

AuthLite: Collective Software's Two-Factor Authentication Solution

Dr. Thomas W Shinder

Many organizations have already seen the writing on the wall: the days of user name and password authentication are coming to an end. We've tried to overcome the weaknesses of the old username and password solution by requiring complex passwords, but users just came up with creative ways to get around password complexity requirements, and hackers came up with more sophisticated methods (such as rainbow tables) for cracking passwords. Bill Gates said at the 2004 RSA conference that passwords "just don't meet the challenge for anything you really want to secure." It's clear that other methods for authenticating users must be employed to meet the security challenges of the 21st century.

The solution is multi-factor authentication. Most commonly deployed as two-factor authentication, multi-factor authentication requires more than a user name and password. There must be something else provided in order to verify that the user is whom the user claims to be. That additional "factor" can be a biometric reading, a smart card, or a device that enables a one-time password. The important thing is that an authentication factor in addition to an easily stolen username and password must be required to assure that the person logging on is indeed that user.

Two-factor authentication solves a lot of problems. Some of them include:

- **Phishing attacks.** With two-factor authentication, phishers could not steal user names and passwords and gain access to private information; since they cannot steal the second factor, the user name and password ends up being worthless to the attacker later on
- **Identity theft.** Much of what we see in the area of identity theft is moving online; identity thieves might be able to steal or guess private information about a person, such as a pet's name, user name, password, or date of birth, but they won't be able to steal the second factor, making it impossible for them to impersonate the victim
- **Complex and multiple passwords.** Users come up with creative means to subvert complex passwords, and become even more enraged by having to remember complex passwords for multiple systems; two-factor authentication removes this onus from the user, so that the only things required are a relatively simple password and a second factor

Given all of the advantages of two-factor authentication, you have to wonder why it's not universally deployed on all networks, regardless of size. There are several reasons why this is the case, the two major ones being:

- **Cost** - Most two-factor authentication systems are extraordinarily expensive, leading them to be used only by large enterprises with deep pockets
- **Complexity** - Most two-factor authentication systems are complex to set up and configure, some of them requiring dedicated server resources and their own authentication repositories to make them work

These reasons are a one-two punch when it comes to total cost of ownership (TCO). First, there is the high cost of the two-factor authentication solution itself, and then there are the steep costs in initial administrative overhead. There are also ongoing administrative costs, as many of these solutions are not tightly integrated with Microsoft® Windows® Active Directory®, and thus often require that the administrator troubleshoot at multiple levels in a multi-tier solution. Add to this steep ongoing licensing fees and a three-year refresh for hardware keys, and you end up with "three strikes and you're out," when it comes to total cost.

What is needed is a two-factor authentication solution that is easy on both the pocketbook and on the administrator deploying the solution. This is where Collective Software comes in. Collective is well-known for "keeping its ears to the railroad track" by staying close to the user community and coming up with real-world solutions that solve real-world problems. In the authentication arena, Collective does it again by introducing its new two-factor authentication solution, AuthLite.

Introducing AuthLite

AuthLite uses an innovative USB key that implements a one-time, password-based approach to two-factor authentication. For domain-joined computers, users can program their own keys; there's no need for administrators to spend expensive hours setting up keys. For users connecting from machines that aren't part of the domain, there is the option for provisioning keys administratively, so they're ready to work without the user having to do anything—avoiding expensive help desk calls.

AuthLite is an exception in the two-factor authentication space: No additional servers are needed. The solution is tightly integrated with Active Directory, and a small AuthLite component is installed on domain controllers. This removes the need to troubleshoot other servers that can introduce complexities and complications when they interface with Active Directory.

After Active Directory is prepared, a client-side component can be installed on workstations and servers that belong to the AuthLite-enabled domain. After that, users log onto their workstations by plugging their AuthLite keys into the computer, touching the lighted ring on the face of the key, and entering their passwords. Once logged in, users can change their initial passwords to less unwieldy ones, as they now have the AuthLite key that protects them from compromise.



AuthLite can do more than protect interactive logins to domain-member machines. AuthLite can also be used to secure remote-access connections. For remote-access VPN users, an AuthLite key can enable secure two-factor authentication. Organizations can use AuthLite with Windows Routing and Remote Access Service (RRAS)-based remote access VPN servers, or leverage the enhanced security access controls provided by the ISA Server 2006 VPN server with AuthLite's integrated support for ISA 2006 remote access VPN services.

ISA Server 2006 customers can further extend the value of their Internet Security and Acceleration (ISA) Server investments by using AuthLite's tight integration with ISA Server 2006 Web Publishing. When you pair AuthLite with ISA Server Web Publishing, you can enable the use of strong, two-factor authentication to connect to key Web services, such as Microsoft® Outlook Web Access (OWA), Microsoft SharePoint® Server services, and Microsoft Dynamics CRM. With strong two-factor authentication, you reduce the risk of enabling remote access, extending the value of your technology investments by allowing partners, consultants, contractors, and even customers to access information stored on your network application servers. This protection can even be extended to sites accessible by mobile devices.

As with any security solution, you have to ensure that it's implemented correctly. For example, some solutions actually leave traces of the logon credentials on the users' hard drives, or store the password on the key. If either the computer or the key is lost or stolen, there is a risk of compromise. In contrast, AuthLite never stores user credentials in any way, mitigating the risk of a lost or stolen key or computer.

Let's take a closer look at AuthLite to see how it solves the installation, configuration, and usability issues that prevent two-factor authentication from being more commonly deployed.

Installation

We found the AuthLite installation process to be quick and easy. Depending on your deployment scenario, you will have to install the AuthLite components on different machines:

- Workstations – If you want your users to log into the Active Directory domain using two-factor authentication, then you'll need to deploy the 32- or 64-bit client component; you can do this

manually, but most administrators will use an automated approach, such as Windows Server Group Policy, or Microsoft System Center Configuration Manager

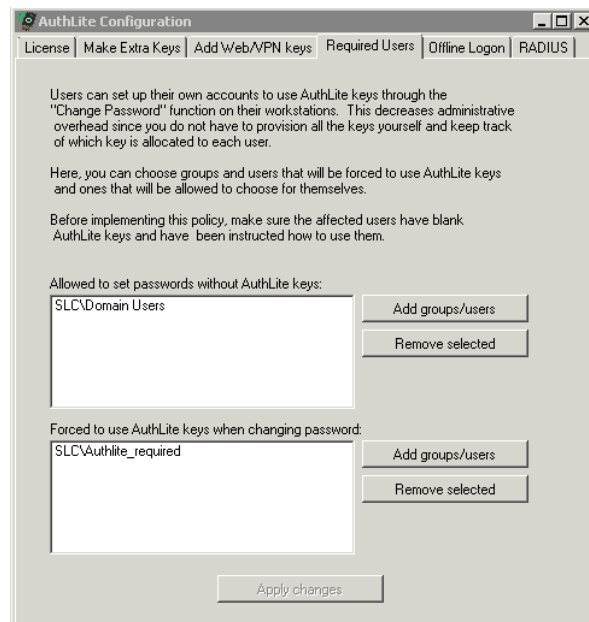
- Domain Controllers – An AuthLite component needs to be installed on domain controllers so that it can work with Active Directory to perform authentication
- ISA Server – There is an ISA Server component that needs to be installed so that Web publishing rules can be configured to use AuthLite authentication; note that if you only want to use VPN authentication with AuthLite and ISA Server, no AuthLite component is required on the ISA Server
- Member Servers – If you want to enable interactive logon for servers, the AuthLite component will need to be installed

Installation of the AuthLite components was easy, and I had no issues with the installation process. I wasn't presented with cryptic dialog boxes, nor did I have to perform any arcane or complex pre-configuration requirements on my network before installing the AuthLite components. No complex command line configuration steps were required. However, you do need to have the Microsoft .NET Framework version 2 installed on Windows XP and Windows Server 2003 machines. This isn't installed on these operating systems by default, but the good news is that the installer checks for it and tells you if it's not installed.

Configuration

Configuring the AuthLite software on the domain controller is a snap. The AuthLite configuration is done in a single dialog box that contains six tabs, from which you can configure all of the back-end features. On these tabs there are a number of configurable options that allow you to:

- Make extra keys, so that users have a spare in case they need to keep an extra key at another location
- Provision keys for users who connect from non-domain machines, so that they can connect through a VPN, or access Web servers securely published by ISA Server 2006
- Specify user groups that are required to use the AuthLite key, and groups that can choose to use the key or the conventional user name and password approach
- Enable domain-joined machines to use offline logon so that those who need to log on can do so when they're off the network; users still need the key to log on
- Configure the pre-shared secret and the port number for the AuthLite RADIUS server uses when authenticating connections for VPN users and users who access Web sites published by ISA Server 2006



Overall, I found configuring the AuthLite domain controller component to be very intuitive and straightforward. I only had to confer with the documentation for a single issue to find more information about a specific configuration option. In contrast to other two-factor authentication schemes I've worked with, I'd put the AuthLite authentication repository configuration component in the "no-brainer" category. Any IT generalist should be able to get this up and running in less than an hour.

User Experience

If users don't like using it, any two-factor authentication solution will fail. The password change and user logon experience have to be natural and user-friendly. If the solution fails to meet those requirements, users will balk and you'll have wasted your investment in two-factor authentication. In this area, we found AuthLite to be the model citizen of a user-friendly solution.

The screenshot on the right shows the change password experience, which includes a simple checkbox that enables the user to use the AuthLite key for authentication.



The screenshot on the left shows the end-user experience, when the user logs on to the computer using the AuthLite key.

Logging on is very simple. The user just needs to insert the key, press the key button, and enter the password. That logs the user on.

In the same way, changing the password to enable AuthLite for authentication is a matter of putting a checkmark in a checkbox.

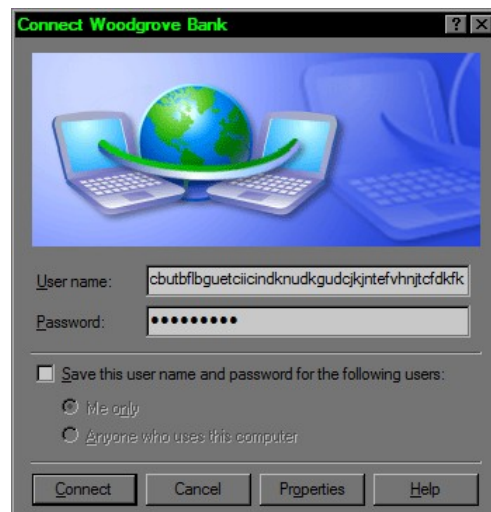


When the users change their passwords, they'll

be able to use simpler, easier-to-use and -remember passwords without causing concerns about authentication security, since the AuthLite key is required for authentication. Of course, you would only want to consider relaxing password security requirements for users who are required to use AuthLite — but not too much; the password should have some level of complexity. For users who have the option to use either AuthLite or username/password security, you should continue to enforce complex passwords.



VPN connections using the AuthLite key are also very simple. The user doesn't need to enter a user name, just press the button on the AuthLite key and the username field is populated with the one-time password. Then enter the password and click Connect. It's as easy as that.



In the same way, the experience of logging onto Web sites published by ISA Server is just as easy and intuitive. Just connect to the logon page for the published site, press the button on the key, and enter

the password. Now you have the ease of use of AuthLite logon to published Web resources, and the security inherent in strong, two-factor authentication.

The only downsides I initially perceived regarding the user experience was that for the VPN and Web connections, the AuthLite one-time password was remembered from session to session, and that the logon page for the ISA logon form said "Domain\user name," which can be confusing to some users.

However, a quick check of the AuthLite documentation detailed solutions to these problems, so what would have been issues are easily solved using the AuthLite support materials.

Documentation & Support

A product can be best-of-breed and claim to do everything you ever wanted it to do, but if the documentation isn't up to speed and leaves me hanging, then the product goes back on the shelf. Life is too short to have to spend time figuring out how to do things that should be covered in the Help files. And if I have to call for help, I want to know that my questions are answered and that things are fixed fast, with no push-back from the vendor.

I found the AuthLite documentation to provide all the information I needed to get the solution running for the scenarios I tested. It was easy-to-read and -interpret. It didn't include a bunch of marketing-driven terminology that I had to memorize, something that especially irks me when I have to learn about a new product. Step-by-step instructions were complete, and used language any Windows IT generalist can understand to get up and running fast and without frustration.

The AuthLite documentation goes one step further – it integrates links to video help files on the Internet that you can use to watch the actual configuration process.

This is of great help to people like me who get tired of reading all day and just want to watch how it's done so that I can do it the same way. The videos are well done and worth your time.

However, nothing is perfect and there are some additional scenarios that the documentation covers that I did not test because I couldn't really wrap my head around what they were trying to say. I'm sure I could have asked support personnel about these scenarios and they would have helped me with them, but in general I'd rather get my answers from the docs instead of calling the support line.

When it comes to support, what can I say? Collective Software has to have one of the most responsive, polite, and enthusiastic support teams with which I've ever had the pleasure of working with. A couple of times I had a question about why something wasn't working with my configuration, so I got on the phone with support. I left a message and they got back to me within an hour. They actually listened to my problem and got me a solution before I hung up. And for one issue that was related to a design change request on my part, they actually *had an update to the application the next day*. That isn't something you see from your typical software vendor!

Videos

[Setting up an account to use AuthLite](#)



Value

There are a lot of good two-factor authentication solutions on the market, so when I look for a product that's right for my business, I have to take both features *and* TCO into account. That's especially true in today's economic climate. This is where AuthLite really shines – in the category of solution value.

AuthLite licensing starts at \$28 per user, with the keys costing \$20 each. When I look at the major players in the two-factor authentication game, I see the total price of these other solutions ranging anywhere from two to four times the cost of AuthLite. What I *don't* see from other offerings in this market is two to four times the features or security that AuthLite offers. This excellent value should make anyone with TCO in mind put AuthLite in front of the crowd.

Assessment

So, how did AuthLite do? Quite well. AuthLite turned out to be an easy-to-install and -configure solution that didn't require me to add more servers to my infrastructure. Ongoing management was almost zero, and my users were able to provision their own keys and log on to their computers, log on to the VPN, and log onto ISA Server-published Web sites with no problems after a short introduction on how to use the keys in these three logon scenarios. I was able to deploy the solution on the server in less than an hour, including the time I spent reading the documentation, and the same applied for getting both the VPN and Web publishing working. AuthLite's impressive feature set and ease of use combine to make it the value leader the two-factor authentication market.

The only major limitation I see in the product is that for Web site and VPN authentication, it needs to use its own built-in RADIUS server, which lacks the policy support included with most industry standard RADIUS servers, such as the Microsoft Internet Authentication Service (IAS) or Network Policy Server (NPS) solutions. This could make it a bit problematic for some enterprises to deploy this solution. For small and mid-sized firms that don't already make extensive use of RADIUS however, this shouldn't pose any problems at all. On the bright side, Collective Software informs me that future iterations of the product will support standard RADIUS, leading this to be a non-issue in the future.

On a 5-point scale, I'd give AuthLite the following ratings:

Installation – 5/5

Configuration – 5/5

User Experience – 4.5/5

Documentation -- 4.5/5

Value – 5/5

Overall – 4.8/5

For more information on AuthLite, visit www.authlite.com