Handbuch
Trap-Receiver 2x2 Digital I/O PoE

Typ	Trap-Receiver 2x2 Dig.
Modell	#57656 FW 3.24
Release	DE 3.21 02/2011 CF

Irrtum und Änderung vorbehalten:

Da wir Fehler machen können, darf keine unserer Aussagen ungeprüft verwendet werden. Bitte melden Sie uns alle Ihnen bekannt gewordenen Irrtümer oder Missverständlichkeiten, damit wir diese so schnell wie möglich erkennen und beseitigen können.

Führen Sie Arbeiten an bzw. mit W&T Produkten nur aus, wenn sie hier beschrieben sind und Sie die Anleitung vollständig gelesen und verstanden haben. Eigenmächtiges Handeln kann Gefahren verursachen. Wir haften nicht für die Folgen eigenmächtigen Handelns. Fragen Sie im Zweifel lieber noch einmal bei uns bzw. Ihrem Händler nach!

Inhalt

1. Einführung

Der **Trap-Receiver** von W&T ermöglicht die **Überwachung** von Ereignissen auf dem Netzwerk. Empfängt das Gerät einen SNMP-Trap bzw. eine Syslog-Message, findet eine definierte **Aktion** statt. Es können z.B. lokal 2 Verbraucher geschaltet werden.

Die Outputs können als Pulsausgang konfiguriert werden, um mit dem Trap-Receiver einen **externen Software-Watchdog** zu realisieren.

Hinweis: Eine aktive Überwachung der Netzwerkteilnehmer findet nicht statt. Diese Aufgabe übernimmt der IP-Watcher #57655.

Die Verbindung zwischen In-Events und Out-Events findet in 12 möglichen „Aktionen“ statt. Eine Meldung an einen entfernten Empfänger wird zum Beispiel per Mail, FTP, SNMP oder Syslog über ein TCP/IP-Netzwerk abgesetzt.

Sowohl die netzwerktechnischen Ausgänge (Mail, SNMP u.a.) als auch die digitalen Ausgänge können sowohl von Netz-Events als auch von User-Eingaben per **Button** und digitalen Eingängen beeinflusst werden. Mit Hilfe der Konfiguration kann eine individuelle Quittierungsmöglichkeit geschaffen werden. Eine **Quittierung** stellt die ordnungsgemäße Erkennung und Behandlung einer Meldung (ggf. Alarm) durch einen Bediener sicher.

Ein integrierter **Webserver** stellt Konfigurationsseiten zur Einstellung der Geräteparameter zur Verfügung. Das Bedienen und Beobachten der Aktionen erfolgt über eine browserbasierte Software, die ebenfalls vom Webserver des Trap-Receivers in jeden Browser geladen werden kann. Diese Software zeigt in einer selbstaktualisierenden Darstellung den derzeitigen Zustand der aktivierten Aktionen an, und sie bietet die Möglichkeit, per Klick Einfluss zu nehmen.

Die Spannungsversorgung kann entweder via „Power over Ethernet“ über das Netzwerk oder über ein externes Netzteil erfolgen.

Durch seine Eigenschaften eignet sich der Trap-Receiver besonders gut für **autarke Überwachungsaufgaben**. Wird ein Ereignis (SNMP-Trap bzw. eine Syslog-Message) auf dem Netzwerk erkannt, kann lokal ein Ausgang geschaltet werden, zum Beispiel eine Rundumleuchte oder eine Hupe. Eine Alarmierung über ein Netzwerk erreicht schnell auch weit entferntes Personal und fordert es zum Handeln auf.

Die Netzwerkalarmierung erlaubt die Benutzung einer bestehenden Netzwerkinfrastruktur und bietet somit die Möglichkeit, Nachrichten individuell und ohne zusätzliche Verkabelung zu verschicken. Bedienen und Beobachten ist dank der integrierten, browserbasierten Software nicht nur im Intranet, sondern auch weltweit über das Internet möglich.

2. Inbetriebnahme

Um den Trap-Receiver in Ihr Netzwerk einzubinden und in Betrieb zu nehmen, sind nur wenige Schritte notwendig:

Spannungsversorgung, Netzwerkanschluss, Konfiguration der Grundeinstellungen und schließlich Konfiguration der In-Events, Out-Events und Aktionen.

2.1 Spannungsversorgung

Im Folgenden sind die zwei Möglichkeiten beschrieben, den Trap-Receiver mit Spannung zu versorgen.

Die hier beschriebenen Arten der Spannungsversorgung liefern ausschließlich die Betriebsspannung für das Gerät. Die Beschaltung der In- und Outputs erfordert eine zusätzliche Versorgung.

Wird das Gerät via PoE mit der benötigten Betriebsspannung versorgt, kann das Anschließen oder Entfernen einer zusätzlichen externen Spannungsquelle im laufenden Betrieb zu einem Neustart des Trap-Receivers führen.

2.1.1 externe Spannungsversorgung

Schließen Sie eine Spannungsversorgung von 18V...48V DC (+/-10%) oder 18Veff...30Veff AC (+/-10%) an der Klemme auf der Unterseite des Gerätes an. Sie können hierzu die von W&T angebotenen Netzteile oder alternativ jede beliebige Spannungsversorgung verwenden, welche die technischen Voraussetzungen erfüllt.

Die externe Spannungsversorgung des Gerätes ist in Netzwerken ohne PoE-Unterstützung immer erforderlich, kann aber auch in PoE-Umgebungen angewendet werden.

Bei Versorgung mit Gleichspannung muss nicht auf die korrekte Polung geachtet werden.

Die Versorgung des Gerätes mit 12V DC ist ebenfalls möglich. Hierbei ist jedoch der schlechte Wirkungsgrad des Netzteils und die damit verbundene erhöhte Stromaufnahme zu beachten.

2.1.2 Spannungsversorgung über PoE

Der Trap-Receiver ist für den Einsatz in „Power over Ethernet"-Umgebungen gemäß IEEE802.3af ausgerüstet. Die Spannungsversorgung erfolgt hierbei durch die Netzwerkinfrastruktur über den RJ45-Anschluss. Das Gerät unterstützt sowohl die Phantom-Speisung über die Datenpaare 1/2 und 3/6, wie auch die Spare-Pair-Speisung über die ungenutzten Adernpaare 4/5 und 7/8.

Um der versorgenden Komponente ein Powermanagement zu ermöglichen, identifiziert sich der Trap-Receiver als Gerät der Leistungsklasse 2 mit einer Leistungsaufnahme von 3,84W bis 6,49W.

Mit einem externen Netzteil kann der Trap-Receiver auch in Netzwerken ohne PoE-Unterstützung eingesetzt werden.

2.2 Beschaltung der Inputs

Der erlaubte Eingangsspannungsbereich liegt bei +/-30V gegen die Bezugsmasse.

Die Schaltschwelle der Inputs liegt bei 8V +/-1V. Niedrigere Spannungen werden als OFF bzw. 0-Signal erkannt. Spannungen über 8V wertet der Trap-Receiver als ON bzw. 1-Signal. Eingangsspannungen zwischen 7V und 9V sollten vermieden werden, da eine eindeutige Zuordnung nicht garantiert werden kann.

Das folgende Anschlussbeispiel zeigt die Ansteuerung von zwei Inputs. Dabei ist es wichtig, dass die beiden Signale den gleichen Massebezug haben.

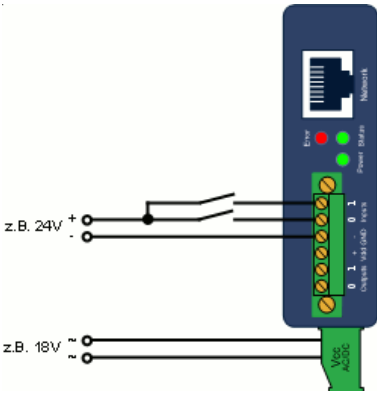


Abb.: Ansteuerung der zwei digitalen Inputs

Sollen über die Inputs die Zustände potentialfreier Kontakte überwacht werden, kann auch die Versorgungsspannung des Gerätes als Signalspannung genutzt werden. In diesem Fall ist es erforderlich, den Trap-Receiver mit einer Gleichspannung von 12V-30V zu betreiben.

Eine Rückführung von einem Output des Gerätes kann sehr einfach durch eine Brücke erfolgen. Der entspr. Output muss dann für interne Versorgung konfiguriert werden.

2.3 Beschaltung der Outputs

Die zwei Outputs des Trap-Receivers sind stromtreibend.

Eine zusätzliche Versorgungsspannung für die Outputs kann zwischen 6V und 30V Gleichspannung liegen und wird über die Anschlüsse Vdd und GND im Klemmenbereich der Outputs eingespeist. Der maximale Schaltstrom pro Ausgang liegt bei 500mA.

Mit induktiver Last (z. B. einem Relais) beschaltete Outputs sollten mit einer Freilaufdiode vor Beschädigung geschützt werden.

Die Outputs verfügen zusätzlich über eine thermische Überlastsicherung und sind kurzschlussfest.

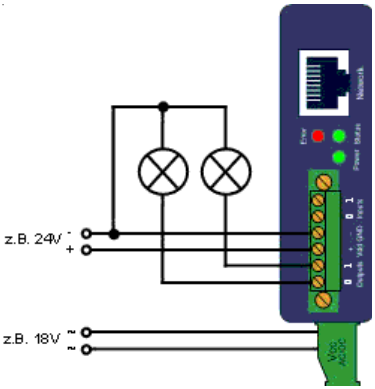


Abb.: Outputbeschaltung mit separater Versorgung

Bei der Dimensionierung der Ausgangsspannungsversorgung sollte der benötigte Strom berücksichtigt werden. Wird das Gerät über ein externenes Netzteil mit 12V-30V DC versorgt, dessen Leistung zusätzlich für die Versorgung der an den Outputs angeschlossenen Verbraucher ausreicht, kann die Outputversorgung ebenfalls an die Geräteversorgung angeschlossen werden.

Der Bereich der Geräteversorgungsspannung überschreitet den Bereich der schaltbaren Output-

spannung. Sollten Sie die Geräteversorgung auch für die Versorgung der Outputs nutzen, darf die Spannung höchstens 30V betragen.

In der Konfiguration ist auch einstellbar, dass die Versorgungsspannung des Trap-Receivers intern auf die Klemmen Vdd und GND geschaltet wird. In dem Fall ist eine externe Hilfsspannung nicht erforderlich. In Summe können die Outputs bei aktivierter interner Hilfsspannung mit maximal 150mA belastet werden.

2.4 Netzwerkanschluss

Der Trap-Receiver verfügt über einen IEEE 802.3 kompatiblen Netzwerkanschluss auf einem geschirmten RJ45-Steckverbinder. Die Belegung entspricht einer MDI-Schnittstelle (siehe Abbildung), sodass der Anschluss an einen Hub oder Switch mit einem 1:1 verdrahteten und geschirmten Patchkabel erfolgt.

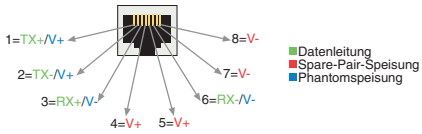


Abb.: Belegung der RJ45-POE-Netzwerkbuchse

Ab Werk arbeitet der Trap-Receiver netzwerkseitig in der Betriebsart „Auto-Negotiation“. Datenübertragungsgeschwindigkeit und Duplexverfahren werden hierbei mit dem angeschlossenen Switch / Hub automatisch verhandelt und entsprechend eingestellt.

Der Netzwerkanschluss ist sowohl gegenüber der Versorgungsspannung als auch gegenüber den digitalen IOs mit 1kV galvanisch getrennt.

Dank der integrierten „Power over Ethernet“-Technologie kann das Gerät über den Netzwerkanschluss mit der nötigen Betriebsspannung versorgt werden.

2.4.1 Vergabe der IP-Adresse mit dem WuTility

Nachdem die Hardware wie oben beschrieben entweder über PoE oder ein externes Netzteil mit der nötigen Spannung versorgt wurde, muss die für den Betrieb in einem TCP/IP-Netzwerk erforderliche IP-Adresse vergeben werden. Die notwendigen Werte (IP-Adresse, Netzmaske etc.) erfragen Sie bitte bei Ihrem zuständigen Systemadministrator.

Die vergebene IP-Adresse muss netzwerkweit eindeutig sein.

Für die Vergabe der IP-Adresse stehen mehrere Alternativen zur Verfügung. Um das Verfahren so komfortabel wie möglich zu gestalten, haben wir das Programm *WuTility* entwickelt, welches Sie von unserer Homepage *http://www.wut.de* kostenlos herunterladen können. Dieses Verfahren wird im Folgenden beschrieben. Eine Zusammenstellung möglicher Alternativen finden Sie im Anhang dieser Anleitung.

Stellen Sie sicher, dass Sie sich mit dem PC, mit dem Sie die IP-Adresse vergeben möchten, im gleichen Subnetz wie der zu konfigurierende Trap-Receiver befinden. Beide Geräte müssen an das Netzwerk angeschlossen sein.

Beim Start durchsucht das *WuTility* automatisch das lokale Netzwerk nach angeschlossenen W&T-Netzwerkgeräten und zeigt diese in einer Inventarliste an. Der Scanvorgang lässt sich beliebig oft durch Betätigen der Schaltfläche *Scannen* wiederholen.

Wählen Sie aus der angezeigten Liste nun den Trap-Receiver aus. Haben Sie mehrere unkonfigurierte W&T-Netzwerkgeräte in Ihrem Netz, können Sie eine eindeutige Zuordnung von Listeneintrag und Endgerät über die MAC-Adresse treffen:

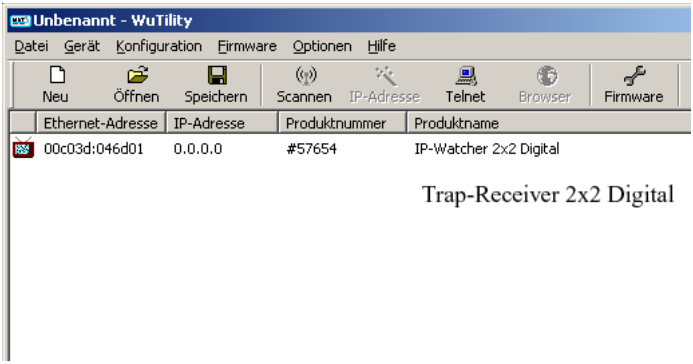


Abb.: WuTility mit gefundenem W&T Netzwerkgerät

Markieren Sie das gewünschte Gerät. Über die Schaltfläche *IP-Adresse* erreichen Sie den Konfigurationsdialog. Geben Sie dort die gewünschten Netzwerkparameter für das Gerät ein. Bestätigen Sie nach der Eingabe den Dialog durch Betätigen der Schaltfläche *Weiter*:

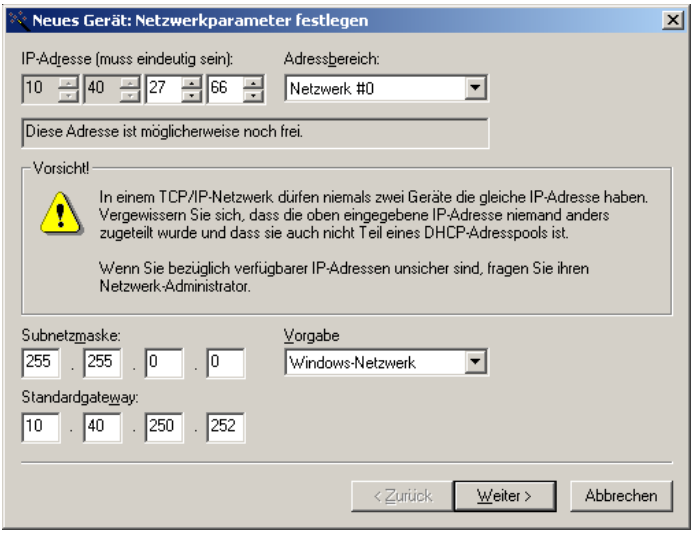


Abb.: Konfigurationsdialog für Netzwerkparameter

Im folgenden Fenster kann zur automatischen IP-Adressvergabe der BOOTP- oder der DHCP-Client des Gerätes aktiviert werden:

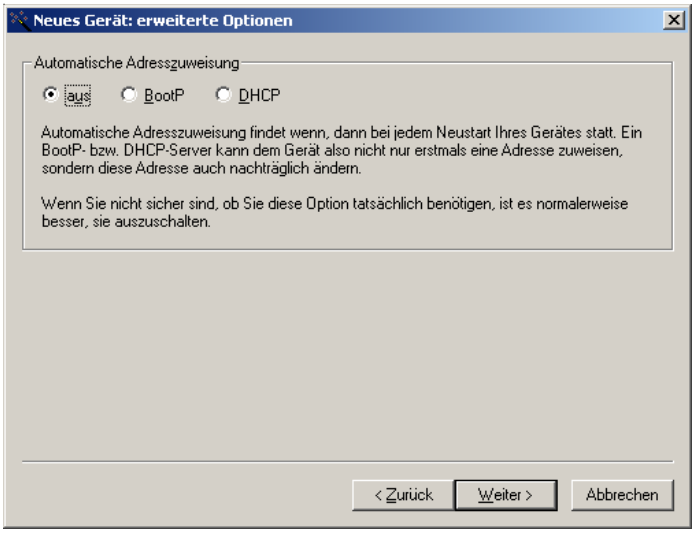


Abb.: Konfigurationsdialog für Adressvergabeverfahren

Mit Betätigung der Schaltfläche *Weiter* werden dem Trap-Receiver die eingegebenen Netzwerkparameter zugewiesen. Alle Spalten der Inventarliste im *WuTility* werden mit Informationen gefüllt. Ein Klick auf die Schaltfläche *Browser* öffnet Ihren Standardbrowser und Sie sehen die Startseite des Gerätes.

2.4.2 Automatische IP-Adressvergabe

Viele Netzwerke nutzen für die zentralisierte und dynamische Vergabe der Netzwerkparameter DHCP (Dynamic Host Configuration Protocol) oder auch das im folgenden Kapitel beschriebene Vorgängerprotokoll BOOTP. Mit den Werkseinstellungen ist DHCP in Ihrem Trap-Receiver aktiviert, so dass es in Netzwerkumgebungen mit dynamischer IP-Adressvergabe ausreicht, das Gerät an das Netzwerk anzuschliessen. Die folgenden Parameter können mit Hilfe von DHCP zugewiesen werden:

- IP-Adresse
- Subnetzmaske
- Gateway
- DNS-Server
- Lease-Time

Zur Vermeidung ungewollter Adressvergaben oder Adressänderungen, empfehlen wir, die Protokolle DHCP und BOOTP/RARP zu deaktivieren, sofern diese nicht ausdrücklich in der jeweiligen Netzwerkumgebung genutzt werden. Netzwerkgeräte von W&T mit fälschlich zugewiesenen IP-Adressen können nachträglich mit Hilfe des WuTilitys neu konfiguriert werden.

2.4.2.1 Aktivierung/Deaktivierung von Vergabeverfahren

Mit der Werkseinstellung ist DHCP aktiviert. Zur Deaktivierung, der Festlegung eines anderen Vergabeverfahrens oder auch zum späteren Wiedereinschalten stehen die folgenden Möglichkeiten zur Verfügung:

- **WuTility:** Markieren Sie in der Inventarliste den gewünschten Trap-Receiver und betätigen Sie die Schaltfläche *IP-Adresse*. Im ersten Dialogfenster tragen Sie die zu vergebenen Netzwerkparameter ein und bestätigen mit *Weiter*. Aktivieren Sie im folgenden Dialog das gewünschte Protokoll zur automatischen IP-Adressvergabe oder schalten Sie dort diese Option aus. Mit *Weiter* werden abschließend die konfigurierten Parameter im Gerät übernommen.
- **Web-Based Management:** Über das Web-Based Management können die Protokolle alternierend aktiviert bzw. beide deaktiviert werden. Detailinformationen hierzu finden Sie im Kapitel *Netzwerk-Grundeinstellungen*.

2.4.2.2 Systemname

Zur Unterstützung einer eventuell automatisierten Aktualisierung des DNS-Systems durch den DHCP-Server identifiziert sich der Trap-Receiver innerhalb von DHCP mit seinem Systemnamen. Werksseitig lautet dieser *Trap-Receiver 2x2 Digital-* gefolgt von den letzten drei Stellen der Ethernet-Adresse. Zum Beispiel lautet der werksseitig eingestellte Systemname eines Trap-Receivers mit der Ethernet-Adresse 00:c0:3d:01:02:03 *Trap-Receiver 2x2 Digital-010203*. Der Systemname des Gerätes kann über das Web-Based Management geändert werden.

2.4.2.3 Lease-Time

Die vom DHCP-Server bestimmte und übermittelte Lease-Time legt die Gültigkeitsdauer der zugewiesenen IP-Adresse fest. Nach Ablauf der halben Lease-Time versucht der Trap-Receiver bei dem zuweisenden DHCP-Server die Gültigkeit zu verlängern bzw. die Adresse zu aktualisieren. Ist dieses bis zum Ablauf der Lease-Time nicht möglich, zum Beispiel weil der DHCP-Server nicht mehr erreichbar ist, löscht der Trap-Receiver seine IP-Adresse und startet eine zyklische Suche nach alternativen DHCP-Servern zwecks Zuweisung einer neuen IP-Adresse.

Ist DHCP aktiviert, wird die verbleibende Lease-Time zusammen mit der aktuellen IP-Adresse im Menüzweig

```
Home >> Doc >> Property
```

in Sekunden angezeigt.

Sollte nach Ablauf der zugewiesenen Lease-Time der DHCP-Server nicht erreichbar sein, löscht der Trap-Receiver seine IP-Adresse. Alle bestehenden TCP- und UDP-Verbindungen zwischen dem Gerät und anderen Netzwerkteilnehmern werden hierdurch unterbrochen. Um Störungen dieser Art zu vermeiden, empfehlen wir, die zu vergebene Lease-Time im DHCP-Server möglichst auf unendlich zu konfigurieren.

2.4.2.4 Reservierte IP-Adressen

Der Trap-Receiver stellt Dienste zur Verfügung, die andere Teilnehmer (Clients) im Netzwerk nach Bedarf in Anspruch nehmen können. Für die Verbindungsaufnahme wird von diesen natürlich die aktuelle IP-Adresse des Gerätes benötigt, so dass es in diesen Anwendungsfällen sinnvoll ist, auf dem DHCP-Server eine bestimmte IP-Adresse für den Trap-Receiver zu reservieren. In der Regel erfolgt dieses durch die Bindung der IP-Adresse an die weltweit einmalige Ethernet-Adresse des Gerätes, welche dem Aufkleber am Gehäuse entnommen werden kann.

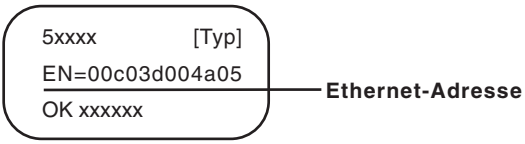


Abb.: Ethernet-Adresse auf dem Sticker auf der Geräteseite

2.4.2.5 Dynamische IP-Adressen

Eine völlig dynamische IP-Adressvergabe, bei welcher der Trap-Receiver mit jedem Neustart oder auch nach Ablauf der Lease-Time eine andere IP-Adresse bekommt, ist nur in Netzwerkumgebungen mit automatischer Querverbindung zwischen den Diensten DHCP und DNS sinnvoll. Das heißt: bei der Neuzuteilung einer IP-Adresse an das Gerät aktualisiert der DHCP-Server anschließend automatisch auch das DNS-System. Dem jeweiligen Domain-Namen wird hierbei die neue IP-Adresse zugeordnet. Für Detailinformationen zu Ihrer Netzwerkumgebung wenden Sie sich im Zweifel an Ihren Systemadministrator.

Für Timeserver-Anfragen, das Versenden von Emails oder andere Client-Anwendungen, bei denen das Gerät aktiv die Verbindung zu im Netzwerk befindlichen Server-Diensten sucht, können auch dynamische, sich ändernde IP-Adressen genutzt werden.

3 Bedienen und Beobachten aus dem Browser / SNMP

Ist der Trap-Receiver mit den nötigen Basis-Netzwerkparametern konfiguriert und an das Netzwerk angeschlossen, kann die weitere Konfiguration und das Bedienen / Beobachten des Gerätes aus dem Browser bzw. per SNMP erfolgen.

3.1 Vergabe der Basis-Netzwerkparameter

Rufen Sie durch Eingabe der IP-Adresse in der Adresszeile Ihres Browsers die Startseite des Trap-Receivers auf und blenden Sie über den Link *Menü einblenden* das Konfigurationsmenü des Gerätes ein. Alternativ können sie auch die Adresse

```
http://<IP-Adresse des Trap-Receivers>/index.htm
```

aufrufen. Hierbei ist das Konfigurationsmenü bereits sichtbar und muss nicht manuell eingeblendet werden.

Wählen Sie den Menüpunkt *Config/Login*.

Sie werden nun aufgefordert, ein Passwort einzugeben. Im Auslieferungszustand ist kein Passwort vergeben, sodass Sie ohne Eingabe auf den Button *Login* klicken können. Sie sind jetzt mit Administratorrechten eingeloggt.

Wählen Sie auf der nächsten Seite den Konfigurationsweg mit Hilfe der Profile aus.

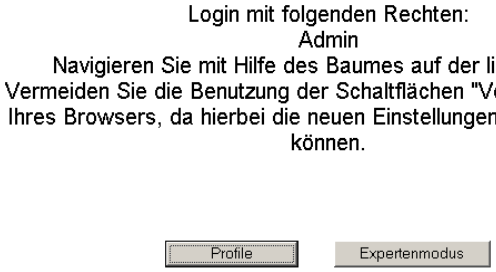


Abb.: Auswahl für Profile oder Expertenmodus

Selektieren Sie das Profil *Basisparameter Netzwerk* und klicken Sie auf den Button *Profil anzeigen*.

Abb.: Profilauswahl

Das Gerät zeigt jetzt blau hinterlegt die nötigen Menüpunkte an, die für die Konfiguration des gewählten Profiles angepasst werden müssen. Über die rot hinterlegten Menüpunkte *Logout* und *Profiles* können Änderungen gespeichert oder verworfen werden oder ein neues Profil zur weiteren Konfiguration des Trap-Receivers dargestellt werden.

Bearbeiten Sie zunächst den Punkt *Network* und loggen Sie sich anschließend über *Logout* aus. Tragen Sie auf der folgenden Seite alle erforderlichen Netzwerkparameter ein und übernehmen Sie diese mit einem Klick auf den Button *Zwischenspeichern*.

Abb.: Netzwerkkonfiguration

Der Button *Logout* leitet das Ende des Konfigurationsvorgangs und das Speichern der vorgenommenen Änderungen im Gerät ein.

Mit einem abschließenden Klick auf den Button *Speichern* sichern Sie Ihre Einstellungen im Gerät und beenden die Konfigurationssitzung. Wurden während der Sitzung Netzwerkparameter geändert, führt das Gerät automatisch einen Neustart durch, um die geänderten Werte zu übernehmen.

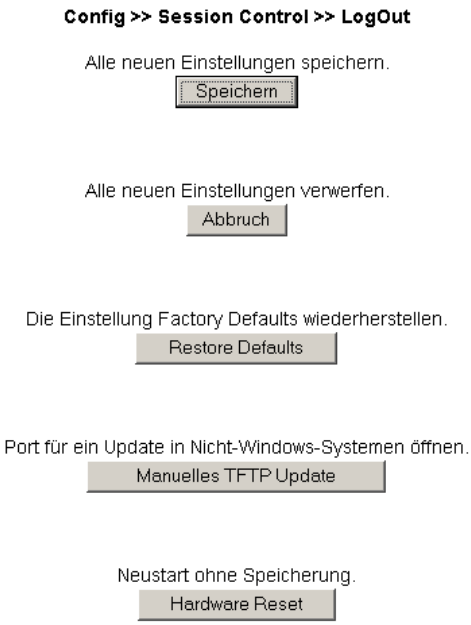


Abb.: Logoutoptionen

Das Gerät ist jetzt für den Betrieb in Ihrem Netzwerk bereit. Nutzen Sie für weitere Konfigurationen ebenfalls die Profile und lassen Sie sich so durch den Konfigurationsprozess führen.

3.2 Sprachauswahl

Beim ersten Aufruf einer der Steuerungsseiten (*home.htm*) vom geräteeigenen Webserver werden Sie aufgefordert, die Gerätesprache auszuwählen.

Geben Sie in der Adressleiste Ihres Browsers die IP-Adresse des Gerätes oder die IP-Adresse gefolgt vom Namen einer der Steuerungsseiten ein und senden Sie die Anfrage ab. Wählen Sie auf der geladenen Seite die gewünschte Systemsprache und bestätigen Sie die Auswahl durch Betätigen des Buttons *OK*. Dieser Konfigurationsschritt ist hiermit abgeschlossen und Sie werden zur Startseite des Gerätes weitergeleitet.

3.3 Adressen spezieller Seiten / Funktionen

Es gibt Seiten, die Sie direkt aus dem Browser adressieren können. Im Folgenden sind die URLs kurz erläutert und aufgelistet.
http://<IP-Adresse des Trap-Receivers>/home.htm

Die Hauptseite (Home-Seite) stellt selbstaktualisierend den Geräte-Zustand dar:

- die konfigurierten Aktionen sind aufgelistet. Der letzte Auftretens-Zeitpunkt wird festgehalten. Wurde die Aktion noch nicht durchgeführt, ist der Einschalt-Zeitpunkt des Gerätes angezeigt. Die Bereitschaft zu neuen Aktionen ist am Farbton der Schrift erkennbar: schwarz (bzw. grau) zeigt an, dass laut Zeitfenster die Aktion ausführbar (grau: nicht ausführbar) ist.

- der Klemmenstatus der digitalen Ein- und Ausgänge wird angezeigt.
- Im Bedienbereich werden die konfigurierten Buttons angezeigt. Dies geschieht abhängig von den eingestellten Rechten, die Buttons zu betätigen. Diese Rechte können eingestellt werden unter *Config >> Device >> Prepare In-Events >> Buttons >> Button x*.

Folgender Link ruft die Home-Seite, wie oben beschrieben, mit eingeblendetem Konfigurationsmenü auf:
http://<IP-Adresse des Trap-Receivers>/index.htm

Die User-Seite kann vom Kunden erstellt werden.
http://<IP-Adresse des Trap-Receivers>/user.htm

Diagnosemeldungen können unter folgender Adresse abgerufen werden:
http://<IP-Adresse des Trap-Receivers>/diag.htm

Die MIB-Datei erhalten Sie auch durch folgende Eingabe im Browser: http://<IP-Adresse>/mib.zip.

Ein Hardware-Reset (Power on Reset) wird gestartet mit
http://<IP-Adresse des Trap-Receivers>:8888

3.3.1 Home-Seite

Die Home-Seite wird aufgerufen mit der Adresse

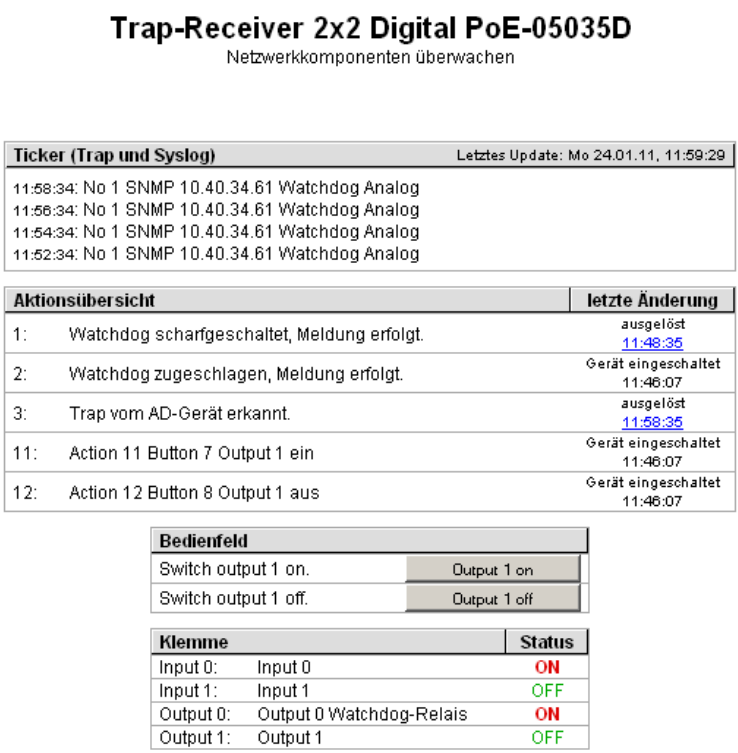
```
http://<IP-Adresse des Trap-Receivers>/home.htm
```

Sie

- bietet eine Übersicht über die eingegangenen Netzwerk-Events und den Status der Klemmen (Input und Output) und aller konfigurierten Aktionen.
- ermöglicht, konfigurierte Buttons zu betätigen und damit die definierten Aktionen / Quittierungen auszulösen.

Am oberen Bildrand sind Links zu finden, über die das Konfigurationsmenü eingeblendet werden kann. Des Weiteren kann dort über Kontrollelemente ein Login durchgeführt werden.

Die dargestellten Informationen werden einmal pro Sekunde aktualisiert. Dies geschieht automatisch, ohne Eingriff des Benutzers. Der Zeitpunkt der letzten Seiten-Aktualisierung ist in der Zeile „Ticker (Traps und Syslog)“ dargestellt. Bei der dort abgebildeten Zeit handelt es sich um die Systemzeit des Trap-Receivers. Wird die Zeitangabe mit einem hochgestellten Sternchen abgeschlossen, ist die Systemuhr des Gerätes mit dem in der Konfiguration eingestellten Timeserver synchronisiert.



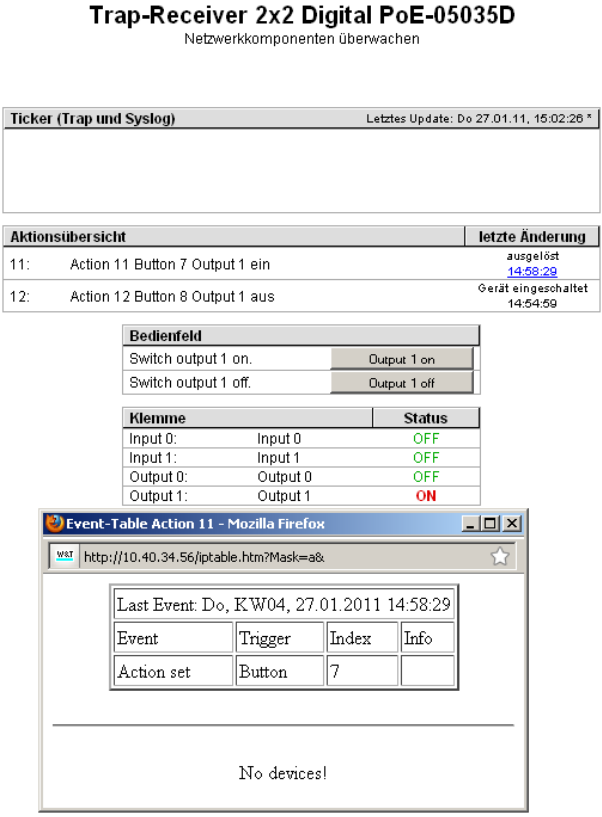
Unter der Geräte-Bezeichnung befindet sich eine Tickerbox, in der die letzten aufgetretenen SNMP Traps bzw. Syslog Mes-

sages eingetragen werden. Außerdem ist die letzte Aktualisierungszeit der Seite in der Box-Überschrift enthalten.

Darunter befindet sich die Aktionsübersicht. Hier sind die aktiven Aktionen gelistet mit Nummer, Name und der letzten Änderung. Sollte eine Aktion seit Einschalten des Gerätes noch nicht durchgeführt worden sein, ist der Aktion der Geräte-Einschaltzeitpunkt zugeordnet.

Darunter befindet sich das Bedienfeld, in dem die konfigurierten Buttons gelistet sind (ggf. Zugangs-Berechtigungen beachten!). Links steht der Button-Text als Beschreibung, rechts der Name des Buttons, der hier betätigt werden kann.

Am unteren Rand sind dann die Klemmen dargestellt mit Klemmen-Ort, vom Kunden ggf. vergebenen Klemmen-Namen und physikalischem Klemmen-Status.



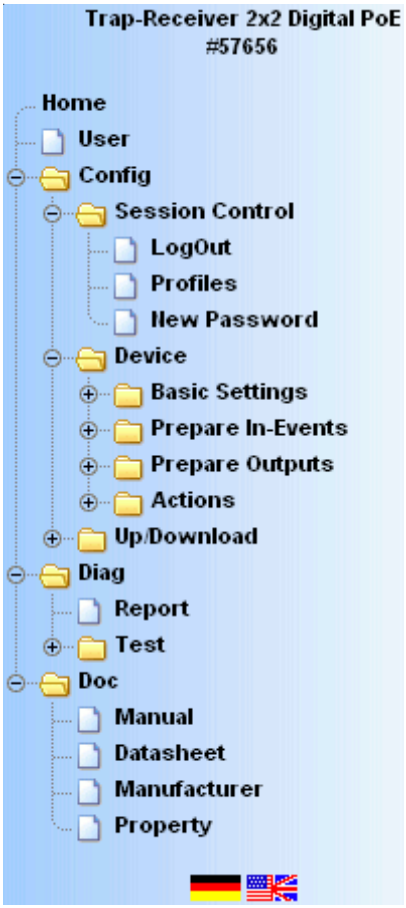
Bei Betätigung eines Links unter der Spalte „letzte Änderung“ öffnet sich ein weiteres Fenster mit einer Event-Table, in der Sie weitere Informationen zum aufgetretenen Event finden.

Die Events werden zur Runtime gehalten, aber nach Stromausfall bzw. Hardware-Reset sind alle Events gelöscht und können auch in der History List nicht mehr gefunden werden. In diesem Fall zeigt das Gerät „Gerät eingeschaltet“ und den Poweron-Zeitpunkt an.

3.3.2 User-Seite

Die User-Seite kann vom Kunden gestaltet werden. Visualisiert werden kann:

- Status der Eingänge
- Status der Ausgänge
- Gerätezeit



Das Konfigurationsmenü erlaubt Zugriff auf die Konfigurationsseiten, Diagnose und Dokumentation.

Der Link zum Ausblenden des Konfigurationsmenüs ist nur dann unter dem Menübaum sichtbar, wenn im rechten Teil des Browsers die Hauptseite (*home.htm*) dargestellt wird.

Andernfalls wird eine Konfigurationsseite angezeigt, die auf einen laufenden Konfigurationsvorgang schliessen läßt. Für diesen ist der Zugriff auf den kompletten Menübaum erforderlich, weshalb an dieser Stelle das Ausblenden des Menüs nicht unterstützt wird.

3.5 Login und Logout

Je nach Login unterscheidet der Trap-Receiver zwischen drei verschiedenen Zugriffsberechtigungen:

- *Default User*: Diesen Status hat zunächst jeder Bediener, der ohne Passwort auf das Gerät zugreift. Der Status des Trap-Receivers kann jetzt ausgelesen und dargestellt werden. Die Konfiguration zu verändern ist jedoch nicht möglich.
- *Administrator*: Das Administratorkennwort gewährt vollständigen Zugriff auf das Gerät. Die Manipulation der Konfiguration ist jetzt möglich.
- *Operator*: Die Zugriffsrechte des Operators sind abhängig von der Konfiguration auf das Betätigen der Buttons und das Ändern der Gerätezeit und Gerätesprache beschränkt.

Unabhängig von der Zugriffsberechtigung hat jeder Bediener die Möglichkeit, aufgelaufene Fehler über die Diag-Seite auszulesen und Geräteinfomationen in der Rubrik *Doc* einzusehen.

Je mehr Zugriffsrechte ein Benutzer hat, desto umfangreicher ist der Menübaum. Aufgrund des Logins werden nicht verfügbare Punkte ausgeblendet.

Ein Login kann entweder über den Dialog in der rechten oberen Ecke auf der Seite *home.htm* oder über den Unterpunkt *Config/ Login* über den Menübaum erfolgen. Der Dialog auf der Hauptseite ist nur dann sichtbar, wenn der Menübaum ausgeblendet ist.

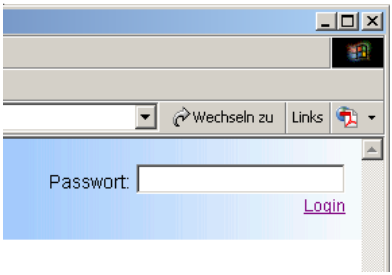


Abb.: Logindialog auf den Hauptseiten

Beim Login ist unerheblich, wo dieser durchgeführt wird. Wurde die Konfiguration des Gerätes jedoch geändert, muss der Logout über die „Config"-Seite im Menübaum erfolgen. Wird der Logout über eine der Hauptseiten durchgeführt, gehen die vorgenommenen Änderungen verloren.

Ein Login mit Administratorrechten überschreibt einen bereits bestehenden Login. In diesem Fall wird der Benutzer während des Login-Vorgangs aufgefordert, den bereits bestehenden Login zu übernehmen. Die bislang bestehende Session wird abgebrochen.

Abb.: Aufforderung auf der Home-Seite, einen bestehenden Login zu übernehmen

Die Abweisung eines Logins erfolgt bei falscher Passworteingabe oder wenn versucht wird, einen bestehenden Login mit unzureichenden Zugriffsrechten zu überschreiben.

Abb.: Meldung für abgewiesenen Login auf einer Hauptseite

Das eingegebene Passwort wird mit dem MD5-Algorithmus (abgeleitet vom RSA Data Security, Inc. MD5 Message Digest Algorithm) zu einer Hashsumme verarbeitet und verschlüsselt übertragen.

Nach einer Zeitüberschreitung von ca. 30min findet automatisch ein Logout statt. Ein entsprechender Hinweis wird dem Nutzer gegeben. Ein erneuter Login ist durchführbar.

3.6 Up- und Download

Wenn Sie alle Geräte-Einstellungen vorgenommen haben, ist es sinnvoll, die Konfiguration abzuspeichern.

Unter der Rubrik *Up/Download*, die ebenfalls über das Konfigurationsmenü zu erreichen ist, kann die Gerätekonfiguration aus- und eingelesen werden:

```
Config >> Up/Download >> Download
```

und

```
Config >> Up/Download >> Upload
```

Beim Download der Gerätekonfiguration, die im XML-Format gespeichert ist, können Sie die Einstellungen des Trap-Receivers auslesen. In der Datei können Sie Modifikationen vornehmen. Die geänderten Einstellungen können dann über die Upload Funktion wieder in das Gerät eingespielt werden.

Für den XML-Upload muss nicht die vollständige XML-Datei hochgeladen werden. Auch Teilbereiche (für einzelne Parameter) der Konfiguration werden vom Gerät akzeptiert, wenn die XML-Syntax korrekt ist.

Die Konfiguration des Trap-Receivers muss mit dem Ausdruck

```
<io-Digital2x2TR2.1>
```

beginnen und mit dem Ausdruck

```
</io-Digital2x2TR2.1>
```

enden. Die Folge der einzustellenden Parameter entspricht der Reihenfolge der Punkte im Konfigurationsbaum ab dem Punkt *Device*.

Die Syntax zur Konfiguration per XML ist Folgende:

```
<Option>
    <Parameter1>Wert</Paramter1>
    <Parameter2>Wert</Paramter2>
</Option>
```

Die einzelnen Optionen und Parameter entsprechen den Konfigurationspunkten im Menübaum.

Beachten Sie, insbesondere bei Massenupdates und -konfigurationen, dass stets die in der XML-Datei gespeicherte IP-Adresse im Gerät programmiert wird. Diese muss erst angepasst werden.

Des Weiteren kann die SNMP-MIB in komprimierter Form herunter geladen werden, die für das Einbinden des Gerätes in SNMP-Managementsysteme erforderlich ist. Je nach gewählter Systemsprache laden Sie die deutsche oder die englische Version.

Zusätzlich können Sie ein individuelles Logo in das Gerät laden. Bitte achten Sie darauf, nur entsprechend geringe Auflösungen zu nutzen.

3.7 Besonderheiten bei SNMP / MIB-Browser

Das Gerät kann auch über SNMP konfiguriert bzw. betrieben. Damit können Sie automatisiert auf das Gerät zugreifen oder per MIB-Browser. Die beschreibende MIB-Datei erhalten Sie von unserem Webserver oder auch durch folgende Eingabe im Browser: http://<IP-Adresse>/mib.zip. Dort erfahren Sie die OIDs und die Inhalte, die genutzt werden können.

Wenn kein Passwort vergeben ist, muss im MIB-Brower mit z.B. wtTrapReceiver2x2SessCntrlPassword SET ein beliebiges Passwort, z.B. ‘public’, übergeben werden.

Ob eine Session eröffnet wurde, lässt sich mit wtTrapReceiver2x2SessCntrlConfigMode GET kontrolliert werden. 1 steht dann für eine Session, 0 für NoSession.

Die Werte werden übernommen, wenn die Session mit wtTrapReceiver2x2SessCntrlLogout SET 1 beendet wird. SET 2 beendet die Session ohne Speichern der Änderung.

Mit wtTrapReceiver2x2SessCntrlLogout SET 3 wird das Gerät auf Factory Default zurück gesetzt.

Hinweis: Die MIB des Gerätes kann direkt mit http://IP-Adresse/mib.zip vom Gerät abgeholt werden. Zusätzlich befinden sich die MIBs zum Gerät bei WuT auf dem Web-Server (s. www.wut.de//e-5wwww-15-inde-000.php).

4 Grundeinstellungen - Basic Settings

4.1 Spracheinstellung - Language

Sie können über das Konfigurationsmenü die Systemsprache des Gerätes bestimmen. Dies kann entweder über den Fahnen-Link unter dem Konfigurationsmenü erfolgen, oder navigieren Sie zu:

```
Config >> Device >> Basic Settings >> Language
```

Abb.: Fahnen-Link unter dem Konfigurationsmenü

Auf der aufgerufenen Seite wählen Sie die gewünschte Sprache aus und übernehmen Sie die Änderung mit *Zwischenspeichern*.

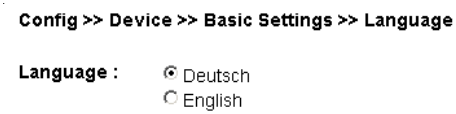


Abb.: Sprachauswahl

Für das Ändern der Sprache benötigen Sie Operator- oder Administratorrechte.

4.2 Gerätebezeichnung - Texte

Rufen Sie im Konfigurationsmenü die Seite

```
Config >> Device >> Basic Settings >> Text
```

auf, um folgende Texte zu editieren:

- Device Name: Name des Trap-Receivers
- Device Text: nähere Gerätebeschreibung
- Location: Ort, an dem der Trap-Receiver installiert ist
- Contact: Kontaktadresse im Servicefall

Übernehmen Sie die vorgenommenen Änderungen, indem Sie auf den Button *Zwischenspeichern* klicken, bevor Sie die Seite verlassen.

4.3 Zeit und Datum einstellen

Zeit und Datum können **manuell** eingestellt werden, zusätzlich können die Informationen aber auch von einem **Time Server** abgeholt werden.

Außerdem kann das Gerät selber als Time Server für andere Geräte im Netzwerk fungieren.

4.3.1 Lokale Uhreinstellung

Für die manuelle Einstellung der Systemuhr bietet das Gerät einen geführten Weg über die Profile. Rufen Sie hierzu das Profil *Lokale Uhreinstellung* auf.

Timezone

`Config >> Device >> Basic Settings >> Time/Date >> TimeZone`

Legen Sie auf dieser Seite die Zeitzone fest, in der sich das Gerät befindet. Die Einstellungen beziehen sich auf UTC (Universal Time Coordinated). Standardwert für Deutschland beträgt eine Stunde. Übernehmen Sie die Einstellungen mit einem Klick auf *Zwischenspeichern*.

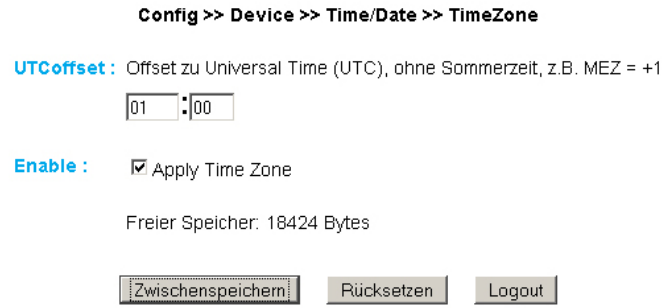


Abb.: Zeitzonenkonfiguration

Summertime

`Config >> Device >> Basic Settings >> Time/Date >> TimeZone >> Summertime`

Wenn Sie wünschen, dass Ihr Gerät automatisch die Sommerzeit berücksichtigt, geben Sie zunächst den Offset zu UTC ein. Der Standardwert (u. a. für Deutschland) beträgt zwei Stunden. Aktivieren Sie diese Funktion über das Kontrollhäkchen *Apply Summertime* und übernehmen Sie die Einstellungen.

Auf den Seiten *Start* und *Stop* kann die Regel modifiziert werden, nach der Beginn und Ende der Sommerzeit festgelegt wird.

Werksseitig eingestellt beginnt die Sommerzeit am letzten Sonntag im März um 2:00 Uhr. Das Ende der Sommerzeit ist voreingestellt auf den letzten Sonntag im Oktober um 3:00 Uhr.

Device Clock

`Config >> Device >> Basic Settings >> Time/Date >> Device Clock`

Wenn Sie keinen Time Server nutzen wollen, haben Sie hier die Möglichkeit, die Uhr manuell einzustellen. Klicken Sie anschließend auf *Logout* und speichern Sie Ihre Einstellungen ab.

4.3.2 Automatische Uhreinstellung per Netzwerkdienst

`Config >> Device >> Basic Settings >> Time/Date >> Time Server`

Die Konfiguration der automatischen Einstellung der Systemuhr via Time Server kann ebenfalls durch ein Profil geführt erfolgen.

Identisch zur lokalen Uhreinstellung müssen auch hier die Seiten *Timezone*, *Summertime*, *Start* und *Stop* konfiguriert werden.

Zusätzlich ist die Konfiguration für den Zeitabgleich per Netzwerkdienst auf der Seite *Time Server* vorzunehmen. Hier können die Adressen von zwei Timeservern hinterlegt werden, damit auch ein Zeitabgleich durchgeführt werden kann, wenn einer der beiden Server nicht erreichbar ist. Mit einem Klick auf das Lupensymbol hinter den Adressen kann die Erreichbarkeit der Server überprüft werden. Im Auslieferungszustand sind bereits zwei gültige Adressen eingetragen.

Aktivieren Sie die Option *Apply Timeserver*, um die automatische Uhreinstellung einzuschalten.

Die voreingestellten Adressen sind nur ein Beispiel und müssen nicht zwangsläufig benutzt werden.

Wenn Sie als Time Server-Adresse einen Namen und keine IP-Adresse eingeben, stellen Sie bitte sicher, dass Sie im Vorfeld sowohl Gateway als auch DNS-Server konfiguriert haben. Eine Adressauflösung ist sonst nicht möglich.

Übernehmen Sie die Änderungen mit *Zwischenspeichern*.

Auf der Home-Seite wird in der Tickerbox das letzte Update der Seite angezeigt. Wenn hinter der Uhrzeit ein „*“ erscheint, ist das Gerät mit dem Time Server synchronisiert.

4.3.3 SNTP-Timeserver aktivieren

Ist die Systemzeit des Gerätes via Abgleich mit einem Time Server synchronisiert, kann der Trap-Receiver selber auch als Time Server für andere Teilnehmer im Netzwerk fungieren.

Unterstützt wird hier SNTP (Simple Network Time Protocol).

Zum Starten des Timeserver-Dienstes aktivieren Sie die Option *SNTP Service* auf der Konfigurationsseite

`Config >> Device >> Basic Settings >> Time/Date >> Time Server`

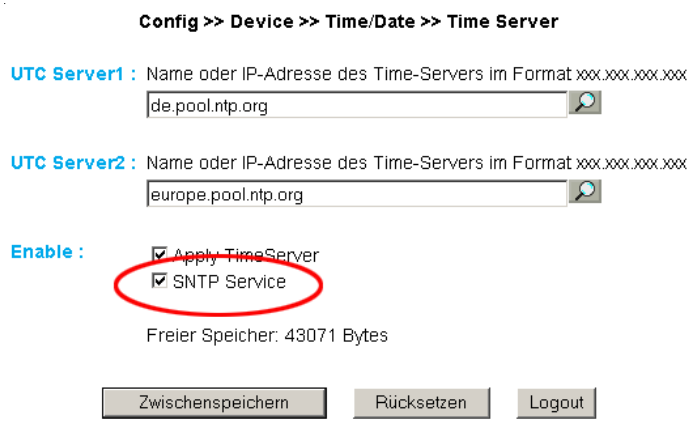


Abb.: Timeserver-Dienst starten

4.4 HTTP-Port

Auf der Seite

`Config >> Device >> Basic Settings >> HTTP`

kann der Port festgelegt werden, über den das Gerät angesprochen wird. Voreingestellt ist der Standard-HTTP-Port 80. Wenn Sie einen anderen Port verwenden möchten, muss dieser unter Umständen explizit beim Seitenaufruf angegeben werden, zum Beispiel für den Aufruf der Seite home.htm:

`http://<IP-Adresse des Trap-Receivers>/home.htm:<Portnummer>`

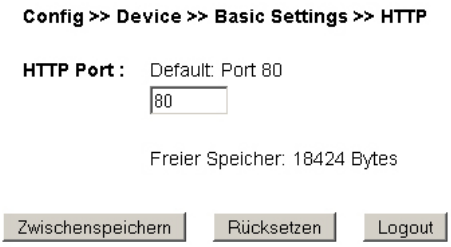


Abb.: Konfiguration der HTTP-Portnummer

4.5 Mail

Dieser Punkt wird näher beschrieben unter:

`Config >> Device >> Actions >> Action X >> Mail`

4.6 System Traps via SNMP und SNMP-Basiskonfiguration

Folgende System Traps können mittels des SNMP-Protokolls an einen SNMP-Manager gesendet werden:

- Cold Start: Wiederanlauf nach Trennen oder Ausfall der Spannungsversorgung
- Warm Start: Wiederanlauf nach Gerätereset

Des Weiteren können im Gerät aufgelaufene Diagnosemeldungen übermittelt werden.

Die SNMP-Konfiguration erfolgt auf der Seite:

`Config >> Device >> Basic Settings >> SNMP`

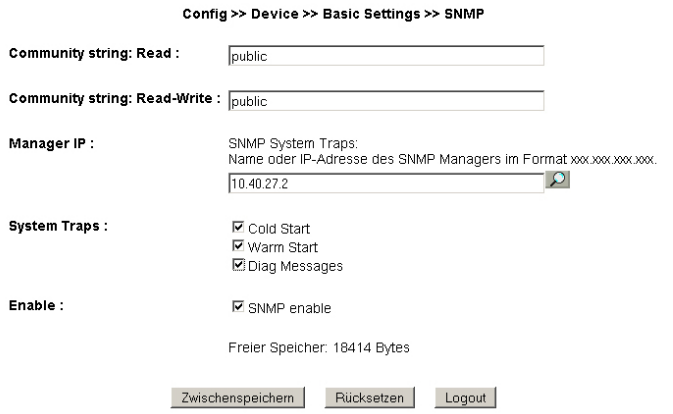


Abb.: SNMP-Konfiguration

SNMP ist im Vergleich zu den anderen Benachrichtigungsverfahren defaultmäßig aktiviert.

Definieren Sie hier die Basisparameter, welche für den SNMP-Betrieb notwendig sind:

- Community String: Read: Mit Hilfe dieser Zeichenkette können Sie in Ihrem SNMP-Manager lesend auf das Gerät zugreifen.
- Community String: Read-Write: Mit Hilfe dieses Strings können Sie in Ihrem SNMP-Manager sowohl lesend als auch schreibend auf das Gerät zugreifen.
- Manager IP: Enthält die IP-Adresse Ihres SNMP-Managers. An diese Adresse werden die SNMP-Meldungen des Trap-Receivers versendet.
- System Traps: Wählen Sie die Meldungen, die versendet werden sollen.
- Enable: Aktivieren Sie die SNMP-Funktion

4.7 UDP

Dieser Punkt wird näher beschrieben unter:

```
Config >> Device >> Actions >> Action X >> UDP
```

4.8 System Messages über Syslog

Identisch zu den SNMP-System Traps können Cold Start, Warm Start und Diagnosemeldungen an einen Syslogserver übermittelt werden.

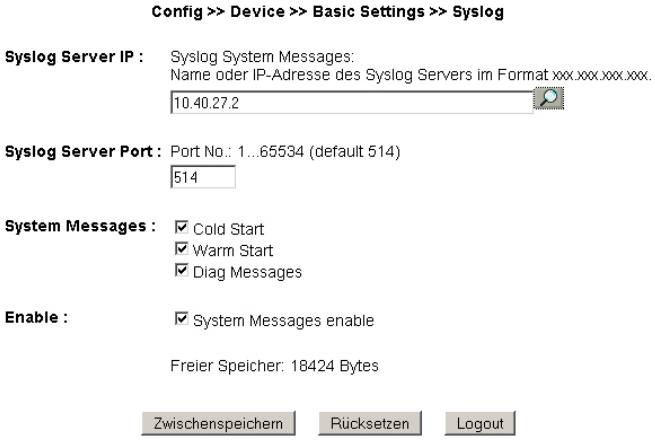


Abb.: System Messages über das Syslog Protokoll

Um dieses Nachrichtensystem zu aktivieren, geben Sie auf der Konfigurationsseite

`Config >> Device >> Basic Settings >> Syslog`

die IP-Adresse eines Syslogservers und die Portnummer ein, über welche die Kommunikation laufen soll.

Markieren Sie die Nachrichtentypen, die an den Server gesendet werden sollen und aktivieren Sie *System Messages enable*.

Sollen von einer der 12 Aktionen Syslog-Messages versendet werden, so ist auch dafür *System Messages enable* aktivieren.

Übernehmen Sie die Einstellungen mit *Zwischenspeichern*.

4.9 FTP

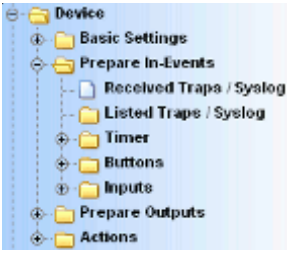
Dieser Punkt wird näher beschrieben unter:

`Config >> Device >> Actions >> Action X >> FTP`

5 Kundeneinstellungen

Um die Aktionen konfigurieren zu können, müssen die Eingänge bzw. In-Events definiert sein. In den einzelnen Aktionen-Formulare werden Ihnen dann nur noch die definierten In-Events zur Auswahl angeboten. Das Verhalten der Netzwerk-Ausgänge (z.B. Mail-Adresse, die benachrichtigt werden soll) wird unter jeder Aktion definiert. Im Aktions-Formular ist ein Filterbereich enthalten, der ggf. angibt, zu welchen Zeiten die Aktion nicht ausgeführt wird.

5.1 In-Events konfigurieren



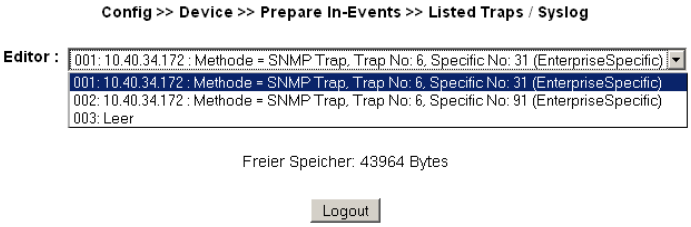
5.1.1 Netzwerk-Ereignisliste

Die Ereignis-Liste kann maximal 1000 Einträge aufnehmen. Auslösebedingung für eine Aktion kann das Auftreten eines Events im Netzwerk sein. Bevor die Aktionen im Detail konfiguriert werden, müssen die zu überwachenden Netzwerkkomponenten in die Liste der bekannten Netzwerk-Ereignisse aufgenommen werden. Aus dieser zentralen Liste erfolgt die Zuordnung der Komponenten zu den einzelnen Aktionen.

Die Verwaltung der SNMP-Traps und Syslog Messages erfolgt auf der Seite *Config >> Device >> Prepare In-Events >> Listed Traps / Syslog*.

Hier finden Sie Funktionen zum ...

- ...Einfügen neuer Ereignisse.
- ...Bearbeiten eines vorhandenen Eintrags.
- ...Löschen eines einzelnen Eintrags.
- ...Löschen aller Einträge.



5.1.1.1 Eintrag einfügen

Über den Button *Einfügen* gelangen Sie zu der Maske, über die neue Geräte / Ereignisse in die Liste aufgenommen werden können.

Der Wert *Item No.* bestimmt die Position des Gerätes in der Liste. Im Feld *IP Addr* geben Sie die IP-Adresse oder den Hostnamen des zu überwachenden Netzwerkteilnehmers an.

Eventuell an dieser Position bereits gespeicherte Einträge werden nach hinten geschoben.

Der Trap-Receiver überwacht nicht aktiv die Netzwerkkomponenten, von denen Ereignisse erwartet werden.

Stellen Sie sicher, dass die gewählten Netzwerkteilnehmer korrekt angeschlossen sind und arbeiten. Ggf. nutzen Sie den IP-Watcher, mit dem Sie feststellen können, ob ein Netzwerk-Teilnehmer noch bereit ist.

Bei *Alias* können Sie einen Freitext eintragen, der Ihnen die Zuordnung der abstrakten IP-Adressen oder Hostnamen zu den realen, zu überwachenden Netzwerkkomponenten erleichtert.

Beenden Sie den Vorgang durch Betätigen der Schaltfläche *Zwischenspeichern*.

5.1.1.2 Einträge bearbeiten

Zum Bearbeiten eines Eintrags wählen Sie diesen über die Pull-Down-Box aus und betätigen Sie die Schaltfläche *Bearbeiten*. Sie gelangen zu einer Maske, die erlaubt, die Parameter des Eintrags zu modifizieren. Beenden Sie den Vorgang mit *Zwischenspeichern*.

5.1.1.3 Löschen

Der über die Pull-Down-Box ausgewählte Eintrag wird beim Betätigen des Buttons *Löschen* aus der Liste entfernt.

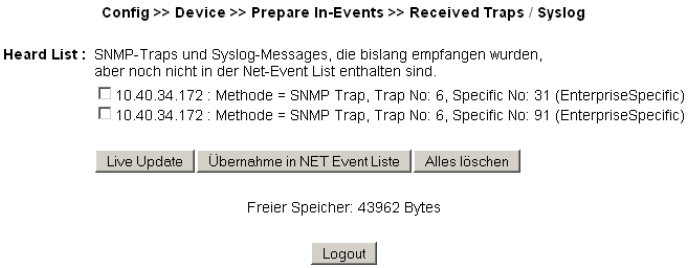
5.1.1.4 Ereignisliste löschen

Das Betätigen der Schaltfläche *Alles löschen* entfernt alle Einträge aus der Ereignisliste.

5.1.1.5 Automatisches Hinzufügen über die Heard List

Config >> Device >> Prepare In-Events >> Received Traps / Syslog

Das Gerät ist grundsätzlich bereit, SNMP-Traps bzw. Syslog-Messages zu empfangen. Die empfangenen Traps werden dann in die Heard List eingetragen.



Durch erneutes Wählen von *Config >> Device >> Prepare In-Events >> Received Traps / Syslog* werden neu eingegangene Netzwerk-Ereignisse angezeigt. Voraussetzung: Ereignisse, die bereits in der Eventliste eingetragen sind, tauchen hier nicht mehr auf.

Es kann gewünscht sein, den Eintritt von Netzwerk-Ereignissen zu visualisieren. Dazu steht die Schaltfläche *Live Update* zur Verfügung. Bei Betätigung stellt das Gerät die letzten beiden eingehende Traps / Messages in der Scan-Box dar.

Während des Scannens sollten die gesuchten Ereignisse stattfinden. Der Fortschritt eines laufenden Scans wird während des Vorgangs durch einen Statusbalken visualisiert. Scan-Abbruch ist durch Betätigen von *Cancel* möglich.

Gefundene Traps / Messages werden nun in die Heard-Liste eingetragen. Dort können die gewünschten Ereignisse angeklickt werden, um sie in die Ereignisliste (auch Watchlist genannt) zu übernehmen.

Schaltfläche *Alles löschen*

Bei Betätigung werden alle neu empfangenen Traps / Messages gelöscht.

Schaltfläche *Übernahme in In-Event-List*

Angeklickte Netzwerk-Ereignisse werden in die Event-Liste übernommen.

Bei Betätigung erfolgt der Wechsel zum Editor, falls keine Traps gefunden wurden. Gefundene Traps müssen angeklickt werden, wenn sie in die In-Event-List übernommen werden sollen.

5.1.2 Timer

Insgesamt können 2 Timer zur freien Verfügung konfiguriert werden.

Wählen Sie im Navigationsbaum beispielsweise:

```
Config >> Divice Prepare In-Events >> Timer >> Timer 1
```

Klicken Sie die Checkbox *Enable* an, wenn Sie den Timer aktivieren wollen.

Geben Sie bei *Name* eine Bezeichnung ein, die auf der Home-Seite im Browser angezeigt wird.

Im Block *Timer 1* legen Sie fest, zu welchen Zeiten der Timer aktiv wird. Die Zeiten werden im sogenannten Cronformat eingegeben. „*“ wird eingesetzt für ‘beliebig’. Stehen beispielsweise in allen Feldern „*“, würde der Timer jede Minute aktiv.

5.1.3 Buttons für die Home-Seite konfigurieren

Beispielhaft sind in der Werkseinstellung bereits die Buttons 7 und 8 konfiguriert.

Insgesamt können 8 Buttons zur freien Verfügung konfiguriert werden.

Wählen Sie im Navigationsbaum beispielsweise:

```
Config >> Divice Prepare In-Events >> Buttons >> Button 1
```

Klicken Sie die Checkbox *Enable* an, wenn Sie den Button aktivieren wollen.

Geben Sie bei *Name* eine Bezeichnung ein, die auf dem Button auf der Home-Seite im Browser angezeigt wird.

Die im Feld *Text* eingetragene Beschreibung kann zum Beispiel die Funktion bzw. die Auswirkung der Button-Betätigung näher beschreiben.

Im Block *Access Level* legen Sie fest, wer die Buttons nutzen und die zugehörigen Aktionen auslösen darf. Gast ist aktiv, wenn kein Login stattfindet. Operator und Administrator müssen sich mit Passwort anmelden. Login ohne vergebenes Passwort führt immer zu Administrator-Rechten.

5.1.4 Porteinstellungen - Inputs

Für jeden der zwei Inputs können individuelle Grundeinstellungen vorgenommen werden.

Um zum Beispiel die Einstellungen für Input 0 zu ändern, wählen Sie im Navigationsbaum:

```
Config >> Divice Prepare In-Events >> Inputs >> Input 0
```

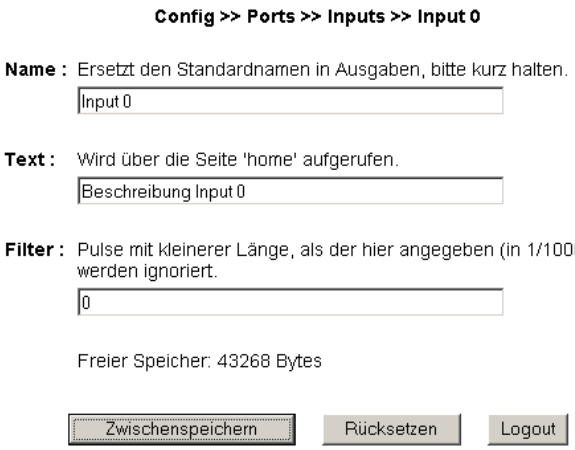


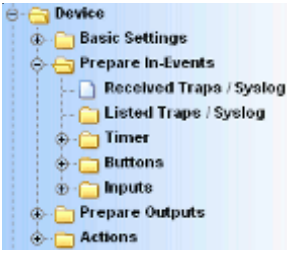
Abb.: Basiskonfiguration „Input 0“

Geben Sie bei *Name* eine Bezeichnung für den Input ein. Diese Bezeichnung wird dann im Browser für den Input 0 angezeigt.

Die im Feld *Text* eingetragene Beschreibung kann zum Beispiel die Funktion oder den Installationsort des Sensors näher beschreiben.

Bei *Filter* können Sie eine Zeit bestimmen, die ein Signal mindestens anliegen muss, um erkannt zu werden. Liegt ein Pegel kürzer als die hier definierte Zeitspanne an, wird er ignoriert. Die Angabe erfolgt in 1/1000 Sekunden. Ist hier kein Wert eingetragen, ist diese Funktion deaktiviert.

5.2 Out-Events konfigurieren



`Config >> Device >> Prepare Outputs >> Output x`

Wählen Sie zum Beispiel die Einstellungen für Output 0.

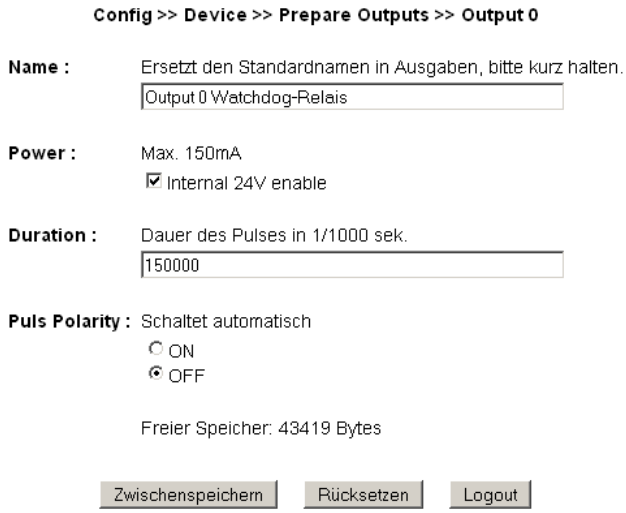


Abb.: Einstellungen Namen und Text von „Output 0“

Name: Geben Sie in dieses Feld eine Bezeichnung für den Output ein. Diese Bezeichnung wird dann im Browser für den Output 0 angezeigt und kann zum Beispiel die Funktion oder den Installationsort des Aktors näher beschreiben.

Power: Hier stellen Sie ein, ob an Vdd 24V zur Verfügung gestellt werden.

Duration: Neben dem rein statischen Schalten der Outputs auf ON oder OFF erlaubt der Trap-Receiver auch die Ausgabe von Pulsen. Das bedeutet, der Output wird geschaltet und hält diesen Zustand für eine Zeit, die der einstellbaren Pulslänge entspricht. Anschließend wird automatisch entsprechend Puls Polarity geschaltet. Tragen Sie bei *Duration* die gewünschte Pulslänge in 1/1000 Sekunden ein. Ein Wert von 1000 entspricht einem 1 Sekunde langen Puls.

Puls Polarity: Der Einschalt- bzw. Ruhezustand des Ausganges ist ab Werk OFF (0V, aus). Sie können auch konfigurieren, dass der Ausgang beim Einschalten des Gerätes ON (Vdd, ein) ist. Damit wählen Sie gleichzeitig aus, dass der Ausgang nach Pulsende ein- bzw. ausgeschaltet wird. Sie können den Ausgang auch manuell in die Richtung von Puls Polarity schalten und kürzen damit einen Puls ab.

5.3 Aktionen (Actions) konfigurieren

Im Trap-Receiver können bis zu 12 verschiedene Aktionen festgelegt werden. Die Auslösung einer Aktion findet aufgrund eines Ereignisses statt. Die sogenannten In-Events können SNMP-Traps, Syslog Messages, Änderungen an den beiden dig. Eingängen, Button-Betätigung und Zeitereignisse sein. Einer Aktion stehen verschieden Out-Events (Netzwerkprotokolle und zwei lokale digitale Ausgänge) zur Verfügung, um das auslösende In-Event zu melden. Quittierungen von Ereignissen können beliebig konfiguriert werden.

Da die Erzeugung von Meldungen um ein Vielfaches schneller erfolgen kann als die Versendung, gibt es Regeln, die das Meldungsaufkommen regulieren:

- Es wird versucht, noch nicht gesendete Meldungen zu zu stellen.
- Wird eine Aktion, deren Meldungen noch nicht komplett versendet sind, erneut ausgelöst, werden alle Meldungen der alten Aktion gelöscht.
- Erfolgt die Auslösung einer Aktion und die Quittierung schneller als das Gerät diese Zustandsänderungen

detektieren kann, ist ein geordneter Meldeablauf nicht mehr möglich. Zu hohe Beschaltungsfrequenz verhindert ebenfalls einen geordneten Meldeablauf.

Entstehen beim Absenden der Meldungen Verzögerungen, zum Beispiel durch Wartezeiten beim Verbindungsaufbau, wirken sich diese Verzögerungen ebenfalls auf die noch nicht versendeten Meldungen aus.

Über das Konfigurationsmenü können Sie die zur Verfügung stehende Aktionen 1-12 parametrieren. Rufen Sie hierzu die Konfigurationsseite

```
Config >> Device >> Actions >> Action X
```

auf.

Geben Sie im Feld *Action Name* einen Namen für die Aktion ein. Dieser Name wird auf allen Steuer- und Bedienseiten angezeigt.

Die Checkbox *Action Enable* muss aktiviert sein, damit die Aktion bei Eintreten der Triggerbedingung durch einen In-Event gestartet wird. Soll die Aktion deaktiviert werden, muss lediglich die Checkbox wieder deaktiviert werden. Es ist unnötig, die Einstellungen zu löschen.

In-Events

Im Block *Listed Traps / Syslog* finden Sie alle Traps, die Sie zuvor in die Liste der Netzwerk-Ereignisse aufgenommen haben. Aktivieren Sie die Checkbox vor den Einträgen, die durch die Aktion überwacht werden sollen. Die Liste enthält Einträge wie z.B.:

10.40.1.1: Methode = SNMP Trap, Trap No: 6, Specific No: 31 (EnterpriseSpecific)

Es können bis zu zwei Timer aktiviert werden, die zuvor in Config >> Device >> Prepare In-Events >> Timer definiert worden sein müssen.

Maximal 8 Buttons können als In-Event angewählt werden, auch sie müssen zuvor definiert werden.

Filter

Time Window: Über das Feld *Time Trigger* bestimmen Sie das Zeitfenster, in dem die Aktion ausgeführt wird. Außerhalb des gewählten Zeitfensters werden die In-Events ignoriert.

Die Zeiten werden im sogenannten Cronformat eingegeben. „*“ wird eingesetzt für ‘beliebig’.

Out-Events

Der Block *Out-Event* enthält sämtliche Meldearten, die über das Netzwerk möglich sind. Wählen Sie hier den gewünschten Kommunikationsweg aus für die Benachrichtigung:

- Mail (SMTP)
- SNMP
- Syslog
- UDP Peer
- TCP Client
- FTP Client

Im Block *Outputs* können Sie das Verhalten der beiden lokalen digitalen Ausgänge konfigurieren. Dazu setzen Sie vorne das Häkchen zur Aktivierung und entscheiden dann, ob der Ausgang aus- oder eingeschaltet werden soll oder ob er seinen Zustand wechseln soll.

5.3.1 Output-Events - Nachrichtentexte formulieren

Für die über das Netzwerk meldenden Benachrichtigungsarten können Meldungen formuliert werden, die auf Anforderung vom Gerät versendet werden:

Die Konfiguration der verschiedenen Meldungen erfolgt auf den untergeordneten Seiten der einzelnen Aktionen, zum Beispiel:

```
Config >> Device >> Actions >> Action 1 >> Mail
```

Dort wählen Sie im Feld *E-Mail-Addr* die Mail-Adresse, an die die gewählte Aktion ihre Meldung absenden soll.

In den Feldern *Subject* und *Action Text* tragen Sie den Betreff und den Nachrichtentext ein, der im Fall einer Akion verschickt werden sollen.

Um die Nachrichtentexte dynamisch mit aktuellen Informationen des Gerätes zu füllen, stehen die in folgender Tabelle aufgeführten Tags zur Verfügung. Diese Platzhalter werden, wenn sie in den Nachrichtentext eingefügt sind, beim Versenden der Meldung durch den jeweils aktuellen Systemwert ersetzt.

```
Time:              <t>
Signle       Input:     <i0>    ..    <i1>
Single       Output:    <o0>    ..    <o1>
All     Inputs     (Hex):   <i>
All     Outputs     (Hex): <o>
```

Im Action Text muss mindestens ein Zeichen stehen, damit der Trap-Receiver tatsächlich eine Mail versendet.

5.3.2 Benachrichtigung per E-Mail

Rufen Sie das Profil *Alarmierung per E-Mail* auf.

Konfigurieren Sie zunächst auf der Seite

```
Config >> Device >> Basic Settings >> Mail
```

die Basiseinstellungen zum Versenden von E-Mails wie im Folgenden erläutert.

Die E-Mail-Funktion erlaubt es, Ihnen eine Benachrichtigungs-Mail an einen oder mehrere E-Mail-Empfänger abzusetzen.

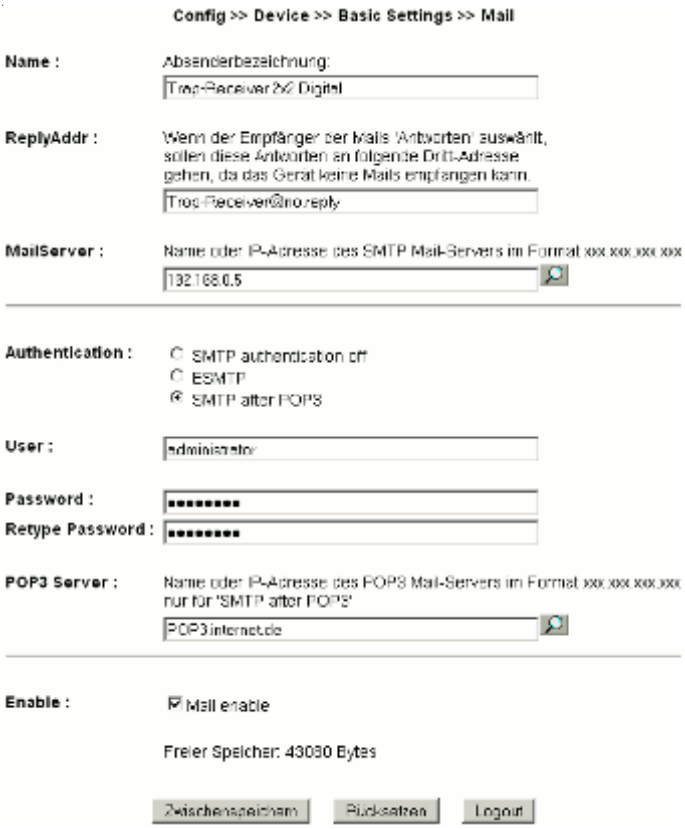


Abb.: Mail-Basiskonfiguratioin

Folgende Parameter sind hier einzustellen:

Geben Sie im Feld *Name* den Namen ein, der beim E-Mail-Empfänger erscheinen soll.

Die *ReplyAddr* stellt die Adresse dar, mit der das Gerät sich identifiziert.

Stellen Sie im nächsten Schritt die IP-Adresse Ihres Mailservers, bzw. dessen Host-Namen (nur bei konfiguriertem DNS-Server) ein, an den sich das Gerät wenden soll. Mit der Lupe rechts können Sie testen, ob der Server erreichbar ist (Ping).

Sollte der E-Mail-Port nicht dem Standardport 25 entsprechen, können Sie den Port mit einem Doppelpunkt an die Adresse anhängen:

```
mail.provider.de:<Port>
```

Sofern eine Authentifizierung am Mailserver notwendig ist, stellen Sie bei *Authentication* das entsprechende Verfahren zur Identifikation des Benutzers ein:

- SMTP authentication off: Keine Authentifizierung
- ESMTP: Es wird ein Benutzername und ein Passwort benötigt, um sich auf dem Mailserver einzuloggen.
- SMTP after POP3: Für einen SMTP-Zugriff ist es notwendig zunächst einen Zugriff über POP3 vorzunehmen, damit der Benutzer identifiziert werden kann. Für diese Einstellung geben Sie zusätzlich einen zugehörigen POP3-Server an.

Aktivieren Sie abschließend die Mail-Funktion über die Checkbox *Mail enable*.

Übernehmen Sie die Änderungen mit *Zwischenspeichern*.

Mailparameter und -texte speziell für jede Aktion

```
Config >> Device >> Actions >> Action x
```

Hier setzen Sie bei Output-Events das Häkchen bei 'Mail'.

Zuletzt ist noch die Definition der Meldungen und der alarmspezifischen Mailparameter erforderlich. Hierzu rufen Sie die Seite

```
Config >> Device >> Actions >> Action x >> Mail
```

auf. Im Feld *E-Mail-Addr* tragen Sie die Adresse des Empfängers ein. Soll die E-Mail an mehrere Empfänger gesendet werden, trennen Sie die Adressen mit einem Semikolon voneinander.

Abschließend konfigurieren Sie die erforderlichen Nachrichtentexte wie im Kapitel *Nachrichtentexte formulieren* beschrieben und übernehmen die Änderungen mit *Zwischenspeichern*.

5.3.3 Benachrichtigung per SNMP-Trap

Rufen Sie zur Unterstützung das Profil *SNMP incl.Alarmierung per Trap* auf.

Konfigurieren Sie zunächst auf der Seite

```
Config >> Device >> Basic Settings >> SNMP
```

die Basiseinstellungen zum Versenden von SNMP-Traps wie im Folgenden erläutert. Aktivieren Sie hier die Checkbox *SNMP enable*. Dadurch wird die SNMP-Funktion im Gerät gestartet, die das Versenden von Meldungen über SNMP verarbeitet.

Übernehmen Sie die Änderungen mit *Zwischenspeichern*.

SNMP-Parameter und -texte speziell für jede Aktion

```
Config >> Device >> Actions >> Action x
```

Hier setzen Sie bei Output-Events das Häkchen bei ‘SNMP Trap’.

Abschließend ist noch die Definition der Meldungen und der spezifischen SNMP-Parameter erforderlich. Hierzu rufen Sie die Seite

```
Config >> Device >> Actions >> Action x >> SNMP
```

auf. Tragen Sie im Feld *Manager IP* die IP-Adresse des SNMP-Managers ein, der die Meldung empfangen und darstellen oder auswerten soll.

Zuletzt konfigurieren Sie die erforderlichen Nachrichtentexte wie im Kapitel *Nachrichtentexte formulieren* beschrieben und übernehmen die Änderungen mit *Zwischenspeichern*.

5.3.4 Benachrichtigung per UDP-Client

Aktivieren Sie auf der Seite

```
Config >> Device >> Basic Settings >> UDP
```

die Option *UDP enable* und übernehmen Sie die Änderung mit *Zwischenspeichern*.

```
Config >> Device >> Actions >> Action x
```

Hier setzen Sie bei Output-Events das Häkchen bei 'UDP Client', damit das Gerät als UDP-Client arbeitet.

Tragen Sie auf der Seite

```
Config >> Device >> Actions >> Action x >> UDP
```

im Feld *IP Addr* die IP-Adresse des empfangenden UDP-Servers ein. Bei *Port* legen Sie den Zielport fest.

Zuletzt konfigurieren Sie die erforderlichen Nachrichtentexte wie im Kapitel *Nachrichtentexte formulieren* beschrieben und übernehmen die Änderungen mit *Zwischenspeichern*.

5.3.5 Benachrichtigung per TCP-Client

```
Config >> Device >> Actions >> Action x
```

Hier setzen Sie bei Output-Events das Häkchen bei 'TCP Client', damit das Gerät als TCP-Client arbeitet.

Tragen Sie auf der Seite

```
Config >> Device >> Actions >> Action x >> TCP
```

im Feld *IP Addr* die IP-Adresse des TCP-Servers ein. Bei *Port* legen Sie den Zielport fest.

Zuletzt konfigurieren Sie die erforderlichen Nachrichtentexte wie im Kapitel *Nachrichtentexte formulieren* beschrieben und übernehmen die Änderungen mit *Zwischenspeichern*.

5.3.6 Benachrichtigung per Syslog

Rufen Sie zur Unterstützung das Profil *Syslog Messages incl. Alarmierung* auf.

Konfigurieren Sie zunächst auf der Seite

```
Config >> Device >> Basic Settings >> Syslog
```

die Basiseinstellung zum Versenden von Syslog System Messages. Aktivieren Sie die Checkbox *System Messages enable*. Diese Option schaltet die Syslog-Funktion im Trap-Receiver frei und ermöglicht so das Versenden von Meldungen unter Verwendung des Syslog-Protokolls.

Übernehmen Sie die Änderungen mit *Zwischenspeichern*.

Syslog-Parameter und -texte speziell für jede Aktion

```
Config >> Device >> Actions >> Action x
```

Hier setzen Sie bei Output-Events das Häkchen bei ‘Syslog Messages’.

Tragen Sie auf der Seite

```
Config >> Device >> Actions >> Action x >> Syslog
```

im Feld *IP Addr* die IP-Adresse des Empfängers ein. Unter *Port* setzen Sie die Portnummer ein, über welche die Kommunikation abgewickelt werden soll.

Zuletzt konfigurieren Sie die erforderlichen Nachrichtentexte wie im Kapitel *Nachrichtentexte formulieren* beschrieben und übernehmen die Änderungen mit *Zwischenspeichern*.

5.3.7 Alarmierung per FTP

Versenden Sie Meldungen via FTP und schreiben Sie diese direkt auf einen FTP-Server.

Rufen Sie zur Unterstützung das Profil *Alarmierung per FTP (Client Mode)* auf.

Konfigurieren Sie zunächst auf der Seite

`Config >> Device >> Basic Settings >> FTP`

die Basisparameter für den Nachrichtenversand per FTP fest.

Tragen Sie bei *FTP Server IP* die IP-Adresse oder den Host-Namen (nur bei konfiguriertem DNS-Server) Ihres FTP-Servers ein, an den die Daten geschickt werden sollen.

Legen Sie im Feld *FTP Control Port* den Port fest, über den die Verbindung stattfinden soll. Der Standardport für FTP-Zugriffe ist 21. Dieser Port ist bereits voreingestellt und sollte auf den meisten Systemen auf Anhieb funktionieren. Sollten Sie einen anderen Port benötigen, befragen Sie hierzu bitte Ihren Netzwerk-Administrator.

Bei *User* und *Password* geben Sie die Zugangsdaten ein, die für den FTP-Zugriff benötigt werden.

Einige FTP-Server verlangen für das Login einen speziellen Account-Eintrag. Sollte dies bei Ihrem Server der Fall sein, tragen Sie den Account-Namen bei *FTP Account* ein.

Ist die Checkbox *PASV* unter *Options* aktiviert, wird der Server angewiesen, im Passiv-Modus zu arbeiten. Dies bedeutet, dass die Datenverbindung durch die Web-Meldung geöffnet wird. Ist diese Option deaktiviert, übernimmt der FTP-Server das Öffnen

der Datenverbindung. Sollte der Server mit einer Firewall geschützt sein, empfiehlt es sich, die PASV-Option zu aktivieren, da sonst unter Umständen Verbindungsversuche abgeblockt werden.

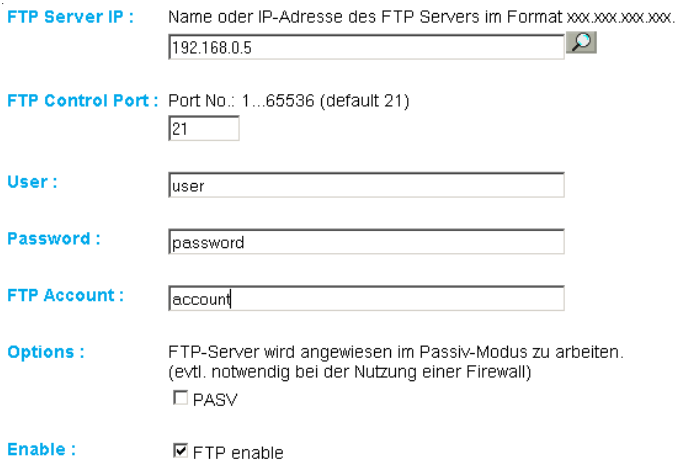


Abb.: FTP-Basiskonfiguration

Aktivieren Sie abschließend die FTP-Funktion des Gerätes über die Checkbox *FTP Enable* und übernehmen Sie die Änderungen mit *Zwischenspeichern*.

FTP-Parameter und -texte speziell für jede Aktion

`Config >> Device >> Actions >> Action x`

Hier setzen Sie bei Output-Events das Häkchen bei 'FTP Client'. Tragen Sie auf der Seite

`Config >> Device >> Actions >> Action x >> FTP`

die gewünschten FTP-Parameter ein.

Legen Sie bei *FTP Local Data Port* den lokalen Datenport des Trap-Receivers fest. Gültiger Wertebereich: 1 .. 65536. Die Eingabe *AUTO* veranlasst das Gerät, den Port dynamisch zu wählen.

Unter File Name tragen Sie den Pfad zu der Datei ein, auf die das Gerät zugreifen soll. Im Dateinamen können die gleichen Tags genutzt werden wie im FTP-Nachrichtentext.

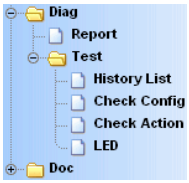
Mit den Optionen STORE und APPEND können Sie wählen, ob die gesendeten Daten in eine neue Datei geschrieben oder an eine bestehende Datei angefügt werden sollen. Existiert die Datei noch nicht, wird sie in beiden Fällen erstellt.

Abb.: FTP-Optionen „STORE“ und „APPEND“

Zuletzt konfigurieren Sie die erforderlichen Nachrichtentexte wie im Kapitel *Nachrichtentexte formulieren* beschrieben. Wünschen Sie einen Zeilenvorschub, fügen Sie ein CRLF durch Betätigen der RETURN-Taste am Ende der Zeile ein. Übernehmen Sie die Änderungen mit *Zwischenspeichern*.

6 Troubleshooting und Test

Der Trap-Receiver verfügt über ein internes Fehlermanagement und Diagnosesystem. Im Konfigurationsbaum ist dieses unter dem Ordner Diag zu finden.



6.1 Report

Treten Fehler auf, werden diese in einem Diagnose Report dokumentiert und können dort jederzeit ausgelesen werden.

Alle Fehlermeldungen werden im Gerät gespeichert und bleiben auch erhalten, wenn die Fehlerursache bereits behoben ist. Ist der Fehler nicht mehr aktuell, wird er aus dem Diagnose Report in das Diagnose Archiv verschoben.

Abb.: Diagnose Report und Diagnose Archiv

Diagnose Report und Diagnose Archiv sind unter Diag >> Report einzusehen.

Durch Betätigen des Buttons *Report löschen* werden alle vorhandenen Meldungen aus dem Speicher gelöscht.

Für das Löschen der beiden Fehlerspeicher über den Button „Report löschen“ ist ein Login mit Administratorrechten erforderlich.

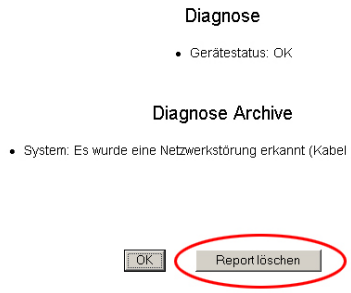


Abb.: Zugang mit Administratorrechten

Ein Reset, unabhängig ob er durch Unterbrechung der Versorgungsspannung oder durch Reset aus der Seite *Logout* ausgelöst wurde, löscht ebenfalls den Report.

Darüber hinaus können Fehler- und Diagnosemeldungen auch über SNMP-Traps oder als Syslog-Systemmeldung verarbeitet werden. Weitere Informationen hierzu finden Sie in den Kapiteln *System Traps über SNMP* und *System Messages über Syslog*.

6.2 History List

Die letzten Ereignisse (In-Events, Out-Events) werden vom Trap-Receiver in der History List mit Zeitstempel protokollert. Das Gerät bietet dem Operator / Administrator die Möglichkeit, dieses Protokoll einzusehen. Außerdem wird für die 12 Aktionen dokumementiert, durch welchen Trigger sie zu welchem Datum und zu welcher Zeit zuletzt gestartet worden sind.

Der Aufruf erfolgt über das Konfigurationsmenü *Diag >> Test >> History List*.

Die Events sind nur zur Laufzeit verfügbar. Nach Reset ist der Speicher gelöscht und die Liste ist leer.

Action	Trigger	Datum - Uhrzeit
Watchdog scharfgeschaltet, Meldung erfolgt.	Action set: Input 0 ⤒	24.01.2011 12:06:35
Watchdog zugeschlagen, Meldung erfolgt.	Action set: Input 0 ⤓	24.01.2011 12:13:05
Trap vom AD-Gerät erkannt.	Action set: NET Event List 1 Watchdog Analog	24.01.2011 12:10:35
Action 4	Power on: Init	24.01.2011 12:03:44
Action 5	Power on: Init	24.01.2011 12:03:44
Action 6	Power on: Init	24.01.2011 12:03:44
Action 7	Power on: Init	24.01.2011 12:03:44
Action 8	Power on: Init	24.01.2011 12:03:44
Action 9	Power on: Init	24.01.2011 12:03:44
Action 10	Power on: Init	24.01.2011 12:03:44
Action 11 Button 7 Output 1 ein	Power on: Init	24.01.2011 12:03:44
Action 12 Button 8 Output 1 aus	Power on: Init	24.01.2011 12:03:44

In / Out Log

In / Out Event	I/O Flag	Datum - Uhrzeit
Mail Action 2	O	24.01.2011 12:13:08
Input 0 ⤓	I	24.01.2011 12:13:05
Output 0 set to state ON	O	24.01.2011 12:10:35
NET Event List Item 1 Alias: Watchdog Analog	I	24.01.2011 12:10:34
Output 0 set to state ON	O	24.01.2011 12:08:35
NET Event List Item 1 Alias: Watchdog Analog	I	24.01.2011 12:08:34
Mail Action 1	O	24.01.2011 12:06:38
Input 0 ⤒	I	24.01.2011 12:06:35
Output 0 set to state ON	O	24.01.2011 12:06:35

last update: Mo, KW04, 24.01.2011 12:18:04

zurück zur Web-IO Homepage

6.3 Check Config

Das Gerät bietet dem Administrator die Möglichkeit, die aktuelle Konfiguration auf einer übersichtlichen Webseite zu überblicken und zu überprüfen.

Der Aufruf erfolgt über das Konfigurationsmenü *Diag >> Test >> Check Config*.

Die Webseite zeigt, welche Zugriffs- und Meldearten mit welchen Parametern aktiviert sind. Dabei nimmt das Gerät eine Plausibilitätsprüfung der Einstellungen vor. Werden fehlende Parameter erkannt, die den ordnungsgemäßen Betrieb der Zugriffsart verhindern, werden die entsprechenden Felder orange hinterlegt. Ein Klick auf den Link der falschen Konfiguration führt direkt zu der entsprechenden Einstellungsseite.

Parameter	HTTP	UDP	SNMP	Mail	Syslog	FTP
Enable Flag	----	OFF	ON	ON	OFF	OFF
Source Port	80	42279	161	auto	514	auto
Source IpAddr	10.40.27.71	10.40.27.71	10.40.27.71	10.40.27.71	10.40.27.71	10.40.27.71
Destination Port	n.a.	n.a.	162	25	----	----
Destination IpAddr	----	----	10.40.27.99	----	----	----
Active	OFF	OFF	**ON**	FAIL	OFF	OFF

Fehlerhafte oder unvollständige Eingaben werden orange markiert.
Wählen Sie in diesem Fall unter Config>>Session Control>>Profiles das entsprechende Profil aus und überprüfen Sie die blau gekennzeichneten Parameter.

Abb.: Übersicht und Plausibilitätsprüfung der Einstellungen mit Fehler

Ferner wird überprüft und angezeigt, welche Übertragungswege für die Aktionen gewählt wurden und ob alle benötigten Parameter konfiguriert wurden. Auch hier werden die Zugangsarten orange hinterlegt, die nicht vollständig konfiguriert wurden.

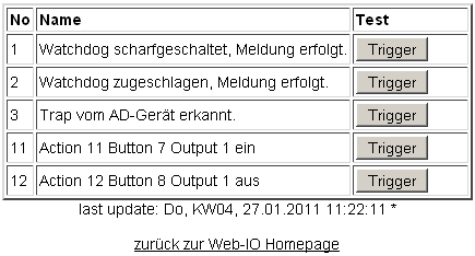
Parameter	Set Output	Alarm Mail	SNMP Trap	UDP Client	TCP Client	Syslog Message	FTP Message
Alarm / Trap	ON	ON	OFF	OFF	OFF	OFF	OFF

Abb.: Übertragungswege der Meldungen

Hier wird auch der Link zur Profilseite angeboten, um nötige Einstellungen leicht vornehmen zu können: *Config >> Session Control >> Profiles*.

6.4 Check Action

Um zu überprüfen, ob die konfigurierten Meldearten bei den aktivierten Aktionen ordnungsgemäß funktionieren, können Sie auf der Seite *Diag >> Test >> Check Action* manuell die Buttons *Trigger* betätigen. Mit diesen Schaltflächen ist es möglich, sämtliche Meldungen der eingeschalteten Aktionen ohne Eintreten der definierten In-Events auszulösen.



No	Name	Test
1	Watchdog scharfgeschaltet, Meldung erfolgt.	Trigger
2	Watchdog zugeschlagen, Meldung erfolgt.	Trigger
3	Trap vom AD-Gerät erkannt.	Trigger
11	Action 11 Button 7 Output 1 ein	Trigger
12	Action 12 Button 8 Output 1 aus	Trigger

last update: Do, KW04, 27.01.2011 11:22:11 *

zurück zur Web-IO Homepage

Mit Betätigung der Taste *Trigger* signalisieren Sie dem Gerät, dass die für die Aktion auslösende Bedingung eingetreten ist. Die Erreichbarkeit verknüpfter Einträge aus der *Event-List* (Watch List) ist hierbei irrelevant, die tatsächliche Auslösebedingung sollte allerdings nicht gleichzeitig erfüllt sein.

Wurde über die Schaltfläche *Trigger* ein künstlicher Trigger gesetzt, ist der Auslösezeitpunkt auf der Seite *home.htm* und natürlich in der History List dargestellt.

6.5 LED

Zur Identifizierung des Gerätes vor Ort können 2 LEDs für 5s eingeschaltet werden, die durch die linke Gehäuse-Seite zu erkennen sind. Die LEDs auf der Frontplatine werden durch diese Funktion nicht beeinflusst.

7 Dokumentation

Die Dokumentation finden Sie im Konfigurationsbaum unter:

Doc

7.1 Manual

Erläuterung der Loginstufen und wichtiger Konfigurationen.

Willkommen beim Wiesemann & Theis IP-Watcher 2x2 Digital An dieser Stelle möchten wir Ihnen eine kurze Einführung für den Umgang mit dem IP-Watcher und dessen Konfiguration geben.	
Login	Es gibt drei Nutzungsstufen, die je nach Login, unterschiedliche Zugriffsrechte erlauben: • **User ohne Rechte** ist jeder, der die Webseite des IP-Watchers aufruft. Es kann nur gelesen werden. • **Admin** Login erlaubt sowohl die Bedienung der Alarme als auch die volle Konfiguration. • **Operator** Login erlaubt die Bedienung der Alarme und die Konfiguration der Alarmausgaben. Das Login erfolgt abhängig vom Passwort unter dem **Menüpunkt Config** Wurde kein Passwort vergeben (Werkseinstellungen), bekommt der Benutzer bei Login immer Admin-Rechte.
Konfiguration	Die Grundkonfiguration erfordert **Admin Login**. Die vielfältigen Funktionen des IP-Watchers bringen auch eine Fülle an Konfigurationsmöglichkeiten mit sich. Lassen Sie davon nicht irritieren! Arbeiten Sie den Navigationsbaum einfach von oben nach unten ab, und überspringen Sie die Punkte die für Ihre Applikation nicht benötigt werden. Die dem IP-Watcher beiliegende **Kurzanleitung** zeigt Ihnen, welche Punkte für welche Betriebsart zu beachten sind. **Die wichtigsten Konfigurationspunkte sind**: • **Netzwerkeinstellungen** Config >> Device >> Basic Settings >> Network Geänderte Einstellungen werden durch Klick auf "Zwischenspeichern" an den IP-Watcher übertragen. Alle Änderungen werden erst nach Logout und Speichern wirksam. Über Config >> Session Control >> Logout >> Restore Defaults kann der IP-Watcher auf Werkseinstellungen zurückgestetzt werden.
Weitere Informationen finden Sie in der dem IP-Watcher beiliegenden Kurzanleitung. Ein ausführliches Referenzhandbuch steht unter www.wut.de auf der Datenblattseite des IP-Watchers zum Download zur Verfügung.	

Abb.: Kurzanleitung „Manual“

7.2 Datasheet

Das Datenblatt gibt Auskunft über die wichtigsten Eigenschaften und technischen Daten des Trap-Receivers.

7.3 Manufacturer

Hier können spezielle Einträge des Betreibers oder Wiederverkäufers vorgenommen werden.

7.4 Property

Auf der Seite *Property* sind Informationen über den Hersteller, die Hard- und Softwareversion und die Identifikation des Gerätes im Netzwerk zu finden.

8 Anhang

8.1 LEDs

Im Folgenden ist die Bedeutung und Funktion der auf der Vorderseite des Trap-Receivers angeordneten LEDs erläutert.

8.1.1 Power-LED

Signalisiert das Anliegen der Versorgungsspannung. Sollte die LED nicht leuchten, überprüfen Sie bitte den korrekten Anschluss der Spannungsversorgung.

8.1.2 Status-LED

Blitzt bei jeglicher Netzwerkaktivität des Web-Gerätes auf. Periodisches Blinken signalisiert, dass der Port eine Verbindung zu einem anderen Teilnehmer hat.

8.1.3 Error-LED

Die Error-LED weist durch unterschiedliche Blinkcodes auf Fehlerzustände am Gerät oder Netzwerkport hin.

1xBlinken: Netzwerkanschluss überprüfen. Das Web-Gerät empfängt keinen Link-Impuls von einem Hub/Switch. Überprüfen Sie das Kabel oder den Hub/Switch-Port.

2x bzw. 3xBlinken: Führen Sie durch Unterbrechen der Versorgungsspannung einen Gerätereset durch. Sollte der Fehler nicht behoben sein, setzen Sie das Gerät auf die Factory Defaults zurück. Da alle Netzwerkeinstellungen zurückgesetzt werden, sollten Sie sich diese zuvor notieren.

Leuchten die LEDs Power, Status und Error gleichzeitig, konnte der nach jedem Start und Reset des Gerätes durchführte Selbsttest nicht korrekt beendet werden. Ursache hierfür könnte ein unvollständiges Firmwareupdate sein. Das Web-Gerät ist in diesem Zustand nicht mehr betriebsfähig. Senden Sie das Gerät bitte über Ihren Fachhändler oder direkt zur Überprüfung an W&T.

8.2 Factory Defaults

Erfordert es die Situation, muss der Trap-Receiver auf seine Werkseinstellungen, die Factory Defaults, zurückgesetzt werden. Dies kann auf verschiedene Arten getan werden:

- über das Web-Based Management
- über den SNMP-Zugang
- über das Brücken der Reset-Jumper

Das Wiederherstellen der Factory Defaults setzt das Gerät in den Auslieferungszustand zurück. Notieren Sie sich vorher sämtliche Einstellungen, um die Konfiguration anschließend wieder rekonstruieren zu können. Außerdem ist es ratsam, die fertige Konfiguration aus dem Gerät zu laden und extern zu sichern.

8.2.1 Web-Based Management

Um die Factory Defaults über das Web-Based Management wiederherzustellen, loggen Sie sich auf den Konfigurationsseiten ein und navigieren Sie zu der Position

```
Config >> Session Control >> LogOut
```

Auf der im Hauptfenster dargestellten Seite können Sie durch Drücken des Buttons *Restore Defaults* die Werkseinstellungen des Gerätes wiederherstellen.

8.2.2 SNMP-Zugang

Wenn Sie über SNMP das Gerät konfigurieren und eine Session als Administrator geöffnet haben, können Sie mit wtTrapReceiver2x2SessCntrlLogout SET 3 das Gerät auf Factory Defaults zurücksetzen (s. Besonderheiten bei SNMP / MIB-Browser).

8.2.3 Reset-Jumper

Können die Factory Defaults nicht über das Webinterface wiederhergestellt werden, besteht die Möglichkeit, die Werkseinstellungen über das Brücken der Reset-Jumperkontakte einzuspielen.

Hierzu muss das Gerät durch Herausziehen der Platinen samt Frontblende geöffnet werden.

Trennen Sie unbedingt vorher die Spannungsversorgung vom Gerät. Der Trap-Receiver kann sonst beschädigt werden.

Auf der größeren Platine befinden sich in einer Ecke vier offene Jumperkontakte. Schließen Sie die Kontakte mit den zwei Jumpern.

Legen Sie für ca. 15s die Spannungsversorgung an den Trap-Receiver an. Das Gerät wird jetzt in seinen Auslieferungszustand zurückgesetzt. Die LEDs an der Front flackern während dieses Vorgangs unregelmäßig.

Nachdem die Werkseinstellungen wiederhergestellt sind, trennen Sie die Spannungsversorgung, entnehmen die Jumper und schließen das Gerät. Beginnen Sie nun mit der Inbetriebnahme.

8.3 Alternative IP-Adressvergabe

Im Folgenden werden Methoden erläutert, mit denen dem Gerät alternativ zum Programm *WuTility* eine IP-Adresse zugewiesen werden kann.

8.3.1 ARP-Kommando

Voraussetzung ist ein PC, der sich im gleichen Netzwerksegment wie der Trap-Receiver befindet und auf dem TCP/IP installiert ist. Lesen Sie die MAC-Adresse des Trap-Receivers am Gerät ab (z.B. EN=00C03D004a05).

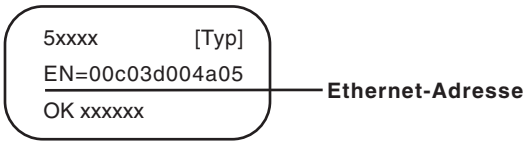


Abb.: Ethernet-Adresse auf dem Sticker auf der Geräteseite

Unter Windows führen Sie zunächst einen *Ping* auf einen anderen Netzwerkteilnehmer aus und fügen dann mit der nachfolgend beschriebenen Kommandozeile einen statischen Eintrag in die ARP-Tabelle des Rechners ein:

```
arp -s <IP-Adresse> <MAC-Adresse>
```

z.B. unter Windows:

```
arp      -s      172.0.0.10      00-C0-3D-00-12-FF
```

z.B. unter SCO UNIX:

```
arp -s 172.0.0.10 00:C0:3D:00:12:FF
```

Führen Sie nun einen *Ping* auf das Gerät aus, hier:

```
ping 172.0.0.10
```

Die IP-Adresse ist jetzt im nichtflüchtigen Speicher abgelegt.

Diese Methode ist nur ausführbar, wenn noch keine IP-Adresse an das Web-IO vergeben wurde, der Eintrag also 0.0.0.0 lautet. Zum Ändern einer bereits bestehenden IP-Adresse müssen Sie das Konfigurationsmenü über den Browser aufrufen.

8.3.2 RARP-Server (nur UNIX)

Die Arbeit mit einem unter UNIX aktivierten RARP-Server basiert auf Einträgen in den Konfigurationsdateien */etc/ethers* und */etc/hosts*. Erweitern Sie zunächst */etc/ethers* um eine Zeile mit der Zuordnung der Ethernet-Adresse des Web-Gerät zur gewünschten IP-Adresse. In */etc/hosts* wird dann die Verknüpfung mit einem Aliasnamen festgelegt. Nachdem Sie das Gerät im Netzwerksegment des RARP-Servers angeschlossen haben, können Sie über das Netzwerk die gewünschte IP-Adresse an das Gerät vergeben.

Ihr Web-Gerät hat zum Beispiel die MAC-Adresse *EN=00C03D0012FF* (Aufkleber auf dem Gerät) und soll die IP-Adresse *172.0.0.10* und den Aliasnamen *WT_1* erhalten.

Eintrag in der Datei */etc/hosts*: 172.0.0.10 WT_1