FortiCASB - Admin Guide

Version 4.1.0

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE

https://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM

https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE

https://training.fortinet.com

FORTIGUARD CENTER

https://fortiguard.com/

END USER LICENSE AGREEMENT

https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdoc@fortinet.com

April 5, 2019
FortiCASB 4.1.0 Admin Guide
00-400-000000-20181031

TABLE OF CONTENTS

Change Log

Date	Change Description
04/05/2019	FortiCASB 4.1 Handbook release. Revised **Getting Started** documentation for Basic Setup and Install IAAS applications. Added documentations for **Topology**, **Resource**, **Resource Profile**, and **Traffic**. **Configuration** merged into **Risk Assessment .**
01/08/2019	FortiCASB 2.1 Handbook. First edition. Changing EU Users IP address from 52.59.74.73 or 18.195.109.67 to 34.254.217.50 or 52.18.7.98, in the section "Show IT discovery".

What's New

FortiCASB version 4.1 brings new and enhanced features listed below

FortiCASB 4.1 Release Highlights

- **Resource** - Added table of summary of all cloud resources in one place. See Resource on page 124 for further details.
- **Topology** - Added topological graph for virtual private network. See Topology on page 134 for further details.
- **Traffic** - Added graphical view for virtual machine cloud traffic. See Traffic on page 138 for further details.
- **Resource profile** - Added detail resource view for all virtual machine instances. See Resource Profile on page 128 for further details.
- **Security integration** - Added functionality to integrate security alerts from IAAS applications. See IAAS Security Integration on page 102 for further details.
- **Risk Assessment**- Merged All Resources and Customized Results from Configuration into single page, Risk Assessment also triggers alerts, which can be viewed in Alert page.
- **Policy** - Added network and integration policy configuration, also remediation feature added to policy page.
- **Alert filters** - Added new enhancement icons on Alert page to filter by categories such as Risk Assessment, Data Analysis, Threat Protection, Integration, etc.
- **Enhanced AWS monitoring** - FortiCASB monitoring has been enhanced. Update the AWS JSON policy to enable enhanced monitoring.
- **Group IPs** - Added functionality to group multiple IPs into one group and track them through IAAS cloud monitoring application.

Change Details

Amazon AWS JSON policy changes

FortiCASB version 4.1 enhances AWS monitoring of Route 53, EMR, S3, EC2, and EKS. The Amazon AWS JSON policy configuration used by FortiCASB has been updated. A table of changes is provided below for reference.

Service	Action	Access level:List	Access level: Read
Route 53	Replace	GetGeoLocations -> GetGeoLocation	

Route 53	Add		GetAccountLimit GetQueryLoggingConfig GetReusableDelegationSetLimit GetTrafficPolicy GetTrafficPolicyInstance GetTrafficPolicyInstanceCount ListTrafficPolicies ListTrafficPolicyInstances ListTrafficPolicyInstancesByHostedZone ListTrafficPolicyInstancesByPolicy ListTrafficPolicyVersions ListVPCAssociationAuthorizationsTestDNSAnswer
Route 53 Domains	Add		CheckDomainAvailability GetContactReachabilityStatus GetDomainSuggestions
EMR	Remove		DescribeJobFlows -> deprecated
EMR	Add		DescribeCluster DescribeEditor DescribeSecurityConfiguration DecribeStep
S3	Remove		GetIpConfiguration
S3	Add		GetAccountPublicAccessBlock GetEncryptionConfiguration
EC2	Add	GetTransitGatewayAttachmentPropagations GetTransitGatewayRouteTableAssociations GetTransitGatewayRouteTablePropagations SearchTransitGatewayRoutes	
EKS	Add	ListClusters ListUpdates	DescribeCluster DescribeUpdate

Follow the directions under **Getting Started > IAAS Applications > Amazon Web Services > Prerequisites on page 34** to use the updated policy.

Introduction

Welcome, and thank you for selecting FortiCASB for your cloud security and monitoring needs.

FortiCASB is Fortinet's cloud-native Cloud Access Security Broker (CASB) service, which provides visibility, compliance, data security, and threat protection for cloud-based services. Using direct API access, FortiCASB enables deep inspection and policy management for data stored in cloud application platforms. It also provides detailed user analytics and management tools to ensure that policies are enforced and that your organization’s data is secure.

FortiCASB works by focusing on Gartner's four pillars of security: visibility, compliance, data security, and threat protection.

- **Visibility**—Visibility is one of the most important aspects of cloud security. FortiCASB uses a series of methods such as data scans and analytics to answer the questions: who accessed information, what was accessed, when it was accessed, and from where did the access originate.
- **Compliance**—FortiCASB provides file content monitoring to find and report on regulated data in the cloud.
- **Data security**—FortiCASB runs scans to check for sensitive data, such as social security numbers or credit card numbers. It then classifies this data under different levels of sensitivity and sends different alerts depending on the sensitivity level of the data accessed.
- **Threat protection**—FortiCASB uses User Entity Behavior Analytics to watch for suspicious or irregular user behavior. It also sends out alerts for malicious behavior.

Features

FortiCASB comes with a series of features that give you visibility of data access and usage, control over data security and threat protection, and peace of mind over compliance with standards and federal regulations.

Visibility

- **Automatic on-demand data scan**—FortiCASB examines existing content in all folders to identify sensitive data subjects or security policies.
- **Cloud usage analytics**— FortiCASB visually summarizes key usage statistics, including trends over different time periods as well as drilldown, access count, and usage over time.
- **User entitlements review**— FortiCASB gives visibility of privileged users, dormant users, and external users.
- **File exposure**— FortiCASB highlights the most shared files overall, as well as each user's most shared files.

Data security and threat protection

- **Cloud data loss prevention**— FortiCASB enforces DLP policies based on data identifiers, keywords, and regular expressions for data both at rest and in traffic.
- **Threat detection**—FortiCASB offers an abundant number of out-of-the-box policies to immediately detect account-centric threats.
- **Malware detection**— FortiCASB features a malware detection policy to detect malicious files before they compromise sensitive data.
- **Geo-location analytics**—FortiCASB visualizes global access patterns and analyzes activity to identify unlikely cross-region access attempts indicative of compromised accounts.
- **Shadow IT discovery** — FortiCASB offers an overview of unsanctioned cloud applications used in the organization and gives users the ability to control application usage.
- **Configuration assessment** —FortiCASB offers an large number of out-of-the-box policies for automated validation of best security practices against the resources on your IaaS platform account.

Compliance

- **Predefined compliance policies**—FortiCASB provides predefined compliance policies designed to help maintain compliance with ISO 270001, NIST 800-53 V4, and NIST 800-171 regulations.
- **Compliance report**—FortiCASB can produce compliance reports for audit purposes. These reports show compliance with ISO 270001, NIST 800-53 V4, and NIST 800-171 regulations.

Getting Started

This chapter provides the procedures for getting started with FortiCASB.

To fully set up FortiCASB, you must do the following:

- Adding companies, business units, and users on page 11.
- Installing IAAS applications on page 33.
- Installing SAAS applications on page 19

Adding companies, business units, and users

FortiCASB account permissions can have one of three levels:

- Administrator—Administrators have full permissions, including the ability to create/access/assign companies and organizations.
- Sub-user with full access—Sub-users from Forticare who have been granted full access also have full permissions, including the ability to create/access/assign companies and organizations.
- Sub-user with limited access—Sub-users from Forticare who have been granted limited access can only view companies they are a part of.

If you are an administrator, continue below.

If you are a user with limited access, not an administrator in charge of setup or a user with full access, skip to the user section.

FortiCASB requires different setup procedures, depending on your organization's hierarchy and needs. A company with a branched hierarchy, such as a company with multiple branch offices or a compartmentalized organizational structure, will have different requirements than a company with only one unified office.

To set up your FortiCASB, you or your organization must have the following in place:

- A valid FortiCASB license. Contact your primary Fortinet Service Provider to obtain a license if you do not already have one.
- An administrator with a Master FortiCare account to add your company, business units, and users in FortiCASB.

In accordance with European Union laws and regulations, all data that FortiCASB collected for European Union (EU) companies must be located in the EU region. To accommodate for this, you can choose to host your CASB cloud service either on the Global site or the EU site.

1. Open your web browser, and go to https://www.forticasb.com/
2. Click **Login**.

You will be redirected to the Fortinet single sign-on webpage.

3. Log into your admin account, or create a new admin account if you do not already have one.
4. Log into your account.
5. FortiCASB account selection page, select an account. (if applicable)

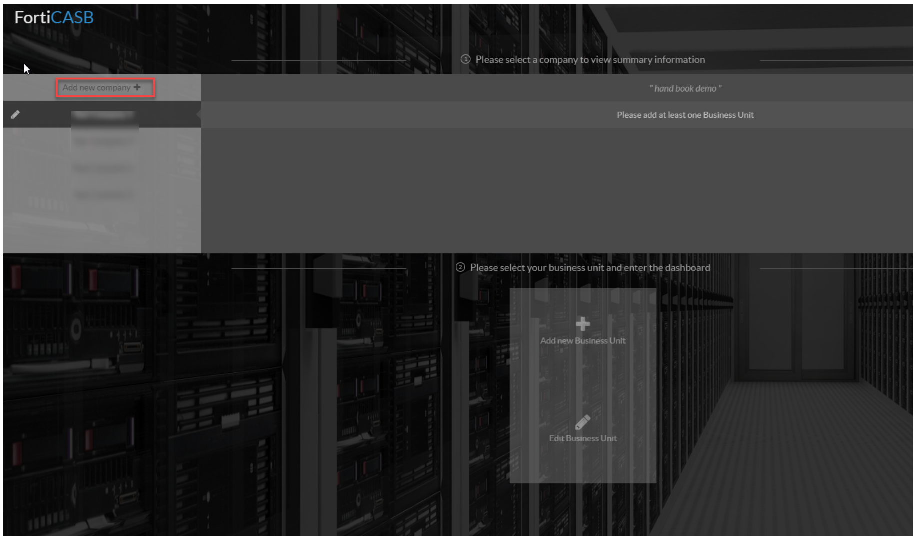
You are now redirected to FortiCASB's company selection page.

If you have a pop-up blocker, it will block the FortiCASB GUI.
Set an exception for the FortiCASB GUI, or open the GUI manually.

Add companies

After selecting a region, the company selection screen will be displayed.

1. Log into FortiCASB: https://www.forticasb.com with your Master FortiCARE account.
2. Once logged in, **Company/Business unit Management dashboard** will appear.
3. Click on **+Add new company** in the left hand side.



Please select a company to view summary information

" hand book demo "

Please add at least one Business Unit

Please select your business unit and enter the dashboard

4. Specify a unique company name, and add a brief description. Then click on **Add Asset**.

Assign a license

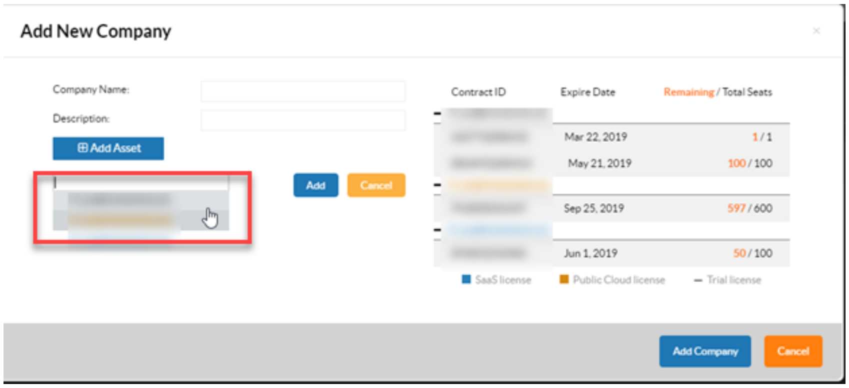
There are two concepts associated with licenses:

- **Contract**—This is the basic license unit. A license contains at least one contract.
- **Seat**—Each contract contains a specific number of seats. The number of seats represents the number of users a contract supports.

There are two types of licenses: a SaaS License and a Public Cloud (IaaS) License:

- **SaaS License**—Each cloud application user consumes one seat in a contract. For example, if your Microsoft® Office Office 365 account contains 50 users, you have to assign at least 50 seats to its organization.
- **Public Cloud (IaaS) License**—Each cloud application consumes one seat, no limitation on the number of users.

5. Click on the search bar and select the desired license (SaaS or Public Cloud), then click **Add**.



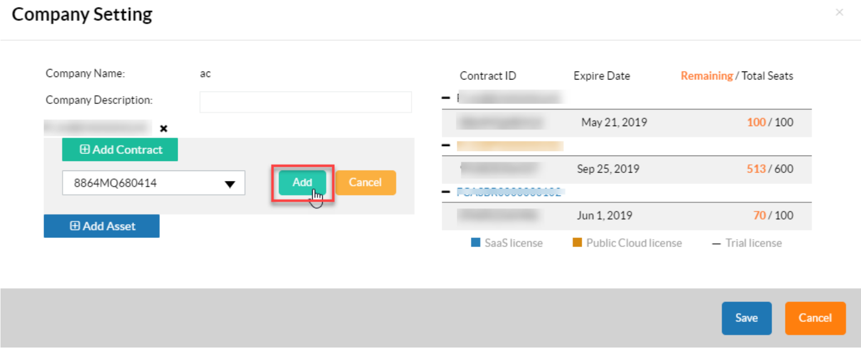
Add New Company

Company Name:

Description:

Contract ID	Expire Date	Remaining / Total Seats
	Mar 22, 2019	1 / 1
	May 21, 2019	100 / 100
	Sep 25, 2019	597 / 600
	Jun 1, 2019	50 / 100

6. Click on drop down menu and select the contract associated with the license, then click **Add**.



Company Setting

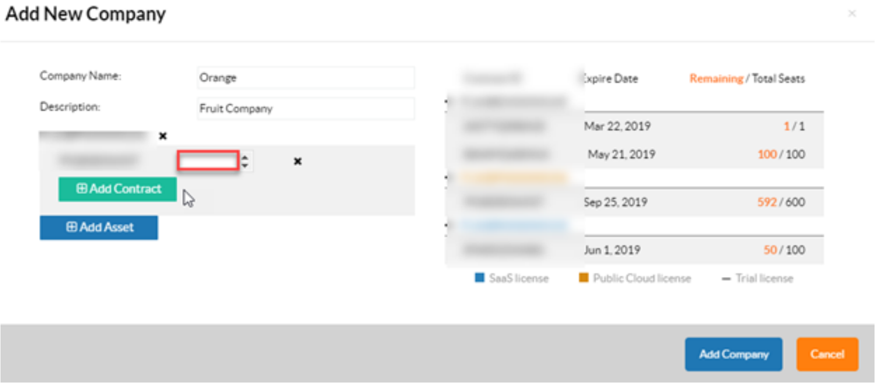
Company Name: ac

Company Description:

8864MQ680414

Contract ID	Expire Date	Remaining / Total Seats
	May 21, 2019	100 / 100
	Sep 25, 2019	513 / 600
	Jun 1, 2019	70 / 100

7. Enter the number of seats you want to assign to this company.



Add New Company

Company Name: Orange

Description: Fruit Company

	xpire Date	Remaining / Total Seats
	Mar 22, 2019	1 / 1
	May 21, 2019	100 / 100
	Sep 25, 2019	592 / 600
	Jun 1, 2019	50 / 100

2

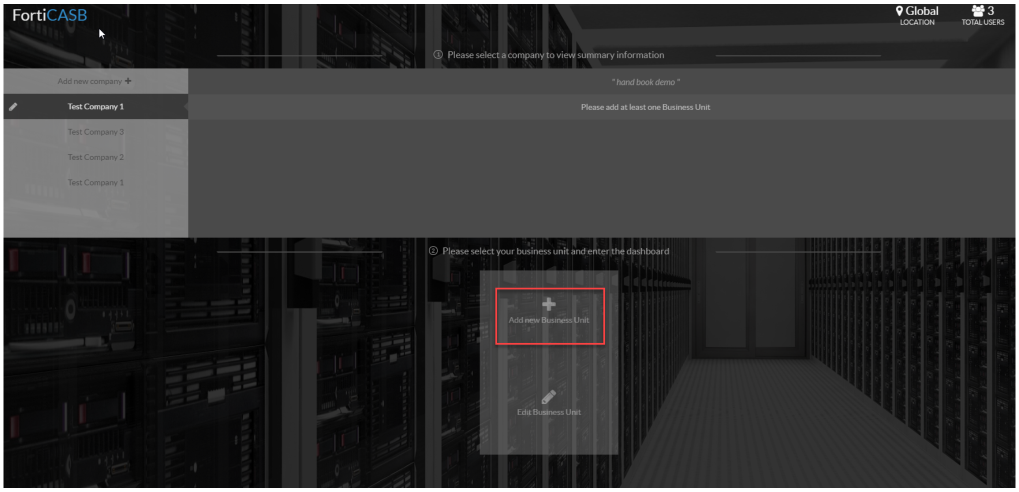
8. To add other license/seat, click on **Add Asset** to add other license/seat.
9. Click on **Add Company** to complete creating new company.
   Repeat this process to add additional companies if applicable.

Note: You can always go back to edit the company setting by clicking on **edit button** ✎ next to the company on the dash board.

Add business units

After creating a company, log into FortiCASB to add a business unit for the company following these steps:

1. Log into FortiCASB: https://www.forticasb.com with Master FortiCARE account.
2. Click on **+Add new Business unit** from dash board.



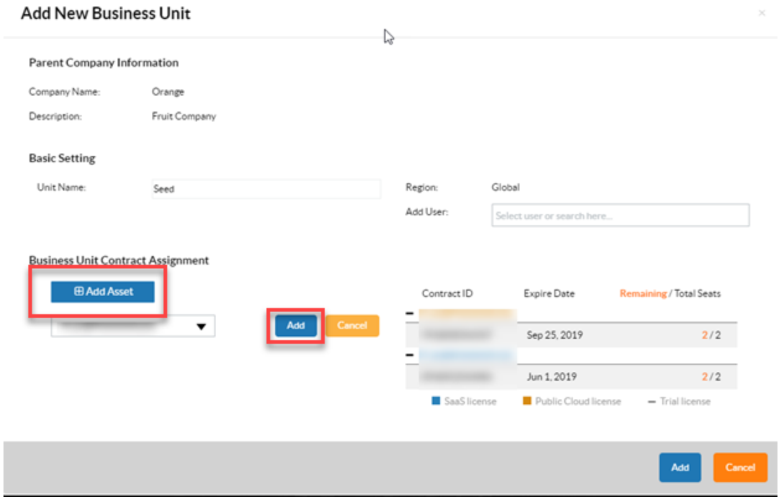
① Please select a company to view summary information

" hand book demo "

Please add at least one Business Unit

② Please select your business unit and enter the dashboard

3. Under **Basic Setting**, enter a unique **Business Unit Name** based on your preference.
4. Click on **Add Asset** button under **Business Unit Contract Assignment**, then choose SaaS license or Public Cloud license from the drop down menu, then click **Add**.



Add New Business Unit

Parent Company Information

Company Name: Orange

Description: Fruit Company

Basic Setting

Unit Name: Seed

Region: Global

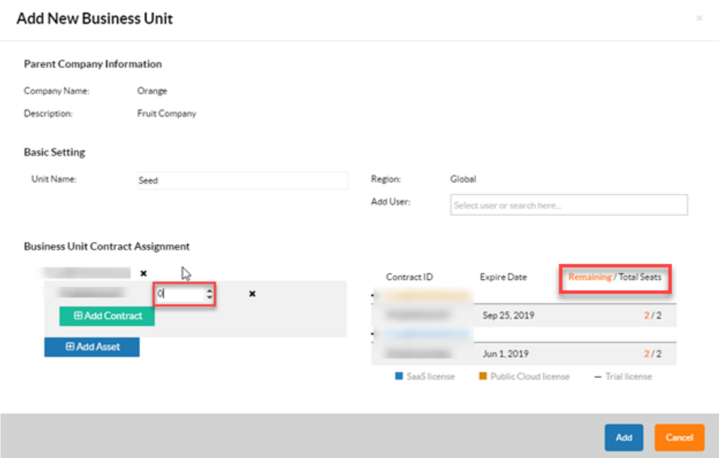
Add User: Select user or search here...

Business Unit Contract Assignment

Contract ID	Expire Date	Remaining / Total Seats
[redacted]	Sep 25, 2019	2 / 2
[redacted]	Jun 1, 2019	2 / 2

■ SaaS license ■ Public Cloud license — Trial license

5. Click on **Add** next to the license selected assign seat.
6. Assign the number of seats you would like to allocate from the company to the business unit.



Add New Business Unit

Parent Company Information

Company Name: Orange

Description: Fruit Company

Basic Setting

Unit Name: Seed

Region: Global

Add User: Select user or search here...

Business Unit Contract Assignment

[redacted] ✖

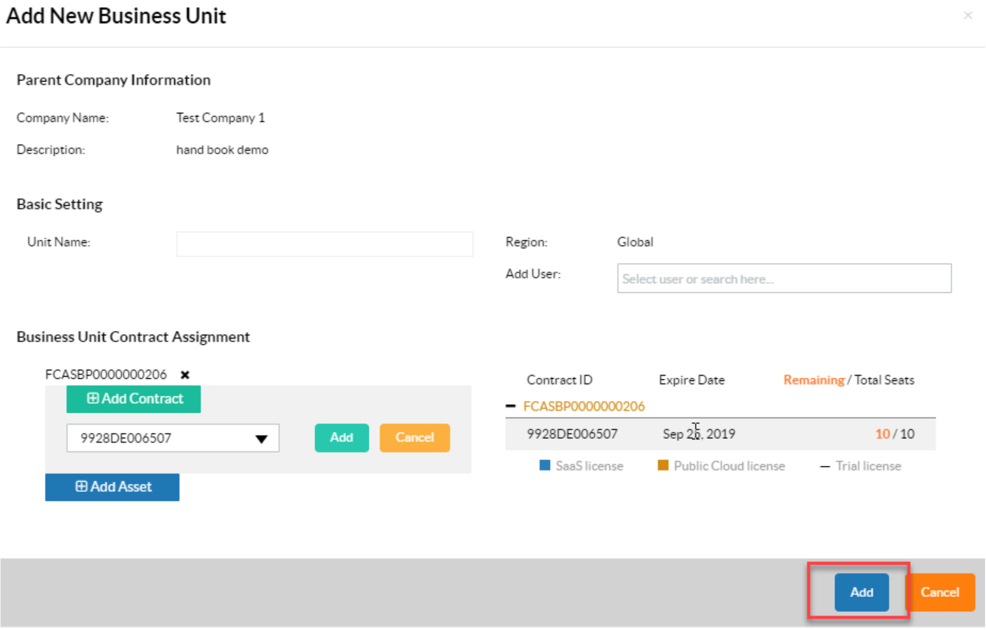
[redacted] 0 ✖

Contract ID	Expire Date	Remaining / Total Seats
[redacted]		
[redacted]	Sep 25, 2019	2 / 2
[redacted]		
[redacted]	Jun 1, 2019	2 / 2

■ SaaS license ■ Public Cloud license — Trial license

Note: The total number of seats available for each license is at the right hand side in the **Remaining/Total Seats** column.

7. Click **Add Asset** and repeat step 5-7 If you want to add other license/seat to the business unit.
8. Once you are done, click on **Add** to complete adding new business unit.



Add New Business Unit

Parent Company Information

Company Name: Test Company 1

Description: hand book demo

Basic Setting

Unit Name:

Region: Global

Add User: Select user or search here...

Business Unit Contract Assignment

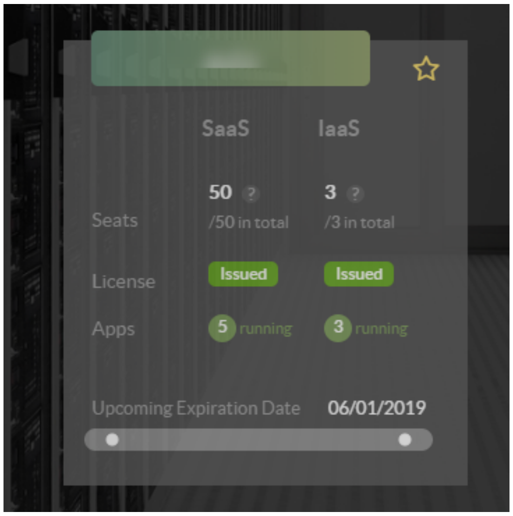
FCASBP0000000206 ✖

9928DE006507 ▼

Contract ID	Expire Date	Remaining / Total Seats
— FCASBP0000000206		
9928DE006507	Sep 26, 2019	10 / 10

■ SaaS license ■ Public Cloud license — Trial license

The new business unit will be shown in the company dashboard with the number of seats assigned to SaaS or IaaS license.



	SaaS	IaaS
Seats	50 ? /50 in total	3 ? /3 in total
License	Issued	Issued
Apps	5 running	3 running

Upcoming Expiration Date 06/01/2019

Repeat this process to add additional business units if applicable.

Sub-user Creation

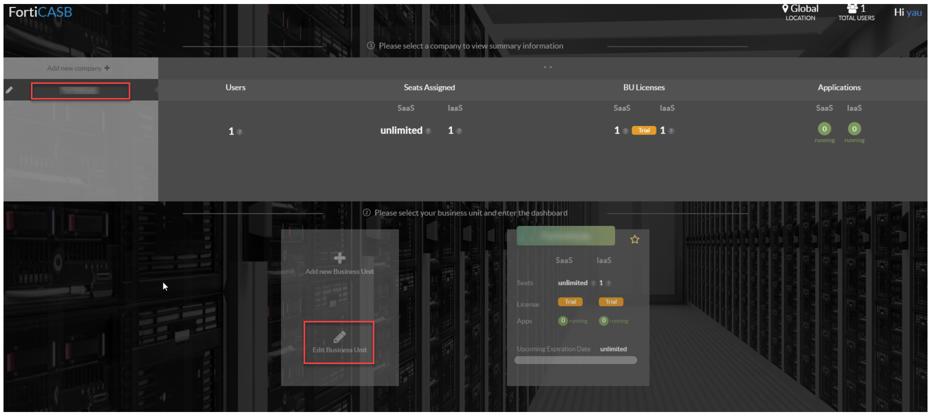
Sub-users can be created to add to the business unit. A FortiCare master account owner can create sub-user account and add the sub-user to the company and the business units in FortiCASB. To create sub-user, follow these steps:

1. Log into FortiCARE: https://support.fortinet.com/Main.aspx.
2. Click on **account management button** in the upper right corner:
3. Click on **Mange User** at the left hand side, then list of users will display.
4. Click on **add user button** on the right hand side:
5. Fill in the **user name**, **e-mail address**, and **phone number** for the sub-user you would like to set up. Select **Full Access** to grant sub-user to have full permissions, including the ability to create/access/assign companies and business units. Select **Limited Access** to only grant the sub-user basic access. Then click **Save**.
6. If **Limited Access** is selected, click on **Add More Products** to select a license.
7. Click **Save**.
   Repeat this process to add more sub-users.

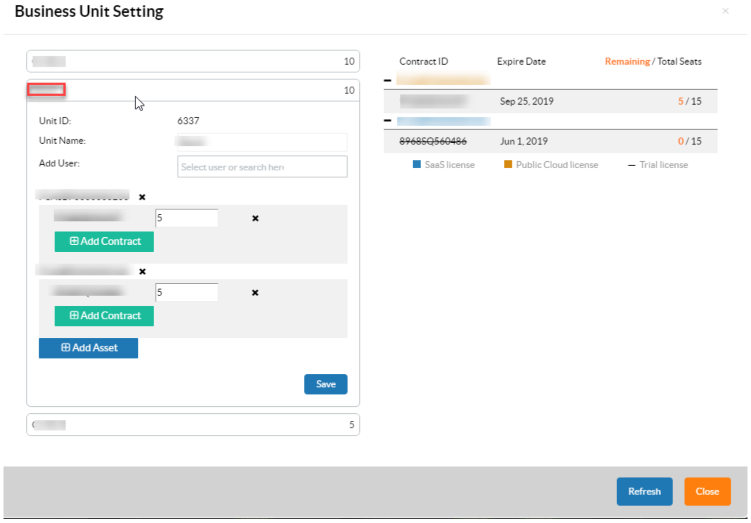
Add users to business unit

FortiCARE Master account holder or full access users can add sub-users to business units.

1. Log into FortiCASB: https://www.forticasb.com with your master FortiCARE account.
2. Select the company at the left hand side, then click on the **Edit Business Unit** at the bottom.



3. If there are multiple business units in the same company, select the business unit you want to add users.



Business Unit Setting

[redacted] 10

[redacted] 10

Unit ID: 6337

Unit Name: [redacted]

Add User: Select user or search here

[redacted] ✖

[redacted] 5 ✖

⊞ Add Contract

[redacted] ✖

[redacted] 5 ✖

⊞ Add Contract

⊞ Add Asset

Save

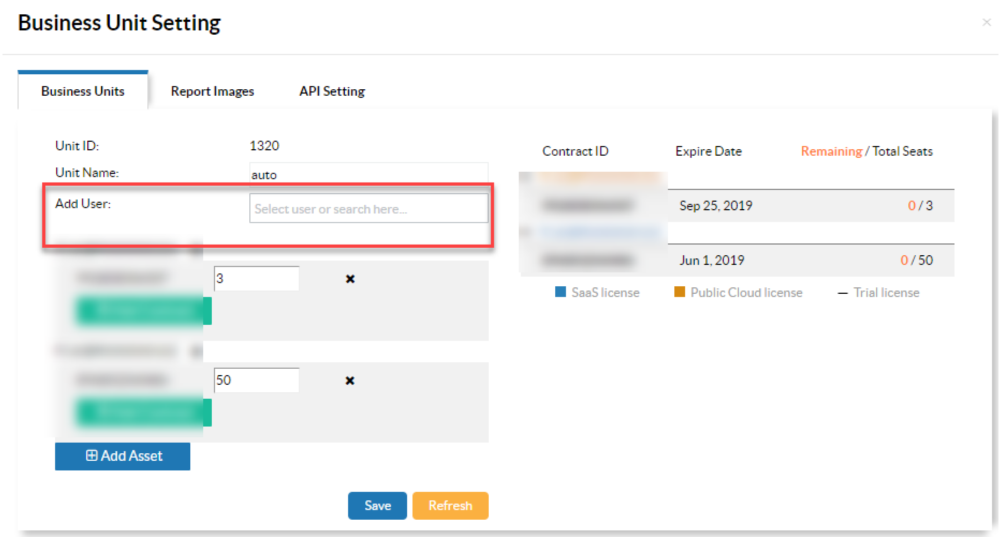
[redacted] 5

Contract ID	Expire Date	Remaining / Total Seats
[redacted]	Sep 25, 2019	5 / 15
~~8968SQ560486~~	Jun 1, 2019	0 / 15

■ SaaS license ■ Public Cloud license — Trial license

Refresh Close

4. In **Add User** field, begin typing user's e-mail address, then select the user.



Business Unit Setting

Unit ID: 1320

Unit Name: auto

Add User: Select user or search here...

[redacted] 3 ×

[redacted] 50 ×

Contract ID	Expire Date	Remaining / Total Seats
[redacted]	Sep 25, 2019	0 / 3
[redacted]	Jun 1, 2019	0 / 50

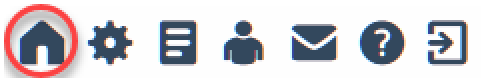
🟦 SaaS license 🟧 Public Cloud license — Trial license

5. Click **Save**. Now the user can log into the business unit with their account. Repeat this process for each user.

Log in as a user

1. Go to www.forticasb.com.
2. Click **Login**.
3. Enter your credentials, and then select a FortiCASB user account (if applicable).
4. Select your company and business unit.

You will be brought to the FortiCASB dashboard. Click on the ⌂ **Switch Company** icon to switch organizations, if applicable.



If your account hasn't been assigned to a business unit, an error message will appear. Please contact your administrator with Master FortiCare account to add you into the business unit.

Install SAAS Applications

Installing SAAS applications

Both administrators and users can add SaaS applications to a company. Once added, everyone in the company can see the application.

Box

FortiCASB offers an API-based approach, pulling data directly from Box via RESTful API. Authentication is done through OAUth2.0. FortiCASB uses an access token for API queries.

Prerequisites

To use API access, your organization must be using one of the following editions (the API is enabled by default):

- Business Edition
- Enterprise Edition
- Developer Edition

The user account installed in FortiCASB must have the following permissions:

- Read and write all files and folders stored in Box
- Manage users
- Manage groups
- Manage enterprise properties

You may either use an existing account or create a new account. If you create a new account, wait at least 24 hours for the new account to take effect before granting access to FortiCASB.

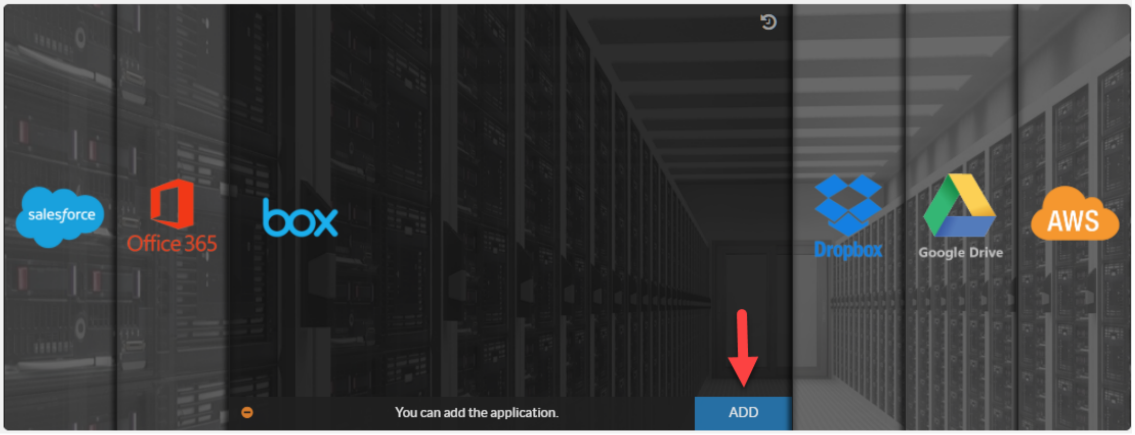
The following features require "Admin User" permission as well:

- User login tracking
- User IP address tracking
- Geographical location tracking
- User password change tracking
- Change admin role tracking

Without "Admin User" permissions, FortiCASB cannot obtain user login IPs. Therefore, any user activity will not appear on the Activity map.

Installation

1. From the menu on the left-hand side, select **Overview > Dashboard**.
2. From the Cloud App Status widget, click **ADD**, located next to Box.



You can add the application.

3. Click **OK**.
   You will be navigated to the Box website for authentication.

4. Log in to authenticate.
   Box will prompt you to allow or deny access.

5. Click **Allow** to grant FortiCASB permissions to monitor your Box application.

After you click Allow, you will be redirected back to the FortiCASB dashboard.

You can check the installation result and SaaS platform monitoring status in the Box dashboard.

For more information on common installation issues, see Troubleshooting on page 144.

Dropbox Business

FortiCASB offers an API-based approach, pulling data directly from Box via RESTful API. Authentication is done through OAUth2.0. FortiCASB uses an access token for API queries.

Prerequisites

To use API access, your organization must be using one of the following Dropbox Business plans:

- Standard Plan
- Advanced Plan
- Enterprise Plan

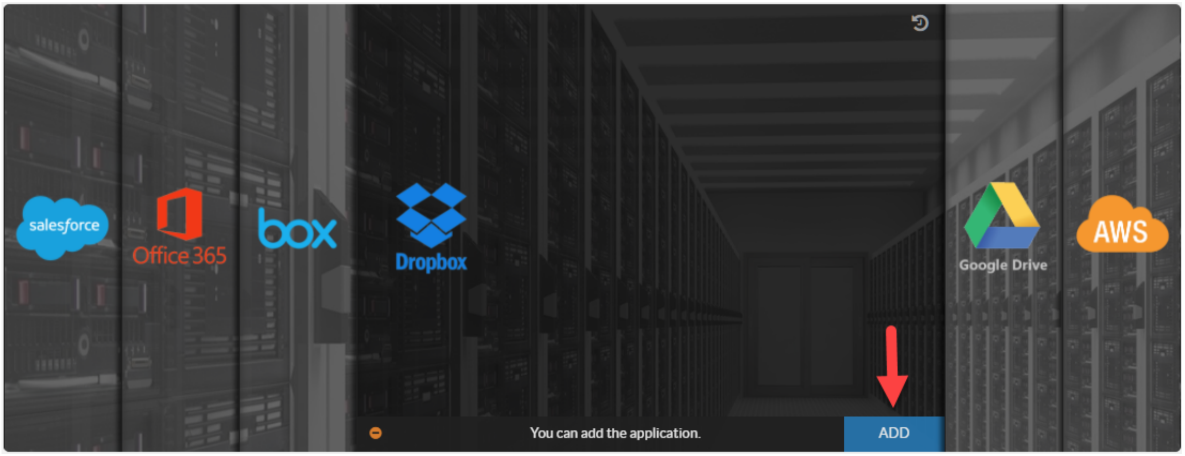
The user account installed in FortiCASB must have the following permission:

- Team Admin

You may either use an existing account or create a new account.

Installation

1. From the menu on the left-hand side, select **Overview > Dashboard.**
2. From the Cloud App Status widget, click **ADD**, located next to Dropbox.



3. Click **OK.**You will be navigated to the Dropbox website for authentication.
4. Log in to authenticate. Dropbox will prompt you to allow or deny access.
5. Click **Allow** to grant FortiCASB permissions to monitor your Dropbox application.

After you click Allow, you will be redirected back to the FortiCASB dashboard.

You can check the installation result and SaaS platform monitoring status in the Dropbox dashboard.

For more information on common installation issues, see Troubleshooting on page 144

Google Drive

FortiCASB offers an API-based approach, pulling data directly from Google Drive via RESTful API. Authentication is done through OAUth2.0. FortiCASB uses an access token for API queries.

Prerequisites

To use API access, your organization must be using one of the following editions (the API is enabled by default):

- Business Edition
- Enterprise Edition

The user account installed in FortiCASB must be a Super Administrator in your G suite account. For steps on how to check if your account is a Super Adminstrator, see Google Drive connection errors on page 153.

Due to Google requirements, only G Suite accounts with a business or enterprise license can use FortiCASB. G suite accounts with a basic license will be unable to use FortiCASB.

You may either use an existing account or create a new account. Wait at least 24 hours for the new account to take effect before granting access to FortiCASB.

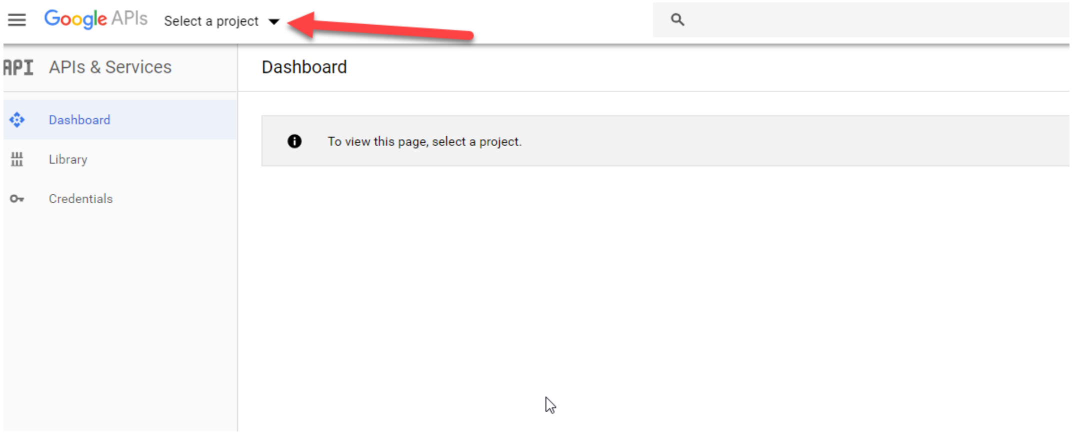
Make sure you create a **service account** for the G Suite account that will be linked to FortiCASB. A service account delegated with **domain-wide authority** is necessary for FortiCASB to visit files in both personal and team drives under your G Suite account.

Without the service account, you can still use FortiCASB. However, the features related to files in FortiCASB, such as Discovery, will not work.

For more information regarding service accounts and domain-wide authority delegation, go to: https://developers.google.com/identity/protocols/OAuth2ServiceAccount#delegatingauthority

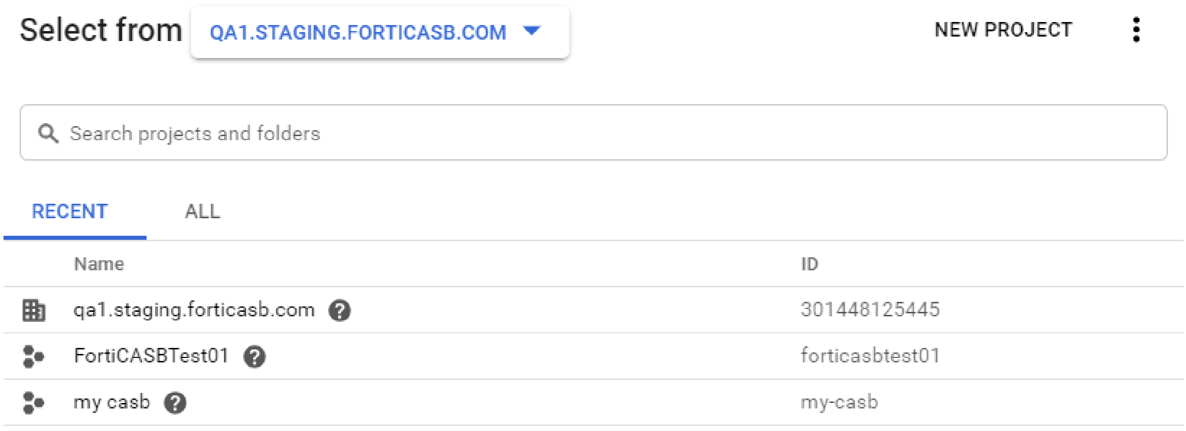
Create Service Google Service Account

1. Go to https://console.developers.google.com and log in with your Google Account.
2. Click on the drop-down menu of **Select a project.**



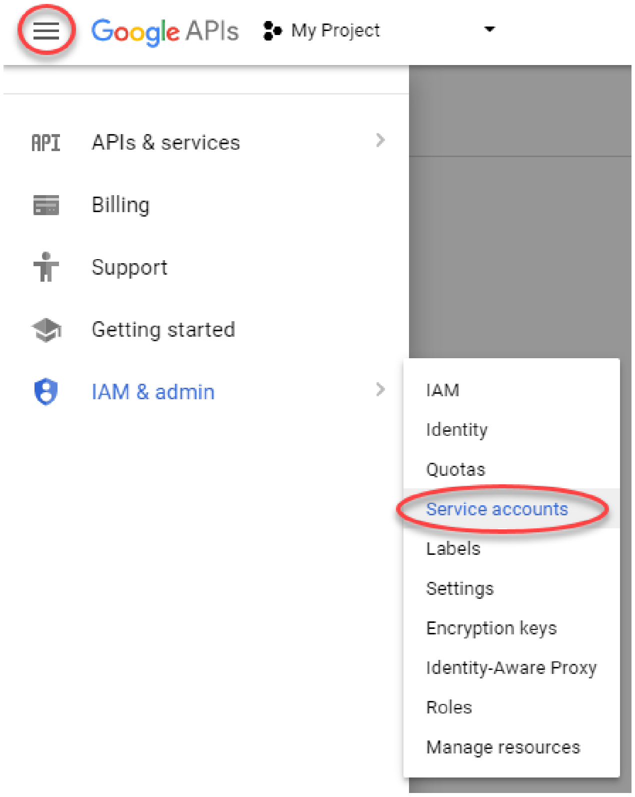
To view this page, select a project.

3. Select an existing project or Create New Project by clicking **New Project**.



Name	ID
qa1.staging.forticasb.com	301448125445
FortiCASBTest01	forticasbtest01
my casb	my-casb

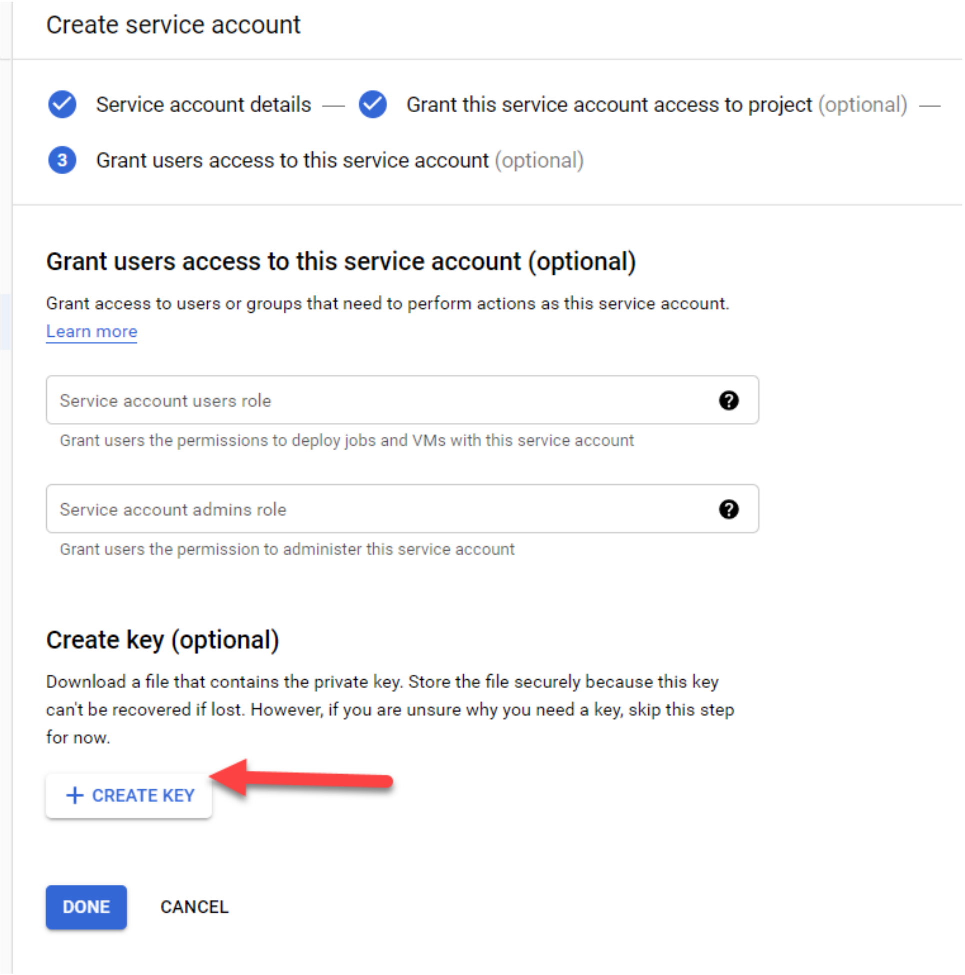
4. Enter a Project Name and click **Create.**
5. Once a project is created, from the **Navigation menu**, go to **IAM & admin > Service accounts**.



6. Click **+Create service account.**
7. Enter a "Service account name" of your preference and click **create**. Service account ID will populate automatically.

Keep the service account ID later for Google drive authentication during installation.

8. Click **Continue** when prompted for entering service account permissions.
9. Click on **+Create Key** and select P12 to create a private key. The P12 private key will be downloaded automatically, then click **Done**.



Create service account

Service account details — Grant this service account access to project (optional) —
3 Grant users access to this service account (optional)

Grant users access to this service account (optional)

Grant access to users or groups that need to perform actions as this service account.
Learn more

Service account users role
Grant users the permissions to deploy jobs and VMs with this service account

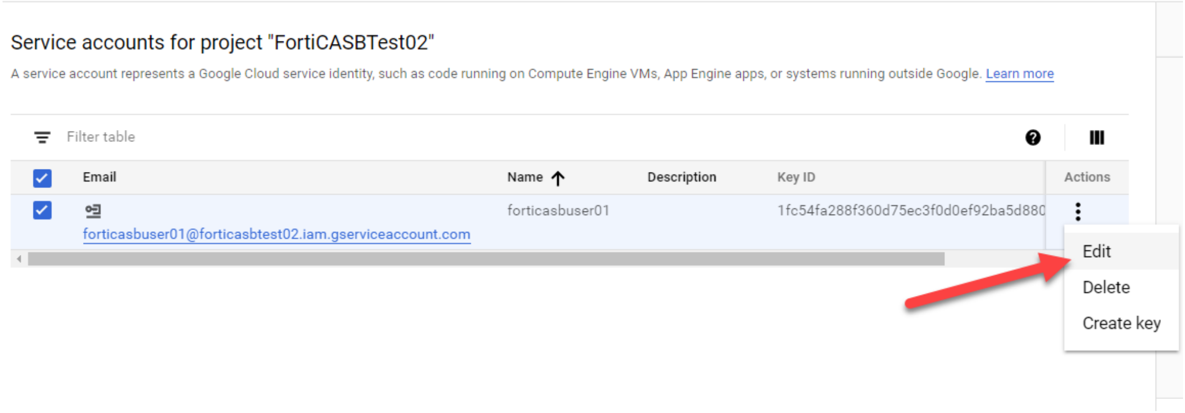
Service account admins role
Grant users the permission to administer this service account

Create key (optional)

Download a file that contains the private key. Store the file securely because this key can't be recovered if lost. However, if you are unsure why you need a key, skip this step for now.

Keep the private key later for Google drive authentication during installation.

10. Once service account is created, select the service account created and click on ⋮ under **Actions** on the right-hand side, then click on **Edit**.



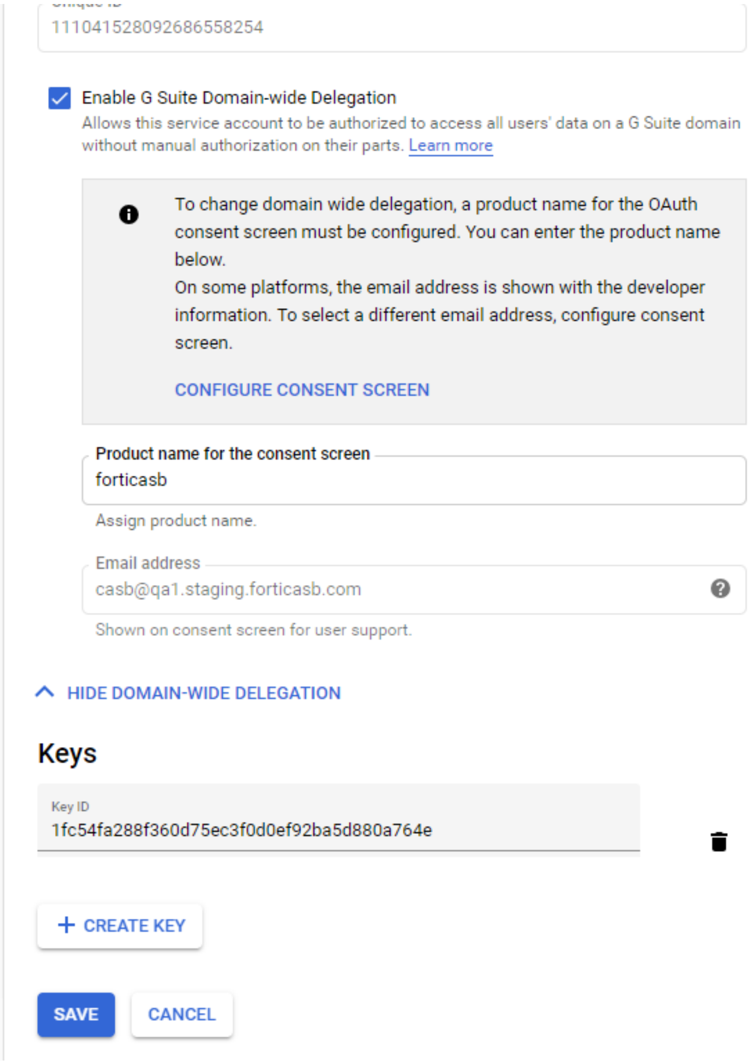
Service accounts for project "FortiCASBTest02"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. Learn more

Filter table

☑	Email	Name ↑	Description	Key ID	Actions
☑	forticasbuser01@forticasbtest02.iam.gserviceaccount.com	forticasbuser01		1fc54fa288f360d75ec3f0d0ef92ba5d880	⋮

11. Enable **G Suite Domain-wide Delegation** and enter in a **Product name for the consent screen**, then click **Save.**



111041528092686558254

☑ Enable G Suite Domain-wide Delegation

Allows this service account to be authorized to access all users' data on a G Suite domain without manual authorization on their parts. Learn more

To change domain wide delegation, a product name for the OAuth consent screen must be configured. You can enter the product name below.
On some platforms, the email address is shown with the developer information. To select a different email address, configure consent screen.

CONFIGURE CONSENT SCREEN

Product name for the consent screen: forticasb

Assign product name.

Email address: casb@qa1.staging.forticasb.com

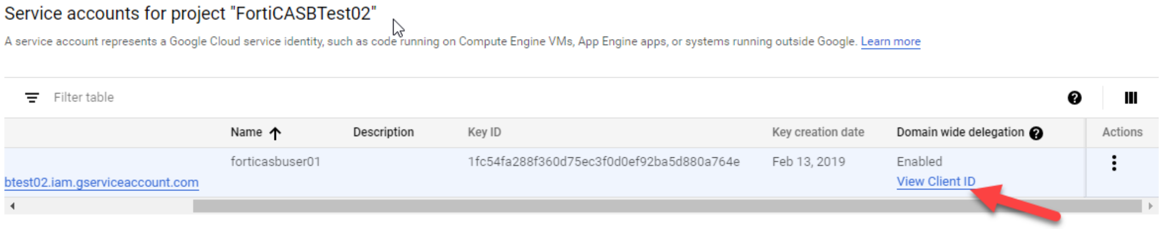
Shown on consent screen for user support.

HIDE DOMAIN-WIDE DELEGATION

Keys

Key ID: 1fc54fa288f360d75ec3f0d0ef92ba5d880a764e

12. Select **View Client ID** from service account that was created, and record down the client ID.



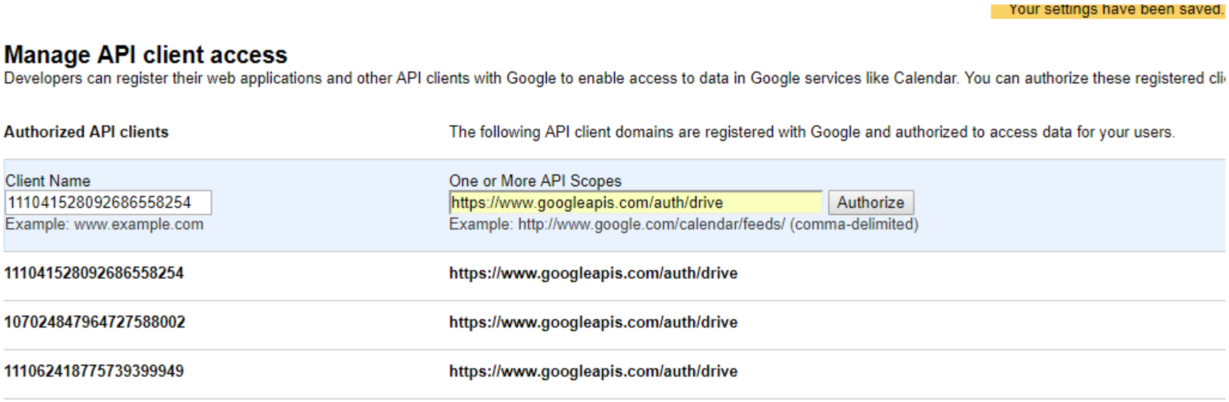
Service accounts for project "FortiCASBTest02"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. Learn more

	Name	Description	Key ID	Key creation date	Domain wide delegation	Actions
btest02.iam.gserviceaccount.com	forticasbuser01		1fc54fa288f360d75ec3f0d0ef92ba5d880a764e	Feb 13, 2019	Enabled View Client ID	⋮

Enable Google Drive API & authorize client ID

1. Go to **Navigation Menu > APIs & Services > Dashboard.**
2. Click on **ENABLE APIS AND SERVICES**.
3. Search for the **Google Drive API** and enable it.
4. Go to https://admin.google.com and log in with the same Google Account.
5. Scroll down and click on **More Controls.**
6. Go to **Security > Advanced Settings.**
7. Click **Manage API client access.**
8. Enter in the Client ID recorded earlier for **Client Name** and **https://www.googleapis.com/auth/drive** for **One or More API Scopes**. Your Client ID should be a string of numbers. Then click **Authorize**.



Your settings have been saved.

Manage API client access

Developers can register their web applications and other API clients with Google to enable access to data in Google services like Calendar. You can authorize these registered cli

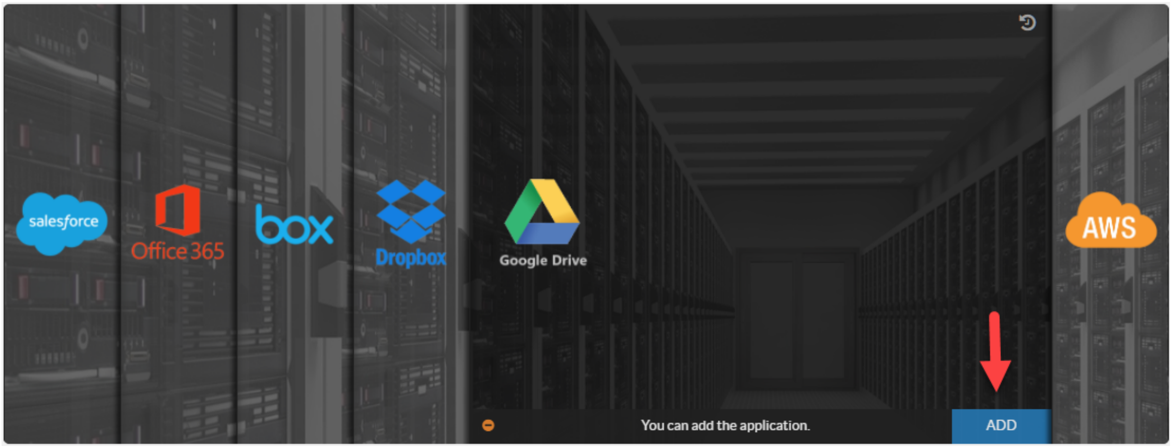
Authorized API clients

The following API client domains are registered with Google and authorized to access data for your users.

Client Name 111041528092686558254 Example: www.example.com	One or More API Scopes https://www.googleapis.com/auth/drive Authorize Example: http://www.google.com/calendar/feeds/ (comma-delimited)
111041528092686558254	**https://www.googleapis.com/auth/drive**
107024847964727588002	**https://www.googleapis.com/auth/drive**
111062418775739399949	**https://www.googleapis.com/auth/drive**

Installation

1. From the menu on the left-hand side, select **Overview > Dashboard**.
2. From the Cloud App Status widget, click **ADD**, located next to Google Drive.



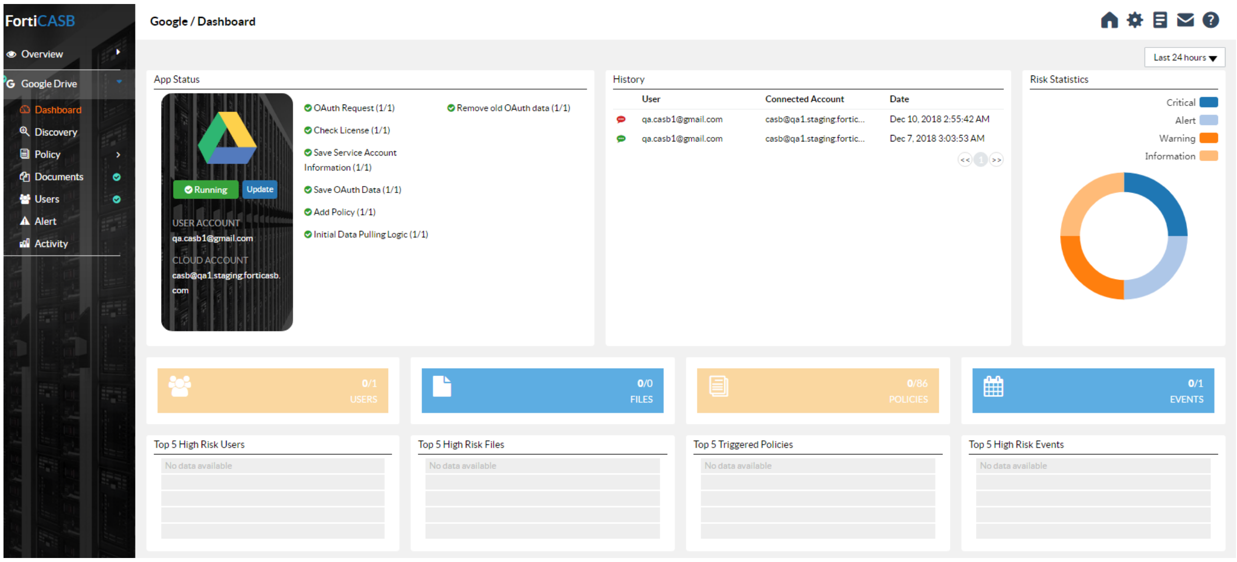
You can add the application.

3. Upload the **service account ID** and **Private Key (P12 File)** from earlier for the G suite account. Your service account ID should end in ".gserviceaccount.com".
4. Click **OK.**

   You will be navigated to the Google website for authentication. Make sure to use the same G suite account for authentication.

   If you have a custom Google domain, enter it here.
5. Log in to authenticate. Google will prompt you to allow or deny access.
6. Click **Allow** to grant FortiCASB permission to monitor your Google application.

You will be redirected back to the FortiCASB dashboard. You can check the installation result and SaaS platform monitoring status in the Google Drive dashboard.



✓ OAuth Request (1/1)
✓ Check License (1/1)
✓ Save Service Account Information (1/1)
✓ Save OAuth Data (1/1)
✓ Add Policy (1/1)
✓ Initial Data Pulling Logic (1/1)
✓ Remove old OAuth data (1/1)

USER ACCOUNT
qa.casb1@gmail.com

CLOUD ACCOUNT
casb@qa1.staging.forticasb.com

	User	Connected Account	Date
	qa.casb1@gmail.com	casb@qa1.staging.fortic...	Dec 10, 2018 2:55:42 AM
	qa.casb1@gmail.com	casb@qa1.staging.fortic...	Dec 7, 2018 3:03:53 AM

Top 5 High Risk Users

No data available

Top 5 High Risk Files

No data available

Top 5 Triggered Policies

No data available

Top 5 High Risk Events

No data available

Office 365

FortiCASB offers an API-based approach. It monitors Office 365 activity by using web notification and by pulling data directly from Office 365 via RESTful API. Authentication is done through OAUth2.0. FortiCASB uses an access token for API queries.

Prerequisites

You may use an existing account or create a new account. If you create a new account, wait for at least 24 hours for the new account to take effect before granting access to FortiCASB.

Make sure your role is "Global Administrator" and that you have the AzureAD "Premium P2" license. Without the AzureAD "Premium P2" license, FortiCASB's Discovery feature cannot see user entitlements. All other functions will not be affected. For more information on how to obtain this license, go to:

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-get-started-premium

You will also need to set up the AzureAD Privileged Identity Management application. For more information on how to do so, go to:

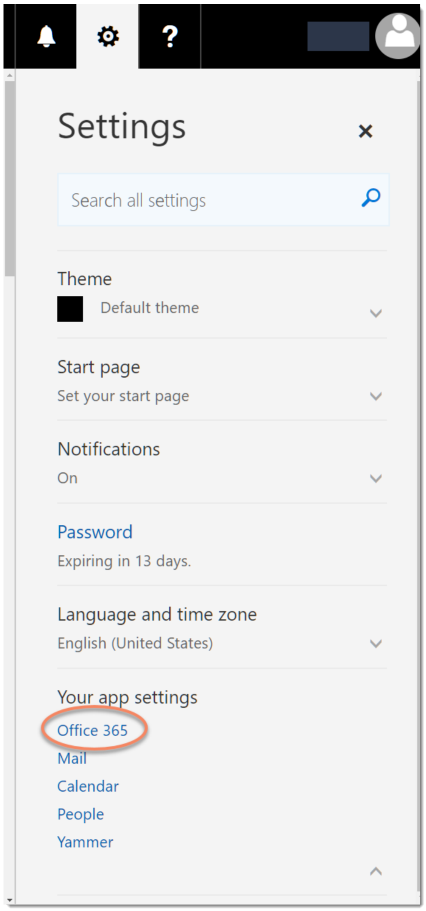
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure.

Make sure your license plan includes Active Directory integration. FortiCASB requires Active Directory support for most of its features. The following Office 365 licenses support Active Directory integration:

- Office 365 Business
- Office 365 Business Essentials
- Office 365 Business Premium
- Office 365 ProPlus
- Office 365 Enterprise E1
- Office 365 Enterprise E3
- Office 365 Enterprise E5
- Office 365 Enterprise K1

To determine what Office 365 license you have, follow the steps below:

1. Log into Office 365 account: https://www.office.com/.
2. Click on Apps button ⠿, located on the top-left corner of your Office 365 home screen.
3. Select **Admin**.
4. Click the Settings button ⚙, located on the top-right corner of your Office 365 admin center.
5. Click **Office 365**, located under "Your app settings".



Theme
Default theme

Start page
Set your start page

Notifications
On

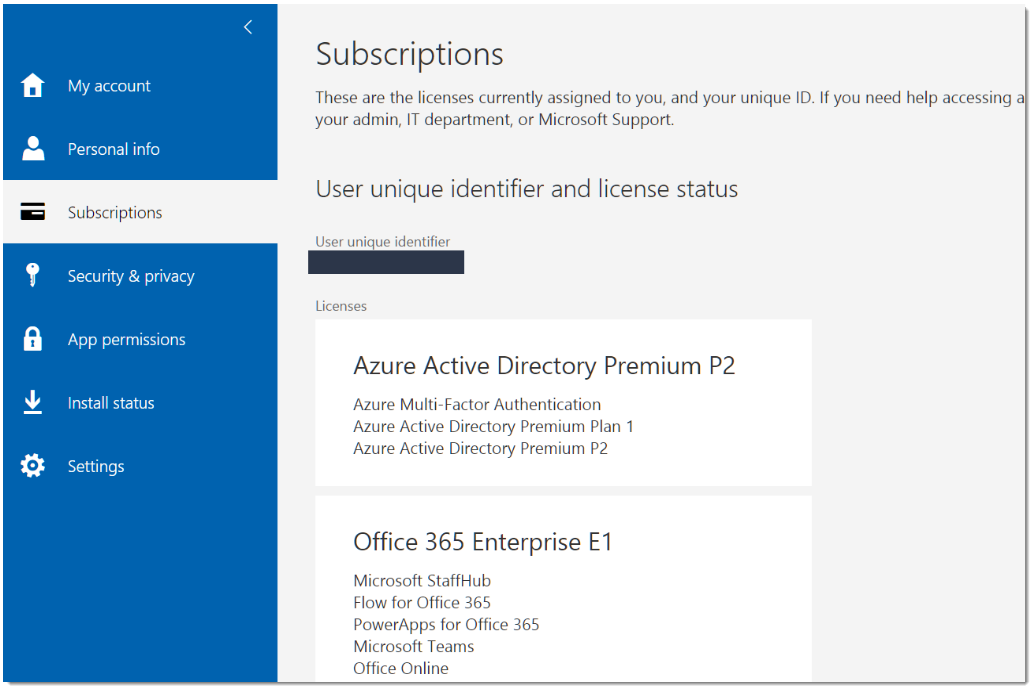
Password
Expiring in 13 days.

Language and time zone
English (United States)

You will be redirected to your Office 365 Account page.

6. Click **View Subscriptions** from the list.

It will display your Office 365 License, along with your Azure Active Directory Premium P2 license, if you have it purchased.



Subscriptions

These are the licenses currently assigned to you, and your unique ID. If you need help accessing a
your admin, IT department, or Microsoft Support.

User unique identifier and license status

User unique identifier
[redacted]

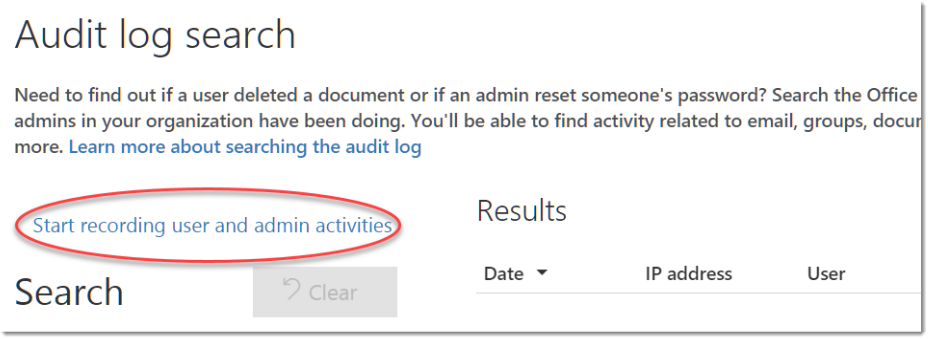
Licenses

Azure Active Directory Premium P2
Azure Multi-Factor Authentication
Azure Active Directory Premium Plan 1
Azure Active Directory Premium P2

Office 365 Enterprise E1
Microsoft StaffHub
Flow for Office 365
PowerApps for Office 365
Microsoft Teams
Office Online

Once you verify that you have AzureAD "Premium P2" license. You must also allow Office 365 to record user and admin activities. To enable this feature, follow the steps below:

1. Search and Click on **Security & Compliance**, from your Office 365 home screen.
2. Click on **Search**>**Audit log search** from the menu on the left-hand side.
3. Click **Start recording user and admin activities**.



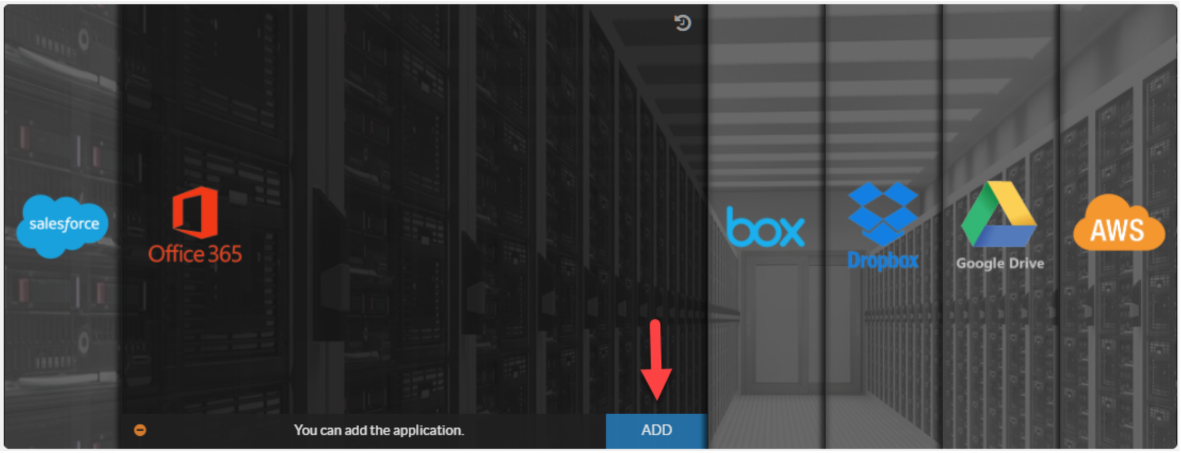
Audit log search

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office
admins in your organization have been doing. You'll be able to find activity related to email, groups, docur
more. Learn more about searching the audit log

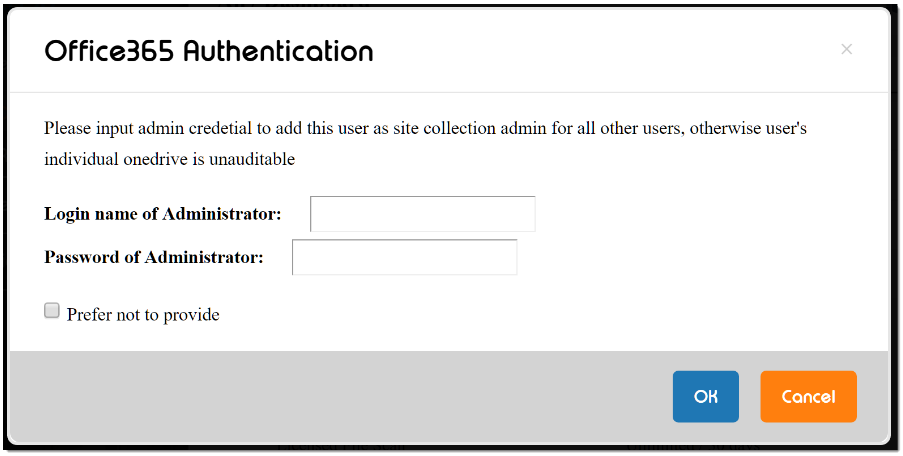
FortiCASB will now be able to monitor Office 365 activity.

Installation

1. Go to **Overview** > **Dashboard**.
2. From the Cloud App Status widget, click **ADD**, located next to Office 365.



You will be prompted to provide administrator credentials. FortiCASB will use this information to add this administrator as the "site collection administrator" of all Office 365 users in the company. This is necessary for FortiCASB to audit files stored inside each user's individual OneDrive.


Office365 Authentication

Please input admin credetial to add this user as site collection admin for all other users, otherwise user's individual onedrive is unauditable

Login name of Administrator:

Password of Administrator:

□ Prefer not to provide

If you don't want FortiCASB to audit users' OneDrives, or just want to do it manually, you can check "Prefer not to provide".

If you have a custom SharePoint homepage URL, you will have to allow collection manually.

See Troubleshooting on page 144

3. Click **OK.**
   You will be redirected to the Office 365 login screen.
   After logging in, Office 365 will prompt you to allow or deny FortiCASB access.
4. Click **Allow** to grant FortiCASB permissions required to monitor your Office 365 application.

   You will be redirected back to the FortiCASB dashboard.

   You can check the installation result and SaaS platform monitoring status in the Office 365 dashboard.

Salesforce

FortiCASB offers an API-based approach, pulling data directly from Salesforce via RESTful API. Authentication is done through OAUth2.0. FortiCASB uses an access token for API queries.

Prerequisites

To use API access, your organization must be using one of the following editions (the API is enabled by default):

- Enterprise Edition
- Unlimited Edition
- Developer Edition
- Performance Edition

The user account installed in FortiCASB must have the following permissions:

- View All Data
- View All Users
- API Enabled

You may either use an existing account or create a new account. If you create a new account, wait at least 24 hours for the new account to take effect before granting access to FortiCASB.

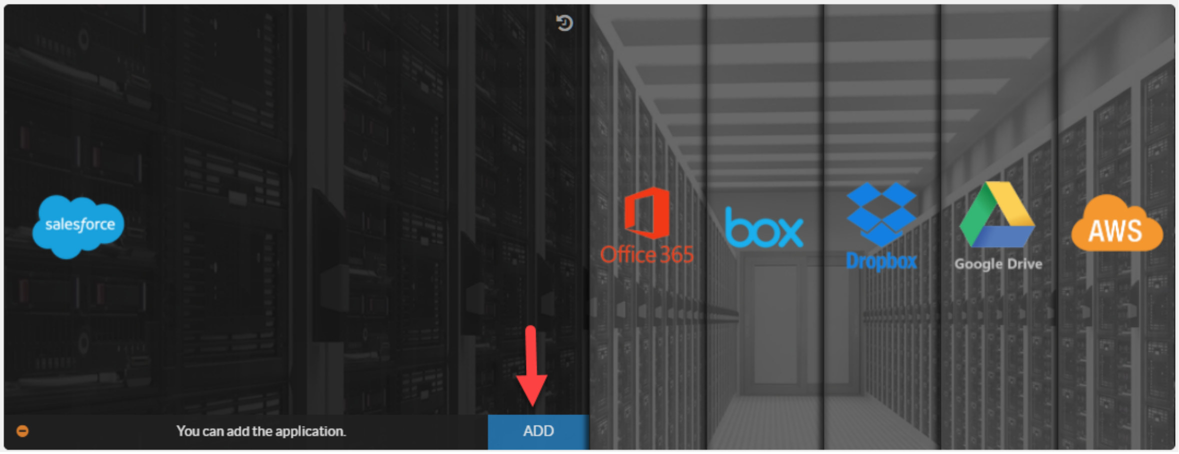
The following features require "Manage Users" permission as well:

- User login tracking
- User IP address tracking
- Geographical location tracking
- User password change tracking

Without "Manage Users" permissions, FortiCASB cannot obtain user login IPs. Therefore, any user activity will not appear on the Activity map.

Installation

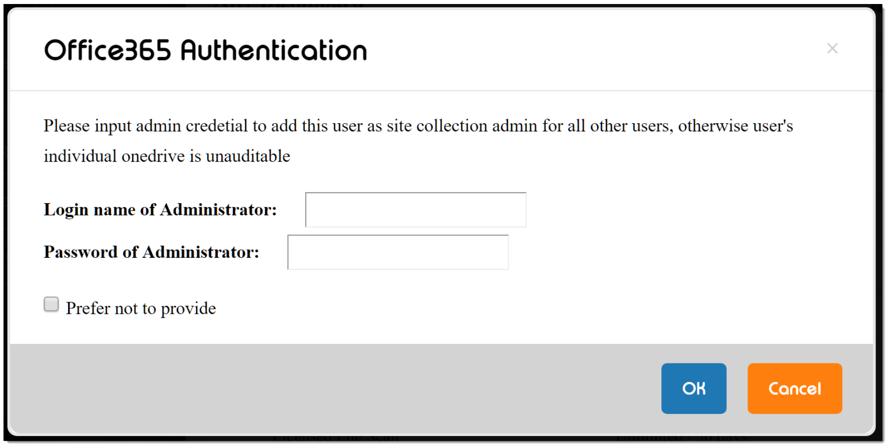
1. . From the menu on the left-hand side, select **Overview > Dashboard**.
2. . From the Cloud App Status widget, click **ADD**, located next to Salesforce.



3. Click **OK**.

You will be navigated to the Salesforce website for authentication.

If you have a custom Salesforce domain, enter it here.



Office365 Authentication

Please input admin credetial to add this user as site collection admin for all other users, otherwise user's individual onedrive is unauditable

Login name of Administrator:

Password of Administrator:

□ Prefer not to provide

4. Log in to authenticate.

   Salesforce will prompt you to allow or deny access.

5. Click **Allow** to grant FortiCASB permissions to monitor your Salesforce application.

   After you click Allow, you will be redirected back to the FortiCASB dashboard.

   You can check the installation result and SaaS platform monitoring status in the Salesforce dashboard.

For more information on common installation issues, see "Troubleshooting on page 144".

Install IAAS Applications

Installing IAAS applications

FortiCASB supports monitoring Amazon Web Services, Google Cloud Platform, and Microsoft Azure. Select the corresponding section from the menu index for an installation guide.

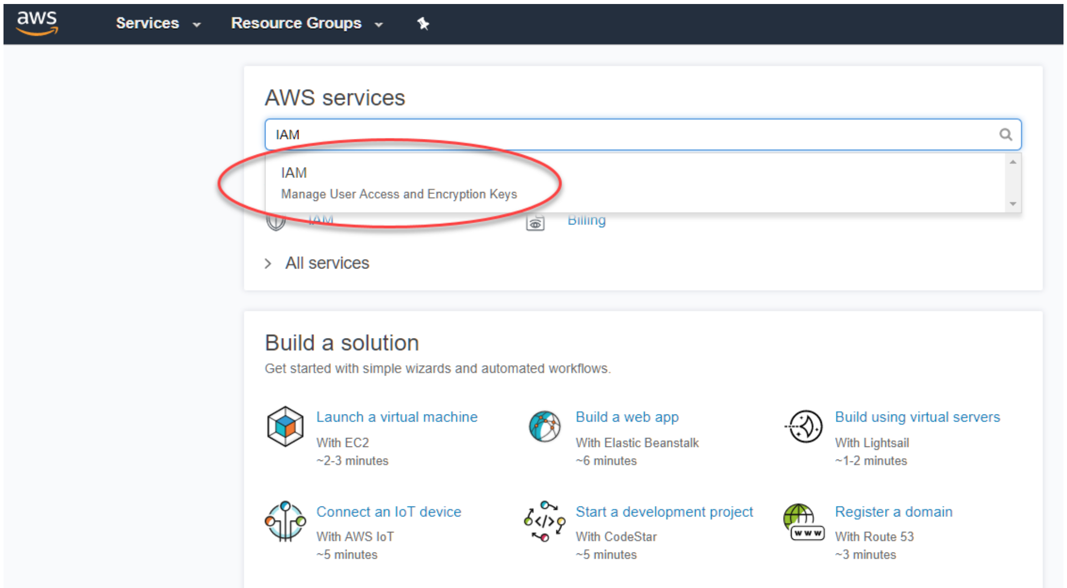
Amazon Web Services

FortiCASB offers an API-based approach, pulling data directly from AWS via RESTful API. Authentication is done through OAUth2.0. FortiCASB uses an access token for API queries.

Prerequisites

You must create a new role in your AWS account for FortiCASB before using FortiCASB with AWS. To create a role, use the following steps:

1. Go to your AWS console dashboard.
2. Search and click **IAM**



3. Click **Policies** from the menu on the left.
4. Click **Create policy.**
5. Go to the JSON tab.
6. Replace the existing JSON code with the following:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "sqs:DeleteMessage",
            "appstream:Describe*",
            "config:Get*",
            "iam:List*",
            "route53:ListTrafficPolicyVersions",
            "sqs:ReceiveMessage",
            "cloudtrail:GetTrailStatus",
            "route53:GetHealthCheck",
            "cloudfront:Get*",
            "codedeploy:List*",
            "guardduty:List*",
            "cloudwatch:Describe*",
            "route53:ListHostedZonesByName",
            "config:Describe*",
            "datapipeline:EvaluateExpression",
            "route53domains:CheckDomainAvailability",
            "rds:Describe*",
            "iam:SimulateCustomPolicy",
            "ec2:ModifySnapshotAttribute",
            "ec2:RevokeSecurityGroupEgress",
            "rds:DownloadDBLogFilePortion",
            "s3:GetBucket*",
            "route53:GetHostedZoneCount",
            "logs:FilterLogEvents",
            "inspector:Describe*",
            "cloudfront:List*",
            "acm:List*",
            "config:Deliver*",
            "sns:*",
            "elasticmapreduce:DescribeSecurityConfiguration",
            "cloudtrail:LookupEvents",
            "route53:GetHealthCheckLastFailureReason",
            "datapipeline:ListPipelines",
            "lambda:List*",
            "sqs:SendMessage",
            "route53:ListVPCAssociationAuthorizations",
            "route53:GetReusableDelegationSetLimit",
            "kms:Describe*",
            "logs:Get*",
            "cloudtrail:DescribeTrails",
            "s3:GetReplicationConfiguration",
            "route53:ListTagsForResources",
            "route53:GetAccountLimit",
            "ec2:RevokeSecurityGroupIngress",
            "sqs:PurgeQueue",
            "s3:PutObjectVersionAcl",
            "waf:List*",
            "route53:GetGeoLocation",
            "workspaces:Describe*",
            "redshift:ModifyClusterParameterGroup",
            "route53:GetTrafficPolicy",
            "elasticloadbalancing:ModifyLoadBalancerAttributes",
            "glacier:ListVaults",
            "iam:GenerateCredentialReport",
            "s3:GetLifecycleConfiguration",
            "tag:GetResources",
            "s3:GetInventoryConfiguration",
            "cloudtrail:StartLogging",
            "acm:Describe*",
            "route53domains:ListTagsForDomain",
            "dynamodb:ListTables",
            "s3:ListBucket",
            "route53domains:GetDomainDetail",
            "datapipeline:ValidatePipelineDefinition",
            "datapipeline:DescribePipelines",
            "route53:ListQueryLoggingConfigs",
            "elasticmapreduce:List*",
            "iam:Get*",
            "elasticmapreduce:DescribeStep",
            "route53:GetCheckerIpRanges",
            "route53domains:ListDomains",
            "route53:ListGeoLocations",
            "elasticmapreduce:DescribeEditor",
            "route53:GetTrafficPolicyInstance",
            "cloudfront:UpdateDistribution",
            "sqs:ChangeMessageVisibilityBatch",
            "s3:PutBucketVersioning",
            "sqs:SetQueueAttributes",
            "kms:EnableKeyRotation",
            "s3:ListBucketMultipartUploads",
            "cloudsearch:Describe*",
            "ecs:Describe*",
            "route53:ListHostedZones",
            "datapipeline:QueryObjects",
            "guardduty:Get*",
            "route53domains:GetContactReachabilityStatus",
            "route53:ListTagsForResource",
            "elasticache:Describe*",
            "sqs:TagQueue",
            "ec2:Describe*",
            "directconnect:Describe*",
            "route53:ListHealthChecks",
            "codedeploy:Get*",
            "s3:GetAccountPublicAccessBlock",
            "rds:ListTagsForResource",
            "s3:ListAllMyBuckets",
            "route53domains:ListOperations",
            "s3:GetObjectVersion",
            "kms:List*",
            "glacier:GetVaultAccessPolicy",
            "sqs:SendMessageBatch",
            "sqs:UntagQueue",
            "logs:Describe*",
            "s3:GetObjectVersionTagging",
            "route53:GetHostedZone",
            "kms:Get*",
            "ses:List*",
            "s3:GetObjectAcl",
            "iam:SimulatePrincipalPolicy",
            "codedeploy:Batch*",
            "ec2:SearchTransitGatewayRoutes",
            "dynamodb:DescribeTable",
            "cloudtrail:ListTags",
            "route53:ListResourceRecordSets",
            "s3:GetObjectVersionAcl",
            "rds:ModifyDBInstance",
            "s3:PutBucketAcl",
            "elasticloadbalancing:Describe*",
            "cloudformation:ListStack*",
            "s3:HeadBucket",
            "es:Describe*",
            "route53:GetHealthCheckCount",
            "sdb:DomainMetadata",
            "route53:ListReusableDelegationSets",
            "ses:Get*",
            "sqs:GetQueueUrl",
            "elasticfilesystem:Describe*",
            "route53:ListTrafficPolicyInstancesByHostedZone",
            "route53domains:GetDomainSuggestions",
            "ec2:GetTransitGatewayAttachmentPropagations",
            "sqs:GetQueueAttributes",
            "elasticbeanstalk:Describe*",
            "route53domains:GetOperationDetail",
            "s3:ListMultipartUploadParts",
            "s3:GetObject",
            "iam:UpdateAccountPasswordPolicy",
            "redshift:Describe*",
            "cloudformation:GetTemplate",
            "ec2:GetTransitGatewayRouteTablePropagations",
            "sqs:DeleteQueue",
            "s3:GetAnalyticsConfiguration",
            "route53:GetHostedZoneLimit",
            "s3:GetObjectVersionForReplication",
            "route53:ListTrafficPolicyInstances",
            "autoscaling:Describe*",
            "s3:ListBucketByTags",
            "route53:GetTrafficPolicyInstanceCount",
            "route53:GetChange",
            "s3:ListBucketVersions",
            "s3:GetAccelerateConfiguration",
            "sqs:ListQueueTags",
            "elasticmapreduce:DescribeCluster",
            "tag:GetTagKeys",
            "s3:GetObjectVersionTorrent",
            "s3:GetEncryptionConfiguration",
            "sns:Get*",
            "sqs:DeleteMessageBatch",
            "elasticache:List*",
            "route53:ListTrafficPolicies",
            "s3:GetObjectTagging",
            "s3:GetMetricsConfiguration",
            "waf:Get*",
            "ecs:List*",
            "ec2:GetTransitGatewayRouteTableAssociations",
            "s3:PutObjectAcl",
            "route53:GetQueryLoggingConfig",
            "sqs:ListQueues",
            "sqs:ChangeMessageVisibility",
            "route53:GetHealthCheckStatus",
            "cloudtrail:UpdateTrail",
            "ds:Describe*",
            "datapipeline:DescribeObjects",
            "route53:GetReusableDelegationSet",
            "datapipeline:GetPipelineDefinition",
            "inspector:List*",
            "sdb:ListDomains",
            "cloudformation:DescribeStack*",
            "route53:ListTrafficPolicyInstancesByPolicy",
            "s3:GetObjectTorrent",
            "sqs:ListDeadLetterSourceQueues",
            "s3:PutBucketPolicy",
            "sqs:CreateQueue",
            "es:List*",
            "lambda:GetPolicy",
            "eks:ListUpdates",
            "eks:DescribeUpdate",
            "eks:DescribeCluster",
            "eks:ListClusters"
         ],
         "Resource": "*"
      }
   ]
 }
```

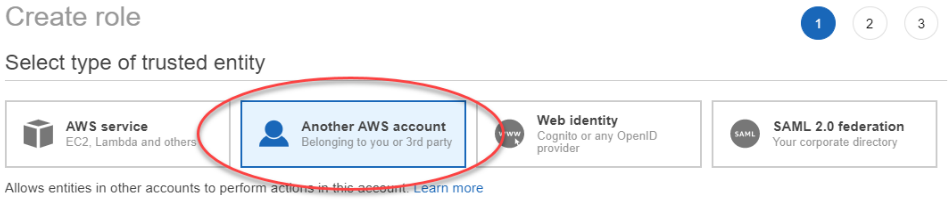
7. Click **Review policy.**
8. Name the new policy.
9. Click **Create policy.**

Your new policy will be created.

Please keep your policy name later for role creation.

Role creation

1. Click **Roles** from the menu on the left.
2. Click **Create role**.
3. Click **Another AWS account.**

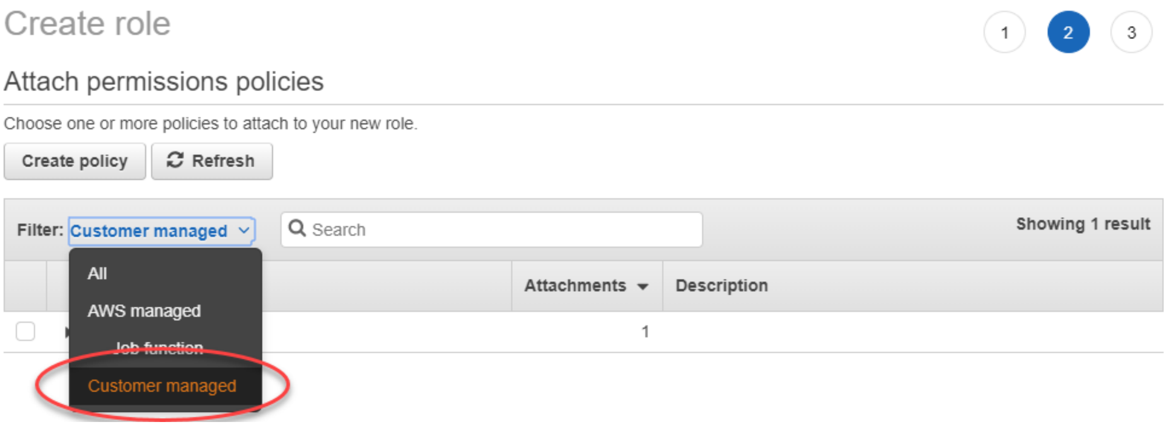


Allows entities in other accounts to perform actions in this account. Learn more

4. Enter the following Account ID: 854209929931.
   Note: This is the Amazon AWS account that FortiCASB uses to monitor the new role that is being created.
5. Select the box **Require external ID** and enter in an external ID of your preference.

Please keep the external ID later for AWS authentication during installation.

6. Make sure the box **Require MFA** is not selected.
7. Click **Next: Permissions.**
8. Click **Filter**, then select Customer managed.



Create role

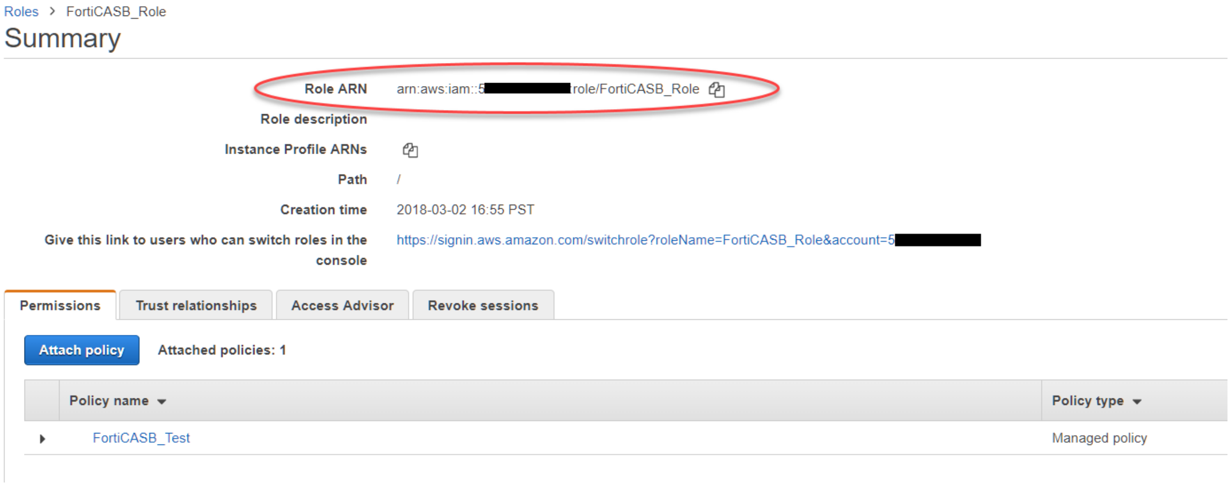
Attach permissions policies

Choose one or more policies to attach to your new role.

Filter: Customer managed

Showing 1 result

9. Select the box for the policy you created earlier.
10. Click **Next: Tag**, and then click **Next: Review**.
11. Enter a name of your preference for the role name.
12. Click **Create role**.
13. Click the role name, and copy the AWS Role ARN.
    Example of AWS Role ARN: arn:aws:iam::123456123456:role/FortiCasbTester



Roles › FortiCASB_Role

Summary

Role ARN	arn:aws:iam::5[redacted]role/FortiCASB_Role
Role description	
Instance Profile ARNs	
Path	/
Creation time	2018-03-02 16:55 PST
Give this link to users who can switch roles in the console	https://signin.aws.amazon.com/switchrole?roleName=FortiCASB_Role&account=5[redacted]

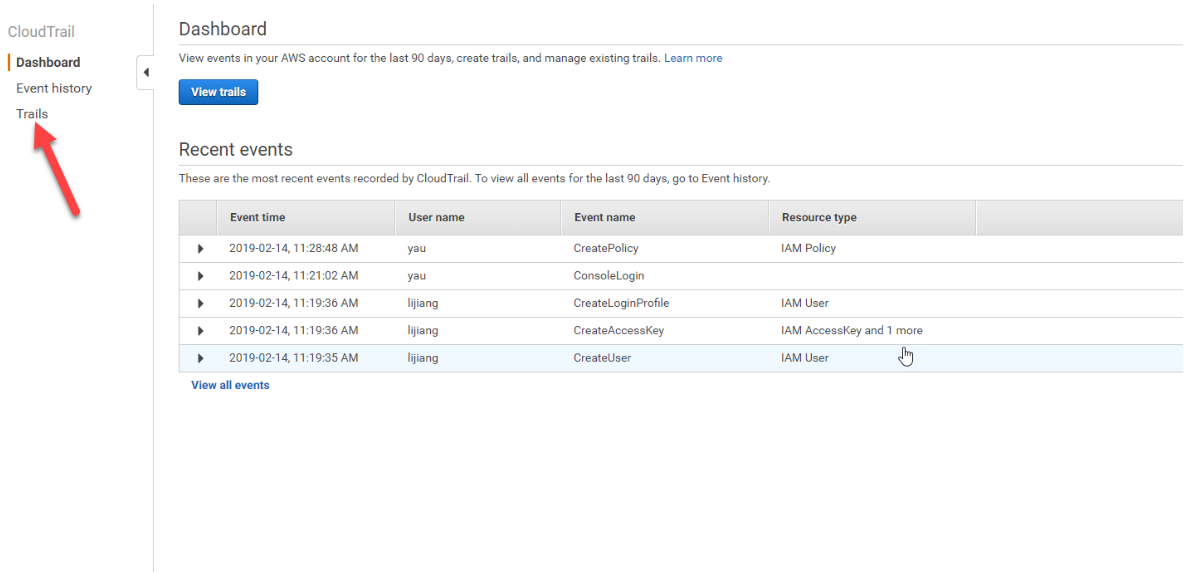
Attached policies: 1

Policy name	Policy type
FortiCASB_Test	Managed policy

Please keep the AWS Role ARN later for AWS authentication during installation.

Configure CloudTrail Setting

1. Go to your AWS console dashboard.
2. Click on services drop down menu and search for **cloudtrail.**
3. Once you are in Cloud Trail, click on **Trails** in the left panel.



Dashboard

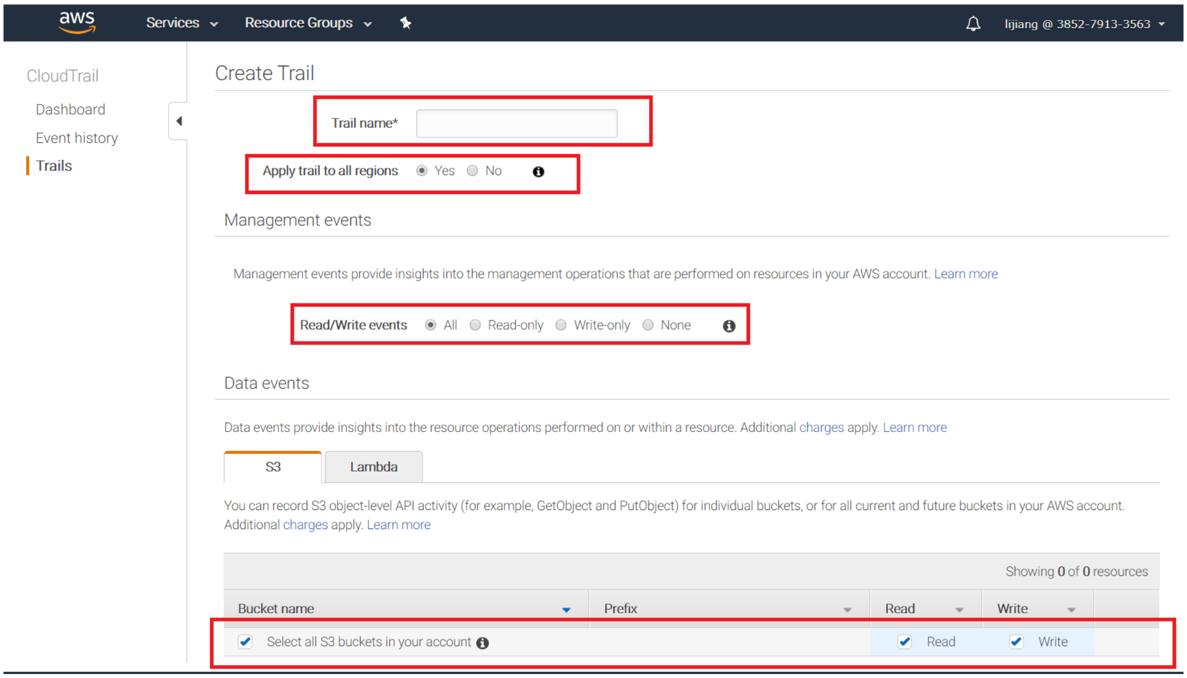
View events in your AWS account for the last 90 days, create trails, and manage existing trails. Learn more

Recent events

These are the most recent events recorded by CloudTrail. To view all events for the last 90 days, go to Event history.

Event time	User name	Event name	Resource type
2019-02-14, 11:28:48 AM	yau	CreatePolicy	IAM Policy
2019-02-14, 11:21:02 AM	yau	ConsoleLogin	
2019-02-14, 11:19:36 AM	lijiang	CreateLoginProfile	IAM User
2019-02-14, 11:19:36 AM	lijiang	CreateAccessKey	IAM AccessKey and 1 more
2019-02-14, 11:19:35 AM	lijiang	CreateUser	IAM User

4. Click **Create trail.**
5. Enter a trail name based on your preference.
6. Select **Yes** to **Apply trail to all regions.**
7. Select **All** for **Read/Write events**.
8. Under **Data event > S3**, check on **Select all S3 buckets in your account**, **Read, and Write.**



Create Trail

Trail name*

Apply trail to all regions ● Yes ○ No

Management events

Management events provide insights into the management operations that are performed on resources in your AWS account. Learn more

Read/Write events ● All ○ Read-only ○ Write-only ○ None

Data events

Data events provide insights into the resource operations performed on or within a resource. Additional charges apply. Learn more

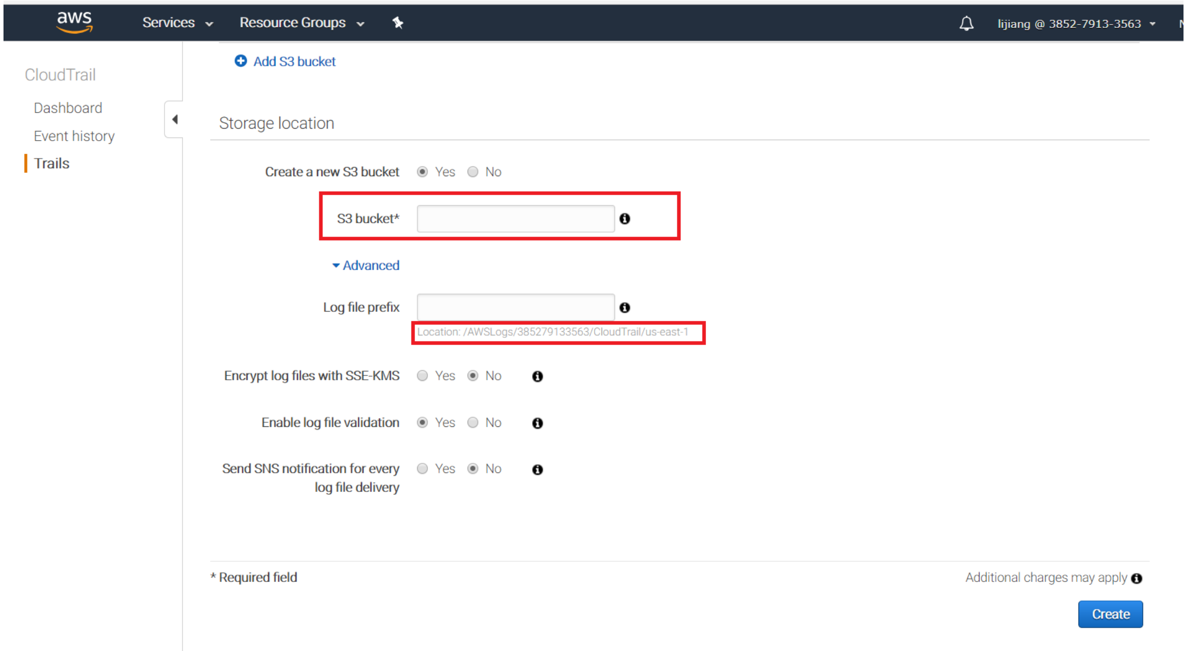
You can record S3 object-level API activity (for example, GetObject and PutObject) for individual buckets, or for all current and future buckets in your AWS account. Additional charges apply. Learn more

Showing 0 of 0 resources

Bucket name	Prefix	Read	Write
☑ Select all S3 buckets in your account		☑ Read	☑ Write

9. Scroll down and click **advanced** to show hidden menu.
10. Name the **S3 bucket** based on your preference, the bucket name is used for CloudTrail S3 bucket for AWS authentication.

Please keep the cloud trail S3 bucket name later for AWS authentication during installation.



Storage location

Create a new S3 bucket ● Yes ○ No

S3 bucket*

Log file prefix

Location: /AWSLogs/385279133563/CloudTrail/us-east-1

Encrypt log files with SSE-KMS ○ Yes ● No

Enable log file validation ● Yes ○ No

Send SNS notification for every log file delivery ○ Yes ● No

* Required field

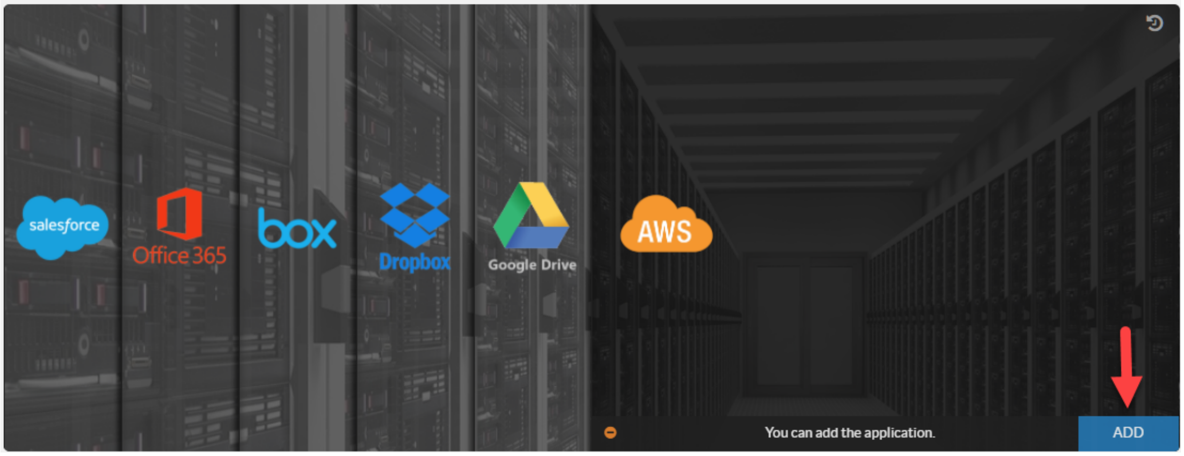
11. Leave the **Log file prefix** blank.
12. Notice the location under **Log file prefix**, the location without the leading forward slash, and all the content up to CloudTrail is the **CloudTrail S3 Log File Prefix**.

For example: if the location is /AWSLogs/123456123456/CloudTrail/us-east-1, then the CloudTrail S3 Log File Prefix is AWSLogs/123456123456/CloudTrail.

Please keep the Cloud S3 Log File Prefix later for AWS authentication later during installation.

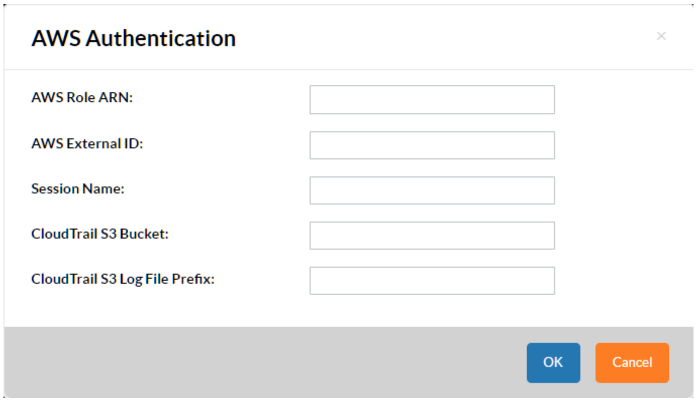
Installation

1. From the menu on the left-hand side, select **Overview > Dashboard.**
2. From the Cloud App Status widget, click **ADD**, located next to AWS.



You can add the application.

3. You will be prompted for your AWS authentication information.
   a. Enter in the **AWS Role ARN** you copied eariler.
   b. Enter in the **AWS External ID** you set earlier.
   c. Enter a **Session Name** for this monitoring session based on your preference.
   d. Enter in the **CloudTrail S3 Bucket** you set earlier.
   e. Enter in the **CloudTrail S3 Log File Prefix** recorded earlier.



AWS Authentication

AWS Role ARN:

AWS External ID:

Session Name:

CloudTrail S3 Bucket:

CloudTrail S3 Log File Prefix:

4. Click **OK**.

You can check the installation result and IaaS platform monitoring status in the AWS dashboard.

Checking application monitoring status

FortiCASB starts to monitor immediately after the application has been successfully installed. To check if FortiCASB is monitoring, look for the green [Running] indicator on the application panel. If an error occurs, the light will turn red, and the application panel will guide you through the troubleshooting process.

Google Cloud Platform

FortiCASB offers an API-based approach, pulling data directly from Google Cloud via a RESTful API. FortiCASB uses your service account credentials for API queries.

Prerequisites

To use FortiCASB with Google Cloud Platform, you must have a **G Suite account, service account**, and the **JSON private key** associated with the service account. The service account must have “**G Suite Domain-wide Delegation**” enabled and **Project Owner/Organization Administrator roles** for monitoring. The projects must also have all the required APIs enabled, as discussed in Google Cloud Platform on page 42.

Steps to setup Google Cloud with FortiCASB

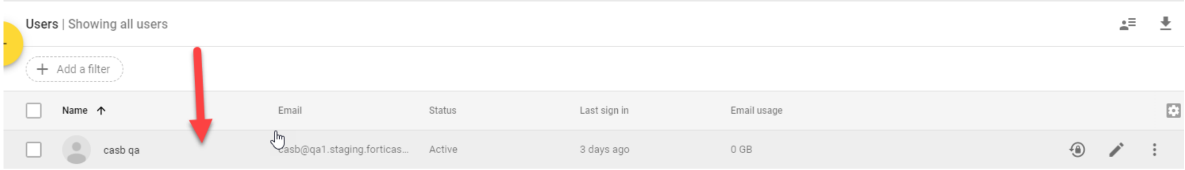
- Configure G Suite Account on page 43
- Configure Service Account on page 44
- Enable required APIs on page 51
- Enable activity and alert monitoring on page 53
- Installation on page 53

Your G Suite account can be either an existing account or a new account. If you have just created a new account, you must wait for at least 24 hours for the account to take effect before granting it access to FortiCASB. The G Suite account to which you connect from within FortiCASB must have the Super Admin role in your G Suite account.

Configure G Suite Account

Use the following steps to check if your account has the Super Admin role:

1. Go to https://admin.google.com/ and log in with your **Google Suite account** credentials.
2. In the upper-left corner, click the **navigation menu** ☰ , and select **Directory>Users**.
3. Click on user account of interest.

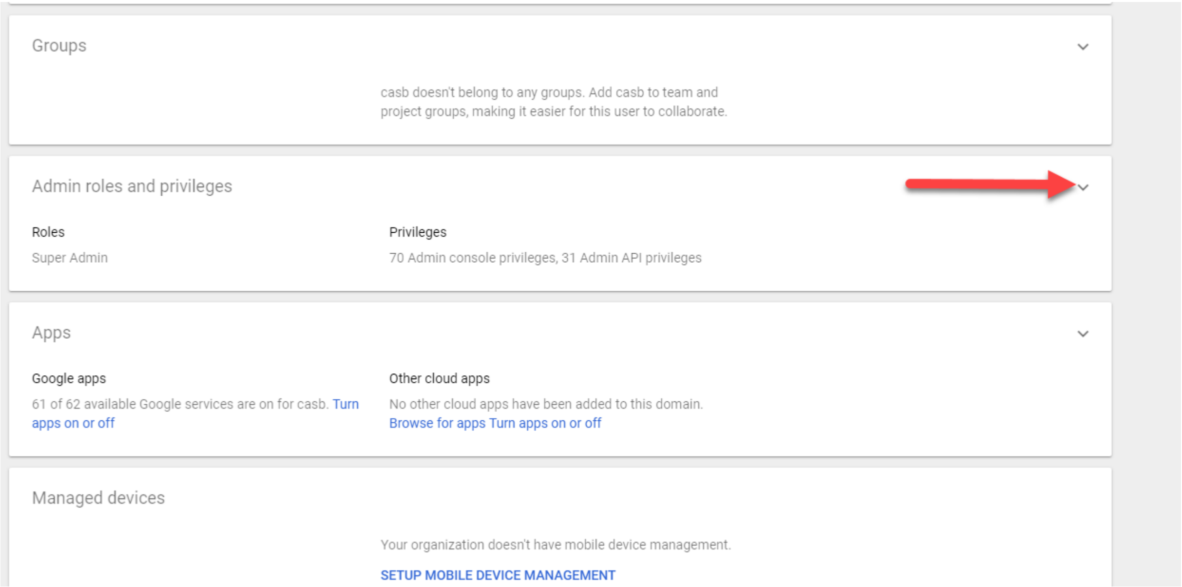


Users | Showing all users

+ Add a filter

□	Name ↑	Email	Status	Last sign in	Email usage
□	casb qa	casb@qa1.staging.forticas...	Active	3 days ago	0 GB

4. Scroll down to the **Admin roles and privileges** section, click the draw-down button.



Groups

casb doesn't belong to any groups. Add casb to team and project groups, making it easier for this user to collaborate.

Admin roles and privileges

Roles	Privileges
Super Admin	70 Admin console privileges, 31 Admin API privileges

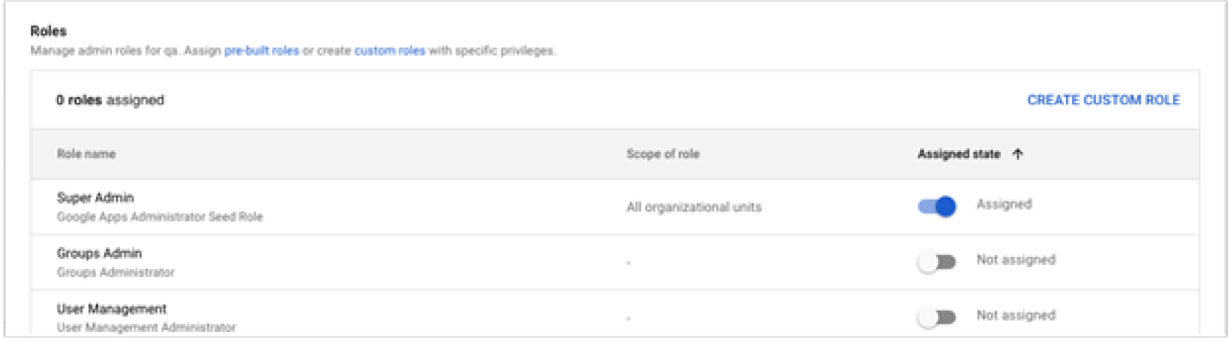
Apps

Google apps	Other cloud apps
61 of 62 available Google services are on for casb. Turn apps on or off	No other cloud apps have been added to this domain. Browse for apps Turn apps on or off

Managed devices

Your organization doesn't have mobile device management.

5. In the **Roles** section, make sure that the **Super Admin role** has been assigned. Otherwise, hover over the Roles section, click the Edit icon, and select Super Admin in the pop-up window.



Roles

Manage admin roles for qa. Assign pre-built roles or create custom roles with specific privileges.

0 roles assigned

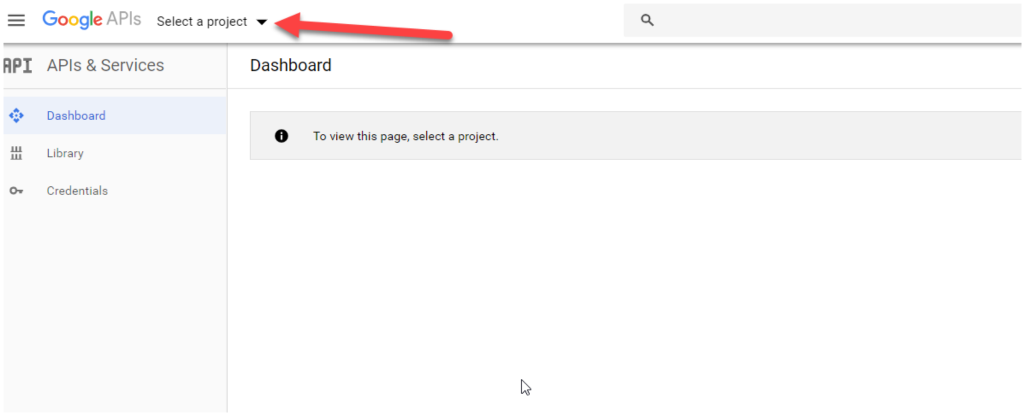
Role name	Scope of role	Assigned state ↑
Super Admin Google Apps Administrator Seed Role	All organizational units	Assigned
Groups Admin Groups Administrator	-	Not assigned
User Management User Management Administrator	-	Not assigned

Configure Service Account

For your service account, you may either use an existing or new account.

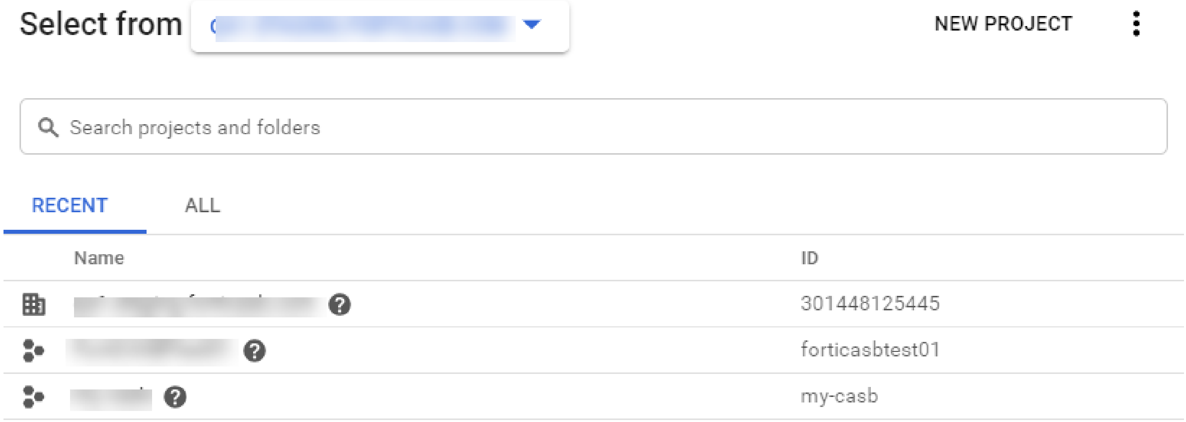
New Service Account Creation

1. Go to https://console.developers.google.com and log in with your **Google Suite account**.
2. Click on the drop-down menu > **Select a project.**



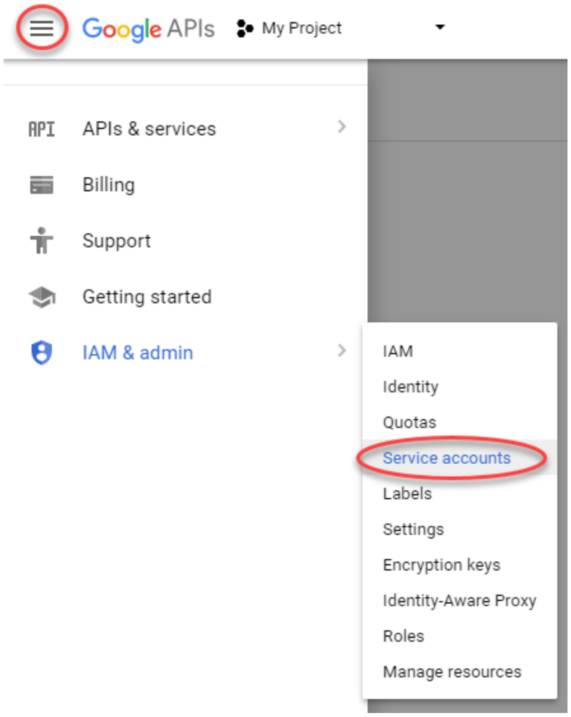
To view this page, select a project.

3. Select an existing project you want to monitor or Create a New Project by clicking **New Project**.



Name	ID
[redacted]	301448125445
[redacted]	forticasbtest01
[redacted]	my-casb

4. Click the Navigation Menu ☰ on the top left corner, go to **IAM & admin > Service accounts.**



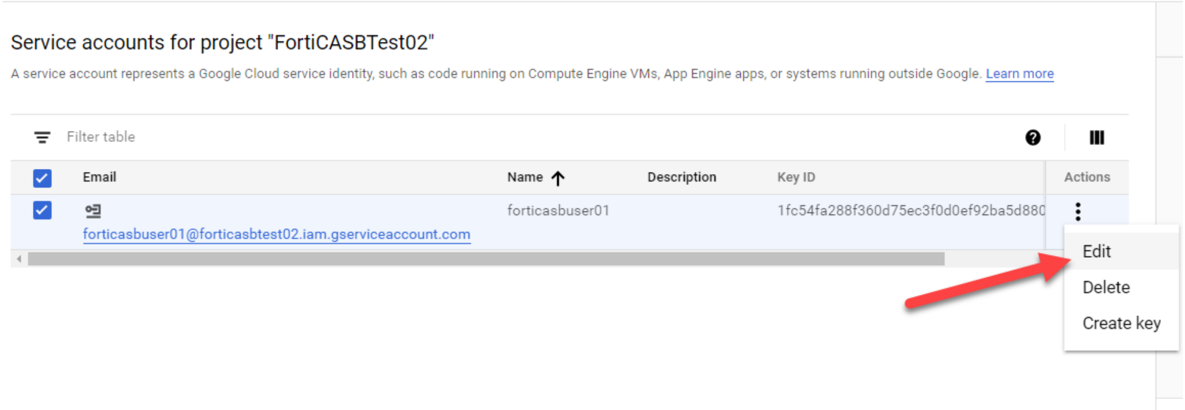
5. Click **+Create service account button**.
6. Enter a **Service account name** of your preference and click **create**. Service account ID will populate automatically.

Keep the service account ID for later during Google cloud authentication during installation.

7. Click **Continue** when prompted for entering service account permissions.
8. Click on **+Create Key** and select JSON to create a private key. The JSON private key will be downloaded automatically, then click **Done**

Keep the JSON key later for Google cloud authentication during installation.

9. Once service account is created, select the service account created and click on under **Actions** ⋮ icon > **Edit**.



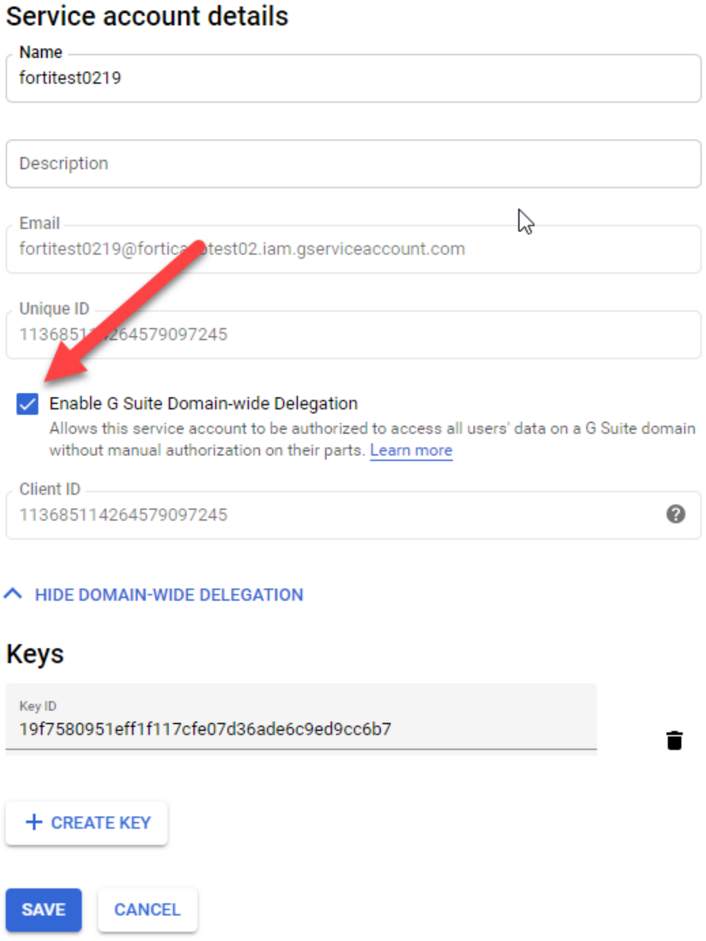
Service accounts for project "FortiCASBTest02"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. Learn more

Filter table

☑	Email	Name ↑	Description	Key ID	Actions
☑	forticasbuser01@forticasbtest02.iam.gserviceaccount.com	forticasbuser01		1fc54fa288f360d75ec3f0d0ef92ba5d880	⋮

10. Enable **G Suite Domain-wide Delegation.**



Service account details

Name: fortitest0219

Description

Email: fortitest0219@forticasbtest02.iam.gserviceaccount.com

Unique ID: 113685114264579097245

☑ Enable G Suite Domain-wide Delegation

Allows this service account to be authorized to access all users' data on a G Suite domain without manual authorization on their parts. Learn more

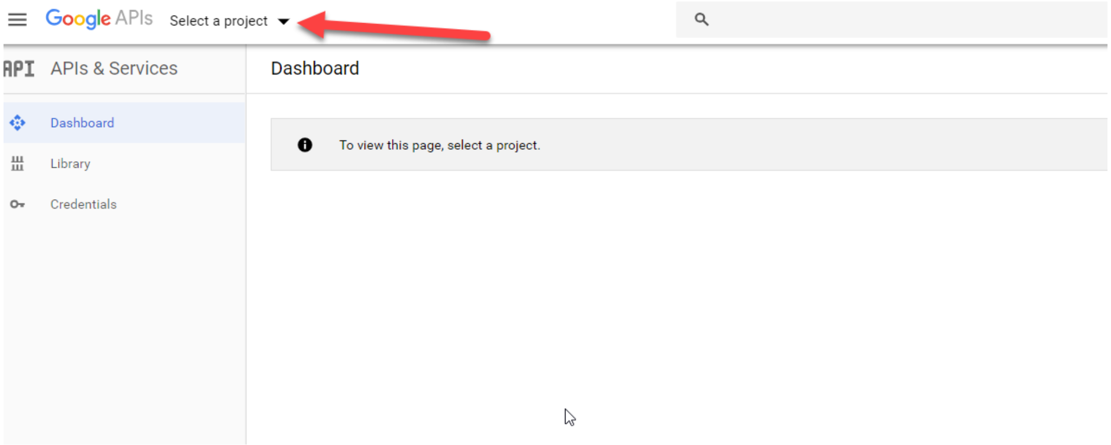
Client ID: 113685114264579097245

Keys

Key ID: 19f7580951eff1f117cfe07d36ade6c9ed9cc6b7

Using Existing Service Account

1. Select the project that contains the service account to be used.

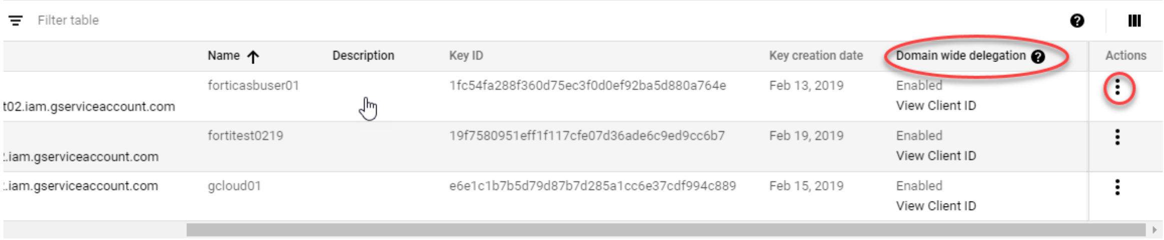


To view this page, select a project.

2.

3. Click the **Navigation Menu** ☰ in the upper-left corner of the page, and select **IAM & Admin > Service Accounts.**

   Note:Make sure **Domain-wide delegation** is enabled. If not, click on **Actions** ⋮ icon **> Edit** to enable it.



	Name ↑	Description	Key ID	Key creation date	Domain wide delegation	Actions
t02.iam.gserviceaccount.com	forticasbuser01		1fc54fa288f360d75ec3f0d0ef92ba5d880a764e	Feb 13, 2019	Enabled View Client ID	⋮
:.iam.gserviceaccount.com	fortitest0219		19f7580951eff1f117cfe07d36ade6c9ed9cc6b7	Feb 19, 2019	Enabled View Client ID	⋮
:.iam.gserviceaccount.com	gcloud01		e6e1c1b7b5d79d87b7d285a1cc6e37cdf994c889	Feb 15, 2019	Enabled View Client ID	⋮

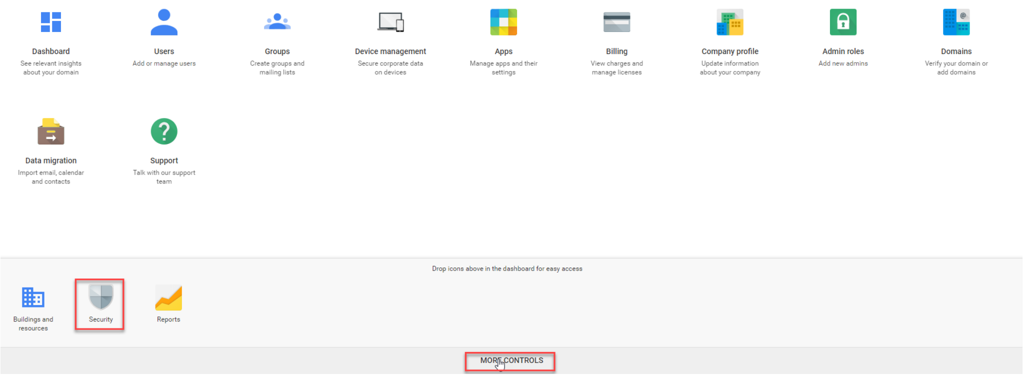
4. If you don’t have a JSON private key, then click **Actions** ⋮ icon **> Edit** , and select **+Create Key.**
5. Select **JSON** in the Key type field, and click **CREATE.**The JSON private key will automatically downloaded.

   Note: Be sure to keep this key and your service account ID for use later during Google cloud authentication.

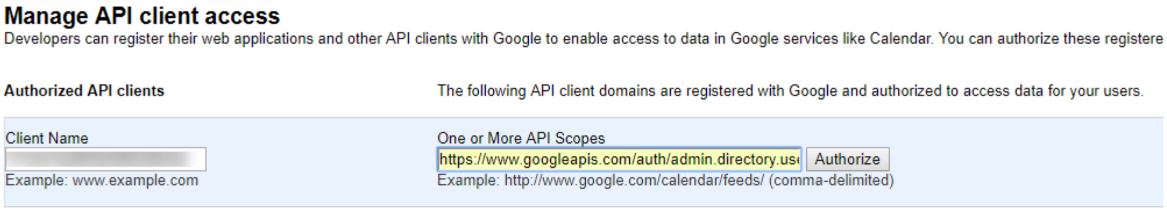
Once your service account is ready, you must grant it API access to the G Suite API.

Grant Service Account API Access

1. Click the **Navigation Menu** ☰ in the upper-left corner of the page, and then select **IAM & admin > Service Accounts.**
2. In the **Domain-wide delegation** column, click **View Client ID.**
3. In the pop-up window, save the client ID for step 7.
4. Go to https://admin.google.com and log into the same Google account.
5. Scroll down and click on **More Controls > Security.**


Dashboard
See relevant insights about your domain
Users
Add or manage users
Groups
Create groups and mailing lists
Device management
Secure corporate data on devices
Apps
Manage apps and their settings
Billing
View charges and manage licenses
Company profile
Update information about your company
Admin roles
Add new admins
Domains
Verify your domain or add domains
Data migration
Import email, calendar and contacts
Support
Talk with our support team
Drop icons above in the dashboard for easy access
Buildings and resources
Security
Reports
MORE CONTROLS

6. In **Security**, scroll down and select **Advanced Settings.**
7. Click **Manage API client access.**



Manage API client access

Developers can register their web applications and other API clients with Google to enable access to data in Google services like Calendar. You can authorize these registere

Authorized API clients The following API client domains are registered with Google and authorized to access data for your users.

Client Name [redacted]
Example: www.example.com

One or More API Scopes https://www.googleapis.com/auth/admin.directory.use Authorize
Example: http://www.google.com/calendar/feeds/ (comma-delimited)

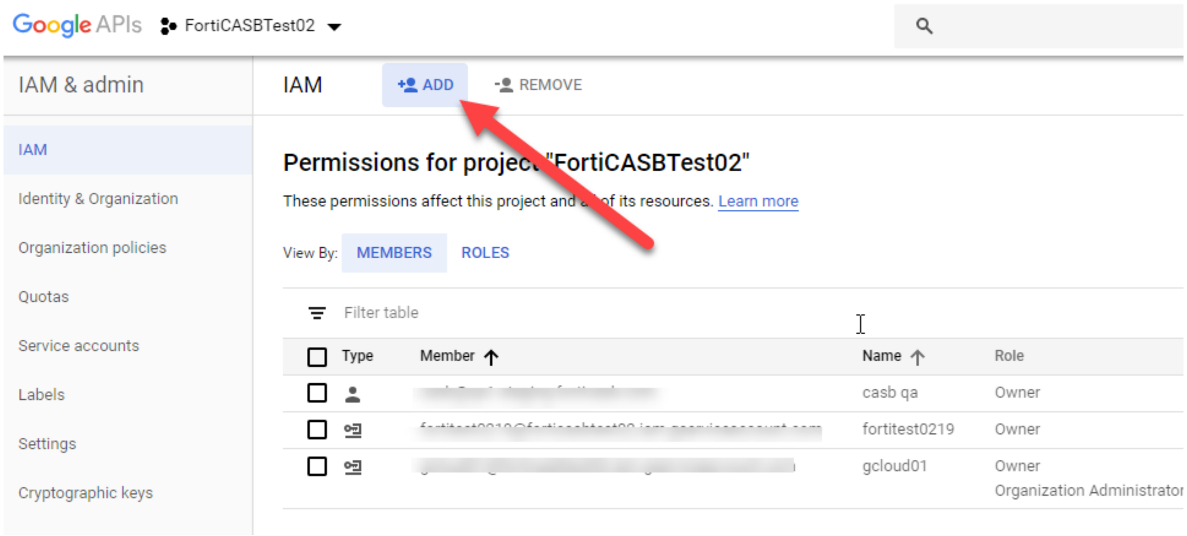
8. In the **Client Name** field, enter the Client ID saved in Step 3. Your Client ID must be a string of numbers.
9. In the **One or More API Scopes** field, enter:

   “https://www.googleapis.com/auth/admin.directory.user,https://www.googleapis.com/auth/admin.reports.audit.readonly".

After getting your service account ID and JSON private key, grant the service account with **Owner** and **Organization Administrator** role for the projects to be monitored.

Grant Service Account Owner Role

1. Select the project to be monitored.
2. Click the **Navigation Menu** ☰ on the upper-left corner, select **IAM & admin > IAM**.
3. Click the **ADD** button on the top.



Permissions for project "FortiCASBTest02"

These permissions affect this project and all of its resources. Learn more

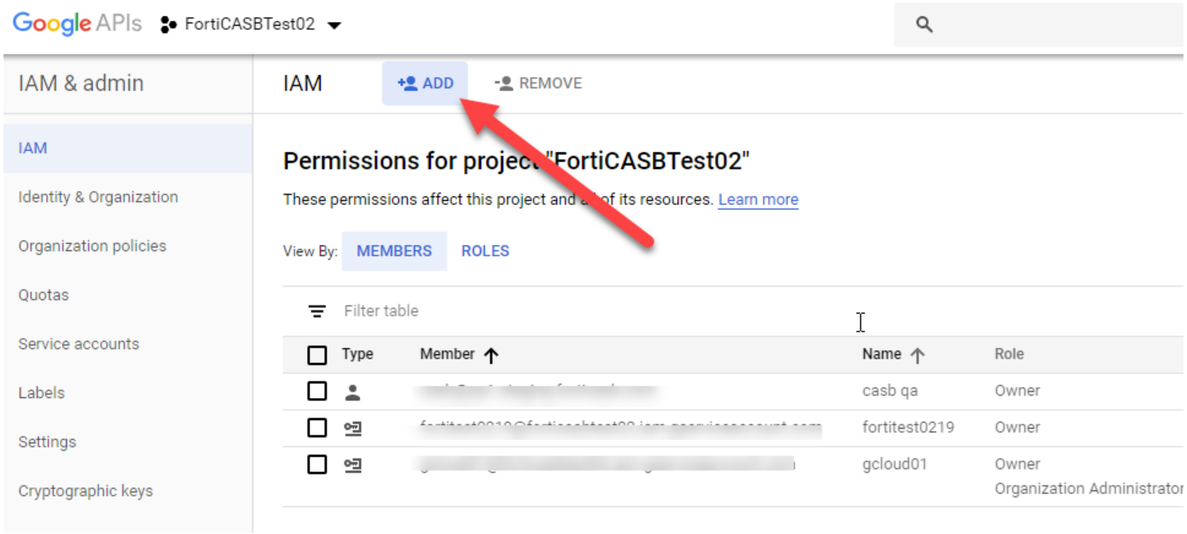
Type	Member	Name	Role
☐	[redacted]	casb qa	Owner
☐	[redacted]	fortitest0219	Owner
☐	[redacted]	gcloud01	Owner Organization Administrator

4. In the **New Members** field, enter the service account ID you want to use.
5. In the Select a role field, select **Project > Owner**.
6. Click the **SAVE** button.
7. Repeat the steps above for all the projects to be monitored.

Additionally, on the same service account, grant **Organization Administrator.**

Grant service account Organization Administrator role

1. Select the project to be monitored.
2. Click the **Navigation Menu** ☰ on the upper-left corner, select **IAM & admin > IAM**.
3. Click the **ADD** button on the top.



Permissions for project "FortiCASBTest02"

These permissions affect this project and all of its resources. Learn more

Type	Member	Name	Role
☐	[redacted]	casb qa	Owner
☐	[redacted]	fortitest0219	Owner
☐	[redacted]	gcloud01	Owner Organization Administrator

4. In the **New members** field, enter the service account ID you want to use.
5. In the Select a role field, select **Resource Manager > Organization Administrator**

Note: You can also enter "Organization Administrator" in the filter for fast access.

6. Click the **SAVE** button.

Enable required APIs

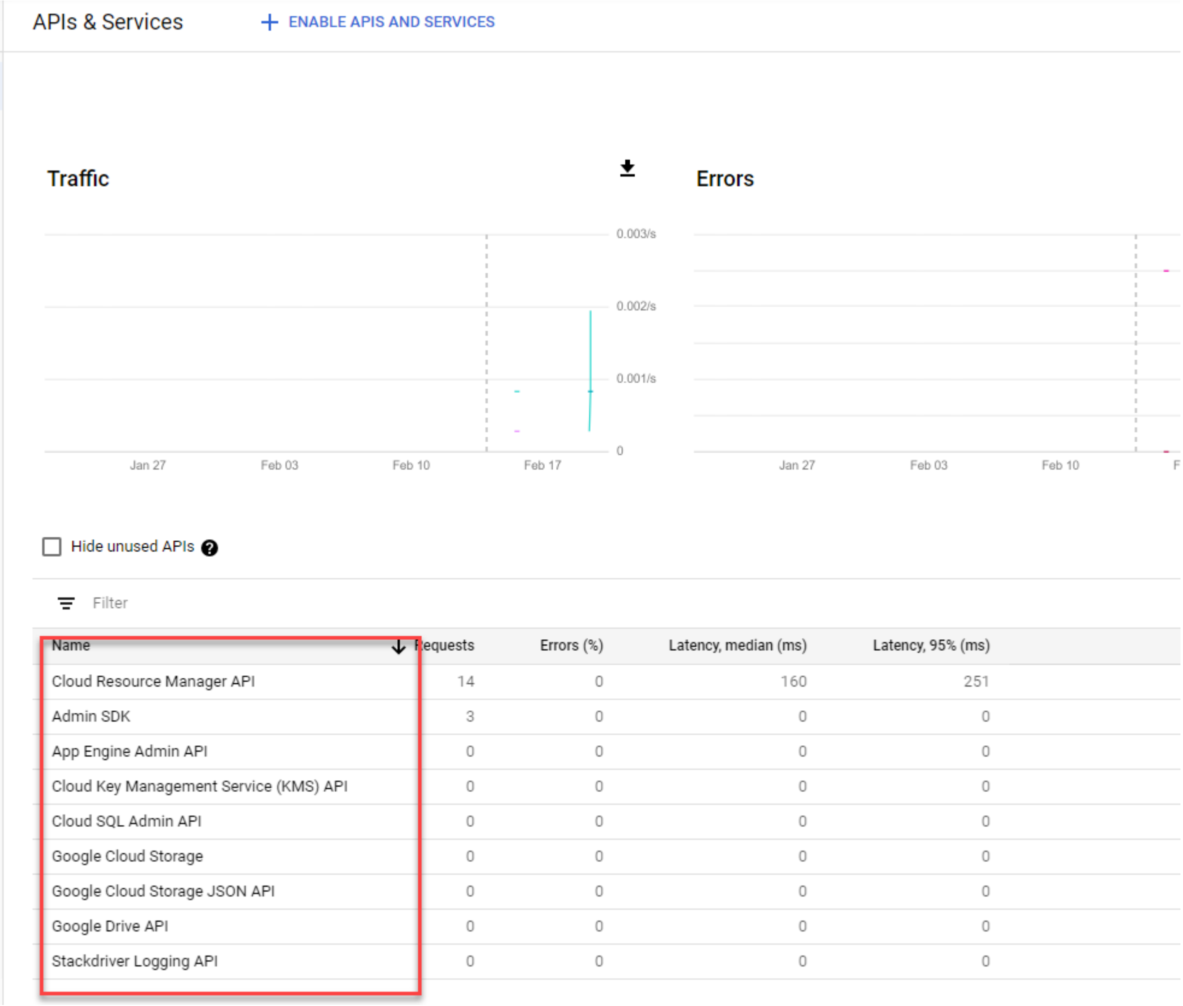
After adding roles to the service account, you must make sure that the following APIs are enabled on all projects for monitoring. This will ensure that FortiCASB can gather information from the Google Cloud.

- Cloud Resource Manager API
- App Engine Admin API
- Cloud Key Management Service (KMS) API
- Compute Engine API
- Cloud SQL
- Google Cloud Storage JSON API
- Google Cloud Storage
- Cloud SQL Admin API
- Stackdriver Logging API
- Admin SDK
- Identity and Access Management (IAM) API

To enable the APIs, do the following:

1. Go to the project to be monitored.
2. Click the **Navigation Menu** ☰ in the upper-left corner, and select **APIs & Services>Dashboard**.

3. In the **Enabled APIs and services** list, make sure that the required APIs are listed (enabled).



Name	Requests	Errors (%)	Latency, median (ms)	Latency, 95% (ms)
Cloud Resource Manager API	14	0	160	251
Admin SDK	3	0	0	0
App Engine Admin API	0	0	0	0
Cloud Key Management Service (KMS) API	0	0	0	0
Cloud SQL Admin API	0	0	0	0
Google Cloud Storage	0	0	0	0
Google Cloud Storage JSON API	0	0	0	0
Google Drive API	0	0	0	0
Stackdriver Logging API	0	0	0	0

If any of the APIs is not enabled, use the below steps to enable it:

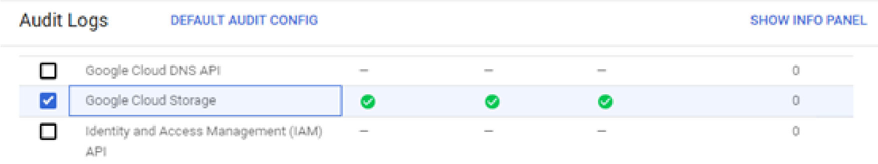
1. Go to the project want to be monitored.
2. Click the **Navigation Menu** ☰ in the upper-left corner, and select **APIs & Services > Dashboard**.
3. Click the **ENABLE APIS AND SERVICES** button on the top.
4. In the **Search for APIs & Services** field, enter the name of a required API.
5. From the search results, select the API.
6. Click the **ENABLE** button.
7. Wait until Google Cloud has enabled the API.

Note: While you are enabling an API, a dialog may pop up prompting you to enable billing. If that happens, follow the prompts onscreen to enable billing.

Enable activity and alert monitoring

If you would like to enable FortiCASB activity and alert monitoring, you must turn on audit logging using the following steps:

1. Go to the project to be monitored.
2. Click the Navigation Menu in the upper-left corner, and select **IAM & admin>Audit Logs.**
3. Select **Google Cloud Storage** in the list.
4. Enable all log types, i.e., **Admin Read, Data Read, and Data Write.**



Audit Logs DEFAULT AUDIT CONFIG SHOW INFO PANEL

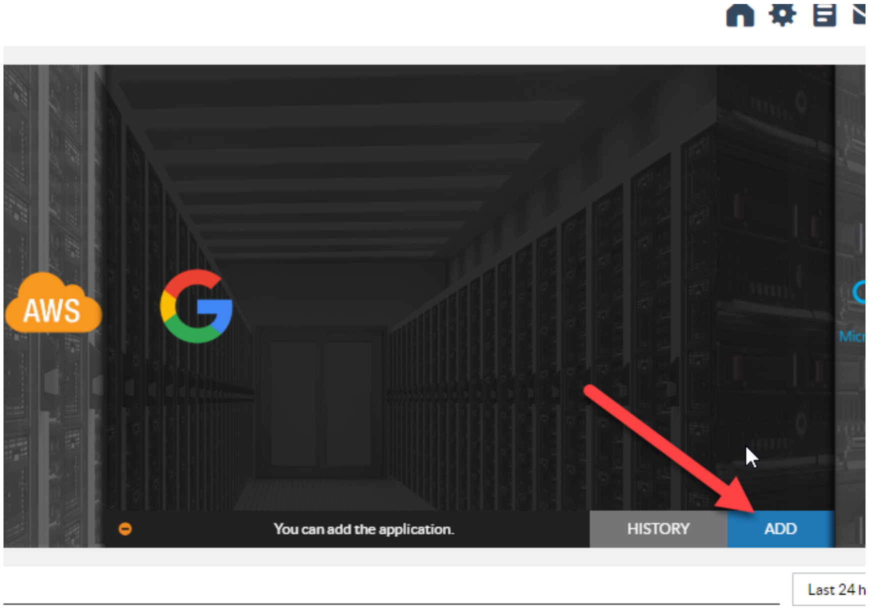
☐	Google Cloud DNS API	–	–	–	0
☑	Google Cloud Storage	✓	✓	✓	0
☐	Identity and Access Management (IAM) API	–	–	–	0

5. Click the **SAVE** button.

Installation

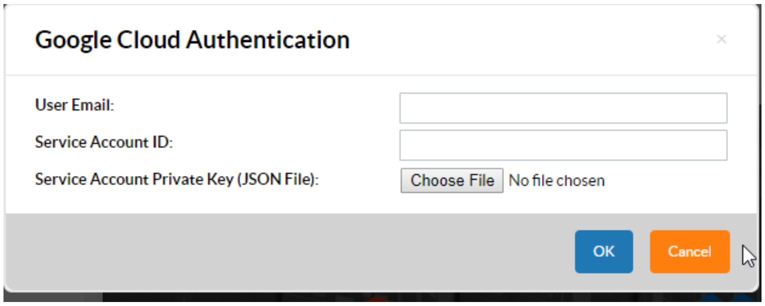
Once you have all the prerequisites in place, you can start installing Google Cloud using the following steps:

1. On the left-side of the page, click the menu, and select **Overview>Dashboard.**
2. From the Cloud App status widget, click **ADD** next to Google Cloud. The Google Cloud Authentication dialog will open.



You can add the application.

3. In Google Cloud Authentication dialog, for **User Email** field, enter your email address which you used to create the service account.



Google Cloud Authentication

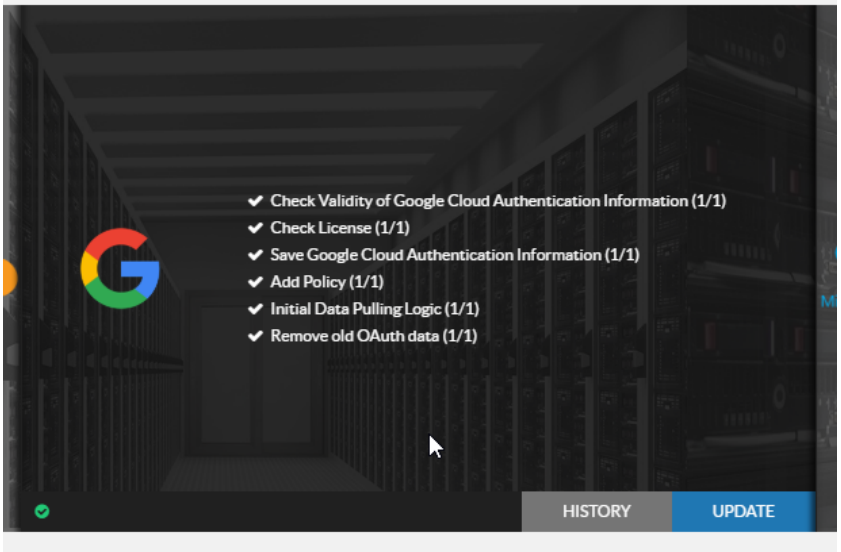
User Email:

Service Account ID:

Service Account Private Key (JSON File): Choose File No file chosen

4. In **Service Account ID** field, enter the ID of your service account. Your service account ID should end in ".gserviceaccount.com".
5. For **Service Account Private Key (JSON File)**, click **Choose** to browse and upload your service account's private key (i.e., a JSON file).
6. Click **OK**.

You will be redirected back to the FortiCASB dashboard. You can check the installation result and IaaS platform monitoring status in the Google Drive dashboard.



✓ Check Validity of Google Cloud Authentication Information (1/1)
✓ Check License (1/1)
✓ Save Google Cloud Authentication Information (1/1)
✓ Add Policy (1/1)
✓ Initial Data Pulling Logic (1/1)
✓ Remove old OAuth data (1/1)

Checking application monitoring status

FortiCASB starts to monitor immediately after the application has been successfully installed. To check if FortiCASB is monitoring, look for the green [Running] indicator on the application panel. If an error occurs, the light will turn red, and the application panel will guide you through the troubleshooting process.

Microsoft Azure

FortiCASB offers an API-based approach. It monitors Azure Cloud activity by using Web notification and by pulling data directly from Azure Cloud via the RESTful API. Authentication is done through OAUth2.0. FortiCASB uses an access token for API queries.

Prerequisites

You may use an existing **Azure AD** account or create a new account. If you create a new account, wait for at least 24 hours for the new account to take effect before granting access to FortiCASB.

Make sure your role is "Global Administrator" and that you have the **AzureAD "Premium P2"** license. Without the AzureAD "Premium P2" license, FortiCASB's Discovery feature cannot see user entitlements. All other functions will not be affected. For more information on how to obtain this license, go to:

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-get-started-premium

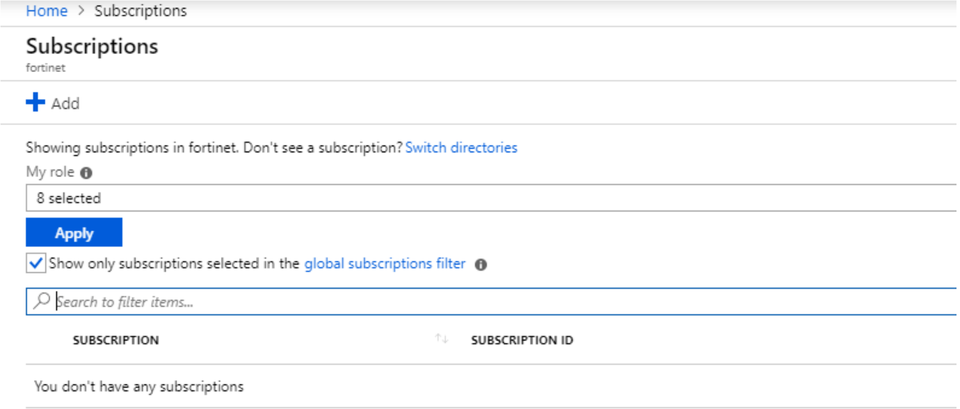
You will also need to set up the **AzureAD Privileged Identity Management** application. For more information on how to do so, go to:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure.

Make sure your license plan includes Active Directory integration. FortiCASB requires Active Directory support for most of its features.

Once you have your Azure license ready, you will need a subscription ID to use FortiCASB. If you do not have a subscription yet, please follow these steps:

1. Log into the Azure portal https://portal.azure.com using your Azure account.
2. Search and click on **Subscriptions**.
3. Click on **+Add** button to add a subscription.



Showing subscriptions in fortinet. Don't see a subscription? Switch directories

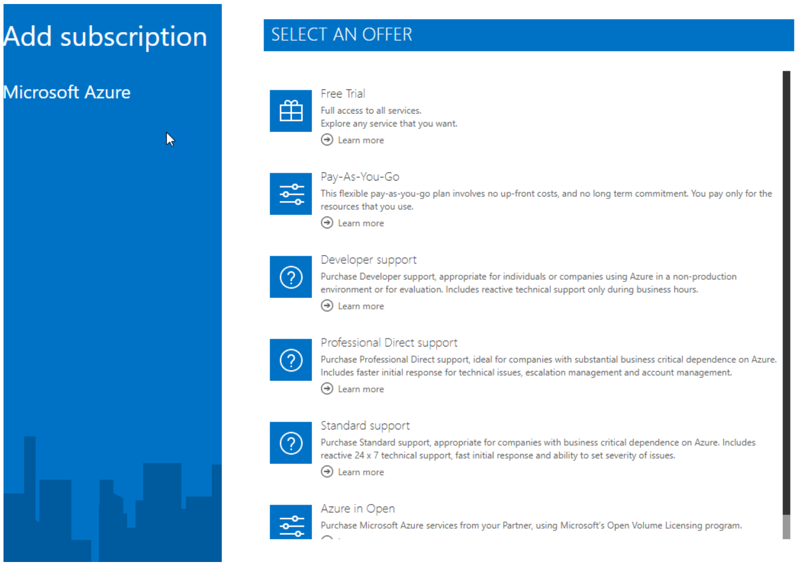
My role: 8 selected

☑ Show only subscriptions selected in the global subscriptions filter

Search to filter items...

SUBSCRIPTION	SUBSCRIPTION ID
You don't have any subscriptions	

4. Select the subscription desired and complete the rest of the billing steps.



Add subscription

Microsoft Azure

SELECT AN OFFER

Free Trial
Full access to all services.
Explore any service that you want.
Learn more

Pay-As-You-Go
This flexible pay-as-you-go plan involves no up-front costs, and no long term commitment. You pay only for the resources that you use.
Learn more

Developer support
Purchase Developer support, appropriate for individuals or companies using Azure in a non-production environment or for evaluation. Includes reactive technical support only during business hours.
Learn more

Professional Direct support
Purchase Professional Direct support, ideal for companies with substantial business critical dependence on Azure. Includes faster initial response for technical issues, escalation management and account management.
Learn more

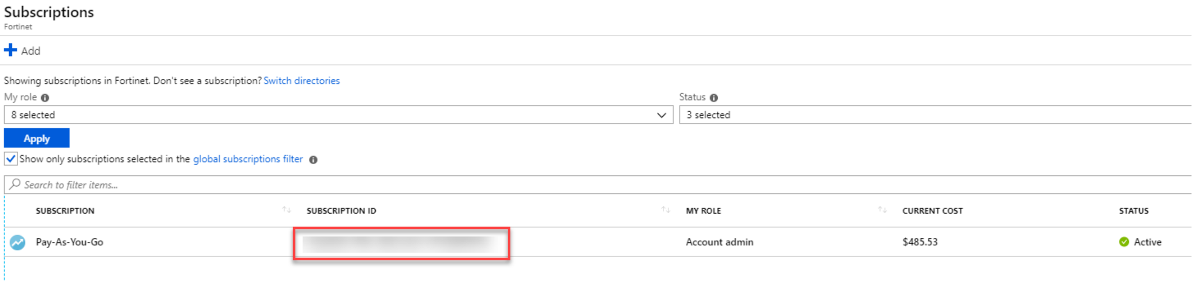
Standard support
Purchase Standard support, appropriate for companies with business critical dependence on Azure. Includes reactive 24 x 7 technical support, fast initial response and ability to set severity of issues.
Learn more

Azure in Open
Purchase Microsoft Azure services from your Partner, using Microsoft's Open Volume Licensing program.

Note: You will need a minimum of "Pay-As-You-Go" subscription to use FortiCASB.

To view your subscription ID after you have setup subscription, please follow these steps:

1. From the portal page, search and click on **Subscriptions**.
2. Once Subscriptions page opens, you will notice the **subscription ID** column next to the **subscription**.



Subscriptions
Fortinet

Showing subscriptions in Fortinet. Don't see a subscription? Switch directories

My role: 8 selected

Status: 3 selected

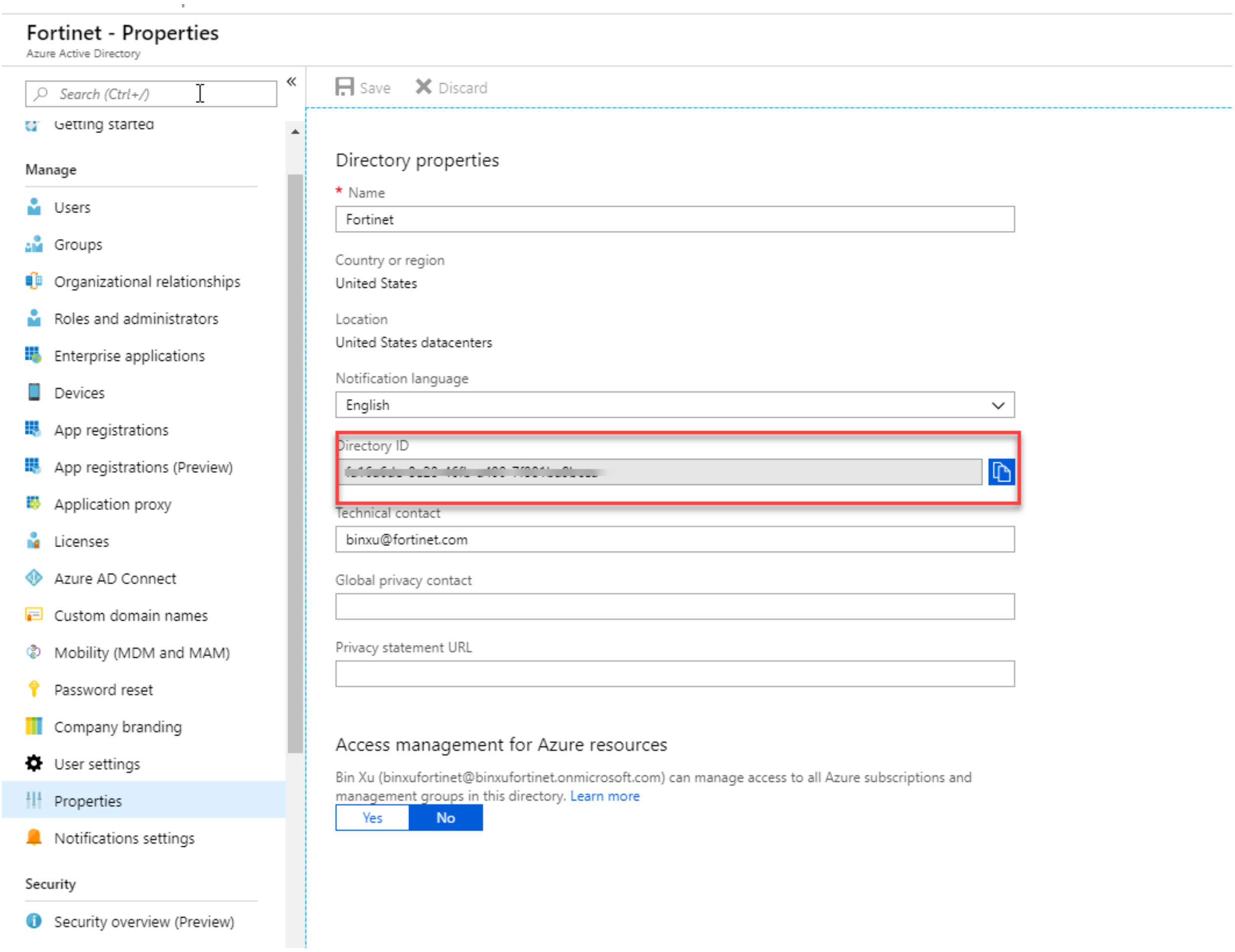
☑ Show only subscriptions selected in the global subscriptions filter

SUBSCRIPTION	SUBSCRIPTION ID	MY ROLE	CURRENT COST	STATUS
Pay-As-You-Go	[redacted]	Account admin	$485.53	✓ Active

Please keep the Subscription ID later for Azure authentication during installation.

Obtain **Directory ID** following the steps below:

1. From the portal page, search and click on **Azure Active Directory**.
2. Click on **MANAGE>Properties.**
3. Under **Directory properties**, you will find Directory ID.



Directory properties

* Name
Fortinet

Country or region
United States

Location
United States datacenters

Notification language
English

Directory ID
[redacted]

Technical contact
binxu@fortinet.com

Global privacy contact

Privacy statement URL

Access management for Azure resources

Bin Xu (binxufortinet@binxufortinet.onmicrosoft.com) can manage access to all Azure subscriptions and management groups in this directory. Learn more

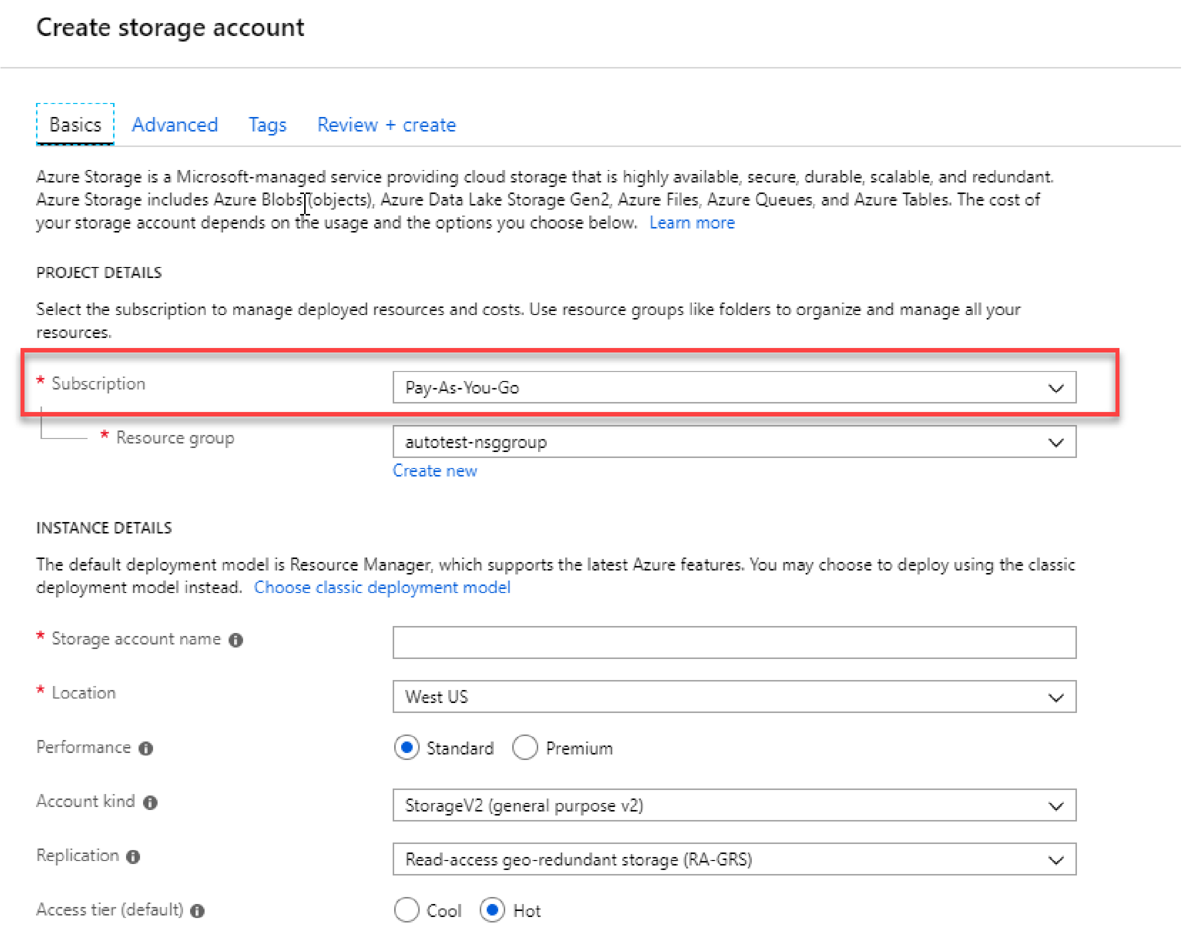
Yes [✓ No]

.

Please keep the Directory ID later for Azure authentication during installation.

A Storage account with blog log monitoring enabled is required to install FortiCASB. If you do not have a storage account yet, please follow the steps below to create a storage account:

1. From the portal page, search and click on **storage account**.
2. Click **+Add** to create a storage account.
3. Under **Basics > Subscription** field. Make sure you select the subscription that is linked to your subscription ID.



Create storage account

Basics | Advanced | Tags | Review + create

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. Learn more

PROJECT DETAILS

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

* Subscription	Pay-As-You-Go
* Resource group	autotest-nsggroup Create new

INSTANCE DETAILS

The default deployment model is Resource Manager, which supports the latest Azure features. You may choose to deploy using the classic deployment model instead. Choose classic deployment model

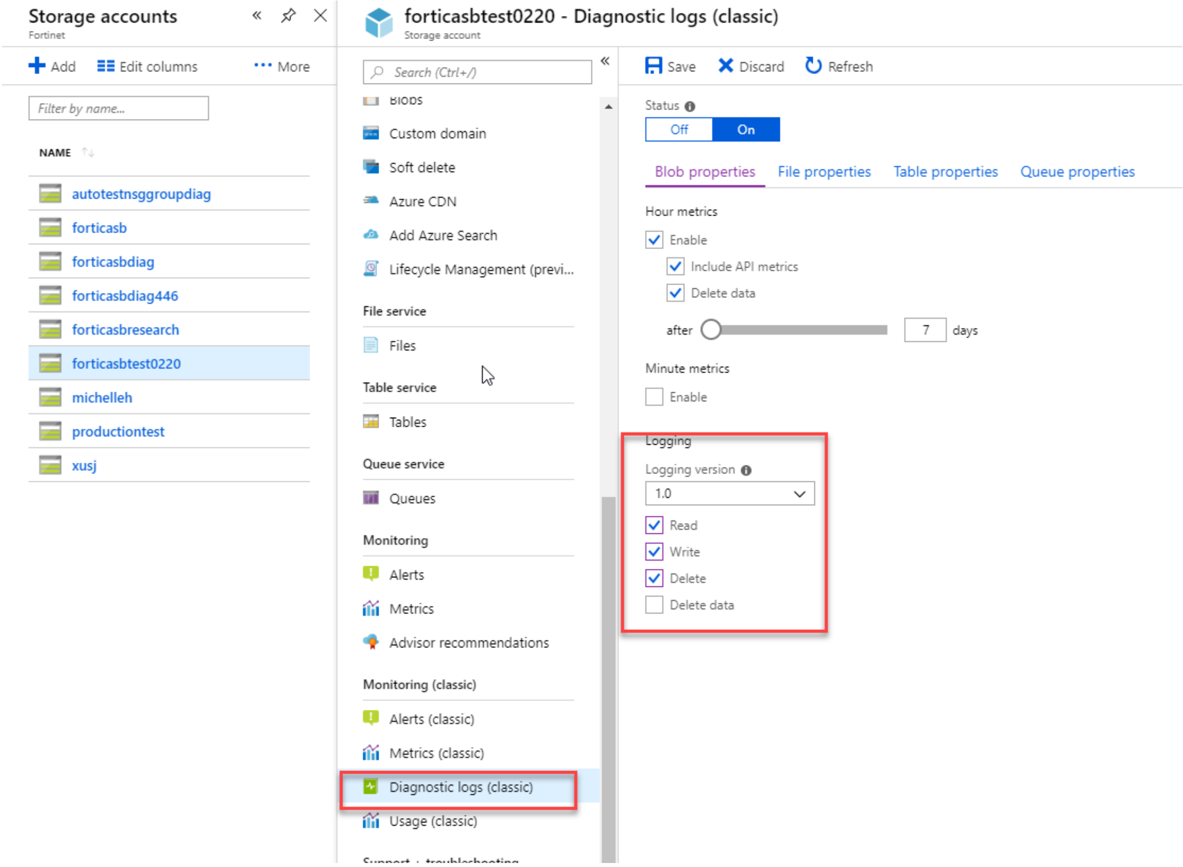
* Storage account name	
* Location	West US
Performance	● Standard ○ Premium
Account kind	StorageV2 (general purpose v2)
Replication	Read-access geo-redundant storage (RA-GRS)
Access tier (default)	○ Cool ● Hot

4. In **Resource group** field, select a resource group based on your preference or create a new one.
5. In **Storage account name** filed , enter an account name based on your preference.
6. Click **Review + create.** Once validation passed, click **Create.**

Once storage account is created, to enable blog log monitoring:

1. Select the storage account of interest.
2. From the left menu, select **Monitoring (classic) > Diagnostic settings**.

3. Turn **On** diagnostic logs. Under the **Blob properties**, enable **Read/Write/Delete** under **Logging**.



Status: Off [✓ On]

Hour metrics

☑ Enable

☑ Include API metrics

☑ Delete data

after 7 days

Minute metrics

☐ Enable

Logging

Logging version: 1.0

☑ Read

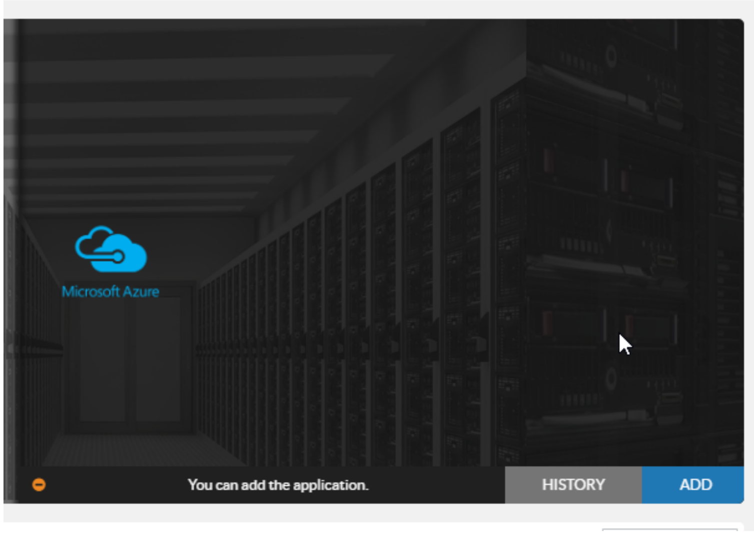
☑ Write

☑ Delete

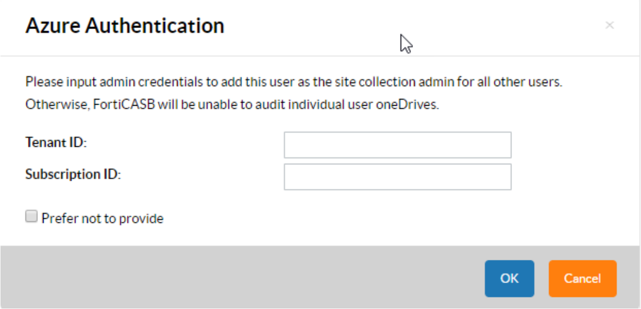
☐ Delete data

Installation

1. From the left-side menu, click **Overview>Dashboard**.
2. From the Cloud App widget, click **ADD** next to Microsoft Azure.



3. You are now prompted to provide your administrator credentials.



Azure Authentication

Please input admin credentials to add this user as the site collection admin for all other users. Otherwise, FortiCASB will be unable to audit individual user oneDrives.

Tenant ID:

Subscription ID:

☐ Prefer not to provide

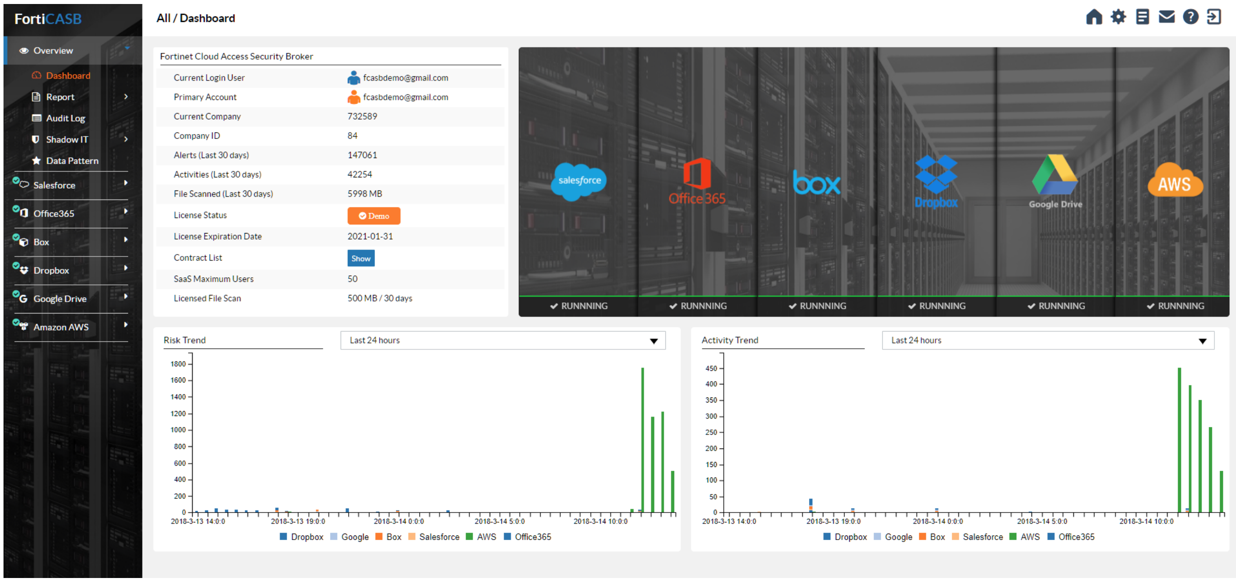
4. Enter Directory ID you saved earlier for **Tenant ID** field.
5. Enter your subscription ID you saved earlier for **Subscription ID** field.
6. Click **OK**.

Note: You can verify your installation and IaaS platform status from the Azure dashboard.

Checking application monitoring status

FortiCASB starts to monitor immediately after the application has been successfully installed. To check if FortiCASB is monitoring, look for the green [Running] indicator on the application panel. If an error occurs, the light will turn red, and the application panel will guide you through the troubleshooting process.

Using FortiCASB



Fortinet Cloud Access Security Broker

Current Login User	fcasbdemo@gmail.com
Primary Account	fcasbdemo@gmail.com
Current Company	732589
Company ID	84
Alerts (Last 30 days)	147061
Activities (Last 30 days)	42254
File Scanned (Last 30 days)	5998 MB
License Status	Demo
License Expiration Date	2021-01-31
Contract List	Show
SaaS Maximum Users	50
Licensed File Scan	500 MB / 30 days

FortiCASB classifies data as either data at rest or traffic data. Data at rest is data uploaded onto the cloud application before it has been linked with FortiCASB, while traffic data is any data uploaded after FortiCASB has started monitoring the cloud application.

Data at rest

You can run scans on the data in your cloud platforms to determine their contents. Depending on the policies you set, FortiCASB will classify this data as either sensitive data or non-sensitive data. This can be seen in the Discovery section for each cloud application.

If you don't run a manual scan, FortiCASB will scan files on an individual basis whenever a user accesses the file.

For more information on policies, see Policies on page 82..

For an explanation of the panels on the Discovery page, see Discovery on page 96.

For more details explaining the Document page, see Documents on page 99.

Traffic data

Activity

FortiCASB monitors user and data traffic for your cloud application. This is shown in the activity page.

For more information on what is monitored and logged as activity, see Activity on page 100.

For more information on how FortiCASB monitors users, see Users.

Alerts

FortiCASB sends you alerts when one of your set policies are triggered.

- DLP policies pertain to the types of data stored in the cloud application.
- Threat protection policies pertain to suspicious user activity.
- Compliance policies pertain to specific regulations, such as HIPAA, PCI, and SOX. See "Policies" on page 38 for specific policy descriptions.

See Policies on page 82 for specific policy descriptions.

Dashboard

For a description of the panels on the dashboard for each cloud application, see Dashboard on page 100.

Reports

FortiCASB allows you to generate reports. See Reports on page 64 for more information.

Audit log

FortiCASB records all administrator activities. You can filter your searches by using the Filter option. To access the Audit log page, go to **Overview > Audit log.**

Shadow IT discovery

When integrated with FortiGate or FortiAnalyzer, FortiCASB is able to provide an overview of all sanctioned and unsanctioned cloud applications throughout your organization. See Shadow IT discovery on page 71.

Data pattern

FortiCASB uses data patterns to create policies for monitoring files. You can create customized data patterns from the Data Pattern page. See Data pattern on page 80 for more information.

Risk Assessment

FortiCASB provides policies that check to see if your cloud application is following best practices. See Risk Assessment on page 133 for more information.

Buckets

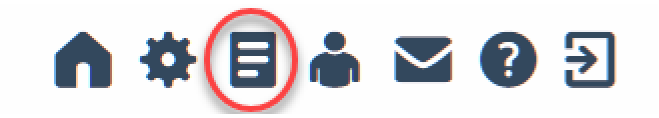
FortiCASB allows you to monitor Buckets in your AWS platform. To access the Buckets page, go to **AmazonAWS > Buckets** from the navigation menu on the left.

Logs

FortiCASB accesses your information by downloading files, scanning the downloads, then subsequently deleting the downloads at regular intervals.

NOTE: For your privacy, FortiCASB does not retain your files. You may check to see when and which files FortiCASB

has downloaded, scanned, and deleted by clicking the Logs button, located at the top-right corner.



General

Reports

FortiCASB allows you to generate C-level, Compliance, and Shadow IT reports.

C-Level reports are quarterly, monthly, or annual reports. Compliance reports give an overview of overall compliance with policies such as HIPAA, SOX/COBIT, and PCI. Shadow IT reports highlight unsanctioned application usage.

You can also export Compliance and Shadow IT reports.

Generating reports

C-Level

1. Go to **Overview > Report > C-Level**.
2. Choose a report type, a report year, and press **OK.**

Compliance

1. Go to **Overview > Report > Compliance**.
2. Click the arrow next to Overall Compliance Report.
3. Configure the settings shown, then click **Save**.
4. Choose to Post, Export, or Preview the report.

Shadow IT

1. Go to **Overview > Report > Shadow IT**.
2. Click the arrow next to Shadow IT Report.
3. Configure the settings shown, then click **Save**.
4. Choose to Post or Export the report.

Viewing reports

You may select previously generated C-Level reports to view from the Overview tab. Click the View icon to view the report.

Exporting reports

While creating a Compliance or Shadow IT report, press the **Export** button. This will save the report in your selected file format.

Event list

This shows the types of events FortiCASB supports. These types of events will be traced at the activity page, and they can also be used as criteria when configuring policy and applying filters.

The File Download event is monitored within the FortiCASB Audit log. To find the audit log, go to **Overview > Audit Log** from the navigation menu on the left.

Salesforce

Login	Login Success
	Login Failed
User	Create User
	Modify User
	Change Password
	Activate User
	Deactivate User
	Change User Profile
	Change User Role
	Change User Email
	Change User Permission Set
Group	Add Group
	Add Group Member
	Update Group
	Change Group Access
	Add External Group Member (Customer)
	Invite People

Profile	Create Profile
	Modify Profile
Permission Set	Add Permission Set
	Modify Permission Set
Feed	Post
	Modify Post
	Comment
	Modify Comment
File	Upload File
	Upload New Version
	Download File
	Edit File
Share	Share File
	Share File with People
	Share File with Group
	Share File via Link
	Download File via Link
Business	Account Modification
	Account Owner Change
	Contact Modification
	Contact Owner Change
	Account Create
	Contact Create

Office 365

Login	Login Success
	Login Failed
User	Create User
	Delete User
	Modify User
	Restore User

	Change Password
	Modify Role
Group	Add Group
	Delete Group
	Add Group Member
	Update Group
	Add Group Owner
	Delete Group Owner
	Set Group Managed By
	Create Group Settings
	Update Group Settings
	Delete Group Settings
	Set Group License
File	Upload File
	Delete File
	Download File
	Modify File
	Access File
	Move File
	Copy File
	Rename File
	Edit File
Share	Share File
	Create Anonymous Link
	Delete Anonymous Link
	Create Company Link
	Delete Company Link
	Company Link Used
Other	Modify License
	Delete Folder
	Create Sharing Invitation
	Edit Company Info

Box

File/Folder	Upload File
	Copy File
	Download File
	Edit File
	Move File
	Preview File
	Rename File
	Open File
	Modify File
	Create Lock
	Comment
Login	Login Success
	Login Failed
User	Create User
	Modify User
	Delete User
Group	Add Group
	Update Group
	Group Add Membership
Metadata	Create Metadata Template
	Update Metadata Template
	Create Metadata Instance
	Update Metadata Instance
Collaboration	Collaboration Invite
	Collaboration Accept
	Collaboration Role Change
	Update Collaboration Expiration
	Collaboration Expiration

Share	Share File
	Update Shared File
	Update Shared Expiration
	Share Expiration

Dropbox Business

Login	Login Success
	Login Failed
	Logout
	Login As User Session Start
	Login As User Session End
User (Member)	Create User
	User Change Name
	User Change Status
	User Change Admin Role
	User Change Email
	Change Password
	Password Restore
	Password Restore All
Group	Add Group
	Delete Group
	Add Group Member
	Remove Group Member
	Group Rename
File	File Add
	File Download
	File Preview
	File Edit
	File Delete

	File Add Comment
	File Move
	File Copy
	File Rename
	File Restore
	File Revert
File Share	Share Link Create
	Share Link Create Password
	Share Link Public
	Share Link Disable
	Share Link Team Only
	Share Link Set Expiration
	Share Link Remove Expiration
	Share Link View
	Share Link Download
	Share Link Team Copy

Google

Login	Login Success
	Login Failure
	Login Challenge
	Logout
File	Create File
	Upload File
	Edit File
	View File
	Rename File
	Move File
	Delete File
	Download File
	Preview File

	Trash File
	Untrash File
User	Create User
	Suspend User
	Unsuspend User
	Modify User
	Change Password
	Create Data Transfer Request
	Delete User
	Assign Role
	Unassign Role

Shadow IT discovery

FortiCASB provides features for shadow IT discovery. By integrating with FortiGate and FortiAnalyzer, FortiCASB gives users a concrete overview of all sanctioned and unsanctioned cloud applications organization wide. Furthermore, FortiCASB calculates a risk score for each application and gives users the ability to control application usage.

FortiCASB's Shadow IT discovery helps users enhance the security of their cloud application environment with the following features:

- **Unsanctioned Application Discovery**—FortiCASB uses logs from FortiGate and FortiAnalyzer as well as its own discovery process to deliver a comprehensive view of risk and usage of cloud applications.
- **Cloud Risk Score**—FortiCASB generates a cloud risk score for each cloud application. This score is calculated using many factors, such as but not limited to: user numbers, size of the company, multi-factor authentication support, and service hosting location. These factors are used to generate scores in multiple criteria, which are then aggregated into one final score. Users can prioritize these criteria to match their needs.
- **Access Control**—Users can block or monitor certain applications using FortiCASB and FortiGate.
- **Data Correlation**—FortiCASB uses data from FortiGate and FortiAnalyzer, as well as its own data to define and identify riskier activities.

Configuration and requirements

Shadow IT discovery requires a FortiGate or FortiAnalyzer policy.

Configuration details depend on your specific setup requirements. See the scenarios below, and find the one which best suits your needs.

Scenario 1: You want to receive logs from FortiGate.

- See FortiGate configuration. After step 13, follow the instructions under Log configuration using FortiGate GUI on page 76l. Then, follow the instructions under FortiCASB configuration as needed.

Scenario 2: You want to receive logs from FortiGate, but it is already providing logs to another device.

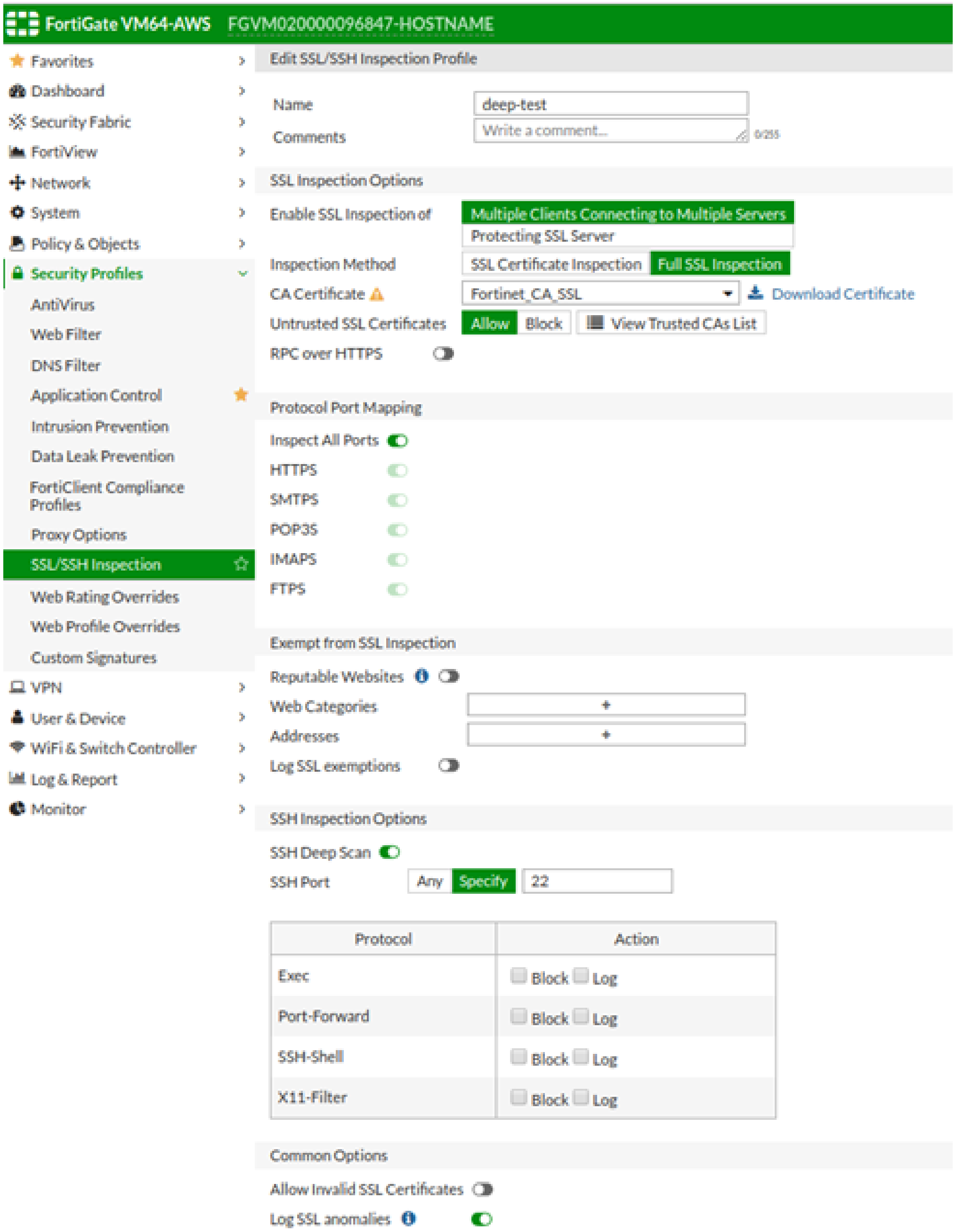
- See FortiGate configuration. After step 13, follow the instructions under Log configuration using FortiGate CLI. Then, follow the instructions under FortiCASB configuration as needed.

Scenario 3: You want to receive logs from FortiAnalyzer.

- See FortiAnalyzer configuration. Then, follow the instructions under FortiCASB configuration as needed.

FortiGate configuration

1. Go to **Security Profiles > SSL/SSH Inspection.**
2. Create a new SSL/SSH inspection profile called **deep-test.**
3. Configure the profile as shown below:



Edit SSL/SSH Inspection Profile

Name: deep-test
Comments: Write a comment... 0/255

SSL Inspection Options

Enable SSL Inspection of: Multiple Clients Connecting to Multiple Servers | Protecting SSL Server
Inspection Method: SSL Certificate Inspection | Full SSL Inspection
CA Certificate ⚠: Fortinet_CA_SSL — Download Certificate
Untrusted SSL Certificates: Allow | Block — View Trusted CAs List
RPC over HTTPS ○

Protocol Port Mapping

Inspect All Ports ●
HTTPS
SMTPS
POP3S
IMAPS
FTPS

Exempt from SSL Inspection

Reputable Websites ○
Web Categories: +
Addresses: +
Log SSL exemptions ○

SSH Inspection Options

SSH Deep Scan ●
SSH Port: Any | Specify 22

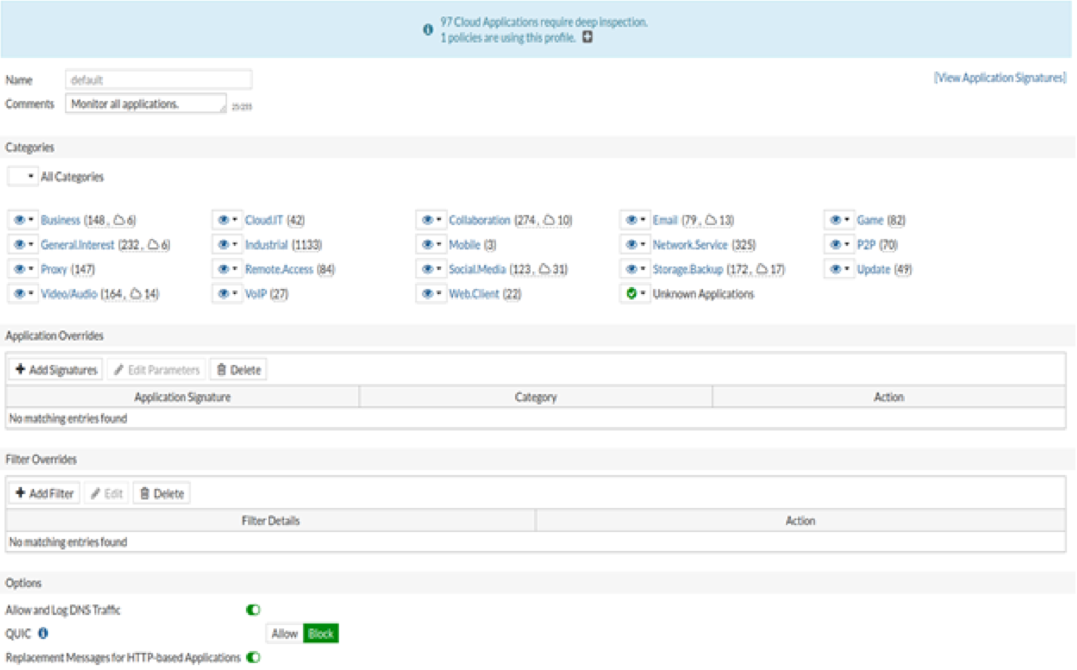
Protocol	Action
Exec	□ Block □ Log
Port-Forward	□ Block □ Log
SSH-Shell	□ Block □ Log
X11-Filter	□ Block □ Log

Common Options

Allow Invalid SSL Certificates ○
Log SSL anomalies ●

4. Go to **Security Profiles > Application Control.**
5. Set all categories to **Monitor**.
6. Under Options, enable **Allow and Log DNS Traffic** and **Replacement Messages for HTTP-based Applications**.

FortiGate 5.6



97 Cloud Applications require deep inspection.
1 policies are using this profile.

Name: default

Comments: Monitor all applications. 25/255

[View Application Signatures]

Categories

All Categories

Business (148, 6)	Cloud.IT (42)	Collaboration (274, 10)	Email (79, 13)	Game (82)
General.Interest (232, 6)	Industrial (1133)	Mobile (3)	Network.Service (325)	P2P (70)
Proxy (147)	Remote.Access (84)	Social.Media (123, 31)	Storage.Backup (172, 17)	Update (49)
Video/Audio (164, 14)	VoIP (27)	Web.Client (22)	Unknown Applications	

Application Overrides

Add Signatures | Edit Parameters | Delete

Application Signature	Category	Action
No matching entries found		

Filter Overrides

Add Filter | Edit | Delete

Filter Details	Action
No matching entries found	

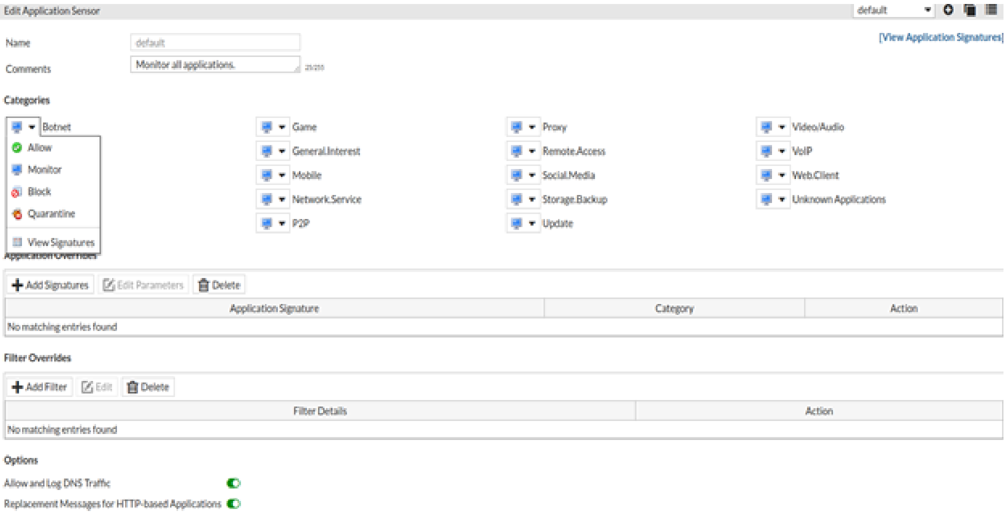
Options

Allow and Log DNS Traffic

QUIC: Allow [✓ Block]

Replacement Messages for HTTP-based Applications

FortiGate 5.4



Edit Application Sensor — default

Name: default

Comments: Monitor all applications. 25/255

[View Application Signatures]

Categories

Botnet	Game	Proxy	Video/Audio
	General.Interest	Remote.Access	VoIP
	Mobile	Social.Media	Web.Client
	Network.Service	Storage.Backup	Unknown Applications
	P2P	Update	

Application Overrides

Add Signatures | Edit Parameters | Delete

Application Signature	Category	Action
No matching entries found		

Filter Overrides

Add Filter | Edit | Delete

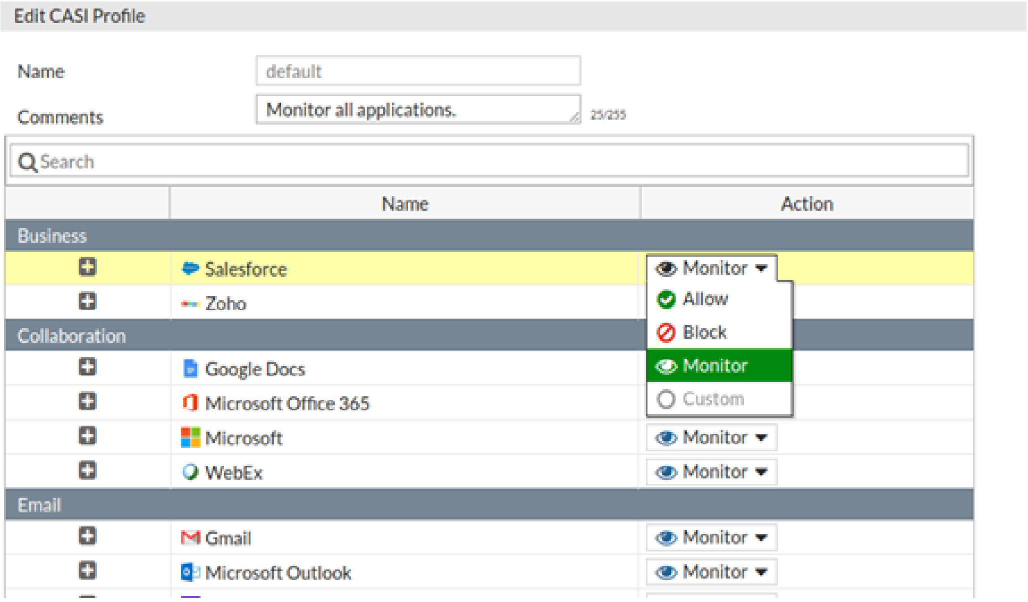
Filter Details	Action
No matching entries found	

Options

Allow and Log DNS Traffic

Replacement Messages for HTTP-based Applications

7. Go to **Security Profiles > Cloud Access Security Inspection**.
8. Under the Action column, set all action to **Monitor**.



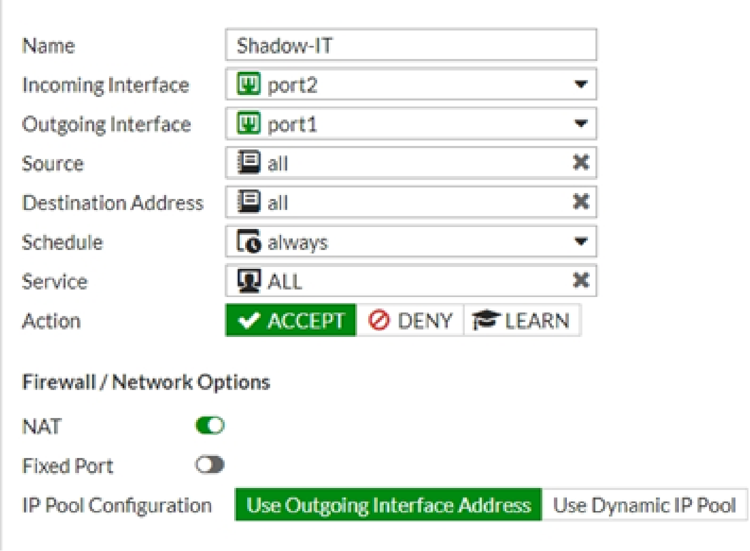
Edit CASI Profile

Name	default
Comments	Monitor all applications. 25/255

Search

	Name	Action
Business		
⊞	Salesforce	Monitor ▾
⊞	Zoho	
Collaboration		
⊞	Google Docs	
⊞	Microsoft Office 365	
⊞	Microsoft	Monitor ▾
⊞	WebEx	Monitor ▾
Email		
⊞	Gmail	Monitor ▾
⊞	Microsoft Outlook	Monitor ▾

9. Go to **Policy & Objects > IPv4 Policy**.
10. Create a new policy named **Shadow-IT.**
11. Configure the policy as shown below:



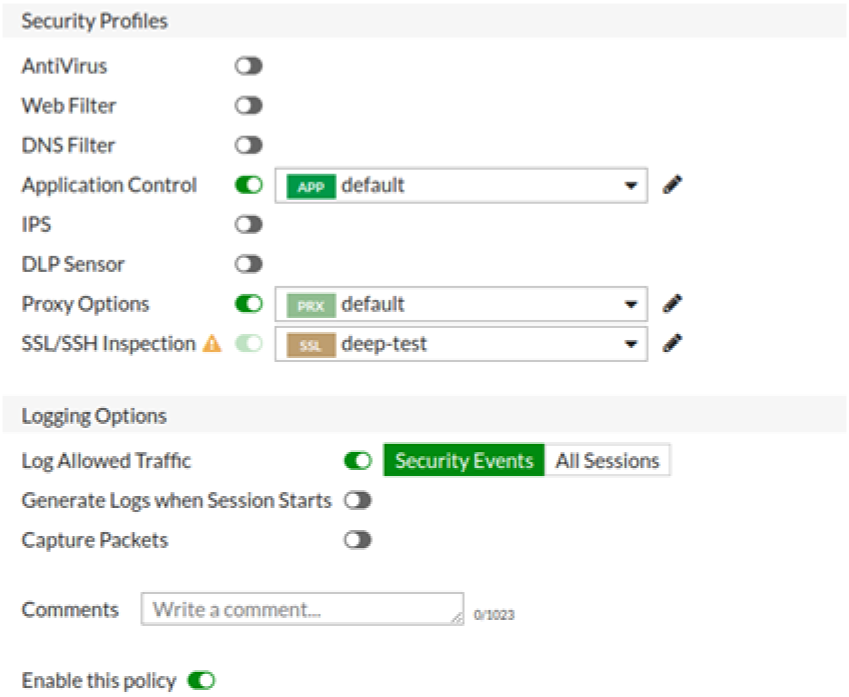
Name	Shadow-IT
Incoming Interface	port2
Outgoing Interface	port1
Source	all
Destination Address	all
Schedule	always
Service	ALL
Action	[✓ ACCEPT] DENY LEARN

Firewall / Network Options

NAT	● on
Fixed Port	○ off
IP Pool Configuration	[✓ Use Outgoing Interface Address] Use Dynamic IP Pool

12. Configure Security Profiles.
    a. To use access control, choose the **Web Filte**r created with the URL filter set.
    b. Open **Application Control** to allow FortiCASB to track how many cloud applications are visited.
    c. To correlate log data with FortiCASB data, make sure **Application Control** is open, and set **SSL/SSH Inspection** to **deep-test**.

NOTE: For FortiGate 5.4, set CASI to the default.



Security Profiles

AntiVirus

Web Filter

DNS Filter

Application Control APP default

IPS

DLP Sensor

Proxy Options PRX default

SSL/SSH Inspection SSL deep-test

Logging Options

Log Allowed Traffic Security Events All Sessions

Generate Logs when Session Starts

Capture Packets

Comments Write a comment... 0/1023

Enable this policy

13. Open Log Allowed Traffic, and select either **Security Events** or **All Sessions**.

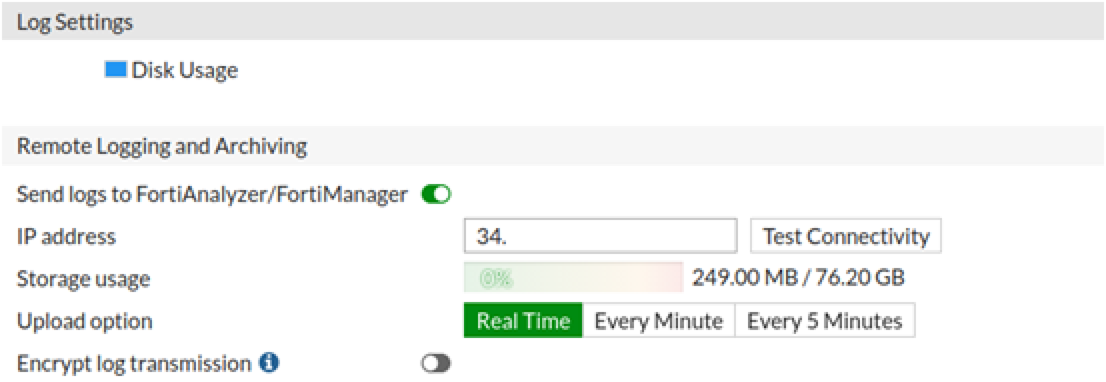
Log configuration using FortiGate GUI

14. Go to **Log & Report > Log Settings.**
15. Open **Send Logs** to **FortiAnalyzer/FortiManager.**
16. Set the FortiCASB receiver's IP address for IP Address.

The FortiCASB receiver IP address can be found by pressing the **Device** button from the FortiCASB Shadow IT dashboard. It will be one of the followin addresses:

Global Users	34.212.87.235 or 52.27.136.156
EU Users	34.254.217.50 or 52.18.7.98

Enter the IP address into the appropriate section of the FortiGate UI, shown below, then click **Test Connectivity.**



Log Settings

Disk Usage

Remote Logging and Archiving

Send logs to FortiAnalyzer/FortiManager

IP address 34. Test Connectivity

Storage usage 0% 249.00 MB / 76.20 GB

Upload option Real Time Every Minute Every 5 Minutes

Encrypt log transmission

Log configuration using FortiGate CLI

17. Login to the FortiGate's CLI mode.
18. Configure log settings for the second FortiAnalyzer device on the FortiGate.

```
#config log fortianalyzer2 setting
  #set status enable
  #set server <FortiCASB server IP>
  #set enc-algorithm high-medium
  #set upload-option realtime
  #set reliable enable
#end
```

19. Configure the log filter to only forward application-ctrl logs:

```
#config log fortianalyzer2 filter
  #set filter-type include
  #set filter "logid(1059028704)"
#end
```

20. Test the connection using the following CLI command:

```
#execute log fortianalyzer test-connectivity 2
```

If the connection is successful, the FortiGate will return the following:

```
Registration: registered
Connection: allow
```

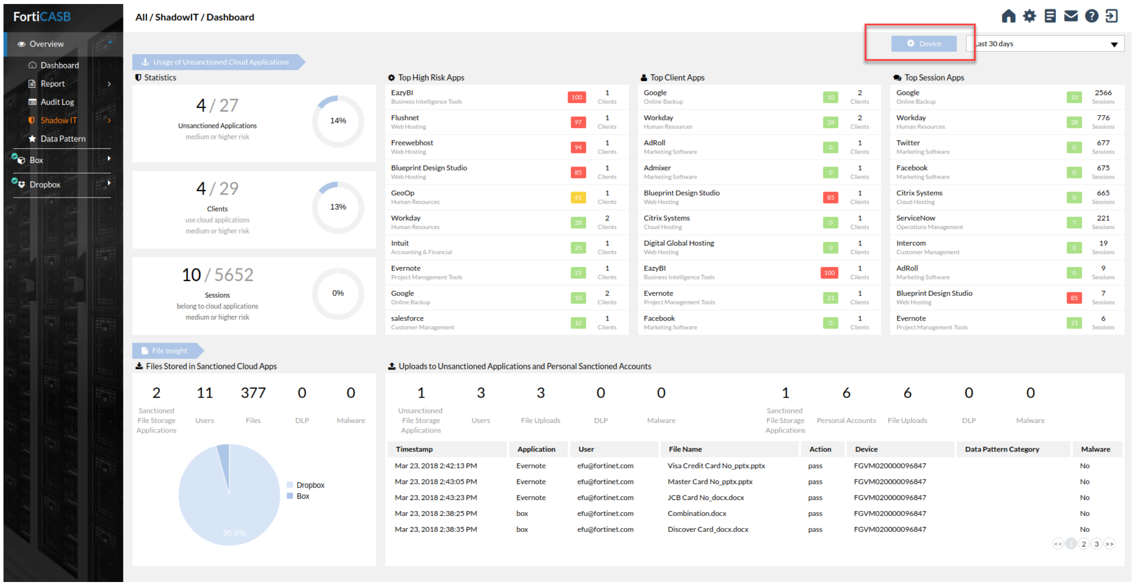
Otherwise, the FortiGate will return an error code.

FortiAnalyzer configuration

1. Provide a public IPv4 address to your FortiAnalyzer. Make sure this IP address with the appropriate TCP port(default 443) can be accessed from the external network, via the internet.
2. Finish steps 1-12 of the FortiGate configuration.
3. Use the following commands to add RPC-permit's read and write permissions to the user:
   a. config system admin user
   b. edit admin
   c. set rpc-permit read-write

FortiCASB configuration

1. Choose the device type to connect.
   a. Click the **Device** button, located on the top right, from the Shadow IT dashboard.



4 / 27
Unsanctioned Applications
medium or higher risk

4 / 29
Clients
use cloud applications
medium or higher risk

10 / 5652
Sessions
belong to cloud applications
medium or higher risk

Top High Risk Apps

EazyBI Business Intelligence Tools	100	1 Clients
Flushnet Web Hosting	97	1 Clients
Freewebhost Web Hosting	94	1 Clients
Blueprint Design Studio Web Hosting	85	1 Clients
GeoOp Human Resources	41	1 Clients
Workday Human Resources	28	2 Clients
Intuit Accounting & Financial	25	1 Clients
Evernote Project Management Tools	21	1 Clients
Google Online Backup	10	2 Clients
salesforce Customer Management	10	1 Clients

Top Client Apps

Google Online Backup	10	2 Clients
Workday Human Resources	28	2 Clients
AdRoll Marketing Software	0	1 Clients
Admixer Marketing Software	0	1 Clients
Blueprint Design Studio Web Hosting	85	1 Clients
Citrix Systems Cloud Hosting	0	1 Clients
Digital Global Hosting Web Hosting	0	1 Clients
EazyBI Business Intelligence Tools	100	1 Clients
Evernote Project Management Tools	21	1 Clients
Facebook Marketing Software	0	1 Clients

Top Session Apps

Google Online Backup	10	2566 Sessions
Workday Human Resources	28	776 Sessions
Twitter Marketing Software	0	677 Sessions
Facebook Marketing Software	0	675 Sessions
Citrix Systems Cloud Hosting	0	665 Sessions
ServiceNow Operations Management	7	221 Sessions
Intercom Customer Management	0	19 Sessions
AdRoll Marketing Software	0	9 Sessions
Blueprint Design Studio Web Hosting	85	7 Sessions
Evernote Project Management Tools	21	6 Sessions

Files Stored in Sanctioned Cloud Apps

2	11	377	0	0
Sanctioned File Storage Applications	Users	Files	DLP	Malware

Uploads to Unsanctioned Applications and Personal Sanctioned Accounts

1	3	3	0	0	1	6	6	0	0
Unsanctioned File Storage Applications	Users	File Uploads	DLP	Malware	Sanctioned File Storage Applications	Personal Accounts	File Uploads	DLP	Malware

Timestamp	Application	User	File Name	Action	Device	Data Pattern Category	Malware
Mar 23, 2018 2:42:13 PM	Evernote	efu@fortinet.com	Visa Credit Card No_pptx.pptx	pass	FGVM020000096847		No
Mar 23, 2018 2:43:05 PM	Evernote	efu@fortinet.com	Master Card No_pptx.pptx	pass	FGVM020000096847		No
Mar 23, 2018 2:43:23 PM	Evernote	efu@fortinet.com	JCB Card No_docx.docx	pass	FGVM020000096847		No
Mar 23, 2018 2:38:25 PM	box	efu@fortinet.com	Combination.docx	pass	FGVM020000096847		No
Mar 23, 2018 2:38:35 PM	box	efu@fortinet.com	Discover Card_docx.docx	pass	FGVM020000096847		No

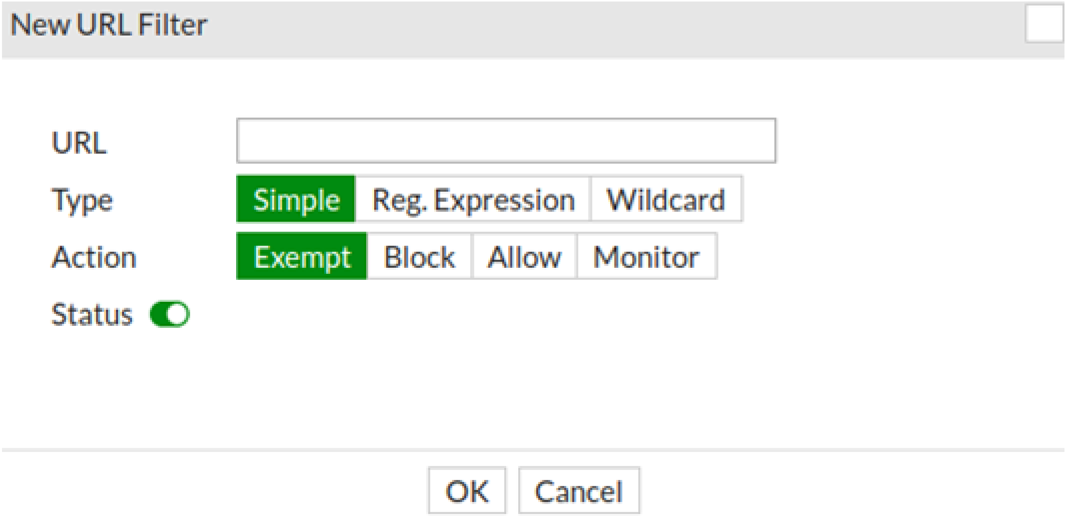
   b. Choose either FortiGate or FortiAnalyzer.
2. Enter the device DevID.
   a. If the DevID is for FortiGate, fill in the other fields.
   b. If the DevID is for FortiAnalyzer, fill in the other fields, then select the FortiGate device(s) to add.

Using Shadow IT discovery

Access control

After analyzing an application using FortiCASB, users can use FortiGate's Web Filter to block or monitor the application.

1. Use FortiCASB to get the host name of the traffic to be controlled.
2. On the FortiGate device, go to **Security Profile > Web Filter.**
3. Under Static URL Filter, choose the URL filter.
4. Click **Create** to add a new URL filter.
5. Choose a Type.
6. Choose an Action.
7. Set Status to **Open**.
8. Click **OK**.



New URL Filter

URL

Type: Simple

Action: Exempt

Status: ●

Shadow IT Dashboard

Usage of unsanctioned cloud applications

All unsanctioned cloud applications are given a ranking based on the risk score, the number of users, and volume of use. FortiCASB uses that data to pinpoint and display the applications, clients, and sessions that are most at risk. FortiCASB also displays the percentage of risky applications, clients, and sessions using pie charts.

File insight

File insight shows the total number of sanctioned cloud applications the organization is using, the total number of users, and the total number of files stored in each cloud application.

Application list

The application list displays all appliations monitored by FortiCASB. Filter the list using the time range box on the top right, the risk score slider on the top left, and the categories checkboxes on the left.

Click a specific application to display detailed information regarding the application.

Data pattern

FortiCASB uses data patterns to create policies for monitoring files. You can create customized data patterns from the Data Pattern page. These data patterns can be used when creating customized policies.

To create a customized data pattern, follow the steps below:

1. Go to **Overview > Data Pattern**.
2. Fill in the settings shown

Name	Enter a name for the data pattern.
Description	Enter a description for the data pattern.
Category	Select a data category from the list.
File Extensions	Specify file types to be monitored.
Uncompressed File Size	Specify the upper bound of an object size, in MB, for a full content scan.
Compressed File Size	Specify the upper bound of a zip file size, in MB, for a full content scan.
Regex Context	Enter in a phrase or string of characters, andwill monitor any file containing that phrase.

3. Click **+Add.**

Group IP

FortiCASB lets you group multiple IPs across different IAAS cloud platforms so you can easily track activities from external or suspicious IPs on your cloud resources.

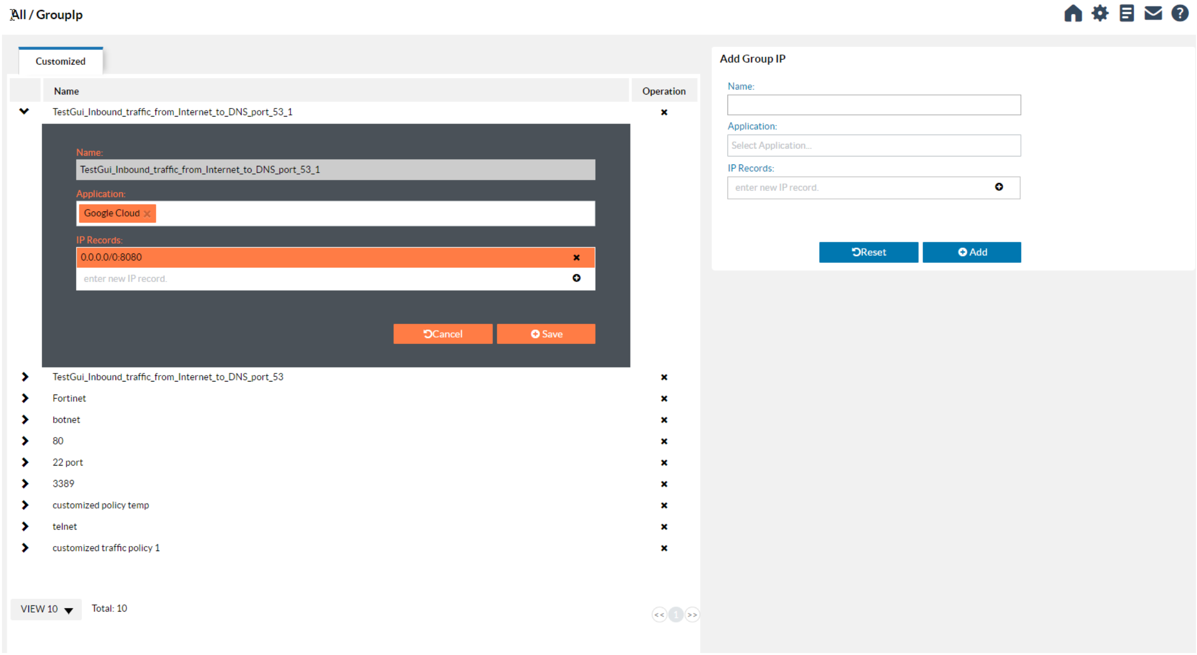
Prerequisites

An active IAAS account installed on FortiCASB.

For installing IAAS account on FortiCASB, please refer to Getting Started > Installing IAAS applications on page 33

1. Log into FortiCASB with your FortiCASB user account: https://www.forticasb.com/
2. In FortiCASB Dashboard, select **Overview** > **Group IP**

3. **Customized** tab lists all groups of customized grouped IPs.
4. **Add Group IP** lets you add customized group IPs to the list.



All / GroupIp

Customized

Name	Operation
TestGui_Inbound_traffic_from_Internet_to_DNS_port_53_1	×
TestGui_Inbound_traffic_from_Internet_to_DNS_port_53	×
Fortinet	×
botnet	×
80	×
22 port	×
3389	×
customized policy temp	×
telnet	×
customized traffic policy 1	×

Name: TestGui_Inbound_traffic_from_Internet_to_DNS_port_53_1

Application: Google Cloud ×

IP Records: 0.0.0.0/0:8080 ×

enter new IP record.

Add Group IP

Name:

Application: Select Application...

IP Records: enter new IP record.

Application Specific Features

Policies

FortiCASB uses policies for two purposes:

- Scans and reports use policies you set to differentiate between sensitive and non-sensitive data.
- Alerts are generated depending on the policies you set.

Default policies

FortiCASB offers Data Analysis (DA) policies, Threat Protection policies, Compliance policies, and Customized policies.

Data Analysis

DA policies keep track of sensitive data. For example, if a user accesses a file containing Social Security Numbers (SSNs) and you have the SSN policy set, FortiCASB will send you an alert.

File types supported for DA scans

Uncompressed	Microsoft Word Document (.doc, .docx)
	Microsoft Powerpoint Document (.ppt, .pptx)
	Microsft Excel Document (.xls, .xlx)
	Text File (.txt, .rtf)
Compressed .zip	.zip
	.tar
	.7z
	.gz

DA policies

Data Analysis policies trigger alerts whenever a monitored file is accessed, regardless of the type of access. If you only want alerts for specific actions, set a Customized policy.

Identity number

US SSN Policy	FortiCASB scans for SSNs during Discovery scans, and triggers an alert when targets with SSNs are accessed.
CN Resident Identity Policy	FortiCASB scans for CN resident identity numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.

Credit card number

Visa Credit Card Policy	FortiCASB scans for Visa credit card numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
MasterCard Policy	FortiCASB scans for MasterCard credit card numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
American Express Policy	FortiCASB scans for American Express credit card numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
Diners Club Card Policy	FortiCASB scans for Diners Club credit card numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
Discover Card Policy	FortiCASB scans for Discover credit card numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
JCB Policy	FortiCASB scans for JCB credit card numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
Maestro Card Policy	FortiCASB scans for Maestro credit card numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.

Driver license number

UK Driver License Policy	FortiCASB scans for UK driver license numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
US-FL Driver License Policy	FortiCASB scans for FL driver license numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
US-CA Driver License Policy	FortiCASB scans for CA driver license numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
CN Driver License Policy	FortiCASB scans for CN driver license numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.

Email address

Email Address	Policy FortiCASB scans for email addresses during Discovery scans, and triggers an alert when targets with email addresses are accessed.

Insurance number

CA Insurance Number Policy	FortiCASB scans for CA insurance numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
UK Insurance Number Policy	FortiCASB scans for UK insurance numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.

Passport number

UK Passport Number Policy	FortiCASB scans for UK passport numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
CN Passport Number Policy	FortiCASB scans for CN passport numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
USA/Germany Passport Number Policy	FortiCASB scans for USA/Germany passport numbers

	during Discovery scans, and triggers an alert when targets with such numbers are accessed.
AU Passport Number Policy	FortiCASB scans for AU passport numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
JP Passport Number Policy	FortiCASB scans for JP passport numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
CA Passport Number Policy	FortiCASB scans for CA passport numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
FR Passport Number Policy	FortiCASB scans for FR passport numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.

Bank account number

China Union Pay Policy	FortiCASB scans for China Union Pay account numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
UK IBAN Policy	FortiCASB scans for UK IBANs during Discovery scans, and triggers an alert when targets with such IBANs are accessed.
Swiss IBAN Policy	FortiCASB scans for Swiss IBANs during Discovery scans, and triggers an alert when targets with such IBANs are accessed.
German IBAN Policy	FortiCASB scans for German IBANs during Discovery scans, and triggers an alert when targets with such IBANs are accessed.
Italian IBAN Policy	FortiCASB scans for Italian IBANs during Discovery scans, and triggers an alert when targets with such IBANs are accessed.
Swedish IBAN Policy	FortiCASB scans for Swedish IBANs during Discovery scans, and triggers an alert when targets with such IBANs are accessed.
Spanish IBAN Policy	FortiCASB scans for Spanish IBANs during Discovery scans, and triggers an alert when targets with such IBANs are accessed.

Birthdate

Birthdate Policy	FortiCASB scans for birthdates during Discovery scans, and triggers an alert when targets with birthdates are accessed.

Malware/Ransomware

Ransomware Encrypted File Detection Policy	FortiCASB scans for Ransomware Encrypted File during Discovery scans, and triggers an alert when targets are accessed.

Threat protection

Threat protection policies track suspicious user behavior. For example, if a user fails to enter his or her password correctly multiple times in a row and you have the Excessive Login Failures policy active, FortiCASB will send you an alert.

Threat protection policies

Access

Excessive Login Failures	Triggers an alert when the number of failed logins for a user exceeds a set threshold.
Password Change	Triggers an alert when passwords are changed.
Suspicious Movement	Triggers an alert when a change in a user's geographic location exceeds threshold parameters.
Unapproved Login Location	Triggers an alert when a user logs in from an unapproved geographic location.

Suspicious Activity

Restricted User	Triggers an alert when a monitored user performs select activities.
Suspicious IP	Triggers an alert when there is activity from a suspicious IP.
Suspicious Time	Triggers an alert when there is activity outside of work hours.
Suspicious Location	Triggers an alert when there is activity from suspicious locations.

Sensitive Activity

Sensitive Event	Triggers an alert when a sensitive event occurs.
Sensitive File	Triggers an alert when a specified sensitive file is accessed.
Ransomware Behavior Detection	Triggers an alert when the directory's file(s) had been replaced.

Abnormal Traffic

Large File Upload	Triggers an alert when a file upload exceeds a size threshold.

Compliance

Compliance policies track files relevant to specific regulations. For example, if a user accesses a file containing private heath information and you have the corresponding HIPAA policy set, FortiCASB will send you an alert.

Compliance policies

SOX-COBIT

SOX-COBIT policies help your organization track and show compliance with the Sarbanes-Oxley (SOX) Act of 2002 using COBIT guidelines. Use these policies to monitor your cloud applications for SOX compliance, then use the Report feature to print a report detailing compliance specifics.

PCI

PCI policies help your organization track and show compliance with the Payment Card Industry Data Security Standard (PCI DSS). Use these policies to monitor your cloud applications for PCI DSS compliance, then use the Report feature to print a report detailing compliance specifics.

In particular, FortiCASB checks for compliance with the following requirements:

HIPAA

HIPAA policies help your organization track and show compliance with the Health Insurance Portability and Accountability Act (HIPAA). Use these policies to monitor your cloud applications for HIPAA compliance, then use the Report feature to print a report detailing compliance specifics.

GDPR

GDPR policies help your organization track and show compliance with the EU General Data protection Regulation (GDPR). Use these policies to monitor your cloud applications for GDPR compliance, then use the Report feature to print a report detailing compliance specifics.

ISO 270001

ISO 270001 is the best-known standard in the family in providing requirements for an information security management system (ISMS). ISO 270001 policies help your organization manage the security of assets, such as financial information, intellectual property, employee details, and information entrusted to you by third parties.

Use these policies to monitor your cloud applications for ISO 270001 compliance, and the Report feature to print a report detailing compliance specifics.

NIST 800-53 V4

NIST 800-53 V4 is the recommended security controls for federal information systems and organizations. It documents security controls for all federal information systems.

Use these policies to monitor your cloud applications for NIST 800-53 V4 compliance, and the Report feature to print a report detailing compliance specifics.

NIST 800-171

NIST 800-171 can help to protect controlled Unclassified Information in Non-federal Information Systems and Organizations.

Use these policies to monitor your cloud applications for NIST 800-171 compliance, and the Report feature to print a report detailing compliance specifics.

Customized

FortiCASB allows you to create personalized policies to suit your orgazational needs. To add a custom policy, click **Add** from the Customized tab.

Custom policies focus on two aspects, content monitoring and activity monitoring. Content monitoring is primarily used to monitor files for sensitive data. Activity monitoring is primarily used to monitor users and user activities.

The following examples illustrate how to create some common custom policies.

Example 1: To monitor all downloads of a public link containing sensitive data

To receive an alert whenever a file containing sensitive data is downloaded from a public link, use the Exposure setting along with the Data Pattern setting. For example, to monitor a Salesforce link containing a social security number:

1. Go to the **Content** tab.
2. Select **Specific Data Patterns**, on the right.
3. Click the box labeled **Data Pattern**, then select DLP SSN.
4. Click the box labeled **Exposure**, then select SALESFORCE_LINK.
5. Go to the **Activity** tab.
6. Select **Specific Events**, on the right.
7. Click the box labeled **Event**, then select Download File.
8. Configure any other settings as needed.

Example 2: To monitor all activities of a group of users

To receive an alert whenever a specific user or group of users performs any action, use the User setting. For example, to monitor a group of users:

1. Go to the **Activity** tab.
2. Select **Specific Users**, on the right.
3. Click the box labeled **User**, then select users to monitor. Alternatively, check the **Exclude** box on the right to monitor all users besides the ones selected.
4. Configure any other settings as needed.

How to set policies

1. Go to **Policy.**
2. Click the arrow next to the policy you wish to configure.
3. Configure the settings as described below.
4. Click **Save**.

The policy you set should be active after a few minutes.

General

Name	Shows the name of the policy. Not configurable.

Status	Specify whether or not the policy is active. A policy is active when it is set to true.
Policy Description	Shows a description of the policy. Not configurable.
Severity Level	Specify the severity level for the policy.
Policy Type	Shows the type of policy. Not configurable.

Context

Matching Threshold	Specify the minimum threshold for an alert. For example, a Credit Card Number policy with threshold set to two will trigger an alert when two or more credit card numbers are in a file.
Data Pattern Monitor Type	Specify either Monitor Activity, Risk Assessment, or both. If Monitor Activity is specified, alerts will be generated in the Alerts menu whenever targets are accessed. If Risk Assessment is specified, FortiCASB will search for the selected data pattern during Discovery scans.

Notification

Enable Email Notification	Check the box to allow FortiCASB to send an email whenever an alert is triggered.
Email Receiver	Either select a user to receive notifications, or enter in an email address.

Configure policies

This feature is available for IaaS only.

Predefined configuration policies

Predefined policies make it easier for you to monitor the configuration issues in the system, and can suggest how to fix issues when they occur.

You can enable the polices by clicking **Policy>Configuration.**

Customized Configuration policies

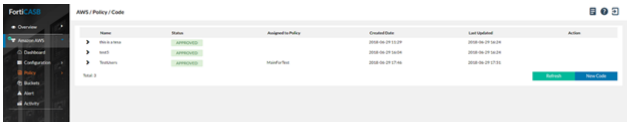
FortiCASB also allows you to create the customized configuration policies.

Code pattern

Here are some characteristics of a code pattern:

- A code pattern is a block of python3 codes.
- A code pattern has a name which will not be modified after the code pattern is created.
- A code pattern has three statuses: PENDING,APPROVED, ERROR. When a code pattern is in PENDING or APPROVED status, the code pattern can not be edited. A code pattern is editable only if the code pattern's status is ERROR. When a code pattern is in APPROVED status, the code pattern can be bound to a Configcustom policy. One Configcustom policy can only be associated with one code pattern.

The graph below shows a list of Code patterns. The associated policy's name is displayed under 'Assigned to Policy' column.



AWS / Policy / Code

Name	Status	Assigned to Policy	Created Date	Last Updated	Action
this is a testa	APPROVED		2018-06-29 11:29	2018-06-29 16:24	
test5	APPROVED		2018-06-29 16:04	2018-06-29 16:24	
TestUsers	APPROVED	MainForTest	2018-06-29 17:46	2018-06-29 17:31	

Total: 3

On the code pattern list page, you can click the **New Code** button to create a new code pattern.

The Code pattern creation page has two fields: Code name and a block of python3 codes.

The Code name can only contain decimal digits, lower- or upper-case alphabetic characters, and spaces. And the length of the Code name must be between 1 and 100 characters in length.

The pythons codes can not contain more than 100000 characters, including comments.

When you write python3 codes, you must define a function run with a parameter aws, it looks like below:

```
def run(aws):
   #here add codes for function run
```

The parameter aws is a proxy of AWS python api boto3.

You can get a client just like you use boto3, such as `iam = aws.client('iam')`.

So far, We only support `iam, s3, ec2, es, rds, elb`. And only some methods of originals.

iam:

```
list_users ,
list_roles,
list_groups,
list_policies,
list_groups_for_user,
list_attached_user_policies,
list_attached_group_policies,
list_attached_role_policies,
list_user_policies,
list_group_policies,
list_role_policies,
get_user_policy,
get_group_policy,
get_role_policy,
get_policy,
get_policy_version
```

s3:

```
list_buckets,
get_bucket_location,
get_bucket_policy,
get_bucket_tagging,
get_bucket_acl
```

ec2:

```
describe_security_groups
```

es:

```
list_domain_names,
describe_elasticsearch_domains
```

rds:

```
describe_db_instances,
describe_db_snapshots,
describe_db_snapshot_attributes,
list_tags_for_resource,
describe_db_cluster_snapshots,
describe_db_cluster_snapshot_attributes
```

elb:

```
describe_load_balancers
```

All supported methods have the same parameters as boto3. For more information, see https://boto3.readthedocs.io/en/latest/reference/services/index.html.

You can also use these methods below:

```
def diff_days_date_and_now(date)
   Get the number of days between a specific date and current date

def parse_json(data)
   Parse a string of json

def dumps_to_json(data)
   Generate a string of json from an object data

def decode_escapes(data)
   Html escapes
```

```
def match_regex_insensitive(value, pattern)
   Match value by a regex, insensitive

def match_regex_sensitive(value, pattern)
   Match value by a regex, sensitive

def match_regex_sensitive_search(value, pattern)
   Search by a regex, sensitive

def set_region(region_name)
   Set a AWS region.
```

You can call it for setting AWS region, if a region is needed. This method must be called outside of function run.

```
def get_region()
   Get the AWS region setted previously

   def set_aws_access_key_id(aws_access_key_id)
   def get_aws_access_key_id()
   def set_aws_secret_access_key(aws_secret_access_key)
   def get_aws_secret_access_key()
   def set_aws_session_token(aws_session_token)
   def get_aws_session_token()

def set_data(*args, **kwargs)
   Save the data you want to save when checking a resource.

def fail(message, resource_id)
   A check is done, and the result is fail.

def warn(message, resource_id)
   A check is done, and the result is fail.

def success(message, resource_id)
   A check is done, and the result is success.

def error(message, resource_id)
   A check is done, and the result is error

def error_user(message)
   def error_sys(message)
```

In the block of python3 codes, you can define multiple functions, but you must make sure no function name is the same as any of above functions.

After you code, you can test your grammar, and check if it meets our conditions using the Test button.

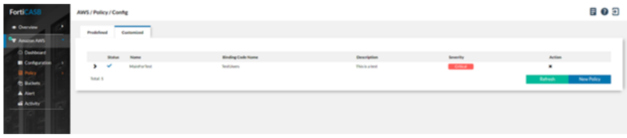
Save the code pattern by click save button. The status is PENDING after the code pattern is saved. The status will be modified to APPROVED automatically after you run the code.

Cancel the code pattern creation using the Close button.

Configcustom policy

A Configcustom policy is a policy which is associated with a code pattern.

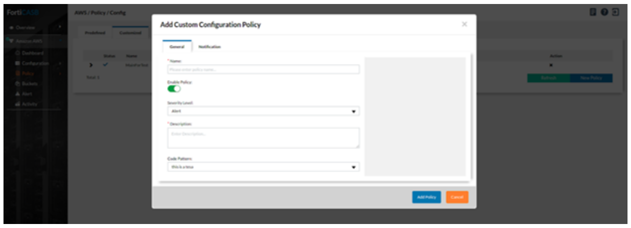
The graph below is a list of Configcustom policies. The name of the code pattern bound to the Cofigcustom policy is showed under Binding Code Name Column.



	Status	Name	Binding Code Name	Description	Severity	Action
›	✓	MainForTest	TestUsers	This is a test	Critical	✖

Total: 1

Click New Policy button to create a new Configcustom policy.



* Name: Please enter policy name...

Enable Policy: ●

Severity Level: Alert

* Description: Enter Description...

Code Pattern: this is a tese

Name—Only contains decimal digits, lower-case or upper-case alphabetic characters, and spaces. Be sure to use no more than 100 characters .

Description—Enter a brief description in less than 200 characters.

Code Pattern— You must choose an available code pattern when you create a Configcustom policy. If there is no available code pattern, you must create one.

To create code pattern, click Add Policy button; To cancel, click Cancel button.

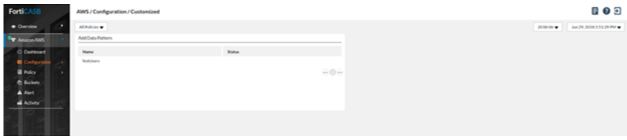
If you want to add notifications, you can choose the Notification tab.

TODO : add notifications

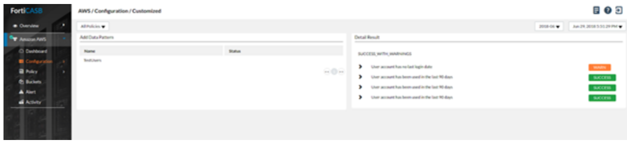
You can add email, SQS, SNS notifications. Adding SQS and SNS are the same as adding global SQS/SNS. Refer to How to set policies on page 89

Configcustom policy results

The graph below shows the results of Configcustom policies.



The All policies drop-down in the upper-left corner contains a list of policies; the two drop-downs on the upper-right are the month and execution batch. You can adjust them to get different results. To see the details of a result, click the result record on the left, and the details will show up on the right.



SUCCESS_WITH_WARNINGS

User account has no last login date	WARN
User account has been used in the last 90 days	SUCCESS
User account has been used in the last 90 days	SUCCESS
User account has been used in the last 90 days	SUCCESS

Click the greater than symbol at the start of each record, you can get the data you saved in the code.

Set policies

1. Go to Policy.
2. Click the arrow next to the policy you wish to configure.
3. Configure the settings as described below.
4. Click Save.

The policy you set should be active after a few minutes.

Parameter	Description
General	
Name	Shows the name of the policy. Not configurable.
Status	Specify whether or not the policy is active. A policy is active when it is set to true.
Policy Description	Shows a description of the policy. Not configurable.
Severity Level	Specify the severity level for the policy.
Policy Type	Shows the type of policy. Not configurable.
Context	
Matching Threshold	Specify the minimum threshold for an alert. For example, a Credit Card Number policy with threshold set to two will trigger an alert when two or more credit card numbers are in a file.
Data Pattern Monitor Type	Specify either Monitor Activity, Risk Assessment, or both. If Monitor Activity is specified, alerts will be generated in the Alerts menu whenever targets are accessed. If Risk Assessment is specified, FortiCASB will search for the selected data pattern during Discovery scans.
Notification	

Enable Email Notification	Check the box to allow FortiCASB to send an email whenever an alert is triggered.
Email Receiver	Either select a user to receive notifications, or enter in an email address.

SQS/SNS

You need add AWS as your monitor application at first

1. Click the Email icon on the right up,
2. Choose the AWS tab. You can see the global SQS and SNS list.
3. Click the **Add** button to add a new SQS or SNS.

For SQS, you can find the SQS URL and region in the detail of the SQS after you've created a queue. For information on how to create a new queue, seehttps://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-getting-started.html. Be sure to grant SendMessage and SendMessageBatch rights to the Role you have added to FORTICASB.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0", "Effect": "Allow", "Action": [
            "sqs:SendMessageBatch",
            "sqs:SendMessage"
         ],
         "Resource": "*"// here you can modify it to a specific Queue Arn
         }
   ]
}
```

For SNS, you can find SNS topic Arn and region in the detail of a topic, after the topic is created(About creat a

new topic, see https://docs.aws.amazon.com/sns/latest/dg/CreateTopic.html. And grant Publish right to the Role which you have added to FORTICASB.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow", "Action": "sns:Publish",
         "Resource": "*" // here you can modify it to a specific SNS Topic Arn
      }
   ]
}
```

Discovery

The Discovery page shows basic information about the data in your cloud application, as well as information about the users with access to your data.

If you would like to sync data, you can run Sync from the user and document page.

Panel descriptions

User Entitlements—shows all users with access to your cloud application.

Privileged User	Any user with specific administrative privileges. For a list of these specific privileges, see Administrative privileges on page 98
Dormant User	Any user that has not accessed the cloud application for at least 30 days.
External User	Any user from an external company with access to your cloud application.

If the User Entitlements panel can't get privileged roles for your Office 365 platform, make sure you have global administrator privileges and have Azure Active Directory Premium P2.

Sensitive Data Discovery—gives an overview of sensitive data on your cloud application.

Sensitive Files	Shows the number of files on your cloud application with sensitive information, out of the total number of files.
High Risk File Owners	Shows how many users own files with sensitive information.
Shared Files	Shows the number of shared files
Malware Files	Shows the number of files with malware scan results

Click the number under Policy Violation to show the specific policies triggered.

Use **Filter** to filter or search through the list.

File Exposure—gives an overview of shared files on your cloud application.

Exposure Summary	Gives a summary of the file exposure. Click to filter the list.
Top File-Sharing Owners	Shows the owners sharing the most files.
Top Users/Groups with access to Shared Files	Shows the users or groups with access to the most files.

External Collaboration—highlights the file shared to the external user/group

External Summary	Gives a summary of the external files.
Top External Domains	Shows external domains which are shared the most files.
Top External Users	Shows external users which are shared the most files.

Click on [...] under Share or Link for more details.
Use **Filter** to filter or search through the list.

Administrative privileges

Salesforce

A user with any of the following administrative permissions is considered a privileged user:

- Assign Permission Sets
- Manage Sharing
- Modify All Data
- Manage Encryption Keys
- View All Data
- View All Users

Office 365

A user with any of the following administrator roles is considered a privileged user:

- global administrator
- billing administrator
- password administrator
- service administrator
- user management administrator
- Exchange administrator
- SharePoint administrator
- Skype for Business administrator

Box

An admin with all of the following permissions is considered a privileged user:

- Manage users and groups
- Make calls on behalf of users
- View all data

Dropbox Business

A Team Admin is considered a privileged user.

Google

A user with any of the following administrator roles is considered a privileged user:

- Super Administrator
- Groups Administrator
- User Management Administrator
- Help Desk Administrator
- Services Administrator
- User Customized Administrator

Documents

The Documents page shows all the files FortiCASB is currently monitoring. The infographic gives an overview of the files categorized by File Type, Sensitive Data, and Share Type.

List filter

- Click on the infographic to filter the list by File Type, Sensitive Data, or Share Type.
- Use the search bar on the top-right side to search by user.

DLP Scanned Documents

Show the number of documents which has been DLP-scanned.

State

- Sensitive: File hit the DLP policies
- External: File shared to the external user/group
- Malware: File hit the malware policies

File download

You can download a file FortiCASB is monitoring by clicking the download link in the Operation column.

Activity

FortiCASB tracks user activities on cloud platforms.

The Activity page contains both a map displaying (approximate) geolocations of events and an activities list.

Map options

- **Activity**—Click on an activity indicator on the map to bring up an activity notification from that specific location.
- **Move**—Move the map by clicking a point and dragging your mouse.
- **Zoom**—Use the buttons on the bottom-right corner of the map to zoom in and out.
- **Refresh**—Click the **Refresh** button to refresh the map.
- **Clear Map**—Click the **Clear Map** button to clear the map of activity indicators.
- **Filter**—Click the **Filter** button to filter the activity notifications shown.

Raw event list

Events that come directly from a cloud API or web notifications are displayed in Javascript Object Notation (JSON) format.

Alert correlation

One activity may trigger multiple alerts. Click the event to open the corresponding alert page.

Dashboard

The dashboard gives an overview of the data in your specific cloud application.

Risk Trend and Activity Trend can also be found on the FortiCASB main dashboard. Click on a platform's name to filter the information shown.

IAAS Features

IAAS Security Integration

IAAS Security Integration

FortiCASB integrates IAAS cloud security features to provide an all in one solution in cloud security monitoring which let you receive multiple IAAS cloud security alerts in one platform.

Amazon AWS Cloud Security Integration

FortiCASB provides AWS cloud integration where it integrates AWS cloud security traffic data and provide real time cloud security monitoring. FortiCWP will receive security alerts from AWS security integration and informs users of probe findings.

Prerequisite

To enable AWS cloud integration with FortiCASB, **Amazon Inspector**, **Amazon Guard Duty**, and **AWS Security Hub** needed to be enabled for FortiCASB to gather cloud security traffic data through AWS API services. Follow these steps to enable Amazon Inspector, Amazon Guard Duty, and AWS Security Hub on Amazon AWS.

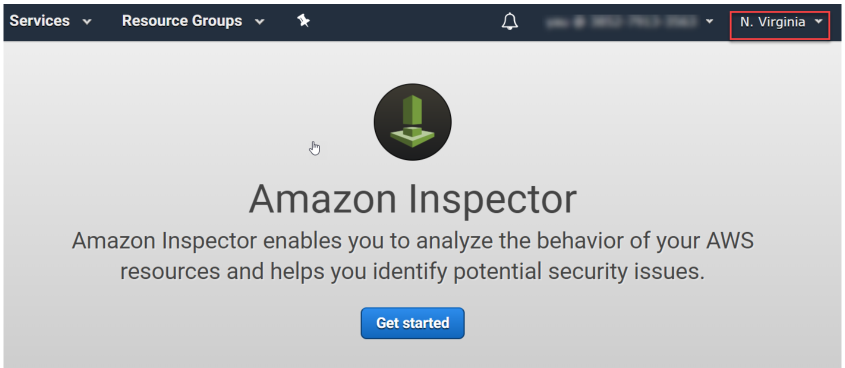
Enable Amazon Inspector:

Amazon Inspector requires administrator or user with specific role/policy to enable. To check the credentials, follow these steps:

1. Log in Amazon AWS console using your AWS account: https://console.aws.amazon.com/.
2. Search and click on **IAM**.
3. Click on **Roles** on the left menu.
4. Search "Inspector" and click on **AWSServiceRoleForAmazonInspector**.
5. Make sure **AmazonInspectorServiceRolePolicy** existed under permission.
6. If not, contact your administrator to have the role/policy assigned to the user.

Once the user has Amazon Inspector role/policy, now log into Inspector to enable it.

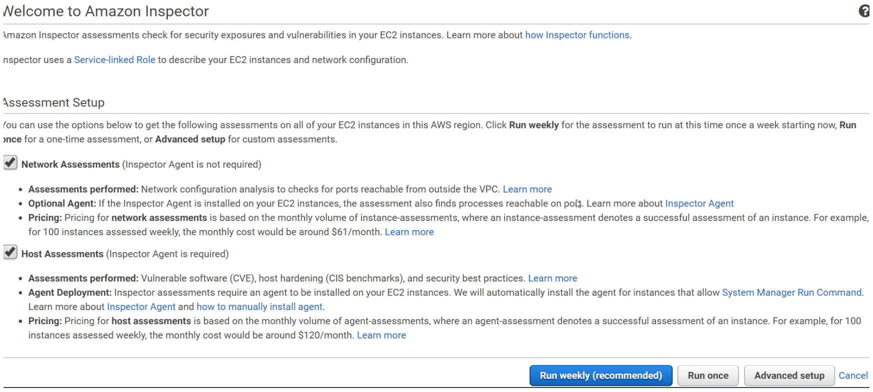
1. Search and click on **Inspector** fomr AWS Console page.
2. Select the **region** which you would like to monitor on the top right corner.



Amazon Inspector

Amazon Inspector enables you to analyze the behavior of your AWS resources and helps you identify potential security issues.

3. Click on **Get Started**.
4. Click **Run Weekly (recommended)**button, with **Network Assessments** and **Host Assessments** selected.



Welcome to Amazon Inspector

Amazon Inspector assessments check for security exposures and vulnerabilities in your EC2 instances. Learn more about how Inspector functions.

Inspector uses a Service-linked Role to describe your EC2 instances and network configuration.

Assessment Setup

You can use the options below to get the following assessments on all of your EC2 instances in this AWS region. Click **Run weekly** for the assessment to run at this time once a week starting now, **Run once** for a one-time assessment, or **Advanced setup** for custom assessments.

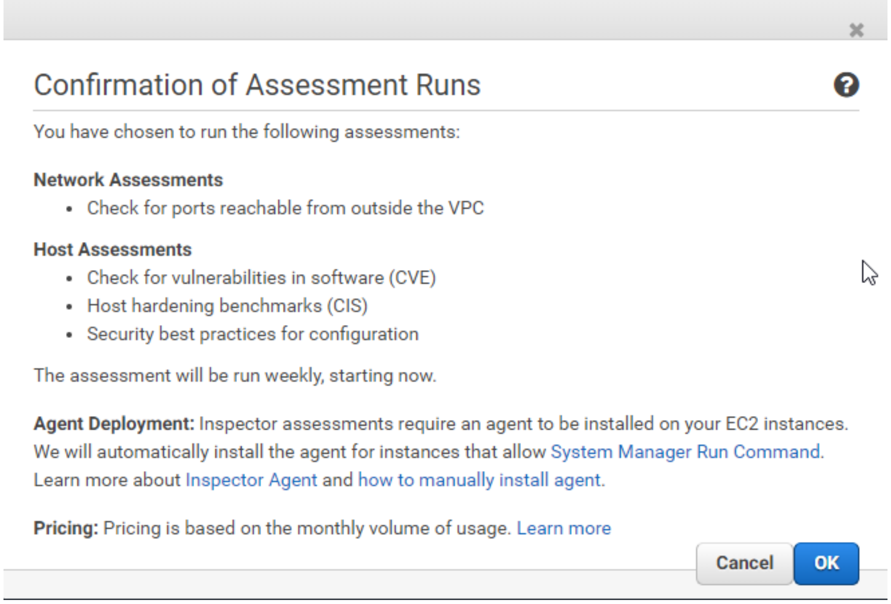
☑ **Network Assessments** (Inspector Agent is not required)

- **Assessments performed:** Network configuration analysis to checks for ports reachable from outside the VPC. Learn more
- **Optional Agent:** If the Inspector Agent is installed on your EC2 instances, the assessment also finds processes reachable on port. Learn more about Inspector Agent
- **Pricing:** Pricing for **network assessments** is based on the monthly volume of instance-assessments, where an instance-assessment denotes a successful assessment of an instance. For example, for 100 instances assessed weekly, the monthly cost would be around $61/month. Learn more

☑ **Host Assessments** (Inspector Agent is required)

- **Assessments performed:** Vulnerable software (CVE), host hardening (CIS benchmarks), and security best practices. Learn more
- **Agent Deployment:** Inspector assessments require an agent to be installed on your EC2 instances. We will automatically install the agent for instances that allow System Manager Run Command. Learn more about Inspector Agent and how to manually install agent.
- **Pricing:** Pricing for **host assessments** is based on the monthly volume of agent-assessments, where an agent-assessment denotes a successful assessment of an instance. For example, for 100 instances assessed weekly, the monthly cost would be around $120/month. Learn more

5. Click **OK** when asking for confirmation.



Confirmation of Assessment Runs

You have chosen to run the following assessments:

Network Assessments
- Check for ports reachable from outside the VPC

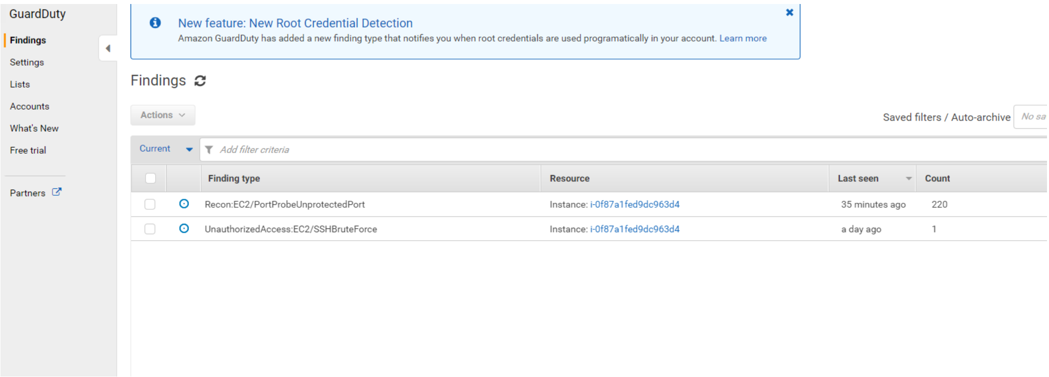
Host Assessments
- Check for vulnerabilities in software (CVE)
- Host hardening benchmarks (CIS)
- Security best practices for configuration

The assessment will be run weekly, starting now.

Agent Deployment: Inspector assessments require an agent to be installed on your EC2 instances. We will automatically install the agent for instances that allow System Manager Run Command. Learn more about Inspector Agent and how to manually install agent.

Pricing: Pricing is based on the monthly volume of usage. Learn more

6. Now Amazon Inspector is enabled. It will produce detailed list of security findings that is organized by level of severity.



New feature: New Root Credential Detection
Amazon GuardDuty has added a new finding type that notifies you when root credentials are used programatically in your account. Learn more

Findings

Finding type	Resource	Last seen	Count
Recon:EC2/PortProbeUnprotectedPort	Instance: i-0f87a1fed9dc963d4	35 minutes ago	220
UnauthorizedAccess:EC2/SSHBruteForce	Instance: i-0f87a1fed9dc963d4	a day ago	1

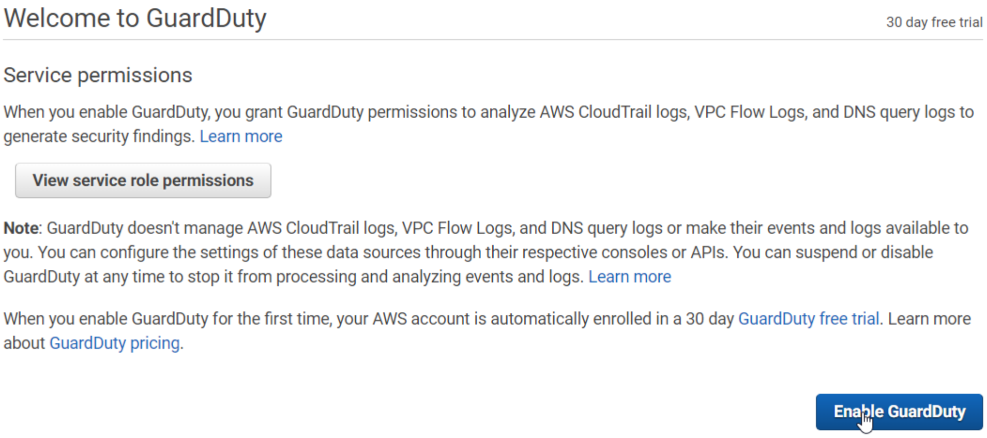
Enable Amazon Guard Duty:

Amazon Guard Duty requires administrator or user with specific role/policy to enable. To check the credentials, follow these steps:

1. Log in Amazon AWS console using your AWS account: https://console.aws.amazon.com/.
2. Search and click on **IAM**.
3. Click on **Roles** on the left menu.
4. Search "Guard Duty" and click on **AWSServiceRoleForAmazonGuardDuty**.
5. Make sure **AmazonGuardDutyServiceRolePolicy** existed under permission.
6. If not, contact your administrator to have the role/policy assigned to the user.

Once the user has Amazon Guard Duty role/policy, log into Guard Duty to enable it.

1. Search and click on **GuardDuty** from AWS Services Menu.
2. Select the **region** to monitor on the top right corner.
3. Choose **Get Started**, and then click on **Enable Guard Duty**.


Welcome to GuardDuty

30 day free trial

Service permissions

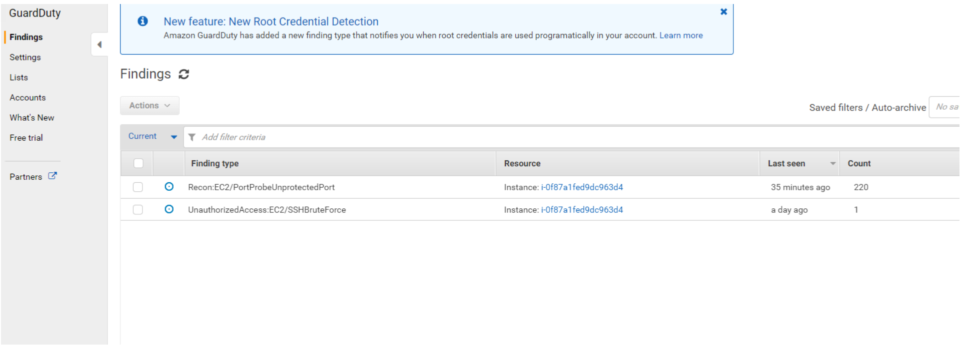
When you enable GuardDuty, you grant GuardDuty permissions to analyze AWS CloudTrail logs, VPC Flow Logs, and DNS query logs to generate security findings. Learn more

Note: GuardDuty doesn't manage AWS CloudTrail logs, VPC Flow Logs, and DNS query logs or make their events and logs available to you. You can configure the settings of these data sources through their respective consoles or APIs. You can suspend or disable GuardDuty at any time to stop it from processing and analyzing events and logs. Learn more

When you enable GuardDuty for the first time, your AWS account is automatically enrolled in a 30 day GuardDuty free trial. Learn more about GuardDuty pricing.

4. Now Guard Duty is enabled, it will start pulling streams of data from AWS CloudTrail, VPC Flow Logs, and

DNS logs to generate security findings.



New feature: New Root Credential Detection

Amazon GuardDuty has added a new finding type that notifies you when root credentials are used programatically in your account. Learn more

Findings

		Finding type	Resource	Last seen	Count
□	○	Recon:EC2/PortProbeUnprotectedPort	Instance: i-0f87a1fed9dc963d4	35 minutes ago	220
□	○	UnauthorizedAccess:EC2/SSHBruteForce	Instance: i-0f87a1fed9dc963d4	a day ago	1

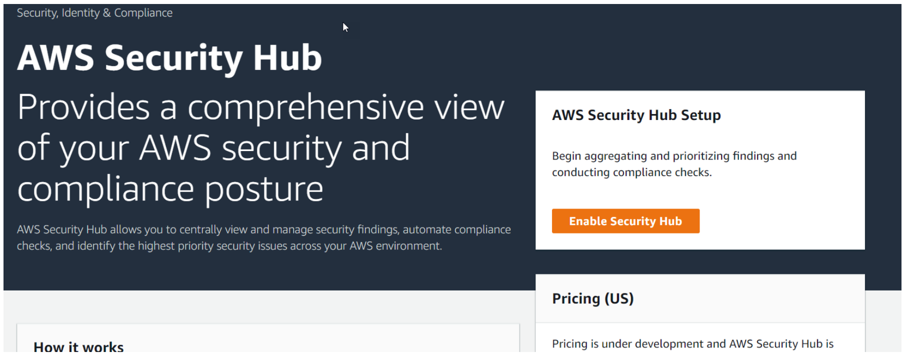
Enable AWS Security Hub:

Amazon Security Hub requires administrator or user with specific role/policy to enable. To check the credentials, follow these steps:

1. Log in Amazon AWS console using your AWS account: https://console.aws.amazon.com/.
2. Search and click on **IAM**.
3. Click on **Roles** on the left menu.
4. Search "Security Hub" and click on **AWSServiceRoleForSecurityHub.**
5. Make sure **AWSSecurityHubServiceRolePolicy** existed under permission.
6. If not, contact your administrator to have the role/policy assigned to the user.

Once the user has Amazon Security Hub role/policy, log into Security Hub to enable it.

1. Search and click on **Security Hub** from AWS Services Menu.
2. Click on **Enable Security Hub**



AWS Security Hub

Provides a comprehensive view of your AWS security and compliance posture

AWS Security Hub allows you to centrally view and manage security findings, automate compliance checks, and identify the highest priority security issues across your AWS environment.

AWS Security Hub Setup

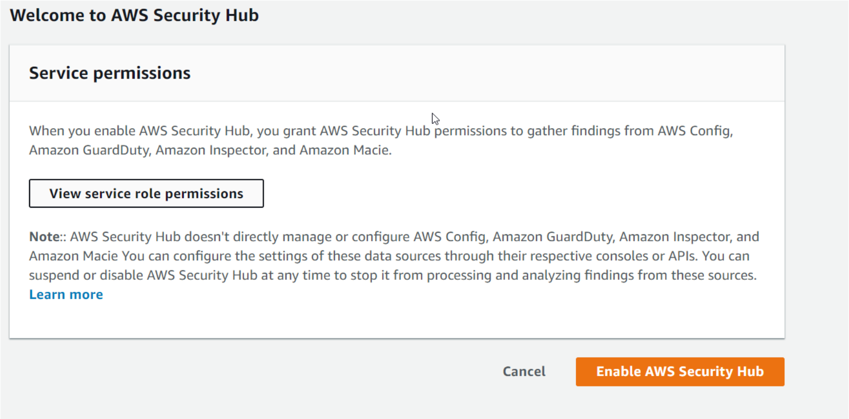
Begin aggregating and prioritizing findings and conducting compliance checks.

Pricing (US)

Pricing is under development and AWS Security Hub is

How it works

3. In the service permissions page, click on **Enable Security Hub**.



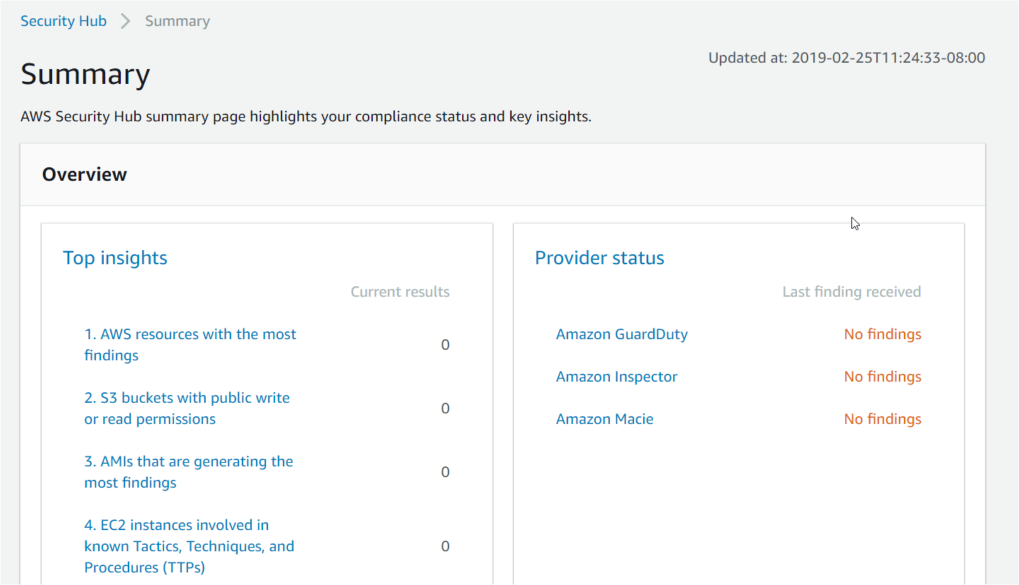
Welcome to AWS Security Hub

Service permissions

When you enable AWS Security Hub, you grant AWS Security Hub permissions to gather findings from AWS Config, Amazon GuardDuty, Amazon Inspector, and Amazon Macie.

Note:: AWS Security Hub doesn't directly manage or configure AWS Config, Amazon GuardDuty, Amazon Inspector, and Amazon Macie You can configure the settings of these data sources through their respective consoles or APIs. You can suspend or disable AWS Security Hub at any time to stop it from processing and analyzing findings from these sources. Learn more

4. After Security Hub enabled, it begins consuming, aggregating, organizing, and prioritizing findings from AWS services.



Security Hub > Summary

Summary

Updated at: 2019-02-25T11:24:33-08:00

AWS Security Hub summary page highlights your compliance status and key insights.

Overview

Top insights

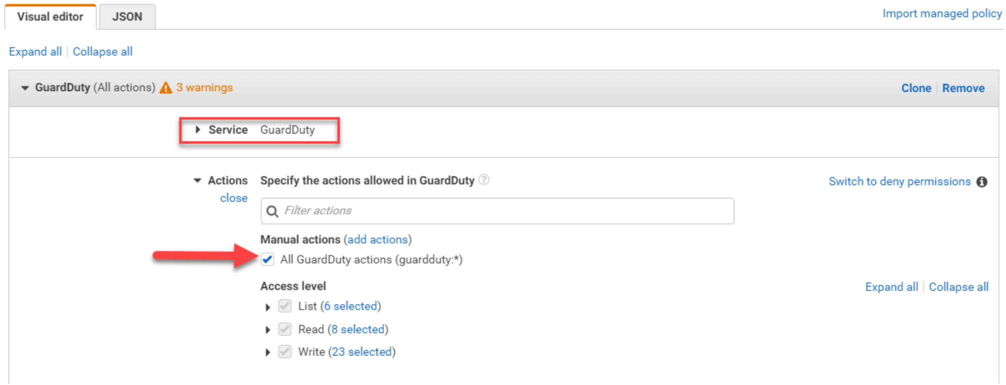
	Current results
1. AWS resources with the most findings	0
2. S3 buckets with public write or read permissions	0
3. AMIs that are generating the most findings	0
4. EC2 instances involved in known Tactics, Techniques, and Procedures (TTPs)	0

Provider status

	Last finding received
Amazon GuardDuty	No findings
Amazon Inspector	No findings
Amazon Macie	No findings

Create customized policy to add to FortiCASB role

1. In AWS portal, click on **Services** drop down menu and select **IAM**.
2. Click on **Policies** in the left menu.
3. Click on **Create Policy**.
4. Under **Visual Editor**, click **Service > Choose a service** to show the search bar.
5. Search **GuardDuty**, and check on "All GuardDuty actions".


Visual editor
JSON
Import managed policy
Expand all | Collapse all
GuardDuty (All actions) 3 warnings
Clone | Remove
Switch to deny permissions
close
Filter actions
Expand all | Collapse all

Service GuardDuty

Actions: Specify the actions allowed in GuardDuty

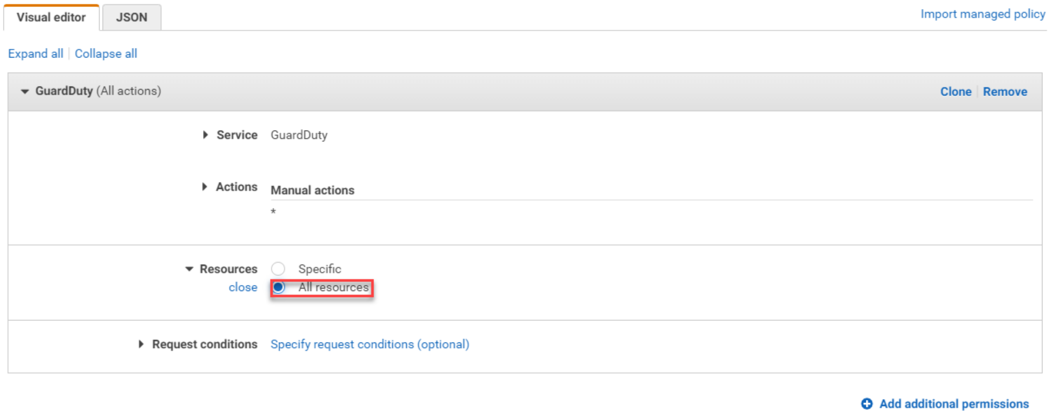
Manual actions (add actions)

☑ All GuardDuty actions (guardduty:*)

Access level

- ☑ List (6 selected)
- ☑ Read (8 selected)
- ☑ Write (23 selected)

6. For the warning received, click on Resources and check on "All resources"



Service GuardDuty

Actions: Manual actions *

Resources: ○ Specific ● All resources

7. Click on **+Add additional permissions** and repeat the steps above to add **Inspector** and **SecurityHub**.
8. Click **Review policy**
9. Fill in the policy name field. (Keep the policy name for later use)
10. Click **Create policy**.

Add policy to FortiCASB role

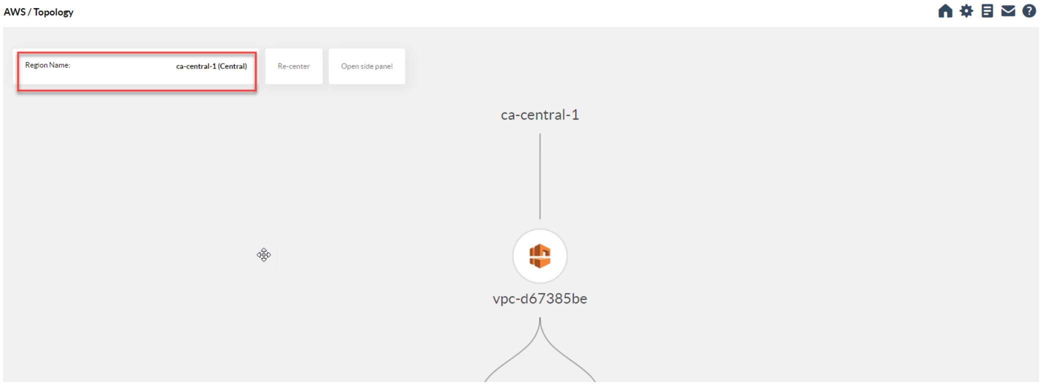
1. Select **Roles** from IAM dashboard.
2. Search and click on the Role created for FortiCASB from Getting Started > Install IAAS Applications > Role creation on page 38.
3. Click on **Attach policies**.
4. Search and check on customized policy created from earlier.
5. Click on **Attach policy**.

Now FortiCASB is able to extract security findings from Amazon Security Hub and integrate into FortiCASB alert.

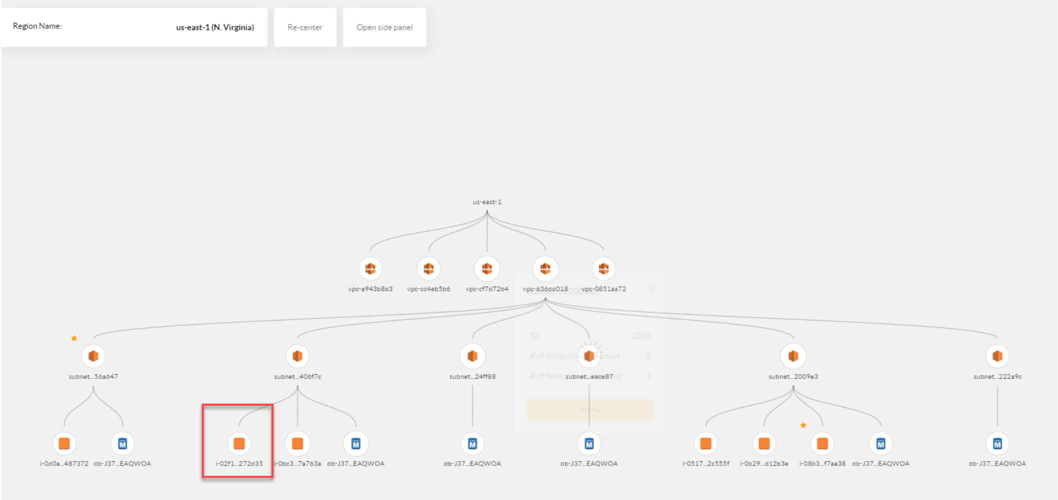
Viewing AWS Cloud Security Findings

After **Amazon Inspector**, **Amazon Guard Duty**, and **AWS Security Hub** are enabled, FortiCASB will provide real time cloud security monitoring.

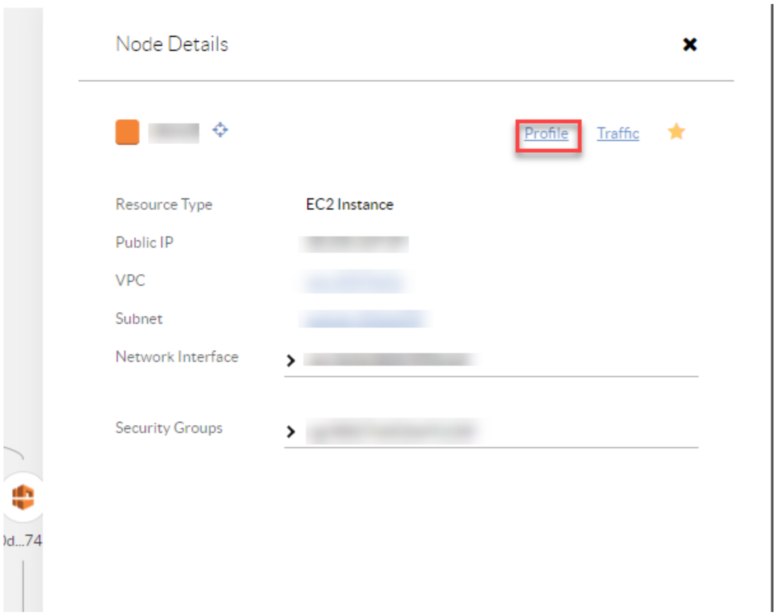
1. Log into FortiCASB: https://www.forticasb.com with your FortiCASB account.
2. Select a **Company > Business Unit.**
3. From FortiCASB dashboard, select **Amazon AWS** on the left menu.
4. Click on **Topology**.
5. Select a **region** to see all the cloud instances under that region.



6. Select a cloud instance under topology.



7. Click on **Profile** of the instance.



Node Details

[redacted] Profile Traffic

Resource Type EC2 Instance

Public IP [redacted]

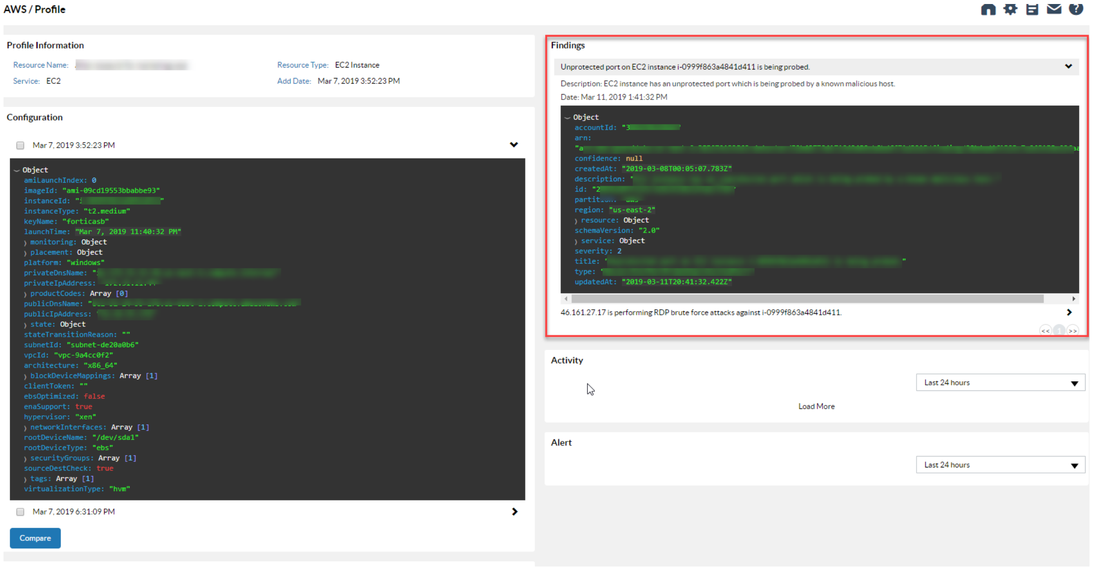
VPC [redacted]

Subnet [redacted]

Network Interface [redacted]

Security Groups [redacted]

8. Under **Findings** will show security findings on the cloud instance.



AWS / Profile

Profile Information

Resource Name: [redacted]
Service: EC2
Resource Type: EC2 Instance
Add Date: Mar 7, 2019 3:52:23 PM

Configuration

□ Mar 7, 2019 3:52:23 PM

```
⌄ Object
  amiLaunchIndex: 0
  imageId: "ami-09cd19553bbabbe93"
  instanceId: "[redacted]"
  instanceType: "t2.medium"
  keyName: "forticasb"
  launchTime: "Mar 7, 2019 11:40:32 PM"
  › monitoring: Object
  › placement: Object
  platform: "windows"
  privateDnsName: "[redacted]
  privateIpAddress: [redacted]
  › productCodes: Array [0]
  publicDnsName: "[redacted]
  publicIpAddress: [redacted]
  › state: Object
  stateTransitionReason: ""
  subnetId: "subnet-de20a0b6"
  vpcId: "vpc-9a4cc0f2"
  architecture: "x86_64"
  › blockDeviceMappings: Array [1]
  clientToken: ""
  ebsOptimized: false
  enaSupport: true
  hypervisor: "xen"
  › networkInterfaces: Array [1]
  rootDeviceName: "/dev/sda1"
  rootDeviceType: "ebs"
  › securityGroups: Array [1]
  sourceDestCheck: true
  › tags: Array [1]
  virtualizationType: "hvm"
```

□ Mar 7, 2019 6:31:09 PM

Findings

Unprotected port on EC2 instance i-0999f863a4841d411 is being probed.

Description: EC2 instance has an unprotected port which is being probed by a known malicious host.

Date: Mar 11, 2019 1:41:32 PM

```
⌄ Object
  accountId: "3[redacted]
  arn:
  "a[redacted]
  confidence: null
  createdAt: "2019-03-08T00:05:07.783Z"
  description: "[redacted]
  id: "2[redacted]
  partit[redacted]
  region: "us-east-2"
  › resource: Object
  schemaVersion: "2.0"
  › service: Object
  severity: 2
  title: "[redacted]"
  type: "[redacted]
  updatedAt: "2019-03-11T20:41:32.422Z"
```

46.161.27.17 is performing RDP brute force attacks against i-0999f863a4841d411.

Activity

Last 24 hours

Alert

Last 24 hours

Microsoft Azure Security Integration

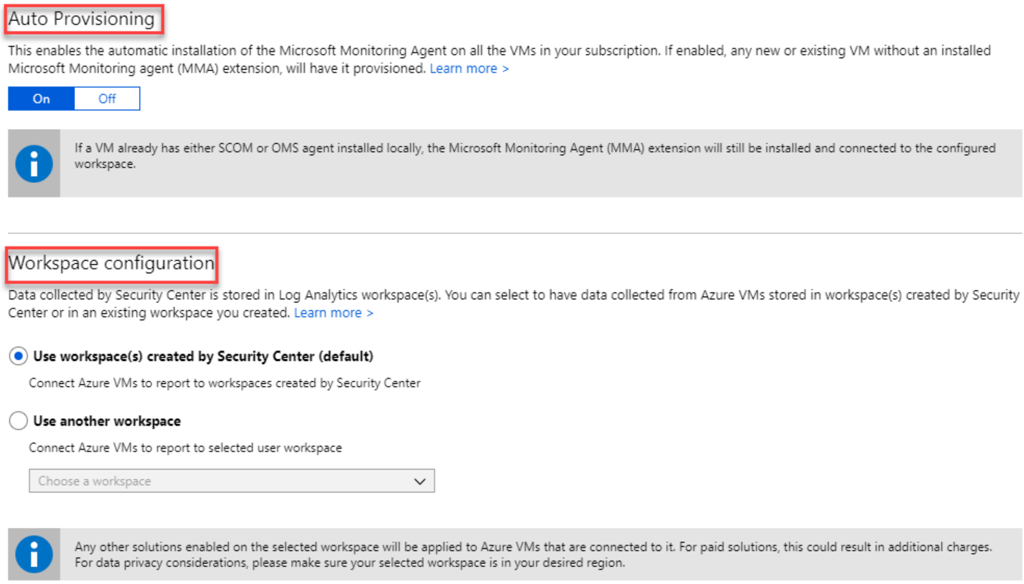
FortiCASB provides Azure cloud integration where it integrates Azure Cloud traffic data and provide real time cloud security monitoring. FortiCWP will receive security alerts from Azure security integration and informs users of probe findings.

Prerequisite

An active Microsoft Azure AD account with security policy setup is required for Microsoft Azure to provide cloud traffic data to FortiCASB.

Before setting up security policy, **Data Collection** needed to be setup first. Follow these steps to setup data collection.

1. Log in to Azure portal with you Azure AD account: https://portal.azure.com/.
2. Search and click on **Security Center**.
3. Click **Security Policy** on Security Center dashboard.
4. Click **Edit Settings** next to your subscription.
5. Under **Auto Provisioning**, select **On**.
6. Under **Workspace configuration**, leave is as "Use workspace(s) created by Security Center (default)".



Auto Provisioning

This enables the automatic installation of the Microsoft Monitoring Agent on all the VMs in your subscription. If enabled, any new or existing VM without an installed Microsoft Monitoring agent (MMA) extension, will have it provisioned. Learn more >

[✓ On] Off

If a VM already has either SCOM or OMS agent installed locally, the Microsoft Monitoring Agent (MMA) extension will still be installed and connected to the configured workspace.

Workspace configuration

Data collected by Security Center is stored in Log Analytics workspace(s). You can select to have data collected from Azure VMs stored in workspace(s) created by Security Center or in an existing workspace you created. Learn more >

● **Use workspace(s) created by Security Center (default)**

Connect Azure VMs to report to workspaces created by Security Center

○ **Use another workspace**

Connect Azure VMs to report to selected user workspace

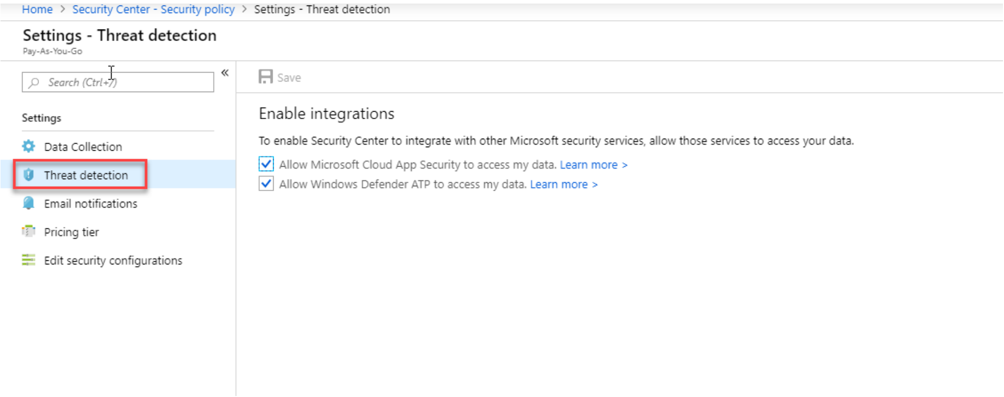
Choose a workspace

Any other solutions enabled on the selected workspace will be applied to Azure VMs that are connected to it. For paid solutions, this could result in additional charges. For data privacy considerations, please make sure your selected workspace is in your desired region.

7. Under **Windows security events**, select "Common".
8. Click **Save** at the top of the page.

After Data Collection is setup, enable integration to allow security center to integrate with other Microsoft security services by allowing other services to access cloud data.

1. Select **Threat Detection** in the settings under **Data Collection**.



Home > Security Center - Security policy > Settings - Threat detection
Search (Ctrl+/)
«
Settings
Data Collection
Threat detection
Email notifications
Pricing tier
Edit security configurations
Save

Settings - Threat detection

Pay-As-You-Go

Enable integrations

To enable Security Center to integrate with other Microsoft security services, allow those services to access your data.

☑ Allow Microsoft Cloud App Security to access my data. Learn more >

☑ Allow Windows Defender ATP to access my data. Learn more >

2. Check on the box next to "Allow Microsoft Cloud app Security to access my data".
3. Check on the box next to "Allow Windows Defender ATP to access my data".

If you have Azure Pay as you go subscription, having Data Collection and Threat detection setup is sufficient for Azure Integration. For Azure full subscription users, you may setup security policy. (optional)

1. On the Security Center dashboard, select **Security Policy**, and then select your type of subscription.
2. On the Security policy blade, select **Security Policy**.
3. On the Security policy - Security policy blade, turn on appropriate policy items to apply to your subscription.
4. Select save at the top of the blade.

After Azure data collection and integration is enabled, ForitCASB is able extract cloud traffic data from Azure and provide real time cloud security monitoring.

Google Cloud Security Integration

FortiCASB provides Google cloud integration where it integrates Google Cloud traffic data and provide real time cloud security monitoring. FortiCWP will receive security alerts from Google security integration and informs users of probe findings.

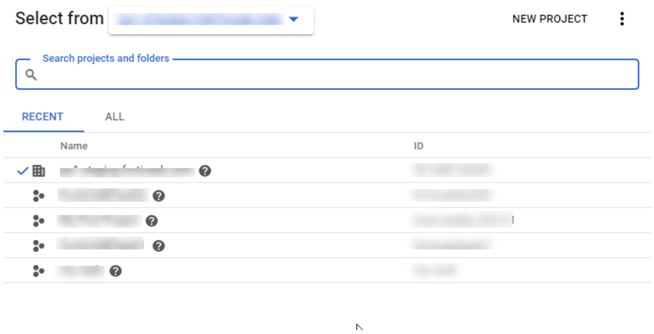
Prerequisite

A project with service account is required to enable Google Cloud integration. If you have not done so please refer to Getting Started > Install IAAS Applications > Google Cloud Platform > Configure Service Account on page 44

To integrate Google Cloud with FortiCASB a Google G Suite Account with access to **Google Cloud Security Command Center** is required.

Configure Cloud IAM roles

1. Go to https://cloud.google.com/ and log in with your Google G Suite Account.
2. Click Navigation menu ≡ in top left corner.
3. Go to **IAM & admin > IAM.**
4. Click on the top **project selector** drop down list.
5. Select the organization that you want to enable Google Cloud Command Center.



6. Select the organization member and click Edit ✎ on IAM page.
7. In edit panel, click **+Add Another Role**.
8. Click on **Select a role**, search **Security Center Admin** and select it.
9. Click **Save**.
10. If the member does not have **Organization Administrator** role, repeat the above steps to add the role.

Enable Google Cloud Security Center and security sources

1. Click Navigation menu ≡ in top left corner.
2. Select **Security > Security Command Center.**
3. Security Command Center Marketplace page will show up. Click on **Go to Cloud Security Command Center**
4. .Click **Next** when asked to enable Security Command Center.
5. On Asset Monitoring Page, under **Enable asset discovery,** select **Include projects**.
6. Select the project which is installed on FortiCASB, and click **Enable.**

Wait a few minutes, refresh and Google Cloud Security Dashboard will appear. Security source needed to be enabled for Google Cloud Security Center to show findings

Enable Security Source

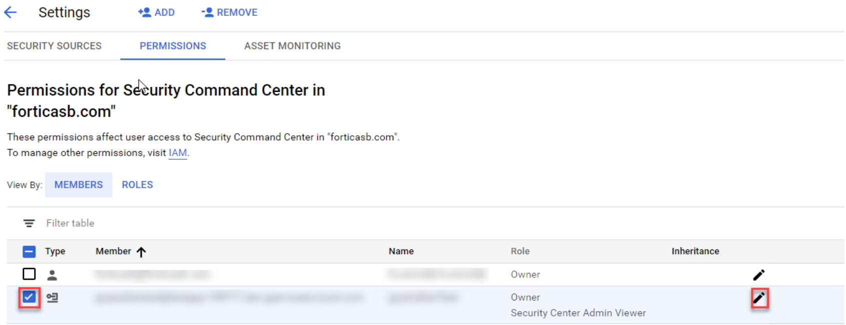
1. Go to **Google Security Command Center** page.
2. Click on **Settings** on the top right, and select **Security Sources** tab.

3. Click to enable **Cloud Anomaly Detection**, **Cloud Security Scanner**, and **Cloud DLP Data Discovery**.

Now findings will be shown in Security Command Center dashboard. We are now ready to grant the service account installed on FortiCASB with Google Cloud Security Center Access. Make sure you have the service account name handy. If not, follow steps from earlier to retrieve service account name: Getting Started > Install IAAS Applications > Google Cloud Platform > Configure Service Account on page 44

Enable Service Account with Security Center Access

1. Click Navigation menu ≡ in top left corner.
2. Go to **Security > Security Command Center**.
3. Click on **Settings** at the top right corner.
4. Choose **Permissions** tab.
5. Select the service account recorded earlier.
6. Click on **Edit Permission** ✎ .

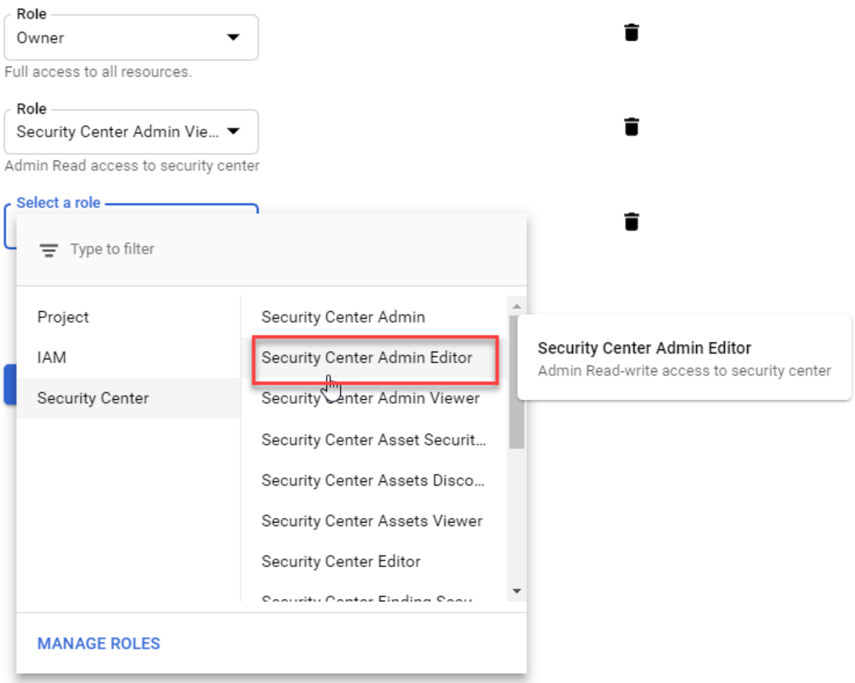


Permissions for Security Command Center in "forticasb.com"

These permissions affect user access to Security Command Center in "forticasb.com".
To manage other permissions, visit IAM.

	Type	Member ↑	Name	Role	Inheritance	
□		[redacted]	[redacted]	Owner		✎
☑		[redacted]	[redacted]	Owner Security Center Admin Viewer		✎

7. In Edit Permissions pop up menu, click **+Add Another Role**.
8. Click on the drop down menu of **Select a role**.
9. Select **Security Center Admin Editor**



Role: Owner
Full access to all resources.

Role: Security Center Admin Vie...
Admin Read access to security center

Select a role

Security Center Admin Editor
Admin Read-write access to security center

Type to filter
Project
IAM
Security Center
Security Center Admin
Security Center Admin Editor
Security Center Admin Viewer
Security Center Asset Securit...
Security Center Assets Disco...
Security Center Assets Viewer
Security Center Editor
MANAGE ROLES

10. Click **Save**

After the service account is granted with Security Center Admin Editor role, FortiCASB will extract cloud traffic data from Google Cloud Platform and provide real time monitoring.

IAAS Traffic Log

Traffic Log Configuration

FortiCASB consolidate all virtual private cloud resources and present in a graphical user interface that is clear and easy to navigate, helping you to quickly target security breaches and intrusions. Follow the following guidelines to setup traffic log to enable Traffic feature on your cloud platforms.

Amazon AWS Traffic Log Configuration

FortiCASB consolidates Amazon cloud traffic logs of all virtual private cloud resources and present in a graphical user interface. By enabling traffic log, FortiCASB lets you be able to monitor all inbound and outbound traffic visually, and remediate suspicious activities on AWS Cloud. To activate Traffic feature on FortiCASB, AWS flow logs needs to be enabled.

Prerequisite

An active Amazon AWS account installed on FortiCASB is required to enable Traffic logging.

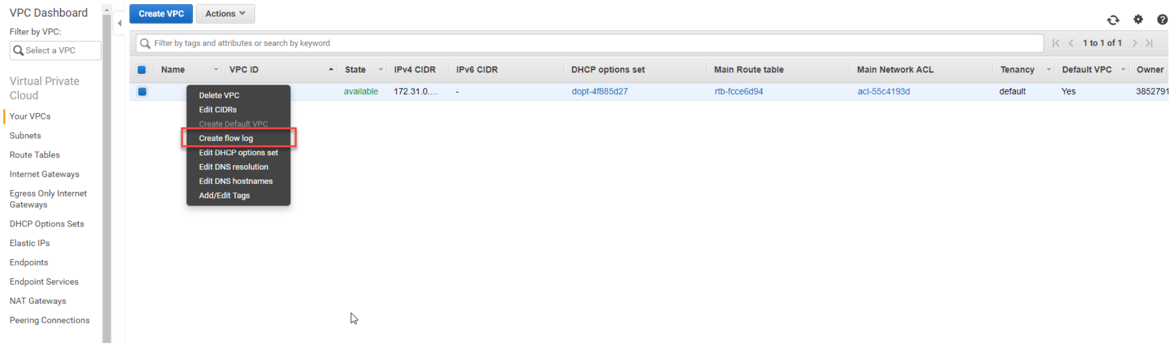
For installing Amazon AWS account on FortiCASB, please refer to Getting Started > Installing IAAS applications on page 33

Create log group on AWS

1. Log into AWS portal: https://console.aws.amazon.com/
2. Click on **Services** and search for "cloudwatch".
3. Click on **Logs** from left menu.
4. Click on **Get Started**. then click on **Create log group** in welcome page.
5. Give a log group name and keep the log group name for later use.
6. Click **OK** to finish creating log group.

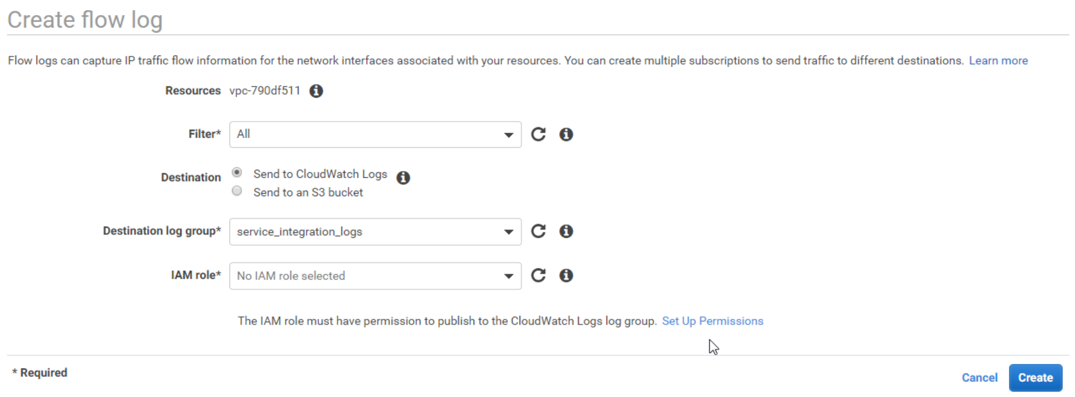
Enable flow log in VPC

1. Click on **Services** and search for "VPC".
2. In VPC Dashboard, click **Your VPCs**.
3. Select all the VPC that you want to create flow log, right click, and select **Create flow log**.



Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set	Main Route table	Main Network ACL	Tenancy	Default VPC	Owner
		available	172.31.0....	-	dopt-4f885d27	rtb-fcce6d94	acl-55c4193d	default	Yes	3852791

4. In **Filter** field, click on drop down menu to select **All**.
5. Make sure **Destination** has **Send to CloudWatch Logs** selected.
6. In **Destination log group**, enter the log group name created earlier.
7. Click on **Set Up Permissions** Under IAM role to grant permission.



Create flow log

Flow logs can capture IP traffic flow information for the network interfaces associated with your resources. You can create multiple subscriptions to send traffic to different destinations. Learn more

Resources vpc-790df511

Filter* All

Destination ● Send to CloudWatch Logs ○ Send to an S3 bucket

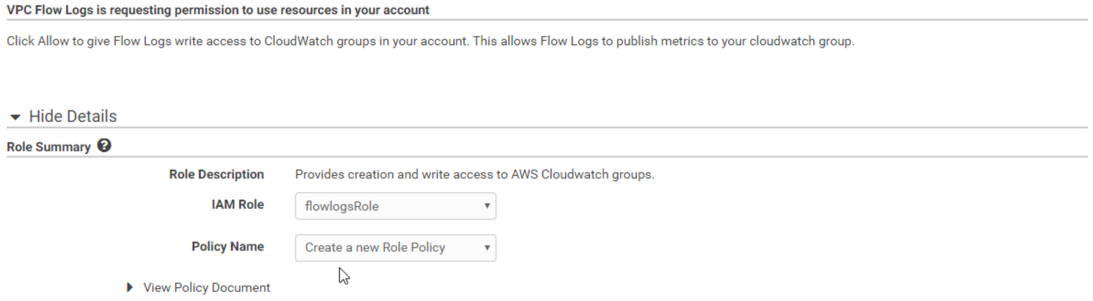
Destination log group* service_integration_logs

IAM role* No IAM role selected

The IAM role must have permission to publish to the CloudWatch Logs log group. Set Up Permissions

* Required

8. In the new pop-up screen, next to **IAM Role**, make sure **flowlogsRole** is selected, for **Policy Name**, make sure **Create a new Role Policy** is selected.



VPC Flow Logs is requesting permission to use resources in your account

Click Allow to give Flow Logs write access to CloudWatch groups in your account. This allows Flow Logs to publish metrics to your cloudwatch group.

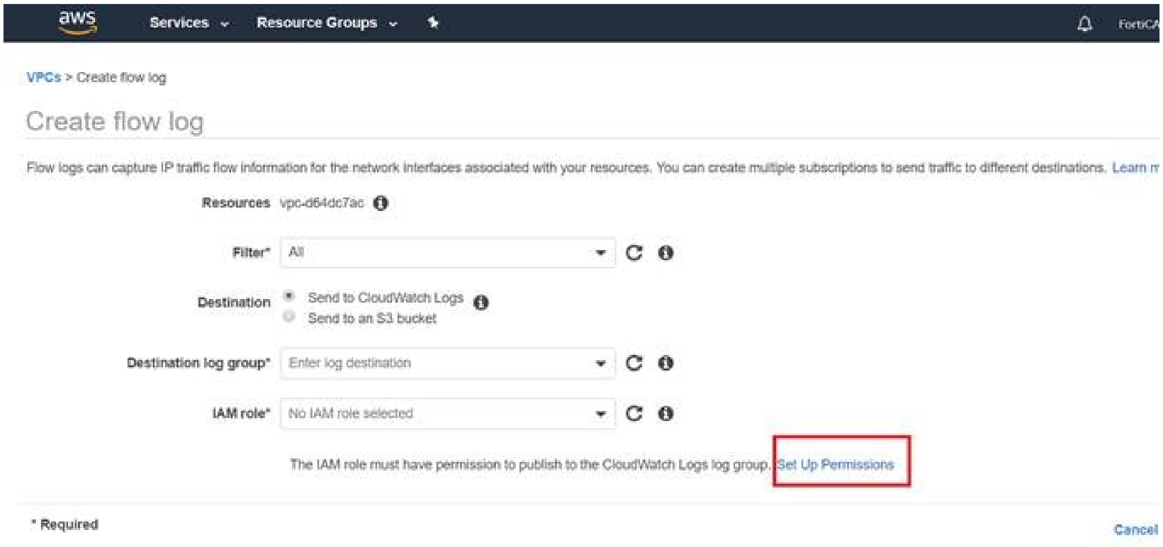
Role Summary

Role Description Provides creation and write access to AWS Cloudwatch groups.

IAM Role flowlogsRole

Policy Name Create a new Role Policy

9. Click **Allow**.
10. Go back to Create flow log page, next to **IAM role**, select **flowlogsRole**. Then go to step 12.
    If **flowlogsRole** is not in the selection, this means that you are setting up VPC flow log for the first time. Click **Set Up Permissions** to set up a new Role.



Create flow log

Flow logs can capture IP traffic flow information for the network interfaces associated with your resources. You can create multiple subscriptions to send traffic to different destinations. Learn m

Resources vpc-d64dc7ac

Filter* All

Destination ● Send to CloudWatch Logs ○ Send to an S3 bucket

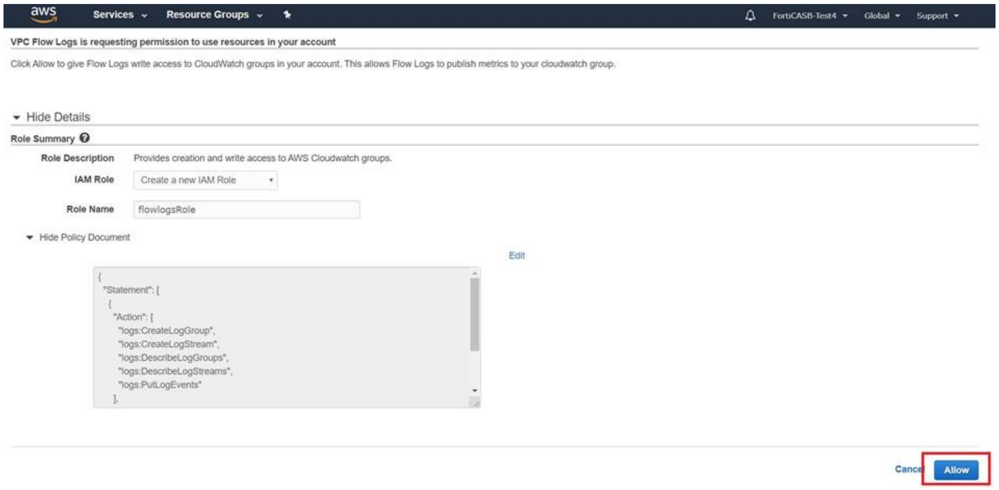
Destination log group* Enter log destination

IAM role* No IAM role selected

The IAM role must have permission to publish to the CloudWatch Logs log group. Set Up Permissions

* Required

11. When Flow Logs Role creation page pop-up, click **Allow** to grant permission to create a Role with the name **flowlogsRole**.



VPC Flow Logs is requesting permission to use resources in your account

Click Allow to give Flow Logs write access to CloudWatch groups in your account. This allows Flow Logs to publish metrics to your cloudwatch group.

Hide Details

Role Summary

Role Description: Provides creation and write access to AWS Cloudwatch groups.

IAM Role: Create a new IAM Role

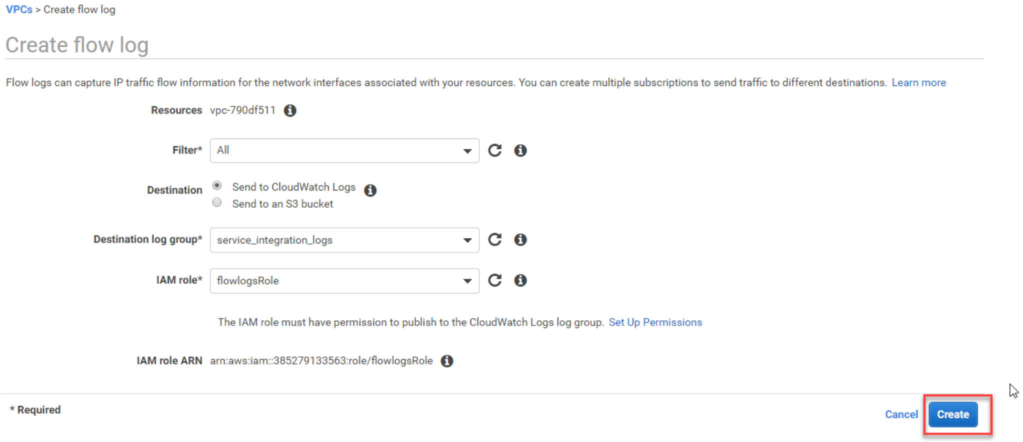
Role Name: flowlogsRole

Hide Policy Document

Edit

```
{
 "Statement": [
  {
   "Action": [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "logs:PutLogEvents"
   ],
```

12. Now go back to "Create flow log" page, select **flowlogsRole** under **IAM role**, then click **Create** to complete the setup.



VPCs > Create flow log

Create flow log

Flow logs can capture IP traffic flow information for the network interfaces associated with your resources. You can create multiple subscriptions to send traffic to different destinations. Learn more

Resources: vpc-790df511

Filter*: All

Destination: ● Send to CloudWatch Logs ○ Send to an S3 bucket

Destination log group*: service_integration_logs

IAM role*: flowlogsRole

The IAM role must have permission to publish to the CloudWatch Logs log group. Set Up Permissions

IAM role ARN: arn:aws:iam::385279133563:role/flowlogsRole

* Required

FortiCASB is now able to extract cloud traffic data from AWS and present in Traffic on FortiCASB.

Microsoft Azure Traffic Log Configuration

FortiCASB consolidates Azure cloud traffic logs of all virtual private cloud resources and present in a graphical user interface. By enabling traffic log, FortiCASB lets you be able to monitor all inbound and outbound traffic visually, and remediate suspicious activities on Azure Cloud. To activate Traffic feature on FortiCASB, Azure flow logs needs to be enabled.

Prerequisites

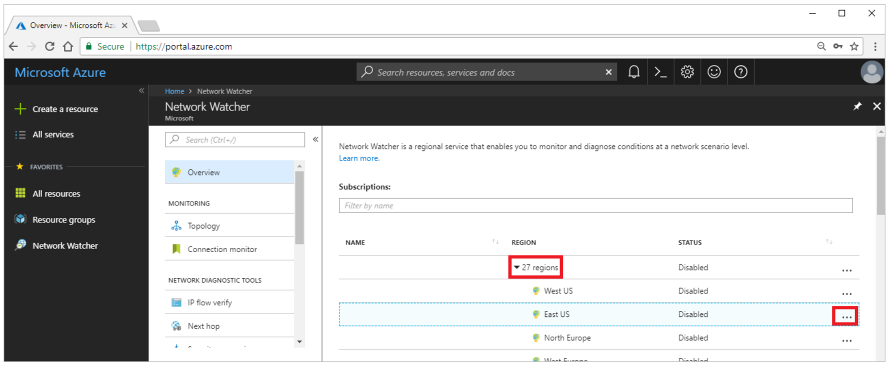
An active Azure Cloud account installed on FortiCASB is required to enable Traffic logging.

For installing Azure Cloud account on FortiCASB, please refer to Getting Started > Installing IAAS applications on page 33

To utilize traffic log from Azure Cloud, an active virtual machine with network watcher is required to activate this feature on FortiCASB. Network Security Group flow logging also requires Microsoft Insights to create flow logs.

Enable Network Watcher

1. In Azure Portal, in the top search field, search and click on **Network Watcher**
2. Select **Regions** to expand it, and select **...** to the right of the targeted region.



Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level.
Learn more.

Subscriptions:

Filter by name

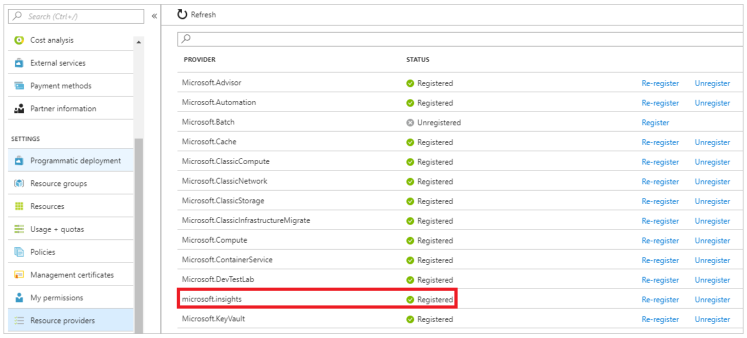
NAME	REGION	STATUS	
	▾ 27 regions	Disabled	...
	West US	Disabled	...
	East US	Disabled	...
	North Europe	Disabled	...
	West Europe	Disabled	

3. Select **Enable Network Watcher**.

Register Insights Provider

1. In Azure Portal, search and click on **Subscriptions**.
2. Select the subscription you want to enable the provider.
3. Select **Resource providers** under **Settings**.

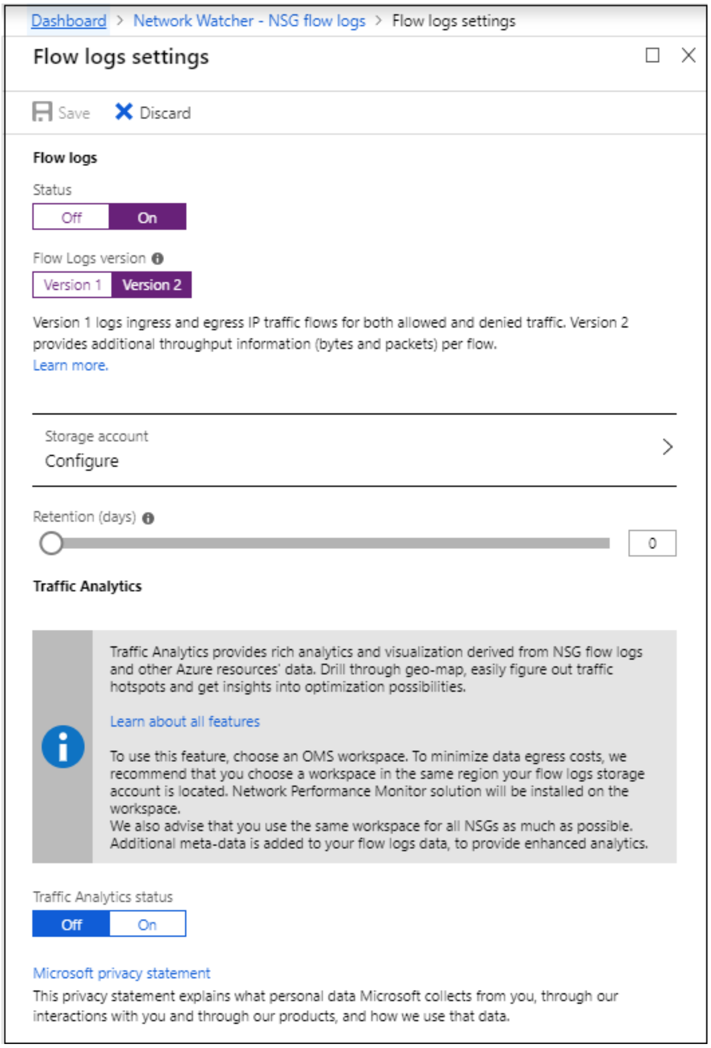
4. Make sure **microsoft.insights** provider is **Registered**. If it is **Unregistered**, select Register.



PROVIDER	STATUS		
Microsoft.Advisor	Registered	Re-register	Unregister
Microsoft.Automation	Registered	Re-register	Unregister
Microsoft.Batch	Unregistered	Register	
Microsoft.Cache	Registered	Re-register	Unregister
Microsoft.ClassicCompute	Registered	Re-register	Unregister
Microsoft.ClassicNetwork	Registered	Re-register	Unregister
Microsoft.ClassicStorage	Registered	Re-register	Unregister
Microsoft.ClassicInfrastructureMigrate	Registered	Re-register	Unregister
Microsoft.Compute	Registered	Re-register	Unregister
Microsoft.ContainerService	Registered	Re-register	Unregister
Microsoft.DevTestLab	Registered	Re-register	Unregister
microsoft.insights	Registered	Re-register	Unregister
Microsoft.KeyVault	Registered	Re-register	Unregister

Enable NSG flow log

1. NSG flow log requires an Azure Storage account to store the flow logs. To create an Azure Storage account, select **+Create** a resource at the top left corner of the portal.
2. Select Storage, and then select **Storage account.**
3. Enter **Storage account name**, **Location**, and select a **Resource group**, then select Create.
   The storage account may take around a few minutes to create. If you are using an existing storage account, make sure that the storage account has **All networks(default)** selected for **Firewalls and virtual networks**, under Setting in storage account.
4. Search and click on **Network Watcher** in the top of Azure portal.
5. Select **NSG flow logs** under **LOGS**.
6. From the list of **NSG flow logs**, select (virtual machine name)-nsg.
7. Under **Flow logs settings**, select **On**.
8. Select flow logging version. Version 2 contains flow session statistics.


Dashboard > Network Watcher - NSG flow logs > Flow logs settings
Save
Discard

Flow logs settings

Flow logs

Status: Off | **On**

Flow Logs version: Version 1 | **Version 2**

Version 1 logs ingress and egress IP traffic flows for both allowed and denied traffic. Version 2 provides additional throughput information (bytes and packets) per flow.
Learn more.

Storage account: Configure

Retention (days): 0

Traffic Analytics

Traffic Analytics provides rich analytics and visualization derived from NSG flow logs and other Azure resources' data. Drill through geo-map, easily figure out traffic hotspots and get insights into optimization possibilities.

Learn about all features

To use this feature, choose an OMS workspace. To minimize data egress costs, we recommend that you choose a workspace in the same region your flow logs storage account is located. Network Performance Monitor solution will be installed on the workspace.
We also advise that you use the same workspace for all NSGs as much as possible. Additional meta-data is added to your flow logs data, to provide enhanced analytics.

Traffic Analytics status: **Off** | On

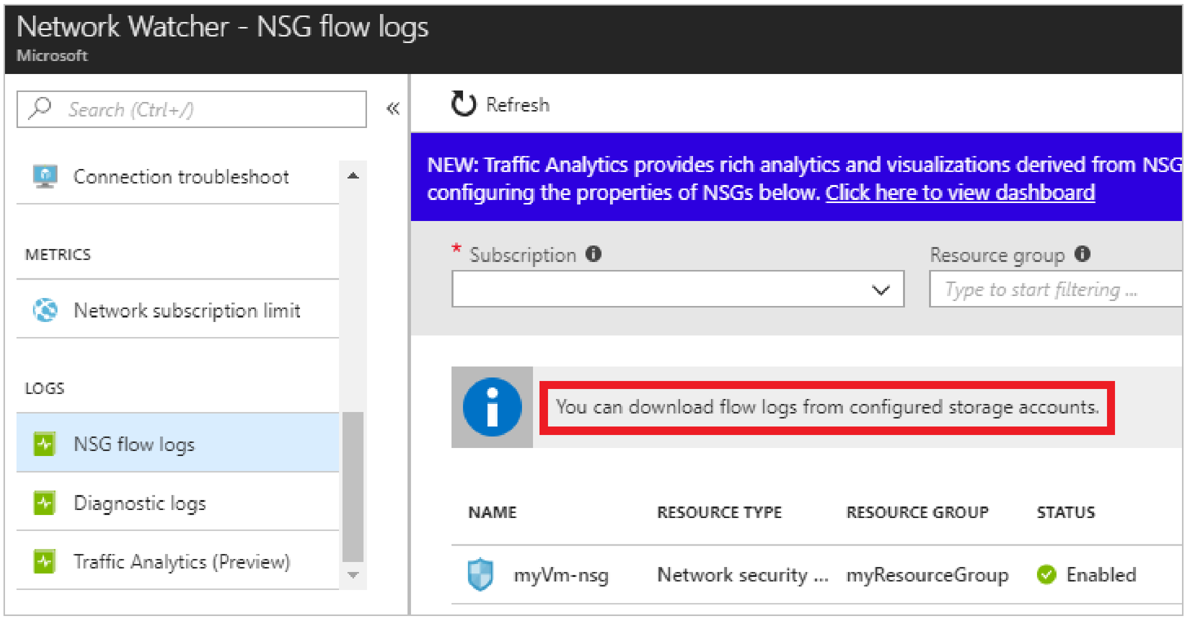
Microsoft privacy statement
This privacy statement explains what personal data Microsoft collects from you, through our interactions with you and through our products, and how we use that data.

9. Select the storage account created earlier in step 3.
10. Set **Retention(days)** to 5 and then select **Save**.

Download/View flow log

1. From Network Watcher portal, select NSG flow logs under LOGS.
2. Select "You can download flow logs from configured storage accounts", as shown in the following:

3.



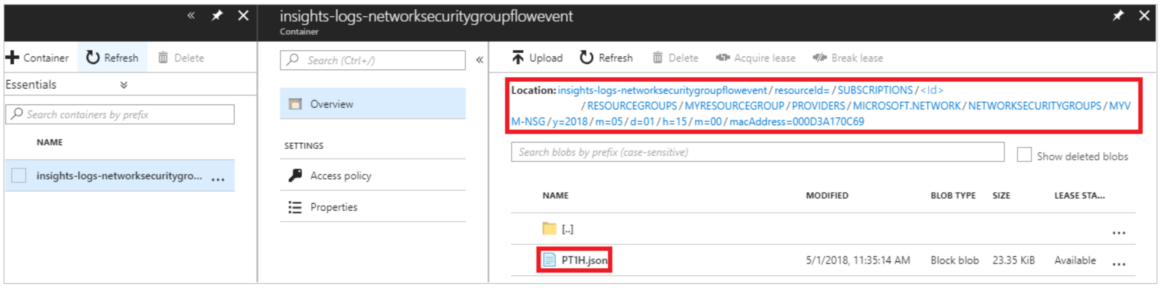
NEW: Traffic Analytics provides rich analytics and visualizations derived from NSG configuring the properties of NSGs below. Click here to view dashboard

You can download flow logs from configured storage accounts.

NAME	RESOURCE TYPE	RESOURCE GROUP	STATUS
myVm-nsg	Network security ...	myResourceGroup	Enabled

4. Select the storage account from step 2 of Enable NSG flow log.
5. Under Blob service, select Blobs, and then select the insights-logs-networksecuritygroupflowevent container.
6. In the container navigate the folder hierachy until you get to a PT1H.json file. Log files are in the following naming convention:

   https://{storageAccountName}.blob.core.windows.net/insights-logs-networksecuritygroupflowevent/resourceId=/SUBSCRIPTIONS/{subscriptionID}/RESOURCEGROUPS/{resourceGroupName}/PROVIDERS/MICROSOFT.NETWORK/NETWORKSECURITYGROUPS/{nsgName}/y={year}/m={month}/d={day}/h={hour}/m=00/macAddress={macAddress}/PT1H.json



Location: insights-logs-networksecuritygroupflowevent / resourceId= / SUBSCRIPTIONS / <Id> / RESOURCEGROUPS / MYRESOURCEGROUP / PROVIDERS / MICROSOFT.NETWORK / NETWORKSECURITYGROUPS / MYVM-NSG / y=2018 / m=05 / d=01 / h=15 / m=00 / macAddress=000D3A170C69

NAME	MODIFIED	BLOB TYPE	SIZE	LEASE STA...
[..]				
PT1H.json	5/1/2018, 11:35:14 AM	Block blob	23.35 KiB	Available

7. Select ... to the right of the JSON file and select download to view the JSON file.

After verifying you can download and view the JSON file, the setting on Azure Cloud is completed. Now FortiCASB is able to capture traffic flow logs and present in Traffic.

Reference

Log network traffic to and from a virtual machine using the Azure portal.

https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-portal#enable-nsg-flow-log

Google Cloud Traffic Log Configuration

FortiCASB consolidates Google cloud flow logs of all virtual private cloud resources and present in a graphical user interface. By enabling traffic log, FortiCASB lets you be able to monitor all inbound and outbound traffic visually, and remediate suspicious activities on Google Cloud. To activate Traffic feature on FortiCASB, Google Cloud flow logs needs to be enabled.

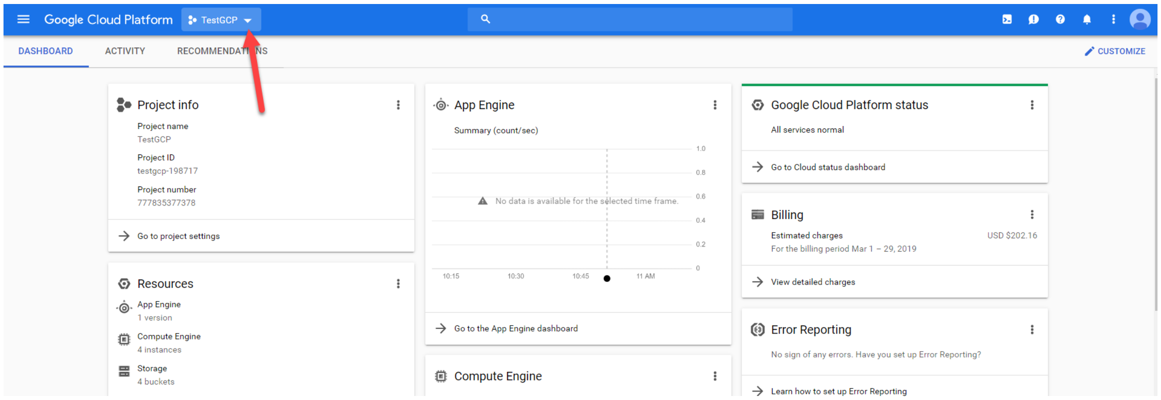
Prerequisite

An active Google Cloud accoung installed on FortiCASB is required to enable Traffic logging.

For installing Google Cloud account on FortiCASB, please refer to Getting Started > Installing IAAS applications on page 33

Enable Flow Logs

1. Log into Google Cloud console with your Google Cloud account: https://console.cloud.google.com/.
2. Select the project to active flow logs from the top project drop down menu.



Google Cloud Platform TestGCP

DASHBOARD ACTIVITY RECOMMENDATIONS CUSTOMIZE

Project info

Project name
TestGCP

Project ID
testgcp-198717

Project number
777835377378

Go to project settings

Resources

App Engine
1 version

Compute Engine
4 instances

Storage
4 buckets

App Engine

Summary (count/sec)

No data is available for the selected time frame.

Go to the App Engine dashboard

Compute Engine

Google Cloud Platform status

All services normal

Go to Cloud status dashboard

Billing

Estimated charges USD $202.16
For the billing period Mar 1 – 29, 2019

View detailed charges

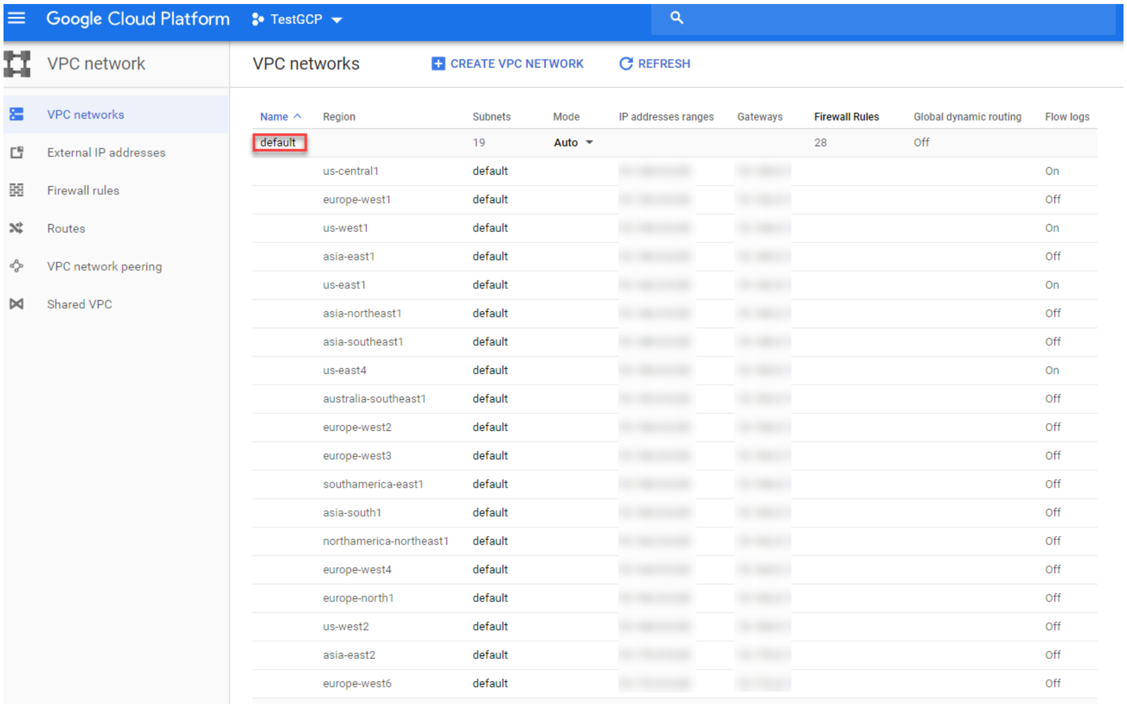
Error Reporting

No sign of any errors. Have you set up Error Reporting?

Learn how to set up Error Reporting

3. Click on top **Navigation button** ☰ and select **VPC networks** > **VPC networks**.

4. In **VPC network** dashboard, click on a VPC name.



Google Cloud Platform TestGCP

VPC network

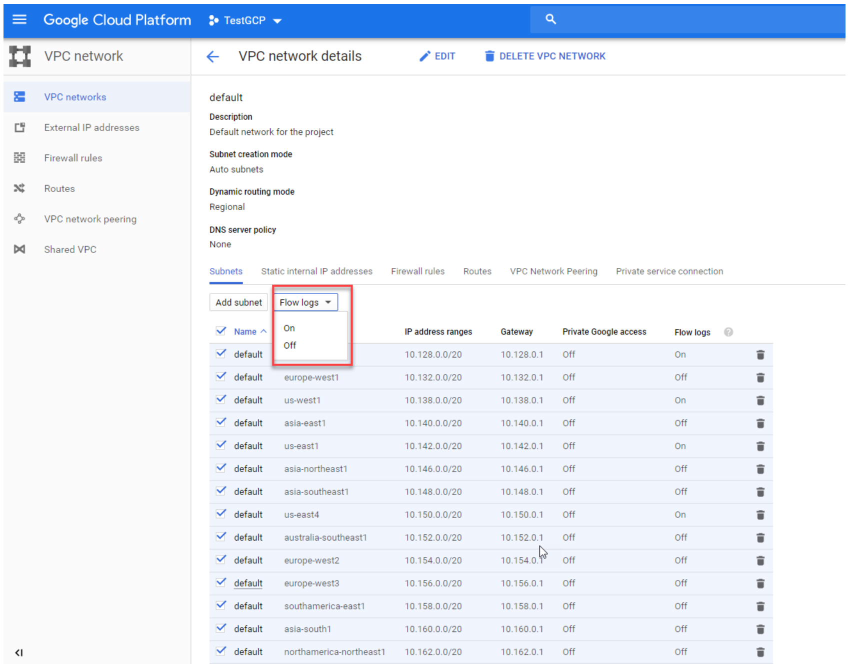
VPC networks CREATE VPC NETWORK REFRESH

VPC networks
External IP addresses
Firewall rules
Routes
VPC network peering
Shared VPC

Name	Region	Subnets	Mode	IP addresses ranges	Gateways	Firewall Rules	Global dynamic routing	Flow logs
default		19	Auto			28	Off	
	us-central1	default		[redacted]	[redacted]			On
	europe-west1	default		[redacted]	[redacted]			Off
	us-west1	default		[redacted]	[redacted]			On
	asia-east1	default		[redacted]	[redacted]			Off
	us-east1	default		[redacted]	[redacted]			On
	asia-northeast1	default		[redacted]	[redacted]			Off
	asia-southeast1	default		[redacted]	[redacted]			Off
	us-east4	default		[redacted]	[redacted]			On
	australia-southeast1	default		[redacted]	[redacted]			Off
	europe-west2	default		[redacted]	[redacted]			Off
	europe-west3	default		[redacted]	[redacted]			Off
	southamerica-east1	default		[redacted]	[redacted]			Off
	asia-south1	default		[redacted]	[redacted]			Off
	northamerica-northeast1	default		[redacted]	[redacted]			Off
	europe-west4	default		[redacted]	[redacted]			Off
	europe-north1	default		[redacted]	[redacted]			Off
	us-west2	default		[redacted]	[redacted]			Off
	asia-east2	default		[redacted]	[redacted]			Off
	europe-west6	default		[redacted]	[redacted]			Off

5. Select All or only the intended subnets to turn on flow logs.

6. Click on **Flow logs** drop down menu and select **On**.



default

Description
Default network for the project

Subnet creation mode
Auto subnets

Dynamic routing mode
Regional

DNS server policy
None

Name		IP address ranges	Gateway	Private Google access	Flow logs
default		10.128.0.0/20	10.128.0.1	Off	On
default	europe-west1	10.132.0.0/20	10.132.0.1	Off	Off
default	us-west1	10.138.0.0/20	10.138.0.1	Off	On
default	asia-east1	10.140.0.0/20	10.140.0.1	Off	Off
default	us-east1	10.142.0.0/20	10.142.0.1	Off	On
default	asia-northeast1	10.146.0.0/20	10.146.0.1	Off	Off
default	asia-southeast1	10.148.0.0/20	10.148.0.1	Off	Off
default	us-east4	10.150.0.0/20	10.150.0.1	Off	On
default	australia-southeast1	10.152.0.0/20	10.152.0.1	Off	Off
default	europe-west2	10.154.0.0/20	10.154.0.1	Off	Off
default	europe-west3	10.156.0.0/20	10.156.0.1	Off	Off
default	southamerica-east1	10.158.0.0/20	10.158.0.1	Off	Off
default	asia-south1	10.160.0.0/20	10.160.0.1	Off	Off
default	northamerica-northeast1	10.162.0.0/20	10.162.0.1	Off	Off

Now FortiCASB is able to extract cloud traffic data from Google Cloud and present in Traffic on FortiCASB.

Resource

FortiCASB displays all cloud resources in detailed list grouped by regions and resource types to give easy access and organized view of all cloud resources for cloud administrators.

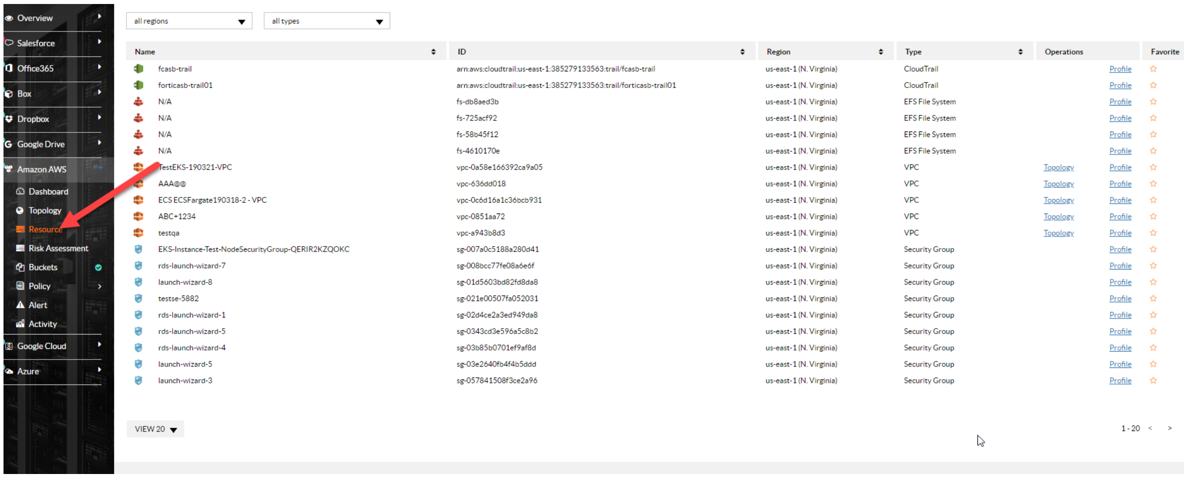
Prerequisites

An active IAAS account installed on FortiCASB is required to use Resource.

For installing IAAS account on FortiCASB, please refer to Getting Started > Installing IAAS applications on page 33

Accessing Resource on IAAS account

1. Log into FortiCASB https://www.forticasb.com/ with your FortiCASB user account.
2. From FortiCASB **Overview** dashboard, select an IAAS account on the left menu.
3. Under the IAAS account menu, click on **Resource**

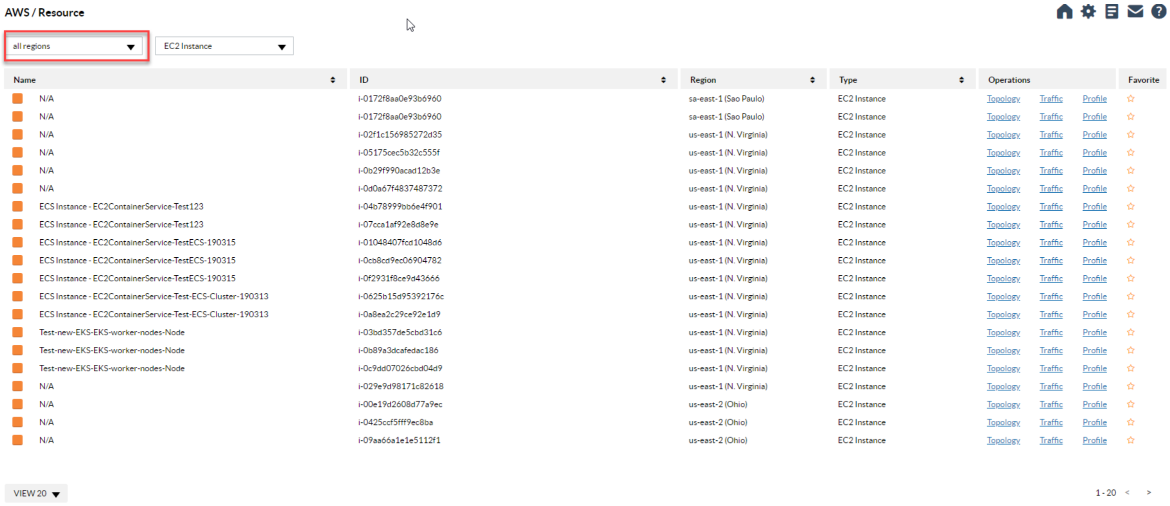


all regions ▼ all types ▼

Name	ID	Region	Type	Operations	Favorite
fcasb-trail	arn:aws:cloudtrail:us-east-1:385279133563:trail/fcasb-trail	us-east-1 (N. Virginia)	CloudTrail	Profile	☆
forticasb-trail01	arn:aws:cloudtrail:us-east-1:385279133563:trail/forticasb-trail01	us-east-1 (N. Virginia)	CloudTrail	Profile	☆
N/A	fs-db8aed3b	us-east-1 (N. Virginia)	EFS File System	Profile	☆
N/A	fs-725acf92	us-east-1 (N. Virginia)	EFS File System	Profile	☆
N/A	fs-58b45f12	us-east-1 (N. Virginia)	EFS File System	Profile	☆
N/A	fs-4610170e	us-east-1 (N. Virginia)	EFS File System	Profile	☆
TestEKS-190321-VPC	vpc-0a58e166392ca9a05	us-east-1 (N. Virginia)	VPC	Topology Profile	☆
AAA@@	vpc-636dd018	us-east-1 (N. Virginia)	VPC	Topology Profile	☆
ECS ECSFargate190318-2 - VPC	vpc-0c6d16a1c36bcb931	us-east-1 (N. Virginia)	VPC	Topology Profile	☆
ABC+1234	vpc-0851aa72	us-east-1 (N. Virginia)	VPC	Topology Profile	☆
testqa	vpc-a943b8d3	us-east-1 (N. Virginia)	VPC	Topology Profile	☆
EKS-Instance-Test-NodeSecurityGroup-QERIR2KZQOKC	sg-007a0c5188a280d41	us-east-1 (N. Virginia)	Security Group	Profile	☆
rds-launch-wizard-7	sg-008bcc77fe08a6e6f	us-east-1 (N. Virginia)	Security Group	Profile	☆
launch-wizard-8	sg-01d5603bd82fd8da8	us-east-1 (N. Virginia)	Security Group	Profile	☆
testse-5882	sg-021e00507fa052031	us-east-1 (N. Virginia)	Security Group	Profile	☆
rds-launch-wizard-1	sg-02d4ce2a3ed949da8	us-east-1 (N. Virginia)	Security Group	Profile	☆
rds-launch-wizard-5	sg-0343cd3e596a5c8b2	us-east-1 (N. Virginia)	Security Group	Profile	☆
rds-launch-wizard-4	sg-03b85b0701ef9af8d	us-east-1 (N. Virginia)	Security Group	Profile	☆
launch-wizard-5	sg-03e2640fb4f4b5ddd	us-east-1 (N. Virginia)	Security Group	Profile	☆
launch-wizard-3	sg-057841508f3ce2a96	us-east-1 (N. Virginia)	Security Group	Profile	☆

VIEW 20 ▼ 1 - 20 < >

4. Click on the top left drop down menu next to **all regions** for desired region where the cloud resource is located.

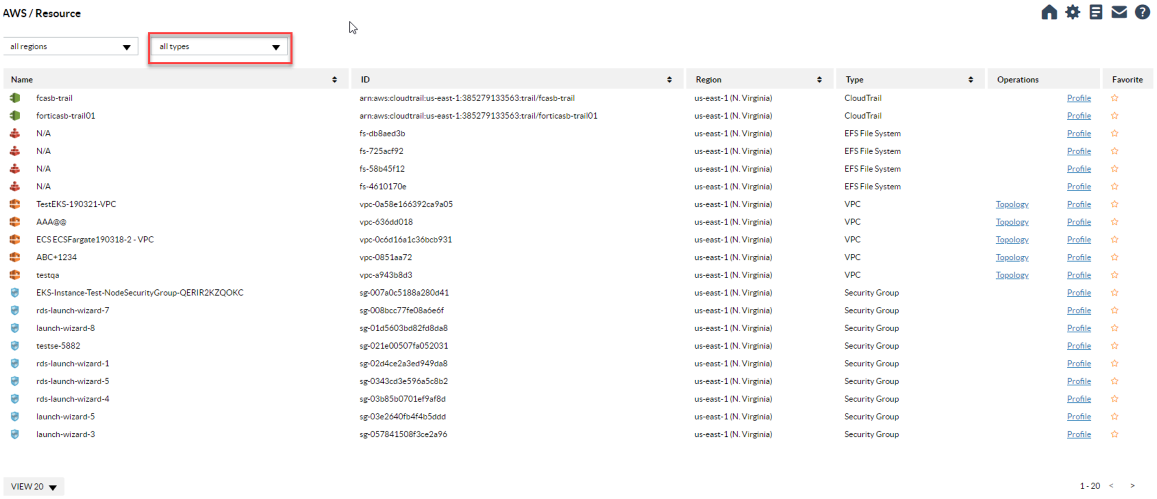

AWS / Resource

all regions ▼ EC2 Instance ▼

Name	ID	Region	Type	Operations	Favorite
N/A	i-0172f8aa0e93b6960	sa-east-1 (Sao Paulo)	EC2 Instance	Topology Traffic Profile	☆
N/A	i-0172f8aa0e93b6960	sa-east-1 (Sao Paulo)	EC2 Instance	Topology Traffic Profile	☆
N/A	i-02f1c156985272d35	us-east-1 (N. Virginia)	EC2 Instance	Topology Traffic Profile	☆
N/A	i-05175cec5b32c555f	us-east-1 (N. Virginia)	EC2 Instance	Topology Traffic Profile	☆
N/A	i-0b29f990acad12b3e	us-east-1 (N. Virginia)	EC2 Instance	Topology Traffic Profile	☆
N/A	i-0d0a67f4837487372	us-east-1 (N. Virginia)	EC2 Instance	Topology Traffic Profile	☆
ECS Instance - EC2ContainerService-Test123	i-04b78999bb6e4f901	us-east-1 (N. Virginia)	EC2 Instance	Topology Traffic Profile	☆
ECS Instance - EC2ContainerService-Test123	i-07cca1af92e8d8e9e	us-east-1 (N. Virginia)	EC2 Instance	Topology Traffic Profile	☆
ECS Instance - EC2ContainerService-TestECS-190315	i-01048407fcd1048d6	us-east-1 (N. Virginia)	EC2 Instance	Topology Traffic Profile	☆
ECS Instance - EC2ContainerService-TestECS-190315	i-0cb8cd9ec06904782	us-east-1 (N. Virginia)	EC2 Instance	Topology Traffic Profile	☆
ECS Instance - EC2ContainerService-TestECS-190315	i-0f2931f8ce9d43666	us-east-1 (N. Virginia)	EC2 Instance	Topology Traffic Profile	☆
ECS Instance - EC2ContainerService-Test-ECS-Cluster-190313	i-0625b15d95392176c	us-east-1 (N. Virginia)	EC2 Instance	Topology Traffic Profile	☆
ECS Instance - EC2ContainerService-Test-ECS-Cluster-190313	i-0a8ea2c29ce92e1d9	us-east-1 (N. Virginia)	EC2 Instance	Topology Traffic Profile	☆
Test-new-EKS-EKS-worker-nodes-Node	i-03bd357de5cbd31c6	us-east-1 (N. Virginia)	EC2 Instance	Topology Traffic Profile	☆
Test-new-EKS-EKS-worker-nodes-Node	i-0b89a3dcafedac186	us-east-1 (N. Virginia)	EC2 Instance	Topology Traffic Profile	☆
Test-new-EKS-EKS-worker-nodes-Node	i-0c9dd07026cbd04d9	us-east-1 (N. Virginia)	EC2 Instance	Topology Traffic Profile	☆
N/A	i-029e9d98171c82618	us-east-1 (N. Virginia)	EC2 Instance	Topology Traffic Profile	☆
N/A	i-00e19d2608d77a9ec	us-east-2 (Ohio)	EC2 Instance	Topology Traffic Profile	☆
N/A	i-0425ccf5fff9ec8ba	us-east-2 (Ohio)	EC2 Instance	Topology Traffic Profile	☆
N/A	i-09aa66a1e1e5112f1	us-east-2 (Ohio)	EC2 Instance	Topology Traffic Profile	☆

VIEW 20 ▼ 1 - 20 < >

5. Click on the top right drop down menu next to **all types** for desired cloud resources.



AWS / Resource

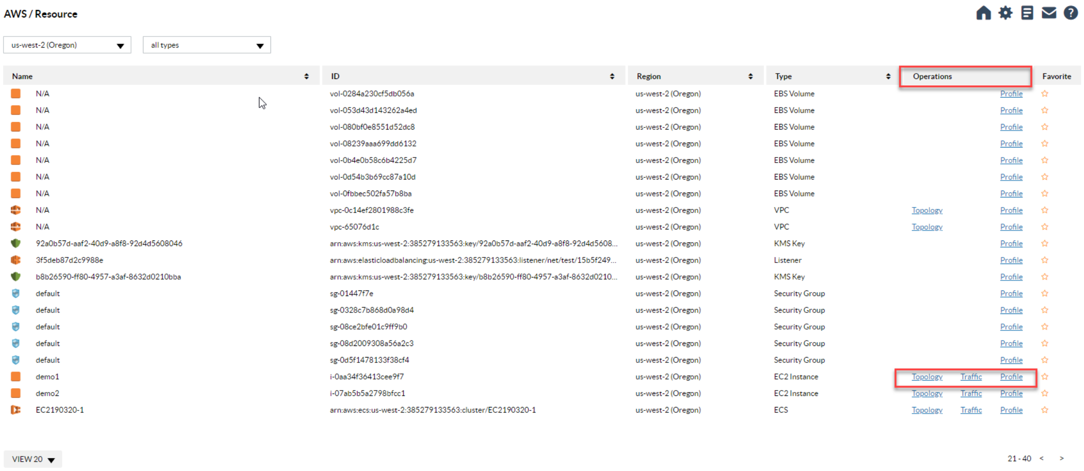
all regions ▼ | all types ▼

Name	ID	Region	Type	Operations	Favorite
fcasb-trail	arn:aws:cloudtrail:us-east-1:385279133563:trail/fcasb-trail	us-east-1 (N. Virginia)	CloudTrail	Profile	☆
forticasb-trail01	arn:aws:cloudtrail:us-east-1:385279133563:trail/forticasb-trail01	us-east-1 (N. Virginia)	CloudTrail	Profile	☆
N/A	fs-db8aed3b	us-east-1 (N. Virginia)	EFS File System	Profile	☆
N/A	fs-725acf92	us-east-1 (N. Virginia)	EFS File System	Profile	☆
N/A	fs-58b45f12	us-east-1 (N. Virginia)	EFS File System	Profile	☆
N/A	fs-4610170e	us-east-1 (N. Virginia)	EFS File System	Profile	☆
TestEKS-190321-VPC	vpc-0a58e166392ca9a05	us-east-1 (N. Virginia)	VPC	Topology Profile	☆
AAA@@	vpc-636dd018	us-east-1 (N. Virginia)	VPC	Topology Profile	☆
ECS ECSFargate190318-2 - VPC	vpc-0c6d16a1c36bcb931	us-east-1 (N. Virginia)	VPC	Topology Profile	☆
ABC+1234	vpc-0851aa72	us-east-1 (N. Virginia)	VPC	Topology Profile	☆
testqa	vpc-a943b8d3	us-east-1 (N. Virginia)	VPC	Topology Profile	☆
EKS-Instance-Test-NodeSecurityGroup-QERIR2KZQOKC	sg-007a0c5188a280d41	us-east-1 (N. Virginia)	Security Group	Profile	☆
rds-launch-wizard-7	sg-008bcc77fe08a6e6f	us-east-1 (N. Virginia)	Security Group	Profile	☆
launch-wizard-8	sg-01d5603bd82fd8da8	us-east-1 (N. Virginia)	Security Group	Profile	☆
testse-5882	sg-021e00507fa052031	us-east-1 (N. Virginia)	Security Group	Profile	☆
rds-launch-wizard-1	sg-02d4ce2a3ed949da8	us-east-1 (N. Virginia)	Security Group	Profile	☆
rds-launch-wizard-5	sg-0343cd3e596a5c8b2	us-east-1 (N. Virginia)	Security Group	Profile	☆
rds-launch-wizard-4	sg-03b85b0701ef9af8d	us-east-1 (N. Virginia)	Security Group	Profile	☆
launch-wizard-5	sg-03e2640fb4f4b5ddd	us-east-1 (N. Virginia)	Security Group	Profile	☆
launch-wizard-3	sg-057841508f3ce2a96	us-east-1 (N. Virginia)	Security Group	Profile	☆

VIEW 20 ▼ 1 - 20 < >

Accessing Traffic, Topology and Profile in Resource

1. After selecting the region and resource type from earlier, **Topology**, **Traffic**, and **Profile** will show under **Operations** column.



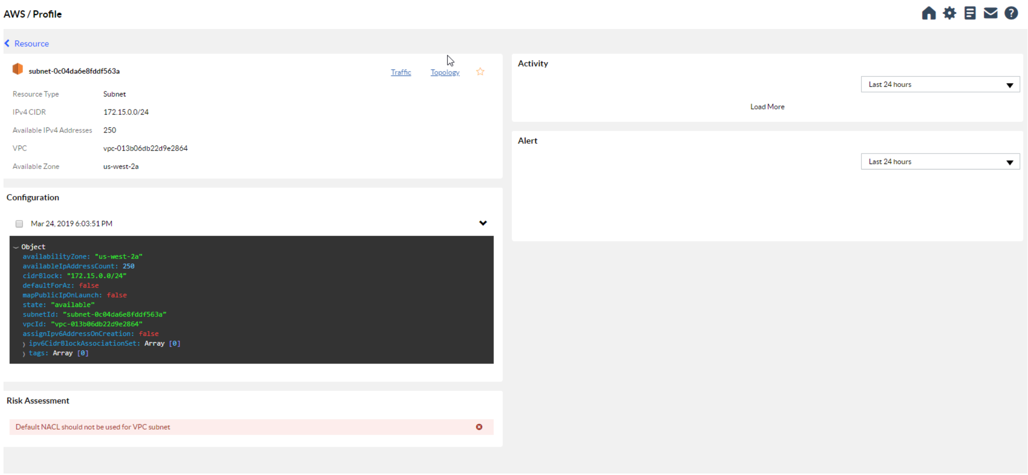
AWS / Resource

us-west-2 (Oregon) ▼ | all types ▼

Name	ID	Region	Type	Operations	Favorite
N/A	vol-0284a230cf5db056a	us-west-2 (Oregon)	EBS Volume	Profile	☆
N/A	vol-053d43d143262a4ed	us-west-2 (Oregon)	EBS Volume	Profile	☆
N/A	vol-080bf0e8551d52dc8	us-west-2 (Oregon)	EBS Volume	Profile	☆
N/A	vol-08239aaa699dd6132	us-west-2 (Oregon)	EBS Volume	Profile	☆
N/A	vol-0b4e0b58c6b4225d7	us-west-2 (Oregon)	EBS Volume	Profile	☆
N/A	vol-0d54b3b69cc87a10d	us-west-2 (Oregon)	EBS Volume	Profile	☆
N/A	vol-0fbbec502fa57b8ba	us-west-2 (Oregon)	EBS Volume	Profile	☆
N/A	vpc-0c14ef2801988c3fe	us-west-2 (Oregon)	VPC	Topology Profile	☆
N/A	vpc-65076d1c	us-west-2 (Oregon)	VPC	Topology Profile	☆
92a0b57d-aaf2-40d9-a8f8-92d4d5608046	arn:aws:kms:us-west-2:385279133563:key/92a0b57d-aaf2-40d9-a8f8-92d4d5608...	us-west-2 (Oregon)	KMS Key	Profile	☆
3f5deb87d2c9988e	arn:aws:elasticloadbalancing:us-west-2:385279133563:listener/net/test/15b5f249...	us-west-2 (Oregon)	Listener	Profile	☆
b8b26590-ff80-4957-a3af-8632d0210bba	arn:aws:kms:us-west-2:385279133563:key/b8b26590-ff80-4957-a3af-8632d0210...	us-west-2 (Oregon)	KMS Key	Profile	☆
default	sg-01447f7e	us-west-2 (Oregon)	Security Group	Profile	☆
default	sg-0328c7b868d0a98d4	us-west-2 (Oregon)	Security Group	Profile	☆
default	sg-08ce2bfe01c9ff9b0	us-west-2 (Oregon)	Security Group	Profile	☆
default	sg-08d2009308a56a2c3	us-west-2 (Oregon)	Security Group	Profile	☆
default	sg-0d5f1478133f38cf4	us-west-2 (Oregon)	Security Group	Profile	☆
demo1	i-0aa34f36413cee9f7	us-west-2 (Oregon)	EC2 Instance	Topology Traffic Profile	☆
demo2	i-07ab5b5a2798bfcc1	us-west-2 (Oregon)	EC2 Instance	Topology Traffic Profile	☆
EC2190320-1	arn:aws:ecs:us-west-2:385279133563:cluster/EC2190320-1	us-west-2 (Oregon)	ECS	Topology Traffic Profile	☆

VIEW 20 ▼ 21 - 40 < >

2. Click on **Profile** to view profile summary of the cloud resource.



subnet-0c04da6e8fddf563a

Resource Type	Subnet
IPv4 CIDR	172.15.0.0/24
Available IPv4 Addresses	250
VPC	vpc-013b06db22d9e2864
Available Zone	us-west-2a

Configuration

□ Mar 24, 2019 6:03:51 PM

```
⌄ Object
  availabilityZone: "us-west-2a"
  availableIpAddressCount: 250
  cidrBlock: "172.15.0.0/24"
  defaultForAz: false
  mapPublicIpOnLaunch: false
  state: "available"
  subnetId: "subnet-0c04da6e8fddf563a"
  vpcId: "vpc-013b06db22d9e2864"
  assignIpv6AddressOnCreation: false
  › ipv6CidrBlockAssociationSet: Array [0]
  › tags: Array [0]
```

Risk Assessment

Default NACL should not be used for VPC subnet

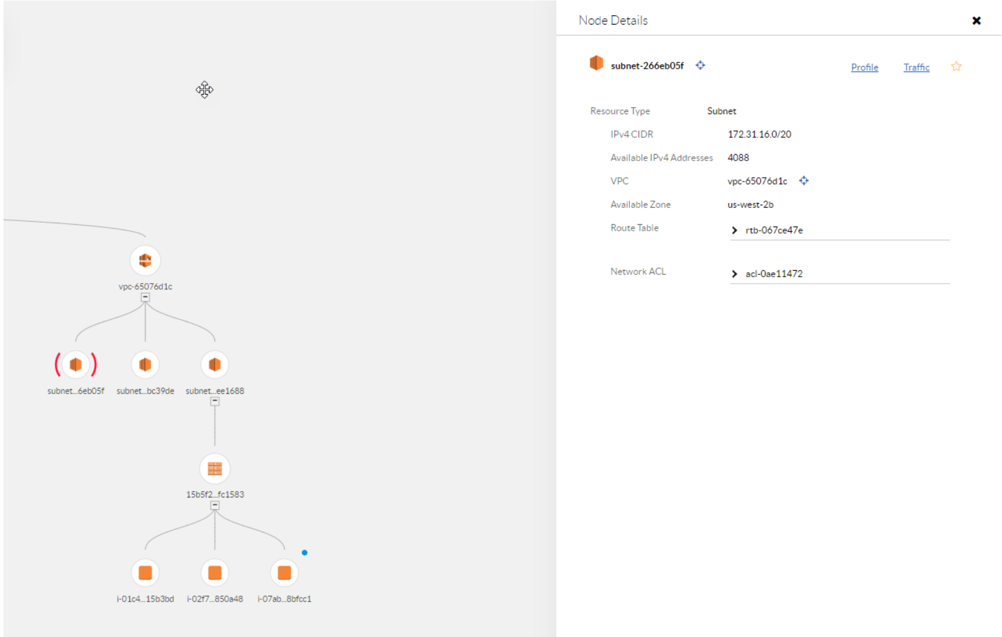
Activity

Last 24 hours

Alert

Last 24 hours

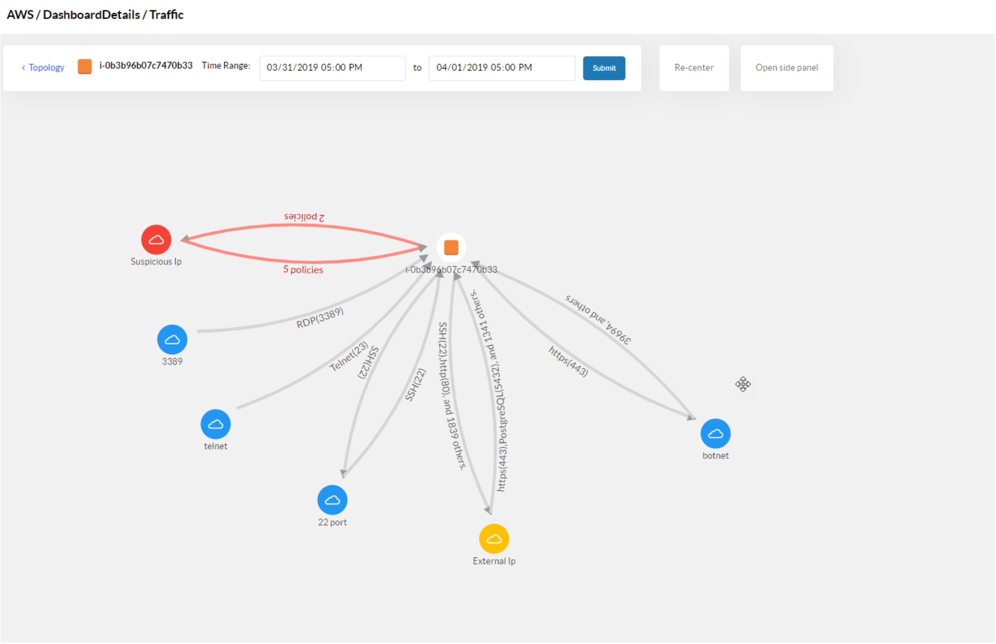
3. Click on **Topology** to show graphical view of the cloud hierarchy the resource belongs to.



subnet-266eb05f

Resource Type	Subnet
IPv4 CIDR	172.31.16.0/20
Available IPv4 Addresses	4088
VPC	vpc-65076d1c
Available Zone	us-west-2b
Route Table	› rtb-067ce47e
Network ACL	› acl-0ae11472

4. Click on **Traffic** to see inbound and outbound source that is accessing the cloud resource.



AWS / DashboardDetails / Traffic

‹ Topology i-0b3b96b07c7470b33 Time Range: 03/31/2019 05:00 PM to 04/01/2019 05:00 PM Submit

Resource Profile

FortiCASB profile shows a summary of all activities and configurations related to the virtual machine instance, as well as the security alerts triggered by risk assessment and cloud security integration from IAAS accounts.

Prerequisites

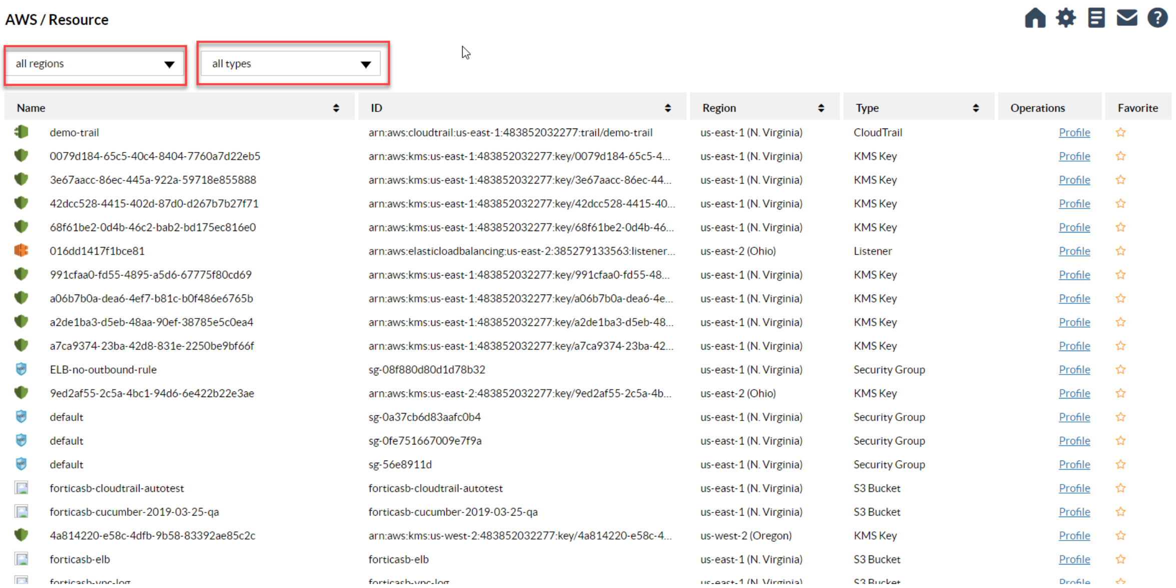
An active IAAS account installed on FortiCASB is required to see resource profile. Traffic log can be enabled to see Traffic in Resource Profile (optional)

For installing IAAS account on FortiCASB, please refer to Getting Started > Installing IAAS applications on page 33

For enabling traffic log, please refer to IAAS Traffic Log > Traffic Log Configuration (optional)

Access Profile through Resource

1. Log into FortiCASB https://www.forticasb.com/ with your FortiCASB user account.
2. From FortiCASB **Overview** dashboard, select an IAAS account on the left menu.
3. Under the IAAS account menu, click on **Resource**
4. Select a **region** from the top left menu and a **type** of cloud instance on the top right menu.

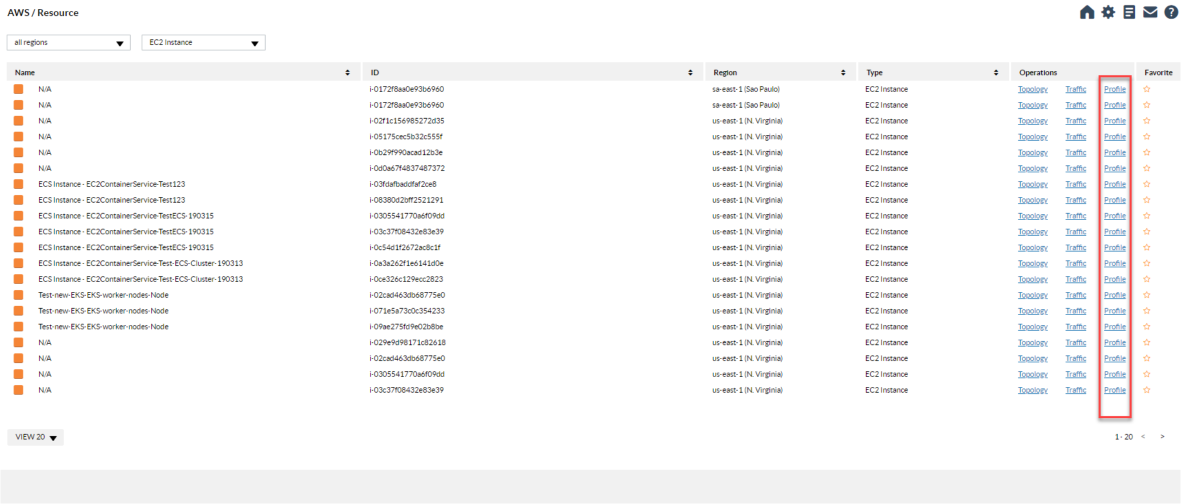


AWS / Resource

all regions ▼ all types ▼

Name	ID	Region	Type	Operations	Favorite
demo-trail	arn:aws:cloudtrail:us-east-1:483852032277:trail/demo-trail	us-east-1 (N. Virginia)	CloudTrail	Profile	☆
0079d184-65c5-40c4-8404-7760a7d22eb5	arn:aws:kms:us-east-1:483852032277:key/0079d184-65c5-4...	us-east-1 (N. Virginia)	KMS Key	Profile	☆
3e67aacc-86ec-445a-922a-59718e855888	arn:aws:kms:us-east-1:483852032277:key/3e67aacc-86ec-44...	us-east-1 (N. Virginia)	KMS Key	Profile	☆
42dcc528-4415-402d-87d0-d267b7b27f71	arn:aws:kms:us-east-1:483852032277:key/42dcc528-4415-40...	us-east-1 (N. Virginia)	KMS Key	Profile	☆
68f61be2-0d4b-46c2-bab2-bd175ec816e0	arn:aws:kms:us-east-1:483852032277:key/68f61be2-0d4b-46...	us-east-1 (N. Virginia)	KMS Key	Profile	☆
016dd1417f1bce81	arn:aws:elasticloadbalancing:us-east-2:385279133563:listener...	us-east-2 (Ohio)	Listener	Profile	☆
991cfaa0-fd55-4895-a5d6-67775f80cd69	arn:aws:kms:us-east-1:483852032277:key/991cfaa0-fd55-48...	us-east-1 (N. Virginia)	KMS Key	Profile	☆
a06b7b0a-dea6-4ef7-b81c-b0f486e6765b	arn:aws:kms:us-east-1:483852032277:key/a06b7b0a-dea6-4e...	us-east-1 (N. Virginia)	KMS Key	Profile	☆
a2de1ba3-d5eb-48aa-90ef-38785e5c0ea4	arn:aws:kms:us-east-1:483852032277:key/a2de1ba3-d5eb-48...	us-east-1 (N. Virginia)	KMS Key	Profile	☆
a7ca9374-23ba-42d8-831e-2250be9bf66f	arn:aws:kms:us-east-1:483852032277:key/a7ca9374-23ba-42...	us-east-1 (N. Virginia)	KMS Key	Profile	☆
ELB-no-outbound-rule	sg-08f880d80d1d78b32	us-east-1 (N. Virginia)	Security Group	Profile	☆
9ed2af55-2c5a-4bc1-94d6-6e422b22e3ae	arn:aws:kms:us-east-2:483852032277:key/9ed2af55-2c5a-4b...	us-east-2 (Ohio)	KMS Key	Profile	☆
default	sg-0a37cb6d83aafc0b4	us-east-1 (N. Virginia)	Security Group	Profile	☆
default	sg-0fe751667009e7f9a	us-east-1 (N. Virginia)	Security Group	Profile	☆
default	sg-56e8911d	us-east-1 (N. Virginia)	Security Group	Profile	☆
forticasb-cloudtrail-autotest	forticasb-cloudtrail-autotest	us-east-1 (N. Virginia)	S3 Bucket	Profile	☆
forticasb-cucumber-2019-03-25-qa	forticasb-cucumber-2019-03-25-qa	us-east-1 (N. Virginia)	S3 Bucket	Profile	☆
4a814220-e58c-4dfb-9b58-83392ae85c2c	arn:aws:kms:us-west-2:483852032277:key/4a814220-e58c-4...	us-west-2 (Oregon)	KMS Key	Profile	☆
forticasb-elb	forticasb-elb	us-east-1 (N. Virginia)	S3 Bucket	Profile	☆
forticasb-vpc-log	forticasb-vpc-log	us-east-1 (N. Virginia)	S3 Bucket	Profile	☆

5. Click on Profile shown under Operations column.



AWS / Resource

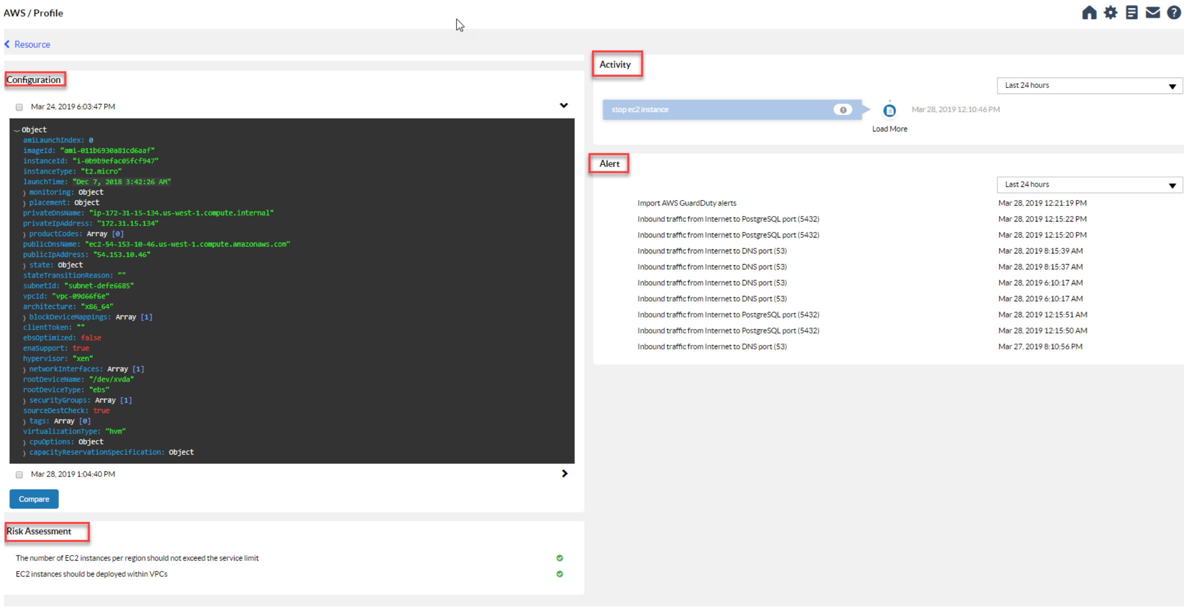
all regions ▼ EC2 Instance ▼

Name	ID	Region	Type	Operations			Favorite
N/A	i-0172f8aa0e93b6960	sa-east-1 (Sao Paulo)	EC2 Instance	Topology	Traffic	Profile	☆
N/A	i-0172f8aa0e93b6960	sa-east-1 (Sao Paulo)	EC2 Instance	Topology	Traffic	Profile	☆
N/A	i-02f1c156985272d35	us-east-1 (N. Virginia)	EC2 Instance	Topology	Traffic	Profile	☆
N/A	i-05175cec5b32c555f	us-east-1 (N. Virginia)	EC2 Instance	Topology	Traffic	Profile	☆
N/A	i-0b29f990acad12b3e	us-east-1 (N. Virginia)	EC2 Instance	Topology	Traffic	Profile	☆
N/A	i-0d0a67f4837487372	us-east-1 (N. Virginia)	EC2 Instance	Topology	Traffic	Profile	☆
ECS Instance - EC2ContainerService-Test123	i-03fdafbaddfaf2ce8	us-east-1 (N. Virginia)	EC2 Instance	Topology	Traffic	Profile	☆
ECS Instance - EC2ContainerService-Test123	i-08380d2bff2521291	us-east-1 (N. Virginia)	EC2 Instance	Topology	Traffic	Profile	☆
ECS Instance - EC2ContainerService-TestECS-190315	i-0305541770a6f09dd	us-east-1 (N. Virginia)	EC2 Instance	Topology	Traffic	Profile	☆
ECS Instance - EC2ContainerService-TestECS-190315	i-03c37f08432e83e39	us-east-1 (N. Virginia)	EC2 Instance	Topology	Traffic	Profile	☆
ECS Instance - EC2ContainerService-TestECS-190315	i-0c54d1f2672ac8c1f	us-east-1 (N. Virginia)	EC2 Instance	Topology	Traffic	Profile	☆
ECS Instance - EC2ContainerService-Test-ECS-Cluster-190313	i-0a3a262f1e6141d0e	us-east-1 (N. Virginia)	EC2 Instance	Topology	Traffic	Profile	☆
ECS Instance - EC2ContainerService-Test-ECS-Cluster-190313	i-0ce326c129ecc2823	us-east-1 (N. Virginia)	EC2 Instance	Topology	Traffic	Profile	☆
Test-new-EKS-EKS-worker-nodes-Node	i-02cad463db68775e0	us-east-1 (N. Virginia)	EC2 Instance	Topology	Traffic	Profile	☆
Test-new-EKS-EKS-worker-nodes-Node	i-071e5a73c0c354233	us-east-1 (N. Virginia)	EC2 Instance	Topology	Traffic	Profile	☆
Test-new-EKS-EKS-worker-nodes-Node	i-09ae275fd9e02b8be	us-east-1 (N. Virginia)	EC2 Instance	Topology	Traffic	Profile	☆
N/A	i-029e9d98171c82618	us-east-1 (N. Virginia)	EC2 Instance	Topology	Traffic	Profile	☆
N/A	i-02cad463db68775e0	us-east-1 (N. Virginia)	EC2 Instance	Topology	Traffic	Profile	☆
N/A	i-0305541770a6f09dd	us-east-1 (N. Virginia)	EC2 Instance	Topology	Traffic	Profile	☆
N/A	i-03c37f08432e83e39	us-east-1 (N. Virginia)	EC2 Instance	Topology	Traffic	Profile	☆

VIEW 20 ▼

1 - 20 < >

6. Profile of the virtual machine instance will be shown.



Mar 24, 2019 6:03:47 PM

```
⌄ Object
   amiLaunchIndex: 0
   imageId: "ami-011b6930a81cd6aaf"
   instanceId: "i-0b9b9efac05fcf947"
   instanceType: "t2.micro"
   launchTime: "Dec 7, 2018 3:42:26 AM"
  › monitoring: Object
  › placement: Object
   privateDnsName: "ip-172-31-15-134.us-west-1.compute.internal"
   privateIpAddress: "172.31.15.134"
  › productCodes: Array [0]
   publicDnsName: "ec2-54-153-10-46.us-west-1.compute.amazonaws.com"
   publicIpAddress: "54.153.10.46"
  › state: Object
   stateTransitionReason: ""
   subnetId: "subnet-defe6685"
   vpcId: "vpc-09d66f6e"
   architecture: "x86_64"
  › blockDeviceMappings: Array [1]
   clientToken: ""
   ebsOptimized: false
   enaSupport: true
   hypervisor: "xen"
  › networkInterfaces: Array [1]
   rootDeviceName: "/dev/xvda"
   rootDeviceType: "ebs"
  › securityGroups: Array [1]
   sourceDestCheck: true
  › tags: Array [0]
   virtualizationType: "hvm"
  › cpuOptions: Object
  › capacityReservationSpecification: Object
```

Mar 28, 2019 1:04:40 PM

The number of EC2 instances per region should not exceed the service limit ✓

EC2 instances should be deployed within VPCs ✓

stop ec2 instance — Mar 28, 2019 12:10:46 PM

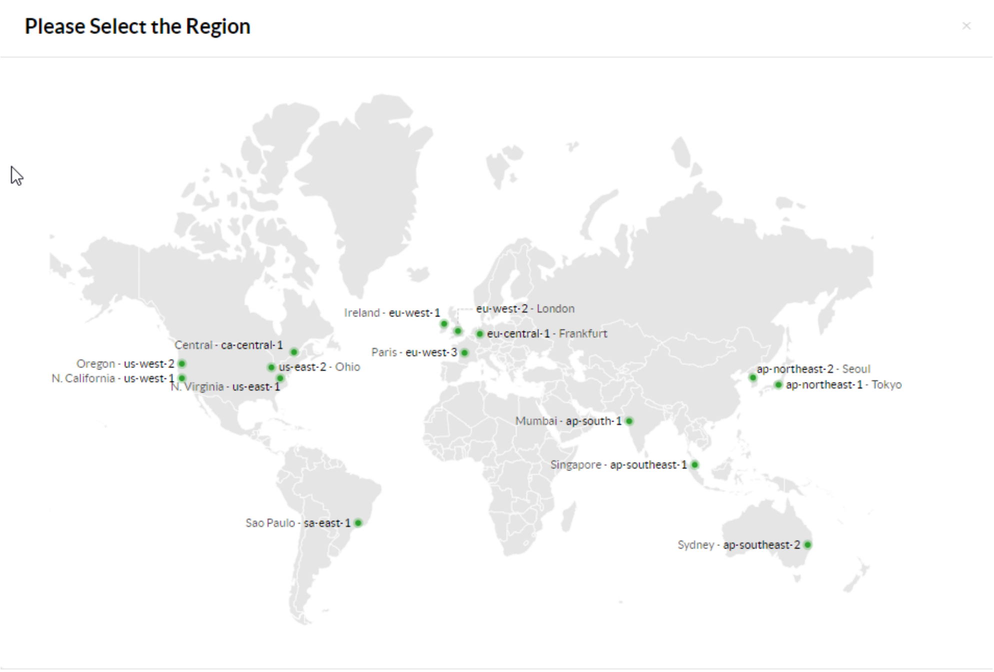
Import AWS GuardDuty alerts	Mar 28, 2019 12:21:19 PM
Inbound traffic from Internet to PostgreSQL port (5432)	Mar 28, 2019 12:15:22 PM
Inbound traffic from Internet to PostgreSQL port (5432)	Mar 28, 2019 12:15:20 PM
Inbound traffic from Internet to DNS port (53)	Mar 28, 2019 8:15:39 AM
Inbound traffic from Internet to DNS port (53)	Mar 28, 2019 8:15:37 AM
Inbound traffic from Internet to DNS port (53)	Mar 28, 2019 6:10:17 AM
Inbound traffic from Internet to DNS port (53)	Mar 28, 2019 6:10:17 AM
Inbound traffic from Internet to PostgreSQL port (5432)	Mar 28, 2019 12:15:51 AM
Inbound traffic from Internet to PostgreSQL port (5432)	Mar 28, 2019 12:15:50 AM
Inbound traffic from Internet to DNS port (53)	Mar 27, 2019 8:10:56 PM

Profile summary:

- **Configuration** - all configuration variables of the virtual machine instance.
- **Activity** - cloud audit logs performed on the virtual machine instance.
- **Risk Assessment** - summary of the policies that the virtual machine instance violated.
- **Alert** - security alerts triggered by Risk Assessment, Data Analysis, Threat Protection, Compliance, and integration.

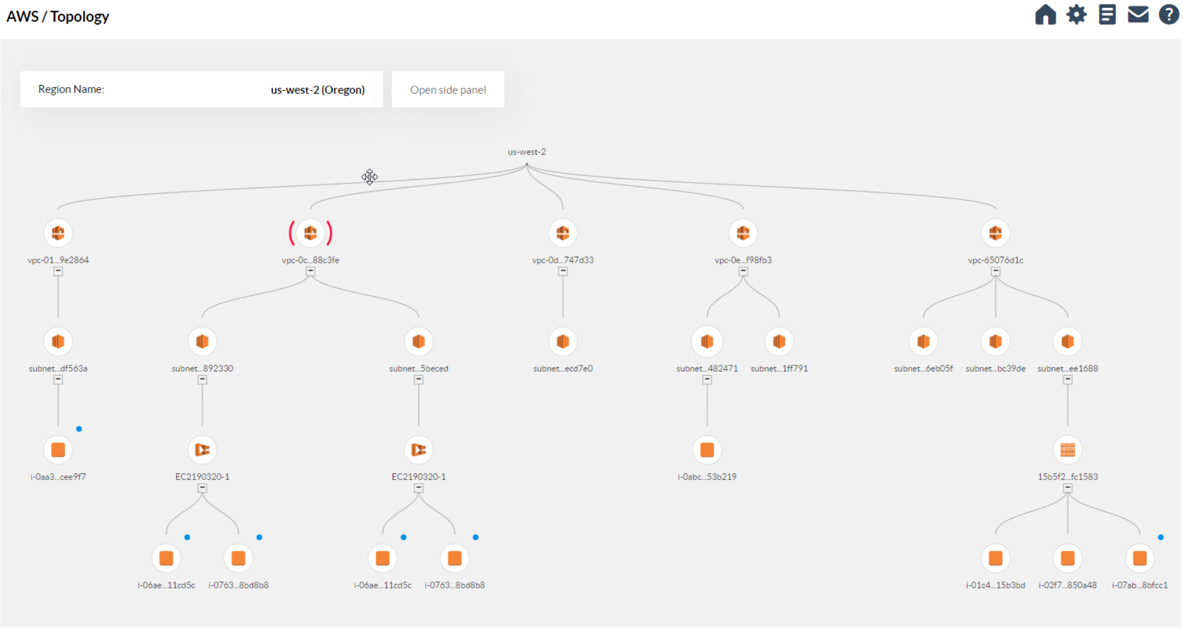
Access Profile through Topology

1. Log into FortiCASB https://www.forticasb.com/ with your FortiCASB user account.
2. From FortiCASB **Overview** dashboard, select an IAAS account on the left menu.
3. Under the IAAS account menu, click on **Topology.**
4. Click on **Region Name** on the top to select a region. For Google Cloud users, please select **Project.**



Please Select the Region

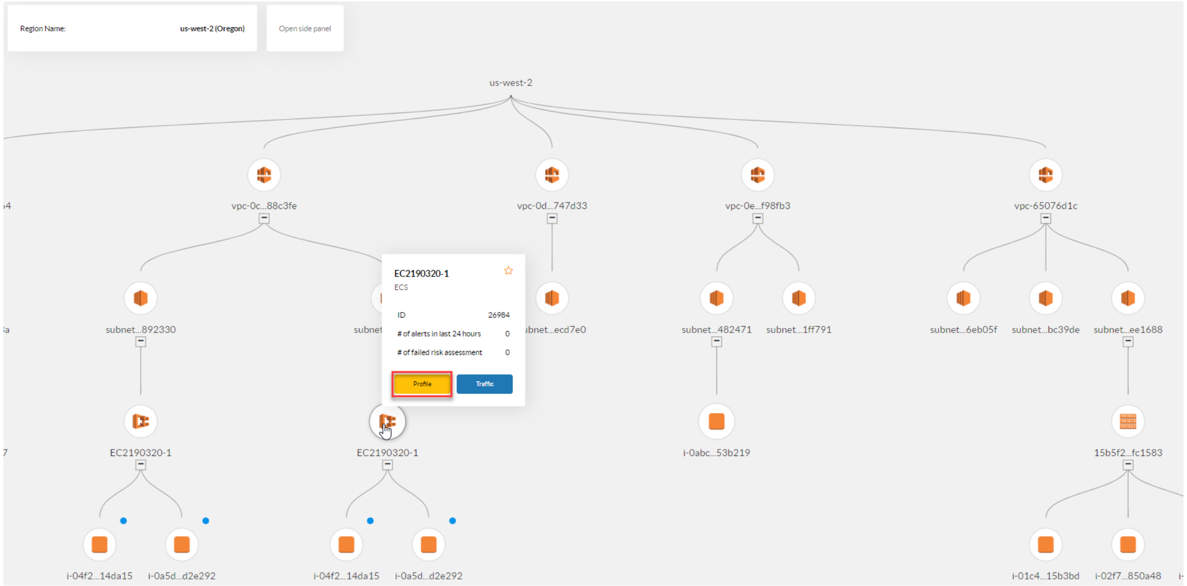
5. After selecting a region, all cloud resources under the region will be shown in one graphical view.



AWS / Topology

Region Name: us-west-2 (Oregon)

6. Move mouse to any virtual machine instance will trigger the **profile/traffic** button.

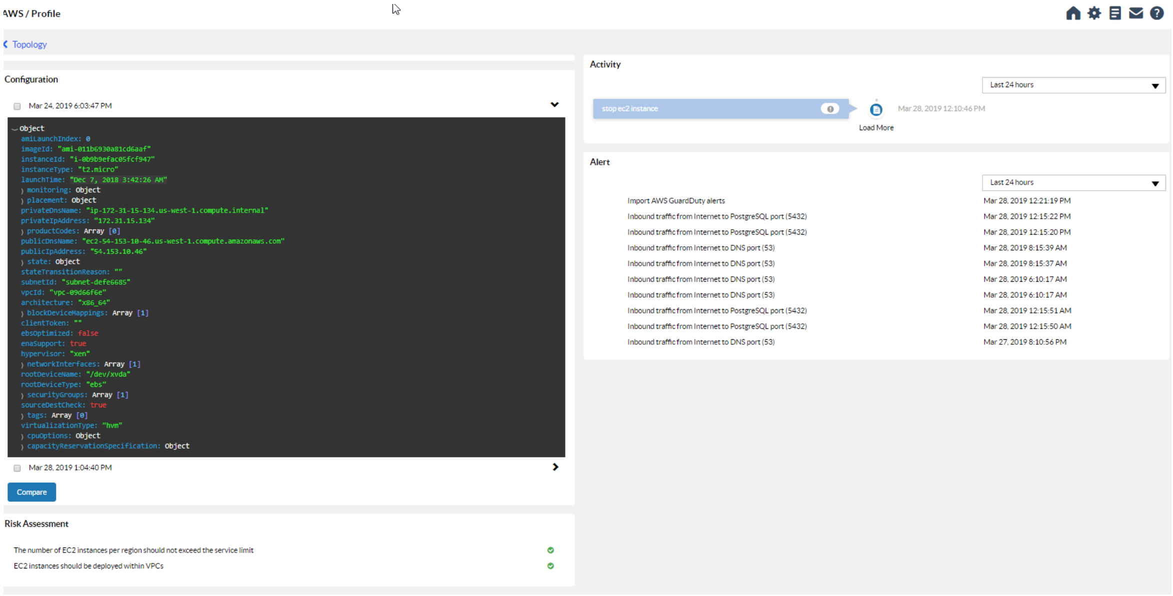


Region Name: us-west-2 (Oregon)

EC2190320-1
ECS

ID	26984
# of alerts in last 24 hours	0
# of failed risk assessment	0

7. Click on Profile will show all the profile summary related to the virtual machine instance.



Configuration

□ Mar 24, 2019 6:03:47 PM

```
⌄ Object
   amiLaunchIndex: 0
   imageId: "ami-011b6930a81cd6aaf"
   instanceId: "i-0b9b9efac05fcf947"
   instanceType: "t2.micro"
   launchTime: "Dec 7, 2018 3:42:26 AM"
  › monitoring: Object
  › placement: Object
   privateDnsName: "ip-172-31-15-134.us-west-1.compute.internal"
   privateIpAddress: "172.31.15.134"
  › productCodes: Array [0]
   publicDnsName: "ec2-54-153-10-46.us-west-1.compute.amazonaws.com"
   publicIpAddress: "54.153.10.46"
  › state: Object
   stateTransitionReason: ""
   subnetId: "subnet-defe6685"
   vpcId: "vpc-09d66f6e"
   architecture: "x86_64"
  › blockDeviceMappings: Array [1]
   clientToken: ""
   ebsOptimized: false
   enaSupport: true
   hypervisor: "xen"
  › networkInterfaces: Array [1]
   rootDeviceName: "/dev/xvda"
   rootDeviceType: "ebs"
  › securityGroups: Array [1]
   sourceDestCheck: true
  › tags: Array [0]
   virtualizationType: "hvm"
  › cpuOptions: Object
  › capacityReservationSpecification: Object
```

□ Mar 28, 2019 1:04:40 PM

Risk Assessment

The number of EC2 instances per region should not exceed the service limit	✓
EC2 instances should be deployed within VPCs	✓

Activity

Last 24 hours

stop ec2 instance — Mar 28, 2019 12:10:46 PM

Alert

Last 24 hours

Import AWS GuardDuty alerts	Mar 28, 2019 12:21:19 PM
Inbound traffic from Internet to PostgreSQL port (5432)	Mar 28, 2019 12:15:22 PM
Inbound traffic from Internet to PostgreSQL port (5432)	Mar 28, 2019 12:15:20 PM
Inbound traffic from Internet to DNS port (53)	Mar 28, 2019 8:15:39 AM
Inbound traffic from Internet to DNS port (53)	Mar 28, 2019 8:15:37 AM
Inbound traffic from Internet to DNS port (53)	Mar 28, 2019 6:10:17 AM
Inbound traffic from Internet to DNS port (53)	Mar 28, 2019 6:10:17 AM
Inbound traffic from Internet to PostgreSQL port (5432)	Mar 28, 2019 12:15:51 AM
Inbound traffic from Internet to PostgreSQL port (5432)	Mar 28, 2019 12:15:50 AM
Inbound traffic from Internet to DNS port (53)	Mar 27, 2019 8:10:56 PM

Risk Assessment

FortiCASB features risk assessment for IaaS which check to see if your organization's IaaS cloud platform follows the recommended best practices.(Take AWS as example in the below)

Predefined

To view AWS predefined policy Scan Report:

1. Go to Amazon **AWS > Risk Assessment**, select Predefined tab
2. All resources in your AWS account is grouped by service and resource types. You can filter the results based on services and regions by selecting target service and region from the dropdown menu on the top right.
3. Click the arrow to the left of a resource to view the pass and failed policies.

Customized

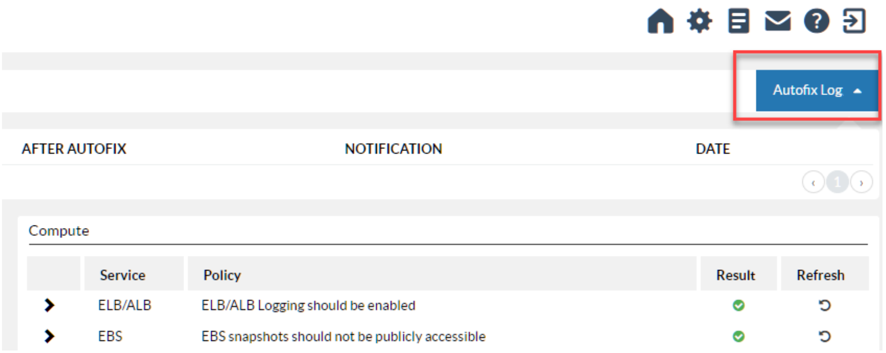
To view AWS customized policy Scan Report:

1. Go to Amazon **AWS > Risk Assessment**, select Customized tab
2. Click on **All Policies** to select customized policy.

Autofix (Only available in AWS)

If the Autofix feature is enabled, FortiCASB will automatically try to fix any policies that fail. For example, if Autofix is allowed for the "CloudTrail shouldn't stop logging" policy, FortiCASB will automatically try to turn on CloudTrail logging.

Autofix scans policies at regular intervals. open the Autofix Log on the configuration detail page to see Autofix results.



AFTER AUTOFIX	NOTIFICATION	DATE

Compute

	Service	Policy	Result	Refresh
›	ELB/ALB	ELB/ALB Logging should be enabled	✓	↻
›	EBS	EBS snapshots should not be publicly accessible	✓	↻

To enable Autofix:

1. Go to **Amazon AWS > Risk Assessment**from the navigation menu on the left.

2. Click the arrow to the left of a policy to view details of the policy.

3. Click **ALLOW AUTO FIX.**

Topology

FortiCASB gives a top down graphical view of the entire virtual private cloud resources based on region.

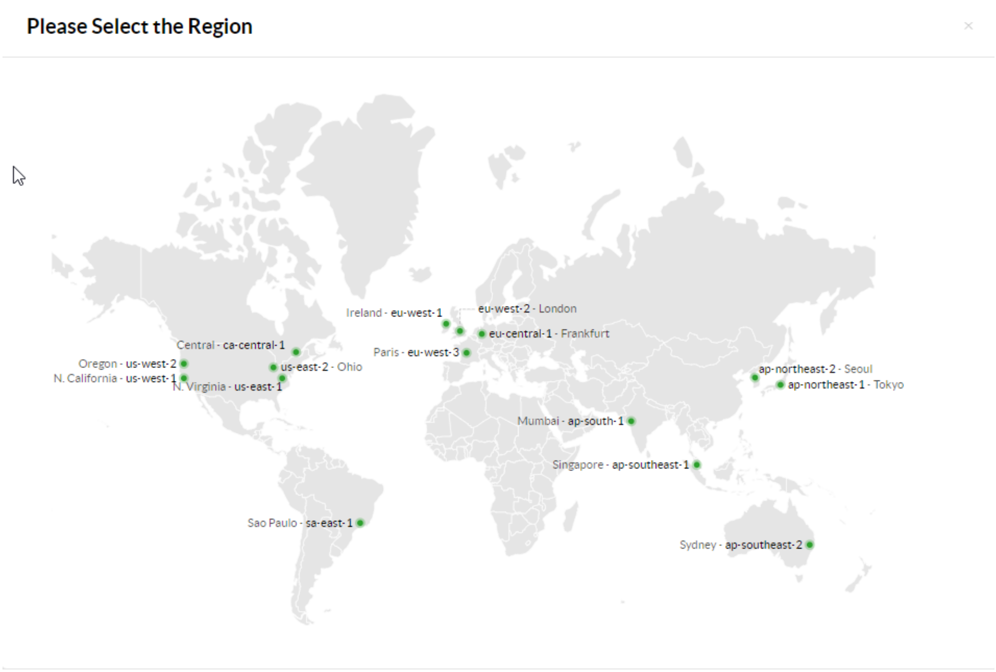
Prerequisites

An active IAAS account installed on FortiCASB is required to use Topology.

For installing IAAS account on FortiCASB, please refer to Getting Started > Installing IAAS applications on page 33

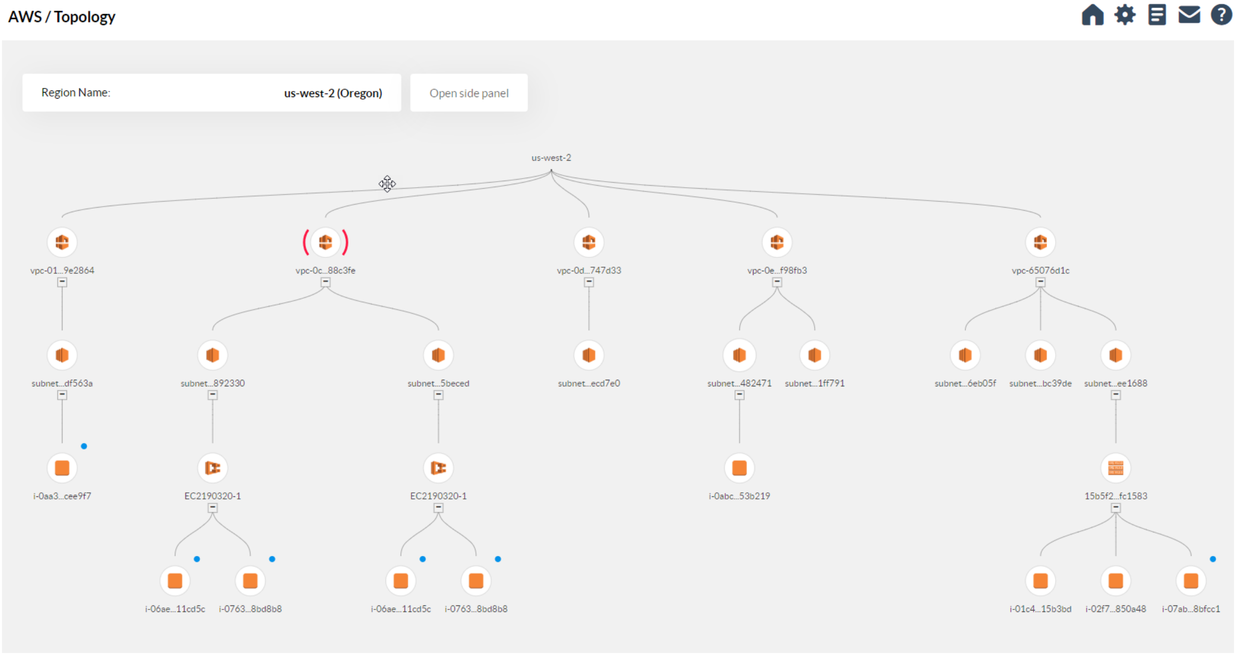
Access Topology from IAAS account

1. Log into FortiCASB https://www.forticasb.com/ with your FortiCASB user account.
2. From FortiCASB **Overview** dashboard, select an IAAS account on the left menu.
3. Under the IAAS account menu, click on **Topology**
4. Click on **Region Name** on the top to select a region. For Google Cloud users, please select **Project.**



Please Select the Region

5. After selecting a region, all cloud resources under the region will be shown in one graphical view.



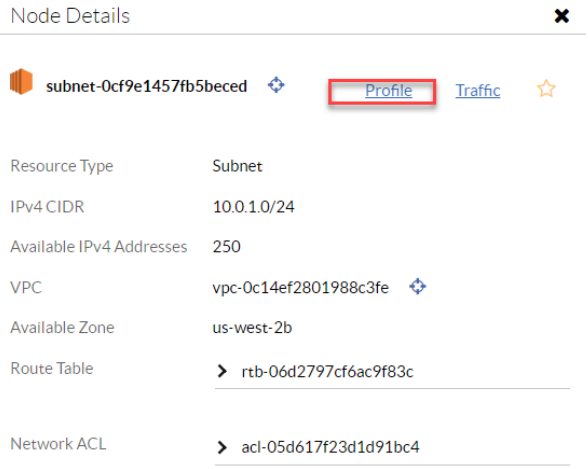
AWS / Topology

Region Name: us-west-2 (Oregon)

All virtual networks under the region as well as all the subnets virtual machine instances are shown in one graphical view.

Access Node Details, Profile, and Traffic

1. In **Toplogy**, click on any of the node on the topology map will show node details on the resource type, IP, virtual network, and the region the node belongs to.
2. In Node Details, click on **Profile**.

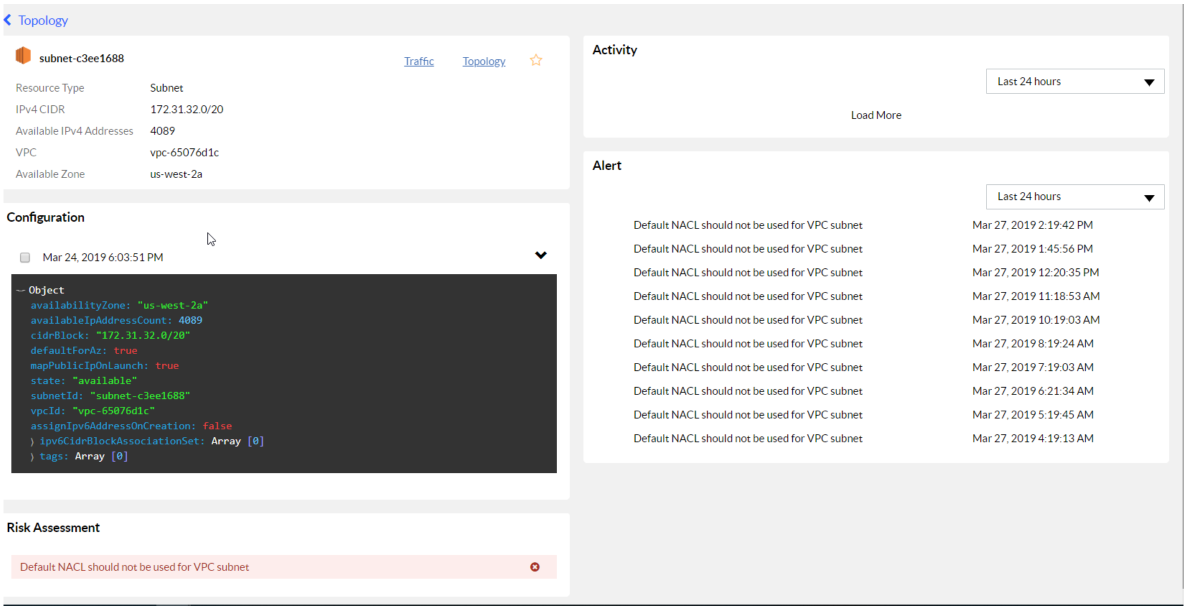


Node Details ✖

subnet-0cf9e1457fb5beced Profile Traffic ☆

Resource Type	Subnet
IPv4 CIDR	10.0.1.0/24
Available IPv4 Addresses	250
VPC	vpc-0c14ef2801988c3fe
Available Zone	us-west-2b
Route Table	› rtb-06d2797cf6ac9f83c
Network ACL	› acl-05d617f23d1d91bc4

3. **Profile** shows a in depth summary, including **Alert, Activity, Configuration, and Risk Assesement.**



‹ Topology

subnet-c3ee1688 Traffic Topology ☆

Resource Type	Subnet
IPv4 CIDR	172.31.32.0/20
Available IPv4 Addresses	4089
VPC	vpc-65076d1c
Available Zone	us-west-2a

Configuration

□ Mar 24, 2019 6:03:51 PM

```
~ Object
  availabilityZone: "us-west-2a"
  availableIpAddressCount: 4089
  cidrBlock: "172.31.32.0/20"
  defaultForAz: true
  mapPublicIpOnLaunch: true
  state: "available"
  subnetId: "subnet-c3ee1688"
  vpcId: "vpc-65076d1c"
  assignIpv6AddressOnCreation: false
  › ipv6CidrBlockAssociationSet: Array [0]
  › tags: Array [0]
```

Risk Assessment

Default NACL should not be used for VPC subnet

Activity

Last 24 hours

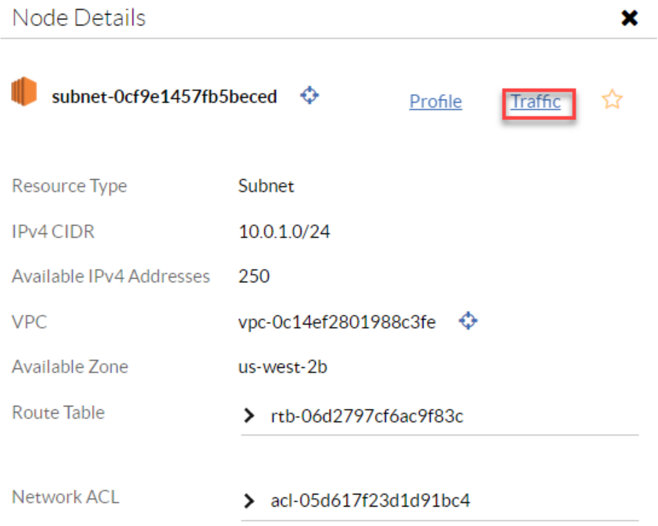
Load More

Alert

Last 24 hours

Default NACL should not be used for VPC subnet	Mar 27, 2019 2:19:42 PM
Default NACL should not be used for VPC subnet	Mar 27, 2019 1:45:56 PM
Default NACL should not be used for VPC subnet	Mar 27, 2019 12:20:35 PM
Default NACL should not be used for VPC subnet	Mar 27, 2019 11:18:53 AM
Default NACL should not be used for VPC subnet	Mar 27, 2019 10:19:03 AM
Default NACL should not be used for VPC subnet	Mar 27, 2019 8:19:24 AM
Default NACL should not be used for VPC subnet	Mar 27, 2019 7:19:03 AM
Default NACL should not be used for VPC subnet	Mar 27, 2019 6:21:34 AM
Default NACL should not be used for VPC subnet	Mar 27, 2019 5:19:45 AM
Default NACL should not be used for VPC subnet	Mar 27, 2019 4:19:13 AM

4. Click on **Traffic** in **Node Details**



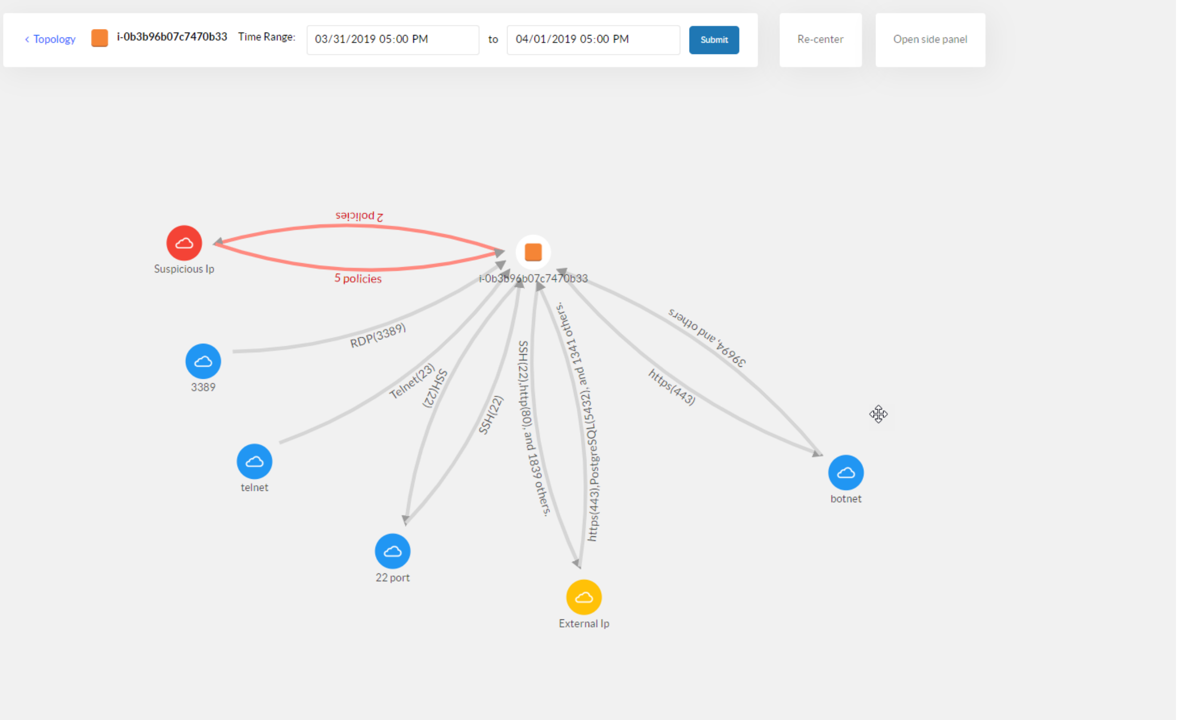
Node Details

subnet-0cf9e1457fb5beced

Resource Type	Subnet
IPv4 CIDR	10.0.1.0/24
Available IPv4 Addresses	250
VPC	vpc-0c14ef2801988c3fe
Available Zone	us-west-2b
Route Table	rtb-06d2797cf6ac9f83c
Network ACL	acl-05d617f23d1d91bc4

5. **Traffic** will show inbound and outbound traffic data of the specific virtual machine instance.

AWS / DashboardDetails / Traffic



‹ Topology i-0b3b96b07c7470b33 Time Range: 03/31/2019 05:00 PM to 04/01/2019 05:00 PM

Traffic

FortiCASB Traffic is an intuitive graphical interface allowing you to interact with all types of sources accessing the cloud resource thus giving an overall diagnostic of the cloud instance health.

Prerequisites

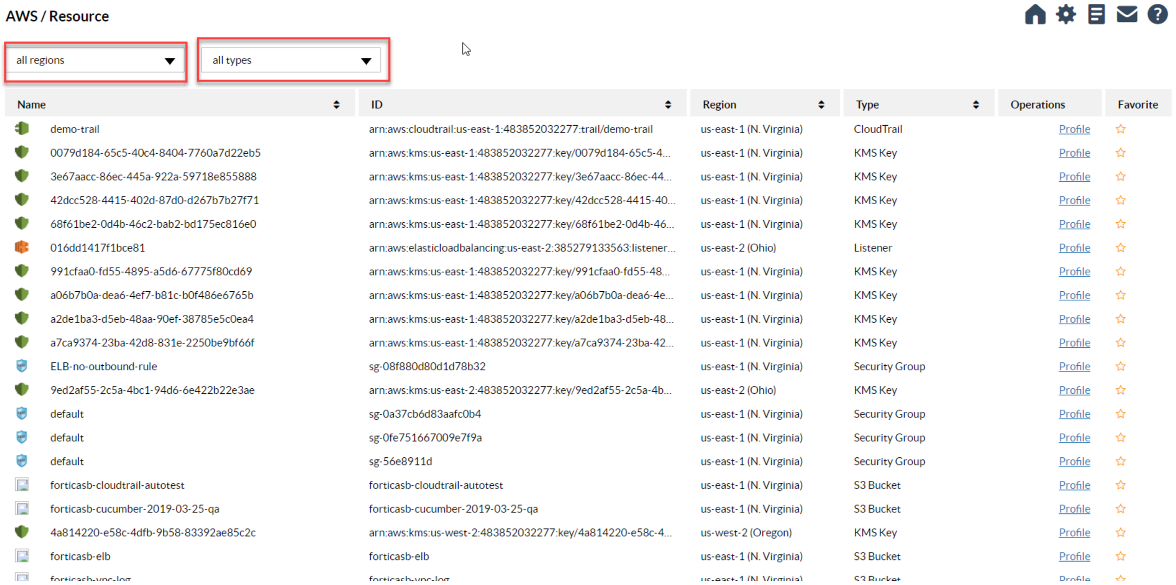
An active IAAS account installed on FortiCASB with traffic log enabled for the IAAS account.

For installing IAAS account on FortiCASB, please refer to Getting Started > Installing IAAS applications on page 33

For enabling traffic log, please refer to IAAS Features > IAAS Traffic Log > Traffic Log Configuration on page 114

Access traffic through Resource

1. Log into FortiCASB https://www.forticasb.com/ with your FortiCASB user account.
2. From FortiCASB **Overview** dashboard, select an IAAS account on the left menu.
3. Under the IAAS account menu, click on **Resource**
4. Select a **region** from the top left menu and a **type** of cloud instance on the top right menu.



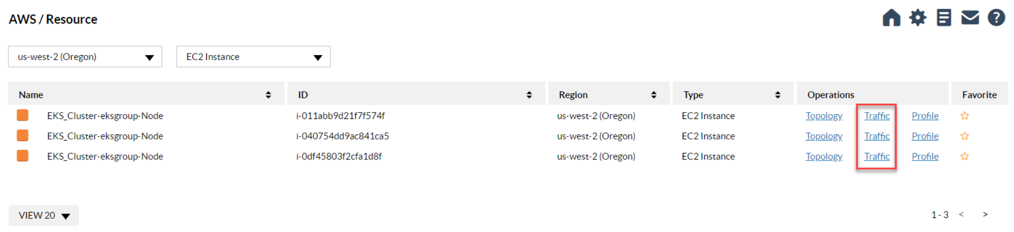
AWS / Resource

all regions

all types

Name	ID	Region	Type	Operations	Favorite
demo-trail	arn:aws:cloudtrail:us-east-1:483852032277:trail/demo-trail	us-east-1 (N. Virginia)	CloudTrail	Profile	☆
0079d184-65c5-40c4-8404-7760a7d22eb5	arn:aws:kms:us-east-1:483852032277:key/0079d184-65c5-4...	us-east-1 (N. Virginia)	KMS Key	Profile	☆
3e67aacc-86ec-445a-922a-59718e855888	arn:aws:kms:us-east-1:483852032277:key/3e67aacc-86ec-44...	us-east-1 (N. Virginia)	KMS Key	Profile	☆
42dcc528-4415-402d-87d0-d267b7b27f71	arn:aws:kms:us-east-1:483852032277:key/42dcc528-4415-40...	us-east-1 (N. Virginia)	KMS Key	Profile	☆
68f61be2-0d4b-46c2-bab2-bd175ec816e0	arn:aws:kms:us-east-1:483852032277:key/68f61be2-0d4b-46...	us-east-1 (N. Virginia)	KMS Key	Profile	☆
016dd1417f1bce81	arn:aws:elasticloadbalancing:us-east-2:385279133563:listener...	us-east-2 (Ohio)	Listener	Profile	☆
991cfaa0-fd55-4895-a5d6-67775f80cd69	arn:aws:kms:us-east-1:483852032277:key/991cfaa0-fd55-48...	us-east-1 (N. Virginia)	KMS Key	Profile	☆
a06b7b0a-dea6-4ef7-b81c-b0f486e6765b	arn:aws:kms:us-east-1:483852032277:key/a06b7b0a-dea6-4e...	us-east-1 (N. Virginia)	KMS Key	Profile	☆
a2de1ba3-d5eb-48aa-90ef-38785e5c0ea4	arn:aws:kms:us-east-1:483852032277:key/a2de1ba3-d5eb-48...	us-east-1 (N. Virginia)	KMS Key	Profile	☆
a7ca9374-23ba-42d8-831e-2250be9bf66f	arn:aws:kms:us-east-1:483852032277:key/a7ca9374-23ba-42...	us-east-1 (N. Virginia)	KMS Key	Profile	☆
ELB-no-outbound-rule	sg-08f880d80d1d78b32	us-east-1 (N. Virginia)	Security Group	Profile	☆
9ed2af55-2c5a-4bc1-94d6-6e422b22e3ae	arn:aws:kms:us-east-2:483852032277:key/9ed2af55-2c5a-4b...	us-east-2 (Ohio)	KMS Key	Profile	☆
default	sg-0a37cb6d83aafc0b4	us-east-1 (N. Virginia)	Security Group	Profile	☆
default	sg-0fe751667009e7f9a	us-east-1 (N. Virginia)	Security Group	Profile	☆
default	sg-56e8911d	us-east-1 (N. Virginia)	Security Group	Profile	☆
forticasb-cloudtrail-autotest	forticasb-cloudtrail-autotest	us-east-1 (N. Virginia)	S3 Bucket	Profile	☆
forticasb-cucumber-2019-03-25-qa	forticasb-cucumber-2019-03-25-qa	us-east-1 (N. Virginia)	S3 Bucket	Profile	☆
4a814220-e58c-4dfb-9b58-83392ae85c2c	arn:aws:kms:us-west-2:483852032277:key/4a814220-e58c-4...	us-west-2 (Oregon)	KMS Key	Profile	☆
forticasb-elb	forticasb-elb	us-east-1 (N. Virginia)	S3 Bucket	Profile	☆
forticasb-vpc-log	forticasb-vpc-log	us-east-1 (N. Virginia)	S3 Bucket	Profile	☆

5. Click on **Traffic** shown under Operations column of any of the cloud instance.



AWS / Resource

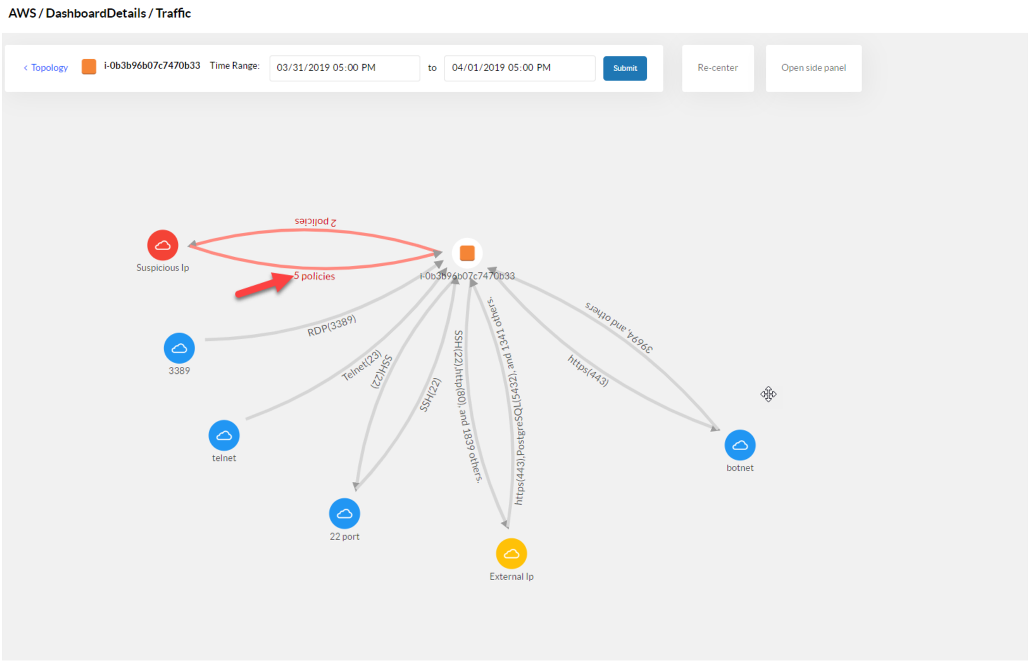
us-west-2 (Oregon) ▼ EC2 Instance ▼

Name	ID	Region	Type	Operations			Favorite
EKS_Cluster-eksgroup-Node	i-011abb9d21f7f574f	us-west-2 (Oregon)	EC2 Instance	Topology	Traffic	Profile	☆
EKS_Cluster-eksgroup-Node	i-040754dd9ac841ca5	us-west-2 (Oregon)	EC2 Instance	Topology	Traffic	Profile	☆
EKS_Cluster-eksgroup-Node	i-0df45803f2cfa1d8f	us-west-2 (Oregon)	EC2 Instance	Topology	Traffic	Profile	☆

VIEW 20 ▼ 1 - 3 < >

6. An Interactive cloud data traffic map will be shown with inbound and outbound traffic of all sources accessing the virtual machine.
7. Clicking on the description on the inbound or outbound traffic will show detail of the source that is accessing the virtual machine.,

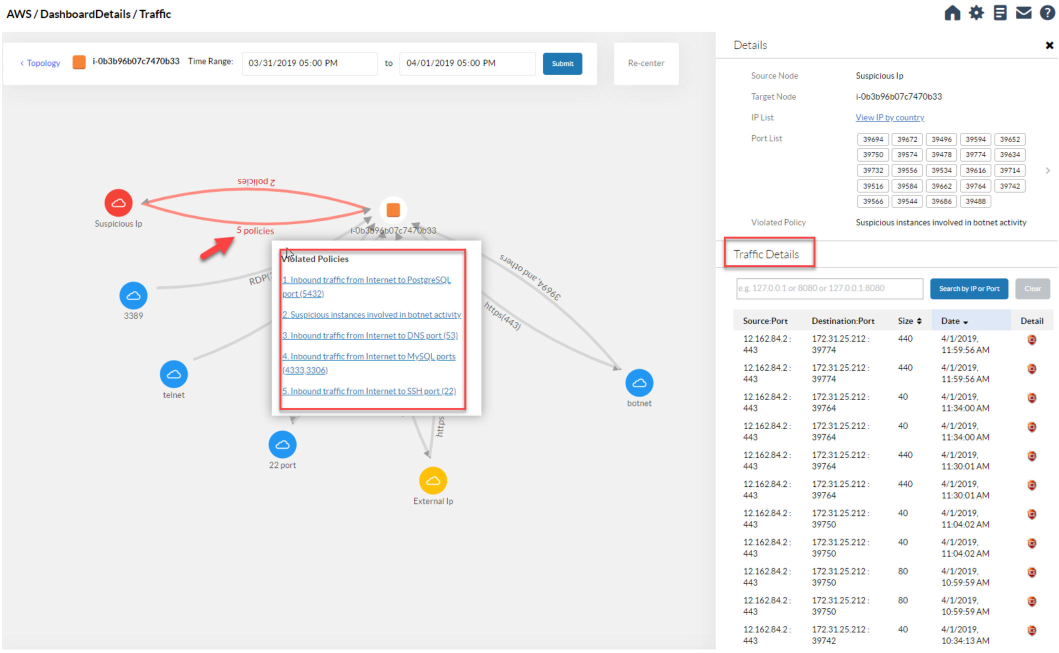
For example, clicking on the traffic coming from a suspicious IP will give a list of **Violated Policies**.



AWS / DashboardDetails / Traffic

< Topology i-0b3b96b07c7470b33 Time Range: 03/31/2019 05:00 PM to 04/01/2019 05:00 PM Submit Re-center Open side panel

Select one of the violated policies will show **Traffic Details** of the brute force attack on the virtual machine. In this way, the cloud administrator can take remediation quickly against the intrusion.



Time Range: 03/31/2019 05:00 PM to 04/01/2019 05:00 PM

Violated Policies

1. Inbound traffic from Internet to PostgreSQL port (5432)
2. Suspicious instances involved in botnet activity
3. Inbound traffic from Internet to DNS port (53)
4. Inbound traffic from Internet to MySQL ports (4333,3306)
5. Inbound traffic from Internet to SSH port (22)

Source Node	Suspicious Ip
Target Node	i-0b3b96b07c7470b33
IP List	View IP by country

Port List	39694 39672 39496 39594 39652
	39750 39574 39478 39774 39634
	39732 39556 39534 39616 39714
	39516 39584 39662 39764 39742
	39566 39544 39686 39488

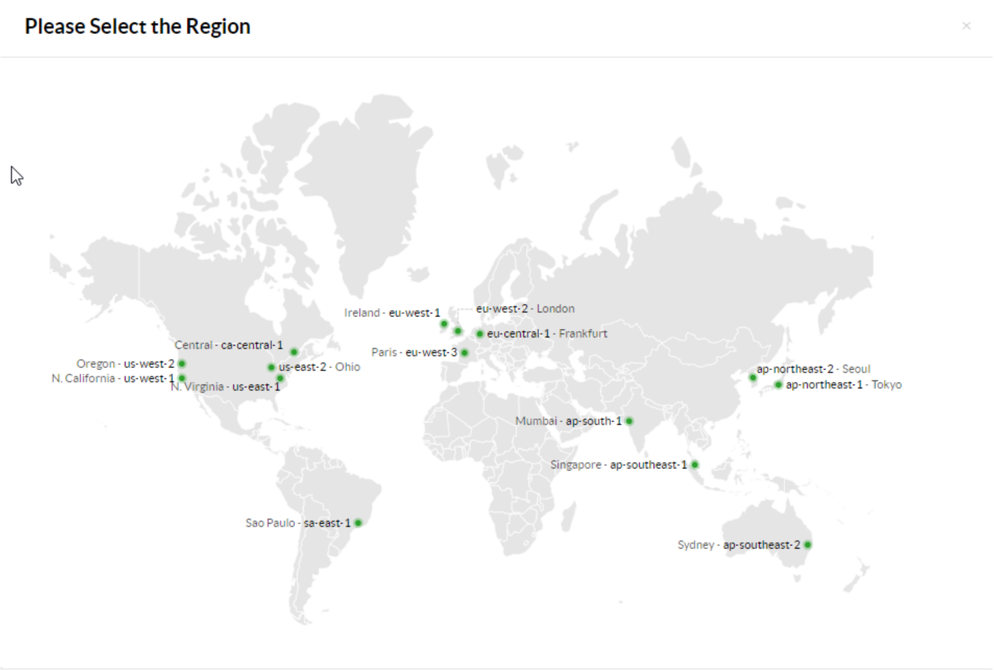
Violated Policy	Suspicious instances involved in botnet activity

e.g. 127.0.0.1 or 8080 or 127.0.0.1:8080

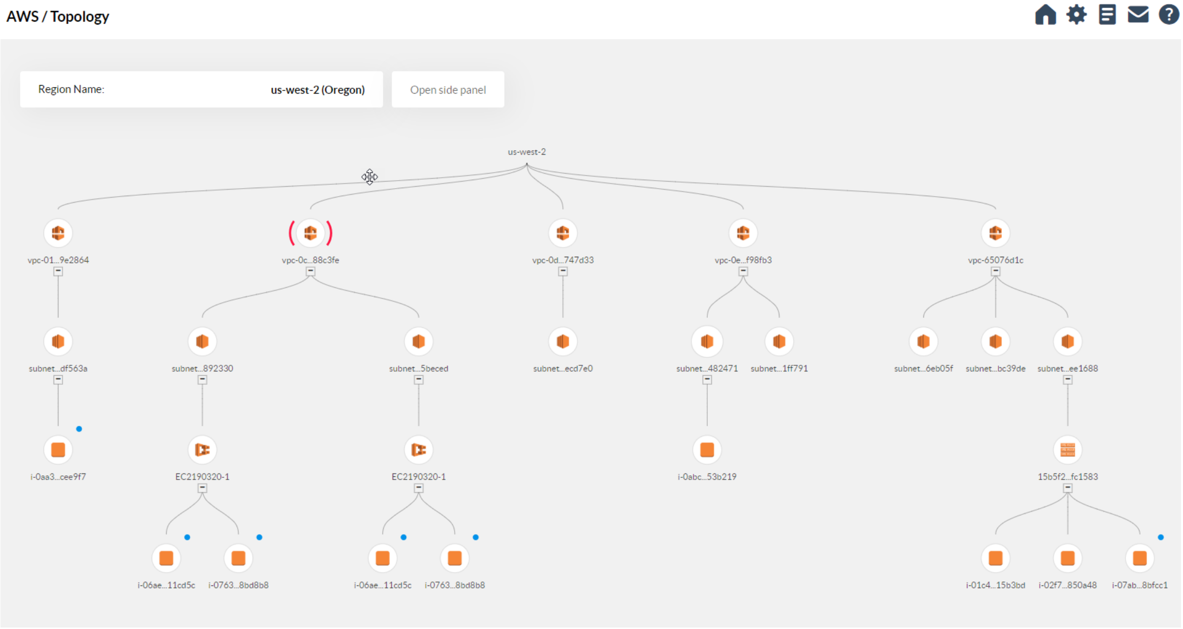
Source:Port	Destination:Port	Size	Date	Detail
12.162.84.2 : 443	172.31.25.212 : 39774	440	4/1/2019, 11:59:56 AM	
12.162.84.2 : 443	172.31.25.212 : 39774	440	4/1/2019, 11:59:56 AM	
12.162.84.2 : 443	172.31.25.212 : 39764	40	4/1/2019, 11:34:00 AM	
12.162.84.2 : 443	172.31.25.212 : 39764	40	4/1/2019, 11:34:00 AM	
12.162.84.2 : 443	172.31.25.212 : 39764	440	4/1/2019, 11:30:01 AM	
12.162.84.2 : 443	172.31.25.212 : 39764	440	4/1/2019, 11:30:01 AM	
12.162.84.2 : 443	172.31.25.212 : 39750	40	4/1/2019, 11:04:02 AM	
12.162.84.2 : 443	172.31.25.212 : 39750	40	4/1/2019, 11:04:02 AM	
12.162.84.2 : 443	172.31.25.212 : 39750	80	4/1/2019, 10:59:59 AM	
12.162.84.2 : 443	172.31.25.212 : 39750	80	4/1/2019, 10:59:59 AM	
12.162.84.2 : 443	172.31.25.212 : 39742	40	4/1/2019, 10:34:13 AM	

Access traffic through Topology

1. Log into FortiCASB https://www.forticasb.com/ with your FortiCASB user account.
2. From FortiCASB **Overview** dashboard, select an IAAS account on the left menu.
3. Under the IAAS account menu, click on **Topology**
4. Click on **Region Name** on the top to select a region. For Google Cloud users, please select **Project.**

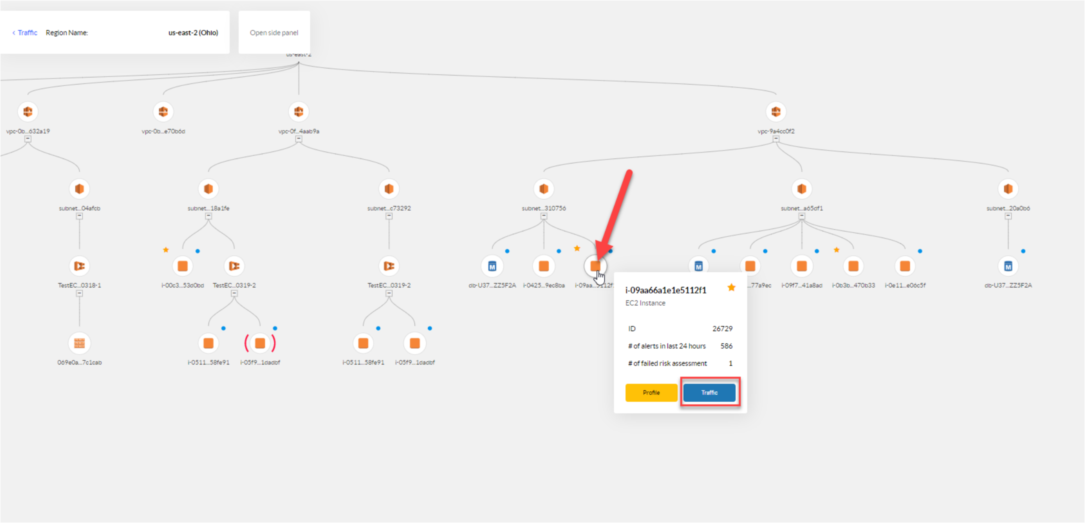


5. After selecting a region, all cloud resources under the region will be shown in one graphical view.


AWS / Topology

Region Name: us-west-2 (Oregon)

6. Move mouse to any virtual machine instance will trigger the **profile/traffic** button.


‹ Traffic Region Name: us-east-2 (Ohio)

Open side panel

i-09aa66a1e1e5112f1

EC2 Instance

ID 26729

# of alerts in last 24 hours 586

# of failed risk assessment 1

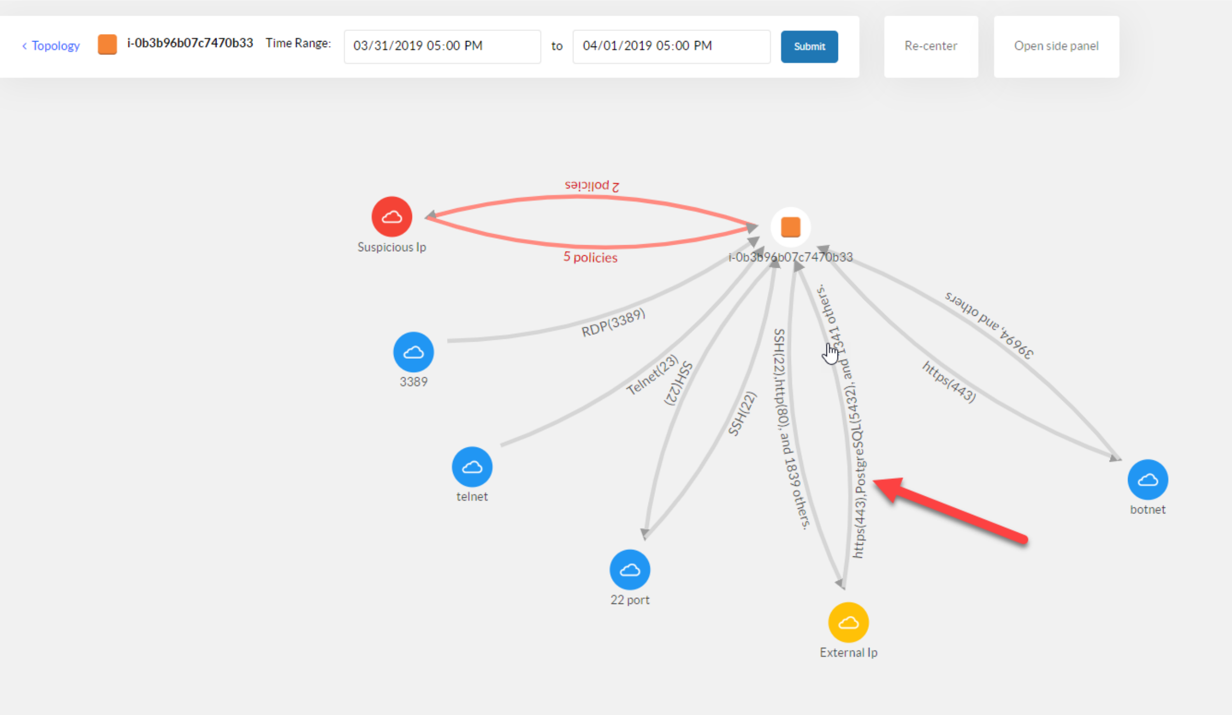
Profile

Traffic

7. Click on **Traffic**, an Interactive cloud data traffic map will be shown with inbound and outbound traffic of all sources accessing the virtual machine.
8. Clicking on the description on the inbound or outbound traffic will show detail of the source that is accessing the virtual machine.,

For example, clicking on the traffic coming from an external IP will give a detail history of accesses from the external IP.

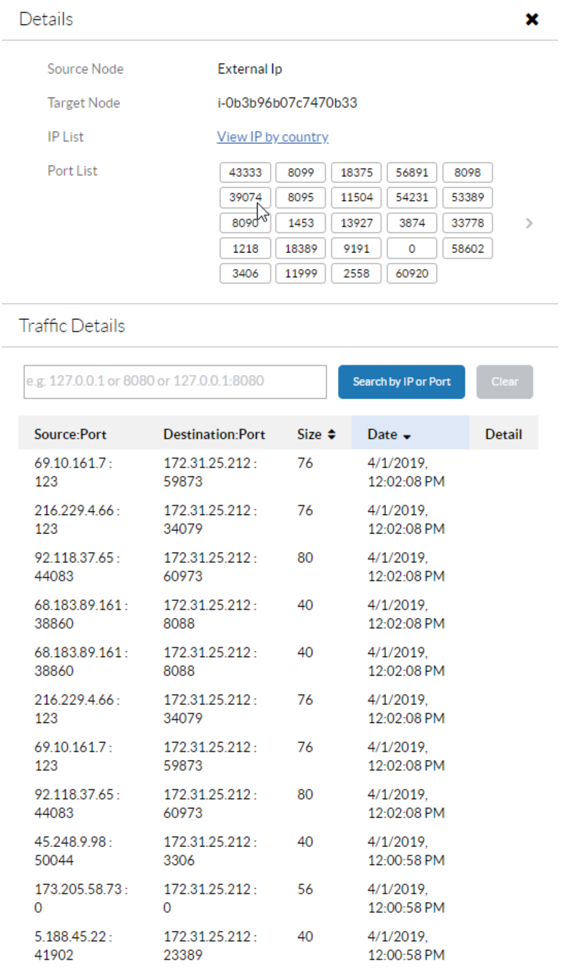
AWS / DashboardDetails / Traffic


‹ Topology i-0b3b96b07c7470b33 Time Range: 03/31/2019 05:00 PM to 04/01/2019 05:00 PM Submit

Re-center

Open side panel

Traffic Details of the external IP shows history of all the sources and destinations IPs as well as the date/time of the initiated call attempt.



Source Node External Ip

Target Node i-0b3b96b07c7470b33

IP List View IP by country

Port List

43333	8099	18375	56891	8098
39074	8095	11504	54231	53389
8090	1453	13927	3874	33778
1218	18389	9191	0	58602
3406	11999	2558	60920	

Traffic Details

e.g. 127.0.0.1 or 8080 or 127.0.0.1:8080

Source:Port	Destination:Port	Size ⇕	Date ▾	Detail
69.10.161.7 : 123	172.31.25.212 : 59873	76	4/1/2019, 12:02:08 PM	
216.229.4.66 : 123	172.31.25.212 : 34079	76	4/1/2019, 12:02:08 PM	
92.118.37.65 : 44083	172.31.25.212 : 60973	80	4/1/2019, 12:02:08 PM	
68.183.89.161 : 38860	172.31.25.212 : 8088	40	4/1/2019, 12:02:08 PM	
68.183.89.161 : 38860	172.31.25.212 : 8088	40	4/1/2019, 12:02:08 PM	
216.229.4.66 : 123	172.31.25.212 : 34079	76	4/1/2019, 12:02:08 PM	
69.10.161.7 : 123	172.31.25.212 : 59873	76	4/1/2019, 12:02:08 PM	
92.118.37.65 : 44083	172.31.25.212 : 60973	80	4/1/2019, 12:02:08 PM	
45.248.9.98 : 50044	172.31.25.212 : 3306	40	4/1/2019, 12:00:58 PM	
173.205.58.73 : 0	172.31.25.212 : 0	56	4/1/2019, 12:00:58 PM	
5.188.45.22 : 41902	172.31.25.212 : 23389	40	4/1/2019, 12:00:58 PM	

Troubleshooting

Information and solutions for the following problems are included in this section:

Getting Started

- I have a new account but no license
- I have renewed my license, but cannot use it.

Salesforce

- I get an "OAuth Request" error.

Office 365

- I get an error at the "Add Sites Collection Admin" step.
- I get an error at the "Add Users" step.
- I get an error at the "Add Groups" step.

Dropbox Business

- I get an "OAuth Request" error.

Google

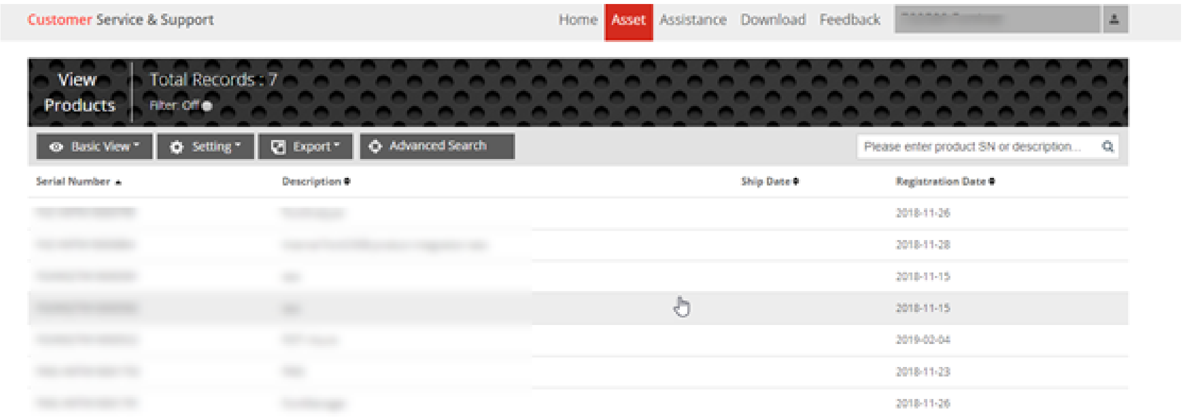
- I can't connect Google Drive to FortiCASB.

Getting Started

New account with No License Error

Please check on your Master FortiCARE account to see if the license is present with these steps:

1. Log into FortiCare https://support.fortinet.com/ with your Master FortiCare account.
2. From the top main menu click on **Asset > Manage/View Products**.
3. Check and see if the licenses you purchased is shown in the product list.



[redacted]

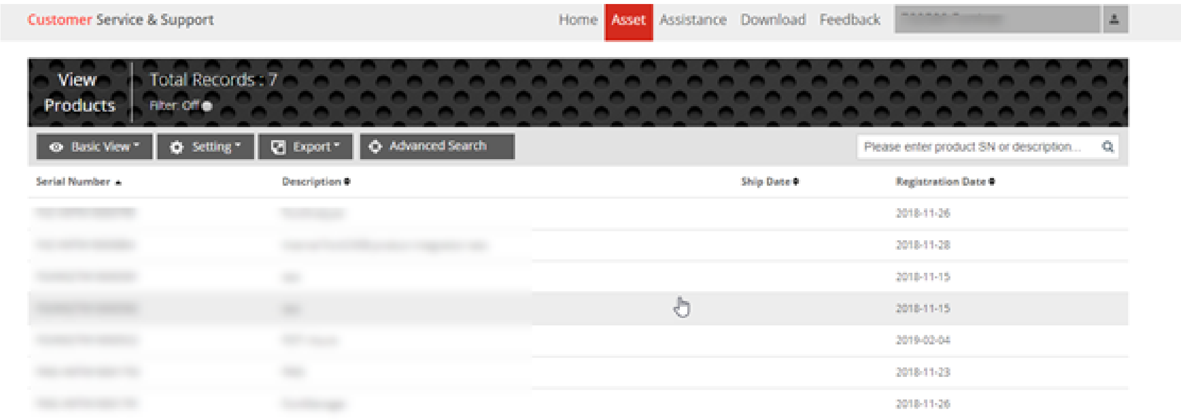
Serial Number	Description	Ship Date	Registration Date
[redacted]	[redacted]		2018-11-26
[redacted]	[redacted]		2018-11-28
[redacted]	[redacted]		2018-11-15
[redacted]	[redacted]		2018-11-15
[redacted]	[redacted]		2019-02-04
[redacted]	[redacted]		2018-11-23
[redacted]	[redacted]		2018-11-26

4. If you find your license on the list, then you can add the license through creating a company. Please see Add companies on page 12.
5. If you do not see the license you purchased is on the list, please contact FortiCARE support.

Renew License error

When you have renewed your license but cannot find it on your FortiCASB Dashboard, follow these steps to see if the license appears in your FortiCARE account.

1. Log into FortiCare https://support.fortinet.com/ with your Master FortiCare account.
2. From the top main menu click on **Asset > Manage/View Products**.
3. Check and see if the license/contract you purchased is shown in the product list.

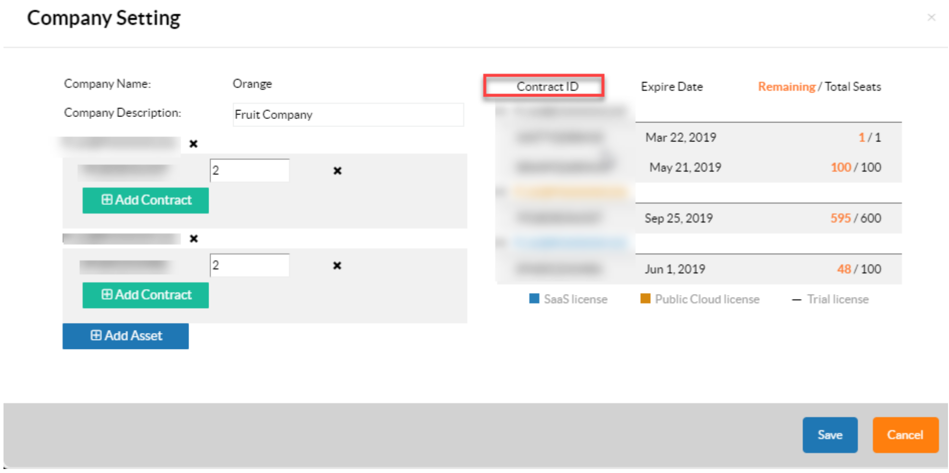


Serial Number	Description	Ship Date	Registration Date
[redacted]	[redacted]		2018-11-26
[redacted]	[redacted]		2018-11-28
[redacted]	[redacted]		2018-11-15
[redacted]	[redacted]		2018-11-15
[redacted]	[redacted]		2019-02-04
[redacted]	[redacted]		2018-11-23
[redacted]	[redacted]		2018-11-26

4. If you do not see the license/contract you purchased is on the list, please contact FortiCARE support.
5. If your license is on the list, then it only need to be assigned to the company/business unit on FortiCASB.

Assign renew license on company/business unit

1. Log into FortiCASB https://www.forticasb.com with your Master FortiCARE account.
2. Select the company which you want the renewed license/contract to go with.
3. Click on edit button next to the company.
4. In the **Company Setting**, locate the **license/contract ID** that you renewed.

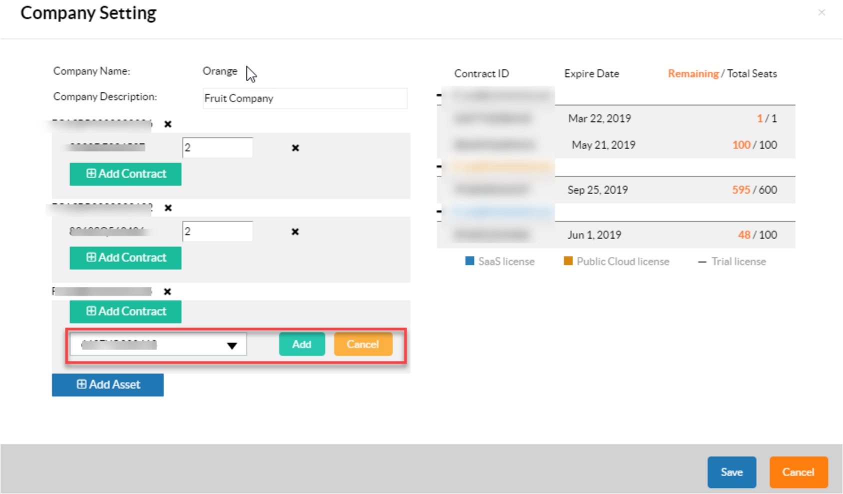


Company Name: Orange

Company Description: Fruit Company

Contract ID	Expire Date	Remaining / Total Seats
[redacted]	Mar 22, 2019	1 / 1
[redacted]	May 21, 2019	100 / 100
[redacted]	Sep 25, 2019	595 / 600
[redacted]	Jun 1, 2019	48 / 100

5. Add the contract ID to the company by clicking on **Add Asset**.
6. Select the license that has the contract ID from the drop down menu, then click **Add.**
7. Select the contract ID from the drop down menu, then click **Add**



Company Setting

Company Name: Orange

Company Description: Fruit Company

[redacted] ✖
[redacted] 2 ✖
⊞ Add Contract

[redacted] ✖
[redacted] 2 ✖
⊞ Add Contract

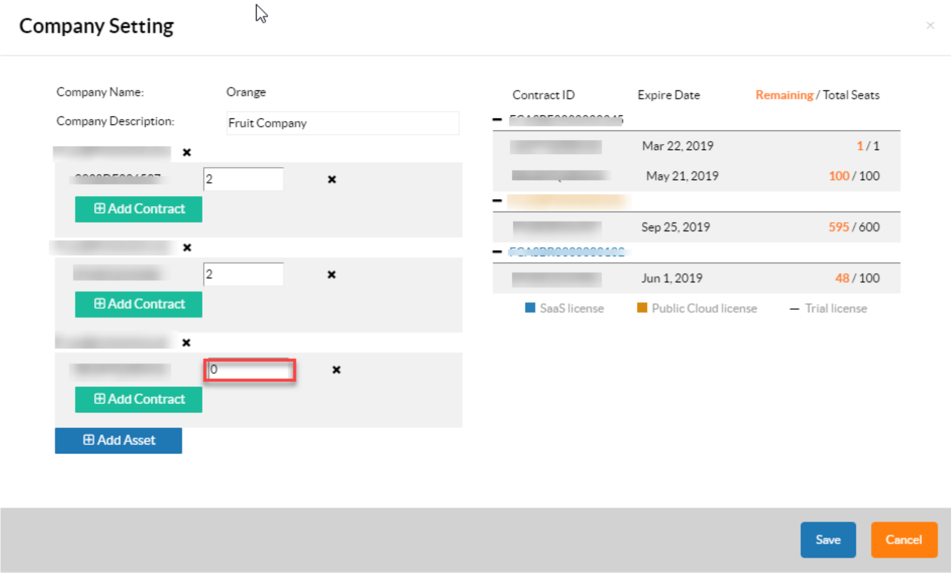
[redacted] ✖
⊞ Add Contract
[redacted] ▼ Add Cancel

⊞ Add Asset

Contract ID	Expire Date	Remaining / Total Seats
– [redacted]		
[redacted]	Mar 22, 2019	1 / 1
[redacted]	May 21, 2019	100 / 100
– [redacted]		
[redacted]	Sep 25, 2019	595 / 600
– [redacted]		
[redacted]	Jun 1, 2019	48 / 100

■ SaaS license ■ Public Cloud license — Trial license

8. In the field next to the contract ID, enter the number of seats you want to assign to this company



Company Setting

Company Name: Orange

Company Description: Fruit Company

[redacted] ✖
[redacted] 2 ✖
⊞ Add Contract

[redacted] ✖
[redacted] 2 ✖
⊞ Add Contract

[redacted] ✖
[redacted] 0 ✖
⊞ Add Contract

⊞ Add Asset

Contract ID	Expire Date	Remaining / Total Seats
– [redacted]		
[redacted]	Mar 22, 2019	1 / 1
[redacted]	May 21, 2019	100 / 100
– [redacted]		
[redacted]	Sep 25, 2019	595 / 600
– [redacted]		
[redacted]	Jun 1, 2019	48 / 100

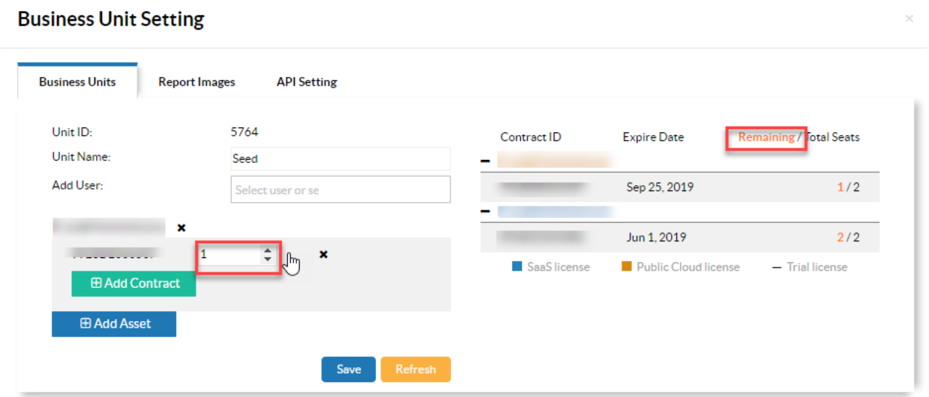
■ SaaS license ■ Public Cloud license — Trial license

9. Click **Save**.

Now you can assign new seats to the business unit under the company. To add more seats to the desired business unit, please follow these steps:

1. From the company management page, select your business unit.
   It will bring you to the FortiCASB dashboard.
2. Click the ⚙ **Business Unit Setting** button, located at the top-right.

3. Now you can add more seats by entering the number of seats in the field next to the contract.
   Note: **Remaining seats** shows number of seats available to add.



Business Unit Setting

Unit ID: 5764

Unit Name: Seed

Add User: Select user or se

[redacted] ×

[redacted] 1 ×

Contract ID	Expire Date	Remaining / Total Seats
[redacted]	Sep 25, 2019	1 / 2
[redacted]	Jun 1, 2019	2 / 2

■ SaaS license ■ Public Cloud license — Trial license

4. Click **Save.**
   Now the business unit have additional seats to add to it's sub-users.

Salesforce

OAuth Request errors

If an error occurs, an error message will be displayed on the Salesforce panel.

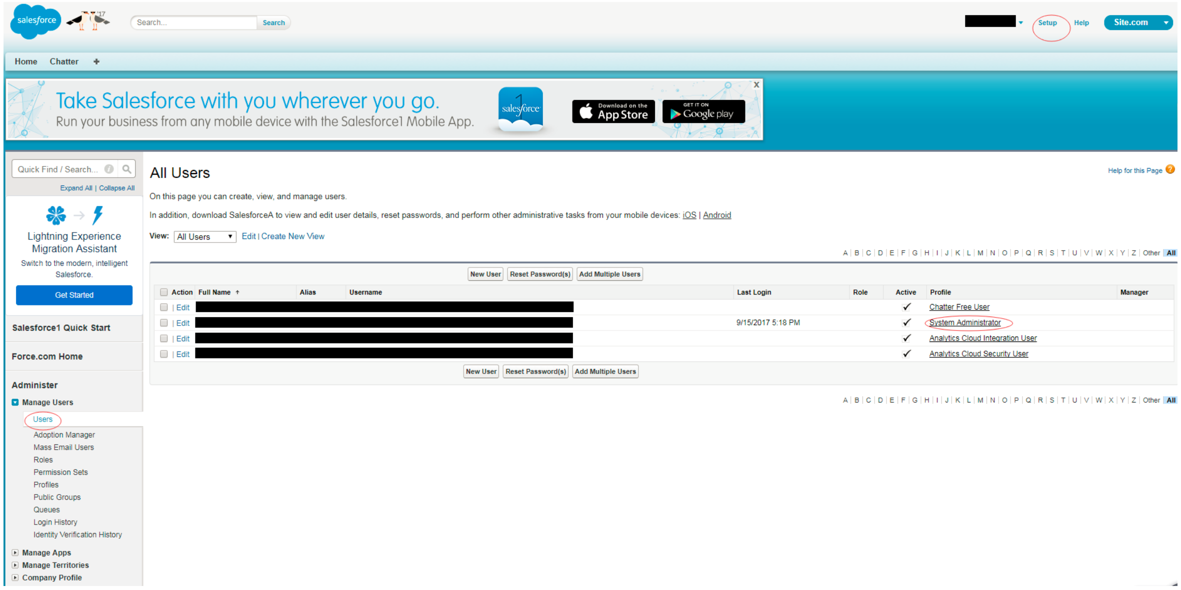
The following sections show some common error messages, as well as possible solutions:

- If your error message says "Saas application API gateway not accessible", go to Saas application API gateway not accessible error on page 148

Saas application API gateway not accessible error

FortiCASB requires users to have three specific Salesforce permissions. To check your Salesforce permissions, follow these steps:

1. From your Salesforce menu, go to **Setup > Manage Users > Users.**
2. Click on the profile of the integrated user.
   For example, if the integrated user is listed as a "**System Administrator**", click on System Administrator under "Profile".


salesforce
Search...
Search
Setup
Help
Site.com
Home
Chatter
Take Salesforce with you wherever you go.
Run your business from any mobile device with the Salesforce1 Mobile App.
Download on the App Store
GET IT ON Google play
Quick Find / Search...
Expand All | Collapse All
Lightning Experience Migration Assistant
Switch to the modern, intelligent Salesforce.
Get Started
Salesforce1 Quick Start
Force.com Home
Administer
Manage Users
Users
Adoption Manager
Mass Email Users
Roles
Permission Sets
Profiles
Public Groups
Queues
Login History
Identity Verification History
Manage Apps
Manage Territories
Company Profile
Help for this Page
A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | Other | All
New User
Reset Password(s)
Add Multiple Users

All Users

On this page you can create, view, and manage users.

In addition, download SalesforceA to view and edit user details, reset passwords, and perform other administrative tasks from your mobile devices: iOS | Android

View: All Users | Edit | Create New View

Action	Full Name ↑	Alias	Username	Last Login	Role	Active	Profile	Manager
□ | Edit	[redacted]	[redacted]	[redacted]			✓	Chatter Free User	
□ | Edit	[redacted]	[redacted]	[redacted]	9/15/2017 5:18 PM		✓	System Administrator	
□ | Edit	[redacted]	[redacted]	[redacted]			✓	Analytics Cloud Integration User	
□ | Edit	[redacted]	[redacted]	[redacted]			✓	Analytics Cloud Security User	

3. Make sure you have the "API Enabled", "View All Data", and "View All Users" permissions enabled.

If you have all these permissions and still encounter the error, your organization could have reached Salesforce's daily API request limit. To check if you have reached this limit, follow these steps:

1. From your Salesforce menu, go to **Setup > Company Profile > Company Information**.
2. Check "API Requests, Last 24 Hours" to see if you have reached your maximum limit.

If you have reached this limit, wait for the next 24 hour period to try again.

Salesforce enforces API call limits based on a per-organization basis, not a per-user basis. If your organization has multiple applications sharing Salesforce API requests, please consolidate usage between applications.

Office 365

Add Site Collection Admin errors

The following sections show some common causes for this error, as well as possible solutions.

- If your azure domain does not end in ".onmicrosoft.com", go to Customized SharePoint homepage URL on page 150

Customized SharePoint homepage URL

FortiCASB's "Add Site Collection Admin" feature currently only supports the default azure domain format (abc.onmicrosoft.com). If you have a custom SharePoint homepage URL, you will have to allow collection manually.

1. From your SharePoint Online Admin Center, click **user profiles.**
2. Use the "Find profiles" feature to find a user, right-click that user's account name, then click **Manage site collection owners.**
3. In the "Site Collection Administrators" box, enter your admin username, then click the icon.
4. Click **OK**. FortiCASB can now audit this user's OneDrives.
5. Repeat steps one through four for each user you wish to audit.
6. From the FortiCASB Office 365 authentication menu, check "Prefer not to provide".

Add Users errors

Even if such an error occurs, FortiCASB will still monitor users that do not trigger this error. For example, in this case, FortiCASB will monitor the 37 users that were added successfully, even if this error is not corrected.

The following sections show some common causes for this error, as well as possible solutions.

- If these users have never logged into their Office 365 accounts before, go to Adding users with new Office 365 accounts on page 150.

Adding users with new Office 365 accounts

Office 365 activates a new user's SharePoint portal when he or she logs in for the first time. For a brand new O365 account, log into the account once to activate the portal, then add the user in FortiCASB.

Add Groups errors

Some groups do not generate or manipulate files. FortiCASB will not monitor these groups. FortiCASB will also not monitor groups the site administrator does not have permission to monitor.

Even if such an error occurs, FortiCASB will still monitor groups that do not trigger this error.

Dropbox Business

OAuth Request error

Please check the user role of the account used to log in to Dropbox Business. This account must have "Team Admin" Permissions.

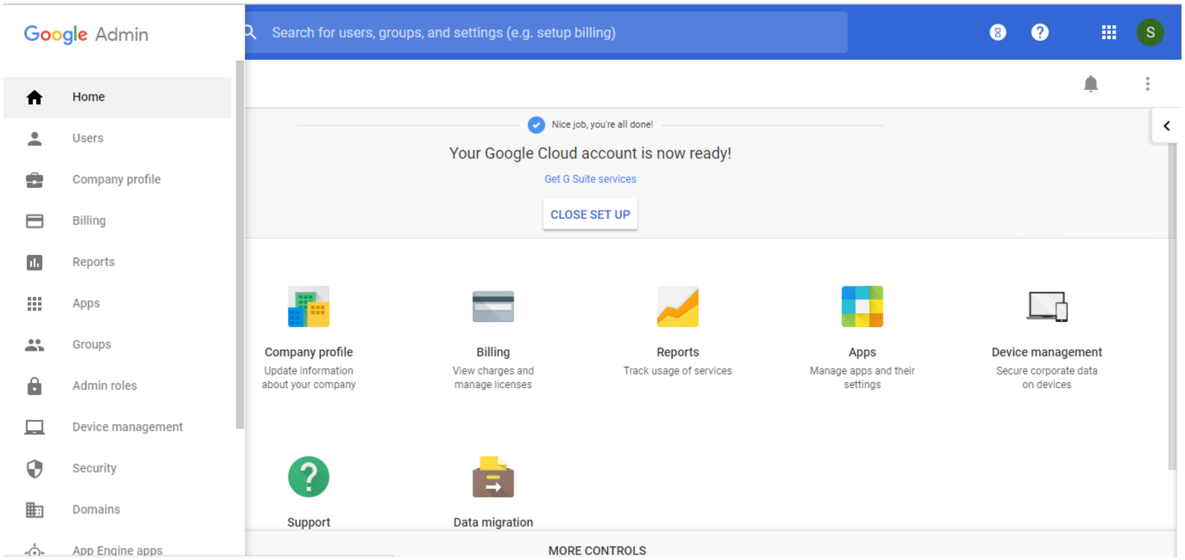
Google

Google Drive connection errors

If FortiCASB will not connect to your Google Drive account, one common reason is because your Google account is not a Super Administrator and does not have the correct permissions.

To check if your Google account is a Super Administrator, go to https://admin.google.com/, and log in with your Google account.

If your interface is the same as the one shown below, you are a Super Administrator.



Nice job, you're all done!

Your Google Cloud account is now ready!

Update information about your company

View charges and manage licenses

Track usage of services

Manage apps and their settings

Secure corporate data on devices

If you are not a Super Administrator, either ask the Super Administrator to grant you Super Administrator permissions or use the Super Administrator's Google account to link to FortiCASB.

If you're unsure who your administrator is, contact your IT department, help desk, or the manager who gave you the account.

Due to Google requirements, only G Suite accounts with a business or enterprise license can use FortiCASB. G suite accounts with a basic license will be unable to use FortiCASB.