Flyer
Security

Advanced Authentication for Your Business

Advanced Authentication at a Glance:

+ A single framework for all your authentication needs
+ Provides mix-and-match method chaining flexibility
+ Support a broad variety of integrations (RADIUS, VPN, OpenID, OATH, FIDO, RACF Windows, Mac OS, Linux, Citrix, VMWare, etc.)

Flexible Design that Fits Your Environment

Organizations taking advantage of various strong authentication solutions are forced to manage and maintain multiple infrastructures. Not only is that approach very expensive and complicated to administer, but it is also less secure. What you need is a single solution for everything. Having a single framework allows you to control authentication via easily configured policies in a single console, which is important when a user, or group of users, either change roles or exit the organization.

With its collection of ready-to-go application integrations (RADIUS, VPN, OpenID, OATH, FIDO, RACF Windows, Mac OS, Linux, Citrix, VMware, and more), Advanced Authentication (AA) offers wide applicability for your environment. In addition, its broad support for a variety of authentication readers and methods provides a level of flexibility that you haven't enjoyed until now. Our AA framework is designed for High availability and internal load balancing for continuous uninterrupted operations, regardless of how large or small your environment. Replication between primary and secondary servers provides data integrity and disaster recovery (over LAN or WAN).

Sharing Information Securely

As organizations continue to evolve their architecture across complex hybrid environments, ease of application deployment and distribution is more important than ever. That's why AA is now available as Docker containers. Because all of their dependencies are bundled into a small set of Docker containers, they can be transferred as needed without any compatibility issues. And it's that avoidance of compatibility issues that make Docker containers a form factor of choice for cloud environments such as Amazon Web Services (AWS). As containers, AA can run on top of a variety of virtualization, hypervisor and cloud-based technologies that best fit your needs. You can also configure AA in specialized models optimized for performance or availability. In summary, with v6 and later Advanced Authentication:

- Is lighter and easier to deploy out
- Is easier to track versions and roll-back to specific previous versions

- Offers simplified maintenance because it avoids much of the effort and risk of problems with application dependencies.

Advanced Authentication for the Disconnected

Professionals on the go often find themselves in surroundings where they are not able to connect to standard authentication sources. While security is important, let's be honest: productivity is paramount. There simply can't be situations where users are blocked from getting their work done or servicing a client. AA supports offline authentication so that these users are able to perform two-factor authentication—or any other kind of strong authentication—at anytime from anywhere, connected or not.

Teaming up AA with your existing applications gives you the ability to ensure the user's identity. Use step-up authentication to a security level that matches the risk.

U2F Ready

Micro Focus is a member and strong supporter of FIDO (Fast Identity Online) Alliance. FIDO U2F (Universal 2nd Factor) provides a way for organizations to support an environment where users manage their own authentication devices. AA provides a solid framework to deliver that support to your applications without the need for development. Not only do organizations benefit from deferring token costs, but users like them because they are able to incorporate a higher level of security across other aspects of their digital life. AA delivers broad application support as well as a lower total cost of ownership. There is no better framework from which to provide a U2F authentication environment.

Strong Authentication across All Your Platforms

In a world where users have a wide range of devices, providing strong authentication across a broad number of platforms is more important than ever. As such, AA provides multi-factor authentication for Windows (desktop/server), OS X, and Linux platforms. You can also use authentication methods based on iOS, Android, and Windows Mobile to secure access these systems.

Strong Authentication for Active Directory Federation Services (ADFS)

ADFS continues to grow as organizations migrate over to Office 365 and Microsoft's Azure platforms. It is important for organizations to update the strength of authentication to match the risk of these offerings. For situations that merit it, AA protects access to your environment through consolidation and integration in a way that it is easy for users to consume while providing a higher level of user verification through MFA (multi-factor authentication). This means that regardless of whether your applications are running on-premises or in a cloud environment, AA can strengthen your ADFS-centric systems from unauthorized access.

Why Us

With a consolidated MFA approach, AA is less complex to configure and maintain than other solutions. Our strength also lies in out-of-the-box integrations that provide a wealth of configurable authentication options. Your entire organization benefits from the increased security and usability. You have the freedom to build new or replace and consolidate MFA infrastructures. This enables your organization to control costs and maximize investments. Lower costs and increased security are what make AA a market-leading solution.

To learn more about Micro Focus® AA Framework, or to start a trial, go to: **www.netiq.com/advanced-authentication**

Contact us at:
www.microfocus.com