



WEBWARE

WEBWARE System-Cockpit

*Fragen
und
Antworten*

Dieses Handbuch ist für

Systemadministratoren / Systemarchitekten

Es wird empfohlen das Handbuch
„WW-DOKU-WW-System-Console“
vorher gelesen zu haben.

V 1.02 13.11.2013

INHALTSVERZEICHNIS

<i>Wie kann ich das WW-System-Cockpit aufrufen ?</i>	1
<i>Welche System-Admin's sind definiert ?</i>	1
<i>Anderem Bediener Administrator-Rechte geben ?</i>	2
<i>Gesperrter Administrator freischalten</i>	3
Ich habe noch einen weiteren Administrator definiert	3
Ich habe keinen weiteren Administrator definiert	4
Ich habe keinen funktionierenden Administrator Zugang mehr ?	4
Konfiguration Details	5
<i>Warum wird mein Ausdruck nicht gefunden ?</i>	5
WEB-Schnittstelle (Externes Netz)	5
WEBWARE Zertifikat	7
<i>Einleitung in Zertifikate..</i>	7
<i>Welche Möglichkeiten haben Sie ein gültiges Zertifikat in Ihre WEBWARE rein zubekommen ?</i>	8
<i>Verwendung von SoftENGINE ausgelieferten Zertifikaten</i>	8
<i>Erstellen eines kostenlosen Zertifikat über StartSSL.com</i>	8
Konfiguration des WW-Servers für StartSSL Zertifikate	8
Erstellung der Chain-Datei unter Windows	9
Konfiguration Ihres WEBWARE-Servers: WWS.INI anpassen	9
<i>Erstellung eines eigenen, selbst Signierten Zertifikates</i>	9

Wie kann ich das WW-System-Cockpit aufrufen ?

Es gibt 2 Arten in das System-Cockpit einzusteigen.

- Benutzer hat Admin-Rechte und eine laufende Anwendung



Aufruf des System-Cockpit's aus der laufenden Anwendung über das Haupt-Menü unter Einstellungen

- Einstieg direkt über den WW-Server



In der Standardeinstellung ist der Zugriff auf das System-Cockpit nur möglich wenn der Benutzer direkt auf dem WW-Server arbeitet und dort mit einem Browser eine Verbindung zum WW-Server aufbaut.

Bei Anmeldung mit normalen Benutzerdaten erhält er hier einen Auswahlbildschirm mit dem er dann direkt in das WW-System-Cockpit ohne zusätzliche WW-Anwendung einsteigen kann.

Welche System-Admin's sind definiert ?

Die WEBWARE wird im Auslieferungszustand mit 3 vordefinierten Administratoren sowie 3 Konfiguratoren installiert. Diese sind nur Benutzbar wenn

- Bei der Installation ein Master-Passwort für die System-Administratoren definiert wurde.
- der Aufruf über den WW-Server direkt erfolgt.

WICHTIG: Nach der Installation sollte für alle 6 System-Admin's mit Hilfe des Master-Passwortes ein individuelles Passwort vergeben werden. Passwörter sind immer erst nach einer erneuten Anmeldung gültig !!

Die System-Admin's haben dabei unterschiedliche Rechte. Diese unterteilen sich in

Es sind folgende Administratoren definiert, diese haben maximal Administratoren .

- Firmen.admin@sc.ww.de (System-Übersicht aktuelle Instanz)
- Global.admin@sc.ww.de (System-Übersicht + Administration Übergreifend)
- Server.admin@sc.ww.de (Gleich wie Global abhängig von Konzern/Cooperation/Cloud-Installation)

Diese System-Konfigurationen

- Firmen.config@sc.ww.de (Systemübersicht/Administration/Konfiguration aktuelle Instanz)
- Global.config@sc.ww.de (Systemübersicht/Administration/Konfiguration/Installation alle Instanzen)
- Server.config@sc.ww.de (Systemübersicht/Administration/Konfiguration/Installation alle Instanzen)

Anderem Bediener Administrator-Rechte geben ?



Steigen sie ins System-Cockpit mindestens mit Server.admin oder Global.admin Berechtigung. Wechseln Sie in den Bereich Administration.

Selektieren Sie einen Benutzer (Zugang>Mitarbeiter > Aktiviert) und wählen Sie aus dem Menü Benutzerrolle ändern.

Wählen Sie eine Admin-Berechtigung aus, und übernehmen Sie die neue Benutzerrolle.

Sie können die Rolle für den Bediener auch nur temporär setzen. Diese bleibt dann bis zum nächsten Serverneustart bestehen.



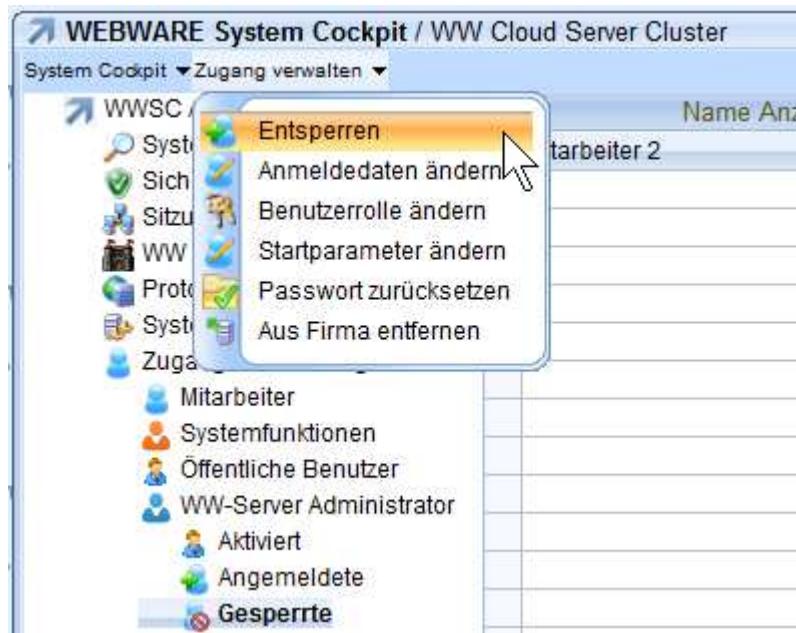
Der Benutzer verschwindet dann im Bereich Mitarbeiter und ist ab jetzt im Bereich der Administratoren sichtbar.

Gesperrter Administrator freischalten

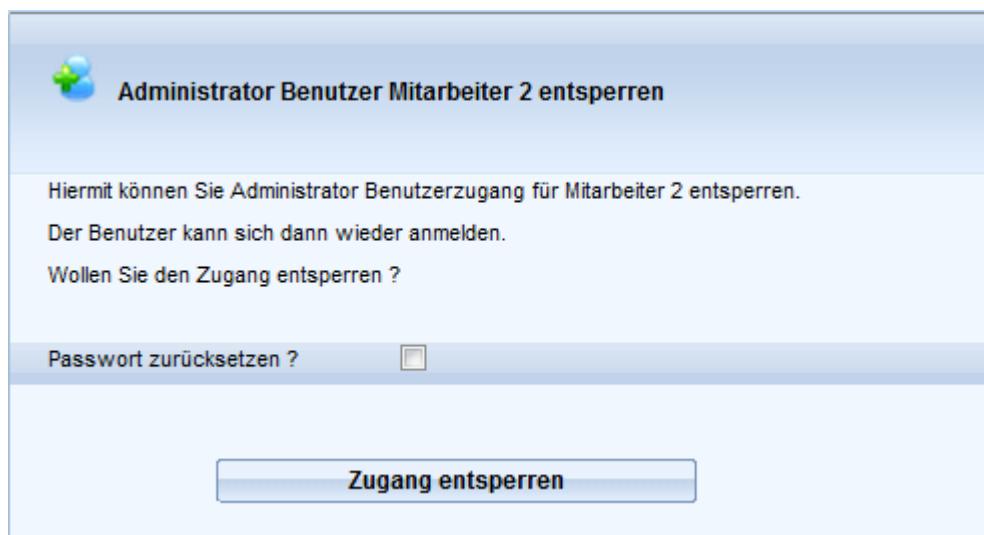
Durch mehrfache Falscheingabe des Passwortes ist es möglich auch Administratoren für den Zugang zum System zu sperren. Standardmäßig ist der Benutzer „0“ mit Admin Rechten ausgestattet. Falls der Zustand auftritt das ein Administrator gesperrt ist, so gibt es mehrere Möglichkeiten diesen wieder freizuschalten.

Ich habe noch einen weiteren Administrator definiert

Wichtig ist das der Administrator über Server- oder Global Adminrechte verfügt. Steigen sie mit dem Administrator ins System-Cockpit über die Anwendung ein und melden Sie sich im Bereich Administration an. In der Zugangsverwaltung gibt es für solche Admin's den Zusatzeintrag WW-Server Administrator.



Bestätigen Sie im folgenden Dialog das Sie den Administrator entsperren wollen. Sie haben die Möglichkeit das Passwort des Admin's zurückzusetzen. Dies führt dazu dass der Benutzer sich mit dem Masterpasswort ein neues Passwort vergeben muss.



Ich habe keinen weiteren Administrator definiert

Für diesen Fall haben Sie die Möglichkeit mit den Standard-Administratoren bzw. Standard-Konfigurationen ins WW-System-Cockpit einzusteigen und den gewünschten Administrator zu Entsperren. Achten Sie darauf das Sie mindestens mit Server.admin/Global.admin oder Server.config/Global.config ins WW-System-Cockpit einsteigen. Nur so erhalten Sie die Anzeige der Administratoren.

Ich habe keinen funktionierenden Administrator Zugang mehr ?

Da das System auf maximale Sicherheit ausgelegt ist, gibt es hier für Sie keine Möglichkeit mehr sich am System anzumelden. Daher wurden die unterschiedlichen vordefinierten Administratoren/Konfiguratoren definiert, die bereits bei der Installation mit einem, nur Ihnen bekannten, individuellen Master-Passwort festgelegt werden. Ebenso werden die Passwörter in einer verschlüsselten Datenbank vorgehalten, das es unmöglich macht die Passwörter von aussen auszulesen.

Sie sollten daher diese Administratoren als „sichere“ Reserve halten um in einem solchen Notfall ins System zu kommen.

Falls der Zugang zum System trotz aller Vorsichtsmassnahmen nicht mehr möglich ist, setzen Sie sich mit dem SoftENGINE-Support in Verbindung.

Konfiguration Details

Warum wird mein Ausdruck nicht gefunden ?

Je nachdem aus welchem Netzbereich Sie auf den WEBWARE-Server zugreifen, kann es sein das Sie hierfür eine erweiterte externe Beschreibung für das Netzwerkzugriff hinterlegen müssen.



Falls ihr Zugang zur WEBWARE hinter einen Router liegt, so ist es möglich das die lokale Netzwerkadresse (Beispiel 192.168.0.1) von der tatsächlich verwendeten Zugriffsadresse abweicht (www.meine-webware.de).

Daher ist es in diesem Fall (WEBWARE ist hinter einem Router, NAT) notwendig der WEBWARE die externe Adresse bekannt zu machen, so dass diese beim Ausliefern von Inhalten (Druck, WWCC, usw..) den WEBWARE-Server korrekt durch den Router adressieren kann.

Hier ein Auszug aus der Dokumentation WW-DOKU-SECURITY-System:

WEB-Schnittstelle (Externes Netz)

- ↗ WWSC Konfiguration 1-WW 1.04
 - ▷ 🔎 System Übersicht
 - ▷ 🛡 Sicherheits Center
 - ▷ 📈 System Prozesse
 - ▷ 🎯 System Laufzeitfunktionen anpassen
 - ↳ 🔒 System Konfiguration
 - ↗ System Information
 - ↗ System Basis Konfiguration
 - ▷ 📁 Programmpfade
 - ↳ 🌐 Netzwerk Anbindung
 - ↗ WEB Schnittstelle
 - ▷ 📁 Intern Schnittstelle

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.

WEBWARE Zertifikat

Frage: Gibt es ein https:// Zertifikat bzw. etwas damit wir das für unsere Demoumgebung umgehen können.

Antwort:

Einleitung in Zertifikate..

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\SOFTENGINE-CERT.pem

BWWSSL_ZERTIFIKAT=demozertifikat\demozertifikat.pem

BWWSSL_PASSWORD4PRIVKEY=demozertifikat

BWWSSL_PRIVATEKEY=demozertifikat\demozertifikat-key.pem

Ein gültiges Zertifikat besteht aus mehreren Bestandteilen:

CA-Zertifikat: Verweis auf die signierende Stelle

Server-Zertifikat: Zertifikat die für Ihren Server ausgestellt wurde

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

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.

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

Der WEBWARE-Server erlaubt es "normale"-Zertifikate (bestehend aus Einzeldateien), und Chain-Zertifikaten (hier sind 3 Zertifikate in einer Datei) zu Verwenden. Im folgenden werden wir Ihnen 3 Möglichkeiten vorstellen mit denen Sie Ihre WEBWARE konfigurieren können.

Verwendung von SoftENGINE ausgelieferten Zertifikaten

Falls Sie keine Änderung in der Konfiguration vornehmen ist das Demo-Zertifikat 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 oder der lokalen HOST-Datei muss der Domain Name des Rechners auf demo.webware.de gesetzt werden. Sie können dann vom Browser aus mit der Adresse https://demo.webware.de auf die WEBWARE zugreifen
- Rufen Sie dann in jedem Browser die Datei (bsp: https://demo.webware.de/)zertifikat.htm auf. Dort wählen Sie das SoftENGINE Zertifikat und installieren Sie dieses als Stamm-Zertifikat

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

Erstellen eines kostenlosen Zertifikat über StartSSL.com

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. Bsp:

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

Konfiguration des WW-Servers für StartSSL Zertifikate

Um den WW-Server in allen Browern 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.

Link auf die FAQ der Firma StartSSL.

<http://www.startssl.com/?app=25>

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>

Erstellung der Chain-Datei unter Windows

Die Chain-Datei besteht aus mindestens 3 Teil-Dateien die hintereinander kopiert werden müssen.

- Server Zertifikat für ihre Adresse
- Intermediate-Zertifikat (Zwischen Zertifikat braucht zum Beispiel FireFOX)
- CA-Zertifikat (Ausstellungsbehörde)

Die einzelnen Dateien findet man in der Toolbox von StartSSL.

- Server: Toolbox > Retrieve Certificate: You will see your newly created certificate. Save it as example.com.crt.
- Intermediate: Toolbox > StartCom CA Certificates: Download "StartCom Root CA (PEM encoded)" (ca.pem)
- CA-Zertifikat: Toolbox > StartCom CA Certificates: Download "Class 1 Intermediate Server CA" (sub.class1.server.ca.pem).

Die Dateien müssen dann hintereinander in die Zielfile kopiert werden. Wobei zuerst die Server, dann die Intermediate und danach die CA-Datei kommen müssen. Achten Sie darauf das hinter jeder Teildatei ein Zeilenwechsel vorhanden ist.

Konfiguration Ihres WEBWARE-Servers: WWS.INI anpassen

In der WWS.INI Datei gibt es für diesen Fall (Chain-Zertifikate) 2 neue Variablen:

BWWSSL_USE_CHAIN_ZERTIFIKAT=J

BWWSSL_CHAIN_ZERTIFIKAT=Pfad-Datei-Name

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_pkı/openssl-kurzreferenz.html

Hier ein YouTube Video

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