



Adito: Open-source, browser-based SSL VPN

By Russ McRee – ISSA member, Puget Sound (Seattle), USA chapter



Prerequisites

Platform independent assuming Java is installed.

Similar Projects

Barracude SSL VPN (commercial)

OpenVPN (free)

Adito is an open source, browser-based SSL VPN solution. What the heck does Adito mean, you ask? *Adito* is an Italian word roughly defining “an entrance to a room or to a building.” Perfect for a VPN solution, yes?

As a topic it came to me by way of a surprising statistic. I had discovered Adito looking for a similar solution to the now defunct SSL-Explorer, a VPN project I had contentedly used a few years ago, before support for it went by the wayside as the code base went commercial. I took a quick look at Adito, and was pleased enough to write a follow up to a three year old blog post I’d written on SSL-Explorer. The traffic to the original SSL-Explorer post had always been a bit surprising in itself, but when I published the Adito follow up the queries and reads were immediate and many. Of the 90 blog posts I’ve written (as I write this column) in three plus years, the Adito post is currently ranked as the third most read post (since I started tracking). Suffice it to say, statistics bear out the fact that an open source, browser-based SSL VPN solution is of great interest and as such warrants attention for *toolsmith*.

I reached out to Samuli Seppanen of Finland to learn more about his project. He characterizes himself as a system administrator, but does some programming and translation work too, and is a hard-core Linux and open source fan. His company had used SSL-Explorer for quite a while when its source was closed. While the fork was not initiated by his company (it was a personal decision), he does spend quite a lot of his work time on Adito.

There is a clear vision about Adito’s near future; some of it is described in the wiki¹ under “Ongoing projects” heading. Samuli hopes the next version of Adito will include the following:

1. Convert Adito into a pure web application which runs under any servlet container (e.g. Jetty or Tomcat). This includes getting rid of the of the non-standard Adito-specific stuff such as the boot module and Java service wrapper. The embedded HSQLDB database will be replaced with an external one. We’ll start with using an external HSQLDB, but PostgreSQL/MySQL/whatever should be trivial to implement later on.
2. Change the Adito build system from Ant to Maven2. The current Ant build scripts are way too complex and prone to breakage. Migration is tightly related to #1, because creating non-standard package formats and directory layouts with Maven2 is much harder than with Ant.
3. Modernize as many components as possible. The Maven2 migration takes care of most of this automatically, but updating some components requires code changes due to API changes.
4. Document Adito and Adito development on all levels.

All of these will lower the barrier of entry to Adito development, which is crucial for Adito as it’s a community open source project. Modularizing Adito will make various deployment scenarios - such as large installations with load balancers - much easier.

They’re also working on re-implementing some of the functionality of SSL-Explorer Enterprise Edition. The two most needed are LDAP authentication and network drive mapping extensions. The LDAP authentication module is already being worked on.

There’s also activity not directly related to the Adito software itself. For example, there are people working on making Adito rPath/Redhat AOS appliances. These will make Adito deployments much easier.

Using Adito Windows installation

Adito works well on any Windows or Linux operating system capable of running a JRE (Java Runtime Environment). For my test environment I installed it on a Windows Server 2003 SP2 virtual machine running on my Ubuntu 8.10 server.

I unpacked `adito-0.9.1-bin.tar.gz` in `c:\adito`. Ensure that you have JRE 6² installed and you’ll also need Apache’s Ant.³

² <http://java.sun.com/javase/downloads/index.jsp>.

³ <http://ant.apache.org/bindownload.cgi>.

¹ <http://adito.wiki.sourceforge.net>.

Unpack Ant in C:\ant to be sure that C:\ant\bin can be made available as an environment variable:

```
Control Panel => System => Advanced
=> Environmental Variables =>
System Variable => Append Path to
include c:\ant\bin
```

Adito requires JDK (Java Development Kit),⁴ which bugs me as I dislike excessive libraries on publicly accessible servers like this; likely future releases will reduce this dependency for those of us of the security mindset. Speaking in my best Dr. McCoy voice: “Damn it, Jim... I’m a security guy, not a developer!” The sole dependency from the JDK is tools.jar, which can be copied from C:\Program Files\Java\jdk1.6.0_11\lib to C:\Program Files\Java\jre6\lib.

Cd back to C:\adito and execute `ant install`. To prevent the *Unable to locate tools.jar* error, copy tools.jar from C:\Program Files\Java\jdk1.6.0_11\lib to C:\Program Files\Java\jre6\lib and C:\adito\lib.

The installer will step through the XML buildfile and ultimately fire up a browser UI at `http://localhost:28080`. You’ll begin with *Step 1 - Configure Certificate*. I chose to create a new certificate, and then set my keystore passphrase.



Install

Welcome to the Adito installation wizard. You will now be guided through the process of configuring the basic options secure service. When complete, you should start the service, logon as the super user and start building the facilities yo available to your users. You may return to this wizard at any time.

Step 1 - Create New Certificate

Please complete the details below to generate your untrusted certificate. You should consider getting this certificate signed.

• Host name: HIO-TEST
 • Organisational unit: HIO
 • Company: Holisticinfosec.org
 • City: Seattle
 • State: WA
 • Country Code: US

Figure 1 – Adito Certificate Configuration

Flesh out the details of your certificate, then move to *Step 2 - Configure User Database*. You can opt to integrate with Active Directory, or use an internal database of users and groups. I recommend this option until you’ve fully vetted Adito with a well controlled test phase in your environment. After all, we’re talking about keys to your castle. While SSL-Explorer was sound, and I’m confident in Samuli’s ongoing efforts to enhance and develop Adito, I want you to be absolutely it passes muster for your enterprise before signing off on it as implementation complete.

You’ll establish your Super User account in Step 3. In Step 4 you’ll set up the web server, and should you need to configure proxy settings you’ll do so in Step 6. If all goes well, the summary page will confirm your success.

⁴ <http://java.sun.com/javase/downloads/index.jsp>.



System Configuration

Here you may configure various system preferences and options to customize the behaviour of your Adito VPN server. Please ensure that Automatic Updates are enabled to ensure you have the latest and most secure version of the software.






Sub-categories	
 Server	Use this link to configure options such as web server settings, network proxy settings and automatic update settings. You can also set security settings here such as password lengths, maximum connection attempts and timeouts.
 Resources	The resources section allows you control over settings concerning Network Places, Profiles and Web forwarding settings.
 Windows Integration	Here you can configure many properties relating to how Adito integrates with your Microsoft Windows file shares and other Windows resources. Options are available that can assist with troubleshooting sharing problems on Windows.
 Security Options	Use this link to access options to configure various security options used by Adito.
 Messaging	Adito can use a number of different methods to communicate messages to administrative and normal users. Here you can configure settings relating to these message delivery methods.

Figure 2 – Adito VPN System Configuration

With your installation process complete, return to `c:\adito` at the command prompt and issue `ant start`.

To configure extensions, applications, web forwards, additional users and other Adito options, open your browser and connect to `https://<AditoServer>` (Figure 2).

Login as the Super User you set up earlier.

Note: As I write this, installing Adito as a Windows service is buggy, and I didn’t have time to get to the bottom of the issue. An interim solution is to create a simple batch script (`cd \adito => ant start`) and use Scheduled Tasks to ensure it restarts along with the system in case of failure or reboot.

Linux installation

Here’s a rapid run through the Ubuntu Linux install process:

```
sudo apt-get install sun-java6-jdk
ant
untar adito-0.9.1-bin.tar.gz to /opt/
adito
cd /opt/adito
sudo ant install
```

To install Adito as a service:

```
sudo ant install-service
sudo /etc/init.d/adito start
ant start
```

Making use of Adito

To finalize my test implementation I set up Adito as a gateway into my virtual environment to allow my address by BackTrack 3 virtual machine from a remote network via SSH.

I first created the user BackTrack from the Access Control => Accounts page via Actions => Create Account (Figure 3).

You can also manage Groups, Policies, Access Rights, Authentication Schemes, and IP Restrictions from this menu. After you create the account, revisit it to apply Security Ques-

Figure 3 – Set up an Adito user

tions and mark it as Enabled. The account will not be available until you complete this step.

I then installed the SSH extension via the *Extension Manager* under the *Configuration* menu. To do so you'll click the *Remote Access* tab in the *Extension Store* view then choose *Install Extension for PuTTY SSH* under *Actions*. Then move to *Applications* under the *Resources* menu and click *Create Application Shortcut* under *Actions*. You'll see the *PuTTY SSH Application Extension* you just installed; click *Next*. Under *Application Details* populate the *Name* and *Description* fields and check *Add to Favorites* then click *Next*. I populated *Hostname* in the *Application Options* view with the IP address of the BackTrack VM. You can add information for additional SSH settings as well as X11 forwarding and tunnels. I clicked *Next*, moving to Step 4, where I added *Everyone* as a *Selected Policy*. You'll want to review policies, this was purely for test purposes. Click *Next* again to reach the *Application Shortcut Summary* screen and click *Finish*. Exit the Wizard and logout of the Super User session.

I logged back in as my BackTrack user and was treated immediately to My Favorites where my Application Shortcut to SSH was waiting for me (figure 4).

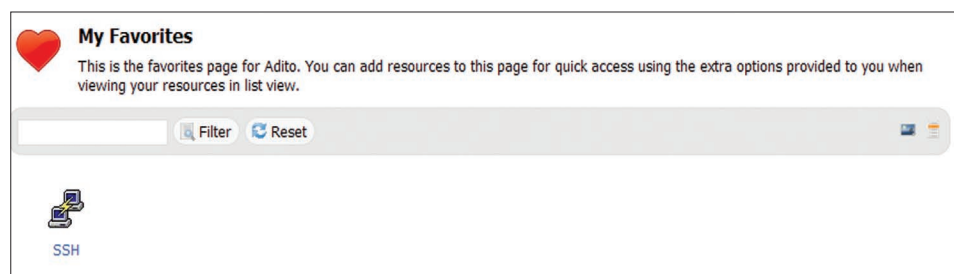


Figure 4 – Adito My Favorites user view

I clicked the SSH shortcut and the PuTTY Java applet fired up, cached the server's host key, and dropped me right at the terminal on my BackTrack VM, after I authenticated (Figure 5).

The capabilities featured in Adito as a viable VPN solution are many. Integration with Active Directory or a UNIX authentication scheme, SSL tunnels, additional extensions; Adito is indeed feature rich and further improvements are pending.

One final note on something I didn't explore but found hopeful. I've long been a fan of the Linux-based open source network firewall Smoothwall Express.⁵ Lurking in one of the install scripts I found reference to starting Adito as a service on SmoothWall. The integration of Adito and SmoothWall on an older Pentium 3 or 4 platform with 3 (internal, external, DMZ or wireless) makes for an ideal gateway guardian to your home or small office network.

In conclusion

Sure, you can buy a commercial appliance, perhaps you've tried OpenVPN, or like me you've used SSLExplorer. Adito

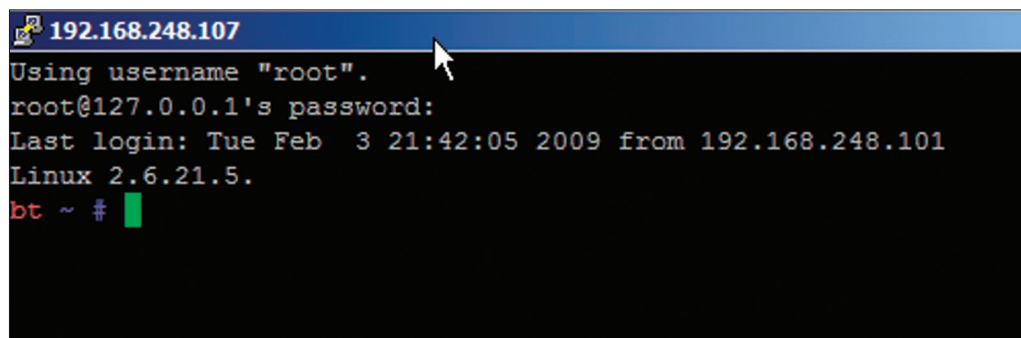


Figure 5 – Adito SSL VPN access to the SSH console

seems to stand firm with all of them for performance and functionality and I'm please this SSL-Explorer fork is in such good care. Make good use of this one, I believe you'll find it quite useful as a remote access solution.

Cheers...until next month.

Acknowledgments

Samuli Seppanen for his feedback and Adito project direction.

About the Author

Russ McRee, GCIH, GCEA, CISSP, is a security analyst working in the Seattle area. As an advocate of a holistic approach to information security, Russ' website is holisticinfosec.org. Contact him at russ@holisticinfosec.org.

⁵ <http://smoothwall.org>.