Enhanced Password Synchronization with Identity Governance & Intelligence

Highlights

- *Self-password recovery via IGI user interface or Windows logon screen*
- *Password change via browser or mobile app*
- *Password synchronization with grouping*
- *Reverse password sync plugin for Active Directory*

Passwords are just one of many forms of authentication and it's important to supplement traditional passwords with second factors. Even still, passwords act a primary layer of defense. Strong password management is critical, especially as the balance between security and convenience evolves. No matter where you are on this authentication journey, IBM Security Identity Governance & Intelligence (IGI) can provide you with full coverage of password management, ensuring that the end user experience is better and more secure.

Password Synchronization
With IGI, you'll be able to select applications for synchronization through Password Synch Group. This refers to the process through which a user maintains a single password across multiple applications, thus cutting down on the number of passwords to remember. If you have several applications, there may be conflicting password policies. For example, one policy might require a maximum password length of six characters, while another requires eight. With IGI, you can create multiple Password Synch Groups, so that within each group there are specific compatible password policies. Only when the password policy is compatible will the passwords be synchronized. Achieve one password across the applications of your choice for greater convenience. When you change your password through IGI, all connected endpoints will be synchronized.

Reverse Password Synchronization
IBM provides a plugin to support reverse password synchronization between Active Directory, (or other platforms), and IGI. This refers to the process where a password change on one of the target systems or applications is captured and used to synchronize all of the other account passwords for that user within the same Password Synch Group. The changed password event can be notified to IGI by a native password interceptor from Active Directory or via REST APIs from other platforms.

The Desktop Password Reset Assistant (DPRA)
DPRA enables Windows users to reset and change their Windows passwords from their desktops, using IGI password validation. After a user changes their password, they must wait until the request is complete in the IGI workflow before they can log in with the new password. If the user changes the password for an account that is part of a password sync group, the new password is synchronized with the user's other accounts that belong to the same password sync group.

For more information

To learn more about this offering, contact your IBM representative or IBM Business Partner.

IBM Security
75 Binney St
Cambridge, MA 02142

Produced in the United States of America
June 2018