

ads-tec GmbH

# IRF2000

## Application Note

## Eingeschränkter Remote Zugriff



## Inhaltsverzeichnis

<b>1</b>	<b>Einführung</b> .....	<b>3</b>
<b>2</b>	<b>Benutzerkonten</b> .....	<b>4</b>
2.1	Neues Benutzerkonto anlegen .....	4
2.2	Benutzerkonto aktivieren .....	5
<b>3</b>	<b>Variablenrechte</b> .....	<b>6</b>
3.1	Variablenrechte für bestimmten Benutzer vergeben.....	6
<b>4</b>	<b>Paketfilter</b> .....	<b>8</b>
4.1	Regelsets .....	8

## Application Note – eingeschränkter Remote Zugriff

Das Original dieser Betriebsanleitung wurde in deutscher Sprache verfasst. Jede nicht deutschsprachige Ausgabe dieser Betriebsanleitung ist eine Übersetzung der deutschen Betriebsanleitung.

# 1 Einführung

Dieses Dokument zeigt, wie Sie einen eingeschränkten Remotezugriff auf Ihrem ads-tec Router einrichten. Ziel ist dabei als Anlagenlieferant einen eingeschränkten Zugriff zu erhalten und dem Endkunden den Admin Account zu überlassen.

### Hinweis:

Oft wird ein Netzwerk über Big-LinX angebunden und dabei folgende Anforderung realisiert:

- Die internen Systeme des Netzwerks hinter dem Router/Firewall dürfen nicht auf das Internet zugreifen.
- Die Big-LinX Teilnehmer dürfen nicht über den Router auf das Internet zugreifen.
- Die Big-LinX Teilnehmer dürfen ausschließlich auf das interne Netzwerk zugreifen und nicht etwa auf ein darüberliegendes Endkundennetzwerk am Uplink des Routers.

### Voraussetzungen:

Eine bestehende und funktionierende Big-LinX Verbindung mit einem ads-tec Router.

Zum Einsatz kommen entsprechende Paketfilter die dies regeln.

(siehe Application Note Big-LinX-only-Filter) Die nachfolgende Abbildung zeigt die entsprechende Topologie.

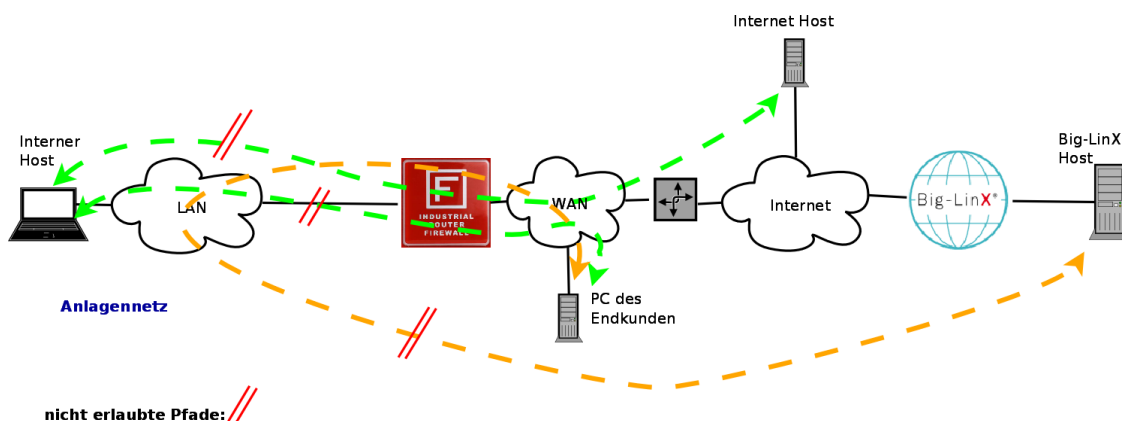


Abbildung 1: Netzwerktopologie

Das Benutzerkonto mit dem eingeschränkten Remote Benutzer bringt hier zusätzliche Sicherheit für diesen speziellen Anwendungsfall.

Dieses Dokument erläutert nun die nötigen Schritte den Benutzer anzulegen und die entsprechenden Rechte zuzuweisen. Im Ergebnis entsteht dann ein Benutzer der als Remote User mit eingeschränkten Rechten genutzt werden kann. Der Benutzer hat daraufhin folgende Rechte:

- Schreibrecht zum Parametrieren des Uplinks
- Schreibrecht zum Parametrieren von Big-LinX
- Schreibrecht für die Durchführung eines Firmware Update

### Hinweis:

Durch diese Einschränkungen hat dieser Benutzer somit auch keine Rechte um Änderungen am Paketfilter vorzunehmen um sich darüber evtl. Zugang zu verschaffen.

Somit eine wichtige zusätzliche erweiterte Sicherung für die bestehende Netzwerktopologie.

## 2 Benutzerkonten

### 2.1 Neues Benutzerkonto anlegen

Auf der Weboberfläche unter Konfiguration-Zugriffsrechte-Benutzerkonten kann ein neues Benutzerkonto erstellt werden. Dazu im Menü „neues Benutzer Konto“ den Benutzernamen sowie ein Passwort angeben. Im nachfolgenden Beispiel heißt der Benutzer „remote“. (Abbildung 2)

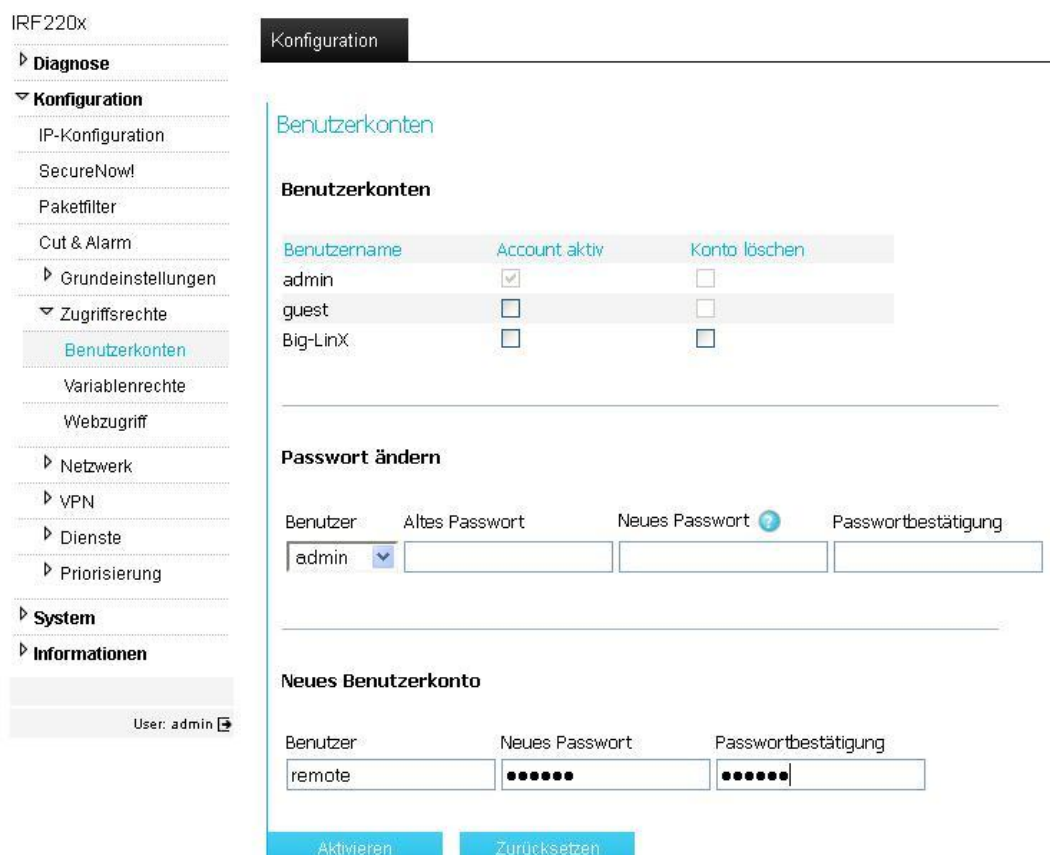


Abbildung 2: neues Benutzerkonto anlegen

## 2.2 Benutzerkonto aktivieren

Über den Button Aktivieren werden die Eingaben bestätigt und das neue Benutzerkonto aktiviert. Das eben eingerichtet Konto wird nun unter Benutzerkonten aufgeführt und hat automatisch einen Haken bei aktiv gesetzt.

### **Hinweis:**

Je nach dem welche eingerichteten Konten aktiv sein sollen kann man an dieser Stelle den Haken setzen oder entfernen. (Abbildung 3)

### **Benutzerkonten**

Benutzername	Account aktiv	Konto löschen
admin	<input checked="" type="checkbox"/>	<input type="checkbox"/>
guest	<input type="checkbox"/>	<input type="checkbox"/>
Big-LinX	<input type="checkbox"/>	<input type="checkbox"/>
remote	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Abbildung 3: Account aktiv

## 3 Variablenrechte

### 3.1 Variablenrechte für bestimmten Benutzer vergeben

Unter Konfiguration – Zugriffsrechte – Variablenrechte lassen sich nun für alle Optionen entsprechend die Schreibrechte per Auswahlfeld aktivieren. (Abbildung 4).

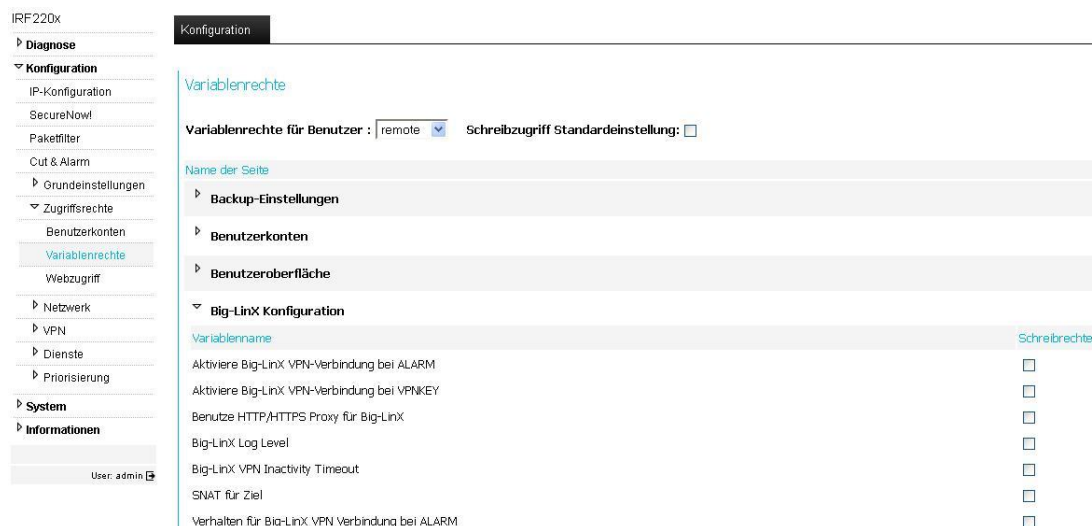


Abbildung 4: Auszug der verschiedenen Variablenrechte

Für unser Beispiel des „Remote“ Benutzers benötigen sie Schreibrechte für die entsprechenden Optionen die erlaubt werden sollen (siehe Abbildung 5):

- Big-LinX Konfiguration
- Big-LinX PIN Konfiguration
- Big-LinX Panel
- Softwareupdate

Über den Button „Aktivieren“ werden die Änderungen übernommen und dem Benutzerkonto zugewiesen.

## Application Note – eingeschränkter Remote Zugriff





▼ Big-LinX Konfiguration 	
Variablenname	Schreibrechte
Aktiviere Big-LinX VPN-Verbindung bei ALARM	<input checked="" type="checkbox"/>
Aktiviere Big-LinX VPN-Verbindung bei VPNKEY	<input checked="" type="checkbox"/>
Benutze HTTP/HTTPS Proxy für Big-LinX	<input checked="" type="checkbox"/>
Big-LinX Log Level	<input checked="" type="checkbox"/>
Big-LinX VPN Inactivity Timeout	<input checked="" type="checkbox"/>
SNAT für Ziel	<input checked="" type="checkbox"/>
Verhalten für Big-LinX VPN Verbindung bei ALARM	<input checked="" type="checkbox"/>
Verhalten für Big-LinX VPN Verbindung bei VPNKEY	<input checked="" type="checkbox"/>
World-Wide-Heartbeat-Intervall	<input checked="" type="checkbox"/>
aktiviere den World-Wide-Heartbeat	<input checked="" type="checkbox"/>
▼ Big-LinX PIN Konfiguration 	
Variablenname	Schreibrechte
Alte Smartcard PIN	<input checked="" type="checkbox"/>
Neue Smartcard PIN	<input checked="" type="checkbox"/>
Smartcard PIN	<input checked="" type="checkbox"/>
Speichere PIN auf dem Gerät	<input checked="" type="checkbox"/>
▼ Big-LinX Panel 	
Variablenname	Schreibrechte
VPN Big-LinX lokaler Informationstext	<input checked="" type="checkbox"/>
VPN Verbindung schalten	<input checked="" type="checkbox"/>
VPN Verbindungstest, letzter erfolgreicher Test	<input checked="" type="checkbox"/>
VPN schalte Verbindung an	<input checked="" type="checkbox"/>
VPN schalte Verbindung aus	<input checked="" type="checkbox"/>
▼ Softwareupdate 	
Variablenname	Schreibrechte
Dateiname und Ort	<input checked="" type="checkbox"/>
Protokoll	<input checked="" type="checkbox"/>
Server Adresse	<input checked="" type="checkbox"/>
Setze Werkseinstellungen der neuen Firmware	<input checked="" type="checkbox"/>
Update von Server	<input checked="" type="checkbox"/>

Abbildung 5: aktivierte Schreibrechte bei den benötigten Optionen

## 4 Paketfilter

### 4.1 Regelsets



Abbildung 6: Regelsets entsprechend der vorgebenden Netzwerktopologie (siehe Abbildung 1)

Mit Hilfe dieser Regelsets wird sowohl der ausgehende als auch der ankommende Traffic über Big-LinX geregelt. (siehe Application Note „Big-LinX only Filter“).

Der zuvor eingerichtete „Remote User“ kann bedingt durch seine eingeschränkten Rechte diese Regeln auch nicht umgehen und birgt daher ein hohes Maß an Sicherheit.