



## VOICELINQ AWS STORAGE

How To: Manage Recordings, Voicemail, and Fax Files

[View Online](#)

Version 1.0 [11/08/2024]

VoiceLinQ, Powered by **DTS Technology, LLC.**

DTS-DSCR: Customer Document



# Table of Contents

---

|                                         |    |
|-----------------------------------------|----|
| Overview.....                           | 2  |
| Why is AWS Storage Important .....      | 2  |
| Functionality Definitions.....          | 3  |
| Offloading Process Rules.....           | 3  |
| Managing Files .....                    | 4  |
| Deleting Files.....                     | 4  |
| Playing Files.....                      | 4  |
| Working with AWS.....                   | 5  |
| Before You Begin.....                   | 5  |
| AWS Storage .....                       | 5  |
| Create an AWS Storage Bucket .....      | 5  |
| AWS Accounts and Security .....         | 6  |
| Create an AWS Identity.....             | 6  |
| Create an AWS Identity Access Key ..... | 7  |
| AWS Policies .....                      | 8  |
| Creating an AWS Policy.....             | 8  |
| Linking VoiceLinQ to AWS.....           | 9  |
| What's Needed .....                     | 9  |
| Contacting DTS Technology .....         | 9  |
| Additional Information .....            | 10 |
| Document Properties.....                | 10 |



# Overview

---

## Why is AWS Storage Important

---

Did you know that voicemail often takes up to 95% of storage needs and is rarely accessed once dormant for 15 days? This guide aims to reduce disk requirements by offloading media files (faxes and voicemails) to a remote storage service when the file has not been accessed for a certain number of days (Default is 15 days).



### PLEASE NOTE!

The default time to store files in VoiceLinQ before moving them to AWS is 15 days. If AWS has not been set up there is a risk of losing saved recordings, voicemail, and/or any fax documents.



### IMPORTANT!

Getting AWS set up is **100% the customers' responsibility** to ensure storage limits are met. DTS Technology is **NOT** responsible for lost media files including, but not limited to, call recordings, voicemails, or fax files.

The Media Offload (NEMO) tool uses the File Replicator to offload voicemails and fax media files to any S3 compatible storage (such as Amazon S3), while still allowing the Core Module and VoiceLinQ to play the remote files. Even though the file storage is saved to AWS, to the everyday user, it's as if nothing has changed.

## Functionality Definitions

---

NEMO functionality is dependent on the **NFR**, the **NMS**, and the **API** working together. There is no UI that controls NEMO. Instead, it's configured in three different areas.

The **NFR** scans the disc and checks voicemail and fax files to upload or download. It does not offload or delete. Its main function is to search.

The **API** performs the upload, deleting the file after a successful upload, and controls how long and when the NFR should scan. API configuration is added to locate the remote destination for offload and allow the system access.

The **NMS (Core Module)** builds the link with the metadata so AWS files can be played within VoiceLinQ. The NMS is driven by system parameters to locate the files in remote storage.

## Offloading Process Rules

---

NEMO offloads voicemail and fax files. The process looks like this:

1. NFR searches the data directory for a voicemail or fax file access timestamp greater than the set value (which defaults to 15 days).
2. If there are files not accessed in that timeframe, then they are scheduled to be offloaded. Meaning, if a file was opened 5 days ago, it will not be scheduled for offloading. If a file was opened 16 days ago, it will be scheduled. If a file is almost due to be offloaded (it's been 14 days), but then the file is accessed, the count will restart, and it will be another 15 days before it will be scheduled for offloading.
3. NFR will then dispatch an event alert to the VoiceLinQ cluster that it wants to take care of the directory for offload. If another NFR in the cluster is already working on it, then it will reply with an event to alert the first NFR. This communication avoids more than one NFR taking care of a single directory concurrently.



# Managing Files

---

## Deleting Files

---

If a voicemail or fax file is deleted before it has been offloaded (such as a user deleting their voicemail when they receive it), then the file is deleted locally. The delete action is kept in sync between the user and the local storage. If a file is deleted before the set value (default 15 days), then it won't make it into remote storage.

After a voicemail has been offloaded, it can still be played from the user's voicemail directory. If the user deletes the voicemail, the file is moved to trash. When the file reaches the point of time set (default is 1 day), then the NMS will purge the cache from the cluster. If the cache is a NEMO file, the NMS will send a request to the API which will then do the work of clearing remote storage media.

## Playing Files

---

Offloaded files are still accessible, such as the case with listening to an offloaded voicemail. From a user's perspective, they will access their voicemail box and play the voicemail like normal. Nothing will change from their point of view.



# Working with AWS

---

## Before You Begin

---

Before using this document, you **must** have an **active** AWS account. This document does not cover the steps needed to create the initial AWS account. It's highly recommended to create this account, if you don't already have one, before proceeding. You can use this link to reference creating an account:

<https://docs.aws.amazon.com/accounts/latest/reference/welcome-first-time-user.html>



### IMPORTANT!

There are costs associated with many features within AWS! Do not assume anything is free within AWS. It is your responsibility to understand any, and all costs associated with AWS. DTS Technology is not responsible for anything AWS related, including supporting AWS features and functionality!



## AWS Storage

---

Please follow the following steps to create the needed storage bucket in AWS. It is assumed you have already read, and fully understand, the previous section, before you Begin.

## Create an AWS Storage Bucket

---

To have VoiceLinQ call recordings automatically saved to an external location you must create, or already have, an AWS S3 Bucket available. AWS is currently the only external storage approved for VoiceLinQ. Please follow the below steps, without skipping any steps, to create your S3 storage account in AWS.

1. While logged into AWS, go to Services, select Storage, then select S3. (*Figure 1*)

2. Select, Create bucket.
3. You will need to give the bucket a name. The name should not contain any upper-case letters or spaces. *(Figure 2)*
4. You will also need to select a region for your bucket. The region should be the closest possible to the desired location using the storage. *(Figure 2)*
5. Continue through the wizard selecting any additional options as desired.

Figure 1

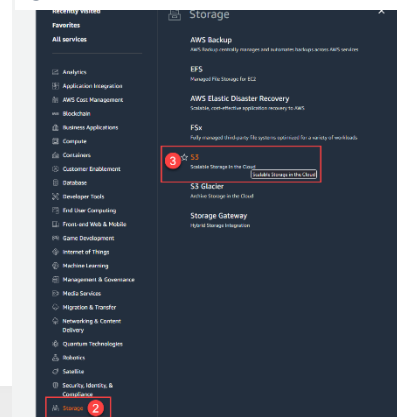
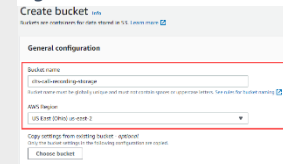


Figure 2



## AWS Accounts and Security

Please follow the following steps to establish a connection to the router.

### Create an AWS Identity

Once the storage bucket is created, an account must be created so VoiceLinQ can be connected to the storage bucket. Please follow the steps below to create an account.



#### IMPORTANT!

If you already have an account created you would prefer to use, please make sure the account has the correct permissions based on the below steps.

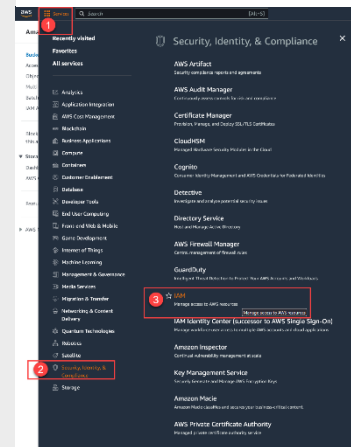


## PLEASE NOTE!

Sensitive information about the account must be shared with DTS Technology to properly create the link from VoiceLinQ to your AWS instance. This includes the bucket name, bucket region, access key, secret key, and bucket prefix. Please create a new account if you do not currently have an account where you can share this information with DTS Technology.

1. While logged into AWS, go to Services, select Security, Identity, & Compliance, then select IAM. (*Figure 3*)
2. Select Users.
3. Select Add users.
4. Create a name for the user.
5. Continue through the wizard selecting any additional options as desired.

Figure 3

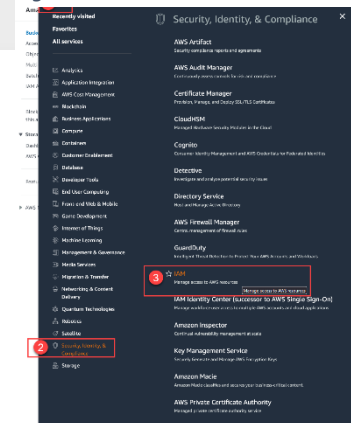


## Create an AWS Identity Access Key

Once the storage bucket and user are created, an account must have an Access Key created so VoiceLinQ can be connected to the storage bucket. Please follow the steps below to create an Access Key.

1. While logged into AWS, go to Services, select Security, Identity, & Compliance, then select IAM. (*Figure 4*)
2. Select Users.
3. Select the user account you want to have the Access Key assigned to.
4. Select Create access key.
5. Under Access key best practices & alternatives, select the option Application running outside AWS.
6. Continue through the wizard selecting any additional options as desired.

Figure 4





# AWS Policies

Please follow the following steps to create the needed policy to allow account access to the storage bucket.

## Creating an AWS Policy

Before you continue, you must have your storage bucket name you want to use to allow your account the needed permissions.

1. While logged into AWS, go to Services, select Security, Identity, & Compliance, then select IAM. (*Figure 5*)
2. Select Policies.
3. Select Create policy.
4. Under Specify Permissions, select the option for JSON. (*Figure 6*)
5. In the Policy Editor, paste the below JSON.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::BUCKET_NAME_HERE"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::BUCKET_NAME_HERE/*"
      ]
    }
  ]
}
```

6. Make sure to replace the text, **BUCKET\_NAME\_HERE** with the name of the storage bucket you created. (*Figure 6*)
7. Select Next to continue.
8. Give the new policy a name, then select Create policy.

Figure 5

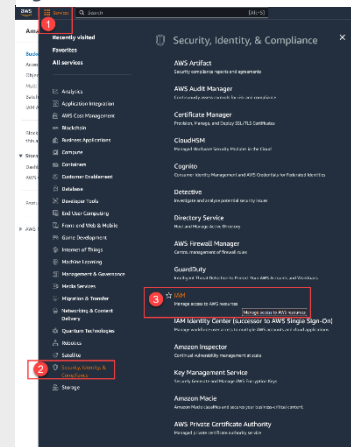
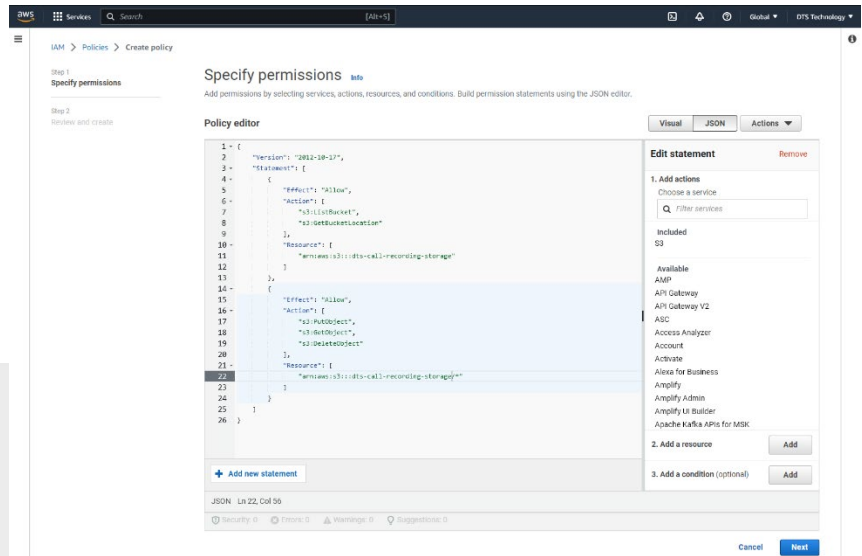


Figure 6



## Linking VoiceLinQ to AWS

### What's Needed

After all the above sections have been completed, the next step is to send your DTS Technology Account Manager the needed information to create the link.

Please send the following:

- Bucket Name:
- Bucket Region:
- Access Key:
- Secret Key:
- Bucket Prefix:



## Contacting DTS Technology

For additional assistance, please call us at, 800.803.1535, email us, [support@dtstechnology.com](mailto:support@dtstechnology.com), or chat with us by going to our website, [dtstechnology.com](https://dtstechnology.com).



## Additional Information

For additional information, please reach out to your sales/support representative and they will be able to help you.



## Document Properties

| Changed By   | Changed Date | Version Control |
|--------------|--------------|-----------------|
| David Pegram | 11/18/2024   | 1.0             |