CommunityWFM

Integration Specification TCN

For CommunityWFM Software Version 5.x+

February 2025

3400 Waterview Parkway, Suite 325
Richardson, Texas 75080

phone 877-668-6870
web CommunityWFM.com

Table of Contents

About this Document

The objective of this document is to outline the method and details of the CommunityWFM integration to TCN. The document assumes that the reader has some basic understanding of TCN and the credentials required to connect to TCN. TCN's REST API and TCN's ability to FTP a file to the CommunityWFM server will be utilized in retrieving information from TCN.

CommunityWFM and TCN Integration

Community integrates with TCN cloud contact center solution with the TCN API and is dependent on TCN to FTP the call volume data to a directory on the CommunityWFM server every 15 minutes. TCN will meet data collection requirements to fully integrate the CommunityWFM application with the TCN platform. The adapter retrieves agent states, call volume history, agent importing and skill importing.

Customer must provide the base URL of their instance of the TCN API.

For example: https://api.tcnp3.com/backoffice/

Customer needs to create a service account user in their TCN system and provide CommunityWFM with an Access Token created for that user. (See attached TCN Partnership Access Token Management.)

Historical Data Collection

CommunityWFM collects historical contact volume data from TCN by reading the call volume file that TCN sends via FTP on a 15-minute interval. The Community Historical Data Collection Service (a .NET Windows service) executes the call for each defined data collection point every 15 minutes and loads the results into vendor-neutral tables inside the Community product database.

Below is the configuration information needed for setting up the historical collection from TCN.

Historical contact volume data collection

Historical contact volume data collection

Base URL:	TCN's backoffice URL
Access Token:	Customer supplied Token
Path to Files:	Path to where FTP file is transferred

Agent State Transaction Data Collection

Community collects agent state transactions from TCN to compare against schedule intervals to provide agent schedule adherence reporting. The Community Adherence Collection Service (a .NET Windows service) executes the query on a user-defined interval (TCN this interval is set to 15 minutes) and loads the results into vendor-neutral tables inside the Community product database.

Below is the required information needed to be able to receive that real-time data stream.

Real-time adherence integration

Base URL:	TCN's backoffice URL
Access Token:	Customer supplied Token
Transaction Collection Interval (minutes):	15

Importing Configuration Data

CommunityWFM supports the ability to import agents directly from the TCN instance via the TCN REST API calls.

Partnership Access Token Management: Now a Client Responsibility

Your Partner currently has access to your TCN account via Access Tokens which will need to be renewed yearly ***by the account owners*** *or service will be interrupted.*

Access tokens provide users with the ability to interact with the TCN platform by making Application Programming Interface (API) calls. These tokens act as secure credentials that authenticate the user and verify their permissions.

Access tokens function like a combination of a username and password, so they must be kept confidential.

Access tokens issued by TCN are valid for one year. Once a token expires, it can be renewed by account owners or users with the appropriate permissions if continued access is needed.

It is important that you never change the access token but renew the existing credentials.

This expiration date enhances security by reducing the risk of unauthorized access. It also ensures that access is actively managed, requiring regular maintenance and periodic reviews to verify who should maintain access to the system.

3RD PARTIES (PARTNERS) SHOULD NOT MANAGE ACCESS TOKENS

Clients who work with third-party partners may need to grant access to certain users on their account. However, these partners should not be given the same level of control as Account Owners. Specifically, they should not have the ability to view, create, or manage access tokens.

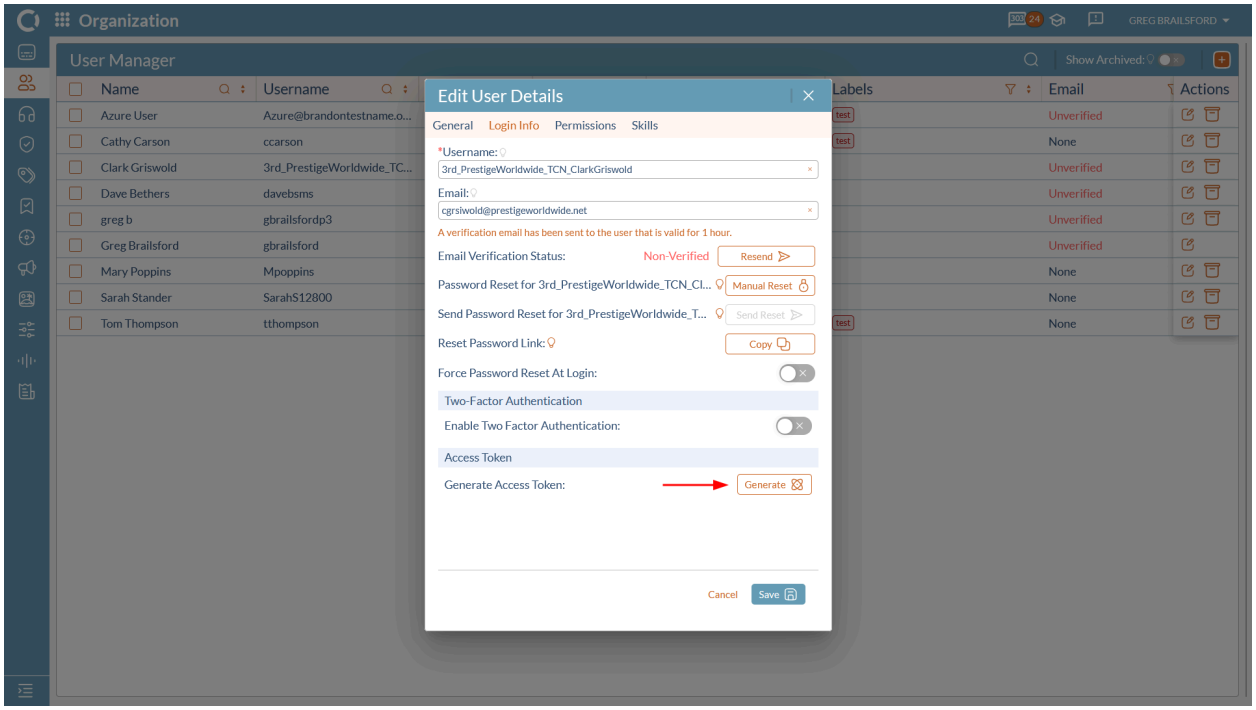
As your business expands to include multiple channels or portfolios, you can create new users.

When creating new logins for partners follow the following naming convention to provide clarity and make it easier to audit.

3rd_PartnerName_OrgName_UserName

- **3rd:** Identifies the user as a third party.
- **PartnerName:** The name of the partner.
- **OrgName:** The name of the Organization in Operator.
- **UserName:** Name of the individual user within the partner organization.

Once a user is created, Account Owners can go to Organization > Users > User Manager, select the user by clicking Edit, and generate a new access token. The new token can then be securely shared with the partner.



EXPIRATION NOTIFICATIONS

To ensure uninterrupted service, access tokens must be renewed before they expire. They do not happen automatically. **It is the account owners responsibility to manage and ensure partners' access does not expire.**

To help prevent disruptions, TCN provides the following notification methods: Email, Room303, and Pop-up alerts.

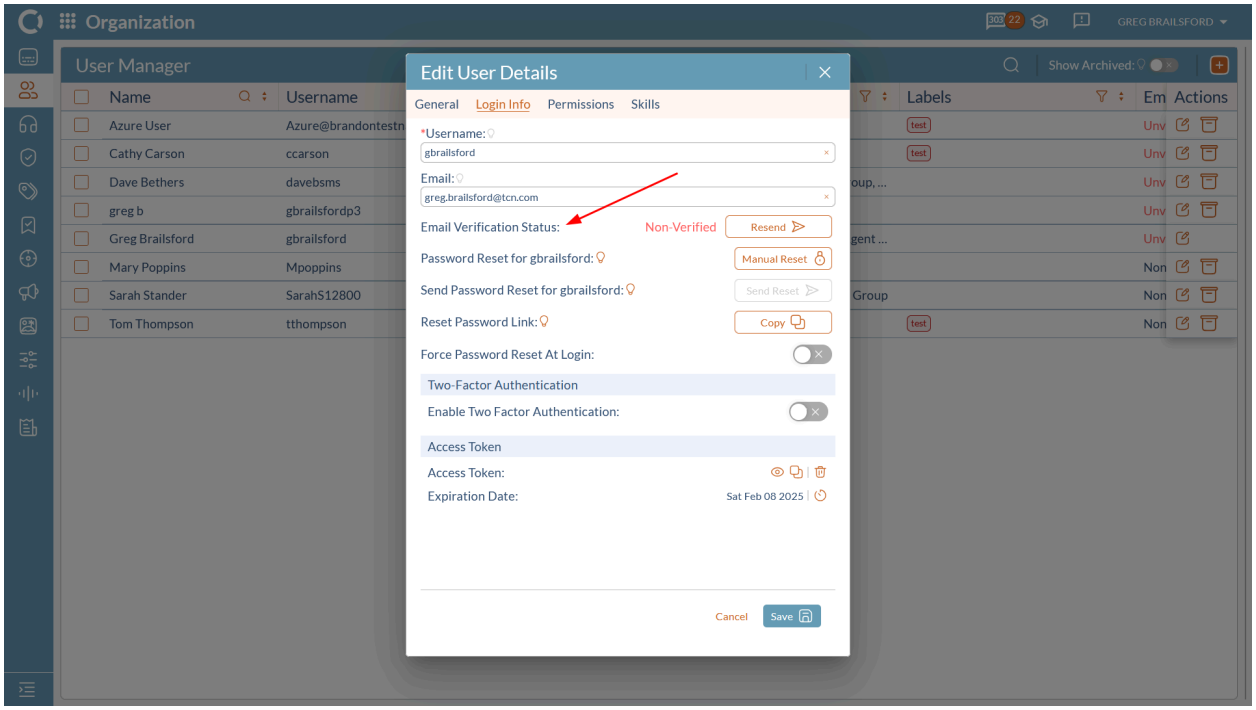
NOTIFICATION GROUPS

The following groups can receive notifications.

- **Individual users:** Receive notifications on any tokens created on their login.
- **Account Owners:** Receive lists of all the users in their organization who have access tokens expiring.
- **Subscription lists:** A manually created custom mailing lists configured under Subscriptions in TCN. They are used to create notification groups for individuals who don't have a user on TCN but still need to be notified about access token expiring.
- **Organization Dashboard:** A new widget on the Organization Dashboard will display users with expiring tokens.

Emails to individual users and account owners will only be sent to **verified** email addresses! To verify an email, TCN sends a confirmation email with a link. The user must click the link to confirm they have access to the email account.

Verification emails can be sent via Organization > User Management > Login Info.



NOTIFICATION FREQUENCY

Notifications of expiring tokens are sent 90 days before expiration, 60 days, 30 days, weekly (3rd to last week), daily (last 2-weeks). Pop-up notifications occur daily when logging in the last 2-weeks.

ADVANCED EMAIL CONSIDERATIONS

- Within the same organization, an email address must be unique and cannot be shared by multiple users.
- A single email address can be associated with different users across multiple organizations.
- Don't use generic or group email addresses when creating users to ensure accountability.

QUESTIONS AND SUPPORT

For questions or help creating users and verifying email addresses you can contact your TCN account manager at 800.745.1900