Smarten
Advanced Data Discovery
Powered by ElegantJ BI

Securing Application Server

Business Intelligence & Advanced Data Discovery

Document Version: 7.0
Product Version: 5.0 and above

Document Information	
Document ID	Smarten-Securing-Application-Server
Document Version	7.0
Product Version	5.0 and above
Date	2-Dec-2018
Recipient	NA
Author	EMTPL

Statement of Confidentiality, Disclaimer and Copyright

This document contains information that is proprietary and confidential to EMTPL, which shall not be disclosed, transmitted, or duplicated, used in whole or in part for any purpose other than its intended purpose. Any use or disclosure in whole or in part of this information without the express written permission of EMTPL is prohibited.

Any other company and product names mentioned are used for identification purpose only, may be trademarks of their respective owners and are duly acknowledged.

Disclaimer

This document is intended to support administrators, technology managers or developers using and implementing Smarten. The business needs of each organization will vary and this document is expected to provide guidelines and not rules for making any decisions related to Smarten. The overall performance of Smarten depends on many factors, including but not limited to hardware configuration and network throughput.

Preface

The Smarten Smarten-Securing Application Server is part of the documentation set for **Smarten Advanced Data Discovery Version 5.x.**

This manual contains information on securing the Wildfly AS for Smarten on supported operating system platforms.

This document is based on Application Server WildFly v 8.2 (formerly JBoss Application server), and you are advised to verify suitability of recommendations in this document for the Application Server version you may be using.

Related Documents:

Smarten-Technical-Specifications	Prerequisites and compatibility of supported software platforms and Client/Server environment for Smarten
Smarten-ApplicationServer-Optimization-Guidelines	Performance tuning: Wildfly Application Server

Note:
Throughout this manual, Smarten Advanced Data Discovery is abbreviated as Smarten.

Contents

1 About this Manual

It contains topics related to securing Wildfly AS for using Smarten Advanced Data Discovery.

1.1 Conventions Used

This manual uses typographical conventions in the text to help distinguish between names of files, instructions, and other important notes that are relevant during installation.

- The names of file directories and files are presented in boldface font.
  For example,

  /system.properties: system.properties file

- Important notes are indicated in blue font color.
  For example,

  > Note:
  > If you don't know on which port your Wildfly JNDI service is running, you can find it in standalone.xml file.

- We have mentioned the file name "Smarten-5.x.x" in various places. The number "5.x.x" represents the Smarten product version number.

2 Self-signed SSL implementation

SSL (Secure Socket Layer) allows web browsers and web servers to communicate over a secured connection, implying that the data being sent is encrypted by one side, transmitted, and then decrypted by the other side before processing. This is a two-way process—both the server and the browser encrypt the traffic before releasing data.

Step 1—Generate key

To generate a self-signed certificate, open command prompt and enter command below:

keytool - genkey - alias ejbi - keyalg RSA - keystore ejbi.keystore -validity 10950

Step 2 – Configure Wildfly

Open the file WILDFLY_HOME\standalone\configuration\standalone.xml and apply below mentioned configuration.

1) Locate <security-realms> tag in standalone.xml. Add below configuration code under this tag.

```
<security-realm name="UndertowRealm">
 <server-identities>
  <ssl>
   <keystore path="./ejbi.keystore"
        relative-to= "jboss.server.config.dir"
        keystore-password="******" alias="ejbi" />
  </ssl>
 </server-identities>
</security-realm>
```

> For "password" attribute in step 2 above, replace "******" with your actual password generated in step 1.

2) Locate below line in standalone.xml:
<http-listener name="default" socket-binding="http"/>

Replace it with below lines:
<http-listener name="default" socket-binding="http" redirect-socket="https" />
<https-listener name="https" socket-binding="https" security-realm="UndertowRealm" />

3 Restrict Access To IP Address

If you want to restrict access to Smarten for certain IP Address or IP Address range,

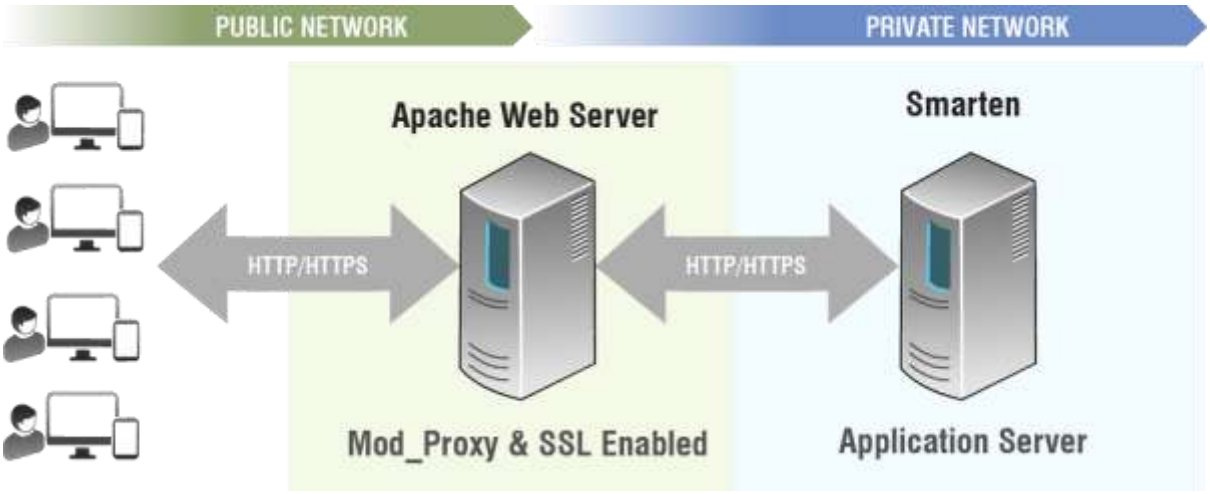
- Open WILDFLY_HOME\standalone\deployments\Smarten.war\WEB-INF\jboss-web.xml file in any text editor.
- Uncomment below mentioned block in the file. You can define allow/deny access for your IP address range.

```
<valve>
        <class-name>org.apache.catalina.valves.RemoteAddrValve</class-name>
                <param>
                        <param-name>allow</param-name>
                        <param-value>XXX</param-value>
                </param>
                <param>
                        <param-name>deny</param-name>
                        <param-value>XXX</param-value>
                </param>
</valve>
```

> For allow / deny parameters, “XXX” parameter value can be a specific IP address, comma separated IP addresses, or IP address range with wild card notation.
> Examples:
> * – Any IP addresses
> 192.168.10.* – IP addresses with specific subnet range
> 192.168.10.1 – Specific IP address

4 Use Apache Web server as a secure proxy for Wildfly Application Server

You can secure your Wildfly application server by configuring Apache web server as a front end server. Any HTTP request from public network to Wildfly server can be routed through Apache server. Wildfly server resides in private network and is completely isolated from public network.



You need to follow below steps for configuration:

- Make changes in Apache configuration file as shown below.

<VirtualHost>

ProxyPreserveHost On
ProxyPass /Smarten <Smarten_Application_Server_URL>
ProxyPassReverse /Smarten <Smarten_Application_Server_URL>

Header edit Location ^http: https: *(This configuration will be applicable only when HTTPS is enabled on Apache server)*

</VirtualHost>

For example,

1. Apache server is running on HTTPS and Smarten Application server is running on HTTP, use following configuration.

<VirtualHost *:443>
...
ProxyPreserveHost On
ProxyPass /Smarten http://10.0.0.1:8080/Smarten
ProxyPassReverse /Smarten http://10.0.0.1:8080/Smarten
Header edit Location ^http: https:
</VirtualHost>

2. Both Apache server and Smarten Application server are running on same protocol (HTTP or HTTPS), use following configuration.

<VirtualHost>
....
ProxyPreserveHost On
ProxyPass /Smarten http|https://10.0.0.1:8080/Smarten
ProxyPassReverse /Smarten http|https://10.0.0.1:8080/Smarten
</VirtualHost>

5 Product and Support Information

Find more information about Smarten and its features at www.smarten.com
Support: support@smarten.com
Sales: sales@smarten.com
Feedback & Suggestions: support@smarten.com
Support & Knowledgebase Portal: support.smarten.com