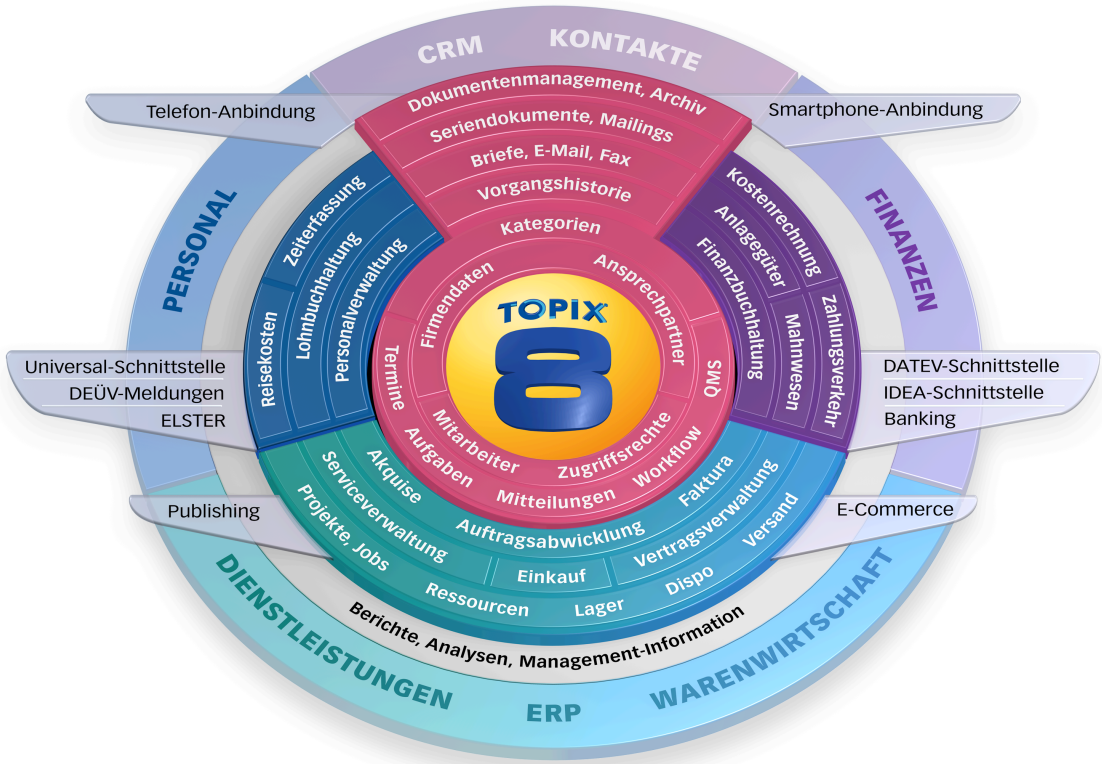


TOPIX:8 Webserver

Stand 14.06.2012

Dieser Text stellt nur eine kurze Übersicht dar. Bei Fragen zur Einrichtung wenden Sie sich bitte ausschließlich an Ihren Netzwerkbetreuer.
Ohne genaue Kenntnis Ihres Netzwerkes und der dazugehörigen Hard- und Software kann Ihnen die TOPIX Informationssysteme AG leider nicht weiterhelfen

Inhalt

Voraussetzungen

Für den Zugriff auf einen TOPIX:8 Webserver, der im Firmennetzwerk steht, sind diese Voraussetzungen erforderlich:

- Der Server muss über eine permanente Internetverbindung verfügen (z.B. über DSL oder Standleitung)
- Der Server muss vom Internet aus als Webserver erreichbar sein
- Der Webserver in TOPIX:8 muss aktiviert sein

Internetverbindung

Haben Sie eine Standleitung mit fester IP–Adresse nach außen, brauchen Sie zum Anmelden diese Adresse (oder einen verknüpften Domaineintrag, z.B. «topix8.meinefirma.de»).

Haben Sie eine Internetverbindung mit wechselnden IP–Adressen, die bei jeder „Einwahl" neu vergeben wird, brauchen Sie ein Hilfsmittel, um an die jeweils aktuelle Adresse zu kommen. Es bietet sich z.B. ein Service wie *DynDNS* an, bei dem der Router oder ein Hilfsprogramm bei jeder neuen Einwahl die neue IP–Adresse an DynDNS melden. Sie sind dann z.B. immer über «meinefirma.dyndns.org» erreichbar.

Zusätzlich muss gewährleistet sein, dass der Router die Internetverbindung ständig geöffnet hält, und nicht nach einer bestimmten Leerlaufzeit trennt, da er sonst von außen nicht mehr erreichbar ist.

Einrichtung DynDNS

Sie melden sich bei einem Service wie z.B.: www.dyndns.com an und erhalten dort einen Benutzernamen und ein Passwort; daraus ergibt sich Ihre Adresse «benutzername.dyndns.org».

Diese Daten tragen Sie in Ihrem Router ein und aktivieren ggf. die DynDNS-Funktion.

Erreichbarkeit

Damit die Anfrage aus dem Internet, die bis zum Router kommt, auch beim TOPIX:8 Server ankommt, müssen Sie den Router so konfigurieren, dass Anfragen aus dem Internet auf den internen TOPIX:8 Server umgelenkt werden. Dies nennt man Port–Forwarding.

Port–Forwarding im Router konfigurieren

Stellen Sie in Ihrem Router ein, dass eingehende Anfragen auf den von Ihnen konfigurierten Port auf die interne Adresse Ihres TOPIX:8 Webservers weitergeleitet werden.

☞ Bitte klären Sie dies unbedingt mit Ihrem IT-Betreuer/-Administrator, es sind detailierte Kenntnisse Ihres Netzwerkes notwendig. Dieser kann Sie auch über die nötigen Sicherheitsvorkehrungen bezüglich der Firewall/Routerkonfiguration beraten.

Sicherheit des TOPIX:8 Webservers

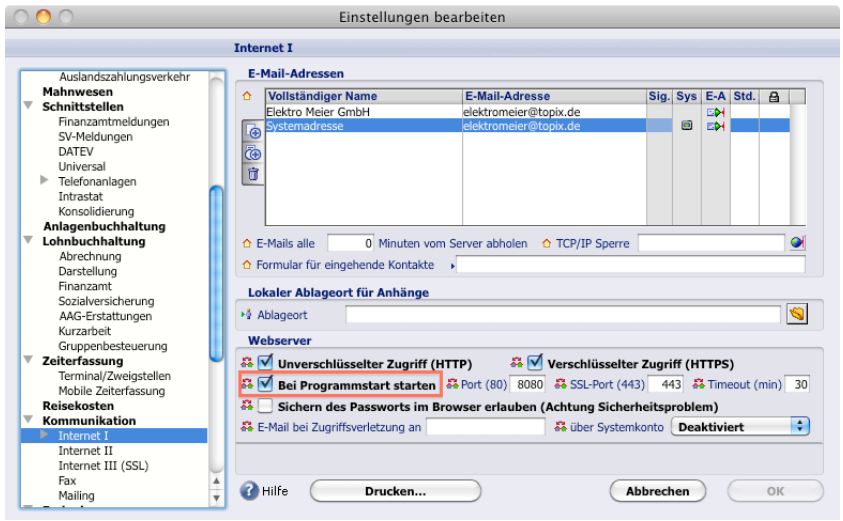
Konfiguration und Start des Webservers

HTTP und/oder HTTPS

Möchten Sie den Zugriff auf den TOPIX-Webserver, z.B. auf das Protokoll HTTPS, einschränken, können Sie die Option *Unverschlüsselter Zugriff* deaktivieren. Der Webserver ist dann auf dem jeweils eingestellten Port weiterhin aktiv. Es werden jedoch je nach Einstellung alle Anfragen über HTTP bzw. HTTPS abgelehnt.

Webserver starten

Der Webserver wird nur gestartet, wenn im Menü *TOPIX8/Datei* > *Einstellungen...* > *Kommunikation* > *Internet I* das entsprechende Ankreuzfeld markiert ist.



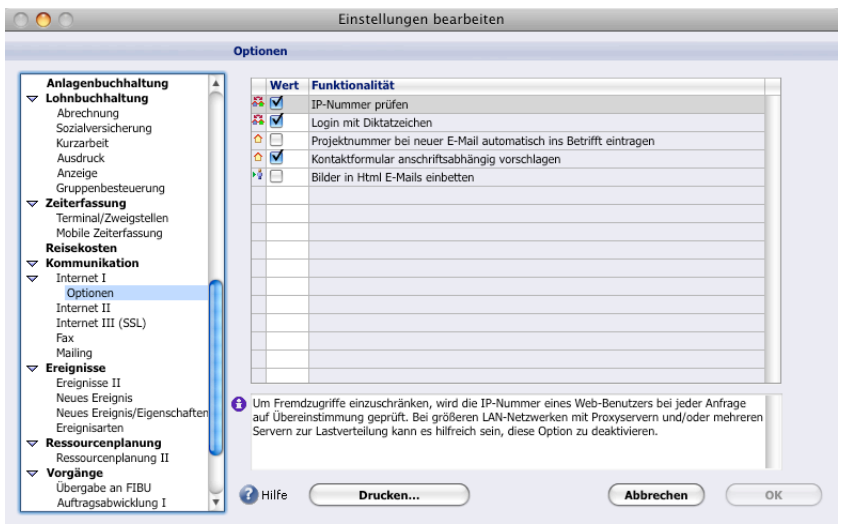
Dabei kann man zur weiteren Sicherheit auch die Portnummer vom Standard (80) auf eine andere, z.B. 12987, ändern. Die Eingabe im Web Browser sieht dann wie folgt aus: «www.topix.ag:12987» oder «192.90.10.23:12987» oder «www.topix.ag:12987/elektromeier.html»

☞ Unter Mac OS X muss für HTTP und HTTPS (SSL) ein Port über 1024 gewählt werden, z.B. HTTP 8080, SSL 8443

Zusätzlich kann eine E–Mail Adresse hinterlegt werden; diese wird immer benachrichtigt, wenn ein Fehler beim Login oder ein Einbruch versucht wird. Diese können Sie auch so einrichten, dass Sie direkt über Ihr Handy mit einer SMS benachrichtigt werden.

Weitere Optionen

Im Menü *TOPIX8/Datei* > *Einstellungen...* > *Kommunikation* > *Internet I* > *Optionen* gibt es weitere Ankreuzfelder:



Für die Zugriffssteuerung auf den TOPIX-Webserver stehen folgende Optionen zur Verfügung:

IP-Nummer prüfen (mandanten-übergreifend)	Diese Option ist gültig für Zugriffe auf den TOPIX-Webserver und damit mandantenübergreifend. Um Fremdzugriffe zu verhindern, wird bei jedem Zugriff die IP-Nummer des jeweiligen Benutzers auf Übereinstimmung zur IP-Nummer zum Zeitpunkt seiner Anmeldung geprüft. Wechselt die IP-Nummer innerhalb einer Sitzung, muss sich der Benutzer erneut anmelden. Dies ist notwendig, damit das Kopieren einer Zugriffsadresse und der Fremdzugriff durch Unbefugte – so genanntes Session-Highjacking - verhindert wird. In Einzelfällen kann diese Prüfung jedoch unerwünscht sein, z.B. in Szenarien mit firmeninternen Proxy-Servern zur Zwischenspeicherung von Internetseiten. Dabei wechselt die IP-Nummer systembedingt möglicherweise bei zeitnahen Zugriffen. In diesem Fall können Sie diese Option deaktivieren. iPhone-Client: Bei Zugriffen über die iPhone-Schnittstelle findet die Prüfung der IP-Nummer generell nicht statt. Da bei der Benutzung über mobile Endgeräte die IP-Nummer je nach Netzverbindung mehrfach wechseln kann, findet die Prüfung der IP-Nummer nicht statt. Verwenden Sie zur Absicherung den *Sicheren Modus* (SSL-Verschlüsselung) in den *Einstellungen* des TOPIX-iPhone-Clients. Hierdurch wird die Sitzungskennung verschlüsselt und Session-Highjacking ist ausgeschlossen. Für verschlüsselte Kommunikation via HTTPS mit dem TOPIX-Webserver wird ein SSL-Zertifikat benötigt. Weitere Hinweise finden Sie im Abschnitt **Absicherung des TOPIX:8-Webservers durch HTTPS** auf **Seite 8**.
Login mit Diktatzeichen (mandanten-übergreifend)	Ist diese Option aktiv, können sich Benutzer am TOPIX-Web-Client mit Ihrem Diktatzeichen als Benutzernamen anmelden. iPhone-Client: Für die Anmeldung mit dem TOPIX-iPhone-Client ist diese Variante generell möglich. Außerdem können Sie auch die Mandantennummer statt -bezeichnung in den Anmeldedaten nutzen.

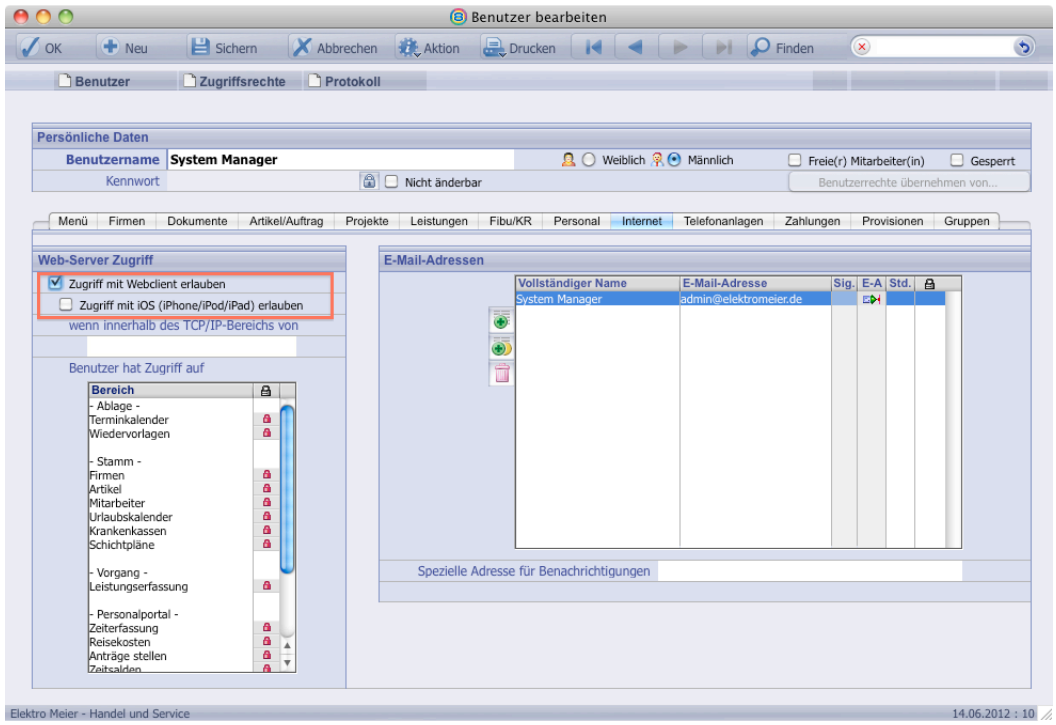
Für die Erzeugung und den Versand von E-Mail-Korrespondenzen gibt es diese Optionen:

Projektnummer bei neuer E-Mail automatisch den Betreff eintragen (mandanten-spezifisch)	Ist diese Option aktiv, wird bei der Erzeugung einer E-Mail-Korrespondenz in TOPIX:8 und anschließender Auswahl eines zugehörigen Projektes automatisch dessen Projektnummer in die Betreffzeile der Korrespondenz eingetragen. Diese Option ist für alle Benutzer des jeweiligen TOPIX-Mandanten gültig.
Kontakt-formular anschriftsabhängig vorschlagen (mandanten-spezifisch)	TOPIX:8 Formulare können sprachbezogen angelegt werden, z.B. Formulare zur E-Mail-Korrespondenz in deutscher und englischer Sprache. Ist die Option aktiv, wird bei der Erzeugung einer Korrespondenz in TOPIX:8 je nach gewählter Empfängeranschrift das Formular in der jeweiligen Landessprache geladen.
Bilder in HTML-E-Mails einbetten (benutzer-spezifisch)	Hat ein Benutzer diese Option aktiviert, kann er HTML-E-Mails mit eingebetteten Bildern versenden. Bilder, die Sie in ein Dokument einer E-Mail-Korrespondenz eingefügt haben, werden beim Versand der E-Mail automatisch mitgesendet. Je nach Programm des E-Mail-Empfängers werden dabei die Bilder stellungsrichtig im Textlauf und/oder in den angehängten Dateien angezeigt.

Zugriff auf den Webserver

Es können nur Benutzer auf den TOPIX:8 Webserver zugreifen, denen auch der Zugriff in der Benutzerverwaltung (im Menü *Stamm* > *Benutzer*) erlaubt wurde.

Hier wird auch der Zugriff via iPhone/iPad Client freigeschaltet.



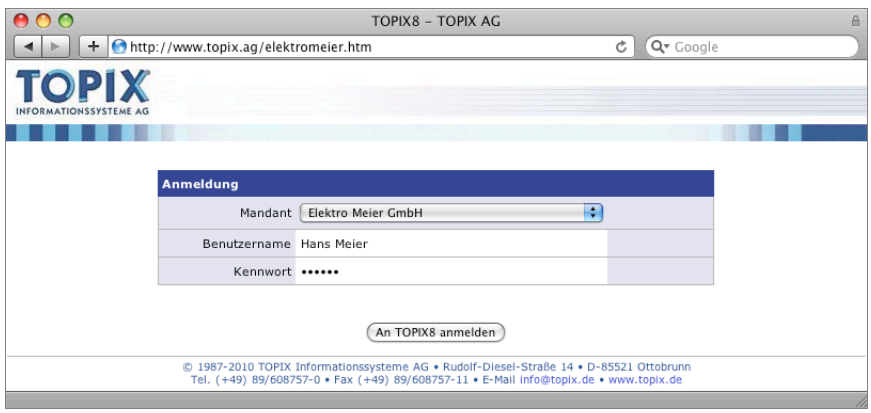
☞ Wenn der Benutzer ein leeres Kennwort hat, kann er nicht auf den Webserver zugreifen.

Es kann zusätzlich der TCP/IP Bereich eingeschränkt werden, von dem aus auf den Webserver zugegriffen werden kann. Jeder Rechner hat eine eigene IP–Adresse, z.B. «192.90.10.99». Sie können nun den Bereich auf «192.90.10.» einschränken. Damit erreichen Sie, dass Benutzer sich nur von einem Computer, der sich innerhalb des gleichen Subnetzes wie der Webserver befindet, und z.B. nicht mehr von zu Hause aus am Webserver anmelden können.

Hier können Sie auch noch einstellen, welche einzelnen Programmbereiche der Benutzer im Browser sehen soll. Darüber hinaus werden die Zugriffsrechte des Benutzers berücksichtigt, d.h. wenn ein Benutzer in TOPIX:8 keinen Termin anlegen, jedoch Termine sehen darf, gelten diese Rechte auch für den Webserver.

Anmeldung am Webserver

Hierbei geben Sie in Ihrem Browser entweder einen Domainnamen ein oder die IP–Adresse des Servers, auf dem das TOPIX:8 Serverprogramm läuft, z.B. «192.90.10.23».
Oder, wenn Sie die Portnummer des Webservers verändert haben: «192.90.10.23:80:12987».



Hier können Sie nun den gleichen Benutzernamen und das gleiche Passwort eingeben wie am TOPIX:8 Arbeitsplatz. Den Benutzernamen müssen Sie dabei eintippen, dies ist eine zusätzliche Sicherheitsstufe.

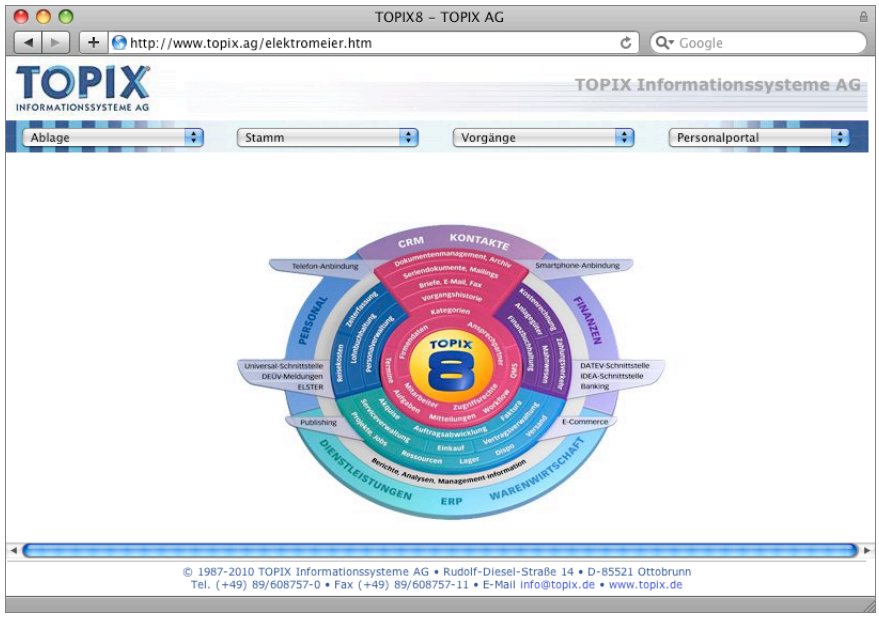
Wenn Sie den Benutzernamen oder das Kennwort dreimal falsch eingegeben haben, wird der Rechner für 30 Minuten gesperrt und bekommt keine Antwort mehr, auch keine Fehlermeldung. Während dieser 30 Minuten können Sie sich nicht mehr am TOPIX:8 Webserver anmelden.

☞ Geben Sie den Namen und das Passwort immer vollständig ein, achten Sie auf Groß– und Kleinschreibung.

Jeder Zugriff auf diese Seite wird mit Datum, Uhrzeit, TCP/IP–Adresse, Web Browser, Betriebssystem usw. protokolliert.

Bei jeder Falscheingabe im Anmeldedialog wird eine E–Mail an den zuständigen Administrator gesendet sowie ein Protokoll aufgezeichnet.

Arbeiten mit dem Webserver



Ihre Zugriffsrechte werden bei jeder neuen Aktion geprüft. Dies sichert das so genannte Internal Hacking, bei dem Mitarbeiter einer Firma versuchen, auf Bereiche zuzugreifen, auf die sie keinen Zugriff haben. Bei jedem Versuch wird an den zuständigen Administrator eine E-Mail gesendet sowie ein Protokoll aufgezeichnet.

Sicherheitsaspekte

Wenn Sie die Sitzung im Web Browser beenden wollen, rufen Sie immer den Befehl *Abmelden* auf, da sonst der Server nicht weiß, ob Sie noch weitere Eingaben vornehmen wollen.

☞ Wenn Sie nur den Web Browser beenden, kann ein anderer Benutzer über die Historie bzw. den Verlauf Ihrer Web–Sitzungen (nur auf Ihrem Computer) auf Ihre letzte Sitzung zugreifen. Diese läuft erst nach 30 Minuten ab, wenn Sie sich nicht ordnungsgemäß abmelden.

In den meisten Web Browsern gibt es eine Einstellung zum Merken von Namen und Kennwörtern. Manche Browser fragen auch nach, ob Namen und Passwort gespeichert werden sollen. Dies ist ein Sicherheitsproblem, da der nächste, der diesen Computer benutzt, nur noch den Namen der Internetseite benötigt (der auch noch in der Historie gespeichert ist, falls diese nicht gelöscht wurde), um ohne Namen und Passwort auf den TOPIX:8 Webserver zugreifen zu können. Dies ist besonders problematisch, wenn Sie bei einem Kunden sind und auf dessen Computer schnell auf Ihre Firmendatenbank zugreifen wollen.

Es gibt Programme auf Computern, die automatisch alle Tastatureingaben protokollieren. Damit lässt sich auch sehr schnell herausbekommen, wie Ihre Passwörter lauten.

Sie sollten also NIEMALS von einem fremden Rechner aus ein Passwort eingeben, dies gilt nicht nur für TOPIX Software, sondern auch für Ihr Homebanking usw. Des Weiteren sollten Sie immer Ihren Computer mit einem Passwort schützen, so dass niemand Ihren Computer unbefugt nutzen kann. Benutzen Sie nie Passwörter wie: 123, liebe, haustiername, geburtsdatum usw., sondern am besten Kombinationen aus Zahlen und Wörtern wie z.B. „12tutnichtweh2“. Dabei gilt: umso länger das Passwort, desto sicherer. Weniger als 8 Zeichen sollte ein Passwort aber nie haben.

Gültigkeit der Einstellungen des TOPIX-Webservers

TOPIX-iPhone-Client

Der TOPIX-iPhone-Client (ab 05.03.2010 im iTunes-App-Store verfügbar) verwendet neben wenigen Ausnahmen folgende Optionen für Anmeldung und Verschlüsselung wie der TOPIX-Web-Client:

Sichere Verbindung	Das SSL Zertifikat muss eingerichtet sein.
Server	Sie müssen die Adresse Ihres TOPIX:8 Servers und den Port eintragen, auf dem der Webserver kommuniziert. Die Adresse wird entweder al IP oder URL eingetragen
Mandant	In dieses Feld muss die Mandentennummer oder der Mandantenname eingetragen werden. Die Mandantennummer finden Sie im Menü *TOPIX8/ Datei* > *Einstellungen...* > *Allgemein* rechts neben dem Feld *Firma 1*
Benutzername	Der TOPIX:8 Benutzername
Kennwort	Das TOPIX:8 Kennwort

Die Ausnahmen sind im Abschnitt **Weitere Optionen** ab **Seite 4** beschrieben.

TOPIX-SOAP-Schnittstelle

Voraussetzung für Anfragen an TOPIX:8 über die SOAP-Schnittstelle ist der TOPIX-Webserver.

Für die Steuerung des Zugriffs gelten dabei die allgemeinen Webserver-Optionen im Menü *TOPIX8/ Datei* > *Einstellungen...* > *Kommunikation* > *Internet I* - Port-Nummern und Protokollaktivierungen. In den Zugriffseinstellungen der Benutzer im Menü *Stamm* > *Benutzer* > *Register Internet* (vgl. **Seite 6**) können Sie den SOAP-Zugriff mit dem jeweiligen Benutzerkonto erlauben oder verbieten. Darüber hinaus nutzt die SOAP-Schnittstelle einen eigenen Anmeldemechanismus, bei dem jede Abfrage Daten zur Authentifizierung enthalten muss. Insbesondere die *Optionen* unterhalb von *Internet I* haben deshalb für die SOAP-Schnittstelle von TOPIX keine Auswirkung.

TOPIX-Webshop-Schnittstelle (Webshop III - Externals)

Die Aufrufe der TOPIX-Webshop-Schnittstelle richten sich an ein Schnittstellenskript eines Externals (Webshop u.a.), welches sich auf dem Webserver des Externals befindet. Deshalb haben die Einstellungen und Optionen des TOPIX-Webservers auf die Funktionsweise der Webshop-Schnittstelle keine Auswirkung.

Absicherung des TOPIX:8-Webservers durch HTTPS (*Einstellungen* > *Internet III*)

Zur Kommunikation mit dem Webserver via HTTPS wird eine SSL-Zertifikatsdatei benötigt. (Digitales Zertifikat mit qualifizierter elektronischer Signatur QES).

Ein solches Zertifikat wird durch Zertifizierungsstellen, so genannte Certificate authorities (CA) bzw. Sign-Trust-Center, erstellt und signiert. Die Anfrage mit Ihren Daten für die Erstellung eines Zertifikates können Sie direkt in TOPIX:8 vornehmen.

Eigene Zertifikate

Möchten Sie ein eigenes, kostenfreies Zertifikat nutzen, können Sie dieses direkt in TOPIX:8 erstellen und für die Verschlüsselung der Kommunikation mit dem TOPIX-Webserver installieren. Beachten Sie bitte, dass diese Zertifikate standardmäßig in Web-Browsern als nicht gültig eingestuft werden. Dies ist der Fall, da zur Absicherung die Bestätigung der Identität des entsprechenden Server-Rechners durch die ausstellende Zertifizierungsstelle gehört. Da Sie in diesem Fall selber das Zertifikat ausstellen und signieren, gilt es als unsicher. Die Verbindung ist hingegen dennoch verschlüsselt, so dass die Daten durch Dritte nicht gelesen werden können.

Beim Aufruf des TOPIX-Web-Clients im Webbrowser erhalten Sie in diesem Fall entsprechende Hinweise zur Unsicherheit des Zertifikats. Sie müssen das Zertifikat extra akzeptieren; in einigen Browsern muss ein als unsicher eingestuftes Zertifikat speziell in die Liste der akzeptierten Zertifikate aufgenommen werden, bevor die Kommunikation damit erlaubt wird. Dies ist ebenso der Fall, falls

Sie ein Zertifikat einer CA benutzen, welche im jeweiligen Browser noch nicht in die Liste der vertrauenswürdigen Zertifizierungsstellen aufgenommen wurde.

Zertifikatsanfrage erstellen

Über die Einstellungen in TOPIX:8 können Benutzer mit Administrator-Rechten eine Anfragedatei zur Zertifikatserstellung erzeugen. Hierfür öffnen Sie im Menü *TOPIX8/Datei > Einstellungen... > Kommunikation > Internet III (SSL)*. Geben Sie die Daten ein, die Sie in das Zertifikat aufnehmen möchten. Die Daten sollten mit dem Whois-Eintrag der abzusichernden Domain übereinstimmen. Für de-Domains können Sie diese Daten bei www.denic.de einsehen.

Allgem. Name (Domain)	Der Domainname des abzusichernden Servers. Es muss sich um einen gültigen DNS-Namen und nicht um eine IP-Nummern handeln. Der Name sollte der Adresse des Servers entsprechen, der mit dem jeweiligen Zertifikat abgesichert werden soll. Läuft ihr Server z.B unter "www.meinedomain.com" tragen Sie diese Adresse vollständig unter "Allgemeiner Name" ein. Beachten Sie auch, daß damit nur die Domain "www.meinedomain.com" und nicht "meinedomain.com" bzw. "subdomain.meinedomain.com" als gültige Adressen bei der Prüfung des Zertifikates im Browser erkannt werden. Rufen Sie z.B. statt "www.meinedomain.com" "meinedomain.com" auf, erhalten Sie Fehler wie "Hostname stimmt nicht überein" oder "hostname mismatch".
Ländercode	Der 2-stellige ISO-3166-1-alpha-2 Ländercode, z.B. "DE".
Ort	Der Ortsname des Firmensitzes
Bundesland	Das Bundesland des Firmensitzes, z.B. "Bayern"
Firma	Firmenname
Abteilung	Geben Sie hier eine Bezeichnung für die Abteilung ein, die im Zertifikat erscheinen soll.
Gültig bis	Das Enddatum des Gültigkeitszeitraums des Zertifikates. Diese Angabe ist nur notwendig, wenn Sie ein eigenes Zertifikat erstellen möchten. Anderenfalls wird der Gültigkeitszeitraum durch die signierende Zertifizierungsstelle bestimmt.
Schlüssel-länge	Die Verschlüsselungsstärke der Signatur des Zertifikates. Diese Angabe ist ebenso nur für die Signierung eigener Zertifikate von Bedeutung.

Nachdem Sie alle notwendigen Angaben eingegeben haben, klicken Sie auf Anfrage generieren... . Wählen Sie im Dateidialog einen Ordner, in den folgende Dateien gespeichert werden sollen:

privKey.pem	Der private Schlüssel für die SSL-Verschlüsselung. Sie benötigen diesen Schlüssel bei der Installation eines dazugehörigen Zertifikates in TOPIX. Verwenden Sie diesen Schlüssel ausschließlich für die Installation mit TOPIX und behandeln Sie ihn vertraulich. Senden Sie diesen Schlüssel niemals via E-Mail oder geben Sie ihn an Dritte heraus.

pubKey.pem	Der öffentlich Schlüssel für die SSL-Verschlüsselung. Dieser Schlüssel ist auch in der Zertifikatsanfrage "request.pem" enthalten und braucht wie der private Schlüssel normalerweise nicht weitergegeben werden.
request.pem	Die Zertifikatsanfrage für die signierende Zertifizierungsstelle oder für die Erstellung und Signierung eines eigenen Zertifikates.
rnd.dat	Eine Arbeitsdatei der Schlüsselgenerierung mit den Primzahlen der RSA-Schlüssel. Diese Datei wird nicht weiter benötigt und enthält ebenso wie der private Schlüssel vertrauliche Daten.

Für die Beantragung bei einer Zertifizierungsstelle benötigen Sie die Datei *request.pem*. Die Zertifizierungsstelle verlangt ggf. weitere Dokumente wie Handelsregisterauszug und Ausdruck der Whois-Daten der Domain (www.denic.de). Die Firmendaten in der Anfrage sollten mit den Daten der Whois-Datenbank übereinstimmen. Sollte dies nicht der Fall sein, können Sie als Eigentümer die Daten entsprechend über Ihren Provider ändern lassen (Modify).

Selbstsignierte Zertifikate erstellen

Sofern Sie auf Ihren TOPIX-Server Zugriff lediglich von einem bekannten Benutzerkreis erwarten, können Sie auch mit einem eigenen Zertifikat mit selbst erstellter Signatur die Kommunikation mit dem TOPIX-Webserver verschlüsseln. Über die TOPIX-Funktion zur Zertifikatserstellung wird ein so genanntes Root-Zertifikat erstellt. Da dieses Zertifikat durch Sie selber elektronisch signiert wird, gilt es in Web-Browsern u.a. als unsicher, da die Zertifizierungsstelle unbekannt ist. Dies ist unter Umständen auch der Fall, wenn Sie ein kommerzielles Zertifikat von einer Zertifizierungsstelle einsetzen, die im jeweiligen Browser eines Benutzers nicht als vertrauenswürdig eingetragen ist. Benutzer, denen Sie HTTPS-Zugriff anbieten, müssen der Benutzung des Zertifikates deshalb explizit im Browser zustimmen und ggf. speziell in den Einstellungen des Browsers das Zertifikat als vertrauenswürdig einstufen.

Zertifikat erstellen:

1. Unter *TOPIX8/Datei > Einstellungen... > Kommunikation > Internet III (SSL)* auf *Anfrage generieren* oder *Zertifikat erstellen* klicken (haben derzeit dieselbeFunktion).
2. Einen Ordner für die Anfrage auswählen.
3. Auf *Zertifikat Installieren* klicken und danach ...
   - den privaten Schlüssel auswählen (*privkey.pem*),
   - Zertifikate auswählen (*cert.pem*)

   Es erscheint die Meldung *Zertifikate wurden erfolgreich installiert, Neustart Webserver*?
4. Wir empfehlen, die Meldung mit *Abbrechen* zu quittieren und nach der Einrichtung des Zertifkates den TOPIX Server einmal komplett neu zu starten, da nur so die Daten der Zertifikate in den Einstellungen korrekt aktualisiert werden.

Fremde Zertifikate erstellen

Fremde Zertifikate können direkt über "Zertifikate Installieren" eingelesen werden.

Für die Installation eines Zertifikates wird der private Schlüssel privKey.pem und das Zertifikat im pem-Format (privacy enhanced mail; base64-kodiert; Dateiendung .pem oder .cer) benötigt. Beide Dateien werden bei der Installation in den Ordner der Programmdatei auf den TOPIX-Server-Rechner kopiert. Sollten Sie durch eine Zertifizierungsstelle das Zertifikat in einem anderen Format erhalten haben (z.B. PKCS #7; .p7b), müssen Sie das Zertifikat vor der Installation konvertieren.

Unter Windows können Sie die Konvertierung beispielsweise durch Im- und Export im Internet Explorer vornehmen:

5. Internet Explorer öffnen und anschließend im Menü *Extras* > *Internetoptionen* wählen.
6. Im Dialog in das Register Inhalte wechseln und auf *Zertifikate* klicken.
7. In der Liste der eigenen Zertifikate das erhaltene Zertifikat importieren.
8. Anschließend das Zertifikat in das Format Base-64-codiert X.509 (.CER) exportieren.

Zertifizierungsstellen (Beispiele)

- VeriSign (weitere Töchter bzw. Marken: *thawte*, GeoTrust, Equifax, RapidSSL)
- Comodo (Anbieter von Sicherheits-Software; zweitgrößte CA im Bereich Wirtschaft)
- GlobalSign (belgischer Anbieter)
- CAcert (nicht-kommerziell; noch nicht flächendeckend als vertrauenswürdig eingestuft)
- D-TRUST (Bundesdruckerei-Gruppe)
- Deutsche Post Com (Signtrust)
- Sparkassen-Finanzgruppe (S-TRUST)
- T-Systems
- DynDNS.com (Geotrust-Zertifikate mit Equifax als Root-CA)