



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			
Workspaces, projects, milestones, tasks, subtasks, comments, messages, attachments	Yes	Yes	NA
Bites, folders	Yes	Yes	Yes
Cisco Files, messages, Webex Teams	No	Yes	NA
Citrix Files, folders, ShareFile	Yes	Yes	Yes
Pages, blogs, comments, Confluence attachments	Yes	Yes	NA
Bites, folders	Yes	Yes	Yes
Eges, folders	Yes	Yes	Yes

Application Type	Data at Rest	Event-Based	Shared Links
Bitbucket, branch, files	Yes	Yes	NA
Bitbucket, branch, files	Yes	Yes	NA
Email content, attachments	Yes	Yes	NA
Google Drive, folders	Yes	Yes	Yes
Projects, issues, issue descriptions, Jira comments, attachments	Yes	Yes	NA
Microsoft OneDrive, files, folders	Yes	Yes	Yes
Microsoft Outlook, Email content, attachments	Yes	Yes	NA
Microsoft SharePoint, files, folders	Yes	Yes	Yes
Microsoft Teams, messaging, attachments handled by Microsoft SharePoint	Yes	Yes	NA
Microsoft Yammer, networks, communities, storylines, posts, comments, replies	Yes	Yes	NA
Notion, pages, database, bookmark, bulleted list item, callout, code, equation, file, headings, image, numbered list item, paragraph, PDF, quote, toggle blocks	Yes	Yes	NA
Salesforce files, libraries, account attachments, contact attachments, chatter attachments (posts and comments)	Yes	Yes	NA
ServiceNow, tables and attachments	Yes	Yes	NA
Slack workspace, channels, messages, files	Yes	Yes	NA
Trello workspaces, boards, lists, cards, comments, attachments	Yes	Yes	NA

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

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

The screenshot shows the Asana home page. On the left is a sidebar with navigation links like Home, My tasks, Inbox, Insights, Reporting, Portfolios, Goals, Projects (including project11, portfolio2, jhbjhbj), and Team (My workspace). The main area displays a survey asking 'How likely are you to recommend Asana to a friend or colleague?' with a scale from 0 to 6. Below it is a message 'Good afternoon, [User Name]' and a summary of tasks completed. A modal window titled 'Account' is open, listing workspaces: 'My workspace' (selected), 'Company or Team Name', 'hhhhhhh', 'team123', 'workspace#2', and 'ws4'. The 'Settings' button in this modal is highlighted with a red box. The top right corner shows a trial status: 'Free trial 16 days left'.

- Click "Apps" at the top bar of the settings window then click;"Manage Developer Apps".

Settings

Profile Notifications Email Forwarding Account Display **Apps** Hacks

Authorized Apps

You have authorized the following applications with [Asana Connect](#).

App Name	Last Access	
 saas-app	In the last day	Deauthorize
Manage Developer Apps		

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

Create new app

X

App name *

<app-name>

Which best describes what your app will do? *

- Automate work in Asana
- Integrate Asana and another tool
- Sync data between Asana and another tool
- Get data out of Asana to create reports
- Other

I agree to the [Asana API Terms](#)

Cancel

Create app

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.

The screenshot shows the Asana Developers platform. On the left, a sidebar for the app 'saas-app' lists several sections: Configure, Basic information, **OAuth** (which is highlighted with a red box), App Components, Test & distribute, App listing details, Manage distribution, and Submit for review. The main content area is titled 'OAuth' and describes it as the preferred method of authentication. It includes a 'View docs' button, 'App credentials' (Client ID and Client secret fields with 'Copy' and 'Reset' buttons), 'Redirect URLs' (with a dropdown containing 'https://apidp.versanow.net/v1/asana/auth-callback' which is also highlighted with a red box), and a checkbox for 'This is a native or command-line app'. There is also a trash bin icon.

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

The screenshot shows the 'Manage distribution' section of the Asana Developers platform. The sidebar has the 'Manage distribution' section selected (highlighted with a red box). The main content area is titled 'Manage distribution' and instructs users on how to distribute their app. It includes a 'View docs' button and a 'Choose a distribution method' section. Under 'Choose a distribution method', there are two options: 'Specific workspaces' (radio button) and 'Any workspace' (radio button, which is selected and highlighted with a red box). Below this, there is a 'Submit to the app directory' section with a note about listing the app in Asana's public app directory and a 'Review submission checklist' link.

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.

The screenshot shows the Asana API Reference page for the endpoint `/workspaces`. The left sidebar has a red circle around the 'Workspaces' section, which contains the 'Get multiple workspaces' endpoint. The main content area shows the endpoint details, including the URL `https://app.asana.com/api/1.0/workspaces`, a brief description, and a 'Customizing the response' section. The right sidebar includes language selection (Shell, Node, Ruby, PHP, Python), authorization (Bearer token), and code examples for Python and curl.

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

Workspace

- Projects
- o Section
 - ? Tasks
 - Subtasks
 - ? Milestones
 - Subtasks
 - ? Attachments
- Users
- o 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/createwebook>. 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.

The screenshot shows the Asana API documentation for the 'Establish a webhook' endpoint. The URL is `/webhooks`. The 'POST' method is highlighted with a red circle. The 'Try It!' button is also circled in red.

QUERY PARAMS

opt_fields array of strings
This endpoint returns a compact resource, which excludes some properties by default. To include those optional properties, set this query parameter to a comma-separated list of the properties you wish to include.

ADD STRING

opt_pretty boolean
Provides the "pretty" output. Provides the response in a "pretty" format. In the case of JSON this means doing proper line breaking and indentation to make it readable. This will take extra time and increase the response size so it is advisable only to use this during debugging.

BODY PARAMS

The webhook workspace and target.

data object

DATA OBJECT

resource string required
A resource ID to subscribe to. Many Asana resources are valid to create webhooks on, but higher-level resources require filters.

target url required
The URL to receive the HTTP POST. The full URL will be used to deliver events from this webhook (including parameters) which allows encoding of application-specific state when the webhook is created.

The screenshot shows the Asana API documentation for the 'Create Webhook' endpoint. The URL is `/webhooks`. The 'POST' method is shown with a code example:

```

1 import asana
2
3 client = asana.Client.access_token('PERSONAL_ACCESS_TOKEN')
4
5 result = client.webhooks.create_webhook({'field': 'value'})
    
```

The 'Try It!' button is visible at the bottom right.

REQUEST

EXAMPLES

RESPONSE

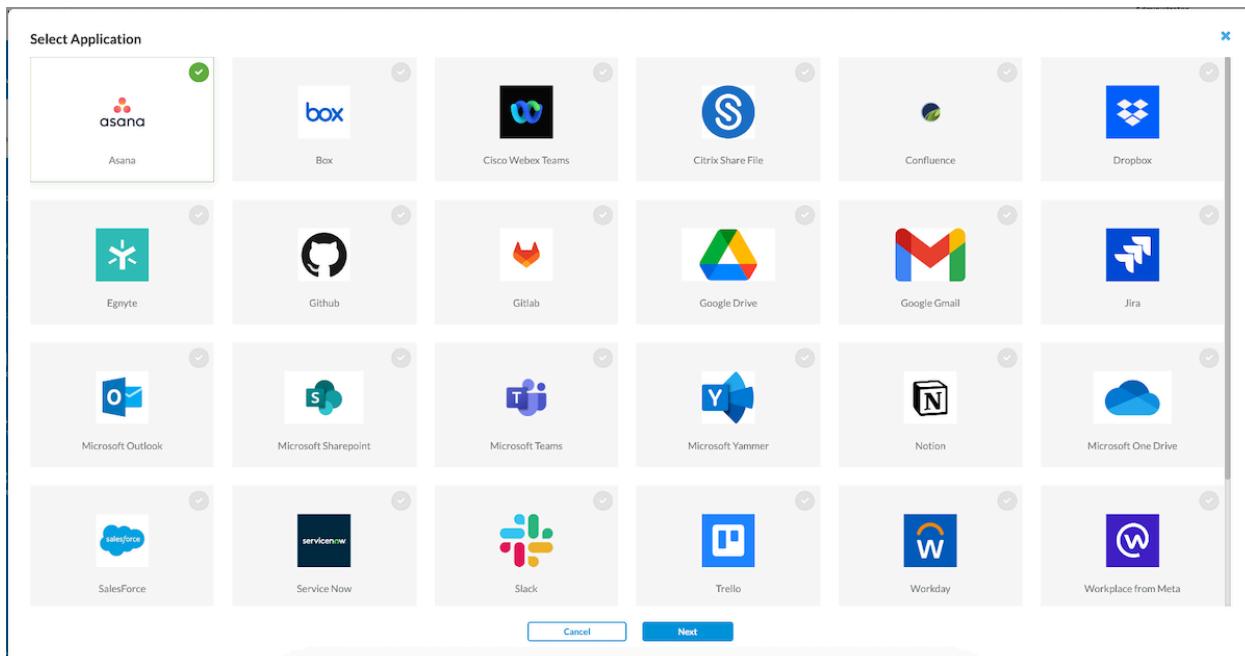
Click **Try It!** to start a request and see the response here! Or choose an example:
application/json

201 400 401 403 404 500

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.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

Add Instance - Asana

 Asana
[View Instructions](#) for setting up Asana instance.
×

Instance Name*

Admin Email*

Retro Scan

Services

API Based Data Protection

Confirm

Instance Add requires configuring your Asana account. [View Instructions](#) for setting up Asana instance.

Yes, I completed the steps required to configure Asana account

Cancel
Submit

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
	<ul style="list-style-type: none"> 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.

- 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.

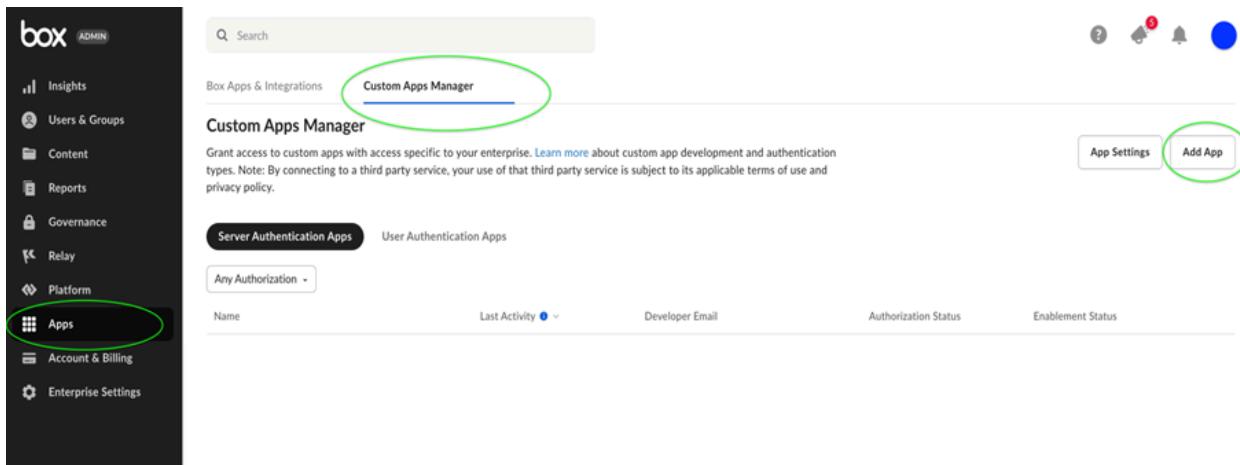
Box API-Based Data Protection

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:

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



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

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

The screenshot shows the Box Admin interface under the 'Custom Apps Manager'. The 'User Authentication Apps' tab is active. A table displays one application entry:

Name	Last Activity	Developer Email	Authorization Status	Enablement Status
Versa API-DP Box Events Connector		support@versa-networks.com	Authorized	Enabled

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.

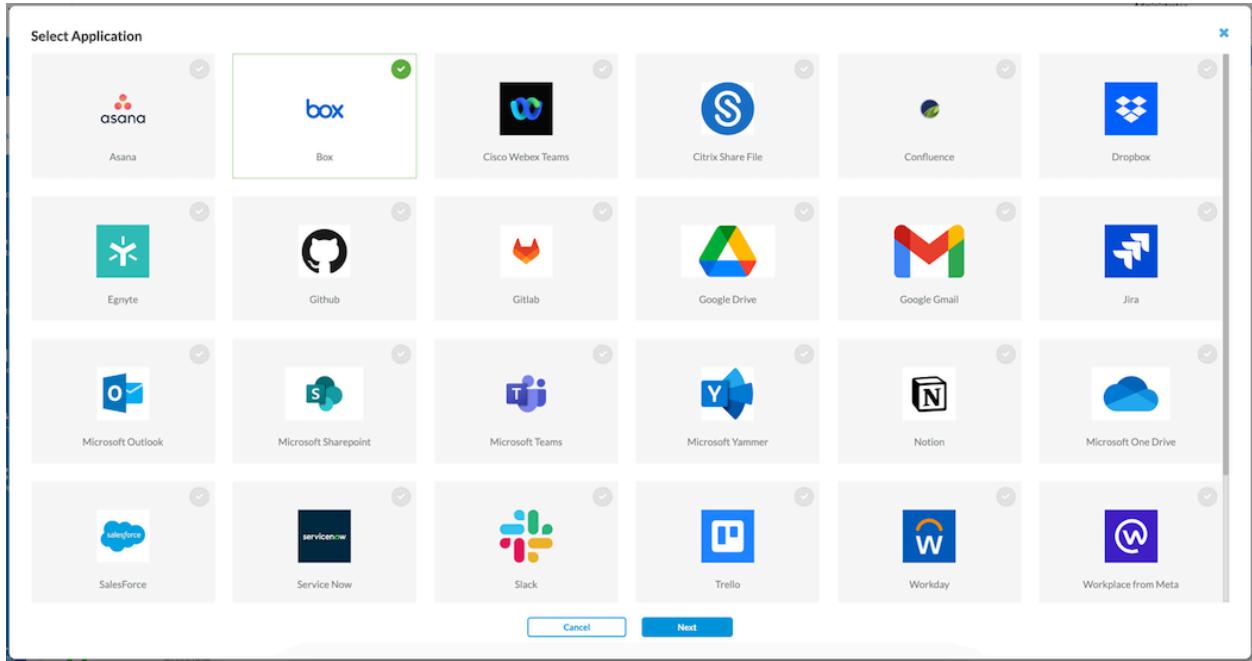
The screenshot shows the Box Admin interface under the 'Custom Apps Manager'. The 'User Authentication Apps' tab is active. A table displays one application entry:

Name	Last Activity	Developer Email	Enablement Status
Versa API-DP Box OAuth2 Connector		support@versa-networks.com	Enabled

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.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

Add Instance - Box

 Box [View Instructions](#) for setting up Box instance.

Instance Name*

Admin Email*

Retro Scan

Services

API Based Data Protection

Forensic

Legalhold

Quarantine

Confirm

Instance Add requires configuring your Box account. [View Instructions](#) for setting up Box instance.

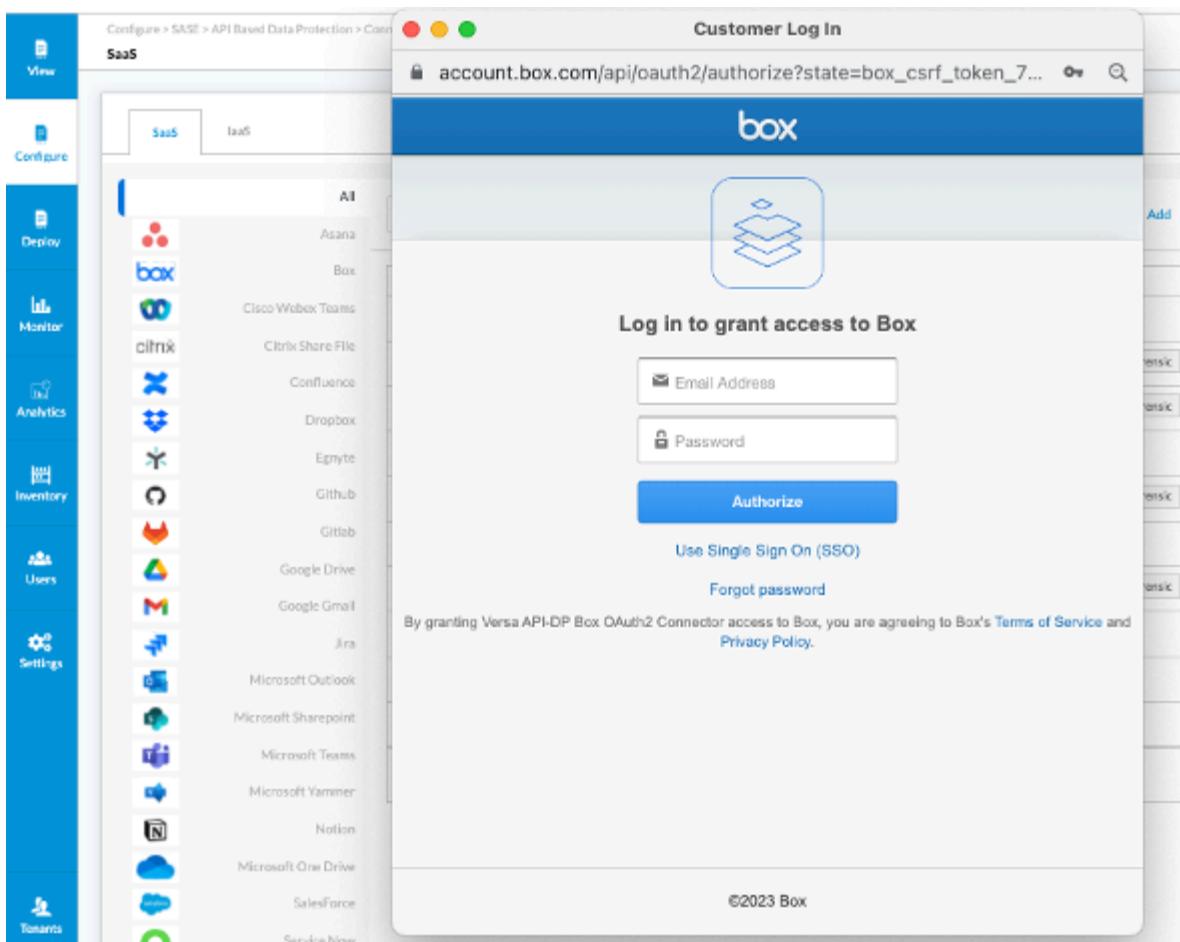
Yes, I completed the steps required to configure Box account

[Cancel](#) [Submit](#)

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
	<ul style="list-style-type: none"> ◦ 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

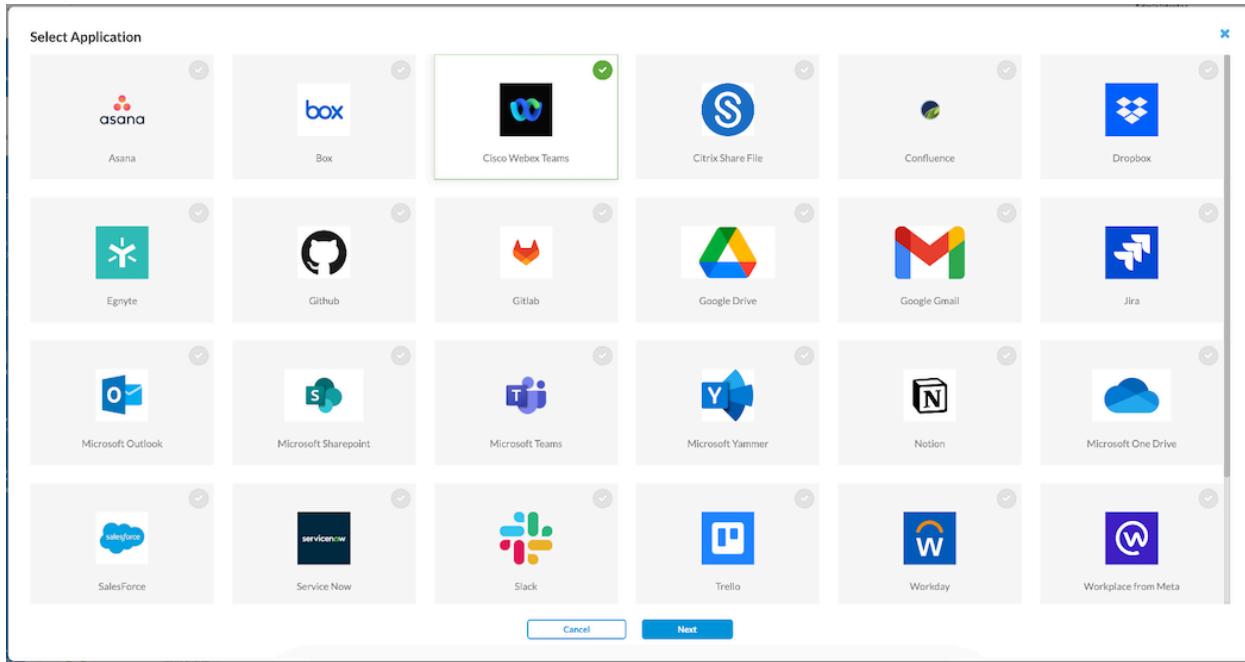
This section describes how to configure the Cisco Webex Teams application for API -baseddata protection.

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.

Add Instance - Cisco Webex Teams



Cisco Webex Teams
[View Instructions](#) for setting up Cisco Webex Teams instance.

Instance Name*

Admin Email*

Organization Name*

Retro Scan

Services
 API Based Data Protection

Provider Information

Confirm

Instance Add requires configuring your Cisco Webex Teams account. [View Instructions](#) for setting up Cisco Webex Teams instance.

Yes, I completed the steps required to configure Cisco Webex Teams account

[Cancel](#) [Submit](#)

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. <ul style="list-style-type: none"> ◦ 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

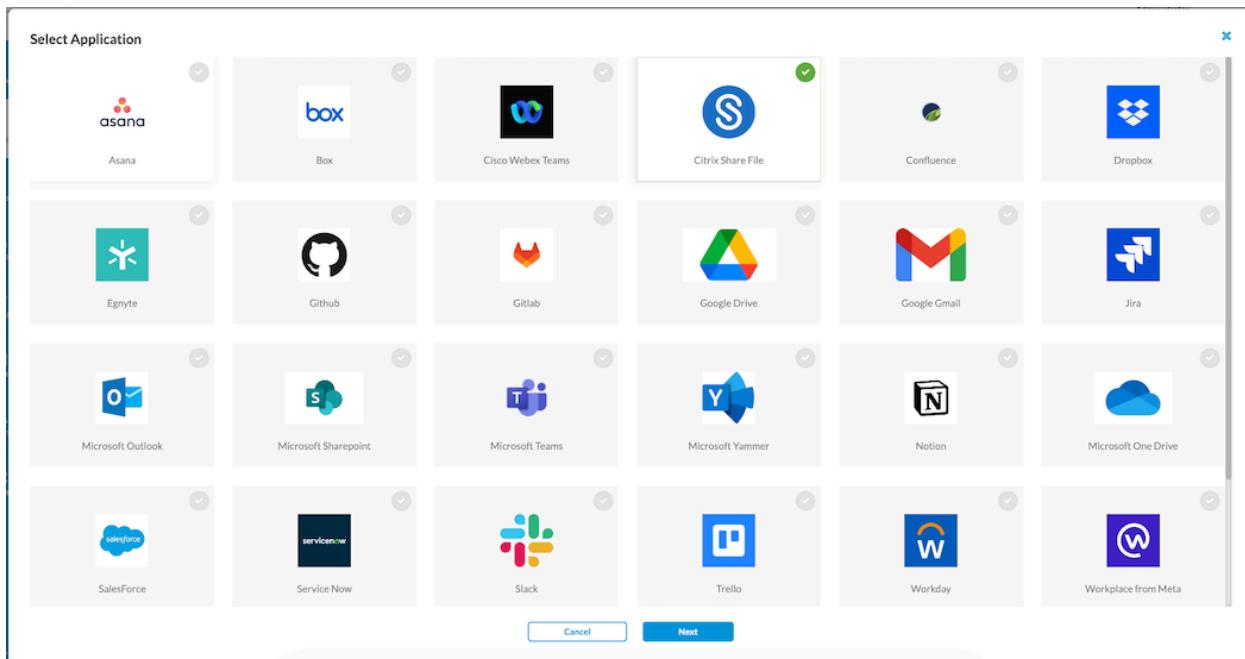
This section describes how to configure the Citrix ShareFile application for API-based data protection.

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.

Add Instance - Citrix Share File

 Citrix Share File
[View Instructions](#) for setting up Citrix Share File instance.

Instance Name*

Admin Email*

Retro Scan

Services

API Based Data Protection

Forensic

Legalhold

Quarantine

Confirm

Instance Add requires configuring your Citrix Share File account. [View Instructions](#) for setting up Citrix Share File instance.

Yes, I completed the steps required to configure Citrix Share File account

[Cancel](#) [Submit](#)

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. <ul style="list-style-type: none"> ◦ API-Based Data Protection—Scan and protect content ◦ Forensic—Use this instance for forensics

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

Field	Description
	<ul style="list-style-type: none"> ◦ 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.

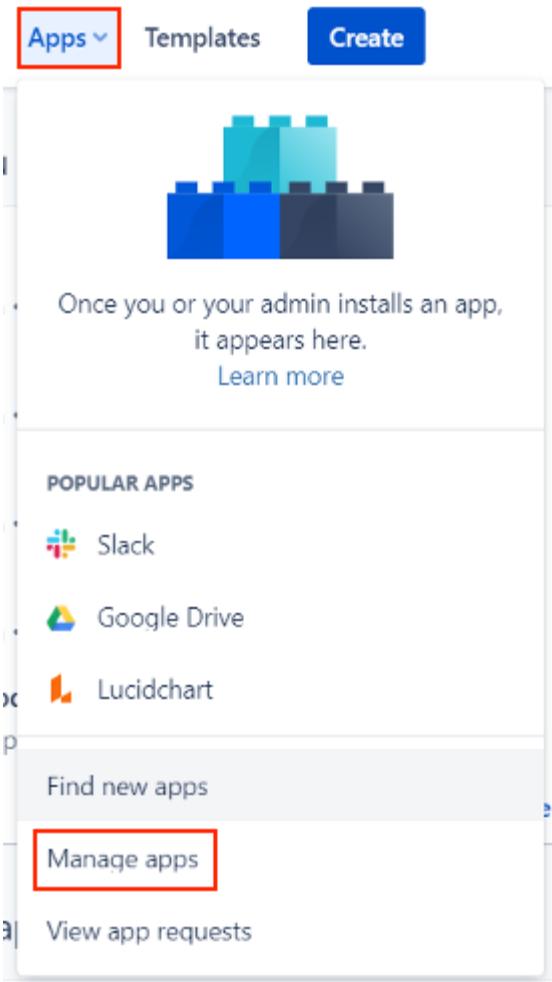
Confluence API-Based Data Protection

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.

Manage apps

You can install, update, enable, and disable apps here. [Find new apps.](#)

[Filter visible apps](#)

[User-installed](#)

[Upload app](#) [Build a new app](#)

User-installed apps

No user-installed apps found in your Confluence instance.

[Audit log](#) [Settings](#)

The Universal Plugin Manager (v1000.0.0.04232e2161a2) by Atlassian

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

Settings

Enable private listings

Enable [private listings](#) to install and license apps which aren't publicly available on the Atlassian Marketplace. These apps haven't been reviewed or approved by Atlassian, and Atlassian's Privacy Policy is not applicable to them.

Enable development mode

[Development mode](#) allows the installation of apps that are not listed on the Atlassian Marketplace.

(i) Private listing and development mode cannot be enabled for Forge apps.



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

Manage apps

You can install, update, enable, and disable apps here. [Find new apps.](#)

[Filter visible apps](#) [User-installed](#) [Upload app](#) [Build a new app](#)

User-installed apps

No user-installed apps found in your Confluence instance.

[Audit log](#) | [Settings](#)

The Universal Plugin Manager (v1000.0.0.04232e2161a2) by Atlassian

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

Upload app

⚠ Please make sure you trust this app before proceeding.

Apps uploaded in developer mode can access data and have not been reviewed or approved by Atlassian. Atlassian's Privacy Policy and Terms of Use do not apply.

Enter the app descriptor URL to upload the app and install

Enter app descriptor URL

Upload

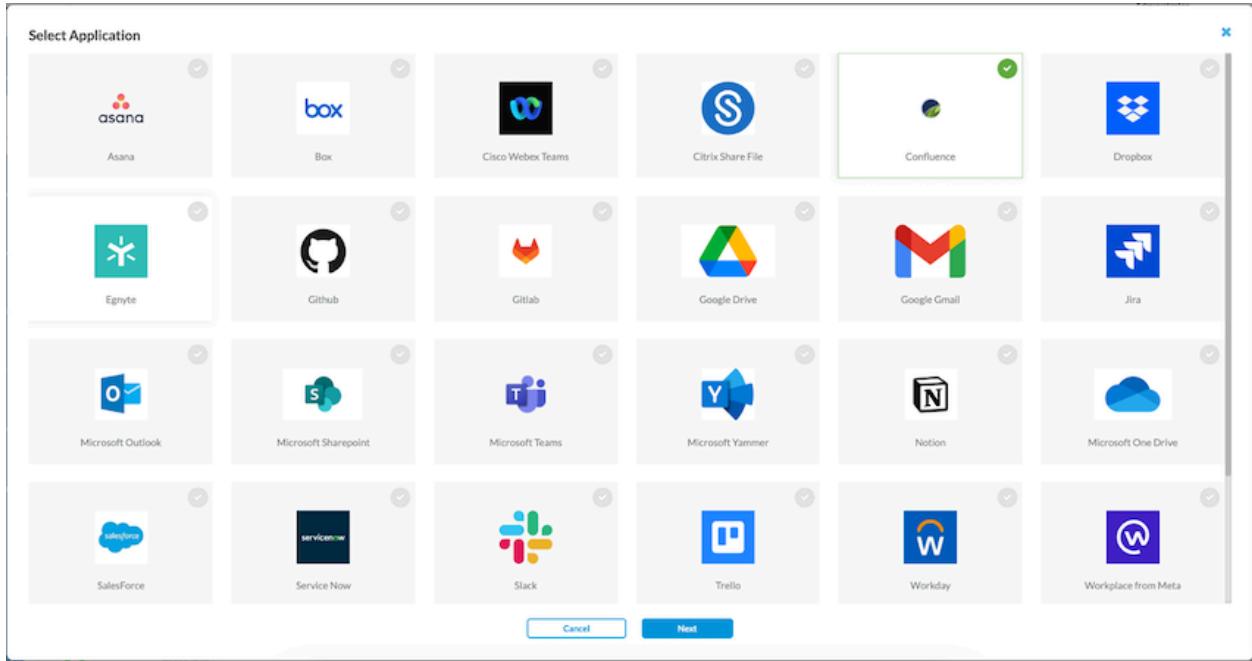
Cancel

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.

The screenshot shows the "Add Instance - Confluence" configuration window. At the top left is a logo of a blue circle with a green leaf. To its right, the text "Confluence" is displayed, followed by a link "View Instructions" for setting up Confluence instance.

Instance Name* **Admin Email***

Retro Scan

Services

API Based Data Protection

Confirm

Instance Add requires configuring your Confluence account. [View Instructions](#) for setting up Confluence instance.

Yes, I completed the steps required to configure Confluence account

Cancel **Submit**

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

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. <ul style="list-style-type: none"> ◦ 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 describes 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.

 **Dropbox**

Developers Documentation Guides Community & Support App Console

My apps Create app



VersaCASB
Status: Development
Permission type: Scoped App

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.

1. Choose an API

Scoped access New

Select the level of access your app needs to Dropbox data. [Learn more](#)



2. Choose the type of access you need

[Learn more about access types](#)

App folder – Access to a single folder created specifically for your app.

Full Dropbox – Access to **all** files and folders in a user's Dropbox.

3. Name your app

Create app

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.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

Creating a Dropbox app

- Configure app settings
- Select access scopes
- Add branding

Status	Development	Apply for production
Development teams	1 / 5	Unlink all teams
Development users	1 / 500	Unlink all users
Permission type	Scoped App	
App key	ogpxoxlt7a2ly6wx	Show
App secret		Show

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

OAuth 2

Redirect URIs

https://apidp.versanow.net/v1/dropbox/auth-callback

https:// (http allowed for localhost)

Allow public clients (Implicit Grant & PKCE)

Generated access token

Chooser / Saver / Embedder domains example.com
If using the Chooser, the Saver, or the Embedder on a website, add the domain of that site.

Webhooks

Webhook URIs	Status
https://apidp.versanow.net/v1/dropbox/webhook	Enabled <input type="button" value="Disable"/>

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

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

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

VersaCASB

Settings Permissions Branding Analytics

Individual Scopes Individual scopes include the ability to view and manage a user's files and folders. [View Documentation](#)

Account Info
Permissions that allow your app to view and manage Dropbox account info

<input checked="" type="checkbox"/> account_info.write	View and edit basic information about your Dropbox account such as your profile photo
<input checked="" type="checkbox"/> account_info.read	View basic information about your Dropbox account such as your username, email, and country

Files and folders
Permissions that allow your app to view and manage files and folders

<input checked="" type="checkbox"/> files.metadata.write	View and edit information about your Dropbox files and folders
<input checked="" type="checkbox"/> files.metadata.read	View information about your Dropbox files and folders
<input checked="" type="checkbox"/> files.content.write	Edit content of your Dropbox files and folders
<input checked="" type="checkbox"/> files.content.read	View content of your Dropbox files and folders

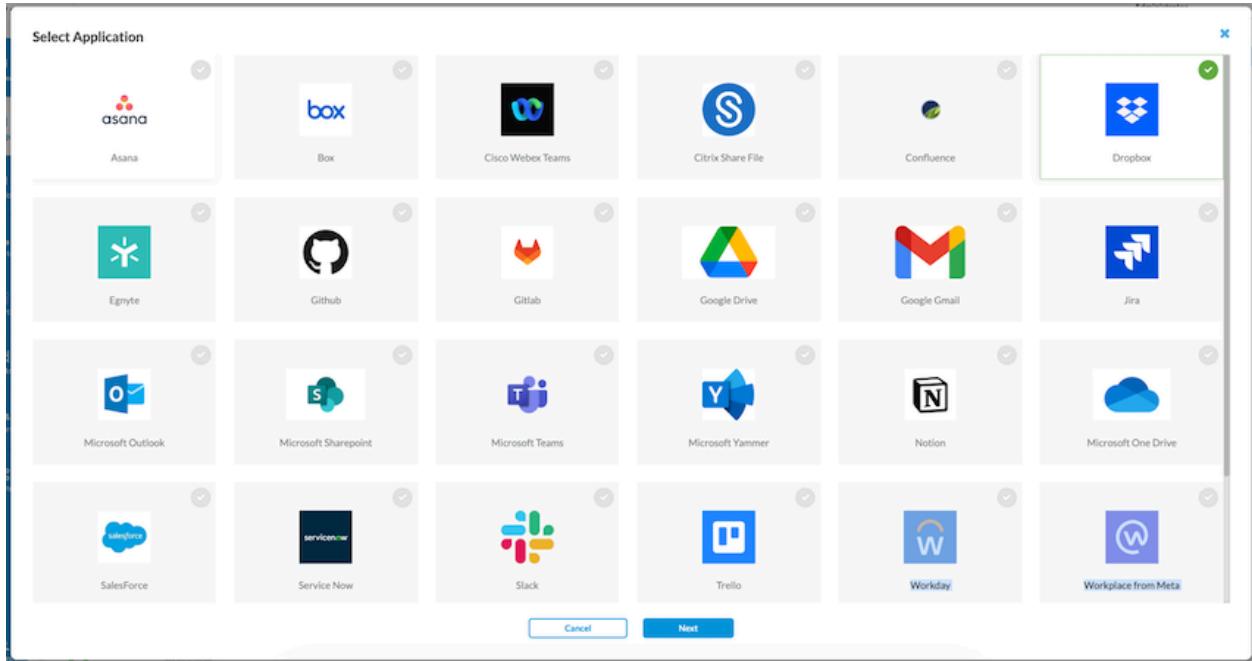
Collaboration
Permissions that allow your app to view and manage sharing and collaboration settings

<input checked="" type="checkbox"/> sharing.write	View and manage your Dropbox sharing settings and collaborators
<input checked="" type="checkbox"/> sharing.read	View your Dropbox sharing settings and collaborators
<input checked="" type="checkbox"/> file_requests.write	View and manage your Dropbox file requests
<input checked="" type="checkbox"/> file_requests.read	View your Dropbox file requests
<input checked="" type="checkbox"/> contacts.write	View and manage your manually added Dropbox contacts
<input checked="" type="checkbox"/> contacts.read	View your manually added Dropbox contacts

OpenID Scopes Scopes used for OpenID Connect.
At this time, team-scoped apps **cannot** request OpenID Connect scopes.
OpenID scopes must be explicitly set in the "scope" parameter on [/oauth2/authorize](#) to be requested.

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.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

Add Instance - Dropbox

 Dropbox
[View Instructions](#) for setting up Dropbox instance.

Instance Name*

Admin Email*

Retro Scan

Services

API Based Data Protection

Forensic

Legalhold

Quarantine

Confirm

Instance Add requires configuring your Dropbox account. [View Instructions](#) for setting up Dropbox instance.

Yes, I completed the steps required to configure Dropbox account

[Cancel](#) [Submit](#)

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
	<ul style="list-style-type: none"> ◦ 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

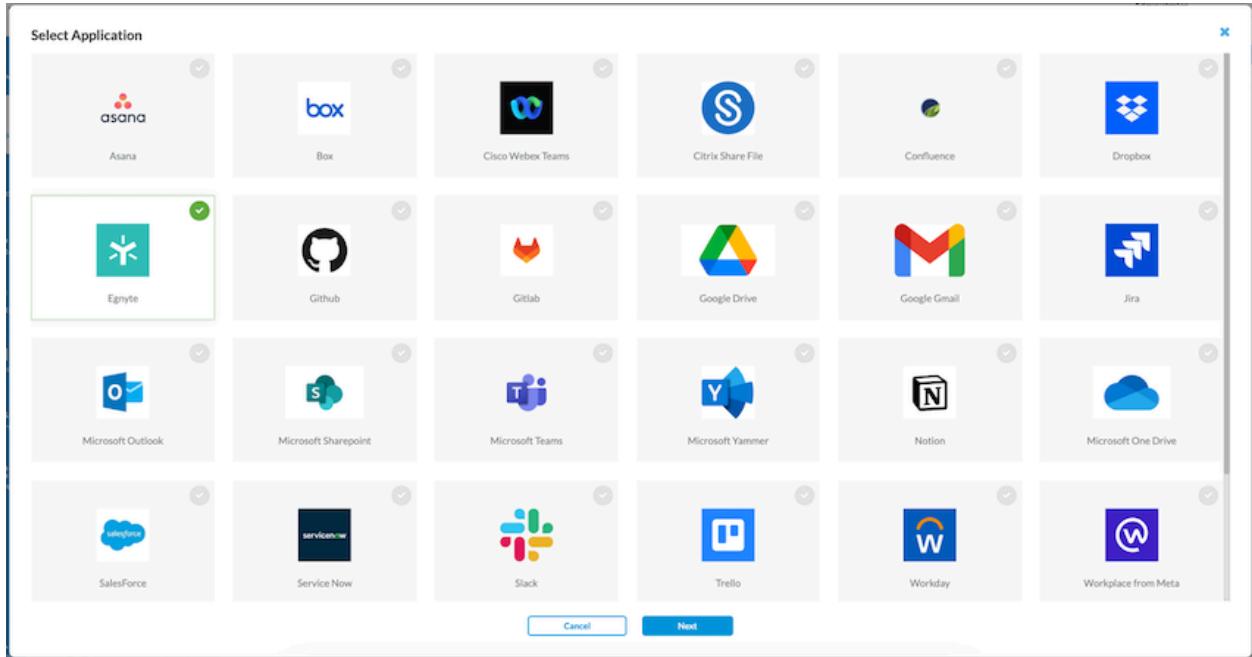
This section describes how to configure the Confluence application for API-based data protection.

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.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

Add Instance - Egnyte

 Egnyte
[View Instructions](#) for setting up Egnyte instance.

Instance Name*

Admin Email*

Domain Name* Retro Scan

Services

- API Based Data Protection
- Forensic
- Legalhold
- Quarantine

Confirm

Instance Add requires configuring your Egnyte account. [View Instructions](#) for setting up Egnyte instance.

Yes, I completed the steps required to configure Egnyte account

[Cancel](#) [Submit](#)

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
	<ul style="list-style-type: none"> ◦ 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.

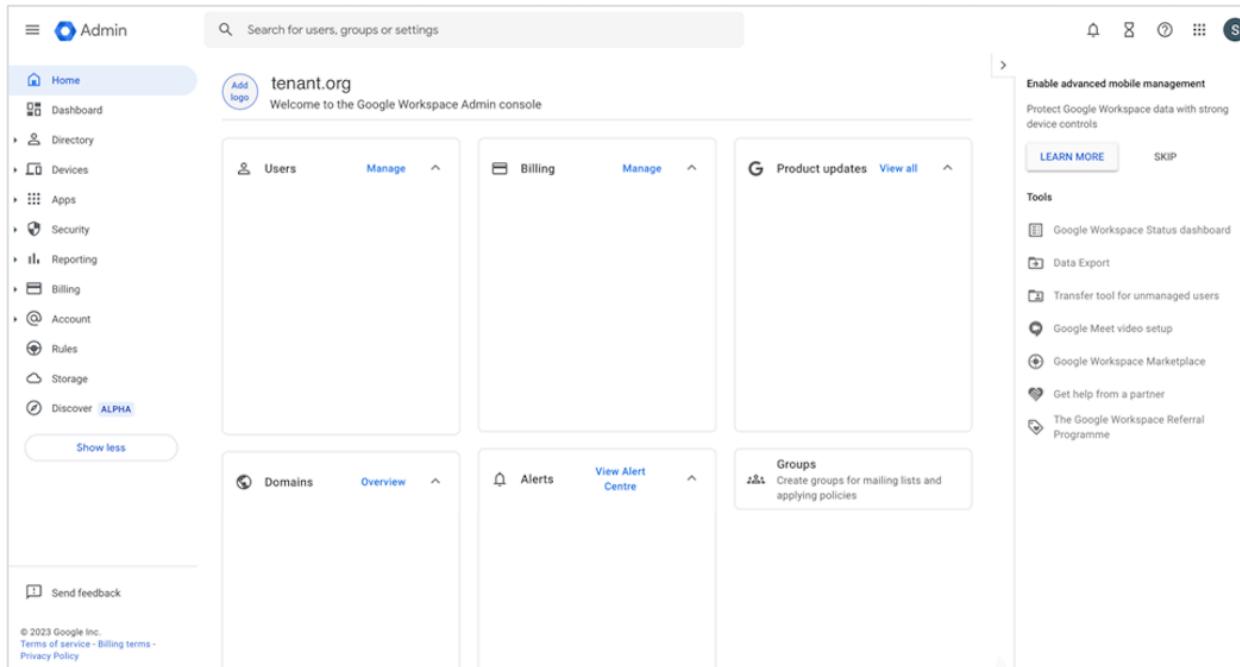
Google Drive API-Based Data Protection

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.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

The screenshot shows the Google Admin interface under the 'Security' section, specifically the 'Domain-wide delegation' tab. On the left, there's a sidebar with various administrative links like Home, Dashboard, Directory, Devices, Apps, Security, Reporting, Billing, Account, and Help. The main content area has a search bar at the top. Below it, a message states: 'Developers can register their web applications and other API clients with Google to enable access to data in Google services like Gmail. You can authorise these registered clients to access your user data without your users having to individually give consent or their passwords.' A 'GOT IT' button is present. The central part of the screen lists 'API clients' with columns for Name, Client ID, and Scopes. There are five entries: 'Versa API DP' (Client ID: 105557577682135063975, Scopes: https://mail.google.com/.auth/admin.directory.user +3 More), 'mailapi' (Client ID: 118977803913220489216, Scopes: https://mail.google.com/.auth/admin.directory.user), 'malware lookup service' (Client ID: 102595913479140598023, Scopes: https://mail.google.com/.auth/admin.directory.user), 'Gdrive-CASB' (Client ID: 116387605955495669804, Scopes: openid https://mail.google.com/.auth/userinfo.email +11 More), and 'malware lookup service' (Client ID: 113866028843424440405, Scopes: openid https://mail.google.com/.auth/userinfo.email +19 More). Buttons for 'View details', 'Edit', and 'Delete' are available for each entry. At the bottom, there are pagination controls for 'Rows per page: 10' and 'Page 1 of 1'.

4. Enter information for the following fields.

The screenshot shows a 'Edit scopes' dialog box. At the top, it says 'Edit scopes'. Below that, there's a 'Client ID' field containing '113866028843424440405'. Underneath, there are two 'OAuth scopes (comma-delimited)' fields. The first field contains 'openid' and the second contains 'https://www.googleapis.com/auth/userinfo.email'. Both fields have a clear 'X' button to the right. At the bottom, there are 'CANCEL' and 'AUTHORISE' buttons.

Field	Description
Client ID	Add client ID 113866028843424440405.
Scopes	Add the following scopes; <ul style="list-style-type: none"> ◦ https://www.googleapis.com/auth/admin.datatransfer ◦ https://www.googleapis.com/auth/

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

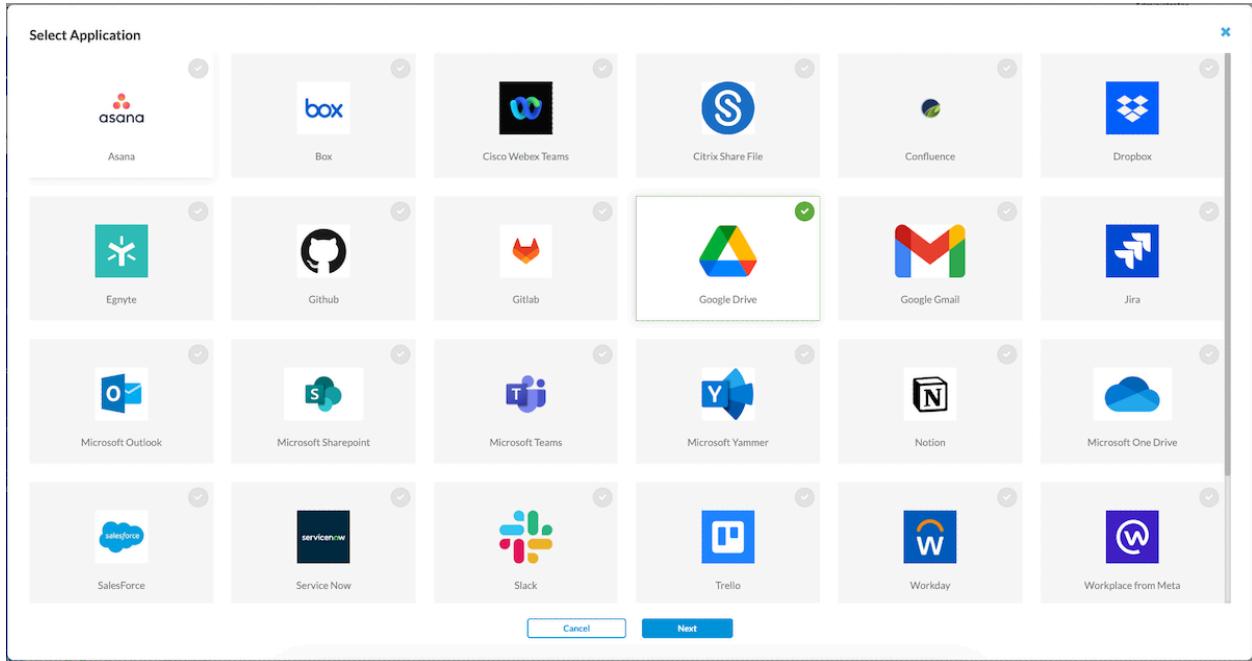
Copyright © 2024, Versa Networks, Inc.

Field	Description
	<ul style="list-style-type: none"> 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.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

Add Instance - Google Drive



Google Drive
[View Instructions](#) for setting up Google Drive instance.

Instance Name*

Admin Email*

Retro Scan

Services

API Based Data Protection

Forensic

Legalhold

Quarantine

Confirm

Instance Add requires configuring your Google Drive account. [View Instructions](#) for setting up Google Drive instance.

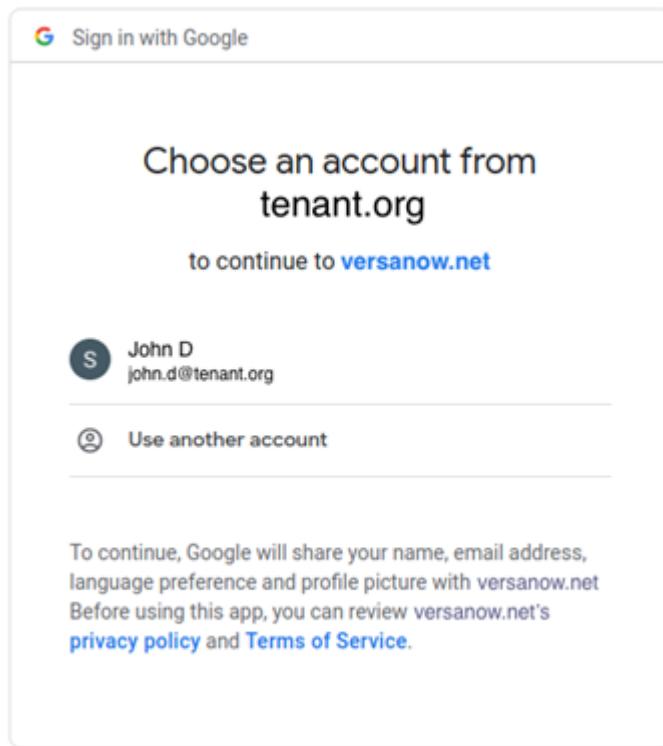
Yes, I completed the steps required to configure Google Drive account

[Cancel](#) [Submit](#)

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. <ul style="list-style-type: none"> ◦ API-Based Data Protection—Scan and protect content.

Field	Description
	<ul style="list-style-type: none"> ◦ 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.

 Sign in with Google

versanow.net wants additional access to your Google Account

 john.d@tenant.org

When you allow this access, **versanow.net** will be able to

 See, edit, create and delete all of your Google Drive files. [Learn more](#)

 **versanow.net already has some access**

See the [3 services](#) to which versanow.net has some access.

Make sure that you trust versanow.net

You may be sharing sensitive info with this site or app. You can always see or remove access in your [Google Account](#).

Learn how Google helps you [share data safely](#).

See versa-test.net's [privacy policy](#) and [Terms of Service](#).

[Cancel](#) [Continue](#)

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.

The screenshot shows the Google Workspace Admin console interface. The left sidebar has a red box around the 'Security' section, and within it, another red box surrounds the 'API controls' link. The main content area shows a 'Users' card with 6 active users and links to add or delete users. To the right is a 'Billing' card with links to manage subscriptions and payment accounts. At the bottom are 'Product updates' and 'Domains' cards.

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

The screenshot shows the 'API controls' page under 'Security'. The left sidebar has a red box around the 'API controls' link. The main content area has a 'Domain-wide delegation' section with a red box around the 'MANAGE DOMAIN-WIDE DELEGATION' button. The 'Domain-wide delegation' section contains text about developers registering web applications and a link to 'MANAGE DOMAIN-WIDE DELEGATION'.

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

Add a new client ID

Client ID **Enter Client ID here**

Overwrite existing client ID ?

OAuth scopes (comma-delimited) X

ps://www.googleapis.com/auth/admin.directory.user

OAuth scopes (comma-delimited) X

<https://mail.google.com/>

CANCEL **AUTHORISE**

Field	Description
Client ID	Enter the client ID 105557577682135063975.
OAuth Scopes	Enter two OAuth scopes: <ul style="list-style-type: none"> ◦ https://mail.google.com/ ◦ https://www.googleapis.com/auth/admin.directory.user

- Click Authorize.

Configure a Gmail Connector

- Under API-Based Data Protection, select Application > Gmail.
- 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. <ul style="list-style-type: none"> ◦ 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.

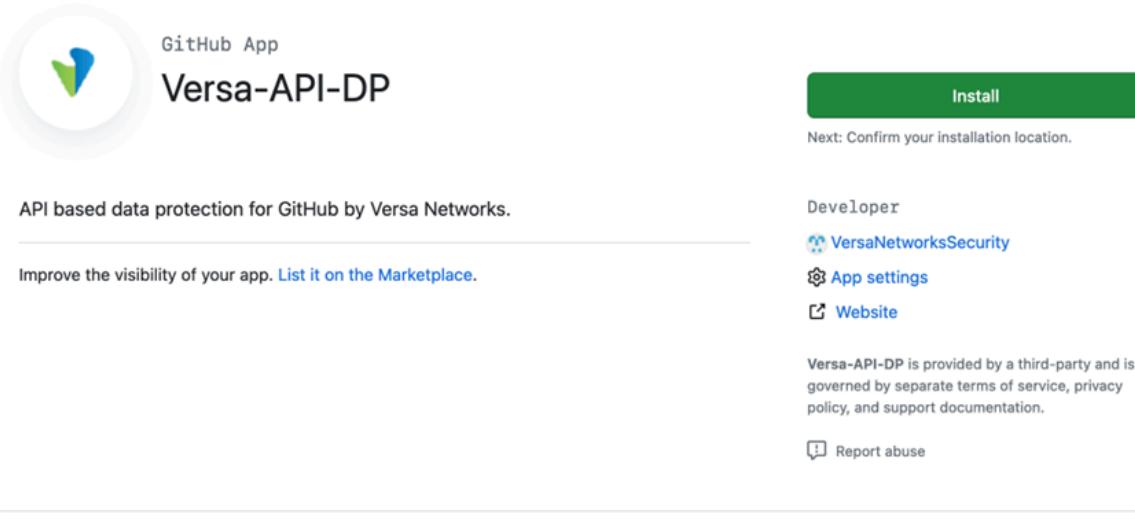
GitHub API-Based Data Protection

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.

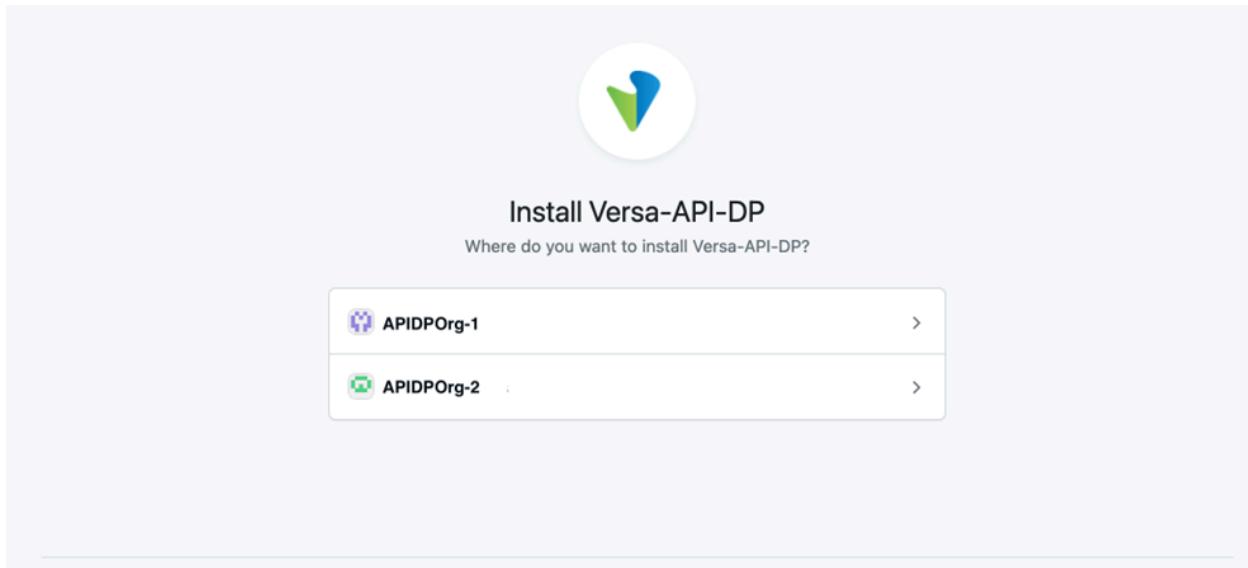


3. Select the user, team, or organization to install GitHub.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

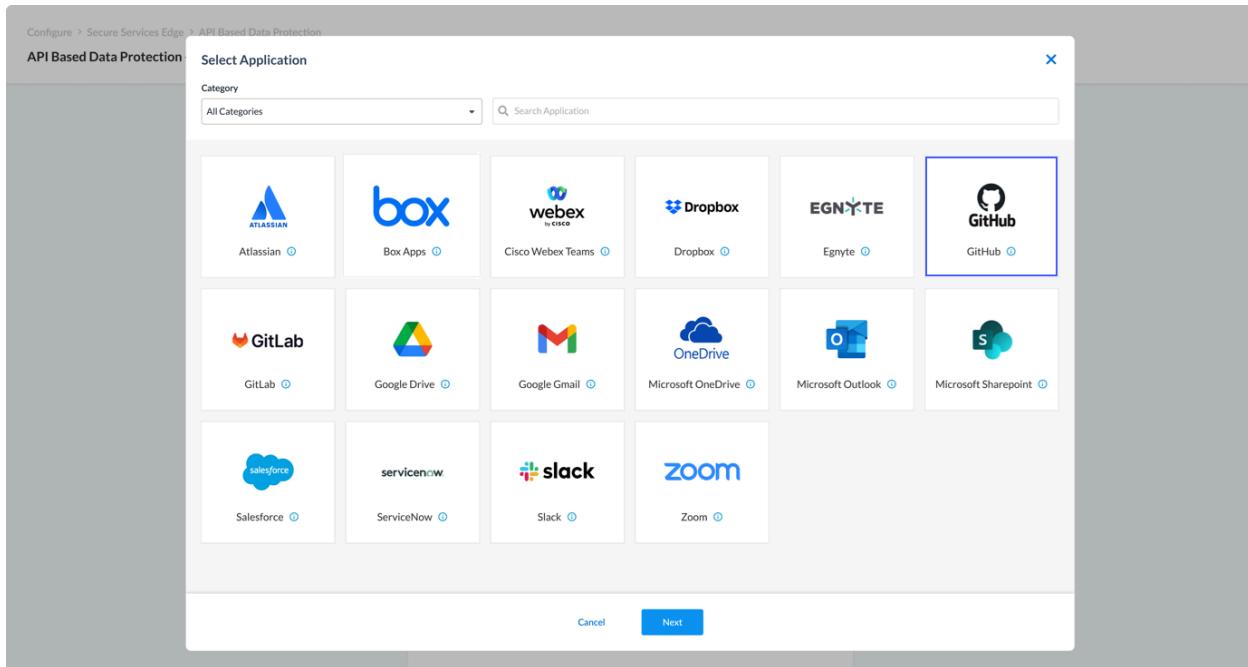
Copyright © 2024, Versa Networks, Inc.



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.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

The screenshot shows a configuration dialog titled "Add Instance - Github". At the top left is a GitHub logo with the text "Github" and a link "View Instructions" for setting up a GitHub instance. Below this are fields for "Instance Name*" (Input Name) and "Admin Email*" (Input Admin Email). A section for "Enter List of Internal Domains*" with a placeholder "Separate list with ','" follows. Under "Services", there are three checkboxes: "API Data Protection", "Multi Geo", and "Security Posture" (selected), with a dropdown menu showing "Every 60 Minutes". A "Confirm" section at the bottom contains a note: "Instance Add requires configuring your GitHub account. View Instructions for setting up GitHub instance." and a checkbox "Yes, I completed the steps required to configure GitHub account". At the bottom right are "Cancel" and "Submit" buttons.

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. <ul style="list-style-type: none"> ◦ API-Based Data Protection—Scan and protect content. ◦ Multi Geo—Use this instance for multiple 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.

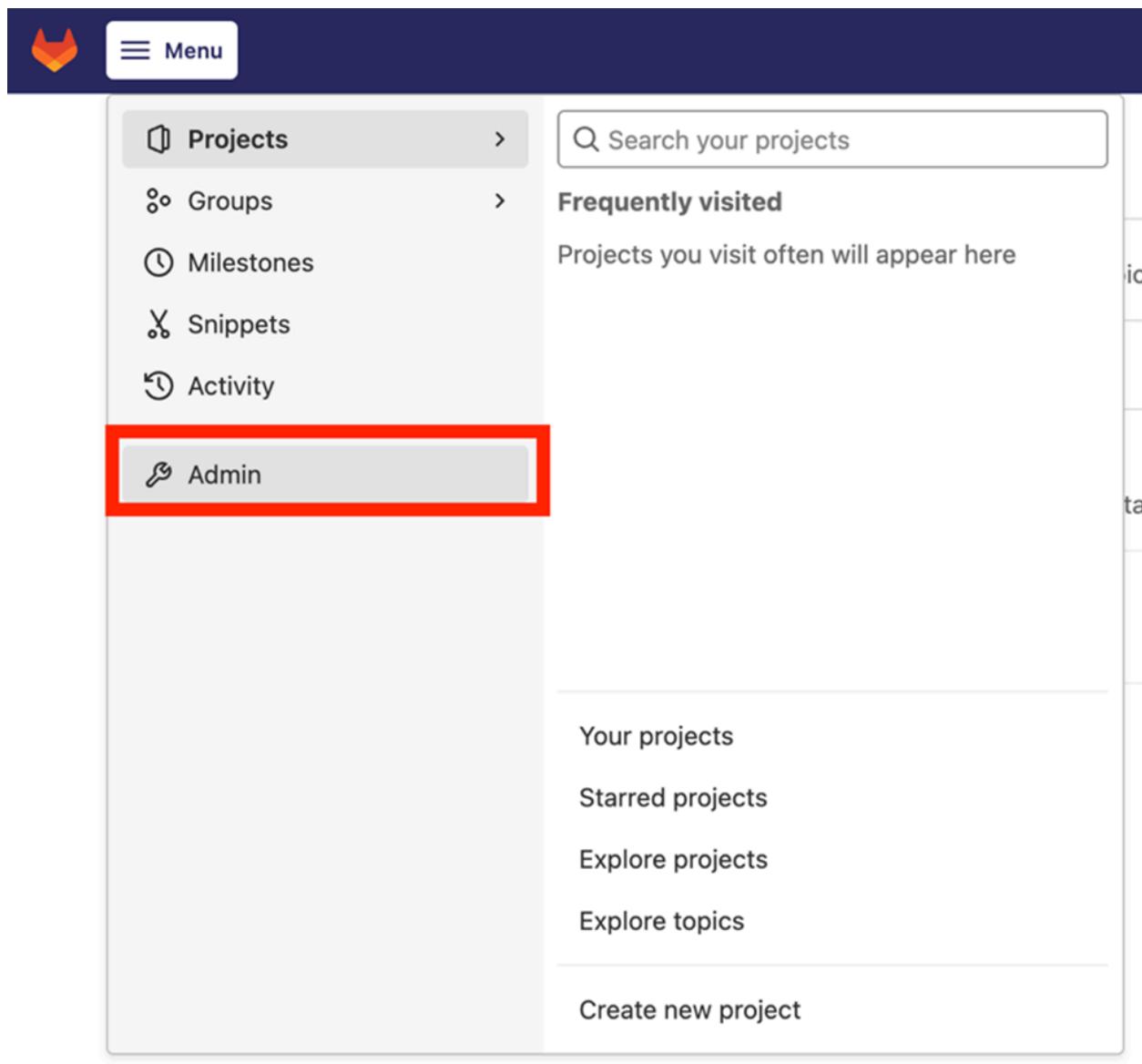
GitLab API-Based Data Protection

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.

The screenshot shows the GitLab Admin Area interface. On the left, there's a sidebar with various options like Overview, Analytics, Monitoring, Messages, System Hooks, Applications (which is selected and highlighted in grey), Abuse Reports, Subscription, Geo, Deploy Keys, Labels, and Settings. A blue button labeled 'New application' is prominently displayed in the center of the main content area. The main title is 'Instance OAuth applications' with the subtitle 'Manage applications for your instance that can use GitLab as an OAuth provider.'

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

Add new application

Name

Redirect URI
Use one line per URI

Trusted Trusted applications are automatically authorized on GitLab OAuth flow. It's highly recommended for the security of users that trusted applications have the confidential setting set to true.

Confidential The application will be used where the client secret can be kept confidential. Native mobile apps and Single Page Apps are considered non-confidential.

Scopes **api**
Grants complete read/write access to the API, including all groups and projects, the container registry, and the package registry.
 read_api
Grants read access to the API, including all groups and projects, the container registry, and the package registry.
 read_user
Grants read-only access to the authenticated user's profile through the /user API endpoint, which includes username, public email, and full name. Also grants access to read-only API endpoints under /users.
 read_repository
Grants read-only access to repositories on private projects using Git-over-HTTP or the Repository Files API.
 write_repository
Grants read-write access to repositories on private projects using Git-over-HTTP (not using the API).
 sudo
Grants permission to perform API actions as any user in the system, when authenticated as an admin user.
 openid
Grants permission to authenticate with GitLab using OpenID Connect. Also gives read-only access to the user's profile and group memberships.
 profile
Grants read-only access to the user's profile data using OpenID Connect.
 email
Grants read-only access to the user's primary email address using OpenID Connect.

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.

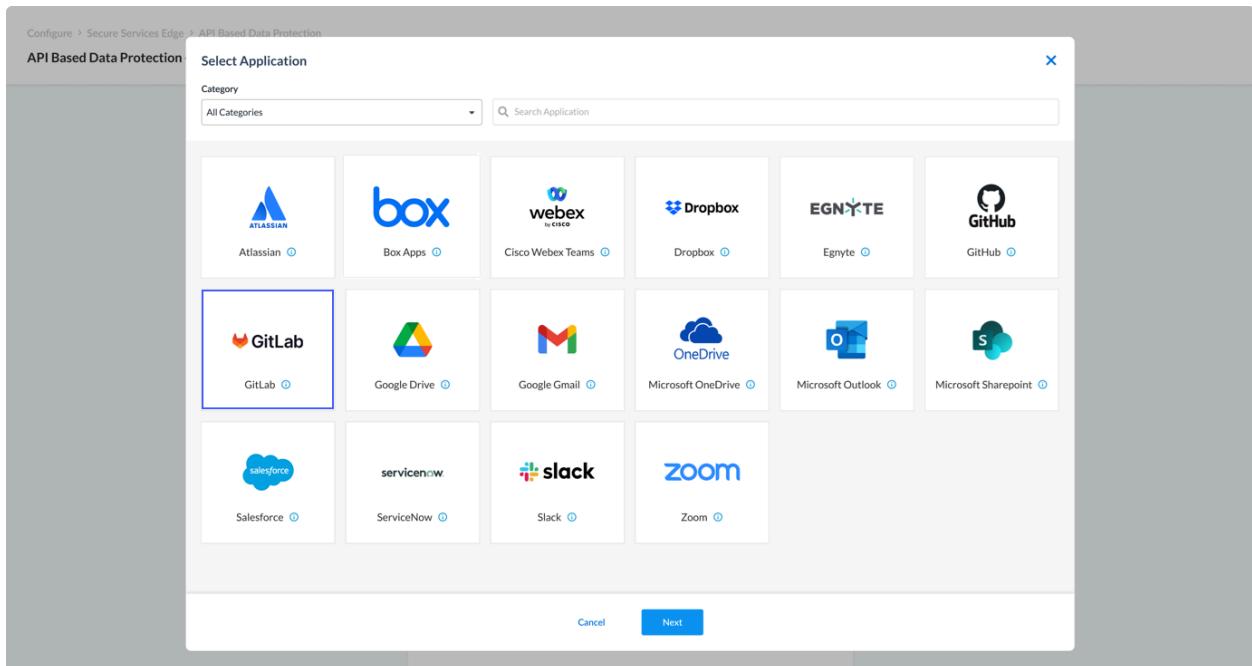
5. Note down the application ID and click Copy icon to copy the secret value. Save this information to use while creating GitLab connector.

Application: Versa-APIDP Demo

Application ID	49ff2383990711b9f568e	
Secret		
Callback URL	https://apidp.versanow.net/v1/gitlab/auth-callback	
Trusted	No	
Confidential	Yes	
Scopes	<ul style="list-style-type: none">api (Access the authenticated user's API)read_api (Read Api)read_user (Read the authenticated user's personal information)read_repository (Allows read-only access to the repository)write_repository (Allows read-write access to the repository)sudo (Perform API actions as any user in the system)openid (Authenticate using OpenID Connect)profile (Allows read-only access to the user's personal information using OpenID Connect)email (Allows read-only access to the user's primary email address using OpenID Connect)	
<button>Continue</button> <button>Edit</button>		<button>Destroy</button>

Configure a GitLab Connector

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



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

Configure > Secure Services Edge > API Based Data Protection

Creating API Based Data Protection Instance - GitLab

GitLab [View Instructions](#) for setting up GitLab instance.

Instance Name* **Admin Email***

Enter List of Internal Domains*
Separate list with ","

Services

- API Data Protection
- Multi Geo
- Security Posture Every 60 Minutes

Confirm
Instance Add requires configuring your Github account. [View Instructions](#) for setting up GitLab instance.

Yes, I completed the steps required to configure Github account

Cancel **Submit**

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. <ul style="list-style-type: none"> ◦ 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.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

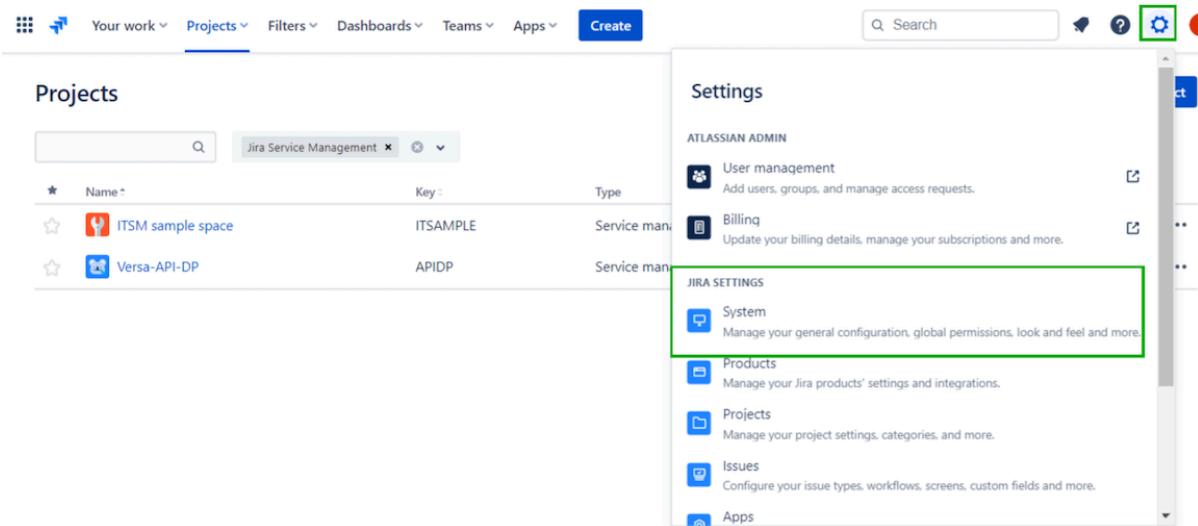
Jira API-Based Data Protection

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.

The screenshot shows the Jira System Settings page. On the left, there's a sidebar with categories like System, Admin Helper, Shared Items, Advanced, and WebHooks (which is highlighted with a green box). The main content area has sections for General Settings (Title: Jira, Email from: \${fullname} (Jira)) and Internationalization (Indexing language: English - Aggressive Stemming, Installed languages: Chinese (China), Chinese (Taiwan), Czech (Czechia), Danish (Denmark), Dutch (Netherlands), English (United Kingdom), English (United States)).

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

The screenshot shows the Jira WebHooks page. The sidebar includes System, Troubleshooting and Support, Security, Automation, and User Interface. The main content shows a message: "No WebHooks are configured." Below it is a warning about the "Webhook limit update": "Starting July 1, 2023, we're putting in place a limit of up to 100 active webhooks per Jira instance. This doesn't affect your existing webhooks in any way." A link to "Jira admin webhooks limit update" is provided. In the top right, there's a "Create" button and a "+ Create a WebHook" button, which is highlighted with a green box.

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

The screenshot shows the Jira 'WebHooks' configuration interface. A new webhook listener is being created with the following details:

- Name:** APIDP-Webhook
- Status:** Enabled
- URL:** https://apidp.versanow.net/v1/jira/webhook
- Description:** (Empty)

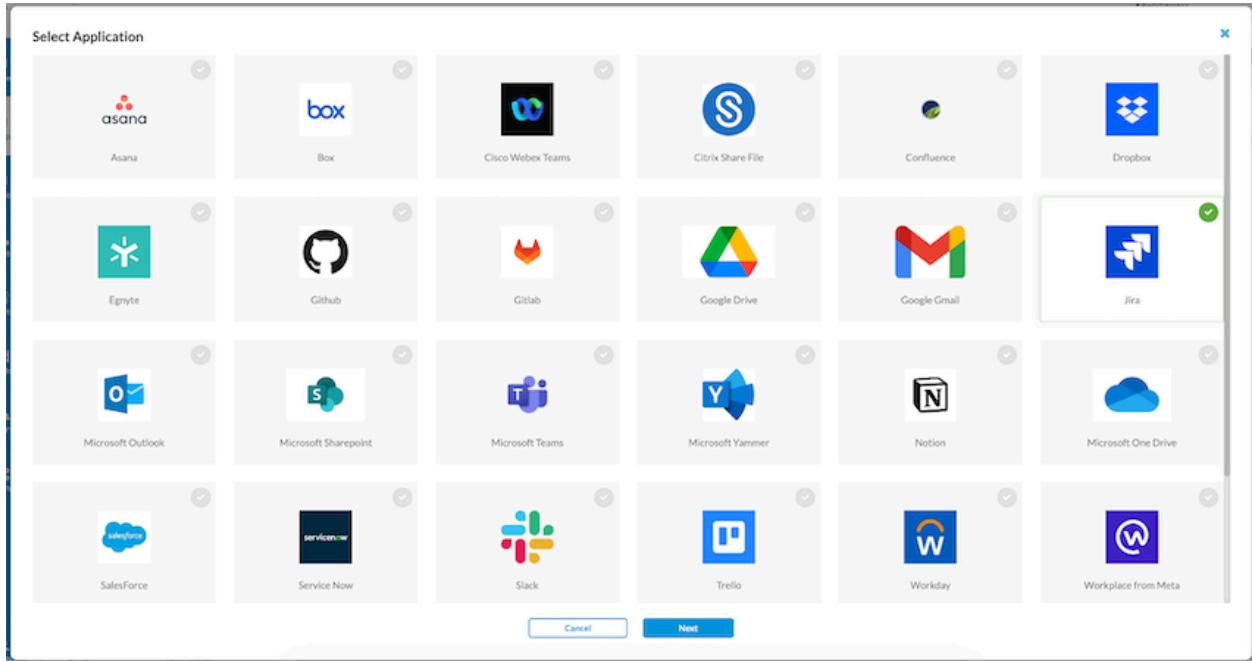
- Select the events that trigger the webhook and click Create at the bottom of the screen.

The screenshot shows the Jira 'Events' configuration interface. Under the 'Issue related events' section, the following checkboxes are selected:

- Issue**: created, updated, deleted
- Comment**: created, updated, deleted
- Attachment**: created, updated, deleted
- Issue link**: created, updated, deleted

Configure a Jira Connector

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



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

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

Add Instance - Jira

 Jira
[View Instructions](#) for setting up Jira instance.

Instance Name*

Admin Email*

Retro Scan

Services

API Based Data Protection

Confirm

Instance Add requires configuring your Jira account. [View Instructions](#) for setting up Jira instance.

Yes, I completed the steps required to configure Jira account

[Cancel](#) [Submit](#)

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. <ul style="list-style-type: none"> ◦ API-Based Data Protection—Scan and protect content.
Confirm	Click to confirm that the steps required to configure the Jira account are complete.

- 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

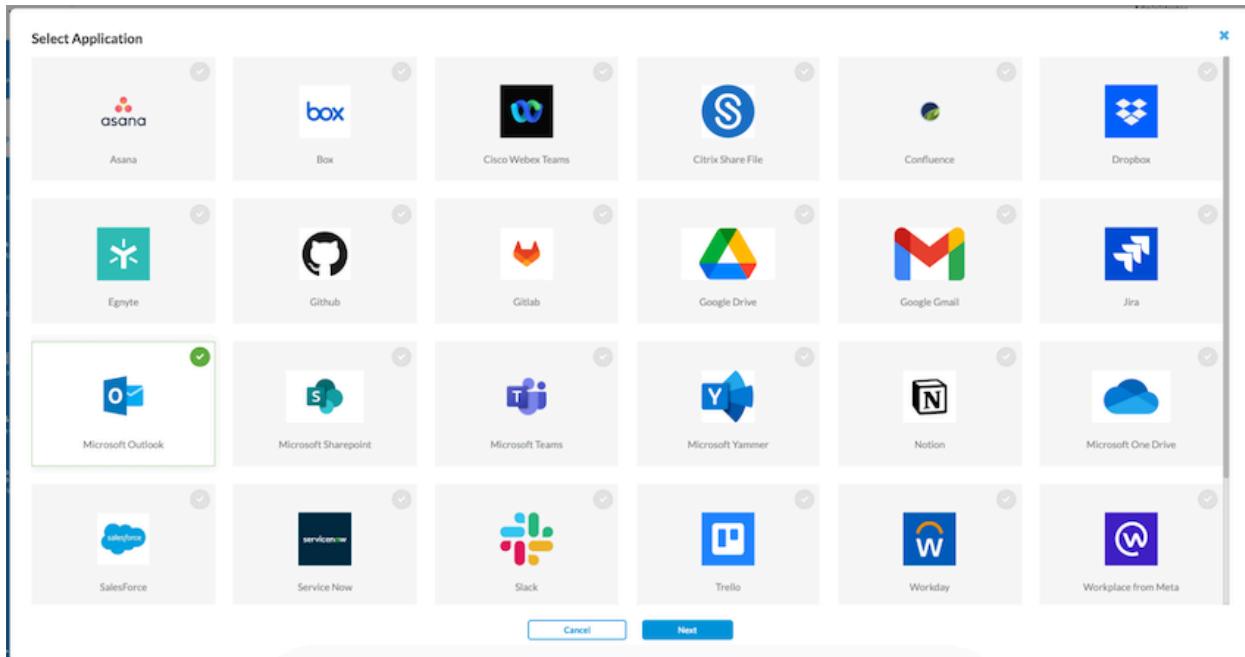
This section describes how to configure the Microsoft Outlook application for API-based data protection.

Configure Microsoft Outlook for API-Based Data Protection

For Microsoft Outlook, no configuration is required.

Configure a Microsoft Outlook Connector

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



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

Add Instance - Microsoft Outlook

 Microsoft Outlook
[View Instructions](#) for setting up Microsoft Outlook instance.

Instance Name*	Admin Email*
<input type="text" value="Input Name"/>	<input type="text" value="Input Admin Email"/>
Enter List of Internal Domains*	
<input type="text" value="Press Enter to add"/>	
<input type="checkbox"/> Retro Scan	
Services	
<input type="checkbox"/> API Based Data Protection	
Confirm	
Instance Add requires configuring your Microsoft Outlook account. View Instructions for setting up Microsoft Outlook instance.	
<input type="checkbox"/> Yes, I completed the steps required to configure Microsoft Outlook account	
<input type="button" value="Cancel"/> <input type="button" value="Submit"/>	

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. <ul style="list-style-type: none"> ◦ API-Based Data Protection—Scan and protect content.
Confirm	Click to confirm that the steps required to configure the Microsoft Outlook account are complete.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

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

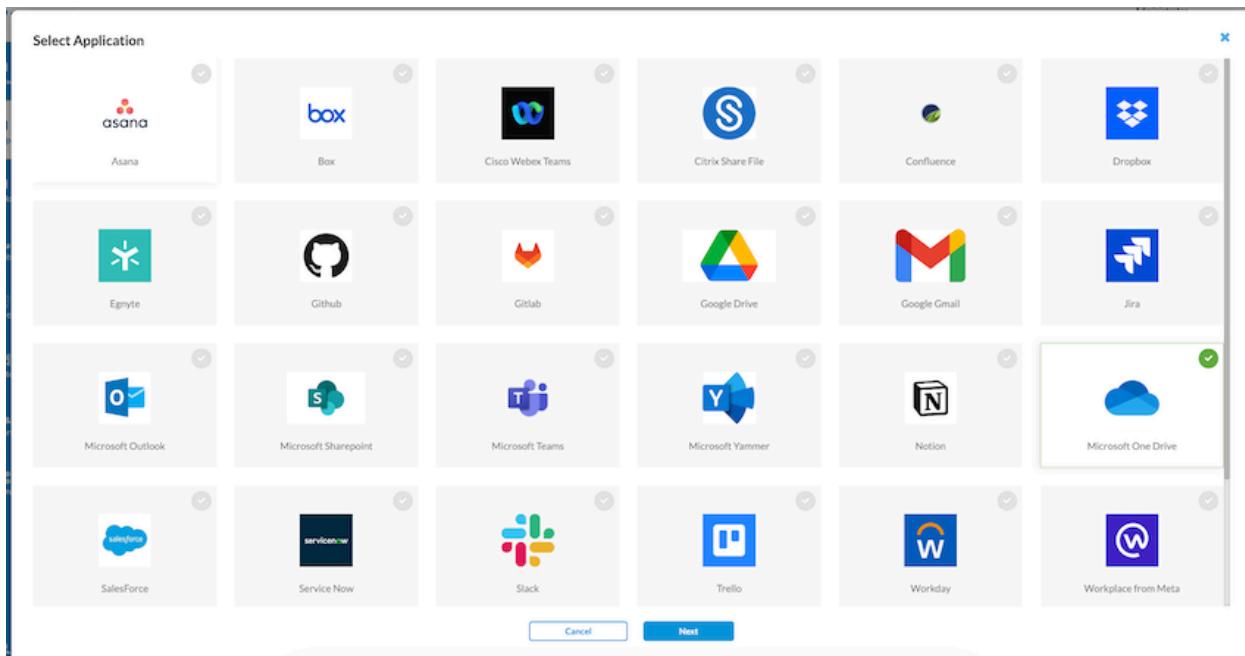
This section describes how to configure the Microsoft OneDrive application for API-based data protection.

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.

Add Instance - Microsoft One Drive

 Microsoft One Drive
[View Instructions](#) for setting up Microsoft One Drive instance.

Instance Name*

Admin Email*

Enter List of Internal Domains*

Retro Scan

Services

API Based Data Protection

Forensic

Legalhold

Quarantine

Confirm

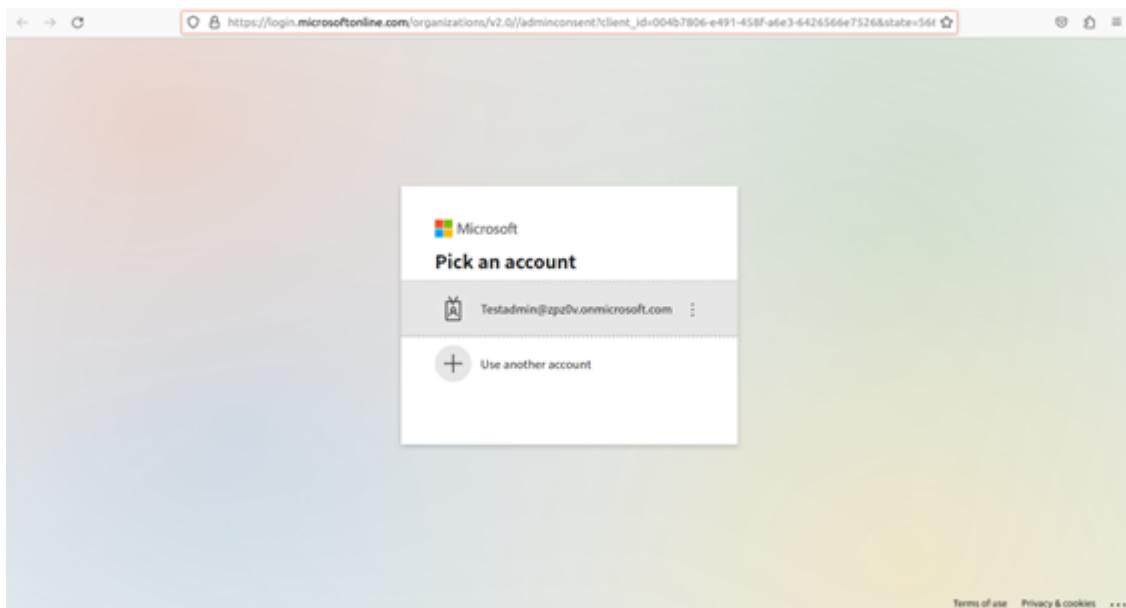
Instance Add requires configuring your Microsoft One Drive account. [View Instructions](#) for setting up Microsoft One Drive instance.

Yes, I completed the steps required to configure Microsoft One Drive account

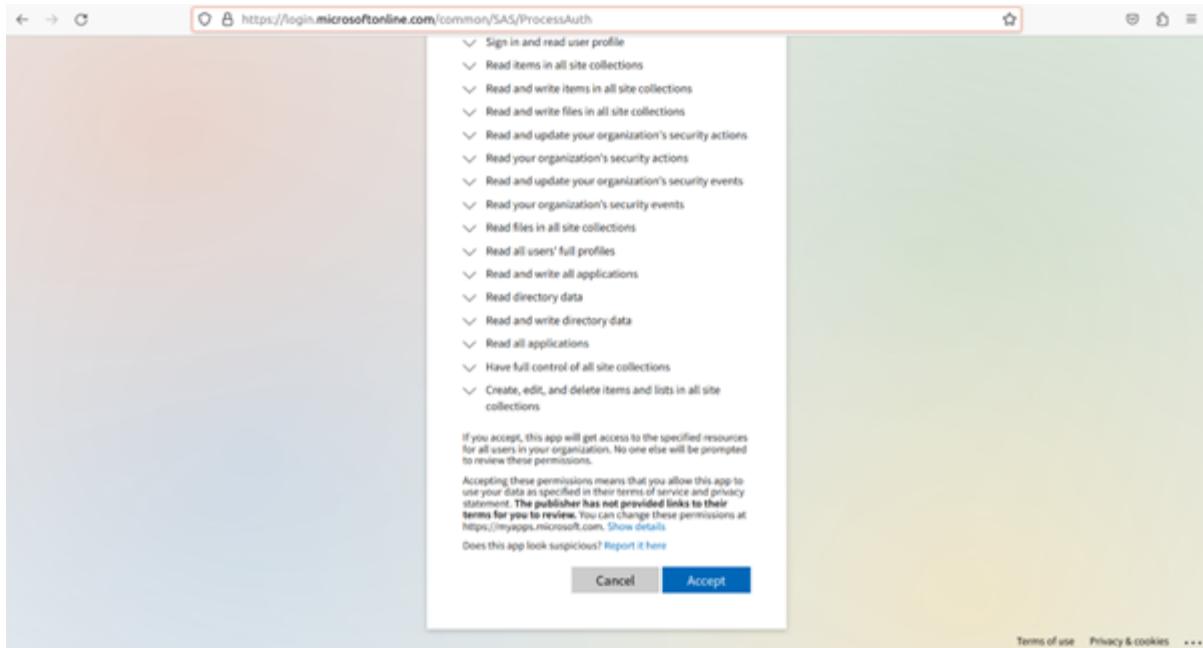
Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email (Required)	Enter an email address of the Microsoft OneDrive administrator account.
Enter List of Internal Domains	Enter domains configured for the organization.
Retro Scan	Click to scan and protect all the files that are present on Microsoft OneDrive at the time of connector creation.
Services	Select the services to use for the instance. <ul style="list-style-type: none"> ◦ API-Based Data Protection—Scan and protect

Field	Description
	<p>content.</p> <ul style="list-style-type: none"> ◦ 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

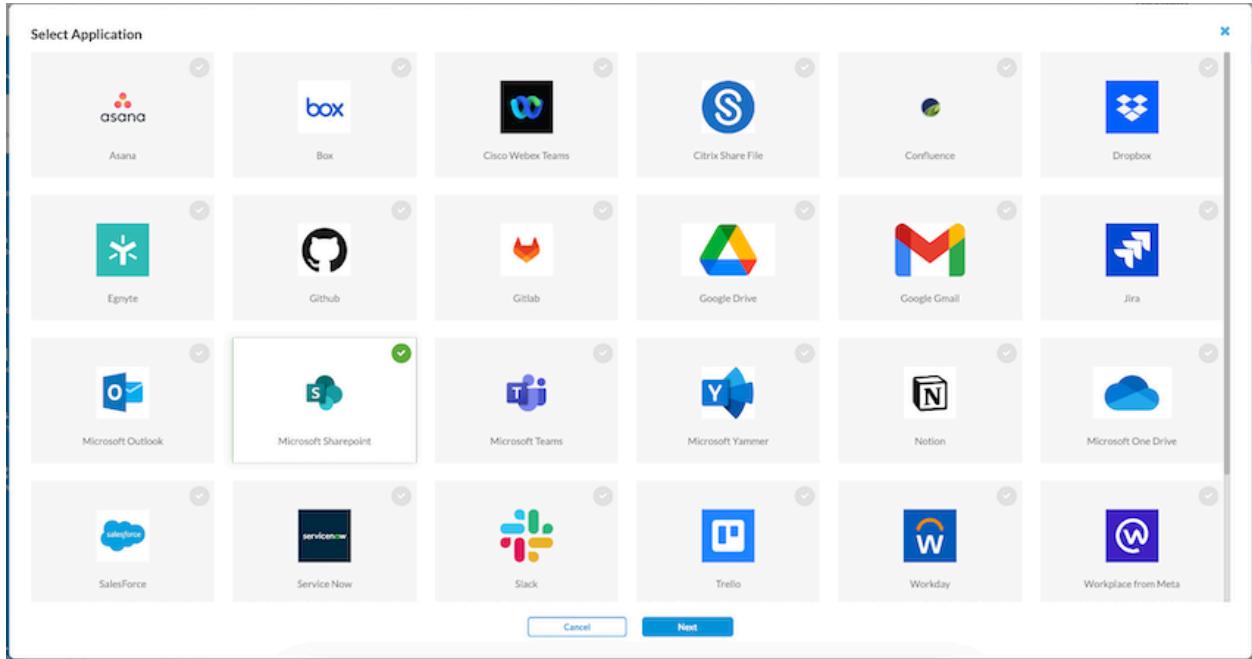
This section describes how to configure the Microsoft SharePoint application for API-based data protection.

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.

Add Instance - Microsoft Office 365 Sharepoint Sites

 Microsoft Office 365 Sharepoint Sites
[View Instructions](#) for setting up Microsoft Office 365 Sharepoint Sites instance.

Instance Name*	Admin Email*
<input type="text" value="Input Name"/>	<input type="text" value="Input Admin Email"/>
Enter List of Internal Domains*	
<input type="text" value="Press Enter to add"/>	
<input type="checkbox"/> Retro Scan	
Services	
<input type="checkbox"/> API Based Data Protection	
<input type="checkbox"/> Forensic	
<input type="checkbox"/> Legalhold	
<input type="checkbox"/> Quarantine	
Confirm	
Instance Add requires configuring your Microsoft Office 365 Sharepoint Sites account. View Instructions for setting up Microsoft Office 365 Sharepoint Sites instance.	
<input type="checkbox"/> Yes, I completed the steps required to configure Microsoft Office 365 Sharepoint Sites account	
<input type="button" value="Cancel"/>	<input type="button" value="Submit"/>

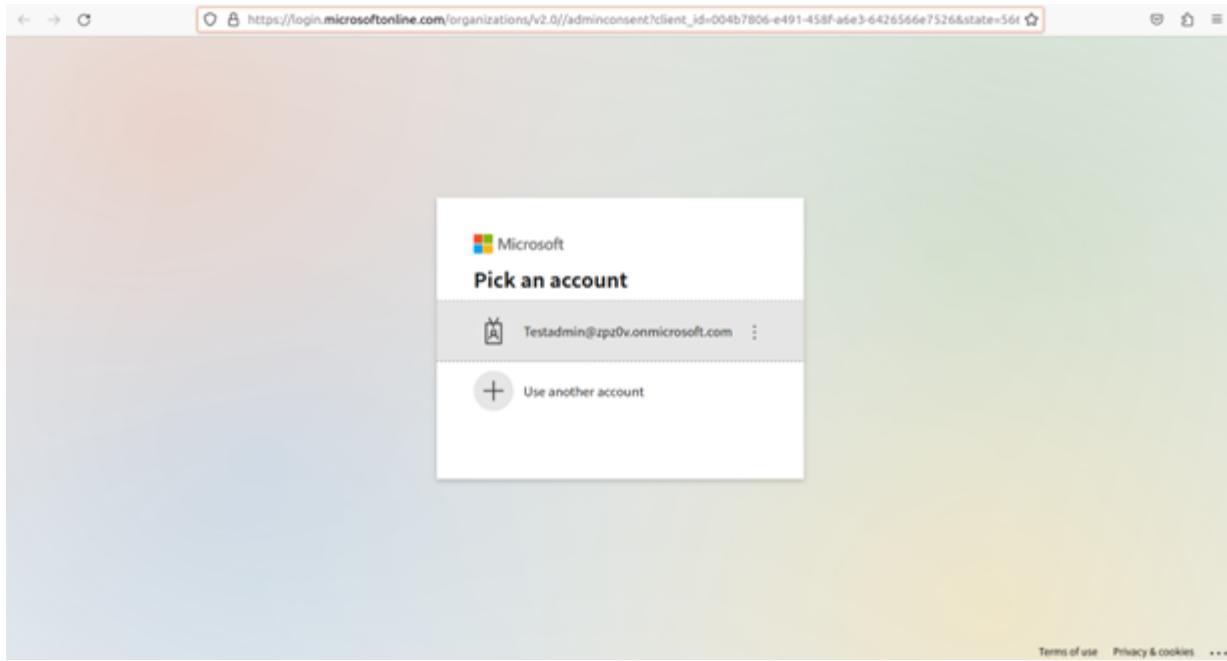
[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

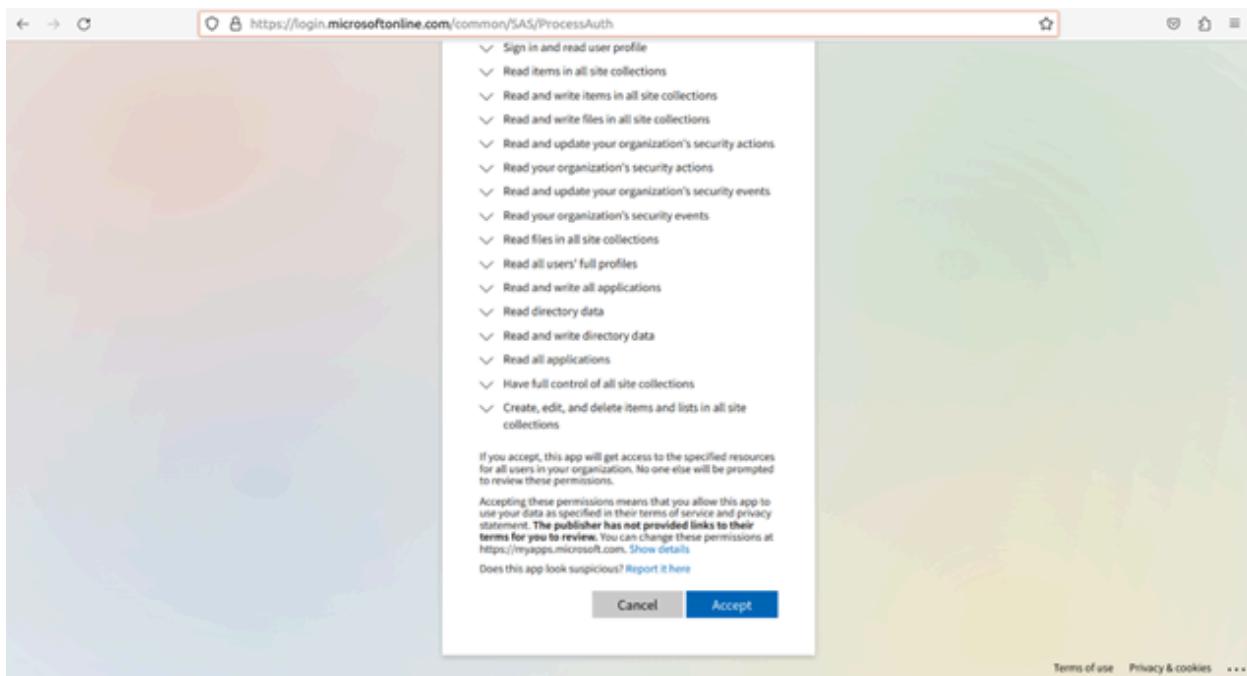
Copyright © 2024, Versa Networks, Inc.

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	<p>Select the services to use for the instance.</p> <ul style="list-style-type: none"> ◦ 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

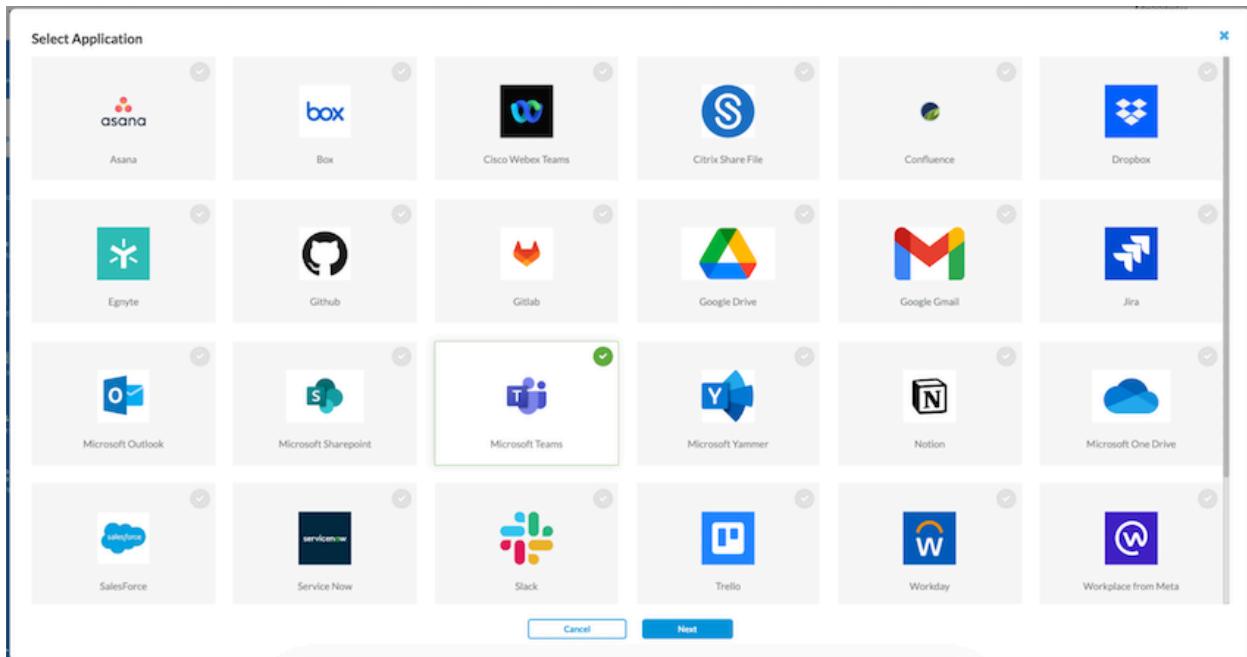
This section describes how to configure the Microsoft Teams application for API-based data protection.

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.

Add Instance - Microsoft Teams



Microsoft Teams
[View Instructions](#) for setting up Microsoft Teams instance.

Instance Name*

Admin Email*

Enter List of Internal Domains*

Retro Scan

Services

API Based Data Protection

Confirm
 Instance Add requires configuring your Microsoft Teams account. [View Instructions](#) for setting up Microsoft Teams instance.

Yes, I completed the steps required to configure Microsoft Teams account

Cancel **Submit**

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. <ul style="list-style-type: none"> ◦ API-Based Data Protection—Scan and protect content.
Confirm	Click to confirm that the steps required to configure the Microsoft Teams account are complete.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

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.”

The screenshot shows the 'My Apps' section of the Microsoft Yammer interface. On the left, there's a sidebar with 'My Apps' and two application entries: 'Versa_APIDP' and 'APIDP'. A green button labeled 'Register New App' is visible. The main area is titled 'Registered applications' and contains a table with two rows. The table has columns for Application, Created at, Modified at, Enabled, and Global. Both applications listed are enabled. The table data is as follows:

Application	Created at	Modified at	Enabled	Global
Versa_APIDP	October 16, 2023	October 16, 2023	✓	
APIDP	September 20, 2023	September 20, 2023	✓	

Below the table, a note says: "The applications listed below are owned by you. For a list of the applications that you have granted API access to, see your user's [profile settings](#)".

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

Register new App

X

All fields are required.

Application Name ?

Versa_API_DP

Organization ?

ABC

Support e-mail ?

test@abc.onmicrosoft.com

Website ?

https://www.abc.com/

Redirect URI ?

https://apidp.versanow.net/v1/msyammer/auth-call

By checking this box, you agree that you have read and agree to the [Viva Engage API Terms of Service](#).

Cancel

Continue

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

My Apps

Versa_API_DP

- Versa_API_DP ✓
 - Basic Info
 - App Directory
 - Open Graph
- Versa_APIDP
- APIDP

Register New App

Keys and tokens

Client ID ? XtrZCehDDxXK8JSUmwg

Client secret ? 9BVqHLjrIxoEWqYnsonyT7keO2QUka4WeJfrehew4

Expected redirect ? https://apidp.versanow.net/v1/msyammer/auth-callback

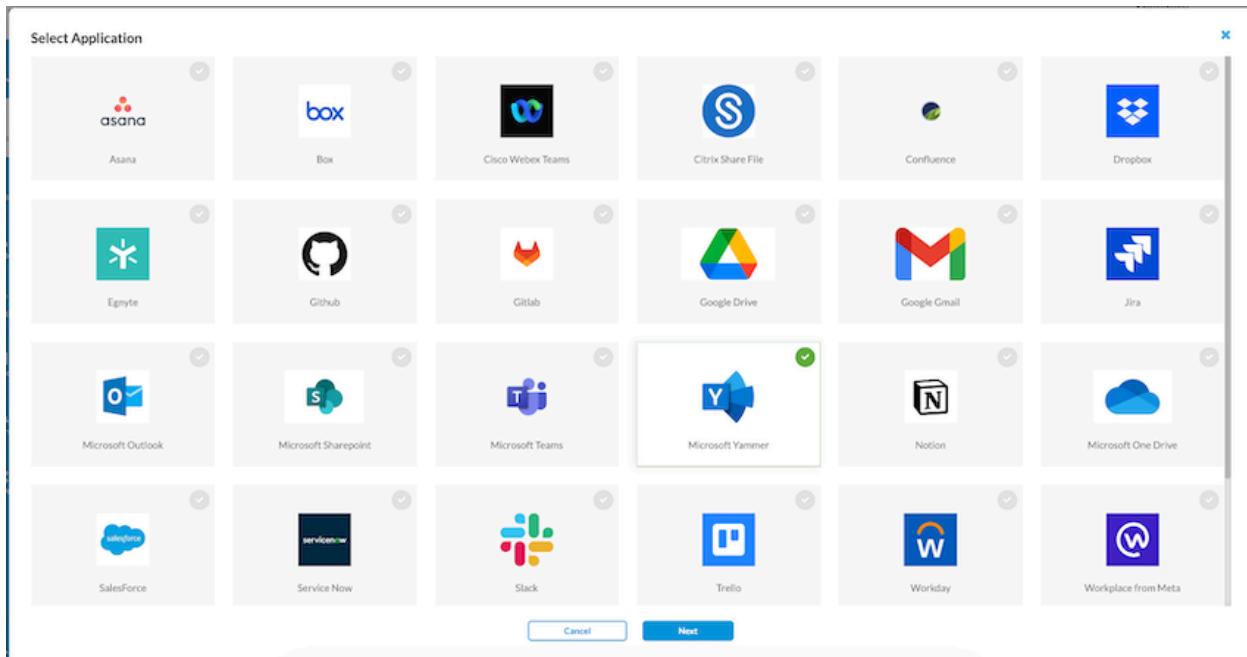
Generate a developer token for this application

Get help

- API documentation
- Site issues
- Partner with Yammer

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.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

Add Instance - Microsoft Yammer

 Microsoft Yammer
[View Instructions](#) for setting up Microsoft Yammer instance.

Instance Name*	Admin Email*
<input type="text" value="Input Name"/>	<input type="text" value="Input Admin Email"/>
Enter List of Internal Domains*	Interval (in Minutes)*
<input type="text" value="Press Enter to add"/>	<input type="text" value="15"/>
<input type="checkbox"/> Retro Scan	
Services	
<input type="checkbox"/> API Based Data Protection	
Confirm	
Instance Add requires configuring your Microsoft Yammer account. View Instructions for setting up Microsoft Yammer instance.	
<input type="checkbox"/> Yes, I completed the steps required to configure Microsoft Yammer account	
<input type="button" value="Cancel"/>	<input type="button" value="Submit"/>

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. <ul style="list-style-type: none"> ◦ 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.

- 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

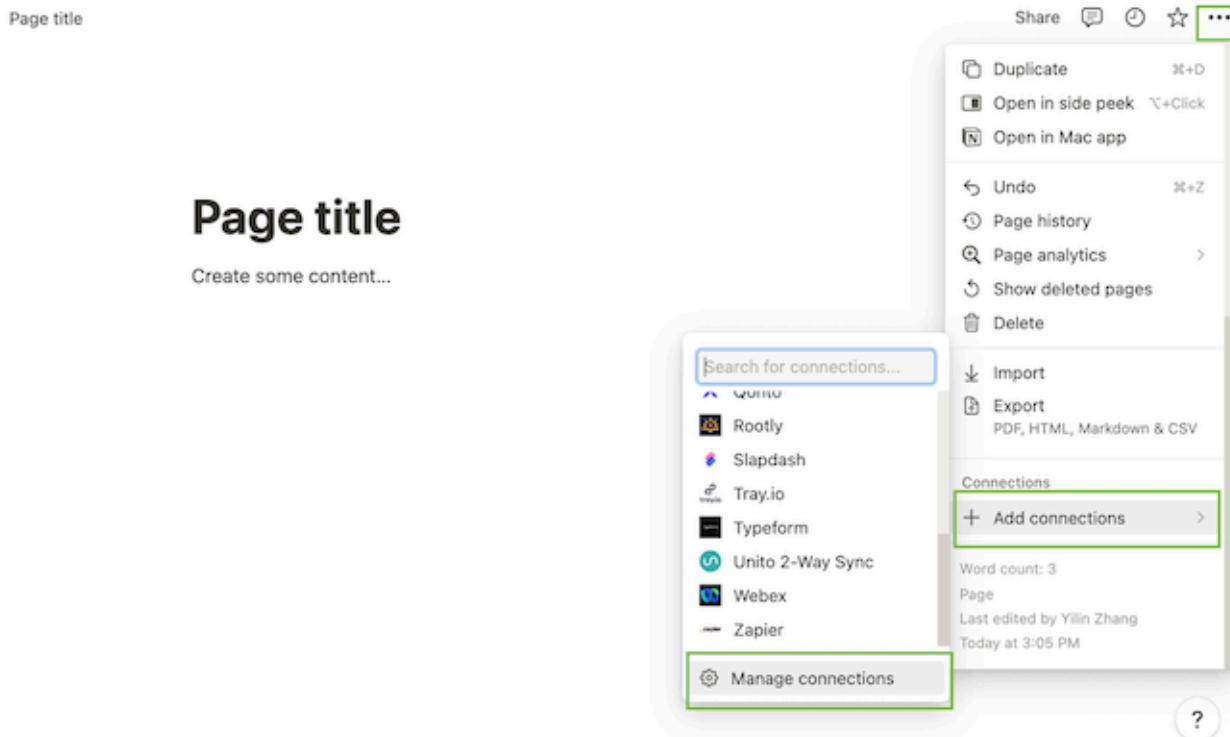
This section describes how to configure the Notion application for API-based data protection.

Configure Notion for API-Based Data Protection

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

To create a new integration:

- Select ellipses in the right corner -> Add connections -> Manage connections.



- Under My connections -> Develop or manage integrations.

The screenshot shows the Notion workspace settings sidebar on the left with 'My connections' highlighted. Below it, the main content area displays three integration cards: GitHub (Workspace), GitHub, and GitLab. Each card has a 'Connect' button. At the bottom, there's a 'See all' link and a 'Develop or manage integrations' option under 'Browse connections in Gallery'.

- Add new integration and put name for the integration.

The screenshot shows the 'My integrations' page with a large title 'My integrations'. It features a 'New integration' button, a 'View all' section with 'Internal' and 'Public' options, and a list of existing integrations. One integration, 'APIDP-Notion', is shown in detail, created by the user, and is a public integration. There's also a 'Create new integration' button.

[← My integrations](#)

Create a new integration

We'll walk you through how to set up a new integration

Basic Information

Basic Information

Type

Internal

Internal integrations are installed to a specific workspace. You can make this integration public later

Associated workspace *

Workspace

Select a workspace to install the integration to. Workspace owners will be able to manage the integration as well. You can upgrade the integration to use OAuth later

Name *

APIDP-Notion

Name to identify your integration to users

Logo

512px x 512px in PNG format is recommended

By submitting, you agree to Notion's
[Developer Terms](#).

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.

[← My integrations](#)

APIDP-Notion

Review and edit integration information.

A

Do you want to make this integration public?



Basic Information

A public integration is available to any Notion user.

Secrets

After submission, only the creator will be able to manage this integration. To transfer ownership of this integration to another user, please contact Notion support.

Capabilities

Distribution

If you've built a public integration, you may be eligible to become a technology partner and get Notion's support in promoting and distributing your integration. Learn more about the Notion Technology Partner Program [here](#).

Capabilities Distribution Organization Information OAuth Domain & URIs	<h2>Organization Information</h2> <p>Company name *</p> <input type="text"/> <p>The name of your company or organization. You may use your own name if this does not apply</p> <p>Website or homepage *</p> <input type="text"/> <p>Used to link to your integration's website or homepage in your integration page and authentication screens</p> <p>Tagline</p> <input type="text"/> <p>A short description of what the integration does</p> <p>Privacy policy *</p> <input type="text"/> <p>Used to link to your integration's privacy policy in your integration page and authentication screens</p> <p>Terms of use *</p> <input type="text"/> <p>Used to link to your integration's terms of use in your integration page and authentication screens</p> <p>Support email *</p> <input type="text"/> <p>Used to link to your integration's support email in your integration page and authentication screens</p>
--	--

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

Secrets

Capabilities

Distribution

Organization Information

OAuth Domain & URIs

OAuth Domain & URLs

Redirect URIs *

`https://apidp.versanow.net/v1/notion/auth-callback` 

In the Notion OAuth flow, users will be redirected to this path after they have authenticated with Notion. The path will be appended with the authorization code for access and must have a protocol. It can't contain URL fragments, relative paths or wildcards, and can't be a public IP address. It must also be included in the token request

Notion URL for optional template

Use this field if you'd like to offer a user a Notion page to duplicate into their workspace during OAuth. URL must be to a public Notion page

Save changes

6. Client-id and secret is under secrets.

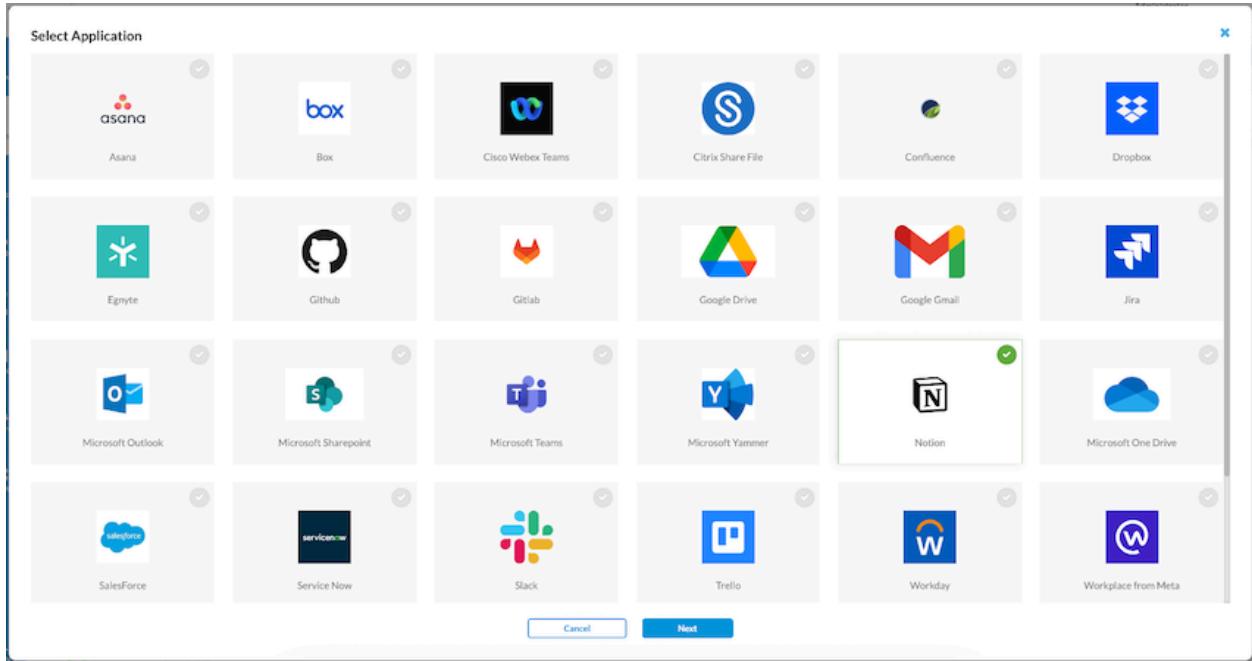
The screenshot shows a configuration page for a connector. On the left, there's a sidebar with options: Basic Information, Secrets (which is selected), Capabilities, and Distribution. The main area is titled "Secrets". It contains three fields: "OAuth client ID" with the value "bd4c18c3-f428-40ab-bfc7-680504954369" and a "Copy" button; "OAuth client secret" with a redacted value and a "Refresh" button; and "Authorization URL" with the value "https://api.notion.com/v1/oauth/authorize?c..." and a "Copy" button.

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.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

Add Instance - Notion

 Notion
[View Instructions](#) for setting up Notion instance.

Instance Name*

Admin Email*

Interval (in Minutes)*
 Retro Scan

Services
 API Based Data Protection

Confirm
Instance Add requires configuring your Notion account. [View Instructions](#) for setting up Notion instance.
 Yes, I completed the steps required to configure Notion account

[Cancel](#) [Submit](#)

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. <ul style="list-style-type: none"> ◦ API-Based Data Protection—Scan and protect content.
Confirm	Click to confirm that the steps required to configure the Notion account are complete.

- 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:

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

The screenshot shows the 'Remote Site Settings' page in the Salesforce setup. The left sidebar has 'Custom Code' and 'Security' collapsed, and 'Remote Site Settings' is expanded, highlighted with a green border. A search bar at the top left contains the text 'remote'. The main content area is titled 'All Remote Sites' and displays a table with one row: 'No records to display'. The table has columns for 'Remote Site Name', 'Namespace Prefix', 'Remote Site URL', 'Active' (with a 'New Remote Site' button), 'Created By', 'Created Date', 'Last Modified By', and 'Last Modified Date'. Navigation links for letters A through Z and 'Other' are at the top right.

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

This screenshot is identical to the one above, but the 'New Remote Site' button in the 'Active' column of the table header is highlighted with a green box.

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

Remote Site Edit

Enter the URL for the remote site. All s-controls, JavaScript OnClick commands in custom buttons, Apex, and AJAX proxy calls can access this Web address from salesforce.com.

Remote Site Edit

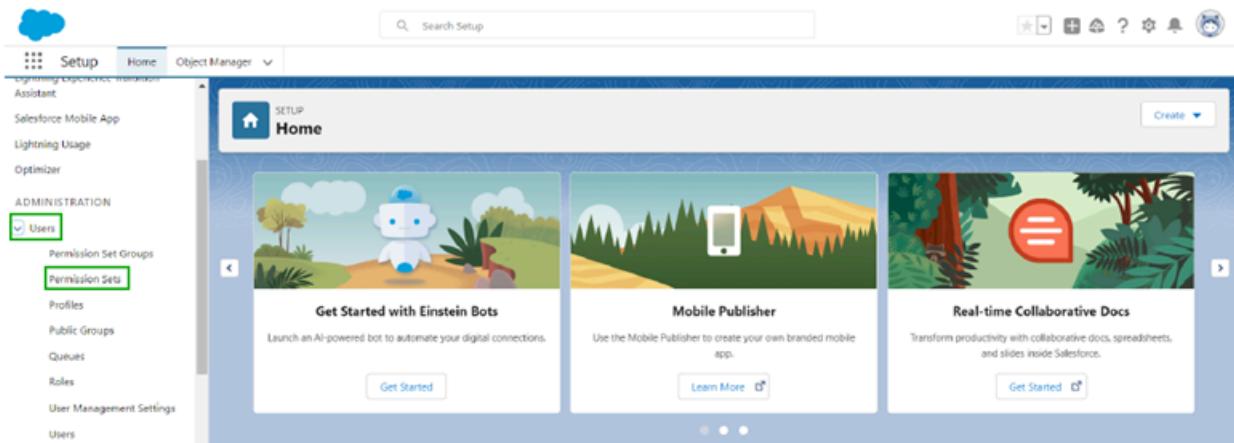
Remote Site Name	<input type="text" value="VersaAPIDP"/>	Save	Save & New	Cancel
Remote Site URL	<input type="text" value="https://apidp.versenow.net/v1/salesforce/webhook"/>			
Disable Protocol Security	<input type="checkbox"/>			
Description	<input type="text"/>			
Active	<input checked="" type="checkbox"/>			
Save Save & New Cancel				

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.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

Permission Sets		
On this page you can create, view, and manage permission sets.		
In addition, you can use the Salesforce mobile app to assign permission sets to a user. Download Salesforce from the App Store or Google Play iOS Android		
All Permission Sets Edit Delete Create New View		
New	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Other All	Help for this Page ?
<input type="checkbox"/> Action	Permission Set Label +	Description
<input type="checkbox"/> Close	Buyer	Allows access to the store. Lets users see products and categories...
<input type="checkbox"/> Close	Buyer Manager	Includes all buyer capabilities, and allows access to manage carts...
<input type="checkbox"/> Close	CRM User	Denotes that the user is a Sales Cloud or Service Cloud user.
<input type="checkbox"/> Close	Commerce Admin	Allow access to commerce admin features.
<input type="checkbox"/> Close	Contact Center Admin	Manage Service Cloud Voice contact centers that use Amazon Con...
<input type="checkbox"/> Close	Contact Center Agent	Access agent features in Service Cloud Voice contact centers that us...
<input type="checkbox"/> Close	Contact Center Supervisor	Access supervisor features in Service Cloud Voice contact centers th...
<input type="checkbox"/> Del Clone	Excellence Profile Manager	Salesforce
<input type="checkbox"/> Close	Facility Manager	Facility Manager
<input type="checkbox"/> Close	FieldServiceMobileStandardPermSet	Field Service Mobile
<input type="checkbox"/> Close	Merchandiser	Commerce Merchandiser User Permission Set License Seats
<input type="checkbox"/> Close	Order Management Agent	Lightning Order Management User
<input type="checkbox"/> Close	Order Management Operations Manager	Lightning Order Management User
1-25 of 25 Selected		
Page 1 of 1		

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

Permission Set Create	
Save Cancel	Help for this Page ?
Enter permission set information	
Label	<input type="text" value="Listing all files"/>
API Name	<input type="text" value="Listing_all_files"/>
Description	This permission set allows users with "View All Data" access to query files without being limited by any restrictions.
Session Activation Required	<input type="checkbox"/>
Select the type of users who will use this permission set	
Who will use this permission set?	
<p>-Choose "None" if you plan to assign this permission set to multiple users with different user and permission set licenses.</p> <p>-Choose a specific user license if you want users with only one license type to use this permission set.</p> <p>-Choose a specific permission set license if you want this permission set license auto-assigned with the permission set.</p>	
Not sure what a permission set license is? Learn more here.	
<input type="button" value="License"/> Salesforce	
Save	Cancel

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.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

Permission Set
Listing all files

Description: This permission set allows users with "View All Data" access to query files without being limited by any restrictions.

API Name: Listing_all_files

Namespace Prefix:

Created By: Test User

Created On: 5/3/2023, 8:06 AM

Session Activation Required:

Last Modified By: Test User

Last Modified On: 5/3/2023, 8:06 AM

Apps

- Assigned Apps**: Settings that specify which apps are visible in the app menu.
- Assigned Connected Apps**: Settings that specify which connected apps are visible in the app menu.
- Object Settings**: Permissions to access objects and fields, and settings such as tab availability.
- App Permissions**: **Permissions to perform app-specific actions, such as "Manage Call Centers"** (highlighted with a green box).
- Apex Class Access**: Permissions to execute Apex classes.
- Visualforce Page Access**: Permissions to execute Visualforce pages.
- External Data Source Access**: Permissions to authenticate against external data sources.
- Flow Access**: Permissions to execute Flows.

Settings that apply to Salesforce apps, such as Sales, and custom apps built on the Lightning Platform. [Learn More](#)

- Click Edit next to App Permissions label.

Permission Set
Listing all files

Permission Set Overview > App Permissions

App Permissions

Call Center

Permission Name	Enabled	Description
Access Conversation Entries	<input type="checkbox"/>	Grants users access to Conversation Entries.
Edit Case Comments	<input type="checkbox"/>	Edit their own case comments but not other user's comments.
Import Solutions	<input type="checkbox"/>	Import solutions for the organization.
Manage Business Hours Holidays	<input type="checkbox"/>	Create, edit, and delete business holidays.
Manage Call Centers	<input type="checkbox"/>	Create, import, edit, and delete a call center configuration.
Manage Cases	<input type="checkbox"/>	Administer case settings, including Email-to-Case and mass transfer of cases.
Manage Categories	<input type="checkbox"/>	Define and modify solution categories settings.
Manage Entitlements	<input type="checkbox"/>	Enable, create, and update entitlement management items.
Manage Macros Users Can't Undo	<input type="checkbox"/>	Create, update, and run macros that include irreversible instructions.
Manage Published Solutions	<input type="checkbox"/>	Create, edit, and delete publicly accessible solutions.
Run Macros on Multiple Records	<input type="checkbox"/>	Run macros on multiple records at the same time.
Transfer Cases	<input type="checkbox"/>	Change a case's owner.

Content

- Select Query All Files checkbox in the Content section.

The screenshot shows the 'Content' section of a Permission Set configuration. It includes a table with columns for 'Permission Name', 'Enabled', and 'Description'. One row, 'Query All Files', is highlighted with a green border.

Permission Name	Enabled	Description
Manage Content Permissions	<input type="checkbox"/>	Create, edit, and delete library permissions in Salesforce CRM Content.
Manage Content Properties	<input type="checkbox"/>	Create, edit, and delete custom fields in Salesforce CRM Content.
Manage record types and layouts for Files	<input type="checkbox"/>	Create, edit, and delete content types in Salesforce CRM Content.
Manage Salesforce CRM Content	<input type="checkbox"/>	Create, edit, and delete libraries and library memberships.
Query All Files	<input checked="" type="checkbox"/>	Allows View All Data users to SOQL query all files in the org.

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

The screenshot shows the 'App Permissions' section of a Permission Set configuration. The 'Call Center' section is expanded, displaying a list of permissions with their descriptions.

Permission Name	Enabled	Description
Access Conversation Entities	<input type="checkbox"/>	Grants users access to Conversation Entities
Edit Case Comments	<input type="checkbox"/>	Edit their own case comments but not other user's comments.
Import Solutions	<input type="checkbox"/>	Import solutions for the organization.
Manage Business Hours Holidays	<input type="checkbox"/>	Create, edit, and delete business holidays.
Manage Call Centers	<input type="checkbox"/>	Create, import, edit, and delete a call center configuration.
Manage Cases	<input type="checkbox"/>	Administer case settings, including Email-to-Case and mass transfer of cases.
Manage Categories	<input type="checkbox"/>	Define and modify solution categories settings.
Manage Entitlements	<input type="checkbox"/>	Enable, create, and update entitlement management items.
Manage Macros Users Can't Undo	<input type="checkbox"/>	Create, update, and run macros that include irreversible instructions.
Manage Published Solutions	<input type="checkbox"/>	Create, edit, and delete publicly accessible solutions.
Run Macros on Multiple Records	<input type="checkbox"/>	Run macros on multiple records at the same time.
Transfer Cases	<input type="checkbox"/>	Change a case's owner.

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=04tDn00000AtV5&isdtp=p1>
 - To install the package in the Sandbox environment, click <https://test.salesforce.com/packaging/installPackage.apexp?p0=04tDn00000AtV5&isdtp=p1>
2. Log in as an administrator.
3. Install users based on the user's requirements.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

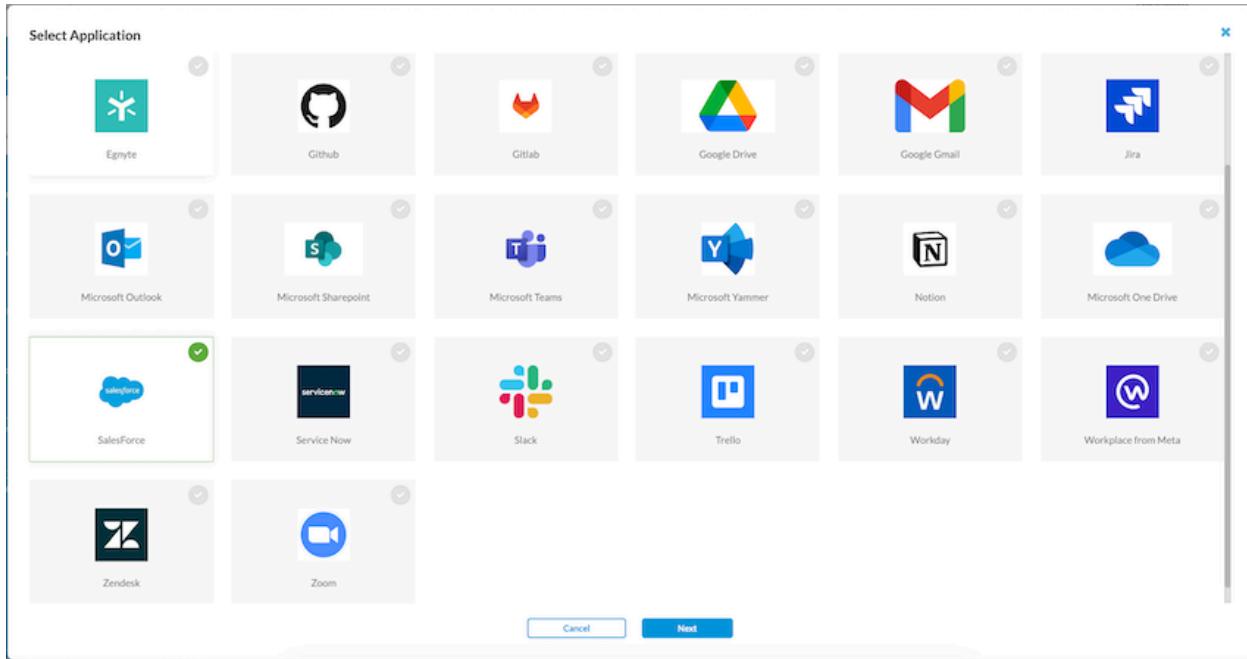
Updated: Wed, 23 Oct 2024 08:39:56 GMT

Copyright © 2024, Versa Networks, Inc.

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.

Add Instance - SalesForce

 **SalesForce**
View Instructions for setting up SalesForce instance.

Instance Name*

Admin Email*

Retro Scan

Services

API Based Data Protection

Confirm

Instance Add requires configuring your SalesForce account. [View Instructions](#) for setting up SalesForce instance.

Yes, I completed the steps required to configure SalesForce account

[Cancel](#) [Submit](#)

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. <ul style="list-style-type: none"> ◦ 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

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

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

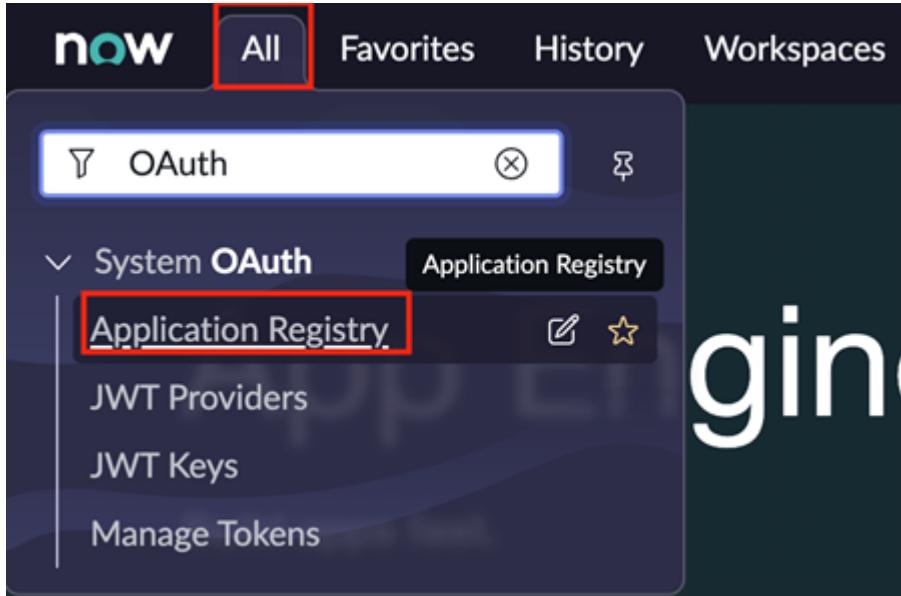
ServiceNow API-Based Data Protection

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.

What kind of OAuth application?

- [Create an OAuth API endpoint for external clients](#)
- [Create an OAuth JWT API endpoint for external clients](#)
- [Connect to a third party OAuth Provider](#)
- [Configure an OIDC provider to verify ID tokens.](#)
- [Connect to an OAuth Provider \(simplified\)](#)

5. Enter information for the following fields.

The screenshot shows the 'Create New Application' form in ServiceNow. The fields filled in are:

- Name: Choose Any Name Here
- Client ID: d079e3063e2221102faed9b078ef4b26
- Client Secret: Either Enter a Custom Secret or Leave Blank
Leave Client Secret blank to automatically generate a string
- Redirect URL: (empty)
- Logo URL: (empty)
- Comments: (empty)
- Application: Global
- Accessible from: All application scopes
- Active: checked
- Refresh Token Lifespan: 8,640,000
- Access Token Lifespan: 1,800

At the bottom left is a 'Submit' button.

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.

Application Registries					Actions on selected rows...	New
All > Name = any name						
Name	Active	Type	Client ID	Comments		
=any name	Search	Search	Search	Search		
any name	true	OAuth Client	d079e3063e2221102faed9b078ef4b26	Search		

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.

The screenshot shows the configuration of an API-based connector. Key fields include:

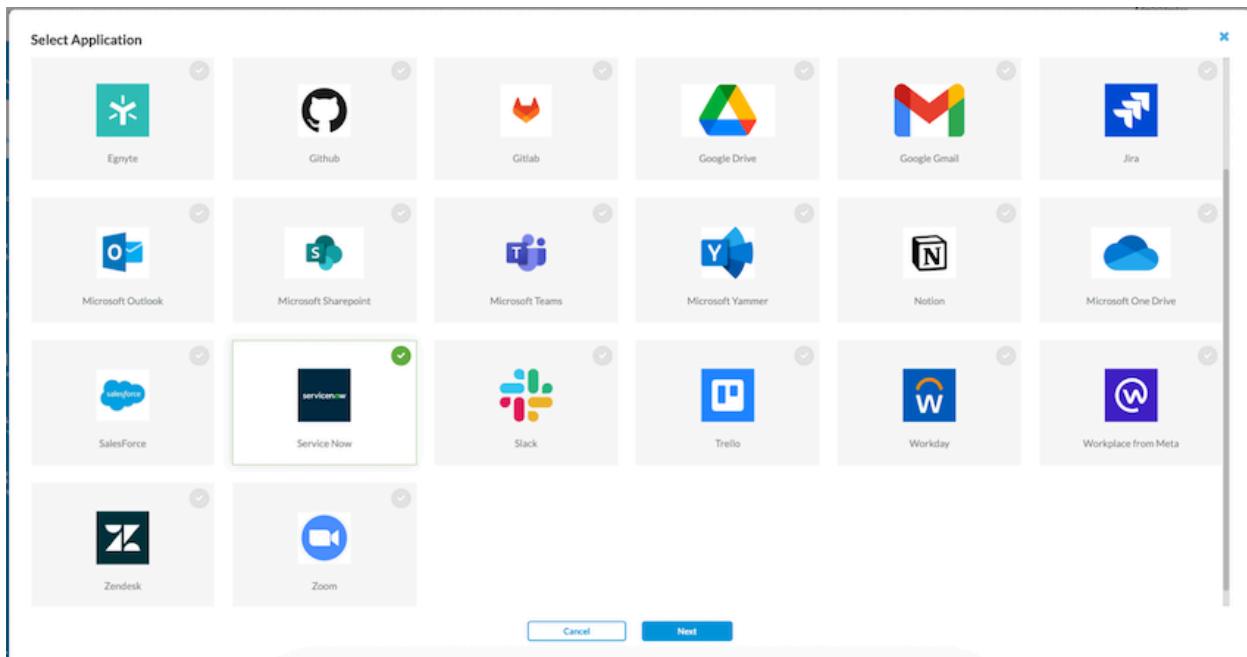
- Name:** any name
- Client ID:** d079e3063e2221102faed9b078ef4b26
- Client Secret:** A masked value (2Abo...) with a lock icon.
- Redirect URL:** A field with a lock icon.
- Logo URL:** A field with a lock icon.
- Comments:** An empty text area.

Configuration options on the right:

- Application:** Global
- Accessible from:** All application scopes
- Active:** Checked
- Refresh Token Lifespan:** 8,640,000
- Access Token Lifespan:** 1,800

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.

Add Instance - Service Now

 Service Now
[View Instructions](#) for setting up Service Now instance.

Instance Name*

Admin Email*

Client ID*

Client Secret*

Domain Name*

Retro Scan

Services API Based Data Protection

Confirm

Instance Add requires configuring your Service Now account. [View Instructions](#) for setting up Service Now instance.

Yes, I completed the steps required to configure Service Now account

[Cancel](#) [Submit](#)

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, <i>companyname.servicenow.com</i>
Retro Scan	Click to scan and protect all the files and other objects that are present on ServiceNow at the time of connector creation.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

Field	Description
Services	<p>Select the services to use for the instance.</p> <ul style="list-style-type: none"> ◦ API-Based Data Protection—Scan and protect content.
Confirm	<p>Click to confirm that the steps required to configure the ServiceNow account are complete.</p>

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

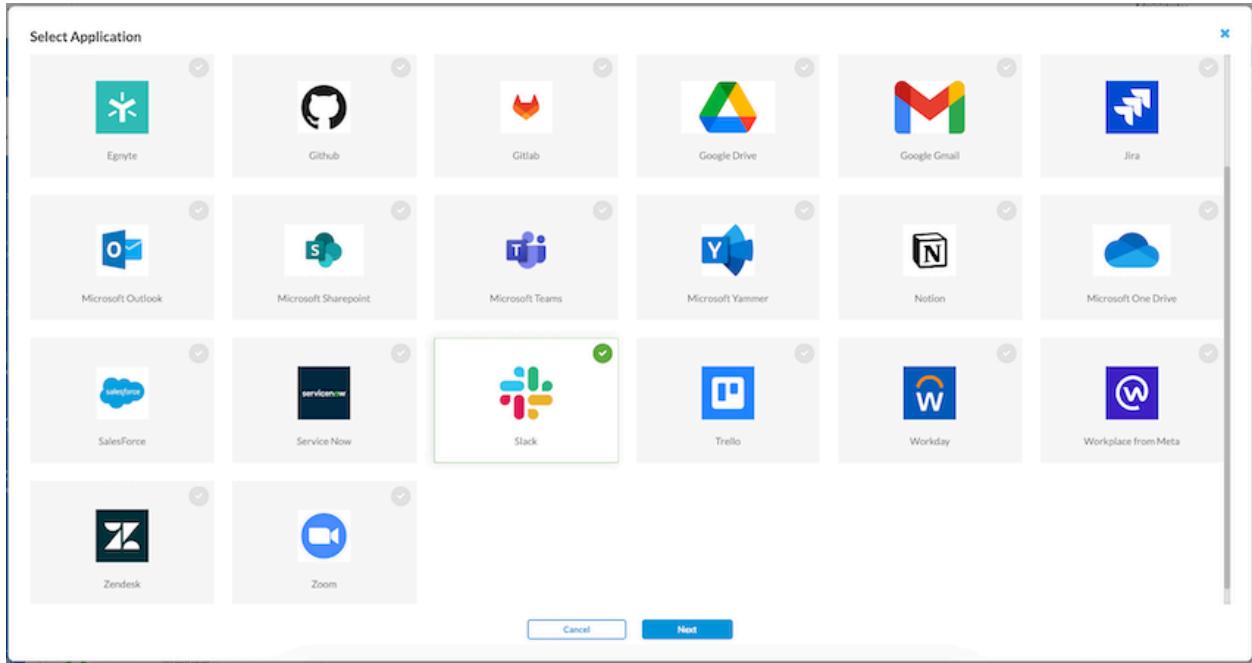
This section describes how to configure the Slack application for API-based data protection.

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.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

Add Instance - Slack



Slack
[View Instructions](#) for setting up Slack instance.

Instance Name*

Admin Email*

Enter List of Internal Domains*

Retro Scan

Services

API Based Data Protection

Confirm

Instance Add requires configuring your Slack account. [View Instructions](#) for setting up Slack instance.

Yes, I completed the steps required to configure Slack account

[Cancel](#) [Submit](#)

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	<p>Select the services to use for the instance.</p> <ul style="list-style-type: none"> ◦ API-Based Data Protection—Scan and protect content.
Confirm	<p>Click to confirm that the steps required to configure the Slack account are complete.</p>

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.

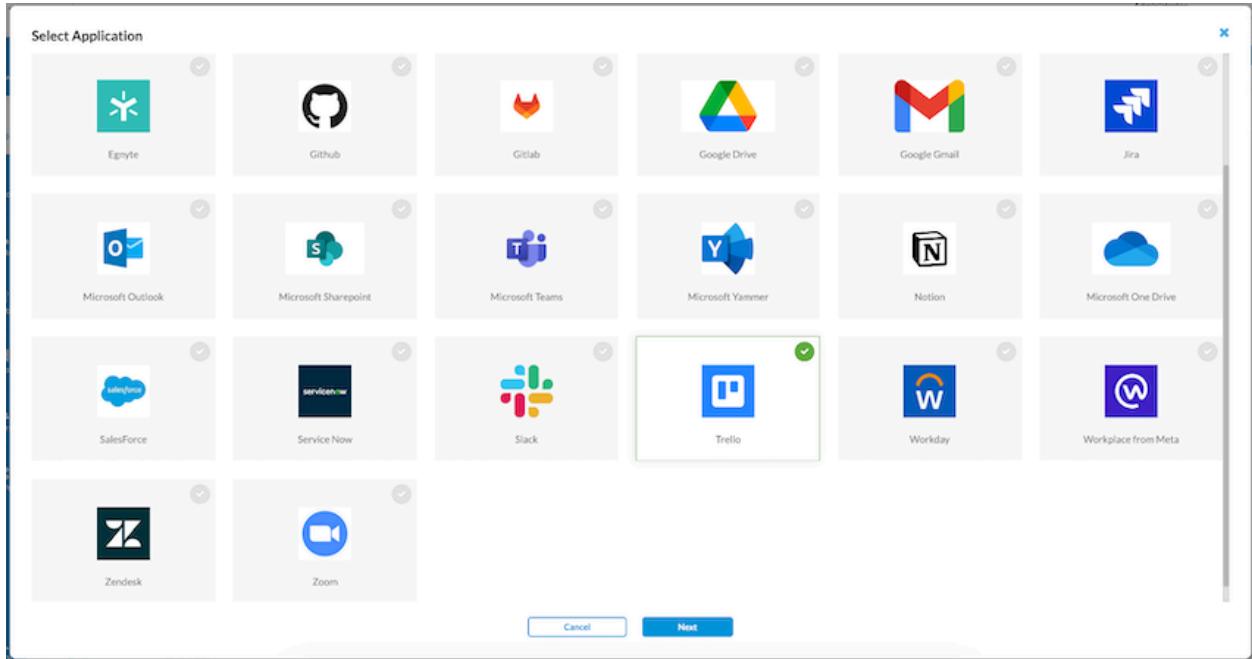
Configure Trello for API-Based Data Protection

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.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

Add Instance - Trello

 Trello
[View Instructions](#) for setting up Trello instance.

Instance Name*

Admin Email*

Retro Scan

Services

API Based Data Protection

Confirm

Instance Add requires configuring your Trello account. [View Instructions](#) for setting up Trello instance.

Yes, I completed the steps required to configure Trello account

[Cancel](#) [Submit](#)

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. <ul style="list-style-type: none"> ◦ 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.

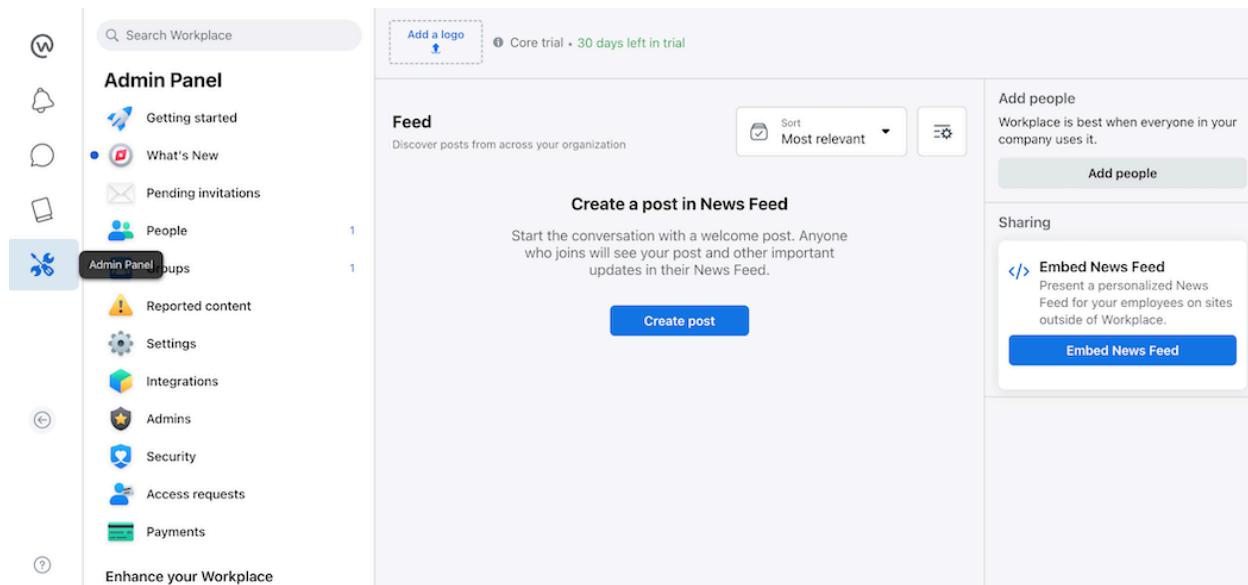
Workplace from Meta API-Based Data Protection

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.

The screenshot shows the Workplace Admin Panel. On the left, there's a sidebar with various icons and links like 'Getting started', 'What's New', 'Pending invitations', 'People', 'Groups', 'Reported content', 'Settings', 'Integrations' (which is selected and highlighted with a red box), 'Admins', 'Security', 'Access requests', 'Payments', and 'Enhance your Workplace'. Below these is a green 'Add people' button. The main content area is titled 'Integrations' with the sub-section 'All integrations'. It shows 'Added to Workplace' (Microsoft Teams Live) and 'Custom integrations' (saas-app, Enabled). There's also a 'Create custom integration' button. Under 'Integrations you can add', there are cards for Microsoft Teams, OneDrive, Microsoft SharePoint, and Salesforce.

- 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.

The screenshot shows the 'Integration details' page for a custom integration named 'saas-app'. The left sidebar has tabs for 'Details' (selected and highlighted with a red box), 'NLP settings', 'Permissions', 'Webhooks', 'Security', and 'Link preview'. The main content area has sections for 'Integration details' (with fields for 'Name, logo & description', 'App ID & App Secret', and 'Access token', all highlighted with red boxes), 'Visibility' (with 'Enabled' and 'Discoverable' switches both set to blue), and a 'Test API Request' button at the bottom.

Configure Workplace Custom Integration Webhooks

To configure Workplace custom integration webhooks:

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

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

Integration details

saas-app

Webhooks

Configure webhooks

Some webhooks aren't necessary depending on the permission you've selected

Resource	Description	Edit
Page	Event and messaging activity about custom integrations on Workplace	
Groups	Membership, comment, and post activity in Workplace groups	
User	Status, timeline and commenting activity for people in your Workplace	
Security	Activity relating to admin behavior and security on Workplace	
Link	Metadata about shareable links and previews	
Community	Activity relating to people sets, surveys and performing exports in this Workplace community	
Knowledge Library	Activity relating to Knowledge Library in this Workplace community	

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

Configure webhooks

Some webhooks aren't necessary depending on the permission you've selected

Page

Event and messaging activity about custom integrations on Workplace



Callback URL

Verify token

mention

Triggered when a custom integration page (bot) is mentioned in a group

messages

Triggered when a custom integration page (bot) is messaged in Workplace Chat

message_reads

Triggered when a message from a custom integration page (bot) is read by the recipient

message_deliveries

Triggered when a message sent by a custom integration page (bot) is delivered

messaging_postbacks

Triggered when a postback button is pressed in Workplace Chat

messaging_referrals

Triggered when the user already has a thread with the bot and user comes to the thread from w.m.me link with a referral parameter

Cancel

Save

Groups

Membership, comment, and post activity in Workplace groups



User

Status, timeline and commenting activity for people in your Workplace



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

Configure webhooks

Some webhooks aren't necessary depending on the permission you've selected

Page

Event and messaging activity about custom integrations on Workplace



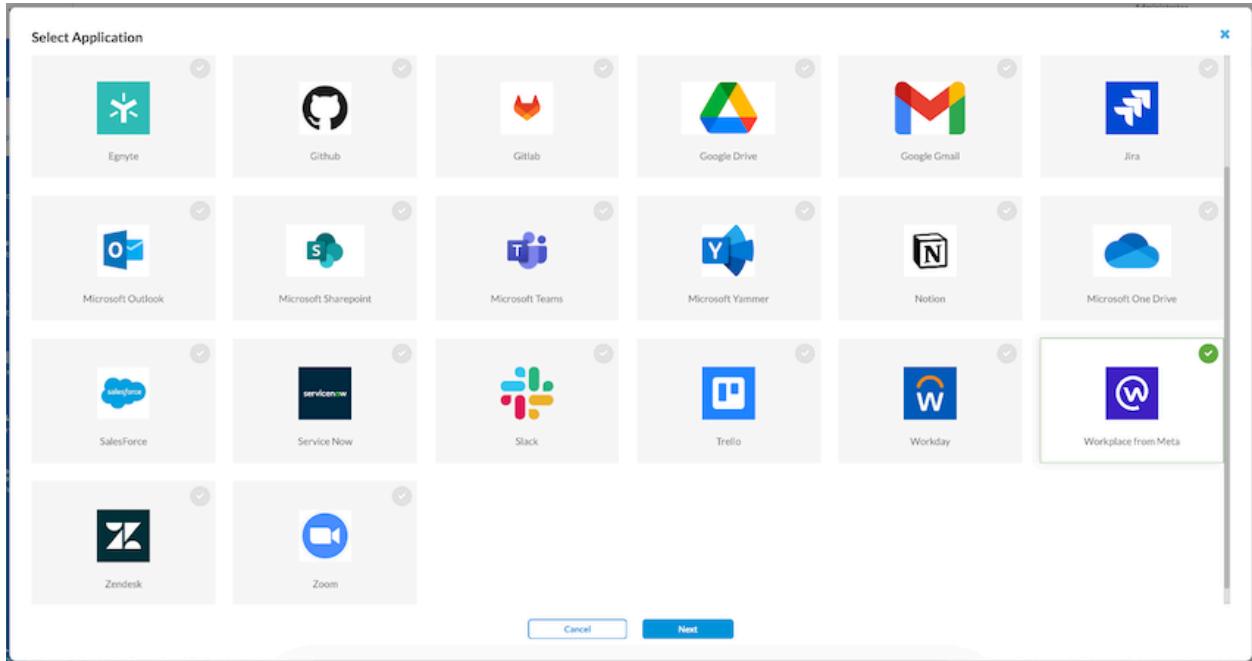
Callback URL <cluster-url>	Verify token <access-token>
<input checked="" type="checkbox"/> mention Triggered when a custom integration page (bot) is mentioned in a group	<input type="checkbox"/> message_deliveries Triggered when a message sent by a custom integration page (bot) is delivered
<input checked="" type="checkbox"/> messages Triggered when a custom integration page (bot) is messaged in Workplace Chat	<input type="checkbox"/> messaging_postbacks Triggered when a postback button is pressed in Workplace Chat
<input type="checkbox"/> message_reads Triggered when a message from a custom integration page (bot) is read by the recipient	<input type="checkbox"/> messaging_referrals Triggered when the user already has a thread with the bot and user comes to the thread from w.m.me link with a referral parameter

Cancel **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.

The screenshot shows the "Add Instance - Workplace from Meta" configuration window. At the top left is the Workplace from Meta logo (a white 'W' inside a blue square). To its right, the text reads "Workplace from Meta" and "View Instructions for setting up Workplace from Meta instance." Below this, there are input fields for "Instance Name*" (with placeholder "Input Name") and "Admin Email*" (with placeholder "Input Admin Email"). There is also a field for "Domain Name*" (placeholder "Input Domain") and a checkbox for "Retro Scan". Under the "Services" section, there is a checkbox for "API Based Data Protection". In the "Confirm" section, it says "Instance Add requires configuring your Workplace from Meta account." followed by a link "View Instructions" and a checkbox for "Yes, I completed the steps required to configure Workplace from Meta account". At the bottom are "Cancel" and "Submit" buttons.

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. <ul style="list-style-type: none"> ◦ 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.

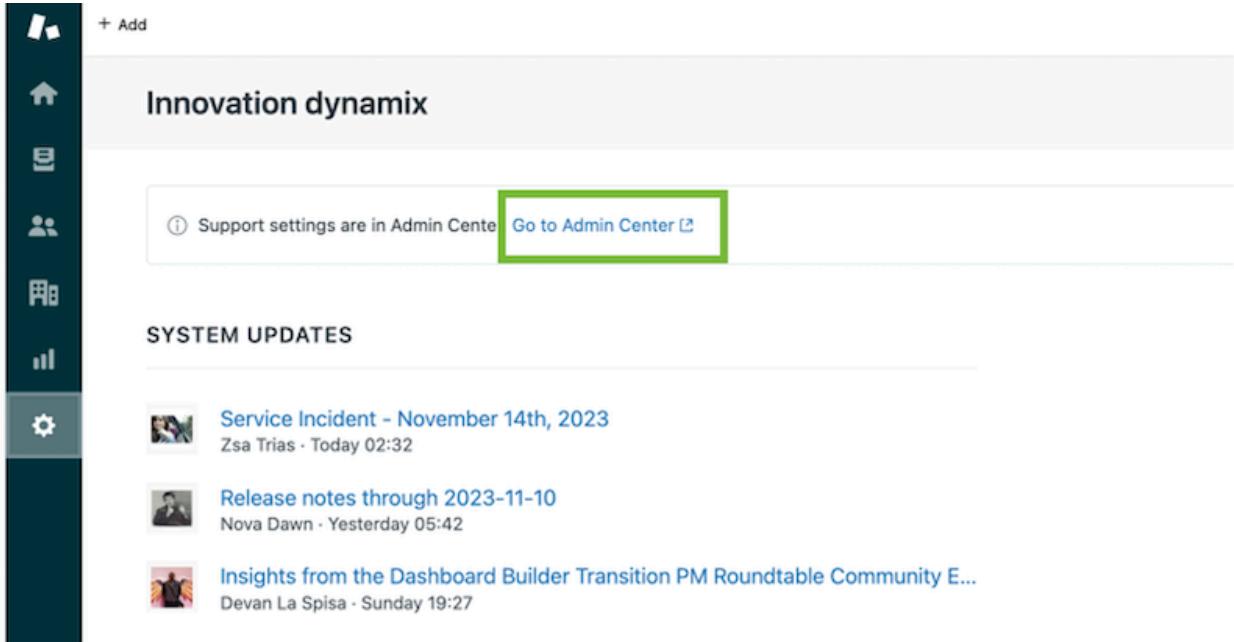
Zendesk API-Based Data Protection

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.



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

APIDP-Zendesk Created about 2 hours ago

Client name
Your client name shown to users when asked to grant access to your application or when viewing the list of apps that have been granted access. **APIIDP-Zendesk**

Description
A short description of your client for users when they're considering granting access to your application.

Company
This name is displayed when users are asked to grant access to your application. The name helps users understand to whom they're granting access.

Logo
Choose an image (JPG or PNG) to display when users are asked to grant access to your application.

Unique identifier
This is the name of your client for use in code. Example: `my_awesome_app`. This identifier is not shown to Zendesk users. You can change the initial suggestion. Identifiers with a `zdp-` prefix are reserved for global OAuth clients. **apidp-zendesk**

Redirect URLs
Specify the URL or URLs that Zendesk should use to redirect users after they decide whether or not to authorize your application to access Zendesk. The URLs must be absolute and not relative, https (unless localhost or 127.0.0.1), and newline-separated. **https://apidp.versanow.net/v1/zendesk/auth-callback**

Secret
This secret token is used by apps redirecting to your client. Please note that the secret is displayed in its entirety only once, so it's important you save it in a safe place. **73621cb8256bed9027719d8f8cbfb7fa0f5f17eeb32af5797c0bd006d4eee780**

Copy

Close **Save**

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

The screenshot shows the Zendesk Admin Center interface. On the left, there's a sidebar with various sections like Apps and integrations, APIs, and Webhooks. The 'Webhooks' section is highlighted. The main area is a configuration form for a new webhook. It has fields for 'Unique identifier' (set to 'apidp-zendesk'), 'Redirect URLs' (set to 'https://apidp.versanow.net/v1/zendesk/webhook'), and a 'Secret' field containing a long token. A note below the secret field says 'Make sure to copy and store this token. We won't show it again after you click Save or leave this page.' At the bottom right are 'Close' and 'Save' buttons.

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.

The screenshot shows the Zendesk Admin Center interface. The left sidebar is expanded to show 'Webhooks' under 'APIs'. The main area displays a table of existing webhooks. One webhook is listed: 'APIDP-Zendesk-webhook' with the endpoint 'https://apidp.versanow.net/v1/zendesk/webhook' and the status 'Active'. A 'Create webhook' button is located in the top right corner of the main area.

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

Create webhook

Select your connection method and add details to create your webhook.

1 Select a way to connect



Zendesk events

Subscribe to one or more events using a single webhook.



Trigger or automation

Connect the webhook using a business rule.

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)

2 Add details

Name* (Required)
APIDP-Zendesk-webhook 19

Description

Endpoint URL*
The endpoint you want to pass data to. [Learn about endpoint URL](#)
<https://apidp.versanow.net/v1/zendesk/webhook>

Request method*
POST

Request format*
JSON

Authentication*
 None
 API key
 Basic authentication
 Bearer token

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

The screenshot shows the Zendesk Admin Center interface. The left sidebar has a navigation tree with 'Home', 'Recently viewed', and 'Objects and rules' expanded. Under 'Objects and rules', 'Business rules' is selected, and 'Triggers' is the active sub-page. The main content area is titled 'Triggers' and contains a brief description: 'Set up event-based rules that run every time a ticket is created or updated. Popular triggers include notifying customers when a new comment is added to their ticket or an out-of-office reply. [Learn about triggers](#)'. Below this is a 'Filter' section with dropdowns for 'Name' and 'Status' (set to 'Active'). A search bar is also present. The table below shows 8 triggers, with the first one, 'Notifications', being the selected row. The table columns are 'Name', 'Description', and 'Triggered (7d)'. The 'Notifications' row has a delete icon in the last column.

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

Conditions

Conditions that must be met for the trigger to run

Meet ALL of the following conditions

Add condition

Meet ANY of the following conditions

Ticket

Is

Created

Comment

Is

Present (publi...)

Add condition

11. For Actions, choose the webhook you created.

The screenshot shows the 'Actions' configuration page. On the left, there's a sidebar with categories like 'Objects and rules', 'Business rules' (which is selected), and 'Apps and integrations'. Under 'Business rules', 'Triggers' is also selected. The main area shows an 'Actions' section with a dropdown menu set to 'Notify by > Active webhook'. A modal window is open, showing a list of available webhooks. One item, 'APIDP-Zendesk-webhook' with the URL 'https://apidp.versanow.net/v1/zendesk/webhook', is highlighted with a green box. Below the modal, the JSON body of the webhook is displayed:

```
1 {
  "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}}"
}
```

At the bottom right of the main actions area are 'Cancel' and 'Save' buttons.

12. Customize the JSON body.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

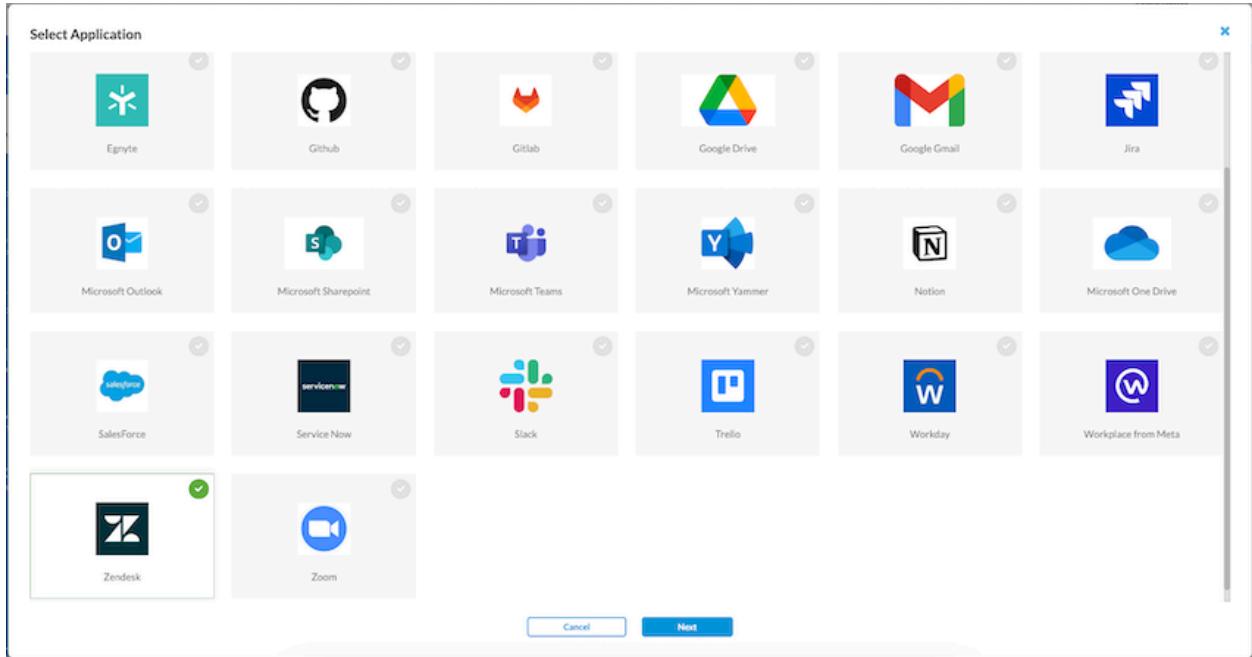
Copyright © 2024, Versa Networks, Inc.

```
{
  "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.

Add Instance - Zendesk

 Zendesk
[View Instructions](#) for setting up Zendesk instance.

Instance Name*

Admin Email*

Domain Name* Retro Scan

Services

API Based Data Protection

Confirm

Instance Add requires configuring your Zendesk account. [View Instructions](#) for setting up Zendesk instance.

Yes, I completed the steps required to configure Zendesk account

Cancel **Submit**

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. <ul style="list-style-type: none"> ◦ API-Based Data Protection—Scan and protect content.
Confirm	Click to confirm that the steps required to configure the Zendesk account

4. Click Submit.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

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

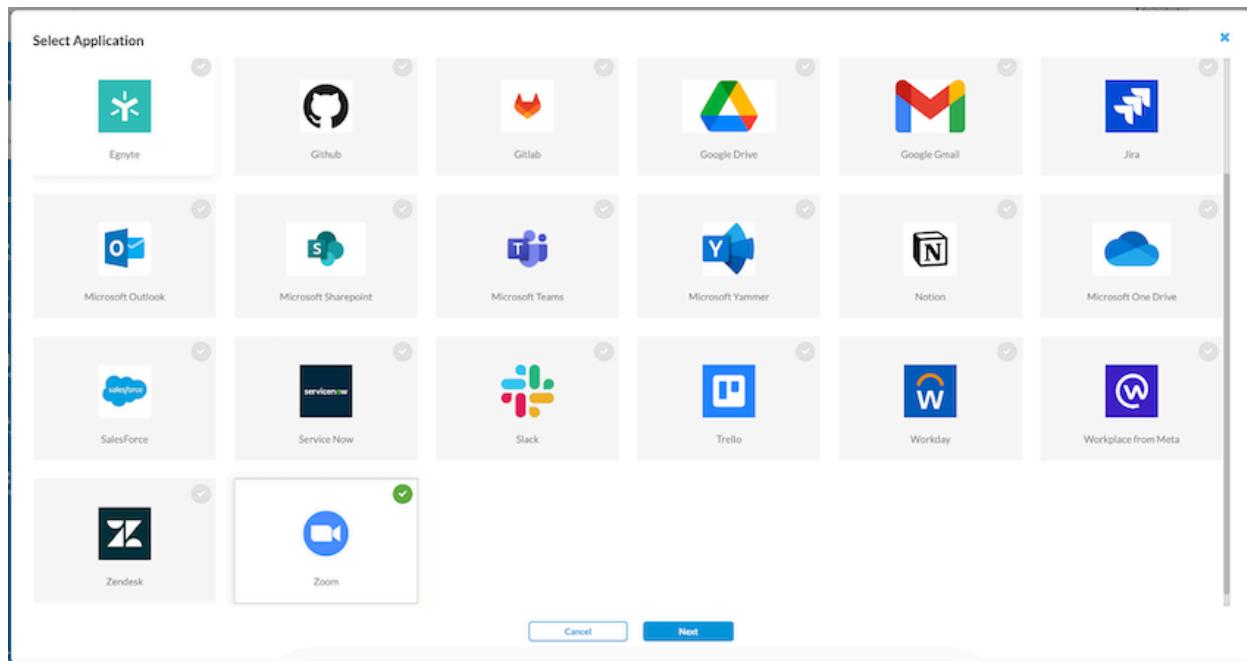
This section describes how to configure the Zoom application for API-based data protection.

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.

Add Instance - Zoom

 Zoom
[View Instructions](#) for setting up Zoom instance.

Instance Name*

Admin Email*

Retro Scan

Services API Based Data Protection

Confirm
 Instance Add requires configuring your Zoom account. [View Instructions](#) for setting up Zoom instance.
 Yes, I completed the steps required to configure Zoom account

[Cancel](#) [Submit](#)

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. <ul style="list-style-type: none"> ◦ 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.

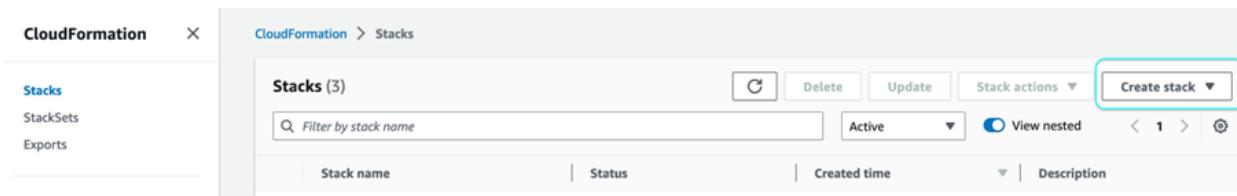
Amazon Web Services API-Based Data Protection

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

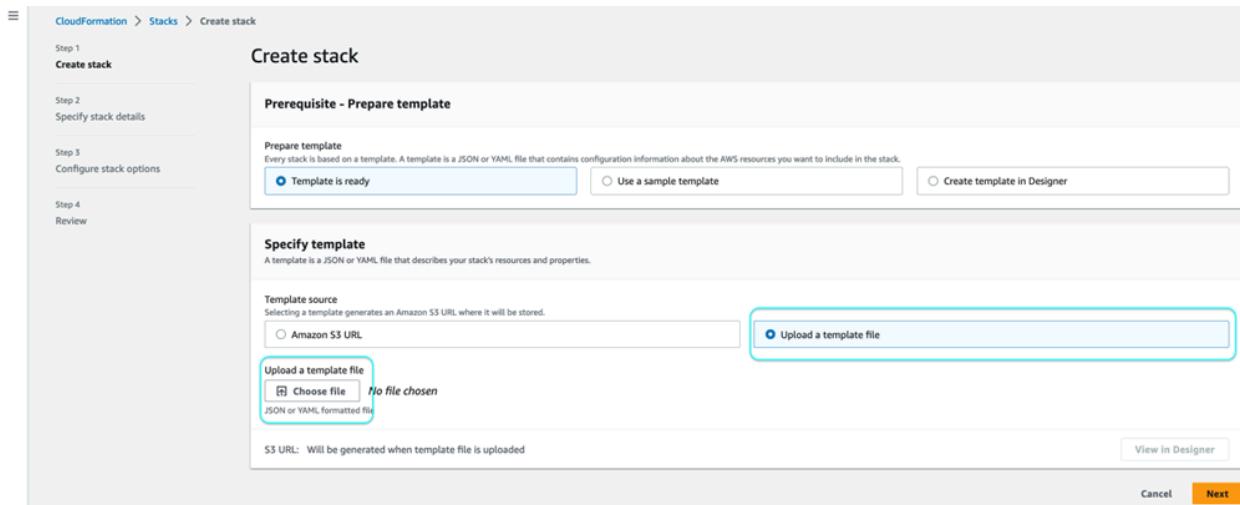
Configure Amazon Web Services for API-Based Data Protection

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

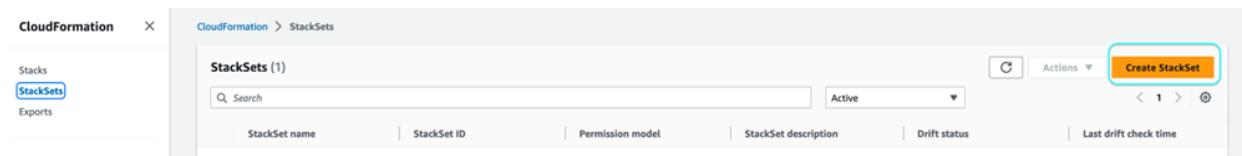
[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

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.

A screenshot of the 'Create StackSet' wizard, Step 1: Choose a template. It shows four steps: Step 1 (Choose a template), Step 2 (Specify StackSet details), Step 3 (Configure StackSet options), and Step 4 (Set deployment options).

- Permissions:** IAM role name ARN - optional. IAM role name for CloudFormation to use for all operations performed on the stack. IAM role name: AWSCloudFormationStackSetAdministrationRole.
- Prerequisite - Prepare template:** Prepar template: Template ready (radio button selected).
- Specify template:** Template source: Upload a template file (radio button selected). Choose file: ./versa-apidp-aws-stackset-setup.yaml chosen.

The 'Next' button is visible at the bottom right.

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.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

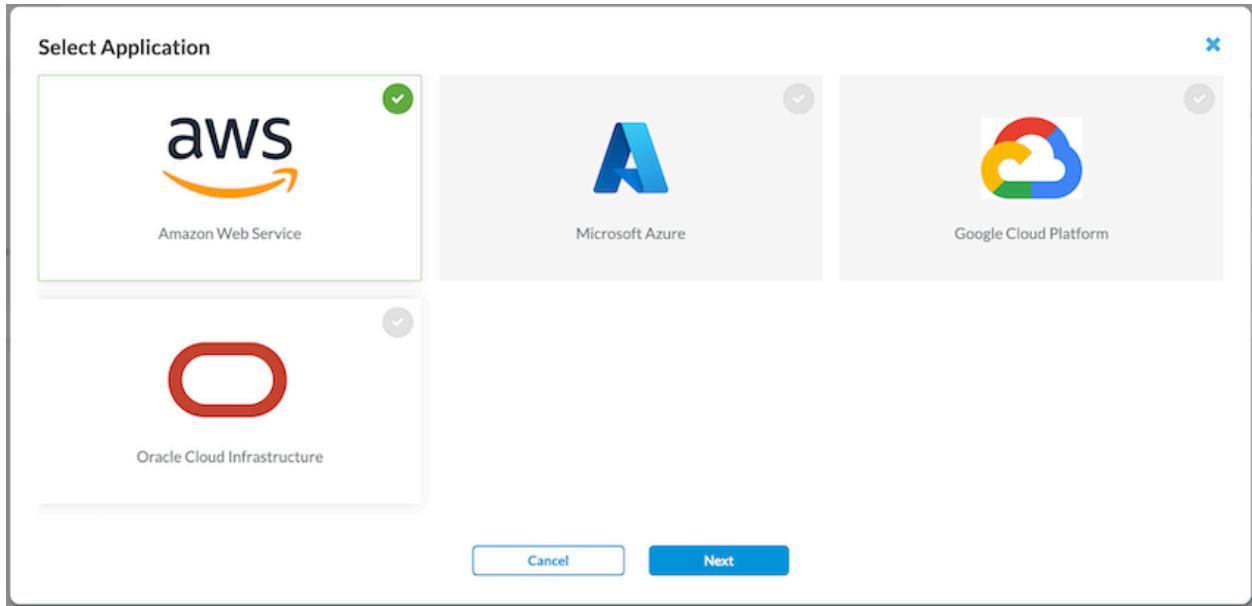
- b. In the Specify regions, select regions, or click Add all regions, and then click Next.

The screenshot shows the 'Create StackSet' wizard at Step 4: Set deployment options. Under 'Accounts', 'Deploy stacks in accounts' is selected. Under 'Specify regions', 'Add all regions' is selected. Under 'Deployment options', there are fields for 'Maximum concurrent accounts - optional' (set to 1), 'Failure tolerance - optional' (set to 0), and 'Region Concurrency' (set to Sequential). Buttons for 'Cancel', 'Previous', and 'Next' are visible at the bottom right.

13. Review StackSet details on the Review page and click Submit. The new StackSet displays on the CloudFormation page.
- Click the StackSet to view StackSet details.
 - 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.
 - Click the Template tab to view the permissions defined in the template.

Configure an Amazon Web Services Connector

- Navigate to "Configure" > "Advanced Security" > "API Based Data Protection" > "Connectors".
- Click the **Add** icon, select Amazon Web Service, then click Next.



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

Add Instance - Amazon Web Service

 Amazon Web Service
[View Instructions](#) for setting up Amazon Web Service instance.

Instance Name*

Admin Email*

Services

API Based Data Protection

Forensic

Legalhold

Quarantine

Provider Information

AWS Account Number*

Versa IAM Role*

External ID* Retro Scan

Confirm

Instance Add requires configuring your Amazon Web Service account. [View Instructions](#) for setting up Amazon Web Service instance.

Yes, I completed the steps required to configure Amazon Web Service account

[Cancel](#) [Submit](#)

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	<p>Select the services to use for the instance.</p> <ul style="list-style-type: none"> ◦ API Based Data Protection—Scan and protect content. ◦ Forensic—Use this instance for forensics.

Field	Description
	<ul style="list-style-type: none"> ◦ 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.

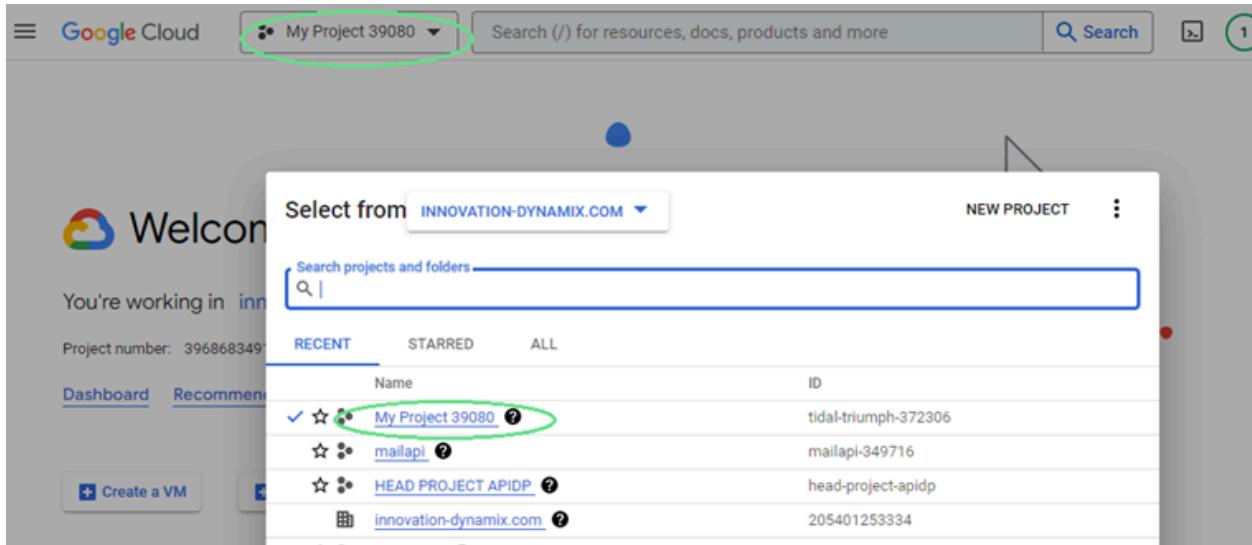
Google Cloud Platform API-Based Data Protection

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.

The screenshot shows the Google Cloud IAM and admin interface. On the left, there's a sidebar with various options like IAM and admin, IAM, Identity and organisation, Policy troubleshooter, etc. The main panel shows "Permissions for project My Project 39080". In the top right corner, there's a search bar with the text "cloud resource manager" (circled in green). A search results overlay is displayed, listing several items under "DOCUMENTATION AND TUTORIALS" and "MARKETPLACE". The "Cloud Resource Manager API" entry is highlighted with a green oval.

4. Click enable to enable the API.

[←](#) Product details



Cloud Resource Manager API

[Google Enterprise API](#)

Creates, reads, and updates metadata for Google Cloud Platform resource containers.

[ENABLE](#)

[TRY THIS API ↗](#)

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

[←](#) Product details



Cloud Pub/Sub API

[Google Enterprise API](#)

Provides reliable, many-to-many, asynchronous messaging between applications.

[ENABLE](#)

[TRY THIS API ↗](#)

6. Search for Pub/Sub and select it.

The screenshot shows the Google Cloud Pub/Sub interface. The top navigation bar includes 'Google Cloud' and 'My Project 39080'. A search bar at the top right contains the text 'pubsub', which is circled in green. The left sidebar has sections for 'Topics', 'Subscriptions', 'Schemas', and 'Pub/Sub Lite'. The main area shows a 'Topics' list with a 'CREATE TOPIC' button. To the right, there's a sidebar titled 'PRODUCTS & PAGES' with sections for 'Pub/Sub' (also circled in green), 'Schemas', 'Schemas Pub/Sub', 'Schemas Sub', and 'Subscriptions'. Below these are 'DOCUMENTATION AND TUTORIALS'.

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.

The screenshot shows the 'Create topic' dialog. The left sidebar is identical to the previous one. The main area has a 'Topic ID *' field containing 'versa-apidp-pubsub-topic', which is also circled in green. Below it is a 'Topic name' field showing 'projects/test-puja-102/topics/versa-apidp-pubsub-topic'. Under 'Encryption', the 'Google-managed encryption key' option is selected. The 'CREATE' button is at the bottom.

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

The screenshot shows the 'Subscriptions' list. The left sidebar now has 'Subscriptions' selected, which is circled in green. The main area lists a single subscription named 'versa-apidp-pubsub-topic-sub'. The table columns include 'State', 'Subscription ID', 'Delivery type', 'Topic name', 'Ack deadline', 'Retention', 'Message ordering', 'Exactly once delivery', and 'Expiry'. The 'Subscription ID' column shows 'versa-apidp-pubsub-topic-sub' with a green circle around it.

9. Click Edit.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

Pub/Sub

Subscription name: projects/test-puja-102/subscriptions/versa-apidp-pubsub-topic-sub

Subscription state: active

Topic name: projects/test-puja-102/topics/versa-apidp-pubsub-topic

METRICS DETAILS MESSAGES

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

Pub/Sub

Subscription name: projects/test-puja-102/subscriptions/versa-apidp-pubsub-topic-sub

Topic name: projects/test-puja-102/topics/versa-apidp-pubsub-topic

Delivery type

Push

Pull

Write to BigQuery

A variant of the push operation. Select this option if you want Pub/Sub to deliver messages directly to an existing BigQuery table. [Learn more](#)

Endpoint URL *

https://apidp.versanow.net/v1/gcp/webhook

Enable authentication [Learn more](#)

Message retention duration

Duration is from 10 minutes to 7 days

Days: 7 Hours: 0 Minutes: 0

Retain acknowledged messages

When enabled, acknowledged messages are retained for the message retention duration specified above. This increases message storage fees. [Learn more](#)

Expiry period

Expire after this many days of inactivity (up to 365)

A subscription is inactive if there is no subscriber activity such as open connections, active pulls or successful pushes.

31 Days

Manage resources

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

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

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

Service accounts for project 'My Project 39080'
A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps or systems.
Organisation policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants for service accounts entirely. [Learn more about service account organisation policies](#).

Filter	Enter property name or value
<input type="checkbox"/>	Email
<input type="checkbox"/>	apidp-project1@tidal-triumph-372306.iam.gserviceaccount.com
<input type="checkbox"/>	test-169@tidal-triumph-372306.iam.gserviceaccount.com

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

The screenshot shows the Google Cloud IAM and admin interface. On the left, a sidebar lists various options: IAM, Identity and organisation, Policy troubleshooter, Policy analyser, Organisation policies, Service accounts (which is highlighted with a green oval), Workload Identity Federat..., Labels, Tags, Settings, Privacy and security, Identity-Aware Proxy, Roles, Audit logs, and Essential contacts. The main area is titled 'Create service account' and contains a step-by-step guide. Step 1, 'Service account details', has a sub-step 1.1 where the 'Service account name' is set to 'apidp-project1'. Step 2, 'Grant this service account access to the project (optional)', and Step 3, 'Grant users access to this service account (optional)', are shown below. At the bottom are 'DONE' and 'CANCEL' buttons.

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

Create service account

Grant this service account access to the project (optional)

Role: Browser
Access to browse GCP resources.

Role: Logging Admin
Access to all logging permissions and dependent permissions.

Role: Pub/Sub Publisher
Publish messages to a topic.

Role: Pub/Sub Subscriber
Consume messages from a subscription, attach subscriptions to a topic and seek to a snapshot.

Role: Storage Admin
Full control of GCS resources.

CONTINUE

Grant users access to this service account (optional)

DONE CANCEL

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

Email	Status	Name	Description	Key ID	Key creation date	OAuth 2 client ID	Actions
apisp-project1@nsdal-trumpf-37230iam.gserviceaccount.com	Green checkmark	apisp-project1		081055459fb417ca7f1209eec575a880399fc9d	17 Jan 2023	117422106089014825919	⋮
				1ee445c30a9c4ca8ffdf567b3cdac8a4d3996745e	17 Jan 2023		⋮

[https://docs.versa-networks.com/Security_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

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

The screenshot shows the Google Cloud IAM and admin interface. The left sidebar has 'Service accounts' selected. The main area shows the 'Keys' tab is active. A green circle highlights the 'ADD KEY' button and the 'Create new key' option under it. Below this, there's a table listing two keys, both marked as Active and Expiry Date is set to 31 Dec 9999. The entire interface is framed by a light gray border.

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

The screenshot shows the same Google Cloud IAM and admin interface as above, but with a modal window open over the 'Keys' table. The modal is titled 'Create private key for 'apidp-project1''. It contains a note about storing the file securely and two radio buttons for 'Key type': 'JSON' (which is selected) and 'P12'. A green circle highlights the 'JSON' radio button. At the bottom right of the modal are 'CANCEL' and 'CREATE' buttons.

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

Type	Principal	Name	Role	Security Insights	Inheritance
apisp-project1	apisp-project1@tdal-triumph-372306.iam.gserviceaccount.com	apisp-project1	Project IAM Admin	0 / 3 excess permissions	
			Pub/Sub Editor	30 / 34 excess permissions	
			Pub/Sub Publisher	★ 1 / 1 excess permissions	
			Pub/Sub Subscriber	2 / 3 excess permissions	
			Storage Admin	29 / 33 excess permissions	

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

Grant access to 'mailapi'

Grant principals access to this resource and add roles to specify what actions the principals can take. Optionally, add conditions to grant access to principals only when a specific criteria is met. [Learn more about IAM conditions](#)

Resource

mailapi

Add principals

Principals are users, groups, domains or service accounts. [Learn more about principals in IAM](#)

New principals

apidp-project1@tidal-triumph-372306.iam.gserviceaccount.com



Assign Roles

Roles are composed of sets of permissions and determine what the principal can do with this resource. [Learn more](#)

Role *
Pub/Sub Admin

IAM condition (optional) ?
+ ADD IAM CONDITION

Full access to topics, subscriptions and snapshots.



Role
Project IAM Admin

IAM condition (optional) ?
+ ADD IAM CONDITION



Access and administer a project's IAM policies.

Role
Storage Admin

IAM condition (optional) ?
+ ADD IAM CONDITION



Full control of GCS resources.

+ ADD ANOTHER ROLE

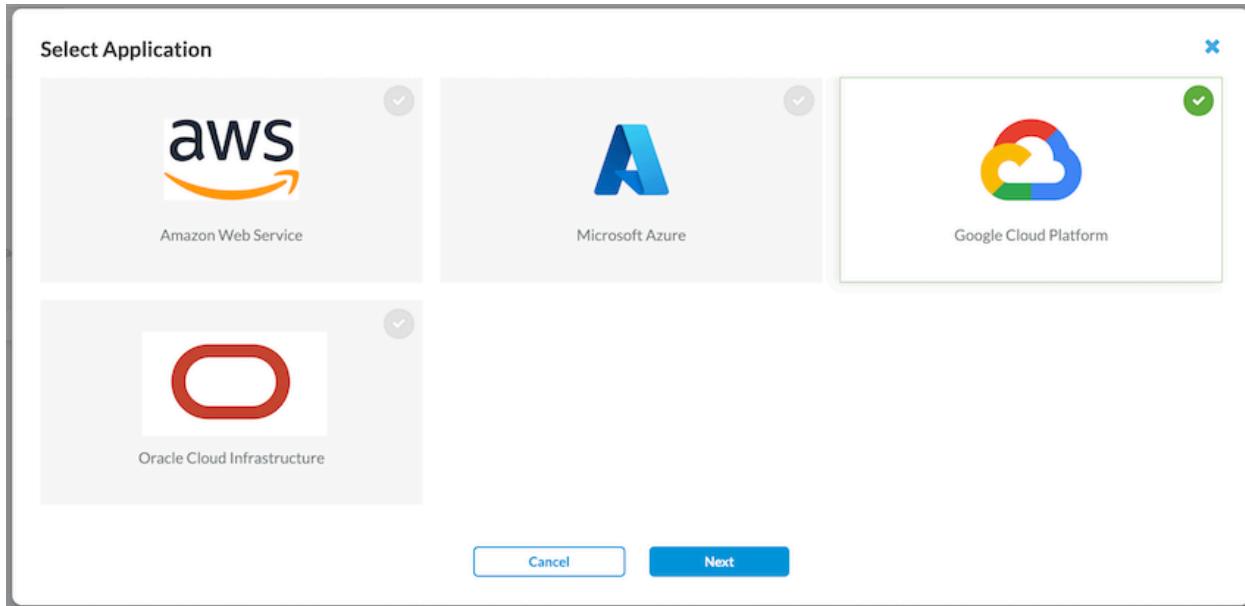
SAVE

CANCEL

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.

Add Instance - Google Cloud Platform

 Google Cloud Platform
[View Instructions](#) for setting up Google Cloud Platform instance.

Instance Name*

Admin Email*

Services

API Based Data Protection

Forensic

Legalhold

Quarantine

Provider Information

Project ID* Retro Scan

Upload the Private Key JSON File*

Confirm

Instance Add requires configuring your Google Cloud Platform account. [View Instructions](#) for setting up Google Cloud Platform instance.

Yes, I completed the steps required to configure Google Cloud Platform account

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	<p>Select the services to use for the instance.</p> <ul style="list-style-type: none"> ◦ API Based Data Protection—Scan and protect content. ◦ Forensic—Use this instance for forensics. ◦ Legal hold—Use this instance for Legal hold.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

Field	Description
	<ul style="list-style-type: none"> ◦ Quarantine—Use this instance for Quarantine files.
Private Key JSON File	Upload the private key JSON file generated for service account.

4. Click Done.

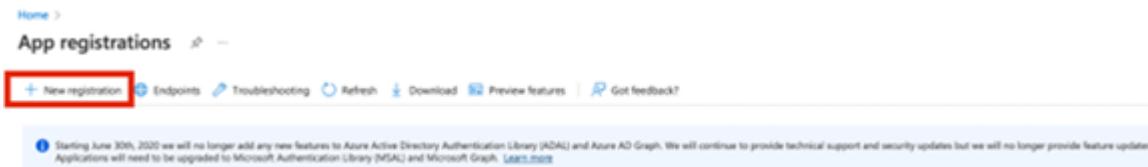
Microsoft Azure API-Based Data Protection

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.

Register an application

* Name

The user-facing display name for this application (this can be changed later).



Supported account types

Who can use this application or access this API?

 Accounts in this organizational directory only (Versa Networks only - Single tenant) Accounts in any organizational directory (Any Azure AD directory - Multitenant) Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox) Personal Microsoft accounts only[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.


Left Blank

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.

- In the search bar, search for Subscription.
- Select the subscription for Versa data protection app.
- Copy the subscription ID.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications..](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications..)

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

Copyright © 2024, Versa Networks, Inc.

Org-1 Subscription

Subscription

Search

Cancel subscription | Rename | Feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Security

Events

Cost Management

Cost analysis

Cost alerts

Budgets

Advisor recommendations

Billing

Billing profile invoices

Settings

Programmatic deployment

Subscription ID: 0e04d6e...b643

Subscription name: Versa Lab Azure

Directory: Versa Networks (versalab.onmicrosoft.com)

Status: Active

Parent management group: ...

My role: Owner

Plan: Azure Plan

Secure Score: Not available

Spending rate and forecast

Current cost: \$16.78

Forecast: \$197.95

View details

Costs by resource

View details

- d. Select Access Control (IAM) in the left menu bar.
- e. Select Add > Add role assignment.

Subscription

Search (Cmd+ /)

+ Add | Download role assignments | Edit columns | Re

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Security

Add role assignment

Add co-administrator

Add custom role

View my level of access to this resource.

View my access

Check access

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

Role Members • Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Name ↑↓	Description ↑↓
Owner	Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.
Contributor	Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, ...

- g. Enter information for the following fields.

Add role assignment

Got feedback?

Role Members • Review + assign

Selected role
Contributor

Assign access to

User, group, or service principal
 Managed identity

Members
[+ Select members](#)

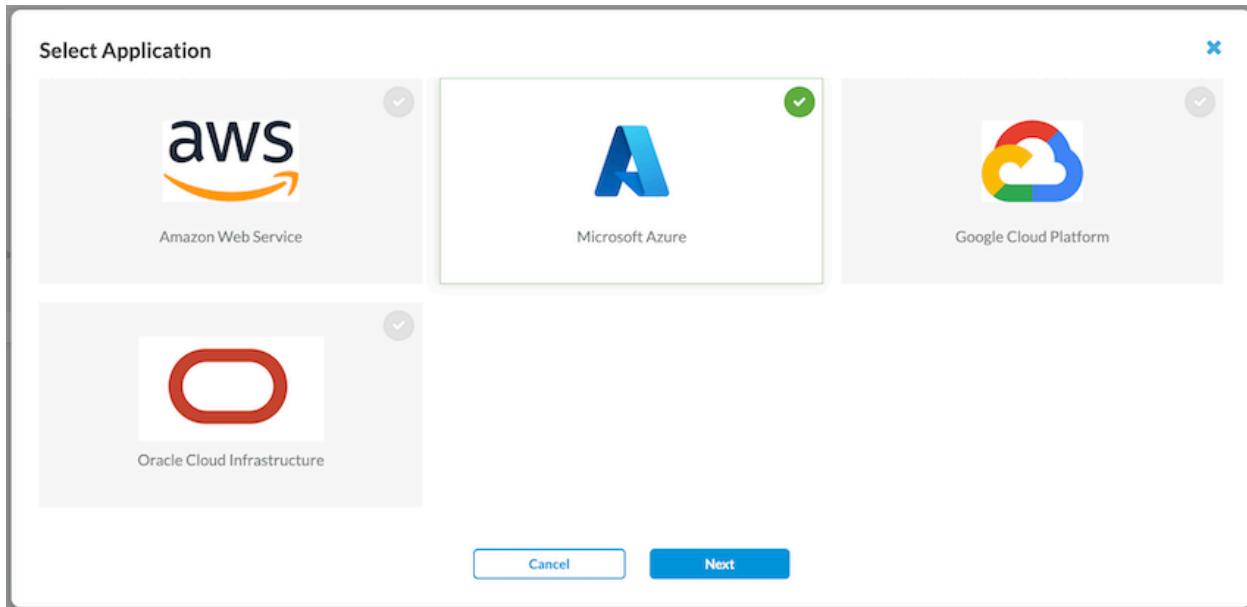
Name	Other
No members selected	Selected members: No members selected. Search for and add one or more members you want to assign to the role for this resource.

- 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.

Add Instance - Microsoft Azure



Microsoft Azure
[View Instructions](#) for setting up Microsoft Azure instance.

Instance Name*

Admin Email*

Services

API Based Data Protection

Forensic

Legalhold

Quarantine

Provider Information

Subscription ID*

Directory ID (Tenant ID)*

Client ID*

Client Secret*

Retro Scan

Confirm

Instance Add requires configuring your Microsoft Azure account. [View Instructions](#) for setting up Microsoft Azure instance.

Yes, I completed the steps required to configure Microsoft Azure account

Cancel **Submit**

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
	<ul style="list-style-type: none"> ◦ 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.

The screenshot shows the Oracle Cloud interface with the navigation bar "ORACLE Cloud" and search bar "Search resources, services, documentation, and Marketplace". The location is "US West (San Jose)". On the left, the "Resources" sidebar has "My groups" selected, with other options like "Integrated applications", "Auth tokens", "Customer secret keys", etc. The main content area is titled "My groups" and shows a table with one group named "Administrators" with the description "Administrators". A search bar "Search by group name or description." is at the top right of the table. A button "Request access to a new group" is also present.

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

The screenshot shows the Oracle Cloud interface with the navigation bar "ORACLE Cloud" and search bar "Search resources, services, documentation, and Marketplace". The location is "US West (San Jose)". On the left, the "Resources" sidebar has "API keys" selected, with other options like "My groups", "Integrated applications", "Auth tokens", etc. The main content area is titled "API keys" and shows a table with two API keys listed: "Fingerprint" (eb:49:9b:80:b3:f8:73:db:a0:55:e8:51:02:ea:5a:dd) created on "Tue, Oct 3, 2023, 16:11:33 UTC" and "05:c2:e0:50:ce:8f:92:71:20:ba:d0:6d:8c:c5:56:a0" created on "Tue, Oct 3, 2023, 16:19:43 UTC". A button "Add API key" is highlighted with a red box. A "Delete" button is also visible.

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

The screenshot shows the Oracle Cloud interface for managing API keys. On the left, a sidebar lists various resources like My groups, Integrated applications, and API keys. The main area is titled 'Add API key'. It includes a note about API keys being RSA key pairs in PEM format. There are three options: 'Generate API key pair' (selected), 'Choose public key file', and 'Paste a public key'. Below this is a 'Public key' section with a download link for the private key, which is highlighted with a red box. At the bottom are 'Add' and 'Cancel' buttons.

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.

The screenshot shows the Oracle Cloud interface for viewing configuration files. A modal window titled 'Configuration file preview' is open. It contains a note about including basic authentication information and pasting it into an OCI config file. Below is a text box showing configuration data, and at the bottom is a 'Copy' button, which is highlighted with a red box. Other buttons include 'Close' and a note to paste into the config 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:

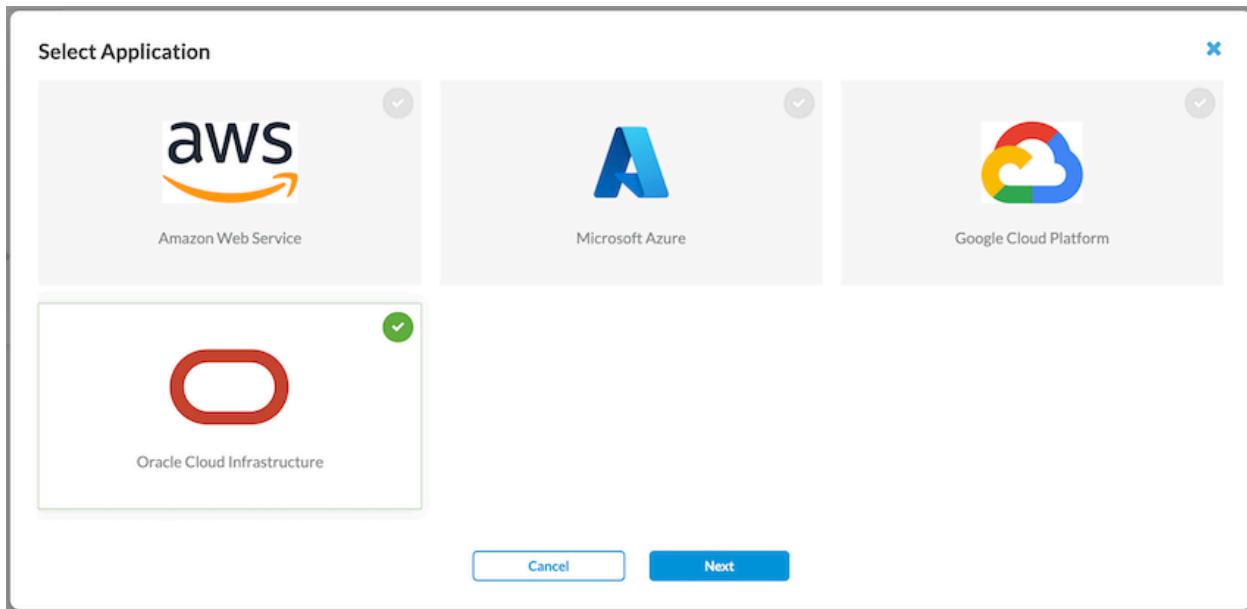
1. Navigate to "Configure" > "Advanced Security" > "API Based Data Protection" > "Connectors".

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Cloud_Applications...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Cloud_Applications...)

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

Copyright © 2024, Versa Networks, Inc.

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.

Add Instance - Oracle Cloud Infrastructure

 Oracle Cloud Infrastructure
[View Instructions](#) for setting up Oracle Cloud Infrastructure instance.

Instance Name*

Admin Email*

Services

API Based Data Protection

Forensic

Legalhold

Quarantine

Provider Information

Config File*

Upload the Private Key JSON File* [Browse](#)

Retro Scan

Confirm

Instance Add requires configuring your Oracle Cloud Infrastructure account. [View Instructions](#) for setting up Oracle Cloud Infrastructure instance.

Yes, I completed the steps required to configure Oracle Cloud Infrastructure account

[Cancel](#) [Submit](#)

Field	Description
Instance Name (Required)	Enter a name for the instance.
Admin Email (Required)	Enter the email address of the Oracle Cloud Infrastructure administrator.
Services	<p>Select the services to use for the instance.</p> <ul style="list-style-type: none"> ◦ 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 authentication information.
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 Cloud Applications.
Confirm	Click to confirm that the steps required to configure the Oracle Cloud Applications.

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](#)