Running Intellicus under SSL

Version: 7.3

intellicus

Power To Understand Your Business

Dated: September 2015

Acknowledgements

Intellicus acknowledges using of third-party libraries to extend support to the functionalities that they provide.

For details, visit: http://www.intellicus.com/acknowledgements.htm

Contents

1 Running Intellicus Portal under SSL

Intellicus is by default installed to work without use of SSL (Secure Socket Layer).

Web browsers and web servers can communicate over a secured connection using Secure Socket Layer.

In this, data by the sender is encrypted before it is being sent. On the other side, it is decrypted before it is processed. Trapping of encrypted data over the Internet is difficult making it relatively secure.

Prerequisite

At the time of installation, Intellicus by default installs tomcat web server. Given here are the instructions of configuring Tomcat to work under SSL. Before going ahead, make sure Intellicus is already installed.

Configuring SSL

This involves updating Tomcat configuration file.

Updating Tomcat Configuration File

Changes related to secure socket are made in Tomcat configuration file: server.xml.

This file has been placed at following location at the time of Installation of Intellicus:

<Intellicus Install Path>\jakarta\conf\server.xml

Windows

In case of windows, Intellicus tomcat uses APR features for performance enhancements. This requires OpenSSL style configuration for HTTPS connector. Intellicus provides the Certificate file (localhost.crt) and the Key file (localhost.key) for this purpose. Please make sure these two files are present in <Intellicus Install Path>/Jakarta/conf folder.

Remove comment from the Connector element related to SSL, which looks like this:

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443
        This connector uses the OpenSSL style configuration
        described in the APR documentation. This connector
                                should be used when APR(tcnative-1.dll)is used -->
    <!--
    <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
               maxThreads="150" scheme="https" secure="true"
               clientAuth="false" sslProtocol="TLS"
```

```
                                    SSLCertificateFile="../conf/localhost.crt"
                                    SSLCertificateKeyFile="../conf/localhost.key"
                                    SSLPassword="intellicus" />
-->
```

You may change the port too, if needed.

Note: Optionally you can generate your own certificate and key files. Please refer the following URL's Configuration section

http://tomcat.apache.org/tomcat-6.0-doc/ssl-howto.html

Linux / Solaris

In case of Linux or Solaris, Intellicus does not use APR by default. In this case a key store file should be used to run tomcat in HTTPS mode. Intellicus provides .keystore file in <Intellicus Install Path>/Jakarta/conf folder.

Remove comment from the Connector element related to SSL, which looks like this:

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443
        This connector uses the JSSE configuration. This connector
        should be used when APR(tcnative-1.dll) is not used-->
<!--
  <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
        maxThreads="150" scheme="https" secure="true"
        clientAuth="false" sslProtocol="TLS"
                                    keystoreFile="conf/.keystore" />
-->
```

You may change the port too, if needed.

Note: Optionally you can generate your own keystore file. Please refer the following URL's Quick start section

http://tomcat.apache.org/tomcat-6.0-doc/ssl-howto.html

Accessing Intellicus running under SSL

To access Intellicus portal running under SSL, your users will specify following URL in address-bar of the browser:

https://<serverIP>:<port>/intellicus

Example: To run Intellicus portal running under SSL (at port 8443) from the same machine, specify following URL in address-bar of the browser:

https://localhost:8443/intellicus .

Accepting the certificate

When for the first time user attempts to access Intellicus running under SSL, he / she is typically presented with a dialog containing the details of the certificate (such as the company and contact name), and asked if he / she wishes to accept the Certificate as valid and continue working.

Some browsers will provide an option for permanently accepting a given Certificate as valid. In this case, the user will not be bothered with a prompt each time he / she visit your site. Other browsers, it becomes necessary to accept the certificate during each visit to the site.