SYSTEM

Version 0.9

Ziel und Zweck

Dieses Dokument ist Teil des Benutzerhandbuchs zur Installation und Konfiguration von BinTec Gateways ab Software-Release 7.1.1. Für neueste Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere **Release Notes** lesen – insbesondere, wenn Sie ein Software-Update zu einem höheren Release-Stand durchführen. Die aktuellsten **Release Notes** sind immer zu finden unter www.bintec.de.

Haftung

Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in Ihrem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Bintec Access Networks GmbH haftet nur im Umfang ihrer Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen, sowie Änderungen und **Release Notes** für Bintec-Gateways finden Sie unter www.bintec.de.

Als Multiprotokollgateways bauen Bintec-Gateways in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen. Bintec Access Networks GmbH übernimmt keine Verantwortung für Datenverlust, ungewollte Verbindungskosten und Schäden, die durch den unbeaufsichtigten Betrieb des Produkts entstanden sind.

Marken

Bintec und das Bintec-Logo sind eingetragene Warenzeichen der Bintec Access Networks GmbH.

Erwähnte Firmen- und Produktnamen sind in der Regel Warenzeichen der entsprechenden Firmen bzw. Hersteller.

Copyright

Richtlinien und Normen

Bintec-Gateways entsprechen folgenden Richtlinien und Normen:

R&TTE-Richtlinie 1999/5/EG

CE-Zeichen für alle EU-Länder

Weitere Informationen finden Sie in den Konformitätserklärungen unter www.bintec.de.

Wie Sie Bintec erreichen

Bintec Access Networks GmbH
Südwestpark 94
D-90449 Nürnberg
Germany

Telephone: +49 180 300 9191 0
Fax: +49 180 300 9193 0
Internet: www.bintec.de

Bintec France
6/8 Avenue de la Grande Lande
F-33174 Gradignan
France

Telephone: +33 5 57 35 63 00
Fax: +33 5 56 89 14 05
Internet: www.bintec.fr

1 Hauptmenü

Im folgenden werden die Felder des Menüs *SYSTEM* beschrieben.

```
VPN Access Setup Tool                    Bintec Access Networks GmbH
[SYSTEM]: Change System Parameters                        MyGateway

 System Name                                VPN Access
 Local PPP ID (default)                     VPN Access
 Location                                   European Union
 Contact                                    BINTEC


 Syslog output on serial console            no
 Message level for the syslog table         info
 Maximum Number of Syslog Entries           50

 External Activity Monitor >
 External System Logging >
 Keepalive Monitoring >
 Password settings >
 Time and Date >

         SAVE                       CANCEL

Enter string, max length = 34 chars
```

Im Menü ***SYSTEM*** werden die grundlegenden Systemdaten Ihres Gateways eingetragen.

Das Menü ***SYSTEM*** besteht aus folgenden Feldern:

Feld	Wert
System Name	Definiert den Systemnamen Ihres Gateways, wird auch als PPP-Host-Name benutzt. Erscheint beim Einloggen auf dem Gerät als Eingabe-Prompt. Wenn kein Systemname gesetzt ist, erscheint beim Einloggen mit dem Benutzernamen `admin` ein Warnhinweis. Als Defaultwert ist der Gerätetyp voreingestellt.

Feld	Wert
Local PPP ID (default)	Diese Eintragung ist zur Identifizierung Ihres Gateways nötig, wenn eine nicht-partnerspezifische ➤➤ **PPP-Authentisierung** (z. B. ➤➤ **PAP** oder ➤➤ **CHAP**) durchgeführt wird.
Location	(optional) Gibt an, wo sich Ihr Gateway befindet.
Contact	(optional) Gibt die zuständige Kontaktperson an. Hier kann z. B. die E-Mail-Adresse des Systemadministrators eingetragen werden.
Syslog output on serial console	Ermöglicht die Anzeige von Syslog Messages auf dem mit der seriellen Schnittstelle des **VPN Access Gateway** verbundenen Rechner. Verwenden Sie diese Einstellung nur, wenn Sie eine Fehleranalyse machen, da massiver Output über die serielle Konsole sich auf den Durchsatz der anderen Schnittstellen auswirkt. Mögliche Werte: ■ *yes* ■ *no* (Defaultwert)

Feld	Wert
Message level for the syslog table	Spezifiziert die Priorität der intern aufzuzeichnenden Syslog Messages. Mögliche Werte: ■ *emerg*: Emergency Messages (höchste Priorität) ■ *alert*: Alert Messages ■ *crit*: Critical Messages ■ *err*: Error Messages ■ *warning*: Warning Messages ■ *notice*: Notice Messages ■ *info*: Info Messages (Defaultwert) ■ *debug*: Debug Messages (niedrigste Priorität) Nur Syslog Messages mit höherer oder gleicher Priorität als angegeben werden intern aufgezeichnet, d. h. dass beim Syslog-Level *debug* sämtliche erzeugten Meldungen aufgezeichnet werden.
Maximum Number of Syslog Entries	Maximale Anzahl an Syslog Messages, die auf dem **VPN Access Gateway** intern gespeichert werden (Wertebereich: *0* ... *1000*). Sie können die gespeicherten Meldungen mittels des Befehls `syslog` auf der SNMP SHell abrufen.

Tabelle 1-1: Felder im Menü ***SYSTEM***

1 Hauptmenü

2 Untermenü *External Activity Monitor*

Im folgenden werden die Felder des Untermenüs *External Activity Monitor* beschrieben.

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[SYSTEM]: [ACTIVMON]: External Activity Monitor              MyGateway


  Client IP Address                    255.255.255.255
  Client UDP Port                      2107
  Type                                 off
  Update Interval (sec)                5




           SAVE                                    CANCEL
```

Im Menü ***System*** ➜ ***External Activity Monitor*** finden Sie die Einstellungen, die nötig sind, um das **VPN Access Gateway** mit dem Windows-Tool Activity Monitor überwachen zu können.

Zweck Mit dem **Activity Monitor** können Windows-Nutzer die Aktivitäten des Gateways überwachen. Wichtige Informationen über den Status von physikalischen Schnittstellen (z. B. ISDN-Leitung) und virtuellen Schnittstellen (z. B. WAN Partner) sind leicht mit einem Tool erreichbar. Ein permanenter Überblick über die Auslastung der Schnittstellen des Gateways ist möglich.

Funktionsweise Ein Status-Daemon sammelt Informationen über das Gateway und überträgt sie in Form von UDP-Paketen zur Broadcast-Adresse des LAN (Standardeinstellung) oder zu einer explizit eingetragenen IP-Adresse. Ein Paket pro Gateway-Schnittstelle und Zeitintervall, das individuell einstellbar ist auf Werte von 1 - 60 Sekunden, wird gesendet. Alle physikalischen Schnittstellen und bis zu 100 virtuelle Schnittstellen können überwacht werden, soweit die Paketgröße von ca. 4000 Bytes nicht überschritten wird. Eine Windows-Anwendung auf Ihrem PC, die mit dem BRICKware Release 5.1.1 und höher erhältlich ist, emp-

fängt die Pakete und stellt die enthaltenen Informationen auf verschiedene Arten dar.

Um den **Activity Monitor** zu aktivieren, müssen Sie:

- das/die zu überwachende(n) Gateway(s) entsprechend konfigurieren,
- die Windows-Anwendung auf Ihrem PC starten und verwenden (siehe **BRICKware for Windows**).

Das Menü ***EXTERNAL ACTIVITY MONITOR*** besteht aus folgenden Feldern:

Feld	Wert
Client IP Address	IP-Adresse, zu der das Gateway die UDP Pakete schickt. Mit dem Standardwert *255.255.255.255* wird die Broadcast-Adresse der ersten LAN-Schnittstelle verwendet. Beachten Sie: Wenn Sie hier die IP-Adresse eines WAN Partners eingeben, der über eine ISDN-Wahlverbindung erreichbar ist, entstehen Ihnen hohe Kosten durch häufiges Aufbauen von ISDN-Verbindungen (im Auslieferungszustand wird alle 5 Sekunden ein Paket geschickt).
Client UDP Port	Port-Nummer für Activity Monitor (Standardwert: *2107*, registriert durch IANA - Internet Assigned Numbers Authority).
Type	Art der Informationen, die mit den UDP-Paketen zur Windows-Anwendung geschickt werden. Mögliche Werte: ■ *off*: deaktiviert **Activity Monitor** (Defaultwert) ■ *physical*: nur Informationen über physikalische Schnittstellen ■ *physical_virt*: Informationen über physikalische und virtuelle Schnittstellen

Feld	Wert
Update Interval <sec>	Update-Intervall in Sekunden. Mögliche Werte: *0* bis *60* (Defaultwert: *5*).

Tabelle 2-1: Felder im Menü ***EXTERNAL ACTIVITY MONITOR***

3 Untermenü *EXTERNAL SYSTEM LOGGING*

Im folgenden werden die Felder des Untermenüs *EXTERNAL SYSTEM LOGGING* beschrieben.

Im Menü ***SYSTEM*** ➜ ***EXTERNAL SYSTEM LOGGING*** werden alle Log Host Einstellungen angezeigt. Im Untermenü ***SYSTEM*** ➜ ***EXTERNAL SYSTEM LOGGING*** ➜ ***ADD/EDIT*** finden Sie Einstellungen für Syslog Messages.

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[SYSTEM] [LOGGING] [ADD]                                        MyGateway


     Log Host
     Level                      info
     Facility                   local0
     Type                       all
     Timestamp                  none


           SAVE                                      CANCEL
```

Alle wesentlichen Ereignisse in den verschiedenen Subsystemen des Gateways (z. B.: ➤➤ **ISDN**, ➤➤ **PPP** usw.) werden in der Form von Syslog Messages (system logging messages) protokolliert.

Je nach eingestelltem Level (acht Stufen von *critical* über *info* bis *debug*) werden dabei mehr oder weniger viele Details sichtbar. Die protokollierten Daten werden intern auf dem Gateway in einer Liste von einstellbarer Länge gespeichert (Die Einstellung der internen Speicherung von Syslog-Meldungen erfolgt im ***SYSTEM*** Hauptmenü). Alle Informationen können und sollten zur Speicherung und Weiterverarbeitung zusätzlich an einen oder mehrere externe Rechner weitergeleitet werden, z. B. an den Rechner des Systemadministrators. Auf dem Gateway intern gespeicherte Syslog Messages gehen bei einem Neustart verloren.

Hinweis

Vermeiden Sie es, Syslog Messages auf Log Hosts weiterzuleiten, die über eine Wählverbindung erreicht werden. Dies kann zu erheblichen Kosten führen.

Achten Sie darauf, die Syslog Messages nur an einen sicheren Rechner weiterzuleiten. Kontrollieren Sie die Daten regelmäßig und achten Sie darauf, dass jederzeit ausreichend freie Kapazität auf der Festplatte des Rechners zur Verfügung steht.

Syslog-Daemon

Die Erfassung der Syslog Messages wird von allen Unix-Betriebssystemen unterstützt. Für Windows-Rechner ist in den **DIME Tools** ein Syslog-Daemon enthalten, der die Daten aufzeichnen und je nach Inhalt auf verschiedene Dateien verteilen kann (siehe **BRICKware for Windows**).

Die Einstellungen für das externe Speichern von Syslog Messages erfolgen in ***SYSTEM*** ➜ ***EXTERNAL SYSTEM LOGGING*** ➜ ***ADD/EDIT***.

Das Menü ***EXTERNAL SYSTEM LOGGING*** ➜ ***ADD/EDIT*** besteht aus folgenden Feldern:

Feld	Wert
Log Host	➤➤ **IP-Adresse** des Hosts, zu dem Syslog Messages weitergeleitet werden.

Feld	Wert
Level	Priorität der zum ***LOG HOST*** zu schickenden Syslog Messages. ***MESSAGE LEVEL FOR THE SYSLOG TABLE*** in ***SYSTEM***. Mögliche Werte: ■ *emerg*: Emergency Messages (höchste Priorität) ■ *alert*: Alert Messages ■ *crit*: Critical Messages ■ *err*: Error Messages ■ *warning*: Warning Messages ■ *notice*: Notice Messages ■ *info*: Info Messages (Defaultwert) ■ *debug*: Debug Messages (niedrigste Priorität) Nur Syslog Messages mit höherer oder gleicher Priorität als angegeben werden an den ***LOG HOST*** gesendet.
Facility	Syslog-Facility auf ***LOG HOST***. Nur erforderlich, wenn der ***LOG HOST*** ein Unix-Rechner ist. Mögliche Werte: *local0 - 7* (Defaultwert *local0*).
Type	Nachrichtentyp. Mögliche Werte: ■ *all*: Alle Messages (Defaultwert) ■ *system*: Syslog Messages außer ➤➤ **Accounting**-Messages ■ *accounting*: Accounting-Messages

Feld	Wert
Timestamp	Angabe der Systemzeit des **VPN Access Gateway** im Syslog. Mögliche Werte: ■ *all*: Systemzeit mit Datum ■ *time*: Systemzeit ohne Datum ■ *none*: keine Systemzeitangabe (Default-wert)

Tabelle 3-1: Felder im Menü ***EXTERNAL SYSTEM LOGGING***

4 Untermenü *SCHEDULE & MONITOR*

Im folgenden werden die Felder des Untermenüs *SCHEDULE & MONITOR* beschrieben.

Über das Menü ***SCHEDULE & MONITOR*** gelangen Sie in die folgenden Untermenüs:

- ***KEEPALIVE MONITORING (HOSTS & IFC)***
- ***EVENT SCHEDULER***

4.1 Untermenü *KEEPALIVE MONITORING (HOSTS & IFC)*

Im Menü ***SYSTEM*** ➜ ***SCHEDULE & MONITOR*** ➜ ***KEEPALIVE MONITORING*** finden Sie Einstellungen für die Funktion "Keepalive Monitoring".

Wenn Sie zwei (oder mehrere) LANs über eine Wählverbindung gekoppelt haben – z. B. das LAN der Firmenzentrale mit dem LAN einer Filiale – befindet sich häufig ein zentraler Server im LAN der Firmenzentrale. Wenn dieser zentrale Server so konfiguriert ist, dass er regelmäßig WAN-Verbindungen zum Gateway im LAN der Filiale aufbaut, z. B. um Daten zu aktualisieren, dann sind diese Verbindungen überflüssig (aber nicht kostenlos), wenn keiner der Hosts in der Filiale erreichbar ist, z. B. weil alle Rechner ausgeschaltet sind. Da erst nach dem Aufbau der Verbindung festgestellt werden kann, dass die Hosts nicht erreichbar sind, entstehen Kosten für den Rufenden, also für die Firmenzentrale.

Mit der Funktion "Keepalive Monitoring" können Sie das Gateway in der Filiale so konfigurieren, dass unnötige WAN-Verbindungen von der Firmenzentrale zur Filiale vermieden werden. In regelmäßigen, einstellbaren Abständen überprüft das Gateway der Filiale, ob die zu überwachenden Hosts in seinem LAN erreichbar sind. Wenn nach drei aufeinanderfolgenden Versuchen keiner der zu überprüfenden Hosts auf eine entsprechende Anfrage antwortet, deaktiviert das Gateway die Schnittstelle zum WAN Partner "Firmenzentrale". Rufe seitens

der Firmenzentrale an nicht erreichbare Hosts werden gar nicht erst angenommen, und es entstehen keine Kosten.

Hinweis

In manchen Ländern (z. B. Schweiz) können trotz Nutzung von Keepalive Monitoring Kosten für diese vergeblichen Einwahlversuche anfallen.

Wenn alle Rechner im LAN der Filiale inaktiv waren, wird beim Einschalten eines zu überwachenden Rechners nicht automatisch sofort eine Verbindung zur Firmenzentrale aufgebaut. Erst wenn das Gateway die Erreichbarkeit eines Rechners registriert hat, wird die Schnittstelle zum WAN Partner "Firmenzentrale" aktiviert, und ein Verbindungsaufbau durch die Firmenzentrale ist möglich. Wieviel Zeit vergeht, bis das Gateway die erneute Erreichbarkeit signalisiert, ist abhängig vom eingestellten Überwachungsintervall (***INTERVAL***).

Hinweis

Der entsprechende WAN Partner, also z. B. die Firmenzentrale, muss auf dem Gateway per CLID (Calling Line Identification) identifiziert werden können. Wenn dies nicht der Fall ist, ist der beschriebene Nutzeffekt von "Keepalive Monitoring" nicht gegeben.

Keepalive Monitoring kann auf dem Gateway nicht für WAN Partner eingerichtet werden, die über einen RADIUS-Server authentisiert werden!

In ***SYSTEM*** ➜ ***SCHEDULE & MONITOR*** ➜ ***KEEPALIVE MONITORING*** sind alle *Hosts* und *Interfaces* aufgelistet, die per Keepalive Monitoring überwacht werden. Unter ***STATE*** ist dabei die Erreichbarkeit der Hosts aufgelistet: *alive*, wenn der Host bei der letzten Überprüfung erreichbar war, *down*, wenn er nicht erreichbar war.

In dem Menü ***WHAT TO MONITOR:*** wird eingestellt, ob die Konfiguration für *hosts* oder *interfaces* vorgenommen wird.

***WHAT TO MONITOR*: Hosts**

Wenn *hosts* gewählt wurde, besteht das Menü ***KEEPALIVE MONITORING*** ➜ ***ADD/EDIT*** aus folgenden Feldern:

Feld	Wert
Group	Definiert eine Gruppe von Hosts, deren Erreichbarkeit vom **VPN Access Gateway** überwacht werden soll. Jeder zu überwachende Host wird einer Gruppe zugeordnet. Insgesamt können 255 Gruppen angelegt werden. Mögliche Werte: *0 ... 255.*
IPAddress	Definiert einen Host, der vom **VPN Access Gateway** überwacht werden soll.
Interval	Definiert einen Zeitintervall in Sekunden, welches zur Überprüfung der Erreichbarkeit von Hosts verwendet werden soll. Mögliche Werte: *0 ... 65536* (Standardwert: *300* s). Innerhalb einer Gruppe wird das kleinste ***INTERVAL*** verwendet.
Source IP	Diejenige IP-Adresse, die das Gateway als Quelladresse des Pakets verwendet, das an den zu überwachenden Host gesendet wird.
DownAction	Definiert, wie der Status der unter ***FIRSTIFINDEX*** und ***RANGE*** festgelegten **VPN Access Gateway**-Schnittstellen gesetzt wird, wenn alle Hosts einer Gruppe nicht erreichbar sind. Mögliche Werte: ■ *down* : Schnittstellen werden deaktiviert (Defaultwert) ■ *none*: keine Aktion ■ *up*: Schnittstellen werden aktiviert Wenn mindestens ein Host einer Gruppe wieder erreichbar ist, wird der Status der Schnittstellen wieder auf den ursprünglichen Wert gesetzt.

Feld	Wert
FirstIfIndex	Definiert die erste Schnittstelle eines Schnittstellen-Bereiches auf dem **VPN Access Gateway**, für welche die unter ***DOWNACTION*** festgelegte Aktion ausgeführt werden soll. Für Wählverbindungen zu WAN Partnern sind Schnittstellen mit Indizes von *10001* bis *14999* vorgesehen. Der Standardwert *10001* bezeichnet die Schnittstelle zum ersten auf dem **VPN Access Gateway** konfigurierten WAN Partner (Wählverbindung). Die Indizes anderer Schnittstellen finden Sie in der ***IFTABLE*** auf der SNMP Shell.
Range	Definiert den Bereich von Schnittstellen auf dem **VPN Access Gateway**, für welche die unter ***DOWNACTION*** festgelegte Aktion ausgeführt werden soll. Wenn Sie ***FIRSTIFINDEX*** = *10001* und ***RANGE*** = *0* einstellen, ist nur die Schnittstelle mit dem Index *10001* betroffen. Wenn Sie ***FIRSTIFINDEX*** = *10001* und ***RANGE*** = *4999* (Defaultwert) einstellen, sind die Schnittstellen mit den Indizes *10001* bis *14999* betroffen.

Tabelle 4-1: Felder im Menü ***KEEPALIVE MONITORING*** *hosts*

WHAT TO MONITOR: Interfaces

Wenn in ***WHAT TO MONITOR:*** *interfaces* gewählt wurde, besteht das Menü ***KEEPALIVE MONITORING*** ➜ ***ADD/EDIT*** aus folgenden Feldern:

Feld	Wert
Interface	Definiert die Schnittstelle auf dem **VPN Access Gateway**, für welche die unter ***ACTION*** festgelegte Aktion ausgeführt werden soll. Hier wird der ***IFINDEX*** eingetragen. Der ***IFINDEX*** ist der ***IFTABLE*** auf der SNMP Shell zu entnehmen.
Trigger	Definiert das Ereignis, auf das eine bestimmte ***ACTION*** folgen soll. Mögliche Werte: ■ down: Schnittstelle ist deaktiviert (Defaultwert) ■ up: Schnittstelle ist aktiviert
Action	Definiert die Aktion, die auf das in ***TRIGGER*** definierte Ereignis folgen soll. Mögliche Werte: ■ *none:* keine Aktion (Defaultwert) ■ *down*: Schnittstelle wird deaktiviert ■ *up*: Schnittstelle wird aktiviert

Feld	Wert
FirstIfIndex	Definiert die erste Schnittstelle eines Schnittstellen-Bereiches auf dem **VPN Access Gateway**, für welche die unter ***ACTION*** festgelegte Aktion ausgeführt werden soll. Für Wählverbindungen zu WAN Partnern sind Schnittstellen mit Indizes von *10001* bis *14999* vorgesehen. Der Standardwert *10001* bezeichnet die Schnittstelle zum ersten auf dem **VPN Access Gateway** konfigurierten WAN Partner (Wählverbindung). Die Indizes anderer Schnittstellen finden Sie in der ***IFTABLE*** auf der SNMP Shell.
Range	Definiert den Bereich von Schnittstellen auf dem **VPN Access Gateway**, für welche die unter ***ACTION*** festgelegte Aktion ausgeführt werden soll. Wenn Sie ***FIRSTIFINDEX*** = *10001* und ***RANGE*** = *0* einstellen, ist nur die Schnittstelle mit dem Index *10001* betroffen. Wenn Sie ***FIRSTIFINDEX*** = *10001* und ***RANGE*** = *4999* (Defaultwert) einstellen, sind die Schnittstellen mit den Indizes *10001* bis *14999* betroffen.

Tabelle 4-2: Felder im Menü ***KEEPALIVE MONITORING*** *interfaces*

4.2 Untermenü *EVENT SCHEDULER*

Ab Systemsoftware 7.1.4 verfügt Ihr Gateway über einen Event Scheduler, mittels dessen es möglich ist, beliebige Einträge in die MIB vorzunehmen, sobals ein bestimmtes (ebenfalls frei konfigurierbares) Ereignis eintritt.

Um Ereignisse wie das Deaktivieren eines Internetzugangs beim Überschreiten eines bestimmten Transfervolumens u. ä. zu ermöglichen, bietet **VPN Access**

Gateway den ***EVENT SCHEDULER***. Dieser ermöglicht es, beliebige Ereignisse beliebigen Aktionen zuzuordnen.

Abgesehen von voreingestellten und einfach zu konfigurierenden Standardanwendungen wie zeit- oder volumengesteuerte Aktivierung von Interfaces, ermöglicht es der Event Scheduler, beliebig auf MIB-Parameter zuzugreifen. Dadurch können beliebige Ereignisse in der MIB als Auslöser ebenfalls beliebiger Aktionen definiert werden.

Achtung!

Die Konfiguration der nicht voreingestellten Aktionen erfordert umfangreiches Wissen über die Funktionsweise unserer Gateways. Eine Fehlkonfiguration kann zu erheblichen Störungen im Betrieb führen. Sichern Sie ggf. die ursprüngliche Konfiguration auf einem PC.

Die Konfiguration des Event Scheduler erfolgt im Menü ***SYSTEM*** ➜ ***SCHEDULE & MONITOR*** ➜ ***EVENT SCHEDULER (TIME & SNMP)***:

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[SYSTEM][SCHEDULED]: Event Schedule                                MyGateway


                    Event Scheduler             disabled

                    Schedule Events >
                    Schedule Commands >

                    SAVE                    CANCEL
```

Im Feld ***EVENT SCHEDULER*** aktivieren oder deaktivieren Sie den Scheduler, per Default ist er deaktiviert. Im Menü ***SCHEDULE EVENTS*** konfigurieren Sie die Ereignisse, die eine bestimmte Aktion auf dem Gateway auslösen sollen, im Menü ***SCHEDULE COMMANDS*** die auszuführenden Aktionen. Die Auslöser (Events) können zu Ereignis-Ketten verknüpft werden, so dass auch komplexe Bedingungen für das Auslösen einer Aktion erstellt werden können.

4.2.1 Konfiguration der Auslöser (Events)

Die Ereignisse, die eine entsprechende Aktion auslösen, werden im Menü *SYSTEM* ➜ *SCHEDULE & MONITOR* ➜ *EVENT SCHEDULER (TIME & SNMP)* ➜ *SCHEDULE EVENTS* ➜ *ADD/EDIT* erstellt bzw. editiert.

Standardmäßig öffnet sich das Menü mit der Maske zur Konfiguration eines Ereignisses vom Typ *time*:

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[SYSTEM][SCHEDULED][SCHED_EVT][ADD]: Scheduler Events          MyGateway

  Index        1        Description
    NextIndex    none
    Type         time


    Condition             dayly
      Start time (hh:mm)
      End time   (hh:mm)

    Status                notavail

                  SAVE                            CANCEL
```

Wenn Sie ***TYPE*** = *value* auswählen, ändert sich das Menü wie folgt:

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[SYSTEM][SCHEDULED][SCHED_EVT][ADD]: Scheduler Events          MyGateway

   Index        1        Description
     NextIndex    none
     Type         value

     Monitored event       user defined
       Table
       Variable
       Index variable
       Index value

     Condition             range
       Compare value
       End value

     Status                notavail

                   SAVE                              CANCEL
```

Je nach Einstellung enthält das Menü folgende Felder:

Feld	Wert
Index	Das Gateway vergibt automatisch eine Index-Nummer für den Eintrag. Der Wert kann aber auch editiert werden. Es stehen alle Werte von *1* bis *65535* zur Verfügung.
Description	Hier geben Sie eine beliebige Bezeichnung für das Ereignis ein. Die maximale Länge des Eintrags beträgt 30 Zeichen.

Feld	Wert
Next Index	Hier geben Sie an, welcher Eintrag dem aktuellen in einer Ereigniskette folgen soll. Die Einträge einer Ereigniskette bilden eine komplexe Bedingung für eine auszuführende Aktion. Wie die Ereigniskette zu einer Aktion führt, wird im Menü ***SYSTEM*** ➜ ***SCHEDULE & MONITOR*** ➜ ***EVENT SCHEDULER (TIME & SNMP)*** ➜ ***SCHEDULE COMMANDS*** konfiguriert.
Type	Hier wählen Sie, welchen Typ von Ereignis Sie als Auslöser einer Aktion definieren wollen: Zur Verfügung stehen: ■ *time* - Die Aktion wird zu bestimmten Zeiten ausgelöst (Defaultwert). ■ *value* - Die Aktion wird ausgelöst, sobald eine MIB-Variable einen bestimmten Wert annimmt.

Feld	Wert
Monitored event	Nur für ***TYPE*** = *value*. Hier können Sie zwischen unterschiedlichen Ereignissen wählen. Zur Verfügung stehen: ■ *user defined* - Sie können frei wählen, auf welchen Wert welcher MIB-Variablen der Scheduler mit einer Aktion reagieren soll (Defaultwert). ■ *WAN interface total charge* - Eine Aktion wird ausgeführt, wenn auf einem WAN-Interface (die Auswahl des Interfaces erfolgt bei der Konfiguration der Aktion) bestimmte Kosten verursacht worden sind. Dazu ist es notwendig, dass dem Gateway vom Provider Gebührenimpulse übertragen werden. ■ *WAN interface total duration* - Eine Aktion wird ausgeführt, wenn ein WAN-Interface für eine bestimmte Zeitdauer aktiv gewesen ist. ■ *WAN interface total RX traffic* - Eine Aktion wird ausgeführt, wenn ein WAN-Interface eine bestimmte Menge an Daten (in Bytes) empfangen hat. ■ *WAN interface total TX traffic* - Eine Aktion wird ausgeführt, wenn ein WAN-Interface eine bestimmte Menge an Daten (in Bytes) gesendet hat.
Table	Nur für ***MONITORED EVENT*** = *user defined*. Hier geben Sie die MIB-Tabelle an, in der sich die MIB-Variable befindet, die für den Auslöser verwendet werden soll, z. B. ***PPPTABLE***.

Feld	Wert
Variable	Nur für ***MONITORED EVENT*** = *user defined*. Hier geben Sie die MIB-Variable ein, die für den Auslöser verwendet werden soll, z. B. ***PPPMAXCONN***.
Index variable	Nur für ***MONITORED EVENT*** = *user defined*. Hier geben Sie die Indexvariable der zuvor ausgewählten MIB-Tabelle ein. Dies ist in einer beliebigen MIB-Tabelle diejenige Variable, die in der Tabellenansicht mit einem Asterisk (*) markiert ist, z. B. ***PPPTYPE***.
Index value	Nur für ***MONITORED EVENT*** = *user defined*. Hier geben Sie den Wert ein, den die Indexvariable für den Tabelleneintrag hat, der für den Auslöser verwendet werden soll, z. B. ***PPPTYPE.1.1***. Die Einträge in einer MIB-Tabelle werden intern indiziert. In der normalen Tabellenansicht wird diese Indizierung nicht angezeigt. Geben Sie auf der Shell `y` ein, um den Tabellenmodus zu deaktivieren. Wenn Sie nun z. B. `pppTable` eingeben, werden die Einträge in einem Format aufgelistet, in dem die Indizierung sichtbar ist. Aus der Kombination der Indexvariablen und ihre Wertes (inklusive des internen Indexes) ergibt sich die eindeutige Identifikation eines bestimmten Tabelleneintrags, auch wenn der Wert der Indexvariablen mehr als einmal auftritt.

Feld	Wert
Condition	Für ***TYPE*** = *time*: ■ *daily* - Die Aktion wird täglich ausgelöst (Defaultwert). ■ *<Wochentag>* - Die Aktion wird wiederkehrend an einem bestimmten Wochentag ausgelöst. ■ *mon-fri* - Die Aktion wird täglich von Montag bis Freitag ausgelöst. ■ *sat_sun* - Die Aktion wird wiederkehrend nur Samstags und Sonntags ausgelöst. ■ *day <1 .. 31>* - Die Aktion wird wiederkehrend an einem bestimmten Tag des Monats ausgelöst. Für ***TYPE*** = *value*: ■ *range* - Die Aktion wird ausgelöst, wenn der Wert der Variablen zwischen zwei bestimmten Werten liegt (Defaultwert). ■ *greater* - Die Aktion wird ausgelöst, wenn der Wert der Variablen einen bestimmten Wert übersteigt. ■ *equal* - Die Aktion wird ausgelöst, wenn der Wert der Variablen einen bestimmten Wert annimmt. ■ *less* - Die Aktion wird ausgelöst, wenn der Wert der Variablen unter einen bestimmten Wert bleibt. ■ *notequal* - Die Aktion wird ausgelöst, wenn der Wert der Variablen einen bestimmten Wert nicht annimmt.

Feld	Wert
Compare value	Der Wert, zu dem der Wert der Variablen in dem durch ***CONDITION*** bestimmten Verhältnis steht. Wenn ***CONDITION*** = *range*, so ist dies der Startwert des Wertebereichs.
End value	Wenn ***CONDITION*** = *range*, so ist dies der Endwert des Wertebereichs.
Start time (hh:mm)	Nur für ***TYPE*** = *time*. Hier geben Sie den Zeitpunkt ein, an dem die Aktion gestartet werden soll.
End time (hh:mm)	Nur für ***TYPE*** = *time*. Hier geben Sie den Zeitpunkt ein, an dem die Aktion beendet werden soll.
Status	Dieses Feld kann nicht editiert werden und zeigt den Status des Auslösers an. Mögliche Werte sind: ■ *active* - Der Auslöser ist derzeit aktiv. ■ *inactive* - Der Auslöser ist inaktiv. ■ *notavail* - Der Status kann nicht festgestellt werden, z. B. wenn der Scheduler nicht aktiviert ist. ■ *error* - Es ist ein Fehler aufgetreten, die Konfiguration des Auslösers ist nicht konsistent.
Last Change	Hier wird der Zeitpunkt der letzten Zustandsänderung angezeigt. Das Feld kann nicht editiert werden.

Tabelle 4-3: ***SYSTEM*** ➜ ***SCHEDULE & MONITOR*** ➜ ***EVENT SCHEDULER (TIME & SNMP)*** ➜ ***SCHEDULE EVENTS*** ➜ ***ADD/EDIT***

4.2.2 Konfiguration der Aktion (Command)

Welche Aktion ausgeführt wird, sobald eines der als Auslöser konfigurierten Ereignisse eintritt, wird im Menü *SYSTEM* ➜ *SCHEDULE & MONITOR* ➜ *EVENT SCHEDULER (TIME & SNMP)* ➜ *SCHEDULE COMMANDS* ➜ *ADD/EDIT* erstellt bzw. editiert.

Standardmäßig öffnet sich das Menü mit den Optionen zur Auswahl einer der voreingestellten Aktionen:

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[SYSTEM][SCHEDULED][SCHED_CMD][ADD]: Scheduler Commands      MyGateway

   Index        1        Description
     Mode                 enable
     1. Event Index       none
     Eventlist Condition  all

     Execute command      disable interface
     Interface            en1-0


     Notify               all

     Status    notavail       Last Change    01/01/1970  0:00:00

                  SAVE                            CANCEL
```

Wenn Sie für das Feld ***EXECUTE COMMAND*** den Wert *user defined* auswählen, ändert sich das Menü wie folgt:

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[SYSTEM][SCHEDULED][SCHED_CMD][ADD]: Scheduler Commands      MyGateway

  Index        1        Description
    Mode                  enable
    1. Event Index        none
    Eventlist Condition   all

    Execute command       user defined
      Table
      Variable
      Index variable
      Index value
      Set value active
          value inactive
    Notify                all

    Status    notavail       Last Change    01/01/1970  0:00:00

                  SAVE                            CANCEL
```

Je nach gewählter Einstellung enthält das Menü folgende Felder:

Feld	Wert
Index	Das Gateway vergibt automatisch eine Index-Nummer für den Eintrag. Der Wert kann aber auch editiert werden. Es stehen alle Werte von *1* bis *65535* zur Verfügung.
Description	Hier geben Sie eine beliebige Bezeichnung für das Ereignis ein. Die maximale Länge des Eintrags beträgt 30 Zeichen.

Feld	Wert
Mode	Hier wählen Sie aus, ob die konfigurierte Aktion aktiv oder inaktiv sein soll. Zur Verfügung stehen: ■ *enable* (Defaulwert) ■ *disable*
1. Event Index	Hier legen Sie das erste Ereignis einer Ereigniskette fest. Die Ereigniskette wird erst von diesem Eintrag an aktiviert, vorhergehende Einträge werden ignoriert. Defaultwert ist *none*.
Eventlist Condition	Hier legen Sie fest, ob alle Einträge einer Ereigniskette zutreffen müssen, damit eine Aktion ausgeführt wird. Zur Verfügung stehen: ■ *all* - Alle Ereignisse einer Ereigniskette müssen auftreten, damit die Aktion ausgeführt wird (Defaultwert). ■ *one* - Mindestens eines der Ereignisse einer Ereigniskette muss auftreten, damit die Aktion ausgeführt wird. ■ *none* - Keines der Ereignisse einer Ereigniskette darf eintreten, damit die Aktions ausgeführt wird. ■ *one_not* - Mindestens eines der Ereignisse einer Ereigniskette darf nicht auftreten, damit die Aktion ausgeführt wird.

Feld	Wert
Execute command	Hier legen Sie die Aktion fest, die aufgrund eines Auslösers ausgeführt wird. Zur Verfügung stehen: ■ *disable interface* - Das im Feld ***INTERFACE*** bestimmte Interface wird deaktiviert (sein ***ADMINSTATUS*** wird auf *down* gesetzt, Defaultwert). ■ *enable interface* - Das im Feld ***INTERFACE*** bestimmte Interface wird aktiviert (sein ***ADMINSTATUS*** wird auf *up* gesetzt). ■ *user defined* - Die Aktion wird in den folgenden Feldern frei konfiguriert.
Interface	Hier wählen Sie aus, welches Interface aktiviert bzw. deaktiviert werden soll, wenn für ***EXECUTE COMMAND*** *disable interface* oder *enable interface* gewählt ist. Defaultwert ist *en1-0*.
Table	Nur für ***EXECUTE COMMAND*** = *user defined*. Hier geben Sie die MIB-Tabelle ein, in der sich die zu setzende Variable befindet.
Variable	Nur für ***EXECUTE COMMAND*** = *user defined*. Hier geben Sie die MIB-Variable ein, die gesetzt werden soll.
Index variable	Nur für ***EXECUTE COMMAND*** = *user defined*. Hier geben Sie die Indexvariable der zuvor ausgewählten MIB-Tabelle ein. Dies ist in einer beliebigen MIB-Tabelle diejenige Variable, die in der Tabellenansicht mit einem Asterisk (*) markiert ist.

Feld	Wert
Index value	Nur für ***EXECUTE COMMAND*** = *user defined*. Hier geben Sie den Wert ein, den die Indexvariable für den Tabelleneintrag hat, der durch die Aktion geändert werden soll. Die Einträge in einer MIB-Tabelle werden intern indiziert. In der normalen Tabellenansicht wird diese Indizierung nicht angezeigt. Geben Sie auf der Shell `y` ein, um den Tabellenmodus zu deaktivieren. Wenn Sie nun z. B. `pppTable` eingeben, werden die Einträge in einem Format aufgelistet, in dem die Indizierung sichtbar ist. Aus der Kombination der Indexvariablen und ihre Wertes (inklusive des internen Indexes) ergibt sich die eindeutige Identifikation eines bestimmten Tabelleneintrags, auch wenn der Wert der Indexvariablen mehr als einmal auftritt.
Set value active	Nur für ***EXECUTE COMMAND*** = *user defined*. Hier geben Sie den Wert ein, den die ***VARIABLE*** durch die Aktion zugewiesen bekommen soll. Der Wert wird gesetzt, sobald ein entsprechender Auslöser aktiv wird und bleibt solange erhalten, bis der Auslöser wieder inaktiv wird.
value inactive	Nur für ***EXECUTE COMMAND*** = *user defined*. Hier geben Sie den Wert ein, den die Variable annimmt, sobald der Auslöser inaktiv wird. Dieser Wert wird der Variablen auch nach einem Neustart des Gateways zugewiesen oder wenn die Systemzeit nicht korrekt eingestellt ist.

Feld	Wert
Notify	Hier wählen Sie aus, welche Mechanismen verwendet werden, um über Aktionen zu informieren. Zur Verfügung stehen: ■ *all* - Es werden sowohl SNMP-Traps als auch Syslog-Meldungen erzeugt. ■ *snmptrap* - Es werden nur SNMP-Traps erzeugt. ■ *syslog* - Es werden nur Syslog-Meldungen erzeugt. ■ *none* - Es werden keine Meldungen erzeugt.
Status	Dieses Feld kann nicht editiert werden und zeigt den Status des Auslösers an. Mögliche Werte sind: ■ *active* - Der Auslöser ist derzeit aktiv. ■ *inactive* - Der Auslöser ist inaktiv. ■ *notavail* - Der Status kann nicht festgestellt werden, z. B. wenn der Scheduler nicht aktiviert ist. ■ *error* - Es ist ein Fehler aufgetreten, die Konfiguration des Auslösers ist nicht konsistent.
Last Change	Hier wird der Zeitpunkt der letzten Zustandsänderung angezeigt. Das Feld kann nicht editiert werden.

Tabelle 4-4: ***SYSTEM ➜ SCHEDULE & MONITOR ➜ EVENT SCHEDULER (TIME & SNMP) ➜ SCHEDULE COMMANDS ➜ ADD/EDIT***

5 Untermenü *PASSWORD SETTINGS*

Im folgenden werden die Felder des Untermenüs *PASSWORD SETTINGS* beschrieben.

Das Einstellen der Paßwörter gehört zu den grundlegenden Systemeinstellungen.

Das Menü ***PASSWORD SETTINGS*** besteht aus folgenden Feldern:

Feld	Wert
admin Login Password/SNMP Community	Paßwort für Benutzername `admin`
read Login Password/SNMP Community	Paßwort für Benutzername `read`
write Login Password/SNMP Community	Paßwort für Benutzername `write`
HTTP Server Password	Paßwort für die HTTP-Statusseite Ihres Gateways
Activity Monitor Password	Paßwort für den ***ACTIVITY MONITOR***

Tabelle 5-1: Felder im Menü ***PASSWORD SETTINGS***

Achtung!

Alle Bintec-Gateways werden mit gleichem Benutzernamen und Paßwort ausgeliefert. Sie sind daher nicht gegen einen unautorisierten Zugriff geschützt, solange die Paßwörter nicht geändert wurden.

Ändern Sie unbedingt die Paßwörter, um unberechtigten Zugriff auf das Gateway zu verhindern.

6 Untermenü *TIME AND DATE*

Im folgenden werden die Felder des Untermenüs *TIME AND DATE* beschrieben.

Systemzeit

Die Systemzeit benötigen Sie, um korrekte Zeitstempel bei der Aufzeichnung von Verbindungsdaten (Accounting) zu erhalten.

Sie können die Systemzeit:

- automatisch beziehen, z. B. über ISDN oder über einen Time-Server. Die entsprechende Konfiguration wird im Menü ***IP*** ➜ ***STATIC SETTINGS*** vorgenommen.
- manuell auf dem Gateway einstellen.

Hinweis

Wenn auf dem Gateway zusätzlich eine Methode zum automatischen Beziehen der Zeit festgelegt ist, haben die auf diese Weise erhaltenen Werte höhere Priorität. D. h. falls das Gateway ein entsprechendes Zeitsignal erhält (z. B. von einem Time-Server), wird eine evtl. manuell eingegebene Systemzeit überschrieben.

Im Menü ***SYSTEM*** ➜ ***TIME AND DATE*** finden Sie Einstellungen zur manuellen Eingabe von Uhrzeit und Datum auf Ihrem Gateway.

Das Menü ***TIME AND DATE*** besteht aus folgenden Feldern:

Feld	Wert
Time is currently controlled by:	Zeigt an, welche Einstellungen für ein automatisches Beziehen der Systemzeit unter ***IP*** ➜ ***STATIC SETTINGS*** festgelegt sind.
Current Time:	Zeigt die aktuell auf dem **VPN Access Gateway** eingestellte Systemzeit an (Datum und Uhrzeit).
New Time:	Hier wird die neue Uhrzeit eingegeben, die das **VPN Access Gateway** verwenden soll (hh:mm).

Feld	Wert
New Date:	Hier wird das neue Datum eingegeben, das das **VPN Access Gateway** verwenden soll (mm/tt/jjjj).

Tabelle 6-1: Felder im Menü ***TIME AND DATE***

Index: System