

## **Juniper Secure Edge**

# CASB and DLP Administration Guide

## Copyright and disclaimer

Copyright © 2024 Lookout, Inc. and/or its affiliates. All rights reserved.

Lookout, Inc., Lookout, the Shield Logo, and Everything is OK are registered trademarks of Lookout, Inc. Android is a trademark of Google Inc. Apple, the Apple logo, and iPhone are trademarks of Apple Inc., registered in the U.S. and other countries. App Store is a service mark of Apple Inc. UNIX is a registered trademark of The Open Group. Juniper Networks, Inc., Juniper, the Juniper logo, and Juniper Marks are registered trademarks of Juniper Networks, Inc.

All other brand and product names are trademarks or registered trademarks of their respective holders.

This document is provided under a license agreement containing restrictions on its use and disclosure and is protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means.

The information contained in this document is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

This document may provide access to, or information on content, products and services from third parties. Lookout, Inc. and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Lookout, Inc. and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

# Contents

<b>About Juniper Secure Edge.....</b>	<b>14</b>
Benefits of Juniper Secure Edge .....	14
Cloud Access Security Broker.....	14
Data Loss Prevention .....	14
<b>Getting started.....</b>	<b>15</b>
Logging in for the first time .....	15
Viewing feature walkthroughs .....	15
Accessing product information, documentation, and customer support .....	15
Version information .....	15
Documentation and videos .....	16
Customer support .....	16
Managing your password and logging out .....	16
Changing your administrative password.....	16
Resetting a forgotten password .....	16
Logging out .....	17
<b>Onboarding cloud applications and suites .....</b>	<b>18</b>
Supported sanctioned cloud applications.....	18
Onboarding process overview .....	18
Enter basic information .....	19
For application suites, select applications .....	19
Select protection modes .....	19
Select configuration settings.....	19
Enter authorization information.....	20
Save the onboarded cloud application.....	20
Onboarding Microsoft 365 suite and applications .....	20
Configuration steps .....	21
Microsoft 365 application suite .....	21
Turning on audit log search and verifying mailbox management by default .....	21
SharePoint / OneDrive .....	21
Creating sites for new SharePoint or OneDrive users .....	21
Creating a Quarantine site in SharePoint .....	23
Onboarding steps.....	23
Enabling audit logging and managing mailbox auditing.....	26
Microsoft 365 API onboarding with Self-Managed OAuth Application .....	26
Creating a custom application.....	26

---

Configuring the custom application .....	27
Onboarding Microsoft 365 using your new application .....	27
Permissions needed for custom onboarding app.....	27
Onboarding Slack Enterprise applications .....	30
Onboarding steps.....	30
Onboarding the AWS suite and applications.....	32
Automated onboarding .....	32
Onboarding with Terraform .....	32
Manual onboarding .....	33
Configuration steps.....	33
Step 1 – Create an Identity Access Management (IAM) role for Juniper CASB .....	33
Step 2 – Create a Cloud Trail .....	34
Step 3 – Create Simple Queue Service (SQS) .....	34
Step 4 – Configure Event Notifications for the Cloud Trail Bucket.....	35
Step 5 – Create an IAM Monitor policy.....	36
Step 6 – Create an IAM DLP policy .....	37
Step 7 – Create an IAM Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) policy .....	39
Step 8 – Create an IAM Key Management Service (KMS) policy .....	41
Step 9 – Attach the policies to the IAM role.....	42
Onboarding steps.....	43
Onboarding Azure applications .....	45
Configuration steps .....	45
Onboarding steps.....	45
Onboarding Azure Blob applications .....	47
Configuration steps .....	47
Creating a custom role .....	47
Registering the EventGrid resource.....	48
Onboarding steps.....	48
Onboarding the Google Workspace suite and applications .....	49
Configuration steps .....	49
Updating API access settings .....	49
Updating folder access information.....	51
Onboarding steps in CASB .....	51
Onboarding Google Cloud Platform (GCP).....	55
Configuration steps .....	55
Onboarding steps.....	58

---

Onboarding Dropbox applications .....	60
Onboarding GitHub applications .....	61
Onboarding the Atlassian Cloud suite and applications .....	62
Entering configuration settings for protection models.....	63
API Access.....	63
Generating an API token (Confluence applications only).....	63
Onboarding Egnyte applications .....	65
Onboarding Box applications .....	65
Configuration steps in the Box Admin Console .....	65
Onboarding steps in the Management Console .....	67
Onboarding Salesforce applications.....	69
Configuration steps .....	69
Enable CRM content .....	69
Enable scanning for structured data .....	69
Enable permissions for DLP scanning.....	69
Enable permissions for viewing event log files.....	70
Enable Event Monitoring.....	70
Enable permissions for Audit Trail events.....	71
Enable permissions for Login History events .....	71
Enable permissions for querying files .....	71
Enable permissions for viewing and modifying data.....	72
Onboarding steps.....	72
Onboarding ServiceNow applications .....	74
Configuration steps .....	74
Onboarding steps.....	74
<b>Post-onboarding tasks .....</b>	<b>76</b>
Applying event filtering to onboarded cloud applications .....	76
<b>Configuring tenants for user access and session activity .....</b>	<b>78</b>
<b>Managing users .....</b>	<b>80</b>
Administrative user management.....	80
Adding new users .....	80
Setting up a user account password policy .....	81
Account status for system administrator and non-administrator roles.....	83
Disabling a non-administrator user account .....	83
Re-enabling a disabled non-administrator user account .....	84
Reassigning the Super Administrator role .....	84

Enterprise user management .....	84
Searching for user information.....	84
Filtering user information .....	85
<b>Configuring CASB for enterprise integration.....</b>	<b>86</b>
Installing an on-premises connector for system services.....	87
Specifications.....	87
Operating systems and software .....	87
Firewall settings .....	87
Minimum requirements for VM configurations .....	88
Log agent, SIEM, and EDLP services .....	88
Downloading the connector .....	88
Pre-installation steps .....	88
Step 1 – Create an agent for the service .....	88
Step 2 – Create an environment.....	88
Step 3 – Create a node.....	88
Installing the connector (SIEM, EDLP, and Log Agent).....	90
Run the following command to start the installation:.....	90
Run the following command to change to the directory in which to install the connector. ....	90
Run the following command to perform the installation.....	90
Enter the default option shown or enter the URL for this installation. .....	91
Enter ID for this tenant.....	91
Enter the unique name for the Node Server. ....	91
Enter the API token (click the API Token button in the Configuration tab) . .....	91
Select an NIC option.....	91
Starting the connector .....	91
Restarting and uninstalling the connector .....	92
Restarting.....	92
Uninstalling .....	92
Additional configuration notes for SIEM.....	92
Additional configuration notes for log agents.....	92
Connecting to a different server .....	92
Write permissions .....	92
Additional configuration notes for EDLP .....	92
Adding Advanced Threat Protection (ATP) services.....	92
Adding external services for Enterprise Data Loss Prevention (EDLP) .....	94

---

Creating a new configuration for EDLP .....	95
Downloading and installing an EDLP agent .....	96
Prerequisites for installing the EDLP agent.....	96
Downloading the EDLP agent.....	96
Installing the EDLP agent.....	96
Stopping and starting the EDLP agent service .....	97
Checking the EDLP agent status.....	97
Symantec DLP response rule configuration (Vontu service).....	97
Configuring the Forcepoint Security Manager and Protector .....	98
Remotely upgrading the SIEM, EDLP, and Log Agents .....	100
Remote upgrade considerations .....	100
Remote upgrade steps for SIEM, EDLP, and Log agents .....	100
Manually upgrading the SIEM, EDLP, and Log Agents .....	101
For CentOS and RHEL .....	101
Upgrading a connector using an RPM package.....	101
For Ubuntu .....	102
Method 1: Installing the latest connector version using a Debian package .....	103
Method 2: Upgrading a connector using a Tar package .....	104
Method 3: Upgrading a connector using a Debian package .....	105
Configuring Security Information and Event Management (SIEM) .....	105
Downloading, installing, and connecting a SIEM agent.....	105
Prerequisites for installation of an SIEM agent .....	106
Downloading .....	106
Installing .....	106
Configuring.....	106
Viewing the authentication token .....	107
Uninstalling a SIEM agent .....	107
Starting, stopping, and checking the status of a SIEM agent.....	107
Viewing SIEM agent logs .....	107
Creating a new SIEM configuration .....	107
Additional actions.....	108
Configuring data classification.....	108
Integration with Azure Information Protection (AIP) .....	109
Retrieving parameters required for AIP RMS connection.....	109
Configuring AIP protection.....	112
Syncing labels .....	112
Label information .....	113

---

Creating a policy with RMS protection.....	113
Creating additional RMS policy templates .....	114
Integration with Google .....	115
Update scopes for your Google account.....	116
Turn on labels for your Google account .....	116
Create labels .....	116
Enable Data Classification for Google labels .....	117
Enable Google Data Classification in CASB.....	117
Create Policies using Google Data Classification.....	117
Policies to Apply Google Labels to Files.....	117
Policies to Detect Google Labels on Files .....	118
Integration with Titus.....	118
Creating and managing user directories .....	119
Manual upload user directory .....	120
Creating a new manual upload directory.....	120
Exporting a manually uploaded CSV file.....	121
Deleting a manually uploaded CSV file .....	121
Configuring an Azure AD user directory .....	121
Creating a new Azure AD user directory .....	121
Syncing an Azure AD user directory .....	121
Configuring an Okta application.....	121
Creating a web application integration in Okta.....	122
User Directories with SCIM Integration.....	123
Setting Up SCIM with Okta.....	124
Setting up SCIM with Azure AD.....	125
<b>Configuring logs .....</b>	<b>127</b>
<b>Creating and managing notifications and alerts.....</b>	<b>128</b>
Creating notification channels .....	128
Creating notification templates .....	129
Creating notifications .....	131
Creating activity alerts .....	132
Types of alerts .....	133
Creating alerts for managed cloud applications .....	133
Creating alerts for Cloud Discovery.....	134
Configuring notification and alert options in System Settings .....	135

---

Selecting alert configurations.....	135
Editing an alert configuration .....	137
Deleting an alert configuration .....	137
<b>Configuring Juniper Secure Edge CASB for policy management.....</b>	<b>139</b>
Policy configuration and creation workflow .....	139
Create content rule templates .....	140
Creating new data types .....	140
Dictionary .....	140
Regex Pattern .....	141
File Type.....	141
File Extension.....	141
File Name.....	141
Composite .....	141
Match Count and Unique Match Count.....	142
Exact Data Match.....	142
Step 1 -- Create or obtain a CSV file with the data to use for matching. ....	142
Step 2 – Create a new data type -- Exact Data Match. ....	142
Step 3 – Create a new DLP Rule template to configure the data matching properties. ....	143
Creating new DLP rule templates .....	145
Creating new document rule templates .....	146
Create Content Digital Rights templates .....	147
Steps for creating CDR templates .....	148
Configure file type, MIME type, and file size for exclusion from scanning .....	150
Exclusion from scanning by Juniper DLP engine .....	150
File type .....	150
MIME type .....	150
File size .....	150
Exclusions from scanning by the CASB scan engine.....	151
File type .....	151
File size .....	151
Configure folder sharing for DLP scanning .....	151
Set number of folder sublevels for scanning .....	151
Configure default policy violation actions .....	152
<b>Creating policies for data protection and application security.....</b>	<b>153</b>
Viewing policy lists.....	154

---

API Access policies.....	154
Creating API Access policies .....	154
API policies with DLP Scan or None as the content inspection type.....	154
API policies with Malware Scan as the content inspection type.....	161
<b>Managing connected applications .....</b>	<b>165</b>
Managing applications from the Connected Apps tab.....	165
Managing AWS key use .....	166
Filtering and syncing connected application and AWS information.....	166
<b>Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) .</b>	<b>168</b>
Cloud applications supported.....	168
Infrastructure Discovery.....	168
Assessment configuration .....	169
Assessment Results tab .....	170
Past Assessment Reports tab .....	170
Adding a new assessment.....	170
Modifying assessment details .....	174
Basic Details tab.....	174
Compliance Rules tab.....	174
<b>Cloud Data Discovery .....</b>	<b>175</b>
Onboard a cloud application for which you want to apply Cloud Data Discovery .....	175
Create a Cloud Data Discovery policy.....	176
Create a Cloud Data Discovery scan .....	176
Associate a scan with a Cloud Data Discovery policy.....	177
View scan details.....	178
Overview tab .....	178
Basic tab .....	179
Policy tab .....	179
Past Scans tab.....	180
Generate a scan report.....	180
Generating activity reports for Box cloud applications. ....	181
<b>Violation management and quarantine.....</b>	<b>186</b>
Quarantine Management.....	186
Selecting information to view .....	186
Pending review.....	186
Reviewed .....	186
Taking action on a quarantined file.....	187

Viewing and searching for quarantined documents.....	187
Selecting information to display and review .....	188
CDD Violation Management.....	188
Selecting information to view .....	189
Taking action on a quarantined CDD item.....	189
<b>Monitoring and managing system activity .....</b>	<b>190</b>
Viewing user and system activity from the Home Dashboard .....	190
Data cards.....	190
Content Scanning .....	190
Content Sharing .....	191
Most Hit Security Policies .....	191
Event details .....	191
By time range .....	192
Viewing additional details .....	192
From a data card.....	192
From the table .....	192
Refreshing all data.....	193
Exporting data.....	193
Monitoring cloud activity from charts .....	193
Application Activities .....	194
Policy Analytics .....	194
Activity Monitoring.....	195
Encryption Statistics .....	195
Privileged User Activities .....	195
Anomalous Activities.....	196
Anomalous activities by geolocation .....	197
Displaying geoanomaly details from the Activity Audit Logs page .....	197
Anomalous downloads, content access, and authentication.....	197
Three-dimensional activity views.....	198
Settings for configuring anomaly information .....	198
Adaptive threshold for permitted user activity rates (Preview feature) .....	199
Tracking of anomaly information .....	199
Settings for anomaly profiles (dynamic anomaly configuration) .....	201
Office 365.....	203
AWS Monitoring .....	203
Customizing and refreshing a dashboard display.....	204

---

Exporting data for reporting .....	204
Printing a report or chart .....	205
Working with activity audit logs .....	206
Filtering data .....	208
Selecting fields to include in the table view.....	210
Viewing additional details from a table entry .....	210
FireEye.....	211
Juniper ATP Cloud .....	212
Viewing anomaly details from the Activity Audit Logs page .....	212
Performing an advanced search.....	212
Viewing additional log details.....	213
Hiding the chart view .....	213
Exporting data.....	213
Monitoring user activity through Admin Audit Logs .....	214
Audit log information .....	214
Filtering and searching for Admin Audit Log information.....	215
Insights Investigate .....	215
Incident Management tab .....	215
Incident Insights tab .....	217
Entity Insights tab.....	218
Viewing and updating user risk information.....	219
<b>Creating, viewing, and scheduling reports .....</b>	<b>220</b>
Uploading a company logo.....	220
Setting a time zone.....	220
Selecting report types for cloud applications.....	221
Visibility .....	221
Compliance .....	221
Threat Protection .....	222
Data Security .....	222
IaaS.....	222
Custom.....	222
Displaying report information.....	222
Scheduling a new report.....	223
Downloading generated reports .....	224
Managing report types and scheduling .....	225
<b>Quick reference: Home dashboard charts .....</b>	<b>226</b>
Application Activities.....	226

---

Policy Analytics .....	226
Activity Monitoring .....	228
Encryption Statistics .....	229
Privileged User Activities .....	230
Anomalous Activities .....	231
Office 365 .....	232
Overview .....	232
Admin Activities .....	233
OneDrive .....	233
SharePoint .....	234
Teams .....	234
IaaS Monitoring Dashboard .....	235
Amazon Web Services .....	235
Microsoft Azure .....	236
Google Cloud Platform .....	239
<b>Quick reference: RegEx examples .....</b>	<b>241</b>
<b>Quick reference: Supported file types .....</b>	<b>242</b>

## About Juniper Secure Edge

---

Juniper Secure Edge helps you secure your remote workforce with consistent threat protection that follows users wherever they go. It provides full-stack Security Service Edge (SSE) capabilities to protect web, SaaS, and on-premises applications and provides users with consistent and secure access from anywhere.

It includes key SSE capabilities including Cloud Access Security Broker (CASB) and Data Loss Prevention (DLP) to protect user access on SaaS applications and ensures that sensitive data in those applications doesn't leave your network if you don't want it to.

## Benefits of Juniper Secure Edge

- Secure user access from anywhere—Support your remote workforce in the office, at home, or on the road with secure access to the applications and resources they need. Consistent security policies follow users, devices, and applications without copying or recreating rule sets.
- Single policy framework from a single UI—Unified policy management from the edge through the data center means fewer policy gaps, elimination of human error, and a more secure environment.
- Dynamic user segmentation—Follow-the-user policy provides automated access control to employees and third-party contractors through granular policy, locking down third-party access as an attack vector.
- Protect access to applications on-premises and in the cloud—Reduce risk by leveraging effective threat prevention services proven to be the most effective on the market by multiple third-party tests to inspect traffic, ensuring secure access to web, SaaS, and on-premises applications from anywhere.
- Transition at a pace that is best for your business—Juniper meets you where you are on your journey, helping to leverage the cloud-delivered security capabilities of Secure Edge for both on-premises edge security at the campus and branch, and for your remote workforce, working from anywhere.

## Cloud Access Security Broker

CASB provides visibility into SaaS applications and granular control to ensure authorized access, threat prevention, and compliance.

Using Juniper's CASB, you can:

- Apply granular controls to ensure authorized access, threat prevention, and compliance.
- Secure your data from unauthorized or inadvertent access, malware delivery and distribution, and data exfiltration.
- Allow organizations to leverage their existing technology investments, whether you are starting on-premises with campus and branch, in the cloud with remote workforce, or a hybrid approach.

## Data Loss Prevention

Juniper's DLP classifies and monitors data transactions to ensure compliance requirements and data security. Juniper's DLP reads files, classifies content (for example, credit card numbers, social security numbers, and addresses), and tags the file as containing a specific category of data. Using your organization's DLP policy, you can add granular controls and add tags (for example, HIPAA and PII) to the files. If anyone attempts to remove the data from your organization, Juniper's DLP stops that from happening.

# Getting started

The following sections provide instructions for the next steps after you have deployed Juniper Secure Edge:

- [Logging in for the first time](#)
- [Viewing feature walkthroughs](#)
- [Accessing product information, documentation, and customer support](#)
- [Managing your password and logging out](#)

Once you log in, you will be provided with options for onboarding cloud applications.

## Logging in for the first time

After your enterprise has purchased Juniper Secure Edge, you will receive an email with a link that provides a username and a temporary password. Click the link.

The username you see in the **Create Account** screen is prepopulated from the email.

1. Enter the temporary password.
2. In the **Password** field, enter a new password for future use. Hints are provided as a guide to the type and number of characters allowed.
3. Re-enter the new password in the **Confirm Password** field and click **Create**.

**Note:** The email link and temporary password expire in 24 hours. If more than 24 hours have passed before you see this email, contact Support to get a new temporary link and password.

When you have completed the login steps, the initial welcome screen appears.

When you are ready to onboard unsanctioned or sanctioned cloud applications, select these areas from the Management Console:

- To initiate cloud discovery for unsanctioned cloud applications: Choose **Administration > Log Agents** to upload log files and create log agents.
- To onboard sanctioned cloud applications: Choose **Administration > App Management**. Then, follow the instructions for onboarding cloud applications.

## Viewing feature walkthroughs

Click the **i** menu to view a list of how-to walkthroughs of Juniper Secure Edge features.

## Accessing product information, documentation, and customer support

Click the **question mark** icon to display the help menu.

## Version information

Click the **About** link.

## Documentation and videos

The following links are available:

- **Walkthrough Videos** – Opens the **Walkthrough Videos** page, with links to videos about product features.
- You can also access links to feature videos from any Management Console page that displays a video link at the upper right.
- **Online Help** – Opens the online help for the product. The help includes a clickable Table of Contents and an index for searching.
  - **Documentation** – Opens a link to a downloadable PDF of the *Juniper Secure Edge CASB and DLP Administration Guide*.

## Customer support

You can contact Juniper Networks Technical Assistance Center (JTAC) 24 hours a day, seven days a week on the Web or by telephone:

- Juniper Support Portal: <https://supportportal.juniper.net/>

### Note

If this is your first time requesting support, please register and create an account at:

<https://userregistration.juniper.net/>

- Telephone: +1-888-314-JTAC (+1-888-314-5822), toll free in U.S., Canada, and Mexico

### Note

For international or direct-dial options in countries without toll free numbers, see <https://support.juniper.net/support/requesting-support>. If you are contacting JTAC by telephone, enter your 12-digit service request number followed by the pound (#) key for an existing case, or press the star (\*) key to be routed to the next available support engineer.

## Managing your password and logging out

Use the following procedures to change your password, reset a forgotten password, and log out.

### Changing your administrative password

1. Click the **Profile** icon.
2. Click **Change Password**.
3. Enter your current password in the **Old Password** field.
4. Enter your new password in the **New Password** and **Confirm Password** fields.
5. Click **Update**.

### Resetting a forgotten password

If you forgot your password, perform the following steps to reset it.

1. From the **Login** screen, click **Forgot your password?**.
2. In the **Forgot Password** screen, enter your username and click **Reset**.

You will receive an email with a temporary password and a link to reset your password.

*This temporary password will expire in 24 hours.* If more than 24 hours have passed since you received your temporary password, you will see a **Token Expired** message when you try to enter your temporary password. If this happens, repeat the first two steps to receive a new temporary password.

3. In the email, click the link for the new temporary password.

The **Forgot Password** dialog box is displayed with your first name, last name, and username filled in.

4. Enter the temporary password provided. If you copy and paste the temporary password from the email instead of typing it, be sure not to copy any extra spaces or characters.
5. Enter your new password in the **New Password** and **Confirm New Password** fields. As you type, tooltips appear at the right that provide guidance for the required format and number of characters.
6. Click **Create**.

## Logging out

Click the **Profile** icon and click **Logout**.

# Onboarding cloud applications and suites

The following sections provide instructions for configuring and onboarding cloud applications and application suites. Once cloud applications are onboarded, you can create and configure policies for those cloud applications.

We support URLs in the proxy that have 64 or more characters.

## Supported sanctioned cloud applications

Juniper Secure Edge supports the following cloud types:

- Atlassian
- AWS
- Azure
- Box
- Dropbox
- Egnyte
- GitHub
- Google Cloud
- Google Drive
- Now
- OneDrive
- Salesforce
- ServiceNow
- SharePoint
- Slack
- Teams

Support is available for custom applications you create to meet your specific data security needs.

For each cloud application you onboard, you will need to provide a **service account** with login credentials for the managed administrative user of that application. These application-specific login credentials enable the administrator to manage the account details for an application and monitor user activity for it.

### Note

Juniper Secure Edge does *not* store cloud-specific administrator credentials.

## Onboarding process overview

Some onboarding steps vary depending on the cloud you are onboarding and the types of protection you choose. The following overview summarizes the onboarding procedure.

From the Management Console, select **Administration > App Management**.

The screenshot shows the 'App Management' interface with the 'Managed Apps' tab selected. At the top, there's a search bar and a 'New' button. Below that, there are filters for 'Order By' and a search bar. The main area displays a list of 9 items, each with a small icon and a link.

Click **New**. Then, perform the following steps.

## Enter basic information

1. Choose a cloud application type.

The screenshot shows a dropdown menu titled 'Choose an App' with the following options listed:

- Azure
- Box
- SAP C4C
- Cloud Trail
- CMIS (Preview)

2. **(Required)** Enter a name for the new cloud application. Use only alphabetical characters, numbers, and the underscore character (\_). Do **not** use spaces or any other special characters.
3. **(Optional)** Enter a description for the new application.

## For application suites, select applications

If you are onboarding a cloud type that is an **application suite**, you will be prompted to select the applications in that suite that you want to protect. Click the check marks for the applications to include.

## Select protection modes

Depending on the cloud type you chose, some or all of the following protection modes will be available. For suites, the selected protection modes apply to the entire suite.

- **API Access** – Provides an out-of-band approach to data security; performs ongoing monitoring of user activities and administrative functions.
- **Cloud Security Posture** – Used for cloud types for which you want to apply Cloud Security Posture Management functionality.
- **Cloud Data Discovery** -- Used for cloud types for which you want to apply Cloud Data Discovery functionality.
- Select one or more protection modes, depending on the type of protection you want to enable for a cloud. You can create policies for the cloud application based on the protection modes you choose.
- Click **Next**.

## Select configuration settings

You will need to set configuration information for the cloud application you are onboarding. These configuration settings will vary, depending on the cloud type and the protection modes you choose.

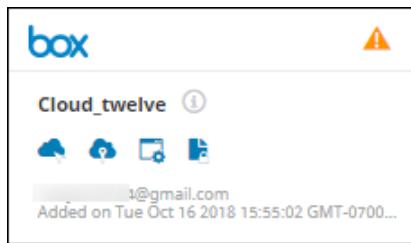
## Enter authorization information

For most protection modes, you will need to go through an authorization step by logging in to the cloud application with your administrator credentials for the account.

## Save the onboarded cloud application

1. Click **Next** to view a summary of information about the new cloud application. The summary shows the cloud type, name and description, the selected protection modes, and other information, depending on the cloud type and selected protection modes for the cloud application.
2. Click **Previous** to correct any information or click **Save** to confirm the information.

The new cloud application is added to the **App Management** page.



The display in the grid shows the following information:

- The **name** of the cloud application.
- A **description** (if provided). To view the description, hover over the information icon next to the cloud application name.
- The **protection modes** available for cloud application. Each icon represents a protection mode. The protection modes you selected for this cloud appear in blue; those not selected for this cloud appear in gray. Hover over each icon to see its protection type.
- The **key assignment status**. The orange icon at the upper right indicates that the application is waiting for a key to be assigned. You can assign a key now or do so later. Once you assign a key to the cloud application, the orange icon is replaced by a green check mark.
- The **user ID** (email address) of the administrator user who onboarded the application.
- The **date and time** the application was onboarded.

The following sections provide instructions for onboarding cloud applications and suites.

## Onboarding Microsoft 365 suite and applications

This section outlines the procedures for onboarding a Microsoft 365 suite and applications and enabling audit logging.

### Note

The following user roles are required for onboarding.

- Office Apps Administrator
- SharePoint Administrator
- Teams Administrator
- Application Administrator

- Cloud Application Administrator
- Guest Inviter
- Privileged Authentication Administrator
- Privileged Role Administrator
- Global Reader
- Compliance Administrator
- Compliance Data Administrator

## Configuration steps

### Microsoft 365 application suite

CASB can provide protection options to the entire suite of Microsoft 365 applications, including Microsoft Teams in addition to OneDrive and SharePoint.

The Microsoft 365 cloud type is an application suite. You can onboard the suite, and then select the applications for which to apply protection. Some configurations, such as key management, will apply to the entire suite and cannot be specified by application. Other configurations can be customized for each application in the suite.

CASB provides a dedicated dashboard for monitoring activity in the Microsoft 365 suite applications. You can select the Microsoft 365 dashboard from the **Monitor** menu.

#### Turning on audit log search and verifying mailbox management by default

For monitoring of applications in the Microsoft 365 suite, you must configure settings for these options:

**Turn on audit log search.** You must turn on audit logging in the Microsoft Security & Compliance Center before you can start searching the Microsoft 365 audit log. Turning on this option enables user and administrator activity from your organization to be recorded in the audit log. The information is retained for 90 days.

For more details and instructions about how to turn on audit log search and turn it off, see

<https://docs.microsoft.com/en-us/office365/securitycompliance/turn-audit-log-search-on-or-off>

### SharePoint / OneDrive

#### Creating sites for new SharePoint or OneDrive users

When new users are added to a SharePoint or OneDrive account, you must perform the following procedure to start monitoring and protecting data in the personal sites for these users. You should also perform a user sync.

Perform the following steps to add sites for new SharePoint or OneDrive users.

1. Log in as the administrator.
2. Go to **Admin > SharePoint admin center > user profiles > My Site Settings > Setup My Sites.**

SharePoint admin center

- site collections
- infopath
- user profiles**
- bcs
- term store

People  
Manage User Properties | Manage User Profiles | Manage User Sub-types | Manage Audiences | Manage User Permissions | Manage Policies

Organizations  
Manage Organization Properties | Manage Organization Profiles | Manage Organization Sub-types

My Site Settings  
Setup My Sites | Configure Trusted Host Locations | Manage Promoted Sites | Publish Links to Office Client Applications | Manage Social Tags and Notes

- Under **Setup My Sites**, check **Enable My Site secondary admin**, and select the admin as the site admin.

Set a secondary owner to receive access in situations in which a user's manager cannot be determined.

**My Site Secondary Admin**

Add a secondary admin for all My Sites.

You can add a user or security group as a second admin to users' My Sites. Typically, the user who the site is being created for is the only site.

Enable My Site secondary admin

Secondary admin:  
[belvita kloud;](#)

- Go to **User Profiles > Manage User Profiles**.

Office 365 Admin

SharePoint admin center

- site collections
- infopath
- user profiles**
- bcs
- term store
- records management

People  
Manage User Properties | **Manage User Profiles** | Manage User Sub-types | Manage Audiences | Manage User Permissions | Manage Policies

Organizations  
Manage Organization Properties | Manage Organization Profiles | Manage Organization Sub-types

My Site Settings  
Setup My Sites | Configure Trusted Host Locations | Manage Promoted Sites | Publish Links to Office Client Applications | Manage Social Tags and Notes

- Under **Manage User Profiles**, right-click the user's profile, and click **Manage site collection owners**. User profiles are not displayed by default. They appear only when you search for them.

SharePoint admin center

Use this page to manage the user profiles in this User Profile Service Application. From this page you can also manage a user's personal site.

Total number of profiles: 7

Find profiles  Find

New Profile | Delete | View: Active Profiles | Manage Sub-types | Select a sub-type to filter the list of profiles: Default User Profile Subtype

Account name	Preferred name
id#:{!j}membership testuser@belvitakloud03.onmicrosoft.com	test2 user
id#:{!j}membership testuser@belvitakloud03.onmicrosoft.com	testuser kloud

**Edit My Profile**

Delete

Manage Personal Site

**Manage site collection owners**

The site admin should now appear in the list of site collection administrators.

**Site Collection Administrators**

Site Collection Administrators are given full control over all Web sites in the site collection. They may also receive site use confirmation mail. Enter users separated by semicolons.

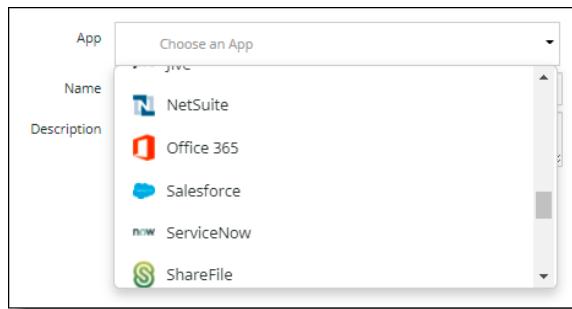
belvita kloud; test2 user;

## Creating a Quarantine site in SharePoint

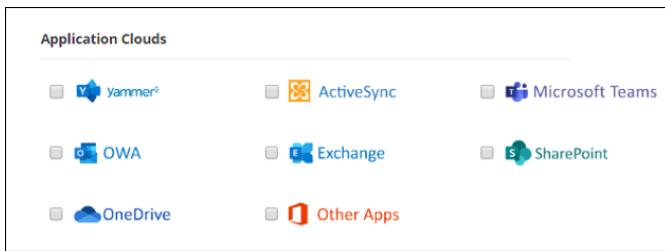
You must create a SharePoint site called **Quarantine-Site** to enable the Quarantine action to work.

## Onboarding steps

1. Go to **Administration > App Management** and click **Add New**.
2. Choose **Office 365**. This is the Microsoft 365 application suite.



3. Click **Next**.
4. Enter a **Name** (required) and a **Description** (optional) for the new cloud application. For the name, use only alphabetical characters, numbers, and the underscore character (\_). Do not use spaces or any other special characters.
5. Select the Microsoft 365 applications in the suite that you want to protect. The named applications are the specific applications that are supported. The **Other Apps** selection includes any unsupported or partially supported applications such as Calendar, Dynamics365, Excel, Word, Planner, Sway, Stream, and Video.



6. Click **Next**.
7. Select one or more **protection modes**. The protection options you see vary, depending on the Microsoft 365 applications you selected in the previous step, and will apply to those applications. You cannot select protection modes for individual applications.

<b>API Access</b>	Available for all Microsoft 365 applications. Must be also enabled if you enable <b>Dynamic</b> or <b>Cloud Data Discovery</b> .
-------------------	---

<b>Cloud Security Posture</b>	Available for all Microsoft 365 applications.  Select this mode if you want to implement Cloud Security Posture Management (CSPM) functionality, also known as SaaS Security Posture Management (SSPM) functionality, for this cloud. For more information about CSPN, see <a href="#">Cloud Security Posture Management (CSPM)</a> .
<b>Cloud Data Discovery</b>	Available for OneDrive and SharePoint applications.  Select this mode if you want to implement Cloud Data Discovery functionality for this application.  Also requires <b>API Access</b> to be enabled.

8. Click **Next**.
9. Enter the following configuration information. The fields you see depend on the protection modes you selected.

The screenshot shows the 'Proxy' configuration section. It includes the following fields:

- Custom HTTP Header Name: Restrict-Access-To-Tenants
- Custom HTTP Header Value: (empty input field)
- Login Domain Prefix: (empty input field)
- Specific Domains: -- Select keywords -- (dropdown menu with edit icon)
- Tenant Identifier Domain Prefix: (empty input field)
- API Settings:
  - Content Collaboration Scan: On (green toggle switch)
  - Internal Domains: (empty input field)

- **Proxy**
  - The **Custom HTTP Header Name** and **Custom HTTP Header Value** fields are configured on the cloud level (as opposed to the cloud application level). If this is the **first** Microsoft 365 cloud application you are onboarding, the values you enter in these two fields will apply to all other Microsoft 365 cloud applications you onboard. If this is **not** the first Microsoft 365 cloud application you are onboarding, these field values will be initialized from the first Microsoft 365 cloud you onboarded.

The remaining fields are configured for the cloud application you are onboarding. Enter values as needed.

- **Login Domain Prefix** -- For example, **companyname.com** (as in <username>@companyname.com)
- **Specific Domains** – Microsoft 365-specific domain names that need to be redirected. Enter or select domains for this cloud application.
- **Tenant Identifier Domain Prefix** -- For example, **casbprotect** (as in **casbprotect.onmicrosoft.com**)
- **API Settings** (required only for API Access protection mode)
  - **Internal Domains** -- Enter one or more internal domains.

- **Content Collaboration Scan** – Toggle is enabled by default. This setting enables events for File CheckIn/CheckOut to be processed. If this toggle is disabled, these events are not processed.
- **Message Aggregation** – Select how to aggregate messages for DLP scanning.
- **Archive Settings** – Enables archiving of files that are either permanently deleted or replaced by Content Digital Rights policy actions. Archived files (including those for SharePoint and Teams) are placed in an **Archive** folder under a **CASB Compliance Review** folder created for the cloud application. You can then review the files and restore them if needed.

#### Notes

- If you onboard Microsoft Teams as a Microsoft 365 application, be sure that an Active Sync directory is created, because the Azure AD is the source of user information. To create a directory, go to **Administration > Enterprise Integration > User Directory**.
- When you change the authorized administrator for a cloud account, if there is any previously archived content in the **CASB Compliance Review** folder that is owned by the previous administrator, you should share it with the new authorized administrator to enable archived data to be reviewed and restored.

The **Archive Settings** option is available for onboarded cloud applications with **API Access** protection mode selected.

Two options are available:

- **Remove from Trash**
- **Archive**

For **Permanent Delete** policy actions, both options are disabled by default; for **Content Digital Rights**, they are enabled by default.

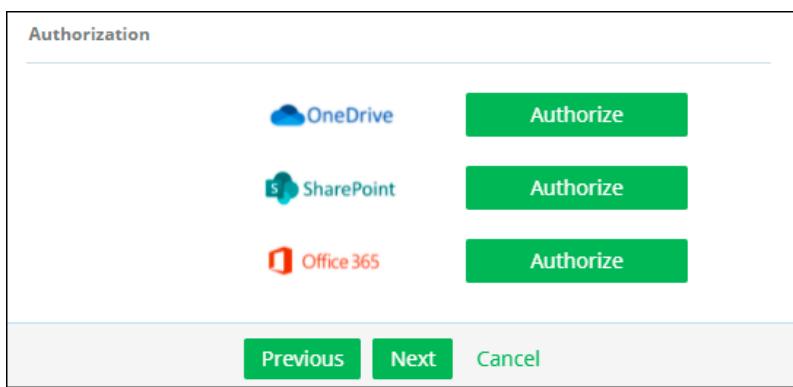
#### Note

For OneDrive cloud applications (Microsoft 365), files for non-administrator user accounts are **not** removed from the Trash when the **Remove from Trash** flag is enabled.

Click the toggles to enable or disable the settings. If you select the **Archive** action, you must also select the **Remove from Trash** option for archiving to be enabled.

Enter the number of days for which to retain archived files. The default value is 30 days.

- **Authorization** -- Authorize the Microsoft 365 components. You will need to provide your Microsoft 365 login credentials when prompted. Click the buttons as follows:
  - **OneDrive and SharePoint** -- Click each **Authorize** button. If you did not select either of these applications earlier, these buttons do not appear.
  - **Office 365** – Clicking **Authorize** authorizes the Office 365 suite components you selected, *except for OneDrive and SharePoint, which must be authorized separately*. This authorization is for monitoring only.



10. Click **Next**.
11. View the summary page to verify that all information is correct. If it is, click **Next**.

The onboarding is complete. The cloud application is added to the list on the **App Management** page.

### Enabling audit logging and managing mailbox auditing

Once you have onboarded a Microsoft 365 suite with applications, you must turn on audit logging in your Microsoft 365 account before you can search the audit log. Event polling will start 24 hours after audit logging is enabled.

For information and instructions regarding about audit logging for Microsoft 365, see the following Microsoft documentation:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/turn-audit-log-search-on-or-off?view=o365-worldwide>

## Microsoft 365 API onboarding with Self-Managed OAuth Application

It is strongly recommended that you use the native OAuth app provided with CASB to onboard the Microsoft 365 application suite, as described above. However, if you prefer, you can use a custom OAuth app for API onboarding. This section describes how to configure a custom app for that purpose.

### Creating a custom application

1. Obtain the Redirect URL for your tenant from the Support team.
2. In the Management Console, go to **Administration > Certificate Management** and select the **Identity Certificates** tab.
3. Locate the certificate whose name starts with “CN=Lookout CASB Application” and click the View icon in the Actions column for that certificate.
4. Click the **Pem Certificate** link and then click the download icon to download the certificate.
5. Log in to your Microsoft Azure administrative portal and go to **App Registrations**. Click **+ New registration**.
6. Enter a name of your choosing for the application.
7. Select **Web** from the platform attribute drop-down and enter the Redirect URL that you obtained in step 1 above. Save the new application.

- Locate the Application ID (aka Client ID) on the Overview page and copy it.

## Configuring the custom application

- Under the **Manage** heading, select **API permissions**.
- Click **Grant admin consent** for your user group.
- Add the necessary permissions. This will depend on which CASB functions you intend to use. See [Permissions needed for custom onboarding app](#) below.
- Under the **Manage** heading, select **Certificates & secrets**. Select the **Client secrets** tab and click **+ New client secret**. Fill in the information as needed. After saving, copy the secret value.

Note: When this secret expires, you will need to update it and then reauthorize your onboarded application in the CASB Management Console.

- While still on the **Certificates & secrets** page, select the **Certificates** tab. Click **Upload certificate** and upload the certificate that you downloaded in step 4 above.
- Copy the Thumbprint value for the certificate.

## Onboarding Microsoft 365 using your new application

You are now ready to onboard the Microsoft 365 suite as described in [Onboarding steps](#) earlier in this section. Keep in mind the following:

- You will need the Client ID (step 8 above), Client Secret (step 12 above), and Certificate Thumbprint (step 14 above).
- Do not select any child applications on the Application Suite page.
- Make sure to select **API Access** as the protection model.
- On the **Configuration** page of the onboarding process, use the **App for API mode authorization** drop-down to select the appropriate option depending on your needs:
  - Custom OAuth App to monitor
  - Custom OAuth App to monitor and detect
  - Custom OAuth App to monitor, detect, and enforce

## Permissions needed for custom onboarding app

The permissions needed by your custom app will depend on how you intend to use CASB with Microsoft 365:

- Monitor only – You will use CASB to monitor your users' Microsoft 365 activity.
- Monitor and detect – You will use CASB to monitor your users' Microsoft 365 activity and detect unauthorized usage.
- Monitor, detect, and enforce – You will also use CASB to take actions on policy violations.

The following table details the permissions needed for each of the above scenarios.

Function	Scope	Permissions needed
Monitor only	Microsoft 365 without Teams	graph:Application:AuditLog.Read.All graph:Delegated:AuditLog.Read.All graph:Application:Application.Read.All mgmt:Delegated:ActivityFeed.Read graph:Delegated:Directory.Read.All graph:Application.User.Read.All graph:Delegated.User.Read.All

		graph:Application.Group.Read.All graph:Application.GroupMember.Read.All graph:Application.Sites.Read.All graph:Application.Directory.Read.All
	Microsoft 365 with Teams	All permissions above, and: graph:Delegated:Chat.Read graph:Application:Chat.Read.All graph:Application:Channel.ReadBasic.All graph:Application:ChannelMessage.Read.All graph:Application:ChannelSettings.Read.All graph:Application:ChatMember.Read.All
Monitor and detect	Microsoft 365 without Teams	graph:Application:AuditLog.Read.All graph:Delegated:AuditLog.Read.All graph:Application:Application.Read.All mgmt:Delegated:ActivityFeed.Read graph:Application:Files.Read.All graph:Delegated:Files.Read.All graph:Application:Sites.Read.All graph:Application:User.Read.All graph:Delegated:User.Read.All graph:Application:Group.Read.All graph:Application:GroupMember.Read.All graph:Delegated:Directory.Read.All graph:Application:Directory.Read.All graph:Application:Organization.Read.All sharepoint:Application:Sites.Read.All
	Microsoft 365 with Teams	All permissions above, and: graph:Delegated:Chat.Read graph:Application:Chat.Read.All graph:Application:Channel.ReadBasic.All graph:Application:ChannelMessage.Read.All graph:Application:ChannelSettings.Read.All
Monitor, detect, and enforce	Microsoft 365 without Teams	graph:Application:AuditLog.Read.All graph:Delegated:AuditLog.Read.All graph:Application:Application.Read.All mgmt:Delegated:ActivityFeed.Read graph:Application:User.Read.All graph:Delegated:User.Read.All graph:Application:Organization.Read.All sharepoint:Application:Sites.FullControl.All sharepoint:Application:TermStore.Read.All graph:Delegated:Sites.Manage.All graph:Application:Sites.Manage.All graph:Application:Directory.ReadWrite.All graph:Delegated:Directory.ReadWrite.All graph:Delegated:Reports.Read.All graph:Application:GroupMember.ReadWrite.All graph:Delegated:Group.ReadWrite.All graph:Application:Group.ReadWrite.All graph:Application:Files.ReadWrite.All graph:Delegated:Files.ReadWrite.All

	Microsoft 365 with Teams	All permissions above, and: graph:Application:Channel.ReadBasic.All graph:Application:ChannelMessage.Read.All graph:Delegated:Chat.ReadWrite graph:Delegated:ChannelMessage.Send graph:Delegated:ChatMember.ReadWrite graph:Application:Chat.ReadWrite.All graph:Application:Chat.UpdatePolicyViolation.All graph:Application:ChannelMessage.UpdatePolicyViolation.All graph:Application:ChannelSettings.ReadWrite.All graph:Application:ChatMember.ReadWrite.All
--	--------------------------	---

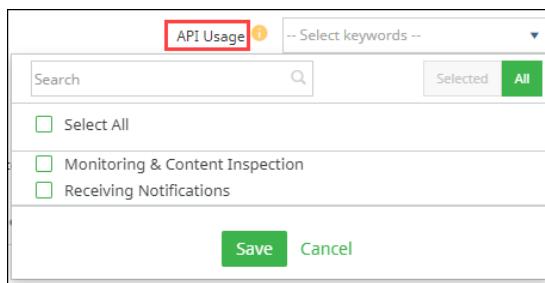
# Onboarding Slack Enterprise applications

This section outlines the procedure for onboarding a Slack enterprise cloud application. For these applications, you can choose several protection modes including **API Access**, which provides expanded access controls that go beyond user IDs, such as denial of logins from non-compliant or compromised devices and from users with patterns of risky behavior.

A non-enterprise Slack application is also available with a smaller number of protection modes.

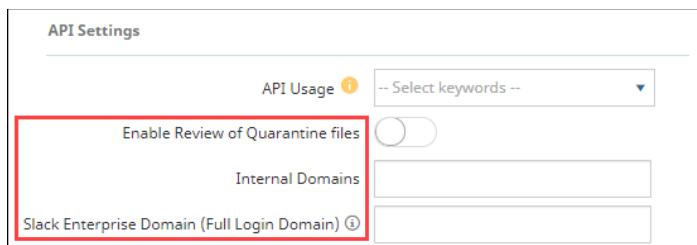
## Onboarding steps

1. Go to **Administration > App Management**.
2. In the **Managed Apps** tab, click **Add New**.
3. Select **Slack Enterprise** and click **Next**.
4. Enter a **Name** (required) and a **Description** (optional). Then click **Next**.
5. Select one or more protection modes.
  - **API Access**
  - **Cloud Data Discovery**
6. Enter the information for the selected protection modes.
  - For **API Settings** – Enter or select the following information:
    - **The API Usage type** -- Defines how this application will be used with API protection. Check **Monitoring & Content Inspection**, **Receiving Notifications**, or **Select All**.



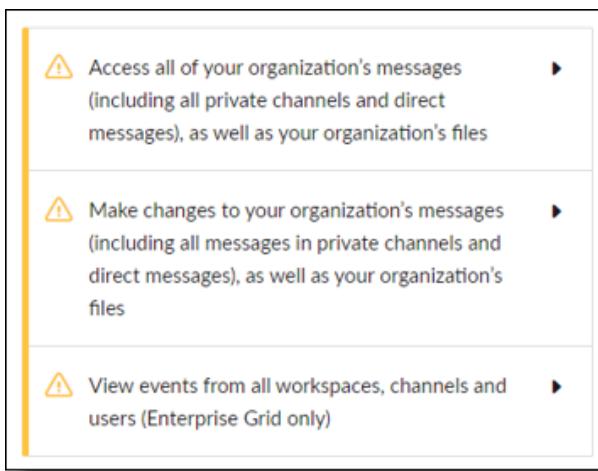
If you select *only Receiving Notifications*, this cloud application is not protected; and will be used only to receive notifications.

- **Enable Review of Quarantine Files** -- Click this toggle to enable reviewing of tombstoned files through the Slack channel.
- **Internal Domains** – Enter any internal domains applicable for this application.
- **Slack Enterprise Domain (Full Login Domain)** -- Enter the full domain for your organization. Example: `https://<name>.enterprise.slack.com`



7. Click **Authorize**. Enter Slack credentials when prompted.
8. Slack displays a prompt requesting that you confirm permissions to access your organization's messages, modify messages, and view elements from workspaces, channels, and users in your organization.

Click **Allow** to confirm these permissions.



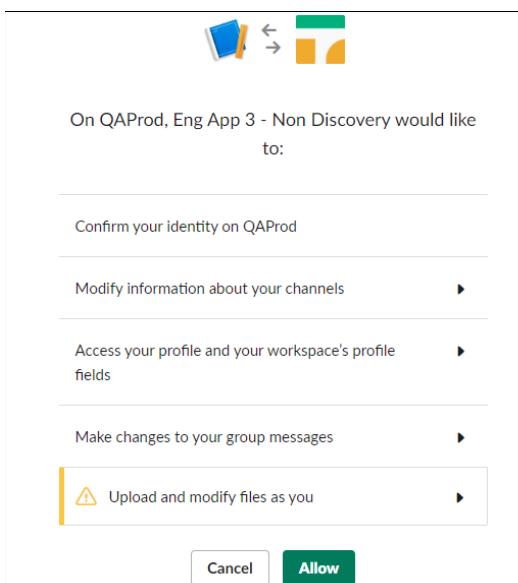
9. Authorize one or more workspaces. Click **Authorize** next to the workspace name to authorize it. At least one workspace must be authorized.
10. When prompted to install the app in the workspace, click **Allow**.

#### Note

If you want to enable additional functionality, each workspace must be onboarded (authorized) separately. If the workspaces are not authorized separately, the following actions will not be supported:

- **Encrypt**
- **Watermark**
- **Removed external shared link**

11. In response to the prompt for non-discovery access, click **Allow**.



12. Click **Next**. The **Key Management** page is displayed.

Request New Key				
KEY NAME	KEY SERVER	DATE CREATED	DATE EXPIRATION	STATUS
Hari	CloudKMS	03/20/2020	03/20/2021	ACTIVE (EXPIRED)
<hr/>				
<a href="#">Previous</a> <a href="#">Next</a> <a href="#">Save</a> <a href="#">Cancel</a>				

13. To request a new key now, click **Request New Key**. The administrator will be notified, and a key will be assigned. Then, click **Save**. If you want to request a new key later, click **Save**.

## Onboarding the AWS suite and applications

This section outlines instructions for onboarding the AWS suite in CASB. You can choose to perform an automated or manual onboarding depending on your needs.

### Automated onboarding

You can onboard the AWS suite automatically using the provided Terraform module.

#### Onboarding with Terraform

1. In the Management Console, select **Administration > System Settings > Downloads**.
2. Locate the file **aws-onboarding-terraform-module-<version>.zip** and download it.
3. Extract the contents of the zip file.

4. Locate and open the file **README-Deployment steps.pdf**.
5. Follow the instructions provided in the README file to complete the automated onboarding.

## Manual onboarding

This section outlines instructions for configuring the AWS suite for manual onboarding in CASB, followed by the manual onboarding instructions.

### Configuration steps

Before you onboard the AWS application, you must perform a set of configuration steps.

**Note:** These configuration steps are only necessary if you plan to onboard AWS in API mode.

To get started, log in to the AWS console (<http://aws.amazon.com>).

Then, perform the following configuration steps.

- Step 1 – Create an Identity Access Management (IAM) role for Juniper CASB
- Step 2 – Create a Cloud Trail
- Step 3 – Create Simple Queue Service (SQS)
- Step 4 – Configure Event Notifications for the Cloud Trail Bucket
- Step 5 – Create an IAM Monitor policy
- Step 6 – Create an IAM DLP policy
- Step 7 – Create an IAM Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) policy
- Step 8 – Create an IAM Key Management Service (KMS) policy
- Step 9 – Attach the policies to the IAM role

### Step 1 – Create an Identity Access Management (IAM) role for Juniper CASB

1. Click **Roles** and select **Create role**.
2. Select **Role Type: Another AWS Account**.
3. **For Account ID**, obtain this ID from the Juniper Networks team. This is the account ID for the AWS account in which the tenant Management Server is onboarded.
4. Under **Options**, check **Require External ID**.
5. Enter the following information:
  - **External ID** – Enter a unique attribute to be used while onboarding AWS S3 in CASB.
  - **Require MFA** – Do not check.
6. Click **Next: Permissions**. Do not attach any policies at this point.
7. Click **Next: Tags** and (optional) enter any tags you want to include to the **Add Tags** page.
8. Click **Next: Review**.
9. Enter a **Role Name** (for example, **Juniper-AWS-Monitor**) and click **Create Role**.
10. Search for the role name you created and click it.

11. Copy the role ARN.
12. Select **Roles > Trust relationships** tab > **Juniper-AWS-Monitor** summary view. Locate the **Conditions** section and copy the **ExternalID** value.

## Step 2 – Create a Cloud Trail

1. From **Services**, go to **Cloud Trail**.
2. Select **Trails** from the left panel.
3. Click **New Trail** and enter the following information.
  - **Trail name** – **ccawstrail** (for example)
  - **Storage location** – Select **Create a new S3 bucket** to create a new bucket or **Use existing S3 bucket** to pick up existing buckets in which to store logs. Enter or select the desired bucket name.
4. Click **Next**. The **Choose log events** screen is displayed.
  - **Events** – Select **Management events** and (optionally) **Data events**.
  - **Management Events** – Select **Read** and **Write**.
  - **Data Events** (optional) – Configure data events if you want to see activity audit logs and AWS monitoring screens.
5. Click **Next**.
6. Click **Create Trail**.
7. Copy the Cloud Trail ARN and S3 Bucket ARN.

## Step 3 – Create Simple Queue Service (SQS)

1. Under **Services**, go to **Simple Queue Service (SQS)**.
2. Click **Create New Queue**.
3. Enter a **Queue Name** and select **Standard Queue** as the queue type.
4. Click **Create Queue**.
5. Copy the new queue's ARN.
6. Go to the **Access Policy** section.
7. Click the **Edit** button and paste the following policy information.

```
{
  "Version": "2008-10-17",

  "Id": " default_policy_ID",
  "Statement": [
    {
      "Sid": "__receiver_statement",
      "Effect": "Deny",
      "Principal": {
        "AWS": "<<Role_ARN>>"
      },
    }
  ]
}
```

```

    "Action": [
        "sns:ReceiveMessage",
        "sns:ChangeMessageVisibility",
        "sns:DeleteMessage"
    ],
    "Resource": "<<Queue_ARN>>",
    "Condition": {
        "ArnNotEquals": {
            "aws:PrincipalArn": "<<Role_ARN>>"
        }
    },
    {
        "Sid": "__sender_statement",
        "Effect": "Allow",
        "Principal": {
            "Service": "s3.amazonaws.com"
        },
        "Action": "sns:SendMessage",
        "Resource": "<<Queue_ARN>>",
        "Condition": {
            "ArnEquals": {
                "aws:SourceArn": "<<S3_Bucket_ARN>>"
            }
        }
    }
]
}

```

In the above code, make sure to replace all of the strings in double brackets ( <>> ) with the appropriate values:

8. Replace <<Role\_ARN>> with the role ARN that you copied at the end of [Step 1 – Create an IAM role for Juniper CASB](#).
9. Replace <<Queue\_ARN>> with the queue ARN that you copied in step 5 of this section.
10. Replace <<S3\_Bucket\_ARN>> with the bucket ARN that you copied at the end of [Step 2 – Create a Cloud Trail](#).
11. Click **Create Queue**.

## Step 4 – Configure Event Notifications for the Cloud Trail Bucket

1. Under **Buckets**, go to the bucket that stores the CloudTrail logs (for example, **awstrailevents**).
2. Click the **Properties** tab for the bucket.
3. Go to the **Event Notifications** section and click **Create event notification**.
4. Enter the following information for the notification.
  - **Name** – any naming (for example, SQS Notification)
  - **Event Types** – Select **All object create events**.
  - **Filters** - Enter any filters to apply to the notification.

- **Destination** – Select **SQS Queue**.
- **Specify SQS Queue** – Select the SQS queue that you created in [Step 3 – Create Simple Queue Service](#).

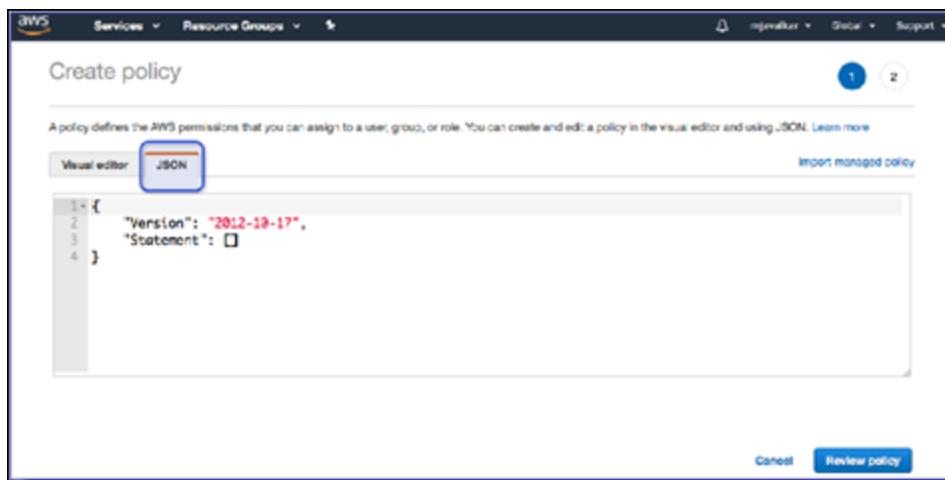
Note: Make sure that your S3 Bucket and SQS queue are in the same region.

#### 5. Click **Save Changes**.

The event is created.

### Step 5 – Create an IAM Monitor policy

1. Click **Services** and select **IAM**.
2. Select **Policies** and click **Create Policy**.
3. Click the **JSON** tab.



#### 4. Copy and paste the following policy information.

```
{
  "Statement": [
    {
      "Action": [
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "iam:Get*",
        "iam>List*",
        "s3:AbortMultipartUpload",
        "s3>DeleteObject",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketNotification",
        "s3:GetObject",
        "s3>ListAllMyBuckets",
        "s3>ListBucket",
        "s3>ListMultipartUploadParts",
        "s3:PutObject"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

```

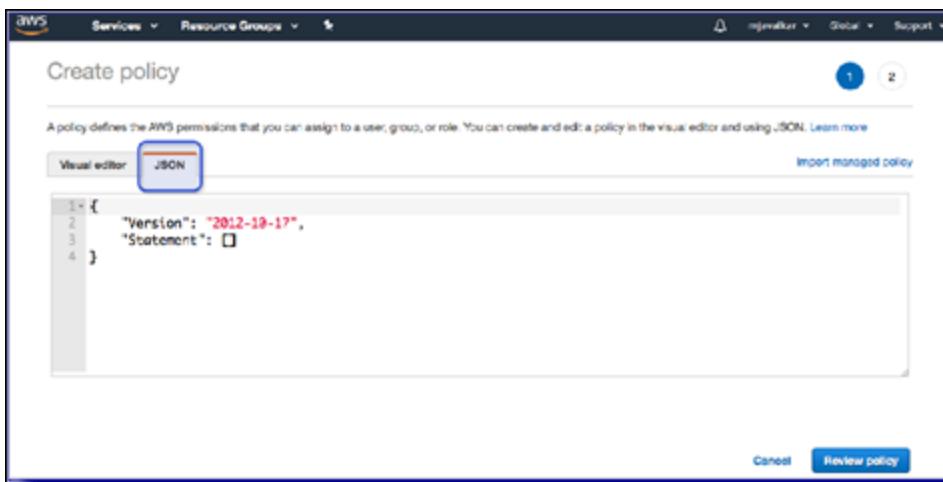
        "s3:PutBucketAcl",
        "s3:PutBucketNotification",
        "s3:PutObject",
        "s3>ListBucketMultipartUploads"
    ],
    "Effect": "Allow",
    "Resource": "*",
    "Sid": "CasbAwsMonitorPolicy"
}
],
"Version": "2012-10-17"
}

```

5. Click **Review Policy** at the lower right portion of the screen.
6. Give the policy the name **iam-monitor-policy** and click **Create Policy**.

## Step 6 – Create an IAM DLP policy

1. Click **Services** and select **IAM**.
2. Select **Policies** and click **Create Policy**.
3. Click the **JSON** tab.

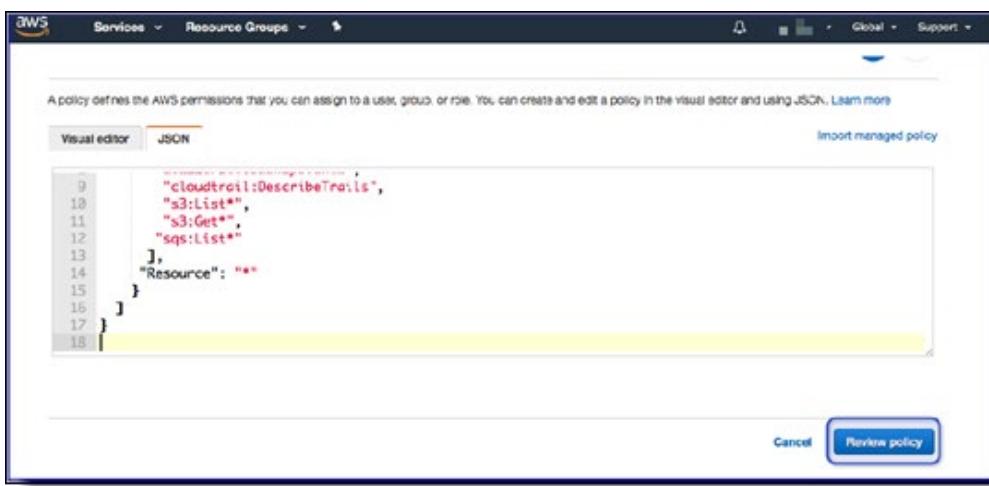


4. Copy and paste the following policy information.

```
{
  "Statement": [
    {
      "Action": [
        "iam:GetUser",
        "iam>ListUsers",
        "iam:GetGroup",
        "iam>ListGroups",
        "iam>ListGroupsForUser",
        "s3>ListAllMyBuckets",
        "s3:PutObject"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

```
    "s3:GetBucketNotification",
    "s3:GetObject",
    "s3:GetBucketLocation",
    "s3:PutBucketNotification",
    "s3:PutObject",
    "s3:GetObjectAcl",
    "s3:GetBucketAcl",
    "s3:PutBucketAcl",
    "s3:PutObjectAcl",
    "s3:DeleteObject",
    "s3>ListBucket",
    "sns>CreateTopic",
    "sns:SetTopicAttributes",
    "sns:GetTopicAttributes",
    "sns:Subscribe",
    "sns:AddPermission",
    "sns>ListSubscriptionsByTopic",
    "sns>CreateQueue",
    "sns:GetQueueUrl",
    "sns:GetQueueAttributes",
    "sns:SetQueueAttributes",
    "sns:ChangeMessageVisibility",
    "sns>DeleteMessage",
    "sns:ReceiveMessage",
    "cloudtrail:DescribeTrails"
],
"Effect": "Allow",
"Resource": "*",
"Sid": "CasbAwsDlpPolicy"
}
],
"Version": "2012-10-17"
}
```

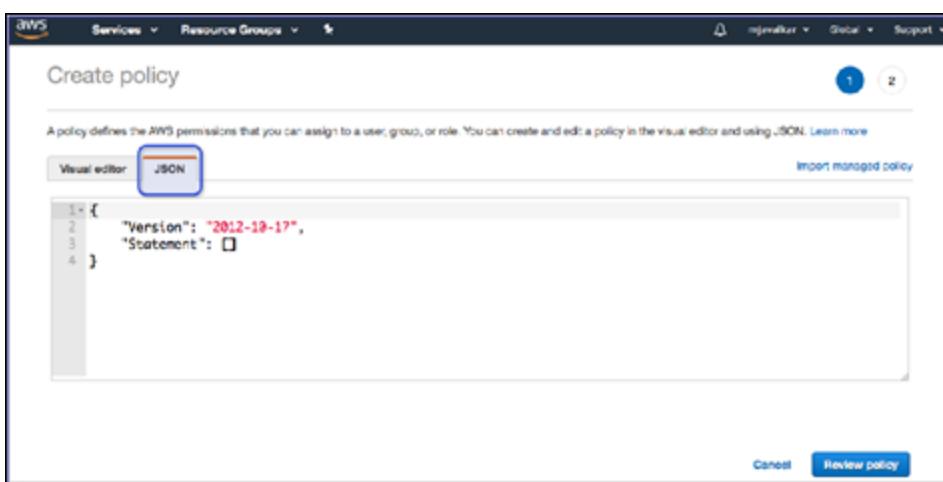
5. Click **Review Policy** at the lower right portion of the screen.



6. Name the policy **iam-api-policy** and click **Create Policy**.

## Step 7 – Create an IAM Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) policy

1. Click **Services** and select **IAM**.
2. Select **Policies** and click **Create Policy**.
3. Click the **JSON** tab.



4. Copy and paste the following policy information:

```

{
  "Statement": [
    {
      "Action": [
        "account:*",
        "cloudhsm:AddTagsToResource",
        "cloudhsm:DescribeClusters",

```

```
"cloudhsm:DescribeHsm",
"cloudhsm>ListHsms",
"cloudhsm>ListTags",
"cloudhsm>ListTagsForResource",
"cloudhsm:TagResource",
"cloudtrail:AddTags",
"cloudtrail:DescribeTrails",
"cloudtrail:GetEventSelectors",
"cloudtrail:GetTrailStatus",
"cloudwatch:DescribeAlarms",
"cloudwatch:DescribeAlarmsForMetric",
"cloudwatch:TagResource",
"config:Describe*",
"dynamodb>ListStreams",
"dynamodb:TagResource",
"ec2>CreateTags",
"ec2:Describe*",
"ecs:DescribeClusters",
"ecs>ListClusters",
"ecs:TagResource",
"elasticbeanstalk>AddTags",
"elasticfilesystem>CreateTags",
"elasticfilesystem:DescribeFileSystems",
"elasticloadbalancing>AddTags",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTags",
"glacier>AddTagsToVault",
"glacier>ListVaults",
"iam:GenerateCredentialReport",
"iam:Get*",
"iam>List*",
"iam:PassRole",
"kms:DescribeKey",
"kms>ListAliases",
"kms>ListKeys",
"lambda>ListFunctions",
"lambda:TagResource",
"logs:DescribeLogGroups",
"logs:DescribeMetricFilters",
"rds>AddTagsToResource",
"rds:DescribeDBInstances",
"redshift>CreateTags",
"redshift:DescribeClusters",
"s3:GetBucketAcl",
"s3:GetBucketLocation",
"s3:GetBucketWebsite",
"s3>ListAllMyBuckets",
"s3>ListBucket",
```

```

    "s3:PutBucketTagging",
    "sdb>ListDomains",
    "secretsmanager>ListSecrets",
    "secretsmanager>TagResource",
    "sns:GetTopicAttributes",
    "sns>List*",
    "tag:GetResources",
    "tag:GetTagKeys",
    "tag:GetTagValues",
    "tag:TagResources",
    "tag:UntagResources"
],
"Effect": "Allow",
"Resource": "*",
"Sid": "CasbAwsCspmPolicy"
}
],
"Version": "2012-10-17"
}

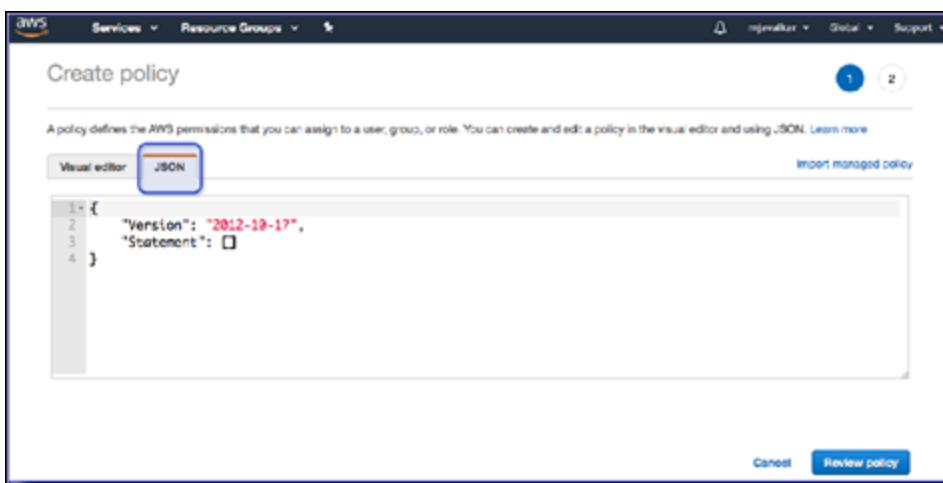
```

5. Click **Review Policy**.
6. Give the policy the name **iam-cspm-policy** and click **Create Policy**.

## Step 8 – Create an IAM Key Management Service (KMS) policy

Perform the following steps if the S3 bucket has KMS enabled.

1. Click **Services** and select **IAM**.
2. Select **Policies** and click **Create Policy**.
3. Click the **JSON** tab.



4. From an S3 bucket, obtain the KMS key for the KMS policy information.
  - a. Click an S3 bucket.

- b. Click **Bucket Properties**.
  - c. Scroll to the default encryption section and copy the AWS KMS key ARN.
- If different keys are assigned to buckets, you will need to add them under **Resource** in the policy information (step 5).
5. Copy and paste the following policy information:

```
{
    "Sid": "VisualEditor0",
    "Effect": "Allow",
    "Action": [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ReEncryptTo",
        "kms:DescribeKey",
        "kms:ReEncryptFrom"
    ],
    "Resource": ["<AWS_KMS_key_ARN>"]
}
```

6. Click **Review Policy**.
7. Give the policy the name **iam-kms-policy** and click **Create Policy**.

### Step 9 – Attach the policies to the IAM role

1. In the AWS console, go to **Services** and select IAM.
2. Select **Roles** and search for the role that you created in [Step 1 – Create an IAM role for Juniper CASB](#).
3. Click on that role and go to the **Permissions** tab.
4. Under **Add permissions**, select **Attach policies**.
5. Select the policies that you created in steps 5, 6, 7, and 8 earlier.
6. Save the role.

## Onboarding steps

1. In the Juniper Management Console, go to **Administration > App Management** and click **New**.

2. Select **AWS** from the dropdown list.
3. Enter a **Name** (required) and a **Description** (optional) and click **Next**.
4. For the application, check **Amazon Web Services** and click **Next**.
5. Select one or more of the following **protection models** by clicking the toggle for each protection model to include.
  - **Cloud Authentication**
  - **API Access**
  - **Cloud Security Posture**
6. Click **Next**.

### Notes

- To onboard AWS in API mode, choose **API Access**.
- **CSPM and SSPM** provides tools to monitor resources used in your organization and assess security risk factors against security best practices for AWS cloud applications. To enable use of CSPM/SSPM, you must choose **Cloud Security Posture** as a protection mode.

7. If you selected **API Access**:
  - a. Click the **AWS Monitoring** toggle and enter the following information in the **API** section of the **Configuration** page. This is the information you had generated in Step 2 of the configuration steps (Create an Identity Access Management (IAM) role for CASB).
    - i. **External ID**
    - ii. **Role ARN**

iii. **SQS Queue Name and SQS Region** (see Step 6 – Create Simple Queue Service [SQS])

The screenshot shows the 'Authentication' section of the AWS CloudFormation Onboarding process. It includes the following fields:

- AWS Monitoring:** A toggle switch that is turned on.
- Account Credentials:**
  - External Id:** An input field.
  - Role ARN:** An input field.
- Proxy:**
  - Specific Domains:** An input field with placeholder text '-- Enter Domain values --' and a pencil icon.
  - Tenant Identifier Domain Prefix:** An input field.
- API Settings:**
  - SQS Queue Name:** An input field.
  - SQS Region:** A dropdown menu with placeholder text '-- Select --' and a downward arrow.
- Authorization:**
  - An AWS logo icon.
  - A green button labeled **Authorize**.

- b. In the **Authentication** section, click the **Authorize** button and click **Next**.

A popup message appears prompting you to confirm that the required policies (according to the selected protection modes) are assigned to the role.

**Note:** Be sure your browser is configured to allow pop-ups to be displayed.

- c. Click **Continue** to confirm that the required policies are displayed.

When the authorization is complete, a green checkmark appears next to the **Authorize** button, and the button label now reads **Re-Authorize**.

- d. Click **Next** to display a summary of the onboarding settings.

- e. Click **Save** to complete onboarding.

The new cloud application is displayed as a tile on the **App Management** page.

## Onboarding Azure applications

This section outlines the procedures for onboarding Azure cloud applications. For Azure Blob Storage onboarding instructions, see the next section.

### Configuration steps

To use the CSPM/SSPM feature for an Azure account, you need a Service Principal that has access to the corresponding subscription.

The Service Principal should have the **Reader** or **Monitoring Reader** role with access to **Azure AD user, group, or service principal** and associated **Client Secret**.

Before onboarding, you should have the **Subscription ID** of the account, and the following information from the Service Principal:

- **Application (Client) ID**
- **Client Secret**
- **Directory (Tenant) ID**

### Onboarding steps

1. From the Management Console, select **Administration > App Management**, and click **Add New**.
2. Select **Azure**. Then, enter the details for the application.
3. Enter a **Name** (required) and a **Description** (optional). The name must include only alphanumeric characters, with no special characters other than the underscore, and no spaces. Then, click **Next**.
4. Select one or more of the following protection modes for the application and click **Next**.
  - **Cloud Authentication**
  - **API Access**
  - **Cloud Security Posture**

The **Cloud Security Posture** mode is required if you want to implement CSPM/SSPM functionality.

5. Depending on the protection modes you selected, enter the required configuration details.

CSPM Settings	
Service Principal's Application Id	<input type="text"/>
Service Principal's Client Secret	<input type="text"/>
Service Principal's Directory Id	<input type="text"/>
Subscription Id	<input type="text"/>
Sync Interval(1-24 Hrs)	<input type="text"/>

- If you selected **App Authorization**, no additional configuration is required. Click **Next** to view the summary information.
- If you selected **API Access**, no additional configuration is needed other than authorization. Go to the **Authorization** step.

- If you selected **Cloud Security Posture**, enter the following information from the Azure configuration steps you performed earlier.
    - **Service Principal's Application Id**
    - **Service Principal's Client Secret**
    - **Service Principal's Directory Id**
    - **Subscription Id**
    - **Sync Interval (1-24 Hrs)** is how often (in hours) that CSPM/SSPM will retrieve information from the cloud and refresh the inventory. Enter a number.
6. Click **Authorize** and enter your Azure login credentials.
  7. Review the summary information to verify that it is correct. If it is, click **Save** to complete onboarding.

# Onboarding Azure Blob applications

This section outlines the procedures for onboarding Azure Blob Storage cloud applications.

## Notes

- Juniper Secure Edge does not support Azure Data Lake Storage generation 2 storage accounts. Juniper is unable to log activity or take actions on blobs using this storage type.
- Juniper Secure Edge does not support content-related actions on immutable containers, due to retention and legal hold policies enforced by Azure.

## Configuration steps

In preparation for onboarding Azure Blob, do the following:

- Ensure that you have an active Azure account and that you have the Subscription ID of the account.
- Ensure that your Azure subscription has at least one storage account with the storageV2 type.
- Ensure that you have a storage account to use for quarantine actions. You will be prompted to select the storage account during onboarding. You can use an existing storage account, or, if you prefer, create a new dedicated storage account for quarantine.
- Create a new custom role at the subscription level, and assign it to an admin account. This will be used for authorization on the Management Console. See details for this step below.
- Ensure that your Azure account has the EventGrid resource registered. See details for this step below.

## Creating a custom role

- Copy the following code into a new text document.

```
{
  "properties": {
    "roleName": "casbrole",
    "description": "CASB role",
    "assignableScopes": [
      "/subscriptions/<Subscription-ID>"]
    },
    "permissions": [
      {
        "actions": [
          "Microsoft.Storage/storageAccounts/read",
          "Microsoft.Storage/storageAccounts/encryptionScopes/read",
          "Microsoft.Storage/storageAccounts/blobServices/read",
          "Microsoft.Storage/storageAccounts/blobServices/containers/read",
          "Microsoft.Storage/storageAccounts/blobServices/containers/write",
          "Microsoft.Storage/storageAccounts/blobServices/containers/immutabilityPolicies/read",
          "Microsoft.Storage/storageAccounts/queueServices/read",
          "Microsoft.Storage/storageAccounts/queueServices/queues/write",
          "Microsoft.EventGrid/eventSubscriptions/delete",
          "Microsoft.EventGrid/eventSubscriptions/read",
          "Microsoft.EventGrid/eventSubscriptions/write",
          "Microsoft.Storage/storageAccounts/write",
          "Microsoft.Storage/storageAccounts/listkeys/action",
          "Microsoft.EventGrid/systemTopics/read",
          "Microsoft.EventGrid/systemTopics/write",
          "Microsoft.Insights/eventtypes/values/Read",
          "Microsoft.Storage/storageAccounts/blobServices/providers/Microsoft.Insights/diagnosticsSettings/read"
        ],
        "notActions": [],
        "dataActions": [
          "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read",
          "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write",
          "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/delete"
        ]
      }
    ]
}
```

```

    accounts/blobServices/containers/blobs/add/action", "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/filter/action", "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/move/action", "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/permanentDelete/action"
    , "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/deleteBlobVersion/action", "Microsoft.Storage/storageAccounts/queueServices/queues/messages/read", "Microsoft.Storage/storageAccounts/queueServices/queues/messages/delete"], "notDataActions": []}]}}

```

2. Replace the text "<Subscription-ID>" with the subscription ID for your Azure account. If desired, you can also replace the roleName and description values.
3. Save the text file with a .json extension.
4. In the Azure console, **navigate to Azure Subscription > Access Control (IAM)**.
5. Click **Add** and select **Add custom role**.
6. For **Baseline Permissions**, select **Start from JSON**.
7. Use the file browser to select and upload the .json file that you saved in step 2 above.
8. If needed, enter or update the name and (optional) description of your new role.
9. Select **Review + Create** to see all settings for your new role.
10. Click **Create** to finish creating the new role.
11. Assign the new role to a user with admin permissions on your Azure account.

## Registering the EventGrid resource

1. In the Azure console, navigate to **Azure Subscription > Resource Providers**.
2. Use the filter field to search for Microsoft.EventGrid. Select it and click **Register**.

## Onboarding steps

1. From the Management Console, select **Administration > App Management** and click **+New**.
2. Select **Azure**. Enter a **Name** (required) and a **Description** (optional). The name must include only alphanumeric characters, with no special characters other than the underscore, and no spaces. Click **Next**.
3. Select **Microsoft Azure Blob Storage** and click **Next**.
4. Select **API Access** (required). If needed, you can also select **Cloud Security Posture** (optional). Click **Next**.
5. For both Azure and Azure Blob Storage, click the **Authorize** button and enter the credentials for the account that you assigned your new role to in the previous section. If prompted, click **Accept** to give Juniper permissions on your Azure account.
6. After you have authorized both accounts, the **Subscription Id** field appears. Select your Azure subscription.

7. The **Destination Storage Account** field appears. Select the storage account that you want to use as a quarantine container.
8. Click **Next**.
9. Ensure that the details shown on the summary page are correct. If they are, click **Next** to finish onboarding.

## Onboarding the Google Workspace suite and applications

This section outlines the procedures for onboarding Google Workspace (formerly G Suite) along with Google Drive applications.

### Configuration steps

The enterprise account used for Google Drive must be part of the Google Workspace business plan.

The authenticated user must be an administrator with super admin privileges.

### Updating API access settings

1. Log in to the Google Workspace application and click **Security** from the left panel.

The screenshot shows the Google Admin interface. The left sidebar has a navigation menu with 'Home', 'Dashboard', 'Directory', 'Devices', 'Apps', 'Security' (which is expanded), 'Settings', 'Alert center', and 'API controls' (which is highlighted with a red box). The 'Security' section contains links for 'Data protection', 'Security rules', and 'Reporting'. The main content area is titled 'API controls' and describes how to enable or restrict access to Google Workspace APIs. It features a checkbox for 'Trust internal, domain-owned apps' (which is checked) and a link to the 'Google Workspace Marketplace'. At the bottom, there are 'CANCEL' and 'SAVE' buttons. Below this is another section titled 'Domain wide delegation' with a 'MANAGE DOMAIN WIDE DELEGATION' button.

2. Under **Security**, click **API controls**.
3. Scroll down and click **Manage Domain-wide Delegation**.

The screenshot shows the Google Admin interface under the 'API Controls' section. The 'Domain-wide Delegation' tab is selected. On the left, there's a sidebar with various admin tools like Home, Dashboard, Directory, Devices, Apps, Security, Settings, and Alert center. The 'API controls' item is highlighted with a red box. The main area shows a table of API clients with two entries. The first entry has columns: Name (CipherCloud...), Client ID (10241585325...), and Scopes (./auth/activity, ./auth/admin.directory.group, +6 More). The second entry has similar columns. There are 'View details', 'Edit', and 'Delete' buttons for each row.

- Click **Add New**.

This is a modal dialog titled 'Add a new client ID'. It contains a 'Client ID' input field, an unchecked checkbox for 'Overwrite existing client ID', and an 'OAuth scopes (comma-delimited)' input field. At the bottom are 'CANCEL' and 'AUTHORIZE' buttons, with 'AUTHORIZE' highlighted by a red box.

- Enter the **Client ID**:

**102415853258596349066**

- Enter the following **OAuth scopes**:

```
https://www.googleapis.com/auth/activity,
https://www.googleapis.com/auth/admin.directory.group,
https://www.googleapis.com/auth/admin.directory.user,
https://www.googleapis.com/auth/admin.reports.audit.readonly,
https://www.googleapis.com/auth/drive,
https://www.googleapis.com/auth/drive.activity.readonly,
https://www.googleapis.com/auth/admin.directory.user.security,
https://www.googleapis.com/auth/userinfo.email
```

- Click **Authorize**.

## Updating folder access information

- From the left panel, click Apps > Google Workspace > Drive and Docs.

The screenshot shows the Google Admin interface with the following details:

- Left Panel:** Shows the navigation tree under "Apps". The "Drive and Docs" option is selected and highlighted with a red box.
- Top Bar:** Shows the title "Google Admin" and a search bar "Search for users, groups or settings".
- Current View:** "Apps > Google Workspace > Settings for Drive and Docs".
- Right Panel:**
  - Service status:** ON for everyone.
  - Sharing settings:** Set global policies for sharing files outside your organization, and define the default link sharing visibility of new files.
  - Migration Settings:** Set who can migrate individual files into shared drives.
  - Manage shared drives:** Manage membership of all shared drives.

- Scroll down and click **Features and Applications**.

The screenshot shows the "Features and Applications" section of the Google Admin interface:

- Left Panel:** Shows the "Drive and Docs" icon.
- Right Panel:** The title "Features and Applications" is highlighted with a red box. Below it, the text "Manage which features and applications are available to users in your organization." is visible.

- Make sure that **Drive SDK** is on.

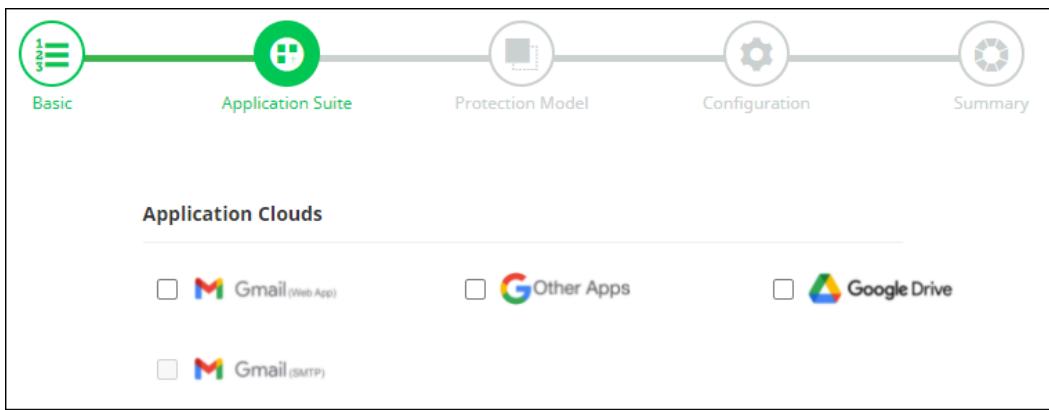
The screenshot shows the "Features and Applications" list in the Google Admin interface:

- Left Panel:** Shows the "Drive and Docs" icon and a sidebar with "Users", "Groups", and "Organizational Units".
- Right Panel:** A list of features:
  - Smart Compose**: Allow users to see Smart Compose suggestions. Status: ON.
  - Google Drive for desktop**: Allow Google Drive for desktop in your organization. Status: ON.
  - Drive**: Allow users to download, install, and use Backup and Sync. Status: ON.
  - Drive SDK**: Allow users to access Google Drive with the Drive SDK API. Status: ON. This item is highlighted with a red box.

## Onboarding steps in CASB

- From the Management Console, select **Administration > App Management** and click **New**.
- Select **Google Workspace** from the list.

3. Enter a **Name** (required) and a **Description** (optional). The name must include only alphanumeric characters, with no special characters other than the underscore, and no spaces. Then, click **Next**.
4. Select Google Drive application.



5. Click **Next** and select one or more **protection models**.

The available protection models depend on the applications you selected in the previous step. The following table lists the protection modes available for each Google Workspace application.

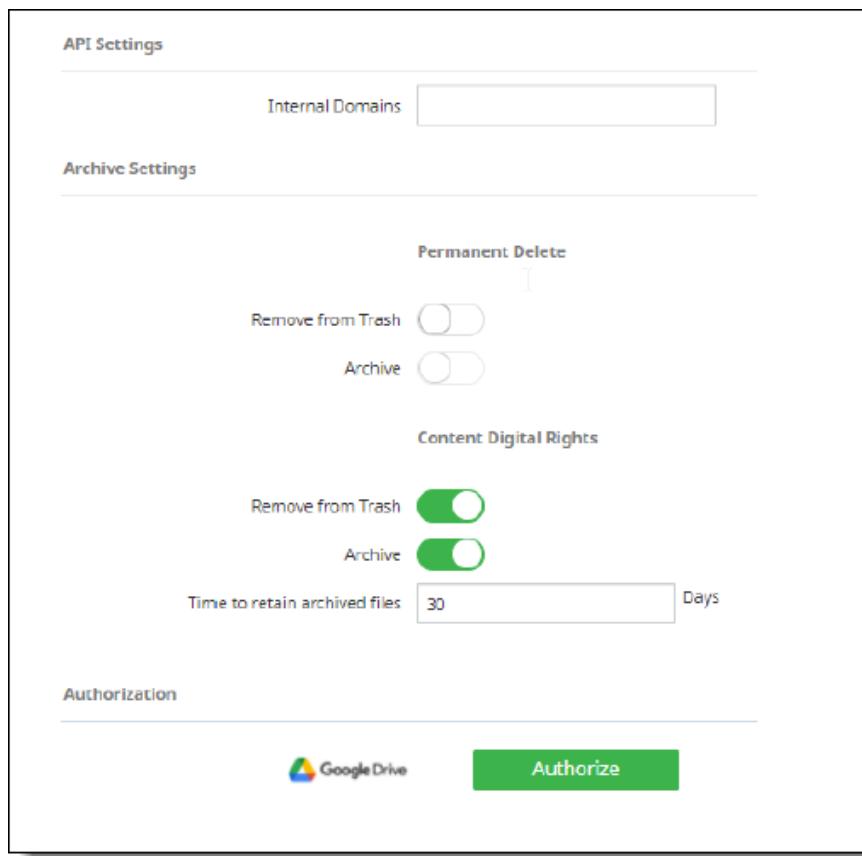
Google Workspace application	Protection models available
Google Drive	API Access Cloud Data Discovery

#### Note

Some protection models require one or other models to be enabled or must be selected for specific functions.

You must select **Cloud Data Discovery** if you want to implement Cloud Data Discovery (CDD) for this cloud application. You must also select **API Access** protection mode in this case.

6. Click **Next**.
7. Enter the following configuration information. The fields you see depend on the protection modes you selected.
  - **API Settings** (required for **API Access** protection mode)



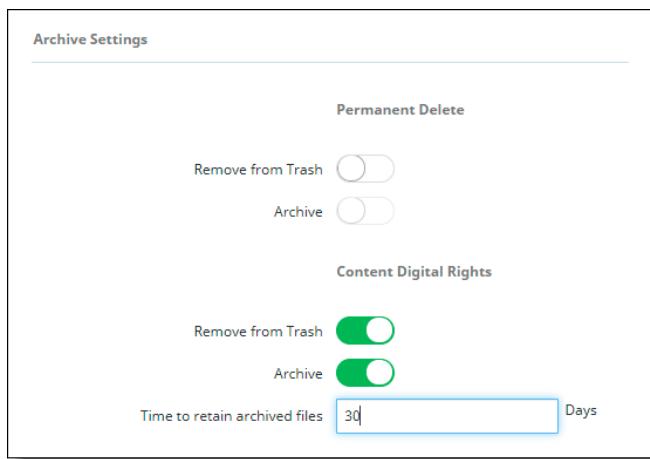
- **Internal domains** – Enter necessary internal domains, along with enterprise business domain.
- **Archive Settings** (for Google Drive) -- Enables archiving of files that are either permanently deleted or replaced by Content Digital Rights policy actions. Archived files are placed in an **Archive** folder under a **CASB Compliance Review** folder created for the cloud application. You can then review the files and restore them if needed.

#### Note

When the authorized administrator for a cloud account is changed in CASB, previously archived content in the **CASB Compliance Review** folder that is owned by the previous administrator should be shared with the new authorized administrator to enable archived data to be reviewed and restored.

Two options are available:

- **Remove from Trash**
- **Archive**

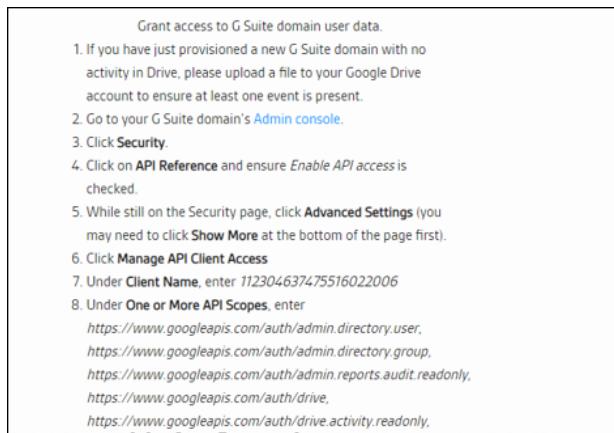


For **Permanent Delete** policy actions, both options are disabled by default; for **Content Digital Rights**, they are enabled by default.

Click the toggles to enable or disable the settings.

Enter the number of days for which to retain archived files. The default value is 30 days.

- **Authorization** -- If you selected Google Drive as one of your Google Workspace applications, authorize Google Drive and click **Next**.



Review the instructions in the screen that appears and click **Continue** to authorize access to your Google Drive account. Enter your account credentials.

In the **Summary** page, review the summary information to verify that all information is correct. If it is, click **Save** to complete onboarding.

# Onboarding Google Cloud Platform (GCP)

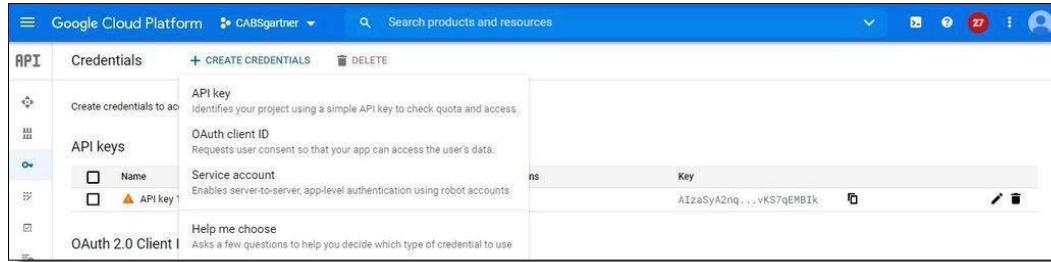
This section outlines procedures for configuration and onboarding of Google Cloud Platform applications.

## Configuration steps

1. Create a service account in GCP Org. You need a service account for enabling CSPM/SSPM. Follow these steps to create a service account.
  - a. In the GCP Console, Select the **IAM and admin** tile > **Service accounts**, and click **Create Service Account**.
  - b. Click the **CREATE AND CONTINUE** button.
  - c. For this service account, provide access to the project and assign a role as Viewer, and click **CONTINUE**.
  - d. Skip the **Grant Users access to this service account**.
  - e. Click **DONE**. Go to the service accounts page.
  - f. Click on the service account which you created for CSPM/SSPM.
  - g. Go to the **KEYS** section, from the ADD KEY dropdown, select **Create new key**.
  - h. Select the Key type as **JSON** and click **CREATE**.

A JSON file will be downloaded. You must upload this file while onboarding the app in the Management Console when you need to specify the Service Accounts Credentials (JSON).

2. Create an OAuth client ID. The OAuth client app is required for enabling GCP monitoring.
  - a. In the Google Cloud Platform, go to the **Credentials** page.



- b. From the **Projects** list, select the project containing your API.
  - c. From the **Create Credentials** dropdown list, select **OAuth client ID**.

The screenshot shows the Google Cloud Platform API Credentials page. The left sidebar has 'API' selected. The main area shows 'Credentials' with a '+ CREATE CREDENTIALS' button and a 'DELETE' button. A red box highlights the 'OAuth client ID' section, which contains a description: 'Requests user consent so that your app can access the user's data.' Below it is a 'Service account' section with a description: 'Enables server-to-server, app-level authentication using robot accounts'. At the bottom is a 'Help me choose' section with a description: 'Asks a few questions to help you decide which type of credential to use'. A table lists three OAuth 2.0 Client IDs:

Name	Creation date	Type	Client ID
AWSQA2	13 Aug 2021	Web application	3... -lg28...
Web	7 Nov 2020	Web	3... -nh9m...

- d. From the dropdown list, select **Web application** as the application type.

The screenshot shows the 'Create OAuth client ID' form. The left sidebar has 'API' selected. The main area has a back arrow and the title 'Create OAuth client ID'. A red box highlights the 'Application type \*' dropdown menu, which contains several options like 'Web application', 'Native application', etc.

- e. In the **Application** field, enter a **Name**.

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information. [Learn more](#) about OAuth client types.

**Application type \***

**Name \***

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

**Info** The domains of the URIs you add below will be automatically added to your [OAuth consent screen](#) as authorised domains.

- f. Fill in the remaining fields as needed.
- g. To add a redirect URL, click **Add URL**.

**Authorised JavaScript origins** [?](#)

For use with requests from a browser

**+ ADD URI**

**Authorised redirect URIs** [?](#)

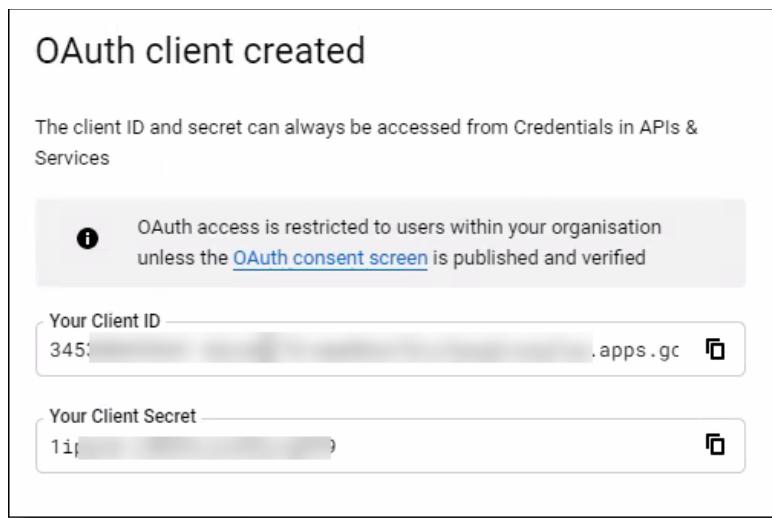
For use with requests from a web server

**+ ADD URI**

**CREATE** CANCEL

- h. Enter the redirect URL and click **Create**.

A message appears with the client ID and the client secret. You will need this information when you onboard the Google Cloud Platform application.

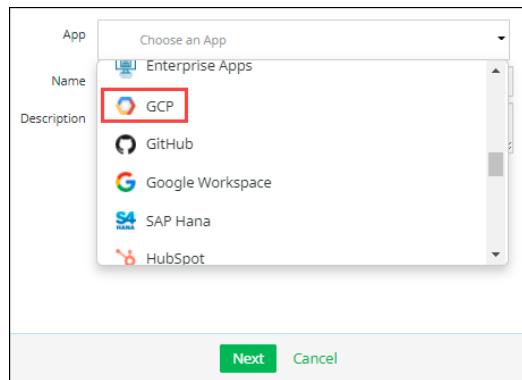


## Onboarding steps

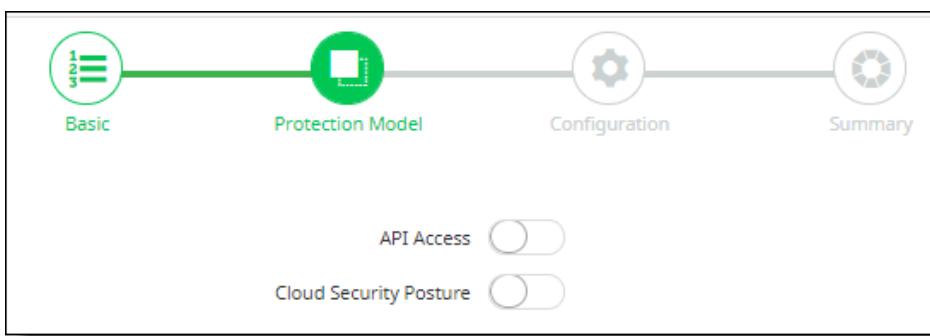
1. From the Management Console, select **Administration > App Management**, and click **New**.
2. Select **GCP** from the dropdown list.

### Tip

To find an app, enter the first few characters of the app name, then select the app from the search results.



3. Enter a **Name** (required) and a **Description** (optional). The name must include only alphanumeric characters, with no special characters other than the underscore, and no spaces. Then, click **Next**.
4. Select one or more **protection models** and click **Next**.

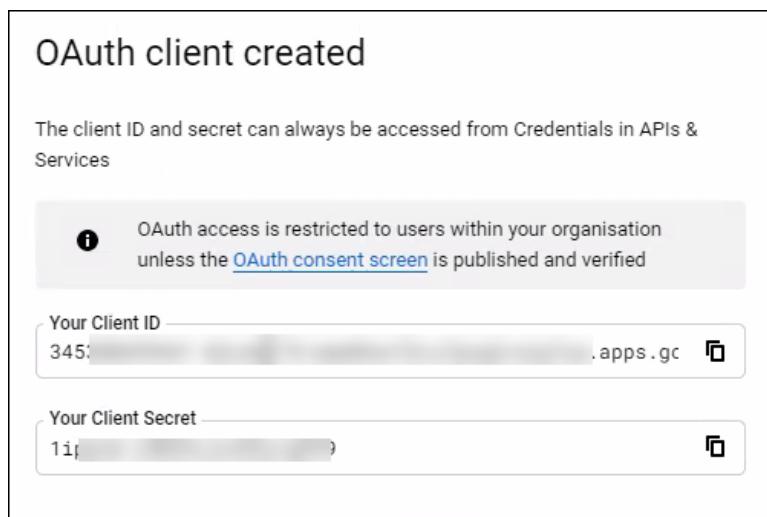


The options are

- **API Access**
- **Cloud Security Posture**

5. Enter the following configuration information. The fields you see depend on the protection models you selected in the previous step.
  - If you selected **API Access**, enter:
    - **Client Id**
    - **Client Secret**

This is the information created during the GCP pre-onboarding configuration steps.



Be sure to enter exactly the same information in the **Client ID** and **Client Secret** fields here.

API Settings	
Client Id	<input type="text"/>
Client Secret	<input type="text"/>

- If you selected **Cloud Security Posture**, enter:
  - **Service Account Credentials (JSON)** --The service account credentials for the JSON file you downloaded in the configuration steps.

- **Sync Interval (1-24 Hrs)** – How often CSPM/SSPM will retrieve information from the cloud and refresh the inventory. Enter a number.

The screenshot shows a 'CSPM Settings' page with two input fields. The first field is labeled 'Service Account Credentials (JSON)' and contains a JSON string. The second field is labeled 'Sync Interval(1-24 Hrs)' and contains a numerical value.

6. Click **Authorize**.

The screenshot shows an 'Authorization' page. It features a 'Google Cloud Platform' logo, a large green 'Authorize' button, and three small buttons at the bottom labeled 'Previous', 'Next', and 'Cancel'.

- If you selected only **Cloud Security Posture**, the **Summary** page appears. Review it and save the new GCP application to complete onboarding.
- If you selected **API Access** or both **API Access** and **Cloud Security Posture**, enter your GCP account login credentials when prompted.

**Note**

- If you entered an invalid client secret or client ID on the **Configuration** page, an error message will appear after you click **Authorize**. Review your client secret and client ID entries, make any corrections, and click **Authorize** again. Once the system recognizes the entries as valid, enter your GCP login credentials when prompted.

After your GCP login credentials have been accepted, save the new GCP cloud application to complete onboarding.

## Onboarding Dropbox applications

This section outlines procedures for onboarding Dropbox cloud applications.

1. From the Management Console, select **Administration > App Management**, and click **New**.
2. From the **Choose an app** list, select **Dropbox**.
3. Enter a **Name** (required) and a **Description** (optional). The name must include only alphanumeric characters, with no special characters other than the underscore, and no spaces. Then, click **Next**.
4. From the **Configuration** page, select one or more protection models:
  - **API Access**
  - **Cloud Data Discovery (CDD)**
5. Enter the following configuration information. The fields you see depend on the protection models you selected in the previous step.
  - If you selected **API Access**, enter one or more internal domains.

You can also configure **Archive Settings**. These settings enable archiving of files that are either permanently deleted or replaced by Content Digital Rights policy actions. Archived files are placed in an **Archive** folder under a **CASB Compliance Review** folder created for the cloud application. You can then review the files and restore them if needed.

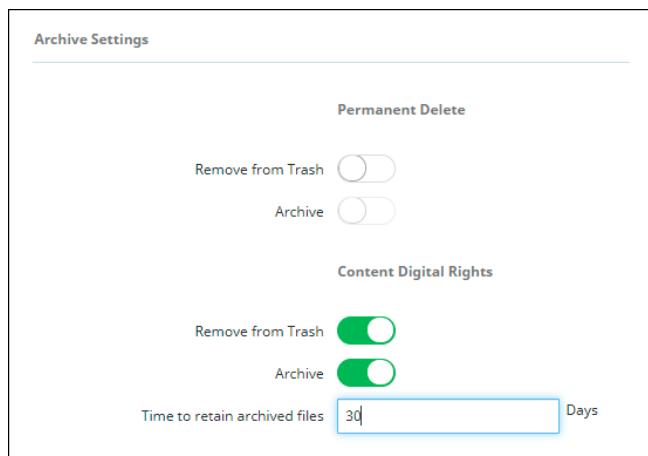
#### Note

When the authorized administrator for a cloud account is changed, previously archived content in the **CASB Compliance Review** folder that is owned by the previous administrator should be shared with the new authorized administrator to enable archived data to be reviewed and restored.

The **Archive Settings** option is available for onboarded cloud applications with **API Access and Cloud Data Discovery** protection modes selected.

Two options are available:

- **Remove from Trash**
- **Archive**



For **Permanent Delete** policy actions, both options are disabled by default; for **Content Digital Rights**, they are enabled by default.

Click the toggles to enable or disable the settings. If you select the **Archive** action, also select the **Remove from Trash** option.

Enter the number of days for which to retain archived files. The default value is 30 days.

Then, click **Authorize**, and enter your Dropbox administrator login credentials.

6. Click **Next** and review a summary to verify that all information is correct. If it is, click **Save**. The new cloud application is added to the **App Management** page.

## Onboarding GitHub applications

This section outlines procedures for onboarding GitHub cloud applications.

1. From the Management Console, select **Administration > App Management**, and click **New**.
2. From the **Choose an app** list, select **GitHub**.
3. Enter a **Name** (required) and a **Description** (optional). The name must include only alphanumeric characters, with no special characters other than the underscore, and no spaces.

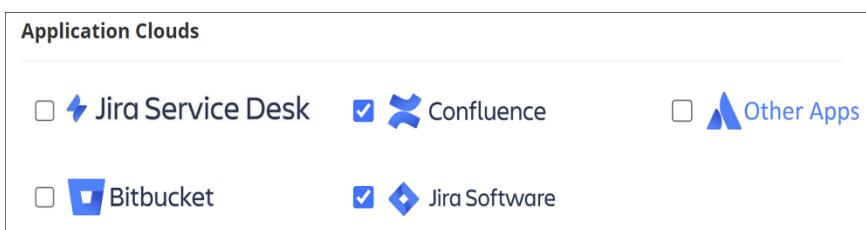
4. Click **Next**.
5. Select one or more protection models:
  - **App Authentication only**
  - **App Authentication and App Access**
  - **API Access**
6. Click **Next**.
7. Enter additional information depending on which protection model you chose:
  - If you selected App Authentication only, then on the next screen, click **New** to add authorized users or user groups. When finished, click **Next**.
  - If you selected App Authentication and App Access:
    - On the Configuration screen, enter your **GitHub Org ID** and **Home Page URL**. In the **Specific Domains** field, enter any domains that you use with GitHub, separated by commas. Click **Next**.
    - On the User Access screen, click **New** to add authorized users or user groups. When finished, click **Next**.
  - If you selected API Access, click the **Authorize** button on the next screen and enter your GitHub login credentials. Select the organizations that you want to onboard, and click the **Authorize** button.
8. Review the summary to verify that all information is correct. If it is, click **Save**. The new cloud application is added to the **App Management** page.

## Onboarding the Atlassian Cloud suite and applications

This section outlines procedures for onboarding the Atlassian cloud suite and applications.

**Note:** For the Confluence application, you must have an enterprise account. CASB does not support free Confluence accounts.

1. From the Management Console, select **Administration > App Management** and click **New**.
2. Select **Atlassian** from the app list.
3. Enter a **Name** (required) and a **Description** (optional). The name must include only alphanumeric characters, with no special characters other than the underscore, and no spaces. Then, click **Next**.
4. Select the applications in the suite to include and click **Next**.



- Select **API Access** protection model.

## Entering configuration settings for protection models

Enter required configuration information for the protection models you selected.

### API Access

- Enter the following API access information.

The screenshot shows a configuration interface for API Settings. At the top, there are two input fields: 'API Token' (empty) and 'Polling Timezone' (set to '--Select--'). Below these is a section titled 'Authorization' containing a 'Confluence' logo and a green 'Authorize' button. The entire interface is contained within a light gray box.

- API Token (Confluence applications only)** – Enter an API token. To create an API token from your Atlassian account, see the following section, Generating an API Token.
- Polling Timezone (Confluence applications only)** – Select a time zone for polling from the dropdown list. The selected time zone must be the same as that of the cloud application instance, not the time zone of the user.
- Authorization** – Click the **Authorize** button next to each app included in the suite.  
When prompted, click **Accept** to authorize domain access for each of the selected apps.  
The **Authorize** button labels will now say **Re-Authorize**.

- Click **Next**.
- Review the information on the **Summary** page. Click **Save** to save and onboard the application.

## Generating an API token (Confluence applications only)

You can generate an API token from your Atlassian account.

- Log into your Atlassian account.
- Select **Administration** from the left menu.
- From the **Administration** page, select **API Keys** from the left menu.

Any API keys you created previously are listed.

Admin / testccmse

## API keys

Create API key

API keys allow you to manage your organisation via the Atlassian Admin APIs. You can update organisation settings and manage user accounts by making requests to HTTP endpoints. Learn more about the [Admin API](#)

Name	Created by	Created on	Expires	Action
Test_9_Aug	ja mail.com	Aug 9, 2022	Feb 28, 2023	<a href="#">Revoke</a>

4. Click **Create New Key** to generate a new key.
5. Give the new key a **name** and select an **expiration date**. Then, click **Create**.

Name

Expires on  (Max expiry is one year from today)

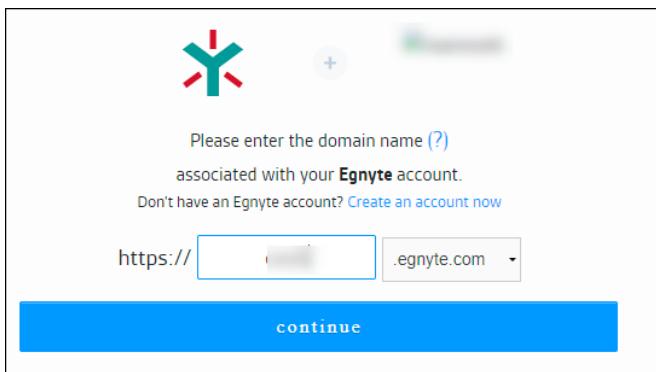
[Back](#) [Create](#)

The new API key is created and is added to the list of keys on the **Administration** page. For each key, the system generates an alphanumeric string that serves as the API token. Enter this string in the **API Token** field in the CASB Management Console.

## Onboarding Egnyte applications

This section outlines the procedure for onboarding an Egnyte cloud application.

1. Go to **Administration > App Management** and click **New**.
2. Choose **Egnyte** from the dropdown list and click **Next**.
3. Enter a **Name** (required) and a **Description** (optional). The name must include only alphanumeric characters, with no special characters other than the underscore, and no spaces. Then, click **Next**.
4. Select **API Access** protection mode.
5. Click **Next** and enter the following configuration information, depending on the protection modes you selected.  
If you selected **API Access**, click **Authorize Egnyte**, and enter your Egnyte login credentials.
6. Enter a domain name associated with your Egnyte account and click **Continue**.



7. Once your authorization is successful, save the new cloud application.

## Onboarding Box applications

This section outlines prerequisite configuration and onboarding steps for Box applications.

### Configuration steps in the Box Admin Console

For connectivity to Box cloud applications, several user account settings are required to enable proper policy creation and visibility into Box user activities.

Perform the following steps to configure the ADMIN account for a Box cloud application.

#### Note

The ADMIN account is required for authorization of a Box cloud application. Authorization or re-authorization cannot be completed with CO-ADMIN (co-administrator) account credentials.

1. Log in to Box using the ADMIN credentials for the Box account.
2. Click the **Admin Console** tab.

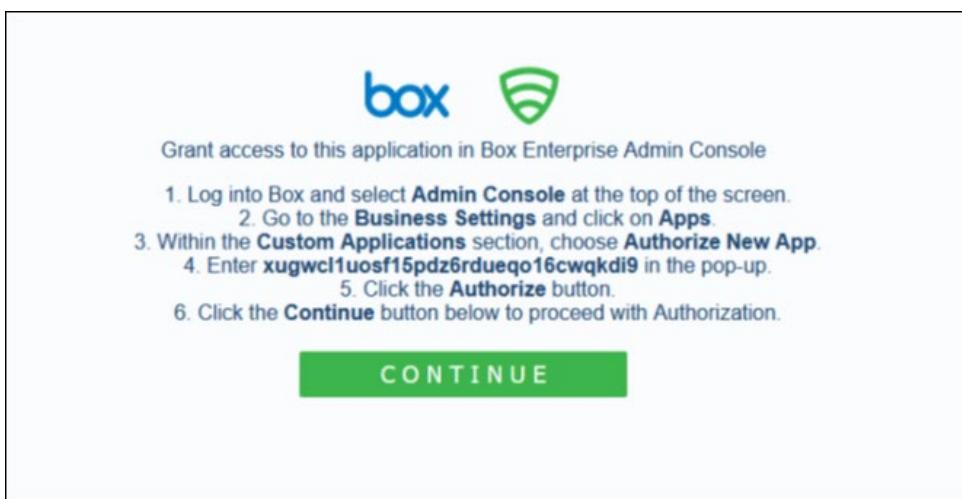


3. Click the **Users** icon.
4. From the **Managed Users** window, select the admin account you want to validate and use to connect to your Box cloud application.
5. Expand the **User Account** information.
6. In the **Edit User Access Permissions** window, be sure that **Shared contacts / Allow this user to see all managed users** is checked.

#### Note

*Do not allow co-administrators to monitor other co-admin activities.* Only an administrator should monitor other co-admin activities.

7. Go to **Apps > Custom Apps**.
8. Choose **Authorize New App**.
9. In the pop-up window that appears, enter the following string:  
**xugwcl1uosf15pdz6rdueqo16cwqkdi9**
10. Click **Authorize**.
11. Click **Continue** to confirm access to your Box enterprise account.



## Onboarding steps in the Management Console

1. Go to **Administration > App Management**.
2. In the **Managed Apps** tab, click **New**.
3. Select **Box** from the list.
4. Enter a **Name** (required) and a **Description** (optional).
5. Click **Next** and select one or more available protection modes:
  - **API Access**
  - **Cloud Data Discovery**
6. Click **Next** and enter the configuration information. The fields you see on the **Configuration** screen depend on the deployment and the protection modes you chose in the previous step.
7. Enter the information needed for each protection mode you select.
  - For **Cloud Data Discovery** -- You must also choose the **API Access** protection mode.
  - For **API Access** – In the **API Settings** section, enter a valid **Admin Email** address for the Box account. *This address must be for the Admin account and not for a co-admin account.* Then, enter the names of **Internal Domains**.

The screenshot shows a configuration interface titled "API Settings". It contains two main input fields: "Admin Email" and "Internal Domains", each represented by a simple rectangular box for text entry.

- For **API Access** – In the **Archive Settings** section, you can enable archiving of files that have been permanently deleted, modified, or otherwise acted on by policy actions. CASB stores archived files in an **Archive** folder under a **CASB Compliance Review** folder created for the cloud application. You can then review the files and restore them if needed.

### Note

When you change the authorized administrator for a cloud account, if there is any previously archived content in the **CASB Compliance Review** folder that is owned by the previous administrator, you should share it with the new authorized administrator to enable archived data to be reviewed and restored.

Three options are available:

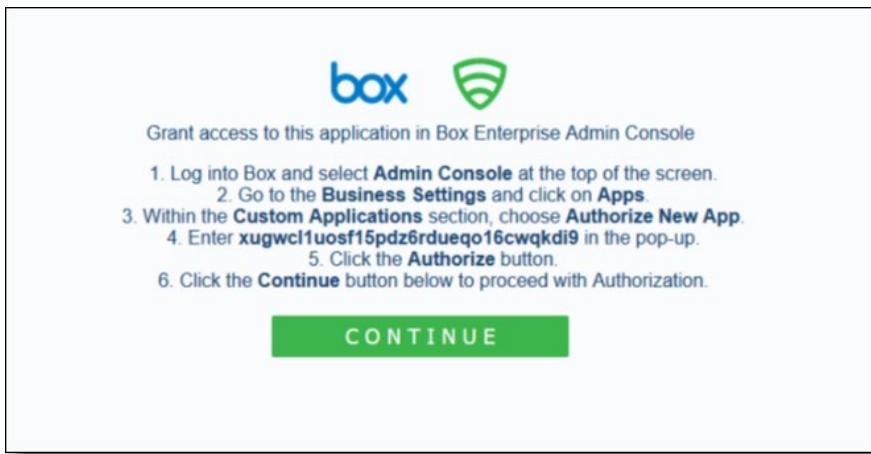
- **Permanent Delete**
  - If you select **Remove from Trash**, then when a file is deleted (either by a user, or by CASB when implementing a policy), CASB will also permanently delete that file so it can no longer be retrieved from the user's trash folder.
  - If you select **Archive** (only available if **Remove from Trash** is selected), then CASB will also archive a copy of the file in the archive folder (see above). An administrator can review the copy and determine what next steps need to be taken. For more information, see [Violation management and quarantine](#).

- **Content Actions** – Applies to files that violate a Content Digital Rights policy. When CASB takes action on a file as configured in the policy, it can also do the following:
  - If you select **Remove from Trash**, then when CASB deletes a file because it violated a policy, CASB will also permanently delete that file so it can no longer be retrieved from the user's trash folder.
  - If you select **Archive** (regardless of whether **Remove from Trash** is selected), then CASB will archive a copy of the file in the archive folder (see above). An administrator can review the copy and determine whether additional actions need to be taken. For more information, see [Violation management and quarantine](#).
  - By default, CASB keeps archived files for 30 days. You can change that if needed by modifying the value in the **Time to retain archived files** field.
- **Collaboration Actions** – Applies to files that violate a collaboration policy. When CASB takes action on a file as configured in the policy (such as the Remove Collaborator action), it can also archive a copy of the file in the archive folder (see above). An administrator can review the copy and determine whether additional actions need to be taken. An administrator can also decide to undo the collaboration action that was taken by CASB. For details, see [Undoing a policy action on files or folders in the Box cloud application](#).

For **API Access**, enter the **Enterprise ID** used to authorize access to Box.

The screenshot shows a configuration interface with a title 'Identity'. Below it is a text input field labeled 'Enterprise Id' with a placeholder box. The entire interface is contained within a light gray rectangular border.

8. When you have entered the required configurations, click **Next** to authorize access to Box.
9. In the **Grant Access to Box** screen, enter the Enterprise ID for this Box account, and click **Continue**.



10. In the **Log in to Grant Access to Box** screen, enter the admin login credentials for the Box account, and click Authorize.

If the administrator has configured an SSO setup, click the **Use Single Sign On (SSO)** link and enter the credentials to authenticate. Any multi-factor authentication information is submitted.

The Box cloud application is onboarded and added to the list of managed applications in the **App Management** page.

# Onboarding Salesforce applications

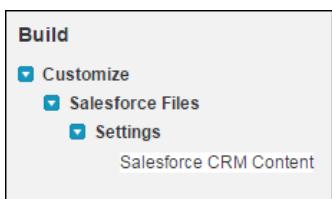
## Configuration steps

CASB for Salesforce scans standard objects such as Accounts, Contacts, Campaigns, and Opportunities, as well as custom objects.

### Enable CRM content

For DLP scanning to work with Salesforce, the **Enable CRM** setting must be enabled in Salesforce for all users. To enable Salesforce CRM content, log in to your Salesforce account and perform the following steps:

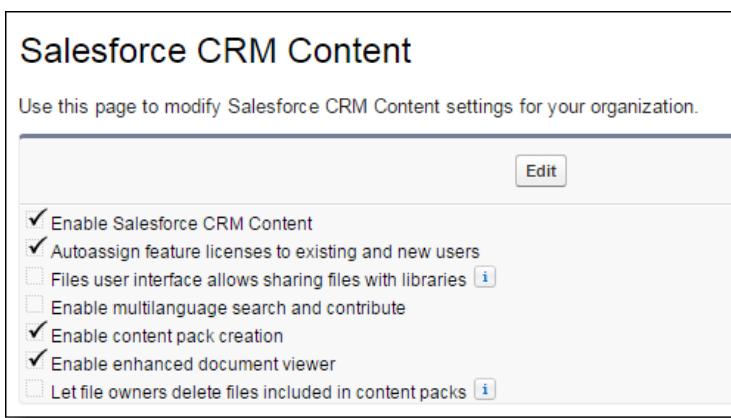
1. Using the **Quick Find** box at the top left, search for **Salesforce CRM Content**.



2. From the search results, click the **Salesforce CRM Content** link.

The **Salesforce CRM Content** settings box appears.

3. If the **Enable Salesforce CRM Content** and **Autoassign feature licenses to existing and new users** options are not checked, check them.



### Enable scanning for structured data

If you are working with structured data, be sure that the **Structured Data** option is enabled.

### Enable permissions for DLP scanning

System administrators have global access to Salesforce standard and custom objects. For non-administrators, the **Push Topics** and **API Enabled** permissions must be enabled for DLP to work, as follows.

### To set the Push Topics option:

- From the **Manage Users** menu, select **Users**.
- From the **All Users** page, select a user.
- In the **User Detail** page for that user, click the **Standard Platform User** link.

[Profile](#)   [Standard Platform User](#)

- Scroll to the **Standard Object Permissions** section.

Standard Object Permissions													
	Basic Access			Data Administration				Basic Access			Data Administration		
	Read	Create	Edit	Delete	View All	Modify All		Read	Create	Edit	Delete	View All	Modify All
Accounts	✓	✓	✓	✓	□	□	Feedback Templates	✓	✓	✓	✓	□	□
Coaching	✓	✓	✓	✓	□	□	Goals	✓	✓	✓	✓	□	□
Contacts	✓	✓	✓	✓	□	□	Goal Links	✓	✓	✓	✓	□	□
D&B Companies	✓						Ideas	✓	✓				
Documents	✓	✓	✓	✓	□	□	Metrics	✓	✓	✓	✓	□	□
Feedback	✓	✓	✓	✓	□	□	Metric Data Links	✓	✓	✓	✓	□	□
Feedback Questions	✓	✓	✓	✓	□	□	Performance Cycles	✓	✓	✓	✓	□	□
Feedback Question Sets	✓	✓	✓	✓	□	□	Push Topics	✓	✓	✓	✓		
Feedback Requests	✓	✓	✓	✓	□	□	Streaming Channels	✓	✓	✓	✓	□	□

- Under **Basic Access/Push Topics**, be sure that **Read**, **Create**, **Edit**, and **Delete** are checked.

### To set the API Enabled option:

- On the **Standard Platform User** page, scroll to the **Administrative Permissions** section.

Administrative Permissions	
Access Chatter For SharePoint	<input type="checkbox"/>
Access Community Management	<input type="checkbox"/>
<b>API Enabled</b>	<b>✓</b>
Can Approve Feed Post and Comment	<input type="checkbox"/>
Chatter Internal User	<input checked="" type="checkbox"/>
Manage Dynamic Dashboards	<input type="checkbox"/>
Manage Health Check	<input type="checkbox"/>
Manage Letterheads	<input type="checkbox"/>
Manage Public Documents	<input type="checkbox"/>
Manage Public List Views	<input type="checkbox"/>

- Be sure that **API Enabled** is checked.

### Enable permissions for viewing event log files

To enable CASB to collect event monitoring data, you must enable user permissions for the **View Event Log Files** and **API Enabled** settings.

Users with **View All Data** permissions also can view event monitoring data. For more information, refer to the following link:

[https://developer.salesforce.com/docs/atlas.en-us.api\\_rest.meta/api\\_rest/using\\_resources\\_event\\_log\\_files.htm](https://developer.salesforce.com/docs/atlas.en-us.api_rest.meta/api_rest/using_resources_event_log_files.htm)

### Enable Event Monitoring

For continuous monitoring of Salesforce activity and DLP controls in API mode, you must enable the 'Event Monitoring' add-on subscription on your Salesforce account. If you do not have this setting enabled, CASB can monitor all activities by admin users but only login/logout activities by non-admin users.

To enable this setting:

1. In your Salesforce account, go to Setup and use the search box to search for **Event Monitoring**.
2. Click on **Event Monitoring Settings**.
3. Enable the **Generate event log files** setting.

## Enable permissions for Audit Trail events

To process **Audit Trail** events, permissions must be enabled for **View Setup and Configuration**.



## Enable permissions for Login History events

To process **Login History** events, permissions must be enabled for **Manage Users**, which also enables permissions for the following settings:

- Requires Reset User Passwords and Unlock Users**
- View All Users**
- Manage Profiles and Permission Sets**
- Assign Permission Sets**
- Manage Roles**
- Manage IP Addresses**
- Manage Sharing**
- View Setup and Configuration**
- Manage Internal Users**
- Manage Password Policies**
- Manage Login Access Policies**
- Manage Two-Factor Authentication in User Interface**

## Enable permissions for querying files

In order to enable CASB to access all file events, you must enable permissions for the admin user that you will use to onboard Salesforce.

1. In your Salesforce account, go to **Setup** and use the search box to search for **Permission Sets**.
2. Create a new permission set, giving it any name of your choosing.
3. Select **App Permissions**.
4. In the **Content** section, check the box for **Query All Files**.
5. Save the permission set.
6. Use the **Setup** search box to search for **Users**.
7. Click the name of the admin user that you will use to onboard Salesforce.

8. In the **Permission Set Assignments** section, click **Edit Assignments**.
9. Select the permission set that you created in step 2 above.
10. Save the user account.

## Enable permissions for viewing and modifying data

In order to enable CASB to access all data, you must enable permissions for the admin user that you will use to onboard Salesforce.

1. In your Salesforce account, go to **Setup** and use the search box to search for **Users**.
2. Click the name of the admin user that you will use to onboard Salesforce, and click the **Edit** button.
3. In the Administrative Permissions section, make sure that the **View All Data** and **Modify All Data** checkboxes are selected.
4. Save the user account.

For Salesforce, users can view file content even when downloading is disabled by default for the account.

## Onboarding steps

1. Go to **Administration > App Management** and click **New**.
2. Select **Salesforce** from the list
3. Enter a **Name** (required) and a **Description** (optional) and click **Next**.
4. Select one or more protection modes:
  - **API Access**
  - **Cloud Security Posture**
  - **Cloud Data Discovery**
5. Click **Next** and enter configuration settings. The fields you see depend on the deployment and the protection modes you chose in the previous step.

- For **API Access** – Enter a **Salesforce Subdomain**.

Identity

Salesforce Subdomain

Authorization

Authorize

Previous Next Cancel

- For **Cloud Security Posture** – No other details are needed.
- For **Cloud Data Discovery** -- No other details are needed.

#### 6. Click **Authorize**.

Please specify your Salesforce instance type and click continue.  
Check the checkbox for sandbox and custom domain authentication.

Salesforce

Sandbox or Custom domain

**CONTINUE**

7. Select the Salesforce instance from the dropdown list.
8. If this authorization is for a custom or a sandbox domain, click the box. Then, click **Continue**.

salesforce

Username

Password

**Log In**

Remember me

[Forgot Your Password?](#) [Use Custom Domain](#)

Not a customer? [Try for Free](#)

© 2020 salesforce.com, Inc. All rights reserved. | [Privacy](#)

9. Enter the administrator login credentials for this Salesforce account. Make sure to use the same administrator account that you assigned permissions to in the [Enable permissions for querying files](#) section above. Then, click **Log In**.

## Onboarding ServiceNow applications

The following section provides instructions for onboarding ServiceNow applications.

### Configuration steps

Before onboarding the ServiceNow application, create an OAuth application.

1. Log in to ServiceNow as an administrator.
2. To create an OAuth application, go to  
**System OAuth > Application Registry > New > Create an OAuth API endpoint for external clients.**
3. Enter the following information:
  - **Name** – Enter a name for this OAuth app.
  - **Redirect URL** – Enter the appropriate URL.
  - **Logo URL** – Enter the appropriate URL for the logo.
  - **PKCE Required** -- Leave unchecked.
4. Click **Submit**.
5. Open the newly created app and note the **Client ID** and **Client Secret** values.

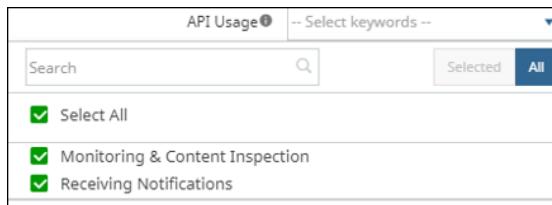
Next, if you want to use Cloud Data Discovery (CDD) with ServiceNow, you must enable domain separation.

1. Log in to your ServiceNow developer account.
2. Click the profile icon and select **Activate Plugin**.
3. For the entry **Domain Support - Domain Extensions Installer**, select **Activate plugin with demo data** from the **Activate** drop-down.
4. Wait a few minutes and verify that you have received an email indicating that the activation was successful.

### Onboarding steps

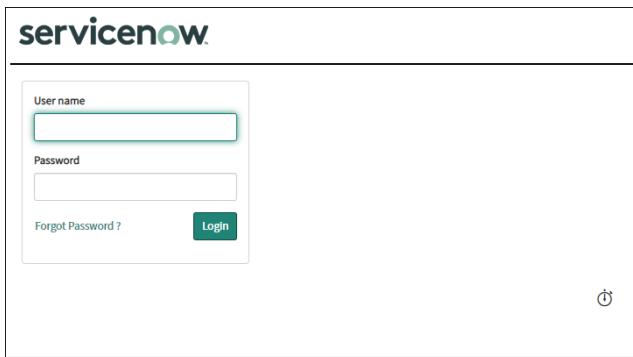
1. From the Management Console, go to **Administration > App Management**.
2. In the **Managed Apps** tab, click **New**.
3. Select **ServiceNow** and click **Next**.
4. Enter a **Name** (required) and a **Description** (optional). Then click **Next**.
5. Select one or more protection modes and click **Next**.
6. On the **Configuration** page, enter the information for the protection modes you selected in the previous step.

- For **API Access**, enter:
  - The **API Usage type**, which defines how this application will be used with API protection. Check **Monitoring & Content Inspection**, **Receiving Notifications**, or **Select All**. If you select only **Receiving Notifications**, this cloud application is not protected; it is used only to receive notifications.



- The OAuth App Client ID
- The OAuth App Client Secret
- The ServiceNow Instance ID
- For **Cloud Data Discovery**, enter
  - The OAuth App Client ID
  - The OAuth App Client Secret
  - The ServiceNow Instance ID

7. Click **Authorize**.
8. When prompted, log in to the ServiceNow application.



9. When prompted, click **Allow**.

If authorization is successful, you should see a **Re-Authorize** button when you return to the Management Console. Click **Next** and **Save** to complete onboarding.

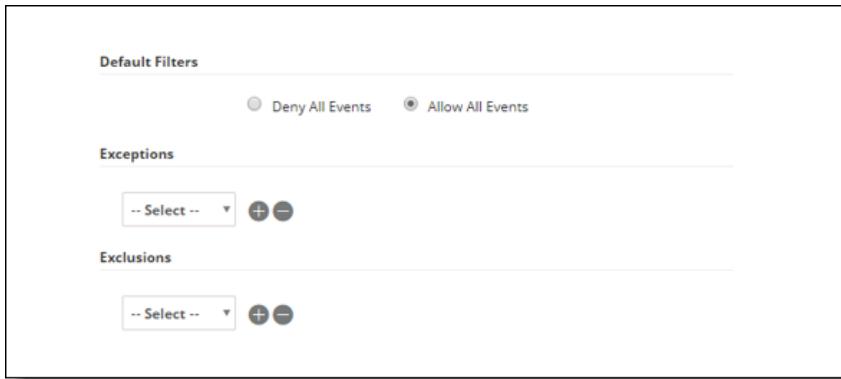
# Post-onboarding tasks

Once you have onboarded cloud applications, you can filter events for those applications.

## Applying event filtering to onboarded cloud applications

If you selected **API Access** as a protection mode, you can select event filtering options for that cloud application after it is onboarded.

After you have onboarded a cloud application with **API Access** as a protection mode, you can set default filters for allowing or denying all events for users, user groups, domains, or events. These filters can help narrow the focus to specific groups and will require less processing time and less demand on system resources.



### To apply event filtering:

1. Go to **Administration > App Management**.
2. Select the cloud to which you want to apply event filtering by checking the pencil option.
3. Select filtering options as follows:
  - **Default filters** – Choose a default filter.
    - **Deny All Events** – No events are processed.
    - **Allow All Events** – All events are processed.
  - **Exceptions** – Select exceptions to the chosen filter for users or user groups. For example, if you want to apply an exception for one group -- the engineering team -- the default filter actions would be applied as follows:
    - For **Deny All Events**, *no events* are processed except those for the engineering team.
    - For **Allow All Events**, *all events* are processed except those for the engineering team.
  - **Exclusions** – Select any criteria that should not be included in the exceptions. For example, you might opt to deny (not to process) events for staff in engineering except for managers. Using this example, the default filter exclusions would be applied as follows:
    - For **Deny All Events** -- **No events** are processed except for the engineering team. The managers are **excluded** from this exception, which means that **events for managers within the engineering team are not processed**.

- For **Allow All Events** -- Events **are** processed except for the engineering team. The managers are **excluded** from this exception, which means that **events for managers within the engineering team are processed**.

4. Click **Next**.

# Configuring tenants for user access and session activity

You can set conditions for tenant access by:

- Specifying authorized IP addresses for user access
- Entering session timeout information
- Choosing a time frame for login access to Juniper Support.

## To configure tenant access settings:

1. Go to **Administration > System Settings**.
2. Select **Tenant Configuration** from the left menu.
3. Configure the settings as follows.

### Authorized IP addresses

You can allow access to the tenant for only the IP addresses you authorize. When users with Application Administrator, Key Administrator, or Application Monitor roles want to log in to the Management Console, the system checks their IP addresses against those authorized addresses.

- If the match with a valid IP address is **not** found, login is denied and the message **Invalid IP user range** is displayed.
- If a match with a valid IP address **is** found, the user can log in.

### Notes

This validation process does **not** apply for:

- System Administrator, Operations Administrator, or Service Administrator logins
- **Login with IdP**



To specify authorized IP addresses for access to the tenant, click in the **Authorized IP Addresses** field.

Authorized IP Addresses	
1 Restriction(s)	
49	

Enter one or more IP addresses you want to authorize for access to the tenant. Separate each IP address with a comma.

Click **Save** to close the entry box and select other configuration settings on the page.

## Session Timeout

Enter a time (in minutes, any number between 1 and 120) after which a session expires, and another login is required. The default value is 30 minutes.

## Login access to Juniper Support

System administrators and application administrators can enable or disable access to Juniper Support by service administrators and operations administrators. You can deny access or select the number of days available access.

In the **Juniper Networks Support** field, select an option. The default selection is **No Access**. You can also select access for 1 day, 3 days, or 1 week.

Click **Save** to save all tenant configuration settings.

# Managing users

---

CASB provides three options for managing users:

- **Administrative**, which enables control of user access by role for the Management Server and Hybrid Key Management System
- **Enterprise**, which provides an integrated view of users in their enterprise, and their account information

## Administrative user management

CASB provides role-based access control to provide clear distinction of user access privileges and responsibilities. You can add new users as needed.

All user information is identical for the Management Server and the Hybrid Key Management System (HKMS), although the sets of users are maintained separately.

### Adding new users

**To add users:**

1. Go to **Administration > User Management** and click the **Administrative User Management** tab.
2. Click **New**.
3. Enter the following information:
  - **User Name** – Enter a valid email address for the user.
  - **Role** – Use the check boxes to select one or more roles for the user.
    - **System Administrator** – Can perform all system administration functions, including onboarding cloud applications, adding and removing users, creating and assigning keys, and restarting the Management Server.
    - **Key Administrator** – Can create, assign, and remove keys, and monitor other system functions.
    - **Application Administrator** – Can create and manage applications and monitor other system functions.
    - **Read-Only User** – Can monitor system functions through the Management Console, view alerts, and export reports. Cannot create or modify functions such as onboarding cloud applications, adding users, editing user information, or configuring system settings.
    - **Compliance User** – Can only access a subset of Management Console functions related to compliance. Can view data and download reports on the screens they have access to, but cannot create or modify functions.

#### Note

Hosted deployments include two additional users with unique roles: **Services Administrator** and **Operations Administrator**. These users are assigned by Juniper Networks and cannot be deleted.

4. Click **Apply**.
5. Click **Save**. The new user is added to the list. The new user will receive an email notification with a temporary password and will be asked to select a permanent password.

## Setting up a user account password policy

CASB provides a default password policy. You can change the default settings to meet your organization's needs.

### To change the user account password policy:

1. Go to **Administration > User Management**.
2. Click the **User Account Password** Policy link.

The **Password Policy** screen is displayed. (The **Save** button becomes active once you begin entering changes.)

This password policy applies only to the local user account.

Minimum Length	8
Maximum Length	13
Lowercase Characters	1
Uppercase Characters	1
Special Characters	1
Numerics	1
Enforce Password History	
Enforce Password History	3
Passwords recommended	
Password Expiration Period	
Password Expiration Period	6
Months	
Invalid Login Attempts Allowed	
Invalid Login Attempts Allowed	3
Lockout Effective Period	
Lockout Effective Period	5
Minutes	

**Save**    **Cancel**

3. Change the policy items as needed:

Field	Description
<b>Minimum Length</b>	<p>Specifies the minimum number of characters that can make up a password for a user account. You can set a value of between 1 and 13 characters. To specify that no password is required, set the number of characters to (zero).</p> <p>A minimum of 8 characters is recommended. This number is long enough to provide adequate security, but not too difficult for users to remember. This value also helps to provide adequate defense against a brute force attack.</p>
<b>Maximum Length</b>	<p>Specifies the maximum number of characters that can make up a password for a user account.</p> <p>If you specify 0 (zero), the allowed length will be unlimited. A setting of 0 (unlimited) or a relatively large number such as 100 is recommended.</p>

Field	Description
<b>Lowercase Characters</b>	<p>Specifies the minimum number of lowercase characters that must be present in a password for a user account.</p> <p>If you enter 0 (zero), no lowercase characters are allowed in the password. A minimum of 1 lowercase character is recommended.</p>
<b>Uppercase Characters</b>	<p>Specifies the minimum number of uppercase characters that must be present in a password for a user account.</p> <p>If you enter 0 (zero), no uppercase characters are allowed in the password. A minimum of 1 uppercase character is recommended.</p>
<b>Special Characters</b>	<p>Specifies the minimum number of special characters (for example, @ or \$) that can make up a password for a user account.</p> <p>If you enter 0 (zero), no special characters are required in the password. A minimum of 1 special character is recommended.</p>
<b>Numerics</b>	<p>Specifies the minimum number of numeric characters that must be present in a password for a user account.</p> <p>If you enter 0 (zero), no numeric characters are required in the password. A minimum of 1 numeric character is recommended.</p>
<b>Enforce Password History</b>	<p>Specifies the number of unique new passwords that must be associated with a user account before an old password can be reused.</p> <p>A low number allows users to use the same small number of passwords repeatedly. For example, if you select 0, 1, or 2, users can reuse old passwords more quickly. Setting a higher number will make using old passwords more difficult.</p>
<b>Password Expiration Period</b>	<p>Specifies the period of time (in days) that a password can be used before the system requires the user to change it. You can set passwords to expire after a number of days between 1 and 99, or you can specify that passwords never expire by setting the number of days to 0 (zero).</p>
<b>Invalid Login Attempts Allowed</b>	<p>Specifies the number of failed login attempts that will cause a user account to be locked. A locked account cannot be used until it is reset by an administrator or until the number of minutes specified by the Lockout Effective Period policy setting expires.</p> <p>You can set a value from 1 through 999. If you want the account never to be locked, you can set the value to 0 (zero).</p>

Field	Description
<b>Lockout Effective Period</b>	Specifies the number of minutes that an account remains locked out before automatically becoming unlocked. The available range is from 1 through 99 minutes. A value of 0 (zero) means that the account will be locked out until an administrator unlocks it.

- Click **Save**.

## Account status for system administrator and non-administrator roles

Non-administrator user accounts are disabled automatically after more than 90 days of non-use. When an account is disabled, the user will see a message on the Management Console login screen notifying them that their account is disabled. A system administrator must re-enable the account before the user can log in to the Management Console.

### Note

Accounts for system administrators, service administrators, and operations administrators **cannot be disabled**. Only accounts for Key Administrator, Application Administrator, and Application Monitor roles can be disabled and re-enabled.

On the **Administrative User Management** tab of the **User Management** page, the toggles represent the following conditions:

- System Administrators:** The toggle is visible, enabled by default, and shows as grayed out.
- Services Administrators and Operations Administrators:** The toggle is visible, enabled by default, and shows as grayed out.
- System Administrators** can disable or enable the status of users with Key Administrator, Application Administrator and Application Monitor roles.
- For **existing System Administrators** who have **not** completed the user onboarding process, the toggle shows a status of disabled.
- For **newly created System Administrators** who have **not** completed the user onboarding process, the toggle is not visible.
- For **System Administrators** who **have** completed the onboarding process but have not logged into the application yet, the toggle is enabled but grayed out.
- For **Key Administrator, Application Administrator, and Application Monitor** roles: These users' accounts are disabled after 90 days of non-use. They will be blocked when they try to log in to the Management Console.

### Note

System Administrators whose accounts were disabled previously are now enabled (active).

The following sections provide instructions for system administrators to disable and re-enable non-administrator user accounts.

## Disabling a non-administrator user account

- Click the **bright green** toggle for the enabled non-administrator account.
- When prompted, confirm the action to disable the account.

## Re-enabling a disabled non-administrator user account

1. Click the **dimmed, colorless** toggle for the disabled non-administrator account.
2. When prompted, confirm the action to re-enable the account.

## Reassigning the Super Administrator role

A tenant can only have one Super Administrator account. If you want to reassign the Super Administrator role to a different user, you must do it while logged in with the current Super Administrator account.

1. In the Management Console, select **Administration > System Settings > Tenant Configuration**.
2. If you are logged in with the Super Administrator role, you will see the **Re Assignment of Super Administrator** option.
3. Select the desired user from the drop-down menu. Only users who currently have the System Administrator role are shown here.
4. Click **Send OTP** to receive a one-time password.
5. Retrieve the password from your email and enter it in the **Enter OTP** field. Click **Validate**.
6. Click **Save**. The Super Administrator role is transferred to the user you selected.

## Enterprise user management

The **Enterprise User Management** page provides an integrated view of users in their enterprise and their account information.

### Searching for user information

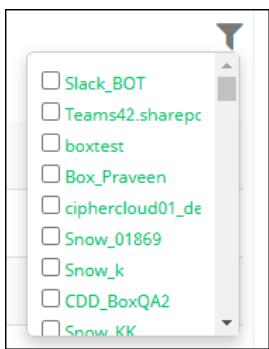
You can search for user information by:

- **account name** (Email), to see which users are associated with a specific account,
- **User Group**, to see which users are part of a specific user group, or
- **User Name**, to see which users (if any) are associated with more than one account.

To perform a search, enter all or part of the username, group name, or email in the **Search** box. Searches are case sensitive. To return to the default list, clear the **Search** box.

## Filtering user information

You can filter the display of information by cloud application. Click the **Filter** icon at the upper right and select the cloud applications to include in the display.



To clear the filter, click anywhere outside of the list box.

# Configuring CASB for enterprise integration

---

You can configure CASB to work with external services to manage user data, gather information about unsanctioned cloud applications, and other functions.

The following topics are provided:

- [Installing an on-premises connector for system services](#)
- [Adding Advanced Threat Protection \(ATP\) services](#)
- [Adding external services for Enterprise Data Loss Prevention \(EDLP\)](#)
- [Configuring Security Information and Event Management \(SIEM\)](#)
- [Configuring data classification](#)
- [Creating and managing user directories](#)
- [Creating and managing enterprise sites](#)
- [Creating notification channels](#)

# Installing an on-premises connector for system services

CASB provides a unified on-premises connector that can be used with multiple services, including SIEM, log agents, and EDLP. The following sections provide specifications and instructions for installing the on-premises connector.

- **Specifications**
- **Downloading the connector**
- **Pre-installation steps**
- **Installing the connector**
- **Restarting and uninstalling the connector**
- **Additional notes**

## Note

Remote upgrades are supported only for agents running on CentOS.

If you are using connector version 22.03 and planning to migrate to version 22.10.90, you can upgrade the SIEM, EDLP, and Log Agents using the manual upgrade procedure. For more information, see the [Manually upgrading the SIEM, EDLP, and Log Agents](#) section.

## Specifications

The following specifications are required for installation of the on-premises connector.

### Operating systems and software

- For SIEM, EDLP, and Log Agent: Red Hat Enterprise, CentOS 8, Ubuntu 20.04.5 LTS (Focal Fossa)
- Java version 17
- bzip2 1.0.6
- RPM version 4.11.3

### Firewall settings

- Allow outbound HTTPS traffic
- Allow the following outbound WSS connections:
  - Based on the location of your tenant, provide the Node Management URL.
  - **For Europe Central-1 [euc1]:**  
wss://nm.euc1.lkt.cloud:443/nodeManagement

- **For United States West-2 [usw2]:**  
wss://nm.usw2.lkt.cloud:443/nodeManagement

**Note** You can identify the Node Management URL from your Management Console URL as follows:

If your Management Console URL is

**https://maxonz-ms.euc1.lkt.cloud/account/index.html#login**

Then your Node Management URL is

`euc1.lkt.cloud`

- **wsg.ciphercloud.io** (applies to SIEM, LOG, and EDLP agents)

**Note** This URL is required only for legacy packages. For the on-premises enterprise connector package, you are not required to specify this URL manually.

## Minimum requirements for VM configurations

Here are the deployment options and minimum hardware requirements. The Base Package contains the NS-Agent and upgrade service.

### Log agent, SIEM, and EDLP services

- 8 GB RAM
- 4 vCPUs
- 100 GB disk space

## Downloading the connector

1. Go to **Administration > System Settings > Downloads**.
2. Select **On-premise Connector** and click the download icon.



3. Save the RPM file for installation on the appropriate VM.

## Pre-installation steps

### Step 1 – Create an agent for the service

1. Go to **Administration > Enterprise Integration** and select the agent to configure.
2. Perform the following steps to configure the agent.

### Step 2 – Create an environment

Perform these basic steps to create an environment.

1. Go to **Administration > Environment Management** and click **New**.
2. Enter a **Name** and a **Description** for the environment.
3. Select **On-premise Connector** as the environment **Type**.
4. Enter an IP address for the location where you want to install the connector.
5. Enable the agent and select a service.
6. Save the environment.

### Step 3 – Create a node

Perform these basic steps to create a node.

1. Go to **Administration > Node Management** and click **New**.
2. Enter a **Name** and a **Description** for the node.
3. Select **Connector** as the node **Type**.
4. Select the environment you created in the previous step.
5. Select the service.
6. Save the node.

Perform the steps in the following sections to install the on-premises connector.

## Installing the connector (SIEM, EDLP, and Log Agent)

Perform the following steps to install the on-premises connector. In the script, the term **Node Server** refers to the connector. In the next sections, the term **node server** refers to the connector.

**Run the following command to start the installation:**

```
[root@localhost home]# rpm -ivh enterprise-connector-21.01.0-105.x86_64.rpm
Preparing... #################################
[100%]
/usr/sbin/useradd -r -g ccns-c ${USER_DESCRIPTION} -s /bin/nologin ccns
Updating / installing...
1:enterprise-connector-0:21.01.0-10##### [100%]
CipherCloud node server has been successfully installed in
/opt/ciphercloud/node-server.

Adding [Systemd] service support
Reloading Systemd daemon
Systemd service node-server has been installed
Please use 'sudo systemctl start node-server' to start the service manually
=====
IMPORTANT=====
Please run 'sudo /opt/ciphercloud/node-server/install.sh' to configure the
node server before starting it for the first time.
=====
```

**Run the following command to change to the directory in which to install the connector.**

```
[root@localhost ~]# cd /opt/ciphercloud/node-server/
```

**Run the following command to perform the installation.**

```
[root@localhost node-server]# ./install.sh
```

Initializing node-server install script. Please wait..

Please enter Management Server endpoint [wss://nm:443/nodeManagement]:

Based on the location of your tenant, provide the Node Management URL:

**For Europe Central-1 [euc1]:**

wss://nm.euclkt.cloud:443/nodeManagement

**For United States West-2 [usw2]:**

wss://nm.usw2.lkt.cloud:443/nodeManagement

**Note:** You can identify the Node Management URL from your Management Console URL as follows:

If your Management Console URL is <https://maxonzm.euclkt.cloud/account/index.html#login>

Then your Node Management URL is  
euc1.lkt.cloud

**Enter the default option shown or enter the URL for this installation.**

Management Server endpoint: <**Node Management endpoint URL**>

**Enter ID for this tenant.**

Input Tenant Id: <**tenant name**>

**Enter the unique name for the Node Server.**

Input Node Server Unique Name: <**node\_name**>

**Enter the API token (click the API Token button in the Configuration tab).**

Input Node Server Token: <**Node API token**>

There are 3 NICS assigned to this host.

- 1) *NIC\_n*
- 2) *NIC\_n*
- 3) <*NIC\_n*>

Please select an option from the above list

**Select an NIC option.**

NIC option (1 to 3): <**n**>

Selected NIC is <*NIC\_n*>

Adding new property ms.endpoint.

Adding new property node.name.

Adding new property node.token.plain.

Adding new property node.nic.

Updating property logging.config

Updating property logging.config

Updating property logging.config

Updating property logging.config

Node server installation is done. Start node server using 'sudo service node-server start'.

## Starting the connector

Run the following command:

```
sudo service node-server start
```

## Restarting and uninstalling the connector

### Restarting

Run the following command:

```
[root@localhost node-server]#sudo systemctl restart node-server
```

### Uninstalling

Run the following command:

```
rpm -ev enterprise-connector
```

## Additional configuration notes for SIEM

- WSG configurations are based on the installing region.
- For SIEM, the spooling directory path should be under **/opt/ciphercloud/node-server**. The directory does not need to be created manually. In the SIEM configuration, provide the directory path and name — for example, **/opt/ciphercloud/node-server/siempooldir**.

## Additional configuration notes for log agents

### Connecting to a different server

KACS and WSG configuration are provided by default. If you need to connect to a different server, use the following commands to override the server and port information.

```
[root@localhost log-agent]# cat /opt/ciphercloud/node-server/config/log-
agent/log-agent.conf
```

```
JAVA_OPTS=-Xms7682m -Xmx7682m -Dkacs.host=kacs.devqa.ciphercloud.in -
Dkacs.port=8987 -Dwsg.host=wsg.devqa.ciphercloud.in -Dwsg.port=8980
```

### Write permissions

If needed, provide the ccns user with write permissions for the spooling directories.

## Additional configuration notes for EDLP

KACS and WSG configurations are based on the installing region.

## Adding Advanced Threat Protection (ATP) services

From this page, you can create and manage configurations to integrate with vendors for advanced threat protection. CASB supports Juniper ATP Cloud and FireEye ATP services.

- From the **Enterprise Integration** page, choose **Threat Management**.
- To display details of a configuration, click the > arrow to the left for that configuration.

## To add a new configuration for threat management:

- Click **New**.

The screenshot shows a configuration dialog with the following fields:

- Name:** Name (highlighted with an orange border)
- Description:** Description
- Vendor:** FireEye
- Service URL:** Service URL (highlighted with an orange border)
- API Key:** API Key (highlighted with an orange border)

Below these fields is a section titled "File Extension and Size Settings" containing two toggle switches:

- File Type Exclusion:** On (green switch)
- File Size Exclusion:** On (green switch)

- Enter the following information. Fields with a colored border at the left require a value.

- Name** -- The name of the service. The name you enter here will appear in the dropdown list of available external services when you create a policy that scans for malware.
- Description (optional)** -- Enter a description of the service.
- Vendor** -- Select a vendor from the list, either FireEye or Juniper Networks (Juniper ATP Cloud).

The screenshot shows a dropdown menu with the following options:

- Vendor:** FireEye
- Service URL:** FireEye (highlighted with a blue checkmark)
- API Key:** Juniper Networks

- Service URL** -- Enter the URL of the service for this configuration.
- API key** -- Enter the API key provided by the service. You can opt to show or hide this key. When the key is hidden, Xs appear for the entry.

>	SkyATP1	Juniper...	https://api.sky.juniper...	Xxxxxxxxxxxxxx	<b>SHOW</b>		
>	FireEye	FireEy...	FireEye	https://feapi.marketpl...	<b>HIDE</b>		

- If you want to exclude file sizes and extensions from scanning by this service, click the **File Type Exclusion** and **File Size Exclusion** toggles to enable these settings. Then, enter the following information.

- For **File Type Exclusion**, enter types of files to be excluded from scanning. Separate each type with a comma.

The screenshot shows the following configuration:

- File Type Exclusion:** On (green switch)
- File types to exclude from scanning:** Enter file types separated by a comma (e.g. pdf, txt)

Below this is a preview area showing a list of file types:

- gpE
- Ywc
- zwr
- eg6
- 2aP
- uqe

- For **File Size Exclusion**, enter a number greater than zero that represents the upper file size threshold for scanning. Files larger than this size will not be scanned.



4. Click **Save**.

The new configuration is added to the list. A successful connection is indicated by a green connector icon.



## Adding external services for Enterprise Data Loss Prevention (EDLP)

You can configure CASB to work with external services to manage user data, gather information about unsanctioned cloud applications, and other functions.

Many organizations have made a significant investment in an enterprise DLP (EDLP) solution. This investment not only counts the capital expenditure on the software and support but also the person-hours and intellectual capital to craft policies that meet the organization's needs. By adding a CASB to an organization, you can extend the access boundary from the endpoint, where traditional enterprise DLP lives, to the cloud and SaaS.

When CASB is integrated with an EDLP solution, policies can be configured to do the initial check on the CASB DLP, and then pass the file/data to the EDLP. Or it can pass everything to the EDLP or a combination of the two.

After the file/data inspection is complete, the policy action is taken. Examples of policy actions include these:

- Encryption
- Deny upload
- Watermarking
- Quarantine
- Allow and log
- User remediation
- Replace file with a marker file

The following topics provide instructions for configuring external services for data loss prevention.

- Creating a new configuration for EDLP
- Downloading and installing an EDLP agent
- Stopping and starting the EDLP agent
- Symantec DLP response rule configuration for Vontu service

## Creating a new configuration for EDLP

1. In the Management Console, go to **Administration > Enterprise Integration > Data Loss Prevention**.
2. Click **New**.
3. Enter the following configuration details. (The values shown are examples.)

Name: EDLP\_Sym  
Description: Description  
Vendor: Symantec  
DLP Server Hostname: 172.\*\*\*  
Service Name: 172.\*\*\*  
ICAP Port: 1

Specify the file size and extensions to exclude

File Type Exclusion:   
File Size Exclusion:

**Save** **Cancel**

- **Name** -- Enter a name for this EDLP service.
  - **Description (optional)** -- Enter a brief description.
  - **Vendor** – Select an external DLP vendor. The options are Symantec or Forcepoint.
  - **DLP Server Hostname** -- Enter the host name or IP address of the server to be used for the external DLP.
  - **Service Name** -- Enter the name or IP address of the service that applies to this configuration.
  - **ICAP port** -- Enter the number for the associated Internet Content Management Protocol (ICAP) server. ICAP servers focus on specific issues such as virus scanning or content filtering.
4. To exclude any file types or size from EDLP scanning, click the toggles to enable exclusions. Then, enter the appropriate file information.

Specify the file size and extensions to exclude

File Type Exclusion:

List file types to exclude from scanning:  
.mp4,.ASF,.MP3,.ASF.GIF,.MOV,.TIFF,.FLV,.MKV,.SWF,.GIF,.WMV,.AVI,.MPG,.DIVX,.BMP

File Size Exclusion:

File Size Exclusion: 10 MB

- For file types, enter the extensions for the file types to exclude, separating each extension by a comma.
  - For file size, enter the maximum file size (in megabytes) to exclude.
5. Click **Save**.

The new configuration is added to the list. Once an agent is downloaded and installed, a connection can be made. A successful connection is indicated on the **Data Loss Prevention** page by a green connector icon.

## Downloading and installing an EDLP agent

After you create at least one EDLP agent, you can download the EDLP agent and install it on a machine or server. The machine you choose for the EDLP agent installation should contain RedHat Enterprise / CentOS 7.x and Java 1.8.

### Prerequisites for installing the EDLP agent

Your environment must include the following components and settings for installing and running the EDLP agent:

- Oracle Server Java 17 or later
- JAVA\_HOME environment variable set
- root or sudo privileges
- Hardware – 4 Core, 8 GB RAM, 100 GB storage

Perform the steps outlined in the following sections to download, install, and start the EDLP agent.

### Downloading the EDLP agent

1. In the Management Console, go to **Administration > System Settings > Downloads**.
2. Select **EDLP Agent** from the list and click the **Download** icon under Actions.



To view information about the file, including version, size, and checksum value, click the Information icon.



The EDLP agent is downloaded as **ciphercloud-edlpagent-20.07.0.22.centos7.x86\_64.rpm**.

3. Move the EDLP agent to its intended machine.

### Installing the EDLP agent

1. From the command line, run the following command:

```
rpm -ivh <RPM Name>
```

For example:

```
rpm -ivh ciphercloud-edlpagent-20.07.0.22.centos7.x86_64.rpm
Preparing... ##### [100%]
Preparing / installing...
1:ciphercloud-edlpagent-20.07.0.22.centos7.x86_64#####
## [100%]
Execute 'EDLP-setup' to setup your EDLP Agent
```

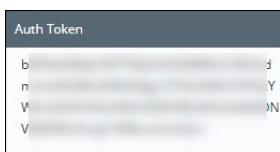
The RPM client will be installed under the following location:

**/opt/ciphercloud/edlp**

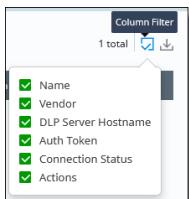
2. Go to the **/opt/ciphercloud/edlp/bin** directory.
3. Run the setup file using the following command:  

```
./edlp_setup.sh
```
4. When prompted, enter the auth token to complete the installation process.

To get the auth token, go to **Administration > Enterprise Integration > Data Loss Prevention (Auth Token column)**.



To hide the auth token from view, click the **Column Filter** icon at the upper right, and uncheck **Auth Token**.



#### Note

You can access logs from the **/opt/ciphercloud/edlp/logs** directory.

## Stopping and starting the EDLP agent service

- To **stop** the EDLP agent service, enter the following command:  

```
systemctl stop ciphercloud-edlp
```
- To **start** the EDLP agent service, enter the following command:  

```
systemctl start ciphercloud-edlp
```

## Checking the EDLP agent status

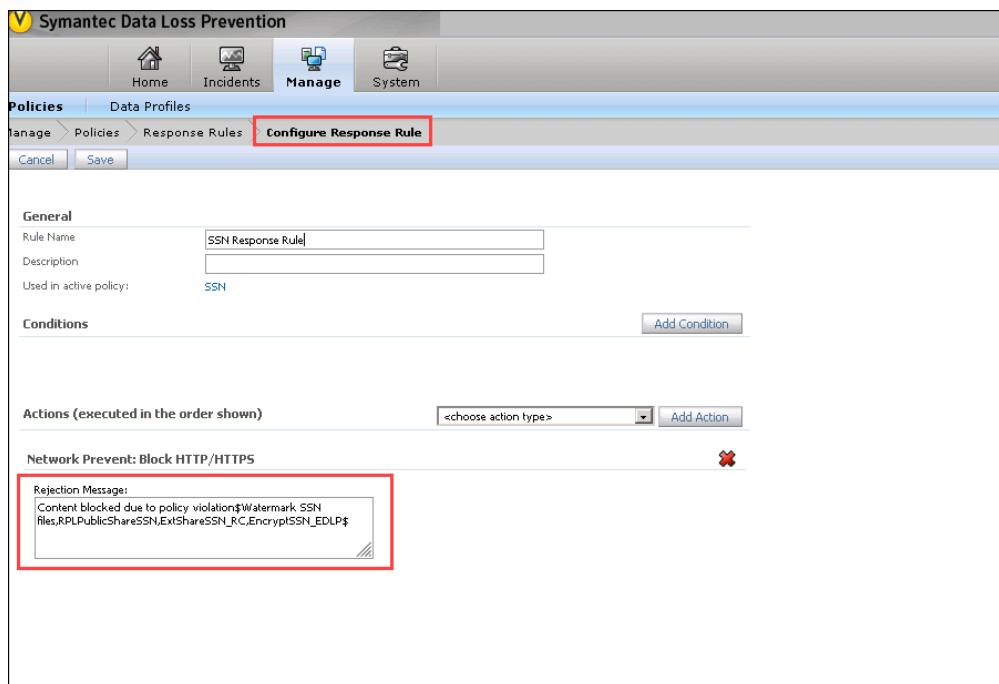
- To **check the status of** the EDLP agent service, enter the following command:  

```
systemctl status ciphercloud-edlp
```

## Symantec DLP response rule configuration (Vontu service)

In the Symantec DLP configuration (**Manage** tab / **Configure Response Rule**), you need to enter information about the violation and the policies violated, as shown, with violation as the keyword. Enclose the name of each violated policy between dollar signs, separated by commas. The policy name or names should be exactly the same as they are entered in CASB. Format the policy entries as follows:

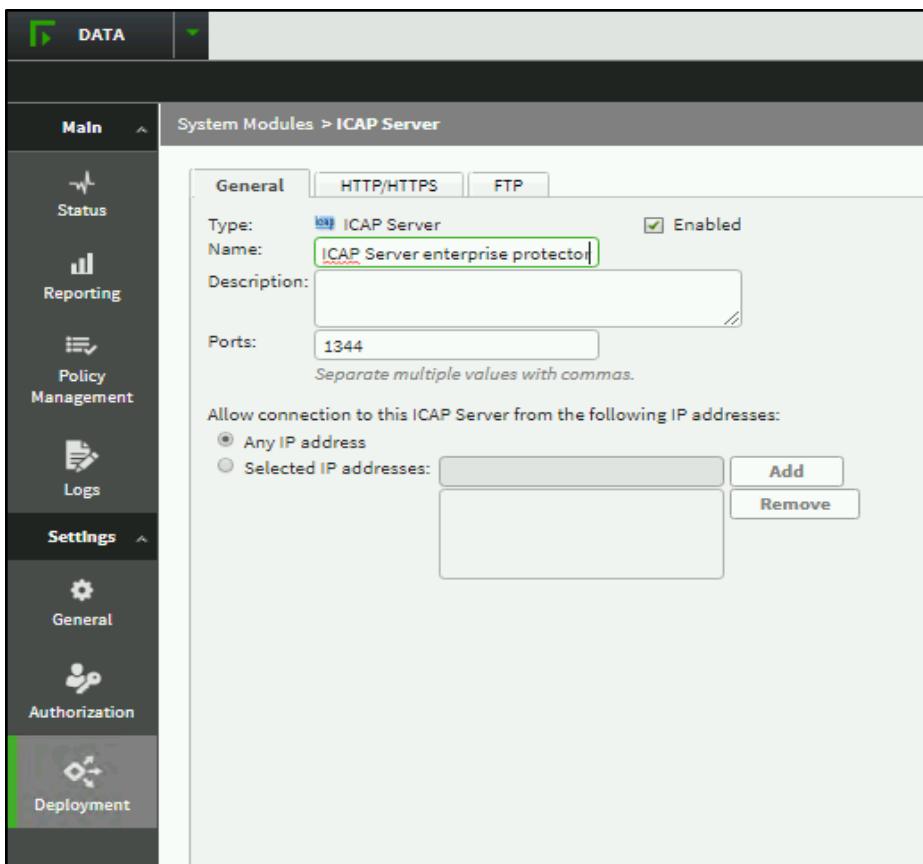
\$PolicyNameA, PolicyNameB, PolicyNameC\$



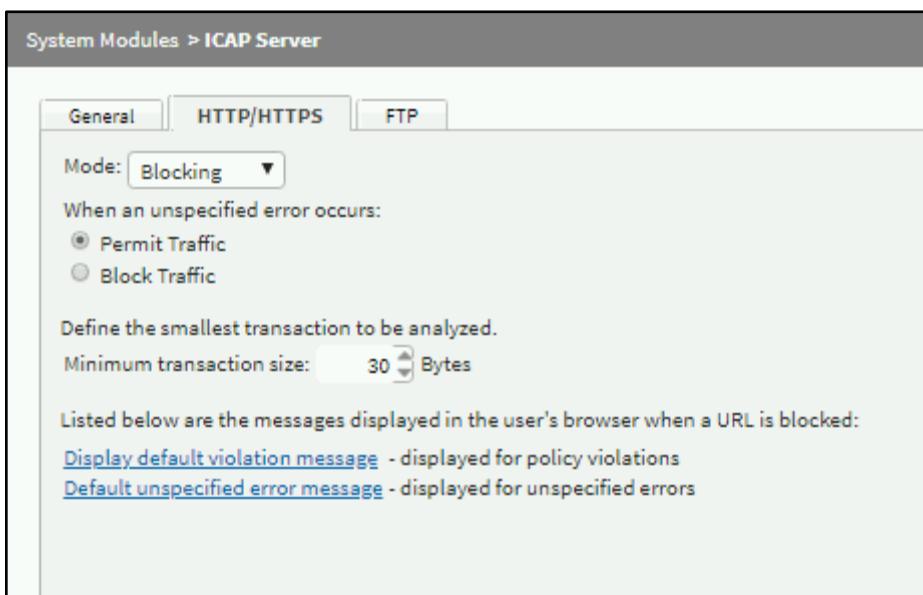
## Configuring the Forcepoint Security Manager and Protector

Perform the following steps to configure the Forcepoint Security Manager and Protector:

1. In the **General** tab, enable the ICAP system module with the default port of 1344.



2. In the **HTTP/HTTPS** tab, set the mode to **Blocking** for the ICAP server.



3. Under **Policy Management**, add a new policy from the Predefined policy list or create a custom policy. Then, deploy the new policy.

## Remotely upgrading the SIEM, EDLP, and Log Agents

### Remote upgrade considerations

Review the following upgrade considerations before performing the remote upgrade of SIEM, EDLP, and Log Agent.

Supported Operating Systems	<ul style="list-style-type: none"> <li>RHEL 8.8</li> <li>CentOS 8</li> </ul>
Supported upgrade path	v22.10.xx to v23.1.1

### Remote upgrade steps for SIEM, EDLP, and Log agents

Perform these steps to remotely upgrade the enterprise connector (SIEM, EDLP, and Log Agent):

- From the Management Console, go to **Administration > Environment Management**.
- Locate the environment associated with the agent services (SIEM, EDLP, or Log Agent), and click on the upgrade icon from the **Version** column.

All the nodes associated with the environment will be upgraded.

**Note:** If the remote upgrade fails, the connector will be rolled back to the previous working version.

# Manually upgrading the SIEM, EDLP, and Log Agents

Depending on your OS and the type of package that you want to install, perform the steps in the following sections to upgrade the on-premises connectors manually. This manual upgrade procedure is applicable for EDLP, SIEM, and Log Agent.

## For CentOS and RHEL

If you installed the rpm package in the previous version, upgrade the connector using an RPM package. For instructions, see the [Upgrading a connector using an RPM package](#) section.

### Upgrading a connector using an RPM package

1. From the **Management Console**, go to **Administration > System Settings > Downloads**.
2. Click the download icon  for the **On-premise Connector** rpm package.

System Settings				
Software Downloads				
Knowledge Base	EDLP Agent	22.03.0.303.cen tos7.x86_64	CipherCloud EDLP Agent	6/7/2022
User Privacy	EDM Data Hashing Tool	22.03.0.002	CipherCloud EDM Data Hashing Tool	6/7/2022
GDPR Configuration	HKMS	22.03.0.47.x86_64	Hybrid Key Management System	6/8/2022
Groups of Interest	HKMS Tar Package	22.03.0.47	Hybrid Key Management System Package for Upgrade	6/8/2022
Software	Log Agent	22.03.0.373.cen tos7.x86_64	CipherCloud Log Agent	6/7/2022
Downloads	Node Server	22.03.0.227.x86_64	Node Server RPM	6/8/2022
Sanctioned Cloud Configuration	Node Server Tar Package	22.03.0.227	Node Server Package for Upgrade	6/8/2022
General Configuration	On-premise Connector	22.03.0.227.x86_64	On-premise Connector	6/8/2022
Blacklisted Emails	On-premise Connector - Debian	22.03.0.227.am d64	On-premise Connector - Debian package for Ubuntu	6/8/2022
Device Settings				
IP Risk Configuration				
Enterprise Authentication				

3. Copy the downloaded RPM package to the Node Server on which you want to install.
4. Log in to the Node Server.
5. Stop the Node Server services:

```
sudo service node-server stop
```

6. Run the following command:

```
sudo yum install epel-release
```

7. Run the following command to upgrade the connector:

```
sudo yum upgrade ./enterprise-connector*.rpm
```

8. Start the Node server services:

```
sudo service node-server start
```

## For Ubuntu

If your previous connector was installed using a **Tar** package, to get the latest connector version, you can either perform a fresh installation using a Debian package (Method 1) or upgrade the connector using a **Tar** package (Method 2).

If your previous connector was installed using a Debian package, you can upgrade the connector using a Debian package (Method 3).

### Method 1 (Recommended): Installing the latest connector version using a Debian package

If your previous connector was installed using a **Tar** package, to get the latest connector version, you can perform a fresh installation of the latest connector version using a **Debian** package. Detailed steps for this procedure are provided below.

#### Pros:

- You can use **service/systemctl** commands to start/stop the services.
- Additional dependencies required for other features are automatically installed by the **apt** command.

#### Cons:

- As this is a fresh installation, you are required to run install.sh script.
- Provide the details such as nodeName, authToken etc, during the installation.

### Method 2: Upgrading a connector using a Tar package

**Pros:**

- No need to run the `install.sh` script again.

**Cons:**

- You need to use the `sudo bash <script>` command for any start/stop operations.
- Before untarring the **TAR** package in the `opt/ciphercloud` directory, you need to delete the old `boot-ec-*jar` file.

### Method 3: Upgrading a connector using a Debian package

Use this procedure if your previous connector was installed using a Debian package.

### Method 1: Installing the latest connector version using a Debian package

**Note:** If you have already installed any connector on your machine using a Tar package, stop the Node Server services and delete the `ciphercloud` directory located under the `opt` directory before starting this procedure.

1. From the **Management Console**, go to **Administration > System Settings > Downloads**.
2. Click the download icon  for the **On-premise Connector - Debian** package.
3. Copy the downloaded Debian package to the Node Server on which you want to install.
4. Log in to the Node server.
5. Run the following command to start the installation in the Linux instance:

```
[ubuntu@localhost home]# sudo apt install ./enterprise-
connector_<version>_amd64.deb
```

Where `<version>` is the current DEB file version in the Management Console.

Note: Make sure you are connected to the internet while performing this installation.

6. Click **Yes** when prompted to save the IPv4 and IPv6 rules.
  7. Run the following command to change to the directory in which to install the connector.
- ```
cd /opt/ciphercloud/node-server
```
8. Run the following command to configure the installation options.

```
./install.sh
```

System response:

```
Initializing node-server install script. Please wait..
```

9. Respond to the system prompts as follows:

```
Please enter Management Server endpoint
```

[wss://nm.<domain>:443/nodeManagement] :

- a. Enter the default option shown or enter the URL for this installation.
- b. Management Server endpoint: <**Node Management endpoint URL**>
- c. Enter the unique ID for this tenant.  
Input Tenant Id: <**tenant name**>
- c. Enter the unique name for the Node Server.  
Input Node Server Unique Name: <**node\_name**>
- d. Enter the API token (click the **API Token** button in the **Configuration** tab)  
Input Node Server Token: <**Node API token**>

Once Node server installation is done. Start node server using 'sudo service node-server start'.

- e. Select **Y** to install with upstream proxy and enter the upstream proxy details.

**Note** If you do not want to use the upstream proxy, specify **N** and press **Enter**.

Does upstream proxy exist? [y/n]: y

Input Host Name of upstream proxy server: 192.168.222.147

Input port number of upstream proxy server: 3128

- f. Enter the username and password if you want to enable the upstream proxy with authorization. Otherwise, press Enter.

Input upstream proxy authorization - user name (Press enter key if no authorization required): **test**

Input upstream proxy authorization - password: **test@12763**

10. Run the following command to start the Node Server:

```
sudo service node-server start
```

## Method 2: Upgrading a connector using a Tar package

**Note:** If you are on the Ubuntu OS, we recommend that you install the latest Debian package. For instructions, see [Installing a new connector with Debian package](#).

1. From the **Management Console**, go to **Administration > System Settings > Downloads**.

2. Click the download icon  for the **On-premise Connector Tar Package**.

3. Copy the downloaded **Tar** package to the Node Server on which you want to upgrade.

4. Log in to the Node Server.

5. Stop the Node Server services using the following command:

```
sudo bash /opt/ciphercloud/node-server/bin/agent/agent stop
```

6. Make a backup copy of the **boot-ec-\*jar** file and save it to a different location.

7. Delete the **boot-ec-verion.jar** file from the /opt/ciphercloud/node-server/lib directory.

8. Untar the **On-premise Connector Tar package** to /opt/ciphercloud:

```
sudo tar -xvf enterprise-connector-<version>.tar.gz --directory /opt/ciphercloud
```

---

```
sudo chown -R ccns:ccns /opt/ciphercloud/node-server
```

This action extracts the contents to the **node-server** directory.

9. Start the Node Server services:

```
sudo bash /opt/ciphercloud/node-server/bin/agent/agent start
```

### Method 3: Upgrading a connector using a Debian package

If your previous connector on the Ubuntu OS was installed using a Debian package, use this procedure for upgrading your connector.

1. From the **Management Console**, go to **Administration > System Settings > Downloads**.
  2. Click the download icon  for the **On-premise Connector - Debian** package.
  3. Copy the downloaded Debian package to the Node Server on which you want to install.
  4. Log in to the Node Server.
  5. Stop the Node Server services:
- ```
sudo service node-server stop
```
6. Run the following command to upgrade the connector:
- ```
sudo apt upgrade ./enterprise-connector*.deb
```
7. Click **Yes** when prompted to save the IPv4 and IPv6 rules.
  8. Start the Node Server services:
- ```
sudo service node-server start
```

## Configuring Security Information and Event Management (SIEM)

From the **Enterprise Integration** page, click **SIEM**.

To view the details of an existing SIEM configuration, click the **>** icon at the left.

### Downloading, installing, and connecting a SIEM agent

After you create at least one SIEM agent, you can download the SIEM agent and install it on a machine or server. The machine you choose for SIEM agent installation should contain RedHat Enterprise / CentOS 7.x, as well as Java 1.8.

If the data you intend to run using the SIEM agent is a directory or file, the SIEM agent must be downloaded to the machine where the files are located.

## Prerequisites for installation of an SIEM agent

Your environment must include the following components and settings for installing and running an SIEM agent:

- Oracle Server Java 17 or later
- JAVA\_HOME environment variable set
- root or sudo privileges

Perform the following steps to download, install, and start a SIEM agent.

## Downloading

1. In the Management Console, select **Administration > Enterprise Integration**.
2. Click the **Download** icon in the row of the SIEM agent you are downloading.  
The SIEM agent is downloaded as **ciphercloud-siemagent-1709\_rc2-1.x86\_64.rpm**.
3. Move the SIEM agent to its intended machine (or to multiple machines as needed).

## Installing

From the command line, run the following command:

```
rpm -ivh <RPM Name>
```

For example:

```
rpm -ivh ciphercloud-siemagent-1709_rc2-1.x86_64.rpm
Preparing... #####
[100%]
Preparing / installing...
1:ciphercloud-siemagent-1709_rc2-1.x86_64#####
[100%]
Execute 'siemagent-setup' to setup your siem Agent
```

## Configuring

Run the **siemagent** setup command to configure the SIEM-agent and paste the authentication token, as outlined in the following instructions.

```
siemagent-setup
```

for example:

```
siemagent-setup
Enter Auth Token:<Auth token>
Initiating CipherCloud siem Agent configuration
Java already configured
Updated CipherCloud siem Agent with Auth Token
Starting CipherCloud siem Agent Service ...
Already Stopped / Not running (pid not found)
Started Log Agent with PID 23121
```

---

Done

## Viewing the authentication token

1. Go to **Administration > Enterprise Integration > SIEM**.
2. Select the SIEM agent you created.
3. In the **Display Auth Token** column, click **Show** to display the token.

## Uninstalling a SIEM agent

To uninstall the SIEM agent, run the following command:

```
rpm -e <RPM name up to x86_64>
```

For example:

```
rpm -e ciphercloud-siemagent-1709_rc2-1.x86_64
Stopped [12972]
Package ciphercloud-logagent with version 1709 has been uninstalled
successfully
```

## Starting, stopping, and checking the status of a SIEM agent

To start an SIEM agent, enter the following command:

```
systemctl start ciphercloud-siemagent
```

To stop an SIEM agent, enter the following command:

```
systemctl stop ciphercloud-siemagent
```

To check the status of an SIEM agent, enter the following command:

```
systemctl status ciphercloud-siemagent
```

## Viewing SIEM agent logs

Go to **/opt/ciphercloud/siemagent/logs/**

## Creating a new SIEM configuration

To create a new SIEM configuration, perform the following steps.

1. From the **Enterprise Integration** page, click **SIEM** and then click **New**.
2. Enter the following information.
  - **Name** (required) – Enter a name for this configuration.
  - **Description** (optional) -- Enter a brief description.
  - **Destinations** – Select one or more destinations to which to apply this configuration. The options are:
    - SaaS Apps (select the category, or expand it to select individual apps)

- Enterprise Apps (select the category, or expand it to select individual apps)
  - Websites (select the category, or expand it to select individual sites)
  - Networks (select the category, or expand it to select individual networks)
  - Admin Audit Logs
  - **Event Type** – Select one or more event types for this configuration. The options are:
    - Activities
    - Violations
    - Anomalies
    - CDD Activities
    - CDD Violations
    - Security Posture
    - Discovery
  - **Vendor** -- Select a vendor. The options are
    - HP ArcSight
    - IBM QRadar
    - Intel Security
    - Log Rhythm
    - Others
    - Splunk
  - **Forwarded Type** -- Select **Spooling Directory**, **Syslog TCP**, or **Syslog UDP**.
    - For **Spooling Directory**, enter the directory path for the log files generated.
    - For **Syslog TCP** or **Syslog UDP**, enter a remote host name, a port number, and a log format (**JSON**, **CEF**, or **CEF\_V2**).
3. Click **Save**.

The new configuration is added to the list. By default, the authentication token is hidden. To display it, click **Show**.

Once an agent is downloaded and installed, a connection can be made. A successful connection is indicated on the SIEM page by a green connector icon.

## Additional actions

In addition to the download action, the **Action** column provides the following two options:

- **Pause** – Pauses the transfer of events to SIEM. When this button is clicked and the agent is paused, the tool tip changes the button label to **Resume**. To resume the transfer, click the button again.
- **Delete** – Deletes the agent.

## Configuring data classification

CASB enables integration with Azure Information Protection (AIP), Google, and Titus for data classification. The following sections outline how to configure these integrations.

## Integration with Azure Information Protection (AIP)

CASB enables integration with Microsoft Azure Information Protection (AIP), which provides additional options for protecting your data. If you have a Microsoft Office account, you can use your Microsoft 365 credentials to add an AIP integration connection and apply it as an action to any policy you create, for any of your cloud applications.

AIP enables use of Active Directory Rights Management Services (AD RMS, also known as RMS), which is server software that addresses information rights management. RMS applies encryption and other functionality limitations for various types of documents (for example, Microsoft Word documents), to restrict what users can do with the documents. You can use RMS templates to protect an encrypted document from being decrypted by specific users or groups. RMS templates group these rights together.

When you create an AIP integration connection, content policies you create provide an **RMS Protection** action that applies protection as specified in the RMS template you choose for the policy.

You can use labels to identify specific types of protection to the documents in your cloud. You can add labels to existing documents or assign or modify labels when the documents are created. Labels are included in the information for the policies you create. When you create a new label, you can click the **Sync Labels** icon in the **AIP Configuration** page to synchronize your labels and enable the newest labels to be assigned.

### Retrieving parameters required for AIP RMS connection

**To enable access to the required parameters:**

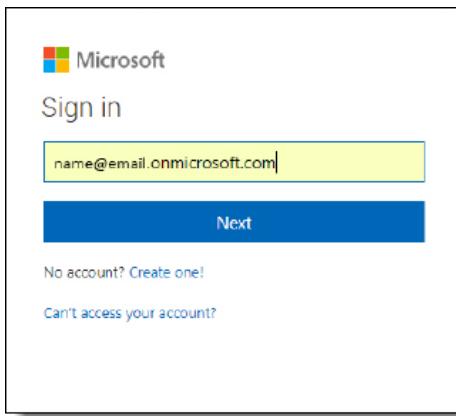
1. Open Windows PowerShell in administrator mode.
2. Run the following command to install the AIP cmdlets. (This action will take a few minutes to complete.)

```
Install-Module -Name AADRM
```

3. Enter the following cmdlet to connect to the service:

```
Connect-AadrmService
```

4. In response to the authentication prompt, enter your Microsoft Azure AIP login credentials.



5. Once you are authenticated, enter the following cmdlet:

```
Get-AadrmConfiguration
```

The following configuration details are displayed

BPOSID :  
9c11c87a-ac8b-46a3-8d5c-f4d0b72ee29a

RightsManagementServiceId :  
5c6bb73b-1038-4eec-863d-49bded473437

LicensingIntranetDistributionPointUrl :  
[https://5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com/\\_wmcs/licensing](https://5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com/_wmcs/licensing)

LicensingExtranetDistributionPointUrl :  
[https://5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com/\\_wmcs/licensing](https://5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com/_wmcs/licensing)

CertificationIntranetDistributionPointUrl :  
[https://5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com/\\_wmcs/certification](https://5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com/_wmcs/certification)

CertificationExtranetDistributionPointUrl:  
[https://5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com/\\_wmcs/certification](https://5c6bb73b-1038-4eec-863d-49bded473437.rms.na.aadrm.com/_wmcs/certification)

AdminConnectionUrl :  
<https://admin.na.aadrm.com/admin/admin.svc/Tenants/5c6bb73b-1038-4eec-863d-49bded473437>

AdminV2ConnectionUrl :  
<https://admin.na.aadrm.com/adminV2/admin.svc/Tenants/5c6bb73b-1038-4eec-863d-49bded473437>

OnPremiseDomainName :

Keys : {c46b5d49-1c4c-4a79-83d1-ec12a25f3134}

CurrentLicensorCertificateGuid :  
c46b5d49-1c4c-4a79-83d1-ec12a25f3134

Templates : { c46b5d49-1c4c-4a79-83d1-ec12a25f3134,

5c6d36g9-c24e-4222-7786e-b1a8a1ecab60 }

FunctionalState : Enabled

```

SuperUsersEnabled : Disabled

SuperUsers : {admin3@contoso.com, admin4@contoso.com}

AdminRoleMembers :
{Global Administrator -> 5834f4d6-35d2-455b-a134-75d4cdc82172,
ConnectorAdministrator -> 5834f4d6-35d2-455b-a134-75d4cdc82172}

KeyRolloverCount : 0

ProvisioningDate : 1/30/2014 9:01:31 PM

IPCV3ServiceFunctionalState : Enabled

DevicePlatformState :
{Windows -> True, WindowsStore -> True, WindowsPhone -> True, Mac ->

FciEnabledForConnectorAuthorization : True
DocumentTrackingFeatureState : Enabled

```

From this output, you will need the highlighted items for the AIP integration connection.

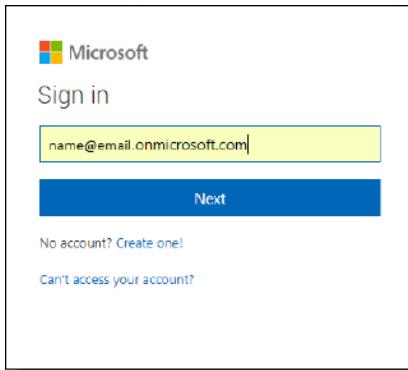
- Run the following command to obtain the base 64 key information:

```
install-module MSOnline
```

- Run the following command to connect to the service:

```
Connect-MsolService
```

- In response to the authentication prompt, enter your Azure AIP login credentials again.



- Run the following command:

```
Import-Module MSOnline
```

- Run the following command to obtain the key information needed for the AIP integration connection:

### New-MsolServicePrincipal

The following information is displayed, which includes the key type (Symmetric) and key ID.

```
cmdlet New-MsolServicePrincipal at command pipeline position 1
Supply values for the following parameters:
```

11. Enter a display name of your choice.

DisplayName: **Sainath-temp**

The following information is displayed. You will need the highlighted information when you create the AIP integration connection.

The following symmetric key was created as one was not supplied  
**qWQikkTF0D/pbTFleTDBQesDhfvRGJhX+S1TTzzUZTM=**

DisplayName	:	Sainath-temp
ServicePrincipalNames	:	{06a86d39-b561-4c69-8849-353f02d85e66}
ObjectId	:	edbad2f2-1c72-4553-9687-8a6988af450f
<b>AppPrincipalId</b>	:	<b>06a86d39-b561-4c69-8849-353f02d85e66</b>
TrustedForDelegation	:	False
AccountEnabled	:	True
Addresses	:	{ }
KeyType	:	Symmetric
KeyId	:	298390e9-902a-49f1-b239-f00688aa89d6
StartDate	:	7/3/2018 8:34:49 AM
EndDate	:	7/3/2019 8:34:49 AM
Usage	:	Verify

## Configuring AIP protection

Once you have retrieved the parameters needed for the connection, you can create the connection in the Azure AIP page.

### To enable AIP configuration:

1. Go to **Administration > Enterprise Integration**.
2. Select **Data Classification**.
3. If the **Azure Information Protection** tab is not displayed, click it.
4. Click the toggle to enable Azure Information Protection configuration.
5. Once AIP configuration is enabled, the **Authorize** button appears for you to access Azure information. (If you have authorized previously, the button is labeled **Re-Authorize**.)
6. When the Microsoft login page appears, follow the prompts to enter your Microsoft login credentials.

## Syncing labels

When a cloud application is onboarded in CASB, you can create new policies or assign policies in Azure. You can sync Azure labels instantly from the **AIP Configuration** page. These labels will be listed with the policy information in the Management Console.

### To sync labels:

1. Go to **Administration > Enterprise Integration > Data Classification > Azure Information Protection**.
2. Click the **Sync** icon at the right above the list of labels to obtain the most recent Azure labels.

When the sync is completed, the newly added labels are displayed, and are ready to be assigned. The date of the last sync action appears next to the Sync icon.

### Label information

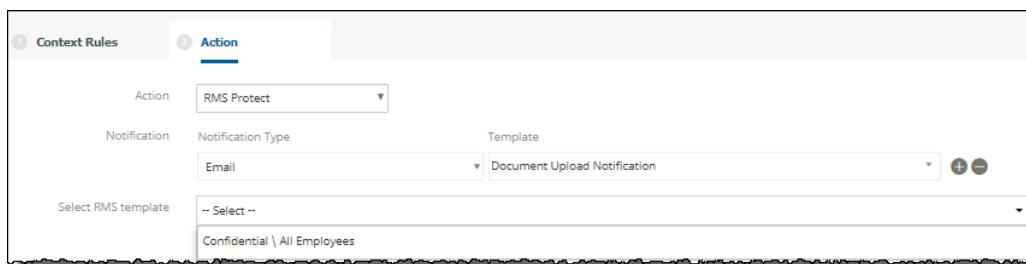
Labels are listed in a table in the lower part of the **AIP Configuration** page. For each label, the list includes the label name, description, and active status (true=active; false=not active). Depending on how the label was configured, the table might include additional details (AIP Tooltip), a sensitivity level, and the label's parent name.

To search for a label in the list, enter all or part of the label name in the Search box above the list, and click the **Search** icon.

### Creating a policy with RMS protection

Once you have created an AIP connection, you can create or update a policy to include RMS protection for your documents. Perform the following steps to create a policy for RMS protection. For more information about options for policy types, content rules, and context rules, see [Configuring Juniper Secure Edge CASB for policy management](#).

1. Create a policy.
2. Enter a name and a description for the policy.
3. Select content and context rules for the policy.
4. Under **Actions**, select **RMS Protect**.



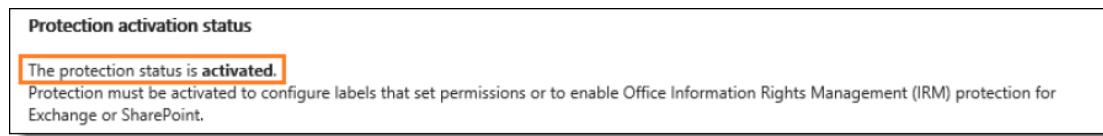
5. Select a **notification** type and template.
6. Select an **RMS template** for the policy. The template you select applies specific protections to the documents. Examples of predefined templates include those listed here. You can create additional templates as needed.
  - **Confidential \ All Employees** -- Confidential data that requires protection, which allows all employees full permissions. Data owners can track and revoke content.
  - **Highly Confidential \ All Employees** -- Highly confidential data that allows employees view, edit, and reply permissions. Data owners can track and revoke content.
  - **General** -- Business data that is not intended for public consumption but that can be shared with external partners as required. Examples include a company internal telephone directory, organizational charts, internal standards, and most internal communication.

- **Confidential** -- Sensitive business data that could cause damage to the business if shared with unauthorized people. Examples include contracts, security reports, forecast summaries, and sales account data.
7. Confirm the policy information and save the policy.

When users open a protected document, the policy will apply the protections specified in the RMS protection action.

## Creating additional RMS policy templates

1. Log in to the Azure portal.
2. Go to **Azure Information Protection**.
3. Verify that the service is active by reviewing the protection activation status.



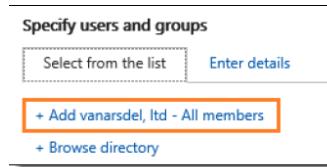
4. If the service is not activated, select **Activate**.
5. Enter a name (label) for the template you want to create.
6. Select **Protect**.



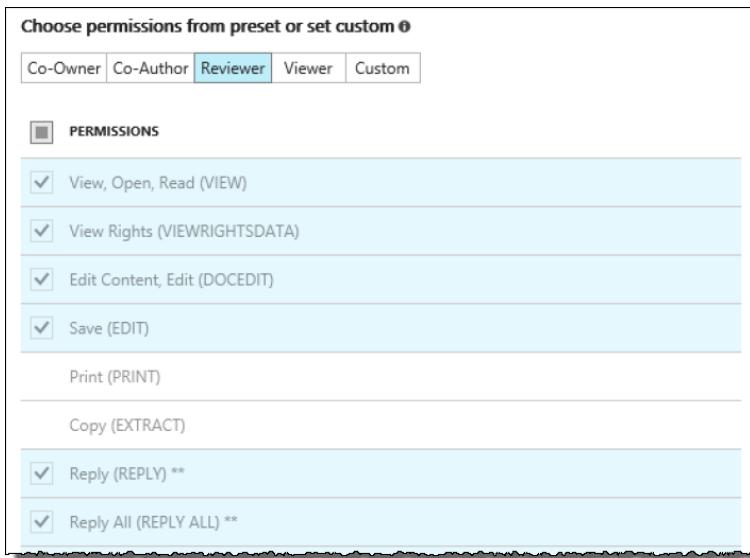
7. Select **Protection**.
8. Select **Azure (cloud key)** to use the Azure Rights Management service for protection of documents.



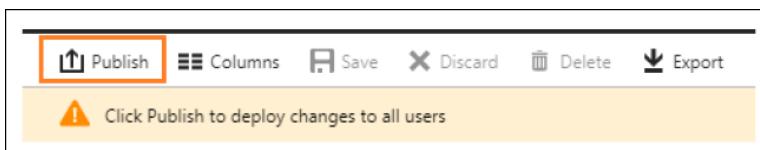
9. Select **Add Permissions** to specify user permissions.



10. From the **Select from List** tab, choose either
  - **<organization\_name> - all members**, which includes all users in your organization, or
  - **Browse directory** to search for specific groups.
 To search for individual email addresses, click the **Enter Details** tab.
11. Under **Choose Permissions from preset or custom**, select one of the permission levels, then use the check boxes to specify the types of permissions.



12. Click **OK** when you are finished adding permissions.
13. To apply the permissions, click **Publish**, then click **Yes** to confirm.



The template is added to the dropdown list for the **RMS Protect** action.

## Integration with Google

CASB can integrate with Google's classification functionality, which provides additional options for securing your data. If you have enabled labels in your Google Suite account, CASB can provide control over your users' use of labels.

You can create policies within CASB to:

- Automatically apply labels to files in Google Suite, and apply specified values to the fields within a label
- Detect labels and label field values that users have added to files, and take appropriate actions on those files

To begin, enable the labels feature on your Google account, create some labels, and enable CASB to read the labels and their associated data from your Google account. You can then create policies within CASB to read and write the labels on your users' Google Drive files.

Keep in mind the following:

- CASB cannot modify your labels' names, field names/types, and other label-specific settings. You must do this from within your Google administration console.
- When you change or create a label, CASB receives this information almost immediately. In addition, CASB syncs labels twice a day to ensure that all label data is captured correctly.

- If you mark a label as inactive within Google Drive, that label remains in place on files that it had been applied to, and CASB can still read it. You can continue to use policies that detect an inactive label.

The following sections describe how to set up and use Google classification labels.

## Update scopes for your Google account

1. Log in to Google Drive with your administrator account.
2. Click on the Admin Console at the bottom of the page.
3. Navigate to **Security > Access and Data control > API controls > Manage domain wide delegation**.
4. Add the following OAuth Scopes (comma-delimited):
 

```
https://www.googleapis.com/auth/activity,
https://www.googleapis.com/auth/admin.directory.group,
https://www.googleapis.com/auth/admin.directory.user,
https://www.googleapis.com/auth/admin.directory.user.security,
https://www.googleapis.com/auth/admin.reports.audit.readonly,
https://www.googleapis.com/auth/drive,
https://www.googleapis.com/auth/drive.activity.readonly,
https://www.googleapis.com/auth/userinfo.email,
https://www.googleapis.com/auth/drive.labels,
https://www.googleapis.com/auth/drive.labels.readonly,
https://www.googleapis.com/auth/drive.admin.labels,
https://www.googleapis.com/auth/drive.admin.labels.readonly
```
5. Click **Authorize** to save your changes.

You must re-authorize your Google Drive account in CASB in order to capture these updates:

1. Make sure that you have already onboarded the Google account that you want to use.
2. In the CASB Management Console, navigate to **Administration > App Management**.
3. Locate the appropriate Google account and click the pencil icon to edit it.
4. On the Configuration screen, click the **Re-authorize** button and enter the appropriate credentials.
5. Click **Save**.

## Turn on labels for your Google account

Before you can begin using Google classification functionality in CASB, you must enable it on your Google account.

1. Log in to the Google Cloud console with your administrator account.
2. Navigate to API & Services > Library.
3. Use the search function to find the Drive Labels API and enable it.
4. Log in to Google Drive with your administrator account.
5. Click on the Admin Console at the bottom of the page.
6. Navigate to Apps > Google workspace > Settings for Drive and Docs > Labels.
7. Select the **Turn Labels On** option and click **Save**.

## Create labels

If you have not already done so, create some labels on your Google account.

1. Log in to [drive.google.com/labels](https://drive.google.com/labels) with your administrator account.
2. Create at least one Badged label and at least two standard labels.
3. (Optional) Create fields for any of the labels, if needed.

## Enable Data Classification for Google labels

1. Log in to Google Drive with your administrator account.
2. Click on the Admin Console at the bottom of the page.
3. Navigate to Security > Access and Data control > Data classification > Drive and Docs > Manage > Select Labels.
4. Select any label and fields that you want to manage with CASB.
5. Click **Save**.

## Enable Google Data Classification in CASB

Next, turn on Google data classification in the CASB Management Console.

1. Make sure that you have already onboarded the Google account that you want to use.
2. In the Management Console, select **Administration > Enterprise Integration > Data Classification**.
3. Select the **Google** tab.
4. From the **Google Account** drop-down, select the appropriate account.
5. Turn on the **Drive Labels** toggle.
6. CASB will retrieve the labels from your Google account. This may take some time.

## Create Policies using Google Data Classification

In CASB, you can use Google labels as follows:

- To apply a specified label or set of labels to files that match certain criteria, you can create Content Digital Rights (CDR) templates that define sets of Google classification labels, and then apply those templates to API Access policies.
- To detect which labels a user has applied to a Google Suite file, and take action accordingly on that file, you can create Document Rule Templates that define the Google labels to look for, and then apply those templates to Cloud Data Discovery policies.

### Policies to Apply Google Labels to Files

First, create a Document Rule Template as described in [Creating new document rule templates](#).

- a. On the “Define Document Rule” tab, turn on the Data Classification toggle, select Google as the label provider, and select the appropriate Google account.
- b. Select Badged or Standard from the **Type** drop-down. The relevant labels from your Google account are shown. Select a label that you want to use in your policy.
- c. If the label you selected has fields defined, specify the values to detect in the fields, if applicable.
- d. Click the plus sign icon to add additional labels.  
Note: You can apply a maximum of five labels to a file. This may be one badged label and four standard labels, or five standard labels.
- e. Specify additional settings for the template if needed.
- f. Click **Next** and then **Save** to save the template.

Next, create a policy as described in [API policies with DLP Scan or None as the content inspection type](#).

- a. In the **Destinations** pane, select the appropriate Google account.
- b. Specify context rules as desired.
- c. On the **Action** tab, under **Content Action**, select **Content Digital Rights** and then select the template that you created in the previous section.
- d. Save the policy.

The label(s) that you configured in the CDR template will be applied to files that match the policy criteria.

### Policies to Detect Google Labels on Files

First, create a CDR template as described in [Create Content Digital Rights templates](#).

- a. For the Type, select either **Documents With Encryption** or **Documents Without Encryption**.
- b. On the **Define Digital Rights** tab, select **Classification**. Select Google as the label provider, and select the appropriate Google account.
- c. Select Badged or Standard from the **Label(s)** drop-down. The relevant labels from your Google account are shown. Select a label that you want to use in your policy.
- d. If the label you selected has fields defined, specify the values to apply to the fields, if applicable.  
Note: If you leave any of the fields empty, then if a user updates those fields on a particular file, CASB will remove the user's inputs when honoring the policy.
- e. Click the plus sign icon to add additional labels.  
Note: You can apply a maximum of five labels to a file. This may be one badged label and four standard labels, or five standard labels.
- f. Click **Next** and then **Save** to save the template.

Next, create a policy as described in [Create a Cloud Data Discovery policy](#).

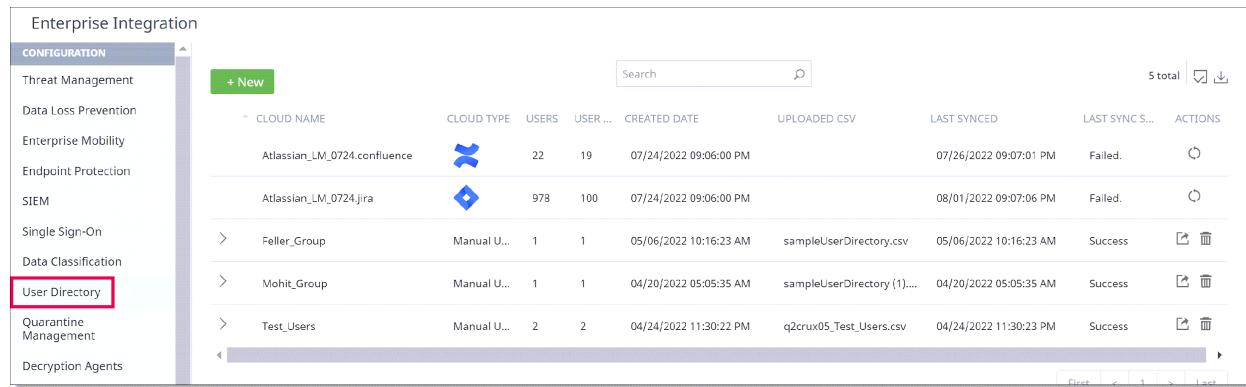
- a. In the **Destinations** pane, select the appropriate Google account.
- b. Specify context rules as desired.
- c. On the **Action** tab, under **Content Action**, select **Content Digital Rights** and then select the CDR template that you created in the previous section.
- d. Save the policy.

### Integration with Titus

1. Go to **Administration > Enterprise Integration > Data Classification**.
2. Click the **Titus** tab.
3. Click the Titus toggle to enable integration.
4. Click **Upload Schema** and select the file containing the data classification configurations.

## Creating and managing user directories

The **User Directory** page (**Administration > Enterprise Integration > User Directory**) displays information about user directories you can create and manage.



The screenshot shows the 'Enterprise Integration' interface with the 'User Directory' section selected. A table lists five user directories:

CLOUD NAME	CLOUD TYPE	USERS	USER ...	CREATED DATE	UPLOADED CSV	LAST SYNCED	LAST SYNC S...	ACTIONS
Atlassian_LM_0724.confluence		22	19	07/24/2022 09:06:00 PM		07/26/2022 09:07:01 PM	Failed.	
Atlassian_LM_0724.jira		978	100	07/24/2022 09:06:00 PM		08/01/2022 09:07:06 PM	Failed.	
Feller_Group	Manual U...	1	1	05/06/2022 10:16:23 AM	sampleUserDirectory.csv	05/06/2022 10:16:23 AM	Success	
Mohit_Group	Manual U...	1	1	04/20/2022 05:05:35 AM	sampleUserDirectory (1)....	04/20/2022 05:05:35 AM	Success	
Test_Users	Manual U...	2	2	04/24/2022 11:30:22 PM	a2cru05_Test_Users.csv	04/24/2022 11:30:23 PM	Success	

For each directory, the page shows the following information:

- **Cloud Name** – The cloud application using the directory.
- **Cloud Type** – The type of directory:
  - Manual upload -- The manual upload directory contains details for your cloud application users and the user groups to which they belong. These details are stored in a CSV file. By identifying user groups and their users, administrators can more easily control or monitor their access to data. You can create and configure multiple manual upload user directories.
  - **Azure AD** -- The cloud directory uses Azure Active Directory functionality to monitor user information and access. Azure AD directory information is displayed for each cloud application. In addition, you can create and configure one Azure AD directory.
- **Users** – The current count of users in the directory.
- **User Groups** – The current count of user groups in the directory.
- **Created Date** – The date and time (local) on which the directory was created.
- **Uploaded CSV** (manual upload directories only) – The name of the uploaded CSV file that contains the user and user group information.
- **Last Synced** (cloud and administrator-created Azure AD directories only) – The date and time (local) on which the last successful directory sync occurred.
- **Last Sync Status** (cloud and administrator-created Azure AD directories only) – The status of the last sync action, either **Success**, **Failed**, **Paused**, or **In Progress**.
  - If the status is **Failed**, try the sync again later. If the sync continues to fail, contact your administrator.
  - If the status is **Paused**, this indicates that the most recent sync attempt exceeded the sync deviation threshold. To restart the sync, click the sync icon in the Actions column and then click **Yes** on the warning pop-up.

For more information about the user directory sync threshold, see [Creating activity alerts](#).

- **Actions** – The actions you can take for the directory.



Cloud and administrator-created Azure AD directories only -- Sync the directory content to retrieve the latest information.

-  Manual upload directories only -- Export CSV files for the directory.
-  Administrator-created Azure AD and manual upload directories only -- Delete the directory.

We have an API connector for Ping Identity to facilitate User Directory sync action. After successful integration, the platform syncs the User Directory from Ping Identity periodically. We also support SCIM functionality for Ping Identity, enabling automated user provisioning to prevent delays in user sync when you add, delete, or modify a user.

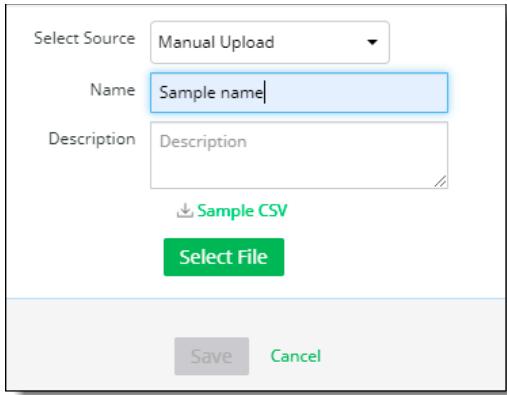
The following sections provide information about creating and managing manual upload and Azure AD user directories.

## Manual upload user directory

Perform the steps in the following sections to create and manage a manual upload directory.

### Creating a new manual upload directory

1. Go to **Administration > Enterprise Integration > User Directory** and click **New**.
2. Select **Manual Upload** from the **Select Source** dropdown list.
3. Enter a **Name** and a **Description** for the directory.



The screenshot shows a modal dialog box titled 'Create New User Directory'. The 'Select Source' dropdown is set to 'Manual Upload'. The 'Name' field contains 'Sample name'. The 'Description' field has the placeholder 'Description'. Below these fields are two buttons: 'Sample CSV' (with a file icon) and 'Select File' (in green). At the bottom of the dialog are 'Save' and 'Cancel' buttons.

The **Select File** button becomes active and the option to download a sample CSV file is displayed. You can download the sample file to create a directory or use a blank CSV file of your own.

The CSV file must use the following format:

- **First column** -- First name of cloud user
- **Second column** -- Last name of cloud user
- **Third column** -- Email ID of cloud user
- **Fourth column** -- User group(s) to which the cloud user belongs. If the user belongs to multiple groups, separate the name of each group with a semicolon.

The sample file available for download is preformatted with these columns.

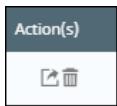
4. Once you have finalized the file with the needed user information, click **Select File** to upload it.

The file name appears above the **Save** button, and the **Save** button becomes active.

- Click **Save**. The uploaded CSV file is added to the User Directory list.

## Exporting a manually uploaded CSV file

- In the **Action(s)** column, click the **Export** icon for the CSV file you want to export, and save the file to your computer.



## Deleting a manually uploaded CSV file

- In the **Actions** column, click the trash can icon for the file you want to delete, and click Yes to confirm the deletion.

## Configuring an Azure AD user directory

Perform the steps in the following sections to create and manage an Azure AD directory.

### Creating a new Azure AD user directory

If no administrator-created Azure AD user directory exists, you can create one. If an administrator-created AD user directory already exists, you must delete it before another one can be created.

- In the **User Directory** page, click **New**.
- Select **Azure AD** from the **Select Source** list.
- Enter a **Name** (required) and a **Description** (optional) for the directory.
- Click **Authorize**.

An **Azure AD creation successful** message appears.

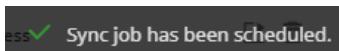
After the directory is created, you can perform a sync to retrieve the latest information.

### Syncing an Azure AD user directory

- In the **Actions** column, click the Sync icon for the Azure AD directory you want to sync.



A sync scheduled message appears at the bottom right corner of the page.



If the sync is successful, the date in the Last Sync column is updated, and the Sync Status shows a status of Success.

## Configuring an Okta application

This section provides instructions for configuring an Okta application for a global User Directory. This configuration includes two procedures, which are outlined in the following sections.

- Creating a web application integration in Okta
- Onboarding an Okta instance in the CASB Management Console

## Creating a web application integration in Okta

**Note** Because the sign-in redirect URI for an Okta web app integration is region-specific, contact Customer Support to find out the correct URI to enter. Enter that URI as instructed in these steps.

1. Log in to the Okta application.
  2. Click the icon at the upper left to display the Okta navigation menu on the left side of the screen.
  3. From the navigation menu, select **Applications > Applications**.
  4. Click **Create App Integration**.
  5. From the **Create a new app integration** page, select:
    - **OIDC – OpenID Connect** as the sign-in method
    - **Web Application** as the **Application type**.
  6. Click **Next**.
  7. From the **New Web App Integration** page, enter or select the following information.
    - **App integration name** – Enter a name for the integration.
    - **Logo** (optional) – Upload your company logo.
    - **Grant type** –
      - Leave the **Client acting on behalf of itself** box unchecked.
      - Under **Client acting on behalf of a server**, check **Refresh Token**.
      - **Sign-in redirect URIs** – Enter the URI provided by Customer Support.
      - **Sign-out redirect URIs** – Leave this field empty.
      - **Controlled access** – Select **Allow everyone in your organization to access**.
      - **Enable immediate access** – Check **Enable immediate access with Federation Broker Mode**.
  8. Click **Save**.
- Okta displays the **Client Credentials** for the app integration you are creating and generates a **Client ID**, which is a public identifier for the client. This identifier is required for all OAuth flows.
- You will need the client ID when you add the Okta instance in the SSE Management Console. To copy the client ID to your clipboard, click the Clipboard icon to the right.
- The **Client Secret** option is selected by default. The **Client Secrets** section shows the last client secret that Okta generated and the date it was created. For new app integrations, the date will be the date on which you created the integration. The characters in the secret are masked by dots. To view the secret, click the eye icon to the right.
- You will need the client secret when you add the Okta instance in the SSE Management Console. To copy the client secret to your clipboard, click the Clipboard icon to the right.
9. Go to the **API Scopes** tab.

10. Grant access to the following four scopes:

- okta.users.read
- okta.domains.read
- okta.groups.read
- okta.roles.read

## Onboarding an Okta instance in the SSE Management Console

After you have created a web application integration in Okta, you can create an Okta instance for the Global User Directory in the CASB Management Console.

1. Log into the Management Console.
2. Go to **Administration > Enterprise Integration**.
3. Select **User Directory** from the left menu and click **New**.
4. Enter or select the following information.
  - **Select Source** – Select Okta.
  - **Name** – Enter a name.
  - **Description** (optional) – Enter a brief description.
  - **OKTA domain** – Enter the appropriate Okta domain.
  - **Client ID** – Enter the client ID from the web application integration you created in Okta.
  - **Client Secret** – Enter the client secret that Okta generated for the integration you created in Okta.
5. Click **Authorize**. Okta displays the password window to verify your credentials.
6. Enter your Okta password and click **Verify**.

The Okta instance is added to the Management Console. The **Last Synced** column is empty until a sync takes place. The **Status** column shows a sync status of Initiated. When the first sync occurs, the sync date and time will appear in the **Last Synced** column. If the sync was successful, the **Initiated** status will be replaced with a status of **Success**.

To request a sync at any time, click the **Refresh** icon in the **Actions** column.

To view and edit the configuration details, click the > arrow to the left. The **Authorize** button now says **Re-Authorize**.

To dismiss the details without editing, click **Cancel**.

To edit the details, make the needed changes and click **Re-Authorize**. When the Okta password prompt appears, enter your password and click **Verify** to update the configuration.

## User Directories with SCIM Integration

You can integrate CASB with Azure AD or Okta using SCIM to continuously sync your user directories. With SCIM, user directory updates are pushed to CASB in real-time, so you do not have to wait for the scheduled sync job to complete.

## Setting Up SCIM with Okta

Before you begin, you must have created an Okta application and configured it in the CASB Management Console, as described in [Configuring an Okta application](#).

Enable SCIM for your Okta user directory as follows:

1. In the Management Console, go to **Administration > Enterprise Integration > User Directory**.
2. Locate the Okta configuration that you have already set up, and click the arrow to the left of it to expand the configuration details.
3. Enable the SCIM toggle.
4. Two new fields are shown, pre-populated with the necessary data: Base URL and API Key. Copy both values for use in the next procedure.
5. Click the **Re-Authorize** button. Enter your Okta administrative credentials to authorize the account.
6. Click **Save**.

Next, create a new Okta application, as follows:

1. In your Okta administration console, select **Applications > Applications**.
2. Click the **Browse App Catalog** button and use the search function to find and select “SCIM 2.0 Test App (Header Auth).”
3. Click the **Add Integration** button.
4. (Optional) Modify the application label if desired.
5. Click **Next**.
6. On the “Sign-On Options” page, select SAML 2.0. Click **Done**.
7. Your new application is shown.
8. Select the **Provisioning** tab and click **Configure API Integration**.
9. Select the **Enable API Integration** checkbox, and enter the Base URL and API token that you saved from within the CASB Management Console in the previous procedure.
10. Click the **Test API Credentials** button. You should see a message confirming that the credentials were successfully verified. Click **Save**.
11. On the Provisioning to App page, click **Edit** and select the **Enable** checkboxes for **Create Users**, **Update User Attributes**, and **Deactivate Users**. Click **Save**.
12. Next, select the **Assignments** tab. From the **Assign** drop-down, select **Assign to People**.
13. Okta displays a list of users. For each user you want to assign to the SCIM application:
  - a. Click **Assign**.
  - b. Verify the user details that are shown in a pop-up, and click **Save and Go Back**.
  - c. The **Assign** link next to the user’s name changes to a label that says **Assigned**.

14. When you have added all desired users, click **Done**.
15. If you want to sync user groups as well:
  - a. Go to the **Push Groups** tab.
  - b. From the **Push Groups** drop-down, select either **Find groups by name** or **Find groups by rule**.
  - c. Search for and select the desired group.
  - d. Click **Save**.
  - e. Repeat as needed for additional groups.

## Setting up SCIM with Azure AD

Before you begin, you must have configured an entry for Azure AD in the CASB Management Console, as described in [Configuring an Azure AD user directory](#).

Enable SCIM for your Azure AD user directory as follows:

1. In the Management Console, go to **Administration > Enterprise Integration > User Directory**.
2. Locate the Azure AD configuration that you have already set up, and click the arrow to the left of it to expand the configuration details.
3. Enable the SCIM toggle.
4. Two new fields are shown, pre-populated with the necessary data: Base URL and API Key. Copy both values for use in the next procedure.
5. Click the **Re-Authorize** button and enter your Azure AD administrative credentials to authorize the account.

Next, create a new Azure AD application, as follows:

1. In your Azure console, click **Enterprise applications**.
2. Click **+ New Application** and then **+ Create your own application**.
3. Enter a name for the application, select the **Integrate any other application** radio button, and click **Create**.
4. When your new application is created and you see the overview screen, select the **Provisioning** tab.
5. Click the **Get started** button.
6. From the **Provisioning Mode** drop-down, select **Automatic**.
7. Enter the URL and API key that you saved from within the CASB Management Console in the previous procedure.
8. Click the **Test Connection** button. You should see a message confirming that the credentials were successfully verified. Click **Save**.

9. The Mappings section is now available. Click the arrow to expand it.

Most values for the User and Group objects in Azure AD have been automatically mapped to the corresponding values in CASB, but there is one mapping that you must modify.

10. Click **Provision Azure Active Directory Users**. Azure AD displays the list of mappings that were automatically created.
11. Locate the mapping where the Azure AD Attribute is ‘NickName’ and click to edit it.
12. Change the **Source attribute** from ‘NickName’ to ‘objectId’ and click **Ok**.
13. Click **Save**.

# Configuring logs

You can configure the level of information for each log along with log file size and organization.

You can select different settings for each item and change them at any time based on your system activity and the type of information you need to track and analyze. Because much of the system activity takes place within nodes, you might need to provide more detail and greater log file capacity for the Node Server.

## Note

Log levels apply only to Juniper classes, not to third-party libraries.

Perform the following steps to configure log settings.

1. Go to **Administration > Environment Management**.
2. Select the on-premises connector environment for which to apply log configuration settings.
3. Click the **Log Configuration** icon.
4. Click the **Log Configuration Override** toggle to display the log settings.
5. Enter or select the following settings.

Field	Description
<b>Log Level</b>	<p><b>Log Level</b> refers to the type of content and level of detail included in logs. The options (in increasing level of detail) are:</p> <ul style="list-style-type: none"> <li>▪ <b>Warn</b> — Includes only errors or warnings of actual or possible problems.</li> <li>▪ <b>Info</b> — Includes informational text about system processes and status, along with warnings and errors.</li> <li>▪ <b>Debug</b> — Includes all informational text, warnings and errors, and more detailed information about system conditions. This information can aid in diagnosing and troubleshooting system issues.</li> <li>▪ <b>Trace</b> — The most detailed level of information. This information can be used by developers to focus on a precise area of the system.</li> </ul> <p>Select a log level.</p>
<b>Number of Log Files</b>	The maximum number of files that can be maintained. When this number is reached, the oldest log file is deleted.
<b>Log File Max Size</b>	The maximum size allowed for a single log file. When the maximum file size is reached, the file is archived, and information is stored in a new file. Each of the remaining logs is renamed to the next higher number. The current log is then compressed and renamed <i>log-name.1.gz</i> . A new log is started with <i>log-name</i> . So, if the maximum is 10, <i>log-name.9.gz</i> is the oldest file, and <i>log-name.1.gz</i> is the newest non-active file.

6. Click **Save**.

# Creating and managing notifications and alerts

---

CASB provides a flexible and comprehensive set of tools for creating notifications for policy enforcement and communication of critical messages regarding protection of data. You can create notifications for a variety of data security needs and cloud applications, devices, and network environments. You can then apply those preconfigured notifications to multiple API access policies. Because notifications are created separately from policies, you can apply notifications consistently across policies and customize them conveniently as needed.

You can also view an audit trail of past notifications and export this information for historical purposes.

Notifications are created and managed from these areas in the Management Console:

- **Administration > Enterprise Integration > Notification Channels** for creating channels used by cloud applications
- **Administration > Notification Management** for creating templates and building notifications with the appropriate templates and channels
- **Administration > System Settings > Alert Configuration** for setting threshold values to receive email notifications

The workflow for creating notifications includes these steps:

1. Create channels to define the communication method for issuing a notification.
2. Create templates to specify the text and format for the notification.
3. Create the notification itself, which includes the channel and the template needed for the notification.

Once you have created a notification, you can apply it to the appropriate policies.

## Creating notification channels

Notification channels define how the notification will be communicated. CASB provides several types of channels for various notification types. Channels are available for email notifications, messages on Slack cloud applications, and marker files.

The **Notification Channels** page (**Administration > Enterprise Integration > Notification Channels**) lists the notification channels that have been created.

To view details for a channel, click the eye icon to the left of the channel name. To close the details view, click **Cancel**.

To filter the columns displayed, click the Filter icon at the upper right, and check the columns to hide or show.

To download a CSV file with a list of channels, click the **Download** icon at the upper right.

### To create a new notification channel:

1. Go to **Administration > Enterprise Integration > Notification Channels** and click **New**.
2. Enter a **Name** (required) and a **Description** (optional but recommended) for the new channel.

3. Select a **notification type**. The options are:
  - **Email** (for notifications as email)
  - **Proxy** (for proxy-related notifications)
  - **Slack** (for notifications pertaining to Slack applications)
  - **ServiceNow Incident** (for notifications pertaining to ServiceNow)
  - **Marker** (for notifications as marker files)
4. Select the Slack Incident or ServiceNow type, the **Cloud Name** field appears. Select a cloud application to which the channel will apply.
5. Save the channel.

## Creating notification templates

Templates define the text and format of a notification. Most templates offer an HTML or plain text format option and offer base text that you can customize.

The **Templates** tab on the **Notifications** page (**Administration > Notification Management**) lists predefined templates and enables you to create additional templates.

You can define the following attributes for each template:

- **Name** — The name by which the template will be referenced.
- **Type** — The action or event for which the template is used. For example, you can create templates to notify users about Slack messages or to send email notifications about alerts or jobs completed.
- **Subject** — A brief description of the template's function.
- **Format** — The format of the template for the application, connector, or function. Options include Email, Slack (format and channel), ServiceNow, SMS, Proxy, Reporting, and configuration changes.
- **Updated On** — The date and time on which the template was created or last updated.
- **Updated User** — The email address of the user to which the template applies.
- **Actions** — Options for modifying or deleting a template.

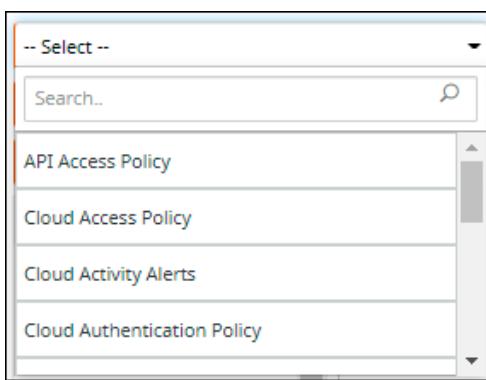
### To create a new notification template:

1. Go to **Administration > Notification Management**.
2. Click the **Templates** tab and click **New**.

**Templates**

Name	<input type="text" value="Enter Name"/>
Description	<input type="text" value="Description"/>
Category	-- Select --
Format	-- Select --
Type	-- Select --
Content Template	<div style="display: flex; justify-content: space-between;"> <span>Variables <small>click to insert</small></span> <span>Message Body</span> <span>Preview</span> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">         Account name          Admin login          Admin name          Advanced Threat Details          All Recipients          Anomaly Type          Anomaly URL          Body          Channel Name       </div>

3. Enter a **Name** (required) and a **Description** (optional).
4. Select a template **Category**. This is the type of action, event, or policy for which the template will be used.



5. Select a **Format** for the template. The formats available depend on the category you chose in the previous step. In this example, the formats listed are for the **Cloud Access Policy** category.

Category	Cloud Access Policy
Format	Proxy Certificate Remediation
Type	-- Select --
Content Template	<div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">         Deny Certificate Remediation          Proxy Certificate Remediation          Warn Certificate Remediation       </div>

6. Select a notification **Type**. The options listed depend on the format you chose in the previous step.

The screenshot shows the 'Content Template' editor interface. At the top, there are dropdown menus for 'Format' (set to 'Proxy Remediation') and 'Type' (set to 'Proxy Remediation'). Below these are sections for 'Content Template' and 'Variables'. The 'Variables' section lists various placeholders such as 'Sender', 'Sharing Type', 'Logo', 'Cloud Name', 'User Name', 'Policy Action', 'Policy Name', 'Start Day', 'Stop Day', 'Tenant Id', 'MES App Dynamic Link', 'File Name', and 'Account Name'. To the right is the 'Remediation Body' text area, which contains the following HTML code:

```

<html>
<head>
<meta name="viewport" content="width=device-width,initial-scale=1.0">
<style>
.content {
    width: 40%;
}
@media screen and (max-width: 1100px) {
.content {
    width: 90%;
}
}
</style>
</head>

```

7. Enter the content for the template in the text area at the right. Scroll down to the areas where you want to enter content.
8. Select any **variables** you want to use from the list at the left. Place the cursor at the point where the variable should be inserted and click the variable name. The list of available variables will vary depending on the format and type of template you are creating.
9. If you are creating an **email** template, select **HTML** or **Text** as the delivery format, and enter a subject.
10. Click **Preview** at the upper right to see how your template content will be displayed.

This screenshot shows the same Content Template editor interface as above, but with a red box highlighting the 'Preview' button located in the top right corner of the 'Remediation Body' panel.

11. Save the template.

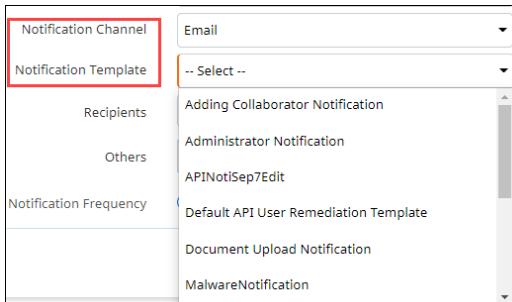
## Creating notifications

Once you have created notification channels and templates, you can create the actual notifications that can be applied to policies. Each notification uses a selected channel and template and is distributed according to the frequency you specify.

### To create a new notification:

1. Click the **Notifications** tab and click **New**.
2. Enter a **Name** (required) and a **Description** (optional).

3. Select a notification **Category**.
4. Select a **Notification Channel**.
5. Select a **Notification Template**. The templates in the dropdown list depend on the channel you selected in the previous step.



6. Depending on the notification channel you selected, you will be prompted to enter additional information. Here are two examples:
  - For an email channel:
    - Select an email template, then check the types of recipients. If you checked **Others**, enter recipient names separated by commas.
    - Select a notification frequency – **Immediate** or **Batched**. For **Batched**, select a batch frequency and a time interval (minutes or days).
  - For a Slack channel:
    - Select a notification template.
    - Select one or more Slack channels.
7. Save the notification.

The new notification is added to the list.

## Creating activity alerts

You can create activity alerts for onboarded (managed) cloud applications and for cloud discovery.

### Managed cloud applications

For each managed-cloud alert, the **Activity Alerts** page shows:

- **Name** -- The name of the alert.
- **Activity** – The type of activity to which the alert applies.
- **Notification** -- The name of the associated notification for this alert.
- **Updated on** -- The date and time on which the alert was updated. The time is based on the **Time Zone** setting configured in the **System Settings** page.
- **Updated by** – The valid username for the user who last updated the alert, or a system update.
- **Status** – A toggle that indicates the status of the alert (active or inactive).
- **Actions** – An icon that, when clicked, enables you to edit information about the alert.

To view the details for an alert, click the icon to the left of the alert name.

Click **Cancel** to return to the list view.

## Cloud discovery

For each cloud-discovery alert, the **Activity Alerts** page displays the following information:

- **Name** – The name of the alert.
- **Updated on** – The date and time at which the alert was last updated. The time is based on the time zone setting configured in the **System Settings** page.
- **Updated by** – The valid username of the user who last updated the alert, or a system update.
- **Notification** – The name of the associated notification.
- **Status** – A toggle that indicates the alert status (active or inactive).
- **Actions** – An icon that, when clicked, enables you to edit information about the alert.

To view the details for an alert, click the icon to the left of the alert name.

Click **Cancel** to return to the list view.

## Types of alerts

For onboarded cloud applications, three types of alerts can be created:

- **Cloud Activity**, which includes alerts about content activity on the cloud application you specify
- **External System Connectivity**, which includes alerts involving your configurations for external connectivity (enterprise DLP, log agent, or SIEM).
- **Tenant Activity**, which provides alerts for anomalies (geolocations, authentications, content deletion, downloads by size and by count) and changes to cloud risk scores.

## Creating alerts for managed cloud applications

1. Go to **Monitor > Activity Alerts**.
2. In the **Managed Clouds** tab, click **New**.
3. Enter an **Alert Name**.
4. Select an **Alert Type**.
  - a. For **Cloud Activity** alerts, enter or select the following information:
    - **Cloud Account** -- The cloud application for the alert.
    - **Activity** -- Check the boxes for one or more activities.
    - **Filters** -- Select the filters for this alert activity type.
      - For **Time Window**, select a day and time range in which the activity occurs.
      - For **Threshold**, enter the number of events, the duration, and time increment (**Mins** or **Hours**) for this activity (for example, 1 event every 4 hours).
      - The **Aggregate Alert Counts** toggle is enabled by default, which indicates that threshold aggregation occurs at the cloud application level. To enable activity count aggregation at the individual user level, click the toggle to disable it.
      - For **User Groups**:
      - Click in the box to the right.
      - Double-click the directory name.
      - Select a group from the list that appears and click the arrow to move it to the **Selected Groups** column.
      - Click **Save**.

- To specify more than one filter, click the + button and select another filter.
- b. For **External System Connectivity** alerts, select the following information:
  - **Services** – Check the boxes for one or more services, including Enterprise DLP, Log Agent, and SIEM.
  - **Frequency** – Select **Once** or **Send Reminders**. For **Send Reminders**, enter a reminder quantity and time increment (day or hour). For example, 2 reminders per day.
- c. For **Tenant Activity** alerts, first select an **Activity Type**: **Anomaly**, **Risk Score Change**, or **User Directory**.
  - For **Anomaly**, select one or more anomaly types to include in notifications. Then, for Filters, select **Time Window** or **Threshold**.
    - For **Time Window**, select a day and time range in which the anomaly occurs.
    - For **Threshold**, enter the number of events, the duration, and time increment (**Mins** or **Hours**) for this activity (for example, 1 event every 4 hours).
    - To specify more than one filter, click the + button.
  - For **User Directory**, select Threshold from the Filters drop-down, then enter a sync deviation value and specify whether it is a count or a percentage.

Each time the user directory is synced, CASB compares the number of user records against the number from the previous sync. If the difference is greater than the sync deviation threshold that you specify, this activity alert will be triggered, and the sync status will show **Paused** on the User Directory page. You can manually restart the sync after reviewing the details.

For more information on user directories, see [Creating and managing user directories](#).

5. Select a notification to send with this alert. The options are based on the notifications you created.
6. Click **Save** to save the alert.

## Creating alerts for Cloud Discovery

1. Click the **Cloud Discovery** tab and click **New**.
2. Enter the following information:

Cloud Discovery	
Alert Name	<input type="text"/>
Content Type	<div style="border: 1px solid #ccc; padding: 2px;">-- Select --</div> <div style="border: 1px solid #ccc; padding: 2px;">-- Select --</div>
Notification	<div style="border: 1px solid #ccc; padding: 2px;">-- Select --</div>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

3. Enter a **Name** for the alert.
4. Select a **Content Type**.
  - **Users** — Enter one or more valid user email addresses for users to be included in the alert. Separate each email address with a comma. Click **Save**.
  - **User Groups** — Check one or more user groups, or check **Select All**. Click **Save**.

- **Cloud Risks** — Check one or more cloud risk levels.
  - **Cloud Category** — Check one or more cloud application categories, for example, **Cloud Storage or Collaboration**.
  - **Total Bytes Threshold** — Enter a number (in kilobytes) that represents the size threshold for triggering an alert. Then, enter a duration quantity and interval.
  - To specify more than one content type, enter the information in the second dropdown list. To specify additional content types, click the + icon at the right, and enter the information in the additional dropdown lists.
5. Select a **Notification** for the type to be used when the alert is sent.
  6. Save the alert.

## Configuring notification and alert options in System Settings

You can configure threshold values for email notifications, and configure logos for templates, from System Settings.

### Selecting alert configurations

1. Go to **Administration > System Settings > Alert Configuration**.
2. Click **Create an Alert**.
3. In the **Alert Configuration** window, enter the following information:

Field	Description
<b>Event Name</b>	<p>The type of event that generates the alert. The options are:</p> <ul style="list-style-type: none"> <li>▪ CPU</li> <li>▪ Memory</li> <li>▪ Disks</li> <li>▪ Threads</li> <li>▪ Service Down</li> <li>▪ Login Failure</li> <li>▪ Certificate Event</li> <li>▪ Service Up</li> <li>▪ Key Creation</li> <li>▪ Node Management</li> <li>▪ Node State Change</li> <li>▪ User Management</li> <li>▪ Connector Management</li> <li>▪ Node Communication Action</li> <li>▪ Environment Management</li> </ul>

Field	Description
<b>Trigger value/Greater or Less</b> <b>Note</b> Alerts fall into two categories: <ul style="list-style-type: none"> <li>▪ those driven by thresholds being crossed, and</li> <li>▪ those driven by events that occur.</li> </ul> This setting pertains to alerts for thresholds. It does not apply to the strict occurrence of events such as a login failure or the creation of a key.	The limit for an event which, if more or less than specified value, triggers an alert. For example: <ul style="list-style-type: none"> <li>▪ If the value for CPU is greater than 90, and system CPU usage goes up to 91%, an alert is triggered.</li> <li>▪ If the value for CPU is less than 10%, and the system CPU usage drops to 9%, an alert is triggered.</li> </ul> Alert notifications are sent to the specified recipient. If you selected <b>Show on the Home</b> page, the alert is listed on the Management Console dashboard. Although administrators are typically most often interested in events that indicate greater-than status, sometimes you might want to know when events drop below the trigger to indicate a possible problem (for example, no activity appears to be taking place).
<b>Environments</b>	The environments to which the alert applies. You can choose specific environments or all environments.
<b>Connectors</b>	If connectors are available, only alerts related to those connectors and their associated applications will be visible.
<b>Email list</b>	The email addresses of those who should receive the alert notifications. The most common recipient is the system administrator, but you can add other addresses. Enter each recipient email address, separating the addresses by commas. System Administrator and Key Administrator will include all users with the matching role. This list can be empty if you only want it to show in the <b>Alert Messages</b> section of the Management Console.
<b>Alert interval</b>	How often the alert should be sent. Select a number and type of interval (hour, minute, or day). Select <b>0</b> to get all instances of an event type, such as <b>Key Creation</b> .
<b>Show Alerts</b>	Click the toggle button to enable alerts to be listed in the <b>Alert Messages</b> section of the Management Console dashboard. You might want to use this option for alerts relating to more serious conditions. Those alert messages will be seen on the dashboard whenever the <b>Home</b> page is displayed.
<b>Description</b>	Enter a description of the alert.

4. Save the configuration.

## Editing an alert configuration

You can edit information about an alert if the conditions related to the alert have changed — for example, if the severity of the alert has increased or decreased, the condition applies to more or fewer environments, or you need to modify recipient email addresses or the alert description.

1. From the **System Settings** page, choose **Alert Configuration**.
2. Select the alert configuration you want to edit.
3. Click the pencil icon.
4. In the **Alert Configuration** dialog box, modify the alert information as needed.
5. Click **Save**.

## Deleting an alert configuration

You can delete an alert configuration if the related event no longer applies, or if you do not need to monitor the event.

1. From the **System Settings** page, choose **Alert Configuration**.
2. Select the alert you want to delete.
3. Click the trash can icon.

4. When prompted, confirm deleting the alert.
5. Click **Save**.

# Configuring Juniper Secure Edge CASB for policy management

The policy management options provided by Juniper Secure Edge enable you to protect the sensitive data stored in your organization's sanctioned and unsanctioned cloud applications. In addition, the Juniper Secure Edge's Secure Web Gateway enables you to set policies to monitor web traffic in your organization and limit access to specific sites or categories of sites.

Through the CASB policy engine in Juniper Secure Edge, you can control access to information by specifying the conditions under which users can access, create, share, and manipulate data, and the actions to address violations of those policies. The policies you set determine what is protected and how.

CASB enables you to configure your security settings to create policies that will protect data stored in multiple cloud applications and devices. These configurations streamline the process of creating and updating policies.

In addition to protecting data, CASB supports Optical Character Recognition (OCR), which can detect sensitive information in image files that have been uploaded to a cloud using Optical Character Recognition (OCR). For example, a user might have uploaded a photo, a screen shot, or other image file (.png, .jpg, .gif, and so on) that shows a credit card number, social security number, employee ID, or other sensitive information. When creating policies, you can enable the OCR option (a checkbox), which will apply protection actions to image files. OCR can be enabled in policies for cloud applications with API protection modes.

OCR protection can also be applied to policies for files that include images; for example, a PDF or a Microsoft Word file that includes one or more images within the file.

## Policy configuration and creation workflow

Policy management in Juniper Secure Edge includes several configuration steps that enable efficient and consistent creation of policies. You can apply these configurations to protect data stored in multiple cloud applications and on a variety of devices and monitor web traffic.

Policy management in Juniper Secure Edge includes several configuration steps that enable efficient and consistent creation of policies. You can apply these configurations to protect data stored in multiple cloud applications and to monitor web traffic.

1. Create content rule templates
2. Create Content Digital Rights templates
3. Configure file type, MIME type, and file size for exclusion from scanning
4. Configure folder sharing
5. Set number of folder sublevels for DLP scanning
6. Configure default policy violation actions
7. Create policies: API Access

The following sections outline these steps.

## Create content rule templates

Content rules identify the content to apply to a policy. Content can include sensitive information in a file, such as usernames, credit card numbers, Social Security numbers, and file types.

For DLP rules, you can create templates that include sets of content rules and apply one of those templates to one or more policies. With content rule templates, you can classify content based on more than one context. Because content rules are configured as a separate process from policy creation, you can save time and enable consistent content information in all of the policies you create.

The content rule templates provided with the product, and those you create, are listed in the **Content Rule Management** page.

The Content Rule Management page has three tabs:

- **Document Rule Templates** -- Specifies overall rules to apply to documents.
- **DLP Rule Templates** -- Specifies DLP rules. When customers create a document rule template, they select a DLP rule if the document template is applied to DLP policies. You can use any of the templates provided with the product or create additional templates.
- **Data Types** -- Specifies data types to apply to this rule. You can use any of the data types provided with the product or create additional data types.

Perform the steps in the following procedures to create additional data types and templates for configuring content rule management.

### Creating new data types

1. Click the **Data Types** tab and click **New**.
2. Enter a **Data Type Name** (required) and a **Description** (optional) for the data type.
3. Select a data **Type** to apply. Options include Dictionary, Regex Pattern, File Type, File Extension, File Name, and Composite.
4. Click **Next**.
5. Enter additional information for the data type you selected.
  - [Dictionary](#)
  - [Regex Pattern](#)
  - [File Type](#)
  - [File Extension](#)
  - [File Name](#)
  - [Composite](#)
  - [Exact Data Match](#)
6. Click **Next** to review a summary for the new data type.
7. Click **Confirm** to save the new data type, or **Previous** to make any corrections or updates.

You can configure data types as follows.

#### Dictionary

Use the **Dictionary** data type for plain text strings.

Select either **Create Keyword** or **Upload File**.

- For **Create Keyword** – Enter a list of one or more keywords; for example, account number,account ps,american express,americanexpress,amex,bank card,bankcard
- For **Upload File** – Click **Upload a File** and select a file to upload.

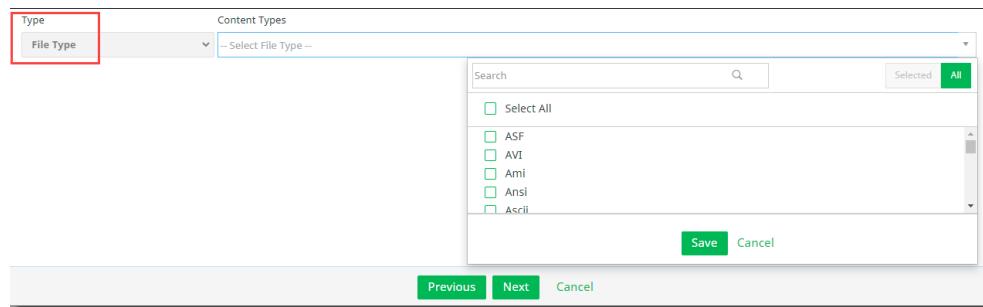
## Regex Pattern

Enter a regular expression. For example:

```
\b\((?([0-9]{3})\))\)?[-.\t]?([0-9]{3})[-.\t]?([0-9]{4})\b
```

## File Type

Check the boxes to select one or more file types or check **Select All**. Then click **Save**.



## File Extension

Enter one or more file extensions (for example, .docx, .pdf, .png)

Click **Save**.

## File Name

Enter one or more file names (for example, PII, Confidential)

Click **Save**.

## Composite

A Composite data type consists of either two **Dictionary** data types or one **Dictionary** type and one **Regex Pattern** type. The first type is automatically set to Dictionary and cannot be changed.

A **Proximity** option is available for the second Dictionary type or the Regex Pattern type after you make a selection from the Type drop-down.

- Select either **Dictionary** or **Regex Pattern** from the **Type** drop-down for the second type.
- Select the desired predefined object from the second drop-down.
- Enter a Match Count and (optional) a Unique Match Count for each entry.
- Enter a **Proximity** value for the second **Dictionary** type or the **Regex Pattern** type.
- (Optional) If you selected a **Regex Pattern** type, use the **Exception** option to enter any exceptions. Click in the **Token Whitelist** text box and enter one or more token keywords, separated with commas. Click **Save** to close the text box.

## Match Count and Unique Match Count

For Dictionary and Regex Pattern data types within a Composite data type, you can specify both a Match Count and a Unique Match Count.

The **Match Count** (required) specifies how many keyword matches must be in a file or record in order for it to be considered a violation of the policy. These matches do not have to be unique; for example, if the match count is set to 3, then three instances of the same keyword within a file will be considered a violation.

The **Unique Match Count** (optional) specifies how many *unique* keyword matches must be present in order to consider the file a violation of the policy. The Unique Match Count value must be equal to or less than the Match Count value.

For example, if the Match Count is 3 and the Unique Match Count is 2, then the file must contain at least three matching keywords and at least two of those must be unique. In this case, a file with two instances of one keyword and one instance of another keyword would be a violation (a total of three matches and two unique values), but a file with three instances of the same keyword would not be a violation.

By default, both the Match Count and Unique Match Count are set to 1 (one), which means that the Unique Match Count is not in use. To make use of this functionality, set the Unique Match Count to a value greater than one but not greater than the Match Count value.

## Exact Data Match

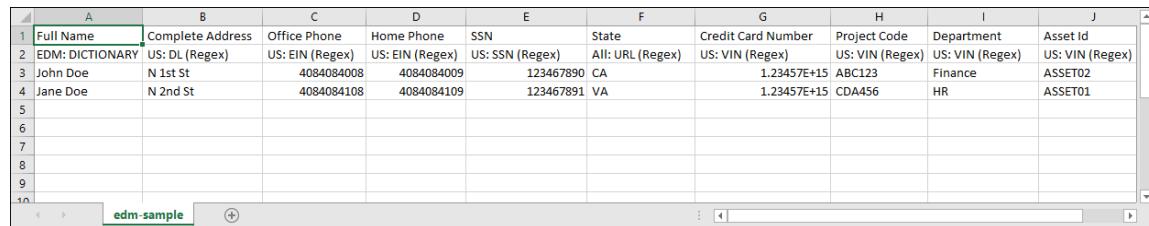
Exact data matching (EDM) allows CASB to identify data in records that matches criteria you specify.

As part of managing data types, you can create an EDM template using a CSV file with sensitive data for which you can define the matching criteria. You can then apply this template as part of a DLP rule in API policies.

Perform the following steps to create an exact data match type and apply DLP rule information.

### Step 1 -- Create or obtain a CSV file with the data to use for matching.

In the second row of the file, map the column headers with data types in CASB. This information will be used to identify the data types that will be matched. In this example, the Full Name column is mapped to the data type Dictionary, and the remaining column headings are mapped to the data type Regex.



The screenshot shows a CSV editor window with a grid of data. The first row contains column headers and data type mappings. The second row contains the actual data. The columns are labeled A through J. The data type mappings are as follows:

	A	B	C	D	E	F	G	H	I	J
1	Full Name	Complete Address	Office Phone	Home Phone	SSN	State	Credit Card Number	Project Code	Department	Asset Id
2	EDM: DICTIONARY	US: DL (Regex)	US: EIN (Regex)	US: EIN (Regex)	US: SSN (Regex)	All: URL (Regex)	US: VIN (Regex)	US: VIN (Regex)	US: VIN (Regex)	US: VIN (Regex)
3	John Doe	N 1st St	4084084008	4084084009	123467890	CA	1.23457E+15	ABC123	Finance	ASSET02
4	Jane Doe	N 2nd St	4084084108	4084084109	123467891	VA	1.23457E+15	CDA456	HR	ASSET01
5										
6										
7										
8										
9										
10										

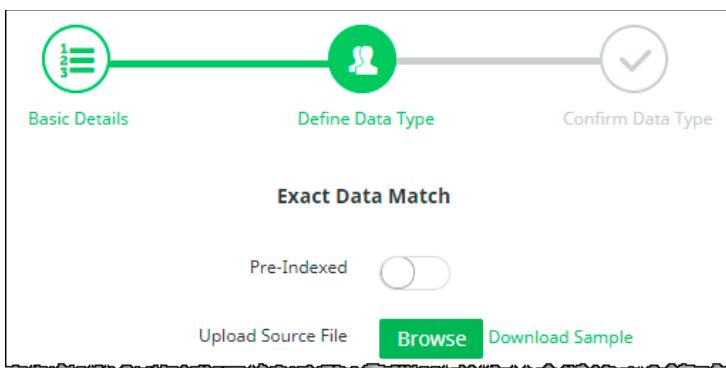
The bottom of the window shows a toolbar with buttons for navigating between files and creating new ones.

### Step 2 – Create a new data type -- Exact Data Match.

1. Click the **Data Types** tab and click **New**.
2. Enter a **Name** (required) and a **Description**.
3. Select **Exact Data Match** as the Type.

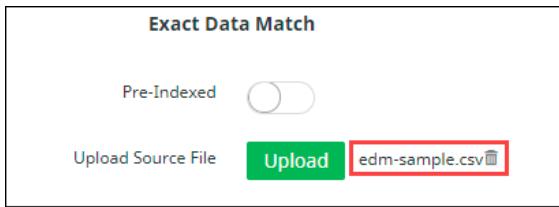
The **Last Modified** timestamp on the Data Type **Basic Details** page shows the time when the agent processed the data set. The **Last Modified** timestamp on the **Data Type List View** page indicates the time the template was created initially or the time of any subsequent manual updates.

4. Click **Next**.
5. Click the **Pre-Indexed** toggle if sensitive data in the CSV file you are uploading has been hashed previously. For files without previous hashing, the data will be hashed when the file is uploaded.



If you want to perform hashing on a file before you upload it, use a data hashing tool provided with CASB. Go to **Administration > System Settings > Downloads** and select the **EDM Hashing Tool**. Download the tool, install it, and apply data hashing to the file.

6. Click **Upload** and select the CSV file to use for the data match. To see a sample file, click Download Sample.



The uploaded file name is displayed. To remove it (for example, if you uploaded an incorrect file or want to cancel the procedure), click the trash can icon.

#### Note

You can replace the uploaded file later as long as the fields in the file are not changed.

7. Click **Next**.
8. Click **Next**, review the summary information, and save the data type. You will use this data type in the next step.

### Step 3 – Create a new DLP Rule template to configure the data matching properties.

1. In the **DLP Rules** tab, click **New**.
2. Enter a **Rule Name** (required) and a **Description** (optional).
3. Select **Exact Data Match** as the Rule Type and click **Next**.

4. Select **Custom Content Rule** as the Rule Template.
5. For **Exact Data Match**, select the EDM data type you created previously. The fields and mapped data types from the CSV file you uploaded previously are listed with a weightage option for each field.

Pre-Match Condition

Exact Data Match		
Field Name	Data Type	Weightage
Complete Address	US: DL (Regex)	.. Select ..
Office Phone	US: EIN (Regex)	.. Select ..
Home Phone	US: EIN (Regex)	.. Select ..
SSN	US: SSN (Regex)	.. Select ..
State	All: URL (Regex)	.. Select ..
Credit Card Number	US: VIN (Regex)	.. Select ..
Project Code	US: VIN (Regex)	.. Select ..
Department	US: VIN (Regex)	.. Select ..
Asset Id	US: VIN (Regex)	.. Select ..

6. Select a weightage for each field. The weightages you choose are used along with the number of fields to match to determine if a record is considered a match. The options are:
  - **Mandatory** – The field must be matched for the record to be considered a match.
  - **Optional** – The field serves as “padding” when determining if a record is matched.
  - **Exclude** – The field is ignored for matching.
  - **Whitelist** – If one or more fields are whitelisted, the record is whitelisted and not considered a match even if it meets all other matching criteria.

Field Name	Data Type	Weightage
Complete Address	US: DL (Regex)	Mandatory
Office Phone	US: EIN (Regex)	Optional
Home Phone	US: EIN (Regex)	Exclude
SSN	US: SSN (Regex)	Mandatory
State	All: URL (Regex)	Mandatory
Credit Card Number	US: VIN (Regex)	Mandatory
Project Code	US: VIN (Regex)	Optional
Department	US: VIN (Regex)	Optional
Asset Id	US: VIN (Regex)	Optional

7. Select the matching criteria for field matching, record matching, and proximity.

Match Criteria	
Minimum Number of Fields to Match	<input type="text" value="5"/>
Minimum Number of Records to Match	<input type="text" value="1"/>
Proximity	<input type="text" value="500"/>

- For **Minimum Number of Fields to Match**, enter a value that equals or exceeds the number of fields with a *mandatory* weightage and equals or is less than the number of fields with an *optional* weightage. This is the number of fields that must match for this rule. For example, if you have four fields with a mandatory weightage and three fields with an optional weightage, enter a number between 4 and 7.
- For **Minimum Number of Records to Match**, enter a value of at least 1. This number represents the minimum number of records that must be matched for the content to be considered in violation.
- For **Proximity**, enter a number of characters that represents the distance between fields. The distance between any two matching fields must be less than this number for a match. For example, if the Proximity is 500 characters:
  - The following content would be a match because the proximity is fewer than 500 characters:  
Field1value + **50** characters+Field3value + **300** characters + Field2value
  - The following content would not be a match because the proximity is greater than 500 characters:  
Field1value + **50** characters+Field3value +**600** characters + Field2value

8. Click **Next**.

9. Review the summary and save the new DLP rule.

You can now apply this DLP rule to API Access policies.

## Creating new DLP rule templates

- Click the **DLP Rule Templates** tab and click **New**.
- Enter a **Rule Name** (required) and a **Description** (optional).
- Select **DLP Rules** as the rule type and click **Next**.
- Select a **Rule Template** from the dropdown list. Then, perform *either* of the following steps.
  - If you selected the **Custom Content Rule** template, select a **Rule Type** and the accompanying value for that type. The options are:
    - Composite** – Select a unique name (for example, VIN, SSN, or Phone).
    - Dictionary** – Select a **keyword list** (for example, US: SSN) , a **match count**, and (optional) a **unique match count**. See [Match Count and Unique Match Count](#) for details.
    - Regex Pattern** – Select a **regular expression** (regex pattern) and a **match count**.

The match count can be any value between 1 and 50. The match count indicates the minimum number of violating tokens to be considered for a violation.

Whatever match count you specify, the DLP engine detects up to 50 violating tokens and takes the actions you have configured (for example, highlighting, masking, redacting, and so on).

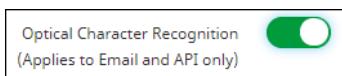
Note: If you select Dictionary, for XML files the attribute you choose must have a value for the DLP engine to recognize it as a match. If the attribute is specified but has no value (example: ScanComments=""), it does not match.

- b. If you select a **predefined rule** template, the **Rule Type** and values are filled in.
5. Click **Next** and review the summary information for the DLP rule template.
6. Click **Confirm** to create and save the new template or click **Previous** to make any corrections needed.

If a template is deleted, the indicated action will no longer be allowed unless the associated policies are disabled or replaced with a different template.

## Creating new document rule templates

1. Click the **Document Rule Template** tab and click **New**.
2. Enter a **Rule Name** (required) and a **Description** (optional).
3. To include Optical Character Recognition (OCR) for API access policies, click the **Optical Character Recognition** toggle.



4. Click **Next**.
5. Enter or select the following information as needed for your template. For each information type to include, click the toggle to enable it.

- **File Metadata** – Enter a range of file sizes to include. Then select file information from the default data types provided with the product, or any data types you created in the **Data Types** tab.

- **File Size Range** - Enter a range of file sizes to include in scanning.

**Note:** DLP and malware scanning are not performed on files larger than 50 MB. To be sure that DLP and malware scanning are available, enter range sizes of 49 MB or smaller in both fields.

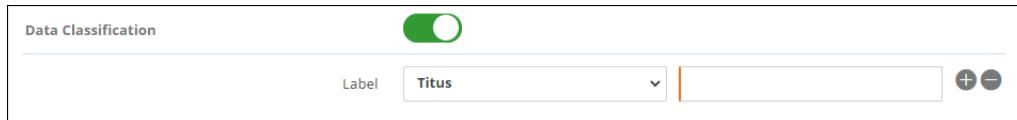
- **File Type** - Select a file type (for example, XML). This option is disabled when minimum and maximum file sizes are 50 MB or larger.
- **File Extension** - Select a file extension (for example, .png).

- **File Name** - Select File Name to specify the exact file name or select Regex Pattern to select a regular expression. In either case, use the drop-down menu to select the value for the policy to find and scan. This may be a predefined data type, or one that you created on the **Data Types** tab.

- **Data Classification**

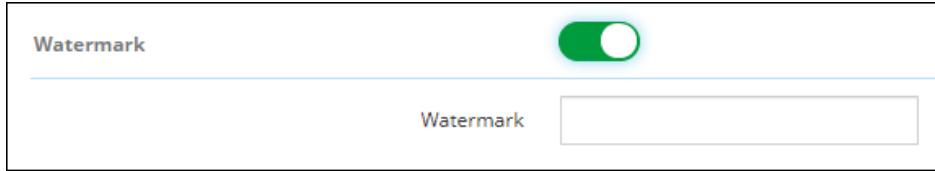


- Select a classification **label** – Microsoft AIP or Titus. Then, enter a label name.



- (Optional) Click the + sign at the right to include both classification labels.

- **Watermark**

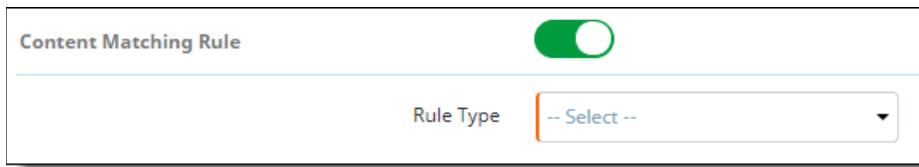


- Enter text for a watermark.

**Note**

For OneDrive and SharePoint applications, watermarks are not locked and can be removed by users.

- **Content Matching Rule**



- Select a DLP rule type from the list.

6. Click **Next** and review the summary information.
7. Click **Save** to confirm the template, or **Previous** to make any corrections.

The template can now be applied to policies you create.

## Create Content Digital Rights templates

Content Digital Rights configurations provide streamlined template management for efficient and consistent application of content classification, customization, and protection options. Templates for content digital rights can be created and the settings applied to multiple policies. The templates can be

accessed and managed through a Content Digital Rights page under the Protect menu in the Management Console.

Content Digital Rights captures all aspects of content classification and protection, in these components.

Where encryption is applied, documents will be tracked by the CDR ID used to encrypt, instead of the ID of the policy that is triggered for encryption.

Once a CDR template is created, it can be modified as needed, but cannot be deleted as long it is still being used.

## Steps for creating CDR templates

Once CDR templates are created, they can be applied to multiple policies as needed.

1. Go to **Protect > Content Digital Rights** and click **New**.
2. Enter a **Name** (required) and a **Description** (optional) for the CDR template.
3. Select the Type of documents to which this template will apply:
  - **Structured** -- Policy applies to structured objects.
  - **Documents with Encryption** -- Policy applies to documents to be encrypted.
  - **Documents without Encryption** -- Policy applies to documents that are not to be encrypted.
4. Click **Next** to add CDR elements.
5. For each component to include, click the toggle to enable it.

- **Watermark Text**

Enter the text for the watermark. Then, select the formatting options for the watermark.

- **Token Obscurity**

Select Mask, Redact, or Document Highlighting.

**IMPORTANT**

The Mask and Redact actions *permanently delete* the selected characters, to prevent unauthorized leaks of data. Masking and redaction cannot be undone once a policy is saved.

**Notes regarding API policy enforcement for Redact, Mask, Watermark/Encrypt actions**

In Salesforce reports (Classic and Lightning versions), the Mask action is not applied to report name, filter criteria, and keyword search. As a result, these items are not masked in the report object.

When an API Protect policy is created with Redact/Mask/Watermark/Encrypt as an action, the policy action is not taken if a file created in Google Drive is renamed and then updated with DLP content.

- **Encrypt**

If the policy will provide an encryption action, select these items to apply specific directions for encryption:

- An encryption key.
- Content expiration – by date, by time, or no expiration.
- If you selected **By Date**, select a date from the calendar.

- If you selected **By Time**, select minutes, hours, or days, and a quantity (for example, 20 minutes, 12 hours, or 30 days).
  - An offline access option.
  - **Always** (default)
  - **Never**
  - **By Time**. If you select **By Time**, select hours, minutes, or days, and a quantity.
6. Add permission objects, which define the scope (internal or external), users and groups, and permission levels.
- a. Click **New** and select permission options.

- b. Scope -- Select Internal or External.
- c. Type –
  - For **Internal** scope, select **Users**, **Groups**, or **Recipients**.
  - For **External** scope, select **Users**, **Domains**, or **Recipients**.

#### Note

The Recipients type applies only to cloud applications that have the Email protection mode selected when the cloud is onboarded.

Depending on the **Type** you choose, the next field will be labeled as follows.

- For **Internal** scope, either **Users** (for users) or **Source** (for groups). If you selected **Recipients**, this next field does not appear. If you selected **Source**, check the names of groups to include.
- For **External** scope, either **Users** (for users) or **Domains**. If you selected **Recipients**, this next field does not appear.

Enter or select the user, source, or domain information.

- For **Users** (Internal or External scope) – Click the pen icon, choose **All** or **Selected**. For **Selected**, enter one or more valid user email addresses, each separated by a comma. Click **Save**.
- For **Source** (Internal scope) – Select a source for the group or groups. From the **Groups List** box that appears, check one or more groups, or all groups. Click **Save**.
- For **Domains** (External scope) – Enter one or more domain names.

Permissions – Select **Allow** (full permissions) or **Deny** (no permissions).

7. Click **Save**. The permission object is added to the list.

- Click **Next** to view a summary of the CDR template and click **Confirm** to save it. The template is listed on the **Content Digital Rights** page. When you assign this template to policies you create, those policy names will appear in the **Assigned Policies** column.

## Configure file type, MIME type, and file size for exclusion from scanning

In hosted deployments, you can specify the file types, MIME types, and sizes of files to be excluded from data scanning. You can specify scanning exclusions for DLP policy types, and for exclusion by the CASB scan engine during malware scanning.

To configure exclusions, go to **Administration > System Settings > Advanced Configuration** and click the **Content Settings** tab. Then, perform the following steps for CASB DLP exclusions, CASB scan engine exclusions, or both.

### Exclusion from scanning by Juniper DLP engine

Click the toggle for each exclusion you want to set.

#### File type

Review the default file types shown and delete those you want to exclude. Because excluded files are not scanned, response time for loading them is faster. For example, rich-media files such as .mov, .mp3, or .mp4 load faster if they are excluded.

File Type Exclusion

List file types to exclude from scanning.

#### MIME type

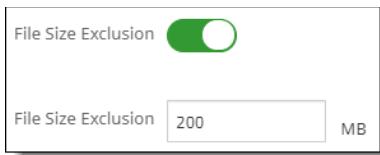
Enter any MIME types to be excluded (for example, text/css, application/pdf, video/\*., where \* acts as a wildcard to indicate any format). Separate each MIME type with a comma.

List MIME types to exclude from scanning.

Enter MIME types separated by a comma (e.g. text/csv; application/pdf; video/\*., where '\*' acts as a wildcard to indicate any format.)

#### File size

Enter a file size (in megabytes) that will serve as the threshold for files to be excluded. Or accept the default value of 200 MB. Any files larger than this size are not scanned. A value greater than zero is required. The maximum value allowed is 250 MB.

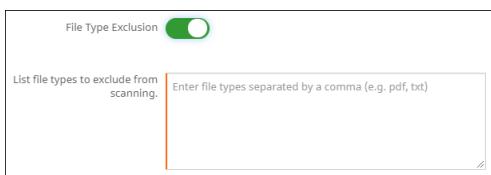


## Exclusions from scanning by the CASB scan engine

Click the toggle for each exclusion you want to set.

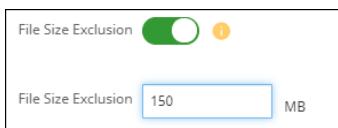
### File type

Enter the file types to exclude. Because excluded files are not scanned, response time for loading them is faster. For example, rich-media files such as .mov, .mp3, or .mp4 load faster if they are excluded.



### File size

Enter a file size (in megabytes) that will serve as the threshold for files to be excluded. Any files larger than this size are not scanned. A value greater than zero is required. The maximum value allowed is 250 MB.



Click **Reset** when finished.

## Configure folder sharing for DLP scanning

You can opt to have DLP scanning performed automatically for files in shared folders.

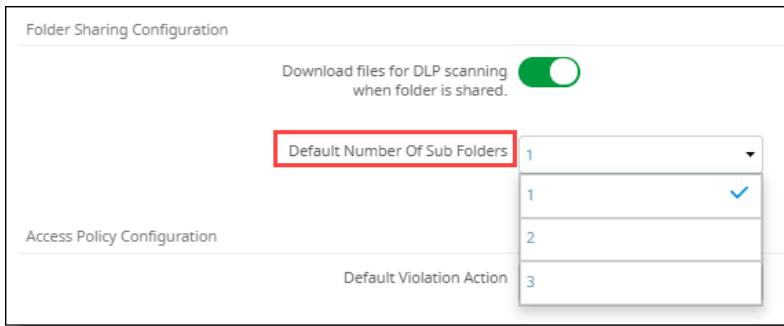
1. Go to **Administration > System Settings > Advanced Configuration** and click the **Content Settings** tab.
2. Under **Folder Sharing Configuration**, click the toggle to enable automatic downloading of files in shared folders.



## Set number of folder sublevels for scanning

1. Go to **Administration > System Settings > Advanced Configuration** and select the **Content Settings** tab.

- Under **Default Number of Sub Folders**, select a number from the dropdown list. The number represents the level of subfolders that will be scanned. For example, if you select 2, data in the parent folder and two subfolder levels will be scanned.



## Configure default policy violation actions

You can set a default violation action – either **Deny** or **Allow & Log**. The action that occurs depends on whether a match is found with an existing policy.

- If a policy match is **not** found, CASB applies the default violation action using a policy called **TenantDefaultAction**. For example, if the default violation action is set to **Deny**, and no policy match is found, CASB applies a Deny action.
- If a policy match **is** found, CASB applies the action from that policy, regardless of which default violation action is set. For example, if the default violation action is set to **Deny**, and CASB finds a matched policy with an action of **Allow & Log** for a specific user, CASB applies the **Allow & Log** action for that user.

### To set a default policy violation action:

- Go to **Administration > System Settings > Advanced Configuration** and click the **Proxy Settings** tab.
- From the **Default Violation Action** dropdown list, select either **Deny** or **Allow & Log**, and click **Save**.

# Creating policies for data protection and application security

---

For CASB, you can create policies that apply to one, some, or all cloud applications in your enterprise.

For each policy, you can specify:

- The types of information to which the policy should apply – for example, content that includes credit card or Social Security numbers, files that exceed a specific size, or files of a specific type.
- The users or groups of users to which the policy should apply, the folders or sites, or whether files can be shared internally, externally, or with the public.
- You can assign one or more protection modes to each cloud application you onboard. These protection modes enable you to apply the types of protection most needed for the data stored on those cloud applications.

You can also create policies that control access to keys that protect encrypted data. If access to a key is blocked by a policy, users cannot access that data protected by that key.

## Note about Slack cloud applications

When creating policies for Slack cloud applications, keep the following items in mind:

- **Remove Collaborator** works only for the following content and context definition:
- Content: **NONE**
- Context: **Member Type**
- Data Type: **Structured**
- Addition of members to a channel is an independent event, which is not associated with messages, files, or any other event in the channel. (The **group\_add\_user** is the event type.)
- The **group\_add\_user** contains no content. There is no structured or unstructured data.
- Because files are org-level properties in Slack, they do not belong to any particular channel or workspace. As a result, you must select structured data as the event type.
- **Member Type** context: By default, Slack is a sharing cloud, and uploading a file or sending a message to a channel is in itself a sharing event. As a result, a new context (apart from the existing sharing type) is available to help manage events for Slack cloud applications.

## Note about Microsoft 365 cloud applications (OneDrive)

- When files are uploaded to OneDrive, the Modified By field in OneDrive displays the name **SharePoint App** instead of the name of the user who uploaded the file.

## Note about capturing events in the Slack thick app

To capture events in the Slack thick app in forward proxy mode, you must log out of both the application and the browser and log in again to authenticate.

- Log out of all workspaces in the desktop Slack app. You can log out from the application grid.
- Log out from the browser.
- Log in to the Slack app again to authenticate.

The following sections provide step-by-step instructions for creating policies to meet your data protection needs.

- Viewing policy lists

- API Access policies

## Viewing policy lists

From the **Protect** page of the Management Console, you can create and update policies, set their priorities, and update the rules that apply to them.

Depending on the type of policy, the policy list page includes tabs that display policies created for specific security and data protection needs.

### API Access policies

Two options for **API Access** policies are available:

- The **Real Time** tab lists policies created for real-time scanning. Most of the policies you create will be real-time policies.
- The **Cloud Data Discovery** tab lists policies created for use with Cloud Data Discovery, which enables CASB to discover sensitive data (for example, Social Security numbers) through scheduled scans in your cloud applications and apply remediation actions to protect that data.

Cloud Data Discovery can be used to perform scans for Box automated clouds.

For more information, see [Cloud Data Discovery](#).

## Creating API Access policies

1. Go to **Protect > API Access Policy**.
2. Make sure that the **Real Time tab** is in view. Then, click **New**.

#### Note

For DLP to work with Salesforce, you must have the following settings enabled in Salesforce:

- **Enable CRM** must be enabled for all users.
  - Sharing settings must be *other than Private*.
  - For non-administrators, the **Push Topics** and **API Enable** permissions must be enabled.
1. Enter a **Name** (required) and a **Description** (optional).
  2. Select a **Content Inspection Type – None, DLP Scan, or Malware Scan**. Then, configure the context and actions for the policy type.
    - API policies with **DLP Scan** or **None** as the content inspection type
    - API policies with **Malware Scan** as the content inspection type

### API policies with DLP Scan or None as the content inspection type

If you choose **DLP Scan** as the content inspection type, you can select options for protection of several types of sensitive data for industries such as banking and health care. You must then select a policy template. For example, if you are creating a policy to encrypt all documents containing U.S. Social Security numbers, select **Personal ID – US SSN** as the policy template. If you are creating a policy to encrypt files of a specific type, select the file type as the policy template.

If you select **None** as the content inspection type, the DLP options are not available.

1. Click **Next** to select cloud applications, context, and actions.
2. Select the cloud applications for the policy.

You can apply additional context options specific to the cloud applications you select, depending on the options available for each application. For example:

- If you are creating a policy for a OneDrive account, you will not see the context option for sites because that option is unique to SharePoint Online.
- If you are creating a policy for SharePoint Online, you can select **Sites** as a context.
- If you are creating a policy for Salesforce (SFDC), **Users** is the only context type option available.

To select *all* cloud applications, check **FileSharing**. This option allows you to select only context definitions that are common across the cloud applications in your enterprise.

3. Under **Content Scanning**, check **Structured Data**, **Unstructured Data**, or both, depending on which cloud applications you are including in the policy.

- **Structured data** – Includes objects (for example, contact or lead tables used by Salesforce). Structured data objects cannot be quarantined or encrypted, and remediation actions cannot be performed on them. You cannot remove public links or remove collaborators. If you did not choose a Salesforce cloud for this policy, this option will be disabled.
- **Unstructured data** – Includes files and folders.

**Note** For Dropbox applications, collaborators cannot be added or removed at the file level; they can be added or removed only on the parent level. As a result, the sharing context will not match for subfolders.

4. Do either of the following actions:

- If the content inspection type is **DLP Scan** –
  - Select a **Rule Template** from the list. These are the templates you created previously (**Protect > Content Rule Management**). If the scanning type is **Structured Data**, the DLP rule templates are listed. If the scanning type is **Unstructured Data**, the document rule templates are listed.
  - To enable scanning by an external DLP service, click the **External DLP** toggle. To perform EDLP scanning, you must have external DLP configured from the **Enterprise Integration** page.
- If the content inspection type is **None** –
  - Go to the next step.

5. Under **Context Rules**, select a context type. Context rules identify to whom the policy is to be applied – for example, which cloud applications, users and user groups, devices, locations, or files and folders. The items you see in the list depend on the cloud applications you have selected for the policy.

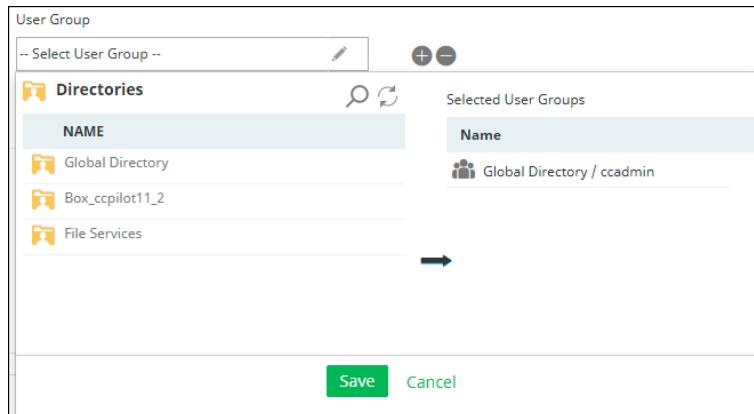
- **Users** – Enter the email IDs of the users to whom the policy applies or select **All Users**.
- **User Groups** – If you have user groups, they will be populated in a list. You can select one, some, or all user groups. To apply a policy to multiple users, create a user group and add the user group name.

User groups are organized into directories. When you select **User Group** as a context type, the available directories containing the groups are listed in the left column.

User groups can be helpful in defining rules for access to specific types of sensitive data. By creating user groups, you can limit access to that data to the users in that group. User groups can also be helpful in managing encrypted content – for example, the finance department might need the extra security of having some of its data encrypted and accessible only to a small group of users. You can identify these users in a user group.

Select a directory to view the user groups it contains. The user groups for that directory are displayed.

Select the groups from the list and click the right-arrow icon to move them to the **Selected User Groups** column and click **Save**. These are the groups to which the policy will apply.

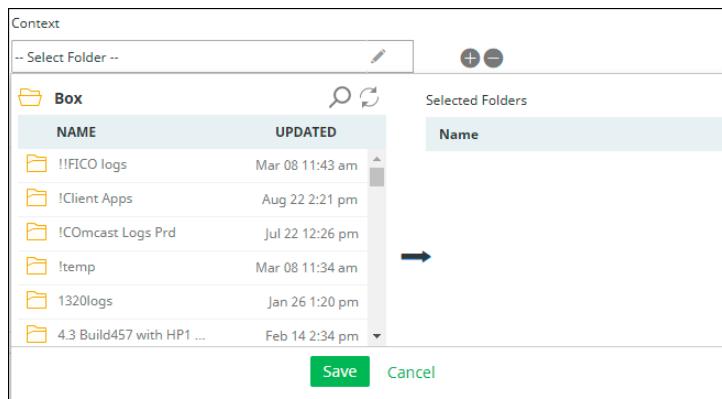


To search for a directory or group, click the **Search** icon at the top.

To refresh the list, click the **Refresh** icon at the top.

## Notes

- If you select **All user groups**, the policy you are creating will apply to all new user groups you create in the future.
- For **Dropbox**, only the **Users** and **User Groups** options are supported.
- When selecting users for **Salesforce**, provide the user's *email address*, not the Salesforce username. Make sure that this email address is for a user, not an administrator. The user and administrator email addresses should not be the same.
- **Folder (Box, OneDrive for Business, Google Drive, and Dropbox cloud applications only)** – For policies that pertain to OneDrive for Business, select the folder (if any) to which the policy applies. For policies that pertain to Box, enter the folder ID of the folder to which the policy applies.



### Note

In OneDrive applications, only folders owned by administrator users are displayed in policies with a **Folder** context type.

**Creating secure folder policies (Box cloud applications only)** -- A folder is treated as a *secure folder* when documents stored in it are encrypted. You can designate a secure folder by creating a secure folder policy. You might want to create such a policy if a folder was moved or copied and you want to be sure that the text in all of its files is encrypted, or if any network or service disruption occurred that might leave files in plain text.

To create a secure folder, set the context as **Folder**, the DLP Rule as **None**, and the action as **Encrypt**.

**Secure folder audits** -- CASB audits secure folders every two hours, checking each one for files that have plain text. If content with plain text is found in any file, it is encrypted. Files that are already encrypted (.ccsecure files) are ignored during the audit. To change the audit schedule, contact Juniper Networks Support.

- **Folder Names** – Enter one or more folder names.
- **Collaboration (Slack Enterprise)** - For policies that pertain to Slack Enterprise, select the Slack Enterprise cloud application to which the policy applies. The following context rules are specific to Slack Enterprise cloud applications:
  - **Users** -- All or Selected
  - **Channels** -- Group chat and Channels shared at Org level
  - **Workspaces** -- Workspaces (all Workspaces are listed, including non-authorized workspaces)
  - **Sharing Type**
  - **Member Type** -- Internal / External
- **Sites (SharePoint Online cloud applications only)** – For policies that pertain to SharePoint Online, select the sites, subsites, and folders to which the policy applies.

### Note

When you select **Sites** as a context type for SharePoint cloud applications, you must enter the full site name to allow CASB to perform a successful search.

- **Sharing Type** – Identifies who the content can be shared with.
  - **External** – Content can be shared with users outside your organization's firewall (for example, business partners or consultants). These external users are known as **external collaborators**. Because sharing of content between organizations has become easier, this policy control can help you exercise greater control over what types of content you share with external collaborators.

If you choose a Sharing type of **External**, a **Blocked Domain** option is available. You can specify domains (such as popular email address domains) to be blocked from access.



- **Internal** – Content can be shared with internal groups you specify. This policy control helps you exercise greater control over who within your organization can see specific types of content. For example, many legal and financial documents are confidential and should be shared only with specific employees or departments. If the policy you are creating is for a single cloud application, you can specify one, some, or all groups as shared groups by

selecting the groups from the dropdown list in the Shared Groups field. If the policy applies to multiple cloud applications, the **Shared Groups** option defaults to **All**. You can also specify any shared groups as exceptions.

The screenshot shows a user interface for defining context rules. At the top, there's a section labeled "Context Rules". Below it, there are two dropdown menus: "Sharing Type" and "Internal". To the right of these is a text input field containing "1 User Group", which is highlighted with a red rectangular border. There are also three small circular icons with symbols (+, -, and a pencil) to the right of the input field.

- **Private** – Content is not shared with anyone; it is available only to its owner.
- **Public** – Content is available to anyone inside or outside the company who has access to the public link. When the public link is active, anyone can access the content without a login.
- **File Sharing** – Select **External**, **Internal**, **Public**, or **Private**. If there are any blocked domains for external sharing, enter the domain names.
- **Folder Sharing** – Select **External**, **Internal**, **Public**, or **Private**. If there are any blocked domains for external sharing, enter the domain names.

6. (Optional) Select any **Context Exceptions** (items to exclude from the policy).

If you selected the context types **Sharing Type**, **File Sharing**, or **Folder Sharing**, you can enable an additional option, **Apply to Content Actions**, to configure whitelisting of domains. Click the toggle to enable this option. Then, select **Whitelist Domains**, enter the applicable domains, and click **Save**.

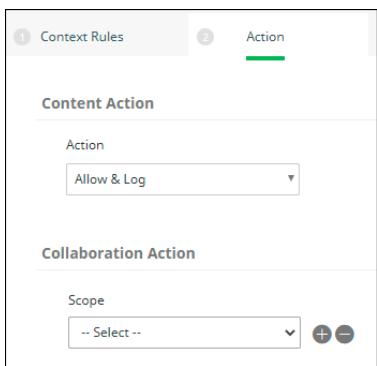
This screenshot shows the "Context Rules" interface with the "Context Exceptions" section expanded. In the "Context Exceptions" section, there is a toggle switch labeled "Apply to Content Actions" which is turned on (green). This switch is highlighted with a red rectangular border. Below the switch, there are two dropdown menus: "Context Type" set to "Whitelist Domains" and "Whitelist Domains" itself, which contains "1 Whitelist Domains". To the right of the "Whitelist Domains" input field are three small circular icons (+, -, and a pencil).

7. Click **Next**.

8. Select **actions**. Actions define how policy violations are addressed and resolved. You can select an action based on the sensitivity of data and the severity of violations. For example, you might choose to delete content if a violation is serious; or you might remove access to the content by some of your collaborators.

Two types of actions are available:

- Content actions
- Collaboration actions



Content actions include:

- **Allow & Log** – Logs file information for viewing purposes. Select this option to see what content is uploaded and what remediation steps, if any, are needed.
- **Content Digital Rights** – Defines content classification, customization, and protection options. Select the CDR template to use for the policy.

#### Note regarding content actions that include watermarking:

For OneDrive and SharePoint applications, watermarks are *not* locked and can be removed by users.

- **Permanent Delete** – Deletes a file permanently from a user's account. *After a file is deleted, it cannot be recovered.* Be sure that policy conditions are being detected properly before you enable this action in production environments. As a rule, use the permanent delete option only for serious violations in which avoiding access is critical.
- **User Remediation** – If a user uploads a file that violates a policy, the user is given a specified time to remove or edit the content that caused the violation. For example, if a user uploads a file that exceeds a maximum file size, the user can be given three days to edit the file before it is permanently deleted. Enter or select the following information.
  - **Duration to Remediate** – The time (up to 30 days) in which remediation must be completed, after which the file is rescanned. Enter a number and frequency for the remediation time allowance.

- **User Remediation Action and Notification** –
  - Select a remediation action for the content. The options are **Permanent Delete** (delete the content permanently), **Content Digital Rights** (comply with conditions included in the Content Digital Rights template you choose), or **Quarantine** (place the content in quarantine for administrative review).
  - Select a **notification type** for informing the user about what action was taken on the file after the remediation time expired.

For more information about notifications, see [Creating and managing notifications and alerts](#).

#### Note

Remediation is not available for cloud applications that store objects and records (structured data).

- **Quarantine** – Quarantine does not delete a file. It restricts user access to the file by moving it to a special area to which only an administrator has access. The administrator can review the quarantined file and determine (depending on the violation) whether to encrypt it, delete it permanently, or restore it. The quarantine option can be used for files that you do not want to remove permanently, but that might require evaluation before further action.

Quarantine is not available for cloud applications that store structured data.

- **AIP Protect** -- Applies Azure Information Protection (Azure IP) actions to the file. For information about applying Azure IP, see [Azure IP](#).
- **Decrypt** – For context type of folder, decrypts content for files when those files are moved to specific folders or when a file's content is downloaded to a managed device, to specified users, groups, and locations, or to an authorized network. The **Decrypt** action is available only for policies with a content inspection method of **None**.

You can specify users or groups to be excluded from enforcement of the policy. In the field to the right, select the user or group names to exclude.

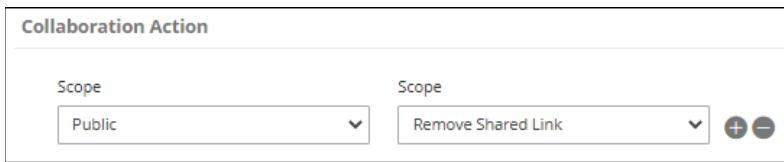
#### Notes

- In the **Exceptions** list, blocked domains are called **Whitelist Domains**. If you have specified blocked domains, you can list domains to exclude from blocking.
- For cloud applications that include unstructured data in the policy, several actions are available, including **Allow & Log**, **Content Digital Rights**, **Permanent Delete**, **User Remediation**, **Quarantine**, and **AIP Protect**.
- For cloud applications that include *only* structured data, only the **Log** and **Permanent Delete** actions are available.

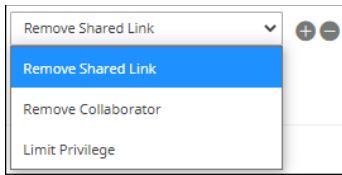
If the policy will apply to a Salesforce cloud application:

- Not all available context and action options apply. For example, files can be encrypted, but not quarantined.
- You can apply protection to both files and folders (unstructured data) and structured data objects.

Collaboration actions can be selected for Internal, External, and Public users. To select more than one user type, click the + icon at the right.



Select an option for the user type(s).



- **Remove Shared Link** – A shared link makes content available without a login. If a file or folder includes a shared link, this option removes shared access to the file or folder. This action does not affect the *content* of the file -- only its access.
- **Remove Collaborator** – Removes the names of internal or external users for a folder or file. For example, you might need to remove the names of employees who have left the company, or

external partners who are no longer involved with the content. These users will no longer be able to access the folder or file.

**Note** For Dropbox applications, collaborators cannot be added or removed at the file level; they can be added or removed only on the parent level. As a result, the sharing context will not match for subfolders.

- **Limit Privilege** – Limits the user action to one of two types: **Viewer** or **Previewer**.
  - **Viewer** enables the user to preview content in a browser, download, and create a shared link.
  - **Previewer** allows the user only to preview content in a browser.

The **Limit Privilege** action is applied on the file level only if the policy content is DLP. It is applied on the folder level if the policy content is **NONE**.

9. (Optional) Select a secondary action. Then, select a notification from the list.

**Note** If **Remove Recipients** is selected as a secondary action with external domains, the policy will act on all external domains if no domain values are entered. The value of **All** is not supported.

10. Click **Next** and review the policy summary. If the policy includes a Salesforce cloud, a **CRM** column will appear next to the **FileSharing** column.

11. Then, perform any of these actions:

- Click **Confirm** to save and activate the policy. Once the policy is in effect, you can view policy activity through your dashboards on the **Monitor** page.
- Click **Previous** to go back to previous screens and edit information as needed. If you need to change the policy type, do so before you save it, because you cannot change the policy type after you save it.
- Click **Cancel** to cancel the policy.

#### **Note**

Once policies are created and violations are detected, it might take up to two minutes for violations to be reflected in dashboard reports.

## API policies with Malware Scan as the content inspection type

1. In the **Basic Details** page, select **Malware Scan**.

2. Select scanning options.

Two options are available:

- **Native Scan Engine** uses the native scanning engine.
- **External ATP Service** uses an external service you choose from the ATP Service dropdown list.

3. Click **Next** to select context options.

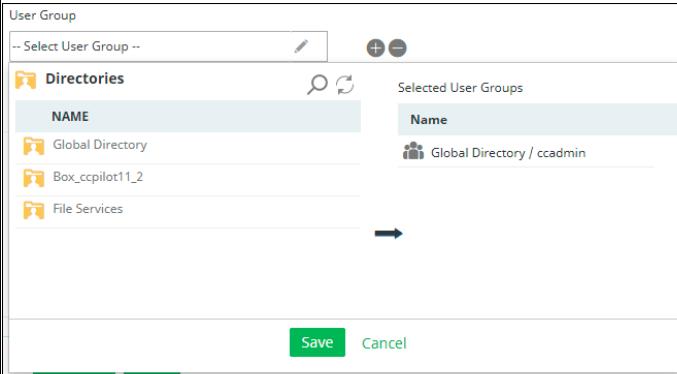
4. In the **Destinations** pane, select one or more applications that you want this policy to apply to.

Note: If you select a Google Drive application here, CASB may be unable to honor the policy for that application due to restrictions created by the Google cloud application's behavior.

Select a **Context Type**. The options available depend on the cloud application that you selected. Options may include **Users**, **User Groups**, **Folder** (for some cloud applications), Folder **Names**, **Sharing Type**, **File Sharing**, and **Folder Sharing**.

To include more than one context type in the policy, click the + sign to the right of the **Context Type** field.

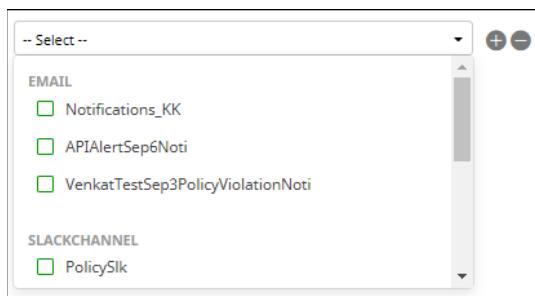
- Enter or select the context details for the context type(s) you chose.

Context type	Context details
<b>Users</b>	Enter valid usernames or select <b>All Users</b> .
<b>User Groups</b>	<p>User groups are organized into directories. When you select User Group as a context type, the available directories containing the groups are listed in the left column.</p> <p>Select a directory to view the user groups it contains. The user groups for that directory are displayed.</p> <p>Select the groups from the list and click the right-arrow icon to move them to the <b>Selected User Groups</b> column and click <b>Save</b>. These are the groups to which the policy will apply.</p>  <p>To search for a directory or group, click the <b>Search</b> icon at the top. To refresh the list, click the <b>Refresh</b> icon at the top.</p>
<b>Folder</b>	Select folders to be included in the policy actions.
<b>Folder Names</b>	Enter the names of folders to be included in the policy actions.
<b>Sharing Type</b>	<p>Select a scope for sharing:</p> <ul style="list-style-type: none"> <li>▪ <b>External</b> – Enter blocked domains and click <b>Save</b>.</li> <li>▪ <b>Internal</b></li> <li>▪ <b>Public</b></li> <li>▪ <b>Private</b></li> </ul>
<b>File Sharing</b>	<p>Select a scope for file sharing:</p> <ul style="list-style-type: none"> <li>▪ <b>External</b> – Enter blocked domains and click <b>Save</b>.</li> </ul>

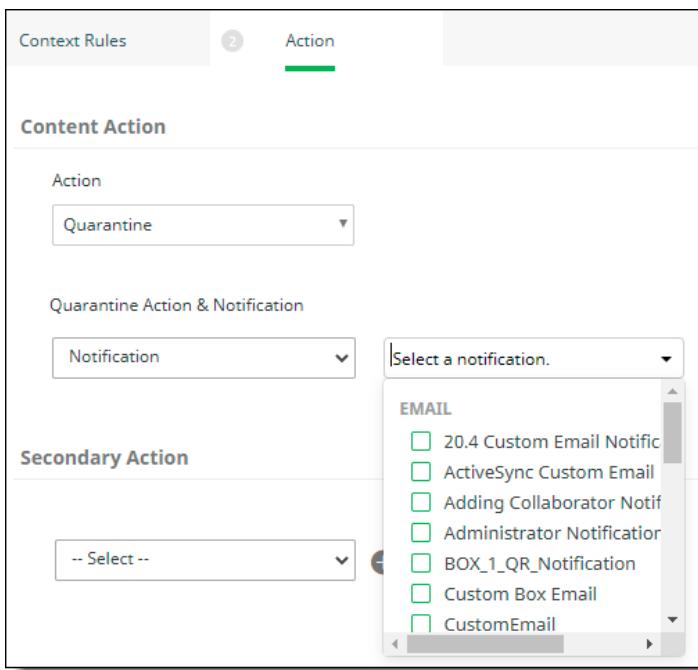
Context type	Context details
	<ul style="list-style-type: none"> <li>- Internal</li> <li>- Public</li> <li>- Private</li> </ul>
<b>Folder Sharing</b>	<p>Select a scope for folder sharing:</p> <ul style="list-style-type: none"> <li>- <b>External</b> – Enter blocked domains and click <b>Save</b>.</li> <li>- Internal</li> <li>- Public</li> <li>- Private</li> </ul>

6. (Optional) Select any **Context Exceptions** (items that will be excluded from policy actions).
7. Select a **Content Action**. The options include **Allow & Log**, **Permanent Delete**, and **Quarantine**.

If you select **Allow & Log** or **Permanent Delete**, choose a notification type as a secondary action (optional). Then, select an email or channel notification from the list.



If you select **Quarantine**, select **Notification** from the **Quarantine Action & Notification** list. Then, select a quarantine notification.



8. Click **Next** and review the policy summary. If the policy includes a Salesforce cloud, a **CRM** column will appear next to the **FileSharing** column.
9. Then, perform any of these actions:
  - Click **Confirm** to save and activate the policy. Once the policy is in effect, you can view policy activity through your dashboards on the Monitor page.
  - Click **Previous** to go back to previous screens and edit information as needed. If you need to change the policy type, do so before you save it, because you cannot change the policy type after you save it.
  - Click **Cancel** to cancel the policy.

## Managing connected applications

---

CASB provides a single location on the Management Console where you can view information about third-party applications connected to the cloud applications in your organization, install additional applications as needed, and revoke access to any applications that are considered unsafe or that could put data security at risk.

Management of connected applications is supported for Google Workspace, Microsoft 365 suite, Salesforce (SFDC), AWS, and Slack cloud applications, and can be used for cloud applications with API protection mode. For Microsoft 365 cloud applications, the applications listed on the Management Console are those that have been linked to Microsoft 365 by the administrator.

To view a list of connected applications, go to **Protect > Connected Apps**.

The **Connected Apps** page view provides information in two tabs:

- **Connected Apps** – Displays information about the applications installed in the cloud applications onboarded in your organization; also provides options for showing additional details and removing (revoking access to) an application.
- **AWS Keys Usage** – For any AWS cloud applications you have onboarded, displays information about the access keys used by administrators for those cloud applications.

## Managing applications from the Connected Apps tab

The **Connected Apps** tab displays the following information about each application.

- **Account Name** -- the name of the cloud to which the application is connected.
- **App Info** -- The name of the connected application, along with the identification number for the application.
- **Created Date** -- The date on which the app was installed on the cloud.
- **Owner Info** -- The name or title of the person or administrator who installed the application, and their contact information.
- **Cloud Certified** -- Whether the application has been approved by its vendor to be published on the cloud.
- **Action** – By clicking the **View** (binocular) icon, you can view details about a connected application. The details shown vary by application, but typically they will include items such as **Account ID**, **Account Name**, **App Name**, **App ID**, **Cloud Certified** status, **Cloud Name**, **Created Date**, and user **Email**.

Details	
KEY	VALUE
Account Id	69994103233
Account Name	O365_UCSF
App Id	403a36ad-8ea6-4299-baeb-8385afa44cb6
App Name	Automation-User
Cloud Certified	Yes
Cloud Name	office365
Created Date	12/25/2018, 09:36:05 PM
Email	

**OK**

## Managing AWS key use

The **AWS Keys Usage** tab lists the access keys used for AWS accounts.

For each key, the tab shows the following information:

- **Account Name** — The account name for the cloud.
- **User Name** — The user ID for the administrator user.
- **Permissions** — The types of permissions granted to the administrator user for the account. If the account has multiple permissions, click **View More** to see additional listings.
- **Access Key** — The key assigned to the administrator user. Access keys provide credentials for IAM users or an AWS account root user. These keys can be used to sign programmatic requests to the AWS CLI or the AWS API. Each access key consists of the key ID (listed here) and a secret key. Both the access key and the secret key must be used to authenticate requests.
- **Action** — The actions that can be taken on each listed account:



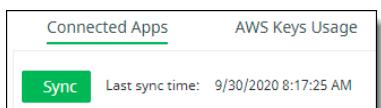
- **Recycle icon** -- Go to the **Activity Audit Logs** page to view activity for this cloud.
- **Disable icon** -- Disable the access key if it is determined to be unsafe as far as data security or is no longer needed.

## Filtering and syncing connected application and AWS information

On both tabs, you can filter and refresh the information displayed.

To filter information by cloud application, check or uncheck the names of the cloud applications to include or exclude.

A sync occurs automatically every two minutes, but you can refresh the display with the most recent information at any time. To do so, click **Sync** at the upper left.



# Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM)

Cloud Security Posture Management (CSPM) and Juniper Networks SaaS Security Posture Management (SSPM) provides organizations with a comprehensive set of tools to monitor resources used in their organizations, assess security risk factors against security best practices, perform the needed actions to prevent misconfigurations that put their data at increased risk, and continually monitor risk. CSPM makes use of security benchmarks such as CIS for AWS and Azure, and SSPM best practices for Salesforce and Microsoft 365 Security Best Practices for Microsoft 365.

## Cloud applications supported

CSPM/SSPM supports the following cloud types:

- For IaaS (Infrastructure as a Service) —
- Amazon Web Services (AWS)
- Azure
- For SaaS (Software as a Service) Security Posture Management (SSPM) —
- Microsoft 365
- Salesforce

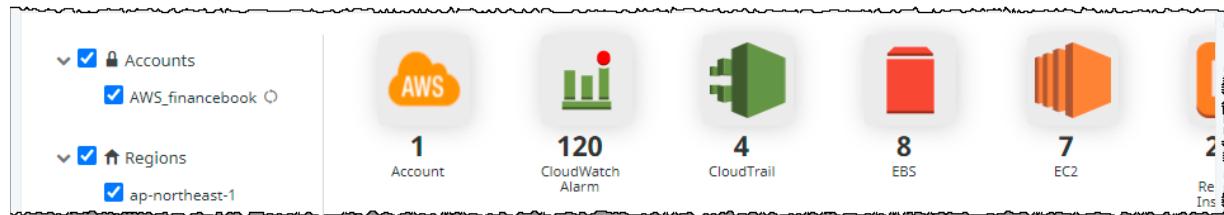
CSPM/SSPM includes two major components:

- Infrastructure Discovery (discovering the resources used for the customer account) (inventory)
- Assessment configuration and execution

## Infrastructure Discovery

Infrastructure Discovery (**Discover > Infrastructure Discovery**) involves identification of the presence and use of resources in an organization. This component applies only to the IaaS cloud applications. Each application includes its own list of resources that can be extracted and displayed.

The **Infrastructure Discovery** page shows the resources available for each IaaS cloud (one tab for each cloud).



At the left of each tab is a list of accounts, regions, and resource groups. You can select and deselect items from each list to filter the display.

The resource icons at the upper part of the page represent the resource type and the number of resources for each type. When you click a resource icon, the system extracts a filtered list for that resource type. You can select multiple resource types.

The table at the lower part of the page lists each resource, showing the resource name, resource ID, resource type, account name, associated region, and the dates on which the resource was first and last observed.

DETAILS	RESOURCE NAME	RESOURCE ID	RESOURCE TYPE	ACCOUNT NAME	REGION	TAGS	FIRST OBSERVED	LAST OBSERVED
	vpc-5c00eb3a	vpc	AWS_autoqa	sa-east-1			01/29/2021 06:0...	02/07/2021 06:08:...
	vpc-745eac12	vpc	AWS_autoqa	ap-southeast-1			01/29/2021 06:0...	02/07/2021 06:08:...
	vpc-bcb94ad7	vpc	AWS_autoqa	ap-south-1			01/29/2021 06:0...	02/07/2021 06:08:...

The **First Observed** and **Last Observed** timestamps help to identify when the resource was first added, and the date it was last seen. If a resource timestamp shows that it has not been observed for a long time, that could indicate that the resource was deleted. When resources are pulled, the **Last Observed** timestamp is updated — or, if a resource is new, a new row is added to the table with a **First Observed** timestamp.

To display additional details for a resource, click the **binocular** icon at the left.

To search for a resource, enter search characters in the **Search** field above the resource table.

## Assessment configuration

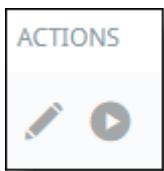
Assessment configuration (**Protect > Cloud Security Posture**) involves creation and management of information that evaluates and reports on risk factors, based on selected rules in the organization's security infrastructure. This component supports these cloud applications and industry benchmarks:

- **AWS** — CIS
- **Azure** — CIS
- **Salesforce** -- Juniper Networks Salesforce Security Best Practices
- **Microsoft 365** -- Microsoft 365 Security Best Practices

The **Cloud Security Posture** page in the Management Console lists the current assessments. This list shows the following information.

- **Assessment Name** -- The name of the assessment.
- **Cloud Application** -- The cloud to which the assessment applies.
- **Assessment Template** -- The template used to perform the assessment.
- **Rules** -- The number of rules currently enabled for the assessment.
- **Frequency** -- How often the assessment is run (daily, weekly, monthly, or on demand).
- **Last Run On** -- When the assessment was last run.
- **Enabled** -- A toggle that indicates whether the assessment is currently enabled (see Questions section).
- **Assessment Status** – The number of rules that were triggered and passed the last time this assessment was run.

- **Not Run** – The number of rules that were not triggered the last time this assessment was run.
- **Weightage Score** -- A color bar that shows the risk score for the assessment.
- **Action** – Enables you to take the following actions for an assessment:



- **Pencil icon** – Edit the properties of an assessment.
- **Arrow icon** – Run an assessment on demand.

By clicking the eye icon at the left, you can view additional details for the most recent assessment.

These details are shown in two tabs:

- **Assessment Results**
- **Past Assessment Reports**

## Assessment Results tab

The **Assessment Results** tab lists the compliance rules associated with an assessment. For each rule included in the assessment, the display shows the following information:

- **Compliance Rule** – The title and ID of the included rule.
- **Enabled** – A toggle that indicates whether the rule is enabled for this assessment. You can enable or disable compliance rules as needed depending on your security assessment of the cloud.
- **Resources Passed/Resources Failed** – The number of resources that passed or failed the assessment.
- **Last Run Status** – The overall status of the last assessment run, either Success or Failed.
- **Last Run Time** – The date and time that the last assessment was run.

## Past Assessment Reports tab

The **Past Assessment Reports** tab lists the reports that have been run for the assessment. A report is generated when an assessment is run and is added to the list of reports. To download a PDF report, click the **Download** icon for that report, and save it to your computer.

The report provides detailed information about the activity for the cloud, including:

- An executive summary with a count of rules and resources passed and failed
- Counts and details about resources that were tested and failed, and remediation recommendations for failed resources

If an assessment is deleted, its reports are deleted also. Only the Splunk audit logs are preserved.

To close the assessment detail view, click the Close link at the bottom of the screen.

## Adding a new assessment

1. From the Management Console, go to **Protect > Cloud Security Posture Management**.

2. From the **Cloud Security Posture Management** page, click **New**.

You will see these fields initially. Depending on the cloud account you select for the assessment, you will see additional fields.

The screenshot shows the 'Cloud Security Posture' interface. The top navigation bar includes 'Home', 'Discover', 'Monitor', 'Protect' (which is highlighted in green), 'Administration', and 'Reports'. To the right are icons for help ('i'), a question mark ('?'), and a user profile ('SD'). Below the navigation is a title 'Cloud Security Posture'. A horizontal progress bar indicates the current step: 'Basic Details' (green circle), 'Compliance Rules' (blue circle), and 'Summary' (blue circle). The 'Basic Details' section contains the following form fields:

- Assessment Name: Input field containing 'Assessment Name'.
- Description: Input field containing 'Assessment Description'.
- Cloud Account: Dropdown menu showing '... Select ...'.
- Frequency: Dropdown menu showing '... Select ...'.
- Assessment Notification: Dropdown menu showing '... Select ...'.
- Audit Notification: Dropdown menu showing '... Select ...'.

At the bottom of the form are two buttons: 'Next' (highlighted in green) and 'Cancel'.

3. Enter this information for the new assessment as indicated for the type of cloud account to be used for the assessment.

Field	IaaS cloud applications (AWS, Azure)	SaaS cloud applications (Salesforce, Microsoft 365)
<b>Assessment Name</b>  Enter a name for the assessment. The name can include only numbers and letters – no spaces or special characters.	Required	Required
<b>Description</b>  Enter a description of the assessment.	Optional	Optional

Field	IaaS cloud applications (AWS, Azure)	SaaS cloud applications (Salesforce, Microsoft 365)
<b>Cloud Account</b> Select the cloud account for the assessment. All information for the assessment will pertain to this cloud. <b>Note</b> The list of cloud applications includes only those for which you have specified <b>Cloud Security Posture</b> as a protection mode when you onboarded the cloud.	Required	Required
<b>Assessment Template</b> Select a template for the assessment. The template option shown pertains to the cloud account you select.	Required	Required
<b>Filter by Region</b> Select the region or regions to be included in the assessment.	Optional	N/A
<b>Filter by Tag</b> To provide an additional level of filtering, select a resource tag.	Optional	N/A
<b>Frequency</b> Select how often to run the assessment – daily, weekly, monthly, quarterly, or on demand.	Required	Required
<b>Notification Template</b> Select a template for email notifications regarding assessment results.	Optional	Optional
<b>Resource Tag</b> You can create tags to identify and track failed resources. Enter text for a tag.	Optional	N/A

- Click **Next** to display the **Compliance Rules** page, where you can select rule enablement, rule weighting, and actions for the assessment.

This page lists the compliance rules available for this assessment. The list is grouped by type (for example, rules pertaining to monitoring). To show the list for a type, click the arrow icon to the left of the rule type. To hide the list for that type, click the arrow icon again.

To display details for a rule, click anywhere on its name.

Compliance Rule Details	
<b>Rule Name</b>	Ensure multi-factor authentication (MFA) is enabled for all IAMusers that have a console password (Scored)
<b>Control Number</b>	1.2
<b>Rule Group</b>	Identity and Access Management
<b>Profile</b>	Level 1
<b>Description</b>	Multi-Factor Authentication (MFA) adds an extra layer of protection on top of a user name and password. With MFA enabled, when a user signs in to an AWS website, they will be prompted for their user name and password as well as for an authentication code from their AWS MFA device. It is recommended that MFA be enabled for all accounts that have a console password.
<b>Resource Name</b>	IAM User
<b>Action</b>	Audit
<b>Active</b>	true
<b>Weight</b>	3

- Configure the rules as follows:

- Enabled** -- Click the toggle that indicates whether the rule will be enabled for the assessment. If it is not enabled, it will not be included when the assessment is run.
- Weight** – The weight is a number from 0 to 5 that indicates the relative importance of the rule. The higher the number, the greater the weight. Select a number from the dropdown list or accept the default weight shown.
- Comments** – Enter any comments that pertain to the rule. A comment can be helpful if (for example) the rule weight or action is changed.
- Action** – Three options are available, depending on the cloud you selected for this assessment.
  - Audit** -- The default action.
  - Tag** (AWS and Azure cloud applications) -- If you selected **Resource Tags** when you created the assessment, you can choose **Tag** from the dropdown list. This action will apply a tag to the rule if the assessment finds failed resources.
  - Remediate** (Salesforce cloud applications) -- When you select this action, CASB will attempt to resolve issues for failed resources when the assessment is run.

- Click **Next** to review a summary of the assessment information.

Then, click **Previous** to make any corrections, or **Save** to save the assessment.

The new assessment is added to the list. It will run on the schedule you selected. You can also run the assessment any time by clicking the arrow icon in the **Actions** column.

## Modifying assessment details

You can modify existing assessments to update their basic information and rule configurations. To do so, click the pencil icon under the **Actions** column for the assessment you want to modify.

The information is displayed in two tabs:

- Basic Details
- Compliance Rules

### Basic Details tab

In this tab, you can edit the name, description, cloud account, filtering and tagging information, templates used, and frequency.

Click **Update** to save the changes.

### Compliance Rules tab

In the **Compliance Rules** tab, you can view rule details, add or delete comments, and change enablement status, weight, and actions. The next time the assessment is run, these changes will be reflected in the updated assessment. For example, if the weight of one or more rules is changed, the count of passed or failed resources could change. If you disable a rule, it will not be included in the updated assessment.

Click **Update** to save the changes.

## Cloud Data Discovery

Cloud Data Discovery enables discovery of data through cloud scans. Using APIs, CASB can perform compliance scanning of data for ServiceNow, Box, Microsoft 365 (including SharePoint), Google Drive, Salesforce, Dropbox, and Slack cloud applications.

With Cloud Data Discovery, you can perform these actions:

- Scan for data such as credit card numbers, Social Security numbers, custom keywords, and RegEx strings.
- Identify this data in objects and records.
- Enable checking public link folders and external collaboration folders for collaboration violations.
- Apply remediation actions including permanent delete and encryption.

You can configure scans in several ways:

- Select a schedule for scans -- once, weekly, monthly, or quarterly.
- Perform full or incremental scans. For full scans, you can select a time period (including a custom date range), which enables you to run scans for shorter durations with reduced sets of data.
- Defer policy actions for scans and review them later.

You can view and run reports for past scans.

The workflow for cloud data discovery includes the following steps:

1. Onboard a cloud for which you want to apply Cloud Data Discovery
2. Create a Cloud Data Discovery policy
3. Create a scan
4. Associate a scan with a Cloud Data Discovery policy
5. View scan details (including past scans)
6. Generate a scan report

The following sections detail these steps.

## Onboard a cloud application for which you want to apply Cloud Data Discovery

1. Go to **Administration > App Management**.
2. Select ServiceNow, **Slack**, **Box**, or **Office 365** for the cloud type.
3. Select **API Access** and **Cloud Data Discovery** protection modes to enable CDD scans.

## Create a Cloud Data Discovery policy

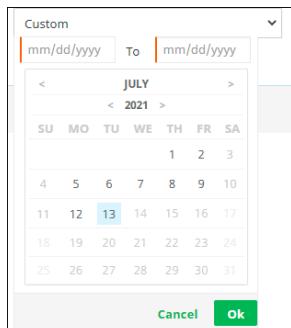
### Note

The cloud scan policy is a special type of API access policy, which can apply to only one cloud application.

1. Go to **Protect > API Access Policy** and click the **Cloud Data Discovery** tab.
2. Click **New**.
3. Enter a policy name and description.
4. Select a content inspection type – **None**, **DLP Scan**, or **Malware Scan**.  
If you select **Malware Scan**, click the toggle if you want to use an external service for scanning.
5. Under **Content Scanning**, select a data type.
  - If you selected **Malware Scan** as the content inspection type, the Data Type field does not appear. Skip this step.
  - For ServiceNow cloud applications, select **Structured Data** if you want to scan fields and records.
6. Perform either of the following steps, depending on the content inspection type you chose:
  - If you selected **DLP Scan**, select a content rule template.
  - If you selected **None** or **Malware Scan**, go to the next step to select a context type.
7. Under **Context Rules**, select a context type and context details.
8. Select exceptions (if any).
9. Select actions.
10. View the details of the new policy and confirm.

## Create a Cloud Data Discovery scan

1. Go to **Protect > Cloud Data Discovery** and click **New**.
2. Enter the following information for the scan.
  - **Scan Name and Description** -- Enter a **name** (required) and a **description** (optional).
  - **Cloud** -- Select the cloud application to which the scan should apply.  
If you select **Box**, see **Options for Box cloud applications**.
  - **Start Date** – Select the date on which the scan should start. Use the calendar to select a date or enter a date in **mm/dd/yy** format.
  - **Frequency** -- Select the frequency at which the scan should run: **Once**, **Weekly**, **Monthly**, or **Quarterly**.
  - **Scan type** – Select either:
    - **Incremental** – All data generated since the last scan.
    - **Full** – All data for the specified time period, including data in previous scans. Select a time period: **30 days** (default), **60 days**, **90 days**, **All**, or **Custom**. If you select **Custom**, enter a start and end date range, and click **OK**.



- **Defer Policy Action** – When this toggle is enabled, the CDD policy action is deferred, and the violating item is listed on the **Violation Management** page (**Protect > Violation Management > CDD Violation Management** tab). There, you can review the items listed and choose actions to take on all or selected files.
3. Save the scan. The scan is added to the list on the **Cloud Data Discovery** page.

### Options for Box cloud applications

If you selected **Box** as the cloud application for the scan:

1. Select a **Scan Source**, either **Automated** or **Report Based**.

For **Report Based**: --

- a. Select a **Scan Report Folder** from the widget and click **Save**.
- b. Select a **start date** from the calendar.

By default, the **Frequency** option is **Once**, and the **Scan Type** is **Full**. These options cannot be changed.

For **Automated** --

- a. Select a Time Period, Start Date, Frequency, and Scan Type as described in the previous steps.
  - b. Enable **Defer Policy Action** as described in the previous steps.
2. Save the scan.

For information about generating reports within the Box application, see **Generating Box Activity Reports**.

## Associate a scan with a Cloud Data Discovery policy

1. From the **Cloud Data Discovery** page, select a scan you created.
2. Click the **Policy** tab. The view in this tab lists the Cloud Data Discovery policies you have created.

POLICY NAME	PRIORITY	ACTIONS
Box_CAPS_Quar	1	

3. Click **Add**.
4. Select a policy from the dropdown list. The list includes only cloud applications that have a protection mode of **Cloud Data Discovery**.
5. Click **Save**.

#### Note

Only the policies associated with the cloud are included in the list.

You can reorder the list of Cloud Data Discovery policies by priority. To do so:

- Go to the **Cloud Data Discovery** page.
- Select a scan name by clicking the > arrow to the left of the scan name.
- In the list of policies, drag and drop the policies to the priority order you need. When released, the values in the **Priority** column will be updated. The changes will take effect after you click **Save**.

#### Notes

- You can reorder the list of cloud data discovery policies by priority for scans in the **Policy** tab, but not on the **Cloud Data Discovery** tab in the **API Access Policy** page (**Protect > API Access Policy > Cloud Data Discovery**).
- Before you can start running scans, you must change the scan status to **Active**.

## View scan details

You can view detailed values and charts that pertain to information from a scan.

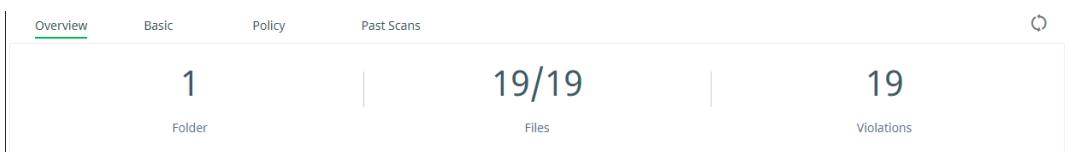
1. On the **Cloud Data Discovery** page, click the > arrow next to the scan for which you want to see details.
2. Click the tab for the type of detail you want to see.

### Overview tab

The **Overview** tab provides graphical detail for items found and policy violations.

The values along the top of the section show current totals and include:

- Folders found
- Files and data found
- Policy violations found



### Note

For ServiceNow cloud types, totals are also shown for structured data items. The line graphs show activity over time including:

- Items found and scanned
- Policy violations

You can select a time range for items to view – Last Hour, Last 4 hours, or Last 24 Hours.

**Since Beginning** will appear in the **Showing Range** list when a successful scan has been completed.

## Basic tab

The **Basic** tab displays the information you entered when you created the scan. You can edit this information.

The screenshot shows the Basic tab configuration form with the following fields:

Scan Name	Box_CAPS_QRScanP_24Mar
Description	(empty)
Select Cloud	Box_CAPS
Start Date	(empty)
Frequency	Once
Scan Type	<input type="radio"/> Incremental <input checked="" type="radio"/> Full
Defer Policy Action	<input type="checkbox"/>
<input type="button" value="Update"/> <input type="button" value="Cancel"/>	

## Policy tab

The **Policy** tab lists the Cloud Data Discovery policies associated with a scan. You can associate multiple policies with a scan.

Each listing shows the **Policy Name** and **Priority**. In addition, you can delete an associated policy by clicking the Delete icon in the **Actions** column.

The screenshot shows the Policy tab with the following data:

POLICY NAME	PRIORITY	ACTIONS
Box_CAPS_Quar	1	

Buttons at the bottom: **Save** and **Cancel**.

To add a Cloud Data Discovery policy to a scan, see [Associate a scan with a Cloud Data Discovery policy](#).

## Past Scans tab

The **Past Scans** tab lists the details of previous scans.

Overview	Basic	Policy	Past Scans
			1 total
SCAN JO... 595	SCAN JOB UUID 6f55fa2f_f3de_4fc8_8...	STARTED ON 03/23/2021 10:34:25 ...	FINISHED ON 03/23/2021 10:39:00 ...
		FOLDER... 1	FILES SC... 19
		VIOLATI... 19	NUMBER... 1
		STATUS Completed	COMPLIANCE STATUS 0%(0/19)

The following information is displayed for each scan:

- **Scan Job ID** – An identifying number assigned for the scan.
- **Scan Job UUID** – A universally unique identifier (128-bit number) for the scan.
- **Started on** – The date on which the scan was started.
- **Finished on** – The date on which the scan was finished. If the scan is in progress, this field is blank.
- **Folders Scanned** – The number of folders scanned.
- **Files Scanned** – The number of files scanned.
- **Violations** – The number of violations found in the scan.
- **Number of Policies** – The number of policies associated with the scan.
- **Status** – The status of the scan since it started.
- **Compliance Status** – How many policy violations were detected as a percentage of total items scanned.
- **Report** – An icon for downloading reports for the scan.

To refresh the list, click the **Refresh** icon above the list.



To filter the information, click the **Column Filter** icon, and check or uncheck the columns to view.



To download the list of past scans, click the **Download** icon above the list.



To generate a report for a scan, see the next section, [Generate a scan report](#).

## Generate a scan report

You can download a report of past scans in PDF format. The report provides the following information.

For generating Box activity reports, see [Generating activity reports for Box cloud applications](#).

- An **executive summary** that shows:
  - **Counts** of total policies enforced, files scanned, violations, and remediations.

- **Scope** -- name of cloud application, total number of items (for example, messages or folders) scanned, number of policies enforced, and the time frame for the scan.
- **Results** -- Number of scanned messages, files, folders, users, and user groups with violations.
- **Recommended remediations** -- Tips for managing and protecting sensitive content.
- **Report details**, including:
  - Top 10 policies based on violation counts
  - Top 10 files with violations
  - Top 10 users with violations
  - Top 10 groups with violations

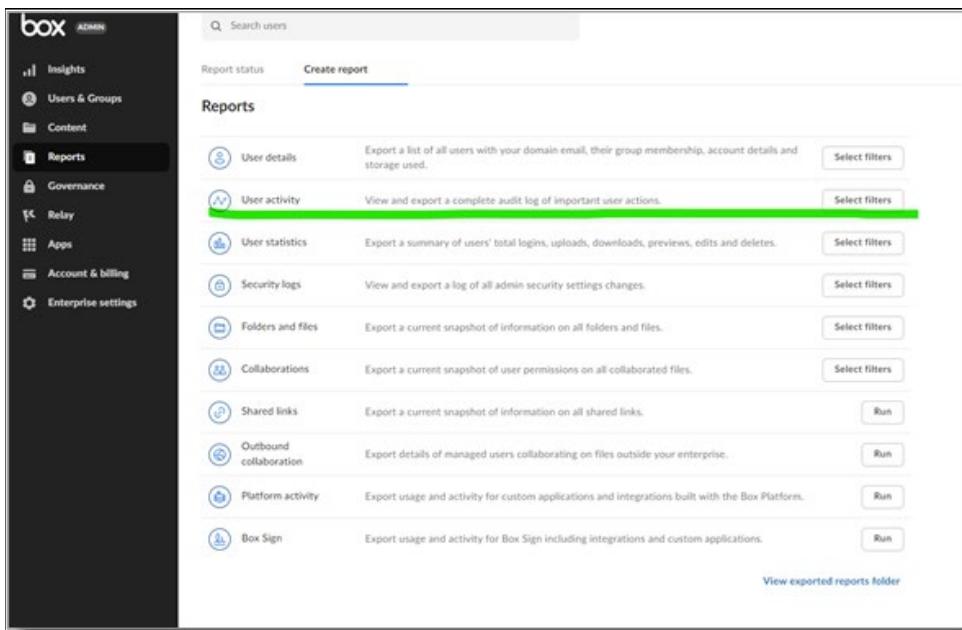
To download a report on a past scan:

1. From the **Cloud Data Discovery** page, display the details for the scan on which you want a report.
2. Click the **Past Scans** tab.
3. Click the **Report** download icon at the right.
4. Save the file for the report (as PDF).

## Generating activity reports for Box cloud applications.

This section provides instructions for generating CSV formatted activity reports within Box.

1. Log into the Box application with your administrator credentials.
2. On the Box admin console page, click **Reports**.



3. Click **Create Report**, then select **User Activity**.

User activity report

0 Filters Selected

**COLUMNS**

Configure the columns for your report. To run a report, you must select at least one column. To view a report inline, you must select all columns marked with an asterisk (\*).

<input checked="" type="checkbox"/> Date	<input checked="" type="checkbox"/> Username*	<input checked="" type="checkbox"/> User email	<input checked="" type="checkbox"/> IP address	<input checked="" type="checkbox"/> Action*
<input checked="" type="checkbox"/> Affected*	<input checked="" type="checkbox"/> Affected ID	<input checked="" type="checkbox"/> Size	<input checked="" type="checkbox"/> Parent folder	<input checked="" type="checkbox"/> Details*

**FILTERS**

Users or groups (optional) Enter user or group names

Start date January 31, 2022

End date February 14, 2022

Affected folders and files Select None selected

**ACTION TYPES**

4. On the **Reports** page, select the columns to include in the report.
5. Select a **start date** and an **end date** for the report.
6. Under **Action Types**, select **Collaboration** and select all of the action types under **COLLABORATION**.

**ACTION TYPES**

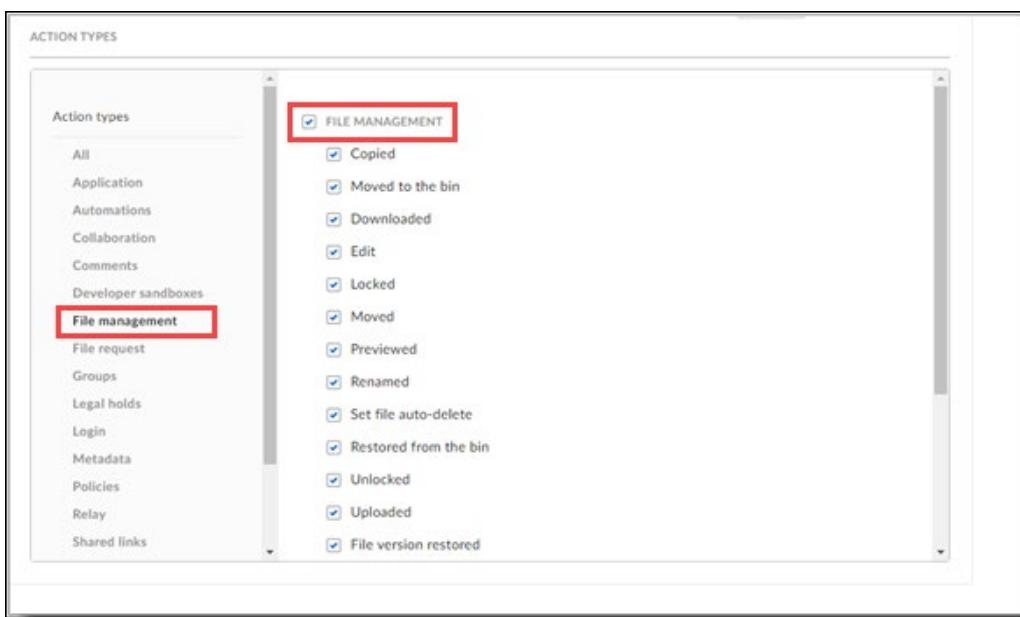
Action types

- All
- Application
- Automations
- Collaboration** (selected)
- Comments
- Developer sandboxes
- File management
- File request
- Groups
- Legal holds
- Login
- Metadata
- Policies
- Relay
- Shared links

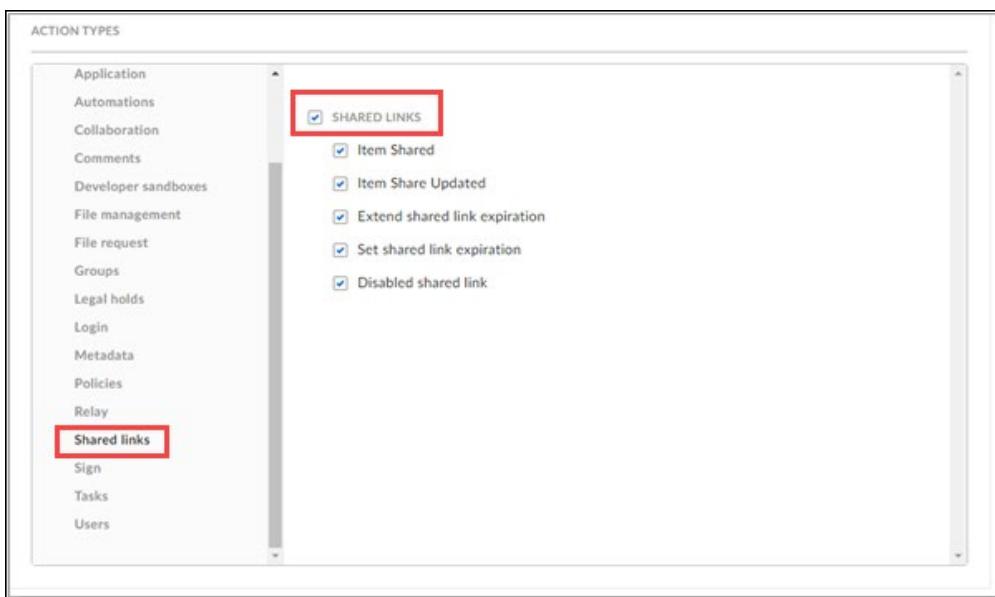
**COLLABORATION**

- Accepted invite
- Changed user or group role
- Extend collaborator expiration
- Removed collaborator
- Invited collaborator
- Rejected invite
- Collaboration expired
- Violated enterprise item transfer policy

7. Select **File Management** and select all of the action types under **FILE MANAGEMENT**.



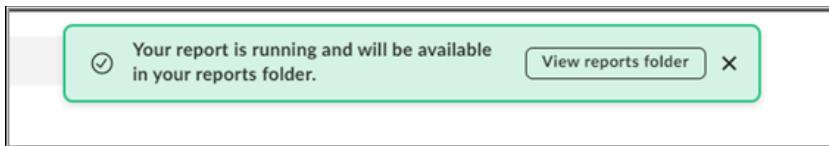
8. Select **Shared Links** and select all of the action types under **SHARED LINKS**.



9. Click **Run** at the top right to submit the report request.

The screenshot shows the 'Reports > User activity' page. At the top right are 'Run' and 'View' buttons. Below them, a message says '33 Filters Selected'. The 'COLUMNS' section lists several filter options with checkboxes: Date, Username\*, User email, IP address, Action\*; Affected\*, Affected ID, Size, Parent folder, Details\*. Under 'FILTERS', there's a section for 'Users or groups (optional)' with a text input 'Enter user or group names' and date pickers for 'Start date' (January 31, 2022) and 'End date' (February 14, 2022). A 'Select' button and a 'None selected' link are also present. The 'ACTION TYPES' section contains two columns of checkboxes. The left column includes Application, Automations, Collaboration, Comments, Developer sandboxes, File management, File request, Groups, Legal holds, Login, Metadata, Policies, and Relay. The right column under 'SHARED LINKS' includes Item Shared, Item Share Updated, Extend shared link expiration, Set shared link expiration, and Disabled shared link.

A popup message appears confirming the request.



When the report is finished running, you can view it in the folder under Box Reports.

All Files > Box Reports

Name

 User Activity run on 2022-02-14 23-37-59

 User Activity run on 2021-12-15 22-24-41

 User Activity run on 2021-11-23 02-21-32

 User Activity run on 2021-11-23 01-38-45

# Violation management and quarantine

Content that has violated a policy can be placed in quarantine for review and further action. You can view a list of documents that have been placed in quarantine. In addition, you can view a list of documents that have been reviewed by the administrator and what actions were selected for those documents.

To view information about files with violating content, go to **Protect > Violation Management**.

## Note

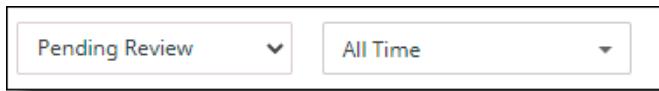
Quarantine actions do not apply to files and folders in Salesforce.

## Quarantine Management

Documents placed in quarantine are listed in the Quarantine Management page and are given a Pending Review status for evaluation before action is taken. Once reviewed, their status is changed to **Reviewed**, with the selected action taken.

### Selecting information to view

To view documents in either status, select a status from the dropdown list.



### Pending review

For each quarantined document that is pending review, the list shows the following items:

- **Policy Type** – The type of protection for the policy that applies to the document.
- **File name** – The name of the document.
- **Timestamp** – The date and time of violation.
- **User** – The name of the user associated with the violating content.
- **Email** – The email address of the user associated with the violating content.
- **Cloud** – The name of the cloud application where the quarantined document originated.
- **Violated Policy** – The name of the policy that was violated.
- **Action Status** – The actions that can be taken on the quarantined document.

Administrators and users can be notified when a document is placed in the **Quarantine** folder.

### Reviewed

For each quarantined document that has been reviewed, the list shows the following items:

- **Policy Type** – The type of policy to address violations.
- **File Name** – The name of the file containing violating content.
- **User** – The name of the user associated with the violating content.
- **Email** – The email address of the user associated with the violating content.
- **Cloud** – The cloud application where the violation occurred.

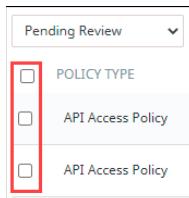
- **Violated Policy** – The name of the policy that was violated.
- **Actions** – The action selected for the violating content.
- **Action Status** – The outcome of the action.

## Taking action on a quarantined file

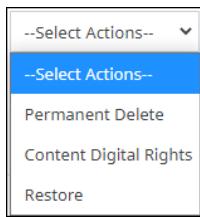
### To select an action on quarantined files in pending status:

Filter the list as needed by clicking the boxes in the left navigation bar and the time dropdown list.

Click the checkboxes for the file names on which to take action.



Select an action from the **Select Actions** dropdown list on the top right side.



- **Permanent Delete** – Deletes the file from the user's account. *Select this option with care*, because once a file is deleted, *it cannot be recovered*. Apply this option for serious violations of company policy in which users can no longer upload the sensitive content.
- **Content Digital Rights** – Applies any actions specified for Content Digital Rights in the policy – for example, adding a watermark, redacting violating content, or encrypting the document.

#### Note

When you select multiple quarantined records on which to apply actions, the **Content Digital Rights** option is not available in the Select Actions list. This is because among the records you selected, only some of them might have been configured for a Content Digital Rights policy action. The **Content Digital Rights** action can be applied only to a single quarantined record.

- **Restore** – Makes a quarantined file available to users again. Apply this option if a review determines that a policy violation did not occur.

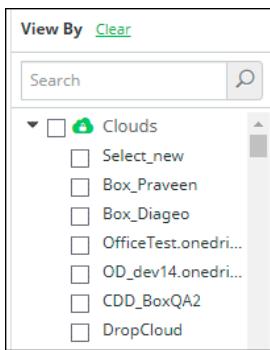
Click **Apply** for the selected action.



## Viewing and searching for quarantined documents

You can filter the view of existing quarantine actions using these options:

- In the settings at the left, check or uncheck how you would like to organize the list of quarantine actions. Click **Clear** to clear all filters.



- At the top of the screen, select a time period from the dropdown list.



To search for a quarantined document, use only **prefix match query** to search the results. For example, to find the file **BOX-CCSecure\_File29.txt**, search by prefix on word search split at special characters. This means you can search by the prefix words—"BOX", "CC", and by "File." The related records are displayed.

## Selecting information to display and review

To filter the view, select the cloud applications from the left navigation bar and the time range from the dropdown menu above the list.

Select the messages you want to review by clicking the checkbox next to each message.

**Note** Sorting is disabled for the **Cloud**, **Subject**, **Recipient** and **File Size** columns.

## CDD Violation Management

The **CDD Violation Management** list shows content violations for Cloud Data Discovery (CDD) policies.

For each file, the list shows the following information:

- Timestamp** – The date and time of the violation.
- Cloud Application** – The name of the cloud application where the violation occurred.
- Email** – The valid email address of the user associated with the violation.
- Action Status** – The completion status for the policy action.
- Policy Action** – The action specified in the policy that was violated.
- Policy Name** – The name of the policy that was violated.

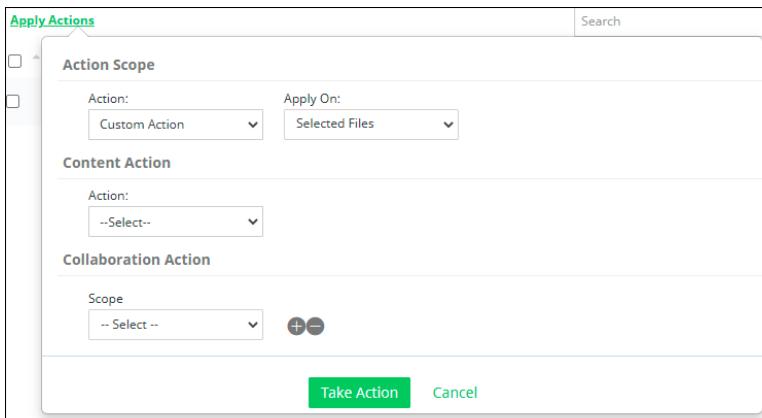
- **File Name** – the name of the file with the violating content.
- **URL** – The URL of the violating content.

## Selecting information to view

From the left panel, choose the items to view – **User Groups**, **Violations**, **Users**, and **Status**.

## Taking action on a quarantined CDD item

1. Click **Apply Actions**.



2. Under **Action Scope**, select an Action -- either **Policy Action** or **Custom Action**.

- **Policy Action** applies the action(s) specified in the policy. Select either **All Files** to apply the policy action to all of the files listed, or **Selected Files** to apply the policy action only to the files you specify.
- **Custom Action** allows you to choose content and collaboration actions to apply to the files.
- **Content action** – Select **Permanent Delete** or **Content Digital Rights**. For **Content Digital Rights**, select a CDR template for the action.
- **Collaboration action** – Select **Internal**, **External**, or **Public**.
  - For **Internal**, choose **Remove Collaborator** and select the user groups to include in the action.
  - For **External**, choose **Remove Collaborator** and enter the domains to blocked.
  - For **Public**, choose **Remove Public Link**.
  - To add another collaboration action, click the + icon at the right and select the appropriate actions.

3. Click **Take Action**.

# Monitoring and managing system activity

---

The following topics outline how you can monitor cloud activity through dashboards, charts, and activity audit logs, monitor user risk information, manage devices, and work with files in quarantine.

- Viewing activity from the Home Dashboard
- Monitoring cloud activity from charts
- Working with activity audit logs
- Monitoring user activity from audit logs
- Viewing and updating user risk information

## Viewing user and system activity from the Home Dashboard

From the **Home Dashboard** in hosted deployments, you can view graphical representations of cloud and user activity in your organization.

The **Home Dashboard** organizes data into these major components:

- **Data cards** showing totals and trending charts for events
- The **total number of events** that are possible threats to your data security (by cloud and by type)
- A more detailed **list of events**. Threats include violations and anomalous activity.

The following sections describe these components.

### Data cards

Data cards contain snippets of important information that administrators can view on an ongoing basis. The numbers and trending charts in the data cards are based on the time filter that you select. When you modify the time filter, the totals shown in the data cards, and the trending increments, change accordingly.

The data cards display these types of information for the cloud applications and time ranges you specify. You can see activity counts for a specific time range by hovering over the date ranges at the bottom of the data card.

The following sections describe each data card.

### Content Scanning

The **Content Scanning** data card shows the following information.

- **Files and Objects** -- The number of files (unstructured data) and objects (structured data) that have been scanned to detect policy violations. For Salesforce (SFDC), this number includes Customer Relationship Management (CRM) objects. When customers onboard cloud applications, CASB scans content and user activity on the cloud applications. Based on the activities performed and the policies set for your enterprise, CASB generates analytics and displays them on the data cards.
- **Violations** -- The number of violations detected by the policy engine.
- **Protected** -- The number of files or objects protected through quarantine, permanent delete, or encryption actions. These remediation actions remove content from users (permanently through delete; temporarily through quarantine) or restrict the ability of content to be read by unauthorized

users (encryption). These analytics provide a view (over time) of how many protective actions have been performed in response to violations that the policy engine has detected.

## Content Sharing

The Content Sharing data card shows the following information.

- **Public Links** -- The total number of public links found across file storage cloud applications. A **public link** is any link that the general public can access without requiring a login. Public links are easy to share and are not secure. If they link to content that contains sensitive information (for example, references to credit card numbers), that information could be exposed to unauthorized users, and could compromise the privacy and security of that data.
- The **Remove Public Link** option provides you with the flexibility of enabling information sharing but also allows you to protect specific types of content. When you create a policy, you can specify public link removal if a public link is included in a file with sensitive content. You can also specify removal of public links from folders that contain sensitive information.
- **External Sharing** -- The number of activities in which content is shared with one or more users outside the organization's firewall (external collaborators). If a policy allows external sharing, a user can share content (for example, a file) with another user who is external. Once content is shared, the user with whom it is shared can continue accessing the content until that user's access is removed.
- **Protected** -- The total number of events for which the public link or an external collaborator was removed. An **external collaborator** is a user outside the organization's firewall with whom content is shared. When an external collaborator is removed, that user can no longer access the content that was shared.

## Most Hit Security Policies

The Most Hit Security Policies card shows a table that lists the top 10 policy hits for each policy. The table lists the policy name and type and the number and percentage of hits for the policy.

### Policies

The Policies card shows in a circle graph the total number of active policies and the count of active and all policies by policy type.

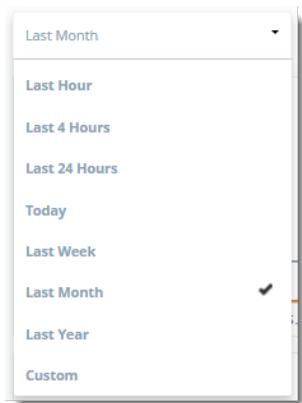
## Event details

Event details provide a table view of all threats for the time filter you specify. The total number of events listed matches the total number shown in the graph at the right.

ACCOUNT NAME	ACTIVITY TYPE	ACTION TYPE	VIOLATION TYPE	APP NAME	EVENT ORIGIN
O365_dev12.sharepoi...	ContentCreate			sharepoint	api
O365_dev12.sharepoi...	ContentCreate			sharepoint	api
O365_dev12.sharepoi...	ContentCreate			sharepoint	api
O365_dev12.sharepoi...	ContentCreate			sharepoint	api
O365_dev12.sharepoi...	ContentDelete			sharepoint	api

You can filter data using the following options.

### By time range



From the dropdown list, choose the time range to include on the **Home** page view. The default time range is **Month**. When you select a time range, the totals and trending increments change.

You can also specify a custom date. To do so, choose **Custom**, click in the first box at the top of the Custom view, then click the preferred **From** and **To** dates from the calendar.

### Viewing additional details

You can display additional details from the data cards, the threat graph, or the table view.

#### From a data card

**For a specific date:** Hover over the date along the bottom of the card for which you want details.

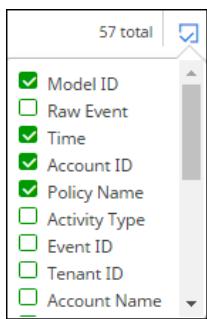
**For the data counts in a card:** Click on the data count for which you want additional details.

The details are displayed in the table view.

#### From the table

Click the **Detailed Analysis** link. All activities from the **Home Dashboard** page are listed in a table on the **Activity Audit Logs** page. From here, you can drill down further by clicking on the bars.

To display more or fewer columns in the table, click the box icon at the right, and select or deselect columns in the list. The field names available for selection depend on the filtering options you have selected. You can display no more than 20 columns in the table.



## Refreshing all data

Click the **Refresh** icon at the upper right corner of the Home Dashboard to update the data for all items on the page.



## Exporting data

You can save a printout of the information on the Home Dashboard.

1. Click the **Export All** icon at the upper right corner of the page.



2. Select a printer.
3. Print the page.

## Monitoring cloud activity from charts

The **Activity Dashboard** page from the **Monitor** tab of the Management Console is the point from which you can view specific types of activity in your enterprise. This activity reflects the results of both real-time and historical data scans.

From the **Monitor** page, you can view the following dashboards:

- Application Activities
- Anomalous Activities
- Office 365
- IaaS Monitoring Dashboard
- Activity Alerts
- Zero Trust Enterprise Access

You can display dashboard views in a variety of ways. You can select all cloud applications for higher-level overviews of your cloud data activity, or you can select specific cloud applications or only one cloud for more detailed information. To view activity for a specific time, you can select a time range.

You can go to the following pages by clicking the menu items.

The following sections describe these dashboards.

## Application Activities

The **Application Activities** dashboard provides the following views.

### Policy Analytics

**Policy Analytics** provides perspectives on the type, quantity, and source of policy triggers in your organization. For example, you can see the total number of policy violations over a specific time (such as a month), as well as a breakdown of violations by cloud, by user, or by policy type (such as external collaborator violations).

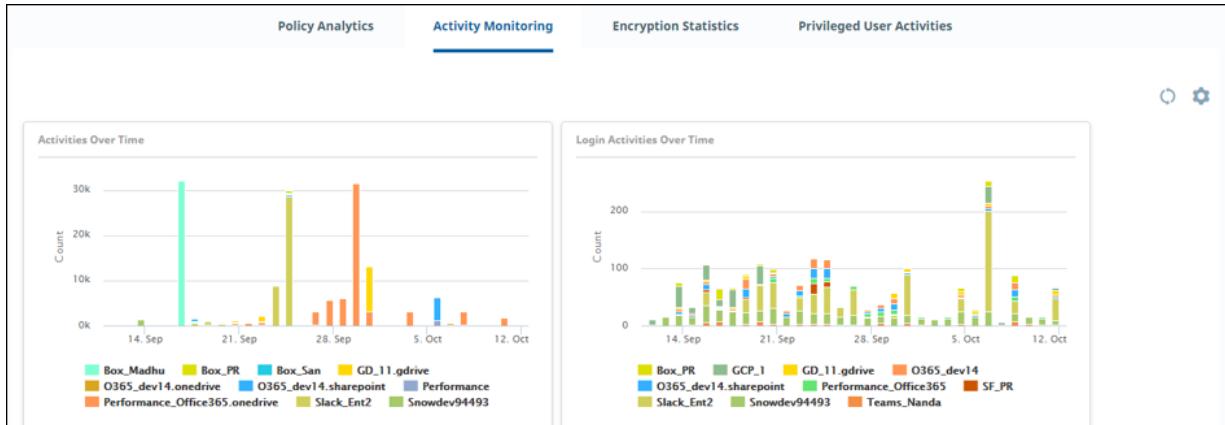
For descriptions, see [Policy Analytics](#).



## Activity Monitoring

**Activity Monitoring** shows quantified views of activities in your organization – for example, by activity type (such as logins and downloads), by time, or by user.

For descriptions, see [Activity Monitoring](#).



## Encryption Statistics

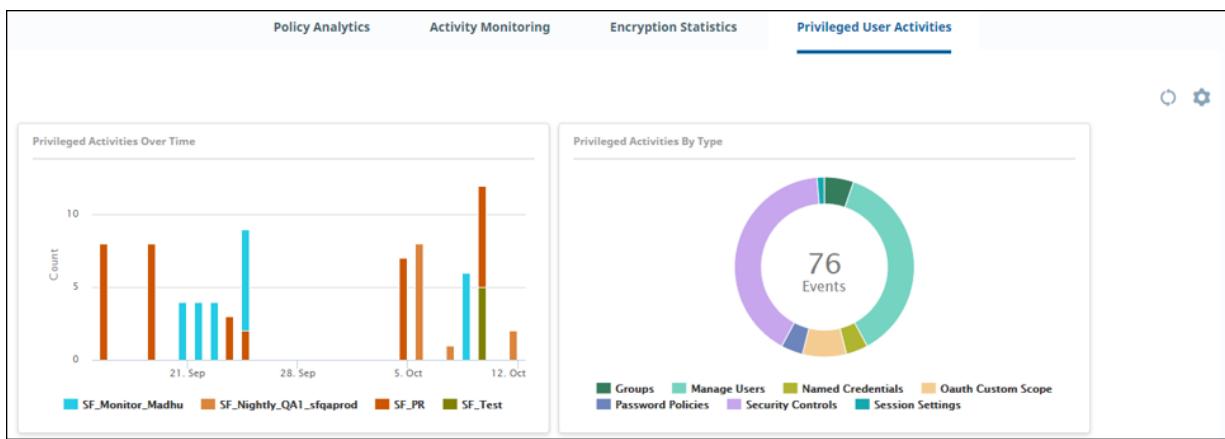
Encryption Statistics shows how encrypted files are being accessed and used in your organization. For example, you can view the highest number of users who have encrypted or decrypted files, how many encryption and decryption activities have taken place over time, or the types of files that have been encrypted.

For descriptions, see [Encryption Statistics](#).

## Privileged User Activities

**Privileged User Activities** shows activities performed by users with higher-level access permissions in an organization. These users are typically administrators and are sometimes referred to as "super users." Users at this level can view the number of accounts created or frozen by an administrator, or how many session settings or password policies were changed. Being aware of privileged user activity is important because these users have permissions under which they can modify settings that could compromise a cloud's security. The information from these dashboards allows the security team to monitor the actions of these users, and act quickly to address threats.

For descriptions, see [Privileged User Activities](#).



## Anomalous Activities

The Anomalous Activities detection engine continuously profiles data attributes and user behavior to detect activity that is out of the ordinary for your enterprise. Monitoring includes the locations from where logins take place (geo-logins), source IP addresses, and devices used. User behavior includes activities such as content uploads and downloads, edits, deletes, logins, and logouts.

Anomalies are not actual policy violations but can serve as alerts for possible data security threats and malicious data access. Examples of anomalies might be an abnormally large number of downloads from an individual user, a higher-than-normal number of logins from the same user, or persistent login attempts by an unauthorized user.

The user profile includes sizes of file downloads across cloud applications, as well as the time of the day and day of the weeks that the user is active. When the engine detects a deviation from the observed behavior over this period, it flags the activity as anomalous.

Anomalies are classified into two types: deterministic and statistical.

- *Deterministic* detection works in real time and detects anomalies as user activity occurs, with a nominal delay (for example, 10 to 30 seconds). The algorithm profiles entities (such as users, devices, applications, content, user locations, and data destination location), attributes (such as access location, source IP address, device used), and the relation between them.
- When an unknown or unexpected new relation is encountered, it is evaluated for suspicious activity. The sample of user activities profiled in this approach is relatively small and grows over time. The accuracy of the anomalies detected using this method is high, although the number of rules or the search space is limited.
- *Statistical* detection creates a user's baseline with a larger activity sample, typically spanning over a 30-day period to reduce false positives. User activity is profiled using a three-dimensional model: the metric observed (location, access count, file size), time of the day, and day of the week. The metrics are grouped by time and day. Activities profiled includes:
  - Content downloads
  - Content access -- uploads, edits, deletes
  - Network access -- logins and logouts

When the engine detects a deviation from the observed behavior over this period, based on clustering techniques, it flags the activity as anomalous. It detects anomalies in non-real time with a delay of typically one hour.

The deterministic algorithm is used for geoanomaly detection. The statistical algorithm is used for anomalous downloads and for content and network access.

To view anomalous activities, go to **Monitor > Anomalous Activities**.

For more details about viewing anomaly reports, see:

- [Anomalous activities by geolocation](#)
- [Displaying geoanomaly details from the Activity Audit Logs page](#)
- [Anomalous downloads, content access, and authentication](#)
- [Three-dimensional activity views](#)

## Anomalous activities by geolocation

The **Anomalous Activities by Geolocation** dashboard is a map view showing geographic pointers where anomalous activity has likely taken place. This type of anomaly is called a **geoanomaly**. If geoanomalies have been detected, the map shows one or more geographic pointers identifying where the activity in question took place.

When you click on a pointer, you can display details about the user's current and previous activities, including their email address, the cloud they accessed, their location, and the activity time. Using the current and previous activity details, you can make comparisons that provide insight into the anomaly. For example, the user might have logged in to two different cloud applications using the same sign-on credentials, from two different locations. The blue pointer represents the location with the current focus. To focus on the other location, click its pointer.

If there are multiple instances of anomalous activity from a geographical area, multiple pointers appear, slightly overlapped. To display information on one of the pointers, hover over the area with the overlapping pointers. In the small box that appears, click the pointer for which you want to view details.

## Displaying geoanomaly details from the Activity Audit Logs page

From the **Activity Audit Logs** page (**Monitor > Activity Audit Logs**), you can select geoanomaly views by clicking the Binocular icon that appears at the left in the activity list.

## Anomalous downloads, content access, and authentication

The following dashboard charts provide information about anomalous activity across cloud applications.

- The **Anomalous Downloads by Size** chart shows a summary count of downloads over time by size of downloaded files.
- Data hijacking in enterprises is often indicated by an abnormally high number of downloads of business-critical data. For example, when an employee leaves an organization, their activity might reveal that they downloaded a large amount of corporate data just before their departure. This chart tells you the number of times an anomalous pattern is found in user downloads, the users who did the downloading, and when the downloads occurred.
- The **Anomalous Content Delete** chart shows the number of delete events for anomalous activity.
- The **Anomalous Authentication** chart shows the number of times an anomalous pattern is found in a user's network access events, including logins, failed or brute-force login attempts, and logouts. Repeated unsuccessful logins could indicate a malicious attempt to gain access to the network.
- The **Anomalous Downloads by Count** chart shows the number of anomalous downloads for your enterprise.

## Three-dimensional activity views

You can also view a three-dimensional chart from which you can observe anomalous activity in relation to normal activity. In this view, activities are represented as data points (also called buckets) on three axes:

- X=hour of day
- Y=aggregated activity count or aggregated download size
- Z=day of the week

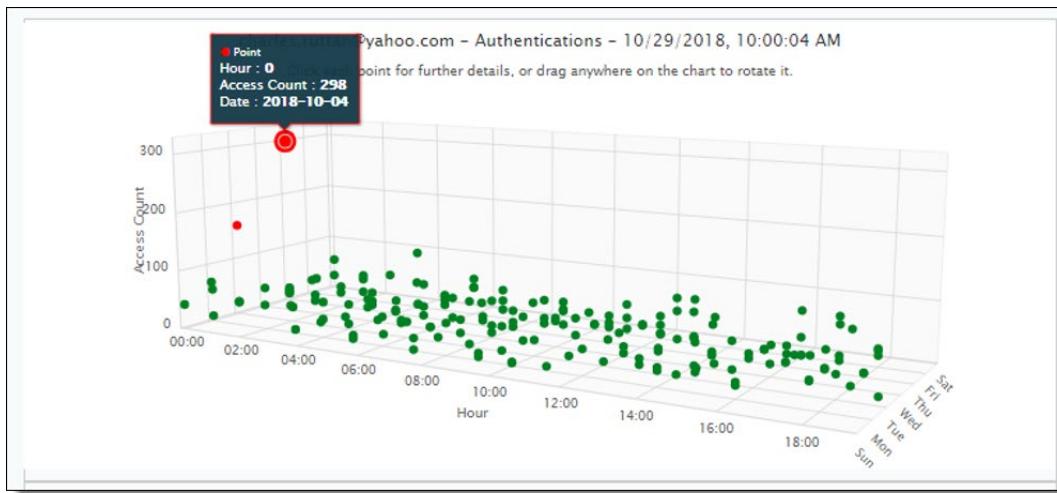
The chart uses a clustering mechanism to illustrate activity patterns and reveal anomalies. These activity clusters can give you a better idea of what types of events are occurring most frequently at specific days and times. The clusters also enable anomalies to stand out visually.

As activities are tracked hour by hour, data points are added to the chart. Clusters are created when relevant activities total at least 15 data points. Each cluster is represented by a different color for its data points. If a cluster has fewer than three data points (buckets), the events represented by those points are considered anomalous, and they appear in red.

Each data point on the chart represents events that occurred on a specific hour of the day. You can get details about the date, the hour, and event count by clicking on any data point.

In this example, the cluster at the lower right has 15 data points. It shows that several events took place during late afternoon and evening throughout the week. The access count was similar for all activities. On one day, the access count was much higher, and the point is shown in red, indicating an anomaly.

The table below the graph lists the events represented in the graph. The list in this example outlines the date and time of the access, the name of the file accessed, the cloud from which the access took place, and the email address of the user who accessed the content.



## Settings for configuring anomaly information

From the **System Settings** page, you can configure how to track, monitor, and communicate information about anomalous activities. For Box cloud applications, you can suppress (allowlist) connected apps included in the cloud account to prevent geoanomalies.

## Adaptive threshold for permitted user activity rates (Preview feature)

The **adaptive threshold** defines a permitted rate of user activity. The configured threshold can be adjusted based on the user activity rate. Being able to configure a threshold enables you to adjust the rate of user activities as needed. If conditions permit, for example, the threshold can be modified to allow a higher rate of activity.

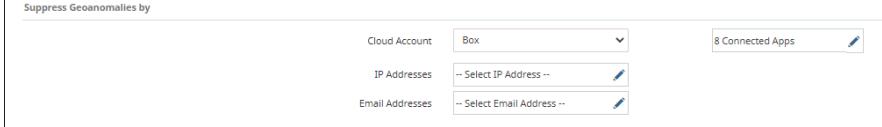
Adaptive threshold configuration evaluates threshold compliance and will allow events up to the defined threshold. CASB also checks the probability of event occurrences after the fixed threshold. If the probability is within the allowed range, the events are allowed. The default value for the variance percentage from peak probability is 50%.

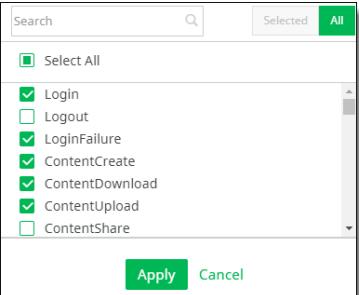
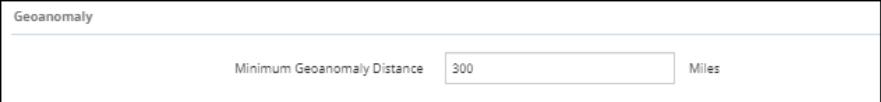
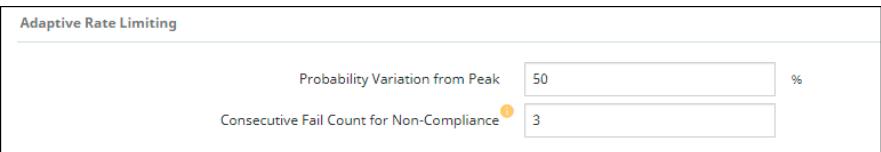
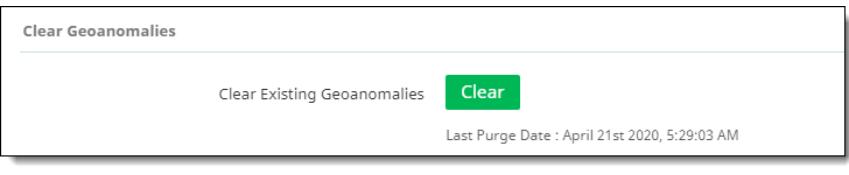
You can also set a consecutive failure count (for example, three failures in a row). When the number of consecutive failures exceeds the specified count, the events are considered non-compliant. The default count is three (3) consecutive failures. It can be adjusted up to 20 or down to 1.

You can choose adaptive threshold as a context type in a policy, where these settings will be applied.

## Tracking of anomaly information

1. Go to **Administration > System Settings > Anomaly Configuration**.
2. Select settings as follows:

Section/Field	Description
<b>Suppress Geoanomalies by</b>	<p>a. Click the field to the right of the Cloud Account field.</p> <p>b. Select <b>Connected Apps</b>.</p>  <p>c. From the <b>Directories</b> list, click the folders for the apps to suppress.</p> <p>d. Click the right arrow to move them to the <b>Connected Apps</b> column.</p> <p>e. Enter the IP Addresses and Email Addresses for which to suppress anomaly information. In each field, separate multiple IP and email addresses with commas.</p>

Section/Field	Description
<b>Activities for Geoanomaly</b>	<p>Search for the activities to track for geoanomalies, select the activities, and click <b>Apply</b>.</p>  <p><b>Note</b></p> <p>For anomalies to be triggered for Microsoft 365 and AWS, you must check <b>O365Audit</b> and <b>AWSAudit</b> from the list.</p>
<b>Geoanomaly</b>	<p>For <b>Minimum Geoanomaly Distance</b>, enter the minimum number of miles for which to track geoanomalies, or accept the default of 300 miles.</p> 
<b>Adaptive Rate Limiting (Preview)</b>	<p>Enter or select the following options that will apply to the tenant:</p> <ul style="list-style-type: none"> <li><b>Probability Variation from Peak</b>, as a percentage (default is 50%)</li> <li><b>Consecutive Failure Rate for Non-Compliance</b> (default count is 3)</li> </ul> 
<b>Clear Geoanomalies</b>	<p>Click <b>Clear</b> to clear previously reported geoanomaly information. After you click <b>Clear</b>, the date and time at which the geoanomalies were last purged appears below the <b>Clear</b> button.</p> 

3. Click **Save**.

## Settings for anomaly profiles (dynamic anomaly configuration)

Dynamic anomaly configurations include profiles for defining behavior that is considered anomalous. These profiles are based on activity category and activity types. Each profile is either predefined (provided for all tenants; cannot be modified or deleted by administrators) or user defined (can be created, modified, or deleted by administrators).

You can create up to four user-defined anomaly profiles. Each profile defines anomalous behavior for an activity category (for example, authentications or content updates), and activities associated with that category (for example, login, content download, or content delete).

NAME	DESCRIPTION	ACTIVITY CATEGORY	TYPE	CREATED DATE	LAST MODIFIED BY	LAST MODIFIED TIME	AC
Anomalous Activities by Geolocation	Chart shows anomalous activity details based on the time and distance	Login	Predefined	05/27/2022 12:13:05 AM	system	05/27/2022 12:13:05 AM	
Anomalous Authentications	Chart shows a summary count of anomalous users over time by count of logins	Login	Predefined	05/27/2022 12:13:05 AM	system	05/27/2022 12:13:05 AM	
Anomalous Content Delete	Chart shows a summary count of anomalous users over time by count of delete activities.	ContentDelete	Predefined	05/27/2022 12:13:05 AM	system	05/27/2022 12:13:05 AM	
Anomalous Downloads by Count	Chart shows a summary count of anomalous users over time by count of downloaded files.	ContentDownload	Predefined	05/27/2022 12:13:05 AM	system	05/27/2022 12:13:05 AM	
Anomalous Downloads by Size	Chart shows a summary count of anomalous users over time by size of downloaded files.	ContentDownload	Predefined	05/27/2022 12:13:05 AM	system	05/27/2022 12:13:05 AM	

The **Anomaly Profiles** page shows:

- The profile Name and Description**
- The Activity Category** (for example, **ContentUpdate**)
- Type** – either **Predefined** (system-generated, cannot be edited or deleted) or **User-Defined** (can be created, edited, and deleted by administrators).
- Created Date** – the date on which the profile was created.
- Last Modified By** – the username of the person who last modified the profile (for user-defined profiles) or system (for predefined profiles).
- Last Modified Time** – the date and time on which the profile was last modified.
- Actions** – an Edit icon for displaying profile details and modifying user-defined profiles.

You can filter the column display or download the list of profiles to a CSV file using the icons at the upper right above the list.

- To show or hide columns, click the Column Filter icon, and check or uncheck column headings.
- To download the listed profiles, click the Download icon and save the CSV file to your computer.

The following procedures outline the steps for adding, modifying, and deleting user-defined anomaly profiles.

### Note

You can have no more than four user-defined profiles. If you currently have four or more user-defined profiles, the **New** button appears dimmed. You must delete profiles to bring the number down to fewer than four before you can add new profiles.

#### To add a new user-defined anomaly profile:

1. Go to **Administration > System Settings**, select **Anomaly Profiles**, and click **New**.

The screenshot shows a 'Profile Details' dialog box. It has four input fields: 'Name' (empty), 'Description' (empty), 'Activity Category' (dropdown menu showing '-- Select --'), and 'Activities' (dropdown menu showing '-- Select --'). At the bottom are 'Save' and 'Cancel' buttons.

2. For Profile Details, enter the following information:

- **Name** (required) and **Description** (optional).
- **Activity Category** – Select a category for defining activities in the profile.

The screenshot shows a dropdown menu for 'Activity Category'. It lists three items: 'Content Upload', 'Content Update', and 'Content Sharing'. 'Content Upload' is highlighted.

- **Activities** – Check one or more activities for the selected category. The activities you see in the list are based on the activity category you selected. The following activity types are available.

Activity Category	Activities
<b>Content Upload</b>	Content Upload Content Create
<b>Content Update</b>	Content Edit Content Rename Content Restore Content Move Content Copy

Activity Category	Activities
<b>Content Sharing</b>	Collaboration Add Collaboration Invite Content Share Collaboration Update

3. Click **Save**.

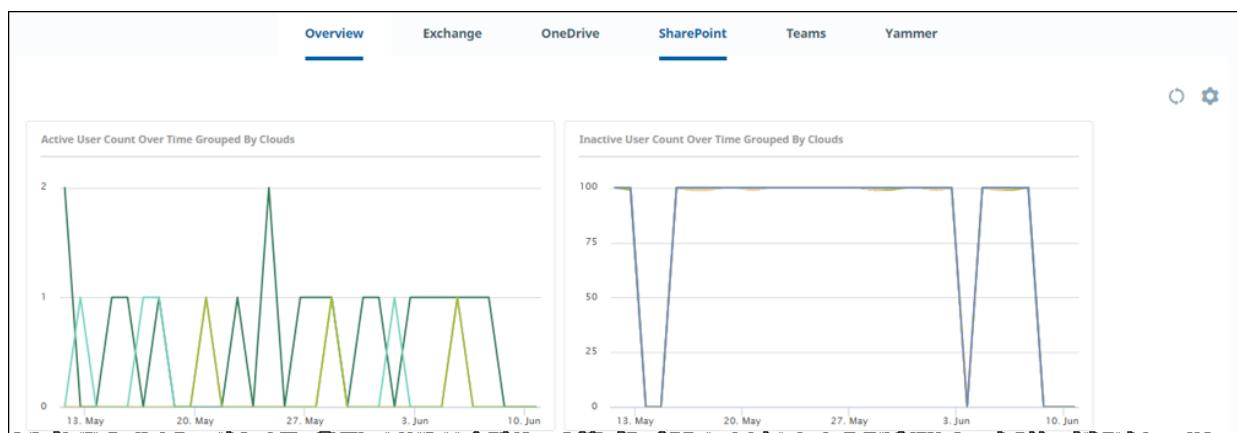
**To modify a user-defined profile:**

1. Select a user-defined profile and click the pencil icon at the right.
2. Make the needed modifications and click **Save**.

**To delete a user-defined profile:**

1. Select a user-defined profile and click the **Trash Can** icon at the upper right above the list.
2. When prompted, confirm the deletion.

## Office 365



The **Office 365** dashboard provides information about activities for the applications in the Microsoft 365 suite. Charts are shown only for the applications you onboarded.

The **Overview** charts summarize user activity information for your onboarded applications. The application charts show user activity for that application.

For chart details, see [Office 365 dashboards](#).

## AWS Monitoring

The **AWS Monitoring** dashboard provides information about user activity by location, time, and number of users.

For chart details, see [AWS Monitoring charts](#).

## Customizing and refreshing a dashboard display

You can move charts around on a dashboard, select which charts appear, and refresh the display for one or all charts.

### To move a chart in a dashboard:

- Hover over the title of the chart you want to move. Click and drag it to the desired position.

### To refresh the display for a chart:

- Hover over the upper right corner of the chart and click the **Refresh** icon.



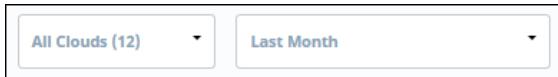
### To refresh the display for all charts on the page:

- Click the **Refresh** icon in the upper right corner of the page.



### To select what data appears in a dashboard:

- In the upper left corner of the page, select the cloud applications and the time range to include.



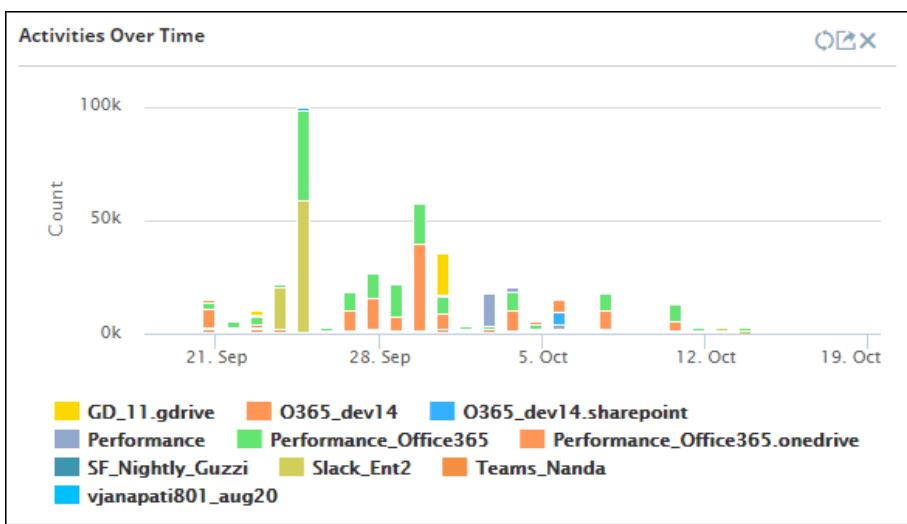
## Exporting data for reporting

You can export the information you need from any chart.

- Select the tab that has the chart whose data you want to export (for example, **Monitor > Activities Dashboard > Policy Analytics**).



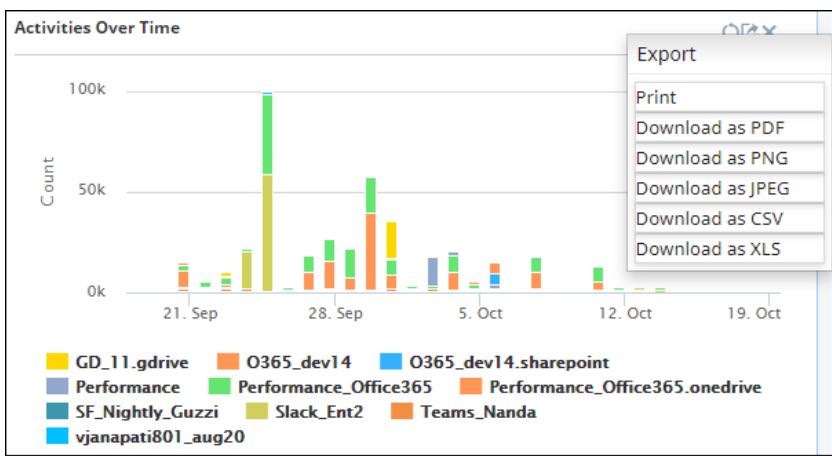
- Select the chart whose data you want.



3. To exclude any items from the export (for example, users), click the items in the legend to hide them. (To show them again, click the items once more.)
4. Hover over the top of the chart, click the **Export** icon in the upper right corner.



Then, select an export format from the list.



5. Save the file.

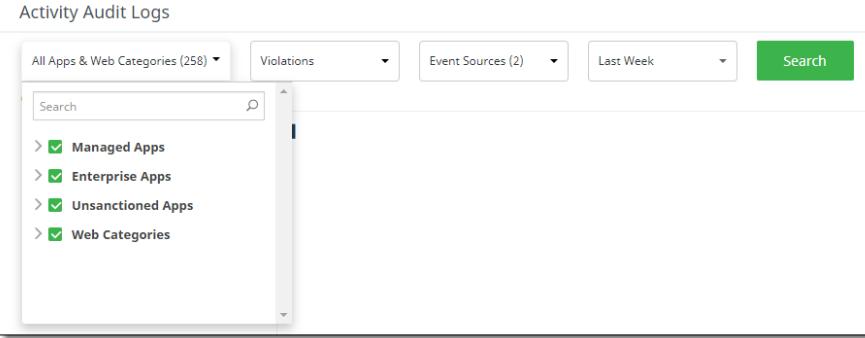
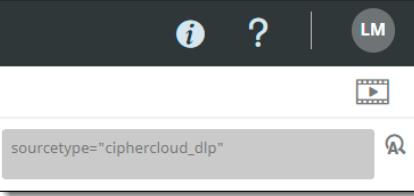
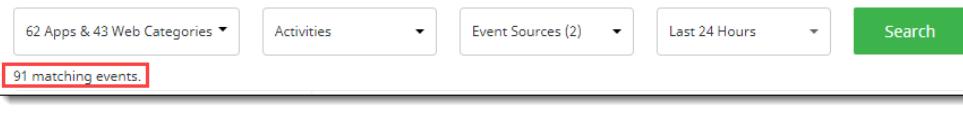
## Printing a report or chart

1. Click the **Export** icon in the upper right corner of the chart whose data you want to print, and select **Print**.
2. Select a printer and print the report.

## Working with activity audit logs

The **Activity Audit Logs** page (**Monitor > Activity Audit Logs**) displays detailed views of data you select from charts, or items you search for. Through this page, you can use the filtering options in the navigation bar to focus on specific users and activities to provide an audit trail or detect patterns of use.

The page shows these items.

<p>Search options:</p> <ul style="list-style-type: none"> <li>▪ <b>Cloud applications</b> (managed, enterprise, and unsanctioned) and web categories</li> <li>▪ <b>Event types</b> (for example, activities, policy violations)</li> <li>▪ <b>Event sources</b> (for example, API)</li> <li>▪ <b>Time range options</b> (for example, last 34 hours, last week, last month)</li> </ul>	
<p>Search query string.</p>	
<p>The total number of events found from the search.</p>	 <p>91 matching events.</p>

<p>Navigation bar from which you can filter your search further by choosing users, user groups, activity types, content types, and policy names on which to search. These filters can be helpful when you need to keep an audit trail on specific users or activities. The search results show the most recent 10,000 records from the selected filter items.</p>	<p>1.3K matching events.</p> <p>Search <input type="text"/> <input type="button" value="Reset"/></p> <p><input type="checkbox"/>  Users <input type="text"/> Search Name <input type="button" value=""/></p> <p><input checked="" type="checkbox"/>  Activity Type <input type="checkbox"/> ContentCreate (4) <input type="checkbox"/> Login (2)</p> <p><input checked="" type="checkbox"/>  Content Type <input type="checkbox"/> MESSAGE (4)</p>																										
	<p>Bar graph display of event data, showing counts for all events found (in addition to the most recent 10,000 records).</p> <table border="1"><thead><tr><th>Time</th><th>Event Count</th></tr></thead><tbody><tr><td>00:00 am</td><td>~80</td></tr><tr><td>01:00 am</td><td>~180</td></tr><tr><td>02:00 am</td><td>~20</td></tr><tr><td>03:00 am</td><td>~220</td></tr><tr><td>04:00 am</td><td>~20</td></tr><tr><td>05:00 am</td><td>~20</td></tr><tr><td>06:00 am</td><td>~10</td></tr><tr><td>07:00 am</td><td>~10</td></tr><tr><td>08:00 am</td><td>~10</td></tr><tr><td>09:00 am</td><td>~10</td></tr><tr><td>10:00 am</td><td>~10</td></tr><tr><td>11:00 am</td><td>~120</td></tr></tbody></table>	Time	Event Count	00:00 am	~80	01:00 am	~180	02:00 am	~20	03:00 am	~220	04:00 am	~20	05:00 am	~20	06:00 am	~10	07:00 am	~10	08:00 am	~10	09:00 am	~10	10:00 am	~10	11:00 am	~120
Time	Event Count																										
00:00 am	~80																										
01:00 am	~180																										
02:00 am	~20																										
03:00 am	~220																										
04:00 am	~20																										
05:00 am	~20																										
06:00 am	~10																										
07:00 am	~10																										
08:00 am	~10																										
09:00 am	~10																										
10:00 am	~10																										
11:00 am	~120																										

<p>Table of event data, showing the newest 500 records. The data is sorted in descending order by time.</p> <p>For additional data, you can export the contents to a CSV file. The export includes the results of the currently selected filters.</p> <p><b>Note</b></p> <p>For ServiceNow cloud applications, the <b>Activity Audit Logs</b> page does not show source details (IP, city, country, country code, IP, origination, source state, or user type) for content download activity.</p>	<table border="1"> <thead> <tr> <th>ACCOUNT NAME</th><th>ACTIVITY TYPE</th><th>ACTION TYPE</th><th>VIOLATION TYPE</th><th>APP NAME</th><th>EVENT ORIGIN</th></tr> </thead> <tbody> <tr> <td>Box_CAPS</td><td>ContentCreate</td><td>Encrypt</td><td>DLP</td><td>box</td><td>api</td></tr> <tr> <td>Box_CAPS</td><td>ContentCreate</td><td>Encrypt</td><td>DLP</td><td>box</td><td>api</td></tr> <tr> <td>Box_CAPS</td><td>ContentCreate</td><td>Encrypt</td><td>DLP</td><td>box</td><td>api</td></tr> </tbody> </table>	ACCOUNT NAME	ACTIVITY TYPE	ACTION TYPE	VIOLATION TYPE	APP NAME	EVENT ORIGIN	Box_CAPS	ContentCreate	Encrypt	DLP	box	api	Box_CAPS	ContentCreate	Encrypt	DLP	box	api	Box_CAPS	ContentCreate	Encrypt	DLP	box	api
ACCOUNT NAME	ACTIVITY TYPE	ACTION TYPE	VIOLATION TYPE	APP NAME	EVENT ORIGIN																				
Box_CAPS	ContentCreate	Encrypt	DLP	box	api																				
Box_CAPS	ContentCreate	Encrypt	DLP	box	api																				
Box_CAPS	ContentCreate	Encrypt	DLP	box	api																				

## Filtering data

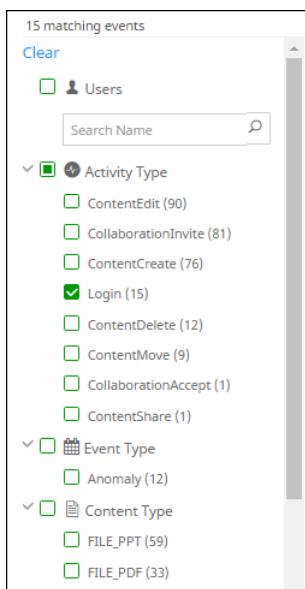
To focus on specific data, you can use the dropdown lists to set filters for the following types of information:

- Cloud applications (managed and unmanaged)
- Event types, including activities, violations, anomalies, Cloud Data Discovery (CDD) activities, CDD violations, and Cloud Security Posture events
- Event sources, **including API, IaaS audit, Office 365 audit, and other event types**
- Time range, including last hour, last 4 hours, last 24 hours, today, last week, last month, last year, and custom by month and day you select

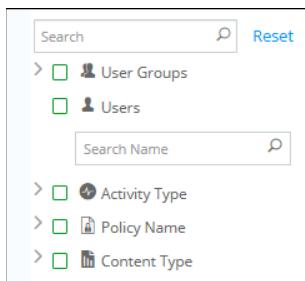
When you have selected the items from the lists, click **Search**.

The screenshot shows a search interface for 'Activity Audit Logs'. At the top, it says 'Activity Audit Logs'. Below that are four dropdown menus: 'All clouds (167)', 'Violations', 'Event Sources', and 'Last 4 Hours'. To the right of these dropdowns is a large green button labeled 'Search'.

In the vertical navigation bar at the left, you can filter the data further:



All available items are listed under each category.

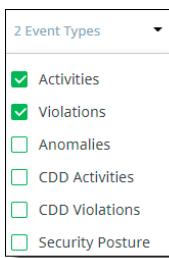


Click the **>** icon to expand the list for each category. If more than 10 items are available for a category, click **More** at the end of the list to see additional items.

#### To filter and search for data:

1. Select the search items from each of the dropdown lists and click **Search**.

The number of items matching the search criteria shows below the dropdown lists.



The search results show the total count of events.

2. In the left menu, select the items to include in the filter.

- To include all items in a category, click the box next to the category name (for example, **Activity Type**).
- To select specific items, click the boxes next to them.
- To search for a user, enter a few characters of the user's name in the **Search** box under the **Users** category. Select the username from the search results.

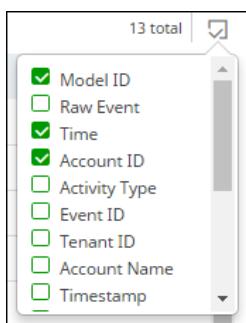
Click **Reset** to clear the filters in the navigation bar. The search items you selected from the search dropdown lists are not affected.

To hide the navigation bar and allow more room to see the data after making your filter selections, click the left-arrow icon next to the **Reset** link.



## Selecting fields to include in the table view

To select fields to appear in the table view, click the icon at the right side of the screen to display a list of available fields. The contents of the list depend on the filtering options you selected.



Check the fields to include in the log; uncheck any fields to exclude. You can include up to 20 fields.

If you have any malware scanning policies that include scanning by an external service, choose the fields that apply to that service to include in the table for those policies. For example, for a policy using FireEye ATP for malware scanning, you can include **ReportId** (a UUID provided as a response by FireEye), **MD5** (available to compare with similar MD5 information), and **Signature Names** (comma-separated values) as fields for FireEye scanning information.

## Viewing additional details from a table entry

To view additional details for a listed violation, click the binocular icon at the left side of the entry. A popup window displays details. The following examples show details from FireEye and Juniper ATP Cloud services.

## FireEye

**Threat Information**

Policy Name: FireEyeATP_Box	Time: 5/6/2020, 7:56:10 AM
Action taken: PermanentDelete	User Email: [REDACTED].ail.c

**Threat Details**

Service Vendor: FireEye	Service Name: FireEye
Content Name: t [REDACTED] exe	Signature Names: FETe [REDACTED]
SHA-256: b0... [REDACTED]	[REDACTED] ib...
MD5: 4 [REDACTED]	[REDACTED]
Report ID: 0 [REDACTED]	[REDACTED]

To display a FireEye report with additional details, click the **Report Id** link.

**Overview**

**Verdict**

Overall	100
Weight:	
Total Hits:	11
Engines Detected:	
<b>Malicious Sample</b>	

**Sample Details**

File Name	c s f 4
File Extension	exe
Md5 hash	47f! [REDACTED] <input type="button" value="Σ"/>
SHA256 hash	b 7 [REDACTED] 1556eea

**Analysis Details**

Submission UUID	0475c0a8-74dd-46cc-8fd8-2806614b9c24
Start Time	2020-05-06 14:57:41.131550
Completed at	2020-05-06 14:57:41
Duration	0
Result	<b>Malicious</b>
Signatures	FETestEvent
Overall Weight	100

## Juniper ATP Cloud

**Threat Information**

Policy Name: SkyATP	Time: 5/5/2020, 8:13:31 AM
Action taken: PermanentDelete	User Email: cc or

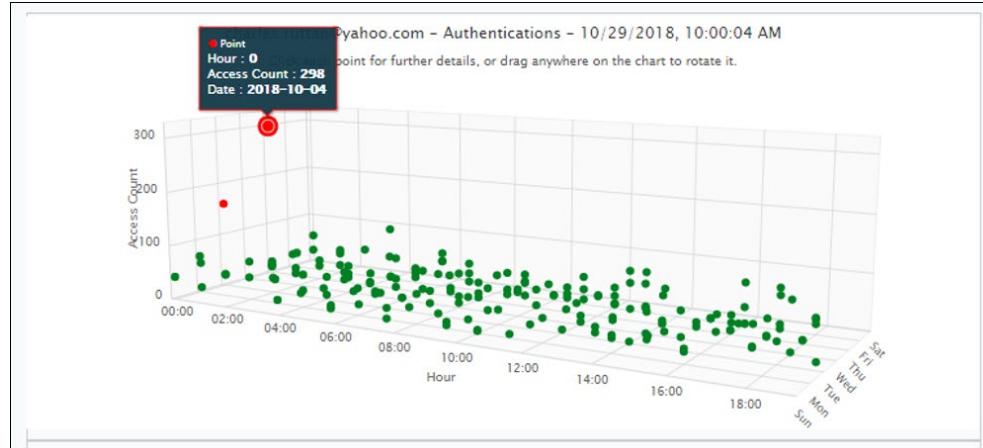
**Threat Details**

Service Vendor: Juniper Networks	Service Name: SkyATP
Malware Type: Trojan	Malware Identity: Unknown
Malware Platform: Unknown	
Threat Score: <b>10</b>	Threat Level: <b>HIGH</b>
Threat Report:	

## Viewing anomaly details from the Activity Audit Logs page

From the **Activity Audit Logs** page, you can display a three-dimensional chart of anomalous activity for a user. To view the chart, click on the **binocular** icon in any table row.

The three-dimensional anomaly view opens in a new window.



For more information about anomalies, see [Anomalous Activities](#).

## Performing an advanced search

The **Search Query** field along the top of the **Activity Audit Logs** page shows the items currently displayed when you select **Admin Audit Logs** from the **Administration** menu, or the items that apply to the details you selected from one of the **Home** page dashboards.

## Note

To perform an advanced search, make sure you understand the format for writing Splunk queries. For most searches, you can find the information you need using the filtering options, and you will not need to perform an advanced search.

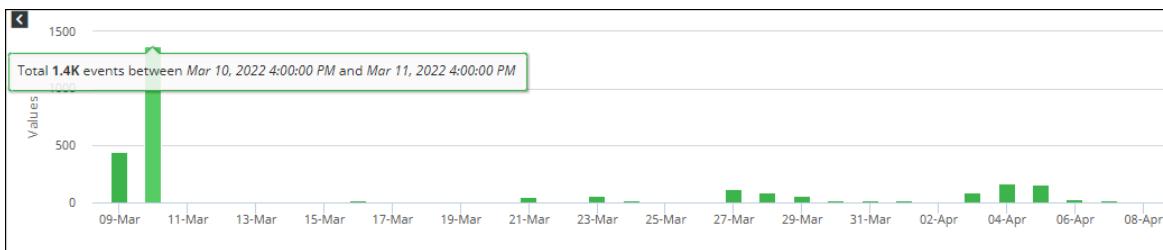
### To perform an advanced search:

1. Click in the **Search Query** field. The field expands.
2. Enter the name/value pairs for the search criteria. You can enter multiple lines of name-value pairs. Up to five lines are displayed. If your search is more than five lines long, a scroll bar appears at the right of the **Search Query** field.
3. Click the **Search** icon. The search results are displayed.
4. To return the query string field to its original size, click the **>** icon at the right. To reset the search criteria to the original values before your search, click the **x** at the right.

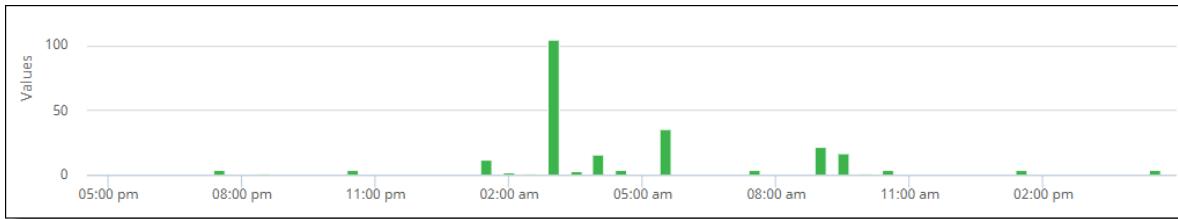
## Viewing additional log details

Do either of these actions:

- Hover over the bar for the date for which you want additional details. A pop-up displays details for that date. In this example, the pop-up shows the number of events in a 24-hour period on April 10.



- Or click the bar of the date for which you want additional details, a new bar chart is displayed with a breakdown of events. In this example, the bar chart displays an hour-by-hour count of events on April 23.



## Hiding the chart view

To hide the chart view at the top of the screen and display only the list of events, click the show/hide chart icon at the right side of the chart view. To display the chart view again, click the icon again.

## Exporting data

You can export data to a comma-separated values (.csv) file, based on the fields and navigation bar filters you have chosen.

### To export data from the Activity Audit Logs page:

1. Select the **Export** icon at the right side of the screen.



2. Select a file name and location.
3. Save the file.

## Monitoring user activity through Admin Audit Logs

Admin Audit Logs (**Administration > Admin Audit Logs**) collects security relevant system events, such as system configuration changes, user logins and logouts, system service status changes, or stopping/starting of nodes. When such changes occur, an event is generated and saved in the database.

### Audit log information

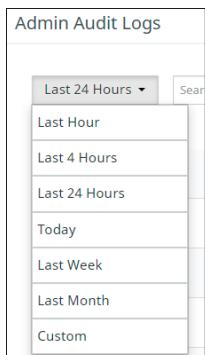
The **Admin Audit Logs** page provides the following information.

Field	Description
<b>Time</b>	The recorded time of the event.
<b>User</b>	If a user generated the event, the name (email address) of that user. If it is an event on a node, the node name is used. If neither a user nor a node was involved, N/A appears here.
<b>IP Address</b>	The IP address of the user's browser (if the user performed the action). If an event is on a node, the node's IP address is shown. If an action is being generated with no user interaction, N/A appears here.
<b>Sub System</b>	The general area where the event takes place (for example, authentication for login activity).
<b>Event Type</b>	The type of event; for example, login, certificate upload, or key request.
<b>Target Type</b>	The area being acted on.
<b>Target Name</b>	The specific location of the event.
<b>Description</b>	Additional details available about the event (shown in JSON format). Click <b>View Details</b> . If no additional details are available, only curly braces {} appear.

## Filtering and searching for Admin Audit Log information

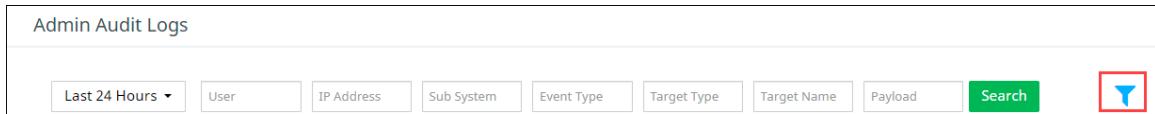
You can target the type of information in the Admin Audit Logs by narrowing the time range or searching for specific types of information.

To filter by time range, select the time range from the dropdown list at the upper left.



### To search for specific information:

Click the filter icon at the upper right. Then click in the boxes to select the information you want to find and click **Search**.



## Insights Investigate

Insights Investigate provides tools for incident management in your organization. You can view incidents that involve policy violations occurring in your organization, assign a level of severity to an incident, and specify the appropriate action. In addition, you can view details about incidents and their sources from several perspectives and obtain additional information about each incident and its source.

To use Insights Investigate functions, go to **Administration > Insights Investigate**.

The **Insights Investigate** page provides information in three tabs:

- Incident Management
- Incident Insights
- Entity Insights

### Incident Management tab

The **Incident Management** tab lists incidents occurring in the organization.

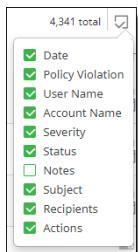
This page lists the total number of incident records found, showing up to 50 records per page. To view additional records, use the pagination buttons at the bottom of the screen.

Four dropdown lists are available from which you can filter the information to show incidents by

- **time period** (today, last 24 hours, week, month, or year, or a date period you specify)

- **cloud** (managed or unmanaged)
- **severity** (low, medium, or high)
- **status** (open, under investigation, or resolved)

The incident management list provides the following information. Use the **Column Filter** at the upper right to show or hide additional columns.



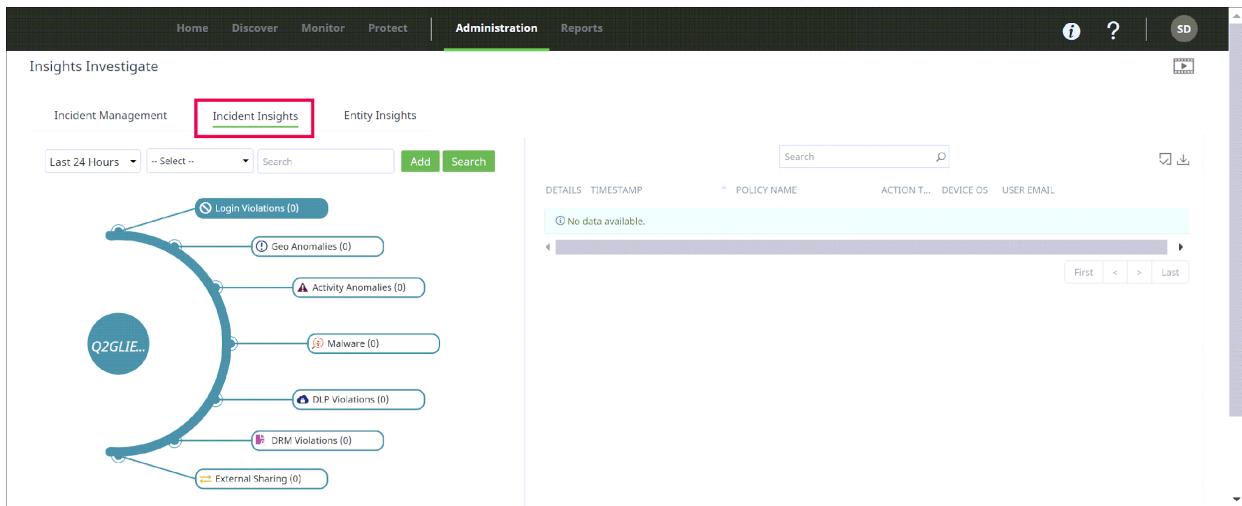
Column	What it shows
<b>Date</b>	The date and time of the last known occurrence of the incident.
<b>Policy Violation</b>	The policy that the incident violated.
<b>User Name</b>	The name of the user for the incident.
<b>Account Name</b>	The name of the cloud on which the incident occurred.
<b>Severity</b>	The severity of the incident — low, medium, or high.
<b>Status</b>	The resolution status of the incident — open, under investigation, or resolved.
<b>Subject</b>	The text of the subject for the violating email.
<b>Recipient</b>	The name of the recipient of the violating email.
<b>Actions</b>	<p>The actions that can be taken for this incident. Two icons are displayed.</p> <ul style="list-style-type: none"> <li>▪ <b>Quarantine</b> -- If the policy that was violated has an action of <b>Quarantine</b>, this icon is enabled. When clicked, this icon takes the administrator to the <b>Quarantine Management</b> page.</li> <li>▪ <b>Activity Audit Logs</b> -- When clicked, this icon takes the administrator to the <b>Activity Audit Logs</b> page. The <b>Activity Audit Logs</b> page shows the same data available on the <b>Incident Management</b> page, in a different format.</li> </ul>

You can use **Search** box to find information about a specific violation.

## Incident Insights tab

The **Incident Insights** tab provides details for these types of incidents:

- Login violations
- Geoanomalies
- Activity anomalies
- Malware
- DLP violations
- External sharing



Each violation type is labeled in the outer circle of a graph showing the tenant's name in the center. The label for each type shows the number of incidents for that type. For example, **DLP Violations (189)** indicates 189 occurrences of DLP violations.

For more precise search results, you can filter this information by date (today, last 4 hours, last 24 hours, week, month, or year. (The default is **Last 24 Hours**.)

You can search for incidents using the **Search** and **Add** buttons. These buttons enable you to conduct more precise searches for the data you need. For example, you can add a query that specifies user AND location AND application. You can include only one user in a search query.

For incident types that have no violations (count of zero), their labels are not highlighted.

For incident types that have violations, a table to the right shows additional details about each violation. The information in the table varies for each incident type. Click the violation label to see the list of incidents for that violation.

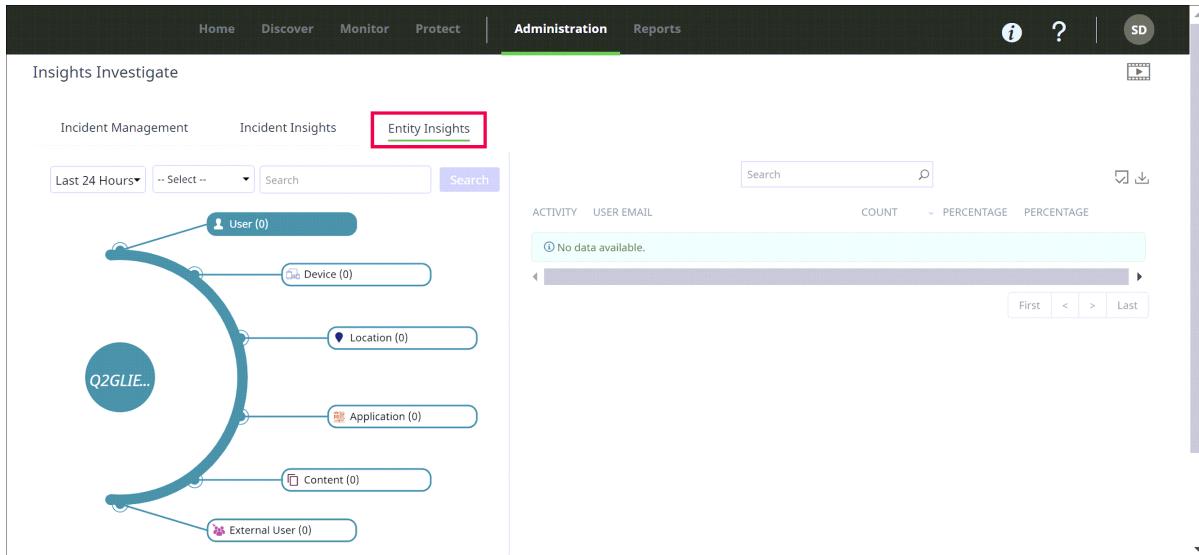
For **DLP Violations**, the table shows the following information for up to 100 records.

You can click the **binocular** icon in the first column of the table row to view a popup with additional details about a violation.

## Entity Insights tab

The **Entity Insights** tab provides details about the entities that are the sources of violations, including:

- User
- Device
- Location
- Application
- Content
- External user



Each entity is labeled in the outer circle of the graph. By default, the tenant name appears in the center circle. The label for each entity shows the name of the entity and the count found for it. For example, User (25) would indicate 25 users found, Device (10) would indicate 10 devices found.

For more precise search results, you can filter this information by date (today, last 4 hours, last 24 hours, week, month, or year. (The default is **Last 24 Hours**.)

You can search for additional details about an entity. For example, if you search for a user by entering the username in the **Search** field, the graph displays the username and their risk level. The user's risk level is displayed as a half-circle around the username. The color indicates the risk level (**low**, **medium**, or **high**).

For entity types that have incidents, a table to the right shows additional details about each incident for the entity. The type of information shown in the table varies according to the entity. Click the entity label to see the table for that entity.

### Notes

- The **Entity Insights** table can display no more than 1,000 records. If your search yielded a high count for an entity, the table displays only the first 1,000 records found, even if the total number of records exceeds 1,000. You might need to refine your search further to keep the total record count at 1,000 or fewer.
- When exporting Entity Insights activity records from the **Activity Audit Logs** page to a CSV file, the export is limited to 10,000 events. If your search yielded an activity count higher than this, the exported CSV file will include only the first 10,000 records found.

## Viewing and updating user risk information

The **User Risk Management** page (**Protect > User Risk Management**) uses information from policy violations, anomalies, and malware events to highlight users who might be posing a risk to your data security. This information can help you determine if policies or user permissions need to be adjusted.

You can update the user risk management settings to set risk thresholds and specify the type of information to include in risk assessments.

To modify user risk assessment settings, click the gear icon to the right above the table. Then, change the following settings as needed.

- Under **Violation Duration**, move the slider to the right or left.
- Under **Threshold**, move the slider to the right or left.
- Check or uncheck the types of information (policy violations, malware incidents, anomalies and policy actions) to include in the risk assessment.

Click **Save** to activate the settings.

# Creating, viewing, and scheduling reports

---

You can create a variety of reports that provide a comprehensive view of information such as:

- how and from where users access data from cloud applications and from websites,
- how and with whom the data is shared, and
- whether users have taken all appropriate security precautions.

In addition, reports provide information that help to identify issues such as these:

- anomalous/anonymous data access
- deviations in the defined policies
- deviations from the defined regulatory compliances
- possible malware threats
- types of websites accessed (for example, shopping, business and economy, news and media, technology and computers, dating, or gambling)

Anomaly reports focus on the User and Entity Behavioral Analysis (UEBA) capability provided by the Juniper Cloud Security Platform. They show anomalous user and content activity, which can indicate insider threats or potential malware or ransomware.

Compliance reports provide insights into your organization's compliance status and adherence to security policies. They show findings from observations of policy violations, users and applications involved, and remediation steps to address non-compliance issues.

You can create reports and run them at a scheduled time on a selected day, or on one day of a week for the entire week. You can also view the scheduled reports and download them for further analysis.

## Note

Reports are generated based on global time zone settings.

## Uploading a company logo

**To upload a company logo to use with reports:**

1. Go to **Administration > System Settings**.
2. Select **Logo and Time Zone**.
3. Enter your **Company Name**.
4. Upload your company logo. Select a logo file from your computer and click **Upload**.  
For the best results, the logo should be 150 pixels wide and 40 pixels high.
5. Click **Save**.

## Setting a time zone

You can select a time zone to apply to reports. When you generate reports, they will be based on the time zone you select.

### To set a time zone:

1. In **System Settings**, select **Logo and Time Zone**.
2. In the **Time Zone** section, select a time zone from the dropdown list and click **Save**.

When you generate a report, the time zone you selected is displayed on the report cover page.



### Web activity report 3 Custom Report

From: 29-Mar-2022 00:00 To: 29-Mar-2022 23:59

Timezone: UTC

## Selecting report types for cloud applications

Juniper Secure Edge CASB offers the following types of reports:

- Visibility
- Compliance
- Threat Protection
- Data Security
- IaaS
- Custom

Each report is categorized into sub-types to provide deeper analysis.

The following sections explain the report types and sub-types.

### Visibility

Visibility reports provide a consolidated view into sanctioned cloud usage patterns and Shadow IT (unauthorized cloud) reporting, detailing how and where users are accessing cloud data.

Visibility is further categorized into these areas:

- **Cloud Discovery** -- Provides details about unauthorized cloud usage.
- **User Activity** -- Provides details about how and where users access the sanctioned and unauthorized cloud applications.
- **External User Activity** -- Provides details about users outside the organization with whom the data has been shared and their activities with the cloud applications.
- **Privileged User Activity** (only if one or more Salesforce cloud applications are onboarded) – Provides details about activities by users with extended credentials.

### Compliance

Compliance reports monitor data in the cloud for compliance with data privacy and data residency regulations as well as cloud risk scoring.

Compliance is further categorized as follows:

- **Compliance violations by user** – provides details about user activities that breach defined security policies in your organization.

- **Sharing violations by user** – provides details about user activities that breach data sharing policies with external users.

## Threat Protection

Threat Protection reports provide analysis of traffic and apply user behavior analytics to find external threats such as compromised accounts and flag suspicious behavior of privileged users.

Threat Protection is further categorized as follows:

- **Anomaly** – Provides information about anomalous, suspicious data access, and unusual user activities (such as simultaneous access of data by the same user login into the system from different devices at different locations).
- **Advanced threat and malware** – Shows a graphical view of threats and malware incidents for the time period selected.
- **Unmanaged device access** – Provides information about user access with unmanaged devices.

## Data Security

Data Security reports provide analysis of file, field, and object protection through encryption, tokenization, collaboration controls, and data loss prevention.

Data Security is further categorized as follows:

- **Encryption statistics** – provides information about file encryption activities by users, devices used for file encryption, files that have been encrypted, any new devices used for encrypting files, list of registered devices by operating system, file decryption by location, and decryption failures over a specified period.
- **Device statistics** – provides information about unencrypted files on unmanaged devices and top 10 users with encrypted files on unmanaged devices.

## IaaS

- IaaS reports provide analysis of activity for **AWS**, **Azure**, and **Google Cloud Platform (GCP)** cloud types.

## Custom

- Custom reports enable you to generate reports from charts in the monitoring dashboards.

## Displaying report information

Perform the following steps to display report information.

In the Management Console, click the **Reports** tab.

The **Reports** page lists the generated reports. If you are logging in for the first time, a blank table is displayed. For each report, the list provides the following information:

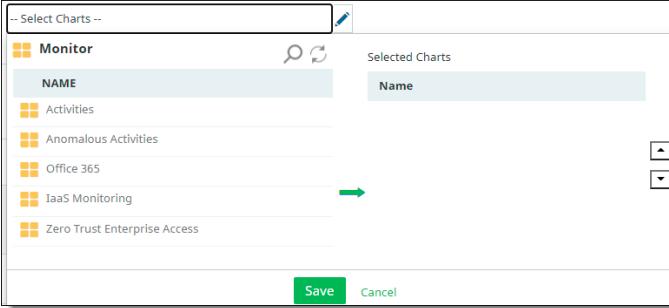
Column	Description
Name	The <b>Name</b> given for the report.

Column	Description
Type	The <b>Type</b> of report. <ul style="list-style-type: none"><li>▪ For CASB – The selected type for the report (for example, <b>Visibility</b>).</li><li>▪ For Secure Web Gateway – <b>Custom</b>.</li></ul>
Sub-Type	<b>Sub-Type</b> of the report. <ul style="list-style-type: none"><li>▪ For CASB – Based on the selected report <b>Type</b>.</li><li>▪ For Secure Web Gateway – <b>Custom</b>.</li></ul>
Frequency	How often the report will be generated.
Actions	Option to delete the report.

## Scheduling a new report

1. From the **Reports** page, click **New**.
2. Enter the following information. Fields with a colored border at the left require a value.

Field	Description
Name	Name of the report.
Description	A description of the report contents.
Filter/Type	Select either <ul style="list-style-type: none"><li>▪ <b>Clouds</b></li><li>▪ <b>Websites</b></li></ul>
User Name	Enter one or more valid email addresses for the users to include in the report. To include all users, leave this field blank.
Configuration/Type	Select a report type. For <b>Clouds</b> , the options are: <ul style="list-style-type: none"><li>▪ <b>Visibility</b></li><li>▪ <b>Compliance</b></li><li>▪ <b>Threat Protection</b></li><li>▪ <b>Data Security</b></li><li>▪ <b>IaaS</b></li><li>▪ <b>Custom</b></li></ul>

Field	Description
	For <b>Websites</b> , the default selection is <b>Custom</b> .
<b>Sub-Type</b>	Select one or more sub types. The options listed are related to the report type you selected.  For <b>Custom</b> reports, double-click the dashboards from which you want to generate reports. In this example, the selectable charts are from any of the dashboards for <b>Cloud</b> report types.  
	Drill down to see a list of available charts, click a chart, and click the right-arrow icon to move it to the <b>Selected Charts</b> list. Repeat these steps for each chart to include.
<b>Format</b>	Select <b>PDF</b> and save the report on your computer. You can open and view the report using a PDF viewer such as Adobe Reader.
<b>Frequency</b>	Select the time-interval at which the report needs to be generated – either <b>Daily</b> , <b>Weekly</b> , or <b>One Time</b> .  <b>For One Time</b> , select the date range for the data to include in the report and click <b>OK</b> .
<b>Notification</b>	Select the type of notification to receive for report activity.

3. Click **Save** to schedule the report. The newly created report is added to the list of available reports.

Once a scheduled report is generated, the system triggers an email notification informing the user that the report scheduling is complete and provides a link to access and download the report.

## Downloading generated reports

As stated in the previous section, the system sends an email when a scheduled report has been generated. Clicking the link in that email takes you to the **Reports** page, where you can view the list of generated reports and select a report to download.

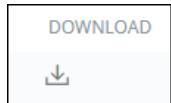
1. From the **Reports** page, click the > icon to select the generated report you want to download.

2. Click the **Reports for Download** tab.

A list of generated reports appears, with the following information.

Column	Description
<b>Generated Date</b>	The date and time when the report was generated.
<b>Report Name</b>	Name of the report.
<b>Report Type</b>	Type of report.
<b>Report Sub-Type</b>	Sub-Type of report (based on <b>Type</b> ). For <b>Websites</b> , the Sub-Type is always <b>Custom</b> .
<b>Report Format</b>	Format of the report (PDF).
<b>Download</b>	Icon for downloading the report.

3. Choose the generated report you want to download by clicking the download icon at the right.



4. Select a destination on your computer and a name for the file.
5. Save the report.

## Managing report types and scheduling

You can update information about reports and their delivery schedules.

1. From the **Reports** page, click the > icon next to the report whose information you want to modify.
2. Click the **Manage Schedules** tab.
3. Edit the report information as needed.
4. Save the report.

## Quick reference: Home dashboard charts

The following tables describe the content available for the dashboards from the **Monitor** menu.

- Application Activities
- Anomalous Activities
- Office 365
- IaaS Monitoring Dashboard
- Zero Trust Enterprise Access

For information about viewing the charts, see [Monitoring cloud activity from charts](#).

## Application Activities

This dashboard displays the following groups of charts:

- Policy Analytics
- Activity Monitoring
- Encryption Statistics
- Privileged User Activities

### Policy Analytics

Chart	What it shows
<b>Files Encrypted by Policy</b>	The number of files encrypted (for example, files with credit card data) in response to policy violations. This chart provides insights into documents that were encrypted based on one or more policy definitions.
<b>Files Encrypted Over Time</b>	The number of files that have been encrypted, which indicates encryption trends that can help you better understand the overall risk posture over time.
<b>Policy Hits over Time</b>	The number of violations or events that the policy engine had detected, indicating trends on the risk posture for your supported cloud applications.
<b>Policy Hits by User</b>	The number of violations or events detected by the policy engine, by user email address; helps identify top users in violation of compliance policies.
<b>Policy Remediations</b>	The total number of policy violation actions over a specified period, with a percentage breakdown for each type of action. This view helps identify remediation actions taken for policy violations, which provides insights into adjustments that might be needed to policy remediations.

Chart	What it shows
<b>Activities Over Time</b>	The number of activities on files, indicating activity trends for your cloud applications.
<b>Policy Hits by Cloud</b>	The total number of detected policy violations or events for all cloud applications, with a breakdown by cloud.
<b>External Collaborator Hits by Cloud</b>	The number of detected policy violations by external collaborators. Helps identify policy violations owing to external collaborators. This is important from the perspective of understanding risk exposure due to external collaborator activities.
<b>Policy Hits by SharePoint Site</b>	For each SharePoint site, the number of detected policy violations or events, by type. Applies only to SharePoint sites; shows policy hits by individual site.
<b>Policy Hits by Location</b>	The number of policy violations or events according to the geographical location where the events occurred.
<b>Public Link Hits Over Time</b>	For each cloud, the number of public link violations. This view shows compliance violations due to public (open) links. These links could provide access to highly sensitive data which is accessible to anyone with the access to the link.
<b>Advanced Threats and Malwares Over Time</b>	For each cloud, the number of threats and malware incidents detected.
<b>Key Access Denied over Time</b>	The number of times that access to a key was denied as defined by key access policies set for your enterprise.
<b>Login Access Denied over Time</b>	The number of times that login was denied.
<b>Login Access Denied by Location</b>	A map showing the locations at which login access was denied.
<b>Top 5 Login Access Denied Users</b>	The highest numbers of login access denials by user.

## Activity Monitoring

Chart	What it shows
<b>Activities Over Time</b>	The number of activities being performed by users for each cloud, indicating activity trends over time.
<b>Login Activities Over Time</b>	For each cloud, the number of login activities.
<b>Users by Activity</b>	Users according to the activities they have performed, providing a view of user activities across cloud applications.
<b>Object Types by Activity (Salesforce cloud applications)</b>	The types of objects associated with an activity.
<b>Login Activities by OS</b>	The total number of login activities for a specified period, and a breakdown by percentage for each operating system from which users logged in. This view helps identify activity by OS.
<b>Top 5 Users by File Download</b>	The total number of files downloaded for a specified period, and a breakdown by percentage for the email addresses of the users with the highest number of downloads.
<b>Downloaded Reports</b>	The names of reports with the highest number of downloads.
<b>Report Downloads by User</b>	The email addresses of users who have downloaded the highest number of reports over time.
<b>User Activities by OS</b>	The number of activities, by cloud, for each operating system to which the users are logged in.
<b>Viewed Reports by User</b>	The types of reports viewed by users over time.
<b>Account Names by Activity (Salesforce cloud applications only)</b>	The names of the accounts with the highest number of activities over time.
<b>Lead Names by Activity (Salesforce cloud applications only)</b>	The names of the leads with the highest number of activities over time.
<b>Viewed Reports by User</b>	The highest numbers of reports viewed by users, from highest to lowest.

Chart	What it shows
<b>Shared Content by Activity</b>	<p>Activities for content that is shared. From this report, you can determine what files are being shared the most (by file name), and what is being done with those files (for example, deleting or downloading).</p> <p><b>Note</b></p> <p>In Salesforce cloud applications, sharing activities will show the file ID instead of the file name.</p>
<b>Login Activity by Location</b>	A circle graph showing counts of login activities by geographical location.
<b>Content Shared by Location</b>	A circle graph showing counts of content sharing activity by geographical location.

## Encryption Statistics

Chart	What it shows
<b>File Encryption Activities by User</b>	For each cloud, the email addresses of users with the highest number of file encryptions and decryptions. This view highlights access to highly sensitive encrypted data by users.
<b>Devices Used for File Encryption</b>	The highest numbers of client devices being used to encrypt and decrypt files. This view highlights access to highly sensitive encrypted data based on devices.
<b>Encryption Activities by File Name</b>	For each cloud, the names of files with the highest number of encryptions and decryptions.
<b>New Devices Over Time</b>	For each cloud, the number of new client devices being used for encryption and decryption.
<b>Encryption Activities Over Time</b>	The number of encryption and decryption activities.
<b>File Decryption by Location</b>	The geographical locations where files are being decrypted, and the number of files decrypted in each location. Provides important insight into the geo-locations from which highly sensitive encrypted data is being accessed.
<b>Registered Devices by OS</b>	Shows the total number of client devices registered for use to decrypt files, and a breakdown by percentage for each type of device.
<b>Client Device Registration Failures Over Time</b>	For each cloud, the number and client device registration failures, month by month.
<b>Decryption Failures Over Time</b>	For each cloud, shows the number of decryption failures, month by month.

## Privileged User Activities

Chart	What it shows
<b>Privileged Activities Over Time</b>	The number of privileged-access activities month by month, for each cloud. This view is typically used to identify insider threats by users who have elevated permissions in the cloud applications.
<b>Privileged Activities by Type</b>	The total number of privileged-access activities, with a percentage breakdown for each activity type. Provides insights into the types of activities being performed by privileged users.
<b>Audit Messages</b>	For each cloud, the names of the highest number of audit messages are generated. Shows specific security setting changes by privileged users.
<b>Accounts Enabled or Disabled Over Time</b>	The number of accounts frozen and unfrozen by the administrator. Shows user account activation and deactivation events per cloud.
<b>Accounts Created or Deleted Over Time</b>	The number of user accounts created or deleted by an administrator.
<b>Delegated Activities Over Time</b>	Delegated activities (activities performed by an administrator while logged in as another user).

## Anomalous Activities

The following charts display anomalous activities.

Chart	What it shows
<b>Anomalous Activities by Geolocation</b>	<p>A map view with geographic pointers indicating where anomalous activity has likely occurred, showing login or cloud activities by the same user across multiple geolocations. This type of anomaly is called a geoanomaly. If geoanomalies have been detected, the map shows one or more geographic pointers identifying where the activity in question took place.</p> <p>This view is typically used to identify account hijacking or compromised account credential scenarios.</p>
<b>Anomalous Downloads by Size</b>	<p>The number of downloads that exceed the expected download activity for your enterprise, by file size.</p>
<b>Anomalous Authentication</b>	<p>The number of times an anomalous pattern is found in a user's network events, including logins, failed or brute-force login attempts, and logouts.</p>
<b>Anomalous Content Delete</b>	<p>The number of content delete activities for anomalous content.</p>
<b>Anomalous Downloads by Count</b>	<p>The number of downloads that exceed expected download activity for your enterprise. This information is typically used to identify data exfiltration attempts by a bad inside actor. This is done by profiling normal user activity and triggering an anomalous activity when unusual download activity takes place for that account.</p>

## Office 365

Several types of charts are available to view information for the Microsoft 365 applications you selected for protection when the Microsoft 365 suite was onboarded. If you do not select an application for protection, the dashboard and charts for that application will not be visible. To add an application for protection after onboarding:

1. Go to **Administration > App Management**.
2. Select the Microsoft 365 cloud type you onboarded.
3. On the **Application Suite** page, select the applications for which you want to add protection.
4. Re-authenticate as needed.

For detailed instructions, see [Onboarding Microsoft 365 cloud applications](#).

Use the following links to view information about the Microsoft 365 charts:

- [Overview](#)
- [Admin Activities](#)
- [OneDrive](#)
- [SharePoint](#)
- [Teams](#)

## Overview

The Overview charts summarize activity for the Microsoft 365 applications you have selected for protection.

Chart	What it shows
<b>Active User Count Over Time Grouped by Clouds</b>	The number of active users for each cloud application over the time range.
<b>Inactive User Count Over Time Grouped by Clouds</b>	The number of inactive users (users with no activity for six months or more) for each cloud application.
<b>Activity Count Over Time Grouped by Cloud applications</b>	The number of activities for each application over the time range.
<b>Activity Count By Location Grouped by Clouds</b>	A map view showing the number of activities in specific locations for each cloud application over the time range. If only one activity occurred, only the location icon is shown; if multiple activities occurred, the number of activities is shown in a circle graph.
<b>Successful Logins Over Time</b>	Counts of successful logins by user over time.

Chart	What it shows
<b>Failed Logins Over Time</b>	Counts of failed logins by user over time.

## Admin Activities

These charts display activity by administrators.

Chart	What it shows
<b>Site Admin Activities Grouped by Activity Type</b>	The number of activities performed by site administrators, by activity type.
<b>User Management Grouped by Activity Type</b>	The number of activities related to user management, by activity type.
<b>Enterprise Settings Grouped by Activity Type</b>	The total number of enterprise settings, by activity type.

## OneDrive

The OneDrive charts display activity for the OneDrive application.

Chart	What it shows
<b>Top 10 Users by Activity</b>	The user IDs of the 10 most active OneDrive users, and the total activity count for each user.
<b>Activity Count Over Time Grouped by Activity Type</b>	The number of OneDrive activities over the time range, by activity (for example, edit, external sharing, file syncing, and internal sharing).
<b>Activity Count by Location</b>	A map view showing the number of OneDrive activities of each type that occurred at specific locations. If only one activity occurred, only the location icon is shown; if multiple activities occurred, the number of activities is shown in a circle graph.
<b>Public Sharing Activity Count Over Time</b>	The number of public sharing activities over the time range.
<b>Top 10 External Users by Access Activity</b>	The user IDs of the top 10 OneDrive users, and the activity count for each user over time.

Chart	What it shows
<b>External Sharing Activity Count Over Time</b>	The number of external sharing activities over the time range.
<b>Anonymous Access Activity Count Over Time</b>	The number of OneDrive anonymous access activities over time. Anonymous access is granted from a link that does not require the user to provide authentication.

## SharePoint

The SharePoint charts display activity for the SharePoint application.

Chart	What it shows
<b>Top 10 Users by Activity</b>	The user IDs of the 10 most active SharePoint users, and the total activity count for each user.
<b>Activity Count Over Time Grouped by Activity Type</b>	The number of activities over the time range, by activity (edit, external sharing, file syncing, and internal sharing).
<b>Activity Count by Location</b>	A map view showing the number of activities of each type that occurred at a specific location.
<b>Public Sharing Activity Count Over Time</b>	The number of public sharing activities over the time range.
<b>Top 10 External Users by Access Activity</b>	The user IDs of the top 10 users, and the activity count for each user, over the time range.
<b>External Sharing Activity Count Over Time</b>	The number of external user activities over the time range.
<b>Anonymous Access Activity Over Time</b>	The number of anonymous access activities over time. Anonymous access is granted from a link that does not require the user to provide authentication.

## Teams

The Teams charts display activity for the Teams application.

Chart	What it shows

<b>Top 10 Users by Activity</b>	The user IDs of the 10 most active users for Teams, and the total activity count for each user.
<b>Activity Count Over Time Grouped by Activity Type</b>	The number of activities in Teams over the time range, by activity type.
<b>Device Usage Grouped by Device Type</b>	The number of devices used to access Teams, by device type.

## IaaS Monitoring Dashboard

This dashboard displays user and activity counts in the following charts:

- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform

### Amazon Web Services

The Amazon Web Services charts display information for EC2, IAM, and S3.

Chart	What it shows
<b>Top 5 Active Users - EC2</b>	The user IDs of the five most active EC2 users.
<b>Top 5 Active Users – IAM</b>	The user IDs of the five most active Identity and Access Management (IAM) users.
<b>Top 5 Active Users - S3</b>	The user IDs of the five most active S3 users.
<b>Top 5 Active Users - AWS Console</b>	The user IDs of the five most active users of the AWS Console.
<b>Top 5 Activities - EC2</b>	The five most frequently performed activities for EC2.
<b>Top 5 Activities – IAM</b>	The five most frequently performed activities for IAM.
<b>Top 5 Activities - S3</b>	The five most frequently performed activities for S3.
<b>Top 5 Activities - AWS Console</b>	The five most frequently performed activities for the AWS Console.

Chart	What it shows
<b>Activity by User Location - EC2</b>	A map view showing the number of EC2 activities that occurred at specific locations. If only one activity occurred, only the location icon is shown; if multiple activities occurred, the number of activities is shown in a circle graph.
<b>Activity by User Location - IAM</b>	A map view showing the number of IAM activities that occurred at specific locations. If only one activity occurred, only the location icon is shown; if multiple activities occurred, the number of activities is shown in a circle graph.
<b>Activity by User Location - S3</b>	A map view showing the number of S3 activities that occurred at specific locations. If only one activity occurred, only the location icon is shown; if multiple activities occurred, the number of activities is shown in a circle graph.
<b>Activity by User Location - AWS Console</b>	A map view showing the number of IAM activities that occurred at specific locations. If only one activity occurred, only the location icon is shown; if multiple activities occurred, the number of activities is shown in a circle graph.
<b>Activities Over Time - EC2</b>	The number of EC2 activities over the time range.
<b>Activities Over Time - IAM</b>	The number of IAM activities over the time range.
<b>Activities Over Time - S3</b>	The number of S3 activities over the time range.
<b>Activities Over Time - AWS Console</b>	The number of activities in the AWS Console over the time range.

## Microsoft Azure

The Microsoft Azure charts display information related to virtual machine use, network configurations, storage, login, container, and Azure AD activity.

Chart	What it shows
<b>Top 5 Active Users – Compute</b>	The User IDs of five most active Virtual Machine users.
<b>Top 5 Active Users – Network</b>	The User IDs of five most active Network Configurations (for example, VNet, Network Security Group and Network Route Table Association and Dissociation) modifying users.

Chart	What it shows
<b>Top 5 Active Users – Storage</b>	The User IDs of five most active Storage Account (Blob Storage and Compute Storage) users.
<b>Top 5 Active Users – Azure Login</b>	The User IDs of five most active users.
<b>Top 5 Active Users – Container Service</b>	The User IDs of five most active Container Service users (for example, Kubernetes or Windows Container).
<b>Top 5 Activities – Compute</b>	The five most frequently performed activities for Virtual Machines (for example, Creation, Deletion, Start Stop and Restart Virtual Machine).
<b>Top 5 Activities – Network</b>	The five most frequently performed activities for Network.
<b>Top 5 Activities – Azure AD</b>	The five most frequently performed activities for Azure Active Directory (Add New User, Delete User, Create Group, Delete Group, Add User to Group, Create Role, Delete Role, Associate to New Roles).
<b>Top 5 Activities – Storage</b>	The five most frequently performed activities for Storage (Create or Delete Blob Storage and Virtual Machine Storage).
<b>Top 5 Activities – Container Service</b>	The five most frequently performed activities for Container Service (for example, Create or Delete Kubernetes and Windows Container service).
<b>Activities Over Time – Compute</b>	The number of Virtual Machine related activities over the time range.
<b>Activities Over Time – Network</b>	The number of Network related activities over the time range.
<b>Activities Over Time – Azure AD</b>	The number of Azure Active Directory related activities over the time range.

Chart	What it shows
<b>Activities Over Time – Storage</b>	The number of Storage related activities over the time range.
<b>Activities Over Time – Container Service</b>	The number of Container activities over the time range.
<b>Activities by Location – Compute</b>	A map view showing the number of Virtual Machine activities that occurred at specific locations. If only one activity occurred, only the location icon is shown; if multiple activities occurred, the number of activities is shown in a circle graph.
<b>Activities by Location – Network</b>	A map view showing the number of Network activities that occurred at specific locations. If only one activity occurred, only the location icon is shown; if multiple activities occurred, the number of activities is shown in a circle graph.
<b>Activities by Location – Storage</b>	A map view showing the number of Storage activities that occurred at specific locations. If only one activity occurred, only the location icon is shown; if multiple activities occurred, the number of activities is shown in a circle graph.
<b>Activities by Location – Azure Login</b>	A map view showing the number of Login activities that occurred at specific locations. If only one activity occurred, only the location icon is shown; if multiple activities occurred, the number of activities is shown in a circle graph.
<b>Activities by Location – Container Service</b>	A map view showing the number of activities that occurred at specific locations. If only one activity occurred, only the location icon is shown; if multiple activities occurred, the number of activities is shown in a circle graph.

## Google Cloud Platform

The Google Cloud Platform (GCP) charts display information for virtual machines, IAM, login, storage, and location activity.

Chart	What it shows
<b>Top 5 Active Users – Compute</b>	The User IDs of five most active Compute users (Virtual Machine Instances), Firewall Rules, Routes, VPC Network).
<b>Top 5 Active Users – IAM</b>	The user IDs of the five most active IAM users.
<b>Top 5 Active Users – Storage</b>	The user IDs of the five most active Storage users.
<b>Top 5 Active Users – Login</b>	The User IDs of five most active users.
<b>Top 5 Activities – Compute</b>	The five most frequently performed activities for Compute (for example, Create Instance, Delete Instance, Create Firewall, Delete Firewall, Disable Firewall, Create Route, Delete Route, Create VPC Network).
<b>Top 5 Activities – IAM</b>	The five most frequently performed activities for IAM.(for example, Two Step Verification Enrolled, Two Step Verification Disabled, Create Role, Delete Role, Change Password, Create API Client, Delete API Client).
<b>Top 5 Activities – Storage</b>	The five most frequently performed activities for Storage (for example, Set Bucket Permissions, Create Bucket, Delete Bucket).
<b>Top 5 Activities – Login</b>	The five most frequently performed activities for the Login (Login Success, Login Failure, Logout).
<b>Activities Over Time – IAM</b>	The number of IAM activities over the time range.
<b>Activities Over Time – Storage</b>	The number of Storage activities over the time range.
<b>Activities Over Time – Login</b>	The number of Login activities over the time range.
<b>Activities Over Time – Compute</b>	The number of Compute activities over the time range.

Chart	What it shows
<b>Activities by Location – Compute</b>	A map view showing the number of Compute activities that occurred at specific locations. If only one activity occurred, only the location icon is shown; if multiple activities occurred, the number of activities is shown in a circle graph.
<b>Activities by Location – IAM</b>	A map view showing the number of IAM activities that occurred at specific locations. If only one activity occurred, only the location icon is shown; if multiple activities occurred, the number of activities is shown in a circle graph.
<b>Activities by Location – Storage</b>	A map view showing the number of Storage activities that occurred at specific locations. If only one activity occurred, only the location icon is shown; if multiple activities occurred, the number of activities is shown in a circle graph.
<b>Activities by Location – Login</b>	A map view showing the number of login activities that occurred at specific locations. If only one activity occurred, only the location icon is shown; if multiple activities occurred, the number of activities is shown in a circle graph.

## Quick reference: RegEx examples

Following are some examples of regular expressions.

Regular expression	Description	Sample data
[a-zA-Z]{4}[0-9]{9}	Custom account number starting with 4 letters followed by 9 digits.	ghrd123456789
[a-zA-Z]{2-4}[0-9]{7-9}	Custom account number starting with 2-4 letters followed by 7-9 digits.	ghr12345678
([a-zA-Z0-9_\.-]+)@([\\da-zA-Z\.-]+)\.([a-zA-Z\.]{2,6})	Email address	Joe_smith@mycompany.com

## Quick reference: Supported file types

CASB supports the following file types. To identify file types for any formats not listed here, contact the Juniper Networks Support team (<https://support.juniper.net/support/>).

File type	Description
<b>Ami</b>	Ami Pro
<b>Ansi</b>	Ansi text file
<b>Ascii</b>	Ascii (DOS) text file
<b>ASF</b>	ASF file
<b>AVI</b>	AVI file
<b>Binary</b>	Binary file (unrecognized format)
<b>BMP</b>	BMP image file
<b>CAB</b>	CAB archive
<b>Cals</b>	CALS metadata format described in MIL-STD-1840C
<b>CompoundDoc</b>	OLE Compound Document (or "DocFile")
<b>ContentAsXml</b>	Output format for FileConverter that organizes document content, metadata, and attachments into a standard XML format
<b>CSV</b>	Comma-separated values file
<b>CsvAsDocument</b>	CSV file parsed as a single file listing all records
<b>CsvAsReport</b>	CSV file parsed as report (like a spreadsheet) instead of a database
<b>DatabaseRecord</b>	Record in a database file (such as XBase or Access)
<b>DatabaseRecord2</b>	Database record (rendered as HTML)
<b>DBF</b>	XBase database file

File type	Description
<b>DocFile</b>	Compound document (new parser)
<b>dtSearchIndex</b>	dtSearch index file
<b>DWF</b>	DWF CAD file
<b>DWG</b>	DWG CAD file
<b>DXF</b>	DXF CAD file
<b>ElfExecutable</b>	ELF format executable
<b>EMF</b>	Windows Metafile Format (Win32)
<b>EML</b>	Mime stream handled as a single document
<b>EudoraMessage</b>	Message in a Eudora message store
<b>Excel12</b>	Excel 2007 and newer
<b>Excel12xlsb</b>	Excel 2007 XLSB format
<b>Excel2</b>	Excel Version 2
<b>Excel2003Xml</b>	Microsoft Excel 2003 XML format
<b>Excel3</b>	Excel version 3
<b>Excel4</b>	Excel version 4
<b>Excel5</b>	Excel versions 5 and 7
<b>Excel97</b>	Excel 97, 2000, XP, or 2003
<b>FilteredBinary</b>	Filtered binary file
<b>FilteredBinaryUnicode</b>	Binary file filtered using Unicode Filtering
<b>FilteredBinaryUnicodeStream</b>	Binary file filtered using Unicode Filtering, not split into segments

File type	Description
<b>FlashSWF</b>	Flash SWF
<b>GIF</b>	GIF image file
<b>Gzip</b>	Archive compressed with gzip
<b>HTML</b>	HTML
<b>HtmlHelp</b>	HTML Help CHM file
<b>iCalendar</b>	iCalendar (*.ics) file
<b>Ichitaro</b>	Ichitaro word processor file (versions 8 through 2011)
<b>Ichitaro5</b>	Ichitaro versions 5, 6, 7
<b>IFilter</b>	File type processed using installed IFilter
<b>iWork2009</b>	iWork 2009
<b>iWork2009Keynote</b>	iWork 2009 Keynote presentation
<b>iWork2009Numbers</b>	iWork 2009 Numbers spreadsheet
<b>iWork2009Pages</b>	iWork 2009 Pages document
<b>JPEG</b>	JPEG file
<b>JpegXR</b>	Windows Media Photo/HDPhoto/*.wdp
<b>Lotus123</b>	Lotus 123 spreadsheet
<b>M4A</b>	M4A file
<b>MBoxArchive</b>	Email archive conforming to the MBOX standard (dtSearch versions 7.50 and earlier)
<b>MBoxArchive2</b>	Email archive conforming to the MBOX standard (dtSearch versions 7.51 and later)
<b>MDI</b>	MDI image file

File type	Description
<b>Media</b>	Music or video file
<b>MicrosoftAccess</b>	Microsoft Access database
<b>MicrosoftAccess2</b>	Microsoft Access (parsed directly, not via ODBC or the Jet Engine)
<b>MicrosoftAccessAsDocument</b>	Access database parsed as a single file listing all records
<b>MicrosoftOfficeThemeData</b>	Microsoft Office .thmx file with theme data
<b>MicrosoftPublisher</b>	Microsoft Publisher file
<b>MicrosoftWord</b>	Microsoft Word 95 - 2003 (dtSearch versions 6.5 and later)
<b>MIDI</b>	MIDI file
<b>MifFile</b>	FrameMaker MIF file
<b>MimeContainer</b>	MIME-encoded message, processed as a container
<b>MimeMessage</b>	dtSearch 6.40 and earlier file parser for .eml files
<b>MP3</b>	MP3 file
<b>MP4</b>	MP4 file
<b>MPG</b>	MPEG file
<b>MS_Works</b>	Microsoft Works word processor
<b>MsWorksWps4</b>	Microsoft Works WPS versions 4 and 5
<b>MsWorksWps6</b>	Microsoft Works WPS versions 6, 7, 8, and 9
<b>Multimate</b>	Multimate (any version)
<b>NoContent</b>	File indexed with all content ignored (see dtsolIndexBinaryNoContent)
<b>NonTextData</b>	Data file with no text to index

File type	Description
<b>OleDataMso</b>	oledata.mso file
<b>OneNote2003</b>	not supported
<b>OneNote2007</b>	OneNote 2007
<b>OneNote2010</b>	OneNote 2010, 2013, and 2016
<b>OneNoteOnline</b>	OneNote variant generated by Microsoft online services
<b>OpenOfficeDocument</b>	OpenOffice versions 1, 2, and 3 documents, spreadsheets, and presentations (*.sxc, *.sxd, *.sxi, *.sxw, *.sxg, *.stc, *.sti, *.stw, *.stm, *.odt, *.ott, *.odg, *.otg, *.odp, *.otp, *.ods, *.ots, *.odf) (includes OASIS Open Document Format for Office Applications)
<b>OutlookExpressMessage</b>	Message in an Outlook Express message store
<b>OutlookExpressMessageStore</b>	Outlook Express dbx archive (versions 7.67 and earlier)
<b>OutlookExpressMessageStore2</b>	Outlook Express dbx archive
<b>OutlookMsgAsContainer</b>	Outlook .MSG file processed as a container
<b>OutlookMsgFile</b>	Microsoft Outlook .MSG file
<b>OutlookPst</b>	Outlook PST message store
<b>PDF</b>	PDF
<b>PdfWithAttachments</b>	PDF file with attachments
<b>PfsProfessionalWrite</b>	PFS Professional Write file
<b>PhotoshopImage</b>	Photoshop Image (*.psd)
<b>PNG</b>	PNG image file
<b>PowerPoint</b>	PowerPoint 97-2003
<b>PowerPoint12</b>	PowerPoint 2007 and newer

File type	Description
<b>PowerPoint3</b>	PowerPoint 3
<b>PowerPoint4</b>	PowerPoint 4
<b>PowerPoint95</b>	PowerPoint 95
<b>Properties</b>	PropertySet stream in a Compound Document
<b>QuattroPro</b>	Quattro Pro 9 and newer
<b>QuattroPro8</b>	Quattro Pro 8 and older
<b>QuickTime</b>	QuickTime file
<b>RAR</b>	RAR archive
<b>RTF</b>	Microsoft Rich Text Format
<b>SASF</b>	SASF call center audio file
<b>SegmentedText</b>	Text segmented using File Segmentation Rules
<b>SingleByteText</b>	Single-byte text, encoding automatically detected
<b>SolidWorks</b>	SolidWorks file
<b>TAR</b>	TAR archive
<b>TIFF</b>	TIFF file
<b>TNEF</b>	Transport-neutral encapsulation format
<b>TreepadHjtFile</b>	TreePad file (HJT format in TreePad 6 and earlier)
<b>TrueTypeFont</b>	TrueType TTF file
<b>UnformattedHTML</b>	Output format only, for generating a synopsis that is HTML-encoded but that does not include formatting such as font settings, paragraph breaks, etc.
<b>Unicode</b>	UCS-16 text

File type	Description
<b>Unigraphics</b>	Unigraphics file (docfile format)
<b>Unigraphics2</b>	Unigraphics file (#UGC format)
<b>Utf8</b>	UTF-8 text
<b>Visio</b>	Visio file
<b>Visio2013</b>	Visio 2013 document
<b>VisioXml</b>	Visio XML file
<b>WAV</b>	WAV sound file
<b>WindowsExecutable</b>	Windows .exe or .dll
<b>WinWrite</b>	Windows Write
<b>WMF</b>	Windows Metafile Format (Win16)
<b>Word12</b>	Word 2007 and newer
<b>Word2003Xml</b>	Microsoft Word 2003 XML format
<b>WordForDos</b>	Word for DOS (same as Windows Write, it_WinWrite)
<b>WordForWin6</b>	Microsoft Word 6.0
<b>WordForWin97</b>	Word For Windows 97, 2000, XP, or 2003
<b>WordForWindows1</b>	Word for Windows 1
<b>WordForWindows2</b>	Word for Windows 2
<b>WordPerfect42</b>	WordPerfect 4.2
<b>WordPerfect5</b>	WordPerfect 5
<b>WordPerfect6</b>	WordPerfect 6

File type	Description
<b>WordPerfectEmbedded</b>	WordPerfect document embedded in another file
<b>WordStar</b>	WordStar through version 4
<b>WS_2000</b>	Wordstar 2000
<b>WS_5</b>	WordStar version 5 or 6
<b>WordList</b>	List of words in UTF-8 format, with the word ordinal in front of each word
<b>XBase</b>	XBase database
<b>XBaseAsDocument</b>	XBase file parsed as a single file listing all records
<b>XfaForm</b>	XFA form
<b>XML</b>	XML
<b>XPS</b>	XML Paper Specification (Metro)
<b>XyWrite</b>	XyWrite
<b>ZIP</b>	ZIP archive
<b>ZIP_zlib</b>	ZIP file parsed using zlib
<b>7z</b>	7-zip archive