New Curity Token Handler Addresses Single Page Application Security

Curity, a leader in API access security and identity management, launches the new token handler for website-level access security for Single Page Applications.

STOCKHOLM, SWEDEN, May 29, 2024 /EINPresswire.com/ -- Curity, a leader in API access security and identity management, today announced the launch of a new token handler offering that delivers website-level access security for Single Page Applications (SPAs). With the Curity Token Handler, a ready-to-deploy Backend for Frontend (BFF) authentication solution, organizations can now leverage SPAs for business advantages, like streamlined user experiences and fast deployment, while maintaining strong defenses against cyber threats.

> By managing API access verification from the users' browser and simplifying implementation, the Curity Token Handler addresses the security and development resource obstacles that slow SPA adoption."
>
> *Jacob Ideskog, Curity CTO*

"SPAs elevate digital customer experiences and can be launched quickly, but secure browser-based authentication is difficult to achieve," Jacob Ideskog, Curity CTO, explains. "By managing API access verification from the users' browser and simplifying implementation, the Curity Token Handler addresses the security and development resource obstacles that have slowed SPA adoption."

An alternative to websites, Single Page Applications have been gaining traction in recent years. SPAs store readily accessible information in the browser instead of pulling data from a backend database. As a result, these lightweight, web applications provide a way to deliver easy-to-navigate, responsive online services such as banking and social media communities. However, security has been an ongoing concern because identity and access management must occur in the user's browser outside of the organization's firewall-protected network.

The Curity Token Handler enables user authentication in the SPA without requiring a network-protected backend data system for identity verification. It uses secure cookies combined with an OAuth proxy that resides on an API gateway for token verification at the application level. Following OAuth Best Current Practices (BCP) for browser-based applications, the Token Handler separates web and API concerns to eliminate dependence on a backend connection and retain the full benefits of a secure SPA architecture.

Additionally, the Curity Token Handler is designed for simplified deployment enabling developers to achieve security without delaying application time-to-launch. It also delivers plug-and-play compatibility with popular API gateways, including Azure API Management (formerly Azure AD), Google Apigee, AWS, Kong and NGINX.

The Curity Token Handler is a complementary addition to the company's flagship product, the Curity Identity Server, and Curity Technology Solutions™.

ABOUT CURITY
Curity is a leading provider of API-driven identity management that simplifies complexity and secures digital services for large global enterprises. Through proven experience, IAM and API expertise, Curity builds innovative solutions that provide secure authentication across multiple digital services. Curity is trusted by large organizations in many highly regulated industries and partners with leading technology and consulting companies. To learn more and understand what is unique about the Curity solution, visit https://curity.io/.

Keri LeBlanc
Curity
email us here
Visit us on social media:
X
LinkedIn
YouTube
Other

This press release can be viewed online at: https://www.einpresswire.com/article/715207272