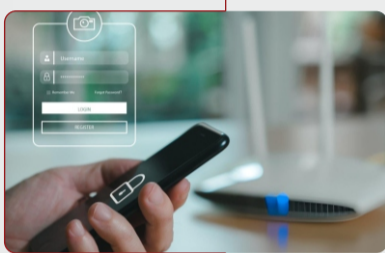


Fortifying Banking with Mute Authentication through Comviva NGAGE CNPaaS

Cyber frauds are reaching new peaks, and they will likely continue at this pace. Therefore, 3-Factor Authentication (3FA) is crucial for significantly enhancing the security posture of online systems and accounts.

The NGAGE CNPaaS platform transforms banking operations with enhanced security for the virtual user to resolve issues in real-time, resulting in increased user experience.



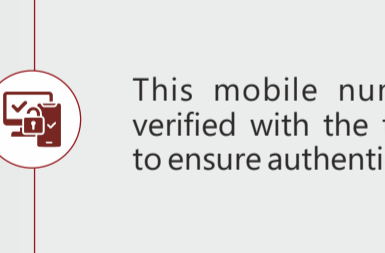
The user opens the banking app and logs in using their credentials.



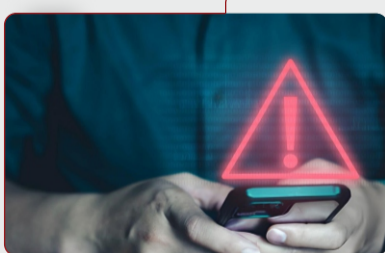
Once the login is successful, the user is prompted to enter an OTP for 2-Factor Authentication (2FA).



After entering the OTP, the banking application performs mute authentication in the backend via Comviva NGAGE CNPaaS to verify the user's identity through their mobile number.



This mobile number is then verified with the telco operator to ensure authenticity.



If there is a mismatch in the mobile number, the login activity fails, preventing unauthorized access.



How Does it Help?

No-Human Intervention

OTP Less

Prevents Hacking

Robust Security

The added verification with the telco operator ensures the user's identity is authentic, adding a layer of security. By removing visible OTPs and handling background checks, NGAGE CNPaaS cuts down on fraud and builds trust in digital banking.

Secure your network and protect your customers with Comviva NGAGE CNPaaS. Embrace the future of authentication and stay ahead in the fight against cyber fraud.

"Schedule A Complimentary Call Today"
For More Information, Please Visit www.comviva.com