2018

HID® ActivID® Authentication Server: A Very Capable and Comprehensive IAM Product

SECURITY INSIGHT REPORT

David Strom

HID® ActivID® Authentication Server: A Very Capable and Comprehensive IAM Product

by David Strom

David Strom (@dstrom, www.strom.com) is one of the leading experts on network and Internet technologies and has written and spoken extensively on topics such as VOIP, convergence, email, cloud computing, network security, Internet applications, wireless and Web services for more than 30 years. He has had several editorial management positions for both print and online properties in the enthusiast, gaming, IT, network, channel, and electronics industries, including the editor-in-chief of Network Computing print, DigitalLanding.com, and Tom's Hardware.com. He has also written two books on computer networking. He began his career working in varying roles in enduser computing in the IT industry. He has a Masters of Science, Operations Research degree from Stanford University, and a BS from Union College.

If you are looking for a comprehensive identity and access management (IAM) tool that can cover just about any authentication situation and provide iron-clad security for your enterprise, you should consider **HID Global's ActivID**. It has a wide range of tools that can lock down your network, cover a variety of multifactor authentication (MFA) methods and token form factors, and provide single sign-on (SSO) application protection.

Having thrown all those acronyms into one paragraph is intentional: this product covers a wide landscape and comes with a massive amount of installation and configuration. Even if you are an IAM specialist, it will take days and probably weeks of effort to get the full constellation of features setup properly and tested for your particular circumstances. There is good news though: you would be hard pressed to find an authentication situation that it doesn't handle.

ActivID comes in several different configurations, each with a somewhat different feature set:

- An **integrated hardware appliance** that contains several web and database servers that handles its various functions (we tested this, running v8, in April 2018).
- A **virtual software appliance** that is at feature-parity with the physical appliance that you install on your own hardware.
- An **authentication server**, which has different backup and HA features depending on how it is configured. This is useful if you need to handle more than two servers or have a wide distributed collection of applications.
- A **remote access AAA server**, which doesn't have as many authentication options and is more of a legacy product.
- A **managed services cloud-based offering**, which will have fewer overall features more appropriate for managed providers.

Strong Authentication Product Line

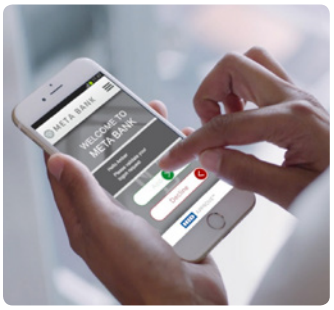
ActivID actually installs six separate services as part of its product. Some of these are designed to operate mostly in the background and don't have much in the way of user interface controls, because they don't require much in the way of daily operation. Those include an **authentication server, an authentication portal and a separate Radius server.** The three other services are where the main business of the product happens and they include:

- The **ActivID console** that manages the overall appliance system characteristics itself, along with reports.
- An **overall management console**, where you will spend the majority of your time configuring and monitoring the IAM processes, policies, and tokens.
- The **user self-service portal**, which is where users go to resolve their own authentication problems and add additional devices.

The heart and soul of ActivID is its support for a wide collection of MFA tokens, including both hardware and software, SMS and email, push notification and biometrics. That is by no means a comprehensive list of tokens, we tested two advanced token methods by setting them up for a sample web app and to authenticate various SAML apps and VPN logins. They worked flawlessly.

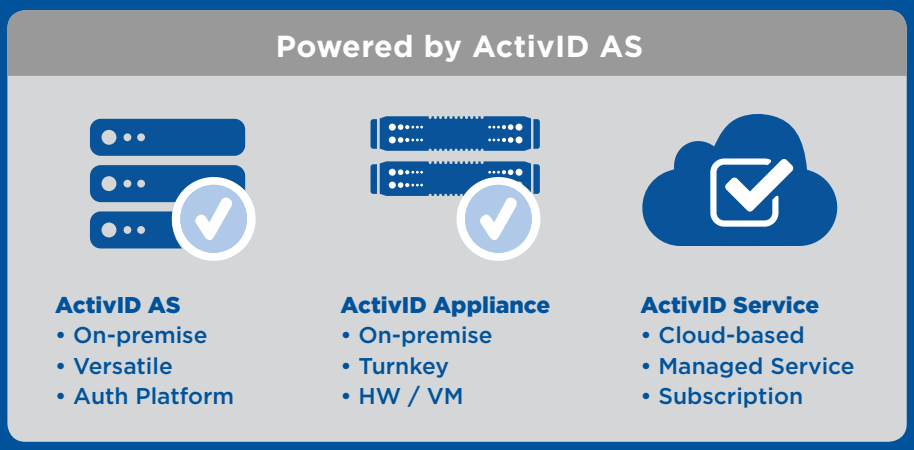
HID Approve™

The first token we tested is the latest v3 of the **HID Approve app** on both Android and iPhones. It also has a Windows 10 version that is available and going through extensive improvements. The app functions similarly on all three supported OS's. Think of this as a replacement for Google Authenticator or similar kinds of apps that have appeared in the past few years. The app runs on the last two major versions of Android and iOS.



These smartphone apps are gaining traction for two big reasons: first, you don't need your users to carry around a separate piece of hardware, like a OTP fob, because they already have their smartphones. Second, they are not compromising security like an SMS or email factor. These apps are a big step up because SMS (and to some extent, email) can be vulnerable to man-in-the-middle and account takeover attacks, something that can be avoided with Approve and other apps.

Setup properly, Approve can offer a solid protection against these issues and still make logins relatively painless. That is the big tradeoff: you can have perfect security if you keep all the users out of your systems, but that isn't very practical. Adding MFA support is accomplished by visiting a few configuration menus; batches of tokens can be quickly configured by importing special seed files that are similar to how this is done on competitors' products.



The HID Approve app also comes with built-in runtime application protection. One of the issues for smartphone apps, particular ones that support protective security measures, is being able to detect if the phones they are using have been tampered with or compromised by hackers. Having this protection is another way to prevent authentication attacks, and shows the lengths that HID has gone to beef up its security. And while many of its competitors offer this protection as an add-on module, it comes as part of the Approve package.

BlueTrust

The second token we tested is the **BlueTrust hardware fob**. OATH passwords are sent via Bluetooth from your phone or computer so a user doesn't have to type in the one-time password digits and can just click the button on the fob to acknowledge their receipt. It supports FIDO standards (which includes Android and NFC) as well. The fob comes with a small LCD display that can either show a one-time password or show a status readout if it is used in Bluetooth mode.

ActivID interoperates with the usual collection of authentication standards, including Radius, OpenID and SAML.

If delivering MFA is your primary focus for purchasing a new identity product, ActivID is probably overkill. But if you are rolling out MFA protection as part of a larger effort to secure your users and logins, then things get more interesting and the case for using HID's product becomes more compelling. For example, ActivID can handle a variety of application authentication situations and also be granular enough to deploy these methods for particular user collections and circumstances. Many older IAM products bolted-on their MFA methods with cumbersome or quirky integration methods, or required you to purchase a separate add-on products for these features, ActivID has had this flexibility built-in from the get-go and has a well-integrated MFA set of solutions.

ActivID interoperates with the usual collection of authentication standards, including Radius, OpenID and SAML. A lot of effort has gone into crafting a very flexible identity infrastructure that can work with these standards. Its design is similar to how the Fast Identity (FIDO) Alliance has been constructed: separating the authentication methods from the actual authentication data stream. However, it doesn't yet support the FIDO protocols but these are on the roadmap for the near future.

Because HID has decoupled the identity from the credentials and devices that are used to prove the authentication, you can mix and match your methods and processes and still maintain the tightest possibly security. ActivID uses a series of channels, adapters and policies to cover the widest possible array of identity circumstances. Let's explain what each of these items is and how the product is architected.

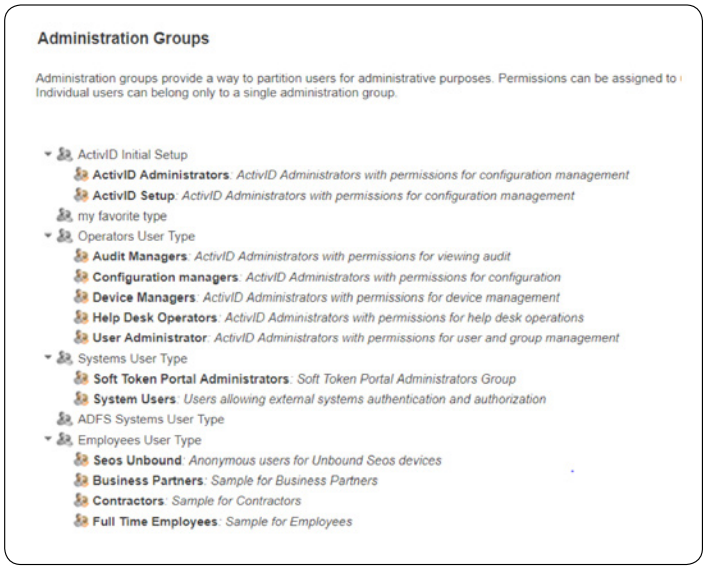
Channels are the pathways between the authentication agent, devices and actual authentications. They can cover a wide range, from push-based mobile notifications to SAML-based Web apps. Each channel supports one or more authentication policies, such as static passwords or OTP tokens or the HID Approve mobile app.

Authentication policies are tied to specific channels and make use of adapters, which connect the type of authentication (such as SAML or OpenID) with the actual authentication devices (such as a OTP token or mobile app). The product comes with dozens of pre-set policies by default, such as a policy for using a OTP token to login to the management console, or to validate your mobile push-based smartphone app. You can add multiple policies to a particular action, such as having different login methods for a user who wishes to authenticate themselves using a variety of tokens, apps, and other methods.

That is a lot to visualize and it will take some careful study to not only separate and distinguish these different elements but to visualize the workflow of setting all this up and how to connect the various moving parts. **Other IAM products have a less complex architecture but also a less capable functional environment.** There are various many-to-one relationships between these terms that takes some sorting out. Once you get used to this nomenclature and understand where to find the relevant configuration menus in the management console, it isn't all that difficult to use.

As an example of how complex IAM products can be, a few years ago OpenID added what is called the Client Initiated Backchannel Authentication dialog. This allows users to be authenticated without their explicit interaction, such as by using a smartphone app that can automatically send the additional factor for the authentication. This feature was recently added to ActivID. One big potential use case for OpenID is the UK's Open Banking initiative, which will allow consumers greater control over how they do banking and to be better able to mix and match various legacy banking services with newer app-based ones. ActivID can be a key player in supporting these advanced transactions with better security than simple usernames and passwords.

On top of the various policies are three types of permissions: what HID calls user types, roles and administrative groups. User types define categories of users, such as operators or employees. Administrative groups provide different roles for various administrative purposes, such as device managers, user administrators, and contractors. *(See screenshot below.)*



Other IAM products have a less complex architecture but also a less capable functional environment.

Finally, roles are more of functional areas, such as granting permissions for audit log viewing or to operate the help desk. The combination of the three (user types, roles and administrative groups) makes for a very granular approach and a powerful way to partition your overall user population. Of course, this means more front-end work to establish the various roles and permission sets. But the process of defining these different groups will also result in a more secure operating environment, since many enterprises gloss over these sets and get sloppy with their security. HID forces you to have a more rigorous approach.

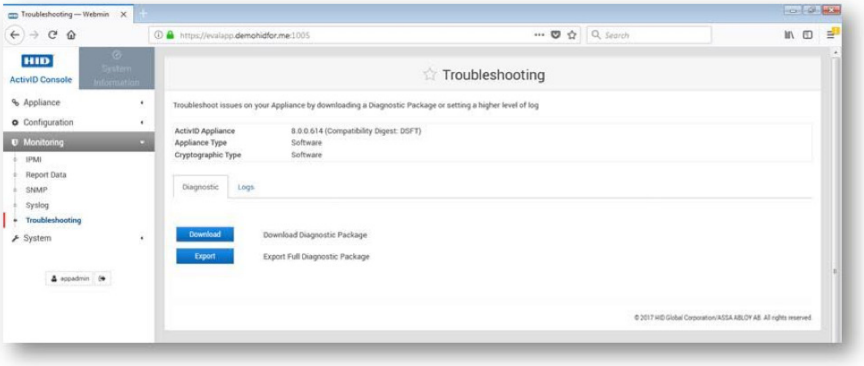
The product has two major weaknesses: documentation and reports. Documentation is a bear. ActivID comes with a thick sheaf of more than a dozen different documents that go into exacting detail about its operations. Navigating this library will take a considerable effort. As an example, while the quick start guide is only two pages, it contains dozens of separate steps that need to happen in a complex sequence.

Reports are handled in the ActivID console, which is a separate web interface from the management and configuration tasks mentioned above. This is also where you will do any troubleshooting, which is one of the more important aspects of any IAM product. Troubleshooting is essential because identity problems usually touch on many different pieces of your computing infrastructure, especially authentications that are introduced when adding a new MFA token type or application login. The syntax for these connection strings is very exacting for any IAM product, and ActivID is no exception.

There is a quick search box at the top of every screen where you can find a particular user or device or use wildcards to zero in on a particular problem area. But that is just the brute force searching. We couldn't test troubleshooting comprehensively, but did get a feeling that some rudimentary error checking is built into the product, so that if you make a major syntax error you will be warned as you are trying to enter the data. You still might have to go to the application logs or audit reports to figure out your particular mistakes.

HID has created a "diagnostic package" that can be sent to their support team to help you figure out how you have lost your way, and you can see the screen to create this data below. They will review this and help you solve your issues.

In this same console ActivID you can create various reports. You choose your data source, select the appropriate domain, and schedule how often it is to be run. See screenshot below. That's great, but the caveat is these reports are intended for machine reading, rather than for humans: you'll need some kind of report writer or post-processing to make the most use of them.



Summary

ActivID is a powerful IAM solution that could be difficult to setup but otherwise is very capable at handling a diverse identity solution that can scale to millions of users and dozens or more applications. A starting price is $25/user/year for a typical installation is in line with many of its competitors, and HID offers consulting and support services to help with installations.

The combination of the three (user types, roles and administrative groups) makes for a very granular approach and a powerful way to partition your overall user population.

Every day millions of people in more than 100 countries use HID Global products and services to securely access physical and digital places. Over 2 billion things that need to be identified, verified and tracked are connected through HID's technology. We work with governments, universities, hospitals, financial institutions and some of the most innovative companies on the planet—helping them to create trusted physical and digital environments so that they and the people who use them can fulfill their potential.

Learn more at ***hidglobal.com/iam***

2018-10-30-hid-iams-david-strom-review-wp-en PLT-04091