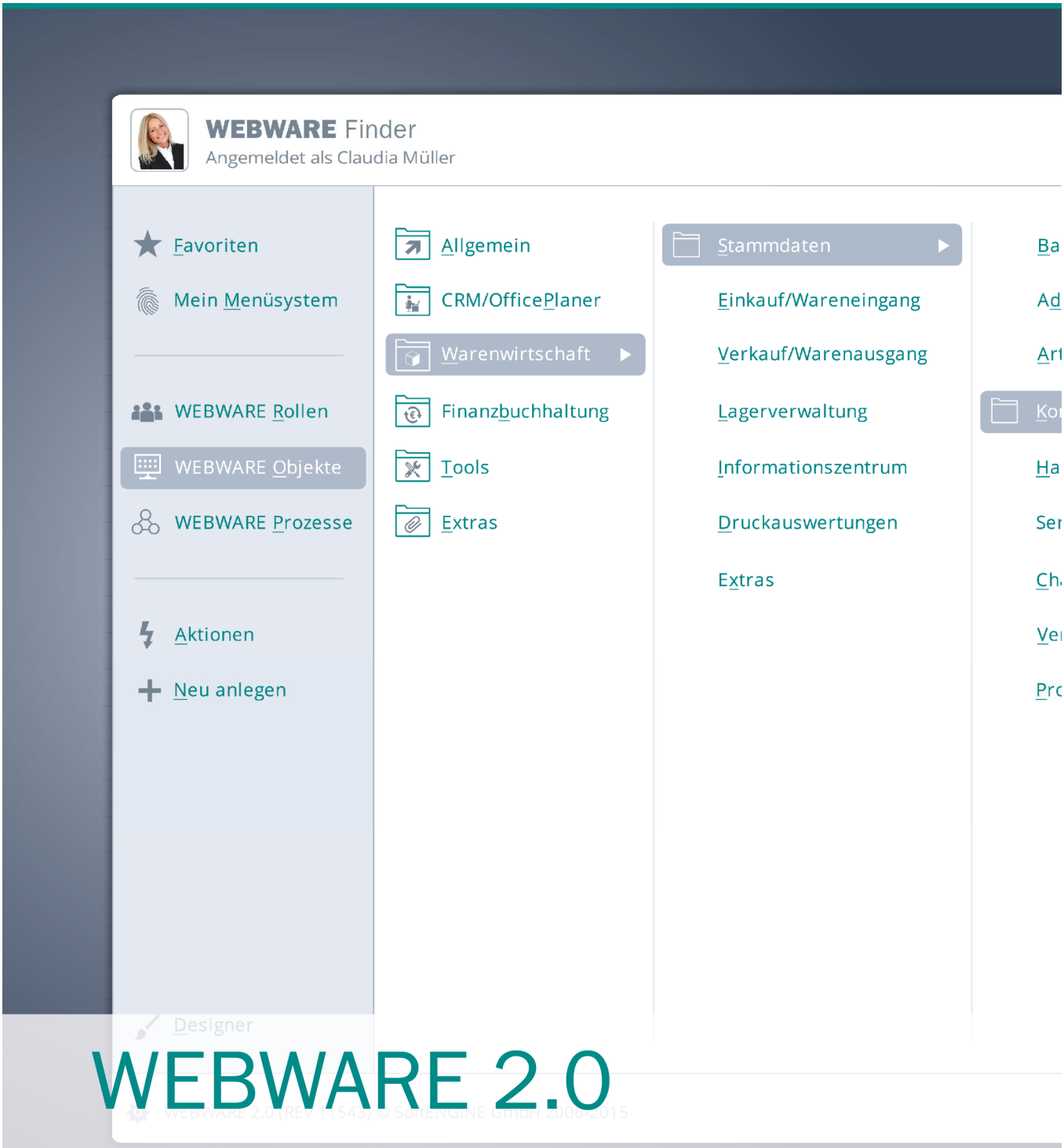
SoftENGINE

Kaufmännische Software für Handel, Industrie und E-Commerce



WEBWARE 2.0

Dokumentation

WEBWARE SECURE Server

Rel 27 vom 23.03.2017

WEBWARE SYSTEM HANDBUCH

Sicherheit geht vor...

Konfiguration einer sicheren WEBWARE Systemumgebung

INHALTSVERZEICHNIS

WEBWARE secure server

Einführung

In diesem Dokument werden die Sicherheitskonzepte, sowie die Konfigurationsmöglichkeiten des WEBWARE Server behandelt. Es wird erklärt welche Sicherheitsfunktionen, wie angewandt werden sollen.

Da der WEBWARE Server teilweise in Internet Umgebungen läuft ist eine sichere Abschottung des RAR-Clusters sowie der restlichen Intranetseitigen Rechner Systeme unumgänglich.

Ziel dieses Dokumentes ist es, eine sichere Systemumgebung zu erhalten, die auf Angriffe bzw. Fehlfunktionen von Programmen/Rechnern sauber und sicher reagiert.

Sicherheitsfunktionen der WEBWARE

- Sitzungsorientierte FireWALL
- Verbindungüberwachung (Intrusion Prevention FireWALL)
- WEBWARE Server kann im DMZ-Bereich eines Intranet's laufen
- SecureNet (Adressranges für Zugriff auf Netzwerkschnittellen der WEBWARE möglich)
- HTTPS-Sub-Systems für eine sichere Datenübertragung
- Login und Passwort-System (Passwort Übertragung mit Hilfe von HASH-Verfahren)
- Verschlüsselte Datenübertragung zwischen den WW-Komponenten
- Protokoll Subsystem (Überwachung und Protokollierung von Systemkritischen Funktionen)

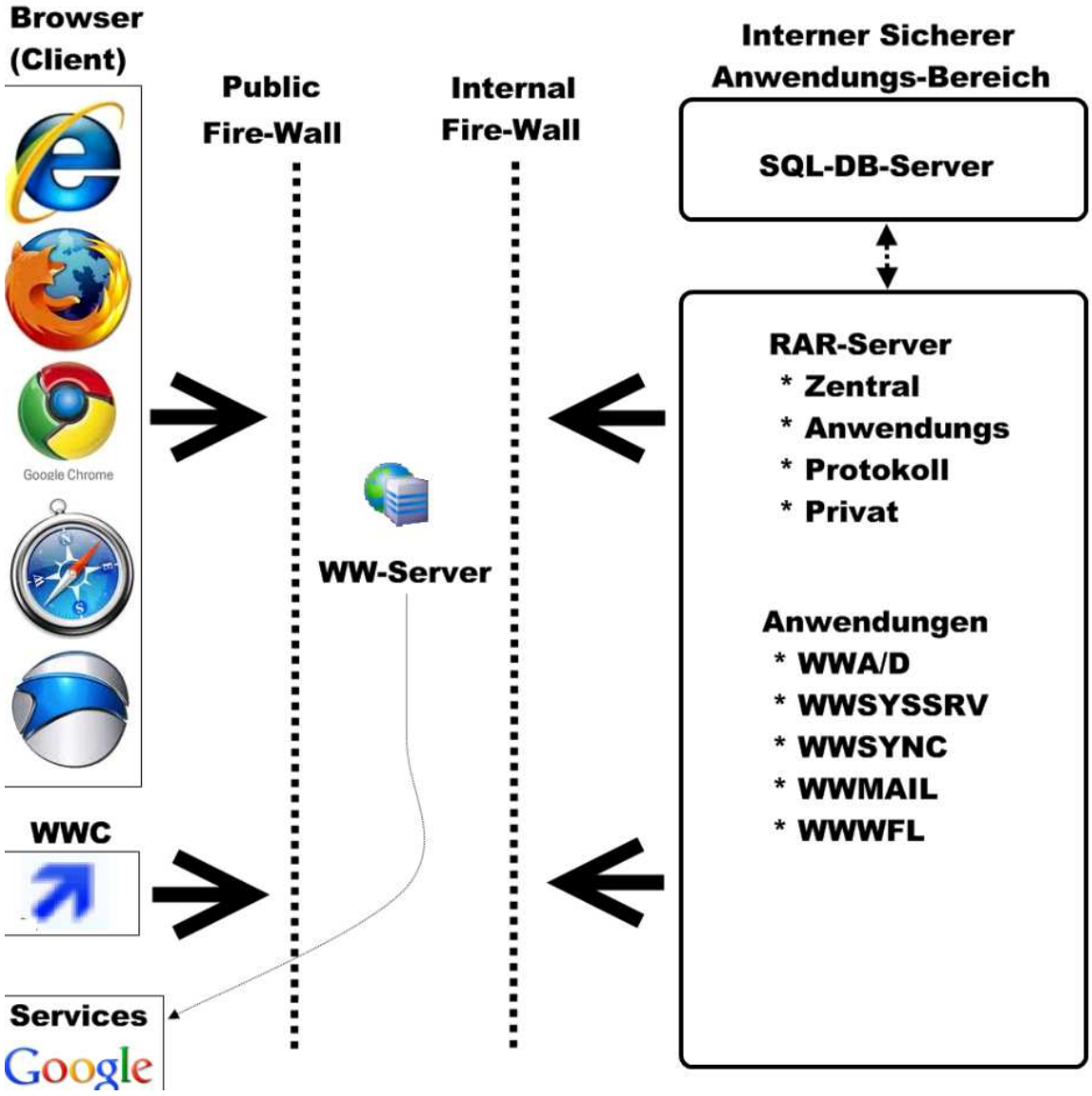
Begriffsbestimmungen

- Browser — Computerprogramm zum Anzeigen von Programminhalte des WW-Server
- Schnittstelle — eine Schnittstelle ist eine Hardware Komponente (Netzwerkkarte)
- Server — ist ein Rechner der Funktionen bereit stellt.
- LUNA — Rechner Verwaltungsprogramm der WEBWARE
- RAR — Remote Applikation Runner (Entfernter Programm Starter)
- Synchro — Datei-/Verzeichnis Abgleich System
- TAPI — Telefon Anbindung
- APP — Anwendung, also ein Computerprogramm
- WWC[C] — Programm zur Anbindung lokaler Ressourcen an die WEBWARE
- FireWALL — Programm bzw. Hardware die Verbindungen zwischen Rechnersystemen überwacht, und bei Bedarf unterbindet.
- Port — ist eine Tür durch die eine Verbindung mit einem Rechnersystem aufgebaut wird
- Installation — eine Programminstallation die eine WW-Datenbank zur Verfügung stellt. Eine Installation hat je einen Netzzugang zum extern und internen Netz.
- WALIS — WEBWARE Automatisiertes Login System

Checkliste für eine sichere Konfiguration

- Passwortsicherheit aktiviert ?
- Verbindungs FireWALL aktiv ?
- Sitzungs-FireWALL aktiv ?
- Protokoll-FireWALL aktiv ?
- Unbekannte RAR-Server verboten ?
- Secure-Net Vorgaben: Intra-Net für Anbindung der RAR-Server ?
- Secure-Net Vorgaben von Netzwerkkarten für Benutzer Geräte gesetzt/notwendig ?
- Secure-Net Vorgaben: Luna-Server ?
- Home-Verzeichnis hat keine WW-Unterverzeichnisse installiert. Kein Bin und auch kein APP
- WWLINK System keine Anonymen Zugänge aktiv ?
- WW-Client Communicator Standardvorgaben angepasst?
- Protokoll Subsystem an Ihre Bedürfnisse angepasst?
- Geräte Zugriffsbeschränkungen gesetzt ?
- Einschränkung des automatisierten Login-System auf sichere Netzbereiche ?
- IntraNet/InterNet Bereiche definiert für Zugriff von Benutzergeräten ?
- Anpassung der Anmeldebildschirme für die IntraNet/InterNet Bereiche ?

Schematische Darstellung WEBWARE System-Umgebung



Grundlegendes Sicherheitskonzept

Es muss immer davon ausgegangen werden, dass ein Rechner der an das Netz (Intra/Internet) angebunden ist, angreifbar ist. Daher ist das Sicherheitskonzept der WEBWARE so aufgebaut, das auch bei Kompromittierung des Internet-Anbindungs-Rechner's das „sichere" Netz nicht angegriffen werden kann. Es darf aus dem unsicheren Netz(Intra/Internet) keine Verbindung ins „sichere" Netz (Anwendungen/Datenbank usw.) möglich sein (über Hardware FireWALL bzw. strikte Netzwerktrennung sicherstellen).

Die Hauptkomponente im WEBWARE-System ist der WEBWARE Server (WWS). Er verbindet die Außenwelt mit der internen sicheren Anwendungsumgebung. Der WWS wird auf einem eigenen Rechnersystem installiert das mindestens 2 Netzwerkkarten hat, und dadurch über einen Zugang zu 2 unterschiedlichen (getrennten) Netzen verfügt.

- Externes Netz (Internet)
- Internes Netz (Intranet, sichere Systemumgebung)

Die Netzwerke sollten nicht über die gleiche Netzwerkleitung laufen. Auf dem WW-Server dürfen keine Datei-/Verzeichnisfreigaben gemacht werden. Ebenso darf der WW-Server keine Datei-/Verzeichnisfreigaben aus dem sicheren Netz verwenden, um einem Angreifer bei erfolgreicher Übernahme des WW-Server's kein Zugriff auf das interne Netz zu gewähren.

Grundproblem: Es wird oft auf einem WW-Server weitere (nicht WEBWARE) SoftWARE installiert. Ein Angreifer kann auch durch solche Software den Zugriff auf das Rechnersystem erhalten. Daher ist es wichtig folgende Regeln bei der Konfiguration strikt zu Beachten:

- Der WW-Server bzw. das Rechnersystem auf dem der WW-Server läuft, darf auf keinen Fall Verbindungen zum „sicheren" Intra-Netz aufbauen.

- Die Netzwerkkarten Protokolle in sichere Netz sollten entsprechend entfernt werden so dass keine Dienste als Netzwerkkartenservice vorhanden sind, die einen Durchgriff auf das sichere Netz erlauben.

- Der WW-Server bzw. das Rechnersystem auf dem der WW-Server läuft, darf nur auf den „erlaubten" Service-Ports ins Internet Verbindungen aufbauen:

    - WEBWARE Update/Lizenz-Server, Google-Apps Verzeichnis

Die Einhaltung dieser Restriktionen muss mit einer FireWALL überwacht werden.

Das bedeutet dass die FireWall Programme zur Abschottung des Rechnersystem folgende Regeln haben:

- Eintragen des/der erlaubten Zugangsport's von Internet zu WW-Server (Bspl: 443)

- Eintragen des/der erlaubten Zugangsport's vom Intranet zu WW-Server (Bspl: 8091,..)

- Verbieten aller ausgehenden Verbindungen auf dem Rechner-System, bis auf WW-Service..

- Strikte Trennung der Teilnetzwerke, **also kein Bridging zwischen Internet/Intranet !!!!!**

- Zugriff auf die Netzwerkkarte Richtung sicheres Netz nur für das Programm WWS.EXE erlaubt, und hier auch nur Annahme von Verbindungen, kein Verbindungsaufbau (listen).

- Unnötige Protkolle aus den Netzwerkkarten entfernen, so dass bei Fremdübernahme des Rechner's kein direktes Verbinden aus dem WW-Server System möglich ist.

Die WEBWARE Systemkomponenten

WEBWARE Server

Der WEBWARE Server ist ein Multi-Internet Server. Er verwaltet je nach Konfiguration eine bis mehrere Installationen. Der WEBWARE Server baut nur in 2 Ausnahmefällen eine Verbindung ins Internet auf.

- Update/Lizenz Server Anbindung
- Google APP's Anbindung

Alle sonstigen Zugriffe werden auf dem WEBWARE-Server nur von „außen" durchgeführt. Dadurch ist es möglich den WEBWARE-Server so zu konfigurieren dass ein Zugriff nur auf den Server, aber nicht von diesem heraus möglich ist.

Die Anbindung und der Zugriff aus dem sicheren Netz erfolgt nur aus dem sicheren Netz heraus. Ein Verbindungsaufbau vom WW-Server aus ist nicht notwendig.

WEBWARE LUNA Server

Der LUNA-Server dient zur Verwaltung von Rechner im „sicheren" Netz. Er wird aus dem System-Cockpit heraus auf einem Rechner als Dienst installiert. Mit Hilfe des LUNA-Servers werden dann aus dem System-Cockpit heraus, Verwaltungsfunktionen ausgeführt.

Der LUNA-Server überwacht einen bis mehrere RAR-Server die auf einem Rechnersystem installiert sein können. Der LUNA-Server meldet sich auf Server-Ebene an, und nicht auf Installationsebene. Für den LUNA-Server wird vom WW-Server ein eigener Dienst-Port (Zugang) zur Verfügung gestellt.

Der LUNA-Server wird bei WEBWARE-Cooperation- sowie WEBWARE-Cloudinstallationen verwendet.

WEBWARE RAR Server

Der RAR-Server dient dazu auf Installationsebene eine Installation an den WEBWARE-Server anzubinden. Hierzu wird vom RAR-Serverauf einen Installationsspezifischen Port zugegriffen, der vom WEBWARE-Server speziell für eine Installation zur Verfügung gestellt wird.

Der RAR-Server erlaubt die Ausführung von folgenden Funktionen, diese werden über die Datei WWR.INI konfiguriert und bereit gestellt:

WEBWARE Synchro Funktion

Um eine Anbindung von Datei-System Komponenten des Installationsverzeichnis an das WEBWARE-Dateisystem (wird physisch auf dem WW-Server gehostet) zu erreichen, wird das Programm WWSYNCHRO.EXE verwendet. Dieses baut eine Verbindung zum WW-Server auf und stellt diesem die gewünschten Verzeichnis- und Dateieinträge aus dem Installationsverzeichnis zur Verfügung.

Die Konfiguration der Verzeichniszugriffe erfolgt mit der Datei WWSYNCHRO.INI.

WEBWARE TAPI Funktionen

Soll eine TAPI-Telefonanbindung erfolgen, so kann das Programm WTAPISRV.EXE verwendet werden. Dieses liest die verfügbaren TAPI-Einheiten eines Rechners aus und stellt diese im WW-Systemcockpit zur weiteren Verarbeitung zur Verfügung.

WEBWARE Anwendungen

WWA.EXE

WEBWARE Benutzer-Anwendungsprogramm. Für jeden Benutzer wird je Sitzung dieses Programm ausgeführt.

WWSYSSRV.EXE

System-Server der die Zugriffe auf die Installationsdatenbank für den WW-Server ausführt.

WWFLSRV.EXE

Programm das als Workflowserver Anwendungsspezifische Aufgaben ausführt.

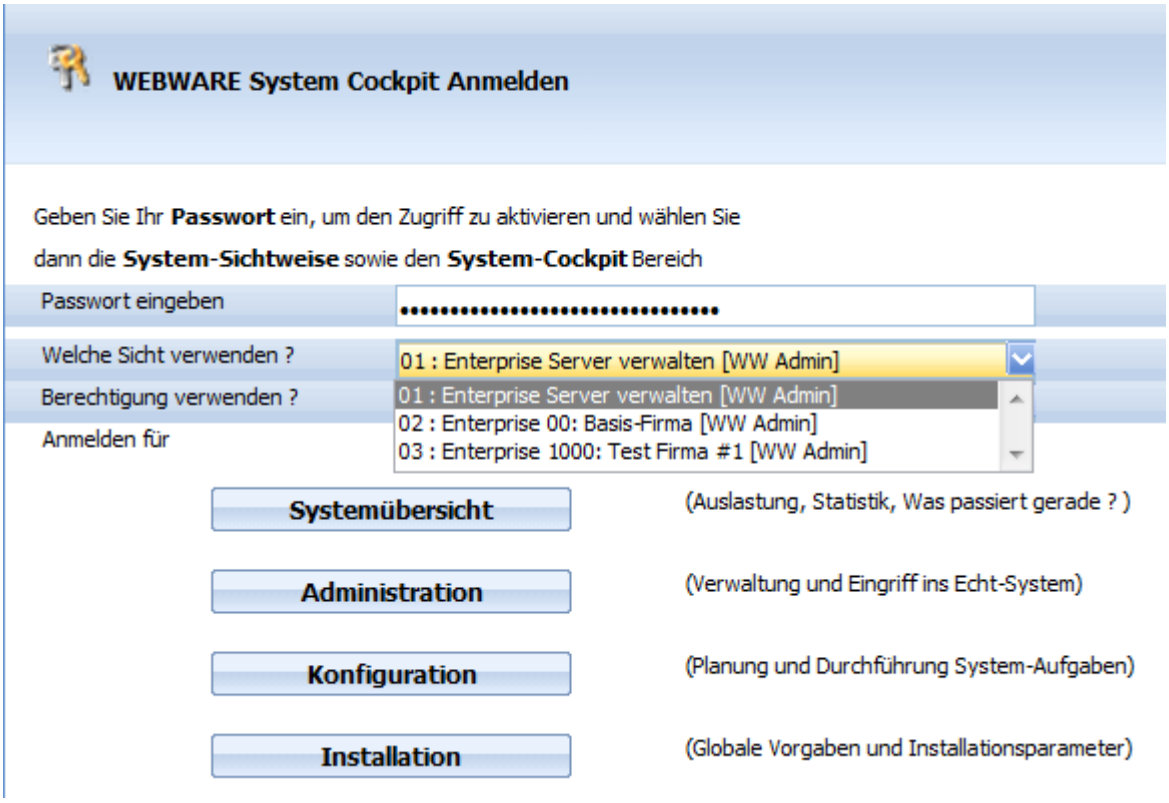
WEBWARE@home Client Communicator

Mit dem WEBWARE-Client Communicator (WEBWARE@home) ist es möglich lokale Ressourcen eines Benutzerrechner in der WEBWARE-Umgebung der Benutzersitzung zu verwenden. Der WWCC bietet dabei folgende Funktionen an.

- Lokale Drucker Integration (Drucken auf meinem Drucker..)
- Lokale TAPI-Integration (Eingangs/Ausgangs Telefonie Befehle auf lokalem Rechner ausführen)
- eBanking (Anbindung von lokal installierten eBanking Hardware, sowie Ausführung eBanking)
- RPC, starten von lokalen Anwendungen aus der WEBWARE heraus
- Datei/Verzeichnisse lokal editieren und Rückübertragung in das Installationsverzeichnis.
- Dateisystem Anbindung. Lokale Dateien in das WEBWARE-Filesystem des Benutzers mappen..
- Importfunktion. Definition eines lokalen Verzeichnis über das Dateien in die WEBWARE importiert werden
- Exportfunktion. Übertragen von Ausgabedateien mit Start eines lokalen Bearbeitungsprogrammes
- Automatische Komponenten Aktualisierung von WEBWARE@home

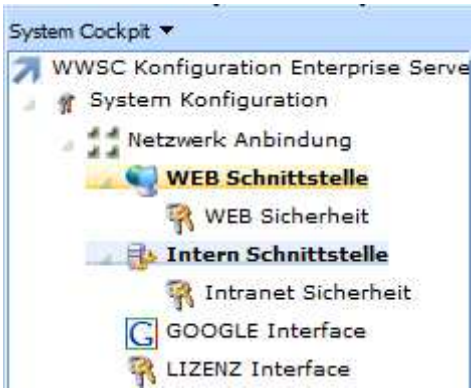
Interne Konfiguration des WEBWARE-Servers

Die Konfiguration de WEBWARE-Systems erfolgt über das WEBWARE-System-Cockpit. Je nach Berechtigung des Administrator bzw. dessen Sichtweise, werden hier weitere/unterschiedliche Funktionen angeboten.



Für globale Servereinstellungen, also Parameter die für alle Installationen des WW-Server gelten, muss mit der Sicht „Server verwalten“ gestartet werden.

Für Servereinstellungen die für eine spezielle Installation geändert werden sollen, mit der Sicht „xxxx-Firma“ gestartet werden.



Die Konfiguration der Sicherheitsfunktionen erfolgt dabei im Bereich Netzwerk-Anbindung. Hier werden die Port’s sowie SecureNET und WEBWARE-FireWALL Vorgaben definiert.

Die Schnittstellen des WEBWARE-Server sind hier als WEB-Schnittstelle (Anbindung Internet/Extern) und Intern-Schnittstelle (Intranet bzw. sicheres Netz) gezeigt.

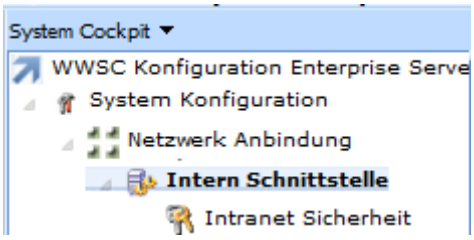
Globale Serverfunktionen

Installationsübergreifend werden zurzeit

- LUNA-Server Anbindung
- Google Integration
- WEBWARE-Update/Lizenzserver Anbindung

Global verwaltet.

Luna Netzzugang



Für die Anbindung von LUNA-Servern muss für den WW-Server eine Netzwerkschnittstelle definiert werden. Diese zeigt ins sichere Netz (intern) und sollte von dem „externen" Netz (Extern) nicht erreichbar sein. Zusätzlich sollte eine Begrenzung der erlaubten Zugangs-IP-Adressen erfolgen, um ein Zugriff auf den WW-Server aus unerlaubten Netzwerkbereichen zu unterbinden.

Parameter für die Netzwerk-Schnittstelle:

LUNA Connector IP-Adresse	local.doops.de
LUNA Connector Port	8092

Zur Aktivierung des LUNA-Subsystems, muss der Parameter LUNA Start Subsystem aktiviert werden.

LUNA Start Subsystem	J

Um nun den Zugriff auf die Schnittstelle nur auf die Rechner bzw. Netzwerkmaske zu beschränken die „sicher" sind kann man im Bereich „Intranet Sicherheit" den Parameter SecureNET vorgeben.

LUNA SecureNet-Zugriffschutz	192.168.13

Hier ist es möglich einzelne Rechneradressen bzw. Netzwerkmasken zu setzen, für die der Zugriff auf den WW-Server LUNA-Port erlaubt ist. Die Vorgabe muss direkt in IP-Notation also nicht als Domain-Namen erfolgen. Falls man mehrere Adressen angegeben will, so reicht es diese mit Leerzeichen zu trennen.

Installationsbezogene Serverfunktionen

Jede Installation hat eine bis zwei Netzwerkverbindung ins externe (Internet) und eine ins interne (sicheres) Netz. Diese können im Bereich Netzwerk Anbindung konfiguriert werden. Der Zugriff kann für alle Schnittstellen mit Hilfe der SecureNET Vorgaben begrenzt werden.

Zusätzlich stehen dem Administrator noch 2 interne FireWALL's der WEBWARE zur Verfügung mit denen auf Sitzungs- sowie Verbindnungsebene der Zugriff überwacht und im Angriffsfall automatisch verboten wird.

WEB-Schnittstelle (Externes Netz)

Die WEBWARE erlaubt es für eine WEBWARE-Instanz, 2 unterschiedliche Netzwerkzugänge zu Verwenden. Damit ist es möglich die gleiche Instanz mit 2 unterschiedlichen Netzwerkadressen sowie Sicherheitsvorgaben zu Betreiben. Also eine "sichere" interne Anbindung getrennt von einer "unsicheren" externen Schnittstelle an einer WEBWARE-Instanz.

Hierzu gibt es im Konfiguration > System-Konfiguration > Netzwerk-Anbindung > WEB Schnittstelle neue Parameter, mit denen eine 2. Schnittstelle definiert werden kann.

Mit der Standardschnittstelle ist es nur möglich eine HTTPS-Schnittstelle zu Betreiben. Die Zusatz-Schnittstelle erlaubt es auch ohne SSL-Verschlüsselung die Daten auszuliefern.

Definition der Standardschnittstelle

Die Standardschnittstelle einer WEBWARE-Instanz wird wie unten gezeigt definiert. Hierzu muss eine Netzwerkadresse (IP-Adresse, oder Domain-Name) sowie ein Port angegeben werden.

Beschreibung	Systemwert
WEB-Standardschnittstelle Netzwerk Karte	local.MeineFirma.de
WEB-Standardschnittstelle Netzwerk Port	443
Mit abweichender externer WEB-Standardschnittstelle	J
WEB-Standardschnittstelle abweichende Netzwerk Karte	Lokale.Domain.de
WEB-Standardschnittstelle abweichende Netzwerk Portnummer	443

Angabe von abweichender externer Adresse

Ist die externe Adresse abweichend von der internen Netzwerkadresse/Port, so kann dies mit dem Parameter "Mit Abweichender externer WEB-Standardschnittstelle" angegeben werden. Dies ist dann notwendig wenn die Netzwerkschnittstelle durch einen Router oder eine Firewall eine abweichende Netzwerkadresse erhält. Zusätzlich müssen dann die Abweichende externe Netzwerkadresse sowie der Port angegeben werden.

Zum Verständnis: Der WW-Server öffnet die Adresse local.MeineFirma.de mit Port 4443 um die Anfragen zu Bearbeiten. Beim ausliefern von Daten wird die abweichende externe Netzwerkbeschreibung gesetzt, also Lokale.Domain.de Port 443. Damit können zum Beispiel Ressourcen, wie Ausdrucke, korrekt heruntergeladen werden.

Die WEB-Standardschnittstelle setzt immer HTTPS als Verbindungsprotokoll voraus. Dies hierzu notwendigen Informationen werden im Bereich HTTP Transport SSL definiert.

Definition einer WEB-Zusatzschnittstelle

Um unterschiedliche Zugänge zu einer WW-Instanz zu Betreiben, kann eine Zusatzschnittstelle mit erweiterten Funktionen definiert werden. Gehen Sie hierzu wie oben beschrieben in den Bereich Netzwerk-Anbindung > WEB-Schnittstelle. Dort finden sie folgende Parameter für die WEB-Zusatzschnittstelle. (Hier nur die relevanten Parameter)

Beschreibung	Systemwert
WEB-Zusatzschnittstelle Netzwerk Karte	Internet.MeineFirma.de
WEB-Zusatzschnittstelle Netzwerk Port	10000
WEB-Zusatzschnittstelle ohne SSL betreiben	J
Externe WEB-Zusatzschnittstelle ohne SSL betreiben	N
Mit Abweichender externer WEB-Zusatzschnittstelle	J
WEB-Zusatzschnittstelle abweichende Netzwerk Karte	Internet.Mein.Router.de
WEB-Zusatzschnittstelle abweichende Netzwerk Portnummer	443

Die ersten beiden Zeilen geben die Netzwerkadresse und den Netzwerkport am lokalen Rechner an, welche für die Anbindung verwendet werden. Die Netzwerkschnittstelle wird dann **gestartet** wenn ein **Port angegeben** wurde. Die Änderung an diesen Parametern stehen erst nach einem Neustart des WW-Server zur Verfügung.

Ist die externe Adresse abweichend von der internen WEB-Zusatzschnittstelle (Adresse/Port), so kann dies mit dem Parameter "Mit Abweichender externer WEB-Zusatzschnittstelle " angegeben werden. Dies ist dann notwendig wenn die Netzwerkschnittstelle durch einen Router oder eine Firewall vorgegeben wird. Zusätzlich müssen dann die Parameter WEB-Zusatzschnittstelle "Netzwerk Karte" und "Port" angegeben werden.

Zum Verständnis: Der WW-Server öffnet die WEB-Zusatzschnittstelle Internet.MeineFirma.de mit Port 10000 um die Anfragen zu Bearbeiten. Beim ausliefern von Daten wird die abweichende externe Netzwerkbeschreibung gesetzt, also Internet.Mein.Router.de 443.

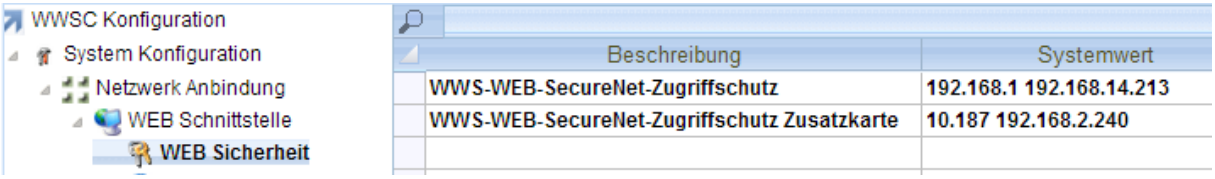
WEB-Zusatzschnittstelle: Zusatzfunktion SSL deaktivieren

Es ist möglich an der WEB-Zusatzschnittstelle das SSL Protokoll zu deaktivieren. **Dies ist nur dann ratsam, wenn der WEBWARE-Server mit Hilfe eines SSL-Proxy/FireWALL usw. betrieben wird**. Der WEBWARE-Server verarbeitet dann die Kommunikation über die WEB-Zusatzschnittstelle ohne das SSL Subsystem.

Hierzu muss der Parameter "WEB-Zusatzschnittstelle ohne SSL betreiben" auf J(a) gesetzt werden. Ist dies der Fall, so geht der WEBWARE-Server davon aus das bei vorhandener "Mit abweichender extern WEB-Zusatzschnittstelle" diese über HTTPS angebunden ist, und wird entsprechend die Externen Referenzen so setzen. Wollen Sie auch über die abweichende externe WEB-Zusatzschnittstelle Daten mit HTTP ausliefern, so muss der Parameter "Externe WEB-Zusatzschnittstelle ohne SSL betreiben" mit J(a) gesetzt werden.

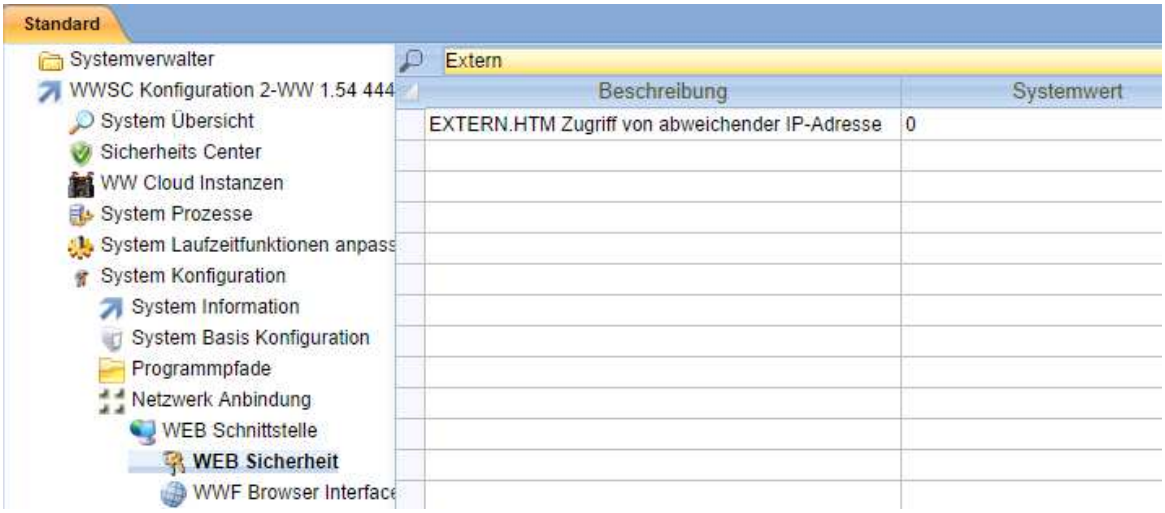
Absicherung über Netzwerkbeschränkung

Um die Schnittstellen weiter abzusichern kann für jede Netzwerkkarte getrennt eine Positivliste von Adressen und Adressbereichen angegeben werden die auf die entsprechende Netzwerkschnittstelle zugreifen dürfen.



Zugriff auf Dateien mit EXTERN.HTM

Um den Zugriff auch in anderen Browser-Fenstern (Vorschau, Download, Anzeige, usw.) zu gewähren, verwendet der WW-Server einen generierten Link auf die Datei https://[Server-Adresse]/EXTERN.HTMxxxxxxxx. Dieser Link dient dazu den Zugriff auf die "sichere" Ressource auch in Browser Fenstern zu Erlauben die nicht die gültigen Sitzungsinsformationen besitzen.

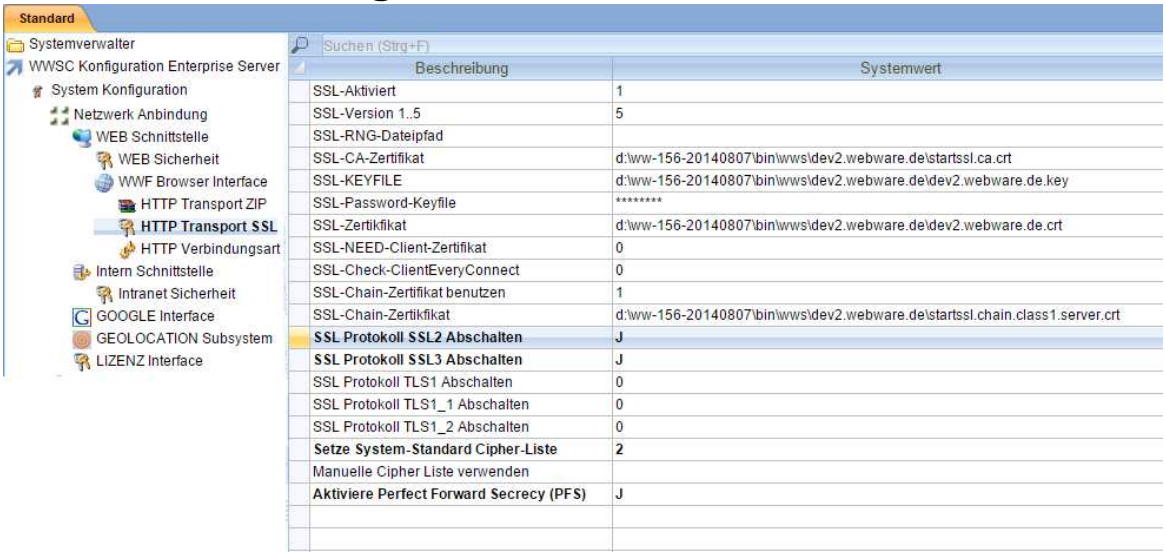


Ab der Release vom 13.10.2014 ist der Zugriff auf solche Link's nur noch von der gleichen IP-Adresse möglich von der die aktuelle Sitzung verbunden ist möglich. Der Link hat dabei eine Gültigkeitsdauer der aktuellen Sitzung.

Will man das alte Verhalten wieder aktivieren, so kann man dies mit dem Systemwert "EXTERN.HTM Zugriff von abweichender IP-Adresse erlauben.." .

Wird ein Zugriff von einer abweichenden IP-Adresse erkannt und der Systemwert erlaubt dies nicht, so wird die Fehlerseite 404 ausgegeben. Intern protokolliert der WW-Server diesen unerlaubten Zugriff in der Sicherheits-Protokoll-Datei (Bin\WWS\SECURITY\[LFD-Nr]\WWS-SECURITY-[Datum].log mit der Fehlernummer 90016 protokolliert.

SSL / Zertifikat / Zugriffssicherheit



Beschreibung	Systemwert
SSL-Aktiviert	1
SSL-Version 1..5	5
SSL-RNG-Dateipfad	
SSL-CA-Zertifikat	d:\ww-156-20140807\bin\wws\dev2.webware.de\startssl.ca.crt
SSL-KEYFILE	d:\ww-156-20140807\bin\wws\dev2.webware.de\dev2.webware.de.key
SSL-Password-Keyfile	********
SSL-Zertikfikat	d:\ww-156-20140807\bin\wws\dev2.webware.de\dev2.webware.de.crt
SSL-NEED-Client-Zertifikat	0
SSL-Check-ClientEveryConnect	0
SSL-Chain-Zertifikat benutzen	1
SSL-Chain-Zertikfikat	d:\ww-156-20140807\bin\wws\dev2.webware.de\startssl.chain.class1.server.crt
SSL Protokoll SSL2 Abschalten	**J**
SSL Protokoll SSL3 Abschalten	**J**
SSL Protokoll TLS1 Abschalten	0
SSL Protokoll TLS1_1 Abschalten	0
SSL Protokoll TLS1_2 Abschalten	0
Setze System-Standard Cipher-Liste	**2**
Manuelle Cipher Liste verwenden	
Aktiviere Perfect Forward Secrecy (PFS)	**J**

Im Bereich System-Konfiguration > Netzwerk Anbindung > WEB Schnittstelle > WWF Browser Interface > HTTP Transport SSL, können Sie die Parameter für den Betrieb mit SSL vorgeben.

Folgende Parameter stehen zur Verfügung

SSL Aktiviert : Dieser Wert muss immer gesetzt sein.

SSL-Version : Hier können Sie einen Wert von 1 bis 5 eingeben. Standard ist 5

0: NO-SSL

1: Benutze SSL 2.0

2: Benutze SSL 3.0

3: Benutze TLS 1.x

4: Benutze DTLS 1.

5: Rückfallsystem aktiviert

SSL-RNG-Dateipfad: Hier können Sie eine Datei angeben die für den Zufallsgenerator verwendet wird.

SSL-CA-Zertifikat: Angabe der CA (Certificat Authority) -Datei für das verwendete Zertifikat

SSL-Keyfile: Vorgabe der Schlüsseldatei für das verwendete Zertifikat

SSL-Passwort Keyfile Hinterlegung des Passwortes für das SSL-Schlüssel Datei (SSL-Keyfile)

SSL-Zertifikat: Angabe der Datei die das Serverzertifikat enthält

SSL-Chain Zertifikat J/N Solle in Chain Zertifikat verwendet werden.

SSL-Chain Zertifikat Pfad/Datei für das verwendete Chain-Zertifikat

SSL Protokoll xx abschalten Hier können einzelnen SSL-Protkoll abgeschaltet werden

xx= SSL2, SSL3, TLS1, TLS1_2, TLS1_2

Setze System Cipher Liste: Wert 0,1,2 folgende Werte sind möglich:

0: Cipher-Liste bis zum 21.10.2014

```
ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:RC4:HIGH:!MD5:!aNULL:!EDH
```

1: Cipher-Liste ab 21.10.2014 mit aktiviertem RC4

```
ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-RC4-SHA:ECDHE-RSA-AES128-SHA:RC4:HIGH:!MD5:!aNULL:!EDH
```

2: Cipher-Liste ab 21.10.2014 ohne aktiviertem RC4

```
ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-RC4-SHA:ECDHE-RSA-AES128-SHA:!RC4:HIGH:!MD5:!aNULL:!EDH
```

!!! ACHTUNG manuelle Änderung der Cipher-Liste kann den Server blockieren !!!

!!! Folgenden Parameter nur setzen wenn Sie wissen was Sie machen. Nähere Info's zum setzen der Cipher-Liste finden Sie hier: https://www.openssl.org/docs/apps/ciphers.html !!!

Falls Sie eine eigene abweichende Cipher-Liste vorgeben wollen, können Sie das mit dem Parameter "manuelle Cipher Liste verwenden" angeben. Nach dem Disablen von RC4, (Auswahl von Cipher-Liste 2) sieht der Server-Test so aus:

Aktiviere Forward Secrecy J/N nähere Inforamtionen weiter unten.

Einleitung in Zertifikate..

Hierzu gibt es eine eigene Dokumentation WW-DOKU-Zertifikate.PDF in welcher die Handhabung von Zertifikaten erklärt wird.

Ein Zertifikat ist direkt an eine Adresse (Bspl: SoftEngine.de oder 192.168.99.99..) gebunden. Daher ist es nicht möglich ein Generelles Zertifikat auszuliefern das für alle Umgebungen passt.

Damit ein gültiges Zertifikat in einem Browser akzeptiert wird, ist es notwendig das das Zertifikat von einer, dem Browser bekannten Stelle (CA), signiert (unterschrieben) wird. Der Browser prüft dabei die Kette von Zertifikaten bis zur Bekannten Stelle (CA).

Achtung!!: Bei einer Fehlkonfiguration ist der Zugriff auf Ihre WEBWARE nicht mehr möglich, da die WEBWARE ein funktionierendes Schlüsselsystem voraussetzt. Falls Ihre WEBWARE nicht mehr ansprechbar ist, fügen Sie folgende Zeilen in Ihre WWS.ini ein:

BWWSSL_CA_ZERTIFIKAT=demozertifikat\startssl.ca.crt

BWWSSL_ZERTIFIKAT=demozertifikat\softengine.meine-webware.de.crt

BWWSSL_PASSWORD4PRIVKEY=meinewebware

BWWSSL_PRIVATEKEY=demozertifikat\private-key.key

BWWSSL_USE_CHAIN_ZERTIFIKAT=J

BWWSSL_CHAIN_ZERTIFIKAT=demozertifikat\startssl.chain.class1.server.crt

Ein gültiges Zertifikat besteht aus mehreren Bestandteilen:

CA-Zertifikat: Verweis auf die signierende Stelle (Certificate Authority)

Server-Zertifikat: Zertifikat die für Ihren Server ausgestellt wurde

Schlüsseldatei: In dieser Datei ist der interne und öffentliche Schlüssel für die Verschlüsselung vorhanden

Das Key-File / Schlüsseldatei kann in der WWS.ini mit folgendem Parameter angegeben werden:

BWWSSL_PRIVATEKEY=[Pfad zu SSL-Dateien]\Schlüssel-Datei

Passwort für Schlüsseldatei: Damit ein WEB-Server die Schlüsseldatei öffnen kann benötigen Sie den zugehörigen geheimen Schlüssel. Die WEBWARE erlaubt es ihnen diesen Schlüssel über die WWS.ini vorzugeben.

HINWEIS: Nach erfolgreicher Konfiguration kann der Eintrag

```
#-INIOK-# BWWSSL_PASSWORD4PRIVKEY=xx
```

entfernt werden, da der Schlüssel in der internen Parameterverwaltung gespeichert wird, und Ihr geheimer Schlüssel damit nicht auslesbar ist.

Welches Format benötigen die Dateien ?

Die Schlüsseldateien sollten im Format PEM vorliegen. Das Serverzertifikat wird dabei an den Client-Browser ausgeliefert so dass dieser die Echtheit der SSL-Domain feststellen kann.

Welche Dateien werden benötigt ?

Man muss hier zuerst in 2 Formate unterscheiden. Die unterschiedlichen Zertifikats-Austeller werden nicht in allen Browsern gleichermaßen akzeptiert. Daher gibt es hier 2 Möglichkeiten:

Einzel-Zertifikate

Bei einem Einzel-Zertifikat wird ein Server-Zertifikat benötigt welches an den Browser-Client ausgeliefert wird und das in einer PEM-Datei nur dieses Zertifikat enthält.

Ein Einzel-Zertifikat kann in der WWS.INI mit folgendem Parameter angegeben werden:

BWWSSL_ZERTIFIKAT=[Pfad zu SSL-Dateien]\Schlüssel-Datei

Chain-Zertifikate

Hierbei wird ein Chain-Zertifikat (PEM-Format) benötigt das in einer Datei 3 Zertifikate enthält. Zuerst das Server-Zertifikat, dann das "Intermediate CA Certificate" und am Schluss das Top-Level CA-Zertifikat.

Diese Zertifikatsart ist eigentlich die bessere da hier dem Client-Browser alle notwendigen Informationen direkt übergeben werden.

Dabei werden die einzelnen Schlüsseldateien einfach hintereinander in eine Text-Datei kopiert und sind dabei durch die Header die in den Schüsseldateien vorhanden sind automatisch getrennt.

Ein Chain-Zertifikat kann in der WWS.INI mit folgenden Parametern angegeben werden:

BWWSSL_USE_CHAIN_ZERTIFIKAT=J

BWWSSL_CHAIN_ZERTIFIKAT=[Pfad zu SSL-Dateien]\Schlüssel-Datei

Welche Möglichkeiten haben Sie ein gültiges Zertifikat in Ihre WEBWARE rein zubekommen ?

Verwendung von SoftENGINE ausgelieferten Zertifikaten

Falls Sie keine Änderung in der Konfiguration vornehmen ist das Standard-Zertifikat Meine-Webware.de als Standard im WEBWARE-Server installiert. Nähere Infos finden Sie in der Datei

\bin\wws\demozertifikat\liesmich.txt

Damit das Zertifikat von Ihrem Browser akzeptiert wird müssen Sie folgende Schritte durchführen.

- Mit Hilfe eines Proxy's/Router/Name-Server oder der lokalen HOST-Datei muss der Domain Name des Rechners auf Meine-Webware.de gesetzt werden. Sie können dann vom Browser aus mit der Adresse https://meine-webware.de auf die WEBWARE zugreifen

- Das Zertifikat ist ein öffentliches Zertifikat das von allen gängigen Browsern akzeptiert wird.

- Das Zertifikat ist gültig bis 02.07.2017

- Bei Vorgabe über HOSTS-Datei ist der Zugriff nur lokal möglich. Bei Verwendung eines Named-Server ist auch der Zugriff von anderen Rechnern die diesen Name-Server verwenden ohne Zertifikats-Fehler möglich.

Anpassung einer bestehenden WWS.INI bei Update eines bestehenden Systemes.

(ersetzen Sie hier *[WWS-PFAD]* mit dem Verzeichnispfad des WW-Servers, bzw. wenn die Zertifikatsdatei unterhalb des WWS-Pfades liegt [bin\wws] kann direkt mit dem Zertifikatspfad begonnen werden)

BWWSSL_ON=J

```
BWWSSL_CA_ZERTIFIKAT=demozertifikat\startssl.ca.crt

BWWSSL_ZERTIFIKAT=demozertifikat\softengine.meine-webware.de.crt

BWWSSL_PASSWORD4PRIVKEY=meinewebware

BWWSSL_PRIVATEKEY=demozertifikat\private-key.key
```

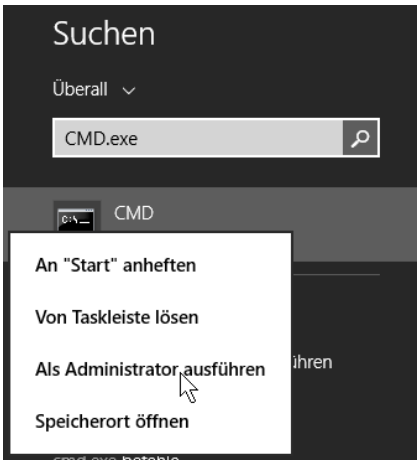
BWWSSL_USE_CHAIN_ZERTIFIKAT=J

BWWSSL_CHAIN_ZERTIFIKAT=demozertifikat\startssl.chain.class1.server.crt

Einsatz auf einem lokalen System, durch Anpassen der HOSTS Datei

Gehen Sie hierzu wie folgt vor, da die Änderung der Datei HOSTS nur von einem Admin möglich ist:

Geben Sie in der Windows-Suche den Begriff CMD.exe ein und starten Sie das gefundene Programm über "als Administrator ausführen"



Wechseln Sie in das Verzeichnis cd c:\windows\system32\drivers\etc

Öffnen Sie in einem Text-Editor die Datei HOSTS (hat keine Datei-Endung)

Fügen Sie nun am Ende der Datei die folgende Zeile ein

127.0.0.1 meine-webware.de

(Hinweis, falls Ihnen ihre Lokale IP-Adresse bekannt ist, können Sie auch diese hier angeben, wenn nicht ist diese mit dem Befehl ipconfig in einer Kommandozeile ermittelbar)

Speichern Sie die Datei ab, und Beenden Sie die Kommando-Zeile (CMD.exe)

Fertig: Nun müsste die WEBWARE als sichere Seite unter der Adresse https://meine-webware.de erreichbar sein.

Erstellen eines kostenlosen Zertifikat über StartSSL.com

!!! Ab Februar 2017 werden von einigen Browser-Hersteller (CHROME/FIREFOX)

Zertifikate von STARTSSL.com nicht mehr akzeptiert. !!!

Es ist möglich bei der Zertifizierungsstelle https://www.startssl.com/ kostenlose Zertifikate zu beantragen. Diese Zertifikate sind 1 Jahr gültig. Es ist nur möglich ein Zertifikat für eine Domain zu beantragen bei der man Zugriff auf eine von 3 Haupt-eMail-Adressen hat. Bspl:

- webmaster@softengine.de
- postmaster@softengine.de
- hostmaster@softengine.de

Konfiguration des WW-Servers für StartSSL Zertifikate

Um den WW-Server in allen Browsern korrekt mit den Start-SSL Zertifikaten verwenden zu können, muss ein sogenanntes Chain-Zertifikat erstellt werden. Dabei muss innerhalb einer Datei der Zertifizierungspfad der einzelnen Zertifikate enthalten sein. Die Chain-Datei muss im PEM-Format vorliegen. Ein Beispiel für ein Chain-Zertifikat finden Sie im Pfad bin\wws\meine-webware.de bzw. bin\wws\demozertifikat.

Link auf einen Artikel der die Erstellung erklärt:

http://www.heise.de/security/artikel/SSL-fuer-lau-880221.html

Link auf einen Artikel der erklärt wie man die Chain-Datei unter Unix erstellt

http://jasoncodes.com/posts/startssl-free-ssl

Schritt für Schritt Erklärung Anlage eines Zertifikates

Um ein eigenes Zertifikat mit Hilfe von STARTSSL zu Erzeugen benötigen Sie die OpenSSL.exe welche von der WEBWARE im bin\wws Pfad mit ausgeliefert wird.

Für dieses Beispiel verwende ich meine-webware.de als Zieldomain.

1. Anmelden bei STARTSSL

Gehen Sie hierzu auf die Seite STARTSSL.com und melden Sie sich mit "Sign Up" dort an.

Wichtig ist das Sie zu einer der 3 eMail Adressen Ihrer Domain Zugriff haben: webmaster@.., postmaster@.., oder hostmaster@..., um sich selbst zu Authentifizieren.

2. Erzeugen eines CSR (Certificate Signing Request)

Hierzu benötigen Sie die OPENSSL.exe. Ein CSR ist ein Text der später an STARTSSL.com übergeben wird, und bei dem alle notwendigen Informationen enthalten sind.

Ersetzen Sie in dem Aufruf den Text meine-webware.de mit Ihrer Domain

```
openssl req -newkey rsa:2048 -keyout meine-webware.de.key -out meine-webware.de.csr
```

In der Folge werden sie aufgefordert einige Informationen einzugeben:

Wichtig ist hier "Enter PEM Pass Phrase" hier ein Passwort für die Schüsseldatei eingeben.

```
D:\>openssl req -newkey rsa:2048 -keyout meine-webware.de.key -out meine-webware.de.csr
Generating a 2048 bit RSA private key
.....................................................................................
.......+++
writing new private key to 'meine-webware.de.key'
Enter PEM pass phrase: meinewebware
Verifying - Enter PEM pass phrase: meinewebware
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:DE
State or Province Name (full name) [Some-State]:Wohnort
Locality Name (eg, city) []:Wohnort
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Meine-Firma
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:meine-webware.de
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:meinewebware
An optional company name []:
```

Nachdem die Erzeugung durchgelaufen ist, erhalten Sie 2 Dateien.

```
02.07.2016  09:25             1.037 meine-webware.de.csr
02.07.2016  09:25             1.834 meine-webware.de.key
```

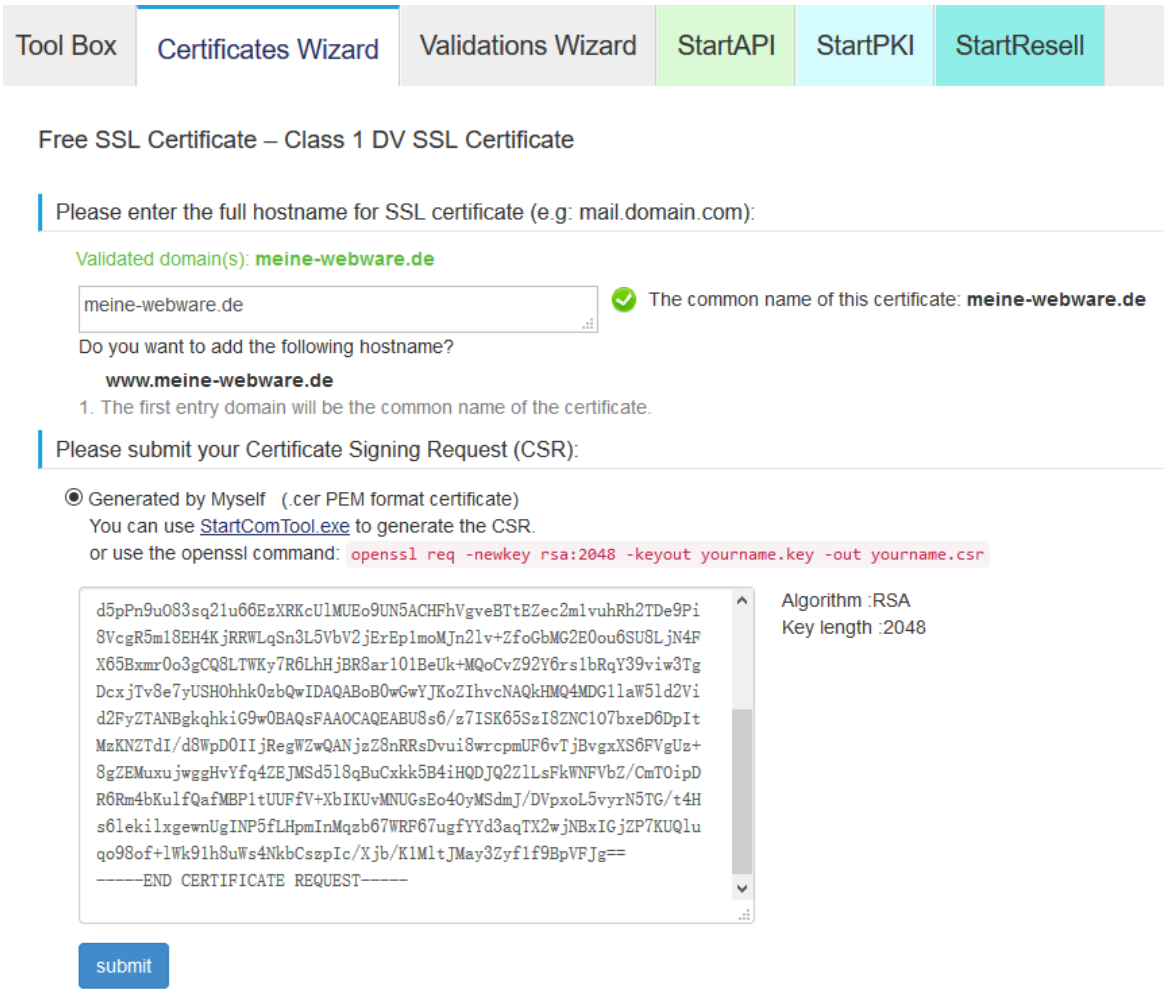
Die meine-webware.de.key ist der geheime Schlüssel der später im WW-Server benötigt wird. (Hierzu gehört auch das vergebene Passwort).

Die 2. Datei ist der CSR der für die Zertifikats Anfrage benötigt wird.

3. Wechseln Sie nun zu STARTSSL.COM

Melden Sie sich an, und Validieren Sie Ihre Domain. Dabei wird für die Domain und auch für die von Ihnen dort einzugebende eMail-Adresse ein Authentification-Code geschickt mit dem Sie sich einmalig authentifizieren müssen.

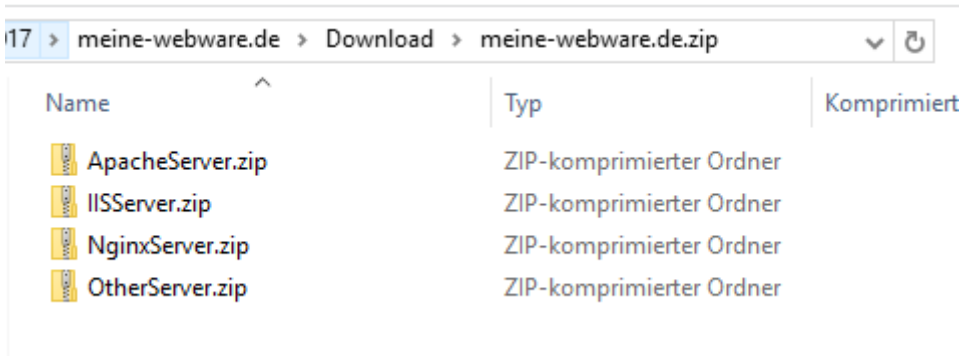
4. Wechseln Sie dann in den Bereich Certificates Wizard



Geben Sie Ihre Domain ein (meine-webware.de) und markieren Sie den Radio-Button (Generated by Myself), und kopieren Sie die CSR-Datei mit Copy&Paste in den Eingabeeditor.

Senden Sie dann die Abfrage mit Submit ab.

Sie erhalten dann einen Link mit dem Sie eine ZIP-Datei herunterladen können. Diese besteht aus mehreren ZIP-Dateien. Hier ist die Datei OtherServer.zip wichtig. Entpacken Sie diese in ein Verzeichnis:



5. Erzeugen der CHAIN-Datei

Wechseln Sie in das Verzeichnis in der Sie die Dateien aus OtherServer.zip kopiert haben. Dort kopieren Sie folgendendes Script mit als Batch-Datei ein (Bspl. Mache.BAT)

REM Kopieren der Meine-webware.de Zertifikate in eine Chain-Datei

type 2_%1.crt > %1.crt

type 2_%1.crt > startssl.chain.class1.server.crt

type 1_Intermediate.crt >> startssl.chain.class1.server.crt

type root.crt >> startssl.chain.class1.server.crt

type root.crt > startssl.ca.crt

Rufen Sie anschließend die Mache.Bat dem Aufrufparameter Ihrer Domain auf. Beispiel:

MACHE.BAT meine-webware.de

Damit wird nun eine Chain-Zertifikatsdatei mit dem Namen startssl.chain.class1.server.crt erstellt.

Sie haben nun alle Dateien zusammen die Sie für das Zertifikat benötigen.

Kopieren Sie nun folgende Dateien in ein Verzeichnis das Sie unterhalb des BIN\WWS-Verzeichnisses für Ihre Domain anlegen. (Bspl: meine-webware.de)

In diesem sollten dann folgende Dateien enthalten sein.

- startssl.ca.crt
- meine-webware.de.crt
- meine-webware.de.key (wurde zuvor von uns selbst erstellt und muss selbst kopiert werden)
- startssl.chain.class1.server.crt

Nun müssen Sie das Zertifikat noch im WW-Server bekannt machen. Sie können dies über das System-Cockpit machen oder wie hier gezeigt durch die Angabe in der WWS.ini. Fügen Sie hierzu folgende Zeilen in die WWS.ini ein:

BWWSSL_CA_ZERTIFIKAT=meine-webware.de\startssl.ca.crt

BWWSSL_ZERTIFIKAT= meine-webware.de \ meine-webware.de.crt

BWWSSL_PASSWORD4PRIVKEY=meinewebware

BWWSSL_PRIVATEKEY= meine-webware.de \private-key.key

BWWSSL_USE_CHAIN_ZERTIFIKAT=J

BWWSSL_CHAIN_ZERTIFIKAT= meine-webware.de \startssl.chain.class1.server.crt

Nach einem Neustart des WW-Servers sollten dann das Zertifikat eingelesen und verwendet werden.

Erstellung eines eigenen, selbst Signierten Zertifikates

Mit Hilfe der OpenSSL - Programme können Sie sich auch ein selbst signiertes Zertifikat erstellen. Das von SoftENGINE ausgelieferte demo.webware.de Zertifikat ist ebenfalls mit openSSL erstellt.

Hier ein Link zu einer Einleitung in Zertifikate:

http://www.openssl.org/docs/HOWTO/certificates.txt

Hier ein Link zu einer Kurz Referenz von OpenSSL

http://www.dfn-cert.de/informationen/themen/verschluesselung_und_pki/openssl-kurzreferenz.html

Hier ein YouTube Video

http://www.youtube.com/watch?v=LHUbQtUeQ0o

Let's Encrypt: Erstellen von WEBWARE Zertifikaten

Bei der integrierten Zertifikats Verwaltung über Let's Encrypt ist zu Beachten das es sich um einen externen Anbieter handelt, dessen Dienstleistung nicht von SoftENGINE garantiert werden kann

https://letsencrypt.org/

Kurze Einleitung zu Zertifikaten

Um Ihren WEBWARE Server Sicher zu Betreiben benötigen Sie ein Zertifikat, also so etwas ähnliches wie einen Ausweis den Sie den Client's (Browsern) beim Verbindungsaufbau vorlegen müssen. Dieses Zertifikat wird dabei für einen Domain-Namen (Bspl: Meine-WEBWARE.de) ausgestellt. Der Client (Browser) prüft nach Erhalt des Zertifikat ob dieses gültig ist. Dabei prüft er neben Gültigkeitsdauer (Start-Termin/End-Termin) auch ob der im Zertifikat angegebene Domain-Namen mit dem Domain-Namen der in der Browser Adressleiste eingegeben wurde übereinstimmt.

Die WEBWARE ermöglicht Ihnen integrierte Zertifikate mit Hilfe der WEB-Platform Let's Encrypt (im folgenden LE benannt) zu Erstellen und zu Verwenden. Dies kann direkt aus dem WEBWARE System-Cockpit erfolgen. Um diese Funktion zu Verwenden sind einige Grundvorrausetzungen zu Erfüllen.

Ein erstelltes Zertifikat muss von LE überprüft und die Berechtigung der Verwendung getestet werden. Hierzu benötigt die LE-Zertifikatsprüfung die Möglichkeit zu Ermitteln ob Sie die Hoheit / Berechtigung über die Domain bzw. Subdomain haben für die Sie ein Zertifikat erstellen wollen.

WEBWARE Zertifikats - Prüfungsverfahren

Die WEBWARE bietet Ihnen 2 Verfahren an mit denen Sie die die Prüfung auf Berechtigung für Ihre Domian durchführen können. (HTTP und FTP)

HTTP-Prüfung

Hier sind 2 Voraussetzungen zu erfüllen. Der Rechner auf dem die WEBWARE betrieben wird, muss aus dem Internet unter dem zu Prüfenden Domain-Namen sowie dem HTTP-Port 80 ansprechbar sein,. Eine weitere Voraussetzung ist das auf dem Rechner ein HTTP-Server auf Port 80 von der WEBWARE gestartet werden kann, welcher aus dem Internet dann auch über den Domain-Namen ansprechbar ist.

Bspl: Wunsch-Domain Meine-WEBWARE.de, hier sollte während der Domain-Prüfung der Zugriff mit http://Meine-WEBWARE.de auf den WEBWARE Rechner möglich sein. (HTTP = Port 80)

Hier ist der Grundablauf dass das Zertifikat angefordert wird, und der Zertifikats-Austeller (LE) eine Anweisung gibt eine Datei in einem bestimmten Pfad unter http://Meine-WEBWARE.de bereit zu Stellen. Kann dieser dann diese Datei über das Internet herunterladen wird das Zertifikat erteilt. Die WEBWARE startet hierzu einen HTTP-Server auf Port 80 über den der Zertifikats-Aussteller (LE) die gewünschte Prüfungsdatei laden kann.

Falls Sie einen Proxy vor Ihren WEBWARE-Server geschaltet haben, können Sie den externen Port 80 (HTTP) auch auf einen anderen internen Port auf dem WEBWARE-Server Rechner routen und mit der WW dort temporär einen HTTP-Server für die HTTP-Challenge starten. Hierzu können Sie den Parameter HTTP abweichender Port 80 verwenden.

FTP-Prüfung

Die WEBWARE bietet ein weiteres Verfahren bei dem die Voraussetzung ist das Sie die Zugangsdaten zum Ftp-Server Ihrer Wunsch-Domain haben.

Notwendige Informationen:

FTP-Server Adresse: ftp://meine-webware.de/www/

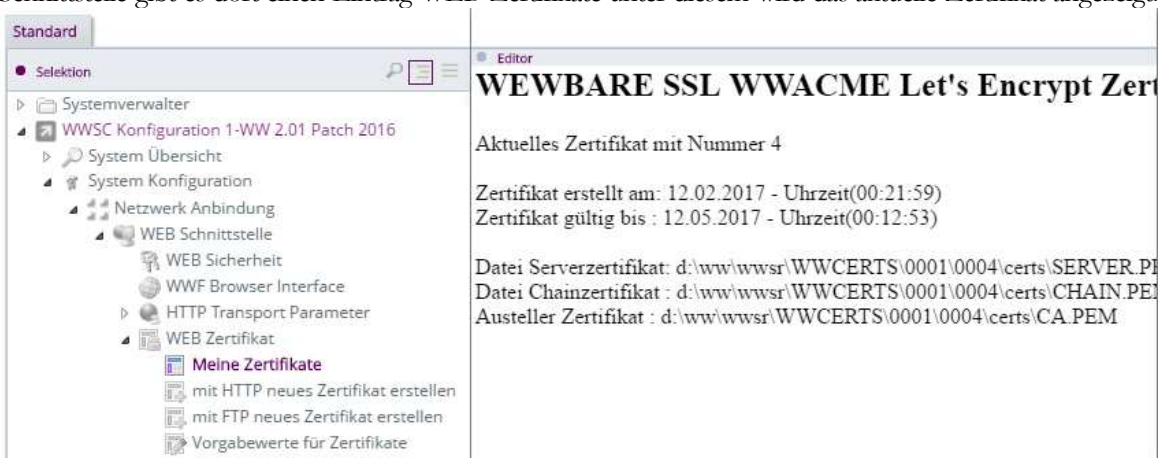
FTP-Server Benutzer: mein_Benutzer..

FTP-Server Passwort: *******

Hier ist der Grundablauf dass das Zertifikat angefordert wird, und der Zertifikats-Austeller (LE) eine Anweisung gibt eine Challenge-Datei in einem bestimmten Pfad unter http://Meine-WEBWARE.de bereit zu Stellen. Kann dieser dann diese Datei über das Internet herunterladen wird das Zertifikat erteilt. Die WEBWARE kopiert vor der Prüfung der Challenge-Datei, diese in den gewünschten Pfad auf dem FTP-Server so dass Ihr Standard-Webserver diese ausliefern kann.

Integrierte Zertifikats Verwaltung

Sie finden die Integrierte Zertifikats Verwaltung im Bereich Konfiguration. Unterhalb der WEB Schnittstelle gibt es dort einen Eintrag WEB-Zertifikate unter diesem wird das aktuelle Zertifikat angezeigt.



Unterhalb finden sie 4 Äste mit folgenden Aufgaben.

- Meine-Zertifikate: Liste Ihrer mit WEBWARE erstellten Zertifikate
- mit HTTP neues Zertifikat erstellen Ein Zertifikat mit HTTP Prüfung erstellen
- Mit FTP neues Zertifikat erstellen EinZertifikat mit FTP Prüfung erstellen
- Vorgabewerte für Zertifikate Hier werden Vorschlagswerte zwischengespeichert

Meine Zertifikate

Hier erhalten Sie eine Liste aller Zertifikate die bisher in der WEBWARE von Ihnen erstellt wurden. Je nach Zustand des Zertifikates werden die Zeilen in unterschiedlicher Farbe dargestellt, ebenso erhalten Sie je nach Zustand des Zertifikates weitere Menü-Punkte im Hauptmenü oben angezeigt.

Code der Farb-Darstellung der Zertifikate:

ROT: Dieses Zertifikat ist nicht gültig und kann nicht verwendet werden.

GRÜN: Dieses Zertifikat hat gültige Zertifikatsdateien und kann unter Berücksichtigung der Gültigkeitsdauer verwendet werden.

BLAU: Dieses Zertifikat ist das aktuell verwendete.

Informationsfelder der Zertifikate

Info:	OK, bedeutet es sind die notwendigen Zertifikatsdateien verfügbar	
Haupt-Domain:	Für welche Haupt-Domain wurde das Zertifikat ausgestellt	
Reichweite:	PRIVATE	Es handelt sich um ein Test-Zertifikat, nicht verwendbar
	PUBLIC	Es ist ein öffentlich gültiges Zertifikat
Gültig bis:	Ein Zertifikat hat ein Verfallsdatum. Hier wird angegeben bis wann das Zertifikat verwendet werden kann.	
Erzeugt am:	Der Browser prüft bei einem Zertifikat ebenfalls der Zeitpunkt ab wann das Zertifikat gültig ist. Da die Zertifikate in der WEBWARE in Echtzeit erstellt und verwendet werden können, sollte dieser Termin immer erreicht werden.	
LE-Code	Code von LE der Angibt ob es bei der Erstellung Probleme gab. (1=OK)	
LE-Informationen	Hier sind weitere Informationen zu finden, falls es Probleme gab	
Hinweise	Hinweise vom WWACME Programm welches die Erstellung durchführt	
Sub-Domains	Hier sehen Sie die Liste der Sub-Domains welche im Zertifikat enthalten sind	

Funktionen für Meine Zertifikate

Markieren Sie ein Zertifikat so werden Ihnen je nach Zustand verschiedene Funktionen angezeigt. Dies ist davon abhängig um welche Art von Zertifikat (PRIVATE/PUBLIC) sowie ob das Zertifikat gültig ist.

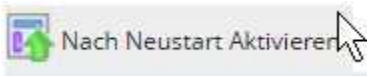
Zertifikat Testen

Wenn Sie ein Zertifikat testen wollen können Sie dies mit dieser Funktion tun. Dabei wird ein interner Test-Zugang für eine Minute gestartet der das Zertifikat bereit stellt. Die Netzwerkkarte für den Zugang wird dabei aus der aktuellen WEBWARE-Instanz geholt. Beim Port wird ein offener ausgehend von Port 2000 gesucht.

Klicken Sie hier auf Starten, so wird ein interner HTTPS-Server gestartet und in Ihrem Browser eine neue Seite mit dem Browser-Zugang angezeigt.

Der Server Beendet sich automatisch nach 1 Minute. Sie können sich zum Beispiel im Chrome-Browser mit F12 in den Entwickler-Tools (Karteikarte Security) weitere Informationen zu dem Zertifikat aufrufen.

Nach Neustart Aktivieren

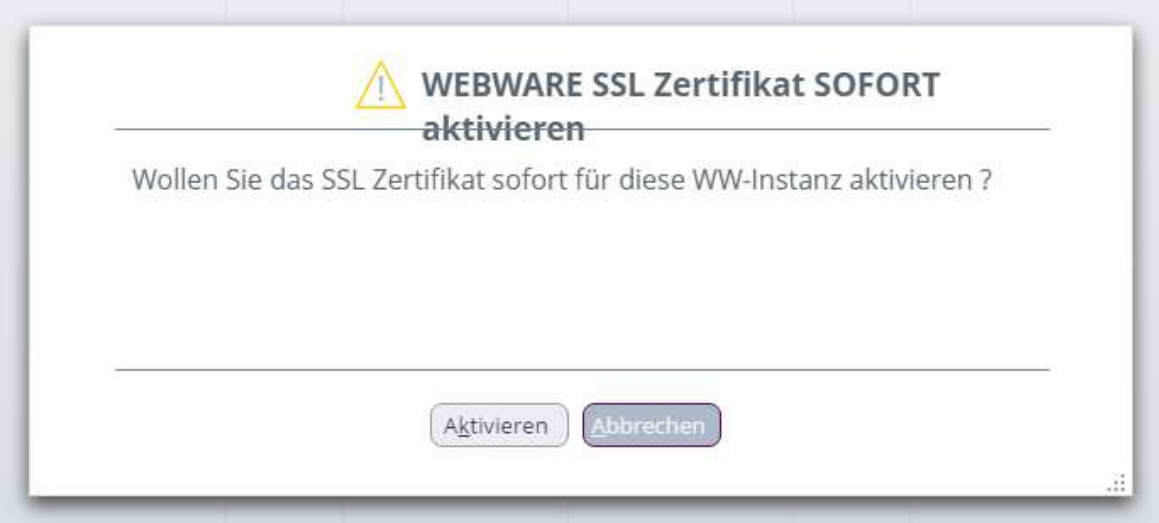


Mit dieser Funktion können Sie ein Zertifikat aus "Meine Zertifikate" als aktives Zertifikat eintragen. Dabei werden die notwendigen Informationen für das Zertifikat eingetragen, und beim nächsten Neustart der WEBWARE wird das Zertifikat dann als Standardzertifikat ausgeliefert.

Sofort Aktivieren

Mit dieser Funktion können Sie ein Zertifikat aus "Meine Zertifikate" als aktives Zertifikat eintragen. Dabei wird das Zertifikat für zukünftige Verbindungsaufbauten verwendet. Diese Funktion kann unter Umständen Seiteneffekte auslösen und sollte nur im Notfall eingesetzt werden. Im Programm entsteht dadurch ein Speicherbereich welcher nicht freigegeben wird.

Denken Sie daran das Sie bei Problemen mit dem Zertifikat keinen Zugang mehr zu Ihrem System haben. Bitte Testen Sie daher das Zertifikat mit der Funktion "Zertifikat Testen" ob es von Ihren Browsern akzeptiert wird.



Beantworten Sie den Dialog mit "Aktivieren" so wird das Zertifikat direkt eingetragen und verwendet.

Da Ihr WEBWARE System zu diesem Zeitpunkt sicherlich mehrere Verbindungen mit dem alten Zertifikat offen hat, werden diese Verbindungen beibehalten und nur neue Verbindungen mit dem neuen Zertifikat geöffnet. Dadurch kann sichergestellt werden das die bestehenden Anwendungen weiter arbeiten können.

Mit HTTP ein neues Zertifikat erstellen

Voraussetzung HTTP Challenge:

Der WEBWARE-Server muss einen HTTP-Server auf Port 80 auf dem WW-Server Rechner erstellen können und dieser HTTP-Server muss aus dem Internet unter der Zertifikatsdomain erreichbar sein.

Wenn Sie im Baum den Ast "mit HTTP neues Zertifikat erstellen" auswählen, so können Sie die Rahmenparameter vorgeben mit welchen das Zertifikat erstellt werden soll.

Folgende Parameter sind teilweise optional (o.) vorzugeben.

Kontakt eMail Let's Encrypt

Geben Sie eine gültige eMail Adresse an welche von Let's Encrypt intern gespeichert wird, und bei Problemen in der Zukunft für Meldungen das Zertifikat betreffend verwendet wird. Die Angabe einer gültigen eMail Adresse ist zwingend.

Haupt-Domain für Zertifiakt

Geben Sie hier die Haupt-Domain an für welche das Zertifikat ausgestellt werden soll. Diese Feld ist zwingend und wird im weiteren bei der Zertifikatsprüfung von Let's Encrypt (Zertifikats-Austeller) verwendet um auf den HTTP-Server (Port 80) der WEBWARE zuzugreifen.

zusätzliche Sub-Domain Liste (optional)

Sie können weitere Sub-Domains angeben welche in dem zu erstellendem Zertifikat enthalten sein sollen. Werden mehrere Sub-Domains angegeben so müssen diese mit einem Komma ohne Leerzeichen voneinander getrennt werden.

Achtung: Die Zertifikats-Prüfung wird ebenfalls für jede Sub-Domain durchgeführt. Dies bedeutet das der WW-Server welcher den HTTP-Server für die Dateiprüfung bereit stellt auch über die angegebenen Sub-Domains aus dem Internet ansprechbar sein muss.

Werden neben der Haupt-Domain, Sub-Domains angegeben so kann das Zertifikat nur erfolgreich erstellt werden wenn alle Prüfungen der Haupt-Domain und Sub-Domains erfolgreich abgeschlossen werden. Ebenso dürfen nicht mehr als 100 Sub-Domains bei der Erstellung mitgegeben werden.

Ländercode

Geben Sie hier einen 2-stelligen Ländercode vor, der für das Zertifikat verwendet wird. Der Ländercode bezeichnet das Land in dem Ihr WW-Server System aufgestellt ist, bzw. ihre Firma angesiedelt ist.

Sie finden unter folgendem link eine Liste von möglichen Codes

https://www.digicert.com/ssl-certificate-country-codes.htm

(Bspl: Deutschland DE, Österreich AT,..)

Firmen Namen Zertifikat (optional)

Geben Sie hier optional einen Namen für Ihre Firma an für die dieses Zertifikat ausgestellt wird. Das Feld muss nicht zwingend ausgefüllt werden.

Firmen eMail Zertifikat

Geben Sie hier eine gültige eMail-Adresse die ins Zertifikat eingetargen werden soll.

HTTP Pfad Home-Verzeichnis

Wenn der HTTP-Server gestartet wird so wird dieses Verzeichnis als HOME-Verzeichnis verwendet. Dieses Verzeichnis muss zwingend angegeben werden. Hier wird das aktuelle HOME-Verzeichnis Ihrer WEBWARE-Instanz vorgeschlagen

HTTP Netzwerkkarte (HTTP = 80)

Geben Sie hier die Netzwerkkarte an, über die der WEBWARE-Server aus dem Internet auf dem Port 80 ansprechbar ist. Hier wird die Netzwerkkarte vorgeschlagen welche für Ihre WEBWARE-Instanz verwendet wird.

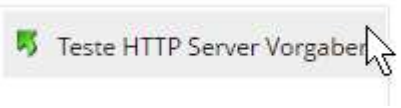
HTTP abweichender Port 80

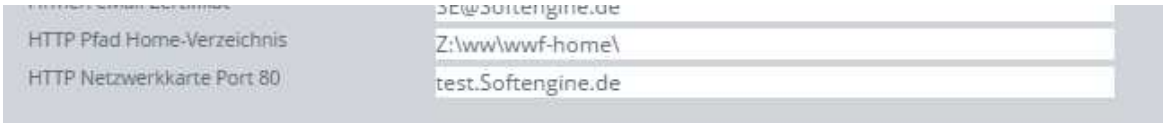
Hier können Sie einen abweichenden internen Port für die HTTP-Challenge angeben. Es ist zu Beachten das der Zugriff für die Prüfung des Zertifikats von Let's Encrypt immer über Port 80 erfolgt. Falls Sie jedoch einen Proxy/Router vorgeschaltet haben mit dem Sie den externen Port 80 auf einen anderen internen Port routen/mappen, können Sie hier den abweichenden internen Port angeben.

Bspl: Extern http://softengine.de (Zugriff erfolgt per HTTP also Port 80). Der Router setzt den externen Port 80 auf den internen HTTP-Port 8080 für den WW-Server um. Geben Sie dann in diesem Feld den Port 8080 (intern) an

Funktion Teste HTTP Server Vorgaben

Damit Sie prüfen können, ob der WEBWARE-Server den integrierten HTTP Server Port 80 starten kann, können Sie mit der Funktion (Teste HTTP Server Vorgaben) einen Test-Server mit einer Laufzeit von einer Minute starten.

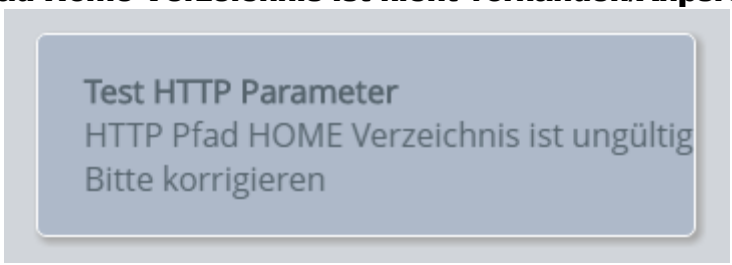




Neben dem HOME-Pfad wird auch der Parameter "HTTP-Netzwerkkarte Port 80" für den Server verwendet.

Sie erhalten dabei folgende Hinweismeldungen

HTTP Pfad Home-Verzeichnis ist nicht vorhanden/Anpsrechbar



HTTP Netzwerkkarte Port 80 nicht öffenbar

Wenn die Netzwerkkarte nicht vorhanden ist, bzw. der Port von einem anderen Programm blockiert ist, so erhalten Sie folgende Fehlermeldung.

OK Netzwerkkarte Port 80 ist öffenbar

HTTP Challenge: Zertifikat Anfordern

Wollen Sie ein neues Zertifikat anfordern so können Sie nach Angabe der Parameter dies mit diesem Befehl auslösen.

Bitte beachten Sie das die Anzahl von Zertifikaten die pro Domain erstellt werden beschränkt ist. Um die Ressourcen von Let's Encrypt zu Schonen sollten Sie für Test's und Prüfung der Eingabeparameter die Funktion "Test-Zertifikat Anfordern" verwenden da hier kein Beschränkung gilt und das Zertifikat nicht global gültig ist.

Nach Auslösen von Zertifikat Anfordern, werden die Zertifikats-Informationen zusammengestellt und eine Konfigurationsdatei erstellt. Ebenso wird für die Dauer der Zertifikatsprüfung der integrierte HTTP Port 80 Server gestartet. Dann wird das Programm bin\wws\wwcers\bin\wwacme.exe gestartet welches die Zertifikatserstellung übernimmt. Sie erhalten mit Hilfe eines Hinweis-Fenster Inforamtionen über den Fortschritt.

Je nach Erfolg oder Misserfolg erhalten Sie dann eine Hinweismeldung.

Konnte ein Zertifikat erstellt werden, so wird dieses in der Zertifikats-Liste im Bereich "Meine Zertifikate" angezeigt und Sie können es von dort aus Aktivieren.

HTTP Challenge: Test-Zertifikat anfordern

Um die Ressourcen von Let's Encrypt zu schonen sollten Sie immer erst versuchen ein Test-Zertifikat zu Erstellen. Dieses hat den Nachteil das es nicht als gültiges Zertifikat eingesetzt werden kann, die Test-Zertifikate aber nicht in der Menge begrenzt sind.

Ansonsten ist der Ablauf gleich zu der normalen Zertifikat Erstellung.

Mit FTP ein neues Zertifikat erstellen

Voraussetzung FTP Challenge:

Der WEBWARE-Server baut während der Dateiprüfung für das Zertifikat eine Verbindung zu Ihrem FTP-Server auf und überträgt in ein Verzeichnis eine Datei welche vom Let's Encrypt Dienst dort abgerufen wird. Daher werden für diesen Vorgang die Zugangsdaten zu dem FTP-Server der Domain benötigt für welche die Domain erstellt wird.

Bei der FTP-Challenge werden Verzeichnisse und Dateien per FTP auf den Server geschrieben welcher per HTTP Port 80 für die Domain Daten ausliefert. Die Verzeichnisse und Dateien werden nach der Prüfung wieder gelöscht.

FTP Challenge:

Folgende Parameter sind teilweise optional (o.) vorzugeben.

Kontakt eMail Let's Encrypt

Geben Sie eine gültige eMail Adresse an welche von Let's Encrypt intern gespeichert wird, und bei Problemen in der Zukunft für Meldungen das Zertifikat betreffend verwendet wird. Die Angabe einer gültigen eMail Adresse ist zwingend.

Haupt-Domain für Zertifiakt

Geben Sie hier die Haupt-Domain an für welche das Zertifikat ausgestellt werden soll. Diese Feld ist zwingend und wird im weiteren bei der Zertifikatsprüfung von Let's Encrypt (Zertifikats-Austeller) verwendet um auf den HTTP-Server (Port 80) der WEBWARE zuzugreifen.

zusätzliche Sub-Domain Liste (optional)

Sie können weitere Sub-Domains angeben welche in dem zu erstellendem Zertifikat enthalten sein sollen. Werden mehrere Sub-Domains angegeben so müssen diese mit einem Komma ohne Leerzeichen von-einander getrennt werden.

Achtung: Die Zertifikats-Prüfung wird ebenfalls für jede Sub-Domain durchgeführt. Dies bedeutet das der WW-Server welcher den HTTP-Server für die Dateiprüfung bereit stellt auch über die angegebenen Sub-Domains aus dem Internet ansprechbar sein muss.

Werden neben der Haupt-Domain, Sub-Domains angegeben so kann das Zertifikat nur erfolgreich erstellt werden wenn alle Prüfungen der Haupt-Domain und Sub-Domains erfolgreich abgeschlossen werden. Ebenso dürfen nicht mehr als 100 Sub-Domains bei der Erstellung mitgegeben werden.

Ländercode

Geben Sie hier einen 2-stelligen Ländercode vor, der für das Zertifikat verwendet wird. Der Ländercode bezeichnet das Land in dem Ihr WW-Server System aufgestellt ist, bzw. ihre Firma angesiedelt ist.

Sie finden unter folgendem link eine Liste von möglichen Codes

https://www.digicert.com/ssl-certificate-country-codes.htm

(Bspl: Deutschland DE, Österreich AT,..)

Firmen Namen Zertifikat (optional)

Geben Sie hier optional einen Namen für Ihre Firma an für die dieses Zertifikat ausgestellt wird. Das Feld muss nicht zwingend ausgefüllt werden.

Firmen eMail Zertifikat

Geben Sie hier eine gültige eMail-Adresse die ins Zertifikat eingetargen werden soll.

FTP Serveradresse

Geben Sie hier die FTP-Serveradresse an, des FTP-Servers welcher die HTTP-Dateien für die Domain-Adresse ausliefert. Die FTP-Adresse muss mit ftp:// beginnen.

FTP Benutzername

Geben Sie hier den Benutzer für den FTP-Server an, mit dem Dateien und Verzeichnisse in das Root-Verzeichnis der Domain geschrieben werden können.

FTP Passwort

Geben Sie hier das Passwort an welches für den Zugang zu dem FTP Server benötigt wird. Das FTP-Passwort wird in eine INI-Datei geschrieben welches nach der Durchführung unkenntlich gemacht wird. Sie haben die Möglichkeit das Passwort (per Default) mit dem System-Wert (Vorgabewerte für Zertifikate > FTP-Passwort speichern) auch in der WEBWARE internen Datenbank verschlüsselt abzulegen so dass es bei erneutem Zugriff automatisch vorgeschlagen wird.

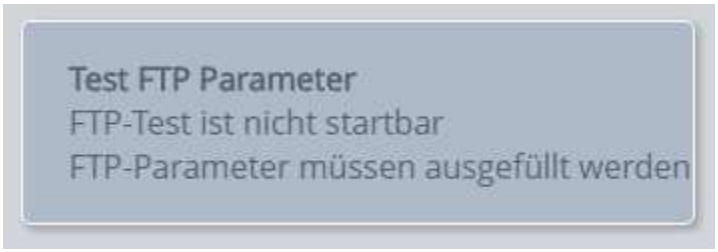
FTP-Port

Hier wird der Standardport 21 vorgegeben.

Funktion Teste FTP Server Vorgaben

Mit dieser Funktion können Sie die Zugangsdaten für einen FTP-Server testen. Dabei wird eine Verbindung zum Test-Server aufgebaut ein Verzeichnis und eine Datei angelegt und gleich wieder gelöscht. Sie benötigen dabei folgende Vorgabewerte:

Sind die FTP-Parameter nicht vollständig ausgefüllt so erhalten Sie eine Fehlermeldung:



Sind die Parameter vorhanden so wird eine Hinweisdialog mit dem Fortschritt angezeigt. Zuerst der Start der Verbindung:

Gibt es beim Zugriff Probleme erhalten Sie folgenden Hinweis:

Nach erfolgreichem Zugriff erhalten Sie einen Hinweis das es funktioniert hat.

FTP Challenge: Zertifikat Anfordern

Wollen Sie ein neues Zertifikat anfordern so können Sie nach Angabe der Parameter dies mit diesem Befehl auslösen.

Bitte beachten Sie das die Anzahl von Zertifikaten die pro Domain erstellt werden beschränkt ist. Um die Ressourcen von Let's Encrypt zu Schonen sollten Sie für Test's und Prüfung der Eingabeparameter die Funktion "Test-Zertifikat Anfordern" verwenden da hier kein Beschränkung gilt und das Zertifikat nicht global gültig ist.

Nach Auslösen von Zertifikat Anfordern, werden die Zertifikats-Informationen zusammengestellt und eine Konfigurationsdatei erstellt. Dann wird das Programm bin\wws\wwcers\bin\wwacme.exe gestartet welches die Zertifikatserstellung übernimmt. Sie erhalten mit Hilfe eines Hinweis-Fenster Informationen über den Fortschritt.

Je nach Erfolg oder Misserfolg erhalten Sie dann eine Hinweismeldung.

Konnte ein Zertifikat erstellt werden, so wird dieses in der Zertifikats-Liste im Bereich "Meine Zertifikate" angezeigt und Sie können es von dort aus Aktivieren.

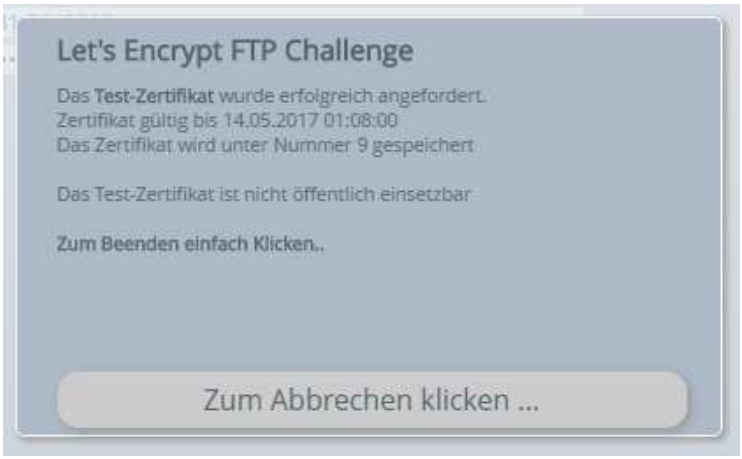
Tritt ein Fehler auf so erhält man nähere Informationen aus der Hinweismeldung.

Weitere Informationen, gerade bei Benutzung von SUB-Domains findet man auch in der INI-Datei im angegebenen Pfad.

FTP Challenge: Test-Zertifikat anfordern

Um die Ressourcen von Let's Encrypt zu schonen sollten Sie immer erst versuchen ein Test-Zertifikat zu Erstellen. Dieses hat den Nachteil das es nicht als gültiges Zertifikat eingesetzt werden kann, die Test-Zertifikate aber nicht in der Menge begrenzt sind.

Ansonsten ist der Ablauf gleich zu der normalen Zertifikat Erstellung.



Verwaltung der Zertifikate

Die Zertifikate werden in folgender Hierachie im Verzeichnis bin\wws\wwcerts abgespeichert.

bin\wws\wwcerts\[4-Stellige WW-Instanz-ID]\[4-Stellige laufende Nummer des Zertifikats]

Ein Verzeichnis bzw. die Konfigurations-Datei sieht dann so aus

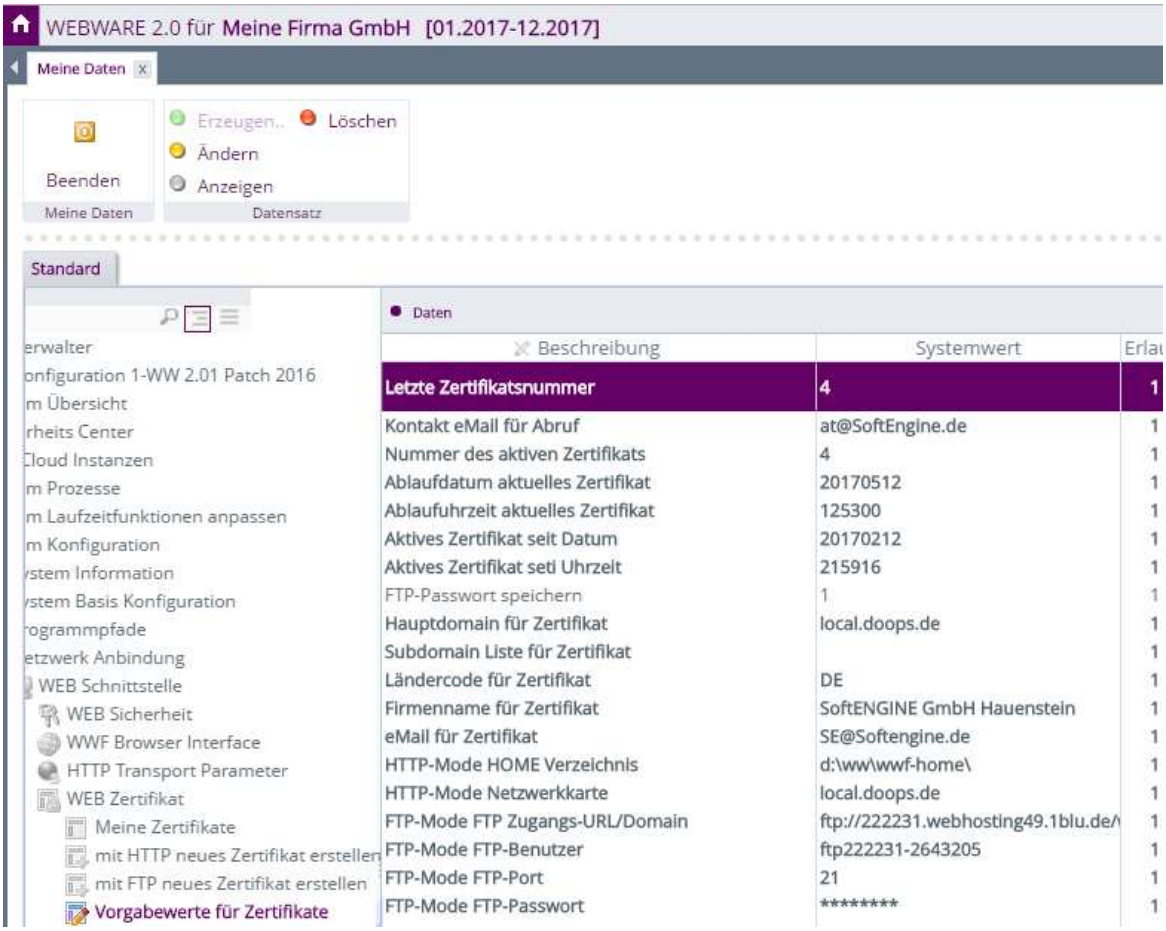
bin\wws\wwcerts\0000\0003\wwacme.ini

Bei einem gültigen Zertifikat finden Sie unterhalb des Zertifikatsordners im Ordner CERTS die 4 WW-Zertifikatsdateien.

Im Ordner CERTS\ORIGINAL finden Sie alle Dateien die von Let's Encrypt erstellt wurden.

Vorgabewerte für Zertifikate

Sie finden hier alle Parameter die für die Zertifikatsverwaltung benötigt werden. Die meisten Parameter werden zur Vereinfachung direkt aus den Eingabemasken der Zertifikatserstellung übernommen und gespeichert.



Hier die einzelnen Parameter in der Übersicht

Letzte Zertifikatsnummer:	Letzte Nummer die für Zertifikate vergeben wurde
Kontakt eMail für Abruf	eMail-Adresse die für Let's Encrpyt verwendet wird
Nummer des aktiven Zertifikats	Nummer des aktiven Zertifikats
Ablaufdatum aktuelles Zertifikat	Wie lange ist das aktuelle Zertifikat gültig
Ablaufuhrzeit aktuelles Zertifikat	Bis zu welcher Uhrzeit ist das Zertifikat gültig
Aktives Zertifikat seit Datum	Wann wurde das Zertifikat als Aktives eingetragen
Aktives Zertifikat seit Uhrzeit	Wann wurde das Zertifikat als Aktives eingetragen
FTP-Passwort speichern	Soll das FTP-Passwort in der WW gespeichert werden ?

...

Die weiteren Parameter sind Sicherungen der Eingabe aus den Zertifikats-Dialogen..

Client-Authentifizierung

Ist die Client-Authentifizierung aktiviert so wird ein zusätzliches CA-Zertifikat der zertifizierenden austellenden Stelle benötigt die die Client-Zertifikate ausgestellt hat. Diese Funktion ist aktuell nicht aktiv.

Der Pfad zu der CA-Datei kann in der WWS.INI mit dem Parameter

BWWSSL_CA_ZERTIFIKAT=[Pfad zu Datei]\Zeritifikat-Datei

angegeben werden.

Aktuelle Sicherheitsvorgaben für SSL

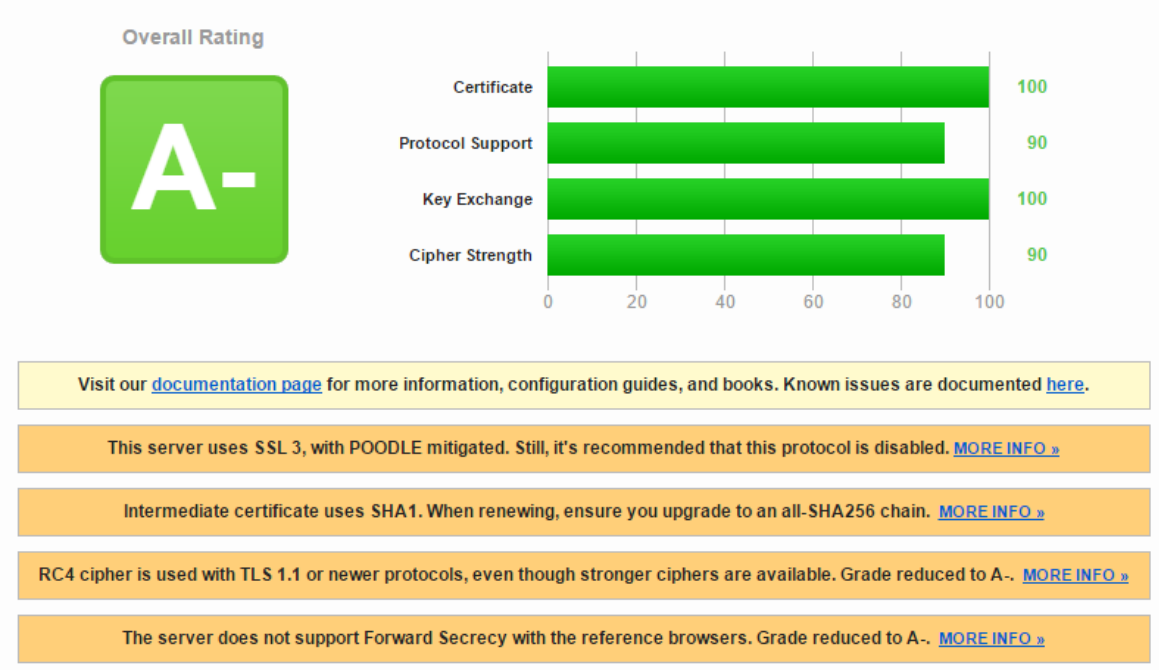
Die Sicherheit eines WEBWARE-Servers, wie auch jeden anderen WEB-Servers muss durch Prüfen und aktualisieren sichergestellt werden.

Wie kann ich meinen WW-Server testen..

Es gibt im Internet eine Test-Seite https://ssllabs.com/ssltest . Dort können Sie Ihren WW-Server überprüfen. Achten Sie darauf den Hacken bei "Do not show .." also "Zeige die Ergebnisse nicht auf der Übersichtsseite" zu setzen. Das Ganze ist nur dann möglich wenn Ihr WW-Server auf dem Standard-Port 443 (HTTPS) läuft.

Beispiel einer Ausgabe:

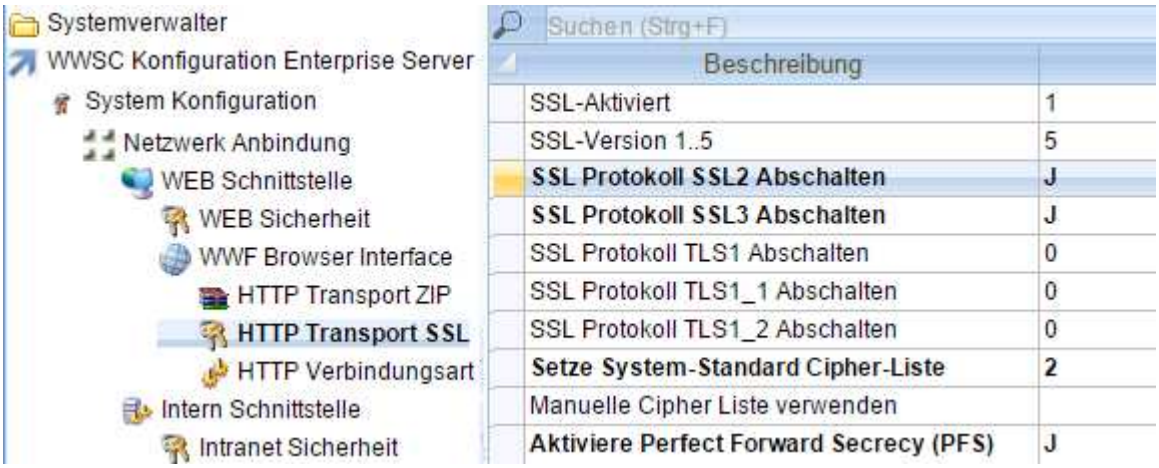
Sicherheitslevel bei einem WW-Server ohne Fix:



Optimale Konfiguration Stand 21 Oktober 2014

Aktuell ist es sinnvoll das SSL-Subsystem SSL2 und SSL3 abzuschalten, da diese nur als Rückfallprotokolle verwendet werden, und aktuell mit der POODLE Attacke ein Sicherheitsrisiko darstellen.

Konfiguration für den WW-Server bitte so vornehmen:



SSL-Aktiviert:	5	Standard-Modus (5)
SSL-Protokoll SSL2		Abschalten
SSL-Protokoll SSL3		Abschalten
System-Standard Cipher		2 = Neue Cipher-Liste ohne RC4
Aktiviere Forward Secrecy		J

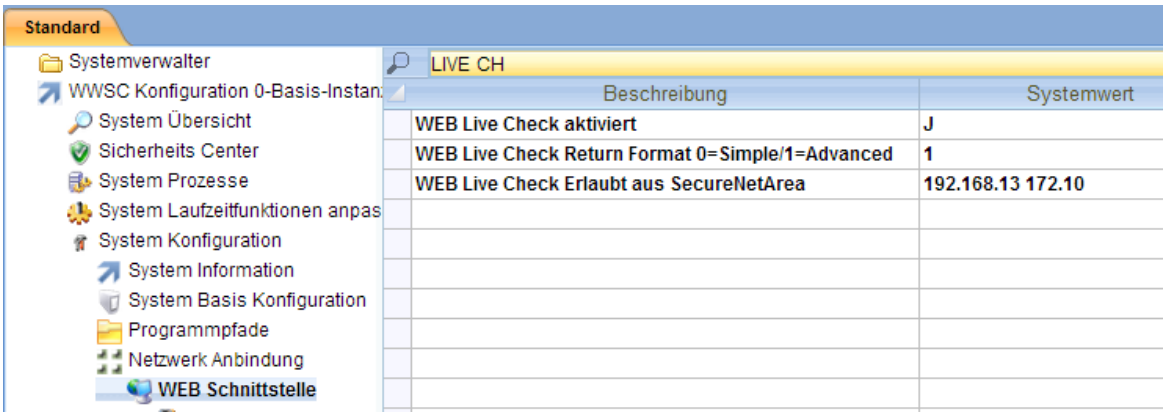
Live-Check Funktion WW-Server über WEB-Schnittstelle

Hiermit haben Sie eine Möglichkeit den WEBWARE-Server von außen auf Funktion zu überprüfen. Hierzu gibt es den Befehl /@LIVECHECK der an die WEBWARE-Server Adresse angehängt werden kann.

Beispiel des Aufrufs:

https://mein-Server-Name.de/@LIVECHECK

Um den Missbrauch der Funktion einzuschränken gibt es hierfür im System-Cockpit mehrere Systemwerte. Ist die Live-Check Funktion nicht aktiviert, so wird mit einer Standardfehlermeldung HTTP 404 reagiert.



Wenn der Live Check aktiviert ist (J), erlaubt es der WEBWARE-Server mit /@LIVECHECK den aktuellen Zustand ihres WEBWARE-Server zu prüfen. Mit Hilfe der Live Check SecureNetArea können Sie den IP-Bereich einschränken von dem aus die Prüfung erfolgen darf. Zusätzlich können Sie noch das Rückgabeformat festlegen.

Hier haben Sie die Auswahl zwischen 0=Simple, also einfaches Format das folgende Information ausgibt:

RUN: OK INSTANCE OK

Wesentlich detaillierte Informationen können sie mit 1=Advanced abrufen. Hier erhalten Sie die komplette Übersicht über Laufzeit, Speicherverbrauch, CPU-Auslastung usw.

WW-SERVER J

Start: **31.10.2013 22:57:01** Dauer: **0 Tage 0:05:51** Build(V 0.9.99/12176 vom 31 Oct 2013)
Prozesse: 28 CPU[0%]/SRVCPU[5%] Speicher[38.121 MB max[39.148 MB]] Frei[6454 MB]/Max[12279 MB]

Schnittstellen
WW WEB IP:192.168.13.130:443 Anfragen[63] Send[5.252 MB] Recv[0.090 MB]
Zusatz-Interface: local.doops.de:8080
WW WWA IP:local.doops.de:8091 Anfragen[14] Send[0.007 MB] Recv[0.079 MB]

RAR-Server
[XL2160C7256CEWW15420131023BINWW1] IP[192.168.13.130:12345] Apps[3/255] CPU[10%] RAM[47% frei 6455 MB von 12279 MB]

Standardprogramme
SYS-Server[CPU(0%) RAM(34.200 MB)] * SYNCHRO[-NEIN-] * MAIL[CPU(0%) RAM(36.030 MB)]
WORKFLOW[-NEIN-] * WW-TAPI[-NEIN-]

Top-Last von 1 Sitzungen
Sitzung[5] Zugriff[0:00:09] XL2160C7256CEWW15420131023BINWW1::WWAPP CPU[0%] RAM[40.910 MB max(40.910 MB)] Benutzer[Systemverwalter/]

!!! Legen Sie dringend ein SecureNetArea fest damit keine internen Informationen von unberechtigten Personen abgerufen werden können. !!!

Konfiguration des Intra- und Internet für Login-System

Um die Anmeldemaske abhängig vom Zugriffsnetz konfigurieren zu können, kann man im System-Cockpit ein SecureNet Bereich für das IntraNet Segment definieren. Die IntraNet Definition wird zum Beispiel auch für die automatisierte Geräte Zugriffsprüfung verwendet.

Intra-Net bedeutet hier der "sichere Netzwerkbereich" von dem von Benutzer zugegriffen wird. Beispiel Internes Firmennetz.

Inter-Net bedeutet alle übrigen Netze die als nicht sicher eingestuft werden. Also alle übrigen Adressbereiche.

Die Definition des IntraNet SecureNet Netzwerks erfolgt unter Intra-Net Anmeldung

Die Anzeige der Sicherheitskritischen Informationen, wie zum Beispiel aktuelle Benutzerliste bzw. auch den Status (angemeldet...) in der Benutzerauswahl des Login-Bildschirm sollte für den InterNet Zugang deaktiviert werden. Hierzu gibt es in beiden Bereichen (IntraNet+InterNet) jeweils Benutzer-Richtlinien und Parameter mit denen der Anmelde-Bildschirm entsprechend angepasst werden kann.

Auch Informationen wie Mandant, Anwendungsauswahl usw. sollten aus dem Internet-Login Bildschirm herausgenommen werden.

Nähere Informationen im Handbuch WW-DOKU-WW-PASSWORT-System.pdf.

Zugangsüberwachung von "Benutzer-Geräten" WW-SHIELD

Ihr WEBWARE-System bietet die Möglichkeit, das Benutzer-Geräte (Desktop-Browser, Tablet-Browser, Phone/Mobile-Browser) nur nach Freigabe durch den Systembetreuer auf das WW-Ssytem zugreifen dürfen.

Dieses System sollte zumindest für den Inter-Net Bereich aktiviert werden. Nach erfolgreichem Login prüft Ihr WEBWARE-Server ob das Benutzer-Gerät bekannt ist und ob ein Zugang erlaubt ist. Ist das Gerät noch nicht registriert, so wird bei Freigabezwang durch den Systembetreuer der Benutzer benachrichtigt und das Benutzer-Gerät in Quarantäne für Neugeräte verschoben.

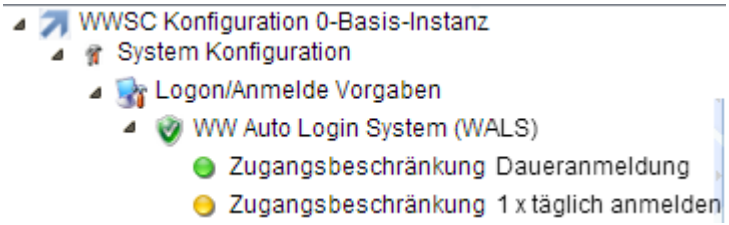
Der Systembetreuer erhält dann eine eMail mit der Aufforderung den Zugangswunsch zu Prüfen und über das WEBWARE-System Cockpit freizugeben.

Die lokalen Netzwerkkarten des WW-Servers sind von der WWSHIELD Überwachung ausgenommen.

Nähere Informationen im Handbuch WW-DOKU-WW-PASSWORT-System.pdf, sowie das handbuch WW-DOKU-WSHIELD-Geräte-zugangs_Kontrolle.pdf.

WALIS WEBWARE Auto Login System

Mit dem WALIS können Sie das automatisierte Anmelde System für Ihr WEBWARE-System aktivieren und verwalten. Dadurch können sich Benutzer ohne Eingabe von Anmeldeinformationen, auf zuvor freigegebenen Benutzer-Geräten, an Ihrem WEBWARE-System anmelden.



!!! Achten Sie bei der Aktivierung darauf, dass Sie die mit Hilfe der SecureNet Bereiche die Netzbereiche für "Daueranmeldung" und "1x Täglich anmelden" setzen.!!!

SecureNetArea unbegrenzter AutoLogin	10.90.31 177.168.167 99.99.99.99

(Daueranmeldung)

SecureNetArea AutoLogin 1x täglich anmelden	99.98,97 192.168.13

(1x Täglich anmelden)

Ebenso sollte Ihr WEBWARE-System so konfiguriert sein das die Auto-Login Funktion je Benutzer/Gerät vom Systembetreuer freigeschaltet werden muss. Sie haben die Möglichkeit die Auto-Login Funktion auf bestimmte Benutzer-Geräte Klassen zu Beschränken (Desktop, Tablet, Phone/Moblie).

Es ist zu überlegen ob der Auto-Login nur während bestimmten Kernzeiten, bzw. Wochentagen aktiviert werden soll.

Nähere Informationen im Handbuch WW-DOKU-WW-PASSWORT-System.pdf.

Konfiguration der Sitzungs-FireWALL

Die Sitzungs-FireWALL dient dazu fehlerhafte Zugriffe von Browsern zu Erkennen. Es kommt zum Beispiel vor das einzelne Browser (Mac Safari) in einen internen Dauerloop verfallen, wobei ständig neue Verbindungen zum WW-Server aufgebaut werden. Mit der Sitzungs-FireWALL können solche Angriffe erkannt werden, und die maximale Anzahl von Sitzungsstarts pro Benutzer begrenzt werden.

Eine Sitzung ist dabei die Auslieferung eines „neuen" Login-Bildschirmes zur Anmeldung. Die Sitzung bleibt normalerweise solange aktiv bis eine WEBWARE-Applikation gestartet und auch wieder Beendet ist.

Hier ist zu Beachten, das Zugriffe mehrerer Benutzer die über einen gemeinsamen Router erfolgen, immer mit der gleichen IP-Adresse erfolgen. So ist es nicht möglich einen einzelnen Rechner zu identifizieren, da jeder Benutzer die gleiche IP-Adresse erhält. In diesem Fall ist es möglich bestimmte Netzwerkbereiche aus der Prüfung herauszunehmen.

Wird von der Sitzungs-FireWALL ein Verstoß gegen die Vorgaben festgestellt, so erhält der Benutzer anstatt einer neuen Sitzung eine Hinweisseite angezeigt die als Parameter hinterlegbar ist, und die im HOME-Verzeichnis der Installation verfügbar sein soll.

Folgende Parameter sind für die Sitzungs-FireWALL konfigurierbar:

Sitzungs FW Benutzer hinter NAT	1
Sitzungs FW max Anzahl Sitzungen je IP/Minute	4
Sitzungs FW Sperrzeit in Sekunden bei Problem	60
Sitzungs FW HTML-Hinweisseite bei Problem	wwintr.htm
Sitzungs FW NAT Erlaubte NAT-Bereiche	192.168.12 192.168.15.99 192.168.14.100

Benutzer hinter NAT (Network Adresse Translation)

Es sind Benutzer vorhanden die über einen gemeinsamen Router angebunden sind. Wenn dieser Parameter gesetzt ist (1) so können mit Hilfe des Parameters „NAT erlaubte NAT Bereiche“ Adressbereiche angegeben werden, die von der Prüfung ausgenommen werden. Der Benutzer hat dann Zugriff ohne Überprüfung.

Max. Anzahl Sitzungen je IP/Minute

Mit dem Parameter kann angegeben werden wie viele Sitzungen maximal je IP-Adresse eröffnet werden dürfen. Bei Überschreiten der maximalen Anzahl von Sitzungsstarts wird die IP-Adresse für eine vorgegebene Zeit gesperrt.

Sperrzeit in Sekunden (bei Problem)

Mit diesem Parameter wird die Sperrzeit angegeben, für die eine IP-Adresse bei erkennen von zu vielen Sitzungsstarts blockiert wird.

HTML-Hinweisseite bei Problem

Wird eine IP-Adresse erkannt die zu viele Sitzungen startet, so wird diese HTML-Seite aus dem WW-Server HOME-Verzeichnis ausgeliefert. Diese Datei kann an Ihre Bedürfnisse angepasst werden.

NAT Erlaubte NAT-Bereiche

Mit diesem Parameter können Adressbereiche angegeben werden, die bei der FireWALL Prüfung ausgeschlossen werden. Hier können direkte Rechner-Adressen sowie auch Teil-Netzwerkadressen angegeben werden. Die Trennung bei Mehrfachangabe erfolgt über Leerzeichen. Hier werden nur IP-Adressen akzeptiert, also keine Angabe von Domain-Namen.

Konfiguration der Verbindungs-FireWALL IPSFW

(IPSFW: Intrusion Prävention System FireWALL)

Eine Sitzung hat meist mehrere Verbindungen gleichzeitig aktiv. Ein Browser verwendet meist mehrere Verbindungen um zum Beispiel beim Laden einer WEBWARE-Sitzung schneller die Programm Ressourcen laden zu können. Die Verbindungs-FireWALL prüft dabei auf Verbindungs-Ebene die Häufigkeit von Verbindungsstarts und greift bei Bedarf ein.

Die Verbindungsüberwachung unterscheitet beim Zugriff die Server-Ebene, also alle Verbindungen die für diese Installation eingehen, sowie die IP-Adress-Ebene, das sind alle Verbindungen einer IP-Adresse.

Bei der Überwachung wird ein Zeitraster von 1 Sekunde, 10 Sekunden und 60 Sekunden verwendet, um die maximal-Werte zu prüfen.

Ebenso können von der internen Überwachung einzelne Verbindungen als Angriff eingestuft werden, was zu einer Zeitweisen Sperrung von einzelnen IP-Adressen führt.

Hier ist zu Beachten, das Zugriffe mehrerer Benutzer die über einen gemeinsamen Router erfolgen, immer mit der gleichen IP-Adresse erfolgen. So ist es nicht möglich einen einzelnen Rechner zu identifizieren, da jeder Benutzer die gleiche IP-Adresse erhält. Dadurch kann die Maximal Anzahl von Verbindungen für eine IP-Adresse früher erreicht werden.

Folgende Parameter stehen bereit:

IPSFW Connect ist aktiv	**1**
IPSFW SRV Max Connects pro Sekunde	80
IPSFW SRV Max Connects pro 10 Sekunde	100
IPSFW SRV Max Connects pro Minute	600
IPSFW IPAdres.Max Connects pro Sekunde	5
IPSFW IPAdres.Max Connects pro 10 Sekunde	20
IPSFW IPAdres.Max Connects pro Minute	100
IPSFW IP-Verbindung Abbrechen bei Überschreiten um	10
IPSFW IP-Verbindung Verzögerung beim Abbrechen	60

IPWSFW Connect ist aktiv

Mit diesem Systemwert kann die Verbindungs-FireWALL für eine Installation aktiviert werden. Wird der Status zur Laufzeit des Servers geändert, so werden beim Abschalten, erkannte Verbindungen noch so abgearbeitet wie sie vorgemerkt werden.

IPWSFW Server Max. Connects pro Sekunde

Vorgabe der maximalen „neuen“ Verbindungen die in der Installation pro Sekunden angenommen werden dürfen. Wird diese maximal Zahl überschritten, so wird der Verbindungswunsch in eine interne Warteschlange aufgenommen und erst bei freien Ressourcen die Verbindung hergestellt.

IPWSFW Server Max. Connects pro 10 Sekunden

Vorgabe der maximalen „neuen“ Verbindungen die in der Installation innerhalb der letzten 10 Sekunden angenommen werden dürfen. Wird diese maximal Zahl überschritten, so wird der Verbindungswunsch in eine interne Warteschlange aufgenommen und erst bei freien Ressourcen die Verbindung hergestellt.

IPWSFW Server Max. Connects pro Minute

Vorgabe der maximalen „neuen“ Verbindungen die in der Installation innerhalb der letzten Minute angenommen werden dürfen. Wird diese maximal Zahl überschritten, so wird der Verbindungswunsch in eine interne Warteschlange aufgenommen und erst bei freien Ressourcen die Verbindung hergestellt.

IPWSFW IP-Adresse Max. Connects pro 1 Sekunde

Vorgabe der maximalen „neuen“ Verbindungen die von einer IP-Adresse innerhalb der einer Sekunde angenommen werden dürfen. Wird diese maximal Zahl überschritten, so wird der Verbindungswunsch in eine interne Warteschlange aufgenommen und erst bei freien Ressourcen die Verbindung hergestellt.

IPWSFW IP-Adresse Max. Connects pro 10 Sekunden

Vorgabe der maximalen „neuen“ Verbindungen die von einer IP-Adresse innerhalb der letzten 10 Sekunden angenommen werden dürfen. Wird diese maximal Zahl überschritten, so wird der Verbindungswunsch in eine interne Warteschlange aufgenommen und erst bei freien Ressourcen die Verbindung hergestellt.

IPWSFW IP-Adresse Max. Connects pro Minute

Vorgabe der maximalen „neuen“ Verbindungen die von einer IP-Adresse innerhalb der letzten Minute angenommen werden dürfen. Wird diese maximal Zahl überschritten, so wird der Verbindungswunsch in eine interne Warteschlange aufgenommen und erst bei freien Ressourcen die Verbindung hergestellt.

IPWSFW IP-Verbindung Abbrechen bei Überschreiten um ..

Wird erkannt das ein Verbindungswunsch von einer IP-Adresse die maximal erlaubte Vorgabe überschreitet erfolgt im Normalfall das eintragen der Verbindung in die interne Warteschlange. Um nun Angriffe von externen Rechnern abzuwehren, kann man mit diesem Parameter vorgeben das die Verbindung nicht in die Warteschlange sondern zum Abbrechen vorgemerkt wird.

Beispiel: Es sind pro Sekunde 5 Verbindungsstarts erlaubt, es werden aber 22 Verbindungsstarts erkannt. Wird dieser Parameter auf 10 gesetzt, so wird ab dem erkennen des 15. Verbindungsaufbau innerhalb einer Sekunde der Zugriff von der IP-Adresse für einen vorgegebenen Zeitraum gesperrt. Verbindungsaufbauten die danach eintreffen werden mit für einen vorgegebenen Zeitraum verzögert und danach abgebrochen.

Der Parameter gilt für die 3 Parameter (IP-Adresse Max. Connects pro (1 Sekunde, 10 Sekunde und Minute).

IPSFW IP-Verbindung Verzögerung beim Abbrechen

Mit diesem Parameter kann vorgegeben werden, dass eine zum Abbrechen vorgemerkte Verbindung erst später geschlossen wird. Dies verhindert dass der Angreifer sofort nach dem Abbrechen eine erneute Verbindung aufbaut, da er auf eine Antwort des WW-Servers warten muss.

Konfiguration der Protokoll-FireWALL PROTFW

(PROTFW: Protokoll FireWALL)

Es ist möglich durch ausnutzen von Protkollfehlern ein mit SSL verschlüsseltes System so unter Last zu bringen das zwar wenige Verbindungen aufgebaut werden, jedoch eine hohe Last erzeugt wird. Dieses Protokollfehler werden mit dieser FireWALL überwacht. Tritt dabei ein Überschreiten der Maximalgrenzen auf (1 Sekunde, 10 Sekunden oder 1 Minute), so werden die Zugriffe der auslösenden IP-Adresse für die vorgegebene Zeit gebannt und abgewiesen.

Ein solches Tool ist http://seclists.org/fulldisclosure/2011/Oct/779

Mit diesem Tool können von einem einzelnen PC sehr viele Verbindungen gestartet werden die durch Protokollfehler einen anfälligen WEB-Server lahm legen können. Der WW-Server ist ab dieser Release von

diesem Protokoll-Fehler nicht mehr beeinflussbar. Mit der Protokoll FireWALL hat man einen zusätzlich Schutz, und kann auf unbekannte Protokollangriffe reagieren.

Folgende Parameter stehen bereit:

PROTFW IPAdres.Max Fehler Protokoll ist aktiv	1
PROTFW IPAdres.Bann ab Max Protokoll Fehler pro Sekunde	5
PROTFW IPAdres.Bann ab Max Protokoll Fehler pro 10 Sekunde	10
PROTFW IPAdres.Bann ab Max Protokoll Fehler pro Minute	20
PROTFW Wie lange wird die IP-Adresse gebannt (Sekunden)	60

PROTFW IP Adres.Max Fehler Protokoll ist aktiv

Mit diesem Parameter kann die Protokoll FireWALL aktiviert werden. Hierbei werden pro IP-Adresse die Protokoll Fehler für die

- Letzte Sekunde
- Letzten 10 Sekunden
- Letzte Minute

aufsummiert. Wird einer der folgenden 3 Max-Werte überschritten, so wird die IP-Adresse für die Vorgabezeit blockiert.

PROTFW IP Adres.Bann ab Max Protokoll Fehler pro Sekunde

Vorgabe der Anzahl Protokoll Fehler die maximal pro Sekunde auftreten dürfen. Wird dieser Wert überschritten so wird die IP-Adresse für die vorgegebene Zeit geblockt.

PROTFW IP Adres.Bann ab Max Protokoll Fehler pro 10 Sekunden

Vorgabe der Anzahl Protokoll Fehler die maximal pro Sekunde auftreten dürfen. Wird dieser Wert überschritten so wird die IP-Adresse für die vorgegebene Zeit geblockt.

PROTFW IP Adres.Bann ab Max Protokoll Fehler pro Minute

Vorgabe der Anzahl Protokoll Fehler die maximal pro Minute auftreten dürfen. Wird dieser Wert überschritten so wird die IP-Adresse für die vorgegebene Zeit geblockt.

PROTFW Wie lange wird die IP-Adresse gebannt (Sekunden)

Wird ein Protokoll Fehler erkannt, und eine der maximal-Vorgaben an Protokoll Fehlern überschritten so wird die IP-Adresse um diesen Wert in Sekunden verzögert.

WW-Systemcockpit Zugriffsschutz

Der Zugriff auf das WW-Systemcockpit ist nur von bestimmten Rechnerressourcen aus möglich. Dadurch kann verhindert werden, das ein Angreifer der im Besitz der Zugangsdaten ist von einem beliebigen Rechner auf das Cockpit zugreifen kann.

Es gibt 3 Parameter mit denen der Zugriff auf das WW-System-Cockpit verändert werden kann.

System Cockpit von Lokaler IP-Adresse erlaubt	1
System Cockpit von dieser IP-Adresse erlaubt	
System Cockpit Zugangspasswort bei Leer	

System Cockpit von Lokaler IP-Adresse erlaubt

Mit diesem Parameter kann festgelegt werden, das der Zugriff von der lokalen IP-Adresse des WW-Server aus erlaubt ist. Dieser Wert ist der Standardwert, also der Zugriff auf das WW-System-Cockpit ist nur vom WW-Server aus direkt möglich. Versucht sich jemand an das WW-System-Cockpit von einer anderen IP-Adresse aus anzumelden, so wird dies abgelehnt.

System Cockpit von dieser IP-Adresse erlaubt

Wird hier eine IP-Adresse angegeben, so ist es möglich sich von dieser IP-Adresse aus anzumelden. Hier kann ein Administrator die IP-Adresse seines lokalen Arbeitsrechners eintragen um das WW-System Cockpit von seinem Rechner aus zu Bedienen. Wird der vorherige Parameter (nur von lokaler IP..) abgeschaltet, so ist nur noch der Zugriff von dieser IP-Adresse möglich.

System Cockpit Zugangspasswort bei Leer

Bei der Installation des WW-Servers muss ein Passwort für den System-Cockpit Zugang vorgegeben werden. Dieses Passwort ist nur für die erstmalige Anmeldung jedes WW-Administrator gültig. Der Administrator wird danach aufgefordert ein gültiges Passwort vorzugeben, welches dann als Zugangspasswort gesetzt wird.

Es gibt folgende vordefinierten Administratoren der WEBWARE, diese unterscheiden sich auch im Zugriffsbereich (admin: Administration; config: Konfiguration)

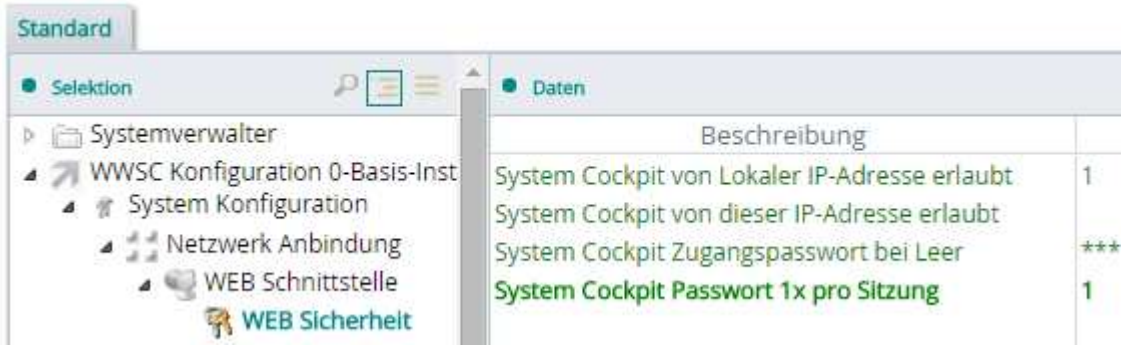
- firmen.admin@sc.ww.de (Ebene Firma, nur bei Cooperation und Cloud-Server)
- global.admin@sc.ww.de (Ebene Installation)
- server.admin@sc.ww.de (Ebene Server)
- firmen.config@sc.ww.de (Ebene Firma, nur bei Cooperation und Cloud-Server)
- global.config@sc.ww.de (Ebene Installation)
- server.config@sc.ww.de (Ebene Server)

System-Cockpit Zugriff mit einmaligen Passwort einrichten

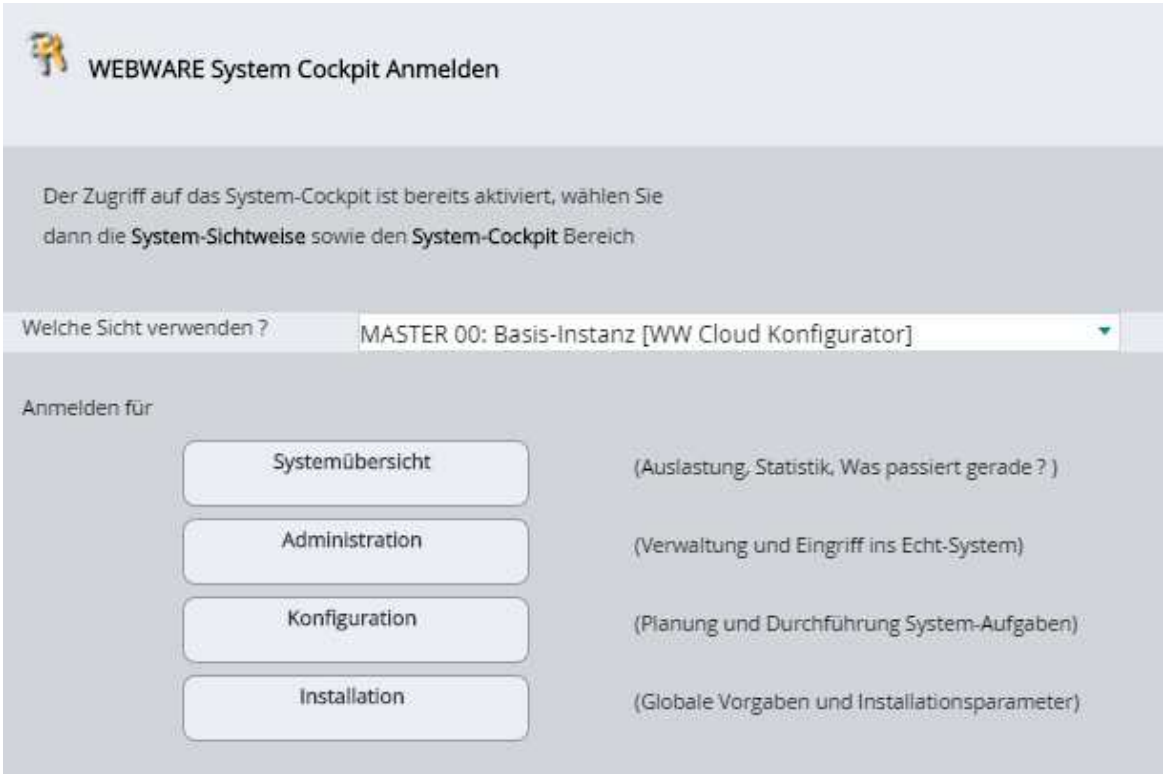
REV: WWS(erver) 12512

Bisher musste man sich bei jedem Zugriff auf das System-Cockpit, bzw. Änderung der Sichtweise auf das System-Cockpit neu anmelden. Dies kann jetzt mit Hilfe eines Systemwertes so geändert werden, das die Anmeldung nur noch einmal pro Sitzung erforderlich ist. Standardmäßig ist dieser System-Wert abgeschaltet.

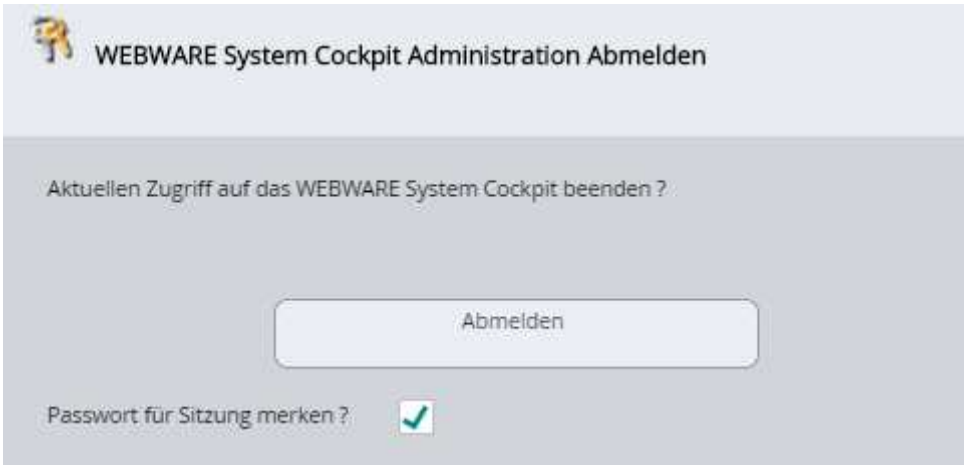
Sie können mit dem System-Wert "System Cockpit Passwort 1x pro Sitzung" die Eingabe des Passwortes auf einmal pro Sitzung begrenzen.



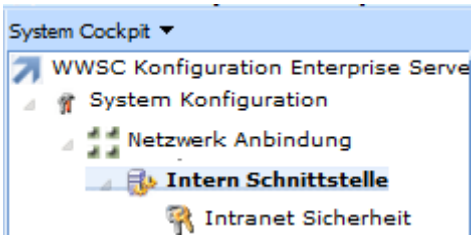
Nach Aktivierung des System-Wertes sowie erfolgreicher erster Anmeldung wird dann der Anmeldebildschirm ohne Passwort-Eingabe angezeigt.



Beim Abmelde-Bildschirm des System-Cockpit's steht dann auch die Option zur Verfügung um das Passwort für die Sitzung zu merken, bzw. durch entfernen des Hakens, die Passworteingeabe für die nächste Anmeldung zu Erzwingen



Intern Schnittstelle (Intra-Net)



Die Netzwerkschnittstelle Richtung sicheres Netz (Intranet) wird im Bereich Intern-Schnittstelle konfiguriert. Weitere Sicherheitsfunktionen findet man im Ast darunter Intranet Sicherheit.

Vorgabe der Schnittstelle für den Intranet-Zugang einer Installation

Mit dem folgenden 2 Parametern kann ein Zugangspunkt beim WW-Server definiert werden, über den sich angebundene RAR-Server, sowie WW-Anwendungen (wwa.exe, wwsyssrv.exe, wtapisrv.exe usw.) anmelden.

WWA-INTRA-IP-Adresse (INTERN)	local.doops.de
WWA-INTRA-IP-Port (INTERN)	8091

Um eine saubere Trennung von Internet und Intranet zu erreichen sollte hier unbedingt eine eigene Netzwerkkarte verwendet werden.

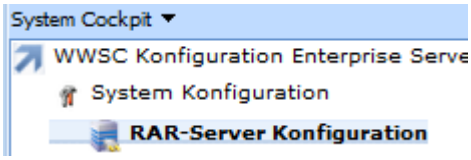
Beschränkung der Adressbereiche/IP-Adressen Intranet

Mit dem folgenden Parameter ist es möglich den Zugang zur Intern-Schnittstelle des WW-Server einzuschränken. Dieser Parameter sollte ausgefüllt werden, da der Zugriff auf diese Schnittstelle nur von einer überschaubaren Anzahl von Rechnern erfolgt.

WWA-INTRA-SecureNet-Zugriffschutz	

Gerade bei WEBWARE Installation bei denen alle Komponenten auf einem Rechner laufen, muss hier der Zugriff auf die interne Kommunikation geschützt werden. Denn hier wäre es möglich den Zugangspunkt auch von der externen Netzseite aus zu verwenden (gleiche IP-Vorgabe bei Intern und Extern Schnittstelle).

Erlaubnis der Anmeldung von unbekannten RAR-Servern



Nachdem eine Installation abgeschlossen ist, sollte dieser Wert zurückgesetzt werden, damit die Anmeldung von RAR-Servern nur von solchen akzeptiert wird, welche sich bereits registriert haben.

Anmeldung von unbekannten WWR/RAR Servern erlauben	1

Wiederherstellung / Umzug / Recovery Funktion

Einleitung

Um die Sicherheitsrelevanten Daten des WEBWARE-Servers, wie zum Beispiel Benutzerpasswörter, Konfigurationsparameter usw. vor Ausspähung und unerlaubter Veränderung zu schützen, sind diese Informationen verschlüsselt. Dadurch ist eine Wiederherstellung bzw. Neuinstallation der WEBWARE auf einem neuen System (Hardware) nur mit Hilfe eines zuvor festgelegten Recovery/Wiederherstellung-Passwortes möglich.

Um diese Funktion der WEBWARE nutzen zu können, müssen Sie wie im folgenden beschrieben vorgehen.

Einrichtung eines Recovery/Wiederherstellung-Passwortes

Hierzu gibt es im System-Cockpit eine Eingabeseite. Melden Sie sich im System-Cockpit mit Ihrem Passwort im Bereich Installation an. Wichtig ist hier, das Sie im Bereich "Welche Sicht verwenden ?", die Server-Ebene (Hier im Beispiel Cloud-Server Cluster, abhängig von der WW-Server Installationsart..) auswählen, da das Recovery-Passwort für den gesamten WW-Server (Server-Ebene) festgelegt wird.

Wählen Sie dann im Bereich des Baumes links, wie unten abgebildet den Bereich WW SQLITE-Passwort aus.

(Dieser Ast im Baum ist nur Sichtbar wenn Sie sich, wie oben beschrieben, im Bereich Installation und auf Server-Ebene anmelden.)

Geben Sie hier nun ein Recovery(Wiederherstellungs)-Passwort vor. Das Passwort muss mindestens 10 Zeichen lang sein, und es werden Groß/Kleinschreibung unterschieden. Es gibt keine Möglichkeit das Passwort anzusehen, daher sollten Sie dieses mit Bedacht wählen und bei der Eingabe darauf achten es korrekt einzugeben.

Hinweis: Im Eingabefeld werden beim Aufruf im Passwortfeld, Sternchen angezeigt, deren Anzahl nichts mit dem aktuell gewählten Passwort zu tun hat.

Ist das Recovery-Passwort nicht speicherbar, so erhalten Sie eine entsprechende Fehlermeldung

Konnte das Recovery-Passwort erfolgreich gespeichert werden, so erhalten Sie folgende Meldung:

Umzug ohne Recovery

Wird ein WEBWARE Server auf neue Hardware umgezogen und es wurde zuvor ein Recovery-Passwort gesetzt, so wird die SQLITE-Datenbank des WW-Servers im Read-Only-Modus betrieben bis die Recovery-Funktion ausgeführt wurde. Dies schützt die SQLITE-Datenbank vor dem Schreiben von Datensätzen mit falschem Schlüssel. Beim Start des WW-Servers wird dabei eine Fehlermeldung in der Console und in den Log-Dateien ausgegeben die auf die Ausführung der Recovery-Funktion aufmerksam macht.

Nach Erfolgter Recovery-Funktion (siehe nächster Absatz), ist dann das Arbeiten normal möglich.

Durchführung einer Wiederherstellung/Recovery

!!! Wichtig: Eine Wiederherstellung/Recovery ist nur mit zuvor gesetztem Recovery-Passwort möglich, dessen Eingabe ist nur in einem laufenden System möglich !!!

Um ein System erfolgreich wiederherstellen zu können gehen Sie bitte in der angegebenen Reihenfolge vor, und Starten Sie das System nur in der Reihenfolge wie unten beschrieben, um die WW-Server-Datenbank nicht zu zerstören.

1. Rückspeichern der Datensicherung

Entpacken / Speichern Sie ihre Datensicherung des WW-Servers in das neue System. Der Datenpfad/Festplattenpfad kann dabei vom dem der alten Installation abweichen.

Beispiel: Alter Pfad: f:\webware-erp\bin\

Neuer Pfad: c:\ww-erp\bin

Beachten Sie jedoch das die Pfade zu den hinterlegten Zertifikaten, falls diese außerhalb des bin-Pfades liegen entsprechend angepasst bzw. in den gespeicherten Pfaden auch im neuen System bereit gestellt werden müssen.

2. Vor dem ersten Start des WW-Servers

Passen Sie nun die WWS.INI Datei im WWS-Pfad (Bspl: C:\ww-erp\bin\wws\wws.ini) mit einem Editor an. Dort müssen die Pfade und die Netzwerkkarte an Ihre neue Hardware angepasst werden.

Beispiel einer WWS.INI Datei vor der Änderung:

```
[WWS]
#-INIOK-#ROOTPATH=" f:\webware-erp\bin\home\"
#-INIOK-#INDEXHTML="ww0403\index.bweb"
PGMDATAWWFS=" f:\webware-erp\bin\WWS\WWFSDB"
#-INIOK-#BWEBIPWORLD=wwerp.Softengine.de
#-INIOK-#BWEBPORT=443
#-INIOK-#WWAIPLOCAL= wwerp.Softengine.de
#-INIOK-#WWAPORT=8091
```

Anpassung der WWS.INI. Entfernen Sie zuerst die #-INIOK-# Einträge damit bei einem Neustart die Änderungen aus der WWS.INI auch eingelesen werden.

Passen Sie danach die Pfade in der WWS.INI an die neuen Pfade an (Bspl: f:\webware-erp\bin wird in c:\ww-erp\bin geändert)

Fügen Sie in der WWS.INI, falls nicht vorhanden, noch die Zielverzeichnisse für Programmpfad, die Performance-Ausgabe, sowie die Security-Meldungen ein (**PGMPATH=.., PERFORM=.., SECURITY=..**) damit diese auch korrekt gesetzt werden.

Beispiel der angepassten WWS.INI Datei nach der Änderung:

[WWS]
ROOTPATH=" C:\ww-erp\bin\home "
INDEXHTML="ww2252\index2.bweb "
PGMDATAWWFS=" C:\ww-erp\bin\wws\wwfsdb"
BWEBIPWORLD=wwerp.Softengine.de
BWEBPORT=443
WWAIPLOCAL=local.doops.de
WWAPORT=8091
PGMPATH= C:\ww-erp\bin\wws
PERFORM= C:\ww-erp\bin\wws \performance
SECURITY= C:\ww-erp\bin\wws\security
BWWSSL_CA_ZERTIFIKAT=demozertifikat\startssl.ca.crt
BWWSSL_ZERTIFIKAT=demozertifikat\softengine.meine-webware.de.crt
BWWSSL_PASSWORD4PRIVKEY=meinewebware
BWWSSL_PRIVATEKEY=demozertifikat\private-key.key
BWWSSL_USE_CHAIN_ZERTIFIKAT=J
BWWSSL_CHAIN_ZERTIFIKAT=demozertifikat\startssl.chain.class1.server.crt

Speichern Sie die Änderungen ab.

Anpassen der Netzwerk-Konfiguration:

Falls Ihr WW-System mit mehreren Netzwerkarten / Portalen bzw. WW-Instanzen konfiguriert ist, sollten Sie das setzen der Netzwerk-Parameter mit dem Befehl SETINSVAL_* in der WWS.INI duchführen.

Sie können damit die Netzwerkadressen sowie Netzwerk-Port für die einzelnen WW-Instanzen, bzw. die Basis-Instanz _00_ setzen.

* Lokale Netzwerk-Karte WEB-Anbindung

* Lokale Zusatz-Netzwerk-Karte WEB-Anbindung

* Lokale Karte RAR-Anbindung

* Entfernte Beschreibung für Lokale Netzwerk-Karte WEB-Anbindung

* Entfernte Beschreibung für die Lokale Zusatz-Netzwerk-Karte WEB-Anbindung

Hierzu fügen Sie entsprechende Befehle in die WWS-INI ein.

SETINSVAL_$$_*=Netzwerkkarte@Netzwerkport

$$ = (jeweils 2 Stellige Zahl) WW-Instanz-Nummer. Die Standard-Basis-Instanz ist die 00

* = Angabe der Netzwerk-Schnittstelle siehe folgende Angaben

WWF_MAIN_NETWORK_CARD_PORT	WEB-Schnitstelle
WWF_EXTRA_ MAIN_NETWORK_CARD_PORT	WEB-Zusatz-Schnittstelle
WWF_REMOTE_MAIN_NETWORK_CARD_PORT	WEB Externe Beschreibung

WWF_REMOTE_EXTRA_ MAIN_NETWORK_CARD_PORT WEB Externe Zusatz Beschreibung

RAR_NETWORK_CARD_PORT RAR interne Anbindung Schnittstelle

Die Angabe von den EXTRA-Schnittstellen sind optional da diese abhängig von Ihrer Konfiguration sind.

Die Parameter werden im Format

Netzwerkkarte@Netzwerkport angegeben. Beispiel meine-webware.de@443

Beispiel für die Angabe in der WWS.INI

SETINSVAL_00_WWF_MAIN_NETWORK_CARD_PORT=meine-webware.de@443
SETINSVAL_00_RAR_NETWORK_CARD_PORT=meine-webware.de@8091

Beispiel WW-Instanz 1 (Angabe mit _01_)..

SETINSVAL_01_WWF_MAIN_NETWORK_CARD_PORT=127.0.0.1@4443
SETINSVAL_01_RAR_NETWORK_CARD_PORT=127.0.0.1@18091

Beispiel Angabe externe abweichende Adresse über WWS.INI

SETINSVAL_00_WWF_MAIN_NETWORK_CARD_PORT=192.168.0.1@443
SETINSVAL_00_RAR_NETWORK_CARD_PORT=192.168.0.2 @8091
SETINSVAL_00_WWF_REMOTE_MAIN_NETWORK_CARD_PORT=meine-webware.de@443

Beispiel WW-Instanz 0 hat 2 WEB-Schnittstellen+Beschreibung

SETINSVAL_00_WWF_MAIN_NETWORK_CARD_PORT=192.168.0.1@443
SETINSVAL_00_WWF_EXTRA_NETWORK_CARD_PORT=192.168.0.1@4443
SETINSVAL_00_WWF_REMOTE_MAIN_NETWORK_CARD_PORT=meine-webware.de@443
SETINSVAL_00_WWF_REMOTE_EXTRA_NETWORK_CARD_PORT=IntraNet.Firma.de@4443
SETINSVAL_00_RAR_NETWORK_CARD_PORT=192.168.0.2@8091

Speichern Sie die WWS.INI bei Änderungen ab. Nach dem ersten Start der WEBWARE werden diese Einträge in der WWS.INI automatisch auskommentiert.

Anpassen von SecureNet Vorgaben an das neue System

Falls Sie im System-Cockpit SecureNET Vorgaben, also Zugriffsbeschränkungen für die Netzwerkkarten hinterlegt haben, so können Sie die ebenfalls über die WWS.ini mit Angabe des Befehls

SETINSNETSECAREA_$$_*=Angabe von Netzwerk-Beschränkungen

in der Datenbank setzen.

$$ = (jeweils 2 Stellige Zahl) WW-Instanz-Nummer. Die Standard-Basis-Instanz ist die 00

* = Angabe der Netzwerk-Schnittstelle siehe folgende Angaben

WWF_MAIN_NETWORK	WEB-Schnittstelle
WWF_EXTRA_NETWORK	WEB-Zusatz-Schnittstelle
RAR_NETWORK	RAR Interne Anbindung Schnittstelle

Für die Vorgabe der Netzwerk-Beschränkungen können Sie wie oben in der Sicherheits-Center Beschreibung Netzwerksegmente vorgeben.

Beispiele:

Setzen alle Karten auf 192.168.. (WW-Instanz 0)

SETINSNETSECAREA_00_WWF_MAIN_NETWORK=192.168.0
SETINSNETSECAREA_00_WWF_EXTRA_NETWORK=192.168.2
SETINSNETSECAREA_00_RAR_NETWORK=192.168.0.90

Auf die Main-Web-Schnittstelle dürfen nur Browser aus dem Netzwerk 192.168.0 zugreifen.
Auf die Zusatz-Karte für die WEB-Schnittstelle nur Browser aus dem Netzwerk 192.168.2 zugreifen.
Auf die interne RAR-Schnitstelle dürfen nur vom Rechner 192.168.0.90 Verbindungen aufgebaut werden.

WW-Instanz 2 Zugriff
SETINSNETSECAREA_02_WWF_MAIN_NETWORK=192.168.18
SETINSNETSECAREA_02_WWF_EXTRA_NETWORK=
SETINSNETSECAREA_02_RAR_NETWORK=192.168.19.100 192.168.19.110
Die Haupt-Karte ist auf das Rechner aus dem Netz 192.168.18 beschränkt
Die Extra-Karte darf alle Verbindungen annehmen
Die Interne RAR-Schnittstelle ist nur für die beiden Rechner 192.168.19.100 und 192.168.19.110 frei.

3. Recovery Funktion des WW-Servers starten

Der WW-Server hat für diesen Fall einen Aufrufparameter der die Übergabe des Recovery-Passwortes erwartet. Gehen Sie hierzu wie folgt vor. Im folgenden nehme ich an das der WW-Server im Pfad C:\ww-erp\bin\wws installiert ist, und dass das Recovery-Passwort WWRECOVERYPASSWORT lautet

Wechseln Sie mit einer Eingabeaufforderung in den Pfad in dem der WW-Server zurückgespeichert wurde. (Bspl: c:\ww-erp\bin\wws)

Starten Sie den WW-Server mit folgendem Aufruf

WWS RECOVERY WWRECOVERYPASSWORT

Erklärung:

WWS	startet das Programm WWS.EXE
RECOVERY	Ausführung der RECOVERY-Funktion
WWRECOVERYPASSWORT	Ihr zuvor festgelegtes RECOVERY-Passwort

Nach Eingabe des Befehls wird der WW-Server gestartet und die interne Datenbank für die neue Hardware konfiguriert. Der Aufruf der Funktion ist mit einem Zeit-Schutz versehen. Nach Ausführen der Funktion ist ein erneuter Aufruf der RECOVERY-Funktion nur nach Ablauf einer Dauer > 1 Minute wieder möglich. Wird ein falsches Passwort übergeben, so verzögert der WW-Server die Bearbeitung und führt kein Recovery durch.

4. Erster Start des WW-Servers

Der erste Start des WW-Servers wird dann wie ein normaler Start durchgeführt. Dabei wird der WW-Server mit dem Befehl

WWS CONSOLE

gestartet. Dort sollten dann keine Fehlermeldungen erscheinen und der WW-Server den Zugriff auf die Benutzer und Anmeldung erlauben.

Falls Sie in der alten Installation absolute Pfade für Zertifikate oder ähnliches angegeben haben, prüfen Sie diese im System-Cockpit und passen Sie diese bei Bedarf an

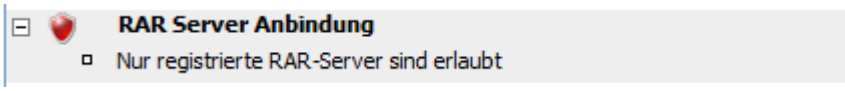
Sicherheits-Center im System-Cockpit

Im WEBWARE System-Cockpit kann man mit dem Sicherheits-Center einen Überblick über den aktuellen Sicherheitszustand der WEBWARE erhalten.

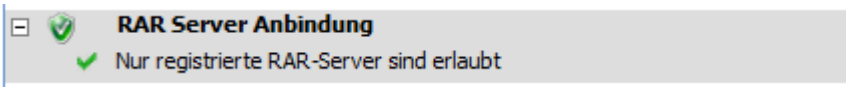
Im Sicherheits-Center werden alle Teilbereiche der WEBWARE bewertet und mit einem Ampel-Symbol über Ihren Sicherheitszustand gekennzeichnet.

Direkte Bearbeitung von Sicherheitsregeln/Systemwerten

Wird der Sicherheits-Center im Administrator bzw. Konfigurationsmodus gestartet kann direkt durch Klick auf einen der Unterpunkte der entsprechende Systemwert geändert werden.



Im obigen Ausschnitt ist zum Beispiel der Bereich RAR-Server Anbindung zu sehen. Dort gibt es nur eine Sicherheitsregel. Ist diese nicht sicher gesetzt, so wird vor der Sicherheitsregel ein pulsierendes Viereck gezeigt. Wird diese nun auf sicher geändert, so ändert sich dadurch die Anzeige in folgender Art:

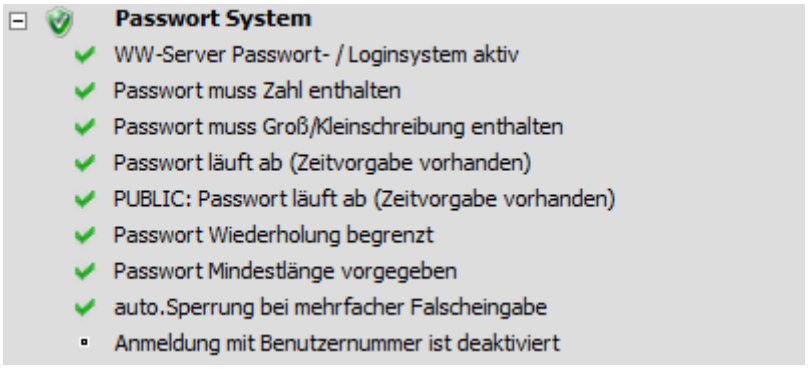


Sicherheits-Center – Die WEBWARE-Teilsysteme

Im Folgenden werden die Teilsysteme der WEBWARE im Sicherheits-Center vorgestellt, und die Sicherheitsregeln gezeigt.

Sicherheits-Center Passwort System

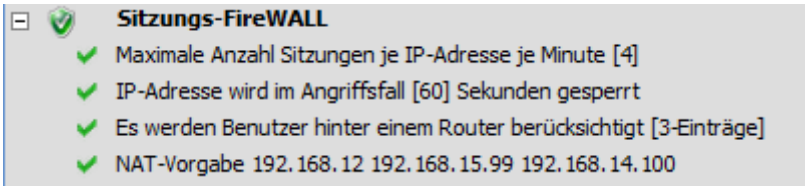
Hier kann man alle Sicherheitsrelevanten Regeln/Systemwerte einsehen und per Klick direkt ändern.



So sieht die Standardinstallation einer WEBWARE aus. Der letzte Eintrag ist nicht als Sicher gekennzeichnet da hier erlaubt ist, sich mit einer Kurzzahl (Benutzernummer) anzumelden.

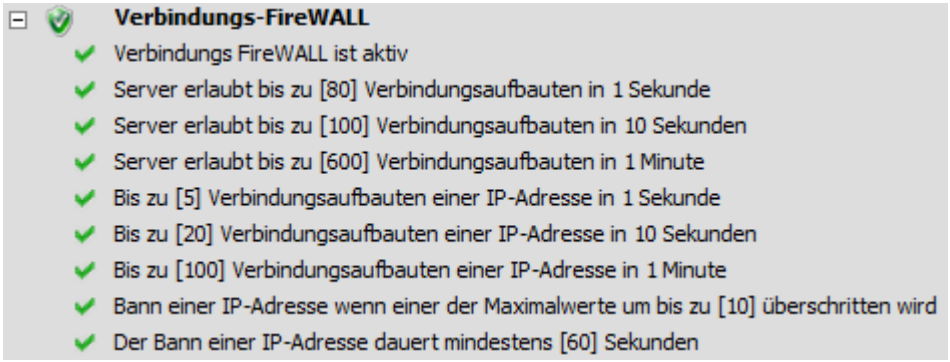
Sicherheits-Center Sitzungs-FireWALL

Die Sitzungs-FireWALL greift auf Ebene der WEBWARE-Sitzungen, also einzelnen Benutzer-Browser-Sitzungen. Hier wird überwacht ob von einzelnen IP-Adressen in einem vorgegebenen Zeitraum zu viele neue Sitzungen aufgebaut werden. Im Fehlerfall werden solche IP-Adressen für einen vorgegebenen Zeitraum blockiert.



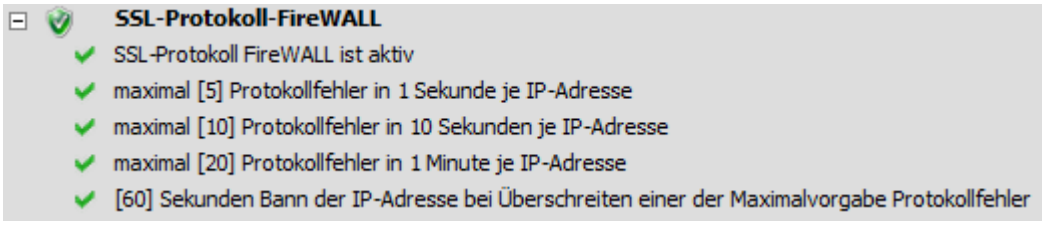
Sicherheits-Center Verbindungs-FireWALL

Jede Sitzung besteht aus mehreren Verbindungen. Mit der Verbindungs-FireWALL wird für jede Verbindung geprüft ob diese beim ersten Verbindungsaufbau für den gesamten Server bzw. für die auslösende IP-Adresse vorgegebene Maximal-Werte überschreitet.



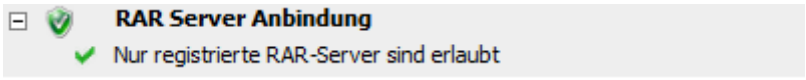
Sicherheits-Center SSL-Protokoll FireWALL

Mit dieser FireWALL können Angriffe die auf SSL-Protokoll-Fehler aufbauen abgefangen werden. Hier ist der Unterschied zu der Verbindungs-FireWALL, das über eine einzelne Verbindung sehr hohe Serverlast erzeugt werden kann.



Sicherheits-Center RAR-Server Anbindung

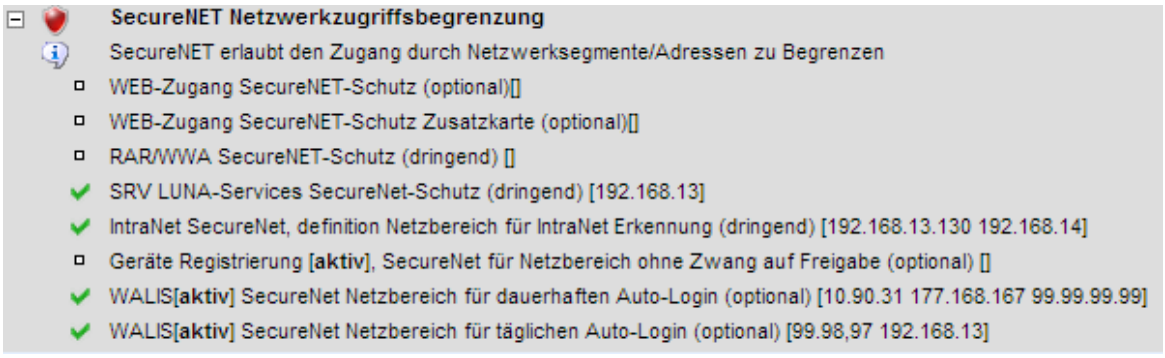
Es ist möglich nach erfolgreicher Installation die Neuanmeldung von bisher nicht registrierten RAR-Servern zu Unterdrücken.



Sicherheits-Center SecureNET Netzwerkzugriffsbegrenzung

Mit Hilfe der SecureNet Zugriffsbegrenzung, können die Verbindungsversuche auf bestimmte Netzsegmente bzw. IP-Adressen eingegrenzt werden. Dadurch kann eine erhöhte Sicherheit erreicht werden.

Die Eingabe der SecureNet Vorgaben kann bis zu 20 Segmente umfassen. Dabei werden die Netzwerkadressen als Zahlen erwartet. Alle Zeichen ausser 0..9 und '.' werden als Trennzeichen gewertet. Es ist darauf zu achten das die Einzelzahlen nie größer als 255 sein können. Es ist möglich auch nur Teilmasken anzugeben. Beispiel 192.168 , damit werden alle Rechner die diese Start-IP-Adresse haben in die SecureNet Regel aufgenommen.



Zwingend ist das die RAR/WWA Schnittstelle, und auch die LUNA-Services Schnittstelle begrenzt werden, Hier besteht die Gefahr das externe Zugriffe auf die internen Schnittstellen des WEBWARE-Server möglich sind, und dadurch weitere Sicherheitsprobleme auftreten könnten.

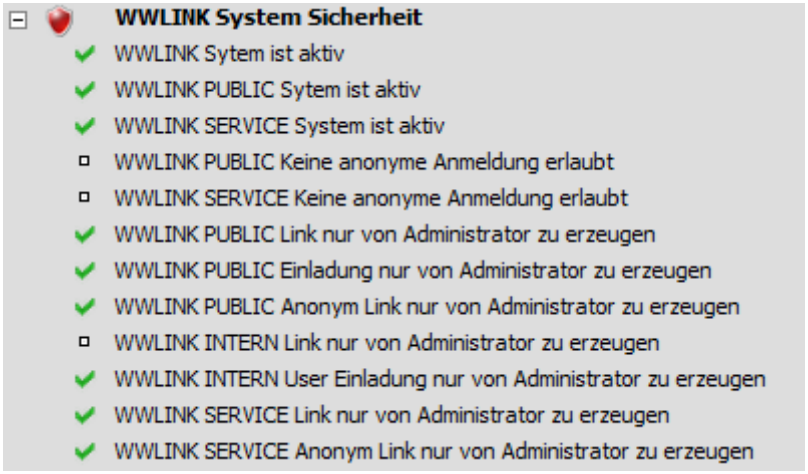
Wichtig ist auch die Intranet Definition für die WEB-Schnittstelle zu setzen. Damit ist es möglich die Rechner aus dem IntraNet und InterNet zu unterscheiden, und zum Beispiel unterschiedliche Login-Masken anzubieten.

Für die optionale Geräte Registrierung kann hier ein SecureNet Bereich angegeben werden, aus dem der Zugriff ohne Freigabe des Systembetreuers erfolgen darf.

Für das WALIS (WEBWARE Auto-Login System) können hier 2 SecureNet Bereiche für erlaubtes Auto-Login definiert werden.

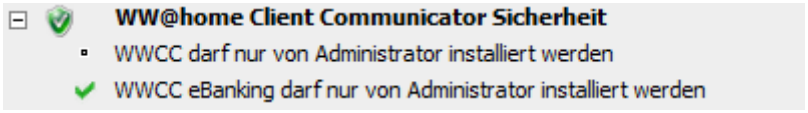
Sicherheits-Center WWLINK System Sicherheit

Hiermit können die Sicherheitsregeln für das WWLINK-System bearbeitet werden.



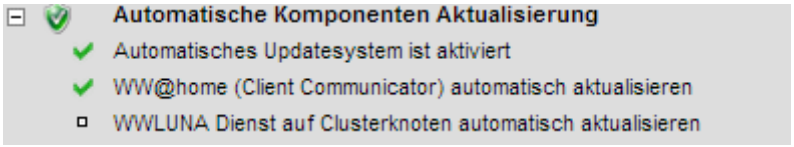
Sicherheits-Center WW@home (WW-Client Communicator)

Da die WW@home (WWCC) Komponenten in den meisten Systemen von allen Benutzern installiert werden dürfen, wird diese nicht zwingend erfordert. Die Installation von eBanking Modulen, sollte jedoch von Administratoren durchgeführt werden.

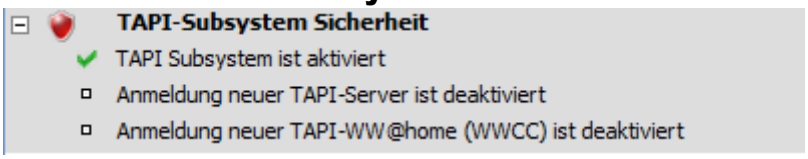


Sicherheits-Center Automatische Komponenten Aktualisierung

Hiermit kann für Teilsysteme die automatische Aktualisierung gesteuert werden. Dadurch können Sicherheitslücken schneller geschlossen werden.



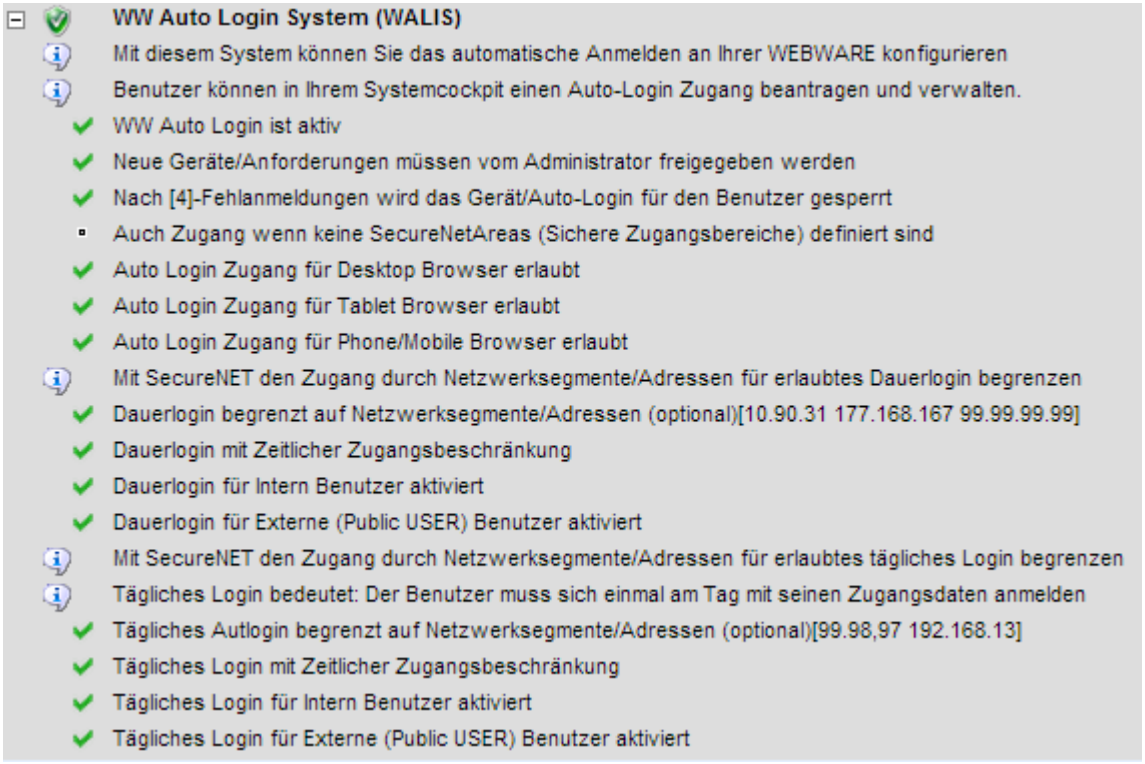
Sicherheits-Center TAPI-Subsystem



Sicherheits-Center WW Auto Login System (WALIS)

Mit dem WALIS können Sie die automatisierte Anmeldung an Ihrem WEBWARE-System aktivieren. Dabei ist es möglich pro Benutzer Gerät (Browser auf Desktop/Tablet/Phone) das automatisierte Anmelden zu aktivieren.

Die Freigabe der Auto-Login Funktion kann vom Systembetreuer pro Benutzer/Gerät erfolgen. Dabei kann dies je nach Geräte Kategorie, also Desktop Browser, Tablet Browser und Phone Browser und entsprechendem Netz



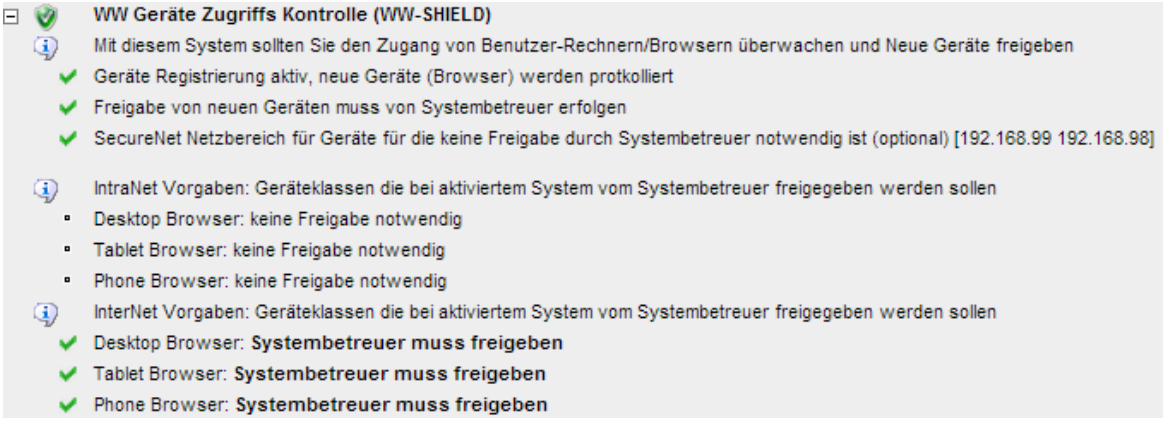
Es können 2 SecureNet Bereiche definiert werden mit denen die Netzwerkbereiche eingeschränkt werden können. Sind diese definiert so ist das Auto-Login nur für Geräte möglich die auch aus den definierten SecureNet Netzwerksegmenten zugreifen. Hier gibt es einen Bereich aus dem die Anmeldung nie, oder mindestens einmal täglich erfolgen muss.

Falls man das automatisierte Login immer freischalten will, so gibt es den Parameter "Auch Zugang wenn keine SecureNetAreas definiert sind". Mit diesem kann bei keiner SecureNet Angabe der Zugriff immer aktiviert werden.

Es gibt hier desweiteren die Möglichkeit den automatischen Zugang nach Tagen und Uhrzeit zu begrenzen.

Sicherheits-Center WW Geräte Zugriff Kontrolle (WWSHIELD)

Mit der Zugriffsüberwachung ist es möglich den Zugang zum Ihrem WEBWARE System zu Beschränken. Dabei kann angegeben werden ob der Zugang aus IntraNet oder InterNet nur nach Freigabe des Systembetreuers erfolgen darf.



Für die erfolgreiche Überwachung muss die Geräte Registrierung, sowie die Freigabe von neuen Geräten durch den Systembetreuer, aktiviert sein.

Hier kann dann nach IntraNet und InterNet angegeben werden, welche Geräte Klassen (Desktop, Tablet, Phone) erst nach einer Freigabe des Systembetreuer, aus den entsprechenden Netzbereichen zugreifen dürfen.

Sitzungs-FireWALL bedienen

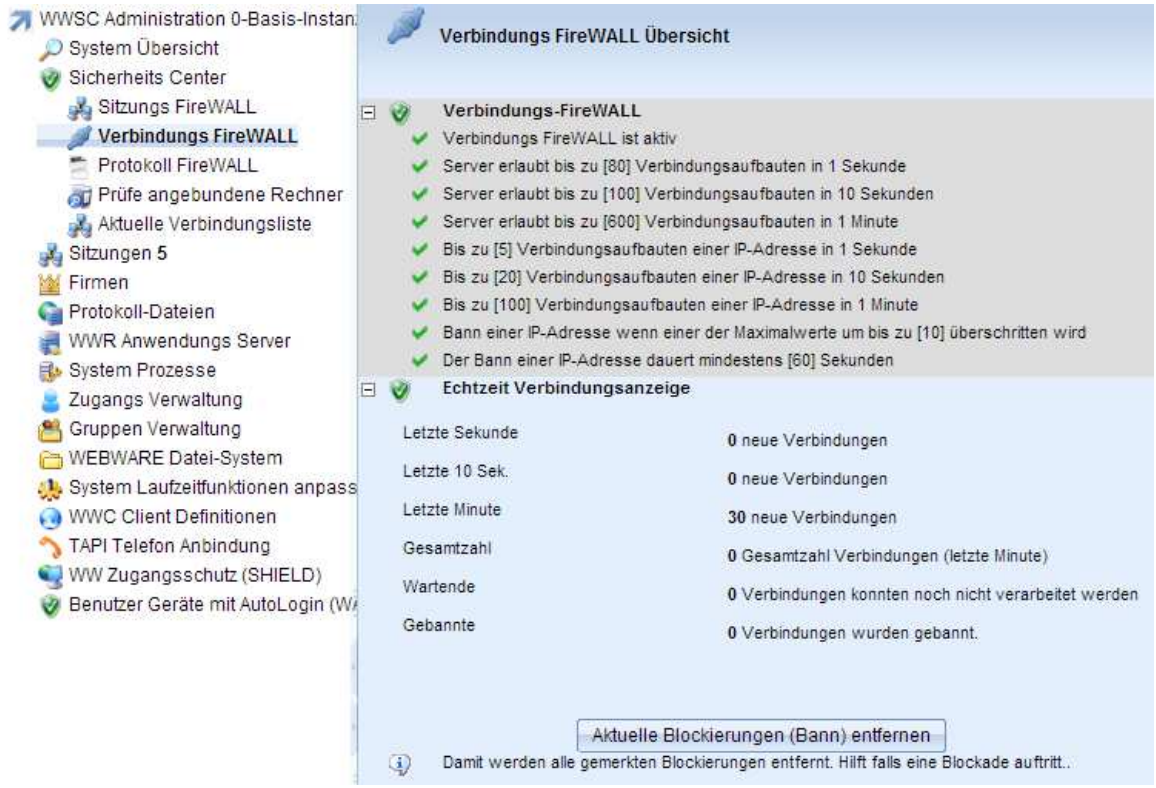
Mit dem Ast Sitzungs-FireWALL können die aktuellen Parameter eingesehen werden. Zusätzlich gibt es hier die Möglichkeit (Admin-/Config- Cockpit) die aktuelle Sitzungsliste zurücksetzen.

Die Sitzungsliste wird verwendet um zu prüfen ob zu viele Sitzungen von einer IP-Adresse aus aufgebaut wurden. Durch löschen der Liste kann der Zugriff für blockierte IP-Adressen wieder hergestellt werden.

Die Sperrung wird über einen Systemwert vorgegeben. (Unten mit 60 Sekunden gesetzt)

Verbindungs FireWALL bedienen

Hier kann man neben den Sicherheitsregeln, auch die aktuellen Zustände der FireWALL überwachen. Diese Werte (Echtzeit Verbindungsanzeige) werden sekündlich aktualisiert. Im unteren Ausschnitt ist ein Angriff mit 2 SSL-DOS Programmen gezeigt. Jeder der Angreifer baute 400er Verbindungen, wobei alle 800 Verbindungen gebannt wurden.



Falls man die aktuelle Blockierliste löschen will, kann man dies mit dem Knopf am unteren Ende der Anzeige durchführen. Dadurch werden alle Blockiereinträge entfernt.

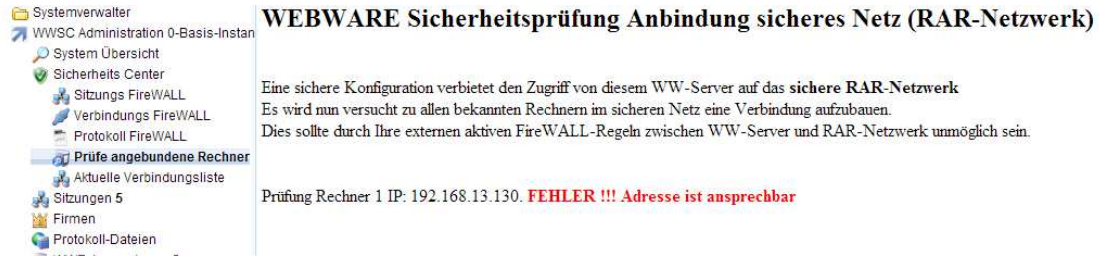
Protokoll FireWALL bedienen

Mit der SSL-Protokoll FireWALL können Protokoll Angriffe überwacht und abgewehrt werden. Bei Erkennung eines Protokoll Fehlers werden anhand der Sicherheitsregeln dieser FireWALL einzelne Verbindungen, und als Resultat auch die IP-Adresse des Angreifers blockieren. Mit dem Schalter „Aktuelle Protokollfehler (Bann) entfernen“, kann die aktuelle Bann-Liste gelöscht werden.

Sicherheitsprüfung angebundener Netzwerke

Mit der Funktion "Prüfe angebundene Rechner", kann geprüft werden ob ein Zugriff vom WW-Server auf die Rechner im sicheren Netzwerk möglich ist. Dies sollte auf keinen Fall möglich sein. Das Sicherheitskonzept der WEBWARE sieht vor das Verbindungen nur aus dem sicheren Netz zum WW-Server aufgebaut werden dürfen.

Diese Funktion ist noch nicht komplett ausgebaut. Zur Zeit wird hier geprüft ob der Rechner ansprechbar ist. Die Prüfungen in diesem Bereich sollen später noch erweitert werden, und geben Ihnen im Moment einen Hinweis das Sie das sichere Netzwerk besser schützen müssen.



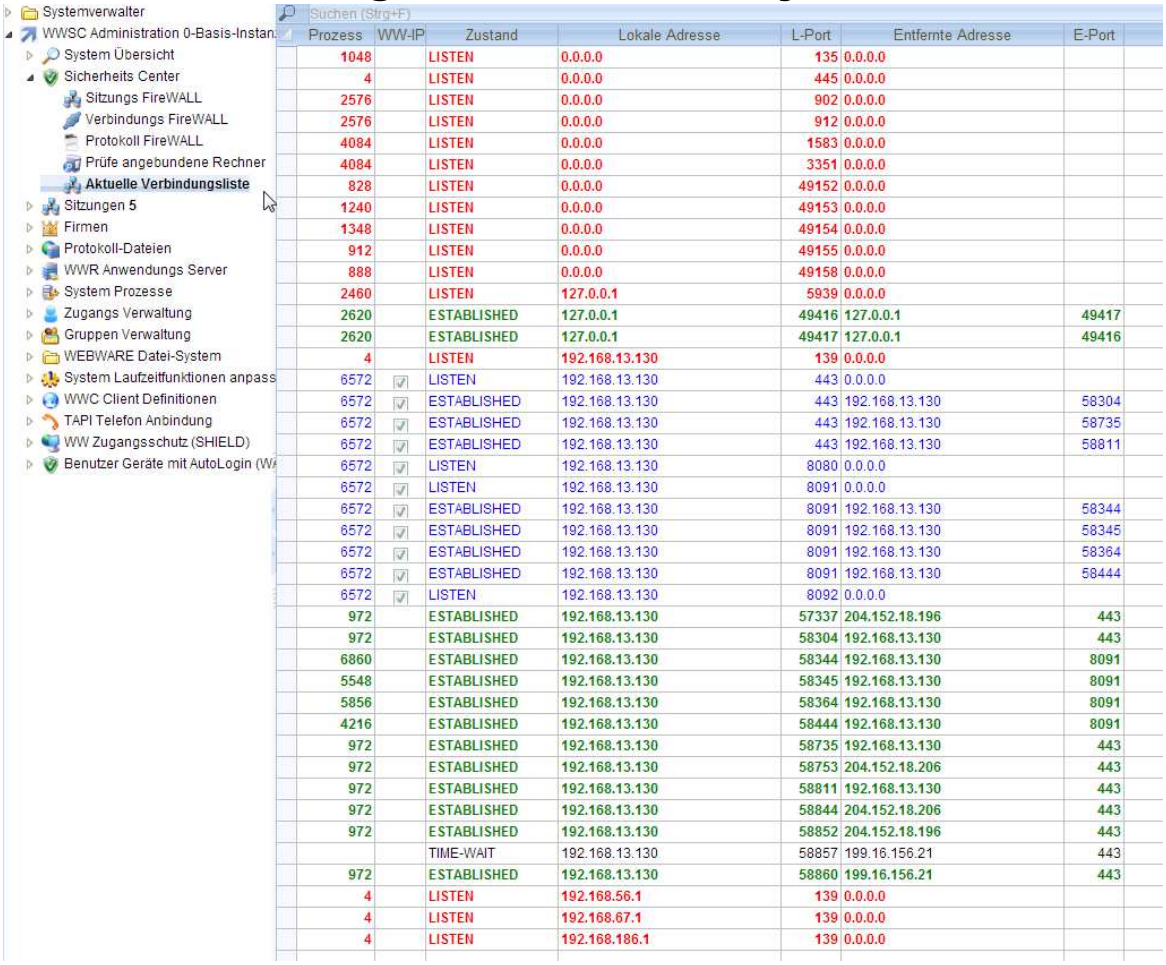
Hintergrund:

Wird der WEBWARE-Server von einem Angreifer kompromittiert, so darf es nicht möglich sein vom WW-Server über Netzwerkfreigaben, bzw. über Netzwerkzugriffe auf das sichere Netz zugreifen zu können. Hierzu ist es notwendig das sichere Netz (RAR-Netzwerk) mit Hilfe einer FireWALL und entsprechenden Regeln vor dem Zugriff zu schützen. Eine weitere Möglichkeit ist es die dedizierte Netzwerkkarte die für die Anbindung des WEBWARE-Servers in das sichere Netz verwendet wird, mit so wenig wie möglich Protokolltreiber auszustatten. Also keine Protpkolle für Netzwerkfreigaben usw. in den IP-Stack der Netzwerkkarte aufnehmen.

Angriffspunkt auf einen WEBWARE-Server muss nicht zwingend das WEBWARE-Server Programm selbst sein. Durch Sicherheitslücken im Betriebssystem oder auch anderen Programmen die auf dem WEBWARE-Server System installiert sind, könnte ein Angreifer Zugriff auf Ihre System erhalten.

Die Prüfung verwendet alle aktuell registrierten RAR-Server und prüft für deren IP-Adressen ob ein Zugriff vom WW-Server aus möglich ist. Da durch "Time-Out"-Fehler (Zeitüberschreitung) die Abarbeitung länger dauern kann, werden die Rechner im 3 Sekunden Takt bearbeitet.

Aktuelle Verbindungsliste Ihres Server-Systems



Prozess	WW-IP	Zustand	Lokale Adresse	L-Port	Entfernte Adresse	E-Port
1048		LISTEN	0.0.0.0	135	0.0.0.0	
4		LISTEN	0.0.0.0	445	0.0.0.0	
2576		LISTEN	0.0.0.0	902	0.0.0.0	
2576		LISTEN	0.0.0.0	912	0.0.0.0	
4084		LISTEN	0.0.0.0	1583	0.0.0.0	
4084		LISTEN	0.0.0.0	3351	0.0.0.0	
828		LISTEN	0.0.0.0	49152	0.0.0.0	
1240		LISTEN	0.0.0.0	49153	0.0.0.0	
1348		LISTEN	0.0.0.0	49154	0.0.0.0	
912		LISTEN	0.0.0.0	49155	0.0.0.0	
888		LISTEN	0.0.0.0	49158	0.0.0.0	
2460		LISTEN	127.0.0.1	5939	0.0.0.0	
2620		ESTABLISHED	127.0.0.1	49416	127.0.0.1	49417
2620		ESTABLISHED	127.0.0.1	49417	127.0.0.1	49416
4		LISTEN	192.168.13.130	139	0.0.0.0	
6572	☑	LISTEN	192.168.13.130	443	0.0.0.0	
6572	☑	ESTABLISHED	192.168.13.130	443	192.168.13.130	58304
6572	☑	ESTABLISHED	192.168.13.130	443	192.168.13.130	58735
6572	☑	ESTABLISHED	192.168.13.130	443	192.168.13.130	58811
6572	☑	LISTEN	192.168.13.130	8080	0.0.0.0	
6572	☑	LISTEN	192.168.13.130	8091	0.0.0.0	
6572	☑	ESTABLISHED	192.168.13.130	8091	192.168.13.130	58344
6572	☑	ESTABLISHED	192.168.13.130	8091	192.168.13.130	58345
6572	☑	ESTABLISHED	192.168.13.130	8091	192.168.13.130	58364
6572	☑	ESTABLISHED	192.168.13.130	8091	192.168.13.130	58444
6572	☑	LISTEN	192.168.13.130	8092	0.0.0.0	
972		ESTABLISHED	192.168.13.130	57337	204.152.18.196	443
972		ESTABLISHED	192.168.13.130	58304	192.168.13.130	443
6860		ESTABLISHED	192.168.13.130	58344	192.168.13.130	8091
5548		ESTABLISHED	192.168.13.130	58345	192.168.13.130	8091
5856		ESTABLISHED	192.168.13.130	58364	192.168.13.130	8091
4216		ESTABLISHED	192.168.13.130	58444	192.168.13.130	8091
972		ESTABLISHED	192.168.13.130	58735	192.168.13.130	443
972		ESTABLISHED	192.168.13.130	58753	204.152.18.206	443
972		ESTABLISHED	192.168.13.130	58811	192.168.13.130	443
972		ESTABLISHED	192.168.13.130	58844	204.152.18.206	443
972		ESTABLISHED	192.168.13.130	58852	204.152.18.196	443
		TIME-WAIT	192.168.13.130	58857	199.16.156.21	443
972		ESTABLISHED	192.168.13.130	58860	199.16.156.21	443
4		LISTEN	192.168.56.1	139	0.0.0.0	
4		LISTEN	192.168.67.1	139	0.0.0.0	
4		LISTEN	192.168.186.1	139	0.0.0.0	

Mit Hilfe der aktuellen Verbindungsliste erhalten Sie eine Übersicht, über alle Netzwerkverbindungen die aktuell auf Ihrem Server-System aktiv sind. Je nach Konfiguration Ihrer System-FireWALL können Angreifer auf Verbindungen die im "LISTEN"-Zustand (Warte auf Verbindungsaufbau) sind, zugreifen.

Pro Zeile wird genau eine TCPIP-Verbindung dargestellt. Neben der Prozess-ID und Kennung, ob die Verbindung von Ihrem WEBWARE-Server Programm verwendet wird, haben Sie Informationen von welcher Lokalen-Netzwerkkarte/Port zu welcher Externen Netzwerk-Adresse/Port die Verbindung aufgebaut wurde.

Mit Hilfe der Suchleiste (oberhalb der Tabelle) können Sie die angezeigten Verbindungsinformationen einschränken.

Um Ihnen einen schnelleren Überblick zu geben, sind die einzelnen Zeilen farblich markiert.

- **BLAU** Verbindung gehört zum WEBWARE-Server, und wird von diesem Verwaltet
- **ROT** Dies ist eine LISTEN-Funktion die je nach System-FireWALL von außen verwendet werden kann. Hier müssen Sie aktiv werden und Prüfen ob diese Schnittstellen/Ports tatsächlich von außen erreichbar sein sollen
- **GRÜN** Dies sind Verbindungen die aktiv sind, und die nicht vom WEBWARE-Server stammen.
- **SCHWARZ** Sonstige Verbindungen

Login und Passwort-System

Nähere Infos zum Login und Passwort-System finden Sie in der Dokumentation: WW-DOKU-WW-PASSWORT-SYSTEM.PDF

WW Protokoll System

Der WW-Server protokolliert je nach Konfiguration die wichtigsten System-Ereignisse. Die Konfiguration des Protokoll Subsystems erfolgt über die WW-System-Console, und kann nur von WW-System-Administratoren durchgeführt werden.

Nähere Infos findet man in der Doku WW-DOKU-WW-Protkoll-Subsystem.pdf

Die Sicherheitsprotokolle werden in der Datei \Bin\WWS\LOGS\WWS-Security-[Datum].log gespeichert.

Hier die Aufstellung der Fehlermeldungen die Protokolliert werden:

Bereich 50000 Meldungen des WWS Servers

Fehler-Nr	Fehler-ID	Fehlerbeschreibung
50001	WWSSYS01	Benutzer hat das Programmende manuell eingeleitet. Der Server und alle Subsysteme werden heruntergefahren (ESCAPE + J)
50002	WWSSYS02	WWS Service wird von außen gestartet mit Ergebnis
50003	WWSSYS03	WWS Service wird nun beendet
50004	WWSSYS04	WWS Service wird von außen zum Beenden aufgefordert
50005	WWSRAR01	WWR Server unbekannt Logon ist verboten
50006	WWSRAR02	WWR Server ist für Anmeldung gesperrt, wird abgelehnt
50007	WWSRAR03	WWR Server will sich entfernen, ist aber hier nicht bekannt
50008	WWSRAR04	WWR Server will Programm-Liste erneuern, ist hier aber nicht bekannt
50010	WWSSYS10	Benutzer hat über die Fensterconsole ein Zeichen eingegeben Angabe Zeichen + Zeichen-Code
50011	SYSCKPIT-50011	Ein Administrator hat die Rechte/Temporäre Recht eines Benutzer/Administratoren geändert für die aktuelle Firma geändert
50012	SYSCKPIT-50012	Abweichende Rolle bzw. Temporäre Rolle eines Benutzer wird entfernt da diese höher als die neu gesetzt Rolle ist
50013	SYSCKPIT-50013	Rolle in Benutzerstammsatz wurde geändert

Sicherheitsmeldungen FireWALL's

Fehler-Nr	Fehler-ID	Fehlerbeschreibung
50100	WWSPGM00	Ein Programm hat sich registriert, jedoch weicht die Dateigröße von der bekannten ab
50200	WWFW0000	Zugriff mit IP-Adresse wurde geblockt, die Adresse ist aktuell in der IP-Blacklist des Adapters vorhanden
50201	WWFW0001	Zugriff mit IP-Adresse wurde geblockt, die Adresse ist außerhalb des vorgegebenen Secure-Net Bereiches für den Adapter
50202	WWFW0002	Es wurden von der gleichen IP-Adresse zu viele neue Sitzungen gestartet, Neue Sitzung wird abgelehnt.
50300	WWIPS000	Konfiguration der IPS Firewall wurde geändert
50301	WWIPS001	IPS Firewall hat eine Verbindung in die Warteschlange gestellt, zu viele Zugriffe. Warte bis weniger Last vorhanden ist
50302	WWIPS002	IPS Firewall hat eine Verbindung gebannt. Es wird nun die vorgegebene Wartezeit eingehalten
50303	WWIPS003	IPS Firewall gebannte Verbindung wird beendet.
50304	WWIPS004	IPS gehaltene Verbindung kann nun verarbeitet werden.
50305	WWIPS005	IPS Protokoll-Firewall hat eine Verbindung gebannt. Zu viele Protokoll-Fehler. Es wird nun die vorgegebene Wartezeit eingehalten.
50306	WWIPS006	PROT Firewall hat zu viele Protokoll Fehler erkannt, die angegebene IP-Adresse wird für die Standardzeit blockiert.

Bereich 60000 Fehler beim Anmelden im Login-System

Fehler-Nr	Fehler-ID	Fehlerbeschreibung
60001	WWFERR002	WWF-Logon Fehler Der angegebene Benutzername/Nummer ist unbekannt
60002	WWFERR002	WWF-Logon Fehler Beim Anmelden wurde für einen Benutzer das falsche Passwort angegeben.
60003	WWFERR003	WWF-Logon Fehler Der Benutzer konnte erfolgreiche verifiziert werden, jedoch besteht bereits eine Anwendung, für diese kann jedoch kein Sitzungs-Menü angezeigt werden.
60004	WWFERR004	WWF-Logon Fehler Der Bediener ist gesperrt
60005	WWFERR005	WWF-Logon Benutzer wurde wegen Falscheingabe des Passwortes gesperrt
60006	WWFERR006	WWF-Logon Benutzerkennung konnte nicht eindeutig zugeordnet werden,

		Mehrfachvorgabe für eMail/Nick-Name/Application-Benutzer-Nummer
60007	WWFERR007	WWF-Logon Passwort Ändern Dialog Fehler bei der Eingabe
60008	WWFERR008	WWF-Logon Konfigurationsproblem RAR-Server bzw. Anwendungs-ID nicht gefunden
60009	WWFERR009	WWF-Logon Benutzer hat einen falschen Mandanten Zugangscode eingegeben
60010	WWFERR002	WEBDAV Logon Fehler Der angegebene Benutzername/Nummer ist unbekannt
60012	WWFERR002	WEBDAV Logon Fehler Beim Anmelden wurde für einen Benutzer das falsche Passwort angegeben.
60013	WWFERR013	WWF-Logon Benutzer erhält eine Zeitsperre wegen Passwort falscheingabe
60020	WLOGPERR1	Public-User WWF-Logon Versuch Zugriff auf Benutzer-Account mit Public-Benutzer Zugang
60021	WLOGPERR2	Public-User Benutzerzugang ist gesperrt
60022	WLOGPERR3	Public-User Vorlage für Benutzer fehlt
60023	WLOGPERR4	Public-User Vorlage-Nummer ist nicht vom Type Vorlage
60024	WLOGPERR5	Public-User Vorlage-Nummer ist gesperrt, kein Public-User mit dieser Vorlage kann sich anmelden
60025	WLOGPERR6	Public-User Standard-Passwortlänge ist zu kurz
60026	WLOGPERR7	Public User Vorlage hat WWPACK oder WWMDEK als Startprogramm eingetragen ist für Start nicht erlaubt
60027	WLOGPERR8	Public User hat WWPACK oder WWMDEK als Startprogramm eingetragen ist für Start nicht erlaubt
60030	WLOGUERR1	Intern-User versucht auf Admin-Konto zuzugreifen ist nicht erlaubt
60031	WLOGUERR2	Intern-User Passwort ist zu kurz es wird ein 32-Byte HASH-Passwort erwartet
60032	WLOGUERR3	Intern-User versucht auf PUBLIC-Zugang zuzugreifen, ist verboten
60033	WLOGUERR4	Intern-User Datensatz ist gesperrt. Zugang nicht möglich
60034	WLOGPERR5	Public-User Standard-Passwortlänge ist zu kurz
60035	WLOGUERR6	Passwort Validierung von WWA für Konto. PW ist zu kurz es wird ein 32-Byte Passwort-Hash erwartet

60036	WLOGUERR6	Passwort Validierung von WWA für Konto. Benutzer ist gesperrt, kein Zugriff erlaubt !!
60040	WLOGSERR1	ADMIN-User Zugang ist gesperrt

Bereich 60051 WW Client Communicator

Fehler-Nr	Fehler-ID	Fehlerbeschreibung
60051	WWCCERR001	WWCC Registrierung eines neuen WWCC ist fehlgeschlagen, Registrierungs-ID nicht bekannt
60052	WWCCERR002	WWCC Entfernungsanforderung eines WWCC ist fehlgeschlagen, WWCC nicht gefunden

Bereich 60080 WW-System-Console

Fehler-Nr	Fehler-ID	Fehlerbeschreibung
60080	WWCONSERR	WW-System Console, Fehler beim Anmelden der Benutzer hat das falsche Passwort eingegeben

Bereich 61000 WALIS WEBWARE Auto Login System

Fehler-Nr	Fehler-ID	Fehlerbeschreibung
610000	WALISERR001	Benutzer versucht Auto-Login zu registrieren, jedoch ist dies nach Vorgabe nicht möglich. IP-Adresse[%s] Benutzer[%0ld-%s]
61001	WALISERR002	Benutzer versucht Auto-Login zu Entfernen, jedoch gab es dabei einen Fehler

Bereich 70000 – 70099 Zugriffsrechtsverletzungen Dateisystem

Fehler-Nr	Fehler-ID	Fehlerbeschreibung
70001	ERR001	SESSION[ ],ERR001,FILE NOT FOUND,… Benutzer hat kein Zugriffsrecht, Datei wird als nicht gefunden markiert.
70002	ERR002	SESSION[ ],ERR002,FILE NOT FOUND,… Die Datei wurde nicht gefunden
70003	ERR003	SESSION[ ],ERR003,FILE NOT FOUND,… Der Pfade zu der Datei war fehlerhaft formatiert, Datei wird als nicht gefunden markiert.

70004	ERR004	SESSION[ ],ERR004,FILE NOT FOUND,… Es wurde versucht eine Datei aus dem WWFS-Dateisystem zu lesen. Die Datei wurde dabei nicht gefunden.
70005	ERR005	SESSION[%08ld],ERR005,FILE NOT FOUND,%s Es wurde versucht eine Datei aus dem HOME-Dateisystem zu lesen. Die Datei wurde dabei nicht gefunden

Bereich 71000 WW LINK System

Fehler-Nr	Fehler-ID	Fehlerbeschreibung
71000	LNK001	LINK wurde nicht gefunden bzw. nicht erlaubt Nähere Infos in der Nachricht

Bereich 80000 Fehler in http Anfragen

Fehler-Nr	Fehler-ID	Fehlerbeschreibung
80001	ERR001	HTTPCHECK ERR001 Befehl […] ist nicht bekannt Ein HTTP-Befehl wird vom System nicht erkannt bzw. zurückgewiesen. Es wird in der Folge eine HTTP 501 Fehlermeldung zurückgegeben

Bereich 81000 Fehler in WWNATIVE Anfragen

Fehler-Nr	Fehler-ID	Fehlerbeschreibung
81000	WWNAT0001	Fehler in HTTP-Anfrage, Hash-Wert für Verbindung nicht Valid. Die Validierungsprüfung der HTTP-Anfrage zeigt das diese nicht Gütig ist. Anfrage wird nicht bearbeitet. Session[%0ld] WWNATIVE-ID[%0ld] USRNR[%0ld] IP-Adresse[%s] Benutzer[%s] WWNATI[%s] WWNATS[%s] CheckedHash[%s]

Bereich 90000 Fehler in Dateisystemanfragen

Fehler-Nr	Fehler-ID	Fehlerbeschreibung
90001	ERR001	SESSION[ ] FILECHECK ERR001 Datei [ ] hat mehrere Punkte hintereinander an Position …" Fehlerhafte Angabe eines Dateizugriffspfades. Dabei wurden mehr als 2 Punkte hintereinander angegeben /sk/.../
90002	ERR002	SESSION[ ] FILECHECK ERR002 Datei [ ] Home-Verzeichniss wird

		verlassen an Position … Fehlerhafte Angabe eins Dateizugriffpfades. Dabei wird das HOME-Verzeichnis unerlaubt verlassen /sk/../../../
90003	ERR003	SESSION[ ] FILECHECK ERR003 Datei [ ] hat mehrere Verzeichniss-Trenner hintereinander an Position .. Fehlerhafte Angabe eins Dateizugriffpfades. /sk////lib
90004	ERR004	SESSION[ ] FILECHECK ERR004 Datei [ ] enthält Falsches Zeichen ( ) an Position … Fehlerhaftes Angabe in einem Dateizugriffpfad. Das Fehlerhafte Zeichen wird mit ausgegeben.
90005	ERR005	SESSION[ ] FILECHECK ERR005 Datei [ ] ACCESS VIOLATION WWFS-AREA FORBIDDEN Es wurde versucht auf ein geschütztes Verzeichnis, wie zum Beispiel das WWFS Verzeichnis zuzugreifen. Der Zugriff wurde abgelehnt
90006	ERR006	SESSION[ ] User[ ] ERR006 WWFS-Access Error in Filename … Der Dateiname beim Zugriff auf eine Datei im WWFS/SV Bereich ist Fehlerhaft, kein Zugriff möglich.
90007	ERR007	SESSION[ ] User[ ] DateiID[ ] ERR007 WWFS-Access Error File-ID not found for FileName … Es wurde keine Datei mit der angegebenen Datei-ID gefunden, bzw. Datei mit dieser ID ist gesperrt
90008	ERR008	SESSION[ ] User[ ] DateiID[ ] Version[ ] ERR008 WWFS-Access Error File-ID+Version not found for FileName … Es wurde keine Datei mit der angegebenen Datei-ID und Versionsnummer gefunden.
90009	ERR009	SESSION[ ] User[ ] FileID[ ] Version[ ] ERR009 WWFS-ACCESS Violation No Rights 2 Read Der Benutzer hat keine Zugriffsrechte um die Datei zu lesen
90010	ERR010	WWFS ACCESS ERROR010 User[ ] File[ ] DELETE NOT ALLOWED Es wurde versucht eine Datei im WWFS zu löschen, obwohl keine Berechtigung für den Benutzer vorliegt
90011	ERR011	WWFS ACCESS ERROR011 User[ ] File[ ] UNDELETE NOT ALLOWED Es wurde versucht eine Datei aus dem Papierkorb wiederherzustellen, obwohl keine Berechtigung vorliegt

90012	ERR012	WWFS ACCESS ERROR012 User[ ] File[ ] FILE IN TRASH NOT ALLOWED Es wurde versucht eine Datei in den Papierkorb zu verschieben, obwohl keine Berechtigung vorhanden ist
90013	ERR013	WWFS ACCESS ERROR013 User[ ] File[ ] FILECHANGE NOT ALLOWED Es wurde versucht eine Datei zu ändern, obwohl keine Berechtigung vorhanden ist
90014	ERR014	WWFS ACCESS ERROR014 User[ ] File[ ] NEWNAME[ ] RENAME NOT ALLOWED Es wurde versucht eine Datei umzubenennen, obwohl keine Berechtigung vorhanden ist
90015	ERR015	WWFS ACCESS ERROR015 User[ ] DIR[ ] NEWNAME[ ] CREATE NOT ALLOWED Es wurde versucht eine Datei in einem Verzeichnis anzulegen, obwohl keine Berechtigung vorhanden ist
90016	ERR016	WWFS ACCESS ERROR016 EXTERN.HTM-Link[] Remote-IP[], Expected-IP[] Unerlaubter Zugriff auf EXTERN.HTM Link [Bspl: https://MeinServer.de/EXTERN.HTM12345678] mit abweichender IP-Adresse [ ], Sitzung hat IP-Adresse[]. Dadurch kann ein Zugriff auf den EXTERN.HTM LINK von einer abweichenden IP-Adresse verhindert werden.

Liste der Dokumentänderungen

Datum	Thema geändert
01.11.2013	LIVECHECK Funktion integriert. Topic: LiveCheck Funktion WEBServer über WEB-Schnittstelle
24.09.2014	Kapitel "Wiederherstellung / Umzug / Recovery Funktion" eingefügt. Neuer Parameter für LUNA-Subsystem starten eingetragen.
13.10.2014	Erweiterung um Funktion: Zugriff auf Extern.HTM nur von IP-Adresse der aktuellen Sitzung beschränken.
17.10.2014	Ergänzung Funktion Start des WW-Servers mit notwendiger RECOVERY-Funktion zum Schutz der Datenbank
21.10.2014	Erweiterung Zertifikat und WW-Server sowie aktuelle Optimale Konfiguration und Test Möglichkeiten..
17.06.2015	Neues Zugriffsrecht um das Passwort beim Zugang ins System-Cockpit nur einmal eingeben zu müssen. (WWS REV: 12512)
08.07.2015	WWPACK+WWMDEK sind für Public-Worker Ausführung nicht mehr erlaubt (WWS-REV: 12527)
11.11.2015	Erweiterung WWS.INI um Startparameter um die Netzwerkarten auch für WW-Instanzen angeben zu können.
13.04.2016	Korrektur der RECOVERY Funktions-Beschreibung hier wurden Punkt 2 und 3 getauscht, da vor dem Ausführen der Recovery-Funktion die WWS.INI bereits angepasst sein soll
26.04.2016	Genauere Beschreibung über Dateiformate und Verwendung von SSL-Schlüsseldateien
08.09.2016	Neue Security-Meldungen 50011 + 50012 + 50013
23.03.2017	Erweiterung/Überarbeitung Recovery-Funktion sowie Zertifikats-Dokumentation aktualisiert