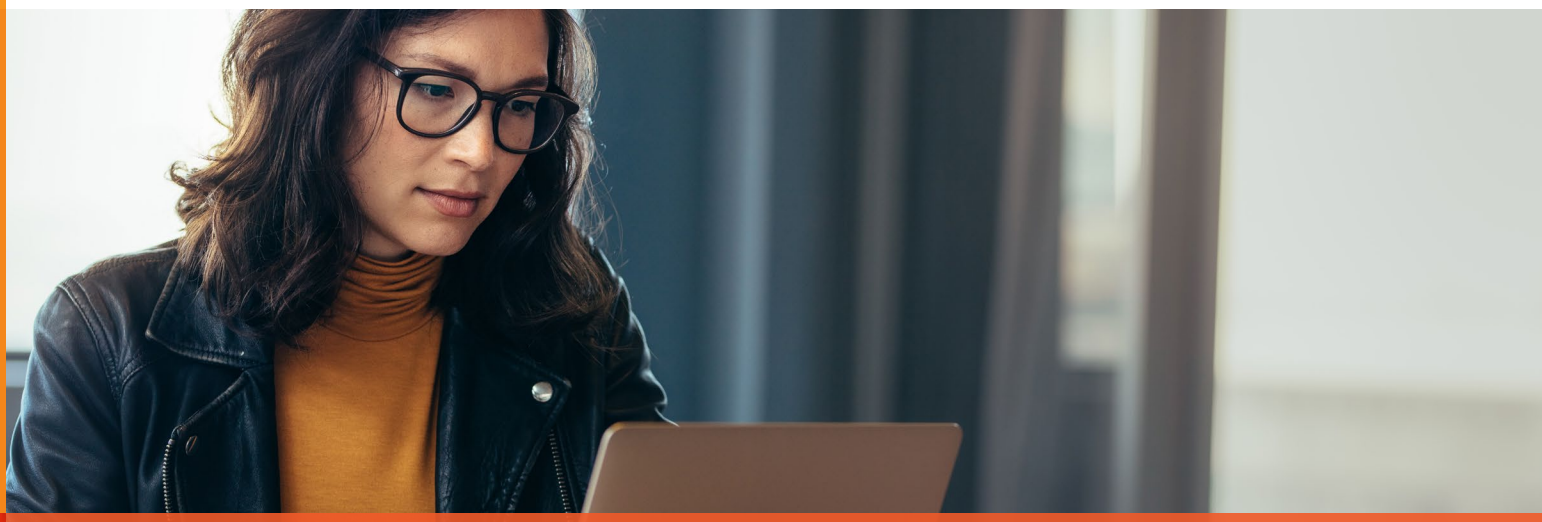


The Importance of Security for Single Sign-On (SSO)

By Matt Cohen, Principal, Advisory Services, CoreLogic®

At the most basic level, single sign-on (SSO) lets people log in once and then easily access an organization's numerous applications, eliminating the need to remember multiple logins and passwords. For end users, SSO improves convenience and workflow.

Some multiple listing organizations have adopted SSO without security designed for real estate industry challenges. This is not ideal – like milk and cookies, security and SSO were made to go together.

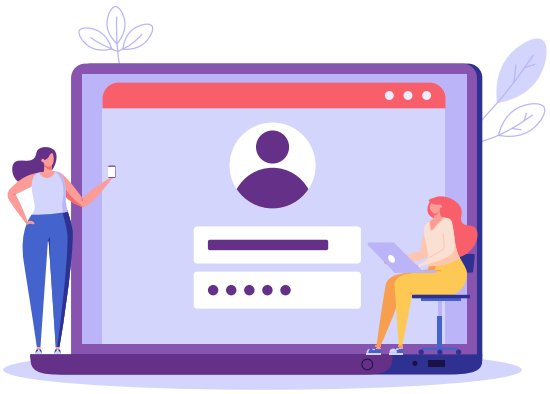
Multiple listing organizations continue to be the hub of an experience that includes confidential and personal information. Listings include confidential remarks and other information that should only be accessed by the authorized professional. When SSO is added, the same login protects access to such information in other platforms including, but not limited to, showing scheduling, lockbox, forms, document management, and transaction management systems. A single misused or stolen credential can result in expensive and embarrassing public disclosure, so login security is very important.

Building the Foundation for SSO

The real estate industry login security challenge is unique and complicated. Some users share login credentials with consumers, as well as with unauthorized non-licensed assistants and other companies. Some brokerages, appraisal companies and other subscribers also share logins to save money, a theft of service that has revenue implications for the multiple listing organization. Most login security systems are designed to prevent credential theft, but the industry has the added challenge of intentional password sharing, which is far more difficult to prevent. Professionals sometimes share computers and other devices in an office and use many devices when they are out-and-about. That is why device and IP address identification security

alone does not meet the security challenge. Most of the credential sharing is also low-level, so overlapping login monitoring is only marginally effective. Thus, some of the most common security measures don't work for our industry.

The Clareity® security tools from CoreLogic® were designed to meet these challenges. Our security experts continue to refine the products using patented and patent-pending technologies including, but not limited to, behavioral biometric and one-time-password options that, especially when layered, provide substantial login security.



SSO Without the Foundation

Login security is not a problem that goes away: as some users are prevented or discouraged from sharing, new users attempt to share. A customer of ours once decided to try another security solution. Once their login security problems returned and could not be denied, they realized they had to return.

When your organization fields SSO, your identity provider (IDP) solution is technically "asserting" to other systems that it reliably knows who is logged in. To make this assertion with confidence, the appropriate effective security system must be implemented.

For more information on the Clareity SSO or strong authentication solutions for multiple listing organizations, please contact your CoreLogic account representative or Amy Gorce at amgorce@corelogic.com.

And, for more information on security assessment and other advisory services, please contact Matt Cohen at macohen@corelogic.com.

Note that security assessments, including livestream assessment of physical security, are still being performed during the pandemic.