webApp.secure

Installation and Setup Guide

webScurity Inc.
9298 Central Ave NE
Suite 402
Minneapolis MN 55434
USA
866.SCURITY Toll Free (US)
763.786.2009 Twin Cities Metro/International
763.786.3680 Fax
support@webscurity.com

Installing and Setting Up webApp**.secure**

It's easy to install webApp**.secure** for evaluation and production. This short document will guide you through the installation process and get you "up-and-protecting" in no time.

Installing webApp**.secure** for Evaluation

To Install webApp.secure on Windows:

1. If you haven't already done so, download wasetup.exe from http://www.webscurity.com/download.htm onto any Win2k/XP or above computer with network access to the Web server (it is not necessary to install webApp**.secure** on the production Web server).
2. Double-click wasetup.exe to begin the installation process.
3. Follow the onscreen instructions.
4. When installation is complete, a webApp**.secure** icon to the MMC-compliant **Admin Console** will be placed on your desktop. The **Quick Start Guide** will automatically be started in a new browser session. Follow the **Quick Start Guide** or continue with these instructions to configure webApp**.secure** for your environment.
5. Double-click the webApp**.secure** desktop icon (or choose Start->Programs->webScurity->webApp.secure PE/SE->Admin) to bring up the **Admin Console**.
6. Expand **wa(Default)**.
7. Expand **Configuration Settings**.
8. Select **Server Info**.
9. Enter appropriate values for **Web Server Name**, **Web Server Port**, **Listen Port**, and **Internet Host Name(s)**. (See respective sections below or the **User Guide** for details.)
10. Press **Apply** to save the changes.
11. To start webApp**.secure**, right-click **wa(Default)**, select **New**, then select **Start Instance**. (Because webApp**.secure** is installed as an NT service, you are free to start, stop, etc. using the standard Windows **Services Administration Tool**.)
12. See the **Testing/Experimenting** section that follows.

To Install webApp.secure on Linux:

1. If you haven't already done so, download the webApp**.secure** RPM from http://www.webscurity.com/download.htm onto any Linux x86 computer with network access to the Web server (it is not necessary to install webApp**.secure** on the production Web server).
2. Initiate the installation process using "rpm –i webApp.secure.pe-3.0-1.i386.rpm" for webApp**.secure Professional** or "rpm –i webApp.secure.se.3.0-1.i386.rpm" for **SE**.
3. Modify /usr/local/wa/etc/WAProperties.xml with your favorite text editor setting appropriate values for the **<web-server-name>**, **<web-server-port>**, **<listen-port>**, and **<host-name>** configuration properties (see respective sections below or the /usr/local/wa/doc/Welcome_unix.pdf for details).
4. Enter "/usr/local/wa/bin/wa &" to start webApp**.secure**. You may need root privileges if using a **<listen-port>** lower than 1000.
5. See the **Testing/Experimenting** section that follows.

Web Server Name
<web-server-name />

The **Web Server Name** configuration property is typically an internal server name (i.e. "stargate") or IP address that, combined with the **Web Server Port/<web-server-port>** property (see below), tells webApp**.secure** how to establish a connection to the Web server (IIS, Apache, etc.).

This is most commonly an internal IP address.

NOTE: This should **not** be the same value as **Internet Host Name(s)/<host-name>** configuration property (see below).

Web Server Port
<web-server-port />

The **Web Server Port** configuration property represents the TCP port number the Web server (IIS, Apache, etc.) is listening on for unencrypted traffic. This property, combined with the **Web Server Name/<web-server-name>** property (see above), tells webApp**.secure** how to establish a connection to the Web server.

For evaluation purposes, the default port 80 is generally appropriate.

Listen Port
<listen-port />

The **Listen Port** configuration property identifies the TCP port number webApp**.secure** should use.

If you installed webApp**.secure** on the same machine as the Web server (IIS, Apache, etc.), you will probably have to set this to something other than port 80 (i.e. 1111).

Internet Host Name(s)
<host-names><host-name /><host-names>

The **Internet Host Name(s)** configuration property identifies the external name of the Web site (i.e. www.xyz-corp.com).

If your Web server uses name-based virtual hosts, there would be an entry for each site.

Testing/Experimenting

Now that webApp**.secure** is installed and running, there are a couple ways to begin testing and becoming familiar with its capabilities **without** altering your production environment.

Method One:

1. Add a "127.0.0.1 www.yourdomainname.com" line to the hosts file on the machine from which you will be running the browser session. (On Windows it is usually \windows\system32\drivers\etc\hosts and /etc/hosts on Linux.)
2. Restart a browser session.
3. In the browser's address bar, enter the URL http://www.yourdomainname.com/ to request the root document of the site.

   The browser will send an HTTP GET request for / to webApp**.secure**. If it is a valid request (which it should be because / is defined as an **Entry Point** by default), webApp**.secure** will forward it to the Web server for processing. The response will be sent back to the browser through webApp**.secure**. It is from this response that webApp**.secure** begins establishing the **Intended Use Guidelines** for the Web site.

   If you installed webApp**.secure** on the same machine as the Web server, you will need to add the value used for the **Listen Port/<listen-port>** configuration property (see above) in the address bar to direct traffic through webApp**.secure** (i.e. http://www.yourdomainname.com:1111/).
4. Entering http://www.yourdomainname.com/password.txt (or any other URI that is not part of the Web site) into the browser's address bar will generate a **403 Forbidden** response from webApp**.secure**. This is simply because password.txt is not a legitimate part of the Web site (it doesn't meet the site's **Intended Use Guidelines**).

Method Two:

1. Set the **Site Test/<site-test>** configuration property **True**.

   Setting **Site Test** to **True** will instruct webApp**.secure** to replace the browser's "Host:" HTTP header with the value of the **Intenet Host Name(s)/<host-name>** configuration property (i.e. www.yourdomainname.com).
2. In the browser's address bar, enter http://localhost/, assuming the browser session and webApp**.secure** are running on the same machine.

   As with method one above, if webApp**.secure** is installed on the same machine as the Web server, you will need to add the value used for the **Listen Port/<listen-port>** configuration property (see above) in the address bar to direct traffic through webApp**.secure** (i.e. http://localhost:1111/).
3. Entering http://localhost/password.txt (or any other URI that is not part of the Web site) into the browser's address bar will generate **a 403 Forbidden** response from webApp**.secure**. This is simply because password.txt is not a legitimate part of the Web site (it doesn't meet the site's **Intended Use Guidelines**).

NOTE: Method two is **not** recommended because fully-qualified URL's in the HTML of the site (links, images, etc.) will bypass webApp**.secure** and go directly to the Web server.

Example Scenarios

Example One – 2 Separate Computers

Web Server Computer Configuration:

Internal Host Name	**stargate**
Public Host Name	**www.xyz-corp.com**
Internal IP Address	**192.168.0.1**
Public IP Address	**209.98.999.123**
Unencrypted HTTP Port	**80**

webApp**.secure** Computer Configuration:

Internal IP Address	**192.168.0.2**

webApp**.secure** Configuration Properties (Windows Admin Console):

Web Server Name	**stargate** or **192.168.0.1** or **209.98.999.123**
Web Server Port	**80**
Listen Port	**80**
Internet Host Name(s)	**www.xyz-corp.com**

webApp**.secure** Configuration Properties (Linux /usr/local/wa/etc/WAProperties.xml):

<web-server-name>**stargate**</web-server-name>
or
<web-server-name>**192.168.0.1**</web-server-name>
or
<web-server-name>**209.98.999.123**</web-server-name>
<web-server-port>**80**</web-server-port>
<listen-port>**80**</web-server-port>
<host-names>
<host-name>**www.xyz-corp.com**</host-name>
</host-names>

The following entry would be added to the hosts file on the webApp**.secure** computer (typically \windows\system32\drivers\etc\hosts on Windows, /etc/hosts on Linux):

127.0.0.1 www.xyz-corp.com
or
192.168.0.2 www.xyz-corp.com

Addressing http://www.xyz-cop.com/ from a browser session on the webApp**.secure** computer will direct the request through webApp**.secure** for validation.

If found to be valid, it will be forwarded on to the Web server for processing.

The Web server's response will then be sent back to the browser through webApp**.secure**.

Example Two – 1 Computer

Web Server Computer Configuration:

Internal Host Name	**stargate**
Public Host Name	**www.xyz-corp.com**
Internal IP Address	**192.168.0.1**
Public IP Address	**209.98.999.123**
Unencrypted HTTP Port	**80**

webApp**.secure** Configuration Properties (Windows Admin Console):

Web Server Name	**stargate** or **192.168.0.1** or **209.98.999.123** or **127.0.0.1**
Web Server Port	**80**
Listen Port	**1111**
Internet Host Name(s)	**www.xyz-corp.com**

webApp**.secure** Configuration Properties (Linux /usr/local/wa/etc/WAProperties.xml):

<web-server-name>**stargate**</web-server-name>
or
<web-server-name>**192.168.0.1**</web-server-name>
or
<web-server-name>**209.98.999.123**</web-server-name>
or
<web-server-name>**127.0.0.1**</web-server-name>
<web-server-port>**80**</web-server-port>
<listen-port>**1111**</web-server-port>
<host-names>
<host-name>**www.xyz-corp.com**</host-name>
</host-names>

It may be necessary to add the following entry to the hosts file on the Web server computer (typically \windows\system32\drivers\etc\hosts on Windows, /etc/hosts on Linux):

127.0.0.1 www.xyz-corp.com
or
192.168.0.1 www.xyz-corp.com

Add "192.168.0.1 www.xyz-corp.com" to the hosts file of any computer that will run a browser session through webApp**.secure**.

Addressing http://www.xyz-cop.com:1111/ from a browser session on the Web server computer will direct the request through webApp**.secure** for validation.

If found to be valid, it will be forwarded on to the Web server for processing.

The Web server's response will then be sent back to the browser through webApp**.secure**.

System Requirements

Compatibility:

- Windows 2000/XP and above, Linux x86
- All major Web browsers
- All HTTP Web servers
- All HTTP application servers
- Fully compatible with HTTP 1.0 and 1.1
- Fully compatible with HTML 3.2 and 4.0, including cascading style sheets
- Fully compatible with client side scripting languages (JavaScript, VBScript, etc.)
- SSL 40/128 bit encryption and global ID

Minimum System Requirements:

- Computer: Pentium III 500 MHz (933 recommended)
- Operating System: Windows 2000/XP, Linux
- 128 Mbytes RAM recommended
- 300 Mbytes free disk space recommended