aruba
a Hewlett Packard Enterprise company

SOLUTION OVERVIEW

STRONG NETWORK SECURITY WITH A SIMPLIFIED USER EXPERIENCE

Aruba and ImageWare Deliver Convenient and Secure Network Access

INTRODUCTION

The explosion of smartphones and tablets is transforming the way we work, communicate, consume services, and manage our personal lives. The combination of mobile devices and cloud-based apps allow us to access enterprise networks, conduct business, or perform banking and personal transactions anywhere in the world, at any time.

This ubiquitous use of mobile devices also puts additional demands on security platforms as password use extends outside of an organizations perimeter. It is proven that 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 most of the time, compromised passwords are used to gain access to resources.

Aruba, a Hewlett Packard 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 authenticate users via traditional methods and supplement network access authentication with biometrics via a selfie, spoken phrase, or swiping their fingerprint to gain access. GoVerifyID introduces hardened biometrics that allow customers to replace (or augment) their passwords or two-factor authentication (2FA).

THE VALUE OF BIOMETRICS FOR AUTHENTICATION

Biometrics and multi-factor authentication (MFA) is the best practice for adding an extra layer of protection on top of username and password 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.
- 67% of data breaches occur due to compromised passwords. (2015 Verizon Data Breach Investigations Report)
- The average cost of a data breach is $3.8 million. (IBM 2015 Data Breach Study)
- The US Federal Government is mandating the use of biometrics for security (Homeland Security Presidential Directives 5 & 12), which often drives requirements in the financial space and other verticals.

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

THE BENEFITS OF BIOMETRICS

With Aruba ClearPass and ImageWare GoVerifyID, customers across any vertical can enjoy:

- Enhanced security: A highly secure user login process due to two-factor out-of-band authentication.
- Reduced IT helpdesk costs: Minimizes the need for IT helpdesk agents to reset passwords, so organizations can save up to 40% on helpdesk tickets. (Gartner)
- Improved user experience: The use of familiar tools that mobile users enjoy today to simplify the authentication process, rather than having to remember and type in a long complex password.

The multi-modal biometric user authentication solution also adds:

- Increased productivity by making it easier for users to gain access to ClearPass protected resources.
- Minimized use of passwords and reduced cost associated with password administration.
- Compliance with various industry regulations, including HIPAA and government security directives.

SUMMARY OF VALUE TO BENEFIT: SECURITY AND BETTER EXPERIENCE							
	Help Desk Staff	**Secret Questions**	**Email Message**	**Text Message**	**Device/ Tokens**	**Single Biometric**	**Multi-Modal Biometric**
IT Labor Costs	High	Low	High	Low	Low	Low	Low
User Setup Efforts	High	High	High	High	High	Easy	Easy
User Usage Efforts	High	High	High	High	High	Easy	Easy
Subject to Loss/Theft	Depends	Depends	Low	Yes	Yes	No	No
Level of Security	Low	Low	High	High	High	Higher	Highest

HOW BIOMETRICS DIFFER FROM TRADITIONAL AUTHENTICATION METHODS

Biometrics are like your own personal password that can't be forgotten, lost, or stolen. Users no longer need to remember complex password rules, answers to security questions, nor do they need to carry a separate single purpose hardware token.

Token/FOB/key card limitations: A user carries an extra device that shows a string of numbers that change on a set time basis. This approach increases security somewhat, but it is expensive due to the purchase of the devices, replacement, and management costs. It also adds another layer of infrastructure and inconvenience for users as they need to keep track of a single purpose device and then read and re-enter codes each time.

HOW DOES THIS WORK?

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

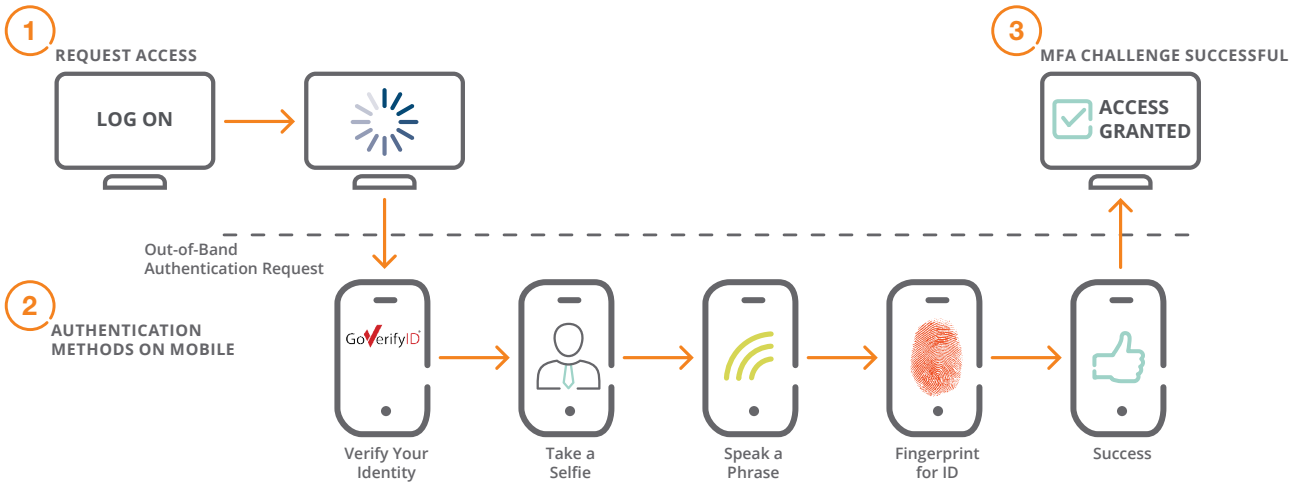


figure 1.0_071116_iws-soa

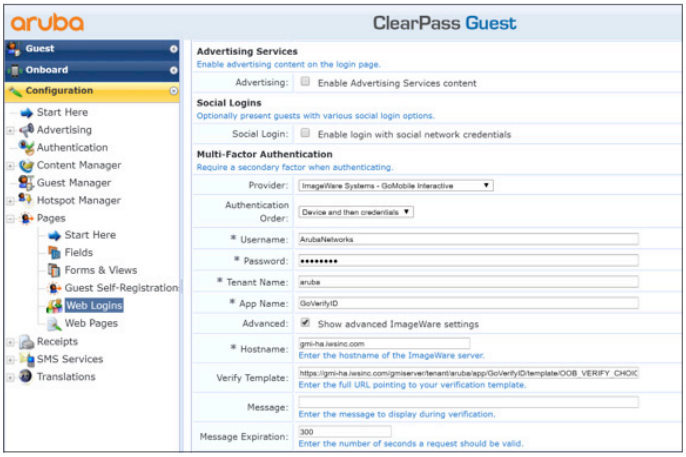
ClearPass and ImageWare Workflow

DEPLOYMENT

The ImageWare solution is provided as a Software as a Service (SaaS) or on premise solution. It is truly a turnkey solution. No specific coding or implementation is needed.

- The solution requires Aruba ClearPass version 6.6 or later.
- The combined solution is provided via standard configuration using the ClearPass Policy Manager.

A ClearPass administrator can setup the authentication policies using the ClearPass Policy Manager to select the ImageWare solution for all users, for specific user roles, or for desired systems.



Built-in ClearPass configuration template

SUMMARY

As mobile permeates our workplace, the use of multi-factor authentication that includes biometrics is becoming a must. It is no longer feasible to rely on users to protect internal resources via lengthy passwords. The shift to more secure access methods is on the horizon and includes benefits like the following and more:

- Customers looking for a better and easier user experience, with reduced password administration costs, and improved security.
- Industries that include: Banking, enterprise, financial services, retail, e-commerce, healthcare, education, utilities, and government agencies.
- Environments that offer subscription based Wi-Fi access (e.g. frequent flyers going through airports on a weekly basis) ImageWare's biometric identity verification capabilities can easily grant customers access using a simple selfie, pass phrase, or fingerprint.

a Hewlett Packard Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com