



WW SHIELD

Geräte Zugangs
Kontrolle
der

WEBWARE

Rel 1 vom 01.07.2013

WEBWARE

WERNER LAUTH

INHALTSVERZEICHNIS

<i>WW SHIELD Geräte Zugangs Kontrolle</i>	<i>1</i>
WW SHIELD Geräte Zugangs Kontrolle - Benutzersicht	2
WW SHIELD Geräte Zugangs Kontrolle Konfiguration	3
<i>Konfiguration der WW-SHIELD Zugangs Kontrolle</i>	<i>3</i>
WW SHIELD IntraNet Vorgaben	4
WW SHIELD InterNet Vorgaben	4
<i>Sicherheits-Center WW SHIELD Zugangs Kontrolle</i>	<i>5</i>
WW SHIELD Geräte Zugangs Kontrolle - Verwaltung	6
<i>WW-SHIELD Zugangs Kontroll Workflow</i>	<i>7</i>
<i>Neue Geräte ohne Anmeldung</i>	<i>8</i>
<i>Quarantäne neue Geräte</i>	<i>8</i>
Löschen/Entfernen	9
Freigeben	9
Details	10
<i>Neue erlaubte Geräte</i>	<i>11</i>
Löschen/Entfernen	11
Sperren/Quarantäne	11
Details	11
<i>Alle freigegebenen Geräte</i>	<i>12</i>
Löschen/Entfernen	12
Sperren/Quarantäne	12
Details	12
<i>Aktuell verbundene Geräte</i>	<i>13</i>
Sitzung Abbrechen	13
<i>Gesperrt + Fehler</i>	<i>13</i>
Freigeben	14
<i>Gelöschte Geräte</i>	<i>14</i>
Wiederherstellen	14

WEBWARE SHIELD



WW SHIELD Geräte Zugangs Kontrolle

Mit WW SHIELD, haben Sie die Möglichkeit für einzelne Geräte (Desktop/Tablet/Phone) den Zugang zu Ihrem WEBWARE-System zu Kontrollieren, und zu Begrenzen.

Dabei können Sie getrennt für IntraNet und InterNet, einzelnen Geräteklassen (Desktop/Tablet/Phone) nur nach erfolgreicher Freigabe durch den Systembetreuer den Zugang gewähren.

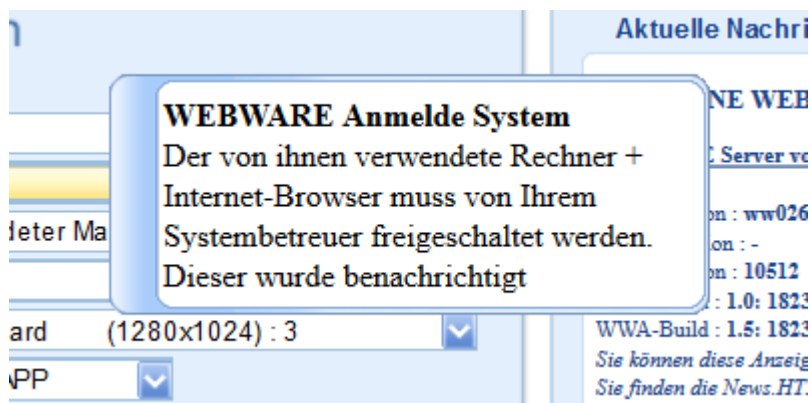
Zusätzlich haben Sie die Möglichkeit, durch Angabe eines SecureNet-Bereiches, gezielt Netzwerksegmente von der Zwangsfreigabe zu Befreien.

WW SHIELD bietet folgende Merkmale:

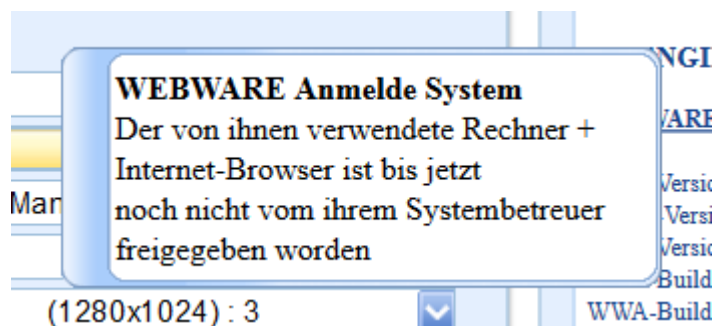
- Registrierung aller Geräte die mit Ihrem WEBWARE System kommunizieren
- Definition von offenen Zugangs-Netz Bereichen, bei denen keine Freigabe erfolgen muss
- Festlegung von Geräteklassen für die eine Zugangsfreigabe erfolgen soll getrennt für IntraNet + InterNet
- Verwaltung der Geräte im System-Cockpit des Systembetreuer
- Benachrichtigung durch das WEBWARE Messaging System bei Anträgen und Statusänderung
- Integration in das Sicherheit-Center im System-Cockpit

WW SHIELD Geräte Zugangs Kontrolle - Benutzersicht

Mit WW SHIELD wird der Zugang zu Ihrem WEBWARE-System auf Geräteebeke begrenzt. Das bedeutet für Sie das der Zugang erst nach Freigabe durch den Systembetreuer erfolgen kann. Möchten Sie sich mit ihrem Gerät (Desktop/Tablet/Phone-Mobile) zum Ersten Mal an Ihrer WEBWARE anmelden, erhalten Sie nach Eingabe der Korrekten Zugangsdaten folgenden Hinweis:



Der Systembetreuer muss nun den Zugang manuell freigeben. Melden Sie sich erneut an, und der Zugang ist noch nicht freigegeben, so erhalten Sie folgende Meldung:



Nach erfolgreicher Freigabe durch den Systembetreuer ist der Zugang dann uneingeschränkt möglich.

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 freigegeben	0
Neue Tablet Geräte muss Admin freigegeben	0
Neue Phone Geräte muss Admin freigegeben	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 freigegeben	J
Neue Tablet Geräte muss Admin freigegeben	J
Neue Phone Geräte muss Admin freigegeben	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 WEBWARE 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.

Sicherheits-Center von XL14-WWS

- + **Passwort System**
- + **Sitzungs-FireWALL**
- + **Verbindungs-FireWALL**
- + **SSL-Protokoll-FireWALL**
- + **RAR Server Anbindung**
- + **SecureNET Netzwerkzugriffsbegrenzung**
- + **WWLINK System Sicherheit**
- + **WW@home Client Communicator Sicherheit**
- + **Automatische Komponenten Aktualisierung**
- + **TAPI-Subsystem Sicherheit**
- + **WW Auto Login System (WALIS)**
- **WW Geräte Zugriffsüberwachung System**
 - Mit diesem System sollten Sie den Zugang von Benutzer-Rechnern/Browsern überwachen und Neue Geräte freigeben
 - ✓ Geräte Registrierung aktiv, neue Geräte (Browser) werden protokolliert
 - ✓ Freigabe von neuen Geräten muss von Systembetreuer erfolgen
 - ✓ SecureNet Netzbereich für Geräte für die keine Freigabe durch Systembetreuer notwendig ist (optional) [192.168.99 192.168.98]
 - IntraNet Vorgaben: Geräteklassen die bei aktiviertem System vom Systembetreuer freigegeben werden sollen
 - Desktop Browser: keine Freigabe notwendig
 - Tablet Browser: keine Freigabe notwendig
 - Phone Browser: keine Freigabe notwendig
 - InterNet Vorgaben: Geräteklassen die bei aktiviertem System vom Systembetreuer freigegeben werden sollen
 - ✓ Desktop Browser: **Systembetreuer muss freigeben**
 - ✓ Tablet Browser: **Systembetreuer muss freigeben**
 - ✓ Phone Browser: **Systembetreuer muss freigeben**

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 weitem 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.

WEBWARE SHIELD Zugangs Kontroll System

Mit dem WW SHIELD Zugangs Kontroll System können Sie den Zugang zu Ihrem System auf bestimmte Geräte begrenzen bzw. überwachen.

Aktuelle Einstellungen

Benutzer Geräte registrieren: **aktiviert**
 Benutzer Geräte von Systembetreuer freigeben: **aktiviert**
 SecureNet Sicherer Bereich in dem keine Freigabe notwendig ist: **vorhanden**
 [192.168.99 192.168.98]

IntraNet Vorgabe für Geräte Freigabe

- Desktop Browser : **Keine Freigabe notwendig**
- Tablet Browser : **Keine Freigabe notwendig**
- Phone/Mobile Browser : **Keine Freigabe notwendig**

InterNet Vorgabe für Geräte Freigabe

- Desktop Browser : **Freigabe durch Systembetreuer**
- Tablet Browser : **Freigabe durch Systembetreuer**
- Phone Browser : **Freigabe durch Systembetreuer**

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

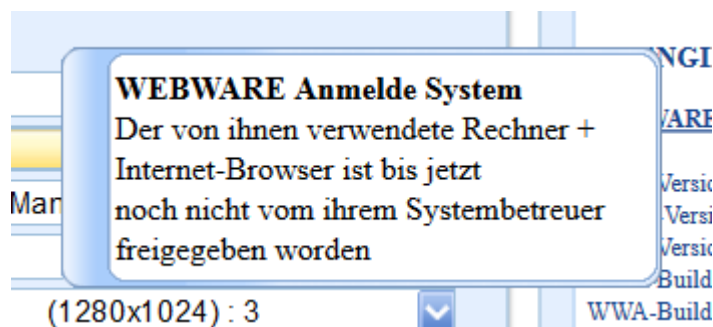


Nach Aktivierung der WW-SHIELD Zugangs Kontrolle, werden alle neu verbundenen Browser-Geräte mit einer Kennung versehen und in einer internen Datenbank mit ihrem aktuellen Zugangs-Status gespeichert.

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.



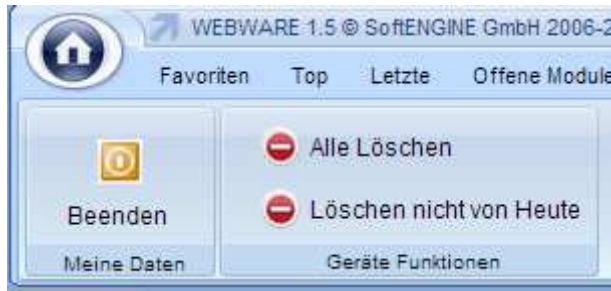
Die Zugangsinformationen werden unterhalb des WW Zugangsschutz (SHIELD) Eintrages in folgende Bereiche unterteilt:

- 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:

☆	WW-Server Quarantäne für neues Gerät, Bitte bearbeiten	WEBWARE-36-Server
Betreff	WW-Server Quarantäne für neues Gerät, Bitte bearbeiten	Antworten Weiterlei
An	SystemAdmin@WW-36.de	

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.

WEBWARE Anmelde- und Login-System

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

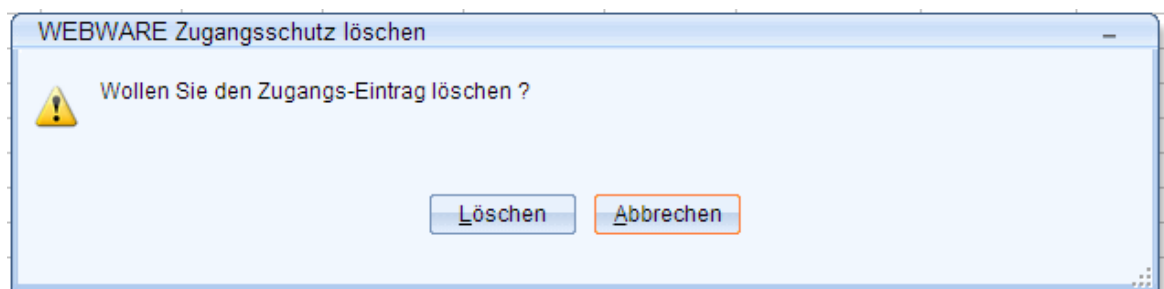
Gehört zu Benutzer	G	Browserinfo	Erzeugt am	Erzeugt um	Verwendet a	Verwendet u	Betriebssys	IP-Adresse	Text
Systemverwalter	D	Firefox 21.0	1.07.2013	11:58:55	1.07.2013	11:59:09	Windows	192.168.13.130	
Mitarbeiter 1	D	MSIE 10.0;	1.07.2013	13:50:47	1.07.2013	14:02:07	Windows	192.168.13.101	

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



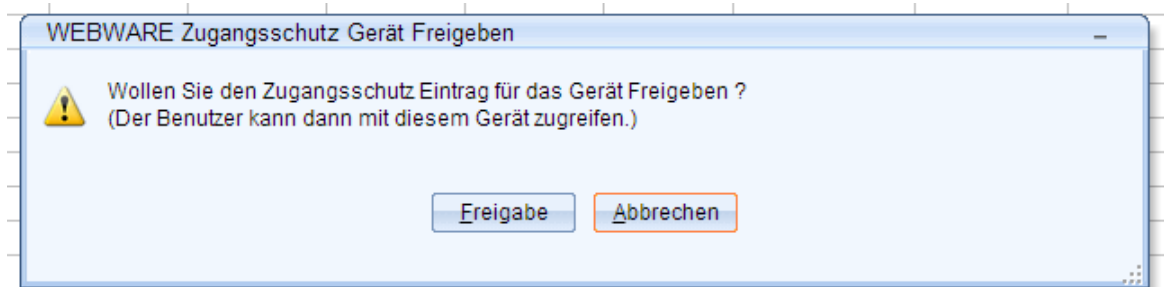
Löschen/Entfernen

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



Freigeben

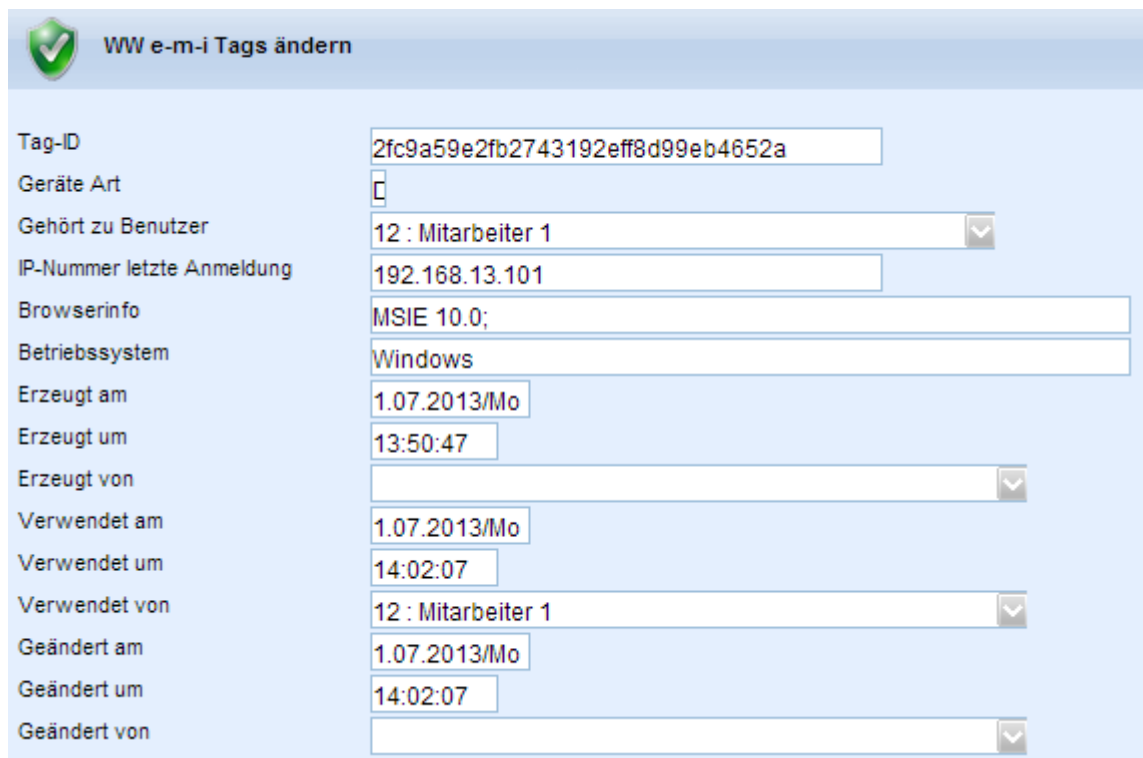
Der Eintrag wird nach einer Sicherheitsabfrage in den Ast Alle freigegebenen Geräte verschoben.



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.



The screenshot shows a web form titled 'WW e-m-i Tags ändern' with a green checkmark icon. The form contains the following fields and values:

Field	Value
Tag-ID	2fc9a59e2fb2743192eff8d99eb4652a
Geräte Art	C
Gehört zu Benutzer	12 : Mitarbeiter 1
IP-Nummer letzte Anmeldung	192.168.13.101
Browserinfo	MSIE 10.0;
Betriebssystem	Windows
Erzeugt am	1.07.2013/Mo
Erzeugt um	13:50:47
Erzeugt von	
Verwendet am	1.07.2013/Mo
Verwendet um	14:02:07
Verwendet von	12 : Mitarbeiter 1
Geändert am	1.07.2013/Mo
Geändert um	14:02:07
Geändert von	

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

Neben der Benutzererkennung, 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

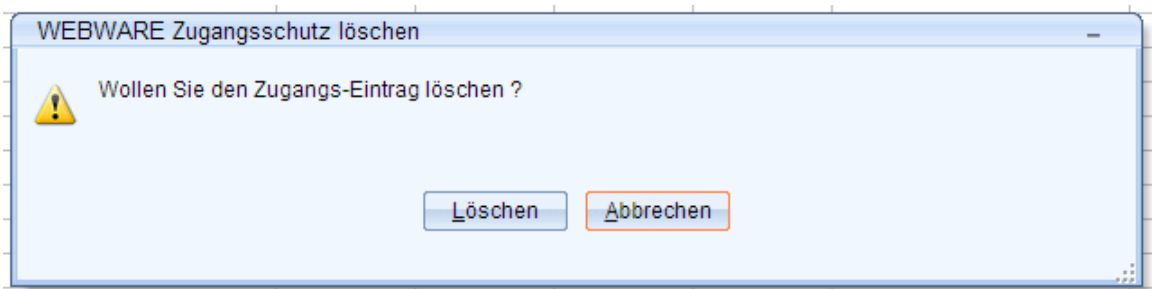
informiert.

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.

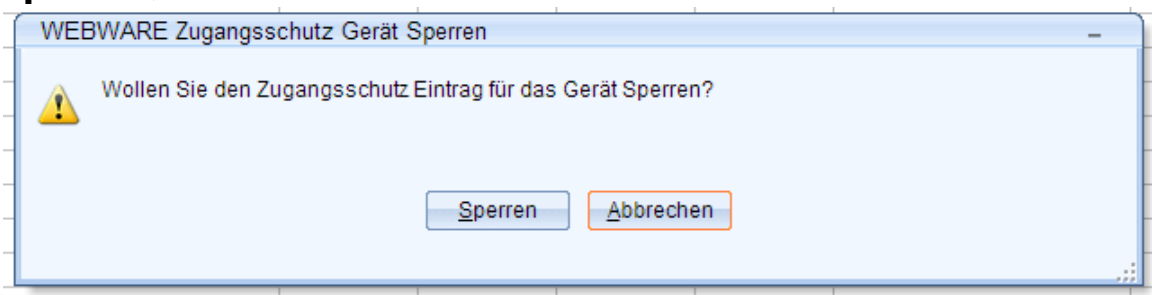


Löschen/Entfernen



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 Info's 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.

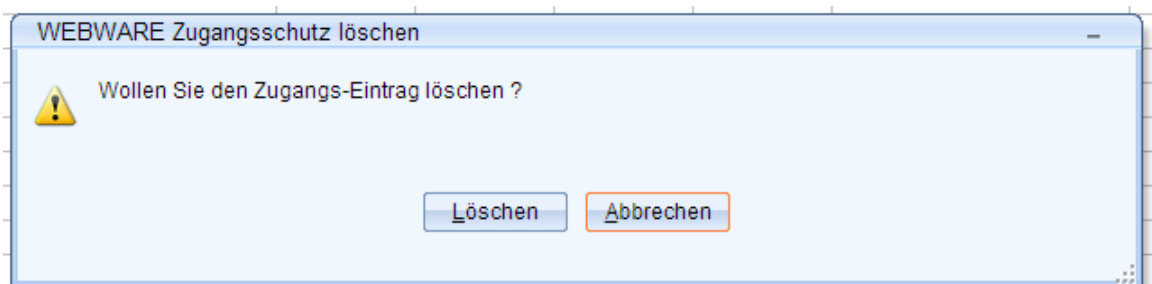
Geräte die in diesem Bereich angezeigt werden, dürfen sich ohne Einschränkungen an der WEBWARE anmelden.

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

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

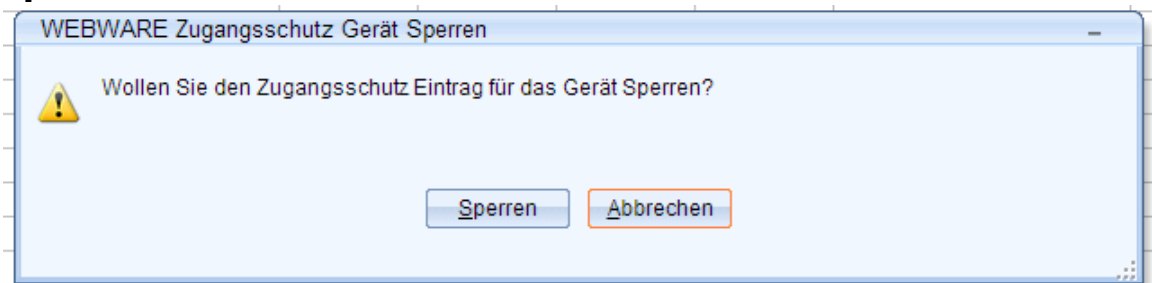


Löschen/Entfernen



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.

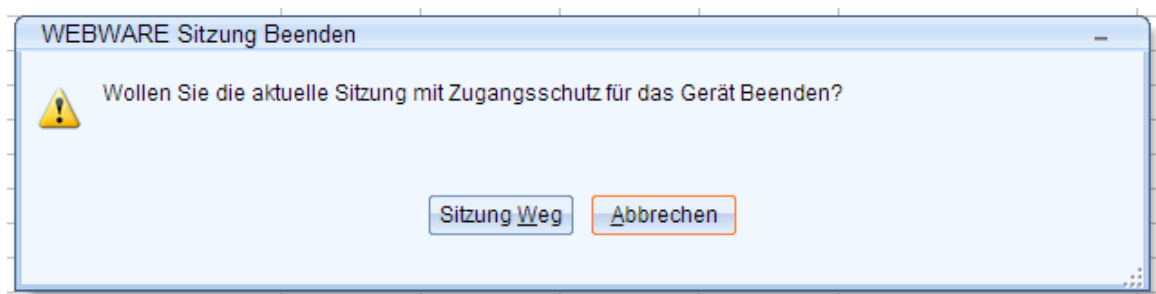
Folgende Funktionen stehen nach Selektion eines Gerätes zur Bearbeitung zur Verfügung.



(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.

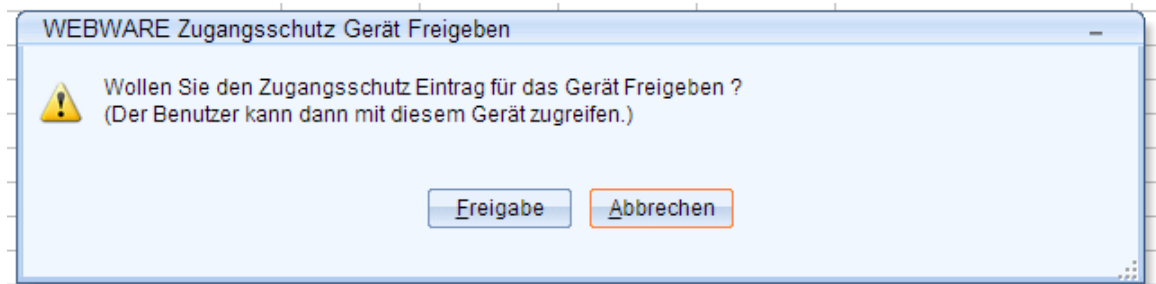
Sie haben nach Selektion eines Geräte-Eintrages folgende Menüfunktionen



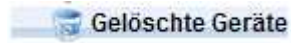
(Löschen/Entfernen + Details, siehe weiter oben.)

Freigeben

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



Gelöschte Geräte



Gelöschte Geräte

Hier werden alle Geräte aufgelistet die während der aktuellen WEBWARE-Server Laufzeit gelöscht wurden. Durch einem WEBWARE-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.

