

Adaptive Authentication

What is Adaptive Authentication?

Adaptive Authentication provides two-factor authentication without the inconvenience of carrying a token. Two-factor authentication relies on something the user knows and something the user has to ensure against fraudulent access to the MLS. Adaptive Authentication uses the machine that the user is logging in from as the second factor (something the user has).

How does it work?

When a user first enrolls in adaptive authentication they will be presented with several security questions that they must provide answers to. The user will also have to register the machine they are logging in from. The authentication platform will now associate the user's logon credentials (username and password) with that particular machine. Each time the user logs in from that machine the system will automatically verify that the machine is associated with that username and password.

The "adaptive" element of the authentication platform learns a user's behavior to detect possible fraud. If a user follows the same patterns when logging into the MLS their logon experience will simply be to enter a username and password. If the system detects a change in behavior then the system will challenge the user with one or more security questions. For example, if an agent generally works from home but then tries to log in from a PC at a different location the system will detect that the machine's identity does not match what was registered. This will be perceived as a change in pattern and will prompt the system to "challenge" the user. Once the security questions have been answered correctly the user will also be asked if they wish to register the new machine. Once registered the system will now associate both machines with the user's behavioral pattern and will not challenge the user again until another change in the user's behavioral pattern is detected.

Other factors that might trigger the system to challenge a user with security questions may be a change in the time of day a user is logging on. If a user generally logs in between 9:00am and 5:00pm and then attempts to log in at 4:00am the system may "challenge" this change in behavior.

The level of challenge or "risk factor" can be determined by the MLS. Some MLSs may allow a wide variance in behavioral patterns without challenging the user and instead rely on the system's reporting tools to identify fraudulent behavior. Other MLSs may set the system to challenge a user when any change in behavioral pattern is detected.

The system enables the MLS to analyze the history of logins (by individual or system wide) to predict trends or detect possible ID sharing. Examples of patterns that might indicate the sharing of IDs would be multiple attempted logins from different IP addresses, concurrent logins geographically apart in a short time span, the same user logged on and off throughout a 24 hour time span etc. The MLS can choose to have the reporting be anonymous (no users identified) or not.

What are the Benefits?

Convenience

- Unless a change of pattern is detected, users only need to enter a username and password
- Simple to use – most users are already using adaptive authentication when using online banking

Cost effective

- Same level of security assurance as a token with less cost
- Adaptive Authentication available for both MLS and Internet Membership Services

Less Support

- Lost or damaged tokens no longer an issue. No more "courtesy access" needed

Security Control

- MLS can control the level of security they wish to impose on their users
- MLS can choose the security questions

Reporting

- Sophisticated reports enable the MLS to view usage trends and detect possible fraud
- Reporting tools provide "just cause" to challenge a potential cheater
- Reports can be generated in PDF or Excel