IMAGEWARE® SYSTEMS

GoVerifyID®

# Accelerate your Authentication Journey with our 2FA, Biometric, and MFA Solutions

## Convenient and Secure Network Access with Aruba ClearPass and GoVerifyID

Aruba, a Hewlett Packard Enterprise company, and ImageWare have joined forces to deliver strong network security with a simplified user experience.

Using ImageWare's GoVerifyID mobile application, Aruba ClearPass customers can replace (or augment) their passwords with two-factor and biometric multi-factor authentication. Rather than typing a password, end users can respond to messages, take selfies, speak phrases, show their palm, and/or swipe their fingers to gain access.

It is proven that even sophisticated passwords are not a viable solution. These antiquated measures are not secure, nor convenient to use on mobile devices. Data breaches are one of the leading security concerns for IT as compromised passwords are most often used to gain access.

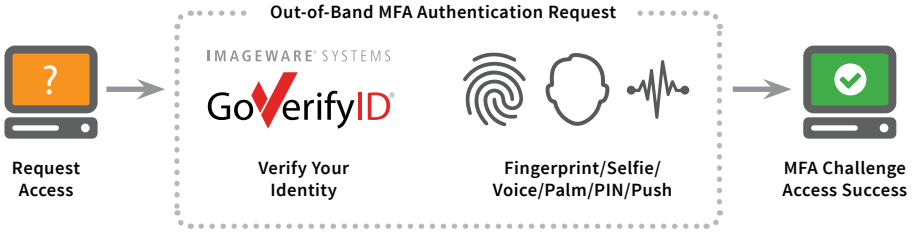
### THE VALUE OF BIOMETRICS FOR AUTHENTICATION

In addition to passwords, two-factor and biometric multi-factor authentication (MFA) is the best practice for adding an extra layer of protection in today's mobile workplace. Several industry factors are driving this adoption, which include:

- The challenges and costs related to using complex passwords.
- The need to simplify the user experience while increasing security.
- The rising costs of data breaches.
- The occurrence of data breaches due to compromised passwords.
- The use of biometrics being mandated by governments, worldwide.

## HOW DOES THIS WORK?

The integration of Aruba ClearPass and ImageWare's GoVerifyID combines convenience and security with a straight forward authentication process. When a user requests access, a secure push notification will be sent to their mobile device to ask them to authenticate. The user can choose to capture face, voice, palm, or fingerprint on their mobile device to identify themselves.




## DEPLOYMENT

ImageWare's GoVerifyID is provided as a Software as a Service (SaaS) or an on-site solution. It is a true turnkey solution. No specific coding or implementation is needed; however, it requires Aruba ClearPass version 6.6 or later. The combined solution is provided via standard configuration using the ClearPass Policy Manager, where an administrator can setup the authentication policies to select ImageWare's solution for all users, for specific user roles, or for desired systems.

## BENEFITS

As mobile technology permeates our workplace, the use of two-factor and multi-factor biometric authentication is becoming more valuable. It is no longer recommended to rely on users to protect internal resources via lengthy passwords. The shift to more secure access methods is now and includes these benefits and use cases:

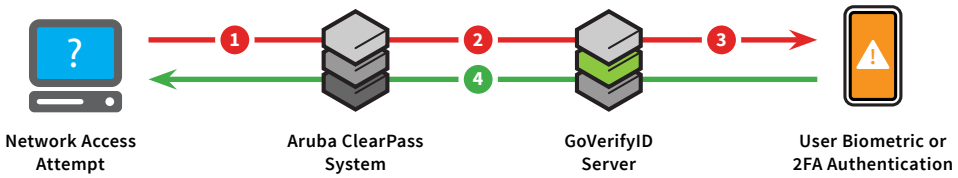
- Improved user experience
- Reduced password administration costs
- Improved network security
- Industries that may benefit most: financial services, retail, e-commerce, healthcare, education, utilities, enterprises, and government agencies
- These benefits also apply to environments that offer subscription based Wi-Fi access (e.g. frequent flyers going through airports on a weekly basis)

## SUMMARY

ImageWare is an Aruba Exchange Partner that provides an integrated 2FA and MFA workflow for ClearPass customers. GoVerifyID allows ClearPass customers to replace (or augment) their password or token-based authentication with a secondary authentication method of their choice, using existing mobile devices.

## Mobile 2FA and Biometric User Authentication: How it works

1. The user attempts to access an Aruba ClearPass managed resource.
2. Aruba ClearPass pings the GoVerifyID server for an authentication request.
3. The user is asked to submit their biometrics or 2FA factor for authentication.
4. Based on the results of the authentication, the user access request is approved or denied.




For more information visit **GoVerifyID.com** or call **(858) 673-8600**

IMAGEWARE SYSTEMS, INC.
*Authentication Assured™*



**V180901**