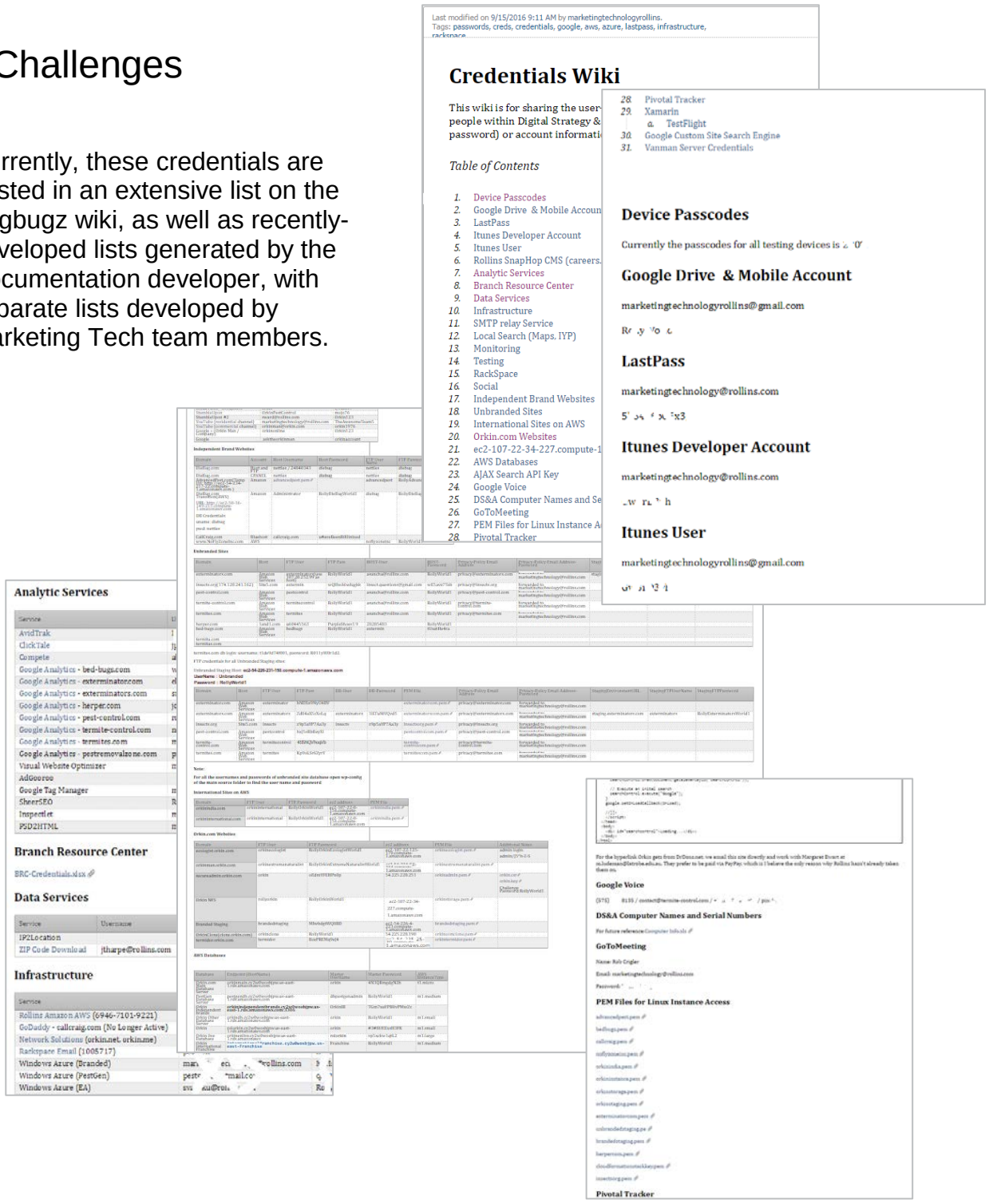
Proposed Marketing Credentials Management

The Rollins Marketing team would benefit from a secure, central storage area for credentials. These credentials are used by specific Marketing teams to access shared tools and to manage various social media accounts.

Current Challenges

Currently, these credentials are hosted in an extensive list on the Fogbugz wiki, as well as recently-developed lists generated by the Documentation developer, with separate lists developed by Marketing Tech team members.



This method is inefficient and ineffective, presenting the following risks and challenges:

- It is important to keep our credentials secure. An outside party, upon gaining access to these credentials, could compromise several of our systems, including social media accounts that represent Orkin to the public. This outside party could be a hacking expert but, more likely, an employee, former employee, or contractor.

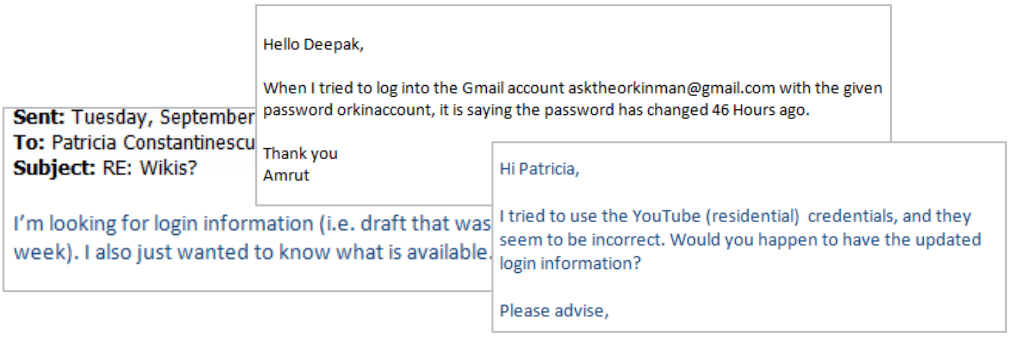
- Fogbugz is widely used by other departments in the Rollins organization, many of whom may have access to the Marketing division of Fogbugz.

- There seems to be no central administrator for the Fogbugz system, so no one is focused on removing former employees and contractors, and their login privileges, from the system. Because Fogbugz is cloud-based, one need not be on the Rollins network to access it.

- Because everyone in the Marketing Department has access to all credentials, all team members have the ability to change these credentials.

  Sometimes it is necessary to change the credentials, and team members do so in good faith. However, the updated credentials may not be communicated to the rest of the team.

  Team members are then locked out of accounts until the appropriate team member is located and the new credentials distributed appropriately.



- The credentials now exist in multiple documents, making it impossible to update all sources to reflect the accurate credentials.

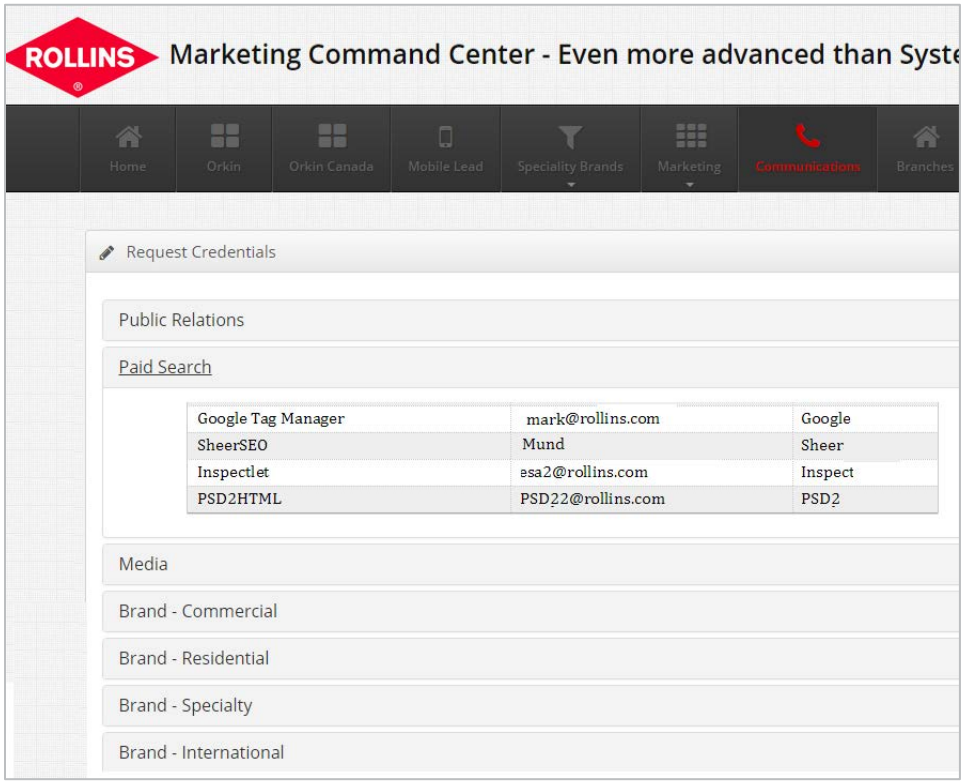
- The Documentation developer is now associated with these credentials, as the go-to person, in the minds of the Marketing team, yet does not have access to the information necessary to respond to inquiries from team members.

Proposed Solution

The following solution, implemented effectively, will streamline the management of Marketing credentials.

Marketing Command Center

Because the Marketing Technology Team controls access to the Marketing Command Center, it is a secure hosting solution. Access to the MCC requires Rollins-issued credentials; therefore, employees and contractors who leave the Rollins organization no longer have access to this tool.



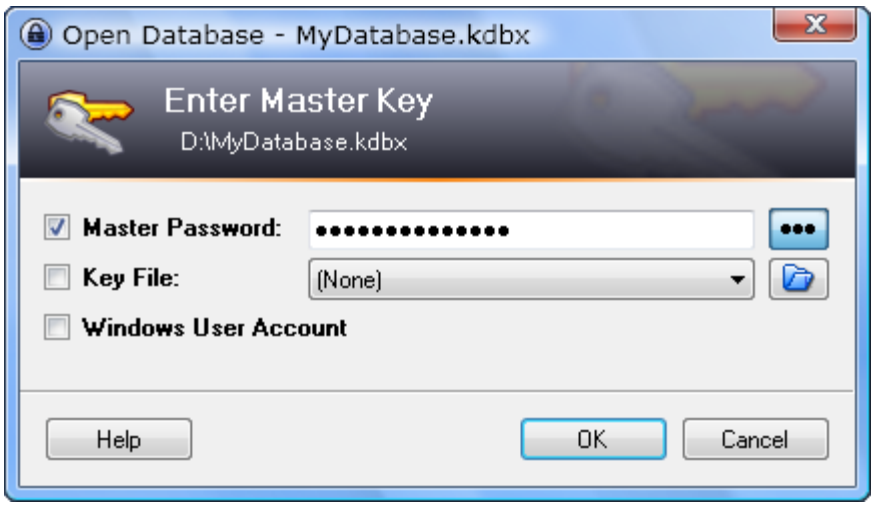
Business Owner Accountability

To ensure that the credentials are updated when changes are made, business owners can be assigned to manage the credentials specific to their team's needs.

The credentials system in the MCC should be separate from the Help Center. This ensures that the Marketing Technology team is not tasked with updating all credentials, and sets the expectation that business owners are responsible for managing the credentials.

Password Management Software

Password management software tools, such as LastPass or KeePass, are used to store and organize passwords. Password managers usually encrypt stored passwords, requiring the user to create a master password: a single, ideally very strong password which grants the user access to their entire password database.



Many password managers include features that can inspire best practices. These features highlight problematic practices such as duplicate credentials and weak passwords.

Use of a password management tool should be considered.