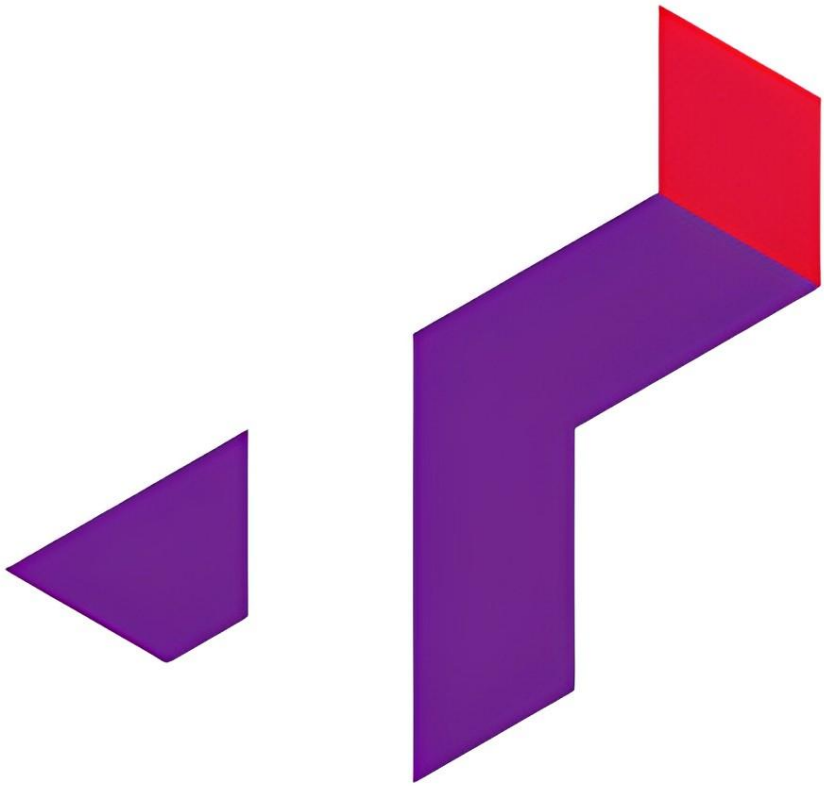
Tetherfi MX Contact Center – AWS Marketplace

Application Deployment Guide



Document Version: 2.0.0
Application Version: TetherfiMXDocker_3.0.0+
Last Updated Date: 2025 August 11

Warranty Information
Tetherfi makes no representations or warranties with respect to the contents or use of this product and specifically disclaims any express or implied warranties of merchantability or fitness for any purpose. Information in this document is subject to change without notice and does not represent a commitment on the part of Tetherfi.

Trademark Information
Tetherfi is a registered trademark of Tetherfi. Other product names may be trademarks or registered trademarks of their respective companies.

Contact Information
For customer inquiries, contact:
60 Paya Lebar Road, #05-09 Paya Lebar Square, Singapore

For technical support inquiries, call: Tetherfi +65 6715 7408
Or email support@tetherfi.com

Content

Introduction

Tetherfi MX Contact Center is a secure, cloud-native platform that unifies voice, chat, email, video, social media, and more into a single interface. **Powered by Edge-AI**, it delivers intelligent automation, routing, real-time insights, and a seamless omnichannel experience. With *built-in integrations* for leading *CRMs* and full *PCI-DSS/GDPR compliance*, MX Contact Center is ideal for enterprises seeking scalable, compliant, and efficient customer engagement.

Tetherfi MX Contact Center Capabilities

- Enables **omnichannel conversations** in your browser by managing all chat, audio, and video interactions with your customer.
- A detailed **customer information panel** that displays all past customer interactions, regardless of where they took place, thereby providing a 360-degree view of the customer journey.
- Enhanced **voice functionality** that facilitates the **easy transfer of calls** to other agents or supervisors for remote assistance.
- Readymade themes to **customize the desktop** based on the agent's preferences.
- **Easy-to-use** call and messaging controls to handle customer interactions effectively.
- **Comprehensive reporting** that allows you to gain valuable insights into your contact center's operations.
- **Intuitive user interface** for supervisors to perform tasks such as agent supervision, **real-time monitoring** of key contact center performance indicators, and **helping** agents with customer interactions.
- The platform features a customizable agent desktop that allows **seamless integration with custom widgets**, enhancing productivity and workflows.
- The IVR, chat, email, and social media workflows are highly configurable through an **intuitive drag-and-drop interaction UI**, enabling rapid deployment and adjustments.
- **No installation required** on the agent's PC, as it includes a web phone that runs on any modern browser supporting WebRTC.
- **Cost-effective** for a small-scale contact center.

Intended Audience

This guide is intended for the following audience:

- **Contact center agents** and **supervisors** who use the Agent Desktop to provide *customer service over different media channels*.

Prerequisites

Users must have a modern browser that supports WebRTC.

- Google Chrome 100+
- Microsoft Edge 100+

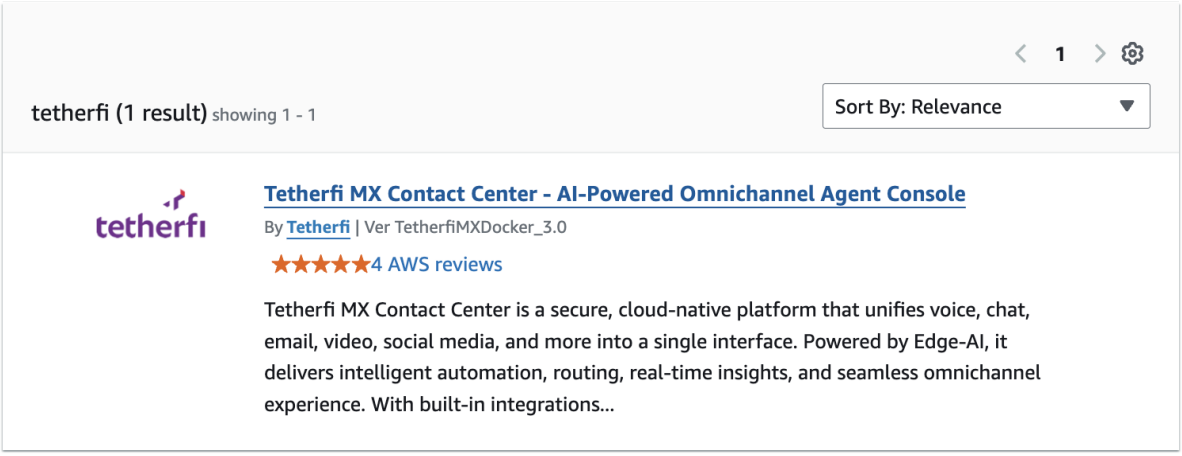
Recommendations

Instance Type	No of Agents	CPU	RAM	IVR Calls + Web phone calls + Video Calls	Text Chat, Social Media Chat	Emails per minute
t2.xlarge	50	4	16	80	150	50
t2.2xlarge	100	8	32	160	300	100

Getting Started

Find in the Marketplace

Open AWS Marketplace and search for “Tetherfi”. You will see options below.

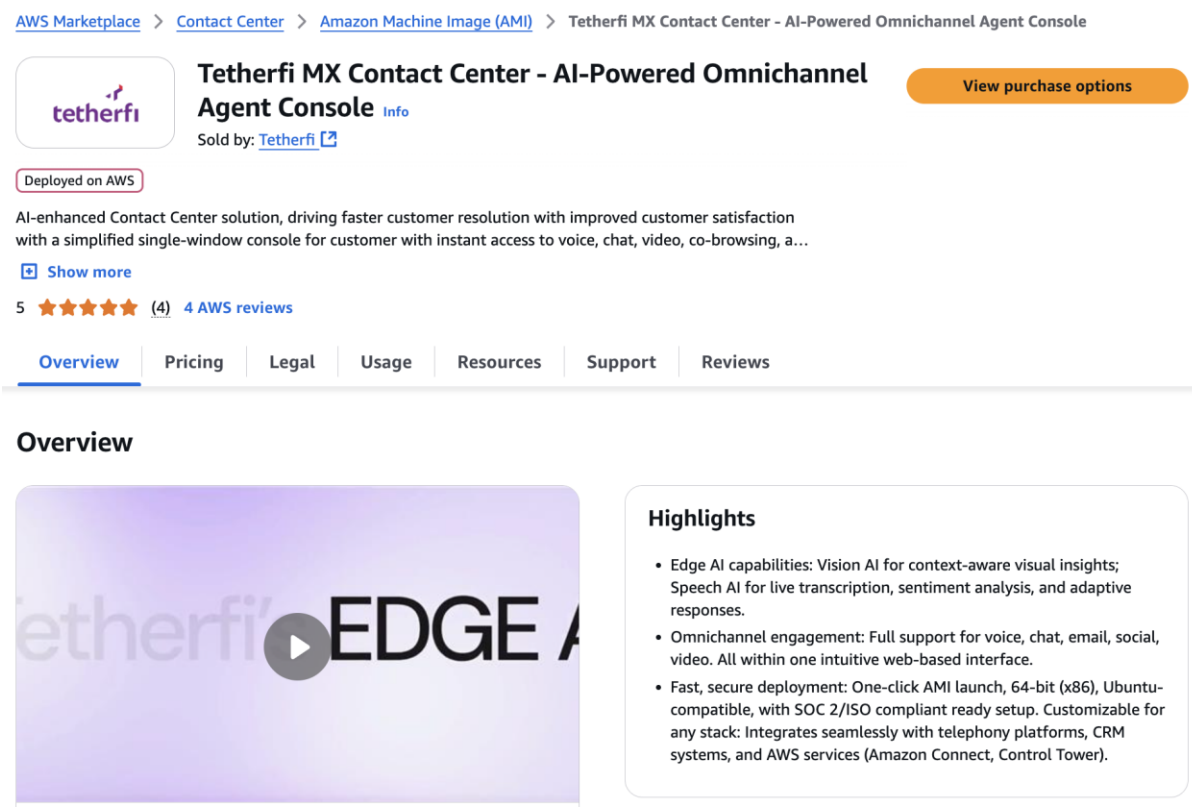


Select the latest version TetherfiMXDcoker_<version>. (TetherfiMXDocker_3.0 for example).

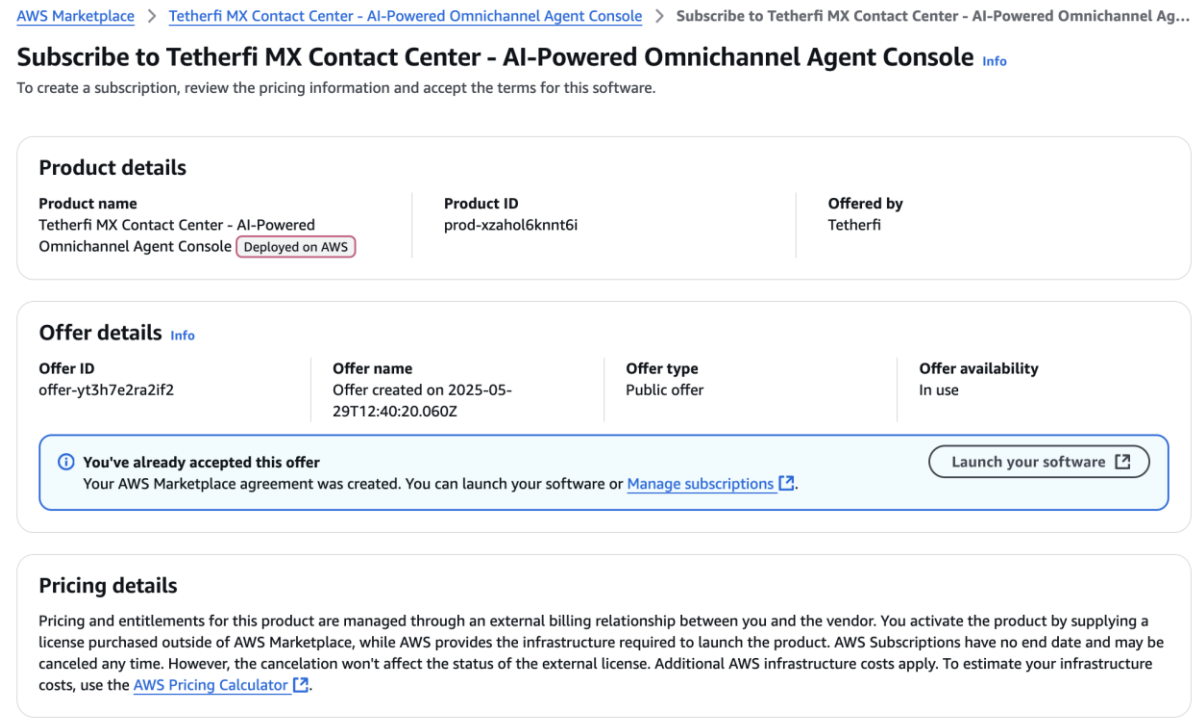
Or, directly go to [AWS Marketplace: Tetherfi MX Contact Center]

Subscribe to Tetherfi MX Contact Center

Click on “View purchase options.”



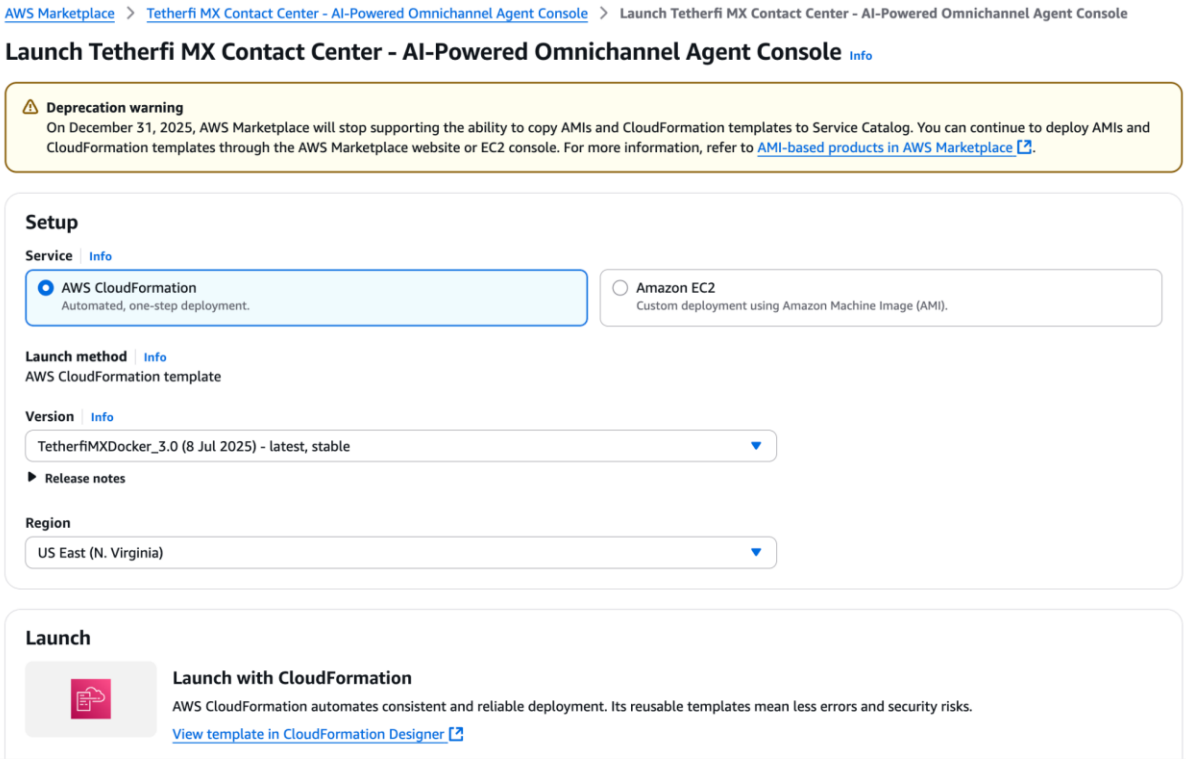
Click on “Subscribe” or “Launch Your Software” if you already have a subscription.



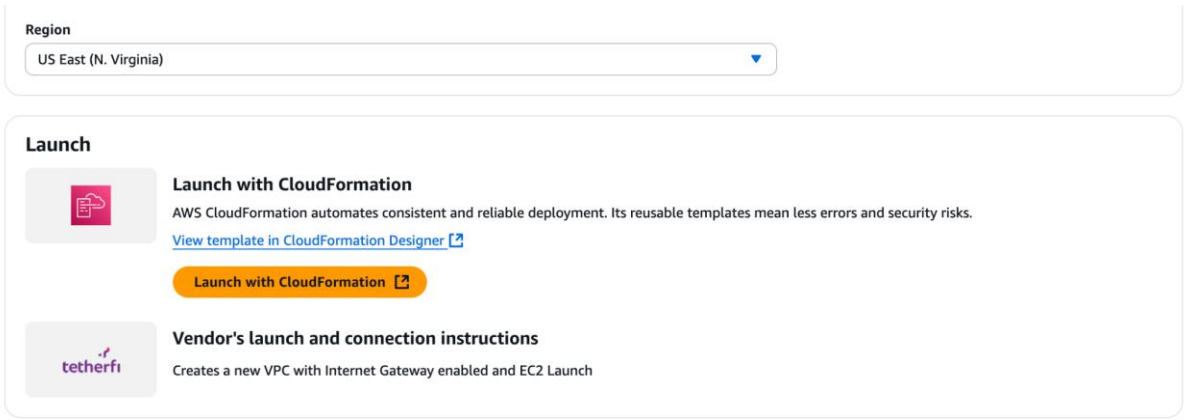
Select “CloudFormation Template” Option.

*Note: If you chose “**Amazon Machine Image**”, there are a **few manual steps** you have to perform later (Create VPC, subnet, security group, Internet Gateway, and Public IP assignment).*

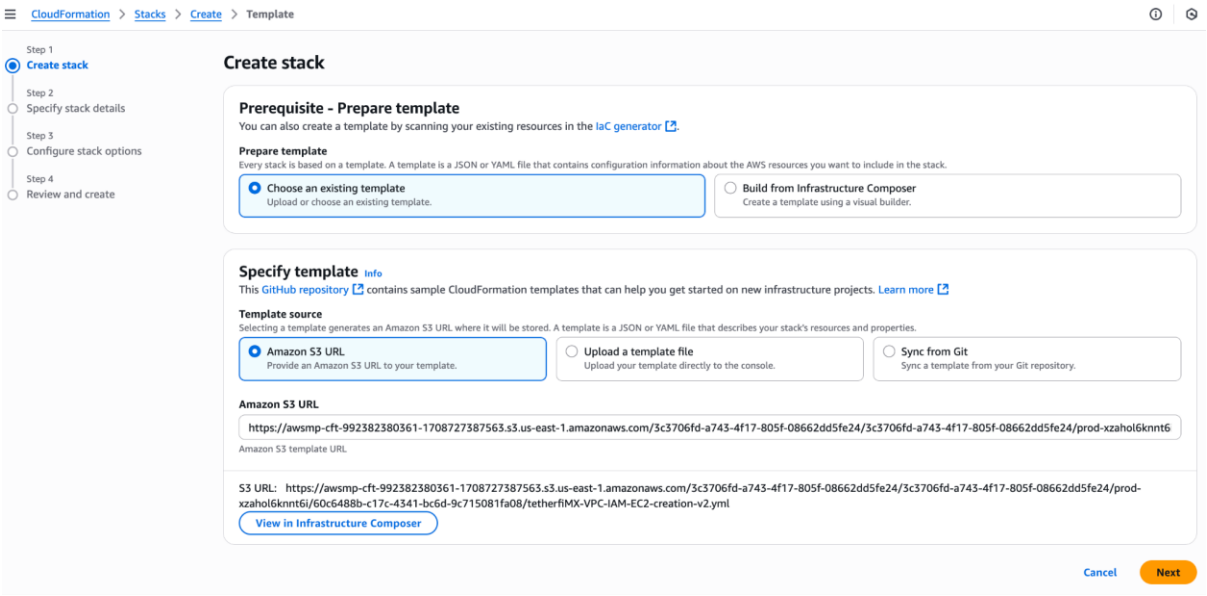
Select the Region and Version of deployment.



Select “Launch with Cloud Formation”.



You will be redirected to the CloudFormation stack page. Click “Next”.



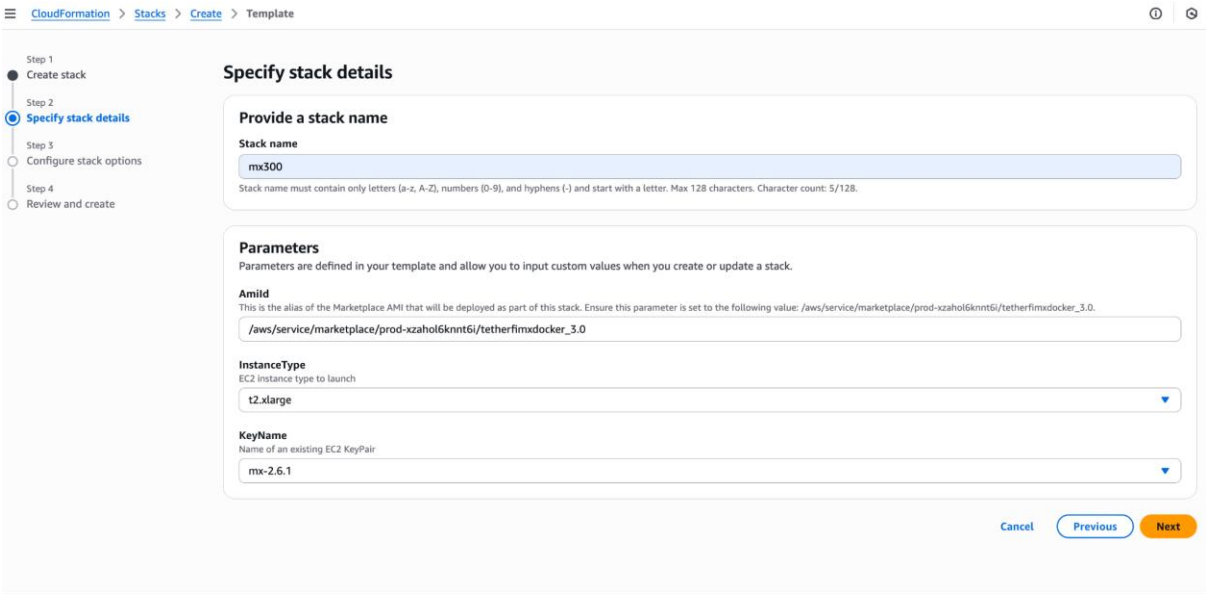
Enter a “stack name”.

Select a KeyName.

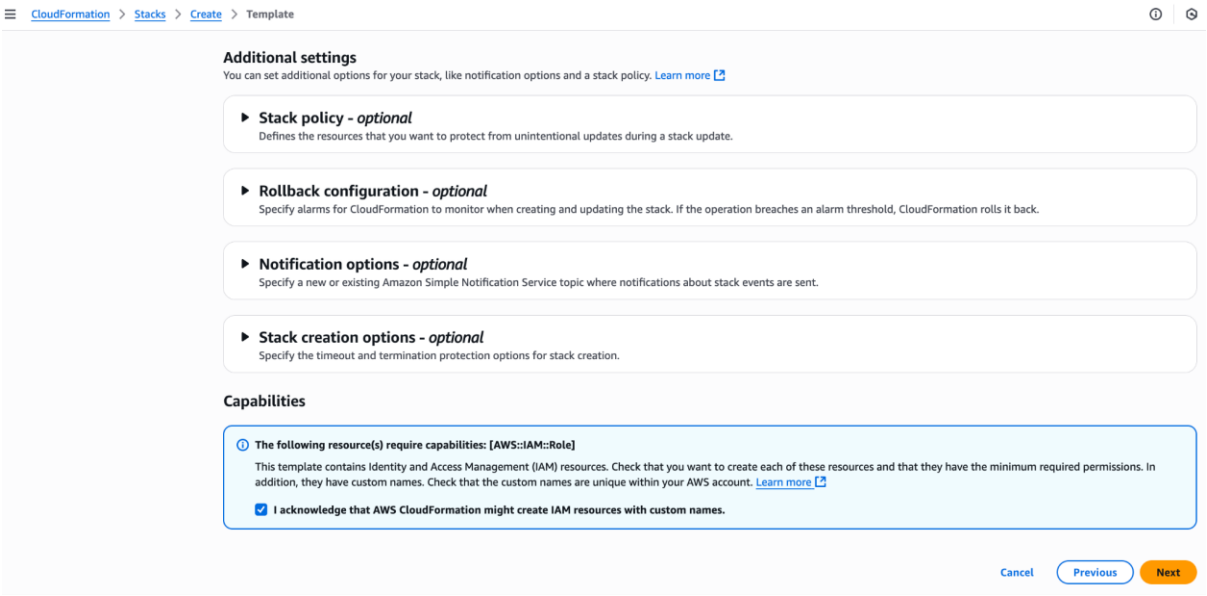
If you do not have a key name here, you can go to the EC2 Network and Security section and create a new key.

Note: Select a key pair to access your EC2. If you do not have a key pair, you can create one first. Do not change the AmiID. You can change the Instance Type as per your requirement. See the Recommendations section for more details on capacity.

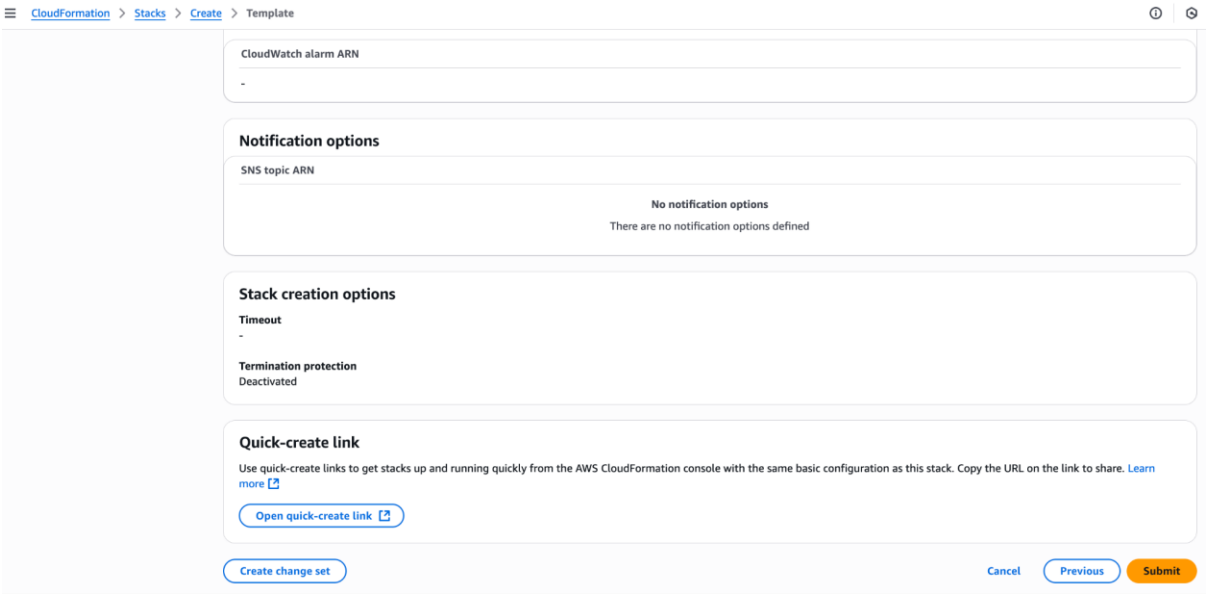
And click “Next”.



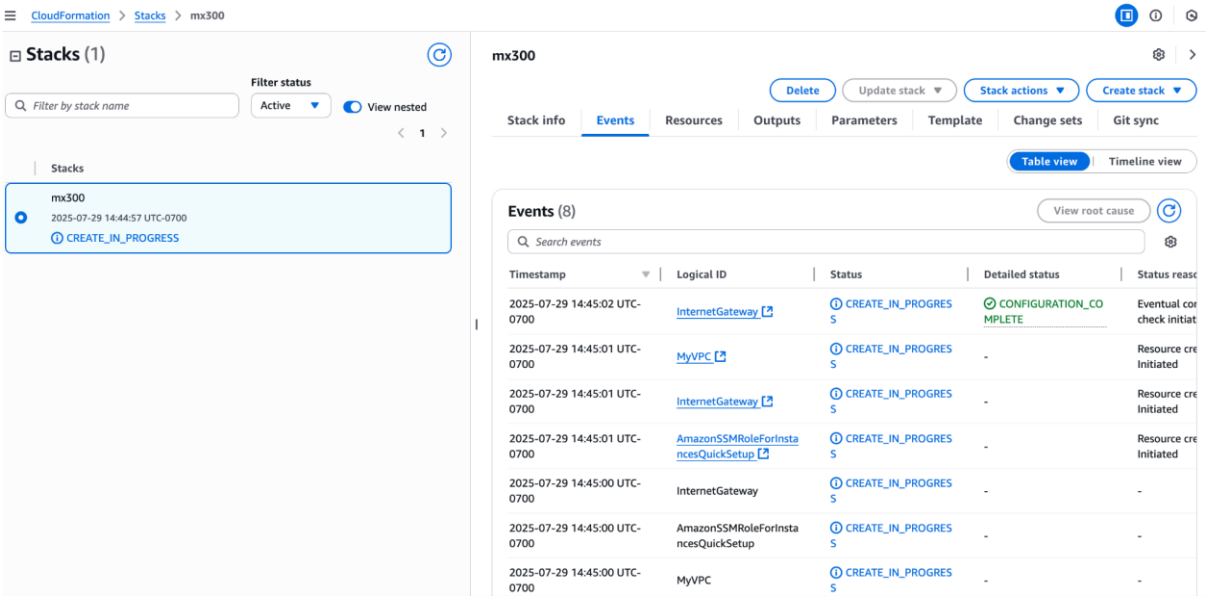
Tick the acknowledgement checkbox and click “Next”.

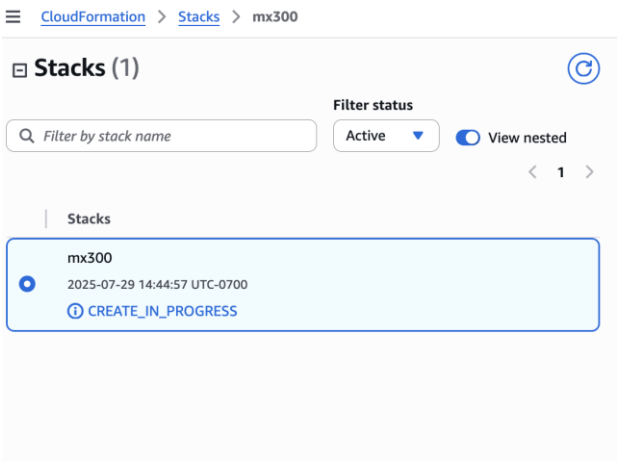


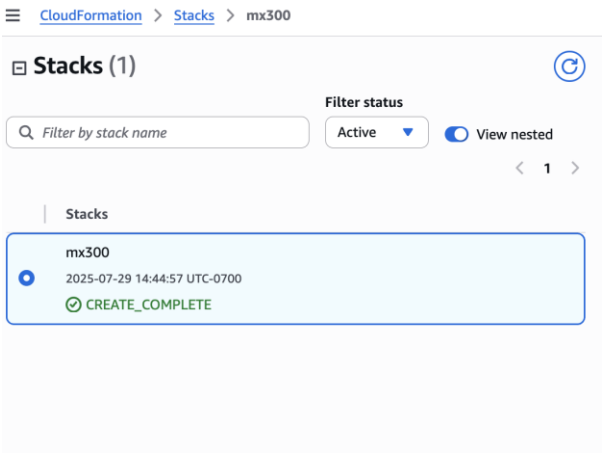
Click “Submit”.



You can now see the progress of the CloudFormation.







Once you see “**CREATE_COMPLETE**” state for the cloud formation stack and the EC2 instance has been created, you can proceed to log in to the EC2 instance. If you want to access the EC2 via SSH, you have to enable the SSH port in the security group. And you can use the key pair you created.

Starting the Application

After the EC2 instance is created, wait for at least 15 minutes for it to create all the required applications.

- You can log in to the EC2 console and try the following command:
  docker ps --format "{{.Names}}"|wc -l

This will give the number of containers started. You should see at least 50 containers.

- You can see the application installation progress in
  '/usr/scripts/logs/script_log_yyyyDDmm_HHmmss.txt' file.

When you see "All containers started", it means the application is ready to be used.
Once the EC2 is up, you can proceed to complete the manual configurations as follows.

Assigning Static IP

The CloudFormation template above will assign a dynamic public IP to the EC2 instance. Later, if you assign an Elastic / Static IP to the EC2 machine, please make sure you restart the EC2 instance so that the application will update the configurations accordingly.

Manual Configurations

Log in to the EC2 instance using SSH.

Configure SIP Trunk

A SIP trunk should be created between Tetherfi MX (Media Server) and your SIP PBX (such as Avaya CM/SM, FreeSwitch, Asterisk PBX, etc) to handle IVR calls, Agent Incoming and Outgoing calls on Web Phones.
To configure this SIP trunk,

- Open, /home/ubuntu/mediaserver/etc/WebRTCServer.conf
- Go to the "Voip" section
- Configure the far-end address (IP, port) of the SIP trunk under "trunk_details" --> "trunks" –> "address", and "port".
- Configure the hotline number or the DNIS for IVR in "Ivr" –> "ForwardingRule". Do not keep this empty. That will cause all outbound calls from Agent Desktop to be routed to the IVR Engine.
- Run "systemctl stop mediaserver"
- Wait for 60 seconds
- Run "systemctl start mediaserver"
- Go to "/tetherfi"
- Run "docker stop tmacserver"
- Run "docker compose up -d tmacserver"

Licensing

The solution comes with a 30 day trail license. During these 30 days, you have to raise a license request to Tetherfi via “support@tetherfi.com”. Please make sure you share below details:

- Organization
- Contact Person
- Contact Number
- Contact Email
- Licensing Requirement
- Number of concurrent agents
- EC2 instance id

Support

During the installation, configuration, or usage, if you face any issues, you can contact Tetherfi support via “support@tetherfi.com”. Please include “AWS Marketplace” in the subject for better routing. Please include below details in the email:

- Organization
- Contact Person
- Contact Number
- Contact Email
- Licensing Requirement
- Number of concurrent agents
- EC2 instance id

User Manual

Login to Open LDAP

- You can log in to the **OpenLDAP** using the credentials below.
  Url: https://<publicip>/phpldapadmin/
  User: cn=admin, dc=openldap,dc=test,dc=com
  Pass: T3th3rf!@dmin

Once you log in, you can create or change users.

Log in to OCM

- Log in to OCMUI using http://public-ip/ocmui/
- Use the default credentials below
  - Username: swfhdevops
  - Password: tetherfi
  - You can change these credentials in the Open LDAP Admin page

Create Agents

The system comes with 5 default users who are supervisors. You can create additional agents as per your requirements in the “User Onboarding Module.”
Please note that agent 50004 has been assigned as the Chatbot agent, so please do not remove or disable agent 50004.

Create Skills

The system comes with a few skills, and one of them is assigned to the Chatbot. You can add more skills in the “SkillConfiguration” module.

Assign Skills to Agents

Open the “Agent Skill Assignment” module. The “Administrator” user has all the skills.
Select the agent you want to assign skills to.
Assign relevant skills.

Chat Self-Service (visual-ivr)

- To configure the Chat Self Service, log in to OCM, go to the “*App*” tab, and select “*Interaction Workflow Chat*”
- Open “Tetherfi” flow and configure it according to your needs.
- Now you can open the visual-ivr (or chatbot) UI
    - https://public-ip/visual-ivr
- You can select “*AgentTransfer*” to route to the agent

Agent Desktop - Chat, Audio, Video

Once the chat self-service is over, the chat can be transferred to a live agent using an “agent” node in IW Chat UI.
Agent Desktop will receive this chat, and customers and agents can use text and multimedia messages to share information.

- Open the agent desktop on https://public-ip/agent-desktop
- Log in to the agent who has the chat skills.
    - Note: If you want to handle voice calls as well, during login, select Webphone mode and provide any number as the extension
- Change agent status to “Available”
- You will receive the chat that was initiated from the visual-ivr in the above section
- Answer the chat
- During a text chat interaction between agent and customer, either party can escalate the interaction to an “audio” or a “video” call. While on an “audio” or “video” call, either party can start screen sharing.

IVR

In your PBX, you have already configured a SIP trunk. In your PBX routing, you can route the IVR calls to the Tetherfi MX Media Server. The DNIS (the called number, 90000 for instance) should be configured in the Interaction Workflow (IW IVR).

- Open IW UI IVR in OCM (Apps tab)
- You can either create a new IVR flow or edit the preconfigured flow for your needs.
- Enter 9000 in the DNIS box and press the search icon
- You will see a flow named “USA”
- Click on the “preview” icon
- Change to “edit” mode.
- You have to remove the existing WAV files and upload your WAV files
- Update the “agent” nodes to route to the above skills you have created (49200, for example) - this can be done in the “intent master”
- Now you can modify the flow as per your requirements and save it.

Once you have configured the IW flow, you can dial the DNIS and listen to the IVR.
Note: Please ensure you have already changed the “ForwardingRule” in Media Server configuration.

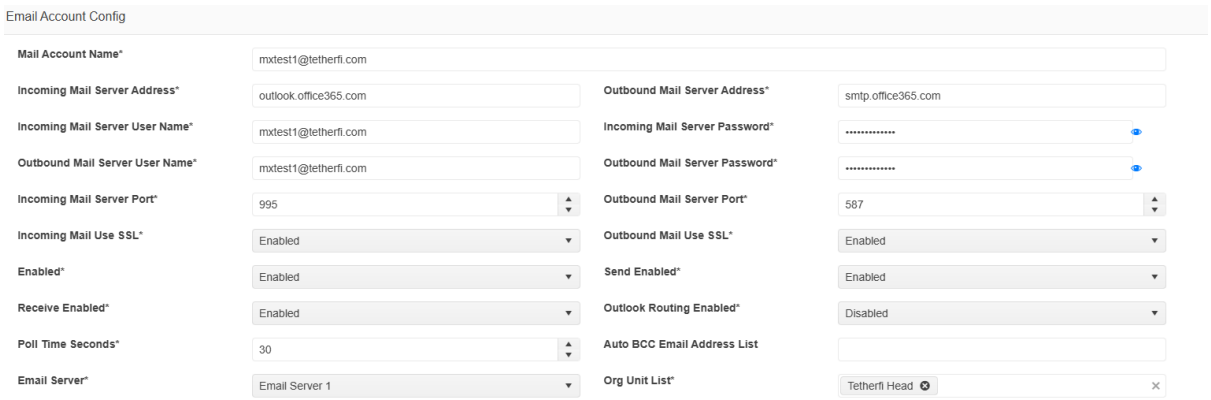
Agent Desktop - Voice Calls

- Open the agent desktop on https://public-ip/agent-desktop
- Log in to the agent who has the voice skills.
- During login, select Webphone mode and provide any number as the extension.

Email Channel

To configure the email channel, you can open the OCM Module “Email Account Config”.
After that, you can open the IW UI for email in the OCM App section.
And then configure your email address in the TetherfiHelpDesk flow.

If you are using SMTP and a POP3 mailbox, you can configure the mailbox as below.



*If you are using a **Microsoft Exchange email account***, you have to use **EWS with OAuth**.

- **Mail Account Name**
  - email address
- **Incoming Mail Server Address**
  - EWSOAuth-https://outlook.office365.com/ews/exchange.asmx
- **Incoming Mail Server User Name**
  - emailaddress; https://outlook.office365.com/.default;ClientID;TenantID;30
  - You can obtain the clientId (AppID) and TenantID (AppOwner TenantId) from Exchange
- **Outbound Mail Server User Name**
  - emailaddress; https://outlook.office365.com/.default;ClientID;TenantID
  - You can obtain the clientId (AppID) and TenantID (AppOwner TenantId) from Exchange
- **Incoming Mail Server Port**
  - 443
- **Incoming Mail Use SSL**
  - Enabled
- **Outbound Mail Server Address**
  - EWSOAuth; https://outlook.office365.com/ews/exchange.asmx
- **Incoming Mail Server Password**
  - Client Secret
- **Outbound Mail Server Password**
  - Client Secret
- **Outbound Mail Server Port**
  - 443
- **Outbound Mail Use SSL**
  - Enabled