Creating S3 bucket for Jobs and Reports

Steps to select the bucket and set the following CORS policy:

1) Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2) Select the created bucket. For example: sharedtablet
3) Click on CORS Configuration
4) Place the given code in CORS configurator editor and Save it.

```
<?xml version="1.0" encoding="UTF-8"?>
<CORSConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <CORSRule>
        <AllowedOrigin> Suremdm URL</AllowedOrigin>
        <AllowedMethod>POST</AllowedMethod>
        <AllowedMethod>PUT</AllowedMethod>
        <AllowedMethod>DELETE</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
    <CORSRule>
        <AllowedOrigin>*</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
    </CORSRule>
</CORSConfiguration>
```

Create an IAM user with the following policy

In this step, you will create an IAM user with a policy:

1) Open the IAM console at https://console.aws.amazon.com/iam/.

2) In the navigation pane, choose Users.

3) Choose Add user.

4) On the Details page, enter the following information:

a) User name—type a unique name. For example : User Name

b) Access type—choose Programmatic access.

Choose Next: Permissions.

5) On the Permissions page, choose Attach existing policies directly, and then choose Create policy.

6) On the Create Policy page, select Create Your Own Policy.

7) On the Review Policy page, enter the following information:

a) Policy Name—type a unique name. For example: User Policy.

b) Description—type a short description for the policy

c) Policy Document—copy and paste code given below in document

Choose Create Policy.

8) Return to the Permissions page. In the list of policies, choose Refresh. To narrow the list of policies, choose Filter Customer managed. Choose the IAM policy you created in the previous step (for example: User Policy.), and then choose Next: Review.

9) On the Review page, choose Create user.

10) On the Complete page, go to the Secret access key and choose Show. After you do this, copy both the Access key ID and Secret access key. You will need both of these identifiers to Configure Your Amazon EC2 Instance.

```
{
        "Version": "2012-10-17",
        "Statement": [
                {
                        "Effect": "Allow",
                        "Action": [
                                "s3:ListBucket",
                                "s3:GetBucketLocation",
                                "s3:ListBucketMultipartUploads"
                        ],
                        "Resource": "arn:aws:s3:::sharedtablet"
                },
                {
                        "Effect": "Allow",
                        "Action": [
                                "s3:AbortMultipartUpload",
                                "s3:DeleteObject",
                                "s3:DeleteObjectVersion",
                                "s3:GetObject",
                                "s3:GetObjectAcl",
                                "s3:GetObjectVersion",
                                "s3:GetObjectVersionAcl",
                                "s3:PutObject",
                                "s3:PutObjectAcl",
                                "s3:PutObjectAclVersion"
                        ],
                        "Resource": "arn:aws:s3:::sharedtablet/*"
                }
        ]
}
```

Generate Access Keys for this user.