Handbuch
IP-Watcher 2x2 Digital PoE

W&T

Typ	IP-Watcher 2x2 Digital PoE
Modell	#57655
Release	DE 3.18 05/2010 PA

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!

W&T

Inhalt

W&T

1. Einführung

Der IP-Watcher von W&T ermöglicht die Überwachung von Netzwerkkomponenten durch zyklisches Ansprechen. Ist ein Gerät nicht mehr erreichbar, kann dieser Zustand durch die Auslösung von lokalen oder entfernten Alarmen gemeldet werden. Lokale Alarme signalisieren die fehlende Erreichbarkeit durch das Schalten eines angeschlossenen Verbrauchers an einen der zwei digitalen Ausgänge. Ein entfernter Alarm wird zum Beispiel per Mail, FTP, SNMP oder Syslog über ein TCP/IP-Netzwerk abgesetzt.

Für alle Alarme kann eine individuelle Quittierung konfiguriert werden. Diese erfolgt entweder über die Beschaltung von einem der digitalen Eingänge des Gerätes (Hardwarequittierung) und/oder über das Senden eines Quittierungsbefehls via TCP/IP über die Steuerungsseite an den IP-Watcher (Softwarequittierung). Eine Quittierung stellt die ordnungsgemäße Erkennung und Behandlung einer Alarmsituation durch einen Bediener sicher.

Ein integrierter Webserver stellt Konfigurationsseiten zur Einstellung der Geräteparameter zur Verfügung. Das Bedienen und Beobachten der Alarme erfolgt über eine browserbasierte Software, die ebenfalls vom Webserver des IP-Watchers in jeden Browser geladen werden kann. Diese Software zeigt in einer selbstaktualisierenden Darstellung den derzeitigen Zustand der aktivierten Alarme an und sie bietet die Möglichkeit, eine Quittierung anstehender Alarme durchzuführen.

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

Durch seine Eigenschaften eignet sich der IP-Watcher besonders gut für autarke Überwachungsaufgaben. Das Schalten eines Ausgangs im Alarmfall kann lokal alarmieren, zum Beispiel mit einer Rundumleuchte. 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 zusätz-

liche 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 IP-Watcher in Ihr Netzwerk einzubinden und in Betrieb zu nehmen, sind nur wenige Schritte notwendig.

2.1 Spannungsversorgung

Im Folgenden sind die zwei Möglichkeiten beschrieben, den IP-Watcher 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 IP-Watchers 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 sehr schlechte Wirkungsgrad des Netzteils und die damit verbundene erhöhte Stromaufnahme zu beachten.

2.1.2 Spannungsversorgung über PoE

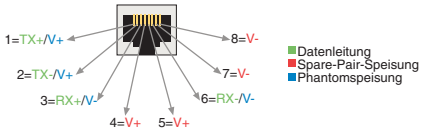
Der IP-Watcher ist für den Einsatz in Power over Ethernet-Umgebungen gemäß IEEE802.3af ausgerüstet. Die Spannungsversorgung erfolgt hierbei durch die Netzwerkinfrastruktur über den RJ45-Anschluss. Das Gerät unterstützt sowohl die Phantom-Speisung über die Datenpaare 1/2 und 3/6, wie auch die Spare-Pair-Speisung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

Um der versorgenden Komponente ein Powermanagement zu ermöglichen, identifiziert sich der IP-Watcher als Gerät der Leistungsklasse 1 mit einer Leistungsaufnahme von 0,44W bis 3,84W.

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

2.2 Netzwerkanschluss

Der IP-Watcher 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.



Belegung der RJ45-POE-Netzwerkbuchse

Ab Werk arbeitet der IP-Watcher 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.

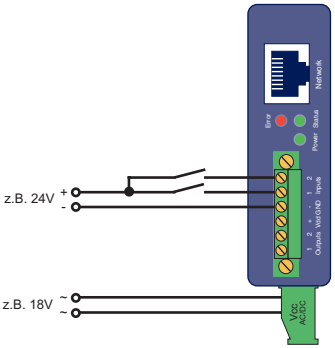
Dank der integrierten Power over Ethernet-Technologie, kann das Gerät über den Netzwerkanschluss mit der nötigen Betriebsspannung versorgt werden.

2.3 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 IP-Watcher 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.



Ansteuerung der zwei digitalen Inputs

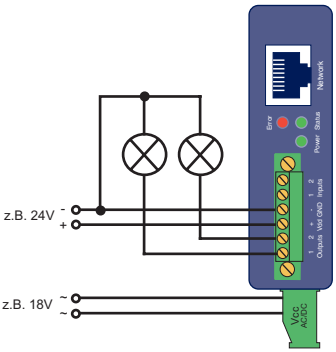
Sollen über die Inputs die Zustände potentialfreier Kontakte überwacht werden, kann auch die Versorgungsspannung des Gerätes als Signalspannung genutzt werden. In diesem Fall ist es erforderlich, den IP-Watcher mit einer Gleichspannung von 12V-30V zu betreiben.

2.4 Beschaltung der Outputs

Die zwei Outputs des IP-Watchers sind stromtreibend. Die 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.



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 Geräteversogungsspannung überschreitet den Bereich der schaltbaren Outputspannung. Nutzen Sie die Geräteversorgung auch für die Versorgung der Outputs, versorgen Sie das Gerät höchstens mit 30V.

In der Konfiguration des Gerätes ist auch einstellbar, dass die Versorgungsspannung des IP-Watchers intern auf die Klemmen Vdd und GND geschaltet wird. Dann Fall ist eine externe Hilfsspannung nicht erforderlich. Jeder Output kann bei aktivierter, interner Hilfsspannung mit maximal 150mA belastet dern.

2.5 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.

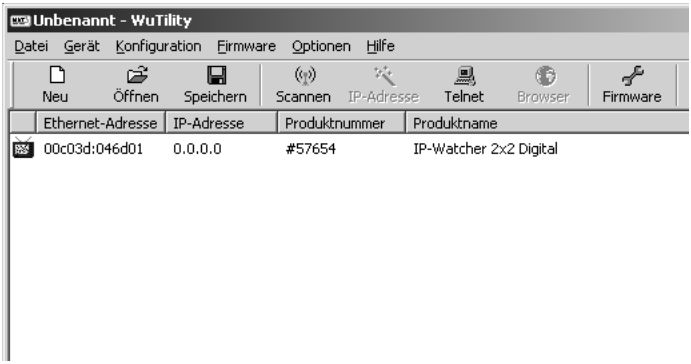
Die vergebene IP-Adresse muss netzwerkweit eindeutig sein.

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* 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 IP-Watcher befinden. Beide Geräte müssen an das Netzwerk angeschlossen sein.

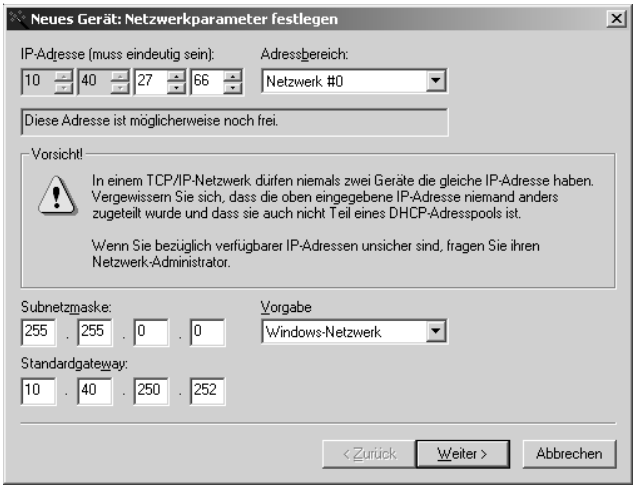
Beim Start durchsucht das *WuTility* automatisch das lokale Netzwerk nach angeschlossenen W&T-Netzwerkgeräten und zeigt diese in einer Inventarliste an. Der Scanvorgang lässt sich beliebig oft durch Betätigen der Schaltfläche *Scannen* wiederholen.

Wählen Sie aus der angezeigten Liste nun den IP-Watcher 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:



WuTility mit gefundenem W&T Netzwerkgerät

Über die Schaltfläche *IP-Adresse* erreichen Sie den Dialog zur Eingabe der gewünschten Netzwerkparameter. Bestätigen Sie die Eingabe mit *Weiter*:



Konfigurationsdialog für Netzwerkparameter

Aktivierung des BOOTP- oder DHCP-Clients, dann *Weiter*:

Konfigurationsdialog für Adressvergabeverfahren

Anschließend werden dem IP-Watcher 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.

2.6 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 IP-Watcher 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.

2.6.1 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 IP-Watcher 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*.

2.6.2 Systemname

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

2.6.3 Lease-Time

Die vom DHCP-Server bestimmte und übermittelte Lease-Time legt die Gültigkeitsauer der zugewiesenen IP-Adresse fest. Nach Ablauf der halben Lease-Time versucht der IP-Watcher 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 IP-Watcher 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
```

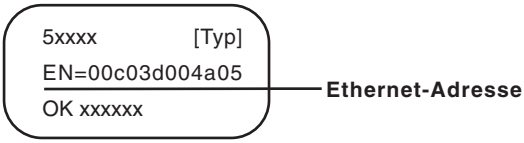
in Sekunden angezeigt.

Sollte nach Ablauf der zugewiesenen Lease-Time der DHCP-Server nicht erreichbar sein, löscht der IP-Watcher

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.

2.6.4 Reservierte IP-Adressen

Der IP-Watcher 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 IP-Watchers benötigt, so dass es in diesen Anwendungsfällen sinnvoll ist, auf dem DHCP-Server eine bestimmte IP-Adresse für den IP-Watcher 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.



Ethernet-Adresse auf dem Sticker auf der Geräteseite

2.6.5 Dynamische IP-Adressen

Eine völlig dynamische IP-Adressvergabe, bei welcher der IP-Watcher 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 Netzwerkungebung wenden Sie sich im Zweifel an Ihren Systemadministrator.

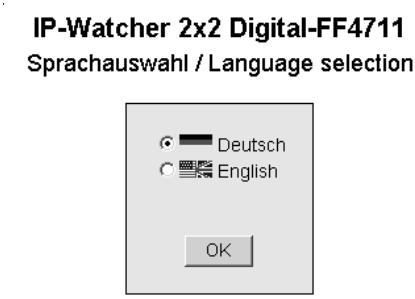
Für Timeserver-Anfragen, das Versenden von Emails oder andere Client-Anwendungen, bei denen das Gerät aktiv die Verbindung zu im Netzwerk befindlichen Server-Diensten sucht, kön-

nen auch dynamische, sich ändernde IP-Adressen genutzt werden.

2.7 Sprachauswahl

Beim ersten Aufruf einer der Steuerungsseiten (*home.htm*, *user.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.



Sprachauswahl bei Erstinbetriebnahme

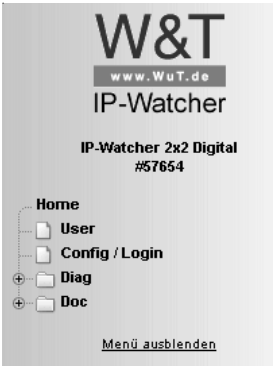
2.8 Vergabe der Basis-Netzwerkparameter

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

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

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

Wählen Sie den Menüpunkt *Config/Login*.

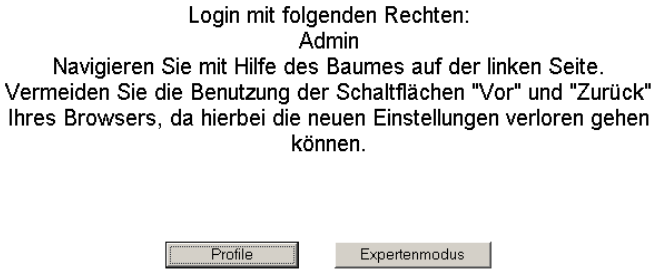


Konfigurationsmenü im Grundzustand

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.

Logindialog

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



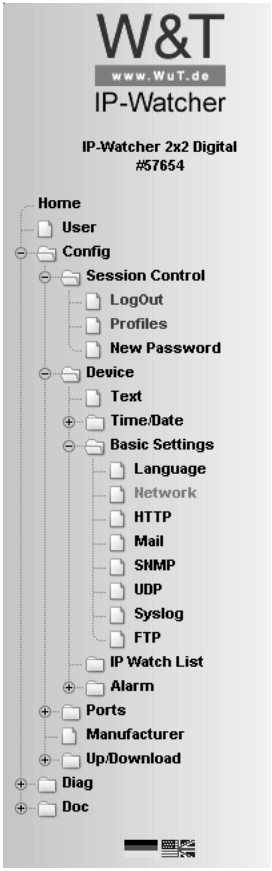
Auswahl für Profile oder Expertenmodus

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

Profilauswahl

Das Gerät zeigt jetzt blau hinterlegt die nötigen Menüpunkte an, die für die Konfiguration des gewählten Profiles angepasst wer-

den müssen. Über die rot hinterlegten Menüpunkte *Logout* und *Profiles* können Änderungen gespeichert oder verworfen werden, oder ein neues Profil zur weiteren Konfiguration des IP-Watchers dargestellt werden.



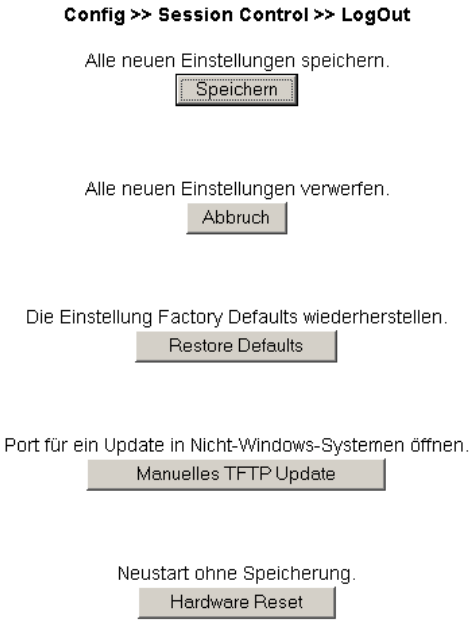
Konfigurationsmenü mit aktivierter Profilunterstützung

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*.

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.



Logoutoptionen

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

3 Bedienen und Beobachten aus dem Browser

Ist der IP-Watcher mit den nötigen Basis-Netzwerkparametern konfiguriert und an das Netzwerk angeschlossen, kann die weitere Konfiguration und das Bedienen und Beobachten des Gerätes aus dem Browser erfolgen.

3.1 Adressen

Es gibt vier Seiten, die Sie direkt aus dem Browser adressieren können. Im Folgenden sind die URLs kurz erläutert und aufgelistet.

Die Hauptseite (Home-Seite) stellt selbstaktualisierend den Zustand der konfigurierten Alarme dar und bietet für eingeloggte Bediener die Möglichkeit, Alarme via Softwarequittierung zu bestätigen:

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

Folgender Link ruft die Home-Seite, wie oben beschrieben, mit eingeblendetem Konfigurationsmenü auf:

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

Die User-Seite zeigt, ebenfalls zyklisch aktualisierend, den Zustand der IOs und aller Alarme an:

```
http://<IP-Adresse des IP-Watchers>/user.htm
```

Diagnosemeldungen können unter folgender Adresse abgerufen werden:

```
http://<IP-Adresse des IP-Watchers>/diag.htm
```

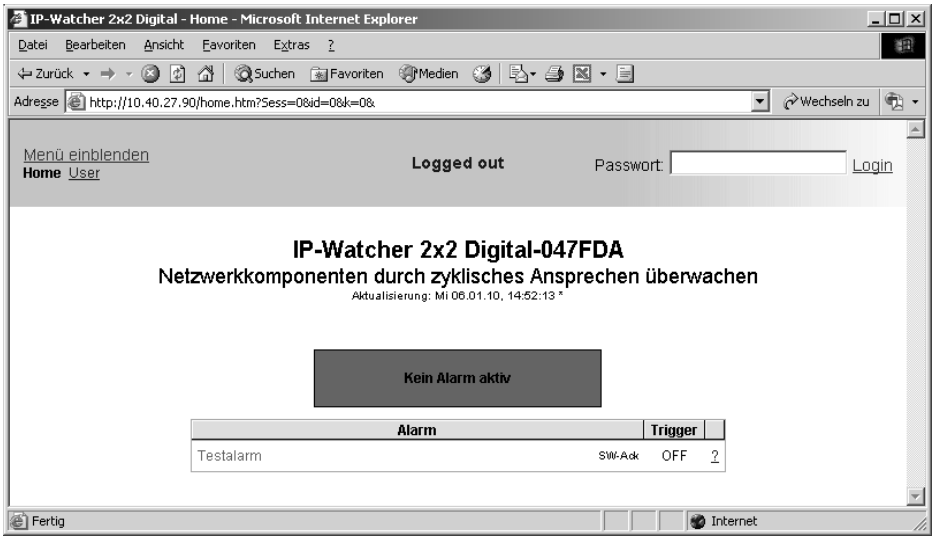
3.2 Home-Seite

Die Home-Seite, die mit der Adresse

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

aufgerufen werden kann,

- bietet eine Übersicht über den Status aller konfigurierten Alarme.
- ermöglicht, anstehende Alarme via Softwarequittierung zurückzusetzen.



Home-Seite im Ausgangszustand

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

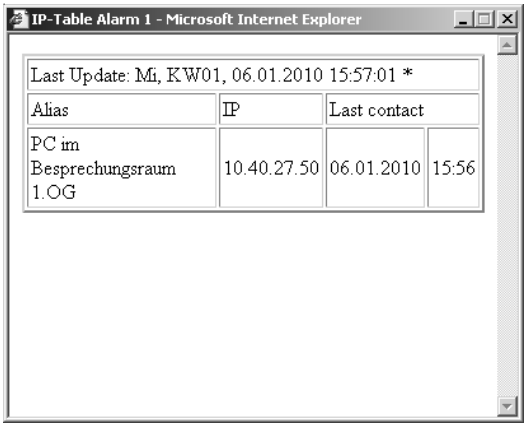
Die dargestellten Informationen werden einmal pro Sekunde aktualisiert. Dies geschieht automatisch, ohne Eingriff des Benutzers. Der Zeitpunkt der jeweils letzten Aktualisierung ist unter den Überschriften dargestellt. Bei der dort abgebildeten Zeit

handelt es sich um die Systemzeit des IP-Watchers. Wird die Zeitangabe mit einem hochgestellten Sternchen abgeschlossen, ist die Systemuhr des Gerätes mit dem in der Konfiguration eingestellten Timeserver synchronisiert.

Unter der Aktualisierungszeit befindet sich eine Meldebox, die zusammengefasst den Status aller konfigurierten Alarme wiedergibt. Ist kein Alarm ausgelöst, ist der Hintergrund der Box grün und die Meldung *Kein Alarm aktiv* wird dargestellt. Sind ein oder mehrere Alarme aktiv, wechselt die Hintergrundfarbe nach rot und die Anzahl der aktiven Alarme wird abgebildet. Wurden über die Testseite im Konfigurationsmenü ein oder mehrere Alarme zu Testzwecken manuell ausgelöst, wird zusätzlich auch diese Information visualisiert. Die Meldebox dient dazu, beim ersten Blick auf die Seite eine Übersicht über den Gesamtstatus zu erhalten. Die farbliche Hinterlegung unterstützt hierbei eine schnelle Wahrnehmung der Situation.

Hauptbestandteil der Home-Seite ist die Übersicht der konfigurierten Alarme. Die Tabelle stellt für jeden Alarm folgende Informationen dar:

- Symbolischen Namen, der über das Konfigurationsmenü vergeben werden kann.
- Information, ob gerade der künstliche Trigger über die Alarm Test-Seite gesetzt ist (rot blinkend).
- Möglichkeiten der Quittierung (Software-, Hardware-Ack).
- Zustand der Auslösebedingung.
- In eingeloggtem Zustand und konfigurierter SW-Quittierung eine Schaltfläche zur Alarmbestätigung. Ist keine SW-Quittierung eingestellt, wird dies textuell dargestellt.
- Ein verlinktes Fragezeichen, über das Detailinformationen zu derzeit nicht ansprechbaren Geräten aufgerufen werden können.



Detailinformationen zu aktuell nicht ansprechbaren Komponenten

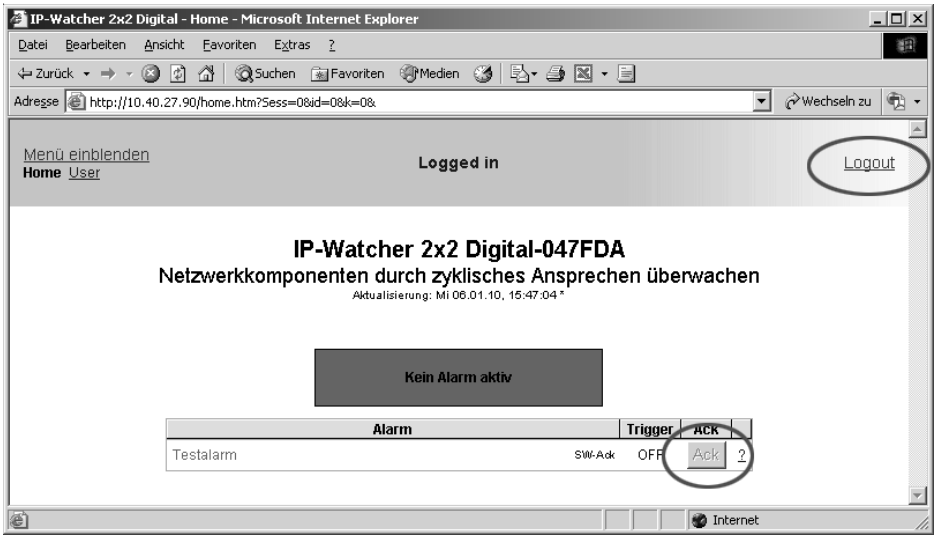
In ausgeloggtem Zustand dient die Seite lediglich zu Beobachtungszwecken. Es ist kein Zugriff auf die Quittierungsschaltflächen möglich. Ein Login mit Operator- oder Administratorrechten ändert dies.

Nach erfolgreichem Login ändert sich die Benutzeroberfläche wie folgt:

- In jeder Zeile erscheint entweder die Schaltfläche zum Quittieren eines anstehenden Alarms oder die Information, dass keine SW-Quittierung konfiguriert ist.
- Die Kontrollelemente für den Loginvorgang am oberen Bildrand werden durch einen Link zum Verlassen des eingeloggten Zustandes ersetzt.

Der symbolische Name der Alarme wird entsprechend dem aktuellen Alarmzustand dargestellt. Wurde der Alarm ausgelöst, ist der Name rot und fett geschrieben; im Ruhezustand ist er grün, in normaler Schriftdicke.

Steht ein Alarm an, der via Softwarequittierung bestätigt werden kann, kann dieser über die entsprechende Quittierungstaste bedient werden.



Home-Seite in eingeloggtem Zustand mit markierten Änderungen

Wird ein Alarm quittiert, fällt er unverzüglich ab, auch wenn der Trigger (Auslösebedingung) nach wie vor ansteht. Eine Wartezeit bis zu einer erneuten Auslösung kann in der Alarmkonfiguration eingestellt werden.

3.3 User-Seite

Die User-Seite bietet einen Überblick über den Zustand der

- Eingänge
- Ausgänge
- aktivierten Alarme

Der Aufruf der Seite erfolgt, wenn nicht über das Anklicken von Links, über die Eingabe folgender Adresse:

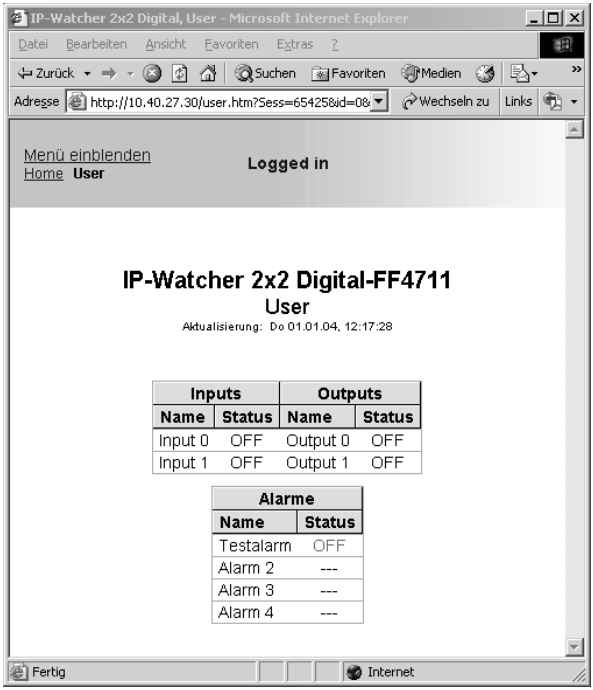
```
http://<IP-Adresse des IP-Watchers>/user.htm
```

Die Darstellung aktualisiert sich zyklisch einmal pro Sekunde. Der Zeitpunkt der letzten Aktualisierung ist über den Tabellen

dargestellt. Die dort abgebildete Zeit ist auch die Gerätezeit des IP-Watchers.

Die Verweise in der linken oberen Ecke erlauben das Einblenden des Konfigurationsmenüs und das direkte Navigieren zu der Home-Seite *(home.htm)*.

In den Übersichten werden aktivierte Inputs und Outputs grün markiert. In deaktiviertem Zustand sind sie schwarz. Alarme sind in aktiviertem Zustand rot, deaktiviert sind sie grün dargestellt.



User-Seite mit selbstaktualisierender Systemübersicht des IP-Watchers

In der Alarmübersicht wird nur der Status der aktivierten Alarme angezeigt. Die restlichen Alarme sind ausgegraut.

Wurde über das Konfigurationsmenü für einen Alarm ein künstlicher Trigger gesetzt, um die Meldungen für den Alarm auszulösen, blinkt in der Alarmübersicht der Hinweis *Test*. Befindet sich ein Alarm in diesem Zustand, muss der gesetzte Trigger

über die Konfigurationsseite erst wieder zurückgenommen werden, bevor das Gerät wieder aufgrund passender Eingangsbeschaltung Alarme auslöst.

3.5 Konfigurationsmenü ein- und ausblenden

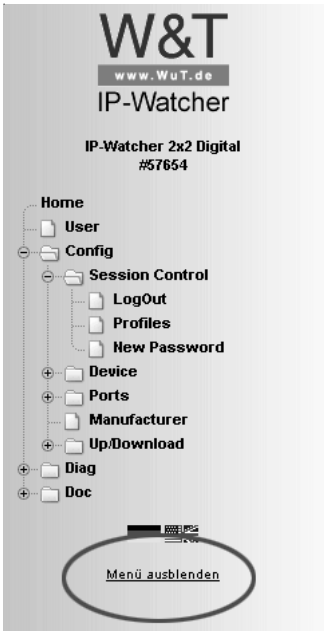
Ist das Konfigurationsmenü nicht sichtbar, bieten die Seiten

- Home (*home.htm*)
- User (*user.htm*)

jeweils in der linken oberen Ecke den Link *Menü einblenden*, um den Menübaum einzublenden..

Link zum Einblenden des Konfigurationsmenüs auf der Home-Seite

Neben dem Link zum Einblenden des Konfigurationsmenüs stellen die oben aufgezählten Seiten auch noch einen Link zum Aufrufen der jeweils anderen Steuerungsseiten zur Verfügung.



Link zum Ausblenden des Konfigurationsmenüs

Der Link zum Ausblenden des Konfigurationsmenüs ist nur dann unter dem Menübaum sichtbar, wenn im rechten Teil des Browsers eine der zwei Hauptseiten (*home.htm*, *user.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.

3.6 Login und Logout

Je nach Login unterscheidet der IP-Watcher zwischen drei verschiedenen Zugriffsberechtigungen:

- *Default User*: Diesen Status hat zunächst jeder Bediener, der ohne Passwort auf das Gerät zugreift. Der Status des IP-Watchers kann jetzt ausgelesen und dargestellt werden.

Alarme zu quittieren oder die Konfiguration zu verändern ist jedoch nicht möglich.

- *Administrator*: Das Administratorkennwort gewährt vollständigen Zugriff auf das Gerät. Die Manipulation der Konfiguration und das Quittieren von Alarmen ist jetzt möglich.
- *Operator*: Die Zugriffsrechte des Operators sind auf das Quittieren von Alarmen, das Ändern der Alarmausgaben, 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 nicht verfügbare Punkte werden 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.

Logindialog auf einer der drei 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 kann einen bereits bestehenden Login überschreiben. In diesem Fall wird der Benutzer während des Login-Vorgangs aufgefordert, den bereits bestehenden Login zu übernehmen.

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.

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.

4 Alarme

Im IP-Watcher können bis zu vier verschiedene Alarme festgelegt werden, deren Auslösung in Abhängigkeit von zu überwachenden Netzwerkkomponenten stehen. Je nach Status der Alarme können Meldungen ausgegeben werden. Dazu stehen verschiedene Netzwerkprotokolle zur Verfügung:

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

Des Weiteren ist es möglich, das beim Eintreten einer zuvor definierten Alarmbedingung auch lokal über das Schalten eines der integrierten digitalen Ausgänge zu melden.

Das Gerät bietet auch die Möglichkeit, quittierbare Alarme zu konfigurieren. Ein quittierbarer Alarm ist nach seiner Auslösung solange aktiv, bis eine Bestätigung eingeht, auch wenn die Auslösebedingung, der Trigger, inzwischen nicht mehr erfüllt ist. Die Quittierung kann per Software über die Seite *home.htm* und/oder per Hardware über die Beschaltung eines zuvor definierten Inputs erfolgen.

Für jeden Alarm können vier Meldungen definiert werden:

- Alarm ON: Wird gesendet, wenn der Alarm durch Eintreten der eingestellten Auslösebedingung aktiviert wird.
- Re-Trigger ON: Wird gesendet, wenn die Auslösebedingung nach einem Abfallen wieder erfüllt ist und der Alarm bereits von einem früheren Trigger aktiviert wurde und immer noch ansteht.
- Trigger OFF: Beim Abfallen der Auslösebedingung wird diese Meldung versendet.
- Alarm Ack: Ein Quittierung des Alarms veranlasst das Gerät, diese Meldung zu senden.

Wird über einen Alarm ein Output geschaltet, ist dieser bei nicht-quttierbaren Alarmen solange aktiv, bis die Auslösebedingung nicht mehr erfüllt ist. Bei quittierbaren Alarmen bleibt der Output bis zur Quittierung aktiv.

Damit ein Alarm ausgelöst werden kann, muss das Triggersignal für mindestens 25ms anstehen. Die Reaktion des IP-Watchers erfolgt...

- ...beim Schalten eines Ausgangs sofort.
- ...bei Mail-Alarmen alle 10s.
- ...bei allen anderen netzwerkbasierten Meldearten einmal pro Sekunde.

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

- Hat das System für einen quittierbaren Alarm eine Quittierung (ACK) empfangen, gilt dieser Alarmzyklus als abgeschlossen. Noch nicht gesendete Meldungen werden auch weiterhin zugestellt.
- Wird ein quittierter Alarm, dessen Meldungen noch nicht komplett versendet sind, erneut ausgelöst, werden alle Meldungen des alten Alarmzyklusses gelöscht. Mit der Aktivierung startet ein neuer Durchlauf, der sich nicht mit Meldungen von vergangenen und bearbeiteten Auslösungen vermischen soll.
- Erfolgt die Auslösung eines Alarms, der Triggerabfall und die Quittierung schneller als das Gerät diese Zustandsänderungen detektieren kann, ist ein geordneter Meldeablauf nicht mehr möglich. Wenn bei einem Alarm aufgrund einer zu hohen Beschaltungsfrequenz, die Quittierung nicht erfasst wird und der Alarm anschließend erneut auslöst, wird dieser Zustand als Re-Triggerung des Alarms gewertet.

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

4.1 IP Watch List

Auslösebedingung für einen Alarm ist stets das Nichterreichen einer Netzwerkkomponente. Bevor die Alarme im Detail konfiguriert werden, müssen die zu überwachenden Netzwerkkomponenten in die *IP Watch List* aufgenommen werden. Aus dieser zentralen Liste erfolgt später die Zuordnung der Komponenten zu den einzelnen Alarmen.

Die Verwaltung der IP-Adressen und Hostnamen erfolgt auf der Seite

`Config >> Device >> IP Watch List`

Hier finden Sie Funktionen zum...

- ...Einfügen neuer Geräte.
- ...Scannen eines Netzwerkbereiches
- ...Bearbeiten eines vorhandenen Eintrags.
- ...Löschen eines einzelnen Eintrags.
- ...Löschen aller Einträge.

Die *IP Watch List* kann maximal 250 Einträge aufnehmen.

Leere IP Watch List

4.1.1 Eintrag einfügen

Über den Button *Einfügen* gelangen Sie zu der Maske, über die neue Geräte in die *IP Watch List* aufgenommen werden können.

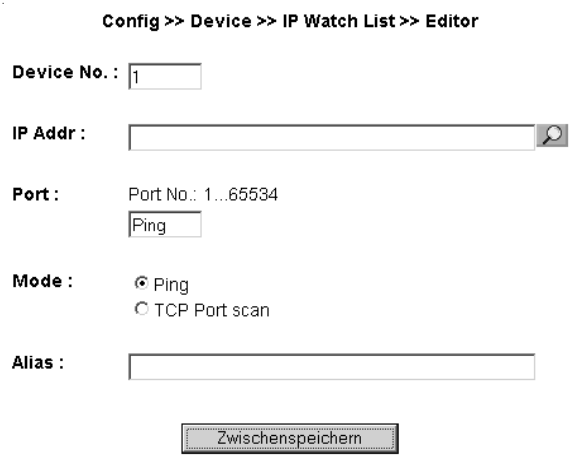
Der Wert *Device No.* bestimmt die Position des Gerätes in der Liste. Im Feld *IP Addr* geben Sie die IP-Adresse oder den Hostnamen des zu überwachenden Netzwerkteilnehmers an.

Der IP-Watcher unterstützt zwei Methoden, mit denen die zu überwachenden Netzwerkkomponenten zyklisch angesprochen werden können:

- Ping: Aussenden eines ICMP-"Echo Request", der gemäß der Protokolldefinition mit einem ICMP-"Echo Reply" beantwortet werden muss.
- Öffnen und Schließen eines TCP-Ports: Es wird ein frei wählbarer TCP-Port geöffnet und wieder ordnungsgemäß geschlossen.

Stellen Sie sicher, daß die gewählte Überwachungsmethode von dem Netzwerkteilnehmer unterstützt wird.

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



Netzwerkkomponente der IP Watch List hinzufügen

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

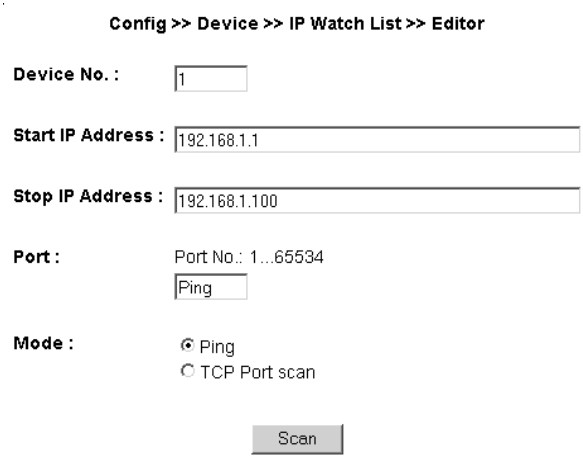
4.1.2 Automatisches Hinzufügen durch Scannen

Hinter der Schaltfläche *Scan* verbirgt sich ein Dialog, mit dessen Hilfe ein definierbarer Netzwerkbereich einmalig abgescannt werden kann. Hierbei werden alle IP-Adressen des vorgegebenen Adressbereichs entweder angeping oder durch Öffnen und Schließen eines wählbaren TCP-Ports angesprochen. Antwortet eine Adresse auf das Ansprechverfahren, nimmt der IP-Watcher diese in die *IP Watch List* auf.

Der Parameter *Device No.* legt die Position fest, ab der gefundene IP-Adressen in die Liste aufgenommen werden. Eventuell an dieser Position bereits gespeicherte Einträge werden nach hinten geschoben.

Tragen Sie in den Feldern *Start IP Address* und *Stop IP Address* die Grenzen des IP-Adressbereichs ein, der durchsucht werden soll. (Beispiel: 192.168.1.1 - 192.168.1.100).

Der Scanvorgang wird über die Schaltfläche *Scan* gestartet. Der Fortschritt eines laufenden Scans wird während des Vorgangs durch einen Statusbalken visualisiert.



Netzwerkbereich absuchen

4.1.3 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*.

4.1.4 Löschen

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

4.1.5 IP Watch List löschen

Das Betätigen der Schaltfläche *Alles löschen* entfernt alle Einträge aus der *IP Watch List*.

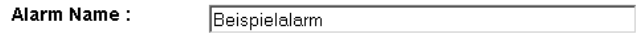
4.2 Alarme konfigurieren

Über das Konfigurationsmenü können Sie die zur Verfügung stehenden Alarme 1 - 4 parametrieren. Rufen Sie hierzu die Konfigurationsseite

```
Config >> Device >> Alarm >> Alarm X
```

auf.

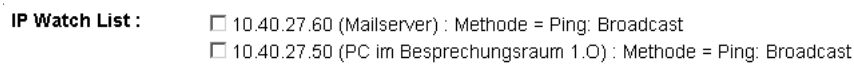
Geben Sie im Feld *Alarm Name* einen Namen für den Alarm ein. Dieser Name wird auf allen Steuer- und Bedienseiten angezeigt.



Die Checkbox *Alarm Enable* muss aktiviert sein, damit der Alarm bei Eintreten der Triggerbedingung ausgelöst wird. Soll der Alarm deaktiviert werden, muss lediglich die Checkbox wieder deaktiviert werden. Es ist dann nicht nötig die EInstellungen zu löschen.

Im Block *IP Watch List* finden Sie alle Netzwerkkomponenten, die Sie zuvor in die *IP Watch List* aufgenommen haben. Aktivieren

Sie die Checkbox vor den Einträgen, die durch den Alarm überwacht werden sollen.

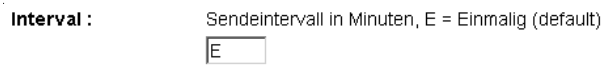


Ordnen Sie einem Alarm mehrere IP-Adressen zu, reicht eine nicht mehr ansprechbare IP-Adresse aus, um den Alarm auszulösen. Ist eine weitere Komponente nicht mehr ansprechbar, löst der Alarm erneut aus.

Über den Parameter *Trigger Count* legen Sie die Anzahl der erlaubten Ansprech-Fehlversuche fest.

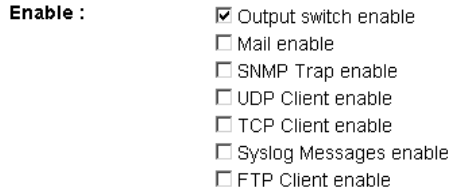
Der Wert *Polling Rate* bestimmt das Intervall in Sekunden, in dem die IP-Adressen und Hostnamen, die dem Alarm zugeordnet sind, angesprochen werden. Beachten Sie hier, dass der Versuch eine IP-Adresse anzusprechen bis zu fünf Sekunden dauern kann, wenn diese nicht mehr erreichabr ist.

Über das Feld *Interval* bestimmen Sie das Sendeinterval des Alarms. Voreingestellt ist *E*, was einem einmaligen Senden entspricht. Sie können hier beliebige Minutenangaben eintragen, nach denen sich der Alarm wiederholen soll.



Die Wiederholung erfolgt nur, solange der Alarm aktiv ist. Bei quittierbaren Alarmen bis zum ACK, ansonsten bis der Trigger abgefallen ist.

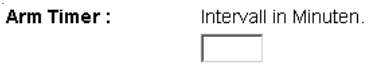
Der Block *Enable* enthält sämtliche Meldearten. Wählen Sie hier den Kommunikationsweg aus, über den der Alarm benachrichtigen soll.



Eine mögliche Quittierung kann im Block *Ack Enable* eingestellt werden. Ausgewählt werden kann eine Hardware- und/oder Softwarequittierung.

Wurde eine Hardwarequittierung ausgewählt, ist bei der Option *Hardware Ack Port* der Input anzugeben, der den Alarm bestätigt. Des Weiteren muss die Flanke bestimmt werden, auf die das ACK triggert.

Tragen Sie unter *Arm Timer* eine Wartezeit in Minuten ein, innerhalb derer der Trigger nach Quittierung des Alarms abfallen muss. Steht die Auslösebedingung nach der Quittierung noch länger als hier eingestellt an, löst der Alarm erneut aus.



Übernehmen Sie die Änderungen mit *Zwischenspeichern*.

4.3 Nachrichtentexte formulieren

Für die über das Netzwerk meldenden Benachrichtigungsarten können jeweils drei verschiedene Meldungen formuliert werden, die je nach Alarmstatus vom Gerät versendet werden:

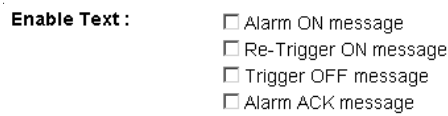
- Alarm ON message: Diese Nachricht wird mit der Aktivierung des Alarms versendet.

- Re-Trigger ON message: Steht der Alarm immer noch an, weil er noch nicht quittiert wurde, der Trigger ist aber schon abgefallen und löst erneut aus, wird diese Nachricht versendet.
- Trigger OFF message: Bei Abfall des Triggers wird diese Meldung verschickt.
- Alarm ACK message: Wird der Alarm quittiert, erfolgt der Versand dieser Meldung.

Die Konfiguration der verschiedenen Meldungen erfolgt auf den Unterseiten der einzelnen Alarme, zum Beispiel:

`Config >> Device >> Alarm >> Alarm 1 >> Mail`

Dort wählen Sie im Block *Enable Text* die zu versendenden Alarme.

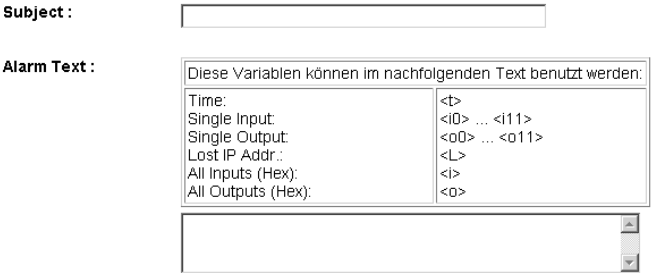


Auswahl der möglichen Meldungen für einen Alarm

In den Feldern *Subject* und *Alarm Text* tragen Sie den Betreff und den Nachrichtentext ein, der im Fall von *Alarm ON message* und *Re-Trigger ON message* versendet werden sollen.

Die Felder *Alarm Ack Subject* und *Alarm Ack Text* enthalten Betreff und Nachrichtentext für die Nachricht, die unmittelbar nach dem Quittieren eines Alarms versendet wird.

Bei *Trigger OFF Subject* und *Trigger OFF Text* tragen Sie die Betreffzeile und den Nachrichtentext ein, die beim Abfall des Triggers versendet werden sollen.



Betreff- und Nachrichteneingabe für aufkommenden Alarm und Re-Trigger

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.

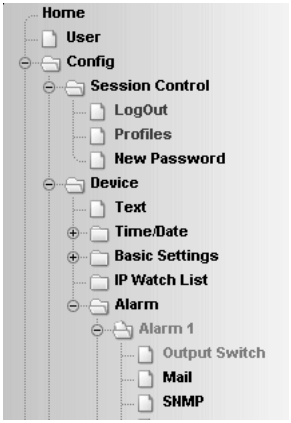
Alarm Variable	Beschreibung
<dn>	Device Name (siehe: Config >> Device >> Text)
<i>	Zustand der Inputs als Bitmuster in hexadezimaler Schreibweise
<i**x**>	Zustand des Inputs Nr. **x** (ON / OFF)
<in**x**>	Name des Inputs Nr. **x**
<o>	Zustand der Outputs als Bitmuster in hexadezimaler Schreibweise
<on**x**>	Name des Outputs Nr. **x**
<L>	Liste mit Detailinformationen zu allen nicht erreichbaren Geräten
<t>	Zeitstempel mit Datum und Uhrzeit im Format: TT.MMM.JJJJ hh:mm:ss
<$y>	Jahr im Format: JJJJ
<$m>	Monat im Format: MM
<$d>	Tag im Format: TT
<$h>	Stunde im Format: hh
<$i>	Minuten im Format: mm
<$s>	Sekunden im Format: ss
x liegt zwischen 0 und 1	

Mailtags zur dynamischen Gestaltung der Nachrichtentexte

Neben den Alarmmeldungen müssen auf den Nachrichtenseiten auch noch die für die Benachrichtigungsart spezifischen Parameter eingestellt werden. Genauere Informationen dazu finden Sie in den jeweiligen Kapiteln.

4.4 Lokale Alarmierung

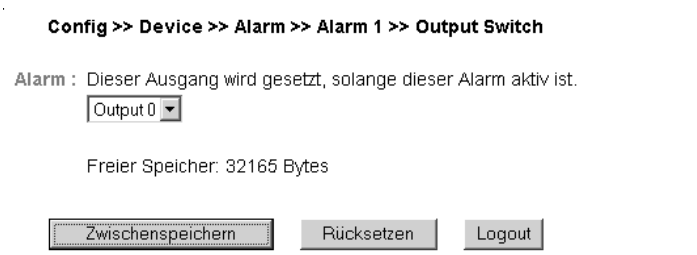
Zum Schalten eines digitalen Ausgangs im Alarmfall rufen Sie das Profil *Lokale Alarmierung* auf.



Profil „Lokale Alarmierung“

Konfigurieren Sie die Alarmbedingung für den gewünschten Alarm gemäß den im Kapitel *Alarme konfigurieren* erläuterten Schritten.

Auf der Unterseite *OutputSwitch* legen Sie den Ausgang fest, der im Alarmfall geschaltet werden soll. Der gewählte Ausgang ist bei quittierbaren Alarmen bis zum ACK aktiv, ansonsten bis die Triggerbedingung nicht mehr erfüllt ist.

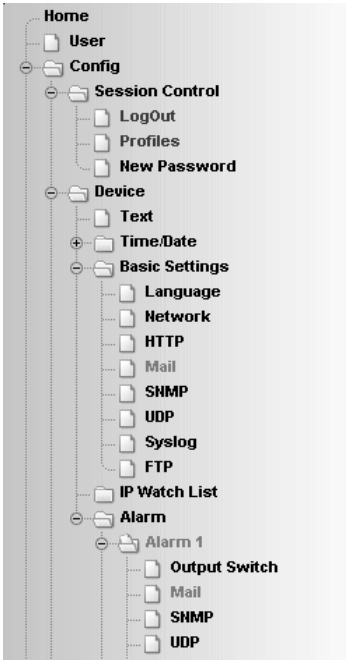


Definition des zu schaltenden Ausgangs

Übernehmen Sie die Änderungen mit *Zwischenspeichern*.

4.5 Alarmierung per E-Mail

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



Profil „Alarmierung per E-Mail“

Konfigurieren Sie die Alarmbedingung für den gewünschten Alarm gemäß den im Kapitel *Alarme konfigurieren* erläuterten Schritten.

4.5.1 Allgemeine Einstellungen

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 Alarmmail an einen oder mehrere E-Mail-Empfänger abzusetzen.

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. 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*.

4.5.2 Mailparameter und -texte

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

```
Config >> Device >> Alarm >> Alarm X >> Mail
```

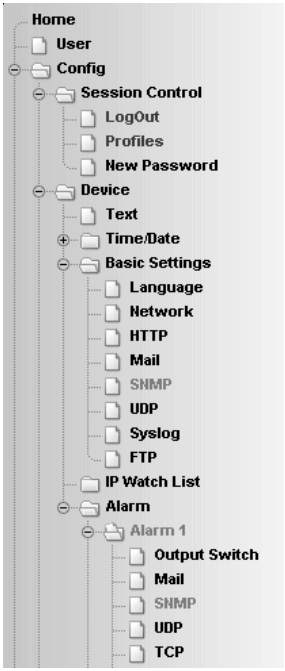
auf.

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*.

4.6 Alarmierung per SNMP-Trap

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



Profil „Alarmierung per Trap“

Konfigurieren Sie die Alarmbedingung für den gewünschten Alarm gemäß den im Kapitel *Alarme konfigurieren* erläuterten Schritten.

4.6.1 Allgemeine Einstellungen

Rufen Sie die Seite

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

auf.

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*.

4.6.2 SNMP-Parameter und -texte

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

```
Config >> Device >> Alarm >> Alarm X >> SNMP
```

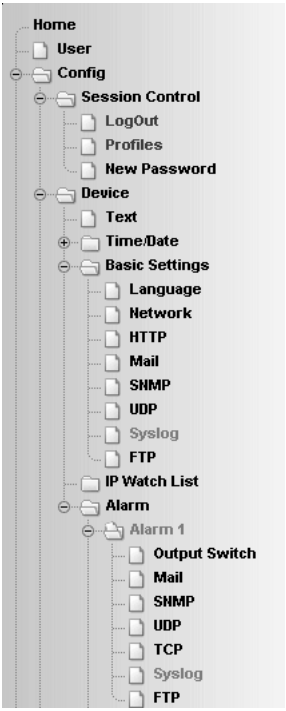
auf.

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

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

4.7 Alarmierung per Syslog

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



Profil „Syslog Messages incl. Alarmierung“

Konfigurieren Sie die Alarmbedingung für den gewünschten Alarm gemäß den im Kapitel *Alarme konfigurieren* erläuterten Schritten.

4.7.1 Allgemeine Einstellungen

Aktivieren Sie auf der Konfigurationsseite

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

die Option System Messages enable.

Diese Option schaltet die Syslog-Funktion im IP-Watcher frei und ermöglicht so das Versenden von Meldungen unter Verwendung des Syslog-Protokolls.

Übernehmen Sie die Änderungen mit *Zwischenspeichern*.

4.7.2 Syslog-Parameter und -texte

Tragen Sie auf der Seite

```
Config >> Device >> Alarm >> Alarm 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.

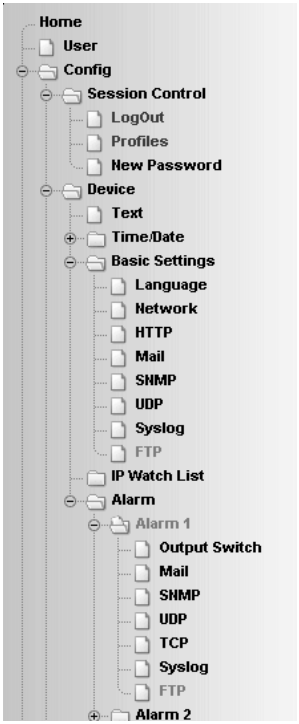
Zuletzt konfigurieren Sie die erforderlichen Nachrichtentexte wie im Kapitel *Nachrichtentexte formulieren* beschrieben und übernehmen die Änderungen mit *Zwischenspeichern*.

4.8 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 die Alarmbedingung für den gewünschten Alarm gemäß den im Kapitel *Alarme konfigurieren* erläuterten Schritten.



Profil „Alarmierung per FTP“

4.8.1 Allgemeine Einstellungen

Legen Sie auf der Seite

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

die Basisparameter für den Nachrichtenversand per FTP fest.

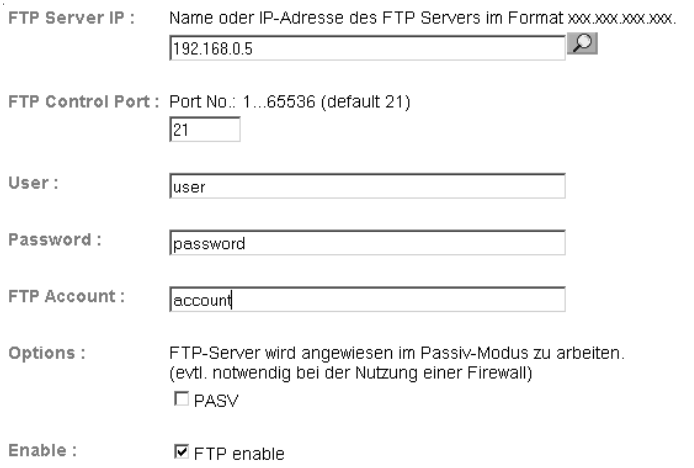
Tragen Sie bei *FTP Server IP* die IP-Adresse oder den Host-Namen (nur bei konfiguriertem DNS-Server) Ihres FTP-Servers ein, an den die Daten geschickt werden sollen.

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 das Web-Alarm 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.



FTP-Basiskonfiguration

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

4.8.2 FTP-Parameter und -texte

Tragen Sie auf der Seite

`Config >> Device >> Alarm >> Alarm X >> FTP`

die alarmspezifischen FTP-Parameter ein.

Legen Sie bei *FTP Local Data Port* den lokalen Datenport des Web-Alarm fest. Gültige Werte liegen zwischen eins und 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-Alarm Text.

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.

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*.

4.9 Alarmierung per TCP-Client

Konfigurieren Sie die Alarmbedingung für den gewünschten Alarm gemäß den im Kapitel *Alarme konfigurieren* erläuterten Schritten.

Tragen Sie auf der Seite

`Config >> Device >> Alarm >> Alarm 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*.

4.10 Alarmierung per UDP-Client

Aktivieren Sie auf der Seite

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

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

Konfigurieren Sie die Alarmbedingung für den gewünschten Alarm gemäß den im Kapitel *Alarme konfigurieren* erläuterten Schritten.

Tragen Sie auf der Seite

`Config >> Device >> Alarm >> Alarm 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 Grundeinstellungen

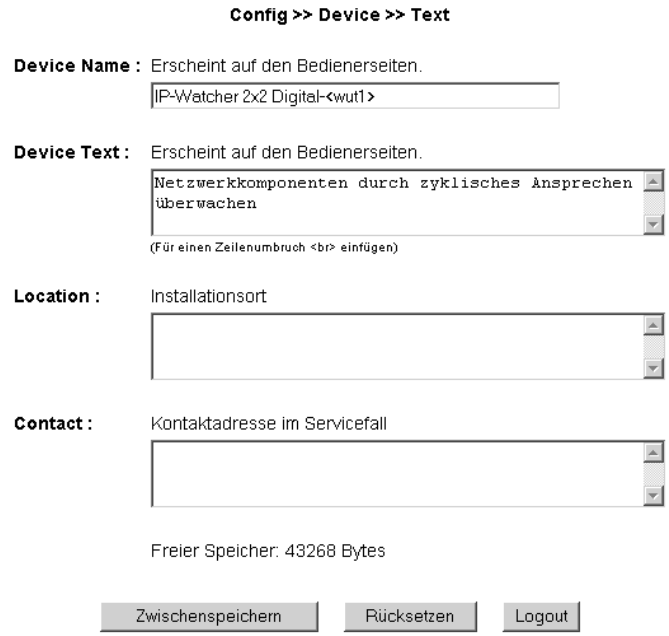
5.1 Gerätebezeichnung

Rufen Sie im Konfigurationsmenü die Seite

`Config >> Device >> Text`

auf, um folgende Texte zu editieren:

- Device Name: Name des IP-Watchers
- Device Text: nähere Gerätebeschreibung
- Location: Ort, an dem der IP-Watcher installiert ist
- Contact: Kontaktadresse im Servicefall

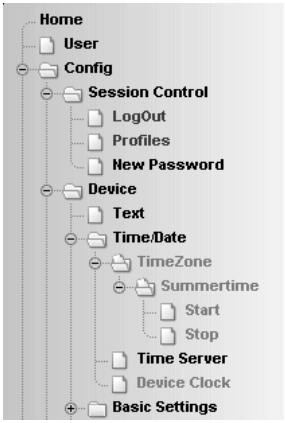


Konfigurationsseite für Gerätetexte

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

5.2 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.

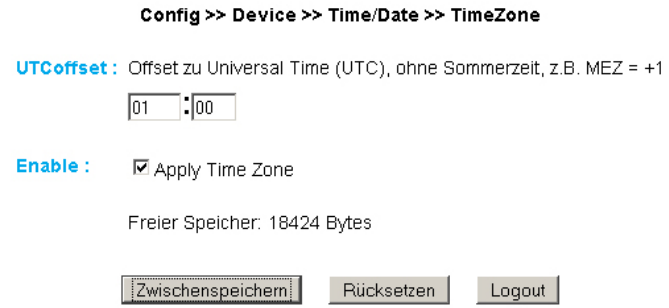


Konfigurationsbaum mit markiertem Profil für lokale Uhreinstellung

Die Systemuhr des IP-Watchers ist batteriegestützt. Dadurch behält das Gerät auch nach Wegfall der Versorgungsspannung die Uhrzeit. Achten Sie beim Wechsel von Batterien auf ordnungsgemäße Entsorgung.

5.2.1 Timezone

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



Zeitzonenkonfiguration

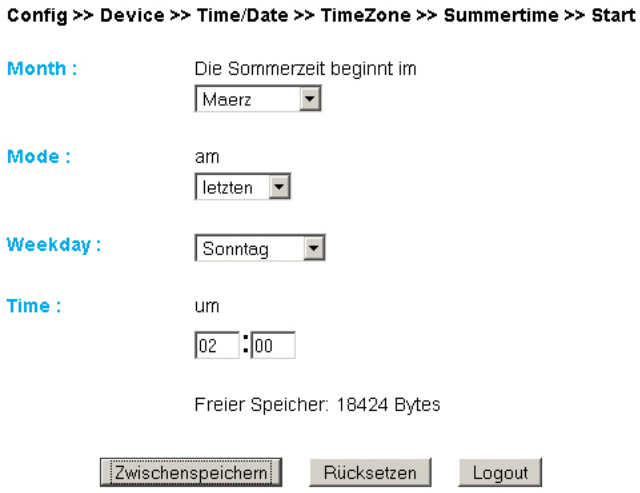
5.2.2 Summertime

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.

Einstellung der Sommerzeit

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

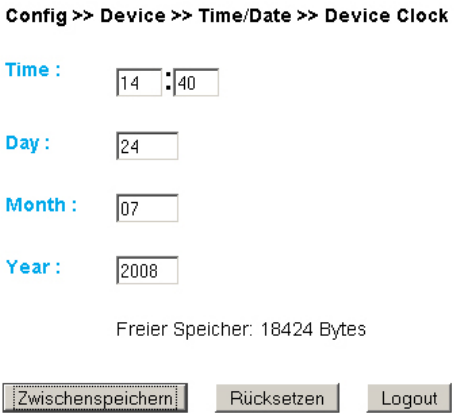
Werksseitig eingestellt beginnt die Sommerzeit am letzten Sonntag im März um 2:00 Uhr. Das Ende der Sommerzeit ist voreingestellt auf den letzten Sonntag im Oktober um 3:00 Uhr.



Regel für den Beginn der Sommerzeit

5.2.3 Device Clock

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



Manuelles Einstellen der Systemuhr

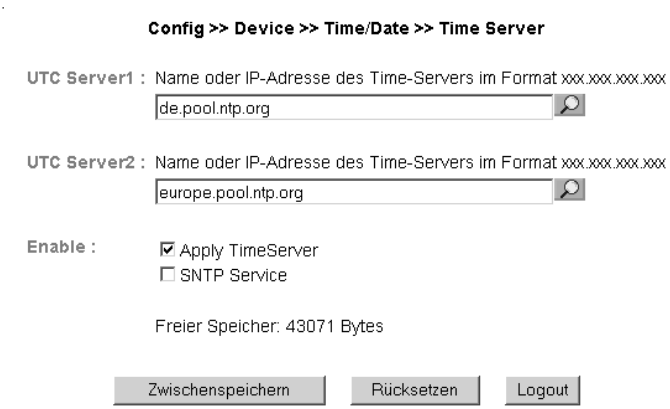
5.3 Automatische Uhreinstellung per Netzwerkdienst

Die Konfiguration der automatischen Einstellung der Systemuhr via Timeserver 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.



Optionen für Timeserver

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

Wenn Sie als Timeserver-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*.

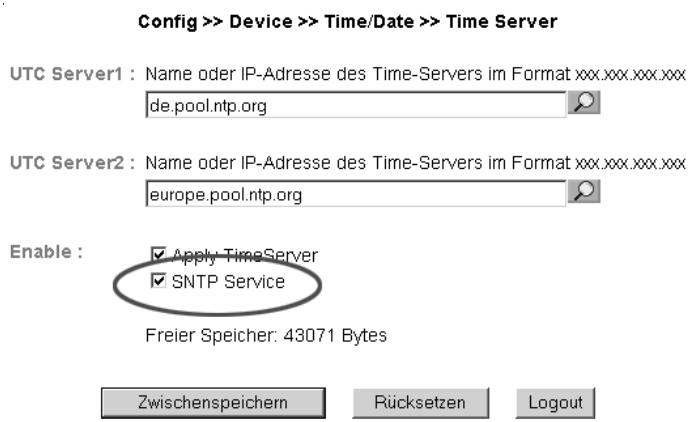
5.4 SNTP-Timeserver aktivieren

Ist die Systemzeit des Gerätes via Abgleich mit einem Timeserver synchronisiert, kann der IP-Watcher selber auch als Timeserver 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 >> Time/Date >> Time Server`

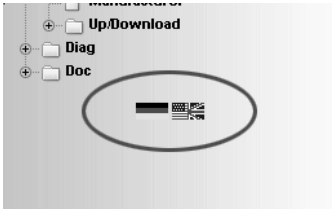


Timeserver-Dienst starten

5.5 Language

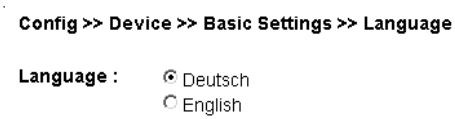
Sie können über das Konfigurationsmenü die Systemsprache des Gerätes bestimmen. Dies kann entweder über den Fahnen-Link unter dem Konfigurationsmenü erfolgen, oder navigieren Sie zu:

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



Fahnen-Link unter dem Konfigurationsmenü

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



Sprachauswahl

Für das Ändern der Sprache benötigen Sie Operator oder Administratorrechte.

5.6 HTTP-Port

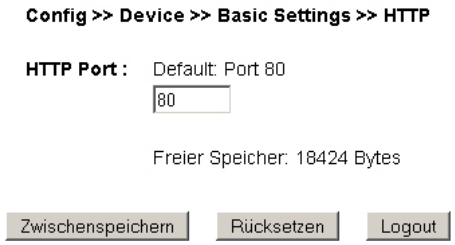
Auf der Seite

`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 IP-Watchers>/home.htm:<Portnummer>
```



Konfiguration der HTTP-Portnummer

5.7 System Traps via SNMP und SNMP-Basiskonfiguration

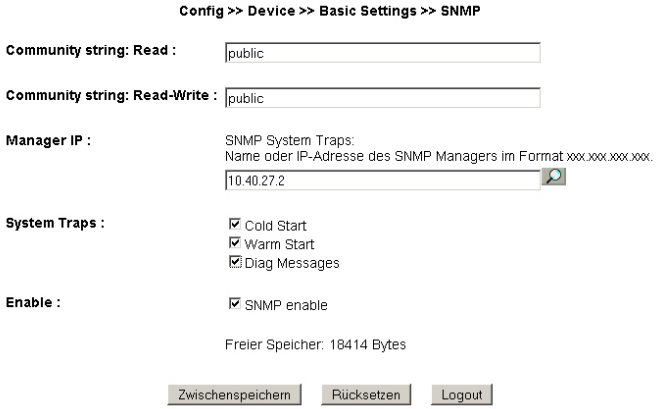
Folgende System Traps können mittels des SNMP-Protokolls an einen SNMP-Manager gesendet werden:

- 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
```



SNMP-Konfiguration

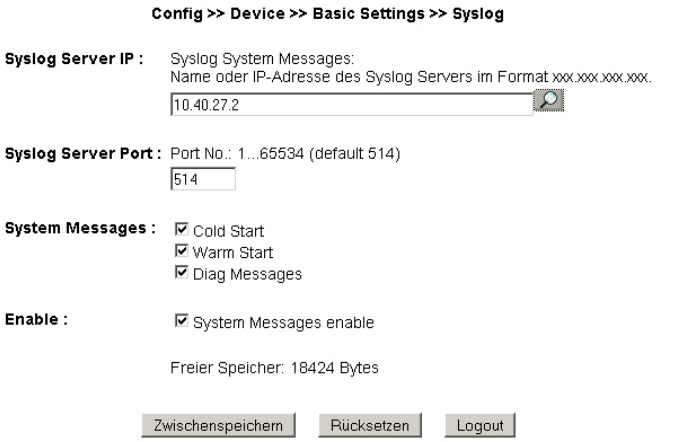
SNMP ist im Vergleich zu den anderen Benachrichtigungsverfahren defaultmäßig aktiviert.

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 Web-Alarm versendet.
- System Traps: Wählen Sie die Meldungen, die versendet werden sollen.
- Enable: Aktivieren Sie die SNMP-Funktion

5.8 System Messages über Syslog

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



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, über welche die Kommunikation laufen soll, ein.

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

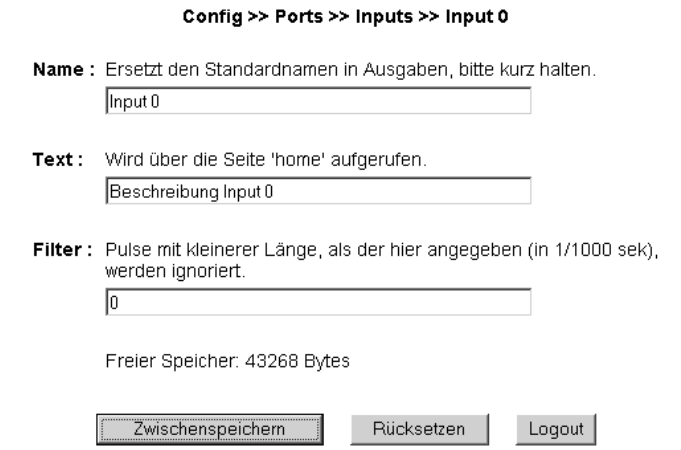
Übernehmen Sie die Einstellungen mit *Zwischenspeichern*.

5.9 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 >> Ports >> Inputs >> Input 0`



Basiskonfiguration „Input 0“

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

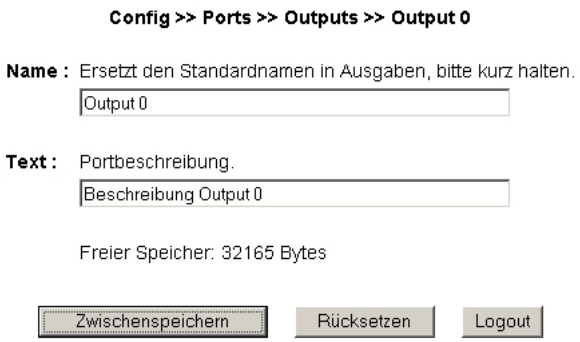
Die im Feld *Text* eingetragene Beschreibung kann zum Beispiel die Funktion oder den Installationsort des Sensors näher beschreiben.

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.

5.10 Porteinstellungen - Outputs

Um zum Beispiel die Einstellungen für Output 0 zu ändern, wählen Sie:

```
Config >> Ports >> Outputs >> Output 0
```



Einstellungen „Output 0“

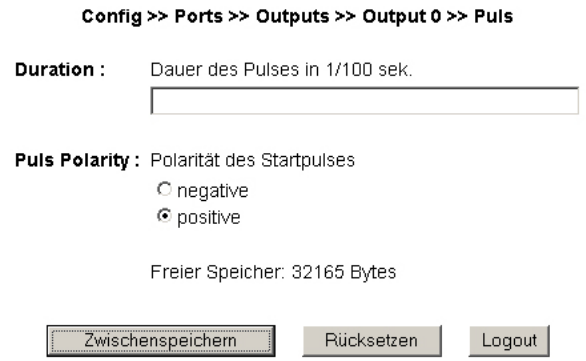
Geben Sie in dieses Feld eine Bezeichnung für den Output ein. Diese Bezeichnung wird dann im Browser für den Output 0 angezeigt.

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

Neben dem rein statischen Schalten der Outputs auf ON oder OFF erlaubt der IP-Watcher auch die Ausgabe von Pulsen. Das bedeutet, ein Output kann für eine voreinstellbare Zeit auf ON oder OFF geschaltet werden und fällt nach der eingestellten Pulslänge wieder zurück auf seinen Ruhezustand.

Um zum Beispiel den Output 0 des Gerätes auf die Ausgabe von Pulsen zu konfigurieren, wählen Sie im Navigationsbaum:

```
Config >> Ports >> Outputs >> Output 0 >> Puls
```



Pulskonfiguration für Outputs

Tragen Sie bei *Duration* die gewünschte Pulslänge in 1/1000 Sekunden ein. Ein Wert von 1000 entspricht einem 1 Sekunde langen Puls.

Ist die Polarität des Pulses auf positiv eingestellt, ist der Output im Ruhezustand nicht geschaltet. Wird der Output durch eine Alarmauslösung auf ON gesetzt, schaltet der IP-Watcher für die eingestellte Pulsdauer die Versorgungsspannung auf den Output.

Bei negativer Pulspolarität liegt der Ruhepegel des Outputs bei der Versorgungsspannung. Beim Schalten des Outputs wird der Pegel für die eingestellte Zeit abgeschaltet.

Tragen Sie eine Pulsdauer von 0 und eine negative Polarität ein, ist der Output invertiert.

Auf

`Config >> Device >> Output Mode`

können Sie durch Aktivieren der Option *Internal 24V enable* von intern 24V auf die Klemmen Vdd und GND schalten. Dadurch entfällt die Notwendigkeit eine externe Hilfsspannung anzulegen. Beachten Sie, dass jeder Output dann nur mit maximal 150mA belaststet werden darf.

6 Troubleshooting und Test

Der IP-Watcher verfügt über ein internes Fehlermanagement und Diagnosesystem. Im Konfigurationsbaum ist dieses unter der Rubrik

```
Diag
```

zu finden.

6.1 Report

Tritt ein 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.

Diagnose Report und Diagnose Archiv

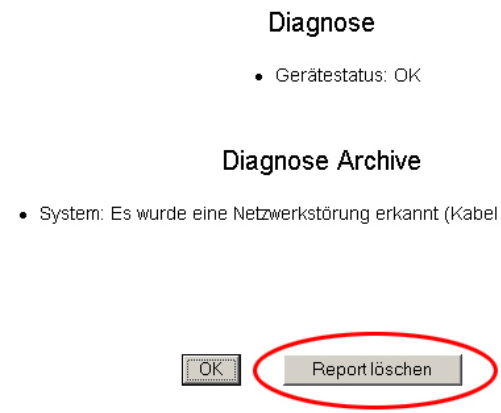
Diagnose Report und Diagnose Archiv sind unter

```
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.



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 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.

Übersicht und Plausibilitätsprüfung der Einstellungen mit Fehler

Ferner wird überprüft und angezeigt, welche Übertragungswege für die Alarme 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

Alarmübertragungswege

6.3 Check Alarm

Um zu überprüfen, ob die konfigurierten Meldearten bei den aktivierten Alarmen ordnungsgemäß funktionieren, können auf der Seite

Diag >> Test >> Check Alarm

manuell Trigger, Quittierung und Reset für die verfügbaren Alarme gesetzt werden.

Mit diesen Schaltflächen ist es möglich, sämtliche Alarmmeldungen der aktivierten Alarme ohne Eintreten der realen Auslösebedingung auszulösen.

Seite zum Testen der aktivierten Alarme

Mit Betätigung der Taste *Trigger* signalisieren Sie dem Gerät, dass die für den Alarm auslösende Bedingung eingetreten ist. Die Erreichbarkeit verknüpfter Einträge aus der *IP Watch List* ist hierbei irrelevant, die tatsächliche Auslösebedingung sollte allerdings noch nicht erfüllt sein. Es handelt sich hierbei um eine virtuelle Alarmauslösung.

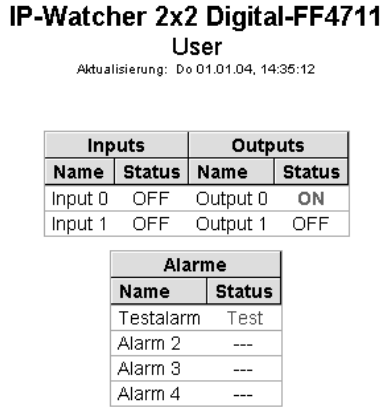
Die Schaltfläche *ACK* quittiert den über *Trigger* ausgelösten Alarm. Die Quittierung ist nur möglich, wenn für den Alarm mindestens ein Quittierungsvariante eingestellt wurde. Ist keine Alarmbestätigung konfiguriert, ist die Schaltfläche ACK ausgegraut.

Der Button *Reset* nimmt den künstlich gesetzten Trigger wieder zurück. Dies ist nach dem Testen der Alarme unbedingt erforderlich, da ansonsten tatsächlich auftretenden Alarme nicht erkannt werden können.

Wurde über die Schaltfläche *Trigger* ein künstlicher Trigger gesetzt, wird dieser auch auf der Seite *home.htm* und *user.htm*

durch blinkende Texte signalisiert. Auf der Seite home.htm wird ein aktivierter Testalarm zusätzlich in der Meldebox über der Alarmtabelle dargestellt.

Seite „home.htm“ mit ausgelöstem Testalarm



Seite „user.htm“ mit ausgelöstem Testalarm

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.	

Kurzanleitung „Manual“

7.2 Datasheet

Das Datenblatt gibt Auskunft über die wichtigsten Eigenschaften und technischen Daten des Web-Alarm.

Artikelnummer:	**#57654 IP-Watcher 2x2 Digital**
Netzwerk:	10/100BaseT autosensing
Protokoll:	TCP und UDP Sockets, Client und Server SNMP inkl. Traps, OPC-Server, Inventarisierung, Gruppenmanagement
Antwortzeiten:	Daten- und Schaltverkehr: typ. 12ms
Digitale Ausgänge:	2 x Digital Out 6V-30V DC, 0.5A, Gruppen mit 2 Ausgängen, max. Gesamtstrom 1A
Digitale Eingänge:	2 x Digital In, max. Eingangsspannung +/-30V, verpolungssicher innerhalb dieses Bereichs Schaltschwelle 8V, +/- 1V, "Ein"-Strom = 2.2 mA
Anschlüsse:	1 x 6-fach Schraubklemmen, steckbar
Galvanische Trennung:	Digital-Ausgänge - Netzwerk: min. 500 V Digital-Eingänge: min 1000 V
Anzeigen:	Status-LEDs Netzwerk
Stromversorgung:	Geräteversorgung: POE, 18-48V DC, 18-30Veff AC Ausgänge: 6-30V DC
Lagertemperatur:	-25°C - 70°C
Betriebstemperatur:	0°C - 60°C
Gehäuse:	Kunststoff-Gehäuse zur Hutschienen-Montage 105 x 75 x 22 mm (l x b x h)
Gewicht:	ca. 140g

Datenblatt des IP-Watchers

7.3 Property

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

Device Information	
Manufacturer	Wiesemann & Theis GmbH
- Address	Porschestr. 12 42279 Wuppertal Germany
- Support Hotline	+49-(0)202-2680-0
- Internet	www.wut.de
Typ	IP-Watcher 2x2 Digital
Order No.	#57654
Software Revision	3.11
Hardware Revision	1.00
Bios Software Revision	3.11.3.00.330
Device Identification:	
Name of Device	IP-Watcher 2x2 Digital-FF4711
System Description	Netzwerkkomponenten durch zyklisches Ansprechen überwachen
Ethernet Address	00-C0-3D-FF-47-11
IP Address	10.40.27.30
DHCP: DNS Server	0.0.0.0
DHCP: Lease Time	00:00:00 sec

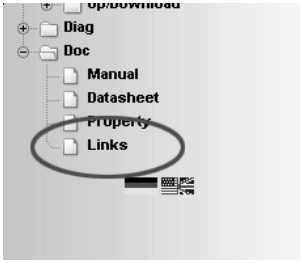
„Property"-Seite

7.4 Links

Ein Klick auf den Menübaumeintrag *Links* lädt eine Webseite vom W&T-Webserver. Diese Seite enthält Links zu den jeweils aktuellen Dokumentationskomponenten. Dazu zählen...

- ...Anleitung
- ...Firmware
- ...Tools
- ...Applikationsbeispiele

Des weiteren finden Sie hier Links zu aktuellen Produkten ähnlicher Produktgruppen.



Link zu aktuellen Linkliste

Zur Darstellung der aktuellen Linkliste ist eine Internetverbindung erforderlich.

8 Anhang

8.1 LEDs

Im Folgenden ist die Bedeutung und Funktion der auf der Vorderseite des IP-Watchers 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-Alarm 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-Alarm 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-Alarm ist in diesem Zustand nicht mehr betriebsfähig. Senden Sie das Gerät bitte über Ihren Fachhändler zur Überprüfung an W&T.

8.3 Factory Defaults

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

- über das Web-Based Management
- 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.

8.3.1 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.

8.3.3 Reset-Jumper

Können die Factory Defaults weder über das Webinterface, noch über den seriellen Notzugang 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 IP-Watcher 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 IP-Watcher an. Das Gerät wird jetzt in seinen Auslieferungszustand zurückgesetzt. Die LEDs an der Front flackern während dieses Vorgangs unregelmäßig.

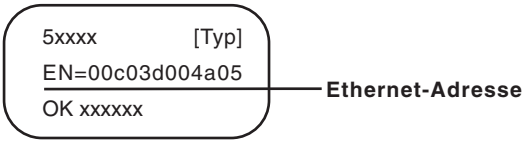
Nachdem die Werkseinstellungen wiederhergestellt sind trennen Sie die Spannungsversorgung, entnehmen die Jumper und schließen das Gerät. Beginnen Sie nun mit der Inbetriebnahme.

8.4 Alternative IP-Adressvergabe

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

8.4.1 ARP-Kommando

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



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-Alarm 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 oder den seriellen Weg wählen.

8.4.3 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-Alarm 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-Alarm 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

Eintrag in der Datei */etc/ethers*: 00:C0:3D:00:12:FF WT_1

Falls der RARP-Daemon noch nicht aktiv ist, müssen Sie ihn nun mit dem Befehl *rarpd -a* starten.

8.5 Firmware Update

Die Betriebssoftware des IP-Watchers wird ständig weiterentwickelt. Das folgende Kapitel beschreibt aus diesem Grund das Verfahren, ein Firmwareupgrade durchzuführen.

8.5.1 Aktuelle Firmware

Die jeweils aktuellste Firmware inkl. der verfügbaren Updatetools und einer Revisionsliste ist auf unseren Webseiten unter der Adresse *http://www.wut.de* veröffentlicht.

Bitte notieren Sie vor dem Download zunächst die auf dem IP-Watcher befindliche 5-stellige Typenbezeichnung. Von unserer Homepage aus erreichen Sie jetzt die nach Artikelnummern sortierte Produktübersicht, über die Sie direkt auf das Datenblatt des Gerätes gelangen. Folgen Sie hier dem Link auf die aktuelle Version der Firmware.

8.5.2 Firmwareupdate über das Netzwerk

Voraussetzung ist ein PC unter Windows 9x/NT/2000/XP/Vista mit einem Netzwerkanschluss und aktiviertem TCP/IP-Stack. Für den Updateprozess benötigen Sie zwei Dateien, die wie bereits beschrieben auf der Homepage zum Download bereitstehen:

- das ausführbare Updatetool für die Übertragung der Firmware in den IP-Watcher
- die Datei mit der neuen Firmware, die in den IP-Watcher übertragen werden soll

Eine spezielle Vorbereitung des IP-Watchers für das Update ist nicht erforderlich.

Das für das Update verwendete *WuTility* erkennt alle in Ihrem Netzwerk befindlichen W&T-Geräte und ist weitestgehend selbsterklärend. Sollten dennoch Fragen oder Unklarheiten bestehen, nutzen Sie bitte die zugehörige Dokumentation oder die Onlinehilfe.

Unterbrechen Sie nie selbständig den Updateprozess durch Trennen der Spannungsversorgung. Nach einem unvollständigen Update ist der IP-Watcher betriebsunfähig.

Mischen Sie niemals Dateien mit unterschiedlichen Versionsnummers im Namen. Dies führt zur Funktionsunfähigkeit des Gerätes.

Der IP-Watcher erkennt selbständig, wann die Übertragung der neuen Betriebssoftware komplett ist und führt dann automatisch einen Reset durch.

8.5 Up- und Download

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 IP-Watchers auslesen und eventuell Modifikationen vornehmen. Die geänderten Einstellungen können dann über die Upload Funktion wieder in das Gerät eingespielt werden.

Für den XML-Upload erstellen bzw. verändern Sie eine Textdatei mit den entsprechenden Parametern und laden diese dann in das Gerät. Die Konfiguration des IP-Watchers muss mit dem Ausdruck

```
<io-Digital2x2IPW.1>
```

beginnen und mit dem Ausdruck

```
</io-Digital2x2IPW.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 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.

8.6 Technische Daten

Netzwerk	Ethernet 10/100BaseT autosensing
Protokoll	TCP- und UDP-Client, FTP, Mail, SNMP inkl. Traps, Inventarisierung, Gruppenmanagement
Antwortzeiten	Daten- und Schaltverkehr: typ. 12ms
Digitale Ausgänge	2 x Digital Out 6V-30V DC, 0.5A, max. Gesamtstrom 1A
Digitale Eingänge	2 x Digital In, max. Eingangsspannung +/-30V, verpolungssicher innerhalb dieses Bereichs Schaltschwelle 8V, +/-1V, "Ein"-Strom = 2.2mA
Anschluss	1 x 6-fach Schraubklemme
Galvanische Trennung	Digitalausgänge - Netzwerk: min. 1kV
Anzeigen	Power-, Status- und Error-LED 4 LEDs für digitale Zustände
Stromversorgung	Geräteversorgung: DC 18V-48V, AC 18V-30V Ausgänge: DC 6V-30V
Lagertemperatur	-25°C - +70°C
Betriebstemperatur	0°C - 60°C
Gehäuse	Kunststoff-Kleingehäuse, 105 x 22 x 75mm (l x b x h)
Gewicht	ca. 140g