CloudFront
VERSION VAULT

Cloud.in
Hostin Services Private Limited

Product User Guide

Document Version: 1.2

Table of Contents

CloudFront
VERSION VAULT

support@cloud.in | www.cloud.in

1. Introduction

CloudFront Version Vault is a centralized tool designed to simplify the management and tracking of AWS CloudFront distribution configurations. It enables users to view versions, and restore changes made to behaviors, origins, error pages, aliases, and Lambda functions. Every configuration update is stored as a version, offering full visibility and control over distribution history.

Dashboard Overview: The dashboard includes two main sections:
- Active Distributions (Default view).
- Deleted Distributions.

Clicking on a distribution ID opens a detailed view with multiple tabs reflecting configuration details similar to the CloudFront console. One key tab is Versions, which displays a list of all saved versions for that distribution.

Version Management

For Active Distributions:
- Roll back to a selected version.
- Copy a version to another distribution.
- Create a new distribution from any version.

For Deleted Distributions:
- Copy a version to an existing distribution.
- Recreate the deleted distribution using a saved version.

Both views allow side-by-side version comparison to easily identify configuration changes.

User Management

- Admins can manage users by providing and managing role based access control.

Schedule Management

- Define cron-based schedules for specific distributions.

SMTP Notifications

- Configure SMTP settings to enable event-based email alerts.

SSL Configuration

- Secure your custom domain with certificate and key configuration.

Discover What's New in v1.2 ✨

- **Detecting and restoring deleted distributions.**
- **Copying a version to another distribution.**
- **Creating a new distribution from a saved version.**
- **Centralized Schedule Management for tracking changes and deletions.**
- **Supports automatic email notifications via SMTP for important events and updates.**
- **Supports SSL configuration to enable secure HTTPS access using custom domains.**

2. Getting Started

2.1 Launching the Instance

- Subscribe to the CloudFront Version Vault AMI from the AWS Marketplace.
- Launch an EC2 instance using this AMI.
- We recommend using a t3.medium instance or higher for smooth performance.

2.2 Security Group Configuration

- Open Required Ports: Ensure that the following Ports are open in your Instance's Security Group.

> **Note: It is recommended to open the below ports only for internal IP Addresses, do not keep ports open for all.** ⓘ

- **Port 443: For accessing the Web App.**

2.3 IAM Role Attachment

1. Open IAM Console >> Go to Roles >> Click Create Role.

2. **Select Trusted Entity:**
   - Choose AWS service.
   - Use Case: EC2.
   - Click Next.

3. **Skip Permissions:**
   - Don't attach any policies here (you'll add an inline policy next).
   - Click Next >> Add a role named **cloudfront-version-vault-role** >> Create role.

4. **Add Inline Policy:**
   - After creating, open the role >> Go to Permissions tab >> Click Add inline policy.
   - Choose JSON tab >> Paste the policy json on page 03.
   - Click Review policy, name it **cloudfront-version-vault-inline-policy** >> Create policy.

5. **Attach Role to EC2 Instance:**
   - Go to EC2 console >> Select instance >> Actions > Security > Modify IAM role.
   - Attach the newly created role.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
         "s3:GetBucketAcl",
                "s3:PutBucketAcl",
                "lambda:ListFunctions",
                "lambda:GetFunction",
                "lambda:ListLayerVersions",
                "lambda:EnableReplication",
                "cloudfront:ListCloudFrontOriginAccessIdentities",
                "cloudfront:ListFunctions",
                "cloudfront:ListOriginAccessControls",
                "cloudfront:ListFieldLevelEncryptionConfigs",
                "cloudfront:ListOriginRequestPolicies",
                "cloudfront:GetDistribution",
                "cloudfront:ListDistributionsByRealtimeLogConfig",
                "cloudfront:ListKeyGroups",
                "cloudfront:ListSavingsPlans",
                "cloudfront:ListRateCards",
                "cloudfront:UpdateDistribution",
                "cloudfront:ListContinuousDeploymentPolicies",
                "cloudfront:GetDistributionConfig",
                "cloudfront:ListUsages",
                "cloudfront:ListResponseHeadersPolicies",
                "cloudfront:ListDistributionsByCachePolicyId",
                "cloudfront:ListDistributionsByLambdaFunction",
                "cloudfront:ListCachePolicies",
                "cloudfront:ListDistributionsByKeyGroup",
                "cloudfront:ListPublicKeys",
                "cloudfront:ListConflictingAliases",
                "cloudfront:ListTagsForResource",
                "cloudfront:ListRealtimeLogConfigs",
                "cloudfront:ListInvalidations",
                "cloudfront:ListFieldLevelEncryptionProfiles",
                "cloudfront:ListDistributions",
                "cloudfront:ListStreamingDistributions",
                "cloudfront:ListKeyValueStores",
                "cloudfront:ListDistributionsByWebACLId",
                "cloudfront:ListDistributionsByResponseHeadersPolicyId",
                "cloudfront:ListDistributionsByOriginRequestPolicyId",
                "cloudfront:CreateDistribution"
            ],
            "Resource": "*"
        }
    ]
}
```

- **Open Browser:** Navigate to your instance's public IP address or DNS name using a web browser.
- **Access CloudFront Version Vault:** The frontend will be accessible at https://<your-instance-public-ip>.

- **Login:** Use the initial login credentials:
- **Username:** admin
- **Password:** AcRW%exB5o%4Qs

> **Note: Please make sure to reset the admin password!** ⚠️

2.4 User Role and Permission

- This application includes three user roles: Read-Only, Editor, and Admin. Each role has specific permissions that define what users can access and modify within the application.

1.Read-Only Role

- **Login & Password Management:** Users can log in and change their password.
- **Access:** Users with this role can only view data related to CloudFront distributions and versions.
- **Restrictions:** They are not permitted to modify, create, or delete any entity.

2. Editor Role

- **Login & Password Management:** Users can log in and change their password.
- **Read-Only Permissions:** The Editor role includes all permissions granted to the Read-Only role.
- **Generate and Rollback CloudFront Versions:** Editors can create new CloudFront versions and perform rollbacks on existing versions.
- **Restrictions:** Editors cannot manage other users or change their roles.

3. Admin Role

- **Login & Password Management:** Admins can log in, change their password, and manage other users passwords.
- **Full Access:** Admins have all permissions assigned to the Editor role.
- **User Management:** Create new users, Change the roles of existing users, Delete users from the application.
- **SMTP Configuration:** Configure SMTP settings to enable event-based email alerts.
- **SSL Configuration:** Secure your custom domain with certificate and key configuration.

Each role is designed to ensure that users have the appropriate level of access for their responsibilities. Be sure to assign roles carefully based on the user's responsibilities and required access level.

The CloudFront Version Vault dashboard enables users to view, manage,and restore CloudFront distribution configurations efficiently with a modern and intuitive interface.

Login Screen
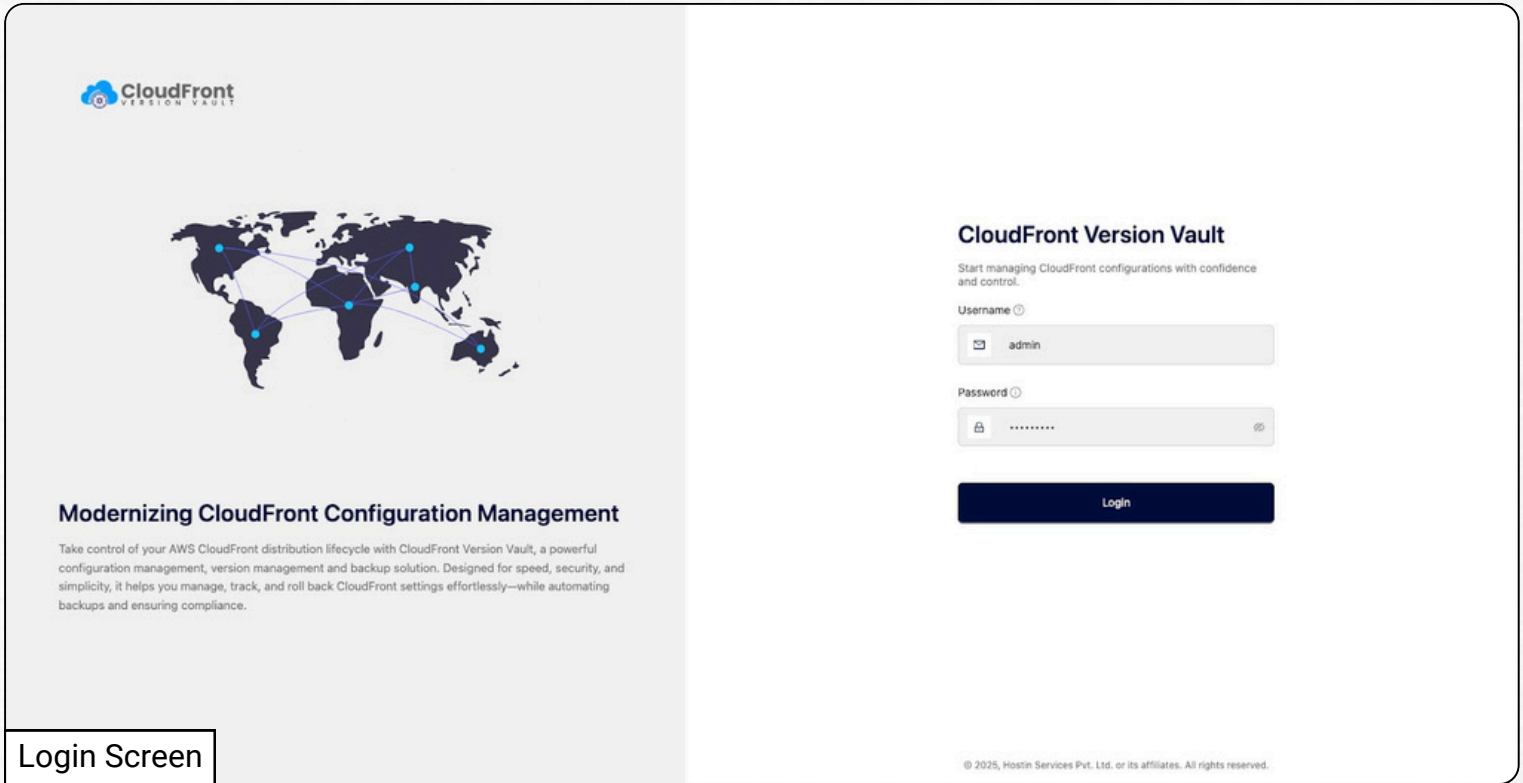
3.1 Application Layout

The application features a persistent sidebar offering the following primary navigation options:
- **Distributions:** View and manage both active and deleted distributions.
- **Users:** The admin manages platform users and their access levels.
- **Settings:** Access password, Schedule management, Email Notifications, SSL Configuration.
- **Logout:** Securely sign out of the application.

3.2 Viewing and Managing Distributions

a. Accessing Distributions
- Click the **Distributions** menu from the sidebar.
- You'll see two tabs at the top:
  - **- Active Distributions (default).**
  - **- Deleted Distributions.**
- Below the tabs, the respective list of distributions is displayed.

Dashboard

b. Distribution Details View:

- Clicking on a Distribution ID opens a detailed view with several tabs, designed to resemble AWS CloudFront's distribution information layout. Tabs include:
- **General Info:** Basic configuration and metadata.
- **Origins:** Origin domain and path settings.
- **Behaviors:** Cache and request behavior configurations.
- **Invalidations:** History of cache invalidations.
- **Aliases:** Alternate domain names.
- **Versions:** Version history of distribution configuration.

3.3 Working with Versions

a. Versions Tab (For Active Distributions)

In the Versions tab of an active distribution:

- You'll find a version table listing all saved configurations.
- For each version, the following actions are available:
- ⟲ **Rollback:** Revert the distribution to this version.
- ⎘ **Copy to Another Distribution:** Apply this version's config to another existing distribution.
- ⎚ **Create New Distribution:** Launch a brand-new distribution using this version's config.
- **Compare:** View configuration differences between two selected versions.

Version Tab - Active

b. Versions Tab (For Deleted Distributions)

In the Deleted Distributions tab, selecting a Distribution ID and navigating to its Versions tab allows you to:

- Copy to Existing Distribution.
- **Recreate Distribution** using a selected version.
- **Compare Versions**

Version Tab - Deleted

3.4 User Management

Accessible via the Users option in the sidebar, the User Management interface allows the admin to perform the following actions:

- **Add, modify, or delete users with the following roles:**
  - **Admin:** Full access to all application features including user and role management.
  - **Editor:** Has the same permissions as the Admin role, except cannot add or modify users.
  - **Read-Only:** Can view distribution info but cannot perform actions.

User Management
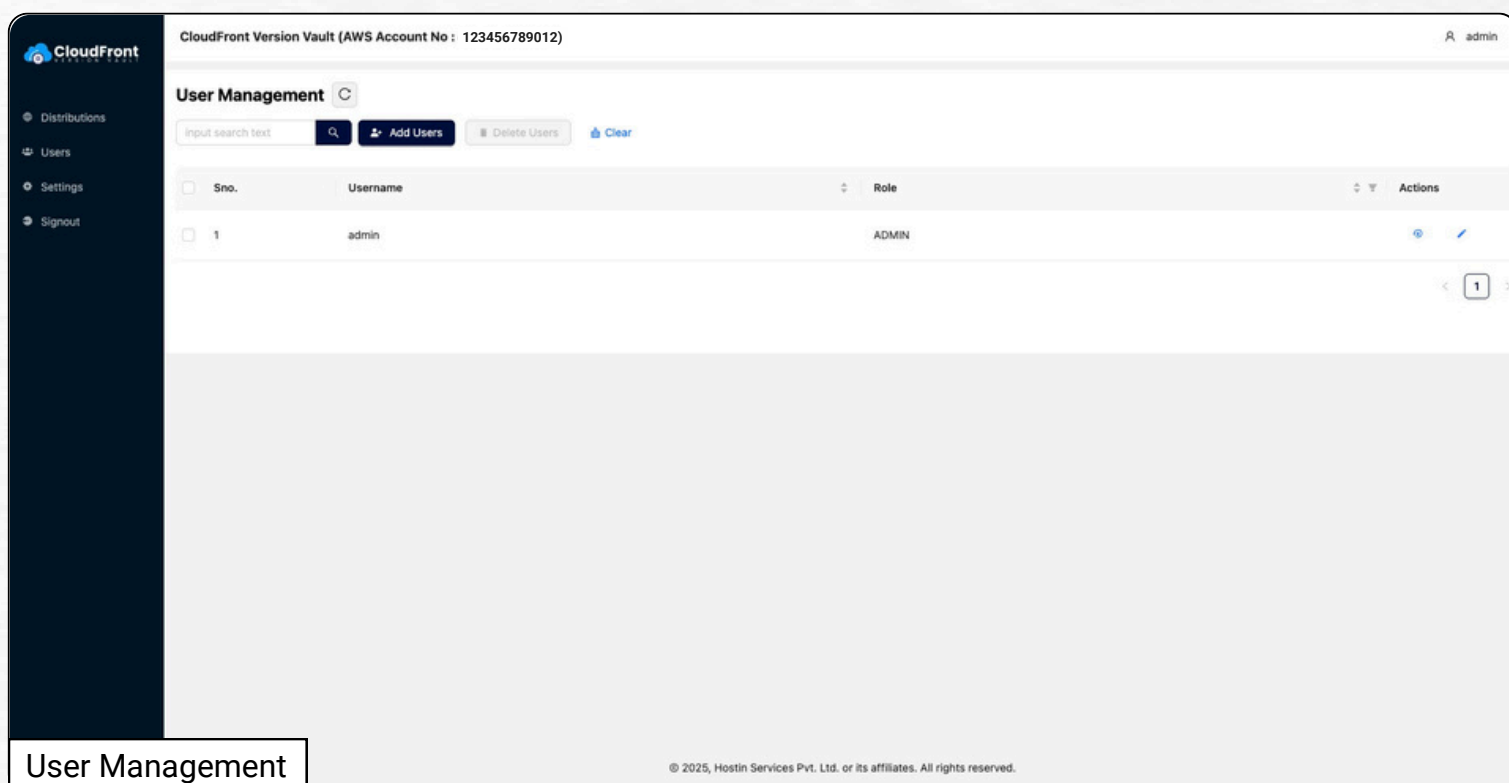
3.5 Settings Tab

Within the Settings menu, the following key options are available:

3.5.1 Change Password

To change your password:

- Go to **Settings.**
- Navigate to the **Change Password tab.**
- Enter your **current password, new password,** and **confirm the new password.**
- Click **Submit** and you're all set!

UI Guide: Manage & Roll Back CloudFront Configurations

CloudFront Version Vault (AWS Account No : 123456789012)　　admin

Settings

Change Password　Schedule Management　Email Notifications　SMTP Configuration　SSL Configuration

* Current Password ⓘ

Enter your current password 🔲

* New Password ⓘ

Enter new password 🔲

* Confirm New Password ⓘ

Re-enter your new password 🔲

Change Password

Distributions
Users
Settings
Signout

© 2025, Hostin Services Pvt. Ltd. or its affiliates. All rights reserved.

Reset Password

🛡 **Tips for Creating a Secure Password**
- Use at least 6 characters.
- Include a mix of uppercase, lowercase, numbers, and special characters.
- Avoid using common words, personal info (like birthdays), or simple patterns (e.g., 123456, password, qwerty).
- Consider using a passphrase (e.g., Purple$Rain!2024Sunny) for better memorability and strength.

3.5.2 Schedule Management

a. Accessing Schedule Management

• Go to Settings >> Schedule Management.

b. Master Schedule

• It checks for configuration changes and monitors deleted distributions across all entries every hour.
• Detect changes in configuration for every distribution.
• Monitor deleted distributions and disk usage, and send alerts if usage exceeds 90% if SMTP and email are configured.

c. Distribution-Specific Schedules

• This schedule monitors changes in a particular CloudFront distribution.

Schedule Management

The master schedule runs regularly to check for any missing CloudFront distributions. It first saves a snapshot of all existing ones. On future runs, it compares the current list with the saved one. If any are missing, they're marked as deleted and shown in the dashboard for easy tracking and recovery.

3.5.3 Email Notification and SMTP Configuration

SMTP is what lets the system send emails (like alerts or updates). You set it up by adding server details, AWS login, and a sender email. A green status shows when it's working.

SMTP Configuration

Notification List

Step 1: SMTP Setup

- The admin adds the email server settings (SMTP).
- Once it's set, the system is ready to send emails.

Step 2: Notification Triggers

The system watches for important events like:

- Low disk space.
- User changes.
- Distribution updates.

When something happens, the system prepares an email.

Step 3: Sending the Email

- The system sends the message using the SMTP server.
- The email goes out from the sender you set up to the right people.
- To manage recipients, the user clicks the mail icon in the Action tab, which opens the mailing list.
  modal. From there, they can add new emails or delete existing ones using the available options.

3.5.4 SSL Configuration

SSL (Secure Sockets Layer) certificates are like a digital passport for your website. They make sure that the connection between your users and your CloudFront distribution is secure and private. This is important for protecting sensitive information and building trust.

Configure SSL

1. Domain Name

- This is the web address (like **yourwebsite.com** or **mail.example.com**) that your SSL certificate is for.
- Enter your domain name here.

2. SSL Certificate

- This is the actual certificate code you received from your SSL provider (like Let's Encrypt, DigiCert, etc.).
- It's a long string of characters that typically starts with **-----BEGIN CERTIFICATE-----** and ends with **-----END CERTIFICATE-----**.
- Carefully copy and paste your complete SSL certificate into this box.

3. SSL Private Key

- Every SSL certificate has a matching private key. This key is crucial for decrypting the secure connection.
- It's another long string of characters, usually starting with **-----BEGIN PRIVATE KEY-----** or **-----BEGIN RSA PRIVATE KEY-----** and ending with **-----END PRIVATE KEY-----** or **-----END RSA PRIVATE KEY-----**.
- Carefully copy and paste your complete SSL private key into this box.
  Keep this private key very secure and do not share it with anyone!

Steps to Configure SSL

Step 1: Go to SSL Configuration
To get started with SSL, simply go to:

- In the left sidebar, click on **Settings**.
- Then, click on the **SSL Configuration** tab.
- On the **SSL Configuration** screen, look for the **Configure** button (usually on the right side).
  Click it to begin setting up your SSL certificate.

Step 2: Fill in Your SSL Details
Now, you'll need to provide three key pieces of information for your SSL certificate:

Step 3: Save Your Configurations

- Once you've entered all three required pieces of information, click the Configure button at the bottom of the pop-up window.

That's it! Your CloudFront Version Vault will now use your provided SSL certificate to secure the connections for your specified domain.

4. Conclusion

CloudFront Version Vault is a robust and intuitive tool designed to streamline the management of AWS CloudFront distributions. It empowers users with full visibility and control over distribution configurations, making tasks like rollback, monitoring, and version management seamless.

With CloudFront Version Vault, you can:

- **Roll back to any previous version of a distribution.**
- **Copy any saved version to another distribution or create a new distribution from it.**
- **Compare two versions side-by-side to identify configuration changes.**
- **Schedule monitoring tasks using cron-based or master schedules.**
- **Receive real-time email alerts via configurable SMTP settings.**
- **Secure your environment using custom SSL certificates.**
- **Manage user access and permissions with role-based controls (Admin, Editor, Read-only).**

We recommend reviewing version history regularly, keeping SMTP and SSL configurations up to date, and enforcing appropriate access control for all users.

Thank you for Trusting CloudFront Version Vault. ✨

CloudFront
VERSION VAULT