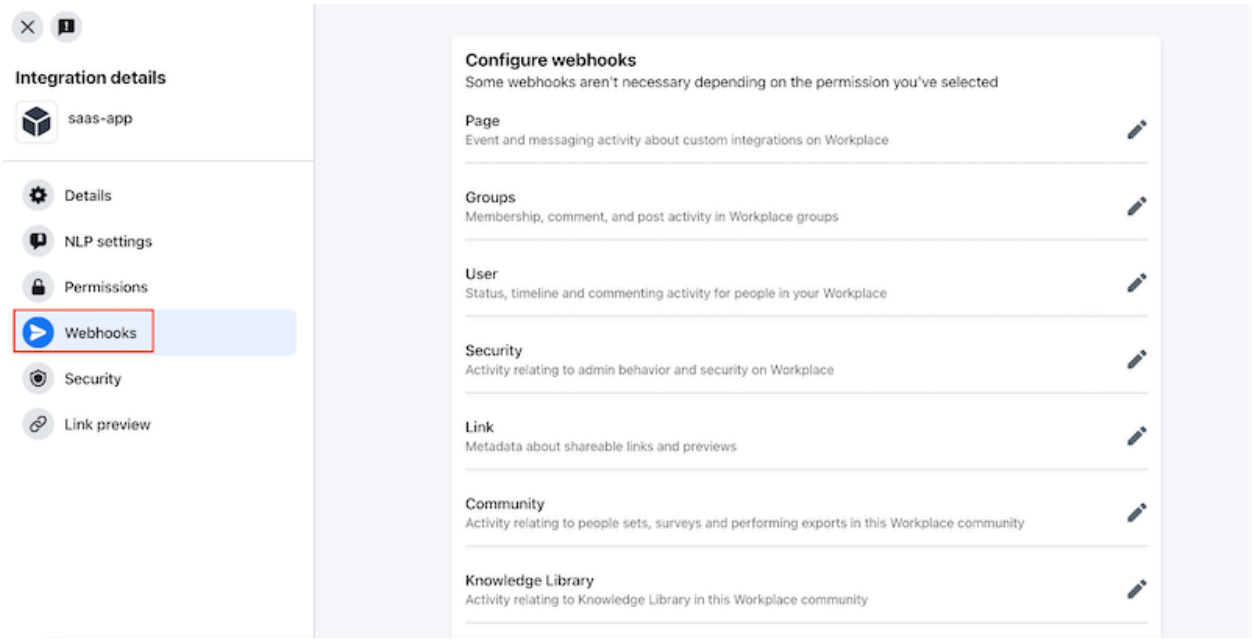
   Note: Custom integrations do not support the OAuth2 flow; as a result, you must use access token shown in this step. This access token does not expire.



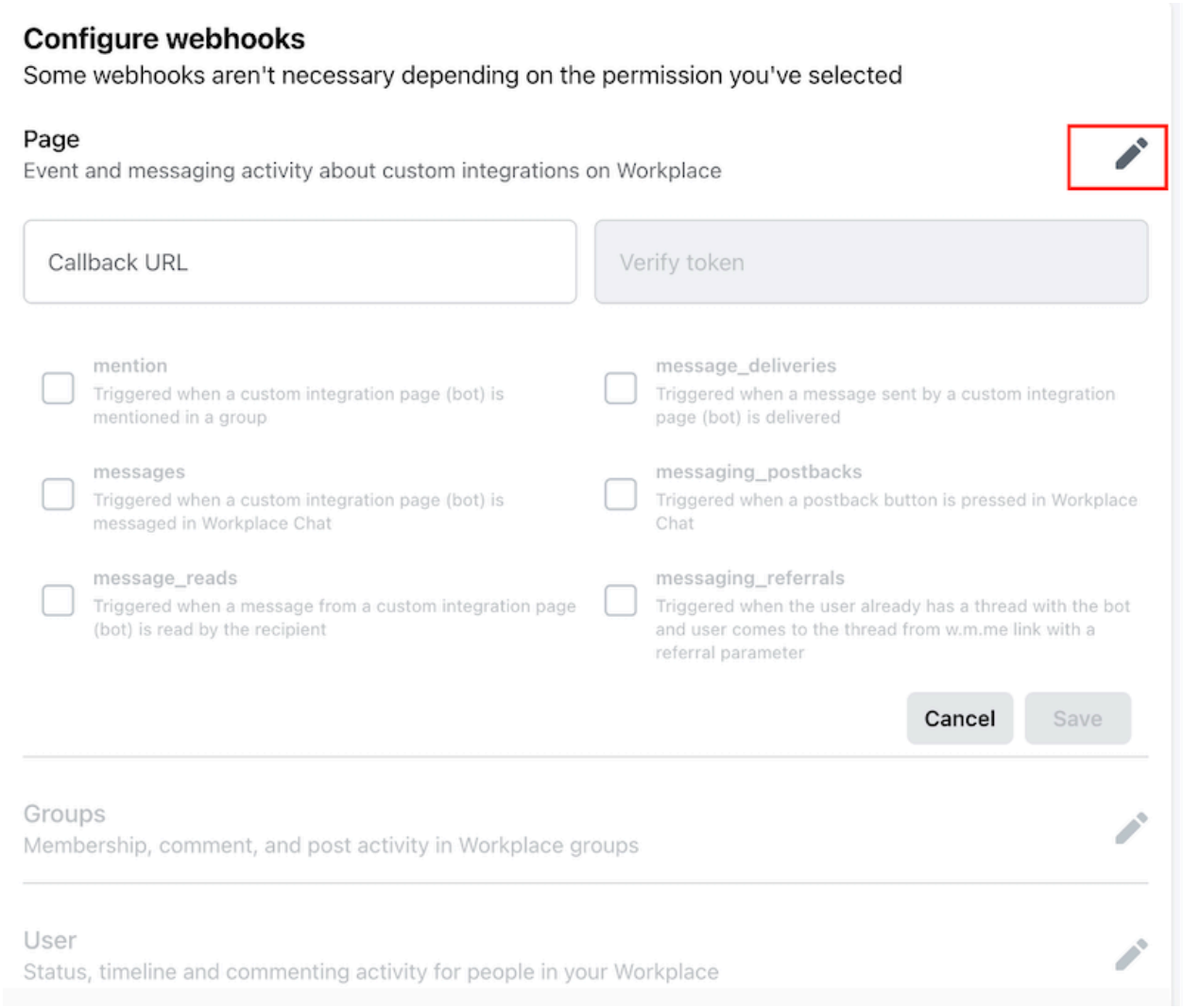
Configure Workplace Custom Integration Webhooks

To configure Workplace custom integration webhooks:

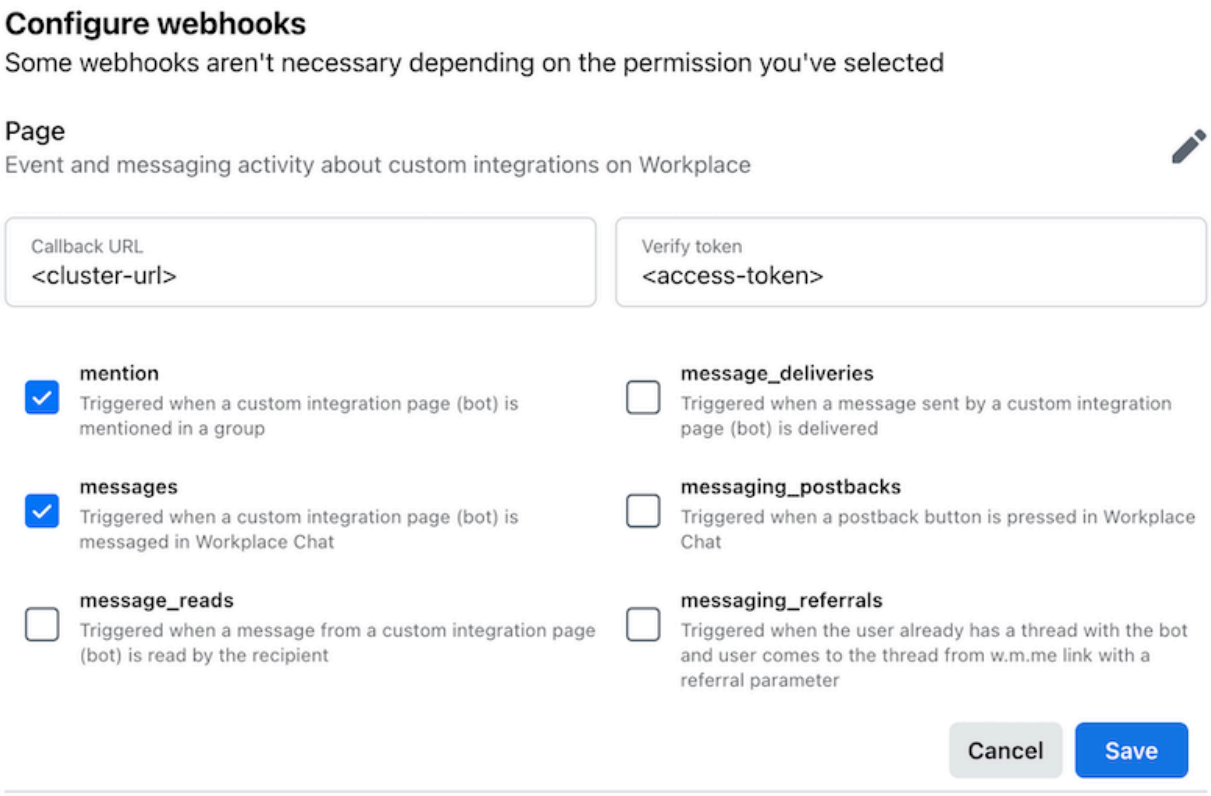
1. In the application window, click Webhooks in the left menu bar.



2. In the webhooks window, configure individual webhooks by clicking the Edit icon next to the resource name.



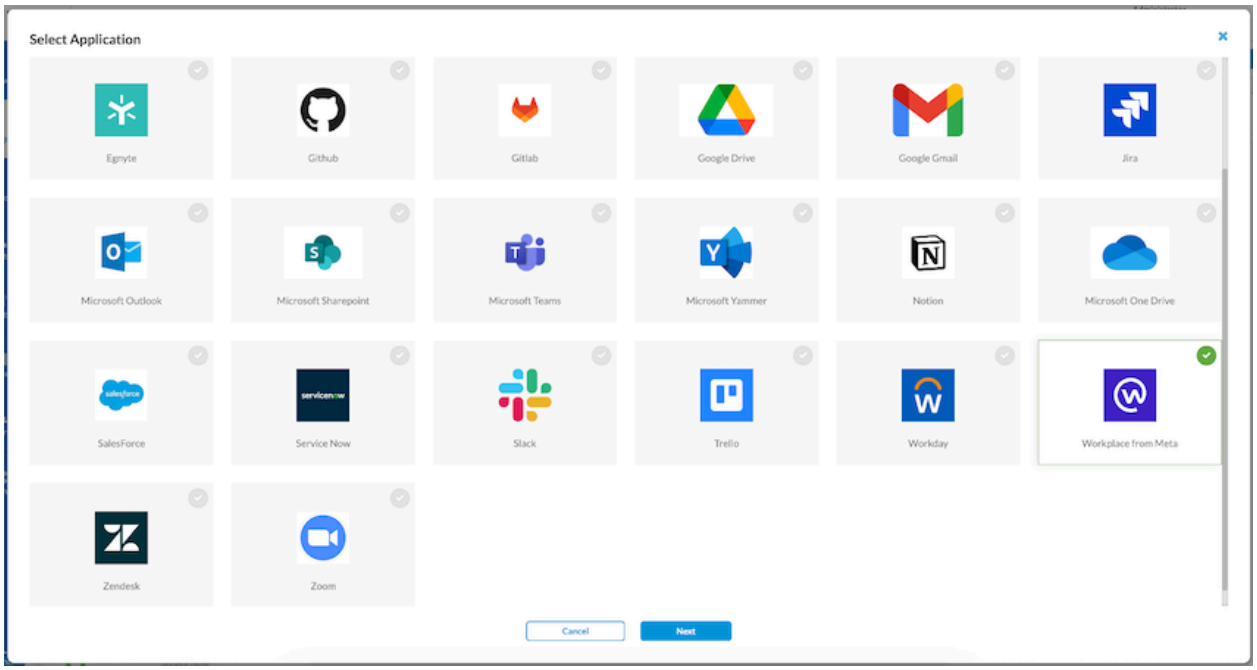
3. Specify the same callback URL and access token for all desired webhooks, select the desired sub-resources, then click Save.



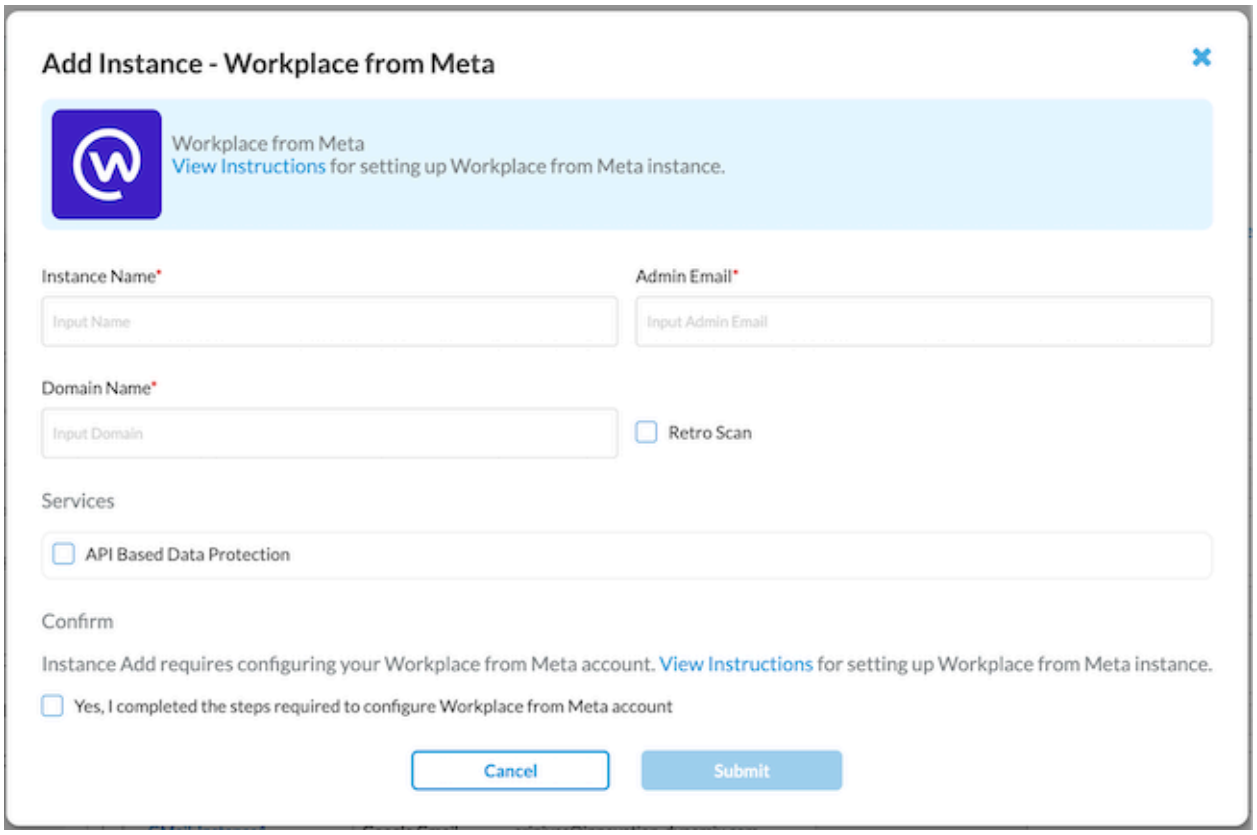
Configure a Workplace from Meta Connector

To configure a Workplace from Meta connector:

1. Navigate to "Configure" > “Advanced Security” > “API Based Data Protection” > “Connectors”.
2. Click the + Add icon, select Workplace from Meta, then click Next.



3. In the Add Instance window, enter information for the following fields.



Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email (Required)	Enter the email address of the Workplace from Meta administrator account.
Domain Name	Enter the domain name of your Workplace from Meta community, for example <*domain*>.workplace.com.
Retro Scan	Click to scan and protect all the files and other objects that are present on Workplace from Meta at the time of connector creation.
Services	Select the services to use for the instance. ◦ API-Based Data Protection—Scan and protect content.
Confirm	Click to confirm that the steps required to configure the Workplace from Meta account are complete.

4. Click Submit.
5. After adding the instance, click “Grant Access” to start the OAuth 2.0 process of granting access to the Versa API-DP cloud. This will open a login prompt for the Workplace from Meta account. Use administrator credentials to log in and grant access.

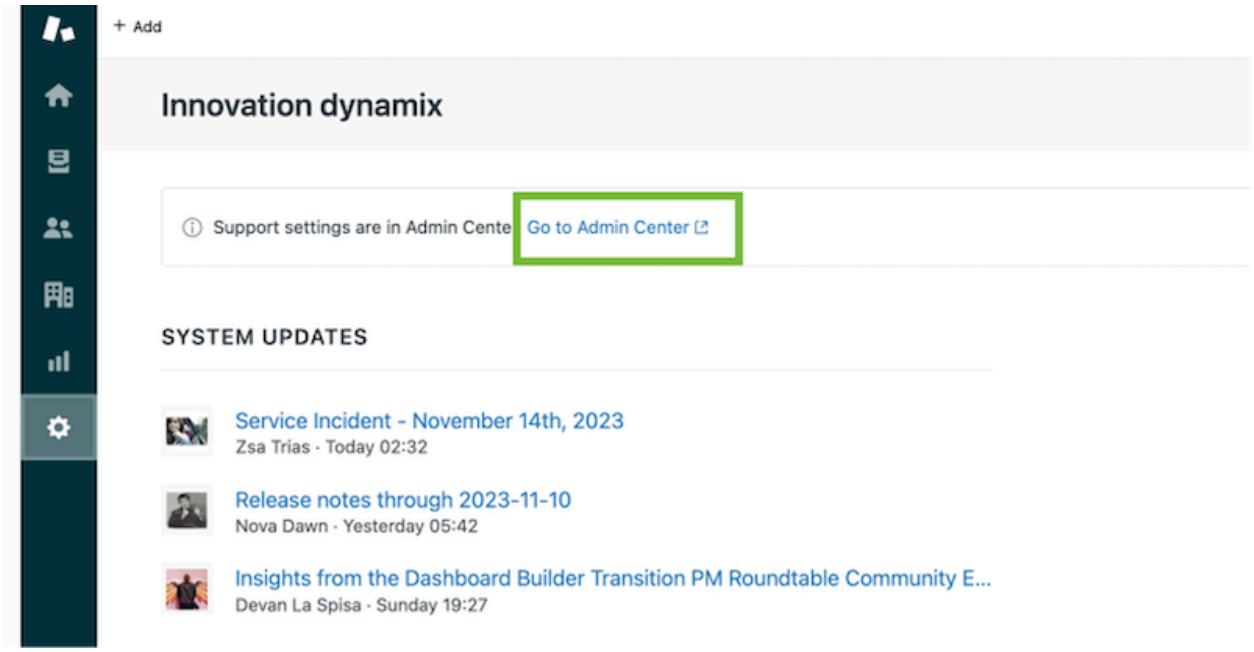
Zendesk API-Based Data Protection

This section describes how to configure the Zendesk application for API-based data protection.

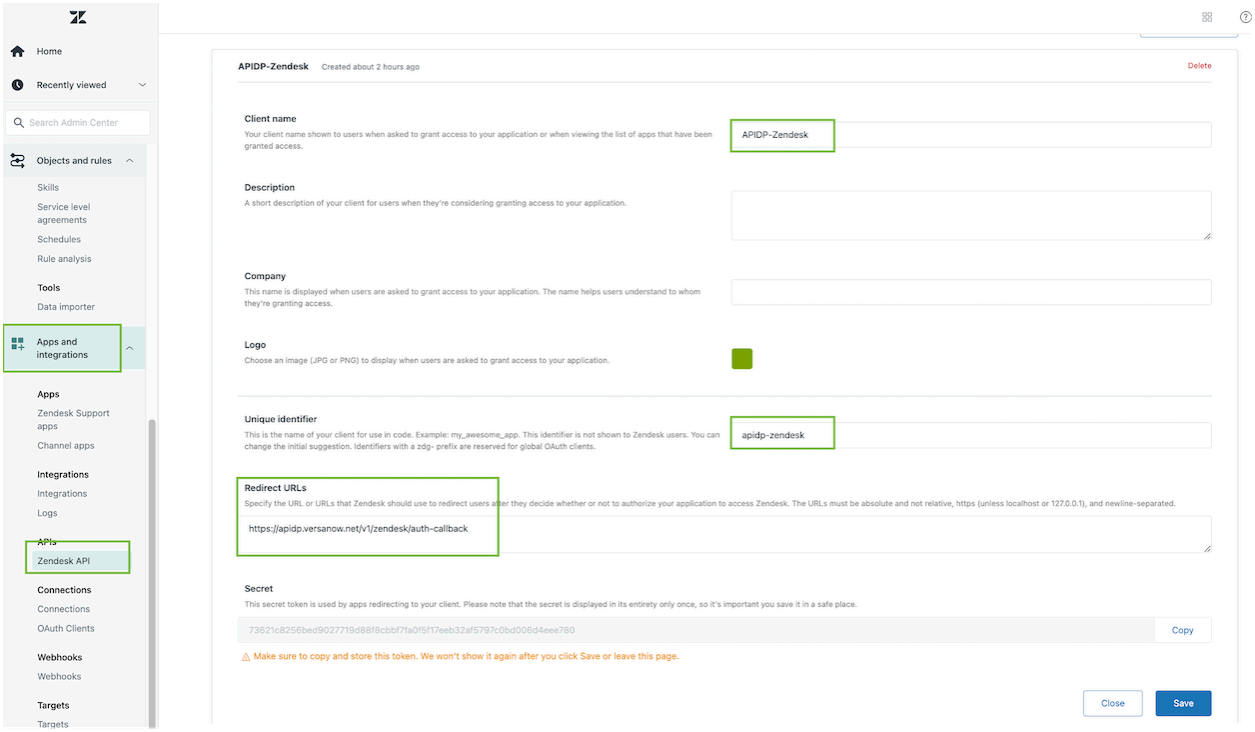
Configure Zendesk for API-Based Data Protection

To configure Zendesk for API-based data protection:

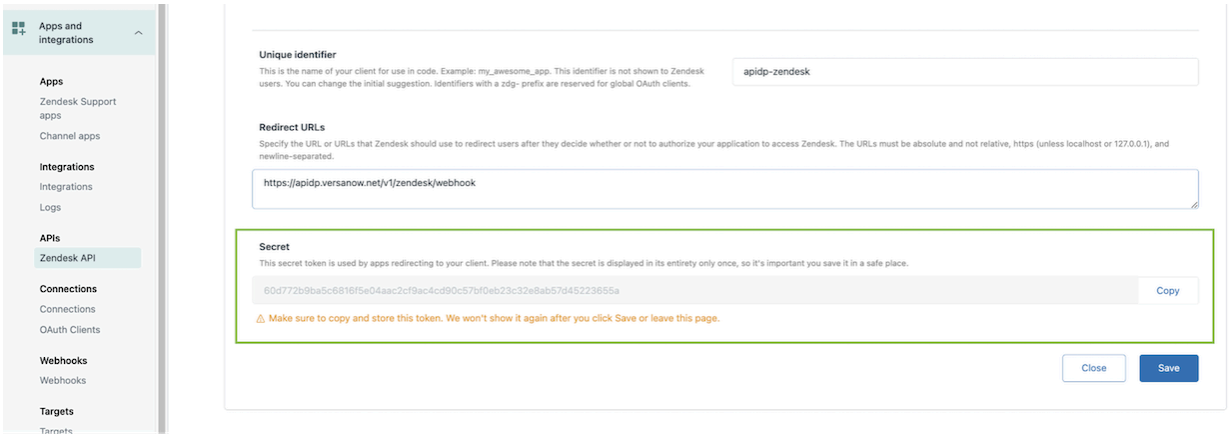
1. Go to the Admin center.



2. Add the OAuth client by navigating to Admin Center > APIs > Zendesk API > OAuth Client > Add OAuth Client.

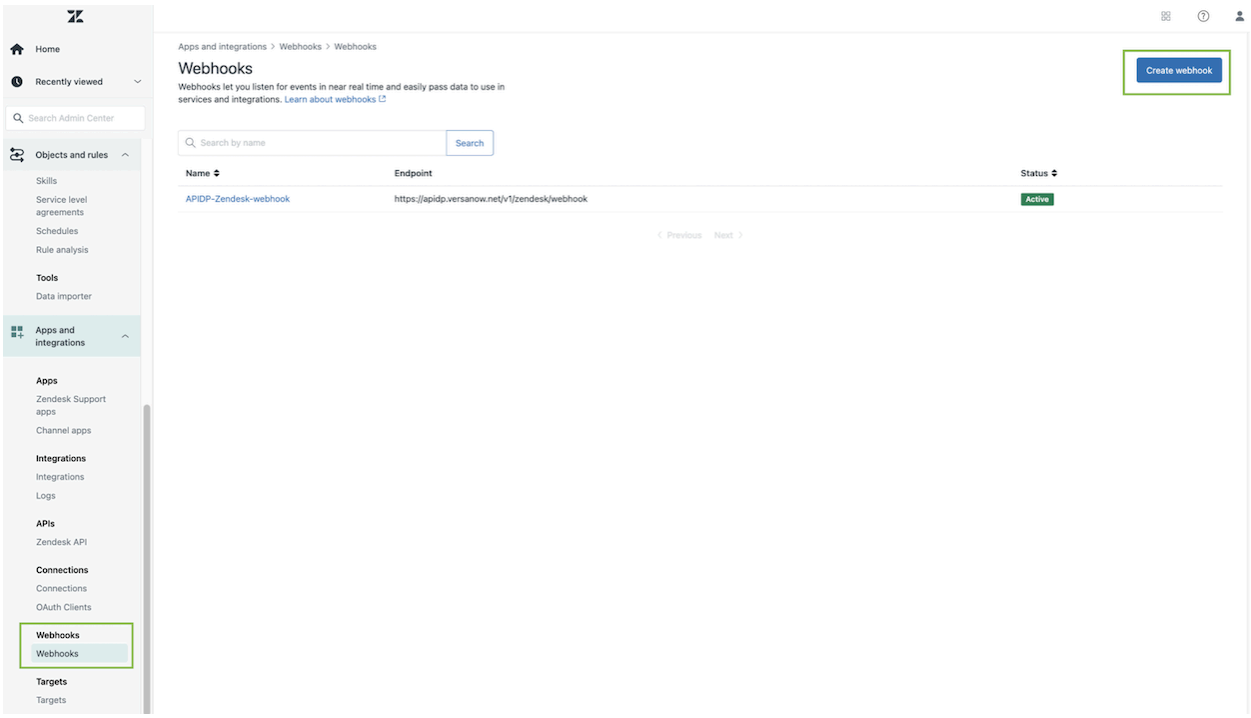


3. Set the unique identifier and redirect URLs, then generate the secret.

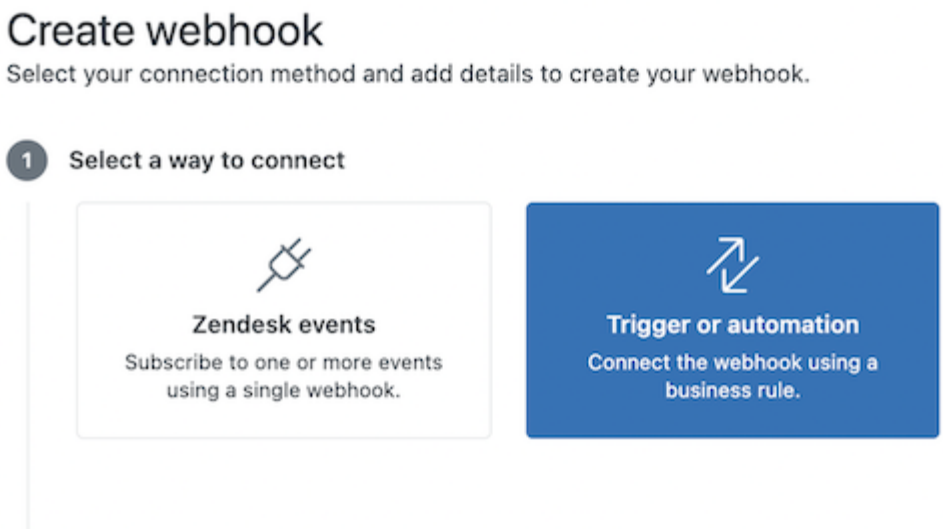


The secret now needs to be stored. The unique identifier and the secret are the client-id and client-secret used to grant access.

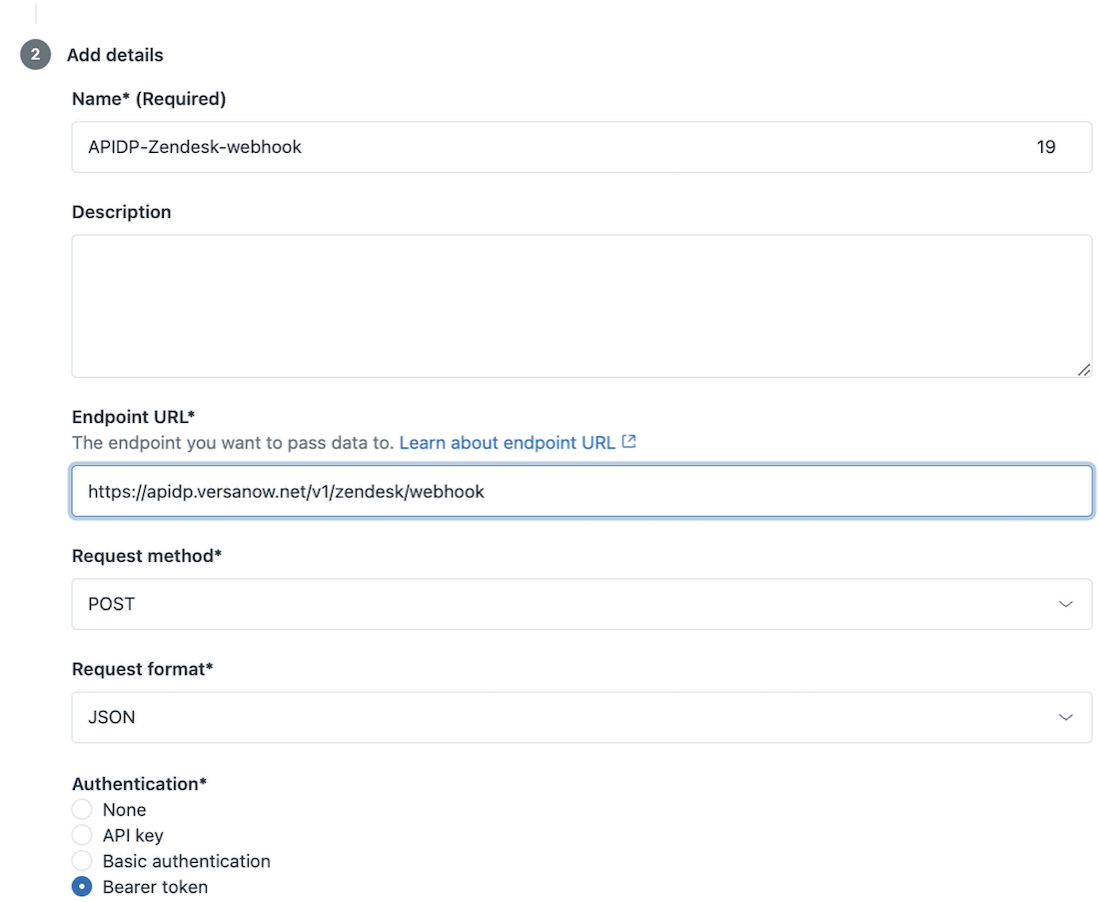
4. Go to Apps and integrations -> Webhooks -> Webhooks.
5. Click the Create Webhook button in the upper right corner of the screen.



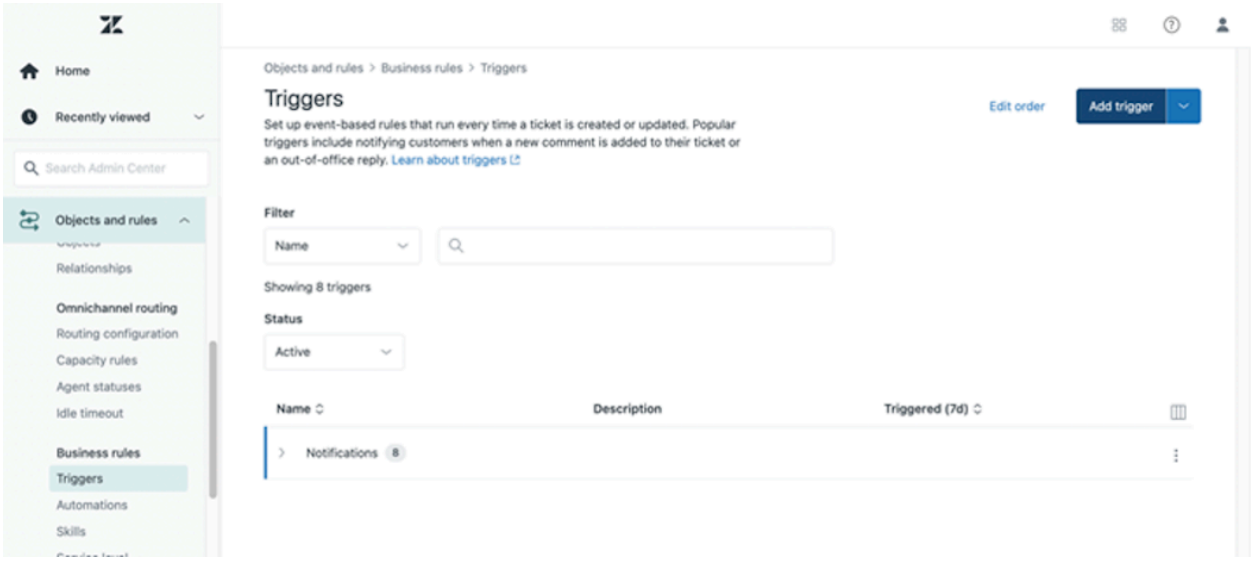
6. In the Create Webhook screen, select Trigger or Automation.



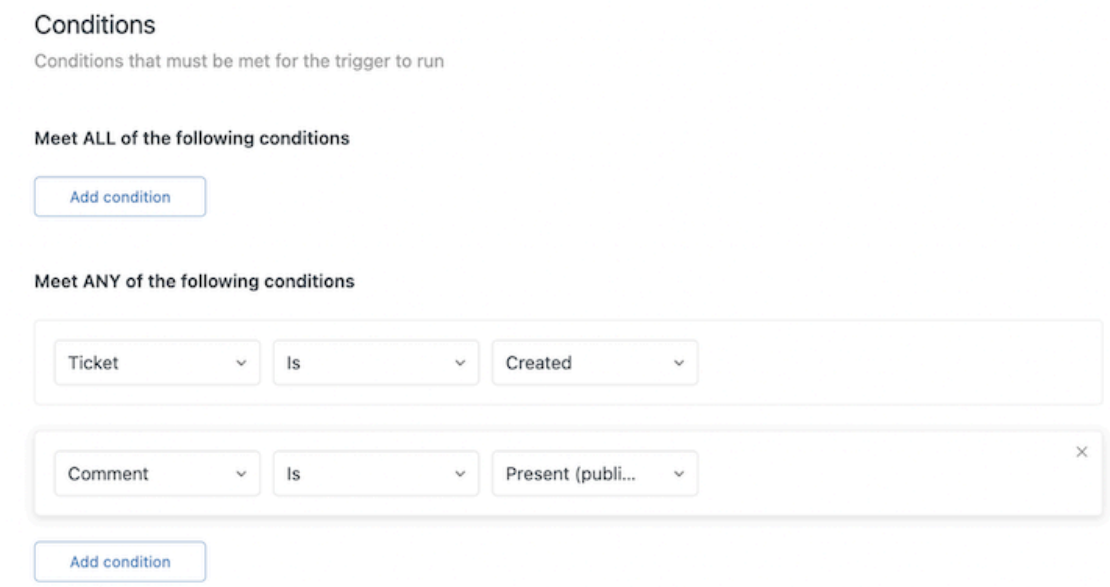
7. Under Add Details, enter the following information:
    a. Enter the Endpoint URL
    b. Select POST as the request method
    c. Select JSON as the request format
8. Set Auth data using token or id and secret (basic authentication)



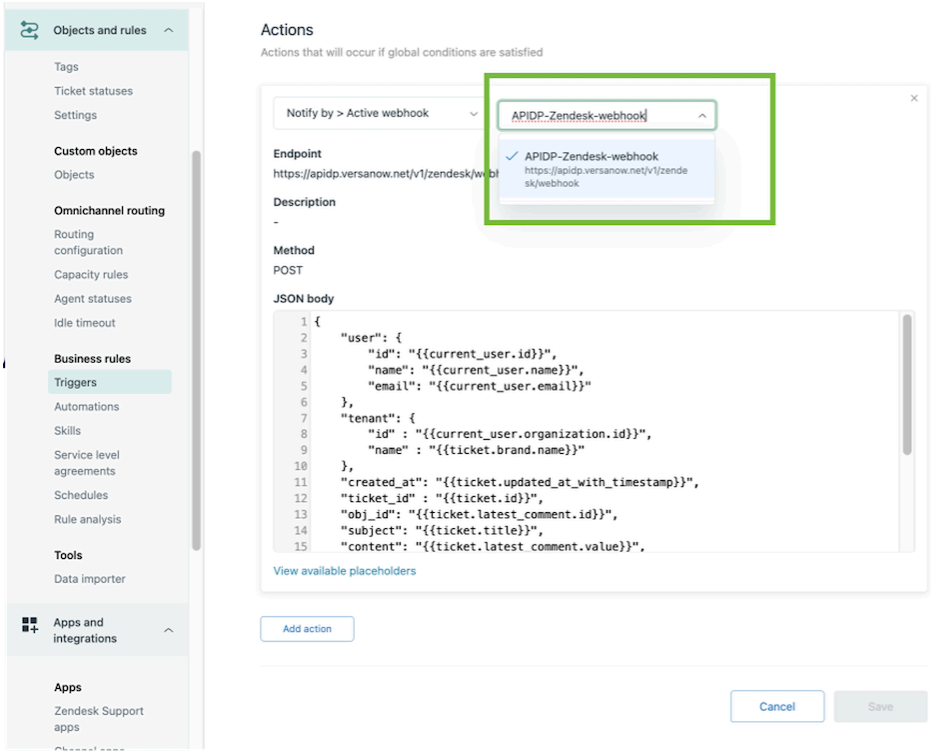
9. Select Business Rules > Triggers in the left menu bar. In the Triggers screen, click the Add Trigger button in the upper right corner.



10. Add conditions when event happens (in this case, a comment is created/updated).



11. For Actions, choose the webhook you created.



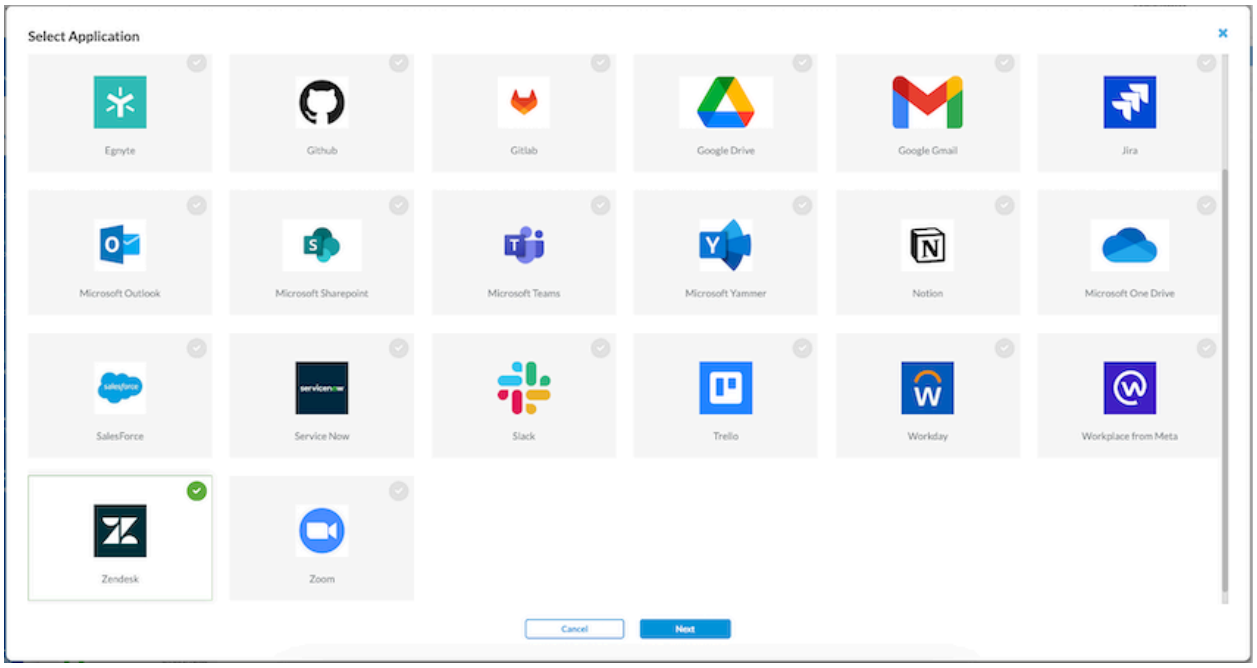
12. Customize the JSON body.

```
{
   "user": {
      "id": "{{current_user.id}}",
      "name": "{{current_user.name}}",
      "email": "{{current_user.email}}"
   },
   "tenant": {
                  "id" : "{{current_user.organization.id}}",
                  "name" : "{{ticket.brand.name}}"
   },
         "created_at": "{{ticket.updated_at_with_timestamp}}",
         "ticket_id" : "{{ticket.id}}",
         "obj_id": "{{ticket.latest_comment.id}}",
   "subject": "{{ticket.title}}",
   "content": "{{ticket.latest_comment.value}}",
   "attachments": [
      {% for attachment in ticket.latest_comment.attachments %}
         {
            "name": "{{attachment.filename}}",
            "url": "{{attachment.url}}"
         }{% unless forloop.last %},{% endunless %}
      {% endfor %}
   ]
}
```

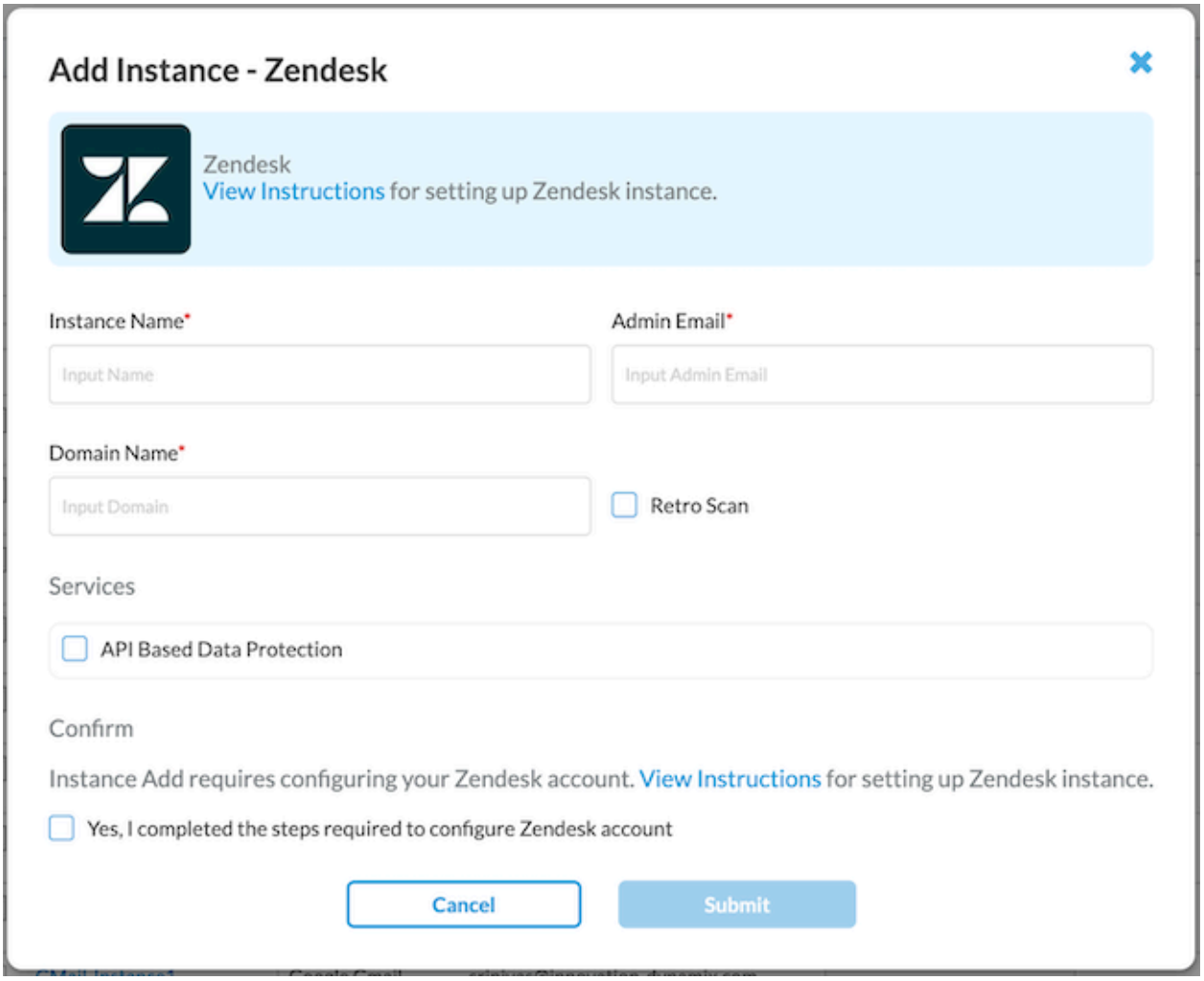
Configure a Zendesk Connector

To configure a Zendesk connector:

1. Navigate to "Configure" > “Advanced Security” > “API Based Data Protection” > “Connectors”.
2. Click the + Add icon, select Zendesk, then click Next.



3. In the Add Instance window, enter information for the following fields.



Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email (Required)	Enter the email address of the Zendesk administrator account.
Domain Name (Required)	Enter the domain name of your Zendesk account.
Retro Scan	Click to scan and protect all the files and other objects that are present
Services	Select the services to use for the instance. ◦ API-Based Data Protection—Scan and protect content.
Confirm	Click to confirm that the steps required to configure the Zendesk accou

4. Click Submit.

5. After adding the instance, click “Grant Access” to start the OAuth 2.0 process of granting access to the Versa API-DP cloud. This will open a login prompt for the Zendesk account. Use administrator credentials to log in and grant access.

Zoom API-Based Data Protection

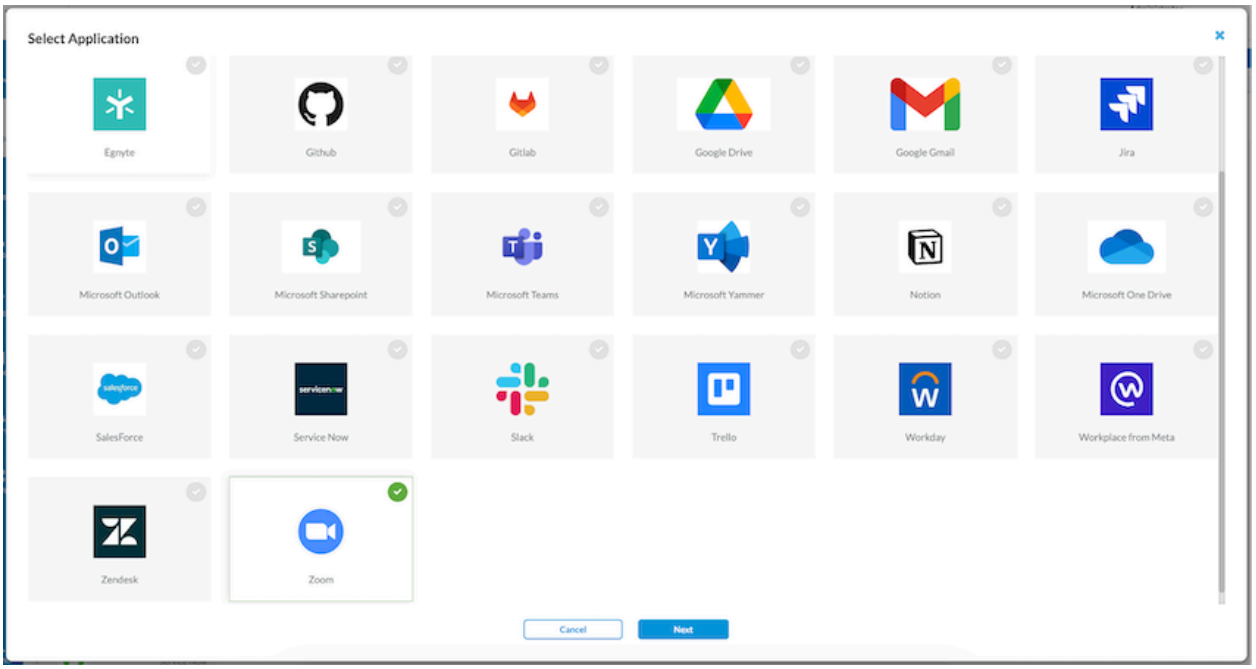
This section describes how to configure the Zoom application for API-based data protection.

Configure Zoom for API-Based Data Protection

For Zoom, no configuration is required.

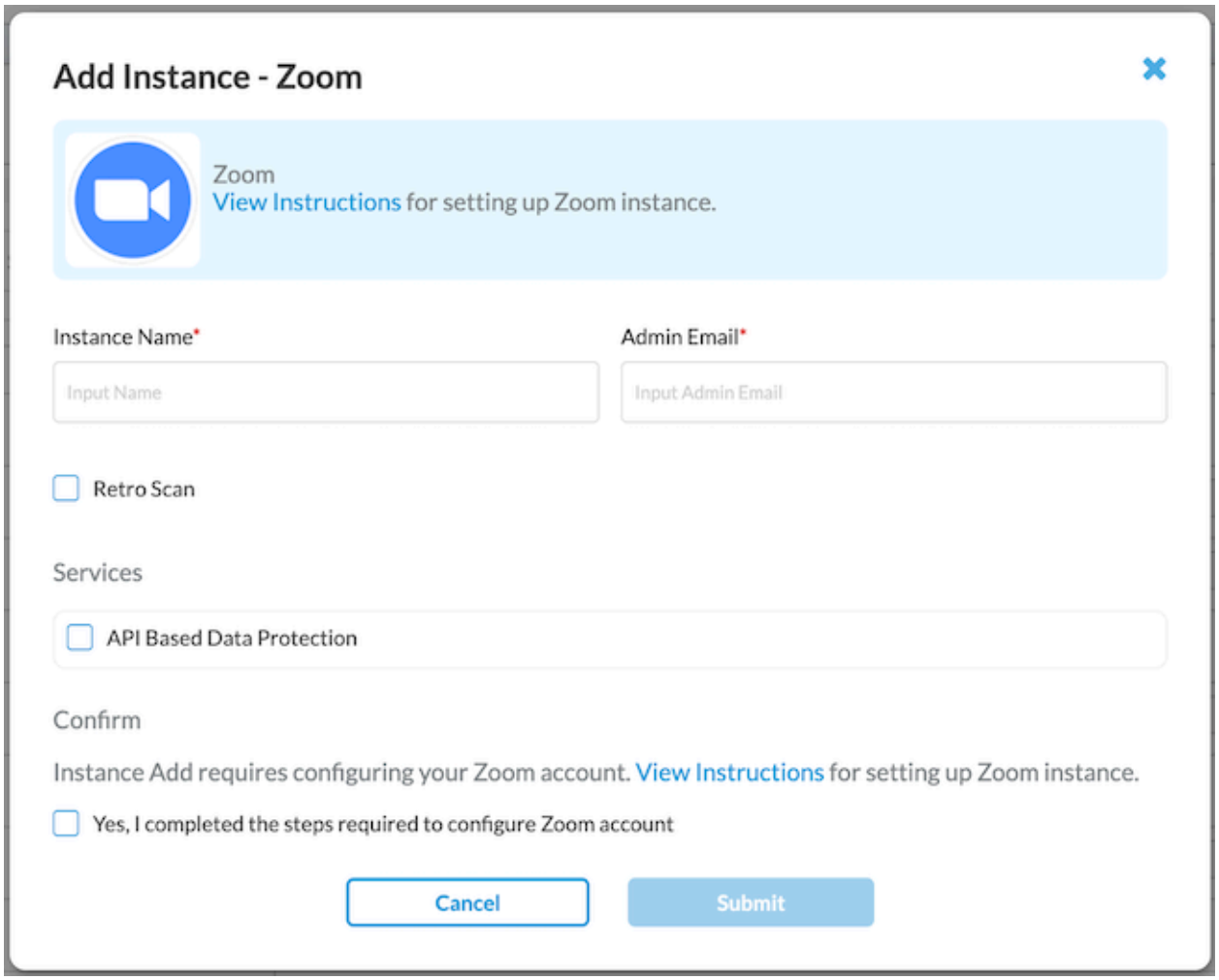
Configure a Zoom Connector

1. Navigate to "Configure" > “Advanced Security” > “API Based Data Protection” > “Connectors”.
2. Click the + Add icon, select Zoom, then click Next.



3. In the Add Instance window, enter information for the following fields.

Updated: Wed, 23 Oct 2024 08:39:56 GMT



Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email (Required)	Enter the email address of the Zoom administrator account.
Retro Scan	Click to scan and protect all the files and transcripts that are present on Zoom at the time of connector creation.
Services	Select the services to use for the instance. ◦ API Based Data protection: Scan and protect content.
Confirm	Click to confirm that the steps required to configure the Zoom account are complete.

4. Click Submit.
5. After adding the instance, select Grant Access to start the OAuth2 process of granting access to the Versa API data protection cloud. This will open a login prompt for the Zoom account. Use Zoom Administrator credentials to log in and grant access.

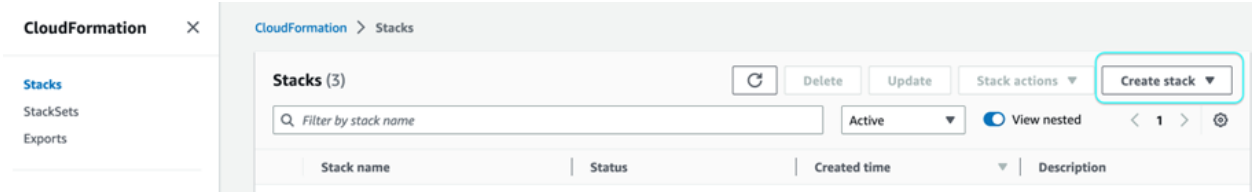
Amazon Web Services API-Based Data Protection

This section describes how to configure Amazon Web Services for API-based data protection.

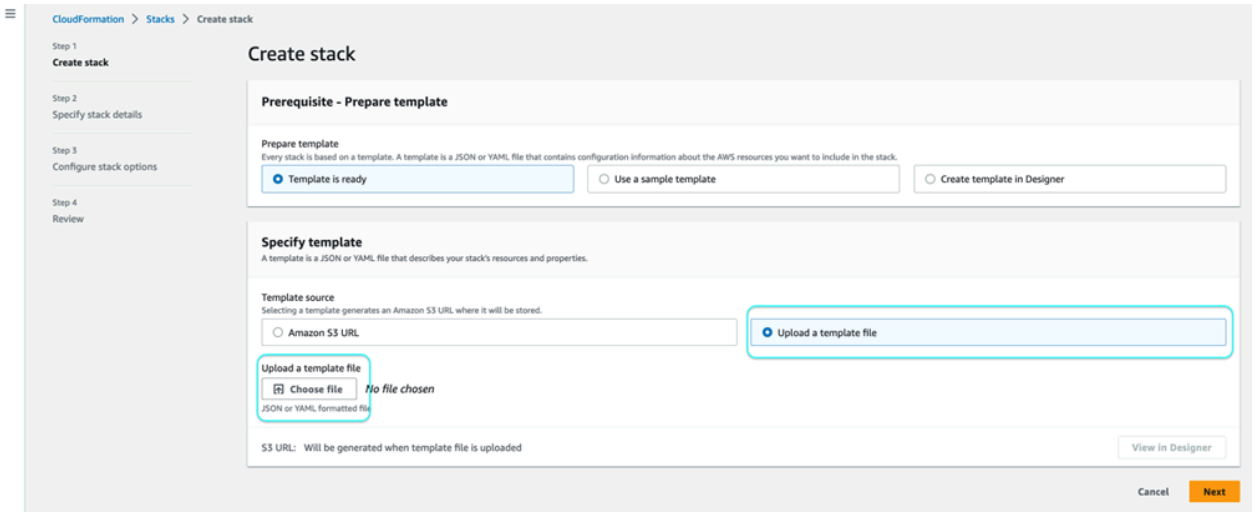
Configure Amazon Web Services for API-Based Data Protection

To configure a new instance for Amazon Web Services:

1. Log in to https://aws.amazon.com/console/ using administrator credentials.
2. Set up cross-account access between Versa API data protection and AWS accounts. API data protection requires permissions to assume a role and scan AWS resources. To set up cross-account access, download the CFT and upload it to a new Cloud Formation Stack in each AWS account.
3. Select Services > CloudFormation > Stacks in the left menu bar, and click Create Stack.



4. Select Upload a template file, click Choose file, and upload the versa-apidp-aws-stack-role.yaml file. Click Next.

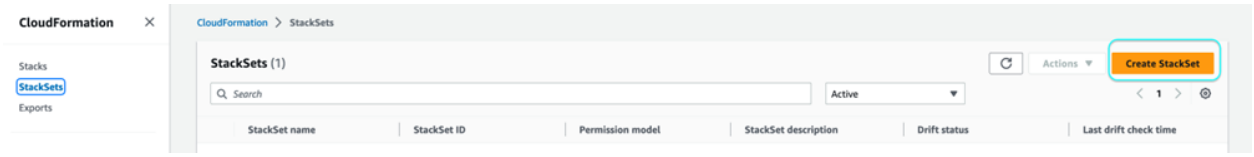


5. In the Specify stack details page, enter a Stack name and click Next.
6. In the Configure stack options page, use the default configuration and click Next.
7. Review stack details on the Review page, click the acknowledgment, and then click Create stack. The new stack

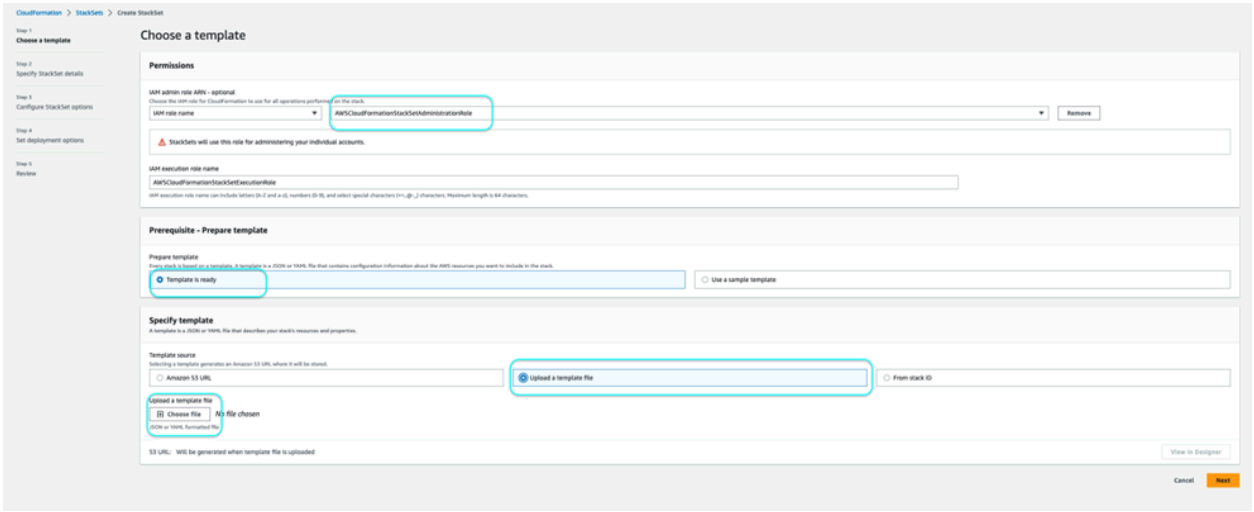
displays on the CloudFormation page.

a. Click the stack to view stack details.
b. Click the Resource tab to view the various components that are part of versa-apidp-aws-stack-role.yaml.
c. Click the Template tab to view the permissions defined in the template.

8. In the CloudFormation page, select StackSets in the left menu bar, and click Create StackSet.



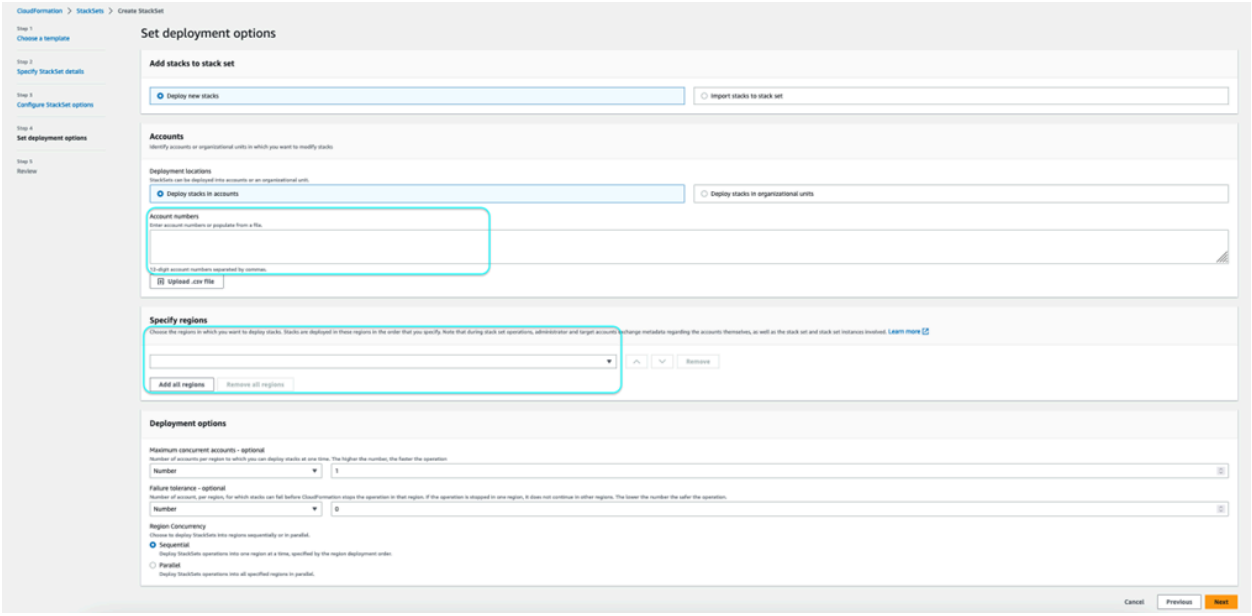
9. Enter information for the following fields and click Next.



Field	Description
IAM Role Name	Enter IAM role name as AWSCloudFormationStackSetAdministrationRole.
IAM Execution Role Name	Ensure IAM execution role name is AWSCloudFormationStackSetExecutionRole
Specify Template	Select Upload a template file.
Upload a Template File	Click Choose file, and upload the versa-apidp-aws-stackset-setup.yaml file.

10. In the Specify StackSet details page, enter a StackSet name and click Next.
11. In the Configure StackSet options page, use the default configuration and click Next.
12. In the Set deployment options page, use the default configuration.
    a. In the Account section, enter AWS account/s.

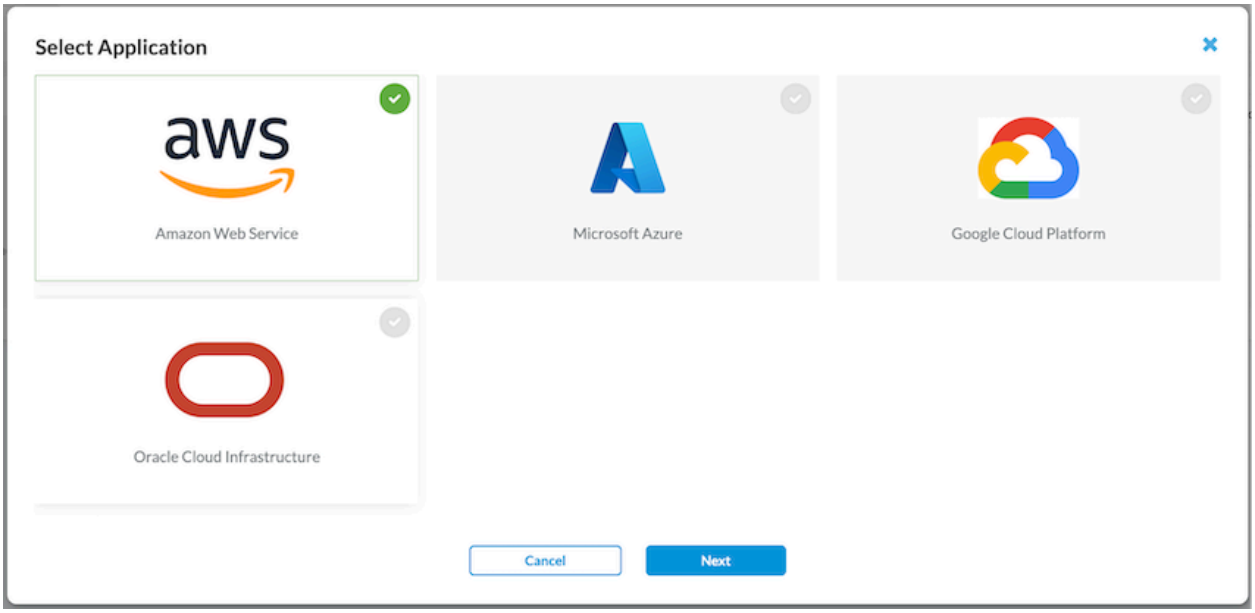
b. In the Specify regions, select regions, or click Add all regions, and then click Next.



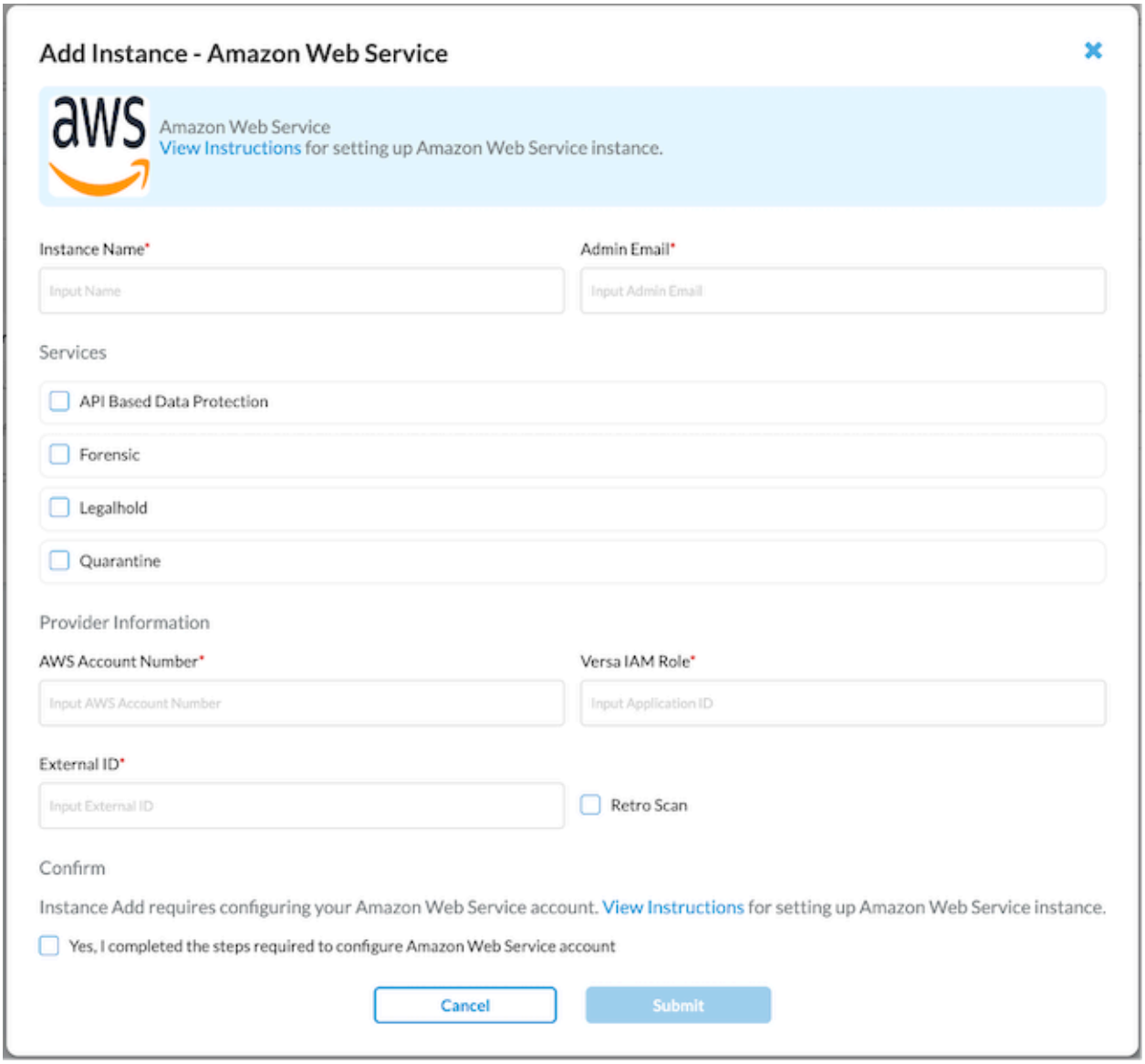
13. Review StackSet details on the Review page and click Submit. The new StackSet displays on the CloudFormation page.
    a. Click the StackSet to view StackSet details.
    b. Click the stack instances to view the stack created in AWS account and AWS region. For details about a stack instance, log in to the stack instance's account, navigate to the region, and then select the desired stack by name.
    c. Click the Template tab to view the permissions defined in the template.

Configure an Amazon Web Services Connector

1. Navigate to "Configure" > “Advanced Security” > “API Based Data Protection” > “Connectors”.
2. Click the ✚Add icon, select Amazon Web Service, then click Next.



3. In the Add Instance window, enter information for the following fields.



Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email (Required)	Enter the email address of the Amazon Web Services administrator account.
Services	Select the services to use for the instance. ◦ API Based Data Protection—Scan and protect content. ◦ Forensic—Use this instance for forensics.

Field	Description
	◦ Legal hold—Use this instance for Legal hold. ◦ Quarantine—Use this instance for Quarantine files.
AWS Account Number	Enter organization AWS account number.
Versa IAM Role	Enter role name created by Cloud Formation Template (CFT) as described above.
External ID	Enter external ID generated by CFT.
Retro Scan	Click to scan and protect all the files that are present on Amazon S3 at the time of connector creation.
Confirm	Click to confirm that the steps required to configure the AWS account are complete.

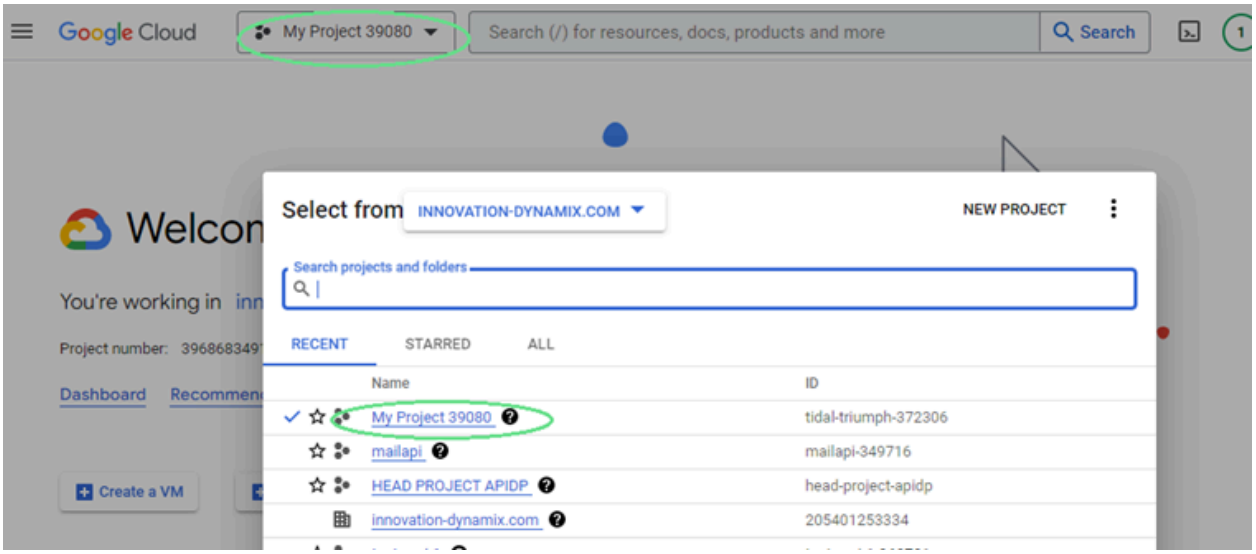
Google Cloud Platform API-Based Data Protection

This section describes how to configure Google Cloud Platform for API-based data protection.

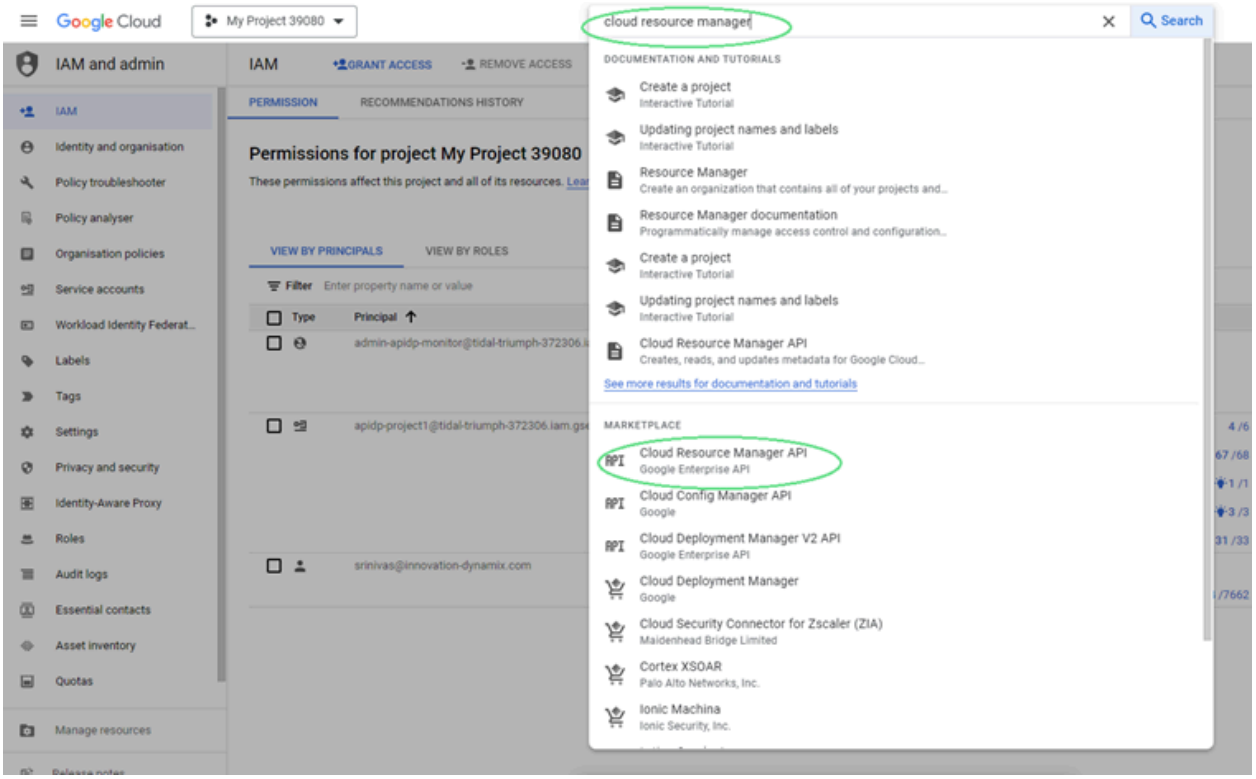
Configure Google Cloud Platform for API-Based Data Protection

To configure a new instance for Google Cloud Platform:

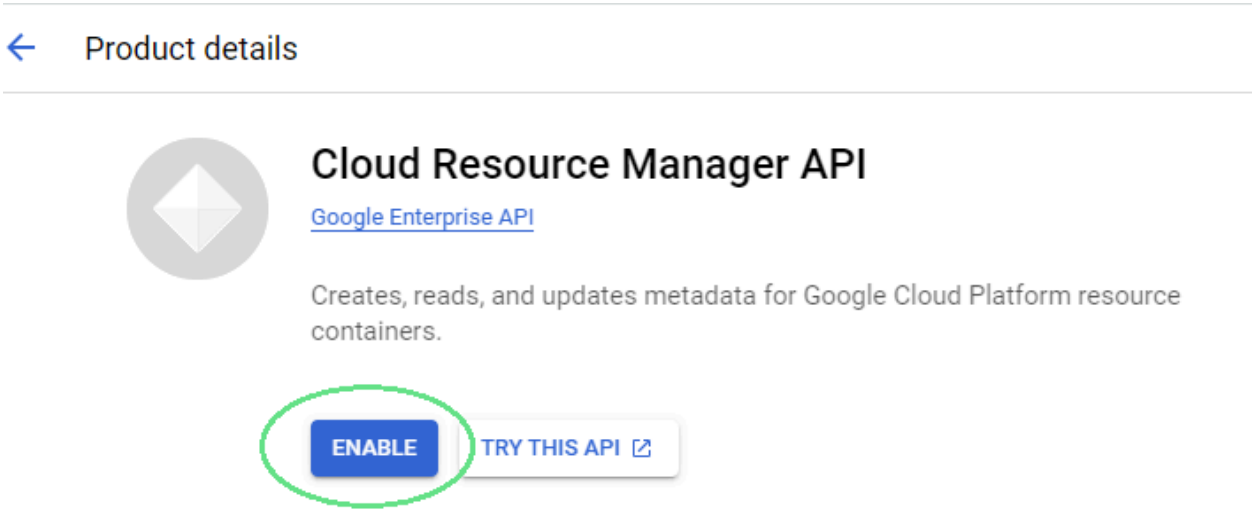
1. Log in to https://console.cloud.google.com/ using administrator credentials.
2. Create a new project or select an existing project. This project has access to other projects that are monitored by Versa API-DP cloud.



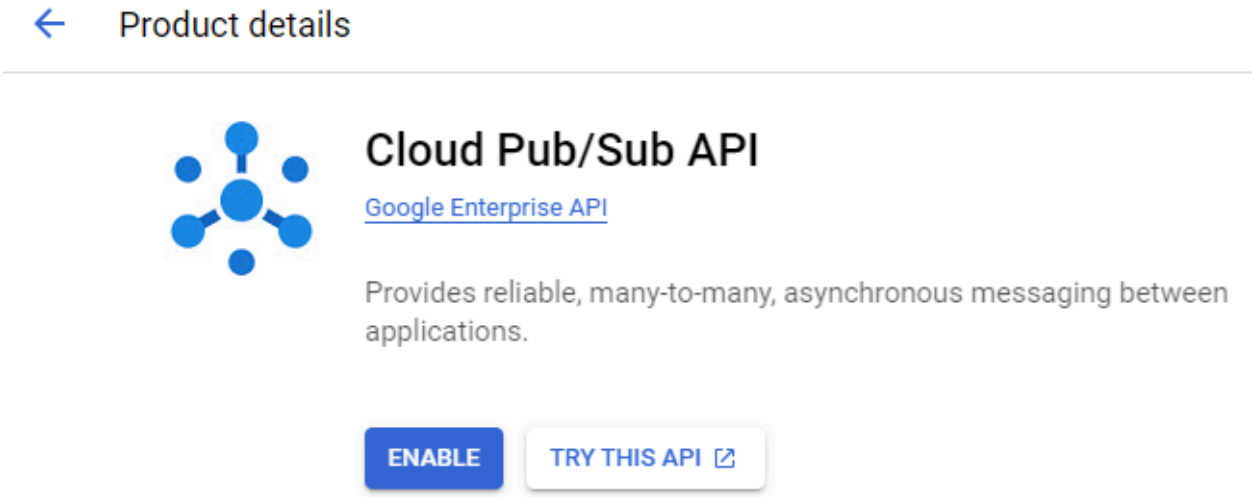
3. Search for Cloud Resource Manager and select the API.



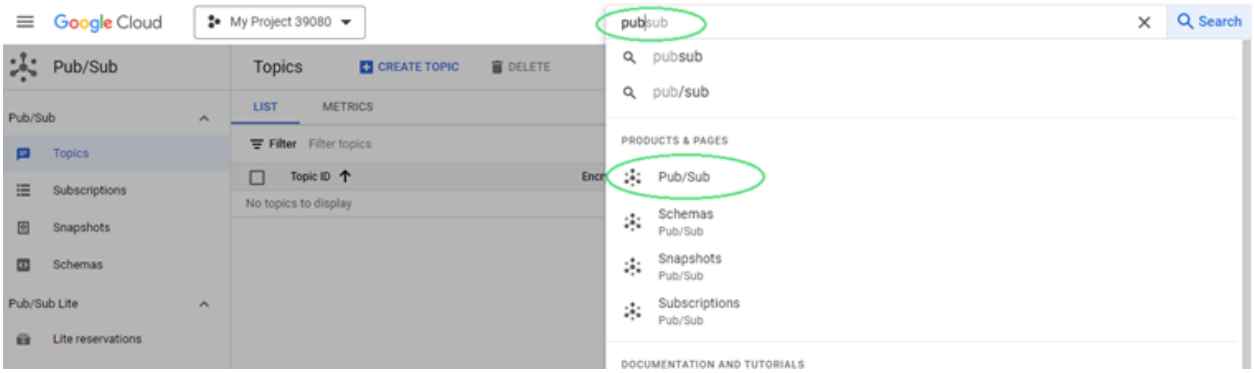
4. Click enable to enable the API.



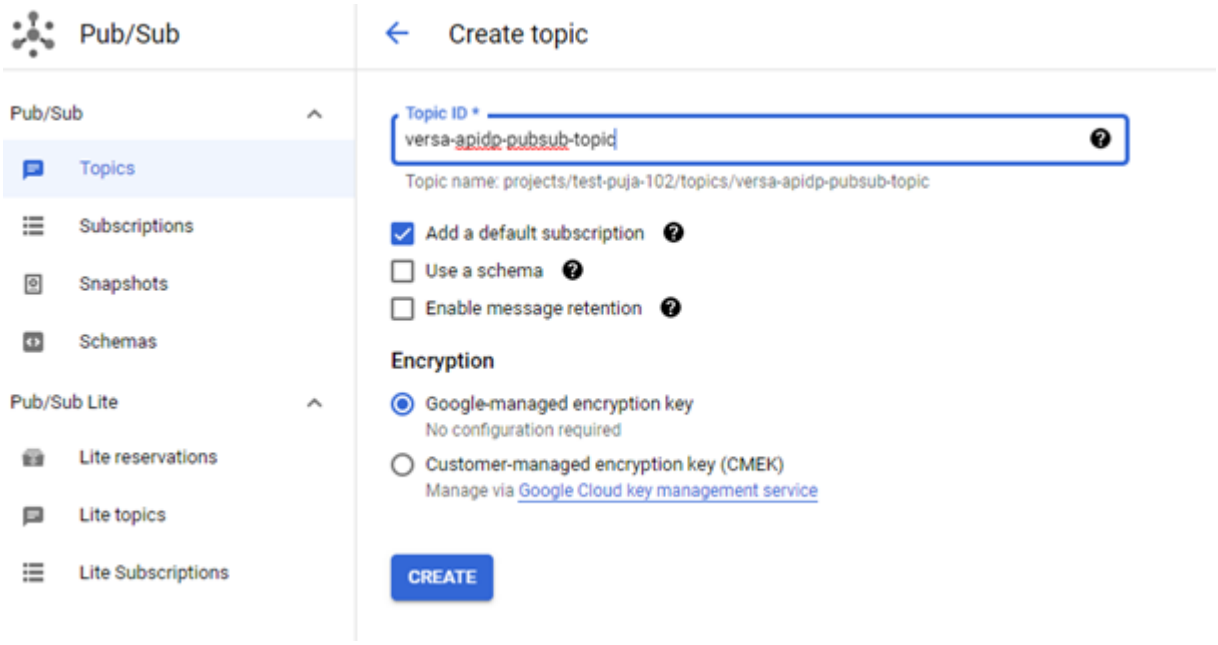
5. Search for Cloud Pub/Sub API and click Enable.



6. Search for Pub/Sub and select it.

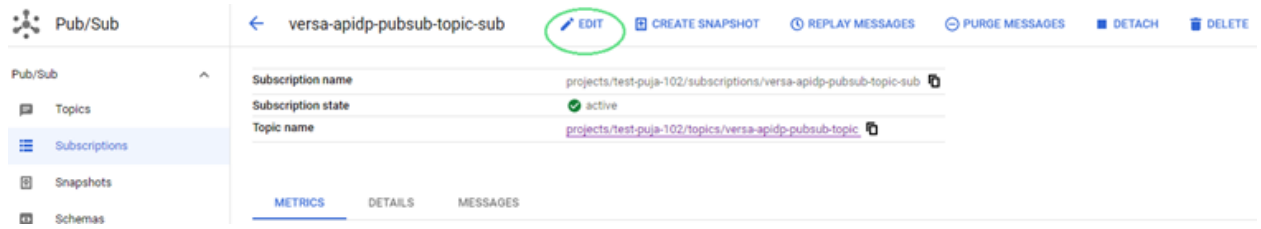


7. Create a Pub/Sub topic in the new project. Enter the Topic ID as versa-apidp-pubsub-topic. Versa API data protection automatically configures a Pub/Sub topic and subscription on the other managed projects. These topics and subscriptions are referenced in the admin project Pub/Sub topic, so the topic name must be the same.

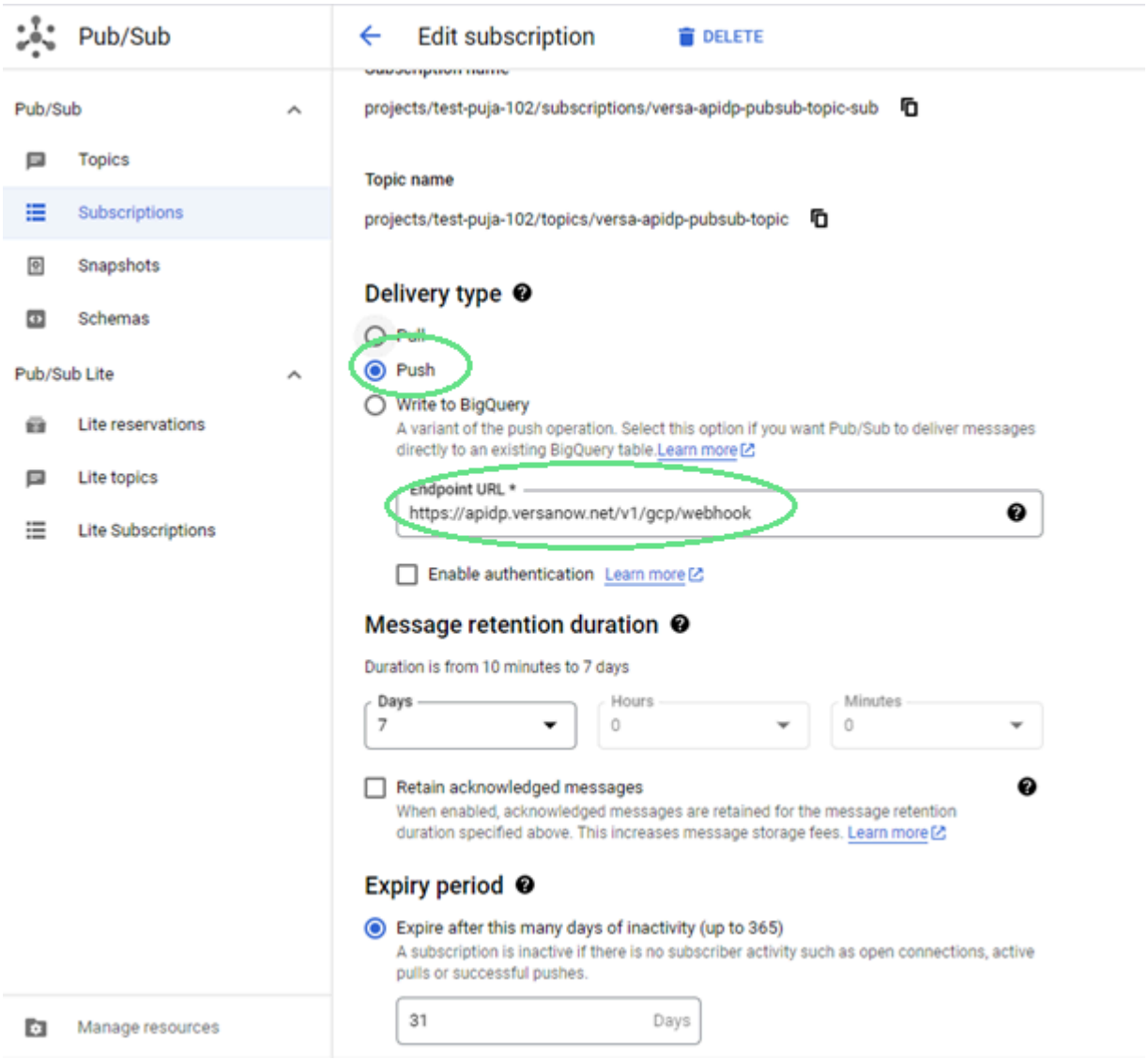


8. Select Pub/Sub > Subscription in the left menu bar.

9. Click Edit.

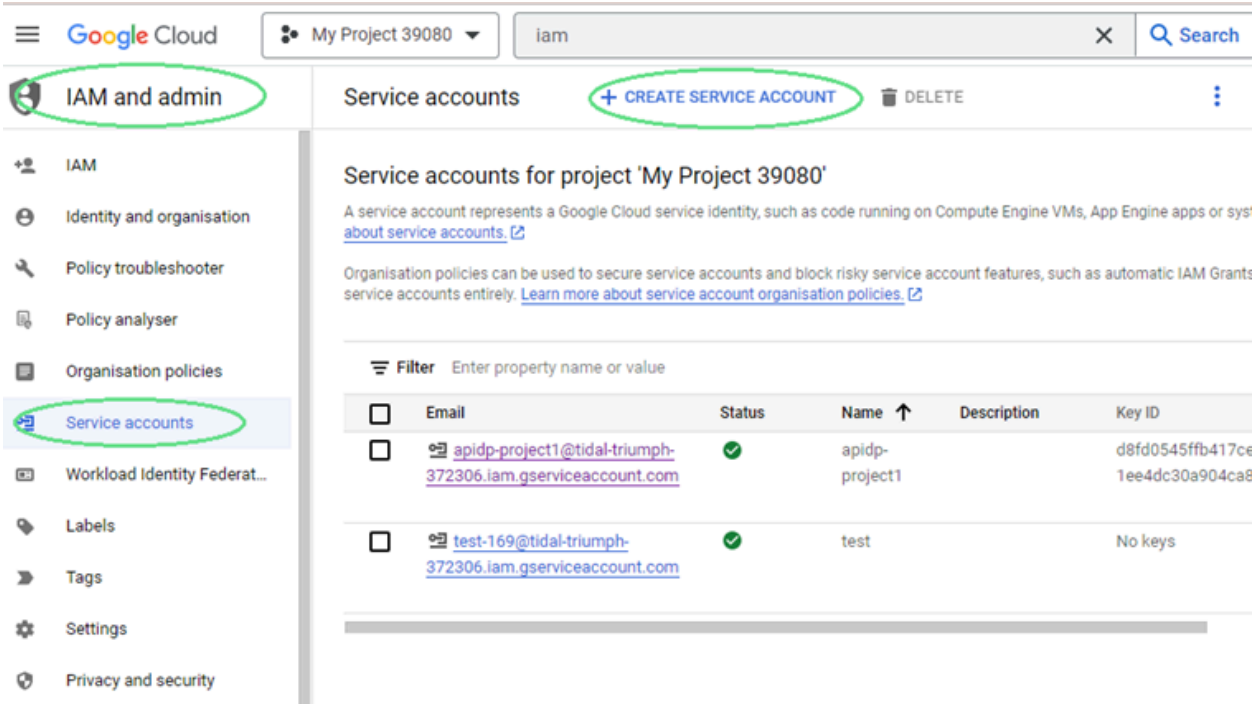


10. In the Edit Subscription pane, enter information for the following fields and then click Update.

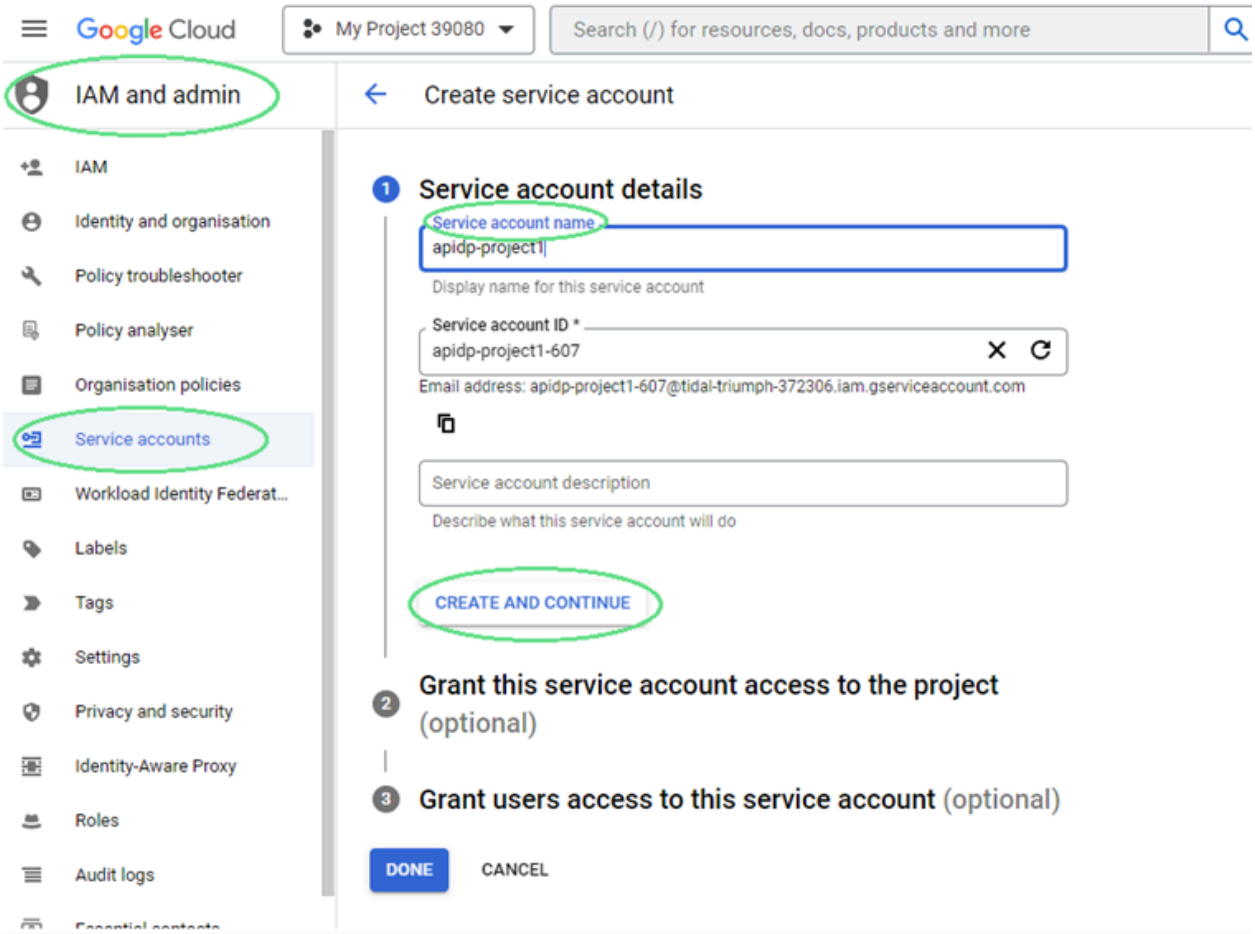


Field	Description
Delivery Type	Select Push.
Endpoint URL	Enter https://apidp.versanow.net/v1/gcp/webhook.

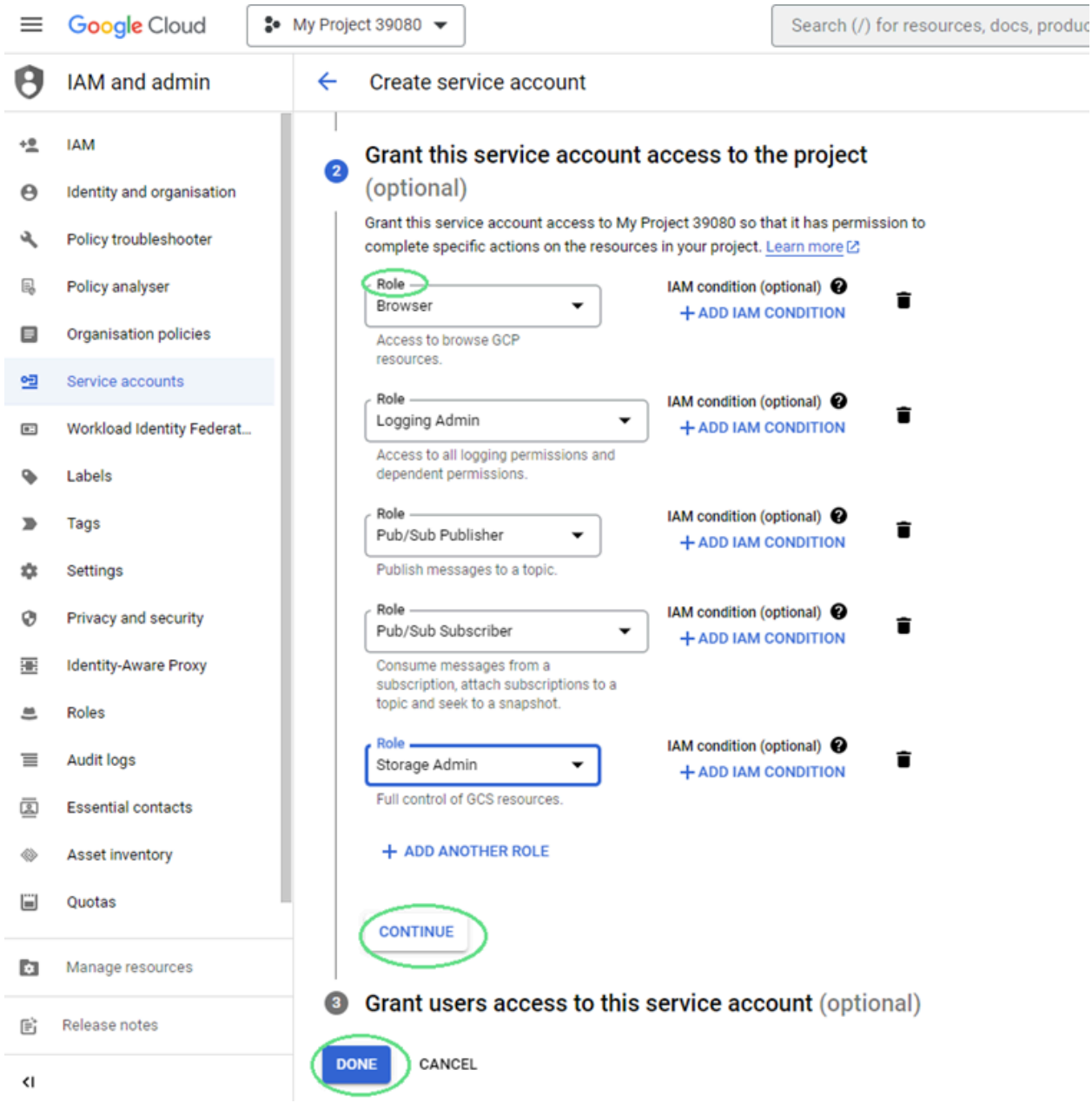
11. In the IAM and Admin portal, select Service Accounts in the left menu bar, and then click + Create Service Account.



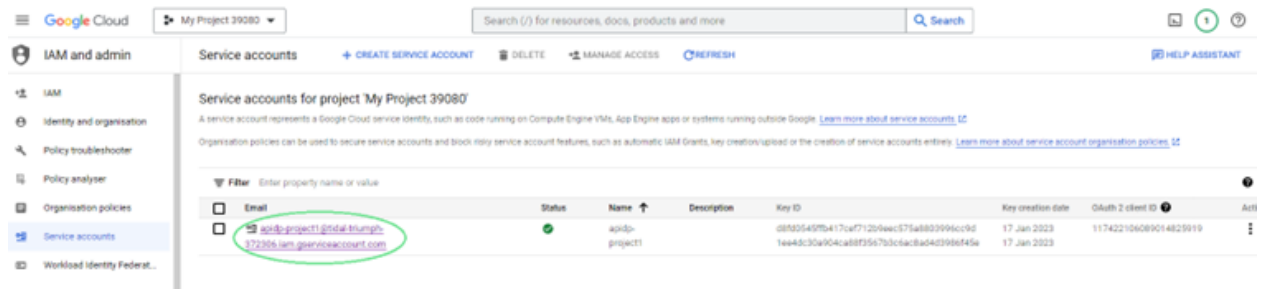
12. Enter a service account name and then click Create and Continue.



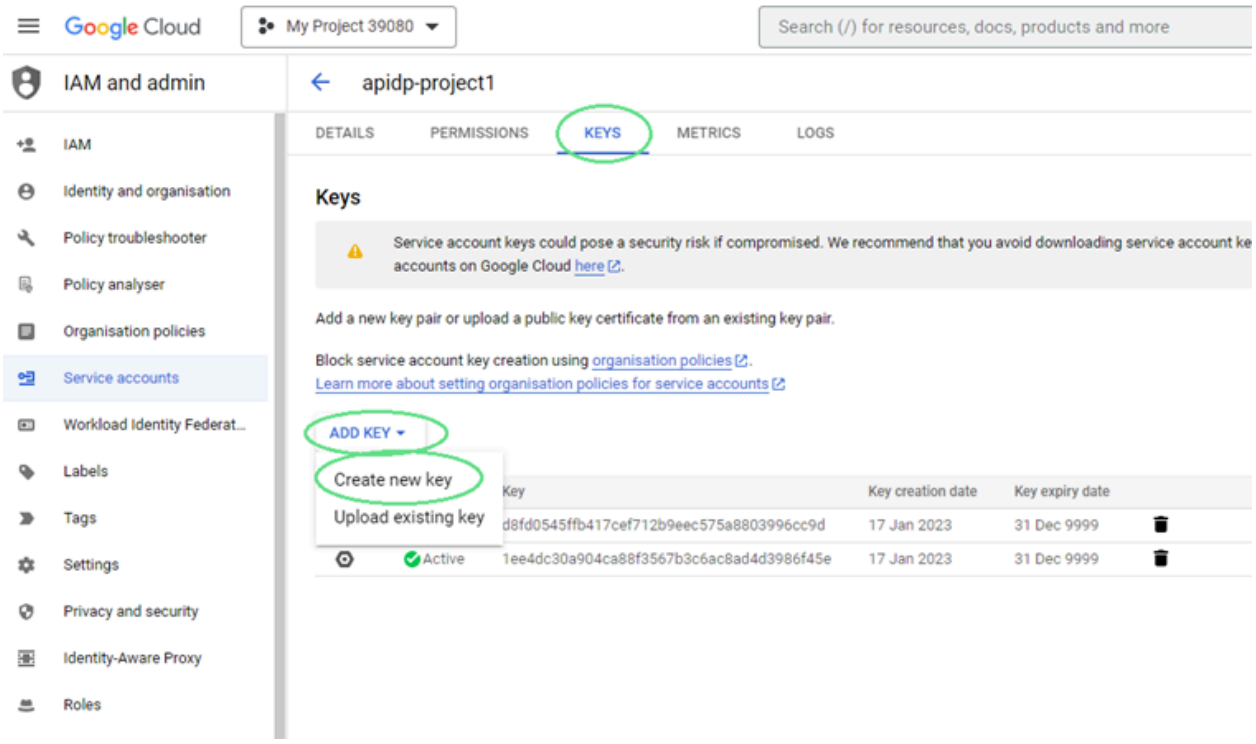
13. Provide the following access to the service account:
    - Browser—Access to browse GCP resources
    - Logging Admin—Access to all logging permissions and dependent permissions
    - Pub/Sub Publisher—Publish messages to a topic
    - Pub/Sub Subscriber—Use messages from a subscription, attach subscriptions to a topic, and seek to a snapshot
    - Storage Admin—Full control of GCS resources



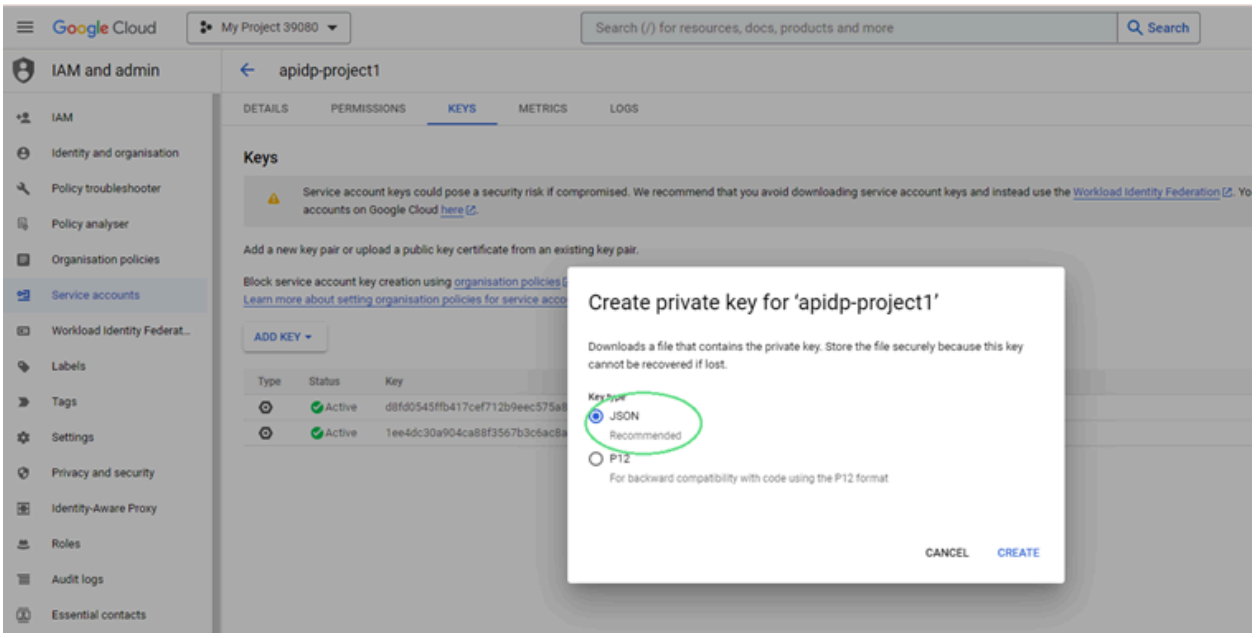
14. Download the JSON keys of the service account and save them to a secured location. Then select the service account.



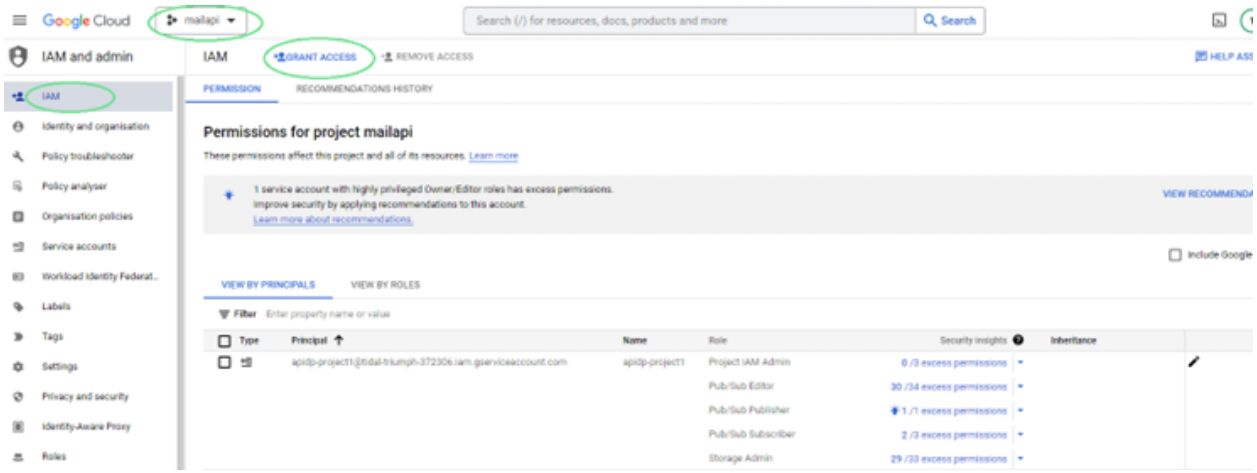
15. To create a new key, click Keys tab. Then click Add Key and select Create New Key.



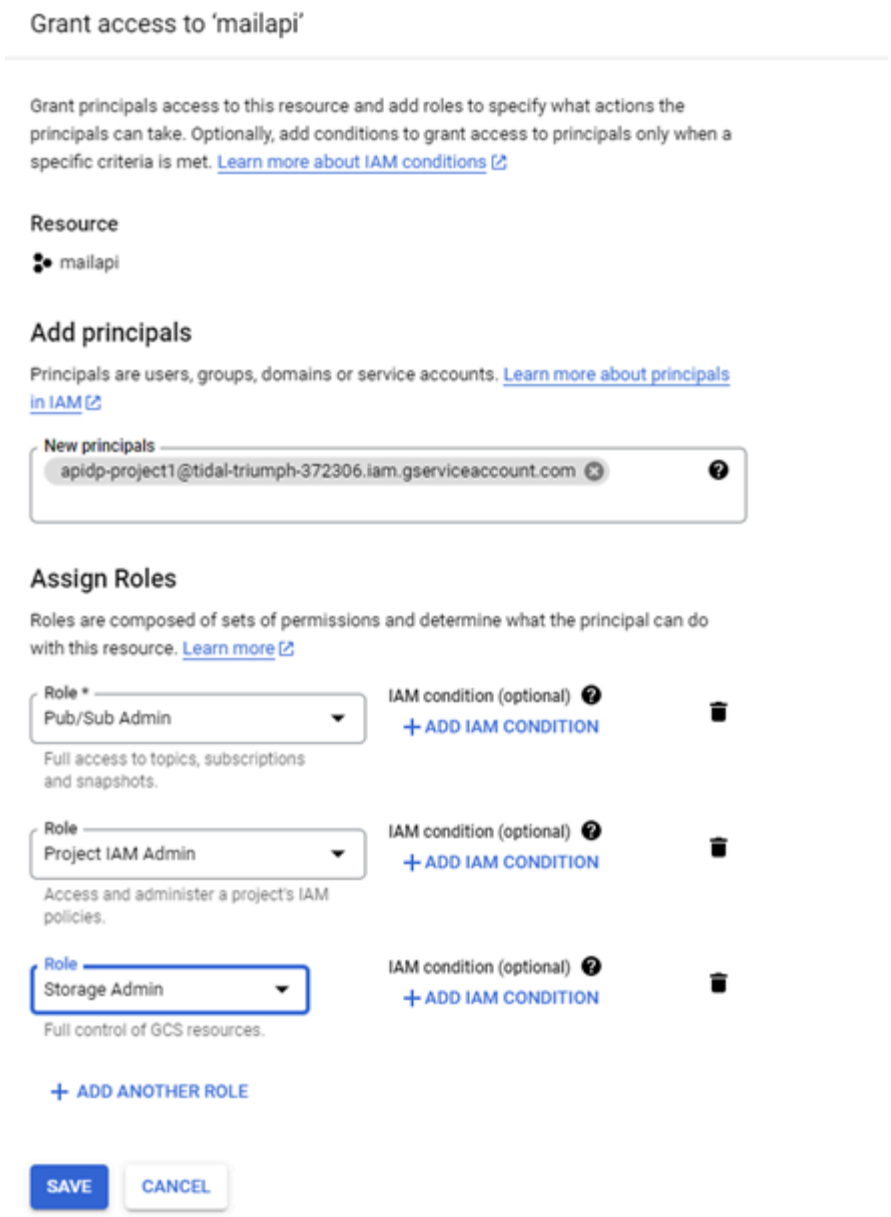
16. In the Create Private Key popup window, select key type as JSON.



17. Select the project, select IAM in the left menu bar, and then click Grant Access.



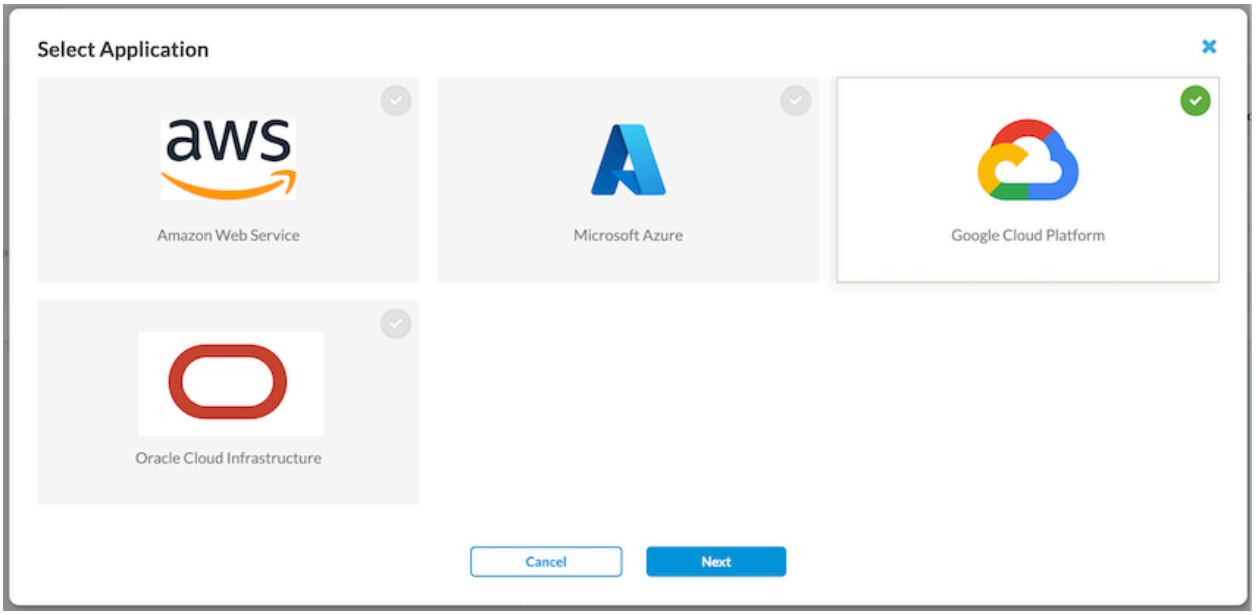
18. Provide the following permissions to the service account:
    - Pub/Sub Admin—Full access to topics, subscriptions, and snapshots
    - Project IAM Admin—Access and administer IAM policies of a project
    - Storage Admin—Full control of GCS resources



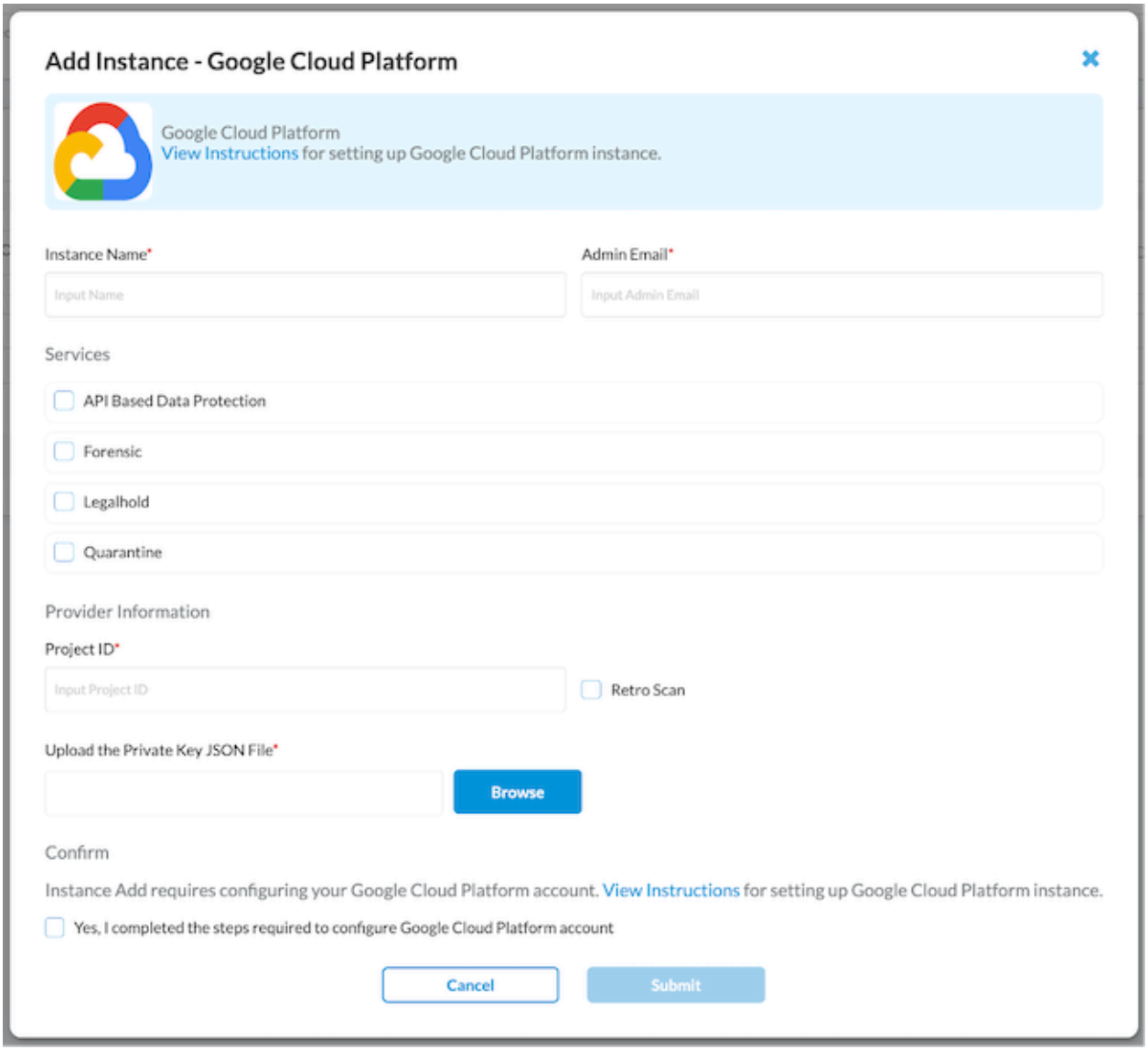
19. Repeat Step 17 and Step 18 for all the projects that Versa API data protection manages.

Configure a Google Cloud Platform Connector

1. Navigate to "Configure" > “Advanced Security” > “API Based Data Protection” > “Connectors”.
2. Click the + Add icon, select Google Cloud Platform, then click Next.



3. In the Add Instance window, enter information for the following fields and click Done.



Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email (Required)	Enter the email address of the Google Cloud Platform administrator account.
Services	Select the services to use for the instance. ◦ API Based Data Protection—Scan and protect content. ◦ Forensic—Use this instance for forensics. ◦ Legal hold—Use this instance for Legal hold.

Field	Description
	◦ Quarantine—Use this instance for Quarantine files.
Private Key JSON File	Upload the private key JSON file generated for service account.

4. Click Done.

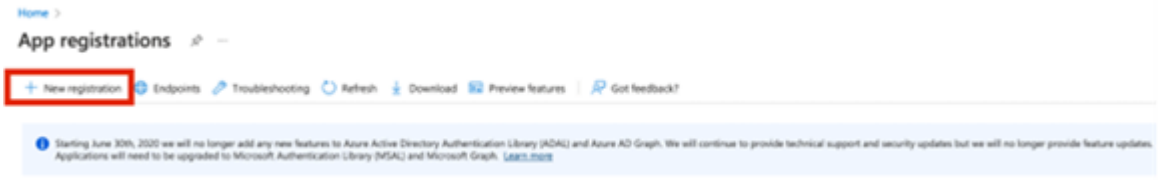
Microsoft Azure API-Based Data Protection

This section describes how to configure Microsoft Azure for API-based data protection.

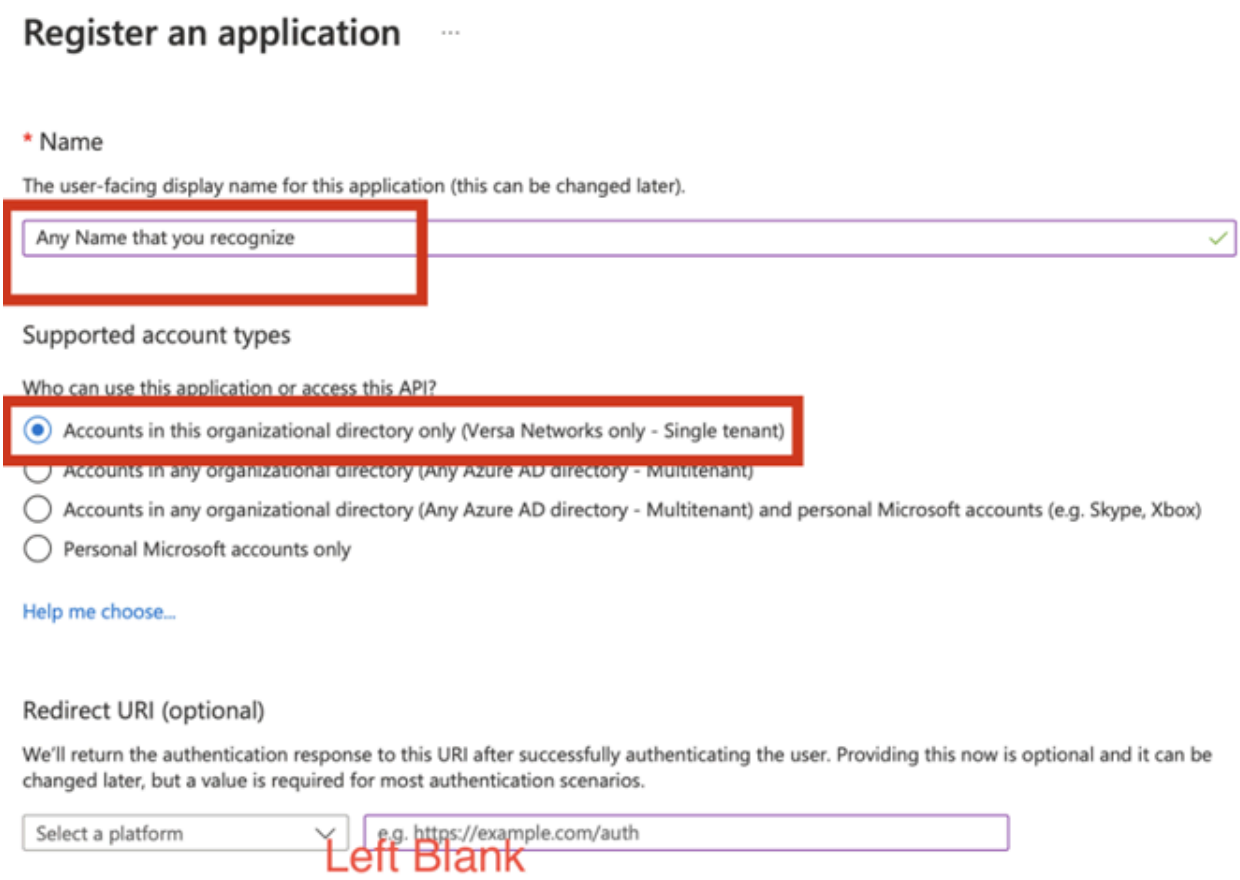
Configure Microsoft Azure for API-Based Data Protection

To configure a new instance for Microsoft Azure:

1. Register app on Admin Azure portal.
   a. Login to portal.azure.com using admin account.
   b. In the search bar, search for App Registration.
   c. Click New Registration.

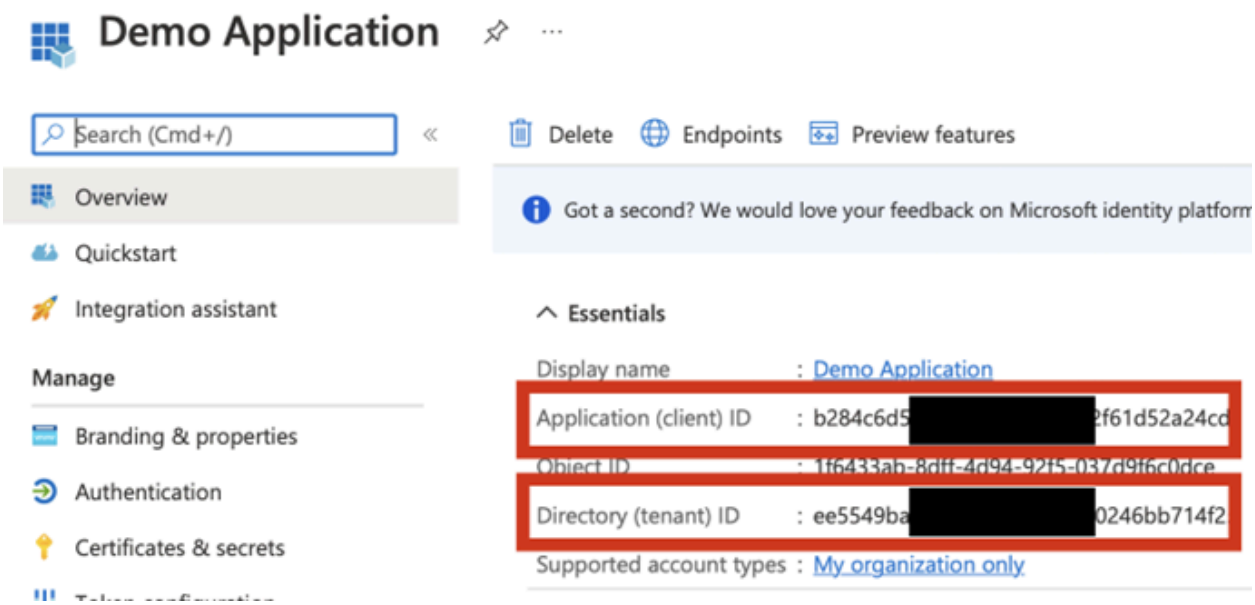


   d. Enter the following information and click Register.

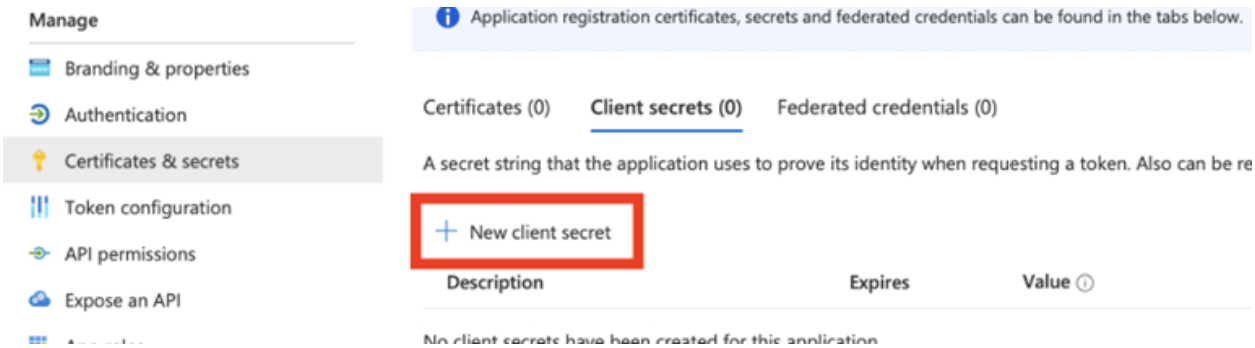


Field	Description
Name (Required)	Enter a name for the application.
Supported Account Types	Select Accounts in this organizational directory only (Versa Networks only - Single tenant).

2. Record client ID, tenant ID, and client secret.
    a. Copy and save application (client) and directory (tenant) ID.

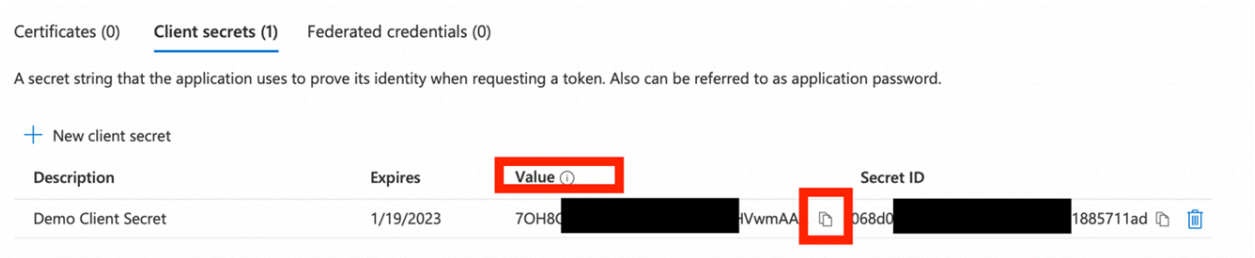


b. Select Certificates and Secrets in the left menu bar, and then click + New client secret.

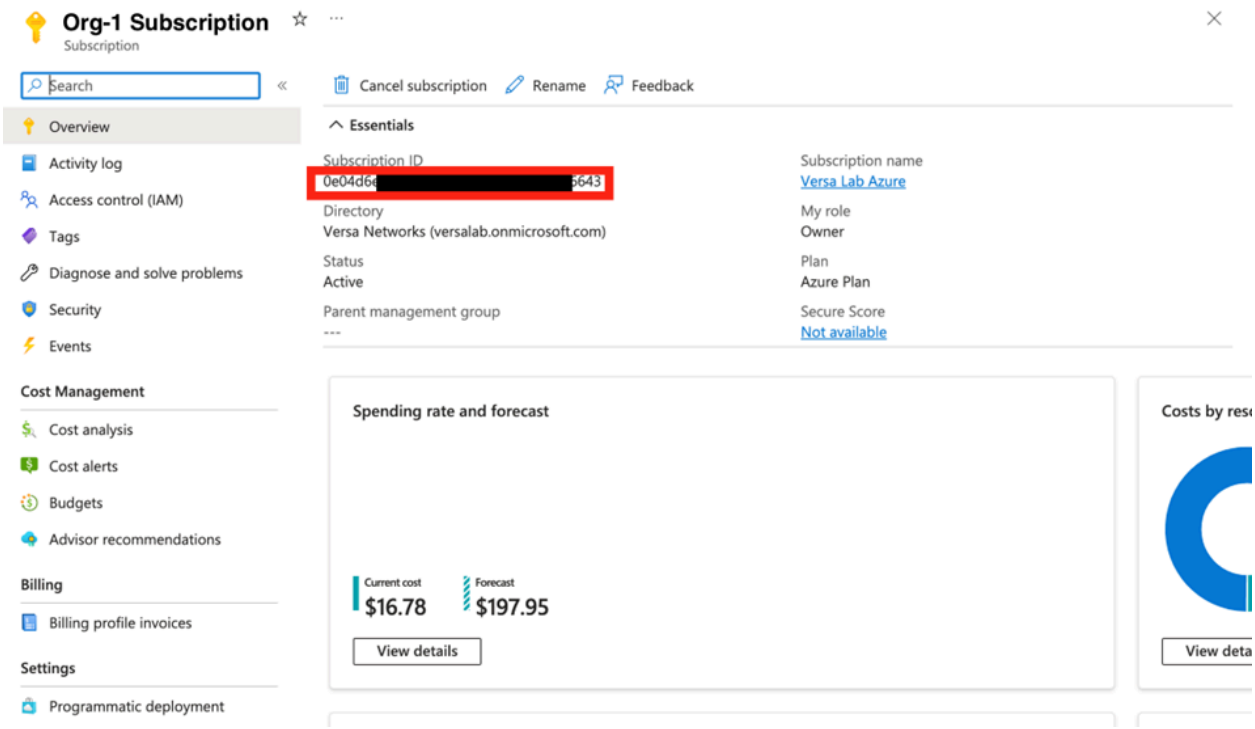


c. Enter a description and expiry time, and then click Add.

d. Copy the Value and save it. The client secret is no longer accessible after you leave the page.

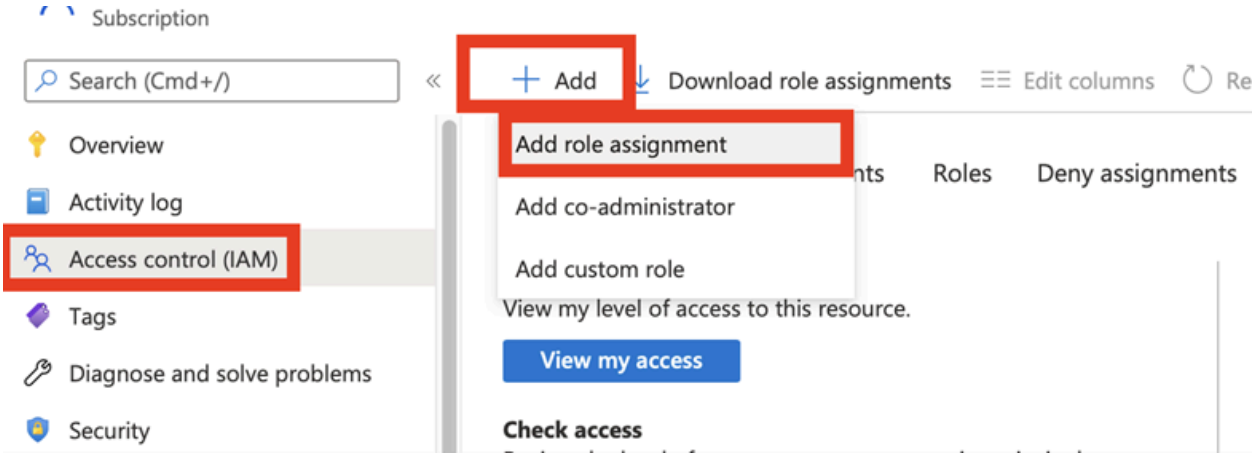


3. Assign role to the application to grant permission.
   a. In the search bar, search for Subscription.
   b. Select the subscription for Versa data protection app.
   c. Copy the subscription ID.

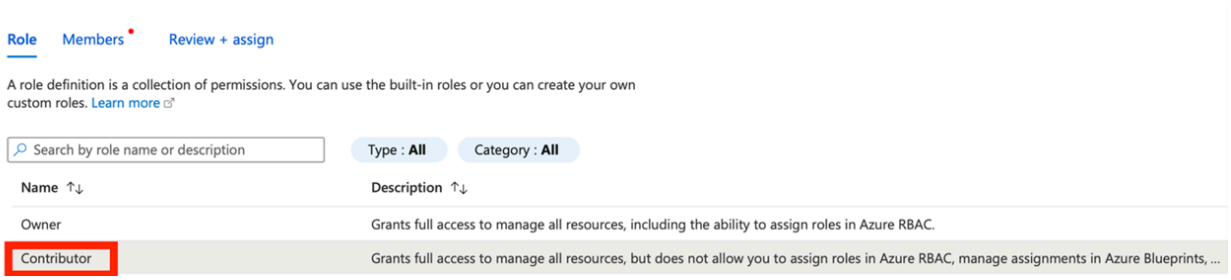


d. Select Access Control (IAM) in the left menu bar.

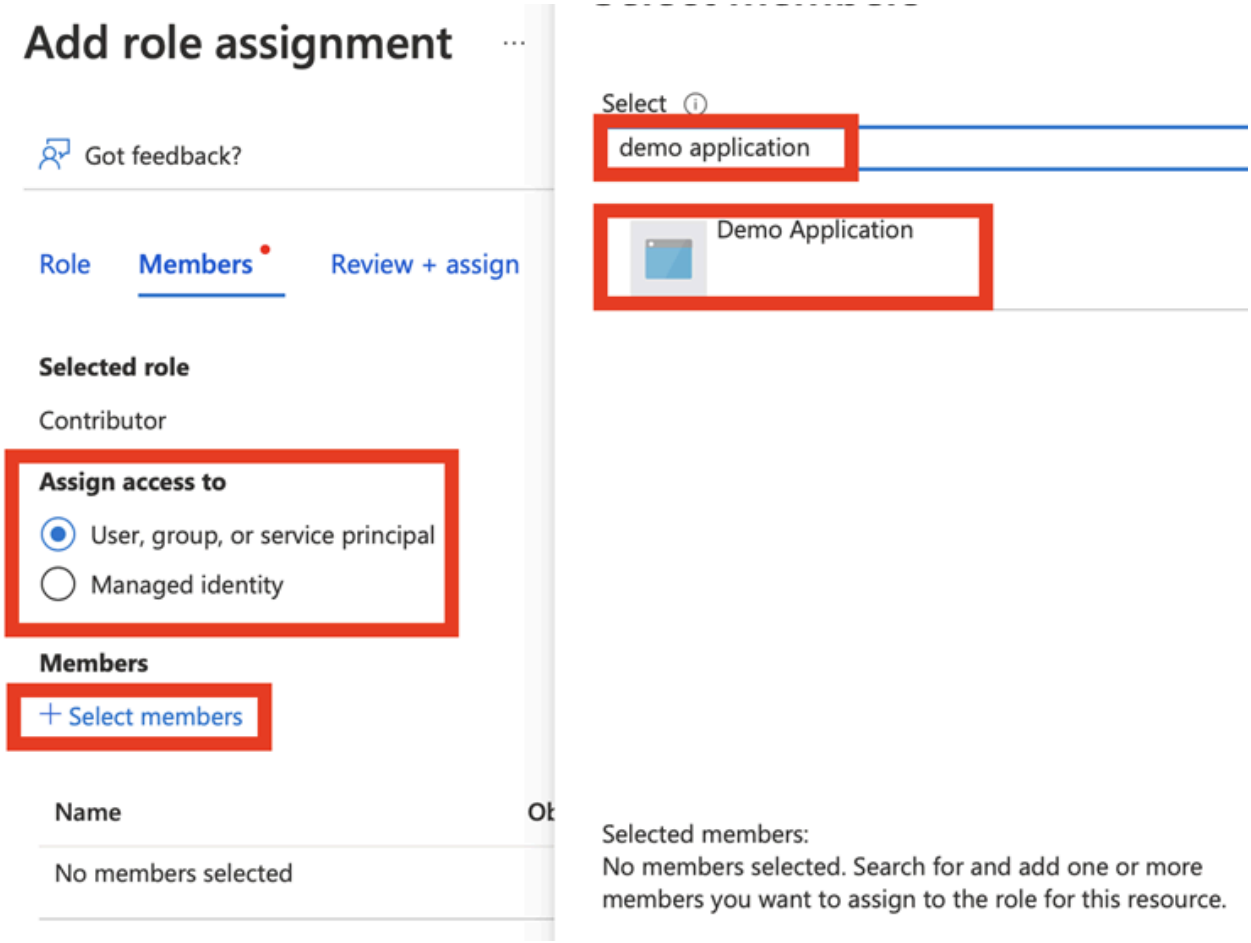
e. Select Add > Add role assignment.



f. In the Role tab, select Contributor and click Next.



g. Enter information for the following fields.

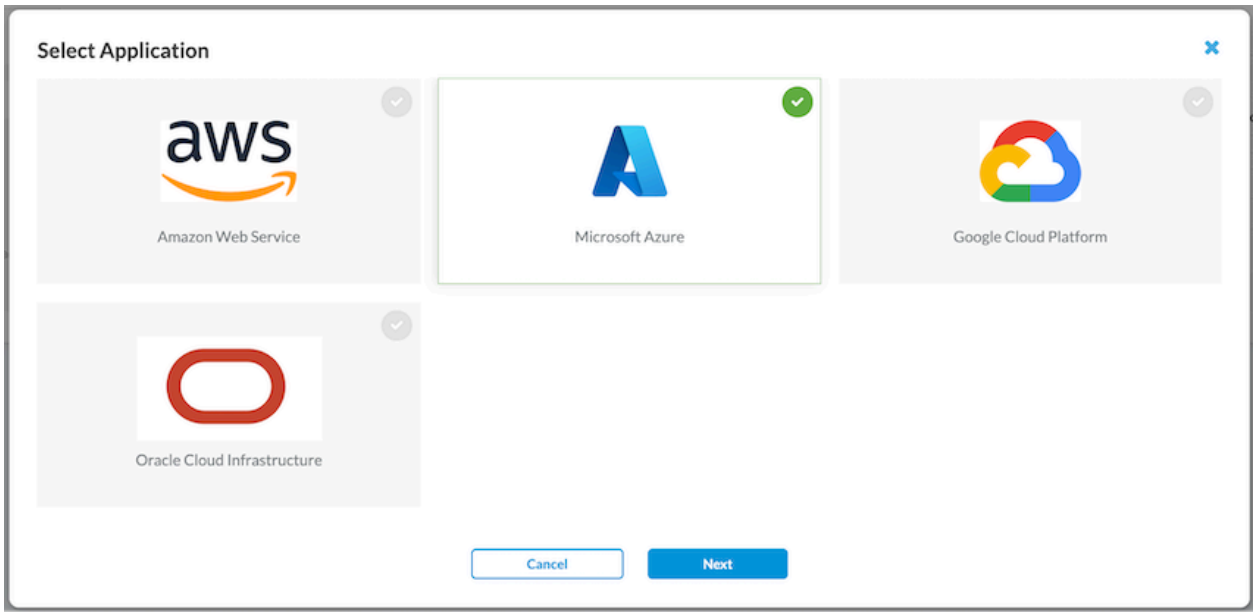


- Select Assign access to as user, group, or service principal.
- Click + Select members and add one or more members to assign the role for the resource.
- Enter the name of the application created.
- Click Application and then click Select.
- Click Review + Assign.

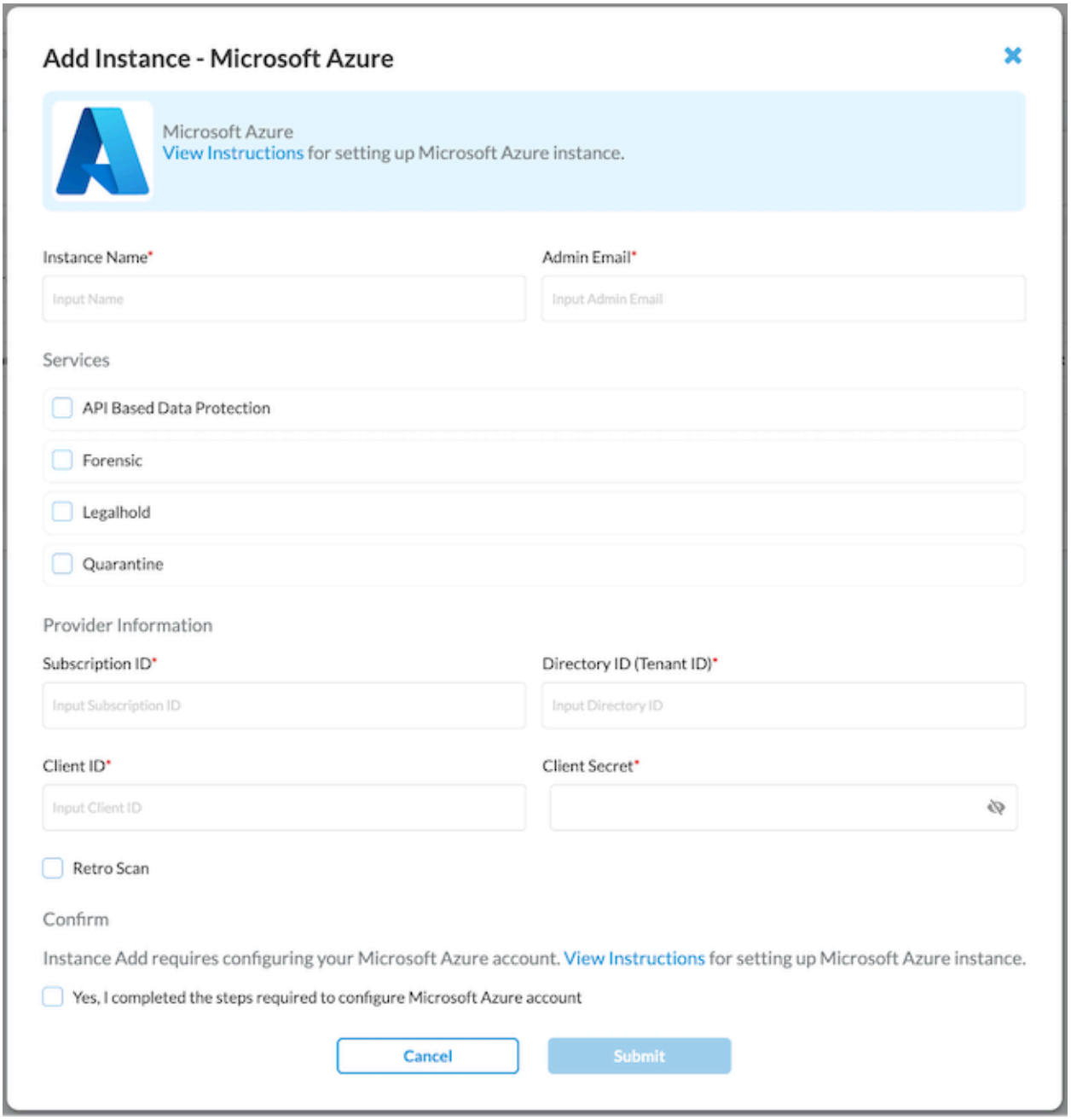
h. Click Review + Assign

Configure a Microsoft Azure Connector

1. Navigate to "Configure" > “Advanced Security” > “API Based Data Protection” > “Connectors”.
2. Click the + Add icon, select Microsoft Azure, then click Next.



3. In the Add Instance window, enter information for the following fields.



Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email (Required)	Enter the email address of the Microsoft Azure administrator account.
Services	Select the services to use for the instance.

Field	Description
	◦ API Based Data Protection—Scan and protect content. ◦ Forensic—Use this instance for forensics. ◦ Legal hold—Use this instance for Legal hold. ◦ Quarantine—Use this instance for Quarantine files.
Subscription ID	Enter the Microsoft Azure subscription ID obtained during the configuration.
Application ID (Client ID)	Enter the Microsoft Azure application ID obtained during the configuration.
Directory ID (Tenant ID)	Enter the Microsoft Azure directory ID of the tenant obtained during the configuration.
Retro Scan	Click to scan and protect all the files that are present on Microsoft Azure at the time of connector creation.
Confirm	Click to confirm that the steps required to configure the Microsoft Azure account are complete.

4. Click Done.

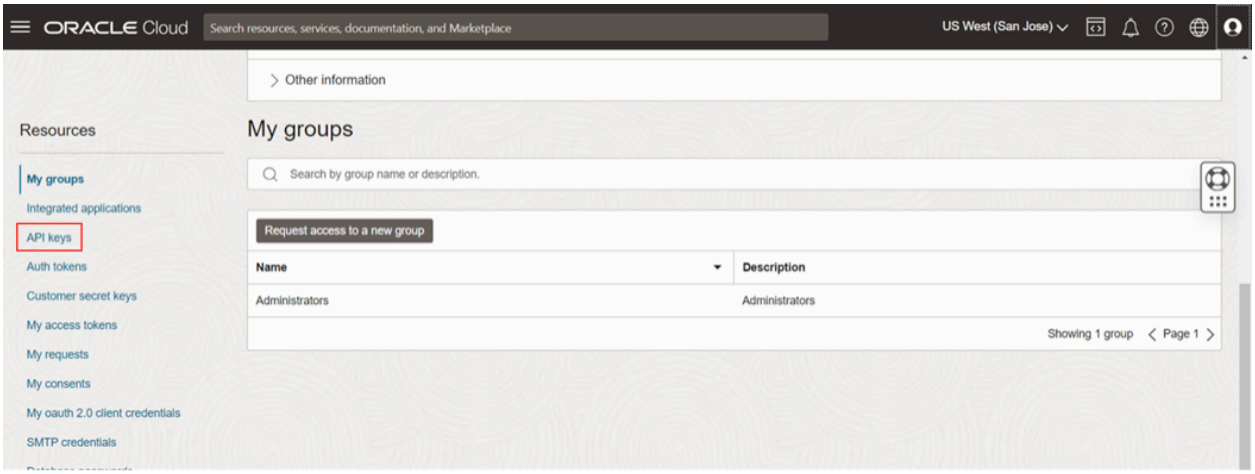
Oracle Cloud Infrastructure API-Based Data Protection

This section describes how to configure Oracle Cloud Infrastructure for API-based data protection.

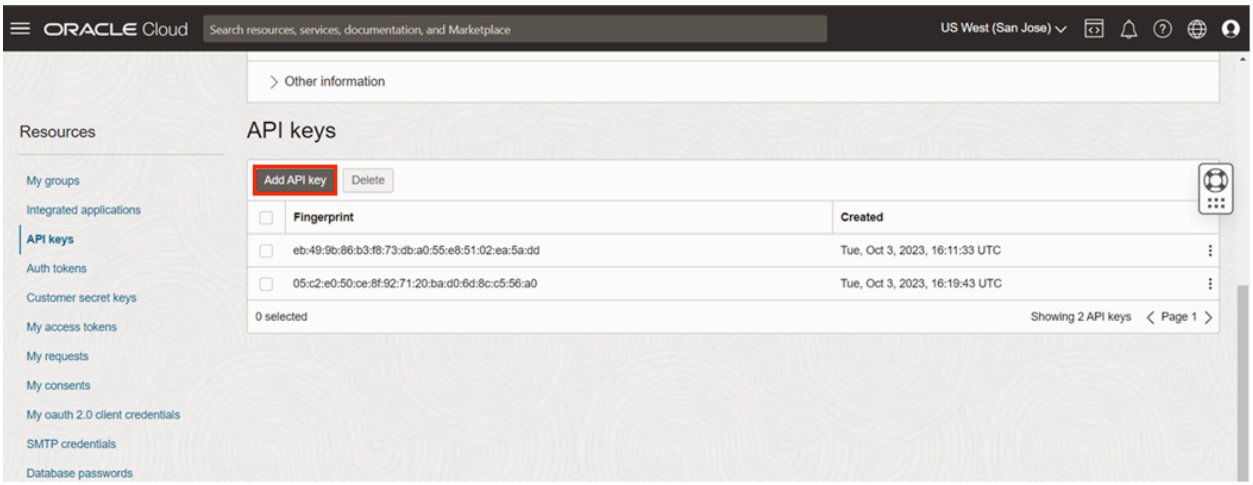
Configure Oracle Cloud Infrastructure for API-Based Data Protection

To configure a new instance for Oracle Cloud Infrastructure:

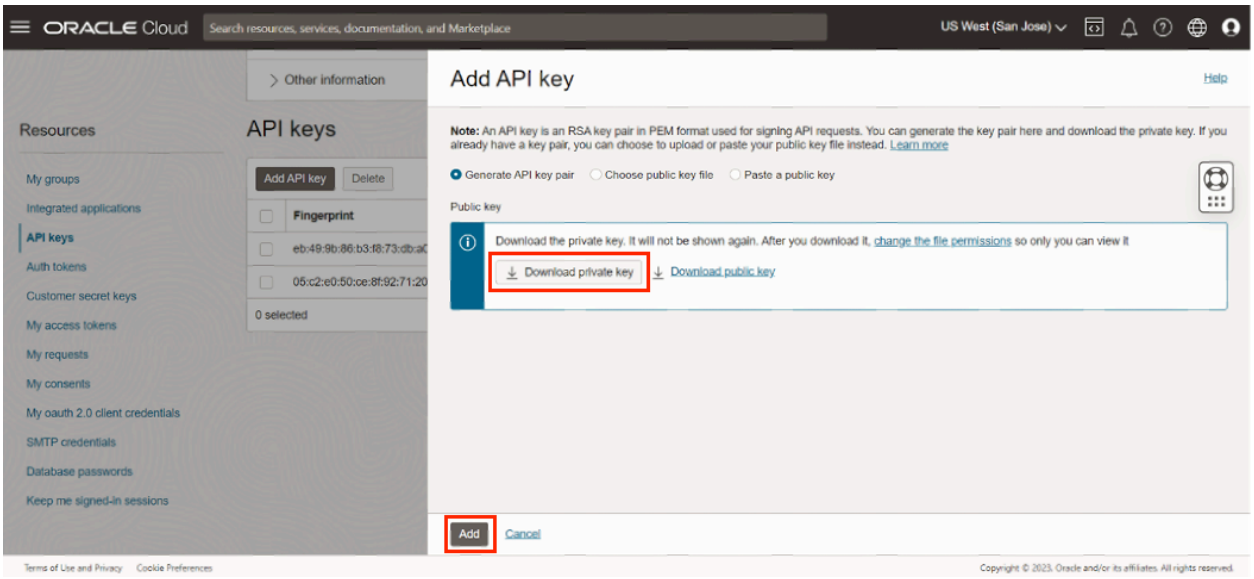
1. Log in to the administrator's profile.
2. Select Resources > API Keys in the left menu bar.



3. In the API Keys window, click Add API Key.

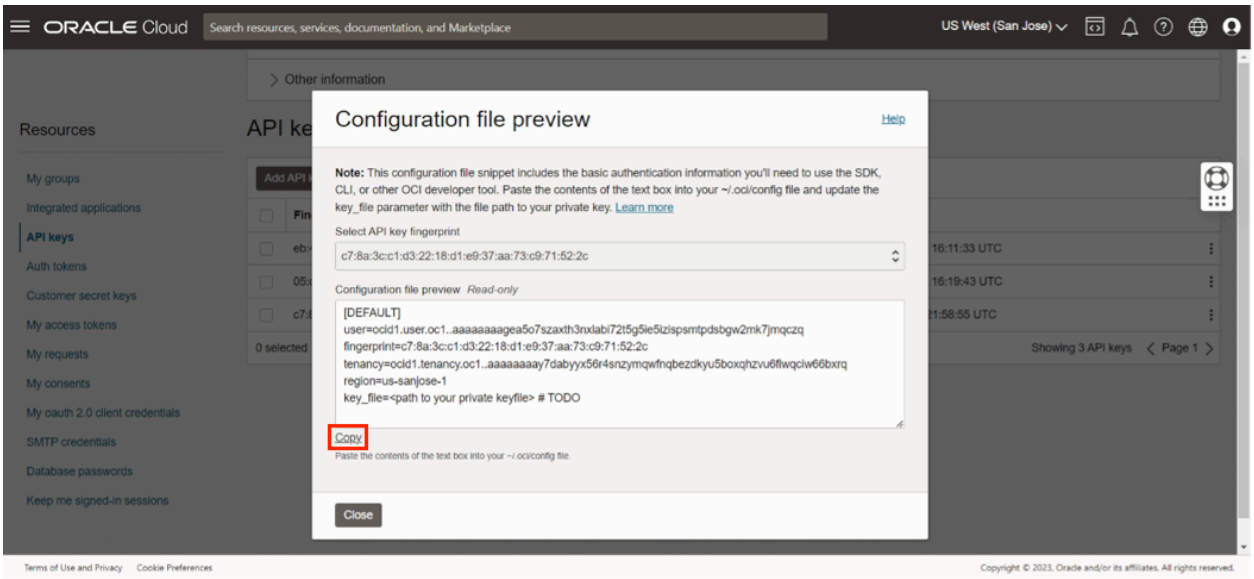


4. In the popup window, click Download private key, then click Add.



5. In the Configuration File Preview screen, click Copy to copy the file contents.

   Note: Do not make any modifications to the copied contents of the configuration file.



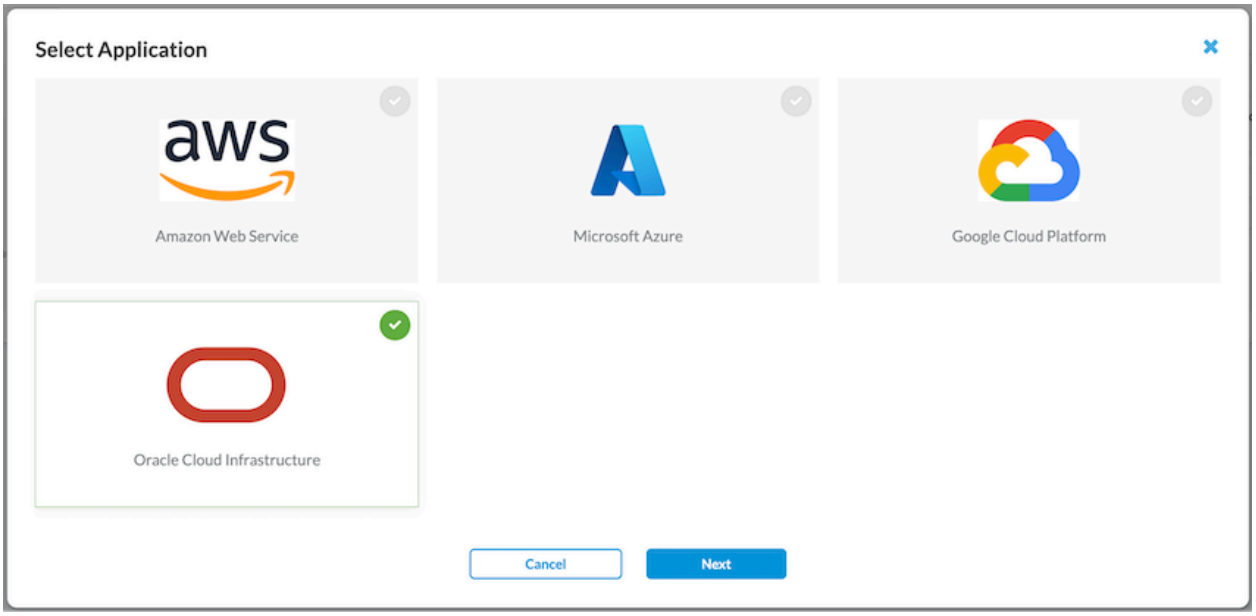
6. Add an instance for Oracle Cloud Infrastructure that includes the private key and the copied configuration file preview information.

Configure an Oracle Cloud Infrastructure Connector

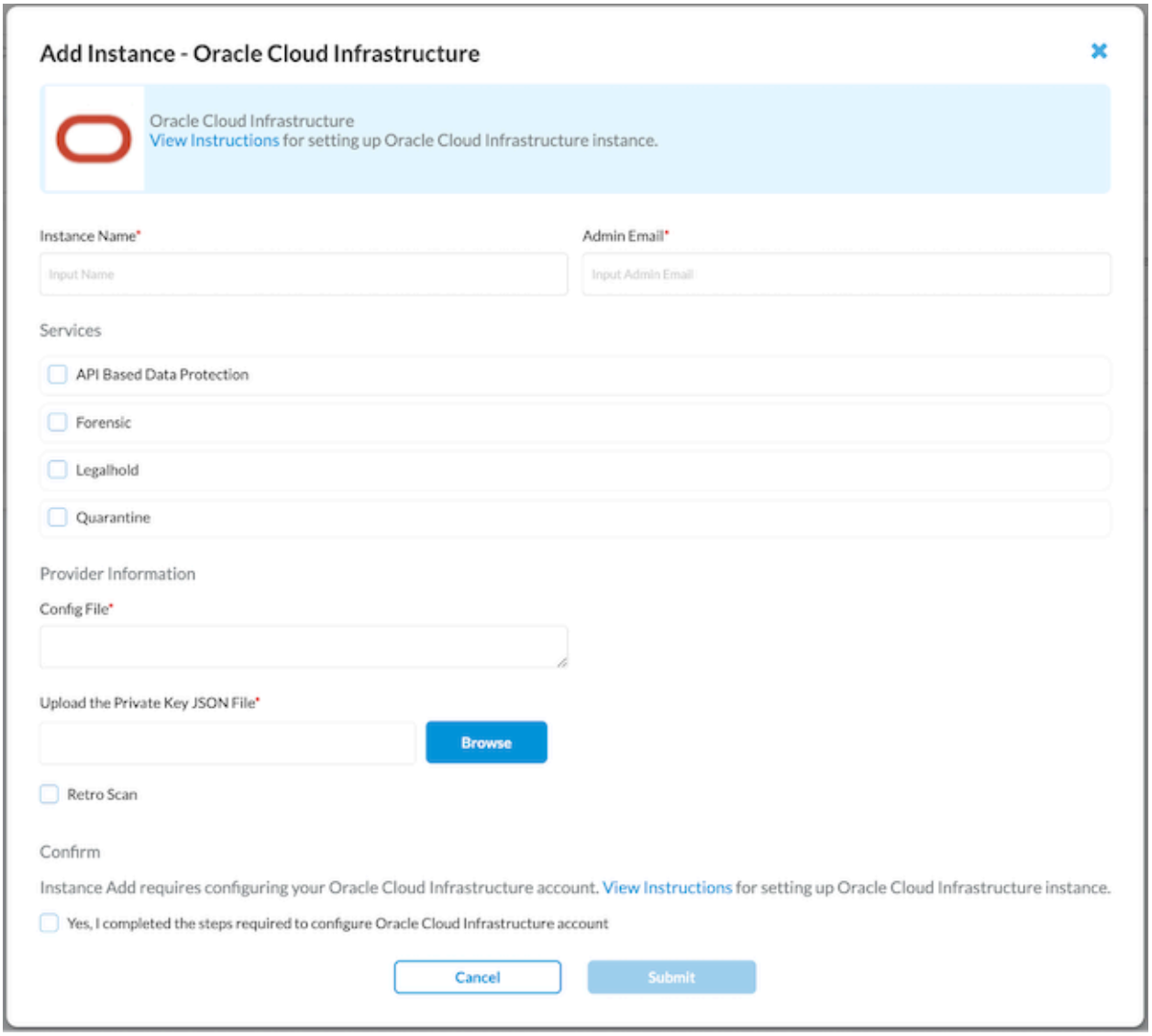
To configure a connector for Oracle Cloud Infrastructure:

1. Navigate to "Configure" > “Advanced Security” > “API Based Data Protection” > “Connectors”.

2. Select the IaaS tab, click the + Add icon, select Oracle Cloud Infrastructure, then click Next.



3. In the Add Instance window, enter information for the following fields.



Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email (Required)	Enter the email address of the Oracle Cloud Infrastructure administra
Services	Select the services to use for the instance. ◦ API Based Data Protection—Scan and protect content. ◦ Forensic—Use this instance for forensics. ◦ Legal hold—Use this instance for Legal hold. ◦ Quarantine—Use this instance for Quarantine files.

Field	Description
Config File	Contents of the admin's configuration file, containing basic authentic
Upload the Private Key JSON File	Upload the private key of the administrator.
Retro Scan	Click to scan and protect all the files that are present on Oracle Clou
Confirm	Click to confirm that the steps required to configure the Oracle Cloud

Supported Software Information

Releases 11.1.1 and later support all content described in this article.

Additional Information

Configure API-Based Data Protection Policy for SaaS