

# **Intrexx Professional Intrexx Compact**

RELEASE 5.2



**Whitepaper**

**Sicherheitsempfehlungen**

# Inhaltsverzeichnis


<b>1. Einführung .....</b>	<b>4</b>
1.1. Vorbereitung der Serverumgebung .....	4
<b>2. Intrexx Installation .....</b>	<b>4</b>
2.1. Intrexx Portal anlegen .....	5
<b>3. Trennung von Portal- und Datenbankenserver .....</b>	<b>6</b>
<b>4. Digitales Zertifikat für den Browser .....</b>	<b>8</b>
4.1. SSL Konfiguration des Webservers (IIS) .....	9
4.2. SSL Konfiguration des Webservers (Tomcat) .....	15
<b>5. Mobile Sicherheit .....</b>	<b>16</b>
<b>6. Zusätzliche Informationen .....</b>	<b>18</b>
<b>7. Über Intrexx .....</b>	<b>18</b>
<b>8. Über United Planet .....</b>	<b>20</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:\programme\intrexx\, unter Linux z.B.  /opt/intrexx/.

Mit <portal> wird ein bestehendes Intrexx Portalverzeichnis bezeichnet. Alle Dateien eines Portals finden Sie auf dem Intrexx Portal Server in diesem Verzeichnis, unter Windows z.B.  c:\ProgramData\intrexx\<portalname>. Das Portalverzeichnis können Sie in den Portaleigenschaften, erreichbar im Hauptmenü *Portal*, ermitteln.

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

## Vorkenntnisse


Für das Verständnis dieses Werkstattbeitrags sind Kenntnisse im Bereich Netzwerkadministration von Vorteil. Hilfreiche Informationen finden Sie in den Intrexx Handbüchern  *Setup* und  *Start*.

## 1. Einführung

Bei der Standardinstallation von Intrexx werden zunächst keine speziellen Sicherheitsmaßnahmen ergriffen, um z.B. die Kommunikation zwischen Client und Server vor Angriffen zu schützen. Um einen Portalserver vor dem Zugriff Dritter abzusichern, bedarf es aber einiger Maßnahmen, die hier im Nachfolgenden behandelt werden.

Mit diesem Whitepaper wird exemplarisch beschrieben, wie Sie einen Intrexx Portalserver mit verschiedenen Ansätzen vor Angriffen und unbefugten Zugriff schützen können.

Diese Anleitung richtet sich im Wesentlichen an Personen mit spezifischen Netzwerk- und Softwarekenntnissen, wie z.B. Systemadministratoren bzw. Fachleute.

 Die Beispiele, Anleitungen, etc. beziehen sich wenn nicht anders angegeben auf das Betriebssystem *Microsoft® Windows Server 2008 R2*.

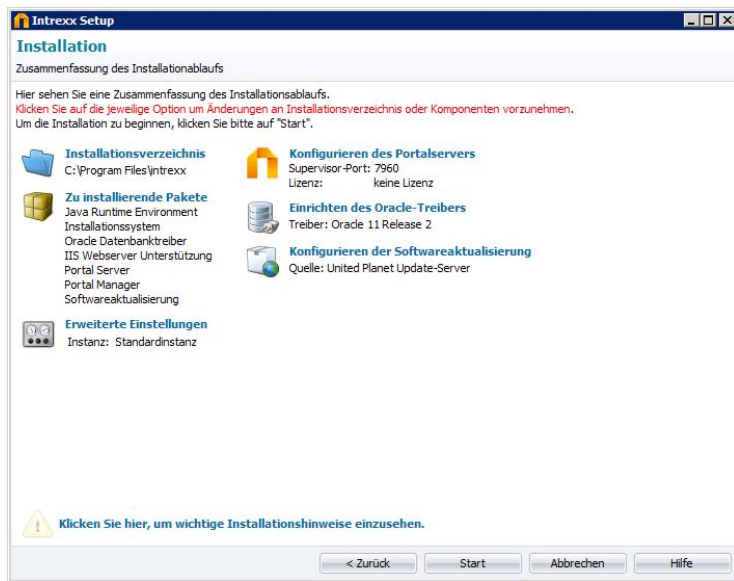
### 1.1. Vorbereitung der Serverumgebung

Die größtmögliche Sicherheit ist nur dann gewährleistet, wenn man bei der Auswahl der Serverplattform folgende Punkte beachtet:

- Aktuellste Serverversion (z.B. Windows Server 2008 R2)
- Installation aller Patches und (Sicherheits-)Updates der jeweiligen Plattform
- Drittanbietersoftware (z.B. Adobe Reader, etc.) stets auf dem aktuellsten Stand halten oder gar vollständig vermeiden
- Generell sichere Benutzerkennwörter verwenden
- Ggf. den Einsatz einer Antivirenlösung in Betracht ziehen
- Ggf. den Server in ein demilitarisiertes Netzwerk integrieren (siehe [Punkt 3.1](#))

## 2. Intrexx Installation

Die Intrexx Installation erfolgt in wenigen Schritten. Dabei ist zu beachten, dass man den Supervisor-Port (Standard-Einstellung auf 7960) umstellen kann. Das ist aus sicherheitstechnischer Sicht aber irrelevant und dient primär der Verwaltung mehrerer installierter Instanzen (Parallelinstallation).



## 2.1. Intrexx Portal anlegen

Beim Anlegen eines Portals gibt es gleich mehrere sicherheitsrelevante Punkte zu beachten.

Im ersten Schritt (*Portalmanager / Portal neu*) wird zunächst der Portalname vergeben. Unter diesem Portalnamen (z.B. *Demo*) wird das Portal dann später erreichbar sein. Das ist deswegen wichtig, weil das Portal über eine URL aufgerufen wird. Diese URL enthält u.a. den Servernamen. In unserem Beispiel lautet der Servername *unitedplanet* und das Portal heißt *Demo*.

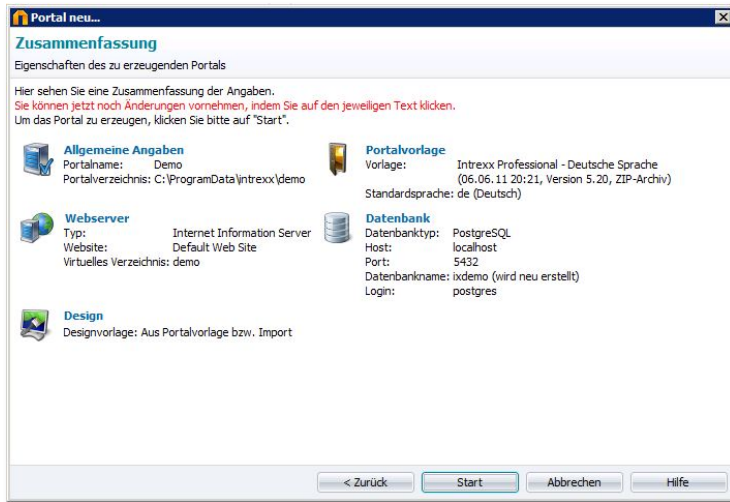
Die komplette URL (zunächst unverschlüsselt) lautet also: <http://unitedplanet/demo>. In Punkt 4, *SSL Konfiguration des Webserver* wird darauf eingegangen, wie man die Portalnutzung via SSL Zertifikat verschlüsselt.

Im nächsten Dialog hat man die Auswahl zwischen einer *Portalvorlage* oder einem *Neuen Portal*.

Danach wird der Datenbankserver gewählt (z.B. PostgreSQL).

Im darauf folgenden Dialog werden nun die Verbindungsdaten zur Datenbank abgefragt. Aus sicherheitstechnischer Sicht kann es Sinn machen, Portal und Datenbank auf unterschiedlichen Servern (möglicherweise noch in unterschiedlichen Netzwerkbereichen) laufen zu lassen. Auf diesen Aspekt wird in Punkt 3, *Trennung von Portal- und Datenbankserver* näher eingegangen.

Es folgt die Zusammenfassung der Eigenschaften des zu erzeugenden Portals.



Mit einem Klick auf  **Start** wird das Portal erzeugt.

### 3. Trennung von Portal- und Datenbankenserver

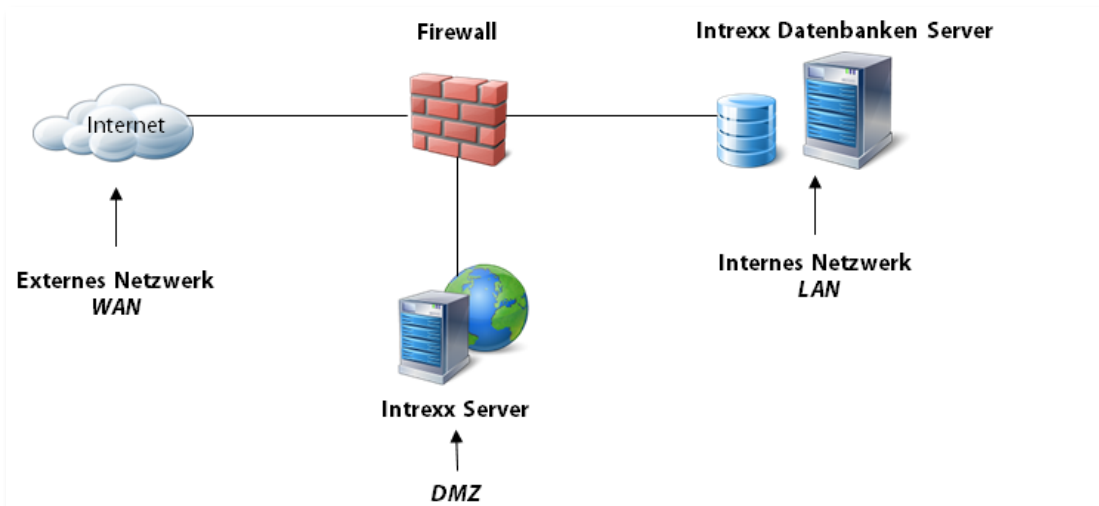
Wie in 2.1 bereits erwähnt, ist es von Bedeutung, ob Portal- und Datenbankenserver auf derselben Maschine liegen, oder ob sie physikalisch und/oder netzwerktechnisch getrennt sind.

In der Datenbank werden alle kritischen Daten wie z.B. Benutzeranmeldung, etc. gespeichert. Die Daten von Intrexx selbst sind lediglich funktional. Sie enthalten also keine kritischen Firmendaten.

Soll der Portalserver von extern erreichbar sein, so muss man zwangsläufig Zugang auf das interne Netzwerk gewähren.

In diesem Fall empfiehlt es sich, eine eigens dafür erstellte DMZ (= Demilitarized Zone) zu erstellen und den Server mit der Intrexx Installation in diese zu setzen. Die Datenbank sollte dann in das geschützte interne Netzwerk gelegt werden, sofern diese geschäftskritische Daten (z.B. Patientendaten) enthält.

Das folgende Schaubild soll die einfachste Form eines DMZ-Aufbaus veranschaulichen:



Das Schaubild zeigt ein einstufiges Firewall-Konzept. LAN und DMZ stellen logisch getrennte Netze dar. Physikalisch sind beide Netze mit der Firewall verbunden. Die Erreichbarkeit aus DMZ und LAN über Internet (z.B. http, smtp, etc.) wird über Firewall-Regeln definiert.

In einem Zwei- oder Mehrstufigen Firewall-Konzept wird die DMZ zusätzlich durch eine eigene, zusätzliche Firewall geschützt. Die Netze sind logisch (ggf. auch physikalisch) getrennt. Die Erreichbarkeit muss dann ebenfalls über Firewall-Regeln definiert und ggf. auf mehrere Firewalls abgestimmt werden.

Weiterführende Informationen finden Sie hier:

 [http://de.wikipedia.org/wiki/Demilitarized\\_Zone](http://de.wikipedia.org/wiki/Demilitarized_Zone).

### **Für Intrexx hat das nun folgende Auswirkungen:**

Die Installation von Intrexx erfolgt auf dem Server in der DMZ. Die Datenbank für das Portal wird im internen Netzwerk (LAN) installiert. Zusätzlich kann man auch den Portalmanager auf einem Client/Server im LAN installieren.

Je nach Konfiguration müssen dann Ports von dem einen in das andere Netz freigeschaltet werden.

In dem Beispiel oben muss also der Datenbank-Port (z.B. 1433) von der DMZ in das interne Netzwerk (LAN) freigeschaltet werden.

Zusätzlich muss der Intrexx Portal-Manager Port (7960), sowie die Soap-Ports eines jeden Portals (8101 & 8102 für das erste Portal, 8103 & 8104 für das zweite Portal, usw.) von dem internen Netzwerk (LAN) in die DMZ freigeschaltet werden, um auf den Intrexx-Server verbinden zu können.

Soll das Portal zusätzlich noch extern per Browser erreichbar sein, muss noch der http-Port (Port 80) per Port-Weiterleitung/NAT von extern in das interne Netz erfolgen.

Weiterführende Informationen finden Sie hier:

 <http://de.wikipedia.org/wiki/Portweiterleitung>

***Wichtig: Es müssen je nach Konfiguration und Anforderung spezifische Ports in bestimmte Richtungen freigeschaltet werden. Das sollte gut durchdacht sein. Denn offene Ports bedeuten stets auch ein erhöhtes Sicherheitsrisiko. So sollte es dringend vermieden werden, Ports von der DMZ in das interne Netzwerk freizuschalten.***

***Im hier beschriebenen Beispiel wird lediglich der Datenbank-Verbindungsport freigeschaltet. Die Freischaltung dieses Ports beinhaltet auch, dass man die Datenbank dahinter stets aktualisiert bzw. alle relevanten Sicherheitsupdates eingespielt sind, um die größtmögliche Sicherheit zu gewährleisten.***

In der folgenden Übersicht, werden Standardports aufgelistet, welche man ggf. im Zusammenhang mit Intrexx benötigt:

Intrexx Portal Manager: 7960  
Intrexx Soap Ports: 8101, 8102 für das erste Portal (Für jedes weitere Portal 8103+n)  
Microsoft® SQL Server: 1433  
PostgreSQL: 5432  
IBM DB2: 50000  
Oracle: 1521  
Apache Derby: 1527  
Internet Information Service (IIS): 80  
HTTPS: 443  
SMTP: 25  
Apache Tomcat: 8080

Weitere Portbeispiele finden Sie hier:

 [http://de.wikipedia.org/wiki/Port\\_%28Protokoll%29](http://de.wikipedia.org/wiki/Port_%28Protokoll%29)

#### 4. Digitales Zertifikat für den Browser

Die Verwendung eines Intrexx Portals erfolgt generell über einen Webbrowser. Die Anfrage an den Webserver bei einem Portalaufruf erfolgt i.d.R. über einen DNS Namen wie z.B. *webserver* sowie den Namen des zugehörigen Portalnamens wie z.B. *sslportal*.

Durch Aufruf der URL <http://webserver/sslportal> wird das Portal intern (LAN) aufgerufen. Möchte man das Portal stattdessen über das Internet (WAN) aufrufen, so muss (neben einer öffentlichen IP-Adresse) eine offizielle Domain registriert werden. Hat man z.B. die Domain *example.org* registriert, so lässt sich das Portal bei entsprechender Port-Weiterleitung von Port 80 WAN-to-LAN/DMZ sowie der Registrierung eines DNS Eintrags, über die URL <http://www.unitedplanet.de/sslportal>, aufrufen.

Für die entsprechende Firewall-Konfiguration siehe **Punkt 3**.

Der Aufruf dieser URL erfolgt dann unverschlüsselt. Die Echtheit des auf die URL <http://www.unitedplanet.de/sslportal> eingetragenen Servers (hier *webserver*) ist nicht gewährleistet. Durch einen sog. *Man-in-the-middle-Angriff* kann ein Dritter vorgeben, auf die DNS-Anfrage zu antworten, dahinter aber einen fremden Server zwischenschalten, um so jeglichen Traffic mitzuschneiden.

 <http://de.wikipedia.org/wiki/Man-in-the-middle-Angriff>

Um die Echtheit des angefragten Servers zu gewährleisten, ist es nötig ein digitales Zertifikat zu verwenden.

Ein digitales Zertifikat soll die Identität & Echtheit eines öffentlichen Schlüssels und damit eines Benutzers, Computers oder Netzwerkes bestätigen. Diese Bestätigung erhält man von einer sog., *Certification Authority* kurz CA genannt (zu Deutsch *Zertifizierungsinstanz*). Offizielle Zertifizierungsstellen sind zum Beispiel VeriSign, Thawte oder GlobalSign, welche auch in den gängigen Browsern bereits „ab Werk“ hinterlegt sind.

Da die Ausstellung eines öffentlichen Zertifikats über offizielle Stellen im Regelfall kostenpflichtig ist, lässt sich ein digitales Zertifikat auch selbst (z.B. mittels Webserver) ausstellen.

Im folgenden Abschnitt wird die Ausstellung eines eigenen digitalen Zertifikats durch den Webserver IIS von Microsoft® erläutert, welches dann für ein Intrex Portal verwendet werden kann.

- Beachten Sie bitte, dass selbst ausgestellte Zertifikate u.U. Sicherheitswarnungen im Browser hervorrufen können, da es sich bei Zertifikatsersteller und zertifiziertem Server um dieselbe Stelle handelt, und sich ein solches Zertifikat somit nur für Testumgebungen eignet. Im Produktiveinsatz von extern erreichbaren Portalen sollten offizielle Zertifizierungsstellen beauftragt werden.

## 4.1. SSL Konfiguration des Webserver (IIS)

Im Folgenden werden die Schritte erklärt, die dazu benötigt werden, ein digitales Zertifikat selbst zu erstellen, um es anschließend für das Intrex Portal nutzen zu können.

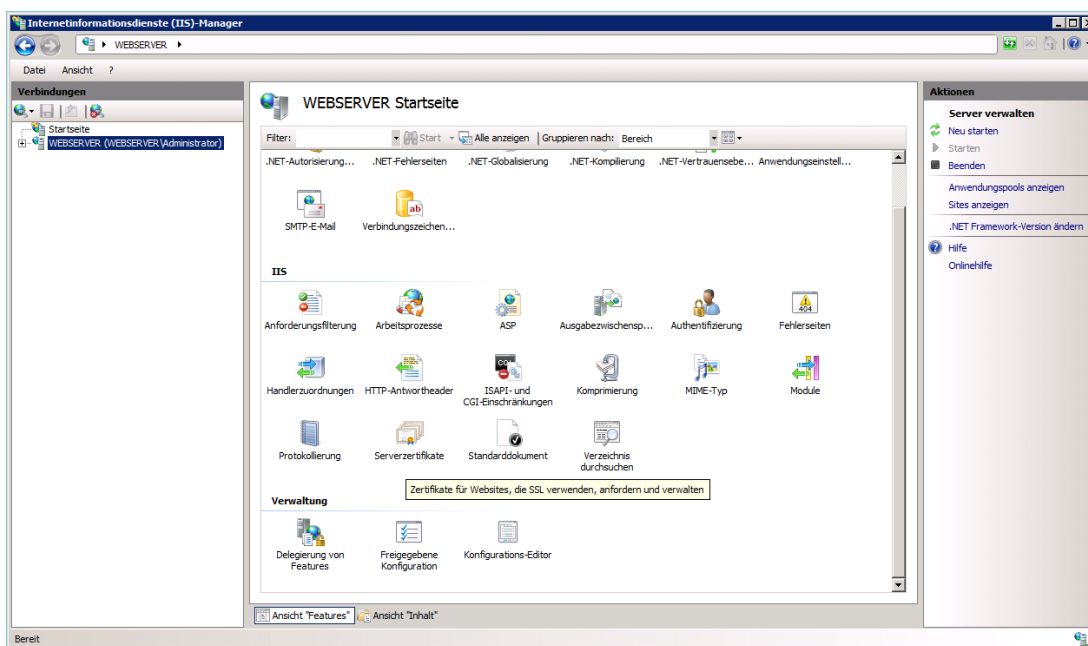
Bei der in diesem Beispiel verwendeten Serverumgebung handelt es sich um:

Serverversion: *Windows Server 2008 R2* (Patchlevel Stand: November 2011)

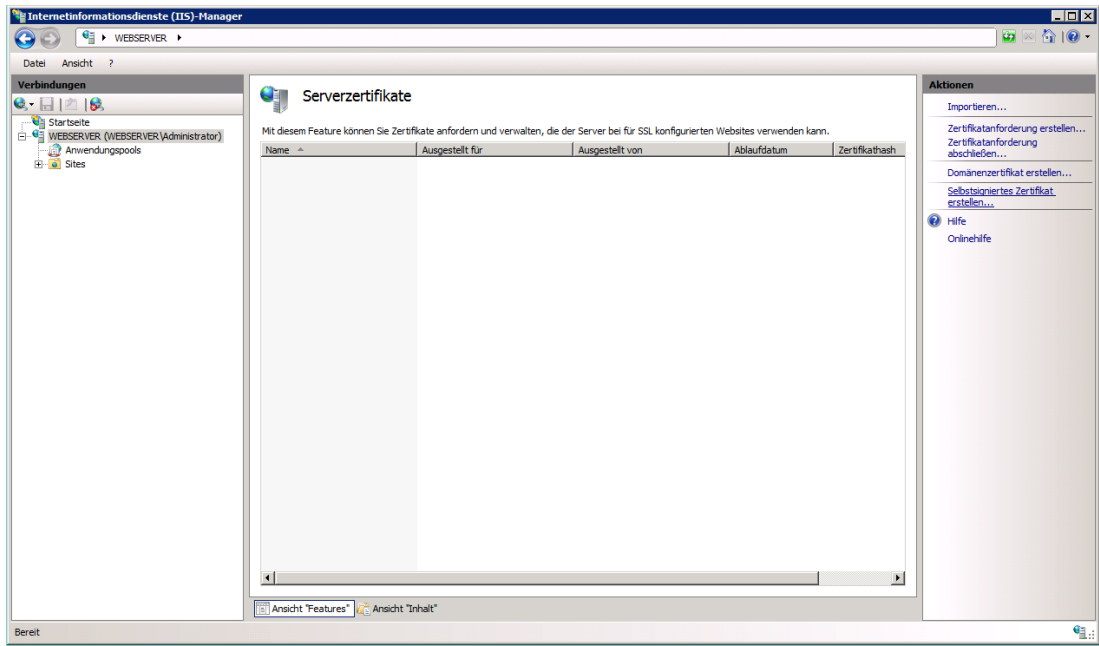
Servername: *webserver*

Internet Information Services (IIS) Version: 7.5 (inkl. IIS-Manager)

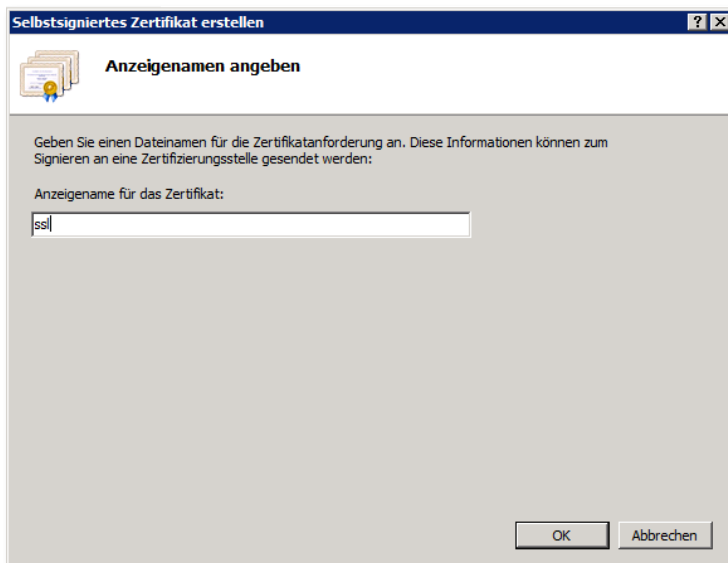
Zuerst wird der IIS-Manager gestartet und der Menüpunkt *Serverzertifikate* aufgerufen.



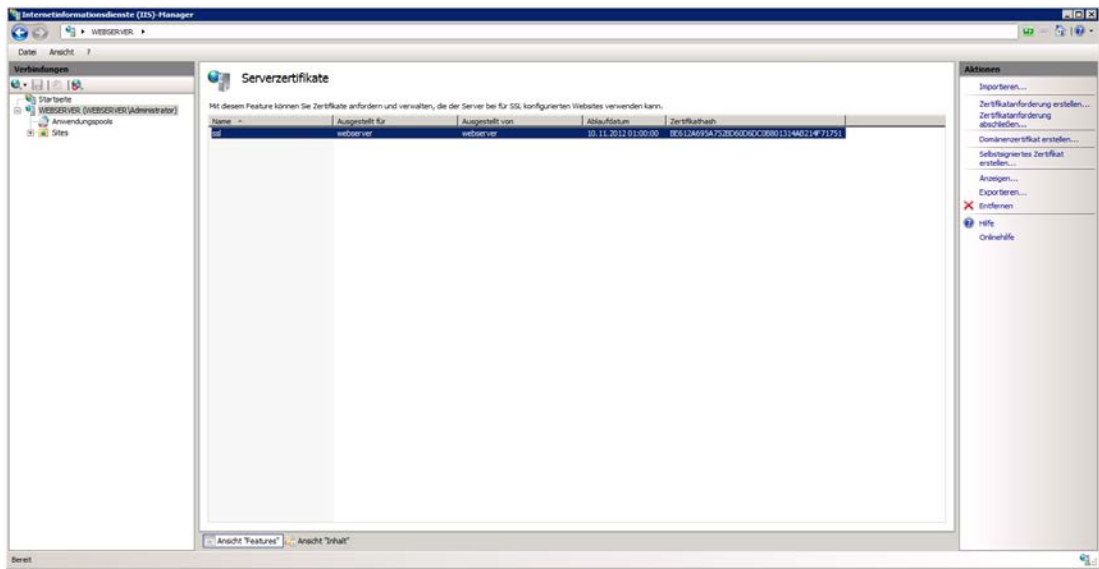
Rechts unter *Aktionen* die Option *Selbstsigniertes Zertifikat erstellen...* wählen.



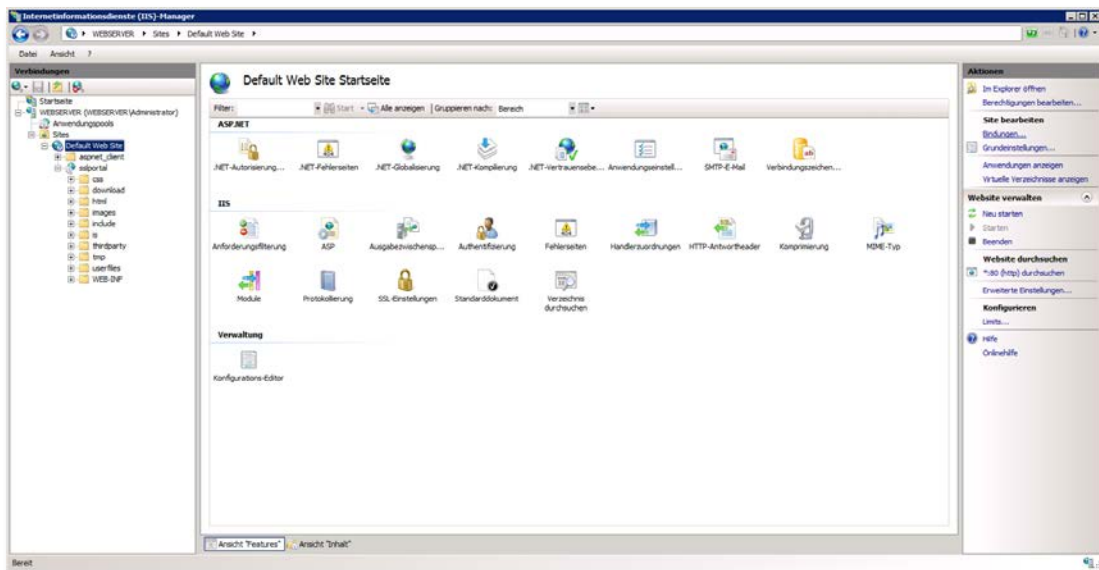
Danach muss ein Anzeigename (hier *ssl*) eingetragen werden. Mit *Ok* bestätigen.



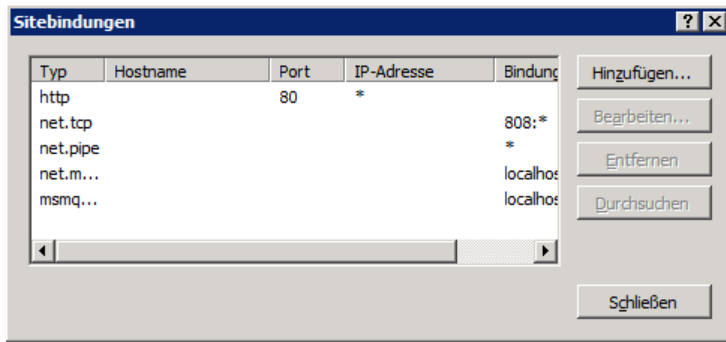
Das Zertifikat erscheint nun unter *Serverzertifikate*.



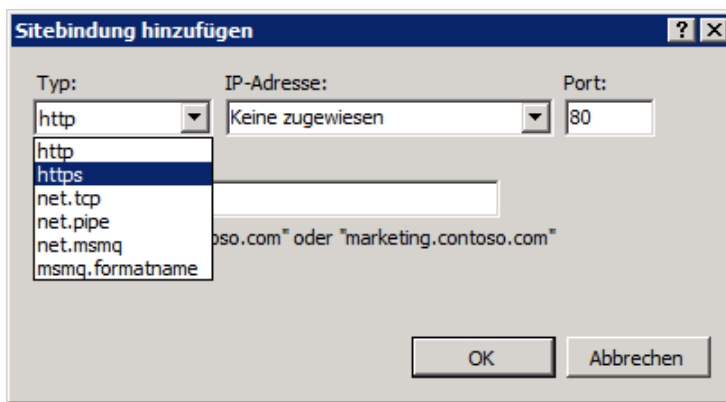
Markieren Sie in der linken Spalte den Menüpunkt *Default Web Site* und wählen rechts unter *Seite bearbeiten* den Punkt *Bindungen...*



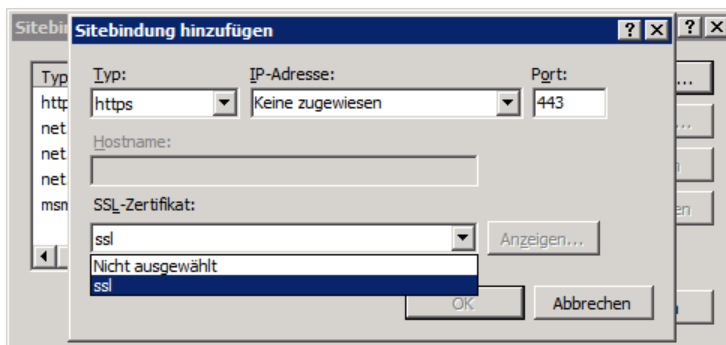
Unter *Sitebindungen* die Option *Hinzufügen* wählen.



Hier wird *https* gewählt. Der Port 443 wird automatisch hinterlegt.

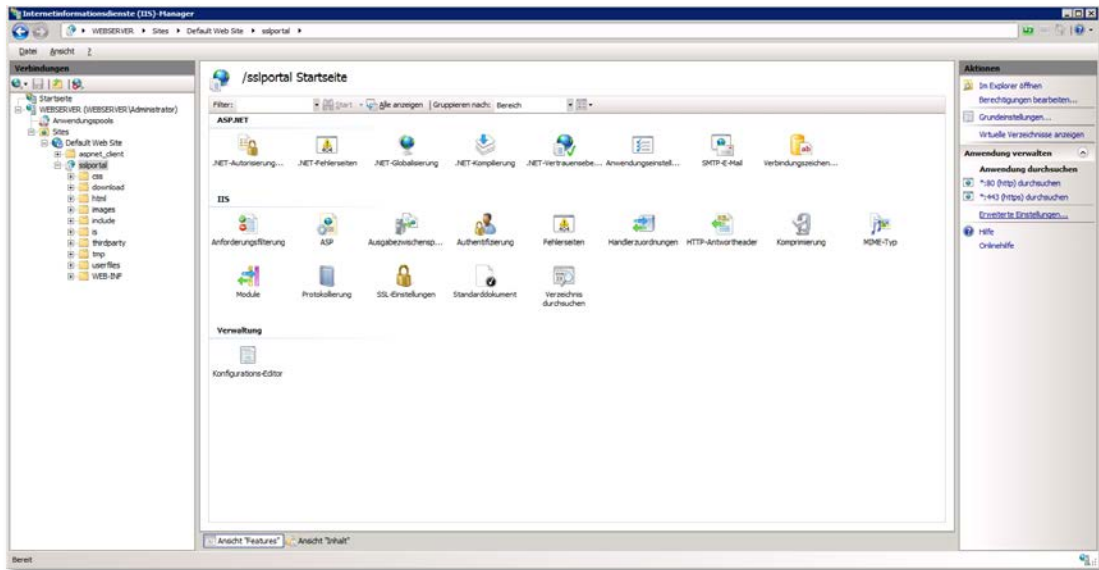


Unter *SSL-Zertifikate* wird nun das im vorigen Schritt erstellte Zertifikat (hier *ssl*) gewählt und mit *Ok* bestätigt

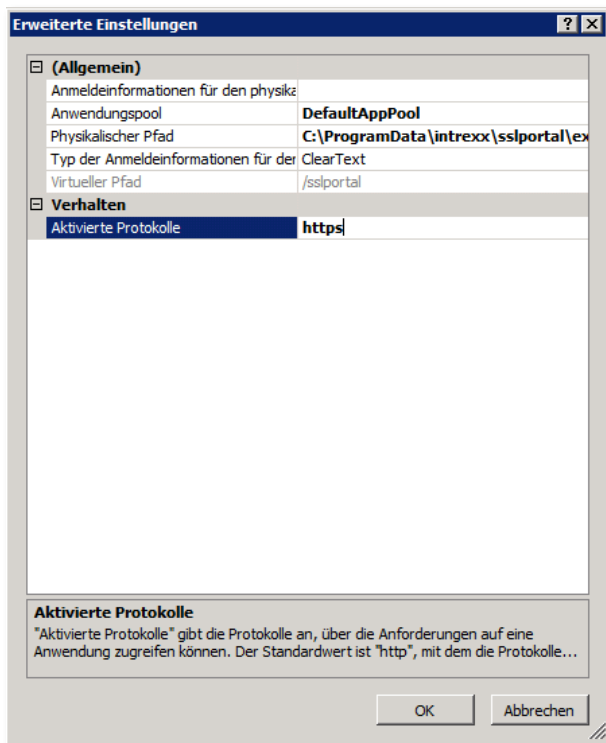


Im Optionsfeld *IP-Adresse* lässt sich eine Bindungsart (z.B. *http*) für jede Website bzw. jedes virtuelle Verzeichnis definieren. Es können also beliebig viele virtuelle Verzeichnisse mit unterschiedlichen IP-Adressen und den dazugehörigen Bindungen existieren.

Anschließend links die Intrexx Portal-Website (hier *sslportal*) markieren und auf der rechten Seite unter *Aktionen* der Menüpunkt *Erweiterte Einstellungen...* wählen.



Im folgenden Fenster unter *Aktivierte Protokolle* den Eintrag *https* vornehmen und mit *Ok* bestätigen.

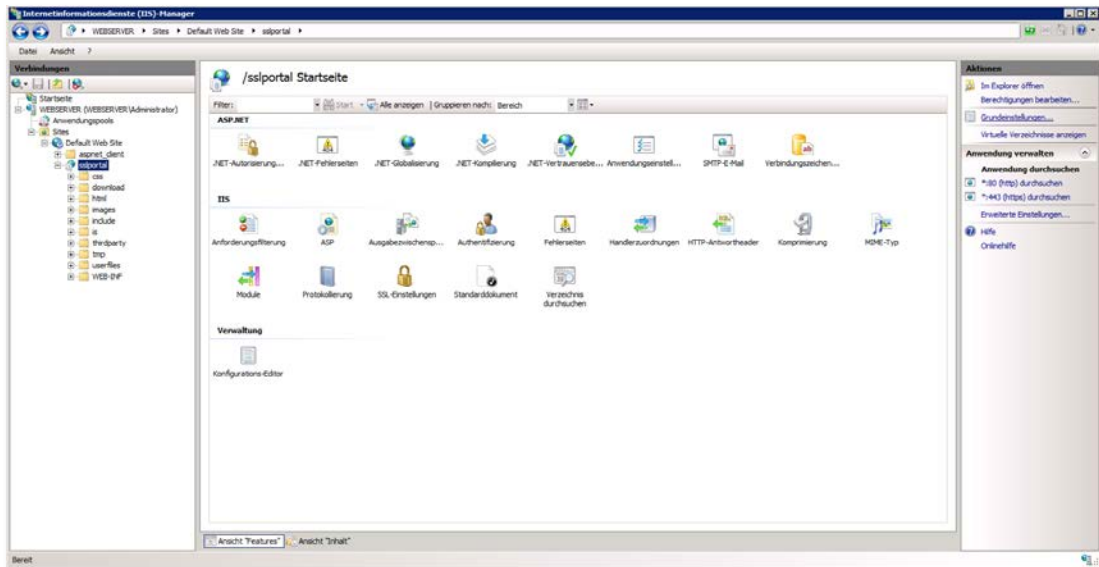


Der Eintrag *https* hat zur Folge, dass sowohl *http*, als auch *https* zum Aufrufen des Portals (*http://.../Portalname* & *https://.../Portalname*) verwendet werden können.

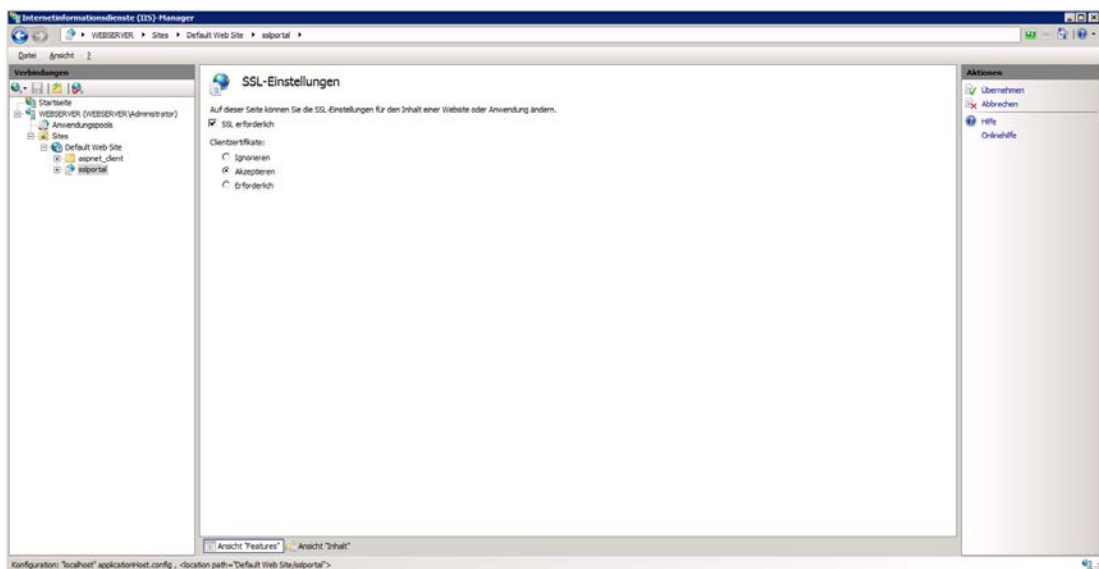
### Optional:

Bei Bedarf kann man den Webserver so konfigurieren, dass er nur noch Verbindungen per https zulässt. Dabei wird wie folgt vorgegangen:

Auf der linken Seite wieder die entsprechende Seite (hier *sslportal*) markieren und die Option *SSL-Einstellungen* wählen.



In den SSL-Einstellungen kann nun bestimmt werden, ob SSL zwingend erforderlich ist.



Wählt man die Einstellung *SSL erforderlich* und bestätigt dies rechts mit *Übernehmen*, so lässt sich das entsprechende Portal nur noch über https (und nicht mehr per http) aufrufen. Darüber hinaus kann bei dieser Option noch differenziert werden, wie Clientzertifikate behandelt werden.

Auszug aus der IIS Hilfe:

*Ignorieren: Dies ist die Standardoption. Bei dieser Einstellung werden keine Clientzertifikate akzeptiert, die bereitgestellt werden.*

*Hinweis:*

*Bei dieser Option ist es nicht erforderlich, die Identität von Clients zu überprüfen, bevor der Zugriff auf Inhalte gewährt wird. Daher stellt dies die Einstellung mit der niedrigsten Sicherheit dar.*

*Akzeptieren: Wählen Sie diese Einstellung aus, wenn Sie Clientzertifikate akzeptieren möchten (sofern diese bereitgestellt werden) und die Clientidentität überprüfen möchten, bevor dem Client der Zugriff auf die Inhalte gewährt wird.*

*Erforderlich: Wählen Sie diese Option aus, um festzulegen, dass Zertifikate die Clientidentität überprüfen müssen, bevor dem Client der Zugriff auf die Inhalte gewährt wird.*

Der Aufruf des Intrexx Portals erfolgt nun über http oder (vorzugsweise) https. Wird https verwendet, bringt der Browser eine Zertifikatswarnung, weil das ausgestellte Zertifikat nicht durch eine offizielle Zertifizierungsautorität bestätigt wurde. Bei einem selbst ausgestellten Zertifikat muss diese Warnung darum immer ignoriert werden. Das Zertifikat sollte heruntergeladen und installiert werden.

## 4.2. SSL Konfiguration des Webservers (Tomcat)

Setzen Sie Apache Tomcat als Webserver ein, führen Sie bitte folgende Schritte aus:

Erstellen Sie mit dem Java keytool ein selbstsigniertes Zertifikat für Tomcat. Öffnen Sie eine Kommandozeile und wechseln Sie in das Intrexx-Installationsverzeichnis `<intrexx>/jre/<os>/<bit>`. Führen Sie folgenden Befehl aus:

```
keytool -genkey -alias tomcat -keyalg RSA
```

Beispiel:

```
c:\>cd c:\intrexx52\bin\windows\amd64
c:\intrexx52\bin\windows\amd64>keytool -genkey -alias tomcat -keyalg RSA
```

Folgen Sie den Anweisungen auf der Konsole und geben Sie die gewünschten Daten ein. Nach Abschluss ist unter `C:\Benutzer\<username>\` eine Datei `.keystore` zu finden. Kopieren Sie die Datei in das Verzeichnis `<intrexx>/tomcat/conf/`.

Im nächsten Schritt ist die Datei `server.xml` im Verzeichnis `<intrexx>/tomcat/conf/` mit einem beliebigen Editor zu öffnen. Navigieren Sie zum Abschnitt

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
```


und kommentieren Sie den darauf folgenden Abschnitt ein, in dem Sie vor und nach dem Abschnitt

```
<Connector port="8443" maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25"
maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS" />
```

die Kommentarzeichen entfernen. Fügen Sie hier die beiden neuen Attribute *keystoreFile* und *keystorePass* hinzu.

```
<Connector port="8443" maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25"
maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true"
keystoreFile="conf/.keystore"
keystorePass="changeit"
clientAuth="false" sslProtocol="TLS" />
```

Tragen Sie unter *keystorePass* das Passwort ein, das Sie beim Anlegen des Zertifikats vergeben haben. Speichern Sie die Eingaben und starten den Tomcat-Dienst über die Dienstkonsole neu.

In einem Webbrowser können Sie nun über <https://localhost:8443> die SSL-Verbindung testen. Prüfen Sie darüber hinaus die Datei *tomcat.log* unter  *<intrex>/log*.

Weitere Informationen finden Sie unter  [Apache Tomcat SSL Configuration](#).

## 5. Mobile Sicherheit

Intrex Portale lassen sich ohne Einschränkung auch über jedes mobile Endgerät nutzen, das über einen Browser verfügt. Die Erreichbarkeit erfolgt dann wie im konventionellen Fall über dieselbe URL. Ebenso lässt sich ein SSL Zertifikat damit nutzen.

Man gelangt mit dem mobilen Endgerät also an genau dieselben Informationen wie vom PC aus auch. Da mobile Endgeräte wie iPhone etc. aber nicht so gut kontrollierbar sind wie PC-Systeme, ist die Sicherheit der Daten gefährdet.

Für den Einsatz mobiler (und oft auch privater) Endgeräte der Mitarbeiter bedarf es also besonderer Vorkehrungen. Diese sind aber ohne eine zentrale Verwaltung nur schwer zu treffen.

Grundsätzlich gilt:

- Betriebssysteme der Geräte immer aktuell halten
- Keine Custom-Betriebssysteme verwenden
- Sicherheitsfeatures der jeweiligen Plattform nutzen (z.B. PIN, Entsperrcode, etc.)
- Zusatzsoftware nur wenn nötig einsetzen
- Keine Benutzernamen oder Kennwörter speichern
- Kein offenes WLAN verwenden
- Wenn möglich VPN Software nutzen
- Keine veralteten Geräte (und damit Betriebssysteme) zulassen
- etc.

Diese allgemeinen Sicherheitsempfehlungen sind für alle gängigen Plattformen wie iOS, Android, Blackberry, etc. gültig.

Dennoch gibt es für die einzelnen Plattformen unterschiedliche Ansätze. So lässt sich ein Blackberry Gerät (Stand November 2011) durch den Blackberry Enterprise Server am besten in ein bestehendes Sicherheitskonzept integrieren. Durch den BES lassen sich Sicherheitsrichtlinien sehr differenziert darstellen. Auch das Löschen des Geräts aus der Ferne (Remote) lässt sich damit durchführen.

Bei iOS oder Android muss man hierfür auf Dritthersteller-Software (Mobile Device Management) zurückgreifen und die Funktionalität ist je nach Anforderung eingeschränkt. Die Funktionalität eines serverseitigen Löschens der mobilen Endgeräte im Verlustfall ist sehr zu empfehlen, da gestohlene oder verlorengegangene Endgeräte das höchste Sicherheitsrisiko darstellen.

Eine weitere Schwierigkeit stellt die Verwaltung der mobilen Endgeräte dar. Sowohl die firmeneigenen als auch privaten Geräten müssen zwingend erfasst und damit verwaltet werden, um gezielt auf Verlust eines Gerätes (und den damit verbundenen Sicherheitsrisiken) reagieren zu können.

## 6. Zusätzliche Informationen

Die in 4.1 beschriebene Konfiguration des Webservers funktioniert analog auch mit anderen Webservern wie z.B. Apache Tomcat.

Zusätzlich gibt es kostenlose Projekte wie OpenSSL, um SSL zu implementieren:

 <http://www.openssl.org/>

Mit Intrexx ist es ebenfalls möglich, Webservices über SSL zu konsumieren bzw. anzubieten:

 [HTTPS Webservices anbieten](#)

Grundsätzlich sollte man Intrexx regelmäßig sichern. Dazu gehört sowohl die Sicherung der Datenbank (Datenbankenexport) sowie die Sicherung der Intrexx-Verzeichnisse (s. Seite 3).

## 7. Über Intrexx

Intrexx ist eine **integrierte plattformunabhängige Entwicklungsumgebung** zur schnellen und einfachen Erstellung und Verwaltung von z.B. multilingualen **Enterprise-, Kundenportalen oder Webapplikationen**. Intrexx ist **einfach erlernbar** und bedarf keiner Programmierkenntnisse. Das Erstellen des Portals erfolgt nach dem Drag & Drop Prinzip. Wer also eine Excel-Tabelle erstellen kann, der kann auch Anwendungen und Formulare wie z.B. ein Urlaubsantragsverfahren erstellen.



Neben dem Erstellen und Betreiben eines Portals lassen sich mit Intrexx ganz einfach vorhandene **Daten integrieren** und **Prozessabläufe** per Mausklick automatisieren. Durch die nahtlose Unterstützung von **mobilen Endgeräten** können alle Daten sehr schnell und verblüffend einfach für Smartphones wie iPhone oder BlackBerry zur Verfügung gestellt werden. So sind alle Mitarbeiter auch außer Haus ohne Medienbruch in alle Geschäftsprozesse eingebunden und ein optimaler Informationsfluss ist gewährleistet.

Intrexx ist dank unzähliger vorbereiteter Templates **schnell eingerichtet** und erlaubt den Aufbau eines Portals oder Intranets innerhalb kürzester Zeit.

Intrexx ist **komplett**. Es verfügt über alles, was man benötigt, um ein leistungsfähiges Portal zu entwickeln und erfolgreich zu betreiben.

### Intrexx enthält (Auszug):

- Modul *Applikationen* zur Anwendungs- und Formularerstellung
- Modul *Design* zur Layouterstellung und Bearbeitung der Menüstruktur
- Modul *Prozesse* für das Abbilden von Workflows und das Erstellen mobiler Anwendungen
- Web Service Orchestrierung
- Komplette Benutzerverwaltung mit LDAP-Anbindung
- Datenintegration mit Einbindung externer Datenquellen (z.B. ERP-Daten)
- Volltext-Suchmaschine

- Link-Integration zur Einbindung von externen Webseiten
- Diverse Werkzeuge zur komfortablen Administration des Portals

Intrex ist **Standardsoftware**, sehr oft installiert und somit auch sehr **preiswert**. Das System besteht im Wesentlichen aus zwei Teilen:

**Intrex Portal Manager:** Er wird auf einem beliebigen Client oder auf dem Server installiert und verfügt über alle Komponenten um Layout, Menü oder Applikationen zu entwickeln und zu verwalten. Auch die Einrichtung der Benutzer mit den Rechten an den jeweiligen Anwendungen eines Portals erfolgt im Portal Manager von Intrex.

**Intrex Portal Server:** Er wird auf einem Server installiert und steuert alle Transaktionen der angelegten Webapplikationen und Portale. Er überwacht die Rechte der Benutzer innerhalb der Transaktionsvorgänge, steuert die gesamten Businesslogiken und regelt den Zugriff auf die Datenquellen.

**Intrex Professional ist grundsätzlich kostenlos per Download verfügbar.** Die Testphase ist auf 30 Tage beschränkt, kann jedoch bei Bedarf entsprechend verlängert werden. Es gibt während dieser Zeit keinerlei Einschränkungen im Programm, alle Module, Anwendungen oder Applikationen können uneingeschränkt betrieben, getestet und verändert werden. Ebenfalls ist die Anzahl der User nicht beschränkt. Die verbleibende Testzeit wird immer in der rechten unteren Ecke des Portal Managers angezeigt. Am Ende der Testphase wird das System automatisch deaktiviert. Über eine spezielle Info-Seite kann bei Bedarf die Testdauer verlängert oder eine gültige Lizenz erworben werden. Alle während der Testphase angelegten Applikationen und erfassten Daten bleiben selbstverständlich erhalten und können weiterhin eingesetzt werden.

Für den Einsatz in einer Produktivumgebung werden für den Betrieb der Applikation oder des Portals entsprechende Benutzerlizenzen für den Intrex Portal Server erforderlich.

Es stehen verschiedene Lizenzgrößen einschließlich einer Runtime-Lizenz zur Verfügung. Intrex passt sich durch die **transparente Lizenzierung** jeder Unternehmensgröße an.

Im Intrex Application Store befinden sich hunderte von freien und kostenpflichtigen Unternehmensanwendungen, die mit wenigen Klicks dem eigenen Portal hinzugefügt werden. Weiterhin gibt es auch fertige Lösungen zum Management von Unternehmensprozessen. Diese komplexen Webapplikationen werden Studio-Lösungen genannt. Sie sind in der Regel bereits im Intrex Portal Manager als Applikationsvorlage enthalten, bedürfen aber im Falle einer produktiven Verwendung einer gesonderten Lizenzierung. Diese erfolgt durch eine einmalige Serverlizenz unabhängig von der Benutzeranzahl.

Der Abschluss eines (optionalen) Service- und Wartungsvertrags gewährleistet immer neueste Technologien und Releases und bietet effizienten Support durch United Planet.

**Intrex Professional steht unter [www.intrex.com/de/intrex-5-professional](http://www.intrex.com/de/intrex-5-professional) kostenlos zum Download bereit.**

## 8. Über United Planet

United Planet gehört mit über 4.000 Installationen und mehr als 500.000 Nutzern seiner Portalsoftware Intrexx allein im deutschsprachigen Raum zu den Marktführern im Segment der mittelständischen Wirtschaft, der öffentlichen Verwaltung und bei Organisationen (z.B. Kliniken). Geführt wird das Unternehmen von Lexware-Gründer Axel Wessendorf.

Mit der plattformunabhängigen Standardsoftware Intrexx lassen sich webbasierte Applikationen bis hin zu kompletten Intranets/Enterprise Portalen mit modernsten Funktionalitäten deutlich schneller erstellen als mit vergleichbaren Programmen wie z.B. Microsoft SharePoint.

Intrexx erlaubt die Einbindung vorhandener Daten aus ERP-Systemen, Microsoft Exchange, Lotus Notes etc., die Erstellung produktiver Workflows und die Generierung von mobilen Apps für Smartphones und Tablet PCs aller Hersteller. Im Intrexx Application Store stehen hunderte von fertigen Apps und komplette Portale zum Download bereit.

### **Kontakt**

#### **Postanschrift**

United Planet GmbH  
Postfach 1731  
79017 Freiburg  
Deutschland

#### **Hausanschrift**

United Planet GmbH  
Schnewlinstr. 2  
79098 Freiburg  
Deutschland

#### **Kommunikation**

Telefon: +49-(0)761-20703-0  
Telefax: +49-(0)761-20703-570  
E-Mail: [info@unitedplanet.com](mailto:info@unitedplanet.com)  
Internet: [www.unitedplanet.com](http://www.unitedplanet.com)

© Februar 2012. United Planet, Freiburg. Alle Rechte vorbehalten.