Know Your AWS Burner Account

Document Prepared by: Cloud & DevOps Center of Excellence

Version 1.9.0

Contents

publicis
sapient

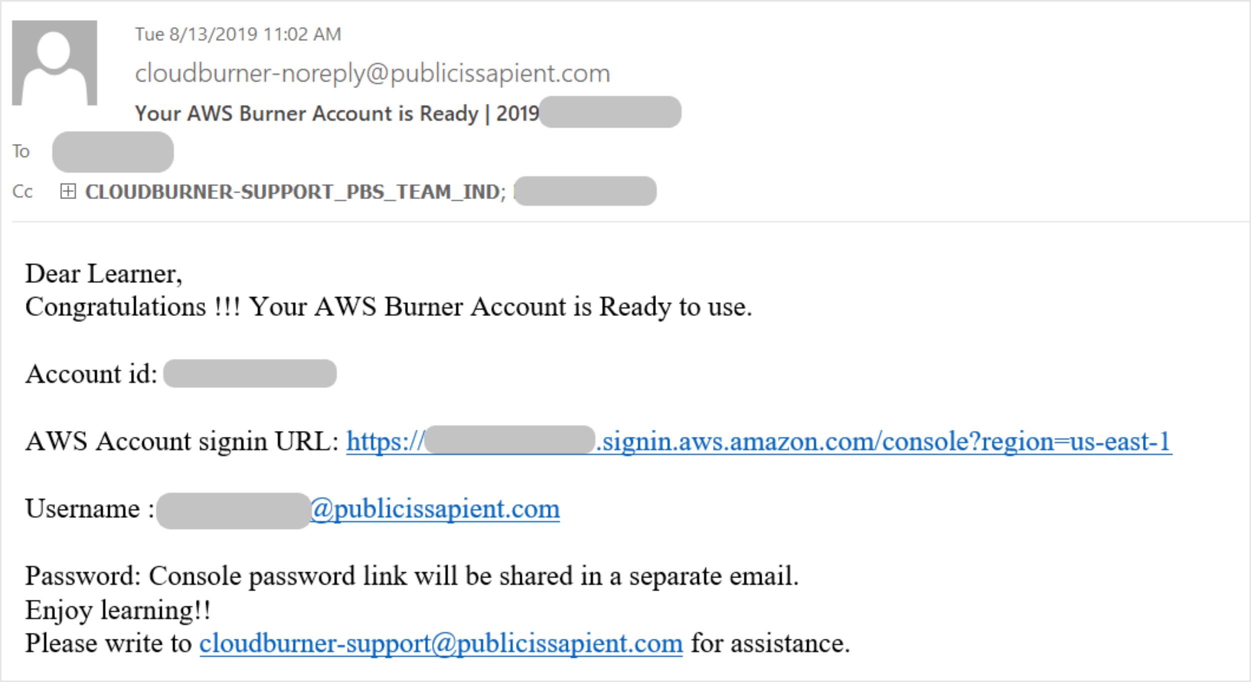
Congratulations on getting your Burner account created successfully on AWS!

Before you get started, please go through this document to familiarize yourself with **What's & How's of your Burner Account**. If you still have questions, please reach out to cloudburner-support@publicissapient.com

1. First Time Login

Note: Make sure you are on PublicisSapient Network otherwise you will see "access restricted" error on AWS console home page upon login. Please refer to ***#ConfigureVPN*** (Section 2) of this document below on how to connect to Lion Checkpoint VPN.

Step 1: Open the emails received from AWS with your username and password link.



Tue 8/13/2019 11:02 AM
cloudburner-noreply@publicissapient.com
Your AWS Burner Account is Ready | 2019[redacted]
To [redacted]
Cc ⊞ CLOUDBURNER-SUPPORT_PBS_TEAM_IND; [redacted]

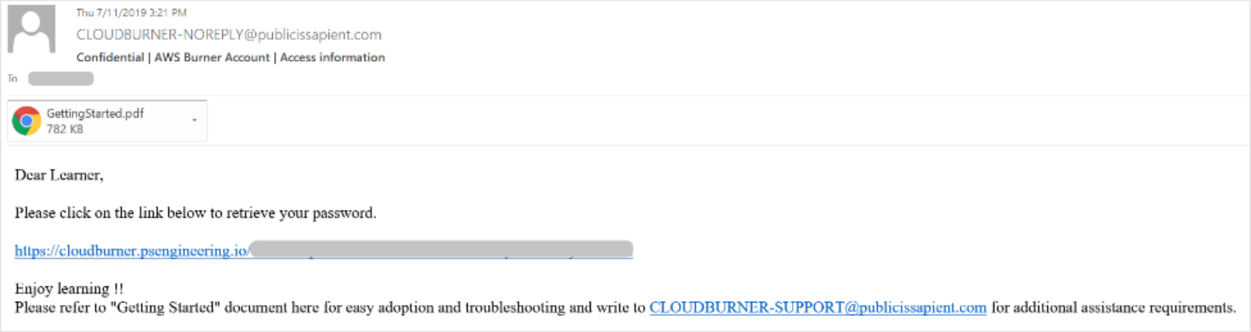
Dear Learner,
Congratulations !!! Your AWS Burner Account is Ready to use.

Account id: [redacted]

AWS Account signin URL: https://[redacted].signin.aws.amazon.com/console?region=us-east-1

Username :[redacted]@publicissapient.com

Password: Console password link will be shared in a separate email.
Enjoy learning!!
Please write to cloudburner-support@publicissapient.com for assistance.



Thu 7/11/2019 3:21 PM
CLOUDBURNER-NOREPLY@publicissapient.com
Confidential | AWS Burner Account | Access information
To [redacted]

Dear Learner,

Please click on the link below to retrieve your password.

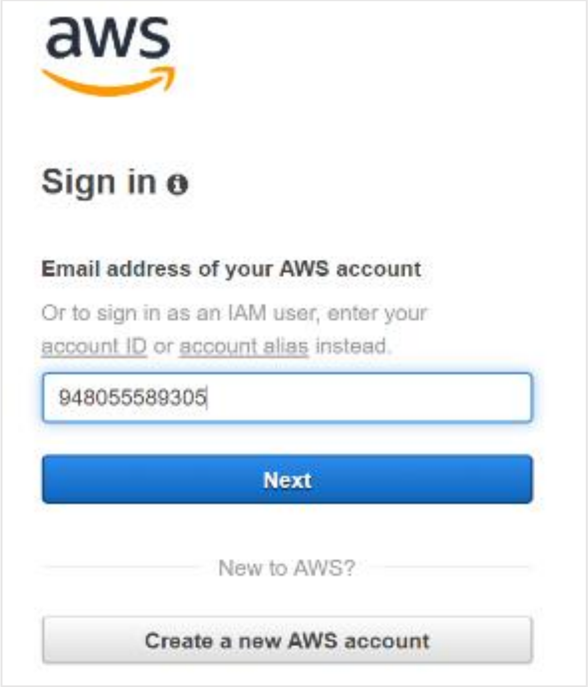
https://cloudburner.psengineering.io/[redacted]

Enjoy learning !!
Please refer to "Getting Started" document here for easy adoption and troubleshooting and write to CLOUDBURNER-SUPPORT@publicissapient.com for additional assistance requirements.

Step 2: Click the temporary password link and copy the temporary password from the browser window.

Step 3: Go to AWS Console.

Step 4: Enter your 12 digit Account Number provided in the email and click Next, as shown below:



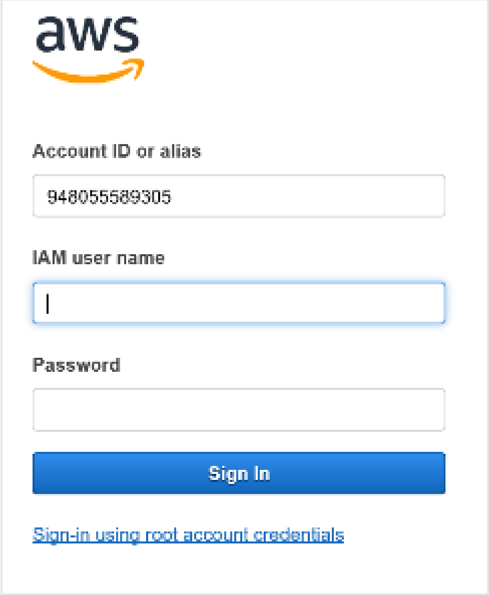
Sign in

Email address of your AWS account

Or to sign in as an IAM user, enter your account ID or account alias instead.

948055589305

Step 5: Now enter your iam username (*same as your publicissapient.com email id*) and temporary password (from step #2) and click Sign In.

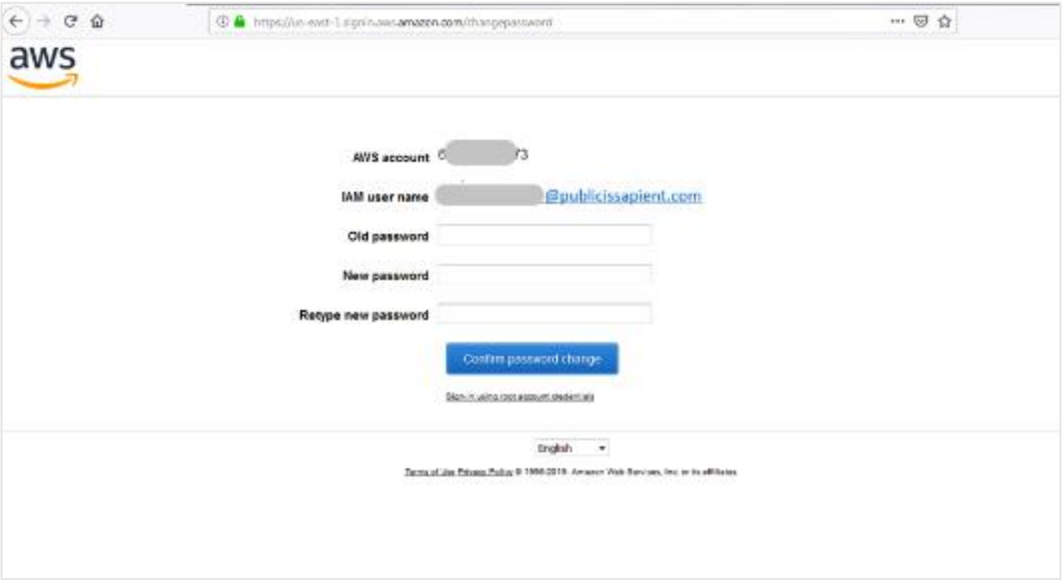


Account ID or alias: 948055589305

IAM user name

Password

Step 6: You will now be prompted to change your temporary password. Generate a new password here and login.



https://us-east-1.signin.aws.amazon.com/changepassword

AWS account 0[redacted]73

IAM user name [redacted]@publicissapient.com

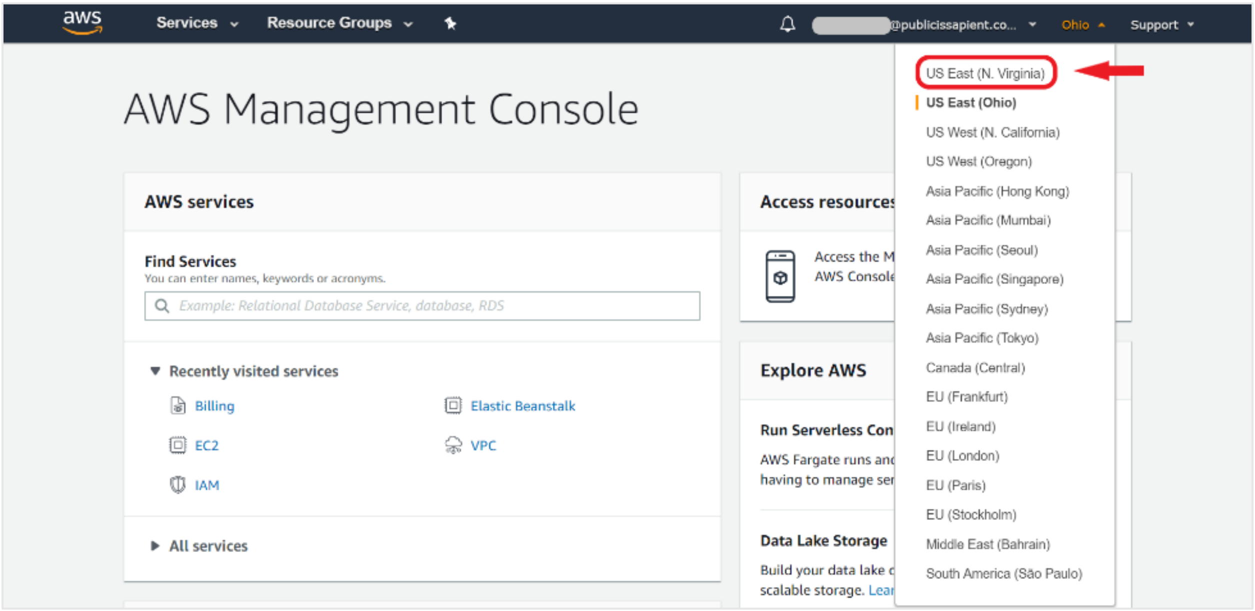
Old password

New password

Retype new password

aws
Confirm password change
Sign-in using root account credentials
English
Terms of Use Privacy Policy © 1996-2019, Amazon Web Services, Inc. or its affiliates.

Step 7: After you have login successfully into AWS Console, make sure the region selected on top right corner is (us-east-1) i.e. **N. Virginia**. The <u>burner account is restricted to be used with US East (N. Virginia) region</u> ONLY.



AWS Management Console

AWS services

Find Services

You can enter names, keywords or acronyms.

Example: Relational Database Service, database, RDS

Recently visited services

- Billing
- EC2
- IAM
- Elastic Beanstalk
- VPC

All services

Access resources

Access the M
AWS Console

Explore AWS

Run Serverless Con
AWS Fargate runs and
having to manage ser

Data Lake Storage
Build your data lake c
scalable storage. Lear

2. Configure VPN

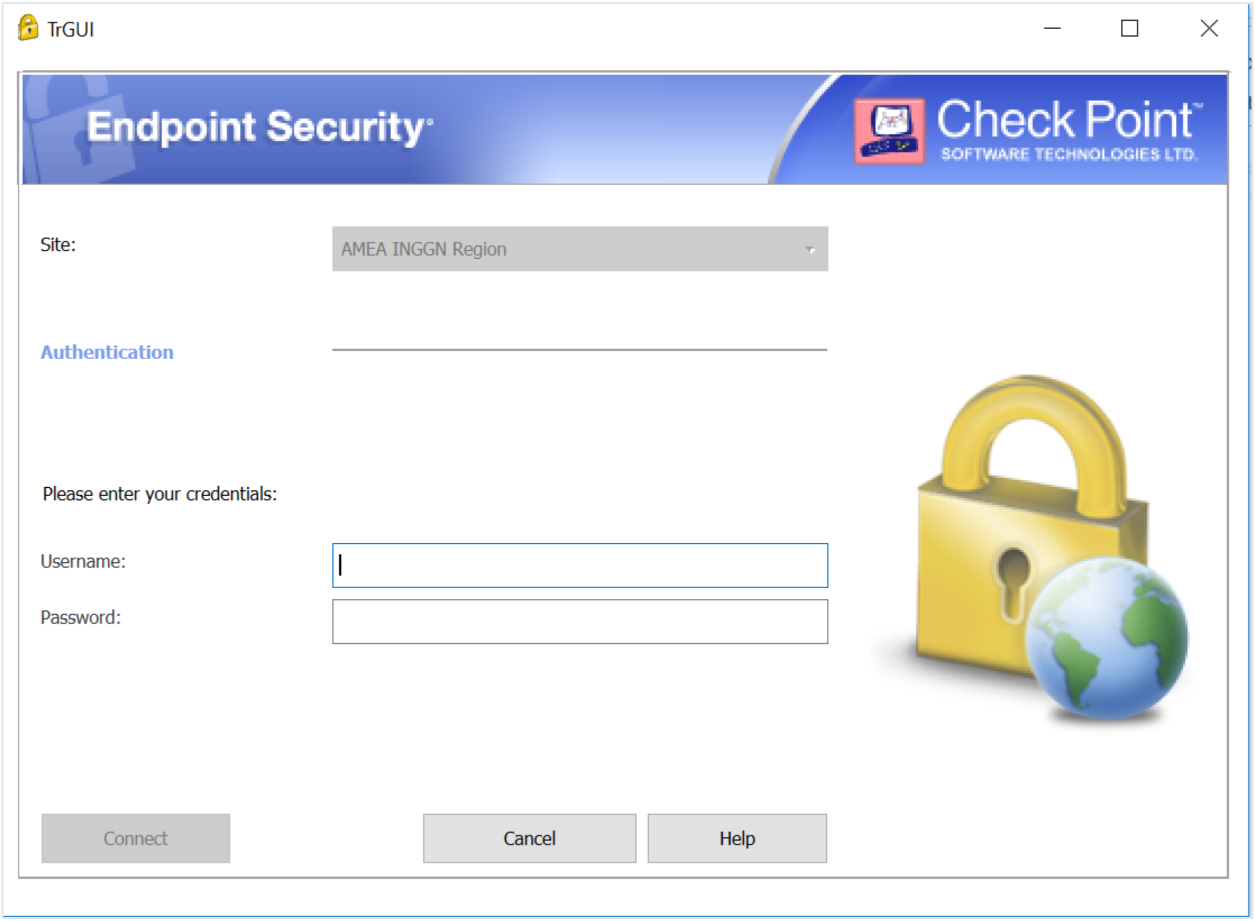
Note:

1. If you are using VPN to access Burner Account, then follow the steps below to configure your Checkpoint VPN to use Burner Account.
2. If Checkpoint VPN is not installed, raise a HD ticket and get Checkpoint installed on your laptop.

Now that you have Checkpoint VPN installed, use one of the methods below to connect to VPN:

Method 1 (Using AMEA INGGN or AMEA INBLR Region)

i. Select **AMEA INGGN or AMEA INBLR Region** from Site Dropdown.



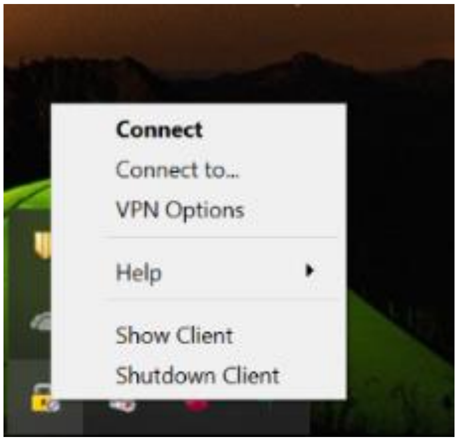
Site: AMEA INGGN Region

ii. Enter your Lion Login credentials to connect.

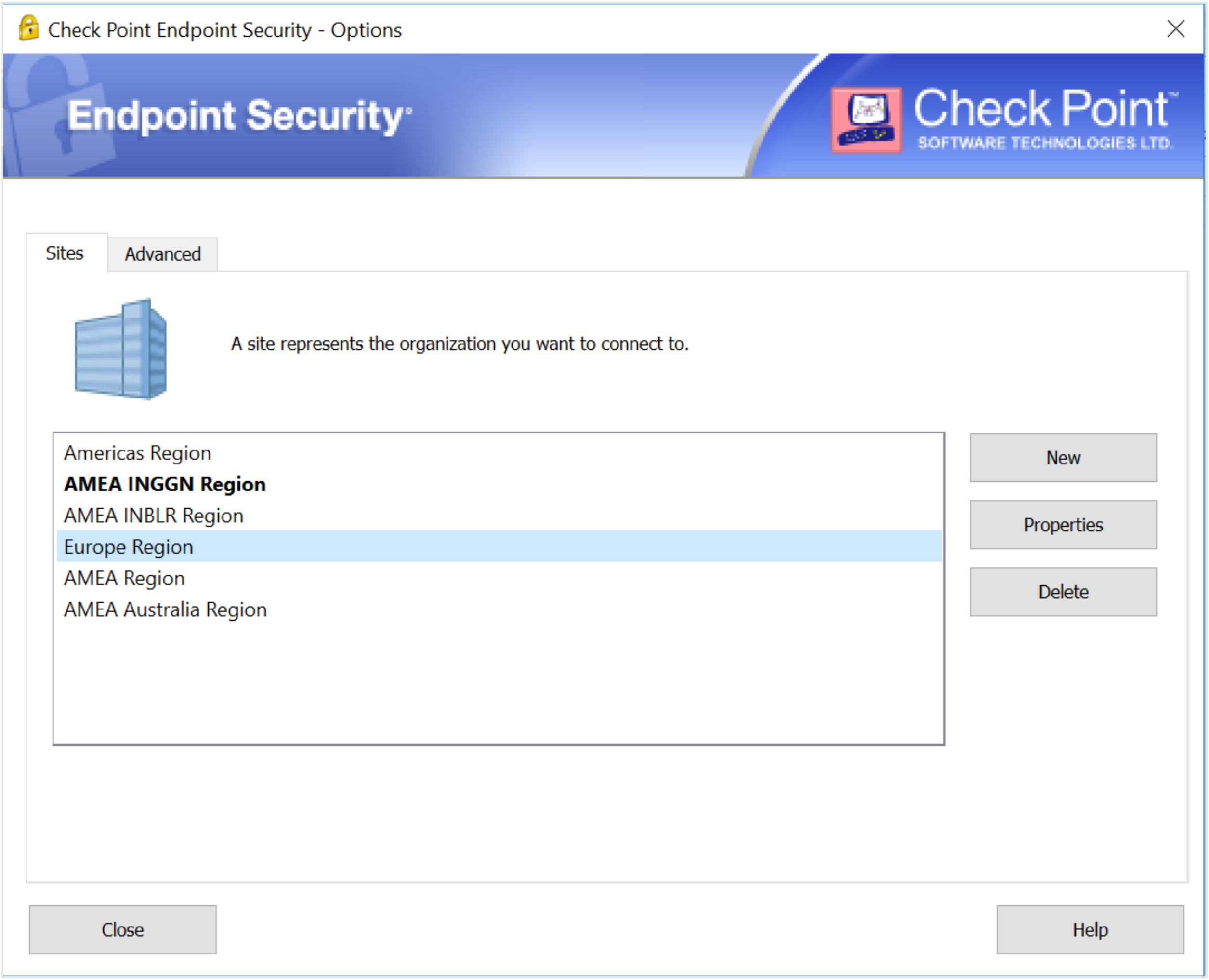
OR

Method 2 (Using Other than INGGN or INBLR VPN Connection)

i. Right click the Checkpoint VPN icon and click VPN Options



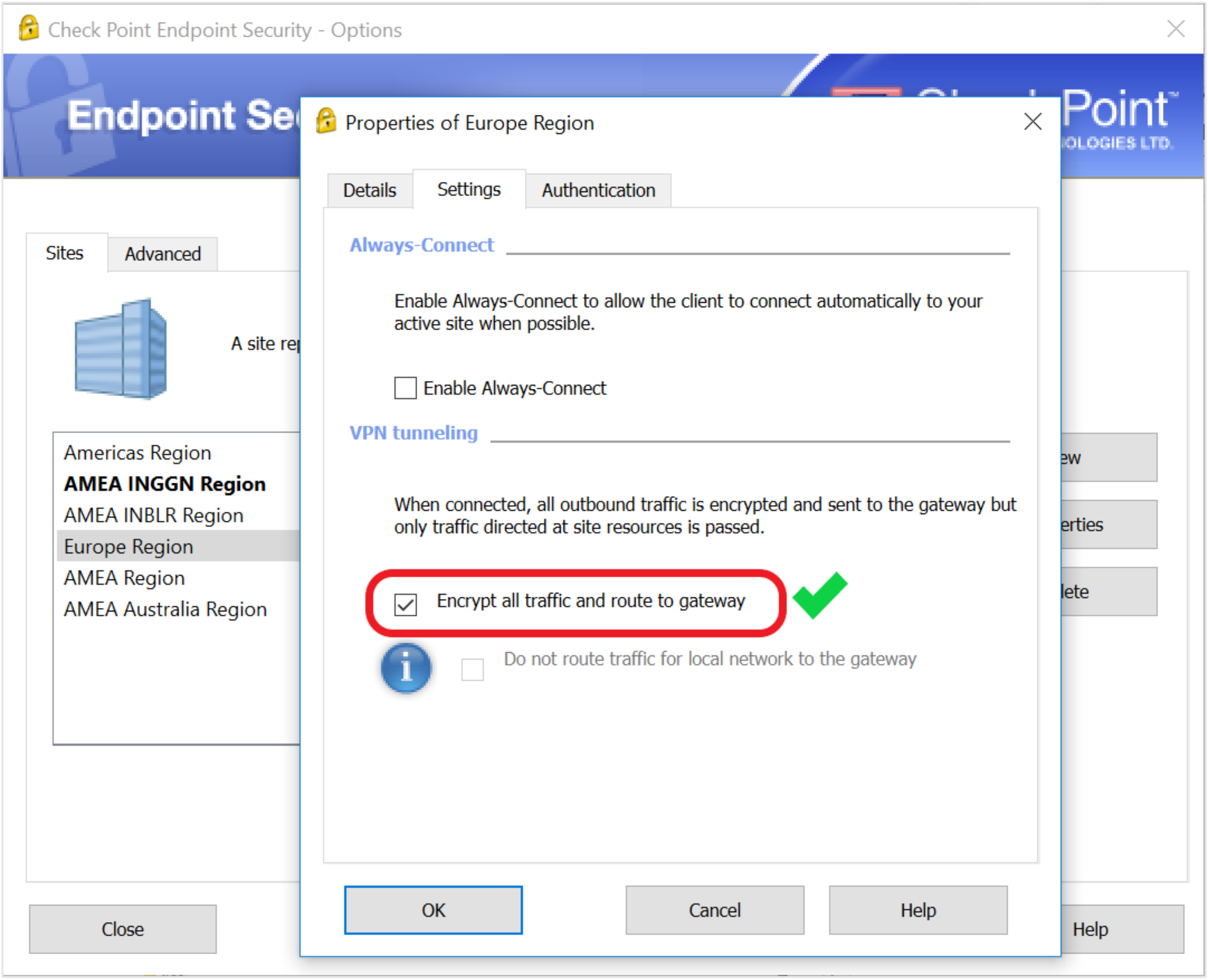
ii. Select the VPN Site depending on your region and click Properties on the right.



A site represents the organization you want to connect to.

Americas Region
AMEA INGGN Region
AMEA INBLR Region
Europe Region
AMEA Region
AMEA Australia Region

iii. Now, Click the **Settings** tab and check the "Encrypt all traffic and route to gateway" as shown below:



Check Point Endpoint Security - Options

Properties of Europe Region

Details | Settings | Authentication

Always-Connect

Enable Always-Connect to allow the client to connect automatically to your active site when possible.

□ Enable Always-Connect

VPN tunneling

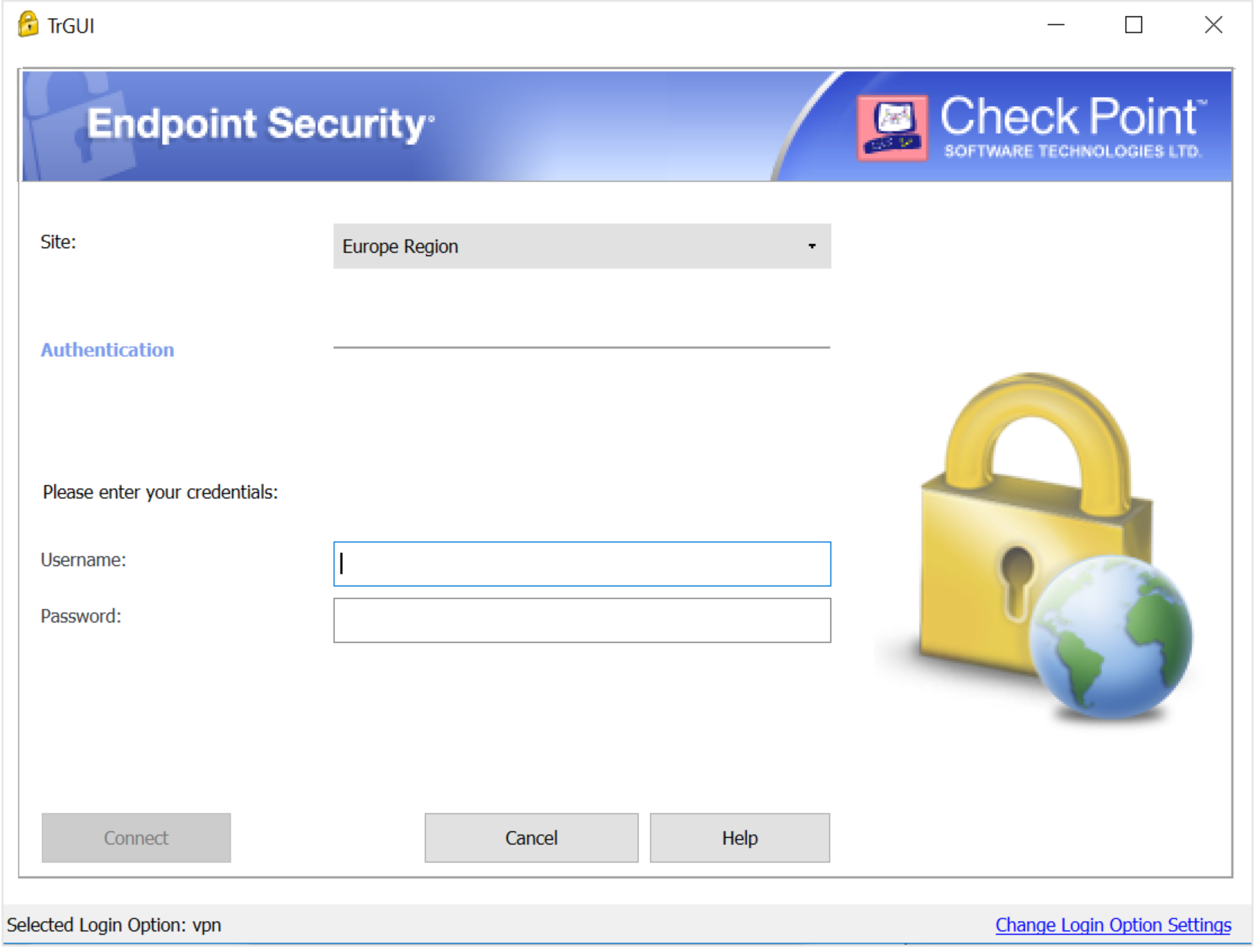
When connected, all outbound traffic is encrypted and sent to the gateway but only traffic directed at site resources is passed.

☑ Encrypt all traffic and route to gateway ✓

□ Do not route traffic for local network to the gateway

iv. Click Ok and close the VPN.

v. Open Checkpoint VPN and select the above configured VPN site from dropdown



TrGUI
Endpoint Security
Check Point
SOFTWARE TECHNOLOGIES LTD.
Authentication
Please enter your credentials:
Username:
Password:
Connect
Cancel
Help
Change Login Option Settings

Site: Europe Region

Selected Login Option: vpn

vi. Enter your Lion Login credentials to connect.

3. Allowed Services & Instance Types

Your Burner Account lets you use as many services as possible to give you a simple & easy learning experience. Below is a list of major services you can use without any restrictions.

Note:

1. *AWS has an exhaustive list of services & resources hence not all allowed services may be listed below.*
2. *Some of the services might show "quota exceeded" errors which means AWS has to explicitly allow the usage of that service. Raise a request with AWS support or Cloud Burner Support.*
3. *In case you are receiving "explicit deny" error message then it is likely that a non-allowed services is being provisioned. Reach out to Cloud Burner Support to clarify.*

Acm	cognito-sync	Kinesis	ses
acm-pca	Comprehend	Kms	Securityhub
Amplify	Config	Lambda	Serverlessrepo
API Gateway	Dax	Lex	Servicecatalog
Artifact	Dms	license-manager	shield
Athena	Dynamodb	Machinelearning	Sms
Autoscaling	EC2	Macie	Snowball
Backup	ECR	Mgh	Sns
cloud9	ECS	Mq	Sqs
Cloudformation	EKS	neptune-db	Ssm
Cloudfront	Elasticache	Opsworks	Storagegateway
Cloudhsm	Elasticbeanstalk	Organizations	Swf
Cloudsearch	Elasticfilestorage	Polly	Transcribe
Cloudtrail	Elasticmapreduce	Quicksight	Translate
Cloudwatch	ElasticSearch	Ram	Trustedadvisor
Codebuild	Events	Rds	Waf
Codecommit	Glacier	Redshift	Wellarchitected
Codedeploy	Glue	Route53	workdocs
Codepipeline	Guardduty	Route53resolver	Xray
Codestar	Health	S3	
cognito-identity	Inspector	Sagemaker	
cognito-idp	Kafka	Secretsmanager	

Allowed Instance Types:

Instance Category	Instance Type	vCPU	Memory (GiB)
Compute Optimized	c5.large	2	4 GiB
Compute Optimized	c5.xlarge	4	8 GiB
General Purpose	t2.micro	1	1 GiB
General Purpose	t3.micro	2	1 GiB
General Purpose	t3.small	2	2 GiB
General Purpose	t3.medium	2	4 GiB
General Purpose	t3.large	2	8 GiB

General Purpose	m5a.large	2	8 GiB
General Purpose	a1.xlarge	4	8 GiB
General Purpose	t3.xlarge	4	16 GiB
General Purpose	m5a.xlarge	4	16 GiB
Memory Optimized	r5a.large	2	16 GiB
Memory Optimized	r5.large	2	16 GiB
Storage Optimized	i3.large	2	15.25GiB

4. Explicit Denied Services

Your Burner Account comes with pre-configured restrictions to prevent misuse of Account and to avoid high monthly bills. These restrictions are applied with lot of due diligence and should not affect your learning experience.

a4b	Gamelift	Mediaconvert	Wam
Appstream	Greengrass	Medialive	Worklink
Ce	Iot	Mediapackage	Workmail
Chime	iot1click	Mediastore	Workspaces
Connect	Iotanalytics	Mobiletargeting	Reserved Instances
Cur	Iotevents	Robomaker	
Directoryservice	Iotsitewise	Route53domains	
Elastictranscoder	Kinesisvideo	sms-voice	
Freertos	Mediaconnect	Sumerian	

5. Burner Account Management

Reset Password

- To reset your AWS Burner Account password, login into the https://cloudburner.psengineering.io and click the **Password Reset** button & a new password link will be sent to your email.

Unable to Change Password

- When login in for the First Time into your AWS Burner Account, it will prompt you to change your password. At this time make sure you are connected to the Publicis Sapient network else you will see the error:

  "Either user is not authorized to perform iam:ChangePassword or entered password does not comply with account password policy set by administrator"

ELB & AutoScaling

- Auto Scaling groups requires a *AWSServiceRoleForAutoScaling* servicelinkedrole and this role already exists in most cases. In accounts where this role does not exists, will see the

Explicit Deny access. Once this role is created, AutoScaling Groups can be created successfully.

- Likewise, ELB requires *AWSServiceRoleForElasticLoadBalancing* servicelinkedrole. Once this role is created (if not already exists in the newly created Burner Account), load balancers can be launched without any restrictions.

Cloud Formation

- Cloud Formation stack can be created only by providing the template url of S3 bucket. Upload your template in a bucket and use the bucket url to create a CF stack.
- Cloud Formation stack will fail if the template is creating an S3 bucket.

6. Burner Account Policies

Available AWS Regions

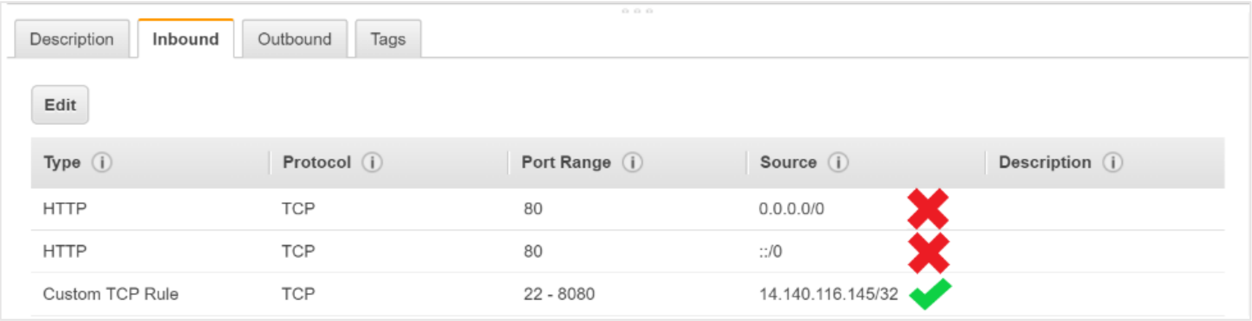
- Only us-east-1 (N. Virginia) region is available for use. All other regions are blocked. Change the region to us-east-1 if the default region is us-east-2 (Ohio) when you sign in.
- Bookmark the sign in url received in the Account Information Email received for easy access to the AWS console & region.

Burner Root Access

- Burner Account root user access is blocked. Only IAM users can be used to access AWS Services (both programmatically & console).

Security Group Ingress Rules

- All Ingress rules with source other than xxx.xxx.xxx.xxx/32 will be auto removed.
- Allowed Ingress rules should be as shown below:



Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0 ✗	
HTTP	TCP	80	::/0 ✗	
Custom TCP Rule	TCP	22 - 8080	14.140.116.145/32 ✓	

Budgets Alerts

- Budget Alerts Notification keeps you aware of your credit usage. Alerts are sent when the usage reaches:
  - 50%

  - 70%
  - 90%

  You will receive alerts when you have used your credits as per above usage. We recommend, you back up your data before you use 100% credit and also shutdown running services that may incur unnecessary costs.

Account Suspension

- Burner Accounts will be automatically suspended as soon as $100 credit is used.
- Suspended accounts cannot launch new services nor can access existing resources.

Account Nuking

- Suspended Burner Accounts older than 48 hours will be automatically nuked and all running services be terminated and data will be deleted.
- It is therefore recommended, to take backups of any config, code & data before the account is suspended.

7. Things to remember

- Every Burner Account comes with $100 credit limit. Unused credits will not be carried-forward.
- User will receive **three notifications** regarding their usage and remaining credit before they exhaust 100% of available credit. Once user consumes available credit, the account is **suspended**.
- A suspended burner account will get **purged**/deleted after 2 days of suspension.
- Data-backup isn't pre-configured on Burner Accounts i.e. user is responsible to **take backups** of their data & configurations.
- User must be in **Publicis Sapient Network** to use AWS console and launch services.
- Only one region ***us-east-1*** i.e. N. Virginia is available to use on AWS Console.
- In case of an error while creating an AWS service, please refer to #3 & #4 of the document.
- User does not have direct access to AWS Technical Support on BURNER account. For any support and assistance requirements, reach out to cloudburner-support@publicissapient.com
- Burner Accounts are free for all Publicis Sapient people. These are available for learning and research purposes and learners should use services prudently.
- Accounts with Zero-activity will be monitored and subject to termination.

8. Best Practices

- Always keep your data backed up. Burner Account does not perform any backups.
- Use the Burner credit wisely: Shutdown/Stop instances and other running services when not in use to make best use of the credit.
- Do not upload client or Publicis Sapient work or credentials or IPs on the Burner Account.
- Be aware of security threats – raise alarm if you find something wrong with your account.
- Do not upload or share objectionable content on Burner Services.
- Do not make the services, resources or applications publicly accessible.
- Do not share your Burner credentials with anyone.