



WALIS  
Automatisches Login  
System  
der  
**WEBWARE**

Rel 2 vom 08.08.2013

WEBWARE

WERNER LAUTH

# INHALTSVERZEICHNIS

|  |           |
|--|-----------|
| <i>WALIS WEBWARE Auto Login System</i>                                   | <i>1</i>  |
| <b>WALIS WEBWARE Auto Login System - Benutzersicht</b>                   | <b>2</b>  |
| <i>Wie kann ich WALIS benutzen ?</i>                                     | <i>2</i>  |
| <i>Programmstart Hinweis auf möglichen Auto-Login</i>                    | <i>3</i>  |
| <i>Antrags Verarbeitung</i>  | <i>3</i>  |
| <i>Verwaltung des Auto-Login Zugangs</i>                                 | <i>4</i>  |
| Zugang Entfernen   | 4         |
| Nächste Anmeldung ohne Automatik   | 4         |
| <b>WALIS WEBWARE Auto Login System - Konfiguration</b>                   | <b>5</b>  |
| <i>Konfiguration des WALIS Auto Login System</i>                         | <i>5</i>  |
| WALIS: Auto Login ist aktiv  | 6         |
| WALIS: Neue Geräte vom Administrator freigeben                           | 7         |
| WALIS: Maximale Anzahl Geräte pro Benutzer                               | 7         |
| WALIS: Maximale Login-Fehler für Sperrung Gerät                          | 7         |
| WALIS: Auto-Login aktiviert, auch wenn kein SecureNet Area definiert ist | 7         |
| WALIS: Für Desktop Browser erlaubt                                       | 7         |
| WALIS: Für Tablet Browser erlaubt.                                       | 7         |
| WALIS: Für Phone Browser erlaubt   | 7         |
| WALIS: Desktop Browser direkt anmelden                                   | 7         |
| WALIS: Tablet Browser direkt anmelden                                    | 7         |
| WALIS: Tablet Browser direkt anmelden                                    | 7         |
| WALIS: Zeige Einladungshinweis für Geräte ohne Auto-Login                | 8         |
| WALIS: Anzeigedauer Einladungshinweis                                    | 8         |
| <i>Zugangsbeschränkung für Dauieranmeldung</i>                           | <i>8</i>  |
| SecureNetArea unbegrenzter AutoLogin                                     | 9         |
| Zeit-Lock definiert  | 9         |
| Auto-Login erlaubt ab- bis- Uhrzeit                                      | 9         |
| Auto-Login Montag-Sonntag erlaubt  | 9         |
| Benutzer dürfen Auto-Login verwenden                                     | 9         |
| Public-User dürfen Auto-Login verwenden                                  | 9         |
| <i>Zugangsbeschränkung 1x täglich anmelden</i>                           | <i>10</i> |
| SecureNetArea AutoLogin 1x täglich anmelden                              | 10        |
| Zeit-Lock definiert  | 10        |
| Auto-Login erlaubt ab- bis- Uhrzeit                                      | 10        |
| Auto-Login Montag-Sonntag erlaubt  | 11        |
| Benutzer dürfen Auto-Login verwenden                                     | 11        |
| Public-User dürfen Auto-Login verwenden                                  | 11        |
| <i>Sicherheits-Center WW Auto Login System (WALIS)</i>                   | <i>11</i> |
| <b>WALIS WEBWARE Auto-Login System - Verwaltung</b>                      | <b>13</b> |
| <i>Wie verwalte ich mein WALIS Auto Login System</i>                     | <i>14</i> |
| WALIS Workflow für Anforderung von Auto-Login Funktionen                 | 14        |
| Quarantäne neue Geräte   | 14        |
| Alle registrierten Geräte  | 17        |
| Aktuell verbundene Geräte  | 18        |
| Gesperrte+Fehler Geräte  | 20        |
| Erzeugte eTags   | 21        |
| Gelöschte Geräte   | 22        |

# WEBWARE WALIS

---



## WALIS WEBWARE Auto Login System

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. Automatisches Dauernmelden

- Automatisches Anmelden mit 1x täglich Anmelden
- SecureNet Bereiche um das Auto-Login auf bestimmte Netzbereiche/Segmente zu Beschränken
- Zeitliche Vorgabe / Wochentag + Kernzeit für erlaubte automatisierte Anmeldung
- Volle Konfiguration der Anmeldeart (Sofort/Vorbelegung Anmeldebildschirm)
- Konfigurierbarer Registrierung Workflow mit Verwaltung durch den Systembetreuer
- Integration in den Sicherheits-Center der WEBWARE
- Integration in das WEBWARE Messaging System, Status- und Antragsmeldungen per eMail
- Freischaltung der Grundfunktion auf Geräte-Art Ebene /Desktop/Tablet/Phone

## WALIS WEBWARE Auto Login System - Benutzersicht

Mit WALIS können Sie als Benutzer der WEBWARE automatisch an die WEBWARE anmelden. Ist das WALIS von ihrem Systembetreuer aktiviert so erhalten Sie, abhängig von Ihrem Standort/Netzanbindung erweiterte Funktionen.

Ziel von WALIS ist es, die Anmeldung zu automatisieren, und Ihnen den Zugang zur WEBWARE zu Erleichtern.

### Wie kann ich WALIS benutzen ?



Wenn WALIS aktiviert ist erhalten Sie in Ihrem System-Cockpit einen neuen Eintrag "Automatisches Anmelden". Damit können Sie den Auto-Login Zugang für ihr aktuelles Gerät(Desktop/Tablet/Phone) anfordern, sowie diesen auch Verwalten.

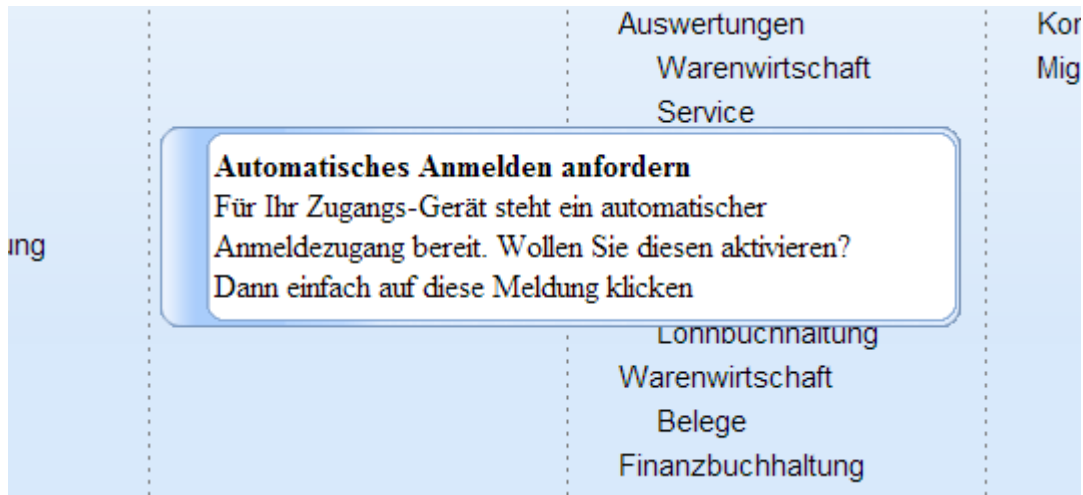


Es gibt nun 2 Möglichkeiten für Sie den Auto-Login zu aktivieren.

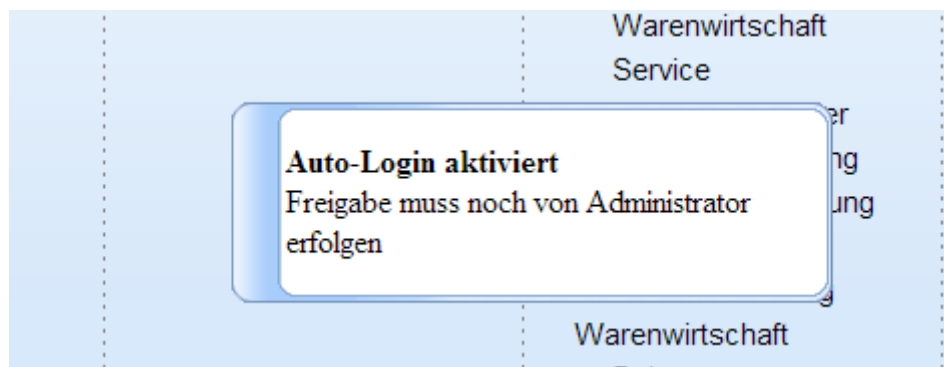
- Auswahl über System-Cockpit "Zugang anfordern" (Siehe Grafik oben)
- Bei aktiviertem Einladungshinweis für Geräte ohne Auto-Login wird ein Fenster mit Aufforderung zum Klick auf das Fenster bei Programmstart gesendet. Dadurch wird ebenfalls die Zugangsanforderung ausgelöst.

## Programmstart Hinweis auf möglichen Auto-Login

Hat der Systembetreuer die automatische Einladungsfunktion aktiviert, so wird bei nicht vorhandenem Auto-Login und passenden Netzwerkzugang beim Programmstart 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:



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.

## Antrags Verarbeitung

Nachdem ein Auto-Login Antrag ausgelöst wurde, erhält der Systembetreuer eine Benachrichtigung, mit der Aufforderung den Antrag zu Bearbeiten. Nach Prüfung gibt der Systembetreuer diesen frei. Ab diesem Zeitpunkt ist der Auto-Login mit Ihrem Gerät möglich.



## Verwaltung des Auto-Login Zugangs



Ist der Auto-Login Zugang angefordert, so wird dies im System-Cockpit wie oben dargestellt.

Hier haben Sie folgende Möglichkeiten.

### Zugang Entfernen

Mit diesem Befehl können Sie den Auto-Login Antrag zurück ziehen. Das aktuelle Gerät erhält dann den Status: Keine Auto-Login Information vorhanden.

### Nächste Anmeldung ohne Automatik

Hiermit können Sie den Auto-Login Zugang für die nächste Anmeldung abschalten. Dies kann nützlich sein, wenn Sie kein sofortiges Anmelden, nach dem Programmende wünschen.

Bei freigegebenem Auto-Login erhalten Sie den unten stehenden Zustand angezeigt.



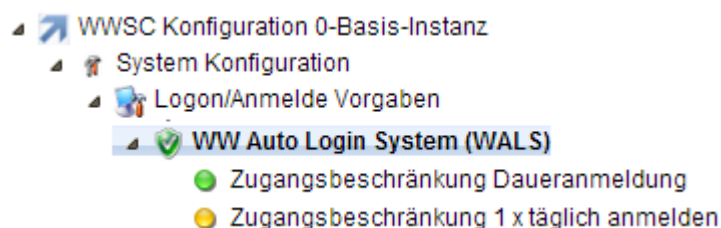
## WALIS WEBWARE Auto Login System - Konfiguration

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                          | J |
| Neue Geräte von Administrator freigeben              | 1 |
| Maximale Anzahl Geräte pro Benutzer                  | 1 |
| Maximale Login-Fehler für Sperrung Gerät             | 3 |
| Auto-Login aktiviert, auch wenn kein SecureNetArea d | 1 |
| für Desktop Browser erlaubt                          | 1 |
| für Tablet Browser erlaubt                           | 1 |
| für Phone Browser erlaubt                            | 1 |
| Desktop Browser direkt anmelden                      | J |
| Tablet Browser direkt anmelden                       | 1 |
| Phone Browser direkt anmelden                        | 1 |
| Zeige Einladungshinweis für Geräte ohne Auto-Login   | J |
| Anzeigedauer Einladungshinweis                       | 5 |



### WALIS: Auto Login ist aktiv

Ist dieser Systemwert gesetzt so wird das WALIS aktiviert, und ist sodann einsatzbereit. Der Anwendungsbutzer 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 maximale Anzahl von aktiven Auto-Login Zugängen je Benutzer festgelegt werden. Wird hier ein Wert vorgegeben, so können Benutzer nur noch einen Auto-Login Zugang beantragen wenn die Anzahl aktive Zugänge noch nicht erreicht ist.

**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.

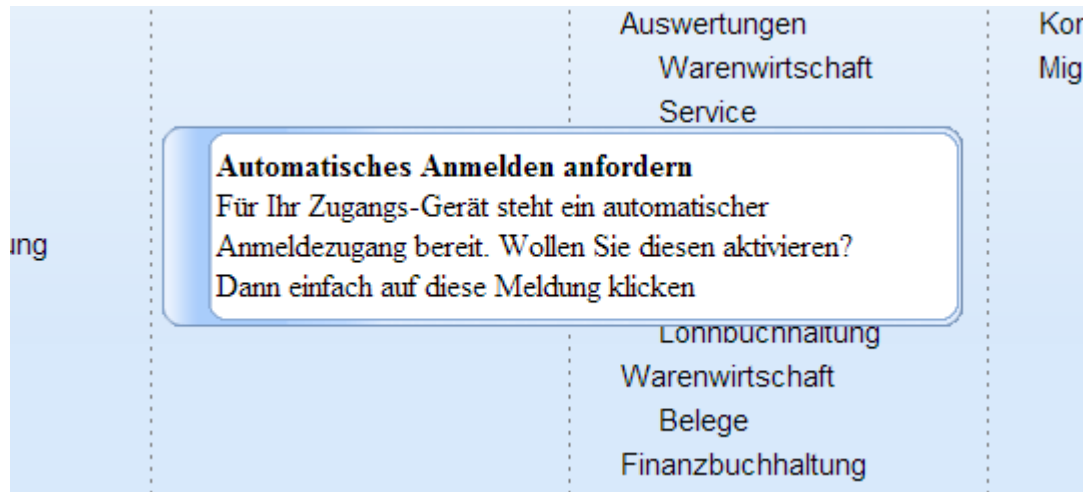
**WALIS: Tablet Browser direkt anmelden**

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.

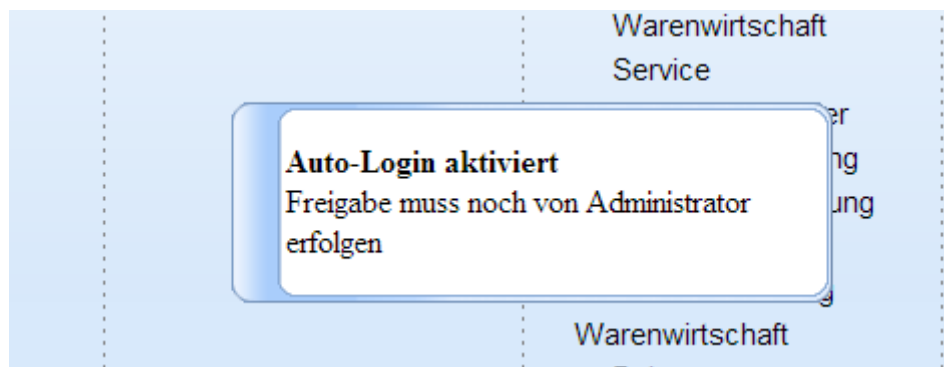
### WALIS: Zeige Einladungshinweis für Geräte ohne Auto-Login

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.

Dies wird nur dann angezeigt wenn dieser Parameter aktiviert ist, und der Benutzer noch nicht die Maximale Anzahl von aktiven Auto-Login Zugängen erreicht hat.



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



### WALIS: Anzeigedauer Einladungshinweis

Hier kann die Anzeigedauer vorgegeben werden, also wie lange die Einladung beim Start angezeigt wird. D

## Zugangsbeschränkung für Daueranmeldung

- WW Auto Login System (WALS)
- Zugangsbeschränkung Daueranmeldung
- Zugangsbeschränkung 1 x täglich anmelden

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

### 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 Komplette 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 vorübergehend abgeschaltet und mit einem Fehler markiert. Der Benutzer kann sich dann nach den Systemrichtlinien normal anmelden.

### Auto-Login Montag-Sonntag 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 vorübergehend 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

-  **WW Auto Login System (WALS)**
-  **Zugangsbeschränkung Daueranmeldung**
-  **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                 |
|--|----------------------------|
| <b>SecureNetArea AutoLogin 1x täglich anmelden</b> | <b>99.98,97 192.168.13</b> |
| <b>Zeit-Lock definiert</b>                         | <b>J</b>                   |
| Auto-Login erlaubt ab Uhrzeit                      | 0                          |
| <b>Auto-Login erlaubt bis Uhrzeit</b>              | <b>240000</b>              |
| 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                          |
| <b>Auto-Login Sonntags erlaubt</b>                 | <b>N</b>                   |
| 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 Komplette 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 vorübergehend abgeschaltet und mit einem Fehler markiert. Der Benutzer kann sich dann nach den Systemrichtlinien normal anmelden.

### Auto-Login Montag-Sonntag 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 vorübergehend 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.

## Sicherheits-Center WW Auto Login System (WALIS)

Das WALIS System ist direkt auch in den WEBWARE Sicherheits-Center integriert. Dort sehen Sie auf einen Blick welche Parameter des WALIS gesetzt sind. Wichtig ist hier das de Systembetreuer die Hoheit über die Freigabe und Verwaltung der Auto-Login Funktion hat.

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

**WW Auto Login System (WALIS)**

- Mit diesem System können Sie das automatische Anmelden an Ihrer WEBWARE konfigurieren
- Benutzer können in Ihrem Systemcockpit einen Auto-Login Zugang beantragen und verwalten.
- ✓ WW Auto Login ist aktiv
- ✓ Neue Geräte/Anforderungen müssen vom Administrator freigegeben werden
- ✓ Nach [4]-Fehlansmeldungen wird das Gerät/Auto-Login für den Benutzer gesperrt
  - Auch Zugang wenn keine SecureNetAreas (Sichere Zugangsbereiche) definiert sind
- ✓ Auto Login Zugang für Desktop Browser erlaubt
- ✓ Auto Login Zugang für Tablet Browser erlaubt
- ✓ Auto Login Zugang für Phone/Mobile Browser erlaubt
- ℹ Mit SecureNET den Zugang durch Netzwerksegmente/Adressen für erlaubtes Dauerlogin begrenzen
  - ✓ Dauerlogin begrenzt auf Netzwerksegmente/Adressen (optional)[10.90.31 177.168.167 99.99.99.99]
  - ✓ Dauerlogin mit Zeitlicher Zugangsbeschränkung
  - ✓ Dauerlogin für Intern Benutzer aktiviert
  - ✓ Dauerlogin für Externe (Public USER) Benutzer aktiviert
- ℹ Mit SecureNET den Zugang durch Netzwerksegmente/Adressen für erlaubtes tägliches Login begrenzen
- ℹ Tägliches Login bedeutet: Der Benutzer muss sich einmal am Tag mit seinen Zugangsdaten anmelden
  - ✓ Tägliches Autlogin begrenzt auf Netzwerksegmente/Adressen (optional)[99.98.97 192.168.13]
  - ✓ Tägliches Login mit Zeitlicher Zugangsbeschränkung
  - ✓ Tägliches Login für Intern Benutzer aktiviert
  - ✓ Tägliches Login für Externe (Public USER) Benutzer aktiviert

## WEBWARE Anmelde- und Login-System

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

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

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

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

|   |   |
|---|---|
| <b>SecureNetArea unbegrenzter AutoLogin</b> | <b>10.90.31 177.168.167 99.99.99.99</b> |
|---|---|

(Daueranmeldung)

|  |                            |
|--|----------------------------|
| <b>SecureNetArea AutoLogin 1x täglich anmelden</b> | <b>99.98,97 192.168.13</b> |
|--|----------------------------|

(1x Täglich anmelden)

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

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



## 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.

The screenshot shows the 'WEBWARE Auto-Login System (WALIS)' configuration window. On the left is a tree view with categories: 'Benutzer Geräte mit AutoLogin' (expanded), 'Quarantäne neue Geräte', 'Alle registrierten Geräte', 'Aktuell verbundene Geräte', 'Gespart+ehler', 'Erzeugte eTags', and 'Gelöschte Geräte'. Each category has sub-items for Desktop, Tablet, and Phone. The right pane shows the configuration for 'Benutzer Geräte mit AutoLogin'.

### WEBWARE Auto-Login System (WALIS)

Mit dem Auto-Login System (WALIS) können Sie die automatisierte Anmeldung an Ihrem System für Benutzer/Netzbereiche verwalten

#### Aktuelle Einstellungen

Auto-Login System ist aktuell: **aktiviert**  
 Freigabe von Auto-Login Anforderungen: **nur durch Systembetreuer**  
 Auto-Login erlaubt auch wenn kein SecureNet-Bereich dafür definiert ist?: **Ja**

#### Auto-Login nach Geräten

- Desktop Browser : **ist erlaubt** Anmeldeart: Anmeldemaske vorbelegen
- Tablet Browser : **ist erlaubt** Anmeldeart: mit direktem Anmelden
- Phone Browser : **ist erlaubt** Anmeldeart: Anmeldemaske vorbelegen

#### Vorgaben für Daueranmeldung - Benutzer muss sich nicht anmelden

SecureNet Netzbereich Daueranmeldung: **ist vorhanden** Netzbereich[10.90.31 177.168.167 99.99.99.99]  
 Daueranmeldung für Interne Benutzer: **ist erlaubt**  
 Daueranmeldung für PUBLIC Benutzer: **ist erlaubt**  
 Daueranmeldung **ist** mit Zeitbeschränkung konfiguriert  
 Zugang erlaubt in der Zeit von 120000 Uhr bis 240000 Uhr  
 Montags Zugang erlaubt : **Ja**  
 Dienstag Zugang erlaubt : **Ja**  
 Mittwochs Zugang erlaubt : **Ja**  
 Donnerstag Zugang erlaubt : **Ja**  
 Freitags Zugang erlaubt : **Ja**  
 Samstags Zugang erlaubt : **Ja**  
 Sonntags Zugang erlaubt : **Nein**

#### Vorgaben für tägliche Anmeldung - Benutzer muss sich 1x am Tag anmelden

SecureNet Netzbereich Daueranmeldung: **ist vorhanden** Netzbereich[99.98,97 192.168.13]  
 Daueranmeldung für Interne Benutzer: **ist erlaubt**  
 Daueranmeldung für PUBLIC Benutzer: **ist erlaubt**  
 Daueranmeldung **ist** mit Zeitbeschränkung konfiguriert  
 Zugang erlaubt in der Zeit von 0 Uhr bis 240000 Uhr  
 Montags Zugang erlaubt : **Ja**  
 Dienstag Zugang erlaubt : **Ja**  
 Mittwochs Zugang erlaubt : **Ja**  
 Donnerstag Zugang erlaubt : **Ja**  
 Freitags Zugang erlaubt : **Ja**  
 Samstags Zugang erlaubt : **Ja**  
 Sonntags Zugang erlaubt : **Ja**

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. Der 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.

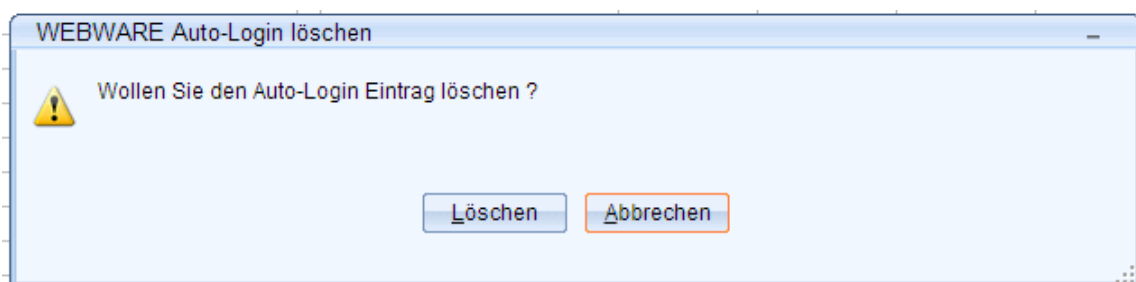
| Suchen (Strg+F)    |   |                           |            |            |             |             |                |                 |
|--------------------|---|---------------------------|------------|------------|-------------|-------------|----------------|-----------------|
| Gehört zu Benutzer | G | Browserinfo               | Erzeugt am | Erzeugt um | Verwendet a | Verwendet u | Betriebssystem | IP-Adresse Text |
| Systemverwalter    | D | Chrome 27.0.1453.11Window | 28.06.2013 | 18:53:42   |             |             | Windows        | 192.168.13.130  |
| Systemverwalter    | D | Chrome 27.0.1453.11Window | 28.06.2013 | 19:17:08   |             |             | Windows        | 192.168.13.130  |

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.



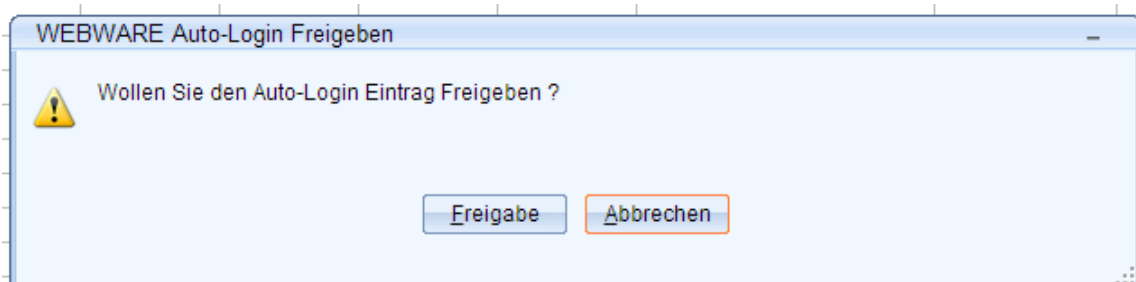
### **Löschen/Entfernen**

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.

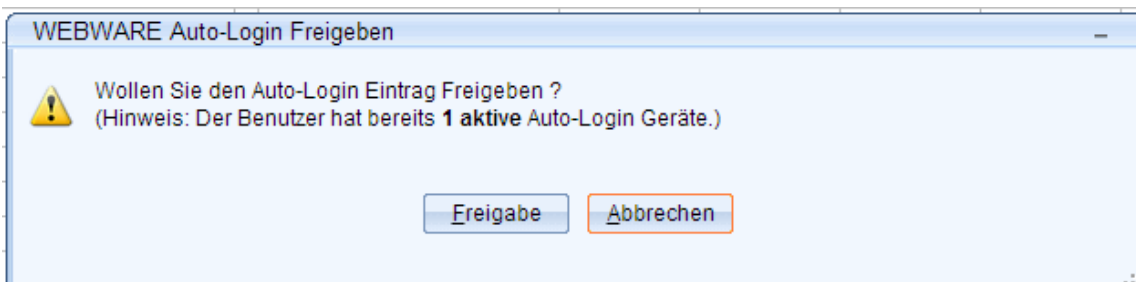


### **Freigeben**

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.

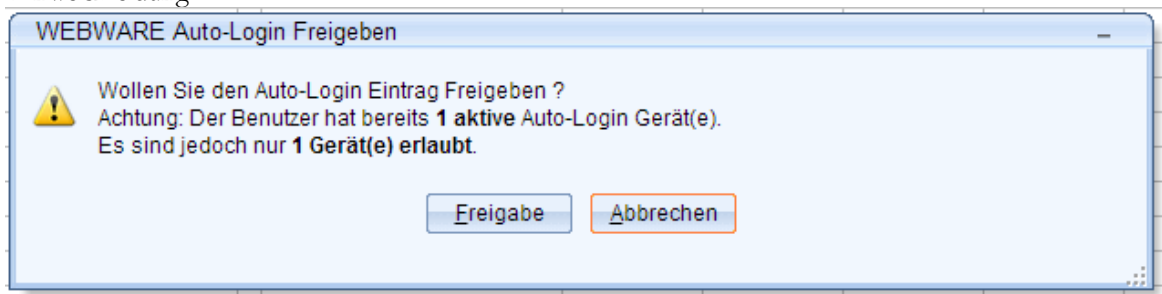


Falls der Systemwert "Maximale Anzahl Geräte pro Benutzer" vorgegeben, so wird geprüft ob für den freizugebenden Benutzer-Eintrag bereits die Maximale Anzahl erreicht ist. Ist die Maximalanzahl noch nicht erreicht, so wird folgender Hinweis angezeigt.




## WEBWARE Anmelde- und Login-System

Wird die Maximale Anzahl von Geräte pro Benutzer überschritten, so erhält der Administrator die folgende Hinweismeldung



## Details

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


**WW e-m-i Tags ändern**

|                            |                                  |
|----------------------------|----------------------------------|
| Tag-ID                     | c29096e5751359471bed227231aad99f |
| Geräte Art                 | <input type="checkbox"/>         |
| Gehört zu Benutzer         | 11 : Systemverwalter             |
| IP-Nummer letzte Anmeldung | 192.168.13.130                   |
| Diese IP-Nummer notwendig  | <input type="checkbox"/>         |
| Start Programm             | <input type="checkbox"/>         |
| Gültig bis Datum           | <input type="text"/>             |
| Gültig bis Uhrzeit         | <input type="text"/>             |
| eTag Bindung aktiv         | <input type="checkbox"/>         |
| mTag: Binde an eTag        | f9e485225f66569cc83bed8ed845d725 |
| Browserinfo                | Chrome 27.0.1453.11Windows       |
| Betriebssystem             | Windows                          |
| Anzahl Anmeldungen         | <input type="text"/>             |
| Anzahl Anmeldefehler       | <input type="text"/>             |
| Erzeugt am                 | 28.06.2013/Fr                    |
| Erzeugt um                 | 18:53:42                         |
| Erzeugt von                | <input type="text"/>             |
| Verwendet am               | <input type="text"/>             |
| Verwendet um               | <input type="text"/>             |
| Verwendet von              | <input type="text"/>             |
| Geändert am                | <input type="text"/>             |
| Geändert um                | <input type="text"/>             |
| Geändert von               | <input type="text"/>             |

## Alle registrierten Geräte


**Alle registrierten Geräte**

☒ Desktop  
☐ Tablet  
☐ Phone

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

| Suchen (Strg+F) | Gehört zu Benutzer | G | Browserinfo               | Erzeugt am | Erzeugt um | Verwendet am | Verwendet um | Betriebssystem | IP-Adresse Text | Anzahl Ann | Anzahl Ann | Tag-ID        |
|-----------------|--------------------|---|---------------------------|------------|------------|--------------|--------------|----------------|-----------------|------------|------------|---------------|
|                 | Systemverwalter    | D | Chrome 27.0.1453.11Window | 26.06.2013 | 0:10:01    | 26.06.2013   | 1:33:30      | Windows        | 192.168.13.130  | 2          | 5          | 9af796b22ab9f |

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 WWAPApplication gestartet.

**Gültigkeits 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.

| Suchen (Strg+F)    |   |                           |            |            |              |             |                |                 |
|--------------------|---|---------------------------|------------|------------|--------------|-------------|----------------|-----------------|
| Gehört zu Benutzer | G | Browserinfo               | Erzeugt am | Erzeugt um | Verwendet ai | Verwendet u | Betriebssystem | IP-Adresse Text |
| Systemverwalter    | D | Chrome 27.0.1453.11Window | 28.06.2013 | 19:17:08   |              |             | Windows        | 192.168.13.130  |



## WEBWARE Anmelde- und Login-System

Sie haben nach Auswahl eines Antrages folgenden Möglichkeiten:

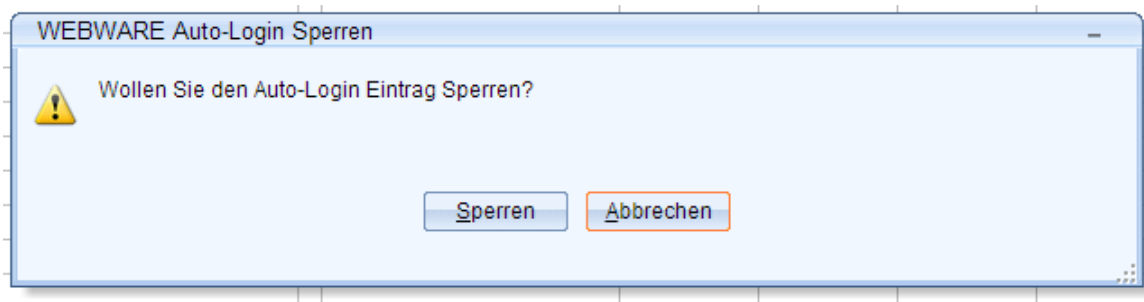


### **Löschen/Entfernen**

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.



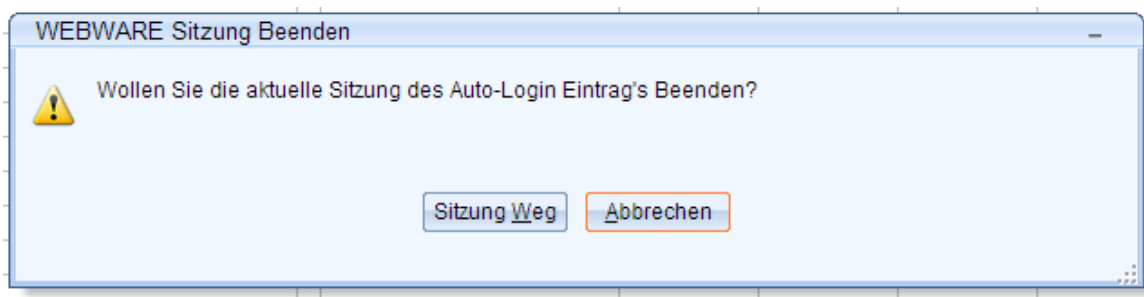
### **Details**

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.

| Suchen (Strg+F) | Gehört zu Benutzer | G | Browserinfo                  | Erzeugt am | Erzeugt um | Verwendet a | Verwendet u | Betriebssystem | IP-Adresse     | Text | Anzahl Ann | Anzahl Ann |
|-----------------|--------------------|---|------------------------------|------------|------------|-------------|-------------|----------------|----------------|------|------------|------------|
|                 | Systemverwalter    |   | D: Chrome 27.0.1453.11Window | 26.06.2013 | 0:10:01    | 26.06.2013  | 1:33:30     | Windows        | 192.168.13.130 |      | 2          | 5          |

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

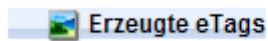
Der Antrag wird in den Ast "Alle registrierten Geräte" verschoben. Der Benutzer erhält in seiner System-Cockpit Anzeige den Hinweis das der Auto-Login Zugang für das Benutzer-Gerät verfügbar ist. Beim nächsten Anmelden werden, je nach Systemrichtlinien, die Anmeldedaten vorbelegt, bzw. die Anmeldung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

| Suchen (Strg+F)    |   |             |            |            |              |
|--------------------|---|-------------|------------|------------|--------------|
| Gehört zu Benutzer | G | Browserinfo | Erzeugt am | Erzeugt um | Verwendet am |
|                    | D |             | 25.06.2013 | 23:46:35   |              |
|                    | D |             | 25.06.2013 | 23:46:35   |              |
|                    | D |             | 26.06.2013 | 0:03:31    |              |
|                    | D |             | 26.06.2013 | 1:22:20    |              |

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



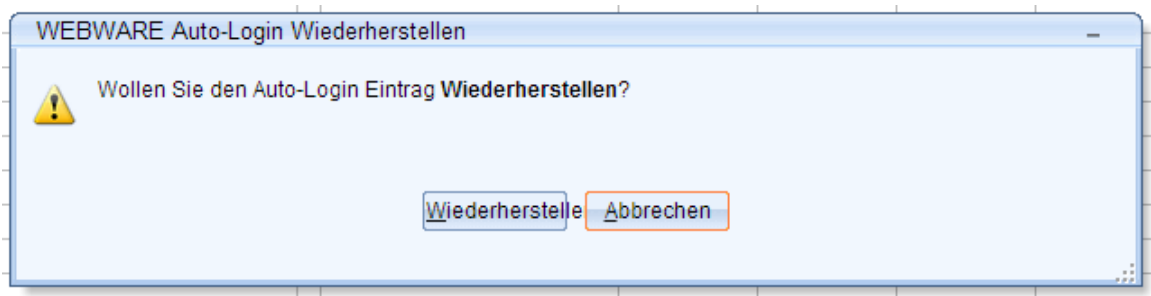
Hier werden die gelöschten Geräte aufgeführt. Diese sind bis zum nächsten Systemstart verfügbar. Danach werden diese unwiederbringlich gelöscht. Sie haben die Möglichkeit Geräte aus der Liste wiederherzustellen.

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"