User-account is locked

How Accounts become locked

There are a number of reasons why a Swivel account may become locked. These relate to a number of different policies that are configurable on Swivel. See also Lockout Account How to guide

Failed Authentication Attempts
To mitigate against brute-force type attacks accounts will become locked after a given number of failed authentication attempts

PIN Expiry
It is possible to set a possible that forces a user to change their PIN every N days. A user can be warned that they are due to change their PIN. If the user does not act on these warnings, and they do not change their PIN in time, their account will become locked. Note that the a scheduled process runs within Swivel to check the status of accounts and lock them if required. If an account becomes locked because of PIN Expiry and is unlocked via the admin console, if the user still does not change their PIN, their account will become locked again when the job runs again. For further information see PIN Expiry How to Guide

Inactive Account
It is possible to set a policy to lock any accounts that have been idle for a certain time. This makes it easy to identify dead-accounts, see Swivel Account Inactive

Change PIN after admin set Change PIN after first log in

It is possible to set a policy to require a user to change their PIN after it has been set by an administrator via the console or via Swivel at account creation. This is to ensure that only the user will know their PIN and that it is changed from the PIN detailed in any provisioning email. If these policies are set then the user can only use that PIN once and must change it before attempting to authenticate with it a second time. If the user does not change their PIN their account will become locked. For further information see the ChangePIN How to Guide.

Related Links

How to Unlock

Lockout Account How to guide