Enterprise - Setting up the Zipwhip Integration

Last Modified on 03/30/2020 7:58 am CDT

What is the Zipwhip Integration?

Zipwhip's texting-for-business integration allows you to text candidates and employers directly from TempWorks and automatically archive conversations to the relevant contact record.

Note This integration requires additional setup and an existing account with Zipwhip. For more information, please contact your TempWorks Account Manager.

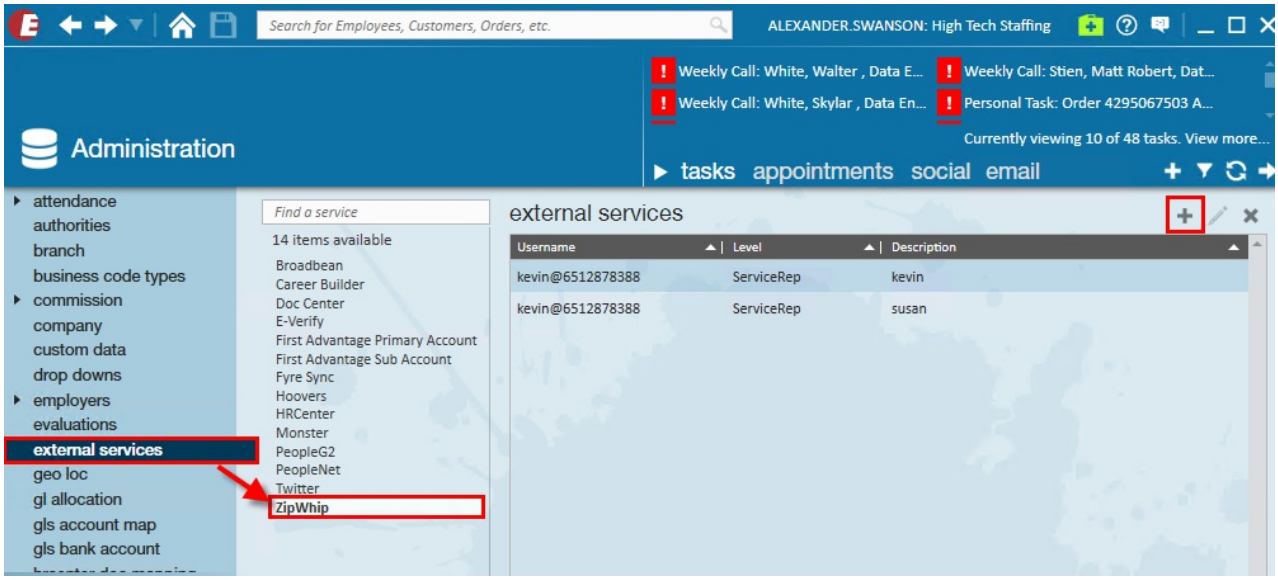
How to Setup the Zipwhip Integration in Enterprise

Note In order to utilize the Zipwhip Integration, users must be logged into apps.ontempworks.com.

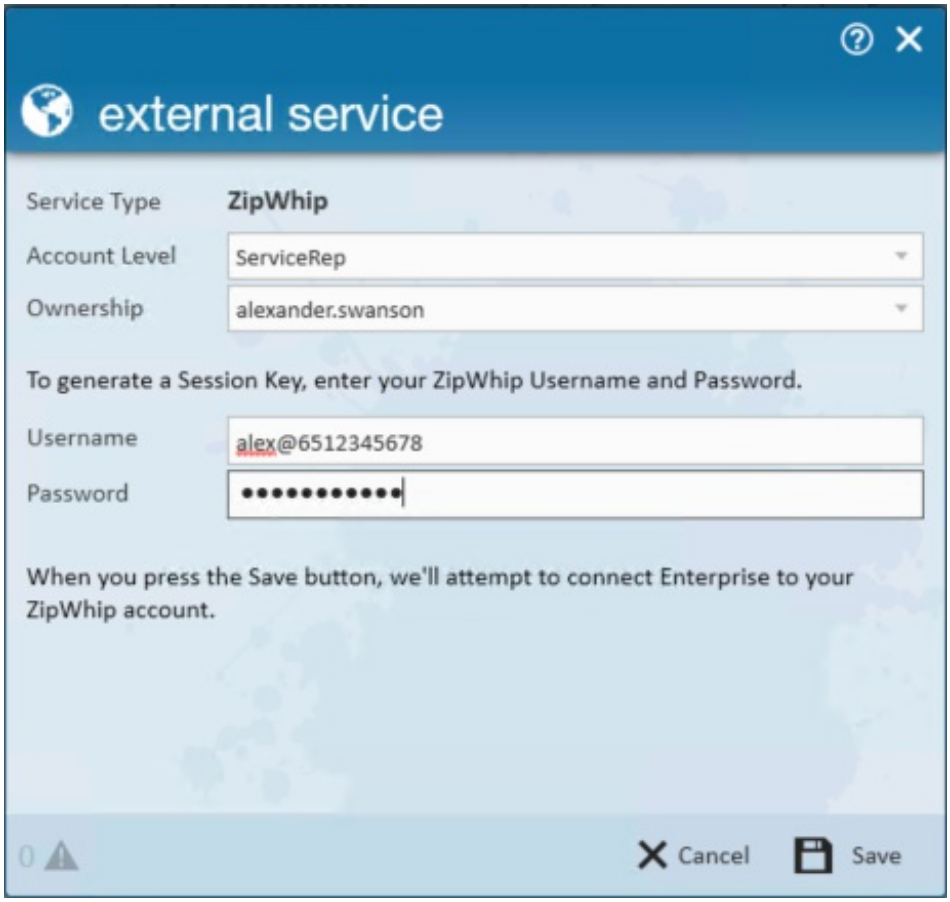
From Enterprise, navigate to All Options > Administration:

Once in the administration area, select the external services section and locate the Zipwhip integration.

Here, users can add credentials with the '+' icon. The type of credentials will be based on your contract with Zipwhip. The most common account types are 'per branch' and 'per user':



For 'per user' accounts, select 'ServiceRep' and then select the user that the credentials are to be assigned to. Input the user's Zipwhip credentials in the 'Username' and 'Password' fields, then select 'Save':



Note When entering in a username, it must include numerical digits only- no parenthesis , dashes, hyphens etc.

After saving these credentials, Zipwhip will be sent a communication key which will allow Enterprise and Zipwhip to communicate with each other.

User Security & Zipwhip

Once you have the integration set up, you will need to make sure your users have the correct permissions to be able to use the Zipwhip integration.

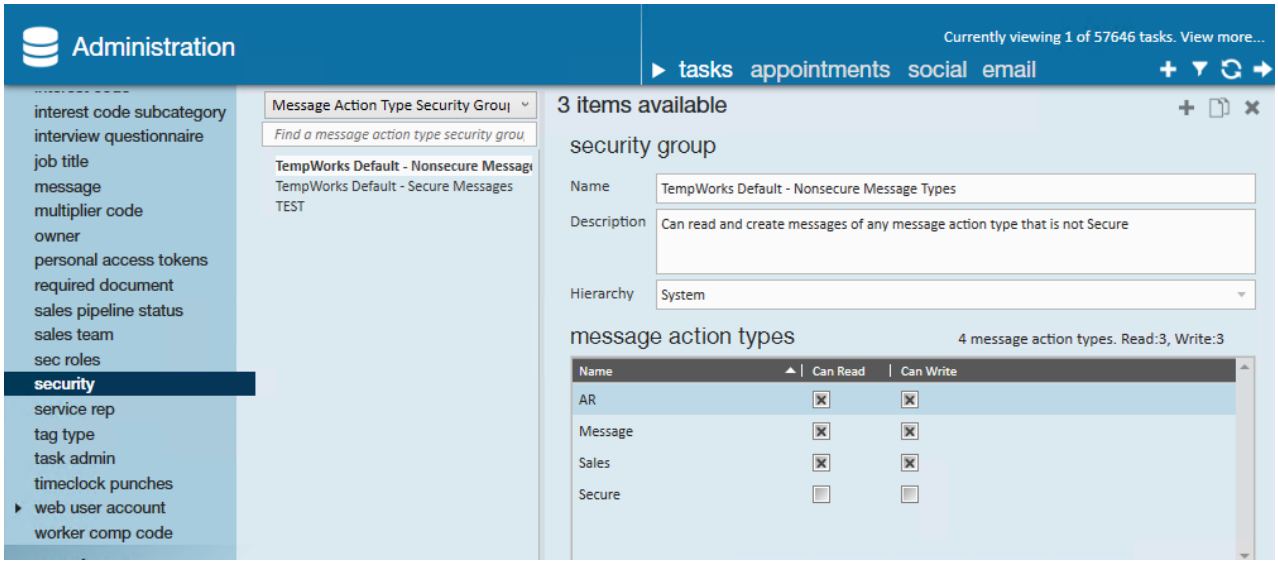
Sec Roles for Zipwhip

Each service rep that will be sending text messages in Enterprise will need to have a Sec Role that gives them the function permission to use Zipwhip. This varies from system to system and should be provided to you during the setup process with our team.

To learn more about Enterprise Security, check out Enterprise - Security Roles.

Security Groups for ZipWhip

Each service rep will need to belong to a security group that will allow nonsecure messages read/write. The reason for this is that Zipwhip utilizes the API to log messages in your system and API security is tied to Security groups. We'd recommend using the TempWorks Default - Nonsecure Message Types group.



To learn more about security groups, check out Enterprise - Security Group Administration.

Related Articles