DataMotion™

/SecureMail

/SolutionBrief

Single Sign-On (SSO) for SecureMail

Challenge: Too Many Login Passwords

With more and more products and services being hosted in the cloud, it is difficult for users to keep track of their multitude of user names and passwords. This can lead to frequent password reuse, or the use of simplistic passwords without appropriate ‘strength’.

Email encryption services often require authentification for their licensed users and recipients. While this process is effective at maintaining message security, it does add yet another password for users to remember.

Solution: Single Sign-On (SSO)

Single sign-on (SSO) provides the capability to authenticate once and be automatically authenticated when accessing additional systems. It eliminates the need to maintain unique login credentials for accessing individual applications and systems, increasing security and user satisfaction.

DataMotion SecureMail SSO

DataMotion SecureMail and the DataMotion SDX Platform now support SSO, representing another milestone in our mission to simplify the sender and recipient experience for email encryption and secure data exchange. SSO allows SecureMail users and their recipients to access their secure messages by logging into their Microsoft Office 365, Google, LinkedIn or Facebook accounts. For enterprise class deployments - corporate Identity Providers (IdPs) based on the widely supported OAuth2 protocol can be integrated to leverage private network credentials and client service portal logins, with Okta integration already provided.

Features and Benefits
Integrates with corporate IdPs based on OAuth2 protocol
Integrates with Microsoft Active Directory
Access secure messages using Microsoft Office 365, Google, LinkedIn or Facebook account login
Eliminates need for extra passwords and eases frustration
Automatic authentication increases security and user satisfaction

Microsoft Active Directory Integration

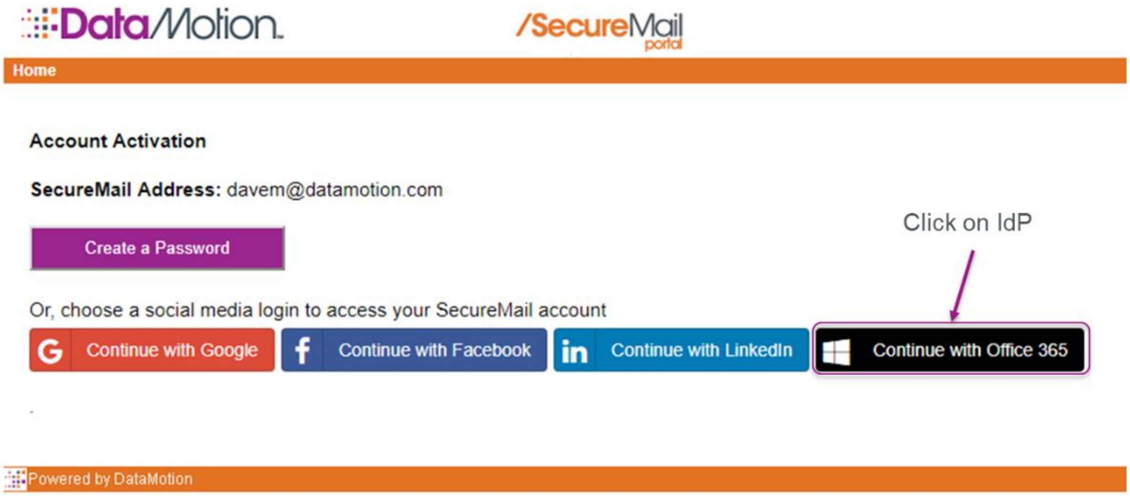
Many Office 365 implementations are integrated with the organization’s existing Active Directory (AD). The DataMotion SSO implementation leverages this capability, requiring users to be validated against their exisitng corporate credentials before being allowed access to their SecureMail account. Users that leave an organization will typically have their AD credentials disabled. Access to their organization’s SecureMail account will be automatically disabled as well, making SecureMail user management effortless for the administrator.

/SolutionBrief

How It Works

To access a user’s SecureMail account, the SecureMail portal presents them with a variety of login options ranging from username and password to one or more IdPs authorized by the SecureMail administrator.

When selecting an IdP method, the Secure Mail service invokes the IdP’s login screen to validate the user, and then grants access to the user/recipient SecureMail account.



Account Activation

SecureMail Address: davem@datamotion.com

Or, choose a social media login to access your SecureMail account

Figure 1: DataMotion SecureMail account activation login screen.

Solution Summary

When users reuse or create simple, ‘weak’ passwords, they decrease the security of all of their accounts. With single sign-on (SSO) for SecureMail, users can log into their SecureMail account using a variety of login options. Integration with corporate IdPs allows users to login with their existing corporate credentials, thus increasing security and user satisfaction.

For more information on SecureMail SSO, visit www.datamotion.com, or contact us at sales@datamotion.com.

www.datamotion.com 800-672-7233