Community Deployment Guide

API Authentication

For Community Software Version 4.3+

Revision 1.1

July 20, 2020

CommunityWFM

phone 877-668-6870
web CommunityWFM.com

3400 Waterview Parkway, Suite 101
Richardson, Texas 75080

API Modifications

The CommunityWebAPI, a Restful service requires authentication by default to prevent unauthorized access to the data behind the service. To access any gated entry points, clients must first authenticate to the API service and submit an authorization header using the process described below. All entry points, with the exception of the version checker, are gated.

Authenticating to the API service

In order to authenticate, clients must make a POST call to AuthenticateEx method with a single parameter "l" (lowercase "L") and a value of (username)|(password). That is, the name of the user pipe-delimited with the user's password.

The AuthenticateEx method will validate the user's identity and password and load the user's info if validated. If the credentials passed are not valid, the service throws an exception and returns the appropriate message to the client.

When successful, the authentication method does a soft-login of the user and retrieves pertinent information to create an authorization token. The service returns this authorization token and additional required user attributes to the client via a JSON object with the following attributes.

JSON object attributes:

agentId (int) is the primary key for the row in the t_agent table for the specified user

userRole (int) is the role id associated with the user (100 = agent, 200 = supervisor, 300 = scheduler, 400 = administrator, 1000 = superuser)

userName (string) is the full name (Last Name, First Name Middle Initial) associated with the user

timeZone (int) is the time zone associated with the user; either specifically assigned to that user or defaulted from the assigned site / enterprise activity

language (string) is not currently implemented

authToken (string) is an encrypted / encoded string that provides the authorization to future calls. This is described below.

Subsequent method invocation

The client must retain the value of the authToken member and supply that to subsequent calls to the API service in an HTTP header named “WFMSGAPIKEY” for any gated entry points (again, nearly all so it is safer just to put it in all calls except AuthenticateEx). In addition, the API service will refresh the token and return it each time a client invokes a gated method. The API service methods will place a new value in a response HTTP header with the same name.

Note the default lifespan of any API authorization token is 20 minutes.