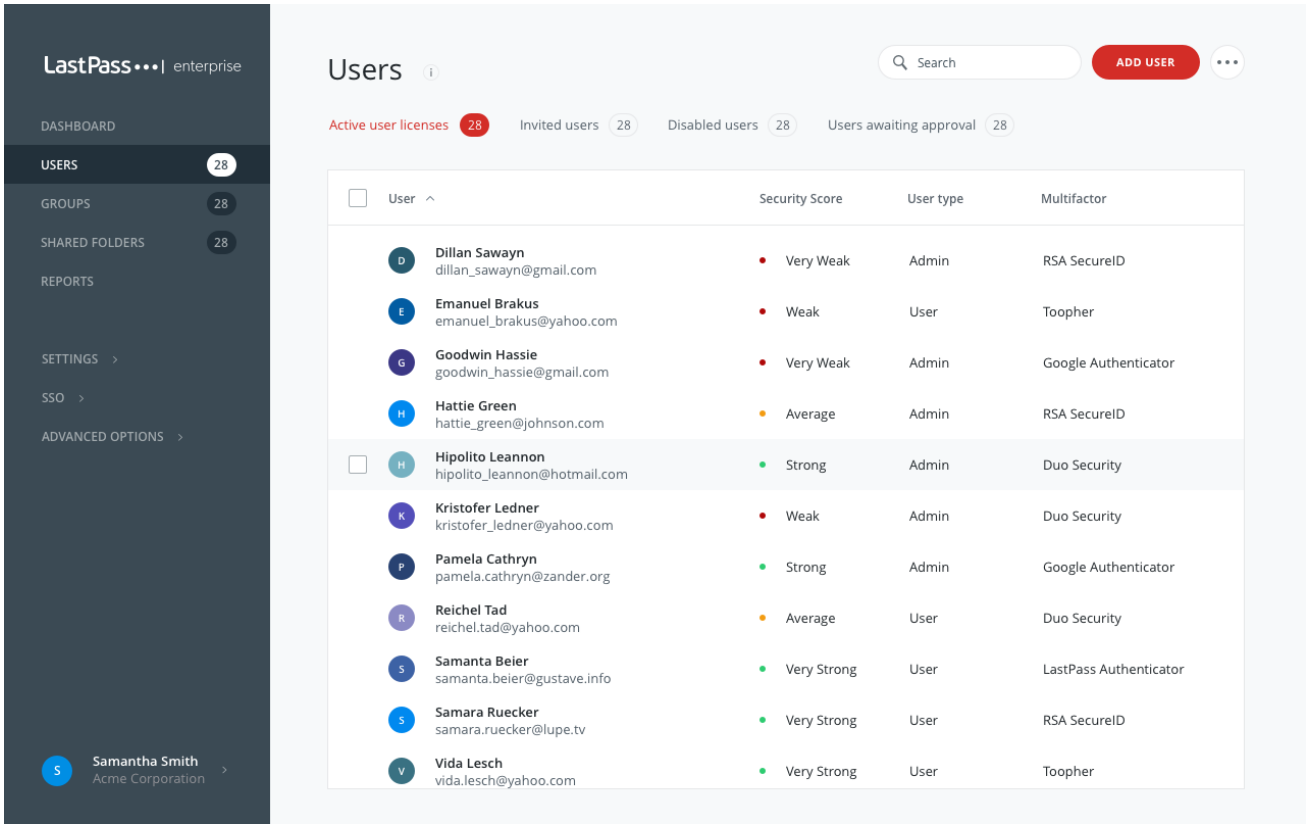
Users Sub-tab

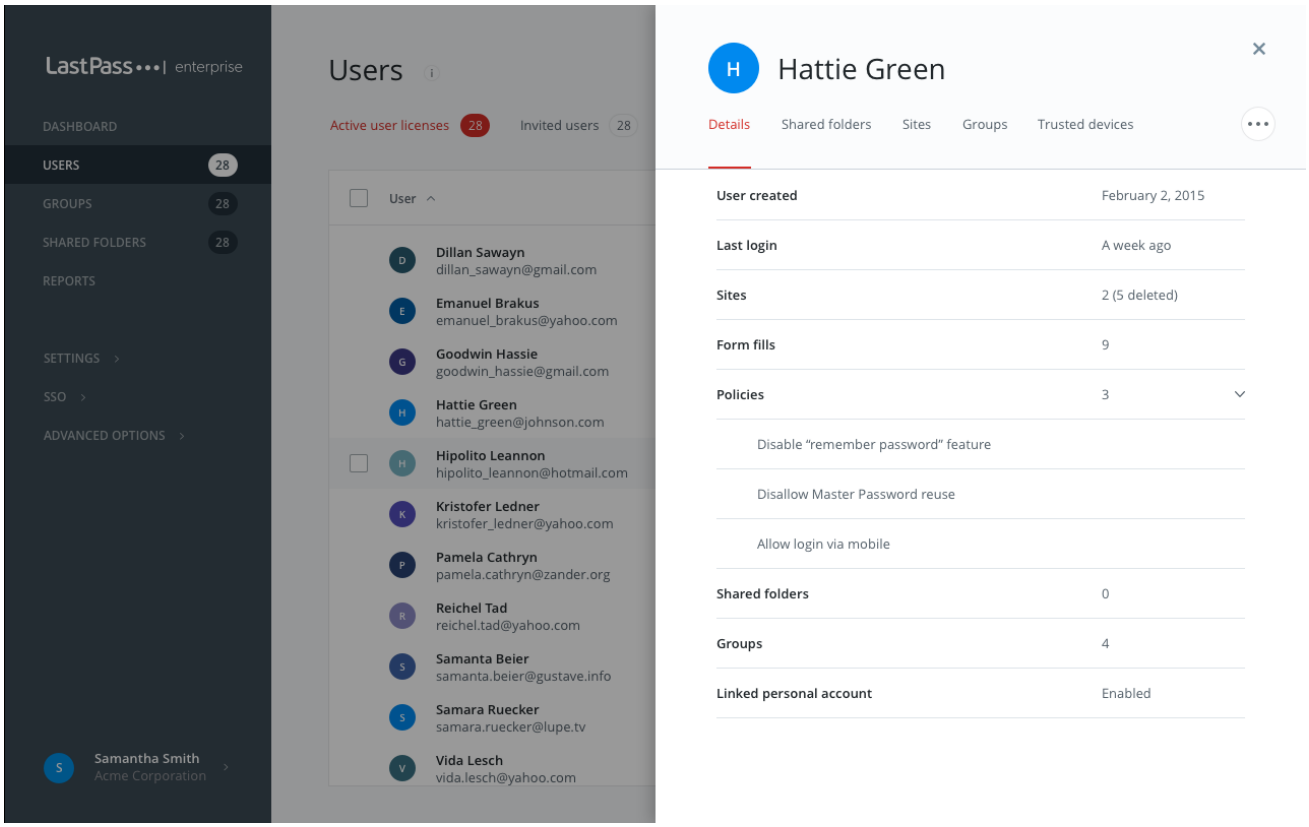
This tab provides you with a complete list of all LastPass accounts that have been provisioned under your enterprise, and several actions that can be taken on each:



Security Score – the security score is based on the score generated when the user runs the 'Security Challenge' from his/her vault. The score is only update and/or displayed when the Security Challenge is run.

User Details – this report offers a summary of the user's account including their general account information, security check score, policies they are subject to, shared folder access and groups they are apart of. You can click on several of these headings in order to see a detailed list pertaining to his/her account including all of the policies that are active on the account and any folders that have been shared or created by the user. Scroll to the bottom of the page and click 'Click to see sites' to see a full, read-

only list of all entries stored in the user's account.



Make or Remove Admin – you can promote any number of users to admin status and remove this status at any time. Granting Admin rights means that the individual will have full access to the Admin Console.

Require Password Reset – This will force the user to manually reset their master password. They will receive the notification to do this the next time the user logs in.

Destroy All Sessions – This will log the user out of all active sessions across all devices – Destroying All Sessions

Reset Password – This option will be available only if the 'Super Admin – Password Reset' policy is enabled and if the user is 'eligible' for reset. For more information, see the 'Super Admin – Password Reset' policy at the bottom of the Policies page.

Disable User – temporarily disable the user's account making it inaccessible to them but not deleting the account

entirely.

Delete User and **Remove User from Company:** At the bottom of the list you see ‘delete user’ or ‘remove user from company’. This is a decision that you should weigh carefully. ‘Delete user’ will delete that user’s account entirely. If the user has saved any personal logins or other data to their vault then they will no longer have access to that data. Some enterprises prefer the ‘Remove user from company’ option which will remove the user from your enterprise account, and will delete all Shared Folders from the user’s account. With this option, the user will continue to have access to his/her account as a standard LastPass user.

Whether a user account is deleted, disabled or removed from the Enterprise, this will in no way impact any remaining users. For example, if the departing employee was an administrator of several Shared Folders, these folders will remain 100% available and intact for all remaining users. That said, there is a possibility that the folder will be left with no Admin. To avoid this scenario, you might consider enabling the Super Admin – Shared Folders policy.

As a best practice and an added precaution, we suggest that any shared credentials be changed upon the exit of an employee regardless of how you choose to manage their exit from LastPass. These changes to any Shared Folder will automatically sync to all assigned users, and this will give you an added layer of security.

Disable Multifactor – This will disable all multifactor authentication services for this User’s account. If the policy “Prevent Multifactor Disable via Email” is enabled, this option will be the only way for multifactor to be disabled.

SuperAdmin Password Reset: If an Admin has been set as a

Super Admin Password Reset via policy, there will be option on this user actions dialog to change the password for that particular user. This change will be immediate and the Admin will be asked to create a new password for the account on the spot.

Edit Name – assign a nickname to the account that may be more recognizable to you than the user’s email address.