

# **Intrexx Professional Intrexx Compact**

RELEASE 5.1



**HTTPS Webservices anbieten**

# Inhaltsverzeichnis


<b>1. Einleitung.....</b>	<b>3</b>
<b>2. AXIS2 konfigurieren.....</b>	<b>3</b>



## Copyright






Das vorliegende Dokument ist in all seinen Teilen urheberrechtlich geschützt. Alle Rechte sind vorbehalten, insbesondere das Recht der Übersetzung, des Vortrags, der Reproduktion und der Vervielfältigung. Ungeachtet der Sorgfalt, die auf die Erstellung von Text, Abbildungen und Programmen verwendet wurde, können weder Autor, Herausgeber oder Übersetzer für mögliche Fehler und deren Folgen eine juristische Verantwortung oder irgendeine Haftung übernehmen.

Die in diesem Werk wiedergegebenen Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. können auch ohne besondere Kennzeichnung Marken sein und als solche den gesetzlichen Bestimmungen unterliegen.



## Schreibkonventionen

In diesem Handbuch werden Textstellen *kursiv* dargestellt, wenn sie sich auf Einstellungen in den abgebildeten Dialogen beziehen. Menüpunkte, die in Kontextmenüs erreichbar sind, sind immer auch über das Hauptmenü erreichbar. Hauptmenüpunkte werden nicht beschrieben, es sei denn, sie sind nicht über das Kontextmenü erreichbar. Eine Beschreibung der allgemeinen Hauptmenüpunkte finden Sie im Handbuch  *Portale*. Programmiercode im Text wird in der Schriftart *Courier* dargestellt. Kontextmenüs können mit einem Klick mit der rechten Maustaste auf das beschriebene Element geöffnet werden.

<intrexx> bezeichnet im Folgenden Ihren Intrexx Installationspfad, unter Windows z.B.  c:\intrexx\, unter Linux z.B.  /opt/intrexx/. Folgende Symbole werden für die Kennzeichnung von speziellen Informationen verwendet:


-  Informationen
-  Verweise auf ein Intrexx Handbuch
-  Verzeichnisse
-  URLs
-  Klick auf Schaltflächen

## Vorkenntnisse

Für das Verständnis dieser Dokumentation sind keine speziellen Vorkenntnisse erforderlich. Hilfreiche Informationen finden Sie in den Intrexx Handbüchern  *Setup* und  *Start*.

## 1. Einleitung

Im vorliegenden Dokument wird beschrieben, wie ein in Intrexx angelegter Webservice per https zertifiziert werden kann.

 Im Folgenden wird davon ausgegangen, dass bereits entsprechende Zertifikate sowie `keystore` und `truststore` vorliegen. Es ist darauf zu achten, dass `keystore` und `truststore` vom Typ *Java Keystore* (Dateiendung `jks`) sind.

## 2. AXIS2 konfigurieren

Um einen Transport per https einzurichten, müssen Änderungen an der Axis2-Konfigurationsdatei vorgenommen werden. Wechseln Sie dazu in das Verzeichnis

 `<intrexx>/org/<portal>/internal/webservice/provider/axis2/conf/`

und öffnen Sie die Datei `axis2.xml` in einem beliebigen Texteditor. Suchen Sie nun nach folgendem Eintrag:

```
<!-- ===== -->
<!-- Non-blocking http/s Transport Listener -->
<!-- the non blocking http transport based on HttpCore + NIO
extensions -->
<transportReceiver
class="de.uplanet.lucy.server.webservice.provider.axis2.transport.
nhttp.HttpCore
NIOListener" name="http">
    <parameter locked="false" name="port">WS_PORT</parameter>
<parameter locked="false" name="non-blocking">true</parameter>
<parameter locked="false" name="hostname">HOST_NAME</parameter>
</transportReceiver>
```

Unterhalb dieses Eintrags ist ein weiteres, momentan noch auskommentiertes, Element `<transportreceiver>`.

Entfernen Sie die Kommentar-Tags, um den Eintrag zu aktivieren.

```
<!-- the non blocking https transport based on HttpCore + SSL-NIO
extensions -->
<transportReceiver
class="de.uplanet.lucy.server.webservice.provider.axis2.transport.
nhttp.HttpCore
NIOSSLListener" name="https">
    <parameter locked="false" name="port">SSL_WS_PORT</parameter>
<parameter locked="false" name="non-blocking">true</parameter>
<parameter locked="false" name="keystore">



    <KeyStore>
        <Location>KEYSTORE.jks</Location>
        <Type>JKS</Type>
        <Password>KEYSTORE_PASSWORD</Password>
        <KeyPassword>KEY_PASSWORD</KeyPassword>
    </KeyStore>
</parameter>
```

```

<parameter locked="false" name="truststore">
  <TrustStore>
    <Location>TRUSTSTORE.jks</Location>
    <Type>JKS</Type>
    <Password>TRUSTSTORE_PASSWORD</Password>
  </TrustStore>
</parameter>
<parameter name="SSLVerifyClient">require</parameter>
<!--      supports optional|require or defaults to none -->
</transportReceiver>

```

Folgende Werte sind korrekt auszufüllen:

Parameter	Beschreibung
<b>SSL_WS_PORT</b>	Port, über den der https-Webservice aufgerufen werden kann. Es ist darauf zu achten, dass dieser Port vom Port für ungesicherte Webserviceaufrufe unterscheidet.
<b>KEYSTORE.jks</b>	Pfad zum Keystore im Format JKS. Der Pfad muss relativ zum Verzeichnis  <intrex>\org\<portal>\internal\webservice\provider\ angegeben werden.
<b>KEYSTORE_PASSWORD</b>	Passwort für den angegebenen Keystore.
<b>KEY_PASSWORD</b>	Passwort für den verwendeten Key.
<b>TRUSTSTORE.jks</b>	Pfad zum Truststore im Format JKS. Der Pfad muss relativ zum Verzeichnis  <intrex>\org\<portal>\internal\webservice\provider\ angegeben werden.
<b>TRUSTSTORE_PASSWORD</b>	Passwort für den angegebenen Truststore.

Wurden die Werte korrekt gesetzt, ist nach folgendem Eintrag zu suchen:

```
<transportSender
class="org.apache.axis2.transport.http.CommonsHTTPTransportSender"
name="https">
  <parameter name="PROTOCOL">HTTP/1.1</parameter>
  <parameter name="Transfer-Encoding">chunked</parameter>
</transportSender>
```



Unterhalb dieses Eintrags ist ein weiteres, momentan noch auskommentiertes, Element `<transportSender>`.

Entfernen Sie die Kommentar-Tags, um den Eintrag zu aktivieren.


```
<!-- the non-blocking https transport sender based on HttpCore +
NIO SSL extensions-->
<transportSender name="https"
class="de.uplanet.lucy.server.webservice.provider.axis2.transport.
nhttp.Http
CoreNIOSSLSender">
<parameter name="non-blocking" locked="false">true</parameter>
<parameter name="keystore" locked="false">
  <KeyStore>
    <Location>KEYSTORE.jks</Location>
    <Type>JKS</Type>
    <Password>KEYSTORE_PASSWORD</Password>
    <KeyPassword>KEY_PASSWORD</KeyPassword>
  </KeyStore>
</parameter>
<parameter locked="false" name="truststore">
  <TrustStore>
    <Location>TRUSTSTORE.jks</Location>
    <Type>JKS</Type>
    <Password>TRUSTSTORE_PASSWORD</Password>
  </TrustStore>
</parameter>

<parameter name="HostnameVerifier">DefaultAndLocalhost</parameter>
<!--supports Strict|AllowAll|DefaultAndLocalhost or the default if
none specified-->
</transportSender>
```

Folgende Werte sind korrekt auszufüllen:

Parameter	Beschreibung
<b>KEYSTORE.jks</b>	Pfad zum Keystore im Format JKS. Der Pfad muss relativ zum Verzeichnis  <intrex>\org\<portal>\internal\webservice\provider\ angegeben werden.
<b>KEYSTORE_PASSWORD</b>	Passwort für den angegebenen Keystore.
<b>KEY_PASSWORD</b>	Passwort für den verwendeten Key.
<b>TRUSTSTORE.jks</b>	Pfad zum Truststore im Format JKS. Der Pfad muss relativ zum Verzeichnis  <intrex>\org\<portal>\internal\webservice\provider\ angegeben werden.
<b>TRUSTSTORE_PASSWORD</b>	Passwort für den angegebenen Truststore.

Speichern Sie die Datei und starten Sie anschließend den Portaldienst neu. Rufen Sie den im Browser die WSDL-Datei auf, um die https-Authentifizierung zu testen. Achten Sie hierbei auf die korrekte Angabe von https statt http und des Ports. Ist der URL korrekt angegeben, muss das verwendete Zertifikat akzeptiert werden. Danach wird die WSDL-Datei im Browser angezeigt.

Wie ein https-Webservice in einem Portal verwendet werden kann, finden Sie im Handbuch  *https Webservices konsumieren*.