Anmelde- und Login-System der WEBWARE

Rel 16 vom 29.06.2015

WEBWARE

INHALTSVERZEICHNIS

WEBWARE Anmelde- / Login-System

Der WEBWARE Server hat 2 mögliche Login-Systeme die verwendet werden können. Das bisherige System-Server basierende, und das neue des WW-Servers. Mit Einführung des WW-Server Login-Systems kommen viele neue Funktionen im Bereich des WW-Systemcockpit hinzu die eine Verwaltung der Benutzer und Überwachung der Passwortrichtlinien erlauben.

Im Folgenden werden die Neuerungen des WW-Login-Systems beschrieben, und erklärt welche Schalter mit Hilfe des System-Cockpit's gesetzt werden können.

Folgende neue Funktionen sind vorhanden:

Passwortbezogende Funktionen

- Neuer Passwort Ändern Dialog mit optisches Hinweisen über Passwort-Richtlinien (visuelles feedback)
- Festlegung von Passwort Gültigkeitsdauer
- Festlegung von Passwort Bestandteilen
- Vorgabe automatische Sperrung nach mehrfacher Falscheingabe des Passwortes
- Vorgabe von global-Passwörter für die Erstanmeldung

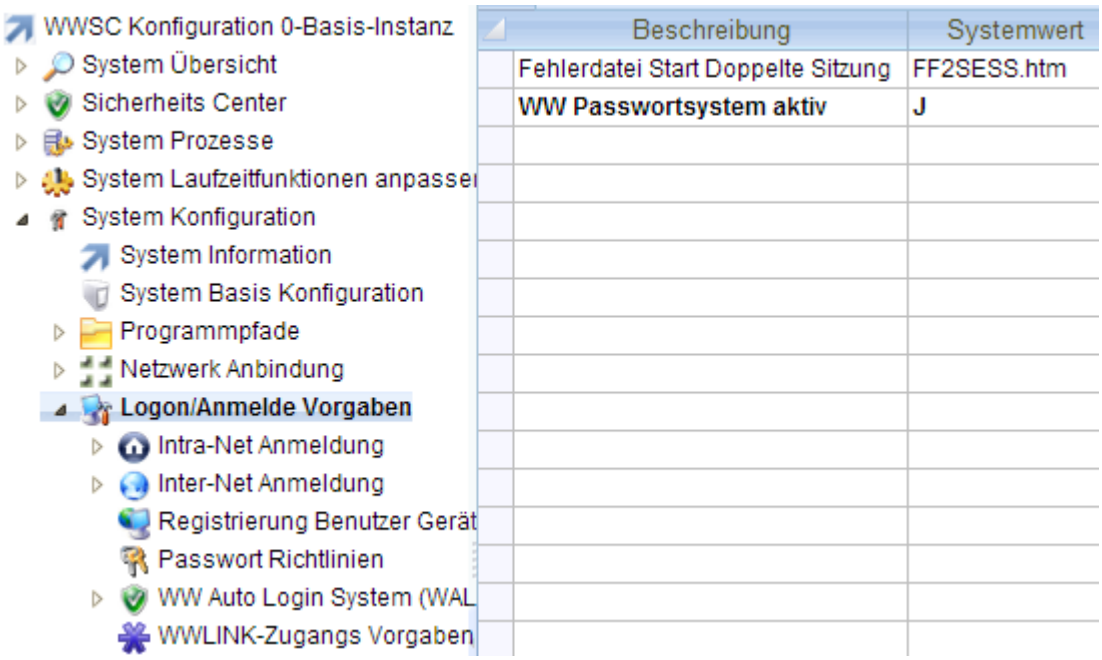
Logon-Bildschirm Intern-Benutzer

- Beschränkung der Anmelde Informationen (Auswahlfenster, Benutzerstatus)
- Anmeldung mit Nick-Name, eMail-Adresse, Benutzer-Nummer
- Individuelle Anpassung und Positionierung von Elementen auf dem Login-Bildschirm

Aktivieren des WW-Login-Systems

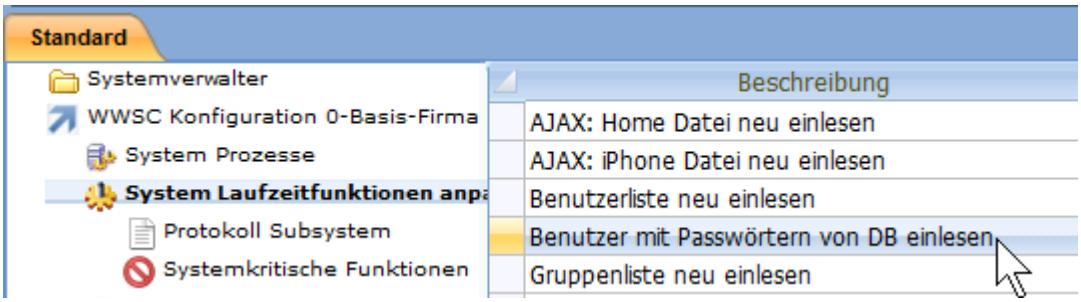
Nach erfolgter Anmeldung im Konfigurationsbereich des System-Cockpit gibt es im Bereich System-Konfiguration > Logon-Vorgaben die folgenden Parameter für die Konfiguration des WW-Login-Systems.

Um das WW-Server Passwort-System zu aktivieren muss der Systemwert **WW Passwortsystem aktiv** (wie unten gezeigt) auf 1 gesetzt werden.



Nach erfolgter Aktivierung wird die Anmeldung- und Benutzerprüfung nicht mehr über den WW-System-Server sondern direkt vom WW-Server durchgeführt. Bei einer Ersteinrichtung ist es möglich die aktuellen Benutzer (intern und public) sowie deren Passwörter in den WW-System-Server zu übernehmen. Hierzu gibt es im **Bereich System Laufzeitfunktionen anpassen** den Befehl *Benutzer mit Passwörtern von DB einlesen.*

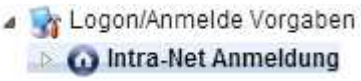
Damit ist es möglich alle im Datenbankbereich vorhandenen Benutzer (intern und public) und deren Passwörter in die WW-Server Datenbank zu Übernehmen.



Definition von IntraNet und InterNet

IntraNet ▸ Sicherer Netzwerkbereich, Firmennetzwerk, VPN-Tunnel geschützt Benutzer Zugriff

InterNet ▸ Alle übrigen Netzbereiche, Zugriff von Netzsegmenten ohne Sicherheit / Tunnel usw.



Um eine Unterscheidung zwischen sicherem und unsicheren Netzwerkbereichen vornehmen zu können, ist es möglich mit Hilfe eines SecureNet IntraNet Eintrages "Sichere Netzwerkbereiche" zu definieren.

SecureNet IntraNet Bereich

Mit dem Parameter "IntraNet Definition SecureNetArea können bis zu 20 Netzsegmente angegeben werden, welche das sichere Netz beschreiben.

Beschreibung	Systemwert
CSS-Datei für Anmeldebilsdchirm	**INTRANET**
IntraNet Anmeldung aktiv	1
Benutze IntraNet Anmeldung auch ohne IntraNet SecureNetArea	0
IntraNet Definition SecureNetArea	**192.168.13.130 192.168.14**

Diese Definition wird in der Folge auch für Prüfungen im Bereich des Auto-Login-Systems (WALIS) und der Zugriffsprüfung/Steuerung verwendet.

IntraNet Anmeldemaske aktiv

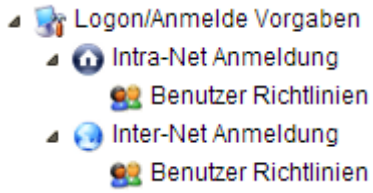
Mit dem Parameter IntraNet Anmeldung aktiv wird der Intra-Net Anmeldebildschirm aktiviert. Dieser Parameter sollte immer aktiv sein.

Auslieferungszustand IntraNet Einstellung

Falls man keine IntraNet Definition angegeben hat Auslieferungszustand, so wird mit dem Parameter "Benutze IntraNet Anmeldung auch ohne IntraNet SecureNetArea" der Zugriff wie bisher auf die IntraNet Login-Maske sichergestellt.

Benutzer-Richtlinien für IntraNet und InterNet

Für jeden Bereich (IntraNet/InterNet) können die Benutzer-Richtlinien getrennt voneinander angegeben werden. Sie finden die Benutzer Richtlinien unterhalb der Entsprechenden Logon/Anmelde Vorgaben für IntraNet + InterNet.



Im Bereich der Benutzer-Richtlinien können Vorgaben für die Hilfs- und vorhandenen Benutzerinformationen in der Logon/Anmelde-Maske gemacht werden. Hier hat man die Möglichkeit je nach Anwendungsfall mehr oder weniger Informationen auf der Anmeldemaske zu platzieren und so die Sicherheit der Informationen zu Erhöhen.

Beispiel: Es ist nicht Ratsam die Benutzerauswahl in einem öffentlichen Zugang anzuzeigen. Ebenso ist die Anmeldung mit der Benutzer-Nummer nur im IntraNet zu verwenden.

Durch aktivieren der entsprechenden Einträge mit einer 1 kann die entsprechende Funktion freigeschaltet werden.

Benutzernummer

Hier kann vorgegeben werden ob sich die Benutzer mit ihrer internen Benutzer-Nummer anmelden dürfen.

IntraNet: Standard, InterNet:Aus

Benutzer-Nickname

Hier kann erlaubt werden ob der Benutzer mit einer eigenen Kennung sich anmelden kann.

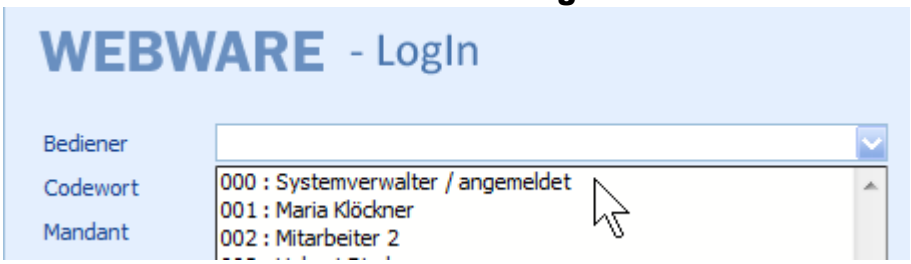
IntraNet: Standard, InterNet: Standard

eMail-Adresse

Hier kann erlaubt werden ob der Benutzer sich mit der hinterlegten eMail-Adresse anmelden darf.

IntraNet: Standard, InterNet:Standard

Auswahlfenster für Benutzerkennung



Hier kann festgelegt werden ob die Auswahlliste für Benutzer angezeigt werden darf.

IntraNet: Standard, InterNet:Aus

Anmeldestatus in Auswahlfenster anzeigen

Falls das Auswahlfenster für Benutzer angezeigt werden darf, kann hierüber festgelegt werden ob der Anmeldestatus der Benutzer angezeigt werden soll (siehe oben Systemverwalter / angemeldet).

IntraNet: Standard, InterNet:Aus

Passwort-Richtlinien

Mit den Passwort Richtlinien ist es möglich das Passwortsystem individuell an die Bedürfnisse des Anwenders anzupassen. Das Systemcockpit erlaubt dabei die Vorgaben hierarchisch entweder für das Gesamtsystem, oder aber für Firmen/Mandanten vorzugeben.

Beschreibung	Systemwert
Erlaube leere Passwörter	1
Intern Passwort bei Leer	********
Passwort erneuern nach Anzahl Tagen	**179**
Public Erlaube leere Passwörter	1
Public Passwort bei Leer	********
Passwort erneuern nach Anzahl Tagen	90
Mindestlänge für Passwörter	4
Maximallänge für Passwörter	32
Passwörter müssen Zahlen enthalten	1
Passwörter muss Groß/Kleinschreibung enthalten	1
Passwörter darf Groß/Kleinschreibung	1
Passwort Falscheingabe, Anzahl bis Sperrung	3
Passwort Falscheingabe, Wartezeit-Modus	1
Neues Passwort, Verbotene Anzahl Wiederholung	3
Erlaubte Zeichen in Passwort	ABCDEFGHIJKLMNOPQRST

Intern Passwort bei Leer

Hier kann ein Passwort vorgegeben werden das für die Erstanmeldung der internen Benutzer gültig ist. Hierzu muss der Schalter „Erlaube leere Passwörter“ auf 1 gesetzt werden. Der Benutzer wird dann direkt nach erfolgreicher Anmeldung zur Eingabe eines eigenen Passwortes aufgefordert.

Public Passwort bei Leer

Hier kann ein Passwort vorgegeben werden das für die Erstanmeldung der Public Benutzer gültig ist. Hierzu muss der Schalter „Public Erlaube leere Passwörter“ auf 1 gesetzt werden. Der Benutzer wird dann direkt nach erfolgreicher Anmeldung zur Eingabe eines eigenen Passwortes aufgefordert.

Festlegung von Passwort Gültigkeitsdauer (intern)

Hier kann vorgegeben werden nach wie viel Anzahl Tagen ein Passwort erneuert werden muss. Wird die Dauer erreicht, muss der Benutzer, nach erfolgreicher Anmeldung, ein neues Passwort eingeben.

Mindestlänge für Passwörter

Hier kann die Mindestlänge für ein Passwort vorgegeben werden. Dieser Parameter dient im Passwortändern Dialog für die Prüfung auf die Mindestlänge des Passwortes.

Maximallänge für Passwörter

Hier kann die Maximallänge für ein Passwort vorgegeben werden.

Passwörter müssen Zahlen enthalten

Hier kann festgelegt werden, ob ein Passwort auch eine Zahl enthalten muss. Dieser Parameter dient im Passwortändern Dialog für die Prüfung eine Zahl vorhanden sein muss.

Passwort muss Groß/Kleinschreibung enthalten

Hiermit kann vorgegeben werden ob im Passwort Groß- und Kleinschreibung vorhanden sein muss. Dieser Parameter dient im Passwortändern Dialog für die Prüfung ob eine gemischte Schreibweise erfüllt ist.

Passwörter darf Groß/Kleinschreibung

Wenn dieser Parameter aktiviert ist, so wird die Groß-/Kleinschreibung ignoriert.

Passwort Falscheingabe, Anzahl bis Sperrung

Hier kann vorgegeben werden wie oft ein Benutzer ein falsches Passwort eingeben darf, bis der Zugang für diesen Benutzer gesperrt wird. Wird vom Benutzer in der Zwischenzeit das Passwort richtig eingegeben, so wird der Fehlerzähler zurückgesetzt.

Erlaubte Zeichen im Passwort

Vorgabe von möglichen Zeichen die ein Passwort enthalten darf. Hier können bestimmte Zeichen für die Eingabe im Passwortdialog gesperrt werden.

Neues Passwort, Verbotene Anzahl Wiederholung

Wenn ein Benutzer ein neues Passwort vergeben will, wird geprüft ob das Passwort bereits einmal für diesen Benutzer vorgegeben wurde. Hier kann die Anzahl von Passwörtern vorgegeben werden, die als letztes gesetzt wurden, und die nicht gleich dem neu gesetzten Passwort sind.

Dadurch hat man die Möglichkeit die Dauerverwendung immer des gleichen Passwortes einzuschränken.

Passwort Anfordern / zurücksetzen Funktion

Es besteht die Möglichkeit für Ihren WEBWARE-Server eine Komfort-Funktion im Passwort Bereich zu aktivieren. Dabei können Sie Benutzern die ihr Passwort nicht mehr wissen anbieten sich ein neues Passwort auf eine zuvor festgelegte eMail-Adresse zu senden zu lassen.

Sie finden die zugehörigen Systemwerte im Bereich Logon/Anmelde Vorgaben > Passwort Richtlinien > Passwort Reset Funktionen.

Aktuell wird vom WEBWARE-Server nur die eMail Kommunikation unterstützt. In einer weiteren Ausbaustufe wird die SMS-Kommunikation noch nachgerüstet.

Beschreibung	Systemwert
Benutzer darf Passwort zurücksetzen	**J**
Passwort per eMail zusenden erlaubt	**J**
Passwort per SMS zusenden erlaubt	0
Public Benutzer darf Passwort zurücksetzen	**J**
Normale Benutzer darf Passwort zurücksetzen	**J**
Public Benutzer dürfen nur im IntraNetz zurücksetzen	0
Normale Benutzer dürfen nur im IntraNetz zurücksetzen	0

Damit das Zusenden von neuen Passwörtern funktioniert müssen folgende System-Werte konfiguriert werden.

- Passwort-Rücksetze Funktion aktivieren
- Benutzer/Public-User und Internet/Intranet Bereich müssen aktiviert sein
- Benutzer/Public-User muss einen eMail Adresse hinterlegt haben.
- eMail-Sub-System muss konfiguriert
- Benutzer eMails muss aktiviert sein
- "Benutzer Neues Passwort"-Meldung muss aktiviert sein

(Weitere Informationen zum Bereich eMail finden Sie in der Dokumentation WMS Messaging System.pdf)

Grundsätzlich wird beim Zurücksetzen so vorgegangen. Das System prüft nach Falscheingabe des Passwortes für einen Benutzer ob für diesen die Rücksetzfunktion angewendet werden kann. Ist dies möglich so wird ein Zufallspasswort in der Länge der minimalen Passwortlänge erzeugt, und im Benutzerstammsatz dieses hinterlegt. Dann wird eine eMail/SMS an den Benutzer mit Serveradresse und Passwort versendet. Bei der nächsten Anmeldung muss dann dieses Passwort eingegeben werden und

Benutzer darf Passwort zurücksetzen

Mit diesem Parameter wird die Zurück Setzen Funktion aktiviert. Ist dieser Parameter nicht aktiv, so kann für diese WEBWARE-Instanz das Passwort nicht zurückgesetzt werden.

Passwort per eMail zusenden erlaubt

Dieser Parameter steuert ob das zurückgesetzte Passwort per eMail zugesendet werden darf. Ist dieser Parameter aktiv so wird geprüft ob der Benutzer eine eMail-Adresse hinterlegt hat. Wenn ja so wird im Fall der Passwortfalscheingabe der Passwort vergessen ? Link angezeigt.

Passwort per SMS zusenden erlaubt

Diese Option hat bis zur Fertigstellung des SMS-Sub-System keine Funktion. Hiermit kann man die SMS-Zustellung des Passwortes erlauben.

Public Benutzer darf Passwort zurücksetzen

Mit diesem Parameter können Sie das Passwort zurücksetzen für Public-Benutzer aktivieren. Ist dieser Wert aktiv so dürfen Public-Benutzer ihr Passwort zurücksetzen. Einzige Ausnahme kann durch den Parameter "Public-Benutzer dürfen nur im IntraNetz zurücksetzen" entstehen.

Normale Benutzer darf Passwort zurücksetzen

Mit diesem Parameter können Sie das Passwort zurücksetzen für normale Benutzer aktivieren. Ist dieser Wert aktiv so dürfen Normale-Benutzer ihr Passwort zurücksetzen. Einzige Ausnahme kann durch den Parameter "Normale Benutzer dürfen nur im IntraNetz zurücksetzen" entstehen.

Public Benutzer dürfen nur im IntraNetz zurücksetzen

Hiermit können Sie die Rücksetze Funktion für Public Benutzer auf den Intra-Netz Bereich begrenzen. Wie Sie den IntraNetzt/IntraNetzt Bereich definieren finden Sie im Handbuch WW-DOKU-WWS-Security-System im Bereich: *Konfiguration des Intra- und Internet für Login-System)*

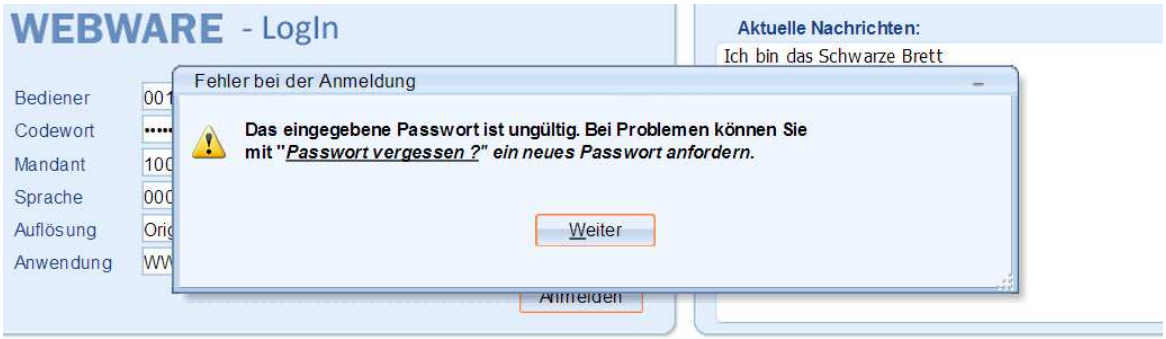
Normal Benutzer dürfen nur im IntraNetz zurücksetzen

Hiermit können Sie die Rücksetze Funktion für Normale Benutzer auf den Intra-Netz Bereich begrenzen. Wie Sie den IntraNetzt/IntraNetzt Bereich definieren finden Sie im Handbuch WW-DOKU-WWS-Security-System im Bereich: *Konfiguration des Intra- und Internet für Login-System)*

Wie funktioniert das Passwort Zurücksetzen ?

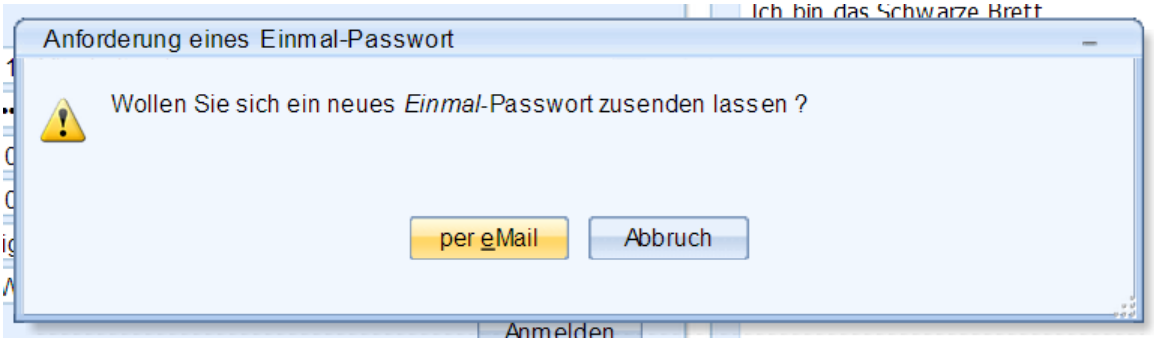
Im folgenden Login habe ich das falsche Passwort eingegeben.

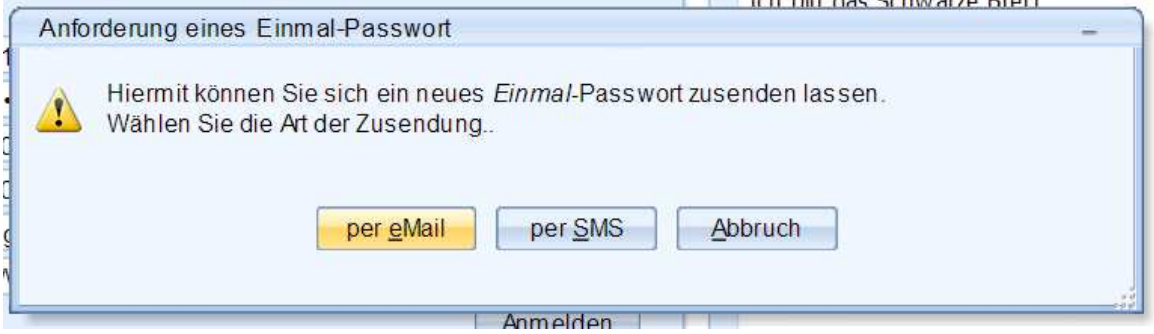
Wenn Sie alle Systemparameter für das Passwort zurücksetzen aktiviert haben, so wird dem Benutzer erst nach Falscheingabe des Passwortes ein Hinweis angezeigt:



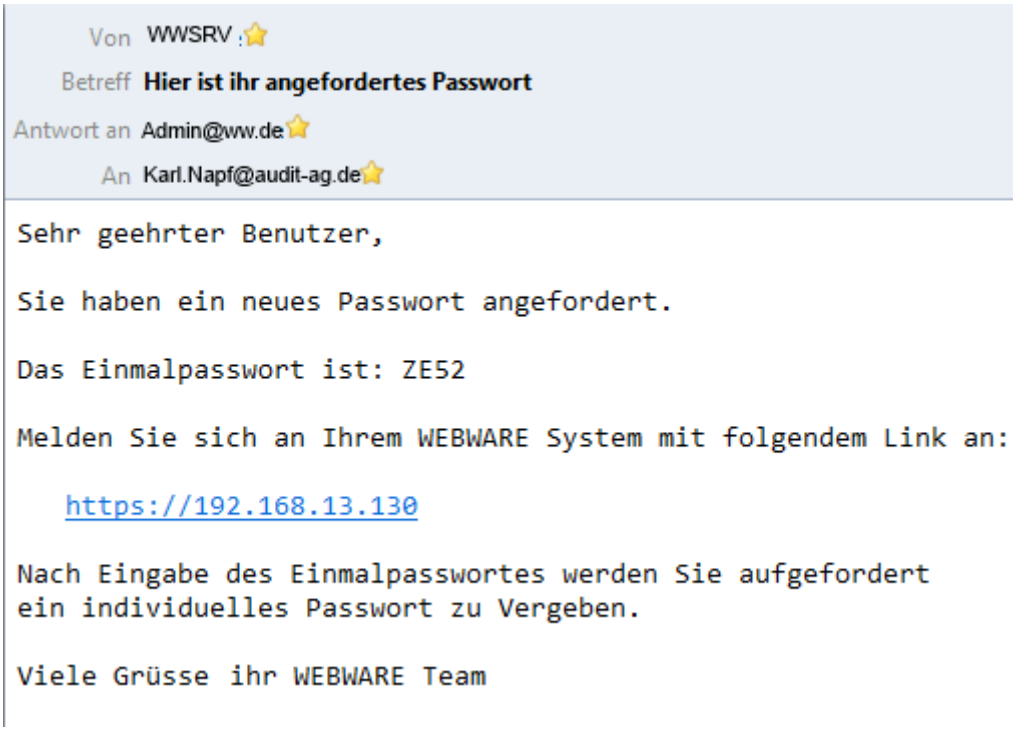
Nach schließen des Hinweises wird oberhalb des Anmelden Knopfes der "Passwort vergessen?" Link angezeigt.

Durch Klick auf den "Passwort vergessen?"-Link wird eine Abfrage angezeigt ob und mit welchem Kommunikationssystem er das Passwort zugesendet haben will.





Die Kommunikation über SMS ist aktuell noch nicht Bestandteil des WEBWARE-Servers. Nach Klick auf eMail wird dann die zugehörige Meldung



Bei der nächsten Anmeldung muss der Benutzer dann das Einmal-Passwort (ZE52) eingeben. Wird dies richtig eingegeben, so muss sofort ein neues Passwort vom Benutzer festgelegt werden.

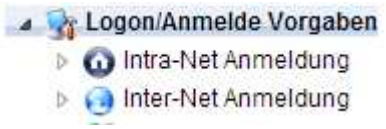
Das Ganze funktioniert genauso beim Public-Benutzer Login-Bildschirm.

Konfiguration der Anmelde/Login-Bildschirme

Es gibt 3 Arten von Anmelde/Login Bildschirme.

- IntraNet Anmeldemaske
- InterNet Anmeldemaske
- Public Worker Anmeldemaske

Konfiguration der Anmelde/Login-Bildschirme Intra/InterNet



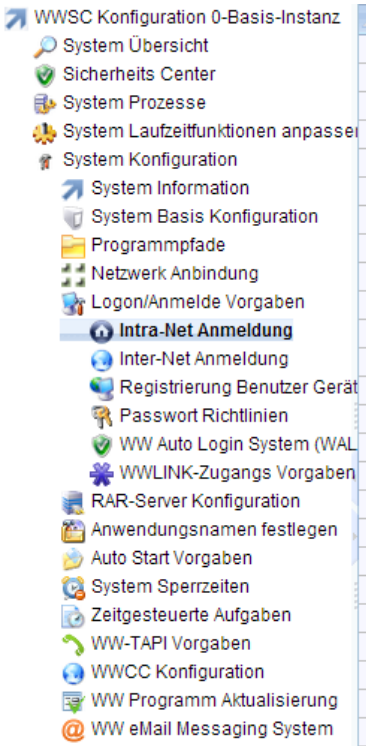
Sie haben die Möglichkeit getrennte Anmelde/Login-Bildschirme für IntraNet und InterNet zu definieren.

Sie finden die jeweiligen Paramter in den jeweiligen Bereichen.

Dadurch können Sie individuelle Bildschirme für jeden Netzbereich definieren. Durch Vorgabe einer CSS-Datei für InterNet und IntraNet können Sie die Oberfläche komplett umgestallten, und auch für die laufende Anwendungen Änderungen an der CSS-Definition der WEBWARE vor nehmen.

Die Position der Eingabefelder und Informationen sowie die Feldauswahl und das Verhalten der Anmelde-Maske können Sie frei definieren.

Im Bereich Logon/Anmelde Vorgaben ist es möglich die Positionierung von Elementen des Logon-Bildschirms zu verändern. Dadurch und mit den Benutzer Richtlinien kann so der Anmelde-Bildschirm individuell angepasst werden.



Beschreibung	Systemwert
X-Position Anmelde-Maske	62
Y-Position Anmelde-Maske	188
Mandantenauswahl einfügen	1
Mandantencodewort einfügen	0
Sprachauswahl einfügen	1
Anwendungsauswahl einfügen	0
News-Bereich einfügen	1
X-Position News-Bereich	468
Y-Position News-Bereich	-27
Breite News-Bereich	304
Höhe News-Bereich	186
X-Position Server-Zertifikat	-4
Y-Position Server-Zertifikat	187
X-Position Client-Zertifikat	478
Y-Position Client-Zertifikat	187
Lokale Anmeldung, Schalter Erweitertes Menü aktiv	**1**
Skalierungs Auswahl einfügen	**J**
Vorgabe Skalierungsmode	3
CSS-Datei für Anmeldebilsdchirm	**INTRANET**
IntraNet Anmeldung aktiv	1
Benutze IntraNet Anmeldung auch ohne IntraNet SecureNetArea	0
IntraNet Definition SecureNetArea	**192.168.13.130 192.168.14**
Neue Desktop Geräte muss Admin freigeben	**N**
Neue Tablet Geräte muss Admin freigeben	**J**
Neue Phone Geräte muss Admin freigeben	**J**

Konfiguration des Login-Bildschirmes Internet – Benutzer

Der Anmeldebildschirm besteht aus einer Maske, dem News-Bereich, der Mandanten-Auswahl, der Sprachauswahl, sowie die Anwendungsauswahl.

X-Position / Y-Position Anmeldemaske

Hier kann die Eingabe-Maske auf der Anmeldemaske positioniert werden. Die Maske besteht aus den Eingabefeldern, sowie dem Anmelden Knopf.

Mandantenauswahl einfügen

Mit aktiviertem Wert (1) wird die Zeile Mandant [ ] in die Anmeldemaske eingefügt.

Mandantencodewort aktivieren

Falls der Zugang über ein zusätzliches Mandantencodewort gewünscht ist, so kann mit dem Parameter „Mandanten-Codewort einfügen“ die Eingabe entsprechend angepasst werden.

Sprachauswahl einfügen

Hier kann die Sprachauswahl Zeile in die Anmeldemaske eingefügt werden.

Anwendungsauswahl einfügen

Hier kann die Anwendungsauswahl in den Anmeldebildschirm eingefügt werden. Diese ist per Default aus, und sollte nur für Tests aktiviert sein.

News-Bereich einfügen

Hier kann entschieden werden ob der News-Bereich (oben rechts) im Anmeldefenster angezeigt wird. Ebenso kann die X/Y-Position sowie Breite und Höhe vorgegeben werden.

Server-Zertifikat

Hier kann die X/Y-Position für die Anzeige des Server-Zertifikat im Anmeldebildschirm vorgegeben werden.

Aktivierung der Programmauswahl über den Login-Bildschirm

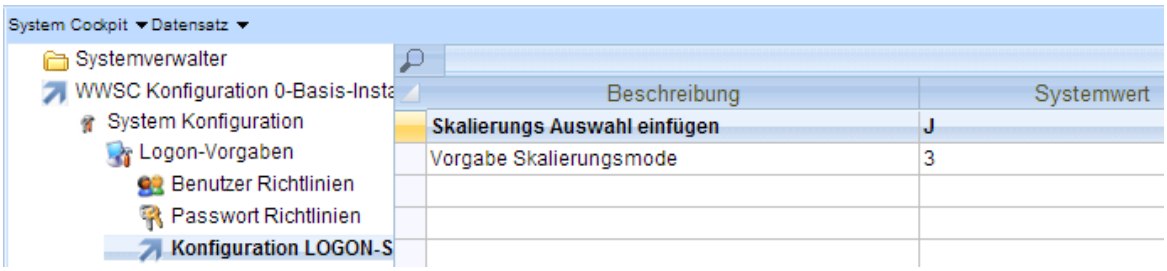
Wenn von einer hinterlegten IP-Adresse (Lokale WW-Server IP-Adresse, bzw. sichere freigegebene IP-Adresse) eine Verbindung zum WW-Server aufgebaut wird, so wird automatisch die Anwendungsauswahl eingeblendet. Damit ist es möglich für Administratoren direkt das WW-System-Cockpit zu Starten. Dadurch entfällt für diesen Fall der Sonderauswahl Bildschirm.

Aktivieren Zoom-Funktion über Login-Bildschirm

Der Login-Bildschirm passt sich automatisch der Bildschirmgröße an. Zusätzlich ist es möglich eine Zoom-Auswahl in den Login-Bildschirm zu Integrieren

Über die Login-Konfiguration ist es möglich die Skalierungsauswahl zu aktiveren, sowie den Standard-Zoom-Faktor festzulegen. Diese Funktionen werden aktuell jedoch nur von WEBWARE 1.5 unterstützt.

Im Standard wird dieses Eingabefeld nicht angezeigt, hierzu muss im System-Cockpit der Parameter "Skalierungs Auswahl einfügen" wie auf dem Bild unten aktiviert werden.



Es ist auch möglich den Standardwert der als Vorgabewert verwendet werden soll mit dem Parameter "Vorgabe Skalierungsmode" festzulegen.

Folgende Werte sind hier möglich:

0: Orginal Anzeigegröße
1: Anzeige Skaliert Maximal (800x600)
2: Anzeige Skaliert groß (1024x768)
3: Anzeige Skaliert Standard (1280x1024)
4: Anzeige Skaliert klein (1600x1280)
5: Anzeige Skaliert minimal (1920x1536)

Zoom-Funktion in der Anwendung (ab WW 1.5)

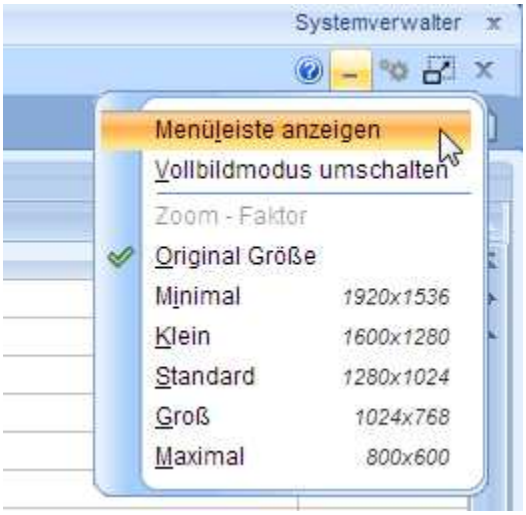
Hier kurz eine Erklärung der Zoom-Funktion, wie sie in der Anwendung verfügbar ist. Um Den Zoom-Faktor in der Anwendung umschalten zu können, wurde das Hauptmenü um den Bereich Ansicht erweitert.

Dort sind nun die möglichen Ansichtsoptionen zusammengefasst.

- Menüleiste anzeigen

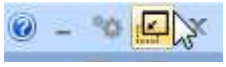
  Hiermit kann die Anzeige der Menüleiste umgeschaltet werden.

Das umschalten war zuvor über den Schnelltaste  /  möglich.
Hier ist nun ebenfalls der Aufruf des Ansicht-Menüs im Schnellzugriff vorhanden.



- Vollbildmodus umschalten

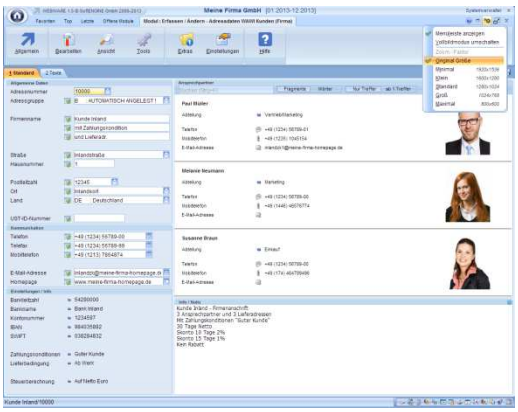
  Hiermit kann die Anzeige zwischen Vollbild und Fenstermodus umgeschaltet werden. Dies ist nur bei Browsern wie Chrome/Safari/FireFOX möglich. Der Microsoft Browser Internet Explorer bietet diese Funktion.

  Das Umschalten ist ebenfalls über die Schnelltaste  ,  möglich.

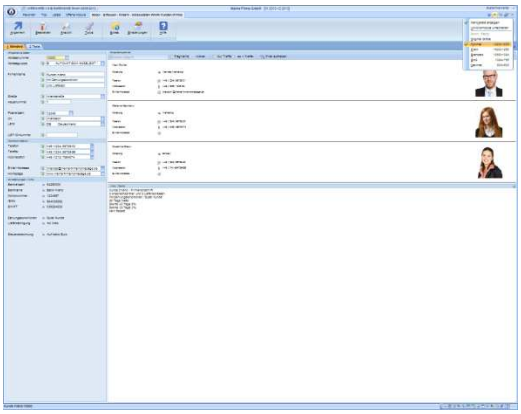
- Zoom Funktion

  Mit der Zoom Funktion kann die Anzeigeauflösung, also die Größe wie die einzelnen Bildschirmelemente dargestellt werden, an Ihre Bedürfnisse angepasst werden.

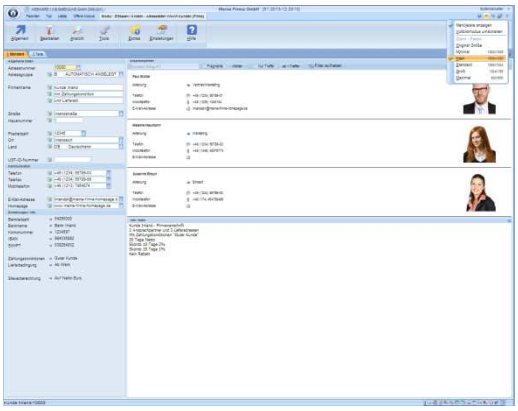
Orginal



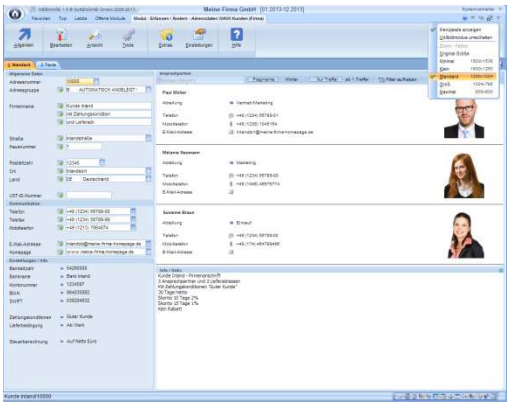
Minimal



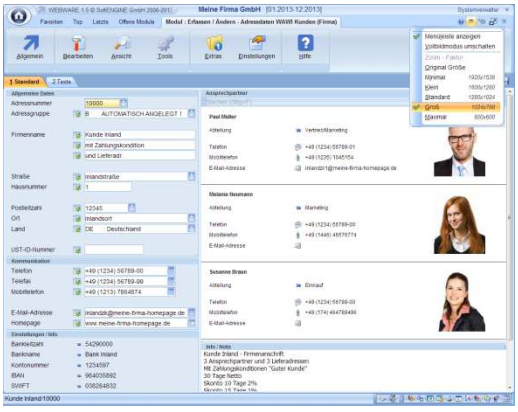
Klein



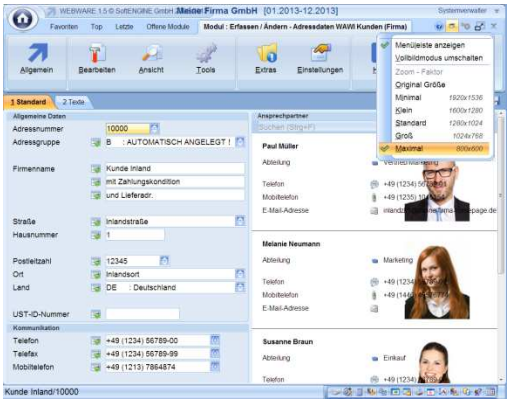
Standard



Groß



Maximal



In den Beispielen oben wurde immer die gleiche Anzeigegröße verwendet. Man sieht auch in den unteren Beispielen das die Anzeigefläche nicht ausreicht um den Kompletten Bildschirm da zu stellen.

In diesem Fall wird eine Scrollbar zum verschieben des Bildinhaltes eingeblendet.

CSS-Datei für Anmeldebildschirm

Hier können Sie eine eigene CSS-Datei bzw. die vorhandene anpassen. Dieses CSS-Datei dient dazu den Anmeldebildschirm und auch darüber hinaus die WW Anwendung an Ihre Bedürfnisse anzupassen.

Achten Sie darauf die CSS-Datei mit genau 8 Zeichen anzugeben und die Dateiendung .CSS nicht anzugeben.

Für den IntraNet Bereich ist de Standardname INTRANET und für den InterNet Bereich INTERNET. Die Datei wird vom WW-Server im Pfad bin\home\css gesucht und ausgeliefert.

Falls Sie Änderungen an der Datei vornehmen (BSPL: BIN\HOME\CSS\INTERNET.CSS) so werden diese bei Neuanmeldung eines Benutzers sofort wirksam.

Beispiel für eine Änderung:

IntraNet mit einem Grünen und InterNet mit einem roten Rahmen ausliefern:

Anpassen bzw einfügen in Datei CSS\INTRANET.CSS

```
#APPLOGONWIN
{
        background-color: green;
}
```

Anpassen bzw. einfügen in Datei CSS\INTERNET.CSS

```
#APPLOGONWIN
{
        background-color: red;
}
```

Bei Fragen über die Konfiguration, wenden Sie sich bitte an die WEBWARE Techniker.

Konfiguration des Login-Bildschirmes Public – Benutzer 1.x

Die Konfiguration des Public-Benutzer Anmeldebildschirm kann durch Anpassung der HTML-Seite \BIN\HOME\PUBLIC.HTM erfolgen. Die Datei kann Individuell an die Benutzerbedürfnisse angepasst werden. Wichtig ist hier aber das der Eintrag form action=…..) nicht geändert wird.

```
<form autocomplete=”ON” action="XXXXXXXXXX/WWPUBLOG" name="WWPUBLOG" method="POST" onsubmit="var f1=window.open('#', 'WWWIN','0','width=900,height=490,top=5,left=5,scrollbars=yes,location=no,directories=no,status=no,menubar=no,toolbar=no,resizable=yes'); f1.focus();" target="WWWIN">
```

So sieht der Standardanmeldedialog für Public-user der WEBWARE aus:

Dieser ist leicht anzupassen. Die Seite selbst muss nicht vom WEBWARE-Server ausgeliefert werden. So ist es möglich auch von anderen Web-Seiten aus, direkt den Login für die WW einzubauen.

!!! Achten Sie darauf das der Zugang zur WW und auch die Seite in der der Anmeldebildschirm integriert wird VERSCHLÜSSELT übertragen wird. !!!

Konfiguration Login Public-Benutzer mit Tablet-Option

Die Konfiguration des Public-Benutzer Anmeldebildschirm kann durch Anpassung der HTML-Seite \BIN\HOME\PUBLICT.HTM erfolgen. Diese Datei hat eine Erweiterung für Tablet eingebaut. Hierbei kann mit einem Schalter die "Optimierung für Tablet" bereits im Zugangsbildschirm gewählt werden. Die Datei kann Individuell an die Benutzerbedürfnisse angepasst werden. Wichtig ist hier aber das der Eintrag form action=…..) nicht geändert wird.

So sieht der Anmeldedialog mit erweiterter Tablet-Optimierungsauswahl für Public-user der WEBWARE aus:

Wird der Schalter "für Tablet optimieren" aktiviert, so wird die WEBWARE im Tablet-Modus gestartet.

WW 2.0 Public-Worker Anmelde-Seiten

EV: WWS-12521, HTML-Dateien Im Build seit 01.07.2015

Wie unter WW 1.x gibt es für die Anmeldung von Public-Workern eine vorgefertigte HTML-Datei, die Sie an Ihre Bedürfnisse anpassen können.

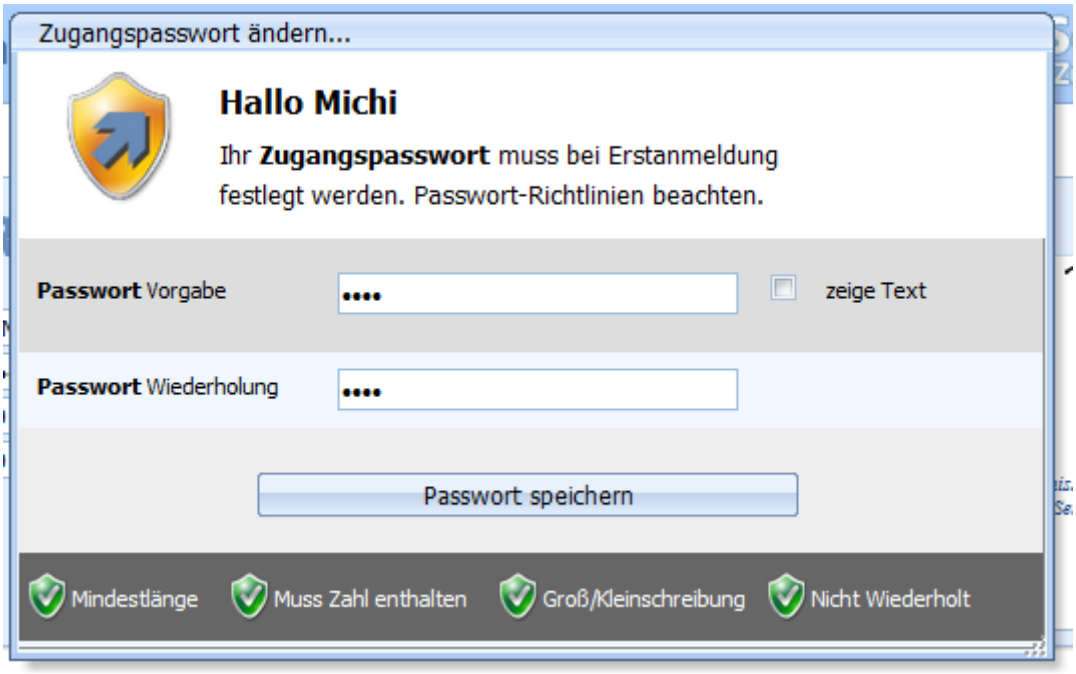
Hier gibt es 2 Einstiegs-Seiten. PUBLIC2.HTM für Normale Oberfläche ohne Auswahl von Touch-optimieren,

und PUBLICT2.htm die eine Check-Box zur Auswahl der Touch-Optimierung mitliefert.

Ziel der beiden Dateien ist es ein HTML-Formular zu füllen und damit eine neue Sitzung beim WW-Server in einem neuen Fenster anzufordern.

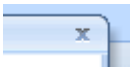
Benutzerinteraktion mit dem Anmelde- / Passwort-System

Bei aktiviertem WW-Server Anmeldesystem ändern sich für den Benutzer einige Programmabläufe.



Der neue Passwort Ändern Dialog besteht aus 4 Bereichen.

- ➔ Benutzerhinweis: Warum soll das Passwort geändert werden
- ➔ Passwort Vorgabe: Eingabe des Passwort mit Wiederholung
- ➔ Passwort speichern Knopf
- ➔ Anzeige ob die Passwortrichtlinien eingehalten sind

Der Dialog kann abhängig von der Aufrufsituation durch das eingeblendete  (X-Symbol) abgebrochen werden. Dies ist nur dann möglich wenn der Dialog aus der Anwendung heraus gestartet wurde. Bei automatischer Anzeige kann der Benutzer diesen Dialog nur durch Eingabe eines neuen, gültigen Passwortes erfolgreich verlassen

Benutzerhinweis

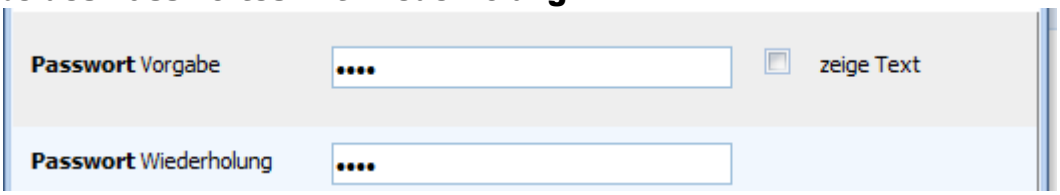
Im oberen Bereich erhält der Benutzer einen Hinweis warum er das Passwort ändern soll/muss:

➔ Neuanmeldung bzw. nach zurücksetzen des Passwortes

➔ Ändern des Passwortes aus Benutzerwunsch

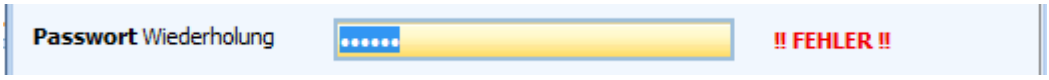
➔ Abgelaufenes Passwort

Eingabe des Passwortes mit Wiederholung



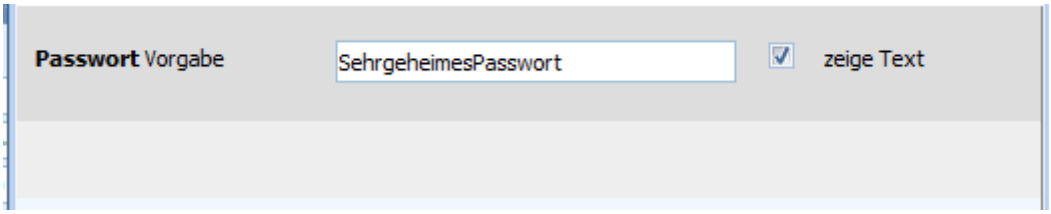
Hier kann der Benutzer im oberen Eingabefeld das Passwort vorgeben. Im unteren Feld muss er das Passwort zur Bestätigung wiederholen.

Falls das unten eingegebene Passwort abweicht erhält er hinter der Passwort Wiederholung eine Fehlermeldung (!! FEHLER !!)



Falls die Eingabe im Klartext erfolgen soll, kann der Benutzer durch setzen des Schalters 

die Klartexteingabe aktivieren.



Rückmeldung über Passwort-Richtlinien

Im unteren Bereich werden bei der Eingabe abhängig von den vorgegebenen Passwortrichtlinien Hinweise ausgegeben. Der Benutzer erfährt so bereits bei der Eingabe (nach kurzer Verzögerung) ob das Passwort den Passwort-Richtlinien entspricht.

Wie die Anzeige aktiviert werden kann, ist weiter oben unter Passwort-Richtlinien beschrieben.

	Fehler nicht eingehalten	OK Richtlinie eingehalten
Mindestlänge eingehalten		
Passwort enhält Zahl		
Groß/Kleinschreibung		
Passwort Wiederholung		

Erstanmeldung eines Benutzers

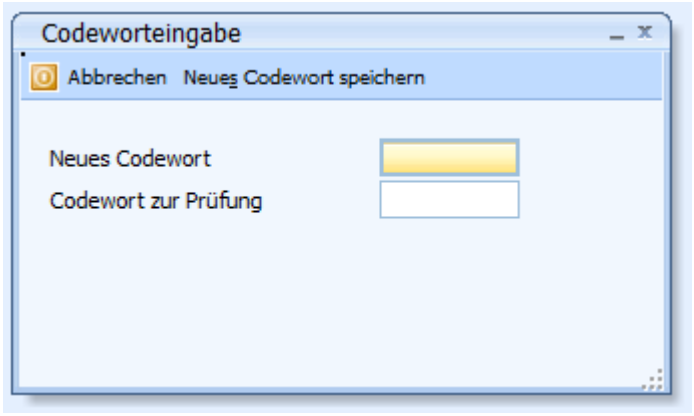
Zuerst wird er bei Erstanmeldung am System zur Vergabe eines neuen Passwortes aufgefordert. Der Benutzer kann hier dann

Ändern des Passwortes aus dem Programm heraus

Der Passwortdialog ist aus dem Programm Menü

oder über die Schnellsuche (Eingabe von Co[dewort]) zu finden.

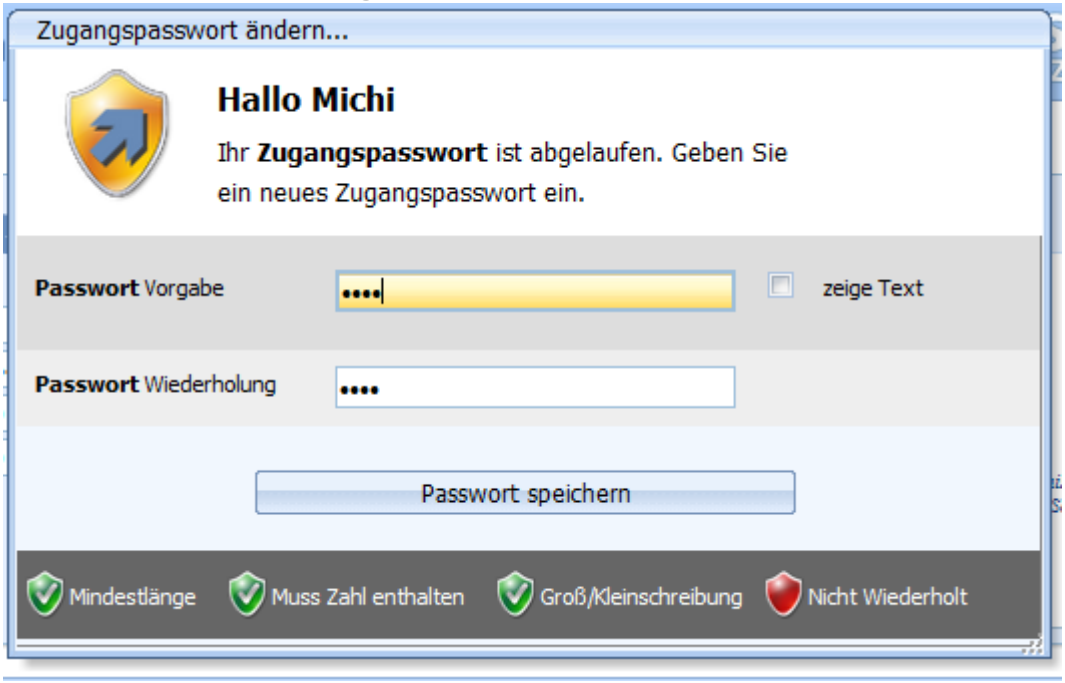
Der alte Passwort-Dialog



wird bei aktiviertem WW-Server Anmeldesystem mit dem folgenden Passwortdialog ersetzt.

Der Benutzer erhält bei Eingabe des Passwortes im unteren Bereich durch die Hinweistexte und Bilder angezeigt ob das eingegebene Passwort den Passwortrichtlinien entspricht.

Erneuern eines abgelaufenen Passwortes



Wird bei der Anmeldung eines Benutzers erkannt dass das Passwort abgelaufen ist, so wird er mit diesem Dialog zur Eingabe eines neuen Passwortes aufgefordert.

WEBWARE Server Administratoren

Die WEBWARE bringt schon vorkonfigurierte Administratoren mit. Diese können verwendet werden um spezielle administrative- bzw Konfigurations- Aufgaben ohne Verwendung einer WW-Anwendung, also nur mit einer WEBWARE-Server Sitzung durchzuführen. 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-Adminstratoren 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 !!

Eine Anmeldung ist nur lokal von dem Rechner möglich auf dem der WEBWARE-Server ausgeführt wird.

Die System-Admin's haben dabei unterschiedliche Rechte.

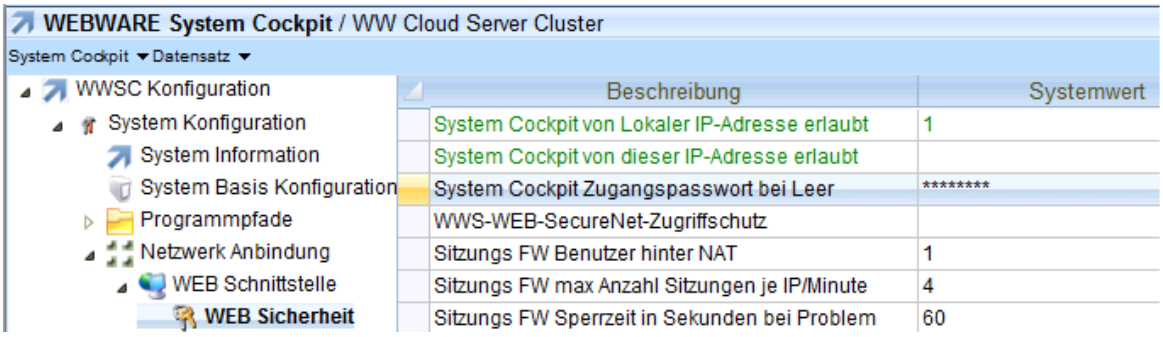
- Firmen.admin@sc.ww.de (System-Übersicht aktuelle Instanz)
- Global.admin@sc.ww.de (System-Übersicht + Administration Übergreifend)
- Server.admin@sc.ww.de (Gleich wie Global abhängig von Konzern/Cooperation/Cloud)

Diese System-Konfiguratioren

- 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)

Änderung von System-Vorgaben System-Cockpit

Der Zugriffsschutz für das System-Cockpit wird im Bereich WEB Sicherheit konfiguriert.



Hier können Sie als Konfiguration-Admin die grünen Vorgabeparameter ändern, um zum Beispiel das Masterpasswort für die Server-Admins zu ändern. Ebenso können Sie hier vorgeben ob die Anmeldung auch von einer weiteren IP-Adresse erlaubt sein soll, sowie den Lokalen Zugriff auf das System-Cockpit abschalten.

WEBWARE Front Line Server (WWFLIS)

Der WEBWARE Front Line Server kurz WWFLIS ist dafür zuständig die Netzwerkverbindungen des WEBWARE-Servers ins Internet bereit zu Stellen. In der aktuellen Ausbaustufe stellt der WWFLIS im Fall das Netzwerkzugangspunkte nicht vom WW-Server verwendet werden eine Hinweisseite für Benutzer bereit. Der WWFLIS arbeitet mit dem WW-Servern auf einem Rechner-System zusammen und erkennt wenn Netzwerk-Zugangspunkte von den WW-Servern nicht mehr verwendet werden, so dass eine sofortige Benutzer Hinweisseite bei Nichterreichbarkeit des WW-Servers angezeigt werden kann.

(Die Hinweisseite kann Individuell angepasst werden, die Texte werden dynamisch eingefügt)

Dabei hostet ein WWFLIS, der als Dienst oder Consolenprogramm gestartet werden kann, alle Zugangspunkte von einem oder mehreren WW-Servern.

Wir unterscheiden 2 Arten von WWFLIS.

- WWFLIS als Rückfall System

  WWFLIS.EXE springt bei Absturz, oder Netzwerk-Zugangspunkt Abschaltung, ein

- WWFLIS direkt im WW-Server

  WW-Server mit gesperrtem Netzwerk-Zugangspunkt, liefert intern die WWFLIS Hinweisseite

WWFLIS als Dienst Installieren

Damit der WWFLIS direkt bei Systemstart bereit steht, lohnt es sich diesen als Dienst zu Installieren. Der WWFLIS verwendet wie der WW-Server und WW-RAR Server das WW Dienst Interface.

Der WWFLIS-Server kann wie die übrigen WW-Server mit den Parametern

WWFLIS [CONSOLE,INSTALL,REMOVE,START]

aufgerufen werden.

➔ CONSOLE

Start der bin\wwflis\WWFLIS.exe als Konsolenanwendung für Debugzwecke bzw. Testzwecke. Hierbei werden Programmausgaben direkt in einem Konsolenfenster angezeigt. Ebenso können per Tastatur Aktionen ausgeführt werden.

➔ START

Start der bin\wwflis\WWFLIS als WINDOWS-Dienst. Dies funktioniert nur wenn der Dienst bereits mit INSTALL registriert wurde.

➔ STOP

Stoppt den Start der bin\wwflis\WWFLIS.exe als Dienst falls er zurzeit aktiv ist.

➔ INSTALL

Installiert die bin\wwflis\WWFLIS.exe als Dienst unter WINDOWS/. Hierbei sollten noch manuelle Änderungen vorgenommen werden, wie zum Beispiel Eintragen eines Benutzer unter dessen Anmeldung der Server Laufen soll (Sicherheit nicht Administrator sondern Benutzerlevel).

Hier können zusätzlich 2 Parameter für Benutzername und Benutzer-Passwort übergeben werden, wenn der Dienst unter einem anderen Benutzerkonto ausgeführt werden soll.

Beim Benutzername ist darauf zu achten, dass dieser in der Domänen Schreibweise, also Rechnername und Benutzername angegeben wird. Bspl: Rechner: COMPUTER01 und Benutzer: KARL muss COMPUTER01\KARL als Benutzername angegeben werden.

WWFLIS.exe WEBWARE Front Line Server Dienst Name:
Der Name für den Dienst wird hier aus der bin\wwflis\wwflis.ini geholt (Parameter WWFLS_SERVICE_NAME). Standardmäßig ist hier " WEBWARE-FrontLineServer" vorgegeben.

➔ REMOVE

Entfernt die Startinformation des WEBWARE Servers aus der Dienste Verwaltung unter WINDOWS

Komponenten des WW Front Line Servers

Folgende Komponenten bzw. Verzeichnisse und Dateien sind im WWFLIS enthalten. Der WWFLIS wird nur im WW-Server installiert und benutzt folgende Standardverzeichnisse

- \BIN\WWFLIS (EXE des WWFLIS und Konfiguration)
- \BIN\HOME\WWFLIS (WEB-Seite mit Konstanten die ausgeliefert werden)

Konfiguration bzw. Konfigurier bare Dateien des WWFLIS

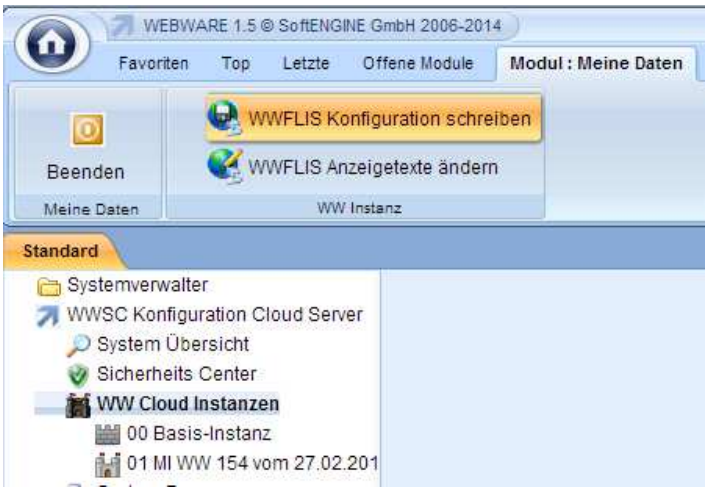
Folgende Dateien können automatisch bzw. manuell vom Administrator für Ihre Bedürfnisse angepasst werden. Die Pfade und Dateinamen sind dabei im WW-System Cockpit an Ihre Systemumgebung anpassbar.

- bin\wwflis\WWFLIS.INI Konfiguration Zugangspunkte/WWFLIS.exe
- bin\wwflis\WWFLIS.TXT Laufzeit-Texte werden vom WWFLIS zyklisch gelesen
- bin\home\wwflis\INDEX.HTM HTML-Seite die als Hinweisseite ausgeliefert wird.

WWFLIS.INI

Die WWFLIS.INI in \BIN\WWFLIS dienst zur Konfiguration des WWFLIS. Hier können bis zu 100 Netzwerkzugangspunkte mit Netzwerkadresse/Port, SSL-Informationen usw. vorgeben um den WWFLIS an Ihre Systemumgebung anzupassen. Sie finden im bin\wwflis Verzeichnis eine Hilfs-INI Datei mit Kommentaren und Beispielen. bin\wwflis\wwflis-original.ini.

Die WWFLIS.INI-Konfiguration kann dabei direkt vom WW-Server System-Cockpit heraus erstellt werden. Hierzu wird im Bereich WW-Instanzen mit dem Befehl WWFLIS Konfiguration schreiben, direkt die WWFLIS.INI im bin\wwflis Verzeichnis erstellt.




```
#  ------------------------------------------------------------
# WWFLIS Konfiguration, diese Datei kann vom WW-Server überschrieben werden !!
# WW-Instanzen > WWFLIS Konfiguration schreiben
#  ------------------------------------------------------------
#
#      WW Front Line Server (WWFLS)  INI Dateien
#      Vorgaben zum Betrieb eines FRONT-LINE-Servers der WEBWARE
#  ------------------------------------------------------------
#      Name des WWFLS für interne Kommunikation
WWFLS_NAME=WWFILS Server
#
#      Vorgabe eines Namens für WWFLS, wird als Namen als Dienst verwendet
WWFLS_SERVICE_NAME=WWFLS_SERVICE
#
#  ------------------------------------------------------------
#
#      Pfad/Datei über die die aktuellen Informationen für Anzeige
#      im Pause-Bildschirm eingelesen werden können
#
#   Falls diese Datei vorhanden ist, werden die Info's
WWFLS_INFO_FILE=.\WWFLIS.txt
#
#  ------------------------------------------------------------
#
#Vorgabe des Netzwerk-Slot's. Der WWFLS erlaubt bis zu 100 Netzwerk-Beschreibungen
#die überwacht werden. Mit der folgenden Variablen kann der Netzwerk-Slot vorbelegt
#werden.
#                          0..99
WWFLS_SET_SERVER_SLOT=0
#
#      Alle Variablen die hierunter kommen werden dann entsprechend in den gesetzten
#      Netzwerk-Slot eingetragen
#
#  ------------------------------------------------------------
#      Pfad zum WWFLS-Home-Verzeichnis, aus dem
#
WWFLS_HOMEDIR=..\home\wwflis
#
#      WWFLS-Index-Html-Datei unterhalb des WWFLS_HOMEDIR
#
WWFLS_INDEXHTML=index.htm
#
#  ------------------------------------------------------------
#      Schnittstelle die Überwacht wird
#
#      Netzwerkkarte die angesprochen werden soll
WWFLS_NETWORKCARD=localhost
#
#      Netzwerkport der überwacht werden soll
WWFLS_NETWORKPORT=443
```

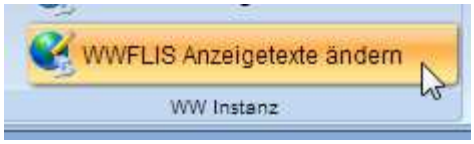
```
#
#  ------------------------------------------------------------
#      SSL Sub-System für Auslieferung eines WW-Server Zertifikates
#             SSL /  OPENSSL Integration zur     Web-Client-Seite
#
#      Soll SSL verwendet werden ZWINGEND !!
WWFLS_USE_SSL=J
#
#             Welche Version       von SSL soll verwendet werden:
#             2=SSL  2.0 /  3=SSL  3.0 /  T=TLS  1.0 /  1=     3.0  mit  Rückfall  auf
       2.0 /  D=     Dynamic TLS   1.0
WWFLS_SSL_VER=1
#
#
#             Zertifikat der       Authorisierungsbehörde mit  der                 die
Clientzertifikate unterschrieben sind
#             Datei  wird im PEM   Format benötigt
WWFLS_SSL_CA_ZERTIFIKAT=.\demozertifikat\SOFTENGINE-CERT.pem
#
#Achtung !!
#Wenn eine der Dateien nicht vorhanden ist, bzw.die Dateien   nicht  zueinander
# passen, kann der WebServer       nicht  gestartet werden.
#
#Pfad Dateiname      für den Privaten Key, muss  zum Server-Zertifikat passn
WWFLS_SSL_PRIVATEKEY=.\demozertifikat\demozertifikat-key.pem
#
#Hier kann ein Passwort für das Key-File angegeben werden, falls verschlüsselt ist
# Ein Passwort wird  erstellt in dem bei openssl.exe die Option      -des3
# angegeben wird dadurch ist       das KeyFile   geschützt
WWFLS_SSL_PASSWORD4PRIVKEY=demozertifikat
#
#Soll ein Chain-File verwendet werden ?
#Ein Chain File ist im PEM Format und enthält mehrere Zertifikate in folgender
# Reihenfolge
#       1. Server-Zertifikat
#       2. Es folgen Intermediate Zertifikate
#       3. Das CA-Zertifikat
#
WWFLS_SSL_USE_CHAIN_ZERTIFIKAT=N
#
#Pfad Dateiname  für das Server-Chaint-File-Zertifikat, wird im PEM Format erwartet
#
#WWFLS_SSL_CHAIN_ZERTIFIKAT=
#
# Pfad Dateiname     für das Server       Zertifikat,   wird im PEM   Format erwartet
WWFLS_SSL_ZERTIFIKAT=.\demozertifikat\demozertifikat.pem
#
#  ------------------------------------------------------------
#
WWFLS_INFO_GRUND="Standard Wartungsarbeiten"
#
WWFLS_INFO_DAUER="Abgeschaltet bis der Arzt kommt"
#
WWFLS_INFO_BIS_DATUM=13.12.2014
#
WWFLS_INFO_BIS_UHRZEIT=14:30
#
WWFLS_INFO_ADMIN="Bei Fragen bitte Tel: 06346/992299 oder eMail WWS@WassnJetzt.de"
#
#  ------------------------------------------------------------
```

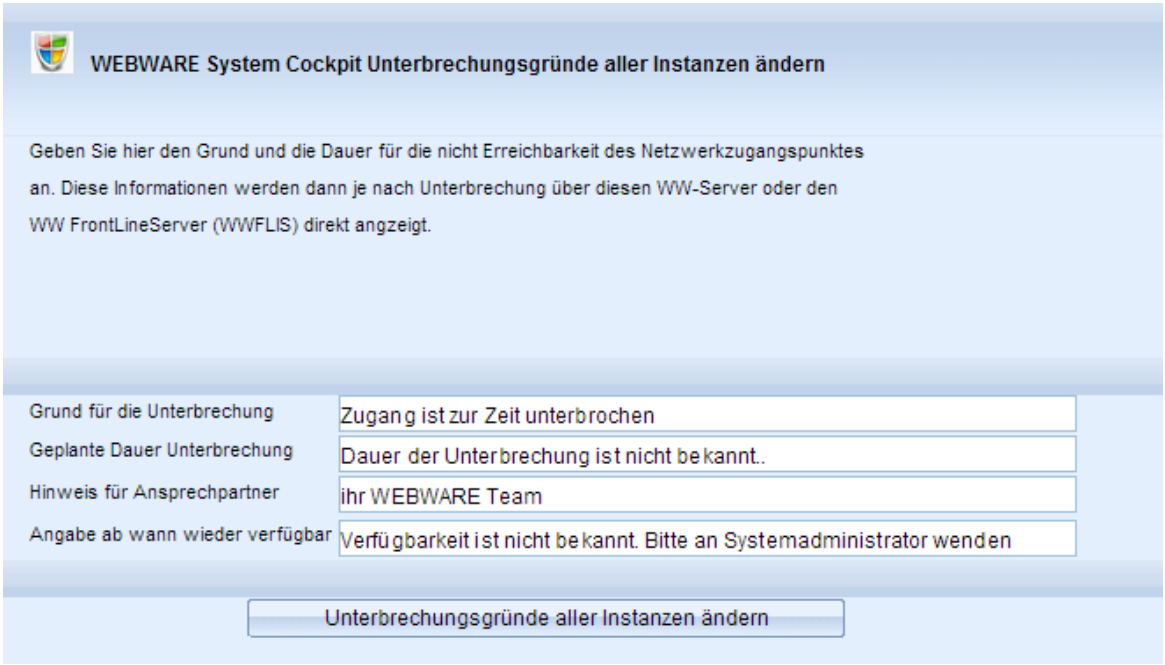
WWFLIS.TXT Anzeigetexte Vorgabe

Da Informationen wie die Dauer oder der Grund für die Anzeige der WWFLIS-Hinweisseite sich ändern können hat man mit der bin\wwflis\WWFLIS.txt Datei die Möglichkeit die Anzeigetexte die in der bin\home\wwflis\INDEX.HTM mit Platzhaltern vorgesehen sind während des Betriebs zu aktualisieren.

```
#
#
#      Vorgabe von Texten für alle Netzwerk Zugangspunkte:
WWFLS_ALL_INFO_GRUND="Geplante Wartungsarbeit XX"
WWFLS_ALL_INFO_DAUER="Vermutlich 3 Stunden nicht verfügbar"
WWFLS_ALL_INFO_BIS_DATUM="21.04.2014"
WWFLS_ALL_INFO_BIS_UHRZEIT="19:00"
WWFLS_ALL_INFO_ADMIN="Bei Fragen Fragen@WEBWARE.de / Tel: 06349/992299"
WWFLS_ALL_INFO_SERVER_NAME=WEBWARE Enterprice Edition/Bosch
WWFLS_ALL_INFO_GEPLANT_BIS="Der Server soll ab Mittwoch 19:00 Uhr wieder verfügbar
sein"
```

Falls Sie diese Texte für alle WW-Zugangspunkte auf einmal im WWFLIS aktualisieren wollen, so können Sie dies mit dem Befehl WWFLIS-Anzeige ändern im Bereich WW-Cloud Instanzen durchführen.



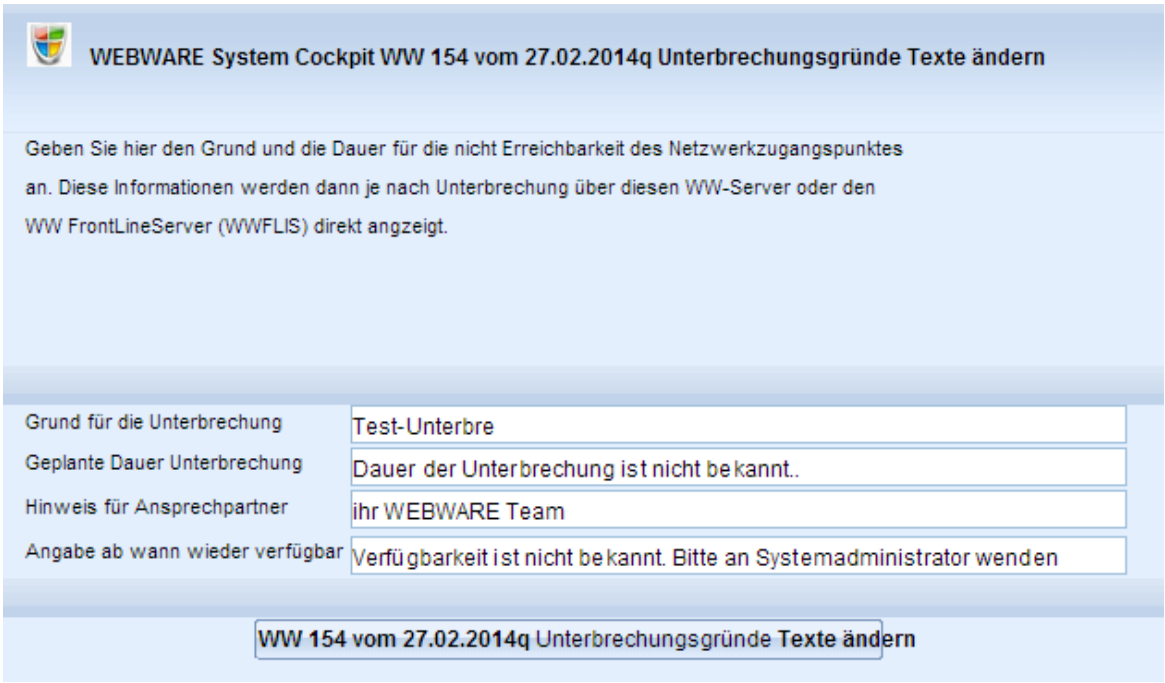


Wollen Sie nur Texte für ein Netzwerkzugangspunkt ändern so können Sie den gewünschten Netzwerk-Zugangspunkt mit der Variable WWFLS_SET_SERVER_SLOT=xx vorgeben. Dabei werden dann die Konstanten nur in diesem Netzwerkzugangspunkt aktualisiert.

```
#      Vorgabe von Einzel-Texten für einzelne Landingpages
WWFLS_SET_SERVER_SLOT=1
WWFLS_INFO_GRUND="Ausfall Accept-Thread  ??"
WWFLS_INFO_DAUER="Vermutlich 2 Stunden nicht verfügbar"
WWFLS_INFO_BIS_DATUM="21.04.2014"
WWFLS_INFO_BIS_UHRZEIT="19:00"
WWFLS_INFO_ADMIN="Bei Fragen Fragen@WEBWARE.de / Tel: 06349/992299"
WWFLS_INFO_SERVER_NAME=WEBWARE Enterprice Edition/Bosch
WWFLS_INFO_GEPLANT_BIS="Der Server soll ab Mittwoch 19:00 Uhr wieder verfügbar sein"
WWFLS_SET_SERVER_SLOT=2
WWFLS_INFO_SERVER_NAME=WEBWARE Cloud-Server Oberalmbach
WWFLS_ALL_INFO_DAUER="Ab Jetzt zum Doppelten Preis !!"
```

Mit der Funktion "Texte ändern" hat man die Möglichkeit die Anzeigetexte pro WW-Instanz auch während der Anzeige zu ändern. Weiter oben wurde die gleiche Funktion auch für alle Instanzen schon gezeigt.

Die WWFLIS-Hinweisseite ist so aufgebaut das Sie sich im Raster von 15 Sekunden selbst aktualisiert. Der WWFLIS-Server liest die Texte im 30 Sekunden Rhythmus ein.



Auslieferungsseite bin\home\wwflis\INDEX.HTM

Die Hinweisseite die bei Aktivem WWFLIS-Zugangspunkt ausgeliefert wird, finden sie in bin\home\wwflis\INDEX.HTM. Dieser Pfad/Dateiname kann im WW-System-Cockpit sowie in der WWFLIS.INI angepasst werden.

Achten Sie bei Änderungen darauf das die Datei nicht zu komplex und das die Reload-Funktion (META-TAG: <meta http-equiv='refresh' content='15'>)erhalten bleibt. Da die Seite dadurch zyklisch vom Browser angefordert wird und damit der Browser automatisch auf den WW-Server weitergeleitet werden kann.

INDEX.HTM (noch vor Redesign..)

```
<html>
<head>
 <meta http-equiv='refresh' content='15'>
 <style>
 .BDYCLS {no-repeat center; color: #008A87; font-family: "Arial Black", Gadget, sans-serif;}
 .SELOG {position:absolute; bottom: 10px; left:0px; width:100%; height:120px; background:white
url(se.png) no-repeat center; color: #008A87;}
 .T1 {position:absolute; top: 70px; left:0px; width:100%; height:60px; font-size: 52px; color:
#008A87;text-align: center;}
 .T2 {position:absolute; top: 200px; left:0px; width:100%; height:30px; font-size: 26px; color:
#008A87;text-align: center; }
 .T3 {position:absolute; top: 260px; left:0px; width:100%; height:30px; font-size: 26px; color:
#008A87;text-align: center; }
 .T4 {position:absolute; top: 320px; left:0px; width:100%; height:30px; font-size: 26px; color:
#008A87;text-align: center; }
 .T5 {position:absolute; top: 400px; left:0px; width:100%; height:30px; font-size: 20px; color:
#008A87;text-align: center; }
 </style>
</head>
<body class="BDYCLS">
<div class="T1">AAAAAAAAAA</div>
<div class="T2">BBBBBBBBBB</div>
<div class="T3">CCCCCCCCCC</div>
<div class="T4">DDDDDDDDDD</div>
<div class="T5">EEEEEEEEEE</div>
<div class="SELOG"></div>
</body>
</html>
```

Dabei werden die Texte mit Hilfe von Platzhaltern in der INDEX.HTM des WWFLIS bei der Auslieferung einkopiert. Hier gibt es 5 Variablen

```
AAAAAAAAAA      Name der WW-Instanz
BBBBBBBBBB      Grund der Unterbrechung
CCCCCCCCCC      Geplante Dauer
DDDDDDDDDD      Administrator Info (Telefon/eMail..)
EEEEEEEEEE      Hinweis ab wann der Server wieder bereit steht.
```

Sie können die Anzeigeseite für aktiver WWFLIS an Ihre Bedürfnisse anpassen. Standardmäßig wird diese im WW-Home Verzeichnis im Unterordner bin\home\WWFLIS abgelegt.

Konfiguration im WW-System-Cockpit

Systemwerte für das WWFLIS innerhalb des System-Cockpit.

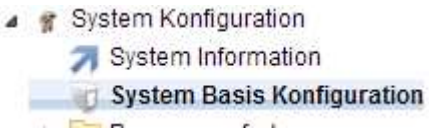
Die Pfade für die Integration des WWFLIS mit dem WW-Server werden im System-Cockpit im Bereich System-Konfiguration > Programmpfade > WW-FrontLineServer Pfade angegeben.

Neben dem Installationsverzeichnis des WWFLIS-Servers (ausgehend vom WW-Server Verzeichnis, also bin\wwflis) können hier die Namen (Programm-Name + Service-Name), die Pfade in denen Die WWFLIS.INI Datei (Komplette Konfiguration des WWFLIS) sowie die WWFLIS.TXT Datei (Vorgabe der Anzeigetexte zur Laufzeit).

Beschreibung	Systemwert
WWFLIS Installations Verzeichnis	..\WWFLIS\
WWFLIS Pfad/Dateiname INI-Datei	..\WWFLIS\WWFLIS.INI
WWFLIS Pfad/Dateiname Text-Datei	..\WWFLIS\WWFLIS.TXT
WWFLIS Name SERVICE	WEBWARE-FrontLineServer
WWFLIS Program Name	WEBWRE-FrontLineServer
WWFLIS Home-Verzeichnis	..\home\WWFLIS\
WWFLIS Startdatei Datei	index.htm

Ebenso wird hier das Grundverzeichnis des WWFLIS innerhalb des HOME-Verzeichnis sowie die gewünschte Start-Datei (INDEX.HTM) hinterlegt.

Der Vorgabewert für den Ansprechpartner kann im Bereich System-Basis Konfiguration je WW-Instanz hinterlegt werden. Dabei gibt es 2 Werte. Wenn der Text Ansprechpartnerhinweistext für Kommunikation ausgefüllt ist, so wird dieser als Variable DDDDDDDDDD vorgeschlagen. Ansonsten der bestehende Text "Name System Administrator für Kommunikation".



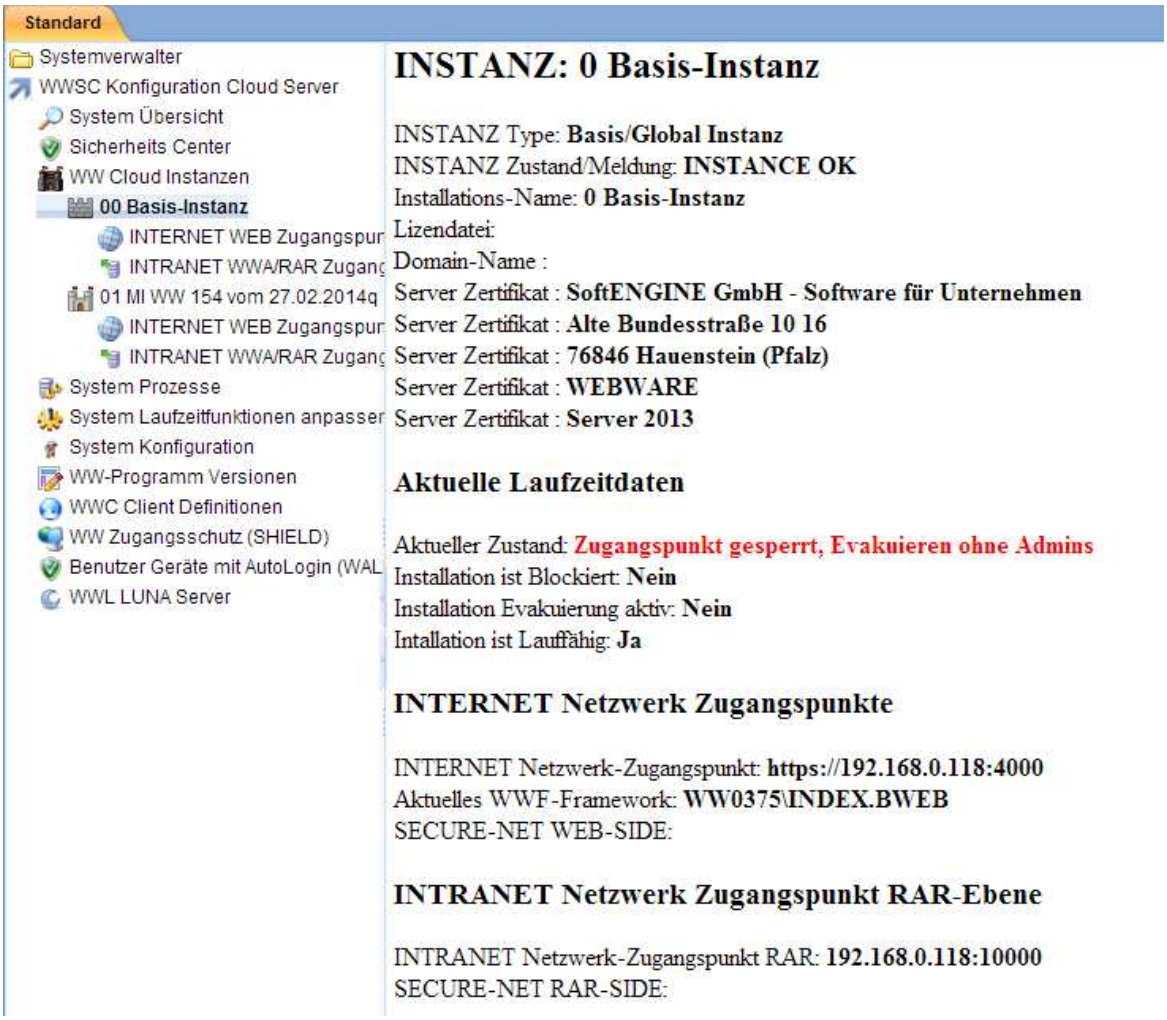
Beschreibung	Systemwert
Name System Administrator für Kommunikation	ihr WEBWARE Team
Ansprechpartnerhinweistext für Kommunikation	**Bei Fragen: Markus.Klemm@SoftENGINE.de Tel: 06392/998877**

Zugriff auf WW-Instanzen

Ab dieser Release ist die WW-Instanz Verwaltung auch bei Enterprise und Cooperation Server im System-Cockpit zu verwenden. Hier werden je nach Server-Art, Anzahl der WW-Instanzen sowie der Einstiegssichtweise ins Systemcockpit (WW-Instanz Sicht, oder Server..), eine bis mehrere WW-Instanzen angezeigt.

Je Instanz gibt es hier jeweils den INTERNET und INTRANET Zugangspunkt zur Verwaltung.

Wird eine WW-Instanz ausgewählt, so erhält man auf der rechten Seite die aktuellen Laufzeit-Informationen zu der Instanz angezeigt.



Auf Ebene der INTERNET (WEB-Anbindung WW-Server) und INTRANET (RAR-Anbindung WW-Server) erhält man jeweils die aktuellen Serverdurchsätze angezeigt.

Wird der INTERNET-WEB Zugangspunkt der WW-Instanz ausgewählt, so erhält man die neuen WWFLIS Funktionen angeboten.

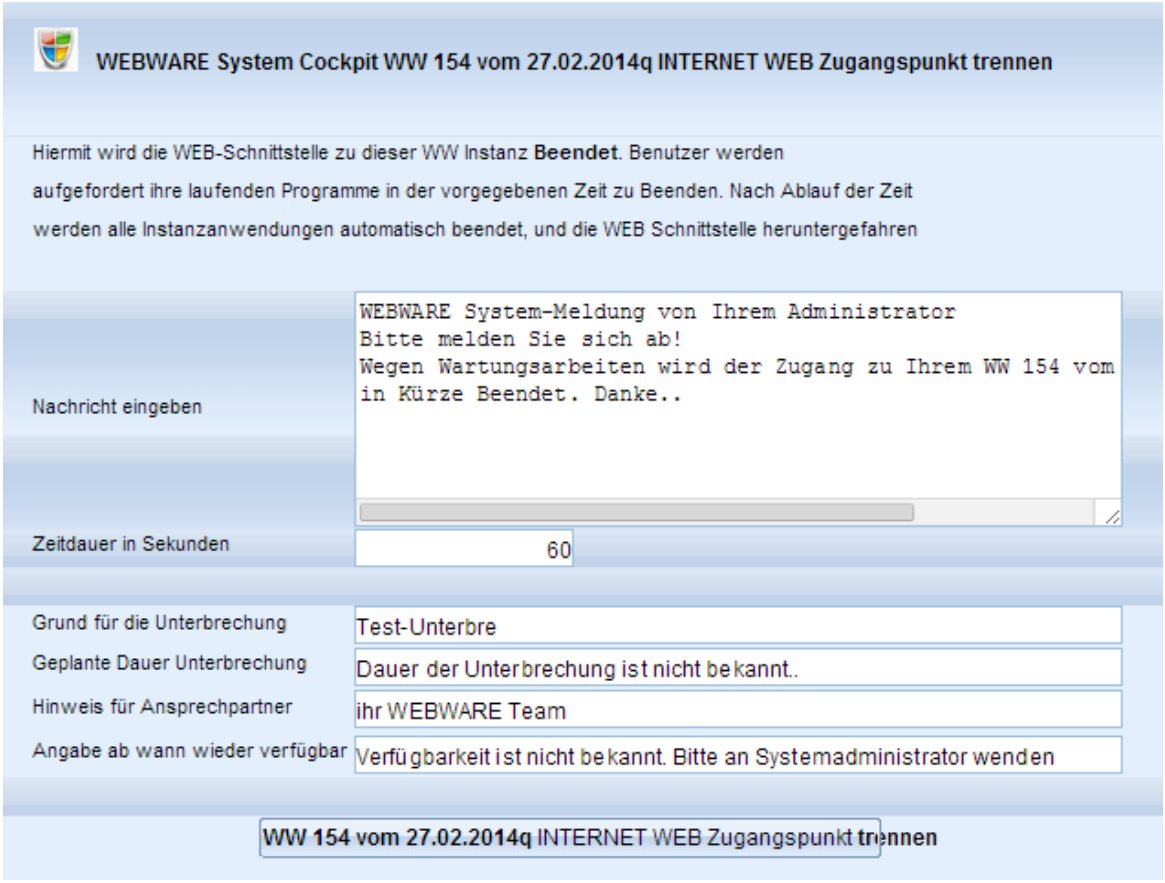
WWFLIS Abschalt/Sperr Funktionen

Man unterscheidet hierbei 2 Arten von Abschaltung/Sperrung des Zugangspunktes. Bei Abschaltung werden alle Ressourcen die für den Zugangspunkt verwendet werden freigegeben. Bei der Sperrung des Zugangspunkt werden die gewünschten Sitzungen Beendet und der Zugriff ist nur noch von der Lokalen-Netzwerkadresse des WW-Server auf die WW-Instanz möglich.

WWFLIS Internet Zugangspunkt abschalten

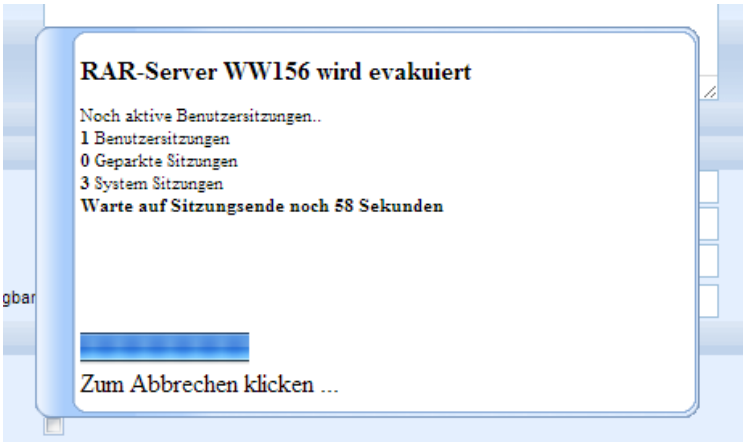
Abschalten bedeutet das alle Netzwerkverbindungen für diese WW-Instanz und über alle Netzwerkadressen/Port's die für diese Instanz konfiguriert sind freigegeben werden und damit kein Zugriff auf die WW-Instanz mehr erfolgen kann. Diese Funktion ist für Update's / Datenbank Reorgs usw. gedacht. Nach Freigabe der Netzwerk-Zugangspunkte springt der WWFLIS ein und liefert die Hinweisseite aus.

Wird dieser Befehl ausgewählt so wird folgende Konfigurationsseite angezeigt.



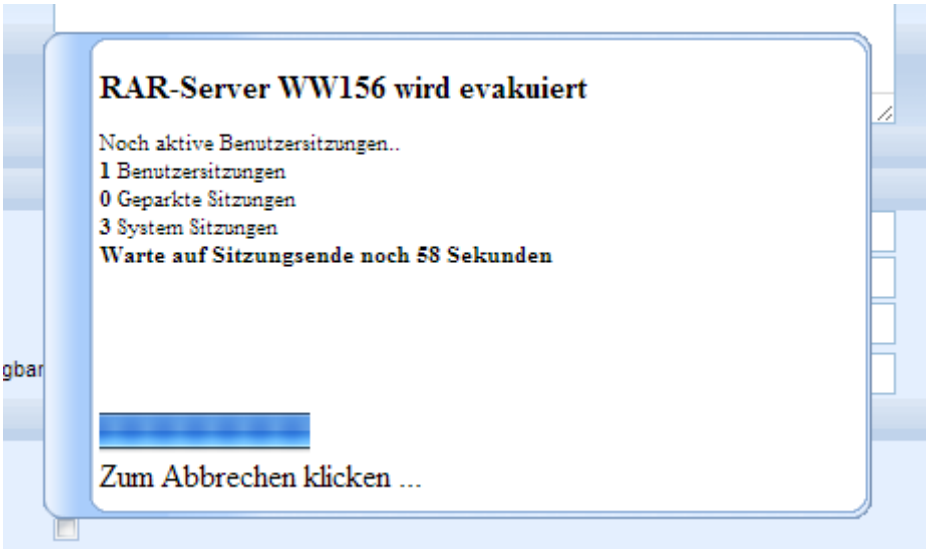
Sie haben im oberen Bereich die Möglichkeit einen Hinweistext sowie eine Zeitdauer in Sekunden anzugeben. Wird der Befehl ausgeführt so werden sämtlichen aktiven Sitzungen (auch die aktive die diesen

Befehl ausführt, wenn Sie in der WW-Instanz läuft) Beendet. Dabei erhalten die Benutzer die Zeitdauer in Sekunden Zeit um Ihre Anwendung ordentlich abzumelden. Hierzu erhalten Sie ein PopUp-Fenster angezeigt das Sie auffordert das Programm zu Beenden.

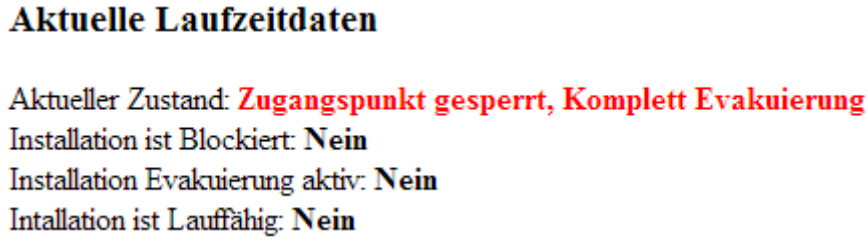


Beenden die Benutzer die Anwendung nicht in der vorgegebenen Zeitdauer, so werden die entsprechenden Sitzungen vom WW-Server nach Ablauf der Zeit automatisch Beendet.

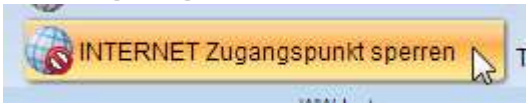
Sie erhalten während der Zeitdauer einen Hinweis über den Fortschritt sowie am Ende einen Hinweis darüber ob die Aktion erfolgreich war.



Ist eine WW-Instanz blockiert oder gesperrt wird dies in der Übersicht für die WW-Instanz in Roter Farbe angemerkt.



WWFLIS Internet Zugangspunkt Sperren



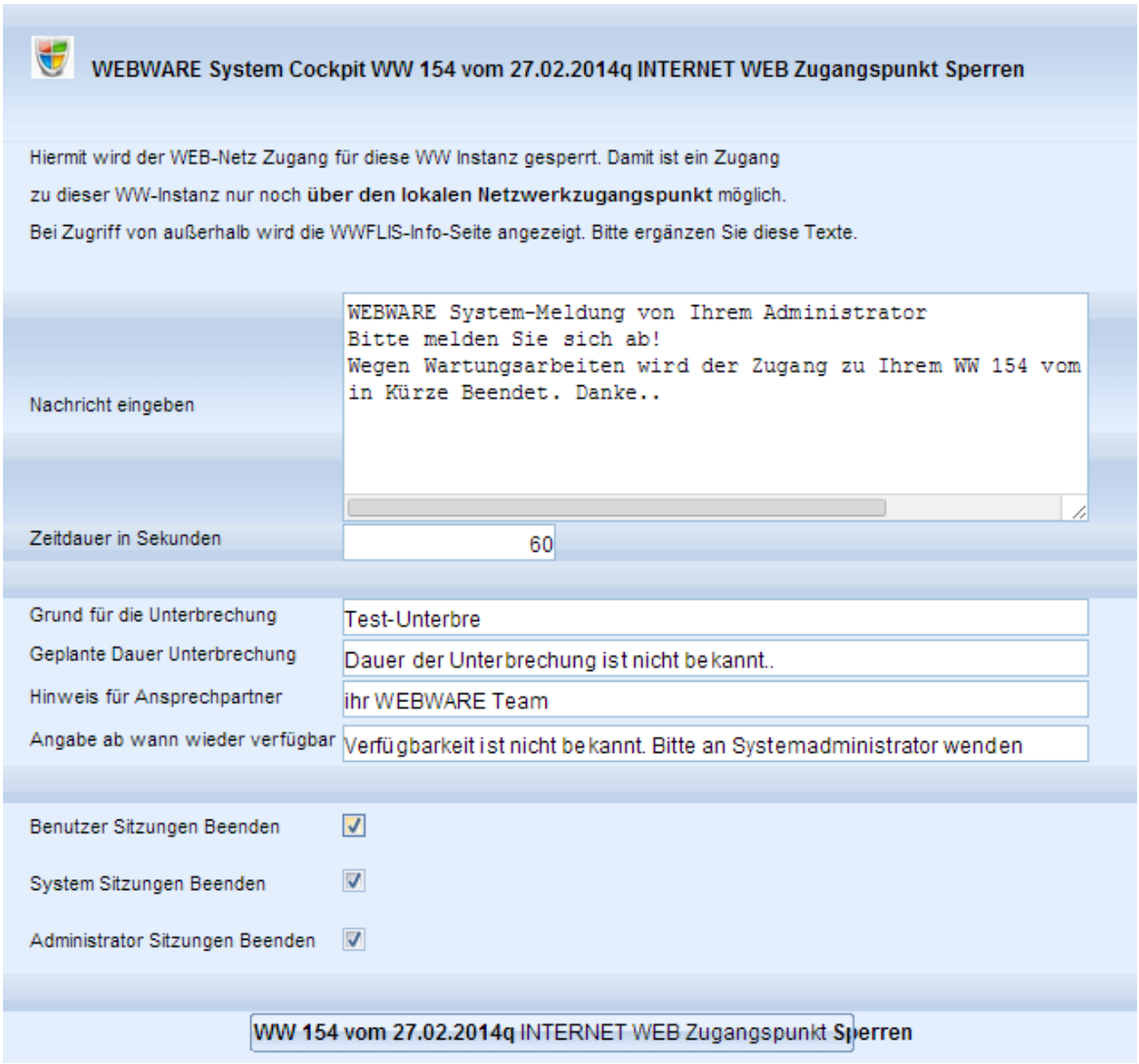
Sperren bedeutet das alle neuen Netzwerkverbindungen für diese WW-Instanz und über alle Netzwerkadressen/Port's die für diese Instanz konfiguriert sind mit der WWFLIS-Hinweisseite informiert werden das die WW-Instanz nicht erreichbar ist.

Sie können bei der Sperrung der WW-Instanz wie schon bei der Abschaltung auch Programme Beenden lassen. Es ist hier jedoch möglich das Sie entscheiden können welche Programme, also Benutzer-Programme, System-Server Programme und Administrator-Sitzungen Beendet werden sollen. Ebenso können Sie hier einen Hinweistext sowie eine Zeitdauer für das Beenden de Anwendungen vorgeben.

Diese Funktion hilft wenn man zum Beispiel kurzfristig den RAR-Bereich sperren will um Update's und Korrekturen durchführen will. Die WWFLIS-Hinweisseite wird hierbei vom WW-Server selbst ausgeliefert.

Eine weitere Besonderheit ist, das der Zugriff wie gewohnt von der lokalen Netzwerkadresse des WW-Servers aus erfolgen kann. Diese Adresse wird vom WWFLIS-Hinweisbildschirm ausgenommen.

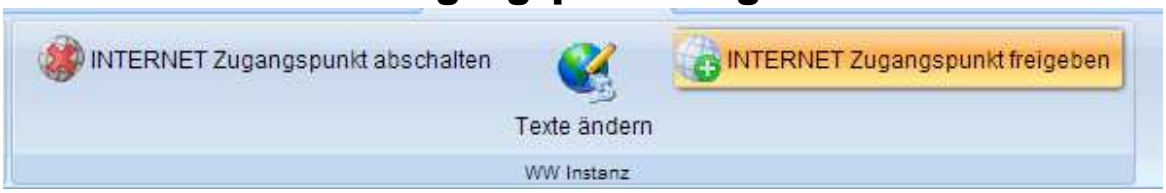
Wird dieser Befehl ausgewählt so wird folgende Konfigurationsseite angezeigt.



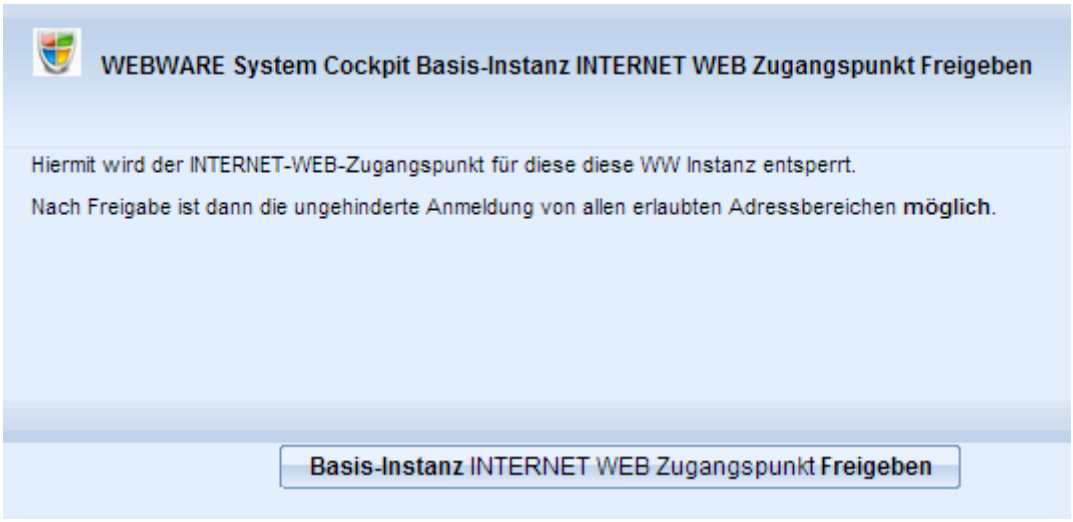
Zusätzlich zu der Abschaltseite haben Sie hier die Möglichkeit zu Wählen welche Programmarten bei der Sperrung Beendet werden sollen. Achten Sie darauf das Sie sich nicht selbst ausschließen. Bei Bedarf können Sie hier die Administrator-Sitzungen nicht Beenden..

System-Sitzungen sind alle Programme von WWSYSSRV.exe bis zu WTAPISRV.exe die vom RAR-Server angeboten werden.

WWFLIS INTERNET Zugangspunkt freigeben

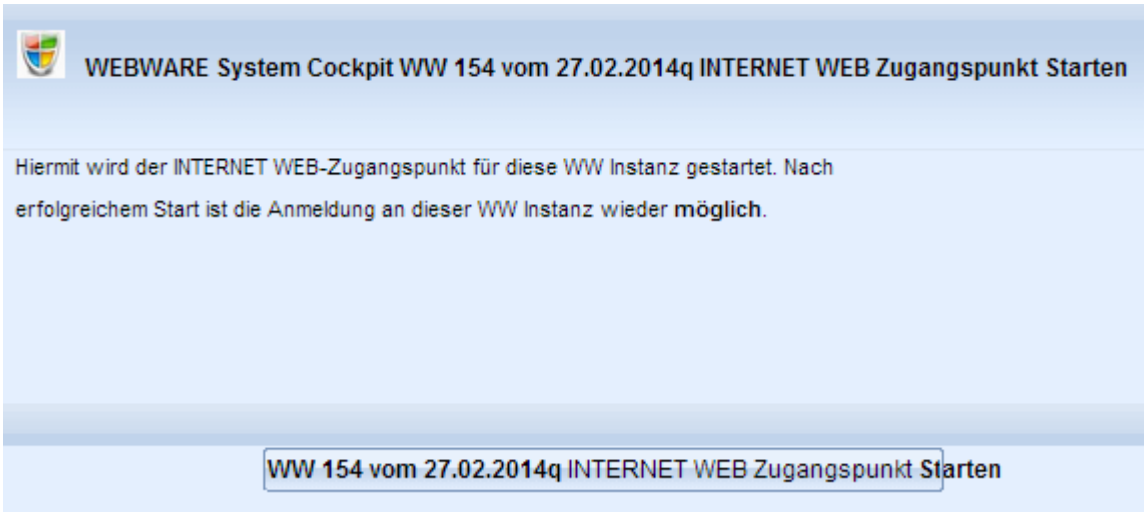


Ist ein INTERNET Zugangspunkt gesperrt, so können Sie diesen mit dem Befehl "INTERNET Zugangspunkt freigeben" mit der folgenden Konfigurationsseite freigeben.



WWFLIS INTERNET Zugangspunkt starten

Ist ein INTERNET Zugangspunkt abgeschaltet, so kann der Zugangspunkt mit dem Befehl "INTERNET Zugangspunkt starten" wieder aktiviert werden.



Nach Hochfahren von Internet und RAR-Zugangspunkten erhält man einen Hinweis das die WW-Instanz wieder verfügbar ist.

Anweisung: WWFLIS Hilfe zur Erstkonfiguration

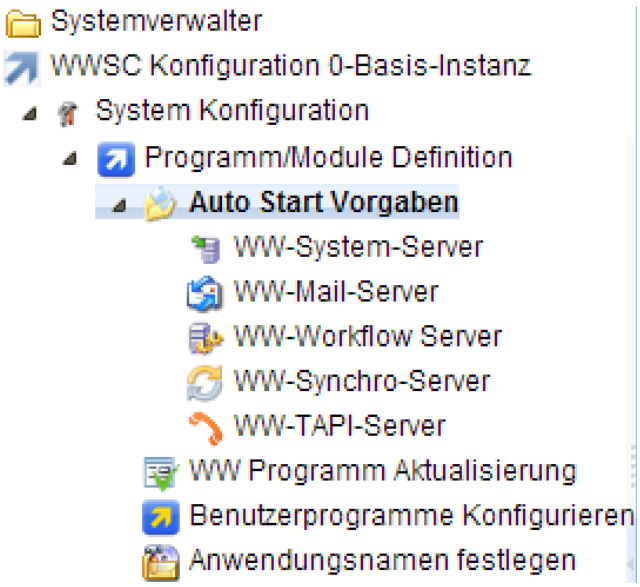
Hier noch einmal in Kürze die Schritte die für die erfolgreiche Inbetriebnahme des WWFLIS auf ihrem WW-System notwendig sind.

- Installieren aktuelles Update/Setup der WEBWARE > 01.03.2014
- Einstieg ins Systemcockpit (Konfiguration > Server-Ebene)
- Erzeugen der bin\wwflis\wwflis.ini wie weiter oben Beschrieben

- Prüfen der bin\wwflis\wwflis.ini -> SSL-Zertifikate stimmen die Pfade ?
- Test mit bin\wwflis\wwflis.exe console -> Gibt es Fehlermeldungen falsche Adressen/SSL usw.
- Falls Test OK, installieren als Dienst mit Administrator-Berechtigung bin\wwflis\wwflis INSTALL
- Einmaliges Starten des Dienstes bin\wwflis\wwflis.exe start
- Bei Bedarf anpassen der Hinweisseite bin\home\wwflis\index.htm

WEBWARE Programm/Module Definition

In diesem Bereich wird erklärt wie Auto-Start Programme, spezialisierte Benutzerprogramme für Ihren WEBWARE-Server verwaltet und Konfiguriert werden. Sie finden die folgenden Bereiche im System-Cockpit im Bereich Konfiguration.



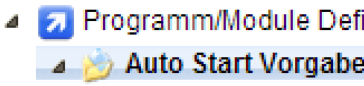
Unter Auto-Start Vorgaben können Sie die einzelnen WEBWARE Basis-Komponenten für den automatischen Start vorbereiten

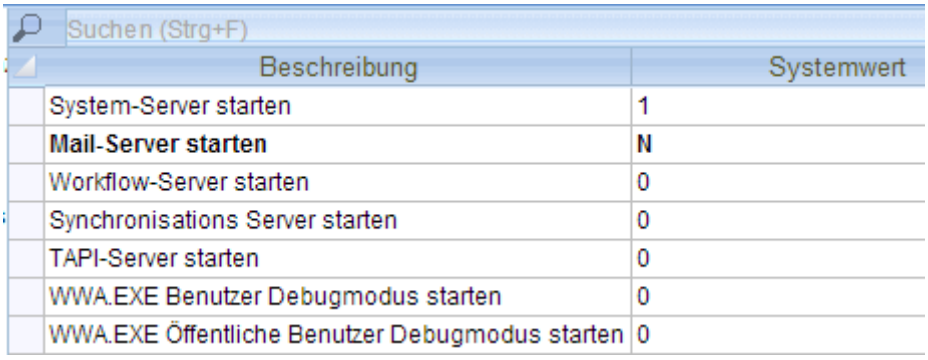
Im Bereich WW Programm Aktualisierung finden Sie Optionen für die automatische Programmaktualisierung, zum Beispiel vom WW@Home Client Communicator

In Benutzerprogramme Konfigurieren können Sie die Standard Start-Programme anpassen, bzw. Individuelle Startprogrammdefinitionen anlegen.

Unter Anwendungsnamen werden die internen Namen für die Anwendungen verwaltet und konfiguriert.

WEBWARE Auto Start Vorgaben





Beschreibung	Systemwert
System-Server starten	1
Mail-Server starten	**N**
Workflow-Server starten	0
Synchronisations Server starten	0
TAPI-Server starten	0
WWA.EXE Benutzer Debugmodus starten	0
WWA.EXE Öffentliche Benutzer Debugmodus starten	0

Hier können die Grundprogramme und Startparameter festgelegt werden wie sie beim Programmstart verwendet werden.

System-Server starten:

Hiermit wird angegeben ob die wwsyssrv.exe bei Verfügbarkeit gestartet werden soll. Dieser Server muss von einem RAR-Server zur Verfügung gestellt werden und wird für den Betrieb des WW-Server benötigt.

Mail-Server starten:

Hiermit wird angegeben ob die wwmail.exe bei Verfügbarkeit gestartet werden soll. Dieser Server muss von einem RAR-Server zur Verfügung gestellt werden und wird für den Betrieb des WW-Sserver benötigt um aus der WEBWARE CRM eMail zu Senden und Empfangen.

Workflow Server starten

Mit dieser Option kann der Start von Workflow Servern aktiviert wird. Diese Option ist bisher noch nicht implementiert.

Synchronisations Server starten:

Ist diese Option aktiviert so wird bei verfügbarem RAR-Server das Progarmm bin\wwsync\wwsync.exe gestartet mit dem Verzeichnisse aus dem APP-Bereich in das Home-Verzeichnis gemapped werden können.

TAPI-Server starten:

Ist diese Option aktiviert so wird das bei verfügbarem RAR-Server das Programm bin\wwtapi\wtapisrv.exe gestartet. Dieses Programm liest die TAPI-Konfiguration des RAR-Servers aus und stellt diese im System-Cockpit für die WEBWARE zur Verfügung.

WWA.EXE Benutzer Debugmodus starten

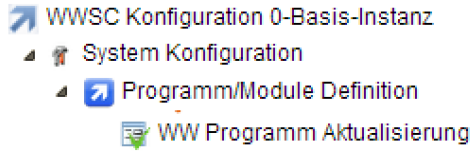
Ist diese Option aktiviert, so wird das Programm WWA.exe (Benutzersitzungen) beim Start mit dem Programm dbgdump.exe gestartet so dass bei Abstürzen eine Dump Datei in das Verzeichnis APP\WWCATCH bzw. APP\BWCATCH geschrieben wird.

WWA.EXE Öffentliche Benutzer Debugmodus starten

Ist diese Option aktiviert, so wird das Programm WWA.exe (Public-Worker Sitzung) beim Start mit dem Programm dbgdump.exe gestartet so dass bei Abstürzen eine Dump Datei in das Verzeichnis APP\WWCATCH bzw. APP\BWCATCH geschrieben wird.

WW Programm Aktualisierung

In diesem Programmpunkt können Sie die aktuellen Build-Nummern der WWCC und LUNA Komponenten einsehen und den automatischen Programm-Update konfigurieren.

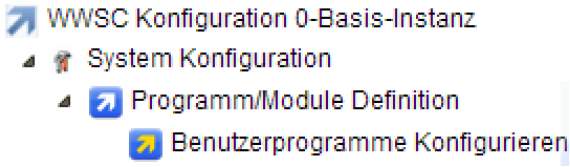


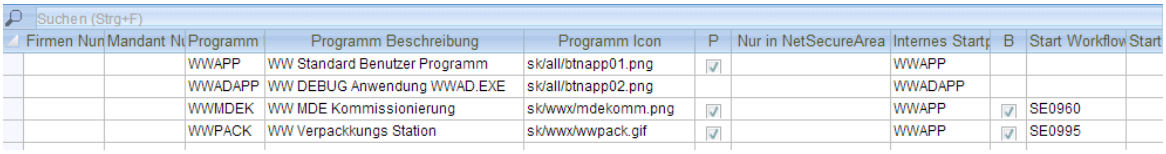
Suchen (Strg+F)

Beschreibung	Systemwert
Auto Programmupdate Aktiv	1
WWCC Auto Programmupdate Aktiv	1
WWCC aktuelle Build-Nummer	1166
WW-LUNA Auto Programmupdate Aktiv	0
WW-LUNA aktuelle Build-Nummer	109

Mit dem Systemwert Auto Programmupdate Aktiv kann das automatische Aktualisieren komplett an/abgeschaltet werden.

WW Benutzerprogramme Konfigurieren

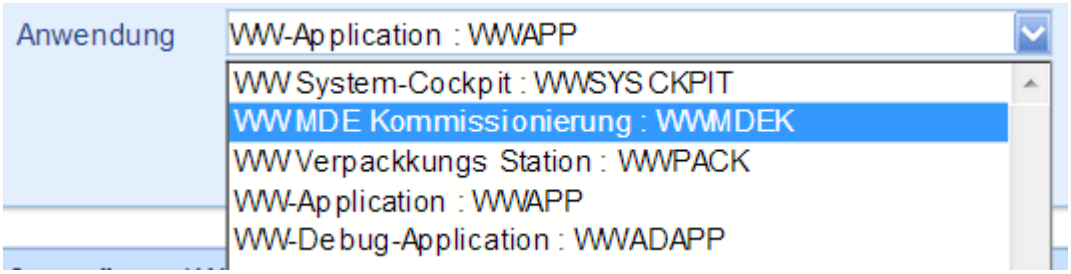




Mit den individuellen Benutzerprogramm Konfigurationen können Sie notwendige Startparameter für die Anwendungen vorgeben. Sie haben auch die Möglichkeit eigene Startprogramm Konfigurationen auch für einzelne Benutzer zu erstellen und individuell zu konfigurieren.

Über die Verwendung und Festlegung der einzelnen Programm-Kennungen lesen Sie bitte im nächsten Abschnitt (Anwendungsnamen festlegen)

Eine Programmdefinition kann Global (Standard bei Auslieferung), oder auf Firmen und Mandanten Ebene individuell angelegt werden. Ebenso ist es möglich einzelne Programme zu deaktivieren, so dass diese nicht manuell auswählbar sind.

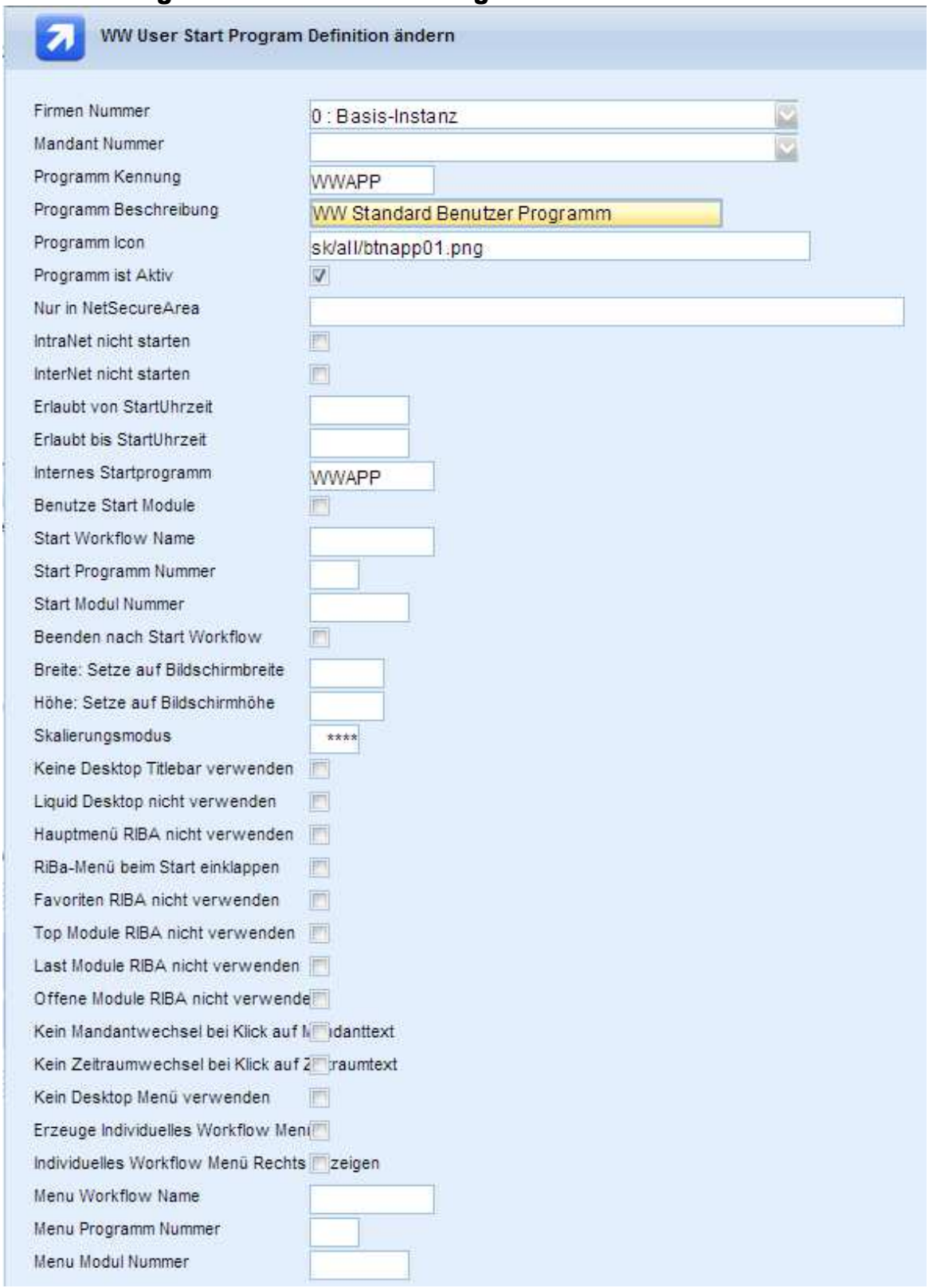


(Hinweis: WW System-Cockpit ist nur direkt auf dem WW-Server verfügbar und wird automatisch eingeblendet..)

Standard Programmdefinitionen

- WWAPP Standard Programm für Benutzer / Öffentliche (Public User) Benutzer
- WWADAPP Debug-Programm das alternativ zu wwapp verwendet werden kann.
- WWMDEK Mobile Daten Erfassung Kommissionierung
- WWPACK Verpackungs Station

Beschreibung der Parameter einer Programmdefinition



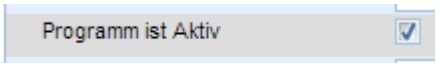
Hauptschlüssel einer Programmdefinition

Der Hauptschlüssel besteht aus Firmen-ID, Mandanten-ID sowie der Programm-Kennung. Der Zugriff erfolgt dann zur Laufzeit über die Programm Kennung abhängig der aktuellen Firma/Mandant.

Programm-Beschreibung

Hier kann ein Text sowie ein Bild für die Programm-Konfiguration hinterlegt werden.

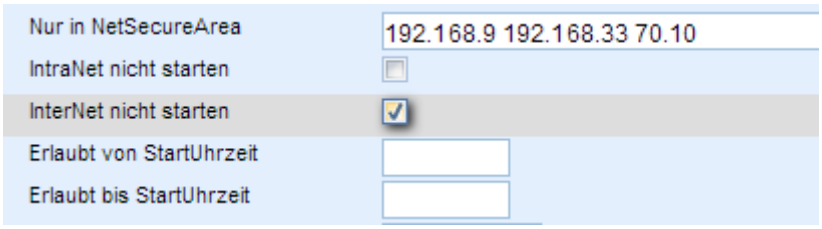
Programmdefinition Aktiv



Ist dieser Schalter aktiviert so ist die Verwendung der Programmbeschreibung im WEBWARE Server möglich.

Begrenzung der Ausführung der Programmdefinition

Mit den folgenden Parametern kann die Ausführung der Programmdefinition nach Zeit, und Zugriffsort begrenzt werden.



Nur in NetSecureArea

Hier können Sie bis zu 20 Netzwerksegmente angeben. Die Ausführung der Anwendung ist dann nur erlaubt, wenn der Benutzer aktuell in einem der Netzwerksegmente die Anwendung starten will.

IntraNet nicht starten

Ist dieser Schalter aktiviert so darf die Programmdefinition nicht aus der definierten Intra-Net Zone heraus ausgeführt werden.

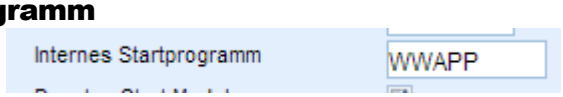
InterNet nicht starten

Ist dieser Schalter aktiviert so darf die Programmdefinition nicht aus der definierten Inter-Net Zone heraus ausgeführt werden.

Startzeit begrenzen

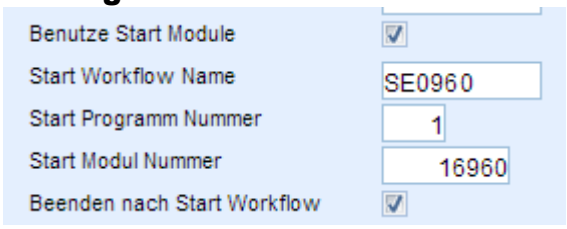
Sie können durch Angabe einer Von-Bis Start-Uhrzeit die Startzeit der Anwendung begrenzen. Sind beide Felder leer, so ist eine dauerhafter Start erlaubt.

Internes Startprogramm



Mit diesem Parameter wird das intern verwendete Startprogramm vorgegeben. Sie können hier aktuell zwischen WWAPP und WWADAPP wählen. Ist der Parameter nicht gefüllt wird entweder die aktuelle Programm-Kennung oder WWAPP verwendet.

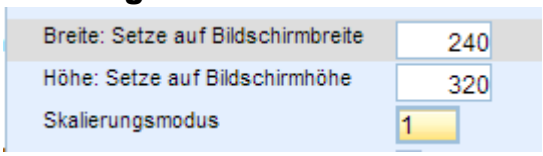
Start-Workflow vorgeben



Mit diesen Parametern können Sie einen Workflow festlegen der bei Programmstart ausgeführt werden soll. Die Ausführung erfolgt nur wenn "Benutze Start Module" als Option gesetzt ist. Aktuell werden nur die Programm-Nummer sowie die Modulnummer verwendet. Später soll die Implementierung eines Workflownamens noch folgen.

Falls das Programm nach Verlassen des Startworkflow automatisch Beendet werden soll, so aktivieren Sie bitte die entsprechende Option.

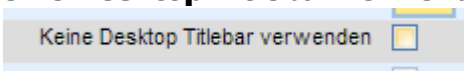
Bildschirmgröße vorgeben



Um spezielle Geräte bzw. spezielle Workflow die auf bestimmte Größen festgelegt sind korrekt auszuführen, können Sie hier die Bildschirmgröße der Anzeige festlegen. Ein Beispiel ist hier zum Beispiel die Mobile Daten Erfassung MDE-Kommissionierung. Da diese Workflow's nur auf Spezialgeräten ausgeführt werden ist hier eine Vorgabe der Bildschirmgröße notwendig. Abhängig vom der Zielanwendung kann hier auch der Skalierungsmodus festgelegt werden.

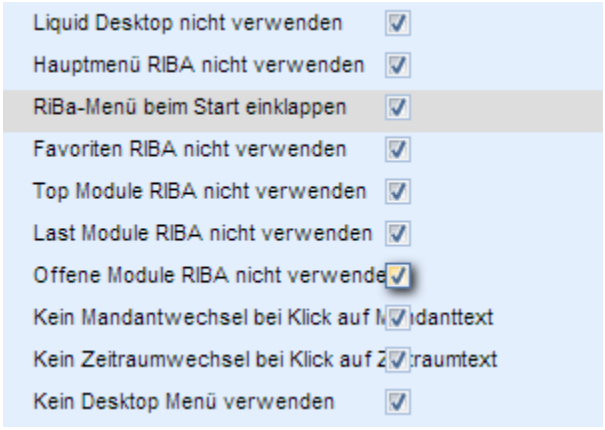
Bei normalen WWAPP-Programmen wir die Desktop-Auflösung (800x600/1024x800/usw ..) verwendet. Bei MDEKOM ist hier definiert das bei 0: die Bildschirmgröße fix ist. bei 1: wird die Anzeige automatisch an die Größe des Gerätes gezoomet.

MDEKOM: Keine Desktop Titlebar verwenden



Dieser Parameter ist nur für die MDEKOM Definition gedacht. Hier kann die obere Titelzeile abgeschaltet werden, um auf kleinen Bildschirmen mehr Platz zu haben. Die Obere Titelzeile zeigt einen Rückwärts-Pfeil, den aktuellen Module-Titel sowie ein Pfeil für das Haupt-Menü

Programm Komponenten abschalten (WWAPP..)



Liquid Desktop nicht verwenden

Hiermit kann die Liquid-Render Engine abgeschaltet werden.

Hauptmenü RIBA nicht verwenden

Ist dieser Schalter aktiviert, so ist der Aufruf des Hauptmenü per Klick auf den Home-Button links oben nicht mehr möglich.

RiBa-Menü beim Start einklappen

Ist dieser Schalter aktiviert so wird das RiBa-Menü oben im Hauptmenü eingeklappt gestartet. Dadurch steht mehr Bildschirm für die Anwendung zur Verfügung.

Favoriten RIBA nicht verwenden

Ist der Schalter aktiviert, so wird die Lasche Favoriten im RIBA Menü nicht mehr angezeigt.

Top Module RIBA nicht verwenden

Ist der Schalter aktiviert, so wird die Lasche Top Module im RIBA Menü nicht mehr angezeigt.

Last Module RIBA nicht verwenden

Ist der Schalter aktiviert, so wird die Lasche Last (Letzte) Module im RIBA Menü nicht mehr angezeigt.

Offene Module RIBA nicht verwenden

Ist der Schalter aktiviert, so wird die Lasche Offene Module im RIBA Menü nicht mehr angezeigt.

Kein Mandantwechsel bei Klick auf Mandanttext

Ist der Schalter aktiviert, so wird kein Mandantenwechsel bei Klick auf den Mandantentext mehr angeboten.

Kein Zeitraumwechsel bei Klick auf Zeitraumtext

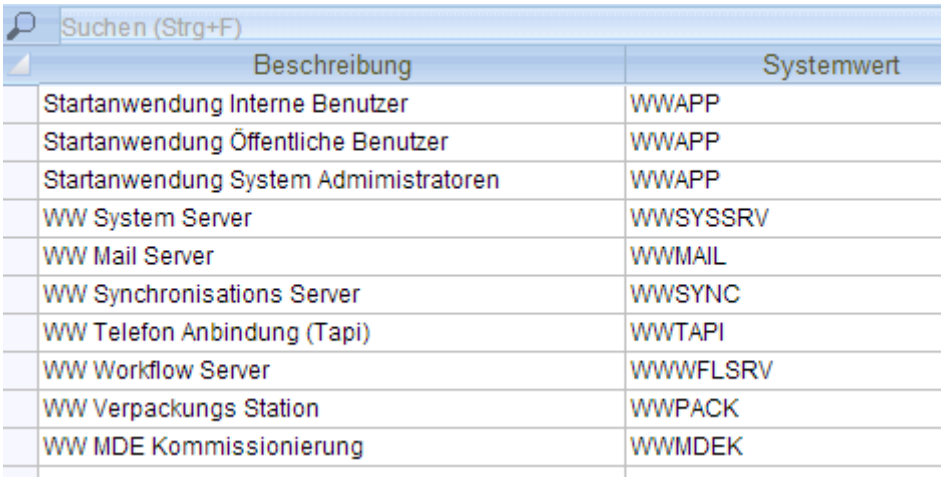
Ist der Schalter aktiviert, so wird kein Zeitraumwechsel bei Klick auf den Zeitraumtext mehr angeboten.

Kein Desktop Menü verwenden

Ist der Schalter aktiviert, so wird das Standard Desktop Menü nicht mehr verwendet (eMenü)

Anwendungsnamen festlegen .. Programm-Namen

Die WEBWARE verwendet einige festgelegte Anwendungsnamen die für die interne Programmstartlogik benötigt werden. Für die WEBWARE Standarddefinitionen sind bereis die notwendigen Programmdefinitionen auf Ebene des Servers definiert. Sie haben jedoch die Möglichkeit diese zu ändern oder neue anzulegen



Beschreibung	Systemwert
Startanwendung Interne Benutzer	WWAPP
Startanwendung Öffentliche Benutzer	WWAPP
Startanwendung System Admimistratoren	WWAPP
WW System Server	WWSYSSRV
WW Mail Server	WWMAIL
WW Synchronisations Server	WWSYNC
WW Telefon Anbindung (Tapi)	WWTAPI
WW Workflow Server	WWWFLSRV
WW Verpackungs Station	WWPACK
WW MDE Kommissionierung	WWMDEK

- WWAPP Standard Startprogramm wwa.exe
- WWADAPP Debug Startprogramm wwad.exe
- WWMDEK Mobile Daten Erfassung Komissionierung Start über wwa.exe
- WWPACK Verpackungsstation Start über wwa.exe

Desweieren gibt es noch Programmnamen die nicht änderbar sind und für andere WEBWARE Programme vewrendet werden.

- WWSYSSRV WEBWARE System Server
- WWMAIL WEBWARE eMail Server
- WWWFLSRV WEBWARE Workflow Server
- WWSYNC WEBWARE Synchronisation Server APP-Verzeichnis <-> HOME-Verzeichnis
- WWTAPI WEBWARE Tapi Server im Bereich RAR
- WWCC WEBWARE Client Communicator (WW@HOME)
- WWS WEBWARE Server
- WWR WEBARE RAR-Server
- WWF WEBWARE Frontend (Browser Engine)

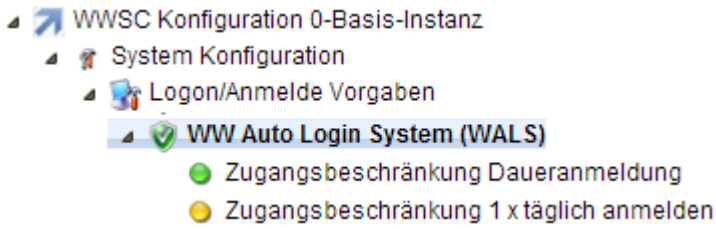
WALIS WEBWARE Auto Login System - Konfiguration

Mit WALIS können Sie den automatisierten Zugang zu Ihrem WEBWARE System konfigurieren und Verwalten. Dabei ist es möglich Benutzer-Geräte (Desktop-Browser, Tablet-Browser und Phone/Mobile Browser) zu kennzeichnen und den Anmeldevorgang zu automatisieren.

Wichtig ist hier das de Systembetreuer die Hoheit über die Freigabe und Verwaltung der Auto-Login Funktion hat. WALIS ist auch im Sicherheits Center der WEBWARE integriert.

Konfiguration des WALIS Auto Login System

Die Konfiguration des WEBWARE AutoLogin System erfolgt im System-Cockpit im Bereich System-Konfiguration, Logon/Anmelde Vorgaben.



Wichtig: Sollte ein Benutzer den Auto-Login aktiviert haben, jedoch von seinem aktuellen Standort kein Auto-Login erlaubt sein, bzw. der Zugangszeitpunkt nicht innerhalb eines erlaubten Bereiches liegt, so wird der Auto-Login für diesen Zugang temporär deaktiviert. Der Benutzer kann sich dann entsprechend normal anmelden.

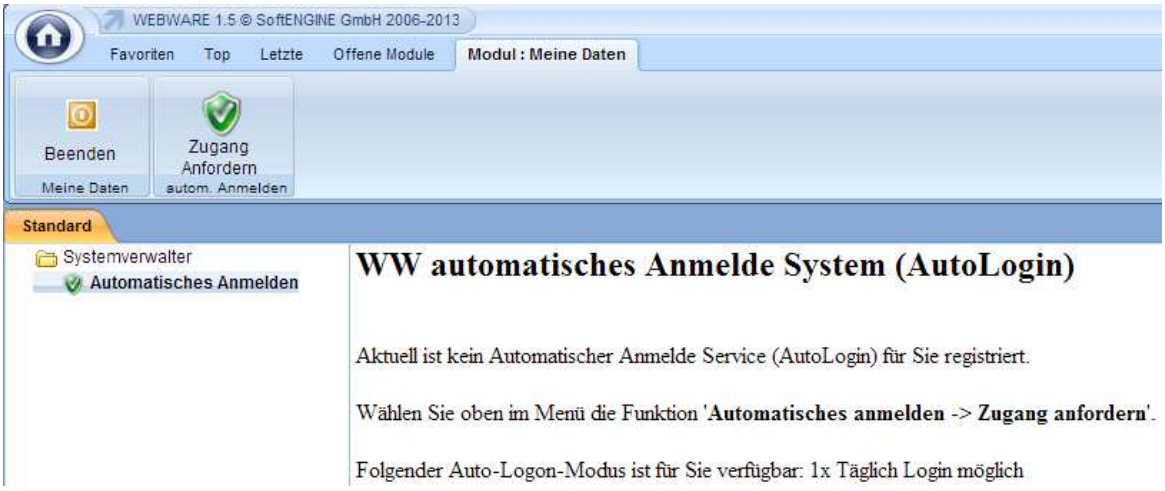
Um das WALIS zu aktivieren, muss der System-Wert Auto-Login System ist aktiv gesetzt sein. Desweiteren sollten SecureNet Netzwerkbereiche definiert werden in welchen der Automatische Login erlaubt ist.

Hier nun die Parameter des WALIS im einzelnen:

Beschreibung	
Auto Login System ist aktiv	1
Neue Geräte von Administrator freigeben	1
Maximale Anzahl Geräte pro Benutzer	66304
Maximale Login-Fehler für Sperrung Gerät	**4**
Auto-Login aktiviert, auch wenn kein SecureNetArea definiert	1
für Desktop Browser erlaubt	**J**
für Tablet Browser erlaubt	**J**
für Phone Browser erlaubt	**1**
Desktop Browser direkt anmelden	0
Tablet Browser direkt anmelden	**J**
Phone Browser direkt anmelden	0
Zeige Einladungshinweis für Geräte ohne Auto-Login	**J**

WALIS: Auto Login ist aktiv

Ist dieser Systemwert gesetzt so wird das WALIS aktiviert, und ist sodann einsatzbereit. Der Anwendungsbenutzer erhält in seinem System-Cockpit einen neuen Eintrag für "Automatisches Anmelden". Mit diesem kann der Benutzer seinen Auto-Login Zugang anfordern, Löschen und bei Bedarf für das nächste Anmelden abschalten.



Es gibt nun 2 Möglichkeiten für den Benutzer den Auto-Login zu aktivieren.

- Auswahl über System-Cockpit "Zugang anfordern"
- Bei aktiviertem Einladungshinweis für Geräte ohne Auto-Login wird ein Fenster mit Aufforderung zum Klick auf das Fenster gesendet. Dadurch wird die Zugangsanforderung ausgelöst.

Ist der Zugang angefordert so wird dies ebenfalls hier im System-Cockpit angezeigt. Der Benutzer kann dann den Zugang entfernen, bzw. die Automatik für das nächste Anmelden abschalten.

Das ganze sieht dann mit Angefordertem Anmelde System so aus:

Nun die Parameter im Einzelnen:

WALIS: Neue Geräte vom Administrator freigeben

Ist dieser Parameter gesetzt, so werden die Zugangsanforderungen in einer Quarantäne-Warteschlange im System-Cockpit eingetragen. Diese werden vom Systembetreuer entsprechend geprüft und freigegeben. Näheres dazu finden Sie weiter unten in diesem Dokument.

WALIS: Maximale Anzahl Geräte pro Benutzer

Hiermit kann die maxmale Anzahl von aktiven Auto-Login Zugängen je Benutzer festgelegt werden.

WALIS: Maximale Login-Fehler für Sperrung Gerät

Wird versucht ein Auto-Login durchzuführen, und es wird ein Fehler festgestellt, dann wird bei Erreichen der Fehleranzahl dieser Auto-Login automatisch gesperrt.

WALIS: Auto-Login aktiviert, auch wenn kein SecureNet Area definiert ist

WALIS sollte nur mit aktivem SecureNet Netzwerk Bereich verwendet werden. Damit sollten Netzwerkbereiche die als Unsicher gelten ausgeschlossen werden. Die beiden SecureNet-Bereiche für Dauer-Login und 1xTäglich Anmelden werden weiter unten besprochen.

Dieser Schalter sollte in einem sicheren System deaktiviert sein, und wird automatisch unwirksam wenn ein SecureNet Bereich für WALIS definiert ist.

WALIS: Für Desktop Browser erlaubt

Ist dieser Wert aktiviert, so ist es erlaubt sich mit WALIS mit Desktop Browser anzumelden.

WALIS: Für Tablet Browser erlaubt.

Ist dieser Wert aktiviert, so ist es erlaubt sich mit WALIS Tablet-Browser anzumelden.

WALIS: Für Phone Browser erlaubt

Ist dieser Wert aktiviert, so ist es erlaubt sich mit WALIS Phone-Browser anzumelden.

WALIS: Desktop Browser direkt anmelden

Ist dieser Wert markiert, so wird beim der WEBWARE-Startseite automatisch die Anmeldung durchgeführt. Gerade auf Desktop-Browser kann das ein Starten beim Ende auslösen. Ist der Wert nicht aktiviert so werden nur die Anmelde-Daten in der Anmeldemaske ausgefüllt.

WALIS: Tablet Browser direkt anmelden

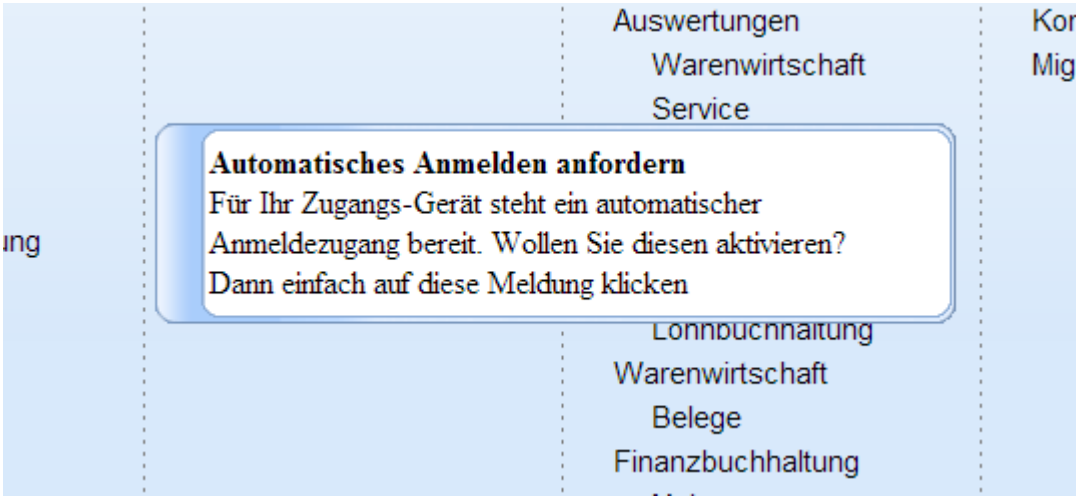
Ist dieser Wert markiert, so wird beim der WEBWARE-Startseite automatisch die Anmeldung durchgeführt. Ist der Wert nicht aktiviert so werden nur die Anmelde-Daten in der Anmeldemaske ausgefüllt.

WALIS: Tablet Browser direkt anmelden

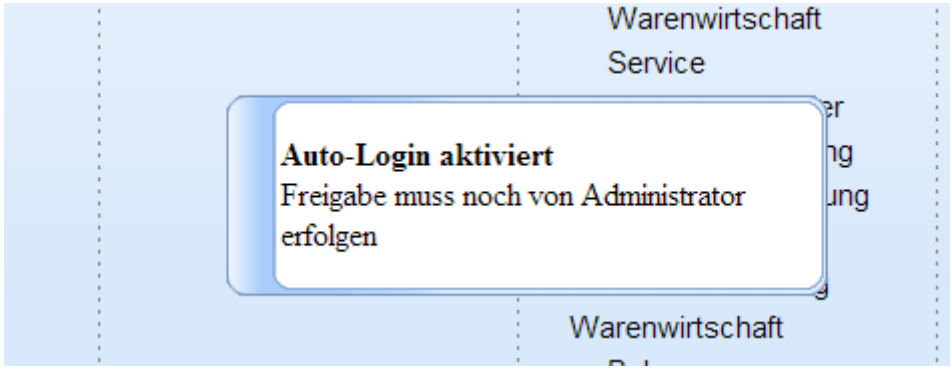
Ist dieser Wert markiert, so wird beim der WEBWARE-Startseite automatisch die Anmeldung durchgeführt. Ist der Wert nicht aktiviert so werden nur die Anmelde-Daten in der Anmeldemaske ausgefüllt.

WALIS: Zeige Einladungshinweis für Geräte ohne Auto-Login

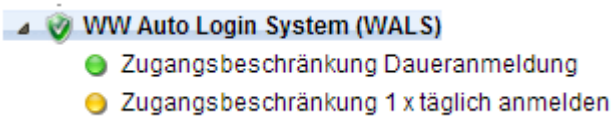
Ist dieser Wert aktiviert, so wird bei nicht vorhandenem Auto-Login und passenden Netzwerkzugang und WALIS-Parameter dem Benutzer eine Einladung zur Anforderung eines Auto-Login Zugang angezeigt.



Bei Klick auf den Hinweis wird dann der Zugang angefordert. Der Benutzer erhält dann eine Rückmeldung mit einer weiteren Hinweismeldung:



Zugangsbeschränkung für Daueranmeldung



In diesem Bereich können Sie den Zugang für Daueranmeldungen definieren. Das bedeutet das der Benutzer nach Aktivierung des Zugangs, sich während der erlaubten Zeiten nicht mehr anmelden muss. Neben einem SecureNet Netzbereich, der die Netzsegmente beschreibt welche für die Daueranmeldung zugelassen sind, gibt es auch die Möglichkeit den Zugang zeitlich zu Begrenzen.

Desweiteren ist es möglich den Bereich für Intern- und Public-User getrennt freizuschalten.

Hier die Parameter für die Zugangsbeschränkung Daueranmeldung im einzelnen:

Beschreibung	Systemwert
SecureNetArea unbegrenzter AutoLogin	**10.90.31 177.168.167 99.99.99.99**
Zeit-Lock definiert	**J**
Auto-Login erlaubt ab Uhrzeit	**120000**
Auto-Login erlaubt bis Uhrzeit	240000
Auto-Login Montags erlaubt	1
Auto-Login Dienstags erlaubt	1
Auto-Login Mittwochs erlaubt	1
Auto-Login Donnerstags erlaubt	1
Auto-Login Freitags erlaubt	1
Auto-Login Samstags erlaubt	1
Auto-Login Sonntags erlaubt	**J**
Benutzer dürfen Auto-Login verwenden	1
Public User dürfen Auto-Login verwenden	1

SecureNetArea unbegrenzter AutoLogin

Hier muss für den Dauer-Login Bereich die erlaubten Netzbereiche angegeben werden. Hier können bis zu 20 Netzsegmente, für die Festlegung der gültigen Netzbereiche angegeben werden. Alle Netzwerkadressen welche aus Teilen oder Komplett einer der Angaben entspricht haben Zugang zum Dauerlogin Bereich.

Zeit-Lock definiert

Soll der Dauerlogin Bereich zeitlich begrenzt werden. Mit diesem Schalter kann die Prüfung auf die Zeitbegrenzung des Dauerlogin Bereiches erfolgen.

Auto-Login erlaubt ab- bis- Uhrzeit

Hier können Sie die Kernzeiten angeben von wann bis wann der Zugang erfolgen per Auto-Login erfolgen darf. Die Angabe erfolgt als einfache Zahl ohne Trennzeichen. Die Uhrzeit 12 Uhr mittags wird wie oben zu sehen, in der Form 120000 (StundeMinuteSekunde je 2 Zahlen) angegeben.

Wird außerhalb der Kernzeit zugegriffen, so wird der Auto-Login für den Zugang vorrübergehend abgeschaltet und mit einem Fehler markiert. Der Benutzer kann sich dann nach den Systemrichtlinien normal anmelden.

Auto-Login Montag-Sontag erlaubt

Hier können Sie die einzelnen Wochentage angeben, an welchen der Zugang per Auto-Login erlaubt sein soll. Ist der aktuelle Wochentag nicht freigegeben, so wird der Auto-Login für den Zugang vorrübergehend abgeschaltet und mit einem Fehler markiert. Der Benutzer kann sich dann nach den Systemrichtlinien normal anmelden.

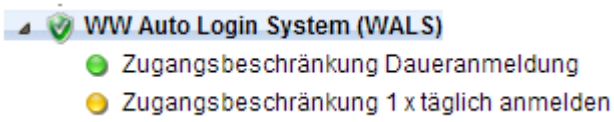
Benutzer dürfen Auto-Login verwenden

Hiermit werden die Intern Benutzer für das Dauer-Auto-Login aktiviert. Werden die übrigen Vorgaben für das Dauerlogin eingehalten, so kann der Benutzer sich direkt ohne Eingabe von Anmeldeinformationen anmelden.

Public-User dürfen Auto-Login verwenden

Hiermit werden die Public-User (öffentliche Benutzer) für das Dauer-Auto-Login aktiviert. Werden die übrigen Vorgaben für das Dauerlogin eingehalten, so kann der Public-User sich direkt ohne Eingabe von Anmeldeinformationen anmelden.

Zugangsbeschränkung 1x täglich anmelden



In diesem Bereich können Sie den Zugang für Automatische Anmeldung, bei der mindestens 1x pro Tag der Benutzer seine Zugangsdaten angeben muss, definieren. Das bedeutet das der Benutzer nach Aktivierung des Zugangs, sich während der erlaubten Zeiten nur jeweils 1x mal täglich anmelden muss. Neben einem SecureNet Netzbereich, der die Netzsegmente beschreibt welche für die Tägliche Daueranmeldung zugelassen sind, gibt es auch die Möglichkeit den Zugang zeitlich zu Begrenzen.

Desweiteren ist es möglich den Bereich für Intern- und Public-User getrennt freizuschalten.

Hier die Parameter für die Zugangsbeschränkung Daueranmeldung im einzelnen:

Beschreibung	Systemwert
SecureNetArea AutoLogin 1x täglich anmelden	**99.98,97 192.168.13**
Zeit-Lock definiert	**J**
Auto-Login erlaubt ab Uhrzeit	0
Auto-Login erlaubt bis Uhrzeit	**240000**
Auto-Login Montags erlaubt	1
Auto-Login Dienstags erlaubt	1
Auto-Login Mittwochs erlaubt	1
Auto-Login Donnerstags erlaubt	1
Auto-Login Freitags erlaubt	1
Auto-Login Samstags erlaubt	1
Auto-Login Sonntags erlaubt	**N**
Benutzer dürfen Auto-Login verwenden	1
Public User dürfen Auto-Login verwenden	1

SecureNetArea AutoLogin 1x täglich anmelden

Hier muss für den täglichen Dauer-Login Bereich die erlaubten Netzbereiche angegeben werden. Hier können bis zu 20 Netzsegmente, für die Festlegung der gültigen Netzbereiche angegeben werden. Alle Netzwerkadressen welche aus Teilen oder Komplett einer der Angaben entspricht haben Zugang zum Dauerlogin Bereich.

Zeit-Lock definiert

Soll der Dauerlogin Bereich zeitlich begrenzt werden. Mit diesem Schalter kann die Prüfung auf die Zeitbegrenzung des Dauerlogin Bereiches erfolgen.

Auto-Login erlaubt ab- bis- Uhrzeit

Hier können Sie die Kernzeiten angeben von wann bis wann der Zugang erfolgen per Auto-Login erfolgen darf. Die Angabe erfolgt als einfache Zahl ohne Trennzeichen. Wie oben in der Parameterliste zu sehen wird der ganze Tag freigeschaltet (0-Uhr bis 24-Uhr). Die Uhrzeit 12 Uhr mittags würde in der Form 120000 (StundeMinuteSekunde je 2 Zahlen) angegeben.

Wird außerhalb der Kernzeit zugegriffen, so wird der tägliche Auto-Login für den Zugang vorrübergehend abgeschaltet und mit einem Fehler markiert. Der Benutzer kann sich dann nach den Systemrichtlinien normal anmelden.

Auto-Login Montag-Sontag erlaubt

Hier können Sie die einzelnen Wochentage angeben, an welchen der Zugang per täglichem Auto-Login erlaubt sein soll. Ist der aktuelle Wochentag nicht freigegeben, so wird der Auto-Login für den Zugang vorrübergehend abgeschaltet und mit einem Fehler markiert. Der Benutzer kann sich dann nach den Systemrichtlinien normal anmelden.

Benutzer dürfen Auto-Login verwenden

Hiermit werden die Intern Benutzer für das Dauer-Auto-Login aktiviert. Werden die übrigen Vorgaben für das Dauerlogin eingehalten, so kann der Benutzer sich direkt ohne Eingabe von Anmeldeinformationen anmelden.

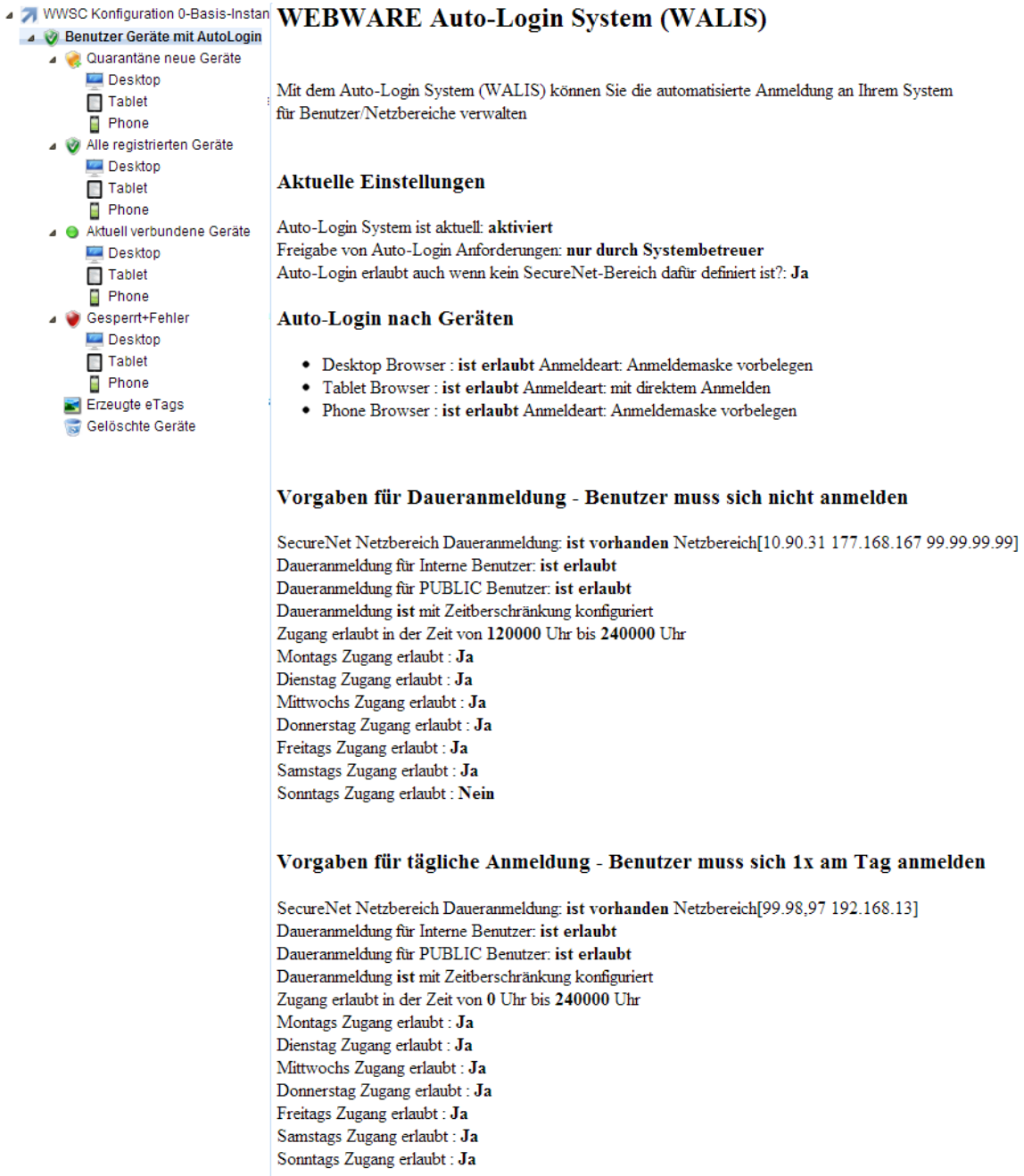
Public-User dürfen Auto-Login verwenden

Hiermit werden die Public-User (öffentliche Benutzer) für das Dauer-Auto-Login aktiviert. Werden die übrigen Vorgaben für das Dauerlogin eingehalten, so kann der Public-User sich direkt ohne Eingabe von Anmeldeinformationen anmelden.

WALIS WEBWARE Auto-Login System - Verwaltung

Im folgenden wird die Verwaltung des WEBWARE Auto-Login System beschrieben. Das WALIS erlaubt es Benutzern sich automatisiert an ihrem WEBWARE System anzumelden. Daher ist hier eine besondere Beachtung der Vorgänge notwendig. Damit Sie als Systembetreuer immer auf dem aktuellen Stand sind, kann WALIS mit Hilfe des WEBWARE Messaging System (WMS) WALIS-Ereignisse per eMail melden. So erhalten Sie zeitnah Hinweise ob neue Benutzeranforderungen vorhanden sind, oder auch ob ein Zugang verwendet wurde.

Es ist wichtig das das automatische Anmelden nur für begrenzte Benutzergruppen, sichere Netzbereiche und die notwendigen Zeiten zu Begrenzen, um einen möglichen Missbrauch vorzubeugen.



Bei Auswahl des Baumeintrages "Bentuzer Geräte mit AutoLogin (WALIS)" erhalten Sie eine Übersicht der aktuellen Einstellungen / Systemrichtlinien für das WALIS angezeigt.

Wie verwalte ich mein WALIS Auto Login System

Steigen Sie hierzu in das System-Cockpit ein. Der WALIS Bereich ist unter Administration und auch Konfiguration (hier mit erweiterten Funktionen) vorhanden.

Hier finden Sie im Funktionsbaum, den Eintrag Benutzer Geräte mit AutoLogin (WALIS). Darunter erhalten Sie jeweils die unterschiedlichen Auto-Login Eintragungen angezeigt.

Eine Auto-Login Beschreibung kann unterschiedliche Zustände haben. Diese finden Sie auch im Funktionsbaum wieder.

Sie können unterhalb der einzelnen Baumfunktionen eine weitere Selektion nach Desktop-Browser, Tablet-Browser und Phone/Mobile-Browser vornehmen.

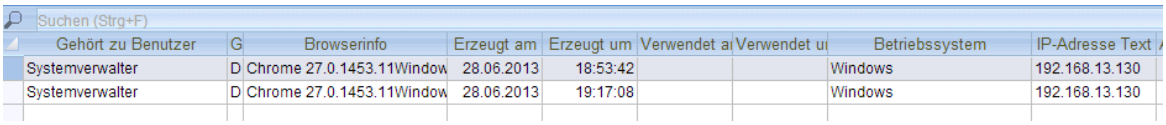
WALIS Workflow für Anforderung von Auto-Login Funktionen

Der Benutzer fordert den Auto-Login an. Dieser Antrag ist in der WALIS-Verwaltung sichtbar. De Systembetreuer prüft den Vorgang und gibt dann den Auto-Login für das entsprechende Benutzer Gerät frei.

Quarantäne neue Geräte

Falls die Systemrichtlinie "Freigabe neuer Auto-Login Geräte durch den Systembetreuer" aktiviert ist, erscheinen hier nach einer Auto-Login Anforderung die Benutzeranträge.

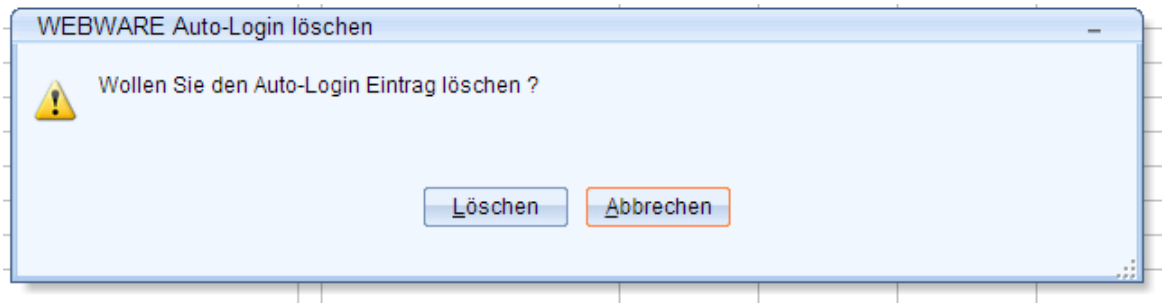
Um einen besseren Überblick zu erhalten kann man die Anzeige nach Desktop, Tablet und Phone selektieren.



In der zugehörigen Liste werden die aktuellen neuen Geräte in Quarantäne angezeigt. Der Systembetreuer kann nach Selektion eines Satzes im Menü aus folgenden Aktionen auswählen.

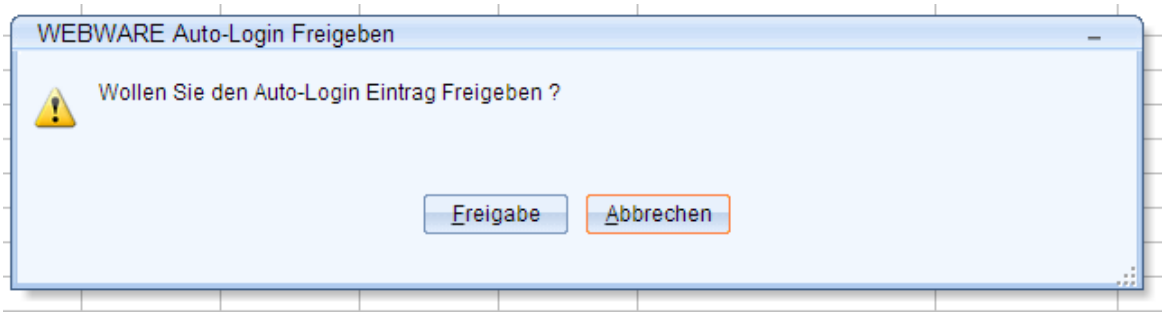
Löschen/Entfernen

Nach Anzeige einer Sicherheitsabfrage wird der Antrag gelöscht und in den Ast Gelöschte Geräte verschoben. Der anfordernde Benutzer erhält in seiner System-Cockpit Anzeige den Hinweis das kein Auto-Login Antrag vorhanden ist.



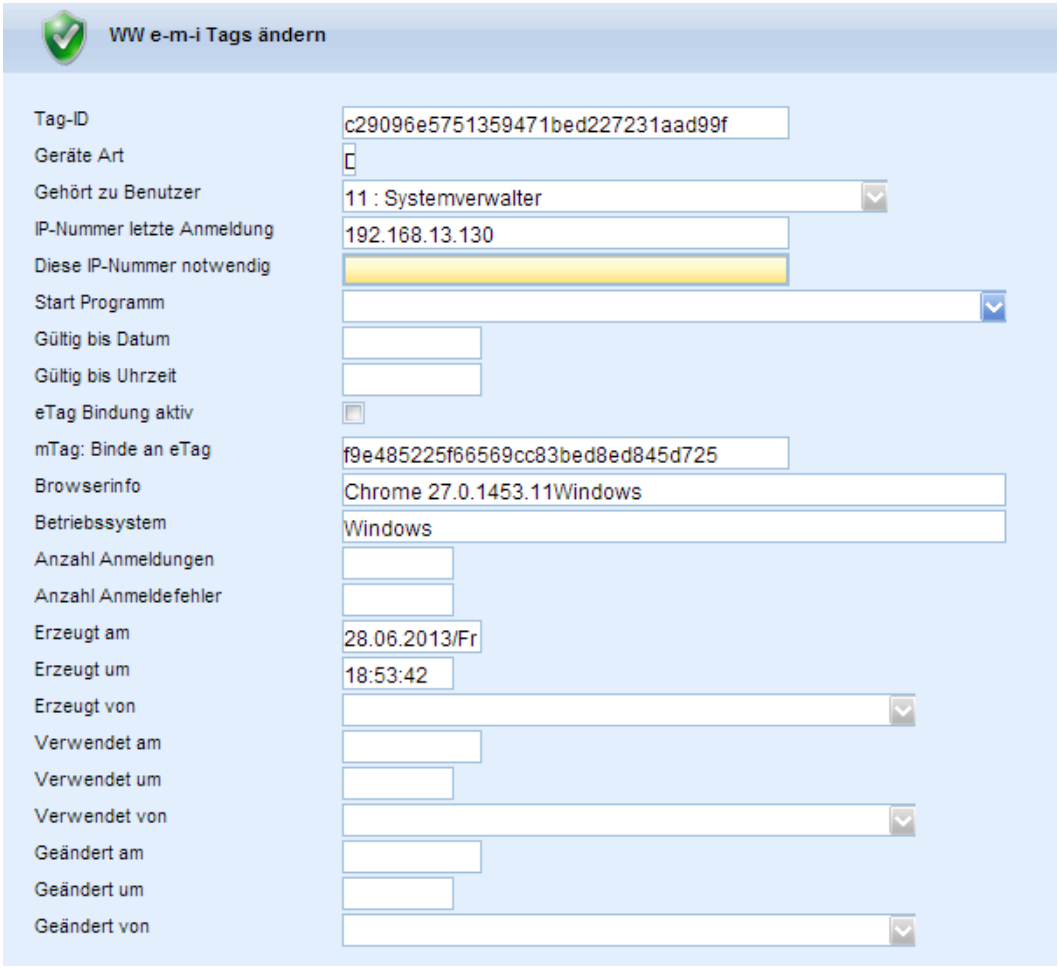
Freigeben

Nach Anzeige einer Sicherheitsabfrage wird der Antrag in den Ast "Alle registrierten Geräte" verschoben. Der Benutzer erhält in seiner System-Cockpit Anzeige den Hinweis das der Auto-Login Zugang für das Benutzer-Gerät verfügbar ist. Beim nächsten Anmelden werden, je nach Systemrichtlinien, die Anmeldedaten vorbelegt, bzw. die Anmeldung direkt ausgeführt.



Details

Hier kann sich der Systembetreuer die genaueren Details des Auto-Login Antrages ansehen.



Alle registrierten Geräte

Hier erscheinen alle Benutzer-Geräte, für die aktuell eine Auto-Login Freigabe erteilt wurde. Sie können die Anzeige nach Desktop, Tablet und Phone selektieren.

In der Liste erhalten Sie weitere Informationen über Erzeugungstermin, letzte Verwendung, IP-Adresse und Anzahl-Anmeldungen/Fehler.

Der Systembetreuer hat nach Selektion eines Eintrages folgende Möglichkeiten.

Löschen/Entfernen

Nach Anzeige einer Sicherheitsabfrage wird der Antrag gelöscht und in den Ast Gelöschte Geräte verschoben. Der anfordernde Benutzer erhält in seiner System-Cockpit Anzeige den Hinweis das kein Auto-Login Antrag vorhanden ist.

Sperren/Quarantäne

Nach Anzeige einer Sicherheitsabfrage wird der Antrag in den Ast Gesperrt/Fehler verschoben. Der Auto-Login ist für dieses Benutzer Gerät dann nicht mehr möglich.

Details

Hier können Details über den Antrag angezeigt werden, aber auch Änderungen an den Vorgaben vorgenommen werden.

Eingabe einer gebundenen IP-Adresse: Im Feld "Diese IP-Nummer notwendig" kann eine feste IP-Nummer angegeben werden, dann ist für diesen Login-Antrag der Auto-Login nur von dieser IP-Adresse möglich. Achten Sie darauf das die IP-Adresse von normalen Internet-Zugängen täglich wechseln kann.

Startprogramm festlegen: Hier können Sie ein Startprogramm festlegen (WWAPP, WWMKOMM, WWPACK) das durch diesen Auto-Login Zugang verwendet wird. Ist das Feld leer, so wird standardmäßig die WWAPPlication gestartet.

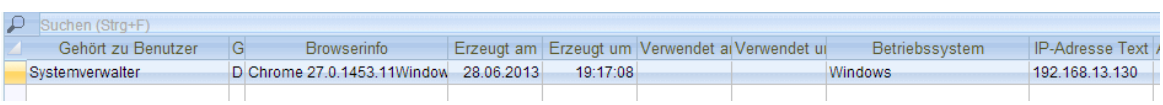
Gültigskeits Zeitraum: Mit den Feldern Gültig bis Datum/Gültig bis Uhrzeit können Sie eine zeitliche Begrenzung für den Auto-Login einbauen. Ab diesem Zeitpunkt ist dann der Auto-Login für diesen Antrag nicht mehr gültig.

eTag Bindung aktiv: Bei Desktop-Browsern ist es möglich eine weitere Sicherheitsebene, das eTag zu verwenden. Dabei wird ein weiterer Wert für die Prüfung herangezogen. Ist dieser Schalter aktiv so wird neben dem Auto-Login Antrag auch das zugehörige eTag geprüft.

Bei Mobile-Browsern kann dieses eTag durch Neustart gelöscht werden.

Aktuell verbundene Geräte

Hier werden alle Auto-Login Geräte angezeigt die aktuell mit einer Anwendung an ihrem WEBWARE System aktiv sind.



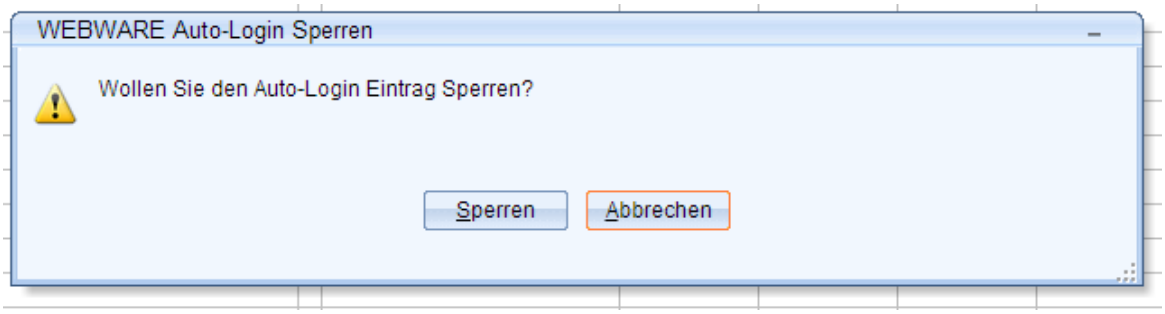
Sie haben nach Auswahl eines Antrages folgenden Möglichkeiten:

Löschen/Entfernen

Nach Anzeige einer Sicherheitsabfrage wird der Antrag gelöscht und in den Ast Gelöschte Geräte verschoben. Der anfordernde Benutzer erhält in seiner System-Cockpit Anzeige den Hinweis das kein Auto-Login Antrag vorhanden ist.

Sperren/Quarantäne

Nach Anzeige einer Sicherheitsabfrage wird der Antrag in den Ast Gesperrt/Fehler verschoben. Der Auto-Login ist für dieses Benutzer Gerät dann nicht mehr möglich.



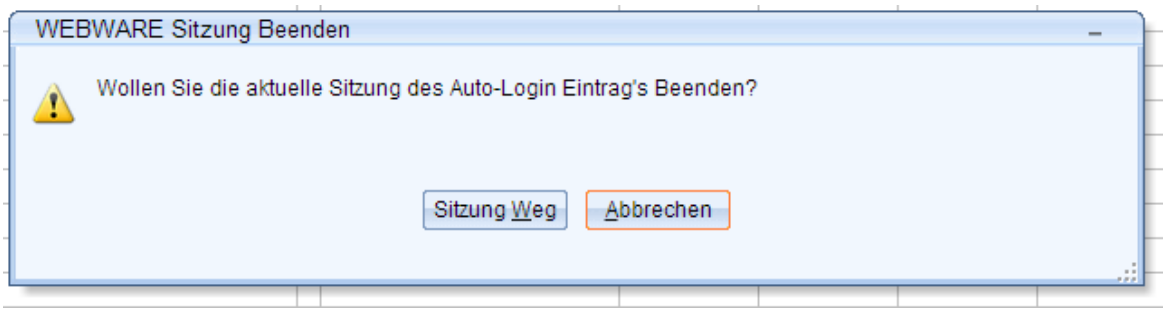
Details

Hier können Details über den Antrag angezeigt werden, aber auch Änderungen an den Vorgaben vorgenommen werden.

Siehe weiter oben unter "Alle registrierte Geräte"

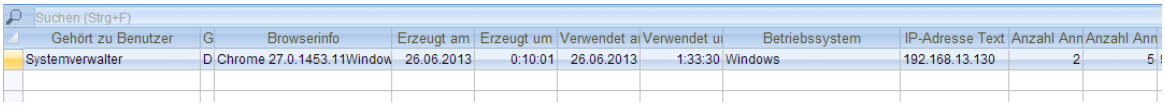
Sitzung Abbrechen

Nach Anzeigen einer Sicherheitsabfrage kann mit diesem Befehl die aktuell verbundene Sitzung Beenden.



Gesperrte+Fehler Geräte

In diesem Bereich werden Anträge aufgeführt wenn Sie manuell gesperrt wurden, bzw. wenn zu viele Fehler bei der Anmeldung aufgetreten sind.



Nach Auswahl eines Antrages aus der Liste haben Sie folgende Möglichkeiten:

Löschen/Entfernen

Der Antrag wird gelöscht und in den Ast Gelöschte Geräte verschoben. Der anfordernde Benutzer erhält in seiner System-Cockpit Anzeige den Hinweis das kein Auto-Login Antrag vorhanden ist.

Freigeben

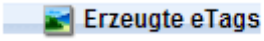
Der Antrag wird in den Ast "Alle registrierten Geräte" verschoben. Der Benutzer erhält in seiner System-Cockpit Anzeige den Hinweis das der Auto-Login Zugang für das Benutzer-Gerät verfügbar ist. Beim nächsten Anmelden werden, je nach Systemrichtlinien, die Anmeldedaten vorbelegt, bzw. die Anmeldung direkt ausgeführt.

Details

Hier können Details über den Antrag angezeigt werden, aber auch Änderungen an den Vorgaben vorgenommen werden.

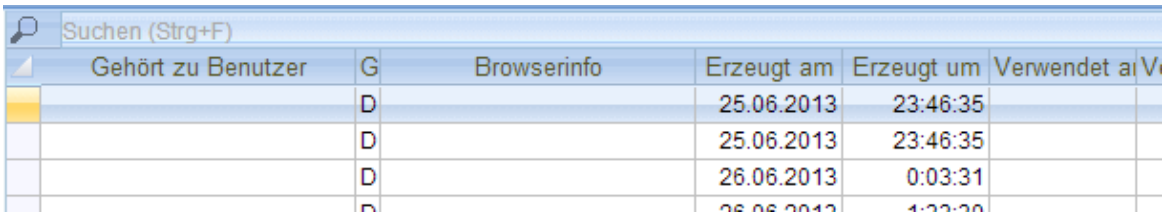
Siehe weiter oben unter "Alle registrierte Geräte"

Erzeugte eTags



Dieser Eintrag ist nur in der System-Konfiguration verfügbar. In der System-Administrations Ansicht ist er nicht vorhanden.

Bei Anmeldung eines Benutzer-Gerätes vergibt ihr WEBWARE-System eine eindeutige Kennung die im Benutzer Gerät abgelegt wird. Diese Kennung bleibt bis zum Löschen des Cache's erhalten. Daher ist das eTag aktuell nur bei Desktop-Browsern sicher einsetzbar. Mobile Browser können bei Speichermangel dieses eTag löschen.



Es besteht die Möglichkeit den Auto-Login Zugang an dieses eTag zu Binden. eTag's sind nicht Benutzerspezifisch, daher wird in der Liste keine "Gehört zu Benutzer" Info angezeigt.

Sie haben folgende Möglichkeiten mit einem Selektierten eTag:

Löschen/Entfernen

Das eTag wird in den Ast Gelöschte Geräte verschoben. Falls ein Auto-Login Antrag mit einem eTag verbunden war, ist ein Anmelden mit diesem Auto-Login Antrag nicht mehr möglich

Details:

Hier kann man sich genauere Info's über das eTag anschauen.

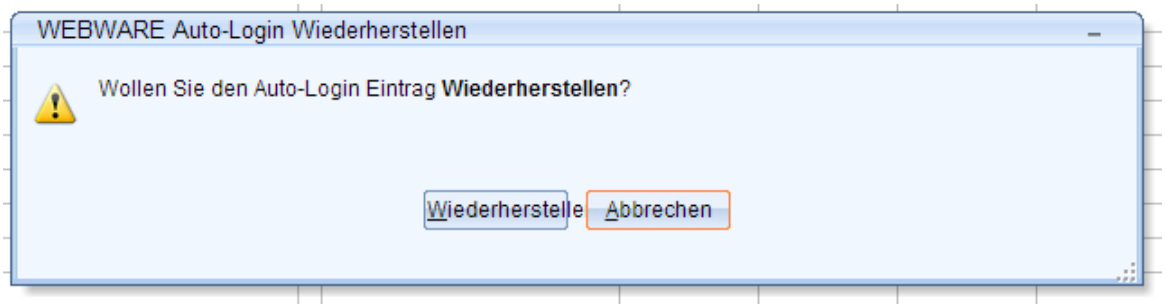
Gelöschte Geräte

Hier werden die gelöschten Geräte aufgeführt. Diese sind bis zum nächsten Systemstart verfügbar. Danach werden diese unwiederbringlich gelöscht. Sie haben die Möglichkeit Geräte aus der Liste wiederherzustellen.

Folgende Menübefehle stehen zur Verfügung.

Wiederherstellen

Mit diesem Befehl kann ein gelöschter Antrag wieder zurückgeholt werden. Nach Anzeige einer Sicherheitsabfrage wird der Antrag in den Ast Alle registrierten Geräte



Details

Hier können Details über den Antrag angezeigt werden, aber auch Änderungen an den Vorgaben vorgenommen werden.

Siehe weiter oben unter "Alle registrierte Geräte"

WW SHIELD Geräte Zugangs Kontrolle Konfiguration

Mit WW SHIELD können Sie den Zugang zu Ihrem WEBWARE System Begrenzen. Dabei ist es möglich Benutzer-Geräte (Desktop-Browser, Tablet-Browser und Phone/Mobile Browser) zu kennzeichnen und abhängig vom Netzsegment/Adresse des Gerätes den Zugang automatisch zu gewähren, oder aber erst nach Freigabe durch den Systembetreuer.

Es gibt die Möglichkeit neben der Konfiguration für IntraNet und InterNet einen eigenen SecureNet Bereich zu definieren aus dem die Anmeldung mit neuen Geräten immer erfolgen darf.

Die lokalen WEBWARE-Server Netzwerkadresse ebenfalls nicht mit dem Zugangsschutz zu Versehen. Dies soll ein Aussperren aus ihrem WEBWARE-System verhindern.

Konfiguration der WW-SHIELD Zugangs Kontrolle

Die Konfiguration der WW-SHIELD Zugangs Kontrolle erfolgt im System-Cockpit im Bereich System-Konfiguration, Logon/Anmelde Vorgaben.

Um die WW-SHIELD Zugangs Kontrolle zu aktivieren, muss der System-Wert "Neue Geräte müssen vom Admin freigegeben werden" aktiviert werden. Ebenso muss der Parameter "Benutzer Geräte Registrieren" aktiviert sein.

Beschreibung	Systemwert
Neue Geräte müssen vom Admin freigegeben werden	J
Netzbereich aus dem keine Freigabe notwendig ist	192.168.99 192.168.98
Benutzer Geräte Registrieren ist aktiviert	J

Dies führt dazu das jedes neue Gerät das an Ihrem WEBWARE System angemeldet wird mit einer Kennzeichnung versehen wird.

Möchten Sie einzelne Netzwerk-Bereiche/Segmente aus der Aktivierungspflicht herausnehmen, so können Sie dies mit dem SecureNet Bereich "Netzbereich aus dem keine Freigabe notwendig ist" angeben.

Beispiel: Sie haben ein internes Firmen-Netz 192.168.99. Geräte aus diesem Netzsegment sollen sich ohne Freigabe anmelden können. So geben Sie wie oben im Beispiel den 192.168.99 an. Sie können bis zu 20 Netzsegmente bzw. genaue Adressen für den Zugriff ohne Anmeldezwang angeben.

Grundsätzlich sind die lokalen Netzwerkadressen des WEBWARE-Server's von der Freigabepflicht ausgenommen, um ein Blockieren des Zugangs zu verhindern.

Erst Durch die Festlegung in der IntraNet und InterNet Definition, welche Geräteklassen freigegeben werden müssen, ist die Zugangskontrolle einsatzbereit.

WW SHIELD IntraNet Vorgaben

Nachdem die Zugangs Kontrolle aktiviert ist, können Sie im Bereich IntraNet Anmeldung angeben welche Geräteklassen im IntraNet durch einen Systembetreuer freigegeben werden müssen.

Beschreibung	Systemwert
Neue Desktop Geräte muss Admin freigeben	0
Neue Tablet Geräte muss Admin freigeben	0
Neue Phone Geräte muss Admin freigeben	0

Standardmäßig sind die Prüfungen im IntraNet deaktiviert.

WW SHIELD InterNet Vorgaben

Für alle Netzwerksegmente die als InterNet definiert sind, gelten die Geräteklassenvorgaben im Bereich Inter-Net Anmeldung.

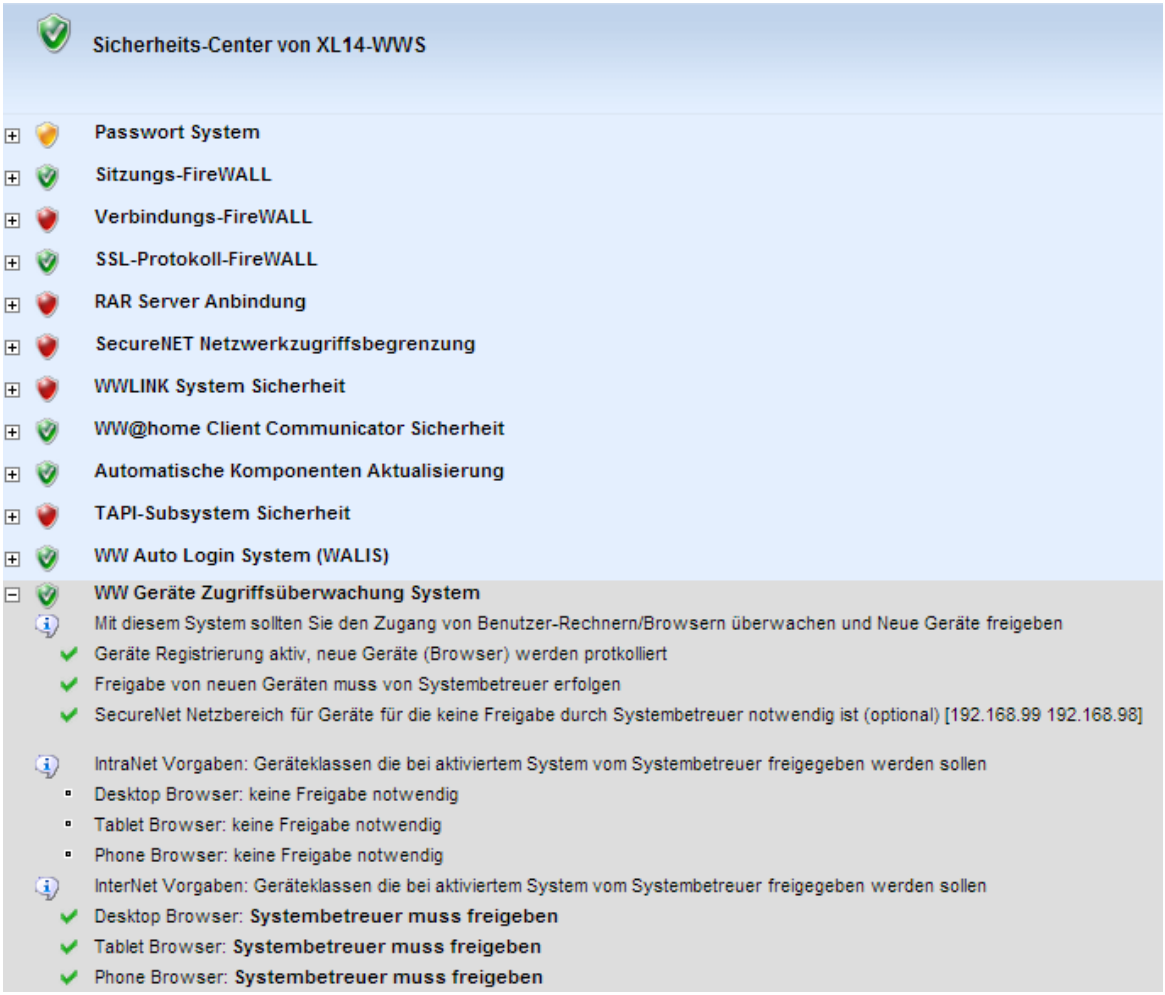
Beschreibung	Systemwert
Neue Desktop Geräte muss Admin freigeben	**J**
Neue Tablet Geräte muss Admin freigeben	**J**
Neue Phone Geräte muss Admin freigeben	**J**

Standardmäßig sind die Prüfungen im IntraNet aktiviert.

Sicherheits-Center WW SHIELD Zugangs Kontrolle

Die WW-SHIELD Zugangs Kontrolle ist direkt auch in den WEBWARE Sicherheits-Center integriert. Dort sehen Sie auf einen Blick welche Parameter für WW SHIELD gesetzt sind. Wichtig ist hier das der Systembetreuer die Hoheit über die Freigabe und Zugriffe auf das WEBWWARE System hat.

Die Freigabe der Zugangsberechtigung kann vom Systembetreuer pro Benutzer/Gerät erfolgen. Dabei kann er dies je nach Geräte Kategorie, also Desktop Browser, Tablet Browser und Phone Browser und entsprechendem Netz vorgeben.



Durch Klick auf die einzelnen Zeilen, können Sie direkt in den betreffenden Systemwert wechseln, und diesen Ändern.

Wichtig: Die Zugriffs Kontrolle ist erst dann aktiv, wenn mindestens eine Geräteklasse in IntraNet oder InterNet für die Freigabe durch den Systembetreuer aktiviert ist.

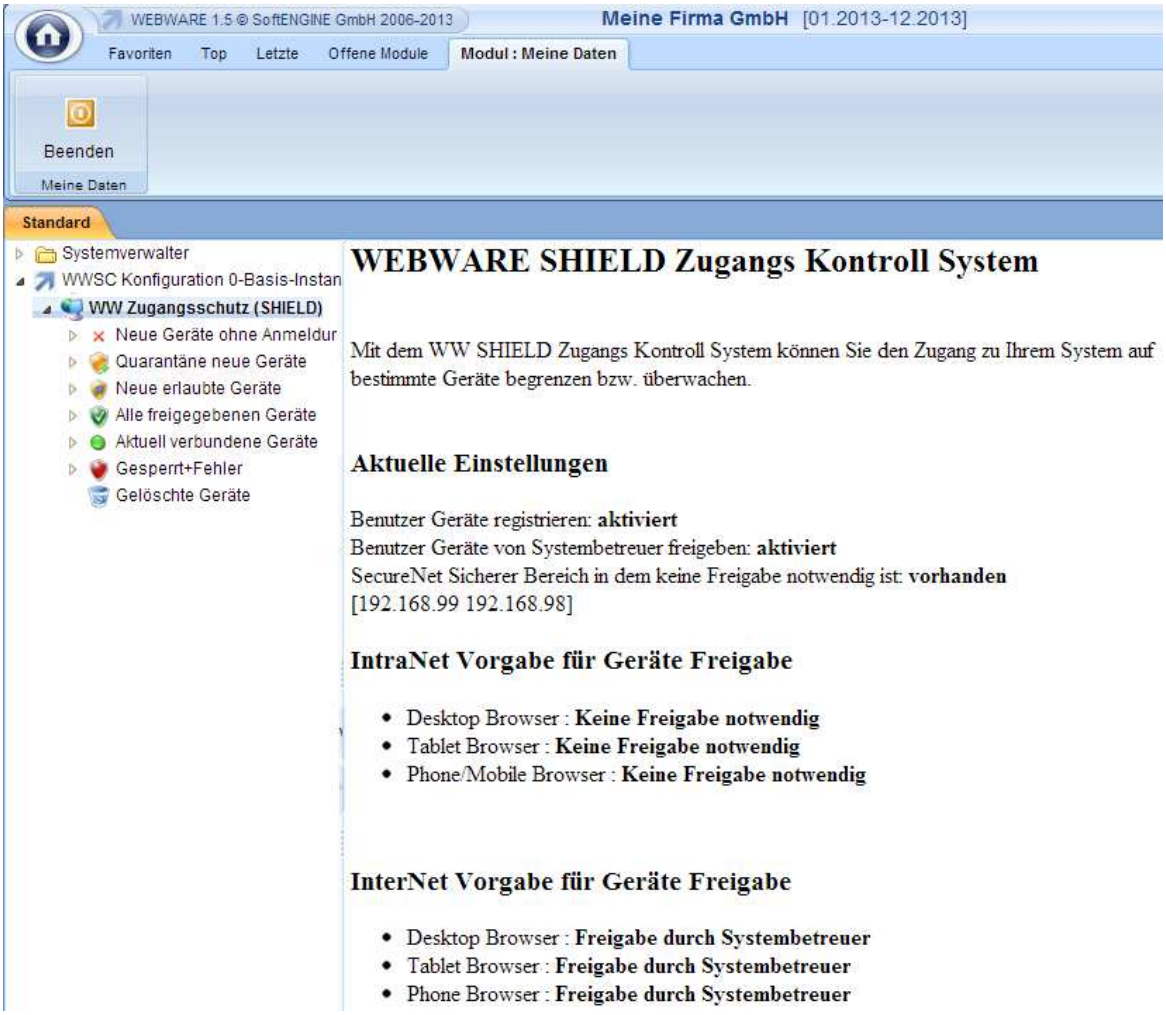
Info's zu den einzelnen Systemwerten finden Sie im weiteren oben.

WW SHIELD Geräte Zugangs Kontrolle - Verwaltung

Im folgenden wird die Verwaltung des WEBWARE SHIELD Zugangs Kontroll System beschrieben. Das WW SHIELD erlaubt den Zugang pro Gerät erst nach Freigabe durch den Systembetreuer und bietet damit eine erhöhte Sicherheit.

Damit Sie als Systembetreuer immer auf dem aktuellen Stand sind, kann WW SHIELD mit Hilfe des WEBWARE Messaging System (WMS) WW SHIELD-Ereignisse per eMail melden. So erhalten Sie zeitnah Hinweise ob neue Benutzeranforderungen vorhanden sind, oder ob sich Zustände von Zugängen geändert haben.

Sie finden den WW-SHIELD Bereich im System-Cockpit unter Administration und Konfiguration (erweiterte Funktionen) wie sie der unten stehenden Grafik entnehmen können.



Bei Auswahl des Baumeintrages "WW Zugangsschutz (SHIELD) erhalten Sie eine Übersicht der aktuellen Einstellungen / Systemrichtlinien für das WW SHIELD angezeigt.

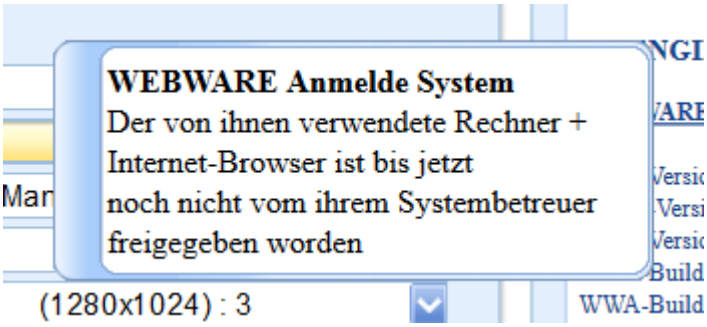
WW-SHIELD Zugangs Kontroll Workflow

Nach Aktivierung der WW-SHIELD Zugangs Kontrolle, werden alle neu verbundenen Browser-Geräte mit einer Kennung versehen und in einer internen Datenbank mit ihrem aktuellen Zugangs-Status gespeichert.

Bei neuen Geräten wird also je nach WW SHIELD Konfiguration zuerst die Freigabe durch den Systembetreuer angefordert.

Beim Zugang prüft nun die WW SHIELD Verwaltung ob das Gerät bereits eine Freigabe hat, oder ob sich das Gerät aus einem Netzwerk-Bereich anmeldet der Zugang ohne Freigabe erlaubt. Trifft mindestens eine der beiden Prüfungen zu, so wird der Zugang gewährt.

Ansonsten erhält der Benutzer einen Hinweis das die Prüfung noch nicht abgeschlossen ist.



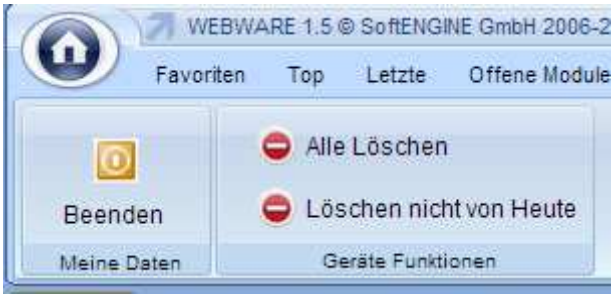
Die Zugangsinformationen werden unterhalb des WW Zugangsschutz (SHIELD) Eintrages in folgende Bereiche unterteilt:

- Neue Geräte ohne Anmeldung
- Quarantäne neue Geräte
- Neue erlaubte Geräte
- Alle freigegebenen Geräte
- Aktuell verbundene Geräte
- Gesperrt + Fehler
- Gelöschte Geräte

Genauere Informationen finden sie in den folgenden Abschnitten. Unterhalb dieser Zustandseinträge kann weiter nach Gerätetype (Desktop/Tablet/Phone-Mobile) selektiert werden.

Neue Geräte ohne Anmeldung

In diesem Bereich werden Geräte/Browser angezeigt die bisher eine Verbindung zu Ihrem WEBWARE-Server System aufgebaut haben, jedoch bisher noch keine erfolgreiche Anmeldung durchgeführt wurde.



Da hier durch automatisierte Angriffe eine große Anzahl von Einträgen entstehen können, gibt es hier im Menü 2 Funktionen mit denen Sie gezielt alle, bzw. alle die vor dem heutigen Tage erstellt wurden, entfernen.

Diese beiden Befehle sind nur sichtbar wenn kein Geräte ausgewählt ist.

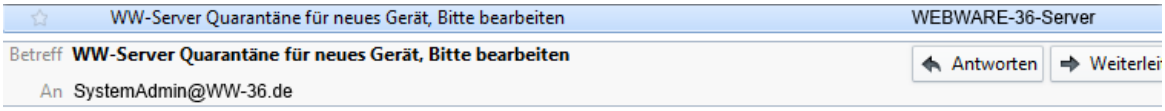
Da bisher keine Benutzeranmeldung für dieses Gerät erfolgt ist, kann die Verbindung zum Benutzer in der Liste der "neuen Geräte ohne Anmeldung" nicht angezeigt werden.

Gehört zu Benutzer	G	Browserinfo	Erzeugt am	Erzeugt um	Verwendet a	Verwendet u	Betriebssystem	IP-Adresse Text
	D	MSIE 10.0;	1.07.2013	13:50:47			Windows	192.168.13.101

Werden einzelne Geräte ausgewählt, so kann man diese mit dem Befehl Löschen/Entfernen in den Ast "Gelöschte Geräte" verschieben.

Quarantäne neue Geräte

Nachdem sich ein Benutzer erstmalig mit einem neuen Gerät/Browser an Ihrer WEBWARE erfolgreich angemeldet hat, erhält er einen Hinweis das der Zugang zuerst von einem Systembetreuer freigeschaltet werden muss. Gleichzeitig wird über das WW Messaging System (WMS) eine eMail an den Systembetreuer versendet mit Info's und Aufforderung zur Prüfung und Freigabe des neuen Gerätes:




```
WEBWARE Geräte Zugangs Überprüfung.

BITTE BEARBEITEN.
System Cockpit im Bereich Geräte Prüfung : Quarantäne neue Geräte

Details:
Bei Ihrem WEBWARE System (XL14-WWS-Basis-Instanz) wurde ein neues Gerät (Desktop-MSIE
10.0;-20130701-13504718-2fc9a59e2fb2743192eff8d99eb4652a)
registriert.

Benutzer (Mitarbeiter 1) hat am 14:02:07 01.07.2013 mit der
IP-Adresse (192.168.13.101) das Gerät zum ersten mal verwendet.

Die aktuellen Systemrichtlinien erlauben keinen Zugriff
ohne Eingriff des Systembetreuers.
```

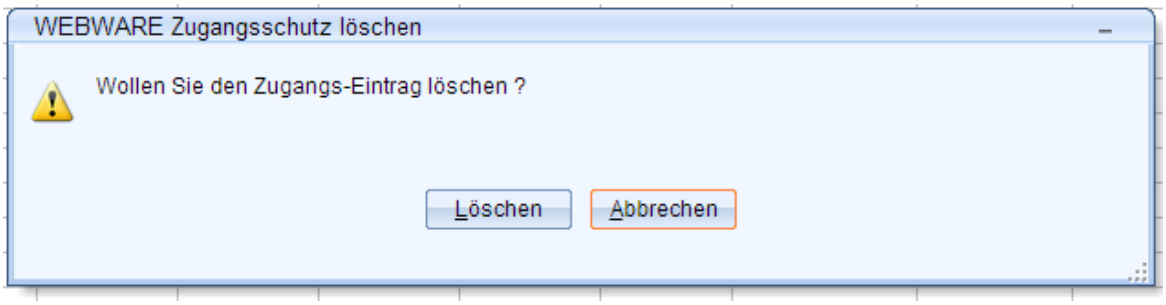
Innerhalb des System-Cockpit wird nun die erfolgreiche Anmeldung im Bereich Quarantäne neue Geräte angezeigt.

Gehört zu Benutzer	G	Browserinfo	Erzeugt am	Erzeugt um	Verwendet a	Verwendet u	Betriebssys	IP-Adresse Text
Systemverwalter	D	Firefox 21.0	1.07.2013	11:58:55	1.07.2013	11:59:09	Windows	192.168.13.130
Mitarbeiter 1	D	MSIE 10.0;	1.07.2013	13:50:47	1.07.2013	14:02:07	Windows	192.168.13.101

Selektieren Sie nun eines der Geräte das Sie freigeben wollen, dann stehen Ihnen im Menü folgende Funktionen zur Verfügung

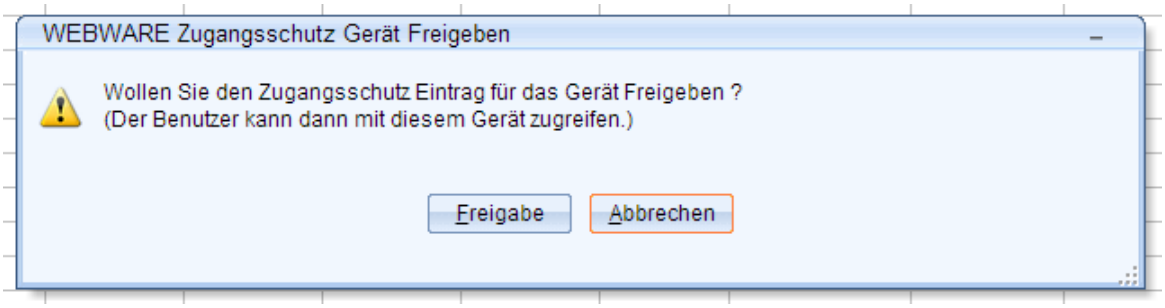
Löschen/Entfernen

Der Eintrag wird nach einer Sicherheitsabfrage in den Ast Gelöschte Geräte verschoben.



Freigeben

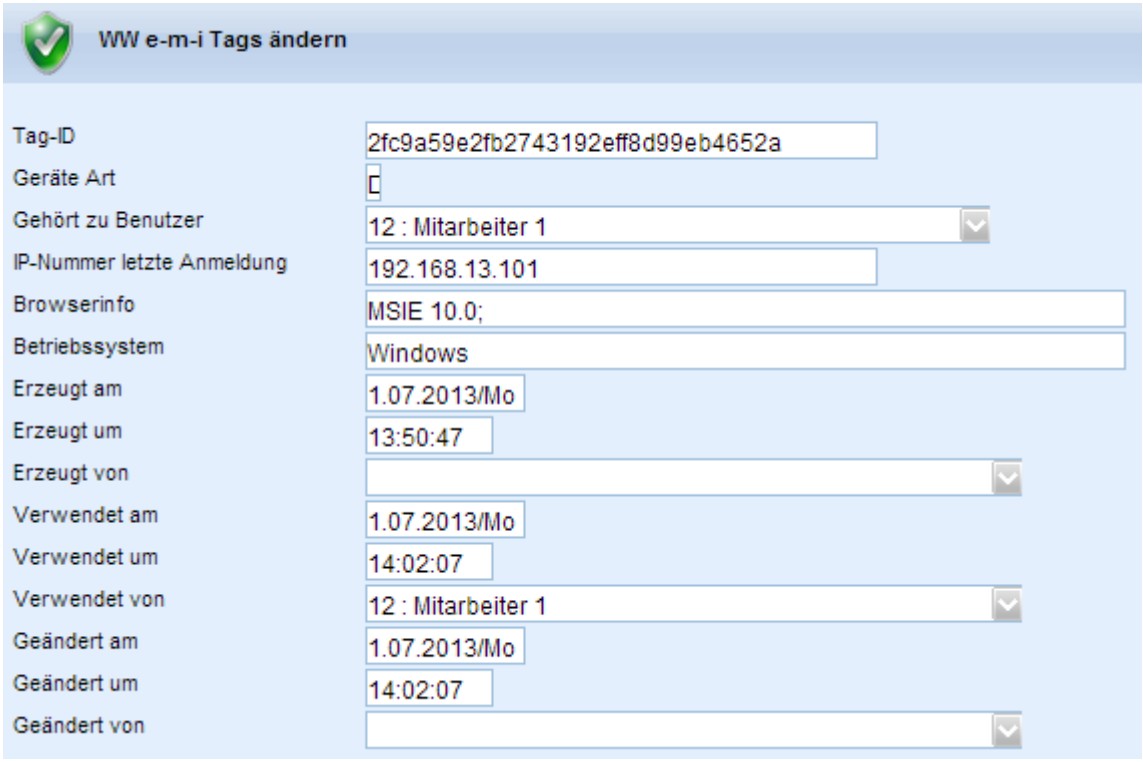
Der Eintrag wird nach einer Sicherheitsabfrage in den Ast Alle freigegebenen Geräte verschoben.



Wurde der Eintrag freigegeben, so kann der Benutzer ab diesem Zeitpunkt mit dem Gerät normal auf Ihre WEBWARE zugreifen.

Details

Mit Details, können Sie sich Info's über die Gerätefreigabe anzeigen lassen.



Die TAG-ID ist eine Konstante die für als Gerätekennung erzeugt wird. Die Geräte Art kann den Wert D=Desktop/T=Tablet oder P=Phone haben.

Neben der Benutzerkennung, erhält man auch Infos über die zugehörige IP-Adresse sowie Browser und Betriebssystem.

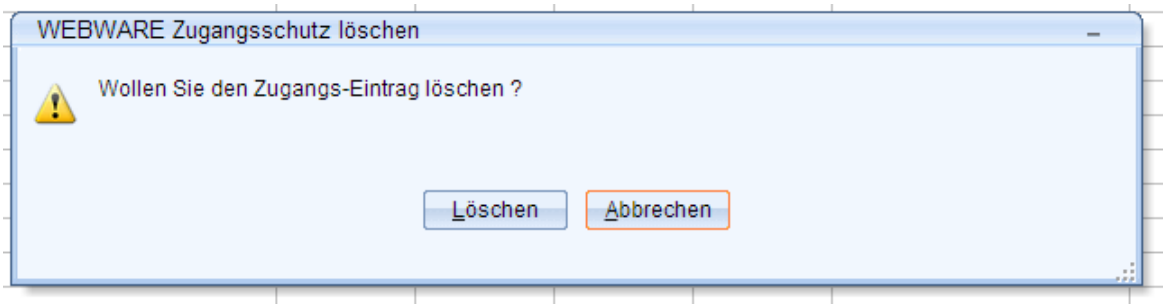
Neue erlaubte Geräte

Hier werden alle Geräte registriert, die auf Grund der Systemrichtlinien, keine Freigabe durch den Systembetreuer benötigen. Werden später die System-Richtlinien so geändert das eine Freigabe durch den Systemverwalter notwendig wird, so werden diese Einträge beim nächsten Zugriff automatisch in den Bereich Quarantäne neue Geräte verschoben, sowie der Benutzer darüber informiert.

Sie können die Anzeige durch Auswahl der Unterordner nach Geräte Kategorien sortieren und anzeigen.

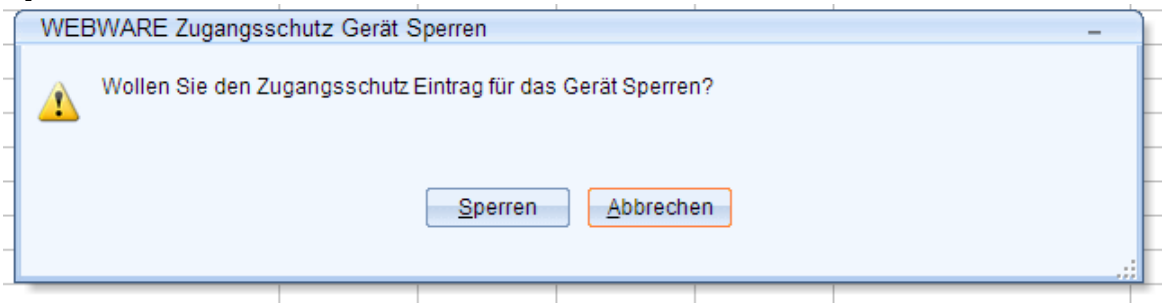
Folgende Funktionen stehen nach Selektion eines Gerätes zur Bearbeitung zur Verfügung.

Löschen/Entfernen



Nach einer Sicherheitsabfrage wird der Eintrag in den Ast Gelöschte Geräte verschoben.

Sperren/Quarantäne



Nach einer Sicherheitsabfrage wird der Eintrag in den Ast Gesperrt + Fehler verschoben. Die Anmeldung für das Gerät wird damit unterbunden.

Details

Anzeige von weiteren Informationen für den Zugangsschutz Eintrag. Nähere Infos siehe weiter oben.

Alle freigegebenen Geräte

Hier finden Sie alle Geräte die vom Systembetreuer für den Zugriff auf dieses WEBWARE System freigegeben wurden.

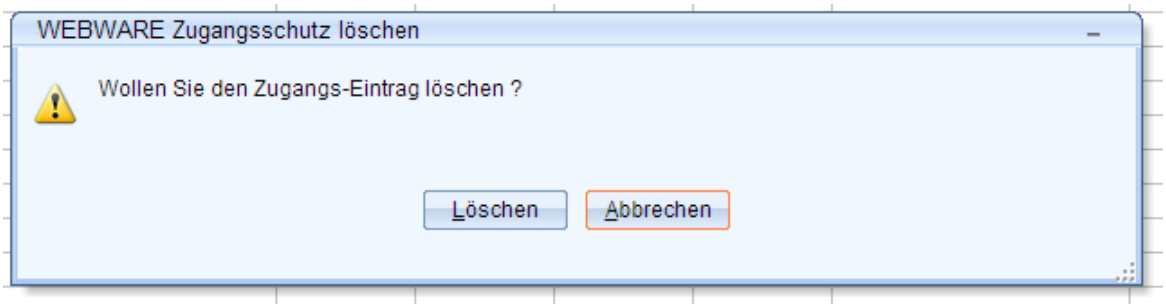
Sie können die Anzeige durch Auswahl der Geräteklassen einschränken.

Geräte die in diesem Bereich angezeigt werden, dürfen sich ohne Einschränkungen an der WEBWARE anmelden.

Nach Selektion eines Geräteeintrages stehen Ihnen folgende Befehle im Menü zur Verfügung:

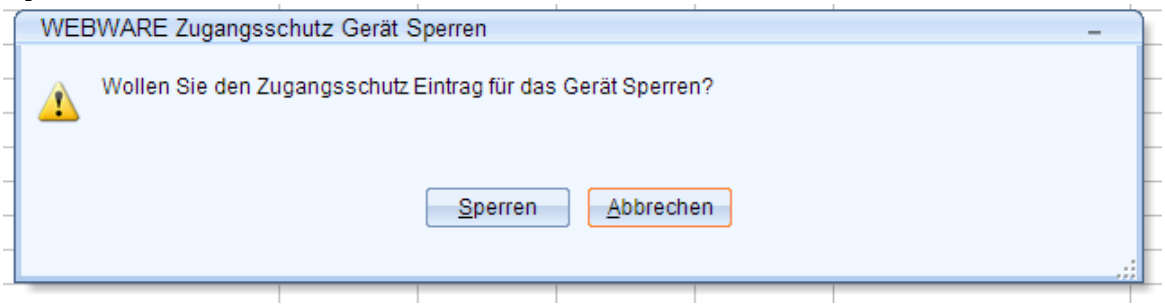
Folgende Funktionen stehen nach Selektion eines Gerätes zur Bearbeitung zur Verfügung.

Löschen/Entfernen



Nach einer Sicherheitsabfrage wird der Eintrag in den Ast Gelöschte Geräte verschoben.

Sperren/Quarantäne



Nach einer Sicherheitsabfrage wird der Eintrag in den Ast Gesperrt+Fehler verschoben. Die Anmeldung für das Gerät wird damit unterbunden.

Details

Anzeige von weiteren Informationen für den Zugangsschutz Eintrag. Nähere Info's siehe weiter oben.

Aktuell verbundene Geräte

Hier werden alle Zugangs-Geräte angezeigt die zur Zeit mit diesem WEBWARE-Server System verbunden sind.

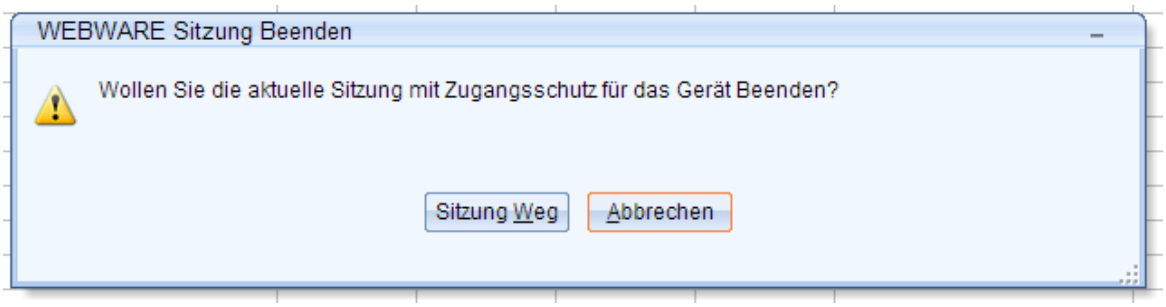
Sie können die Anzeige durch Auswahl der Geräteklasse eingrenzen.

Folgende Funktionen stehen nach Selektion eines Gerätes zur Bearbeitung zur Verfügung.

(Löschen/Entfernen+Sperren/Quarantäne+Details siehe weiter oben)

Sitzung Abbrechen

Mit diesem Befehl können Sie nach Bestätigung der Sicherheitsabfrage die Zugehörige Sitzung abbrechen.



Gesperrt + Fehler

Hier finden Sie alle manuell gesperrten bzw. durch Anmeldefehler gesperrten Zugangs-Geräte.

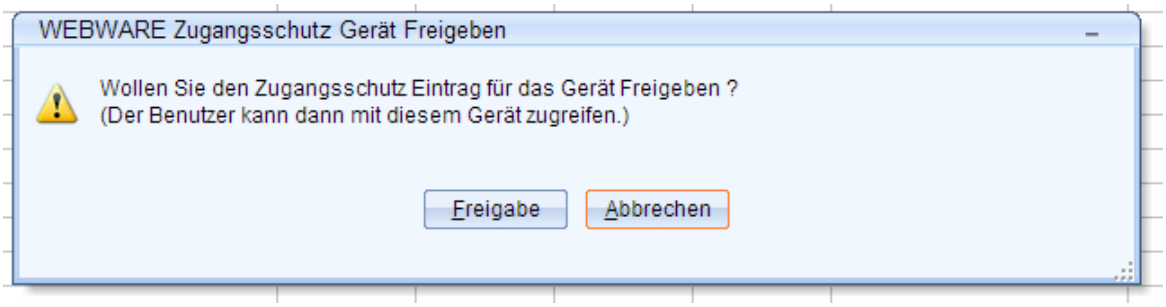
Durch Auswahl einer Geräteklasse können Sie die Anzeige weiter eingrenzen.

Sie haben nach Selektion eines Geräte-Eintrages folgende Menüfunktionen

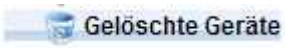
(Löschen/Entfernen + Details, siehe weiter oben.)

Freigeben

Nach Bestätigung der Sicherheitsabfrage, kann der Benutzer mit seinem Gerät uneingeschränkt auf Ihr WEBWARE System zugreifen.



Gelöschte Geräte



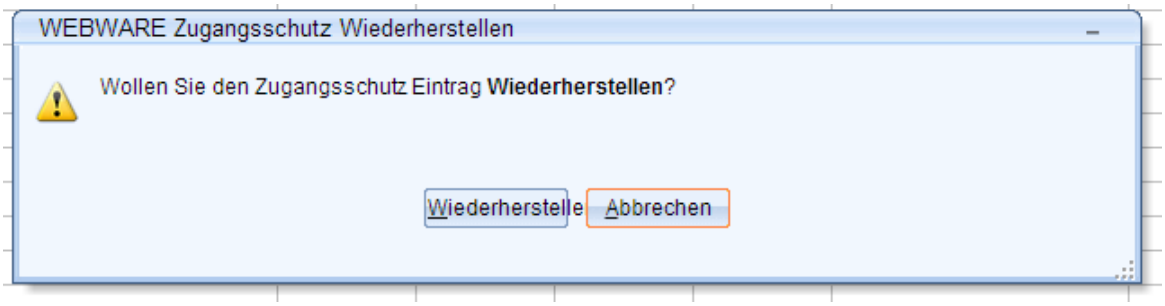
Hier werden alle Geräte aufgelistet die während der aktuellen WEBWARE-Server Laufzeit gelöscht wurden. Durch einem WEBWRE-Server-Neustart wird diese Liste geleert.

Nach Selektion eines Satzes haben Sie folgende Menü-Funktionen:

(Details siehe weiter oben).

Wiederherstellen

Nach Bestätigung einer Sicherheitsabfrage, wird der Datensatz wieder hergestellt. Er wird damit aus dem Ast "Gelöschte Geräte" in den Ast "Alle freigegebene Geräte" verschoben.



WW-LINK automatisiertes Zugangs- und Zugriffsystem

Was ist WW-LINK ?

WWLINK- ist ein integriertes System, mit dem Zugangspunkte per WEB-Link erstellt werden können. Über diese Zugangspunkte können Benutzer und Services auf Ihre WEBWARE Installation zugreifen. Dabei wird nach Benutzerart und Anmeldevorgang unterschieden.

Bei der Erzeugung eines WW-LINK, auf Anwendungsebene, werden dabei Informationen vorgegeben die beim Auslösen eines WW-LINK, den direkten Sprung in eine Anwendungsfunktion, bzw. das Ausführen von Workflow's, mit Übergabe von Parametern, ermöglichen.

Welche Informationen beinhaltet ein WW-LINK ?

- Firmen-Mandanten Zugehörigkeit

  Ein Link wird immer genau einer Installation/Firma/Mandant zugeordnet. Die Verwendung von WW-LINK's über Firmengrenzen hinweg ist nicht möglich.

- WW-LINK Schlüssel

  Der Zugriffs-Schlüssel wird mit einem 32-Byte Hash-Wert gesetzt. Dieser Wert ist eindeutig für den WW-LINK und wird bei externen Zugriffen (https://...Serveradresse.../@LNK.....) sowie bei der internen Benutzung über die WW-Application verwendet.

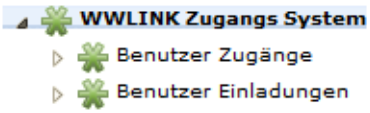
- Arten von WW-LINK's

  Grundsätzlich werden 3 Arten von WW-LINK's nach Benutzergruppen unterschieden.

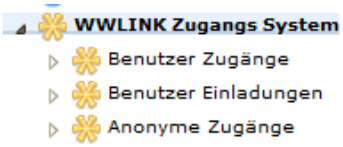
  - Mitarbeiter (Zugang über normale WEBWARE-Anmeldung)
  - Öffentliche Mitarbeiter (Zugang über Public-User System, mit eingeschränkten Rechten)
  - Service-Schnittstelle (Automatisierung, und Ausführung auf Workflow-Server Ebene)

  Die einzelnen WW-LINK's haben je nach Benutzergruppe weitere Unterscheidungen.

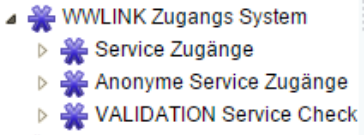
  - Normaler Zugangspunkt
  - Einladungs Zugangspunkt
  - Anonymer Zugangspunkt
  - Validation Service



Mitarbeiter Zugänge



Öffentliche Benutzer Zugänge



Service Zugänge

- Status eines WW-LINK's

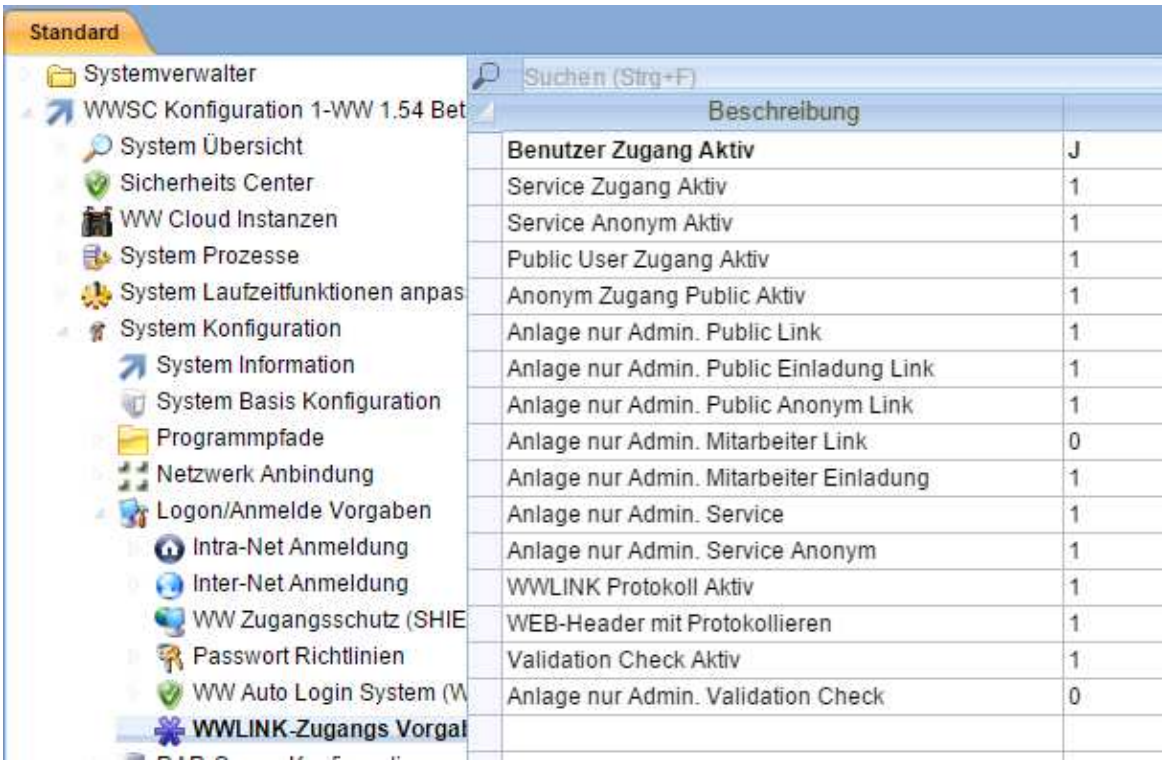
  Ein WW-LINK kann Neu, Benutzt, Gesperrt und Gelöscht sein.

- Beschreibung des WW-LINK's
- Zeitliche Zugangsbeschränkung

  Hier kann ein Datumsbereich angegeben werden, in dem der WW-LINK gültig ist. (Start-, Endedatum)
- Begrenzung der Anzahl Aufrufe
- Anzahl Anonyme Aufrufe
- Start-Workflow und Parameter
- Protkoll über jeden Zugriff auf den Link

Konfiguration und Aktivierung von WW-LINK

Die Verwendung von WW-LINK kann im WW-System-Cockpit im Bereich Konfiguration > System-Konfiguration > WWLINK-Zugangs Vorgaben gemacht werden. Hier können die einzelnen WW-LINK-Zugangsarten (Mitarbeiter, Öffentlich, Service) sowie Ihre Ausprägung (Mit Anmeldung, Anonym) aktiviert werden.



Ebenso kann man hier festlegen ob man zum Erzeugen eines der WW-LINK-Arten Administrator Berechtigung benötigt.

Um einen Überblick auf die WW-LINK Zugriffe zu erhalten, kann hier die WW-LINK Protokollierung aktiviert werden. Um eine Auswertung von WEB-Zugriffen auf einen WW-LINK besser auswerten zu können, ist es auch möglich die Speicherung der HTTP-Protokoll-Daten pro Zugriff zu aktivieren.

Wie wird ein WW-LINK erzeugt ?

Die Erzeugung eines WW-LINK's erfolgt auf Anwendungsebene durch 2 neue GET_RELATION's [4006],[4007]. Dabei wird mit GETREL-4006 ein WW-LINK neu angelegt, und mit GETREL-4007 werden WW-LINK's verwaltet und ausgewertet. Je nach Vorgaben im WW-System-Cockpit ist das Erzeugen von WW-LINK's auf Benutzer mit Administrator Berechtigung begrenzt.

Hier nun die Beschreibung der beiden GETREL-Funktionen

GETREL 4006 Anlegen eines WWLINK's

GET_RELATION[4006!LINKART!LINK_KEY_ID_NAME!ERLAUBT_AB!ERLAUBT_BIS!ERLAUBT_MAX_AUFRUFE!LINK_DESC !START_WORKFLOW!WORKFLOW_PARAM_FORMAT!WORKFLOW_PARAMTER!LINK_USER_ID!ANONYM_MAX_AUFRUFE]

Folgende Übergabeparameter:

- **LINKART**
  Vorgabe welche Art von Link erzeugt werden soll, Werte 10,11,12,20,21,30 und 31
  - 10: Public User Link Link der in einer Public-User-Sitzung gültig ist
  - 11: Public User Einladung für einen Public-User, für Neu-Anmeldung, es wird ein Einmal-Passwort gesetzt
  - 12: Public User Anonym. Zugang für Public-User Sitzung ohne notwendige Anmeldung, Wichtig Nutzer-ID vorgeben und Anzahl erlaubte Anonyme Anmeldungen vorgeben
  - 20: Benutzer Link der in einer Benutzer-Sitzung gültig ist
  - 21: Benutzer Einladung für einen Benutzer, für Neu-Anmeldung, es wird ein Einmal-Passwort gesetzt
  - 30: Service Link erstellen der vom System-Server ohne Benutzersitzung ausgeführt wird, hier ist eine Anmeldung notwendig
  - 31: Service Anonym Servicelink der vom System-Server ohne Benutzersitzung ausgeführt wird, hier ist keine Anmeldung notwendig
  - 32: Service Validation Servicelink der vom WEBWARE Server ohne Benutzersitzung ausgeführt wird, es wird mit HTTP_Status Code die Validierung zurückgegeben.
- **LINK_KEY_ID_NAME**
  Optionaler Name für den Link, dient zum späteren Generischen Zugriff auf den erzeugten Link, Länge Max 32 Zeichen, Nur Gross-Schreibung(Auto)
- **ERLAUBT_AB**
  Vorgabe ab wann der Link gültig ist. Leer=Tagesdatum
- **ERLAUBT_BIS**
  Vorgabe bis wann der Link gültig ist. Leer=Unbegrenzt
- **ERLAUBT_MAX_AUFRUFE**
  Maximale Anzahl von Aufrufen erlaubt
- **LINK_DESC**
  Beschreibung des Links in Text-Form, wird zum Beispiel für GetRel[4007, aktion=4LINK-HASH-HTML] verwendet Länge max 255 Zeichen
- **WORKFLOW_START**
  Name des Workflow der bei LINK-Aufruf ausgeführt werden soll (SE5009)
- **WORKFLOW_PARAM_FORMAT**
  Angabe einer "Versions-Nummer" für das Parameterformat, um auch bei Schnittstellenänderung Kompatibel zu bleiben
- **WORKFLOW_PARAMETER**
  (Optional) Angabe einer Parameter Liste mit dem Trenner ? BSPL: AFeld?BFeld?CFeld, Liste wird bei Aufruf des Workflow als Einzel-Parmaeter aufgeteilt übergeben (max Länge 1024)
- **LINK_USER_ID**
  Optional, bei Anonym Zugang und Einladungen Angabe notwendig. Es ist aber für Intern/Public-User immer geboten auch eine Benutzer-Nr mit anzugeben. So kann der WW-LINK direkt an einen Benutzer gebunden werden.
  ACHTUNG: Bei Mitarbeitern (LINKART 20 oder 21) die Login-Benutzer Nummer angegeben
  Bei öffentlichen Benutzer (LINKART 10,11,12) muss die Public-Worker-ID aus der IDB SE0125 angegeben werden.
- **ANONYM_MAX_AUFRUFE**
  (Optional) Angabe wie oft der Link ohne Anmeldung ausgeführt werden darf, nur bei LINKART = [10,11,32] erlaubt.

Hier ein Beispiel wie ein Link angelegt wird
TMP_4000_32=GET_RELATION[4006!12!!!!10!Hier Klicken!SE5009!!90-30-20!9!!]

4006: Erzeuge neuen WW-LINK
12: Erzeugen einen Anonymen Public-User-Zugang
10: Maximale Anzahl Aufrufe erlaubt
Hier Klicken: Dieser Text wird bei einem HTML-Link als Link-Text verwendet
SE5009: Angabe des Start-Workflow der gestartet werden soll
90-30-20: Parameter der an den Workflow übergeben wird
9: Benutzer-Nummer, hier die Public-User Nummer, da es sich um einen Public-Link handelt

Rückgabewert TMP_4000_32 bei erfolgreichem Anlegen die WW-LINK-Hash-ID, die für weitere Abfrage bei GET_RELATION[4007!TMP_4000_32!..] benutzt werden kann.

Rückgabewerte der GETREL 4006:

Leer: Es wurde kein Link angelegt. Fehlerauswertung mit GETREL[4007 Aktions-Code 0 aufrufen.
WERT: Es wird die erstellte HASHID zurückgegeben (32-Byte Hash). Mit dem kann mit der GETREL[4007… auf weitere Funktionen des WWLINK's zugegriffen werden.

GETREL 4007 WWLINK Verwaltung

GET_RELATION[4007!LINKHASHID!LINKART!LINK_KEY_ID_NAME!LINK_ACTION!USER_ID]

Folgende Übergabeparameter

- **LINKHASHID**
  Hier den 32-Byte HASH-Wert angeben oder optional LINKART und LINK_KEY_ID
- **LINKART**
  (OPTIONAL/ wenn LINKHASHID Leer) Art des Links, wurde beim Erzeugen angegeben, Vorgabe Bei Aufruf 40 zwingend
- **LINK_KEY_ID_NAME**
  (OPTIONAL/wenn LINKHASHID Leer) wurde beim Erzeugen angegeben
- Link Aktion 0..99
  LINK_ACTION 0..19 Lesen von Merkmalen
  - 0 Letzter Status GETREL[4006
    Gebe letzten Status-Code der letzten Abfrage GetRel 4006 zurück (Code + Meldung) Rückgabe: OK / ERR-Fehlermeldung: OK
  - 1: Letzter status GETREL[4007
    Gebe letzten Status-Code der letzten Abfrage GetRel 4007 zurück (Code + Meldung)
    Rückgabe: OK / ERR-Fehlermeldung: OK
  - 2: Gebe Link Info: Liste aller Felder des Links
    Rückgabe:
    Leer=Fehler,
    Wert = Liste getrennt mit ! wie im folgendem Definiert:
    LINKART!LINK_KEY_ID_NAME!ERLAUBT_AB!ERLAUBT_BIS!ERLAUBT_MAX_AUFRUFE!BISHER_AUFGERUFEN!LINK_DESC!START_WORKFLOW!WORKFLOW_PARAM_FORMAT!WORKFLOW_PARAMTER! LINK_USER_ID!ANONYM_MAX_AUFRUFE!ANONYM_ANZAHL_AUFRUFE
  - 3: Gebe LINK-HASH-HTTP
    Rückgabe: Leer=Fehler, HTTP-HASH-Format, hierbei wird die URL zum WW-Server/Server-Link zurückgegeben, Wert kann direkt in einem Browser ausgeführt werden
  - 4: Gebe LINK-HASH-HTML
    Rückgabe: Leer=Fehler, HTML-HASH-Format, hierbei wird ein <a href..> HTML Element mit Beschreibung und Server-Link zurückgegeben
  - 5: Gebe LINK Gültig bis zurück
    Rückgabe Leer=Fehler, Datum Gültigkeitsdauer, falls nicht eingeschränkt wird 31.12.2999 zurückgegeben
  - 6: Gebe LINK Anzahl Aufrufe
    Rückgabe Leer=Fehler, 0..x=Anzahl Aufrufe des Links
  - 7: Gebe aktuellen Status des Links: (Ist Link gültig)
    Rückgabe Leer=Fehler, 1=Neu, 2=Verfügbar benutzt, 3=gesperrt, 9=gelöscht
  - 8: Gebe Einmal-Kennwort für Aktionen GETREL: 4006(11 und 21), sollte direkt nach dem Erzeugen ausgelesen werden
    Rückgabe Leer=Fehler, Text des Einmalkennwortes
  - 9: Gebe LinkArt für LINKHASHID
    Rückgabe Leer=Fehler, LINK_ART siehe Definition GETREL[4006]
  - 10: Gebe LINK_KEY_ID_NAME für LINKHASHID
    Rückgabe Leer=Fehler bzw. kein LINK_KEY_ID_NAME bei Erzeugen gesetzt, Manueller KEY der für den HASH-LINK vorgegeben wurde.
  - 11: Gebe Benutzer-Nummer

```
            Rückgabe Leer=Fehler, 0..999999 hinterlegte Benutzer-Nummer abhängig von LINK-
            Art ob Public/Intern
        o   12: Gebe definierter WORKFLOW-Name für die Ausführung des LINKS
            Rückgabe Leer=Fehler, Wert=Workflow-Name
        o   13:     Gebe Parameter-Format "Versions-Nummer" für Parameter Liste des LINKS
            Rückgabe  Leer=Fehler,  Wert:  0.99999  Versions-Nummer  die  beim  Erzeugen
            vorgegeben wurde
        o   14: Gebe Parameter-Liste
            Rückgabe Leer=Fehler, Wert: Parameter-Liste bereits umgesetzt mit ? Trenner
        o   15: Gebe LINK-Beschreibung
            Rückgabe Leer=Fehler, Wert:    Beschreibung des Links
        o   18:     Gebe die aktuelle LINK-ID aus dem Cache zurück (Benötigt keine weiteren
            Aufrufparameter)
            Rückgabe Leer=Fehler(Keine Daten im Cache), Wert=HashID
        o   19: Lese die Daten für den LINK in den internen Cache
            Rückgabe 0=Fehler, 1=OK
    LINK_ACTION 20..29 Intern User Lese-Funktionen Read/Read-Next
        o   20    Gebe    First-LINK-ID    für    INTERN-USER-ID,    (LINKHASHID    oder
            (LINKART+LINK_KEY_ID_NAME)) + USER_ID
            Rückgabe Leer=Fehler, HASHID für ersten Link des internen Benutzers
        o   21: Gebe NEXT-LINK-ID  für INTERN-USER-ID, LINKHASHID + USER_ID
            Rückgabe Leer=Ende erreicht, Wert für Folge HASHID
    LINK_ACTION 30..39 Intern User Lese-Funktionen Read/Read-Next
        o   30:    Gebe    First-LINK-ID    für    PUBLIC-USER-ID        (LINKHASHID    oder
            (LINKART+LINK_KEY_ID_NAME)) + USER_ID
            Rückgabe Leer=Fehler, HASHID für ersten Link des Public Benutzers
        o   31: Gebe NEXT-LINK-ID  für PUBLIC-USER-ID  LINKHASHID + USER_ID
           Rückgabe Leer=Ende erreicht, Wert für Folge LINK-HASHID
    LINK_ACTION 40..49 Individuelle Such-Funktion mit Angabe von LINK-Art Read/Read-Next
        o   40: Gebe First-LINK-ID für LINK-Art  Nur Übergabe LINKART
            Rückgabe Leer=Fehler, HASHID für ersten Link der LINKART
        o   41: Gebe NEXT-LINK-ID  für LINKART,  LINKHASHID + LINKART
            Rückgabe Leer=Ende erreicht, Wert für Folge LINK-HASHID
    LINK_ACTION 50..99 Setze Status des Links, bzw. Verwaltungs-Funktionen
        o   50: Status des Links auf Gesperrt setzen
            Rückgabe 0:Fehler / 1:OK
        o   51: Status des Links auf Aktiv setzen, (Keine Änderung an Stammdaten)
            Rückgabe 0:Fehler / 1:OK
        o   52: Status des Links auf Aktiv und Frei setzen mit RESET. Dabei werden die
            Zähler (Aufgerufen, und Anonyme Zugänge zurückgesetzt).
            Rückgabe 0:Fehler / 1:OK
        o   99: Link löschen
            Rückgabe 0:Fehler / 1:O
    LINK_ACTION 100..299 Zugriff auf die Programm-Aufruf Parameter
        o   100:     Gebe Anzahl Parameter für diesen WW-LINK 0..99
        o   101-199: Gebe Parameter mit Nummer 1..99
        o   200:     Gebe Länge Parameter-String
        o   201-299: Gebe Länge für den entsprechenden Parameter, 1..99
•   USER_ID         Wird nur für die Abfragen 20,21,30,31 benötigt
•
```

Beispiel eines Aufrufs in einem Workflow-Script:

SCRSE5009_5362_32=GET_RELATION[4006!12!!!!10!Hier Klicken!SE5009!!SCRSE5009_5311_10!9!!]

Hier wird ein anonymer Public-User WWLKINK erstellt für Public-User-Nummer 9.

Wie wird ein WW-LINK angewendet ?

Auf Seite der WWA(pplication) ist es möglich durch Aufruf der GETREL-4007 mit dem LINK_ACTION-Code 3 + 4 eine gültige HTTP-URL (Uniform Resource Locator = WEB-Adresse) für einen WW-LINK zu generieren. Dabei wird die korrekte URL für den aktuellen Server-Zugang verwendet. Ebenso wir die Beschreibung für den WW-LINK bei Code=4 (HTML-Link) zurückgegeben.

So sieht eine WW-LINK Adresse aus:

https://AAAA[:Port]/@LNKbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb

AAAA: Adresse des WEB-Server Beispiel 192.168.0.100 oder webware.MeineDomain.de

bbb…: eindeutige Link-Hash-ID

Es ist dadurch auch möglich die WW-LINK-Adresse manuell auch in einem Browser einzugeben. Hierzu wird die 32-Zeichen lange HASH-ID benötigt, wobei dieser /@LNK als Link –Kennung vorangestellt werden muss..

Wie wird ein WW-LINK in der WW(Anwendung) verarbeitet ?

Nachdem ein WW-LINK ausgelöst wurde, wird in einem SE-Workflow-Script [WWLINK] die weitere Verarbeitung, also den Aufruf des Ziel-Workflow durchgeführt. Dieses Script erhält als Übergabeparameter die eindeutige WW-LINK Hash-ID. Mit Hilfe der GETREL[4007,…] können dann die Rahmenparameter des WW-LINK's ausgelesen werden.

Die im Lieferumfang enthaltene WWLINK-Implementierung liest maximal 2 mögliche Parameter aus und startet den Ziel-Workflow, mit der Übergabe dieser Parameter. Hier können nun individuelle Änderungen an dem Script vorgenommen werden, um weitere Parameter zu lesen, bzw. die Aufruflogik an eigene Bedürfnisse anzupassen.

Wie wird ein WW-LINK aus dem System entfernt ?

Grundsätzlich sollte einem WW-LINK eine Begrenzung in der Form, [maximale Anzahl Aufrufe] bzw. [Vorgabe erlaubter Datums-Bereich] mitgegeben werden. Bei Erreichen einer solchen Begrenzungsvorgabe wird der WWLINK automatisch gesperrt, verbleibt aber im WW-System. Dadurch kann man im WW-System-Cockpit die Verwendung auch von abgelaufenen WWLINK's auswerten.

Im WW-System-Cockpit ist es auch möglich noch aktive WWLINK's zu sperren, oder ganz zu löschen. Nähere Infos dazu finden Sie in diesem Dokument im Bereich Zugangs-Verwaltung WW-LINK-Zugangs System (Mitarbeiter).

Was passiert bei fehlerhaftem Zugriff ?

Wird mit einem Gesperrten WW-LINK bzw. ungültigem WW-LINK-Schlüssel zugegriffen, so gibt der WW-Server nur die Meldung HTTP 404 RESOURCE NOT FOUND zurück. Dadurch sollen einem etwaigen Angreifer keine Informationen über Vorhanden sein bzw. Zustand eines WW-LINK geliefert werden.

Um dem WW-Admin eine Übersicht über fehlgeschlagene Zugriffe zu geben, werden diese in den entsprechenden WW-Log-Dateien protokolliert.

Anwendung eines WW-Validation Link's

Wird ein Validation-Link erzeugt, so kann dieser von externen Systemen verwendet werden um den Link beim WW-Server zu Validieren. Ist der WW-Validation Link gültig, so antwortet der WW-Server mit HTTP Status-Code 200, bei Fehler mit Fehler HTTP 404 RESOURCE NOT FOUND.

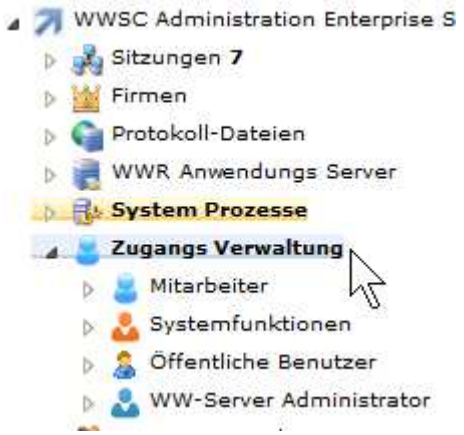
Es ist zu Beachten das die Häufigkeit/Gültigkeit der Prüfung für diesen Link bei der Erstellung eingeschränkt werden kann.

WW-Benutzerverwaltung im System-Cockpit

Innerhalb des System-Cockpit's ist für die System-Administratoren möglich Benutzer sowie den Zugang der Benutzer zu verwalten. Die Benutzerverwaltung findet man im System-Cockpit im Bereich System-Übersicht und Administration.

Zugangs Verwaltung

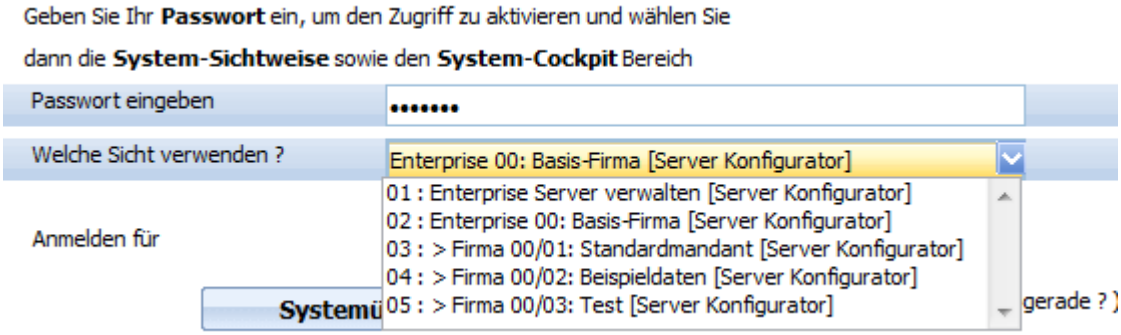
Im Bereich der Zugangsverwaltung können Sie mit dem Menü-Befehl "Benutzer-Verwaltung" die WEBWARE Benutzer-Verwaltung aus dem Datenbankbereich aufrufen.



Im Bereich Zugangs-Verwaltung können die 4 Benutzergruppen verwaltet werden

- Mitarbeiter (interne Benutzer)
- Systemfunktionen, Systemaufgaben
- Öffentliche Benutzer (Public User)
- WW-Server Administratoren

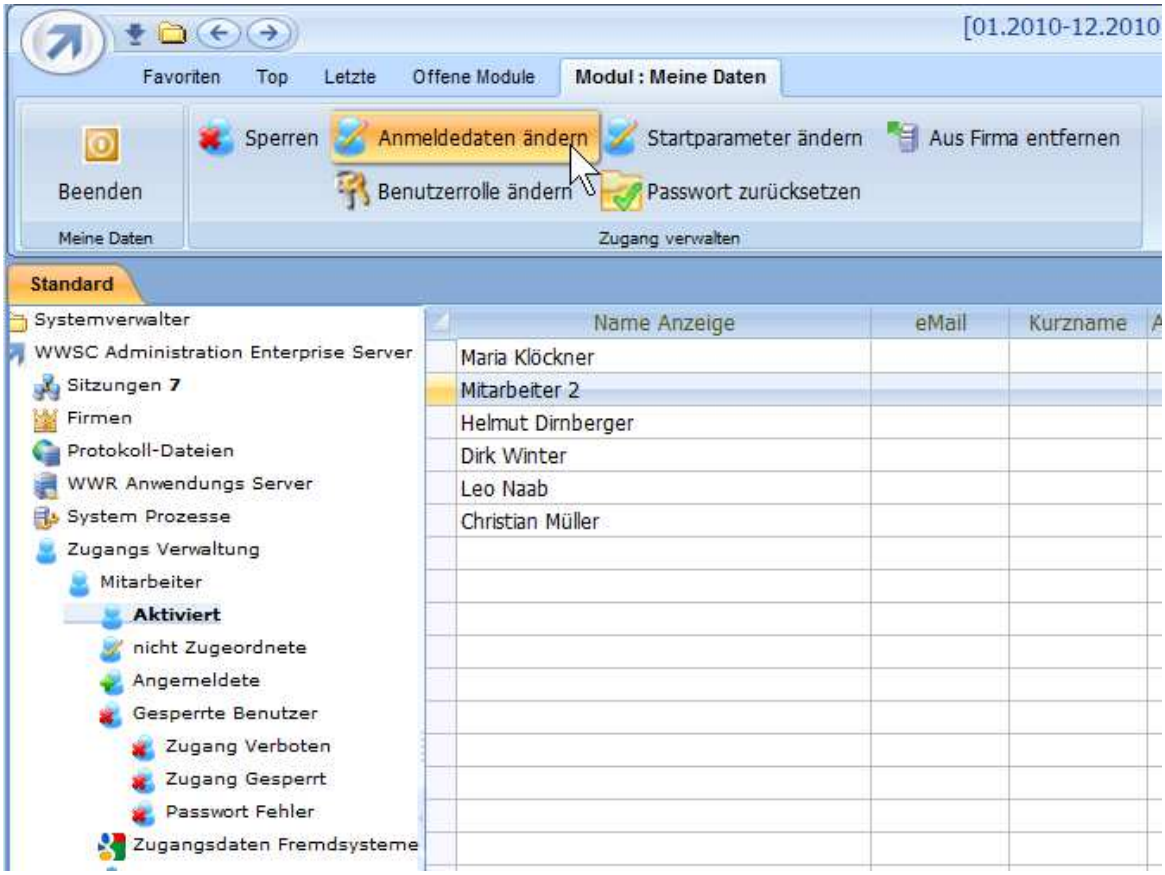
Die WW-Server Administrator-Gruppe ist nur sichtbar wenn der Benutzer die erforderlichen Rechte hat, sowie auf Server-Ebene (Server Konfiguration) in das Systemcockpit eingestiegen wird. (Unten Enterprise Server verwalten, abhängig von Server-Installationsart..)



Mitarbeiter Verwaltung

Im Bereich Mitarbeiter können die Benutzer die Zugang zum internen System Ihrer WEBWARE haben, verwaltet werden.

Wird im Bereich der Zugangsverwaltung ein Ast ausgewählt, so erhält man auf der rechten Seite eine Liste mit zugehörigen Benutzern angezeigt.

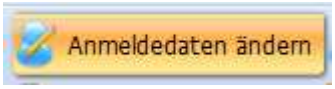


Je nach gewähltem Bereich erscheinen dann in der Menüleiste oben für den Mitarbeiter die möglichen Aktionen.

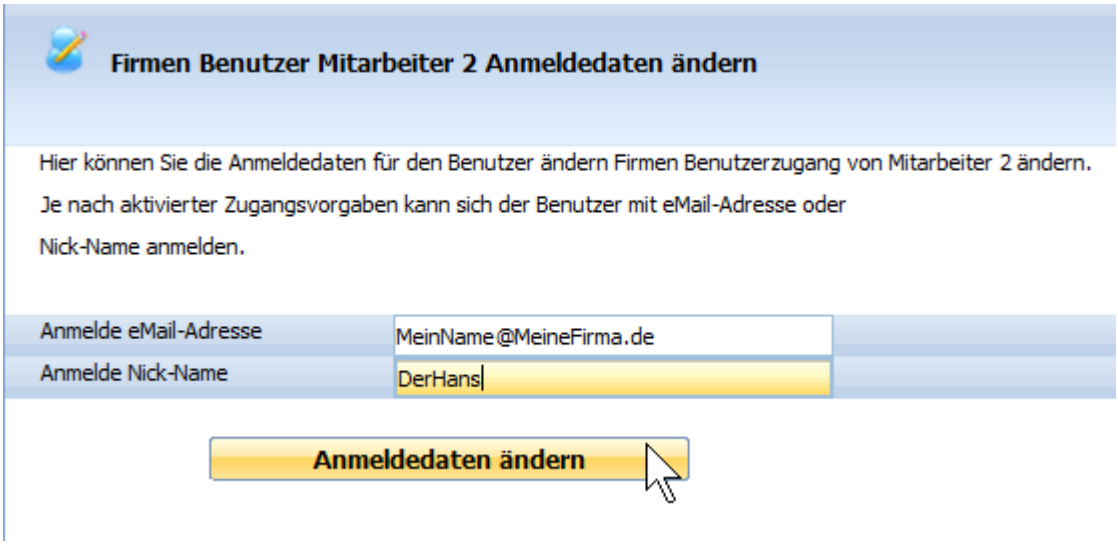
Aktionen für Aktive Benutzer:

Benutzer Sperren: der Zugang ist dann für diesen Benutzer verboten, und er taucht in der Liste Gesperrte Benutzer auf.

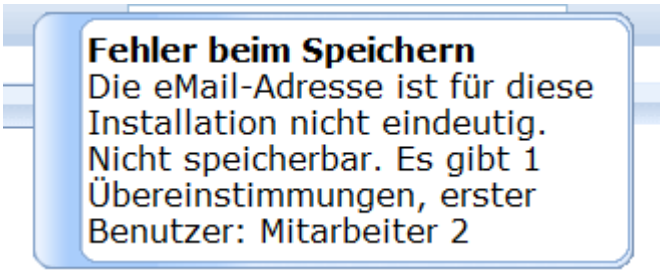
Anmeldedaten ändern



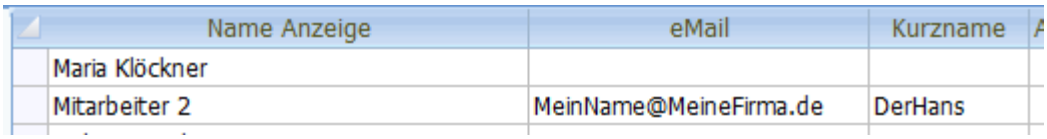
Hier können die Anmeldedaten für den Benutzer geändert werden. Hierzu zählen die Anmelde-eMail-Adresse und der Nick-Name.



Beim Speichern der Anmeldedaten wird geprüft ob die Daten bereits für einen Benutzer vergeben sind, und bei Doppelten Namen eine Fehlermeldung ausgegeben.



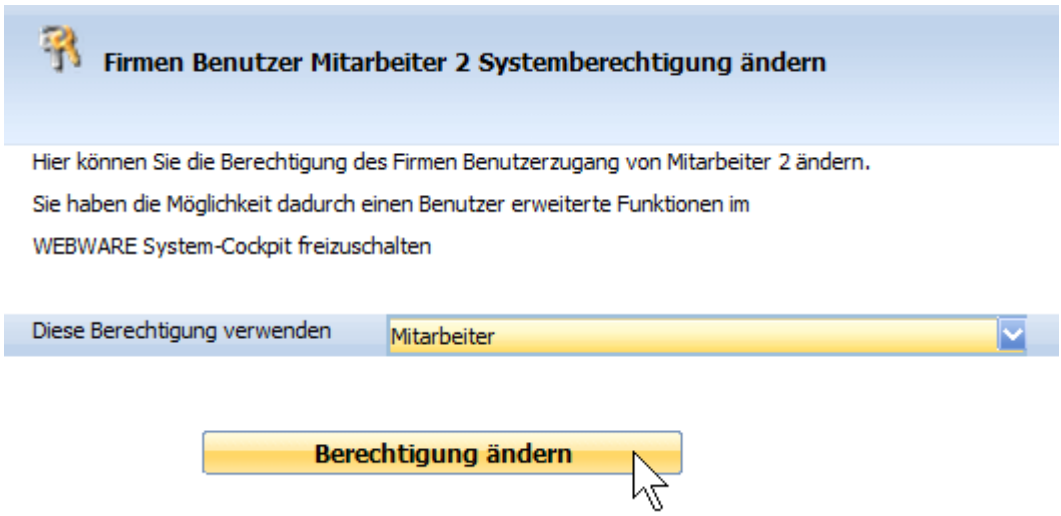
Anzeige der Anmeldedaten in der Benutzerliste:



Name Anzeige	eMail	Kurzname
Maria Klöckner		
Mitarbeiter 2	MeinName@MeineFirma.de	DerHans

Benutzerrolle ändern

Hier kann die Rolle eines Benutzers geändert werden. Nach Auswahl der Funktion wird der Berechtigungsauswahldialog angezeigt.

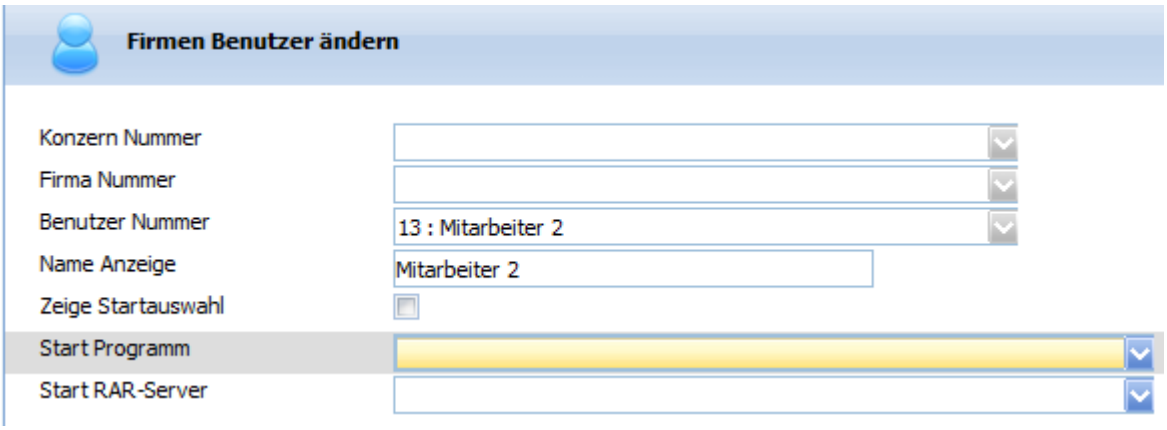


Die möglichen Benutzer-Rollen sind abhängig von der Berechtigung des Administrators der den Dialog aufruft. Es ist nicht möglich eine höhere Berechtigung zu vergeben als die die der Administrator selbst hat.

Wird ein Benutzer als Administrator konfiguriert so wird er in dem Bereich WW-System Administrator angezeigt.

Startparameter ändern

Hier kann das Startprogramm und der gewünschte RAR-Server für einen Benutzer festgelegt werden.



Es besteht auch die Möglichkeit durch Aktivieren des Feldes „Zeige Startauswahl“ ein Start-Bildschirm direkt nach dem Login zu aktivieren mit dem Zum Beispiel Administratoren, direkt in das Systemcockpit wechseln können.

Benutzer Startprogramm Auswahl

Im Start-Bildschirm kann der Benutzer aus mehreren Start-Programmen wählen.

- Start Standardanwendung

  Hier wird die Startanwendung dir für den Benutzer hinterlegt ist gestartet.

- Debug Startanwendung

  Hiermit wird, wenn vorhanden, die WWADAPP Anwendung (WWAD.EXE) für den Benutzer gestartet. Damit kann zum Beispiel eine neuere Testversion im laufenden Betrieb gestartet werden.

- System-Cockpit

  Dies wird für System-Administratoren angezeigt, und ist zusätzlich abhängig von dem Zugangspunkt zum WW-Server.

- Weiter ohne Aktion

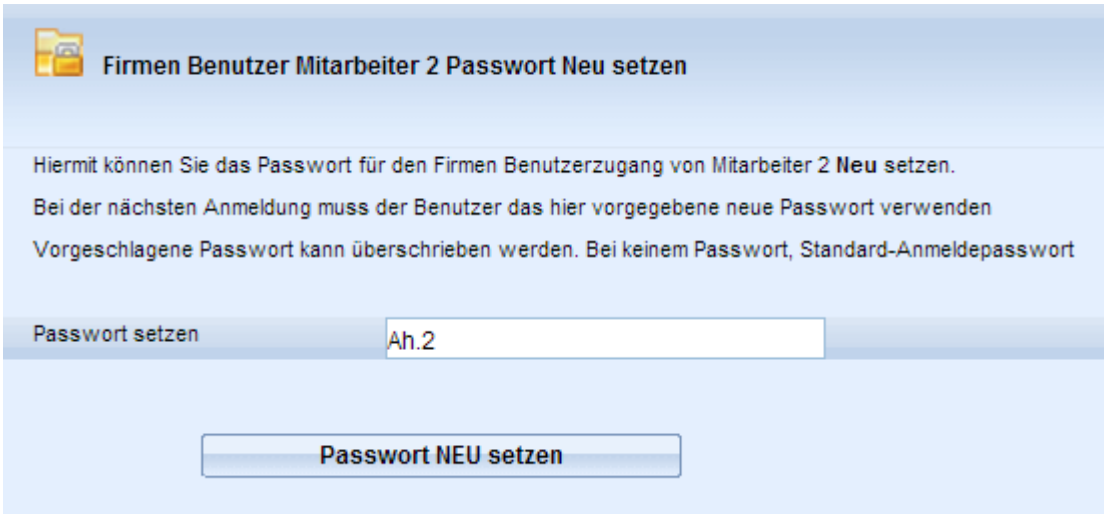
Passwort zurücksetzen

Hier kann das aktuelle Passwort des Benutzers gelöscht werden, und die Eingabe bei der nächsten Neuanmeldung erzwungen werden.

Dieser Knopf wird nur Angezeigt falls die Option für Leere Passwörter aktiviert ist. Ansonsten mus die Funktion "Passwort vorgeben" verwendet werden

Neues Passwort vorgeben

Hier kann für den Benutzer ein neues Passwort vergeben werden.

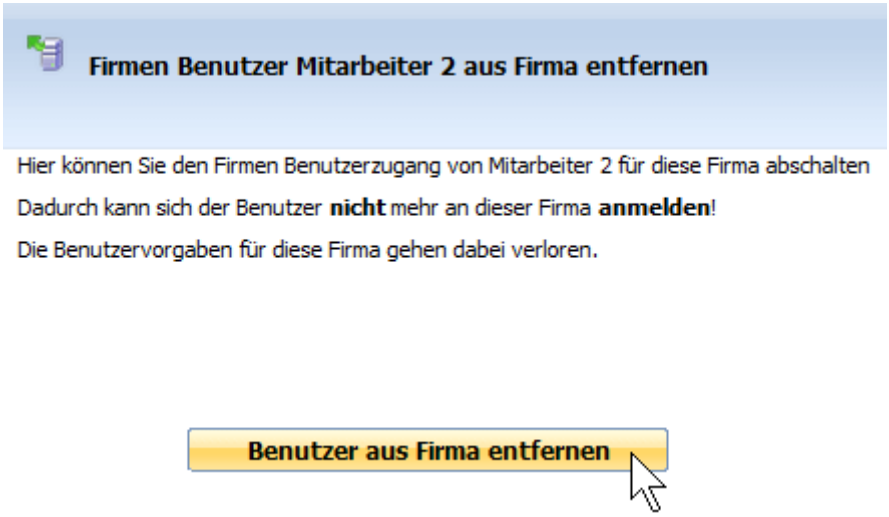


Es wird dabei automatisch ein Passwort erstellt das auf Grund der Passwortrichtlinine Gültig ist. Sie können jedoch dieses Passwort auch überschreiben.

Benutzer aus Firma entfernen

Mit diesem Befehl kann ein Benutzer aus dieser Firma entfernt werden, er erscheint dann im Ast

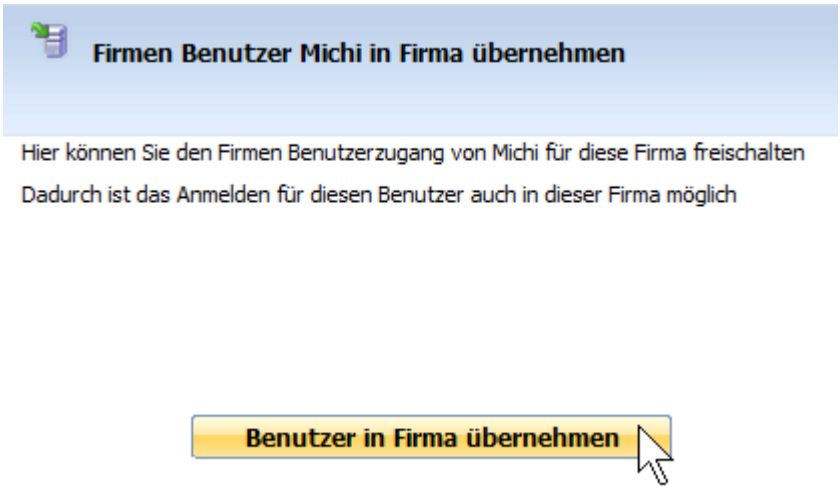
Benutzer


Firmen Benutzer Mitarbeiter 2 aus Firma entfernen
Hier können Sie den Firmen Benutzerzugang von Mitarbeiter 2 für diese Firma abschalten
Dadurch kann sich der Benutzer nicht mehr an dieser Firma anmelden!
Die Benutzervorgaben für diese Firma gehen dabei verloren.
Benutzer aus Firma entfernen

Aktionen für nicht zur Firma zugeordnete Benutzer

In Firma einfügen

Hier kann ein Benutzer der keine Firmenzuordnung hat, der Firma zugeordnet werden.



Aktionen für angemeldete Benutzer

Benutzer sperren

Hiermit kann wie weiter oben beschrieben ein Benutzerzugang gesperrt werden. Es wird jedoch **nicht** die aktuelle Sitzung getrennt.

Anmeldedaten ändern

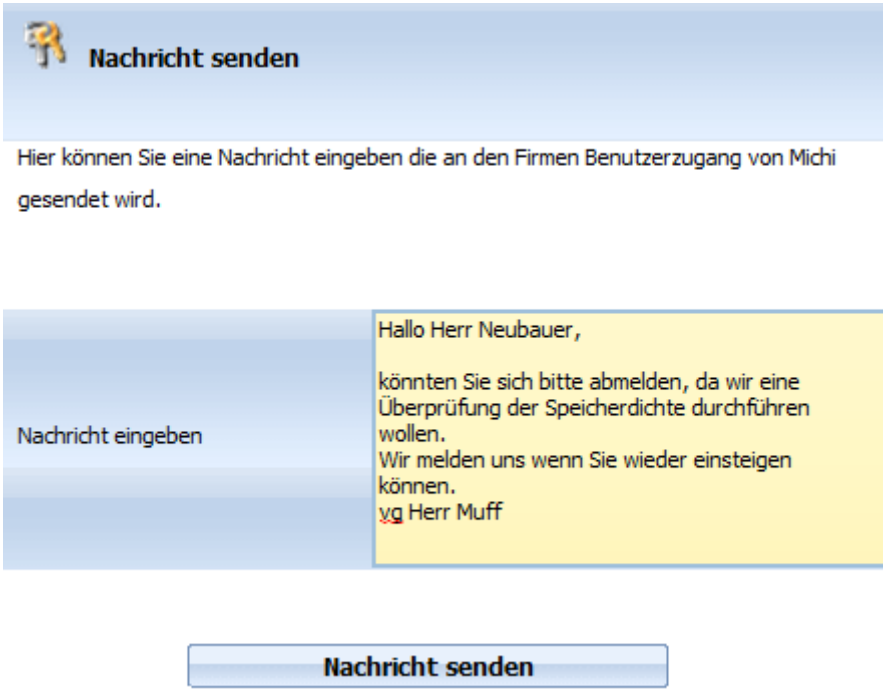
Hiermit können die Anmeldedaten für einen Benutzer geändert werden. Wie weiter oben beschrieben.

Passwort zurücksetzen

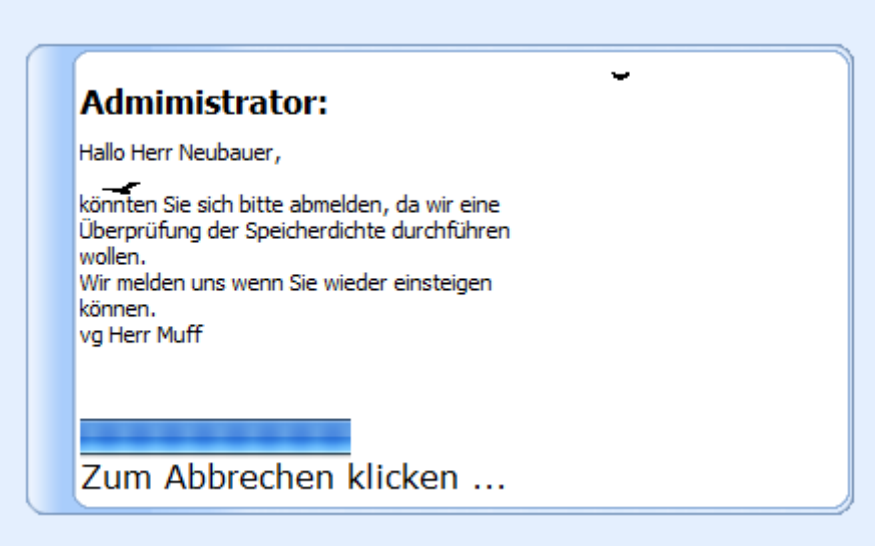
Hiermit kann das Passwort des Benutzers zurückgesetzt werden, so dass bei einer Neuanmeldung ein neues Passwort vom Benutzer vorgegeben werden muss. Dieser Befehl ist nur vorhanden wenn für die entsprechende Benutzerart (Public oder Intern) die Option für Leere Passwörter aktiviert ist.

Nachricht schicken

Hiermit können Sie dem angemeldeten Benutzer eine Meldung schicken. Hierzu wird eine Maske eingeblendet in der der Nachrichtentext eingegeben werden kann.

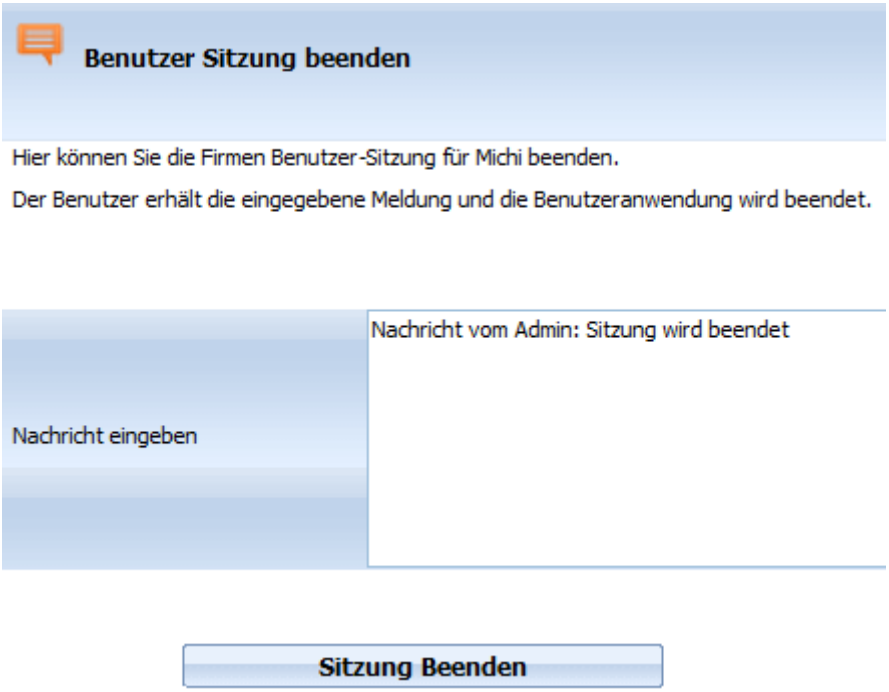


Die Nachricht sieht dann beim Benutzer so aus:



Sitzung trennen

Hiermit können Sie eine Nachricht an den Benutzer der Sitzung senden, sowie danach die Sitzung Beenden



Gesperrte Benutzer verwalten

In diesem Programmbereich ist es möglich gesperrte Benutzer zu verwalten und auch wieder entsperren.

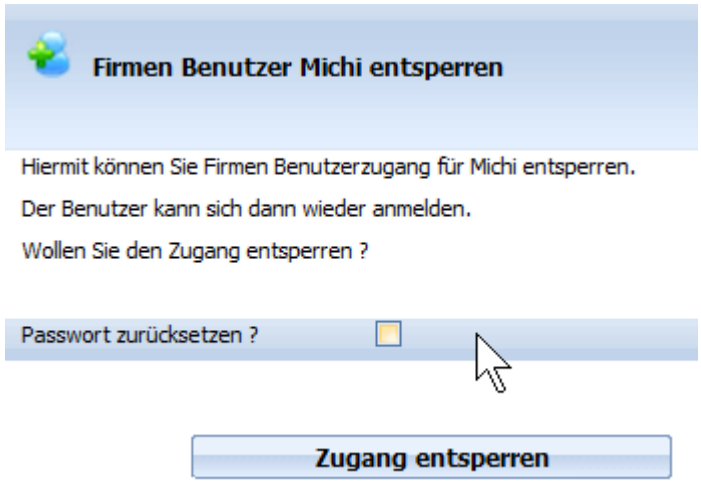
Je nach Sperrzustand des Benutzers werden diese hier in

- Zugang Verboten
- Zugang gesperrt
- Passwort Fehler unterteilt

Für die gesperrten Benutzer sind die folgenden Befehle möglich. Diese wurden zum Teil bereits weiter oben beschrieben.

Benutzer entsperren

Hiermit können Sie die Sperre für den Benutzer aufheben. Mit dem folgenden Dialog kann die Sperre für den Benutzer aufgehoben werden. Zusätzlich gibt es die Möglichkeit das Passwort des Benutzers zurückzusetzen. Beim Zurücksetzen des Passwortes, wird der Benutzer bei der nächsten Anmeldung aufgefordert ein neues Passwort einzugeben.



WW-LINK Zugangs System

WW-LINK Einträge für Mitarbeiter können im Ast WWLINK-Zugangs System verarbeitet werden.

Hier werden für interne Mitarbeiter, Zugänge und Einladungen verwaltet. Wird einer der Ast-Einträge ausgewählt, so erhält man auf der rechten Seite je eine Liste der zugehörigen WW-Link's angezeigt.

In der WW-LINK-Liste erhalten Sie die Infos die einen WW-LINK betreffen. Im Folgenden wir die Liste mit 2 Einträgen gezeigt, um einen Überblick über die Felder zu erhalten:

Art	LINK Beschreibung	Benutzer	WW-Act-Link	Erlaubt ab	Erlaubt bis	Wie oft Au	Bishe	Wie oft An	Anon	Workflow
INTERNER USER	Test-Link Intern User 1	at@doops.de	NEW	3.05.11	31.05.11	4				SE0231
INTERNER USER	Test-Link Intern User 2	at@doops.de	NEW	3.05.11	31.05.11	4				SE0231

Parameter Liste	Erzeugt am	Erzeugt un	Erzeugt von	Verwendet ar	Verwendet	Verwendet vc	Geändert am	Geändert u	Geändert von
SE00001219E?PARAM 2	10.05.2011	0:07:19	Systemverwalter						
SE00001219?PARAM 2	10.05.2011	0:07:20	Systemverwalter						

Felder der WW-LINK-Liste

Art: WW-LINK-Art (Intern-User, Public-User, Service) sowie Ausprägung (Zugang,Einladung,Anonym)

LINK Beschreibung: Text der bei Generierung von HTML-Links verwendet wird

Benutzer: Mitarbeiter / Öffentlicher Benutzer / Service-Funktion die an den WW-LINK gebunden ist.

LINK-Zustand: Neu/Benutzt/Gesperrt

Erlaubt ab: Start-Datum ab wann dieser WW-LINK gültig ist, bei Leer gibt es keine Begrenzung

Erlaubt bis: Ende-Datum bis zu dem dieser WW-LINK gültig ist, bei leer keine Begrenzung

Wie oft Aufrufbar: Anzahl erlaubte Aufrufe mit diesem WW-LINK

Bisher aufgerufen: Wie oft wurde der WW-LINK bisher aufgerufen.

Wie oft Anonym: Wie oft darf dieser WW-LINK Anonym, also ohne Benutzeranmeldung aufgerufen werden, nur gültig für PUBLIC-/ und SERVICE-Zugänge

Anonyme Aufrufe bisher Wie oft wurde der WW-LINK bisher Anonym aufgerufen.

Workflow: Name des Workflows der bei Auslösen des WW-LINK gestartet wird.

Parameter-Liste: Parameter die an den Workflow übergeben werden. Hier können beliebig viele Parameter mit „?" getrennt angegeben werden. Hier gibt es eine Längenbegrenzung auf 1000 Zeichen. Der Designer hat hier die Möglichkeit den SE-Workflow WWLINK zum Starten von WW-LINK's-Workflow individuell anzupassen und diese Parameter darin auszuwerten.

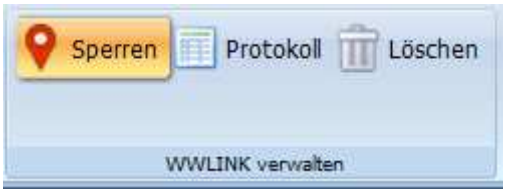
Erzeugt Am/Um/Von: Ersteller-Info

Geändert Am/Um/Von: Änderungs-Info

Benutzt Am/Um/Von: Information über letzte Benutzung

Verwalten von WW-LINK

Je nach Zustand eines WW-LINK stehen im Menü, verschiedene Aktionen zur Verfügung um einen WW-LINK-Eintrag zu verwalten. Jeder WW-LINK Bereich wird dabei immer in Neue WW-LINK's, Benutzte WW-LINK's (mindestens ein Zugriff ist erfolgt), und gesperrte WW-LINK's (Ablauf Gültigkeits-Vorgaben, oder manuelle Sperrung) unterteilt.



Neue und Benutzte WW-LINK Einträge können gesperrt, gelöscht und das zugehörige Benutzungs-Protokoll angezeigt werden.

Wir ein WW-LINK Eintrag gesperrt, so wird er von Neue/Benutzte direkt in den Ast Gesperrte verschoben. Dabei wird der Zustand auf Gesperrt gesetzt, die übrigen Datenfelder werden dabei nicht verändert.

Wird ein WW-LINK Eintrag gelöscht, so wird er direkt entfernt, und ist im Weiteren nicht mehr auswertbar.

Gesperrte WW-LINK Einträge können Freigegeben, Zurückgesetzt, Gelöscht und Ihr Benutzungs-Protokoll angezeigt werden.

Freigeben

Beim Freigeben wird der Status, abhängig von der bisherigen Benutzung auf Neu, oder Benutzt gesetzt.

Zurücksetzen

Beim Zurücksetzen wird der WW-LINK auf „Neu" gesetzt, zusätzlich werden die Datumbeschränkungen entfernt, und die Benutzungs-Zähler auf 0 gesetzt (Anzahl Aufrufe / Anzahl Anonyme Aufrufe). Das Protokoll wird dabei nicht verändert, so dass man im Nachhinein den „alten" Verlauf weiter sehen kann.

Das WW-LINK-Zugriff Protkoll

Grundsätzlich wird jede Aktion die mit einem WW-LINK gemacht wird protokolliert. Dadurch hat der Administrator jederzeit die Möglichkeit über die Verwendung bzw. Missbrauch eines WW-LINK Informationen zu erhalten. Bei jedem vorhandenen WW-LINK besteht die Möglichkeit sich das Zugriff Protokoll anzuzeigen.

Datum	Uhrzeit	WW-Link Z	Zugriff Status	IP-Adresse	A	Sitzu	WWFS-Benutzer	Protokoll Daten
10.05.2011	0:07:14	1	NEW			6	Systemverwalter	
10.05.2011	0:44:38	2	READ	91.33.55.102				GET /@LNK07ca862b06602234a235d1e499eebb56 HTTP
10.05.2011	0:44:47	3	ACCESS PGM START	!7f		29	dw@softengine.de	
10.05.2011	0:45:00	4	READ	91.33.55.102				GET /@LNK07ca862b06602234a235d1e499eebb56 HTTP
10.05.2011	0:45:04	5	READ	91.33.55.102				GET /@LNK07ca862b06602234a235d1e499eebb56 HTTP
10.05.2011	7:45:33	6	READ	217.89.68.99				GET /@LNK07ca862b06602234a235d1e499eebb56 HTTP
10.05.2011	7:45:48	7	ACCESS PGM START	ÙYDc		42	dw@softengine.de	
10.05.2011	7:46:08	8	ERR LINK IS BLOCKE	217.89.68.99				GET /@LNK07ca862b06602234a235d1e499eebb56 HTTP

In der Liste wird der Zeitpunkt, laufende Zugriffs-Nummer für diesen WW-LINK, Art des Zugriffs, IP-Adressse, WW-Sitzungs-Nummer, Benutzer der die Aktion ausgeführt hat protokolliert. Es ist auch möglich die http-Kopf Informationen des Zugriffs zu protokollieren.

Die Aktivierung und Tiefe der Protokollierung kann über das WW-System-Cockpit eingestellt werden. Sie finden die Informationen unter Konfiguration > System-Konfiguration > WWLINK-Zugangs Vorgaben.

Öffentliche Benutzer Verwaltung (Public-Worker)

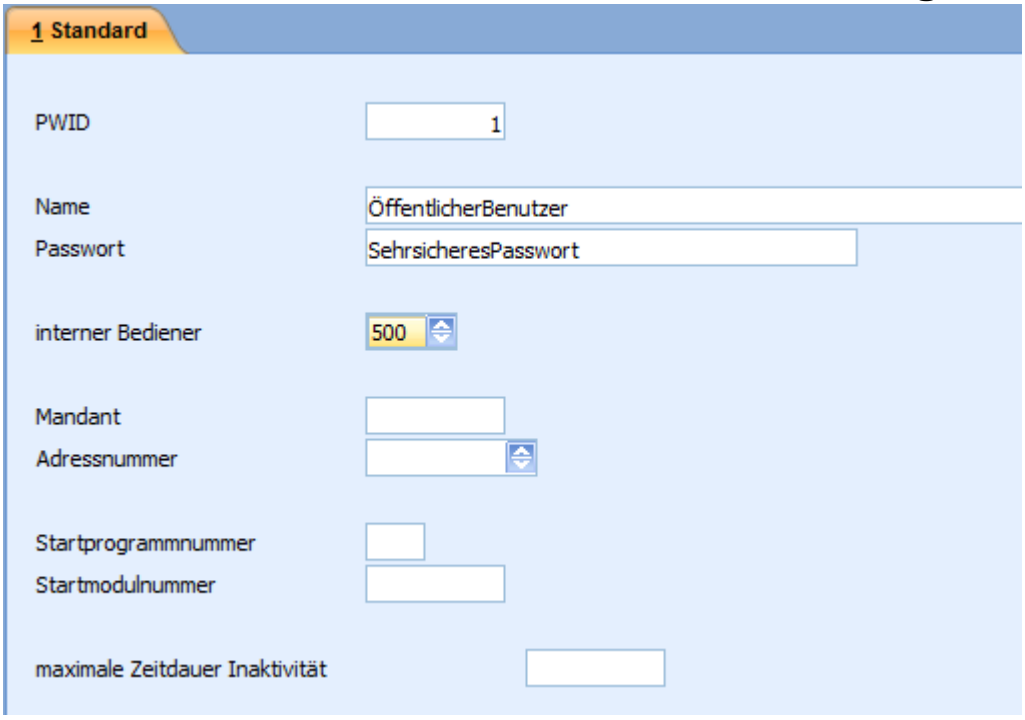
Die öffentlichen Benutzer werden im System-Cockpit unterteilt in

- Aktivierte Benutzer
- Nicht zugeordnete Benutzer
- Angemeldete Benutzer
- Gesperrte Benutzer
- WW-LINK Zugangs System

Neuanlage wird im Bereich der IDB-Verwaltung der WEBWARE-Anwendung durchgeführt. Änderungen von Passwörtern und Zugangsdaten werden dabei automatisch an den WW-Server übertragen und sind dort sofort verfügbar.

Die öffentlichen Benutzer (Public Worker) werden in der IDB „SE0125 – ww public worker“ definiert und einem internen Bediener (Public Worker Vorlage) zugewiesen.

WEBWARE 1.0x Öffentliche Benutzer Verwaltung



Felder der IDB SE0125 (ww public worker)

PWID:	Index des Public Worker Datensatzes
Name:	Geben Sie hier den Namen des Public Workers an
Passwort:	Geben Sie hier das Passwort des Public Workers an

interner Bediener: Geben Sie hier die Public Worker Vorlage an die in der Benutzerverwaltung angelegt wurde.

Mandant (optional): Geben Sie hier den Mandanten an in den sich der Public Worker standardmäßig einloggen soll.

Adressnummer: **Beschränkung der möglichen Angezeigten Aufträge auf eine Adressnummer**

Startprogrammnummer: Geben Sie hier die Programmnummer an die nach dem Anmelden des Public Workers ausgeführt werden soll.

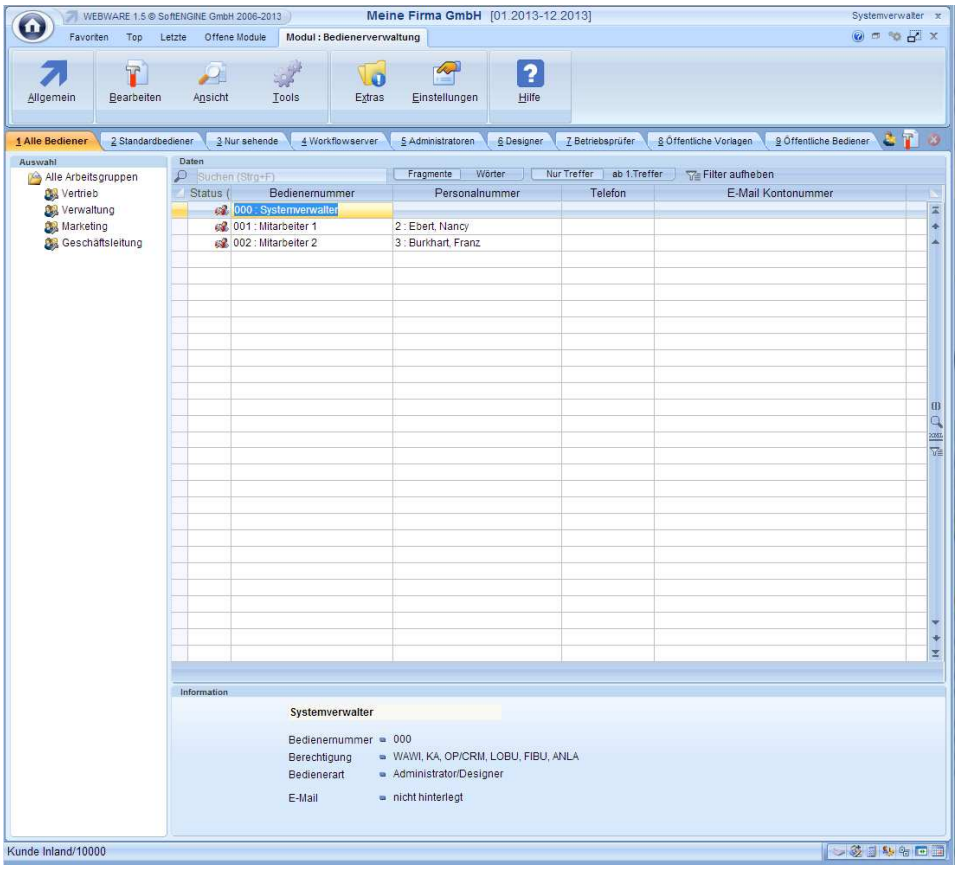
Startmodulnummer: Geben Sie hier die Modulnummer an die nach dem Anmelden des Public Workers ausgeführt werden soll.

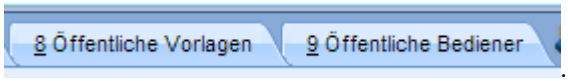
max. Zeitdauert Inaktivität:

WEBWARE 1.5x Öffentliche Benutzer Verwaltung

Die Öffentliche Benutzer Verwaltung (Public Worker) ist ab der Version 1.5 im Designer im Bereich

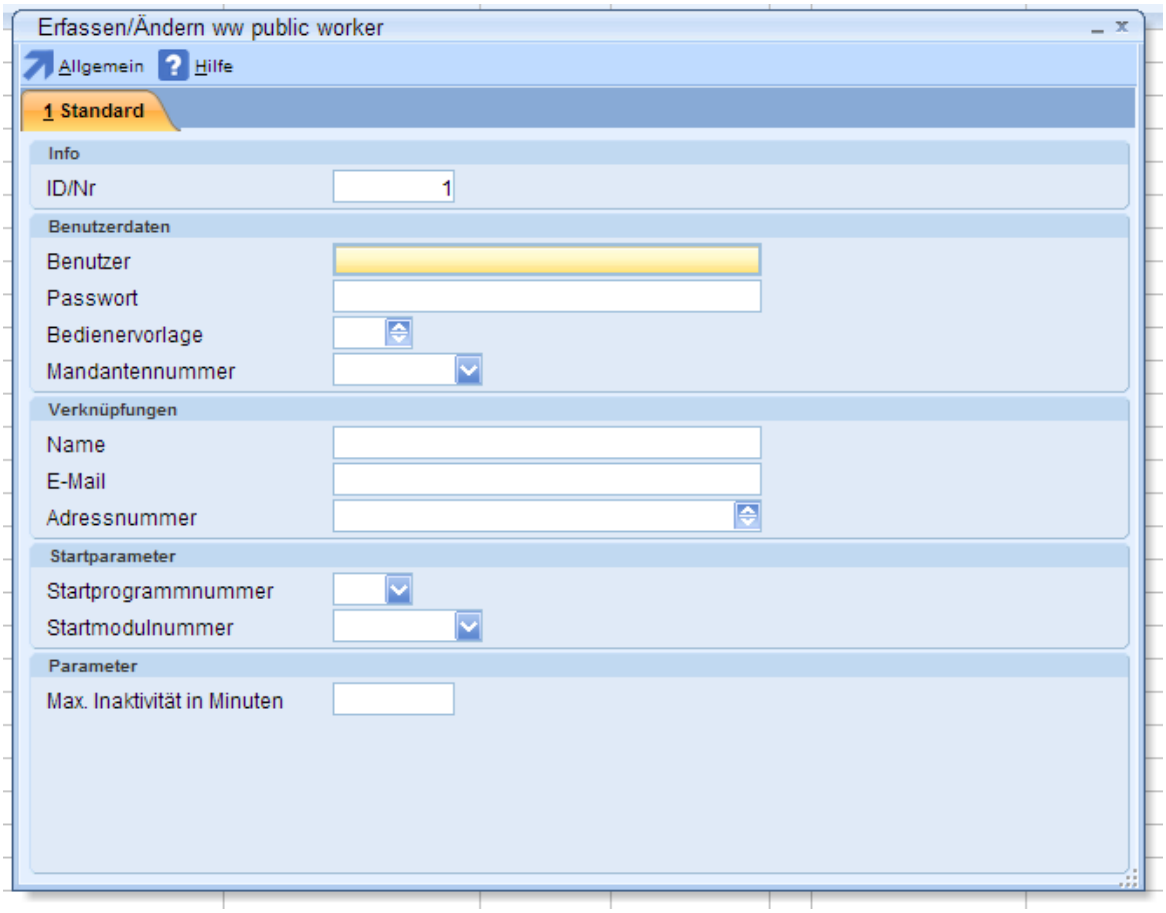
Bedienerverwaltung integriert.



Hier gibt es für die WW 

. Mit diesen können die Öffentlichen Benutzer sowie Öffentliche Vorlagen verwaltet werden.

Mit F3 können neue Öffentliche Benutzer angelegt werden. Die Beschreibung entspricht der Beschreibung weiter oben unter 1.0x Verwaltung.



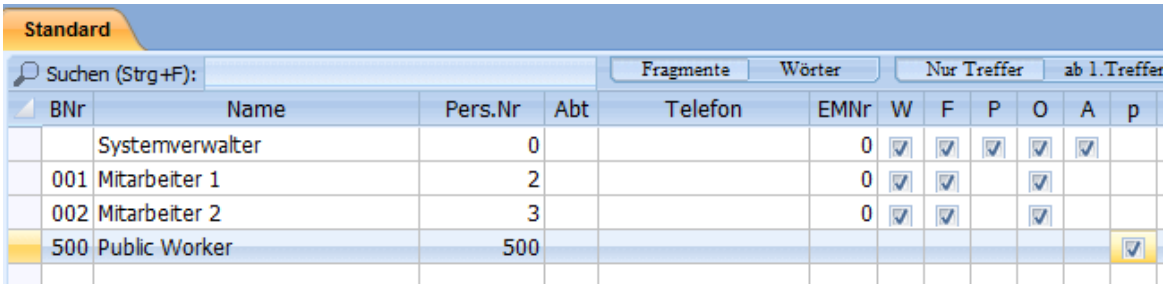
Öffentliche Benutzer Vorlagen

Die Öffentlichen Benutzer werden Aufgrund von Vorlagen gruppiert. Durch Sperrung von Vorlagen können alle Benutzer die diese Vorlage verwenden gesperrt bzw. freigegeben werden.

Eine Vorlage wird im Bereich der Personal-Verwaltung innerhalb der WEBWARE-Datenbank definiert.

Benutzer Vorlagen in WW 1.0 definieren

Dabei wird durch die letzte Spalte „p" (Public Worker) definiert das der Benutzer als Vorlage bzw. Öffentlicher Benutzer verwendet werden soll.

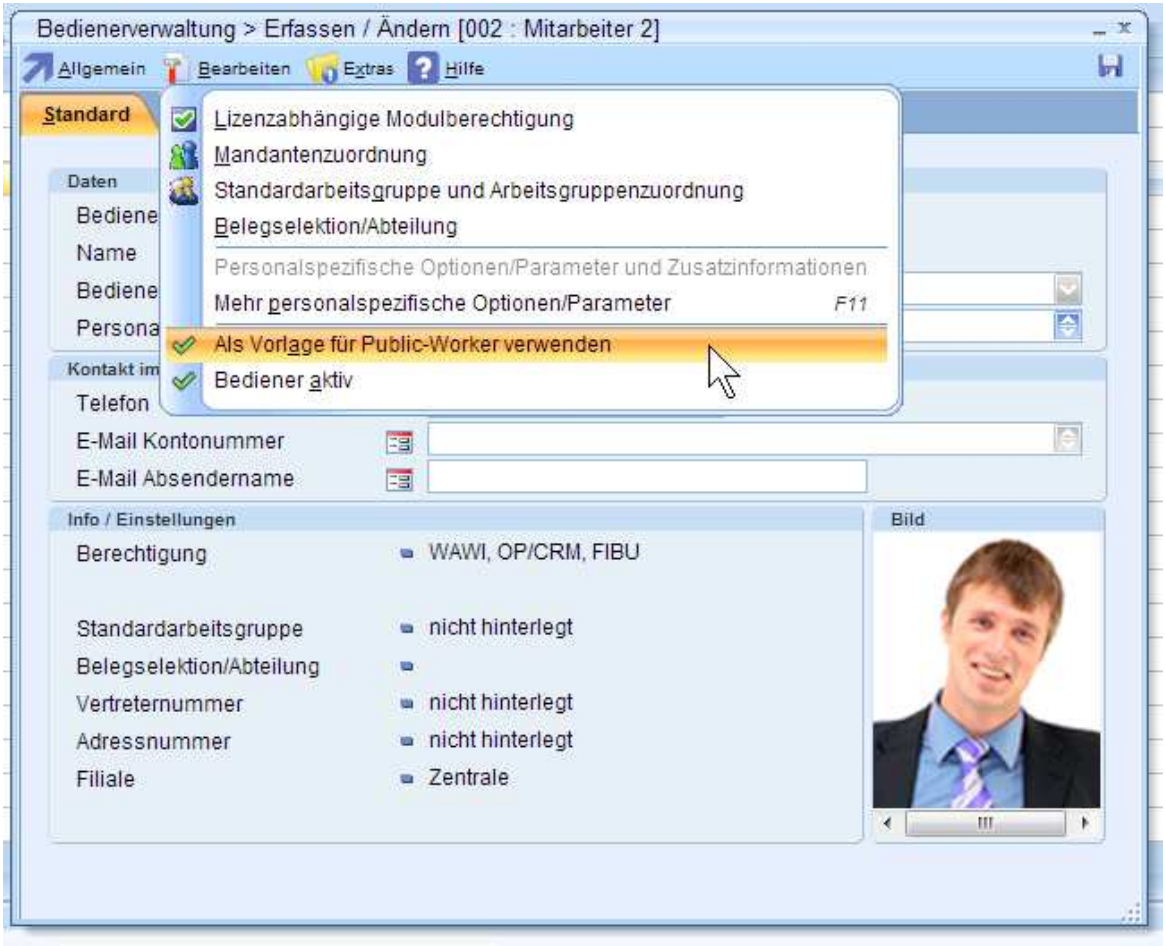


BNr	Name	Pers.Nr	Abt	Telefon	EMNr	W	F	P	O	A	p
	Systemverwalter	0			0	☑	☑	☑	☑	☑	
001	Mitarbeiter 1	2			0	☑	☑		☑		
002	Mitarbeiter 2	3			0	☑	☑		☑		
500	Public Worker	500									☑

Benutzer Vorlagen in WW 1.5 definieren

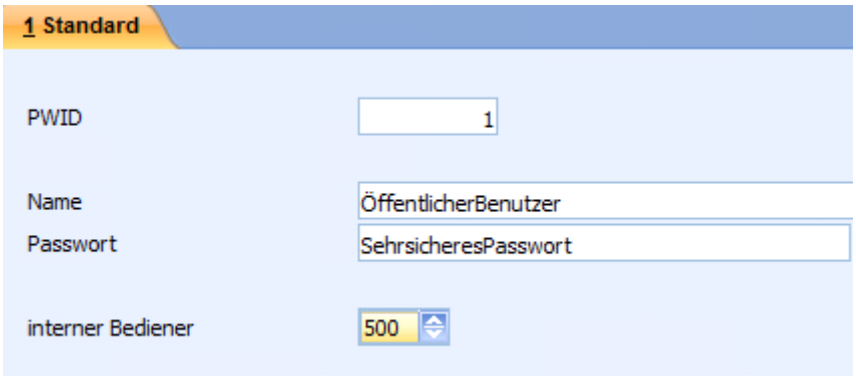
In der WEBWARE 1.5 kann man Vorlagen im Bereich der Bedienerverwaltung definieren. Öffnen Sie hierzu im Designer unter Menü Allgemein die Bedienerverwaltung.

Wählen Sie nun einen Bediener aus den sie als Vorlage für PUBLIC-Worker verwenden wollen aus, und führen Sie den Bearbeiten Dialog aus.

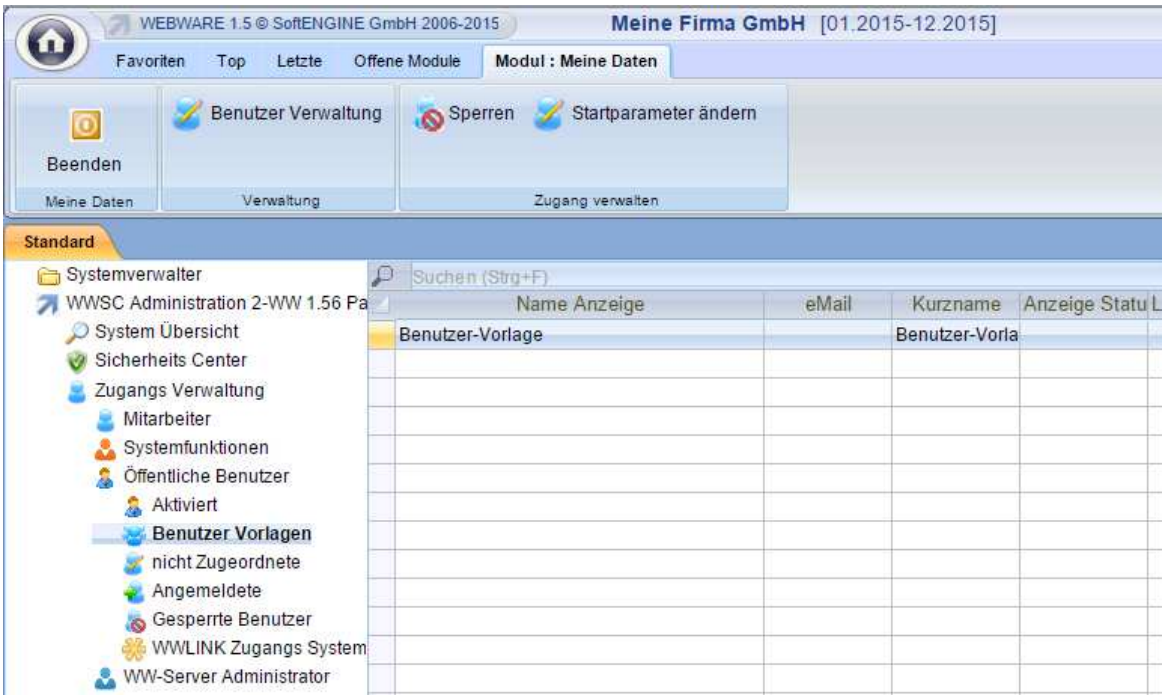


Mit dem Menübefehl Bearbeiten >> „Als Vorlage für Public-Worker verwenden“ können Sie nun den Bediener als Vorlage aktivieren. Durch entfernen der Markierung wird der Mitarbeiter zum normalen Bediener.

Wichtig: Das anmelden mit der Public-Worker Vorlage direkt ist nicht möglich. Nur davon abgeleitete Public-Worker können sich anmelden.



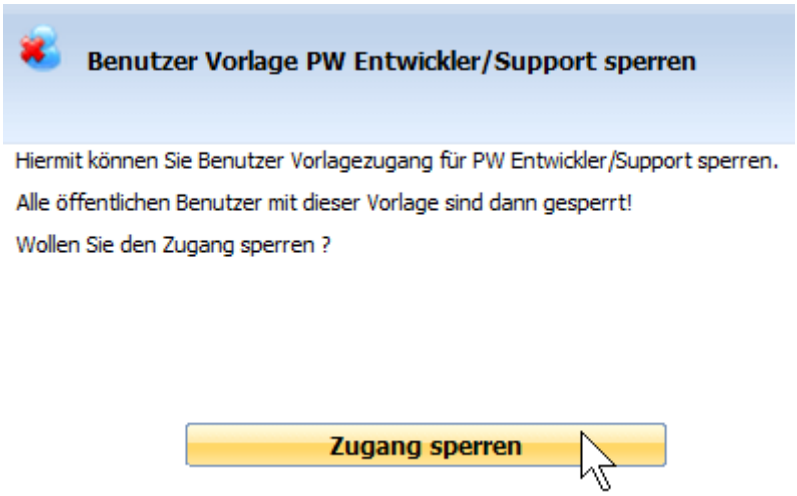
Die Zuordnung eines PUBLIC-Workers erfolgt in der IDB-0125 mit dem Feld „interner Bediener“



Nachdem eine PUBLIC-Worker-Vorlage erstellt ist, ist diese auch im WW-System-Cockpit verfügbar. Mit dem Menü-Befehl "Benutzer-Verwaltung" ist die Programm-Benutzer-Verwaltung jederzeit aufrufbar. Sie können hier wie im Folgenden beschrieben die Vorlagen verwenden.

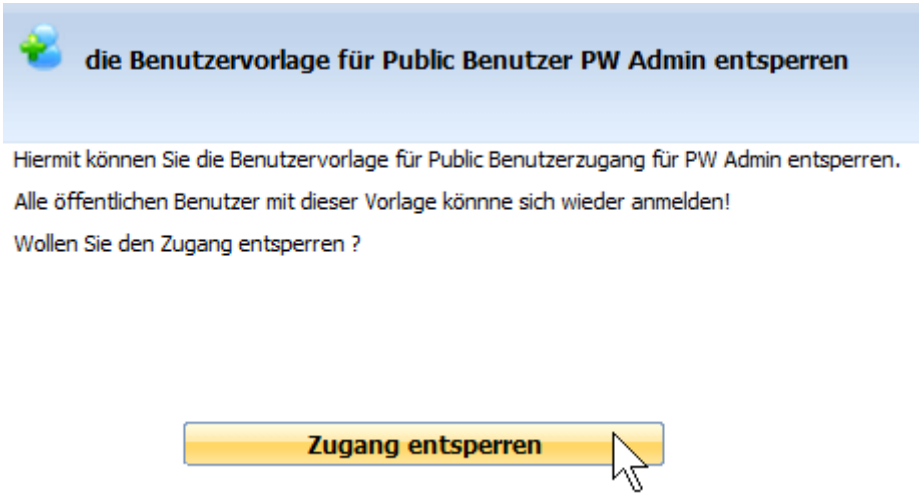
Benutzer Vorlage Sperren

Hiermit können Sie die Benutzervorlage und alle abhängige öffentliche Benutzer sperren.



Benutzer Vorlage Entsperren

Hiermit können Sie eine gesperrte Vorlage, und somit die zugehörigen öffentlichen Benutzer wieder für die Anmeldung freigeben.



Startparameter ändern

Hier kann das Startprogramm und der gewünschte RAR-Server für eine Benutzer-Vorlage definiert werden. Damit können die Startparameter für alle öffentliche Benutzer die von dieser Benutzer-Vorlage abgeleitet sind vorgegeben werden. Falls ein abgeleiteter öffentlicher Benutzer eine eigene Definition für die Startparameter hat, so wird diese verwendet.

Die Startauswahl steht für Benutzer-Vorlage und damit öffentlichen Benutzer nicht zur Verfügung.

Aktionen für aktivierte öffentliche Benutzer

Für die aktivierten öffentliche Benutzer können die obigen Aktionen ausgeführt werden, welche ähnlich der

Funktionen für interne Benutzer sind.

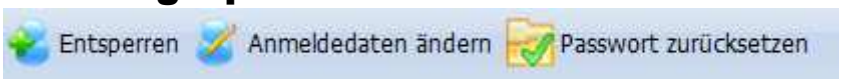
Besonderheit ist hier die Funktion Startparameter ändern

Startparameter ändern

Hier kann das Startprogramm und der gewünschte RAR-Server für einen öffentlichen Benutzer festgelegt werden. Falls hier nichts vorgegeben wird, so wird die Vorgabe der Benutzer-Vorlage verwendet.

Die Startauswahl steht für öffentliche Benutzer nicht zur Verfügung.

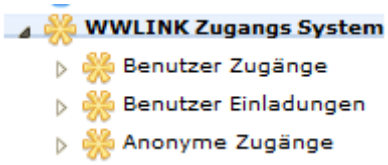
Aktionen für gesperrte öffentliche Benutzer



Für die gesperrten öffentlichen Benutzer können die obigen Aktionen ausgeführt werden, welche ähnlich der Funktionen für interne Benutzer sind.

WW-LINK-Zugangs-System für öffentliche Benutzer

Öffentliche Benutzer haben 3 Arten von Zugangspunkte zum WW-System.



- Benutzer Zugänge
- Benutzer Einladungen
- Anonyme Zugänge

Bei Aktivierung eines WW-LINK eines öffentlichen Benutzers, wird die Anwendung und auch die Benutzeranmeldung über den PUBLIC-Worker Zugang mit eingeschränkten Rechten ausgeführt.

Abweichend zu den normalen Mitarbeiter WW-LINK's ist es möglich auch Anonyme WW-LINK's für öffentliche Benutzer zu erstellen. Dabei ist es möglich ohne Login-Anmelde-Maske direkt für einen Benutzer ein Programm zu starten, und mit dem im WW-LINK hinterlegten Programmteil zu arbeiten.

Wichtig ist das solche Zugänge entweder im Gültigkeitszeitraum, bzw. in der Anzahl Aufrufe begrenzt werden.

Übersicht Änderungen an diesem Dokukment

Änderungsdatum	Änderungsgrund/Erweiterung
Rel 10: 05.11.2013	Bereich Benutzer-Programm Definitionen Neuer Parameter für Verbergen der RiBa-Menüzeile beim Start
Rel 11: 20.11.2013	Passwort Zurücksetzen Funktion integriert.
Rel 12: 01.03.2014	WW Front Line Server Dokumentation aufgenommen, einige Typo's entfernt.
REL 13: 25.06.2014	Neue Funktion Startprogramm/Rar-Server Vorgabe für Public-Worker sowie für die Public-Worker-Vorlage
REL 14: 11.02.2015	Erweiterung von WWLINK um WW-Validation-Link's (Aufruf-Code 32) System-link
REL 15: 28.05.2015	Einbau Informationen das aus dem System-Cockpit Administration>Benutzer-Verwaltung direkt die Benutzer-Verwaltung aus dem Anwendungsbereich aufgerufen werden kann.
REL 16: 29.06.2015	Erweiterung um die WW 2.0 Anmelde-Seiten PUBLIC2.HTM und PUBLICT2.HTM für Public-Worker Anmeldung im neuen Design..