



Quick Guide

PowerPanel[®] Business Management

SNMP-Anbindung und Monitoring
von APC/Eaton USVs

Inhaltverzeichnis

Ziel und Anwendungsbereich.....	3
Voraussetzungen.....	3
Unterstützte SNMP-Versionen.....	3
SNMPv1	4
SNMPv3	5
Bereich der automatischen Erkennung.....	6
Sicherheit	7
PowerPanel Passphrase	8
SSL-Zertifikat	8
Monitoring	8
FAQ	10

Ziel und Anwendungsbereich

Diese Anleitung beschreibt, wie APC und Eaton USVs über SNMP in PowerPanel® Business Management eingebunden und überwacht werden können.

Der Fokus liegt auf der **Netzwerküberwachung über SNMPv1/SNMPv3**, einschließlich Geräteerkennung, SNMP-Konfiguration und Monitoring im Dashboard.

Diese Anleitung behandelt keine USB oder Local Verbindung und keine Shutdown-Konfiguration. Sie dient ausschließlich als Quick Guide für die zentrale Überwachung von Drittanbieter-USVs über Netzwerk/SNMP.

Voraussetzungen

Für die Einbindung von **APC- und Eaton-USVs über SNMP** in PowerPanel® Business Management müssen folgende Voraussetzungen erfüllt sein:

- PowerPanel® Business Management ist installiert und über den Webbrowser erreichbar.
- Die Netzwerkkarte der APC oder Eaton USV ist im Netzwerk erreichbar.
- Die IP-Adresse der USV-Netzwerkkarte ist bekannt.
- SNMP ist auf der APC- oder Eaton-USV aktiviert.
- Die passenden SNMP-Zugangsdaten sind vorhanden:
 - bei SNMPv1: Community-Name, z. B. public oder kundenspezifisch
 - bei SNMPv3: Benutzername, Authentifizierungsprotokoll, Authentifizierungsschlüssel, Datenschutzprotokoll und Datenschuttschlüssel
- Die erforderlichen Firewall-Ports sind freigegeben, insbesondere SNMP-Port 161/UDP und Trap-Port 162/UDP.

PowerPanel® Business Management ist für die zentrale Überwachung mehrerer USV-, PDU- und ATS-Systeme im Netzwerk vorgesehen. Daher kann es auch zur zentralen SNMP-Überwachung kompatibler APC und Eaton USVs verwendet werden.

Unterstützte SNMP-Versionen

PowerPanel® Business Management kann neben CyberPower-Geräten auch USVs von Drittanbietern über SNMP überwachen.

Die Konfiguration erfolgt unter: **Einstellungen → Netzwerkkonfigurationen → SNMP-Konfigurationen** Dort können SNMP-Profile für APC- oder Eaton-Geräte über **SNMPv1** oder **SNMPv3** angelegt werden.

The screenshot shows the 'MANAGEMENT' interface of PowerPanel Business. The 'EINSTELLUNG' (Settings) menu is open, showing 'SNMPv1' and 'SNMPv3' options. The 'SNMPv1' sub-menu is expanded, showing 'Netzwerkkonfigurationen' (Network Configurations) and 'SNMP-Konfigurationen' (SNMP Configurations). The 'SNMP-Konfigurationen' sub-menu is also expanded, showing 'SNMP Community' and 'SNMP Trap Community' options. Below the menu, there is a table of existing configurations:

MIB des Herstellers	Profil-Name	Anwendername	Authentifizierungsprotokoll	Authentifizierungsschlüssel	Privatsphäre Protokoll	Privater Schlüssel
CyberPower	CyberPower V3	cyber snmpv3 user1	Keine		Keine	
EATON			MD5		DES	

SNMPV1

Bei **SNMPv1** erfolgt die Kommunikation über eine sogenannte **SNMP-Community**. Diese Community dient zur Authentifizierung zwischen PowerPanel® Business Management und der APC oder Eaton USV.

PowerPanel® Business Management verwendet die SNMP-Community, um auf die Informationen der USV zuzugreifen. Die Community muss mit der Einstellung auf der Netzwerkkarte der APC oder Eaton USV übereinstimmen.

EINSTELLUNGEN FÜR SNMPV1

Im Fenster **Add SNMPv1** werden folgende Angaben benötigt:

Active: Aktiviert oder deaktiviert dieses SNMP-Profil.

Vendor MIB: Auswahl des Herstellers bzw. MIB-Profiles. Für diese Anleitung wird hier **APC** oder **Eaton** ausgewählt.

Profile Name: Name des SNMP-Profiles. Dieser Name dient zur Identifikation des Profils in PowerPanel® Business Management.

SNMP-Community: Community-Name für den Zugriff auf die USV-Daten. Häufig wird bei SNMPv1 standardmäßig **public** für Lesezugriff oder **private** für Schreibzugriff verwendet. Für administrative Steuerungsfunktionen muss die verwendete Community auf der USV-Netzwerkkarte über die entsprechenden Rechte verfügen.

SNMP-Trap-Community: Community Name für SNMP-Traps. Diese wird verwendet, um Ereignismeldungen der USV an PowerPanel® Business Management zu authentifizieren.

Damit Trap-Meldungen korrekt empfangen werden können, muss die IP-Adresse des Computers, auf dem PowerPanel® Business Management installiert ist, auf der APC- oder Eaton-Netzwerkkarte als **Trap Receiver** eingetragen werden.

The screenshot shows the 'Add SNMPv1' configuration window. The 'Active' checkbox is checked. The 'Vendor MIB' dropdown is set to 'APC (1.3.6.1.4.1.318)'. The 'Profile Name' dropdown is set to 'CyberPower (1.3.6.1.4.1.3808)'. The 'SNMP Community' dropdown is set to 'APC (1.3.6.1.4.1.318)'. The 'SNMP Trap Community' field is empty. The 'CANCEL' and 'SAVE' buttons are visible at the bottom.

HINWEISE ZU SNMPV1

1. Es ist essenziell, dass die SNMP-Community in PowerPanel® Business Management und auf der APC oder Eaton USV übereinstimmt.
2. Wenn die USV nicht gefunden wird oder keine Daten angezeigt werden, sollten die folgenden Punkte geprüft werden: Wurde SNMPv1 auf der Netzwerkkarte der USV aktiviert?
 - Ist die richtige Community eingetragen?
 - Wurde das passende MIB-Profil für APC oder Eaton ausgewählt?
 - Wurde die IP-Adresse von PowerPanel® Business Management - Verwaltungscomputer- zur Trap-Empfängerliste auf der SNMPv1-Einstellungsseite der USV-Netzwerkkarte von APC und Eaton hinzugefügt, um sicherzustellen, dass die Community übereinstimmt?
 - Sind die erforderlichen Netzwerkports freigegeben?

Für die Kommunikation werden insbesondere folgende Ports benötigt:

161/UDP für SNMP-Abfragen

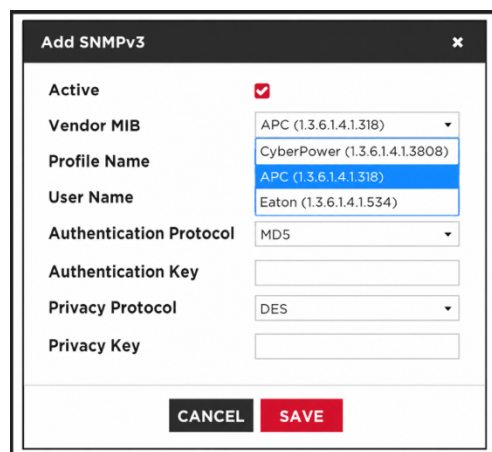
162/UDP für SNMP-Traps

3052 TCP/UDP, 53566/UDP und **53568/TCP** für PowerPanel® Business Management

SNMPV3

PowerPanel® Business Management verwendet die folgenden SNMPv3-Einstellungen für die Kommunikation mit einem sicheren Gerät. Diese Einstellungen können auf der Seite **Einstellungen → Netzwerkkonfigurationen → SNMP-Konfigurationen** von PowerPanel® Business Management sowie auf der SNMPv3-Einstellungsseite der UPS Netzwerkkarte von APC und Eaton konfiguriert werden. Diese Einstellungen müssen übereinstimmen.

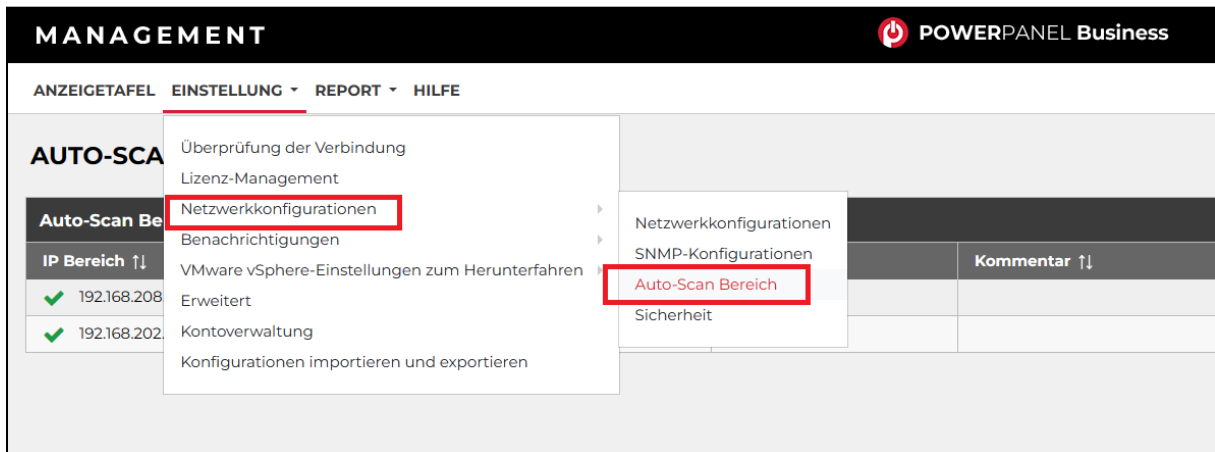
- **Benutzername:** Gibt einen passenden Benutzernamen für das Protokoll an.
- **Authentifizierungsprotokoll:** Legt das Protokoll fest, das für die Authentifizierung der Netzwerkkommunikation zwischen PowerPanel Business und den Geräten verwendet werden soll.
- **Authentifizierungsschlüssel:** Legt den Authentifizierungsschlüssel fest, der für das Authentifizierungsprotokoll verwendet wird .
- **Datenschutzprotokoll:** Legt das Datenschutzprotokoll fest, das zur Verschlüsselung der Daten während der Übertragung zwischen PowerPanel Business und den Geräten verwendet wird.
- **Datenschutzschlüssel:** Legt den Datenschutzschlüssel fest, mit dem Daten für das Authentifizierungs
- **Datenschutzprotokoll** verschlüsselt werden.



Bereich der automatischen Erkennung

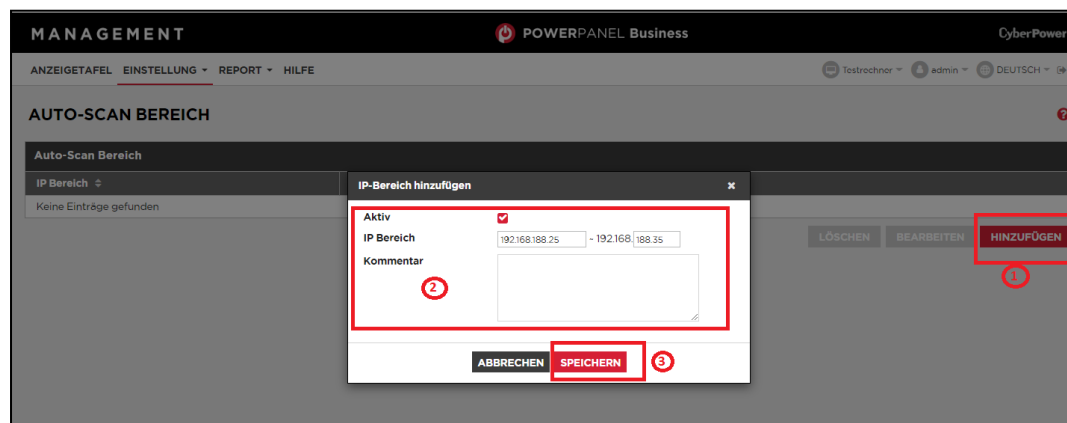
Um Geräte und Computer in verschiedenen Segmenten oder einem bestimmten Bereich zu suchen, können Benutzer auf dieser Seite den IP-Bereich einstellen.

Klicken Sie in der Weboberfläche auf **Einstellung**→**Netzwerkkonfiguration**→**Auto-Scan Bereich**



IP-Bereich hinzufügen

Klicken Sie auf die Schaltfläche **HINZUFUGEN** und es erscheint ein Dialogfeld **IP-Bereich hinzufügen**. Geben Sie alle erforderlichen Daten ein und klicken Sie auf die Schaltfläche **SPEICHERN**, um einen neuen IP-Bereich in die Liste aufzunehmen.

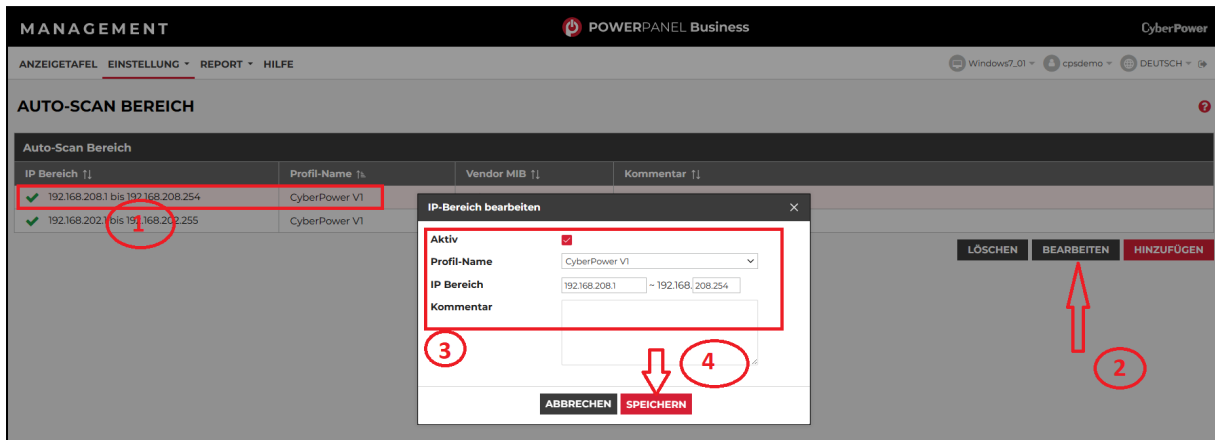


IP-Bereich ändern:

Wählen Sie den IP-Bereich, den Sie ändern möchten und klicken Sie auf die Schaltfläche

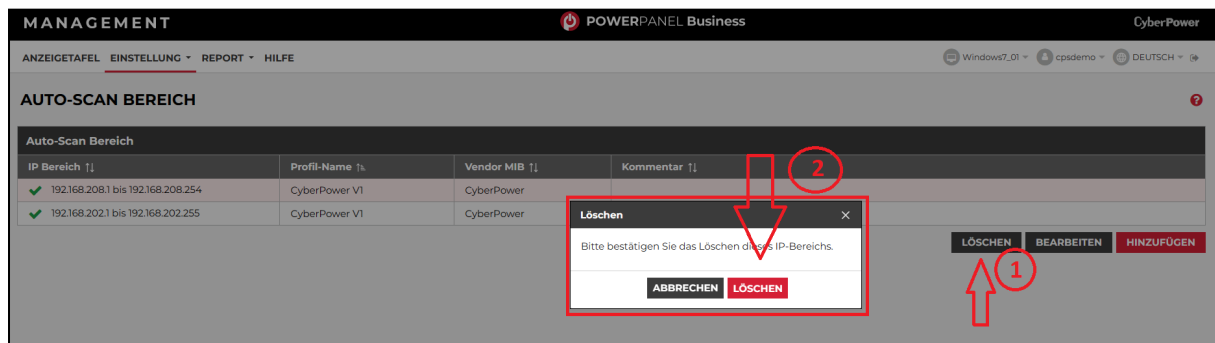
BEARBEITEN . Geben Sie die neuen Daten ein

Klicken Sie zum Abschluss auf die Schaltfläche **SAVE**.



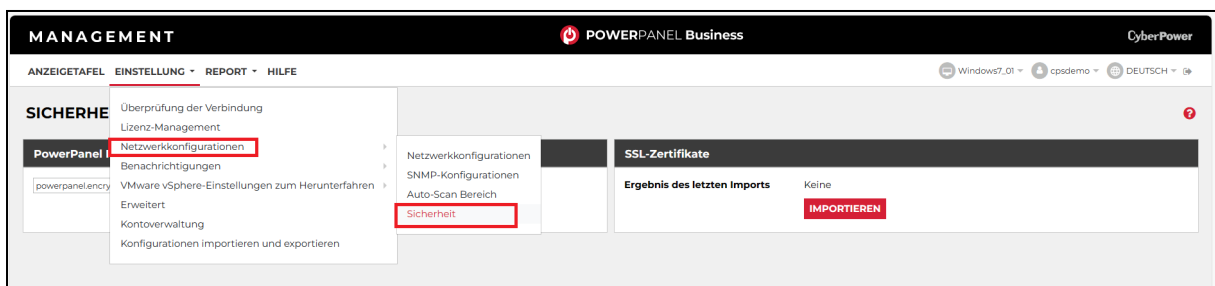
IP-Bereich entfernen:

Wählen Sie den zu entfernenden IP-Bereich aus der Liste der IP-Bereiche aus, und klicken Sie dann auf **LÖSCHEN**, um das Löschen des IP-Bereichs abzuschließen.



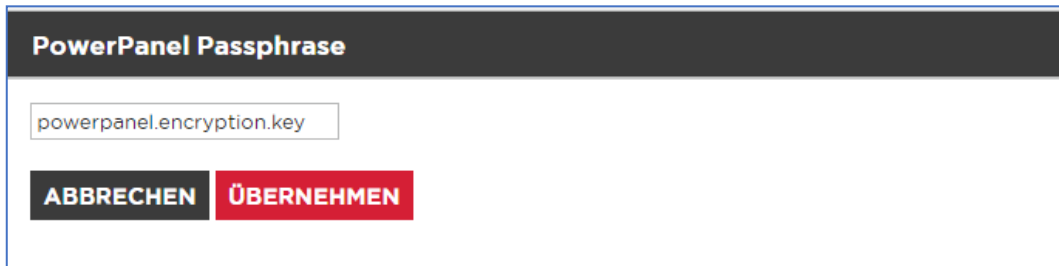
Sicherheit

Klicken Sie in der Weboberfläche auf **Einstellung** und wählen **Sicherheit**.



PowerPanel Passphrase

Der PowerPanel Passphrase wird verwendet, um eine sichere Netzwerkkommunikation zwischen PowerPanel® Business Software und USV RMCARD/PDU herzustellen. Der Standardphrase ist **powerpanel.encryption.key**. Die geheime Phrase kann auf der Seite **EINSTELLUNGEN/Sicherheit** im PowerPanel® Business Software oder auf der Seite System/Authentifizierung in der Webschnittstelle von PDU und UPS RMCARD konfiguriert werden. Die geheime Phrase, die im PowerPanel® Business Software und in den Geräten verwendet wird, muss übereinstimmen.




SSL-Zertifikat

Der Browser des Benutzers, der sich mit der PowerPanel® Business Webschnittstelle verbindet, dient dem SSL-Zertifikat.

Klicken Sie auf die Schaltfläche **IMPORTIEREN**, um den *Assistenten für SSL-Zertifikate* zu starten. Laden Sie die SSL-Zertifikatsdatei hoch.

Geben Sie das Feld **Schlüsselphrase** und das Feld **Keystore-Kennwort** ein. Klicken Sie auf die Schaltfläche **IMPORTIEREN**, um die SSL-Zertifikate zu importieren.

Hinweis: Die Beantragung eines Zertifikats beim kommerziellen Zertifikatsanbieter ist kostenpflichtig



Monitoring

Nach dem Hinzufügen der APC- oder Eaton-USV wird das Gerät im **Dashboard** von PowerPanel® Business Management angezeigt. Dort kann der aktuelle Betriebszustand der USV zentral überwacht werden.

Im Dashboard sind unter anderem folgende Informationen sichtbar:

- aktueller **Status** der USV, z. B. Normal, Warnung oder Kommunikationsverlust
- **Ereignisse** und Warnmeldungen
- **Eingangs- und Ausgangswerte**
- aktuelle **Last**
- **Batteriestatus**

- verbleibende **Laufzeit**
- Standort und verwendetes SNMP-Profil
- Kommunikationsstatus zwischen PowerPanel® Business Management und der USV

MANAGEMENT		POWERPANEL Business		CyberPower					
ANZEIGETAFEL		EINSTELLUNG		REPORT		HILFE			
Status		Suche		Windows7_01		cpsdemo		DEUTSCH	
ANZEIGETAFEL		Standort		Profil-Name		210Wh		225W	
APC Smart-UPS SMT750IC	Normal. Die Batterie ist vollständig aufgeladen.	12F SW	APC v3(Default)	120V	100% 1h:22m	20% 100W			
OLI500RTL2U	Batterie muss ersetzt werden. Die Batterie ist vollständig aufgeladen.	12F SW	CyberPower V1	114V 120.2V	100% 1h:45m	0% 0W			
PDU205WT10ATNET	Eingabe hat keine Belastung. Wechsel auf Quelle A. Normal.	12F SW	CyberPower V1						
PDU205W8FNET-E1	Normal. Ausgang #6 wurde eingeschaltet.	12F SW	CyberPower V1						
ATS	Ausfall der redundanten Versorgung. Eingabe hat keine Belastung. Ausgang #10 wurde eingeschaltet.	Server Room	CyberPower V1	46%RH	29.9°C				
PDU305WT17ATNET	Die Netzwerkkommunikation ist fehlergeschlagen.	12F SW	CyberPower V1	37%RH	29.0°C				2.7A 0W
PDU205W8FNET-E2	Eingabe hat keine Belastung. Ausgang #5 wurde eingeschaltet. Normal.	12F SW	CyberPower V1						
RMCARD205	Normal. Die Batterie ist vollständig aufgeladen.	12F SW	CyberPower V1	111V 120V	100% 1h:43m	0% 10W			
RMCARD205	Batterie muss ersetzt werden. Die Batterie ist vollständig aufgeladen.	12F SW	CyberPower V1	114V 120V	100% 1h:45m	0% 0W			
220	Die Netzwerkkommunikation ist fehlergeschlagen.	12F SW	CyberPower V1						1.6A 129W
Eaton SP 1500i	Normal. Die Batterie ist vollständig aufgeladen.	12F SW	Test0219	119V 120V	100% 1h:40m	15% 90W			
Eaton 9PX 3000i	Normal. Die Batterie ist vollständig aufgeladen.	Server Room	Eaton 3000VA	118V 120V	100% 2h:10m	25% 750W			

Über das Informationssymbol des Geräts können weitere Details geöffnet werden. Dort werden zusätzliche Werte wie Hersteller-MIB, SNMP-Profil, Gerätename, IP-Adresse, Stromquelle und Gerätestatus angezeigt.

Details	
Zusammenfassung	Status
MIB des Herstellers	APC (1.3.6.1.4.1.318)
SNMP-Profil-Name	APC v3(Default)
Name des Geräts	APC smart UPS SMT750IC
Status	Normal
Standort	12F SW
Kontakt	CyberPower Germany
Adresse	<u>192.168.208.125</u>
PC und Ausrüstung	0
Energiequelle	Netzversorgung

FAQ

1. Welches Netzwerkprotokoll wird in PowerPanel® Business verwendet?

SNMP wird für die Kommunikation zwischen REMOTE, PPB Management, PDU oder USV mit RMCARD- PPB Management karte verwendet. HTTP und HTTPS werden zwischen dem Lokalen und dem PPB MANAGEMENT verwendet.

2. Welche Netzwerk Ports werden von PowerPanel® Business verwendet?

Port 3052 (UDP/TCP), Port 53568 (TCP), Port 161(UDP), Port 162 (UDP) und Port 53566(UDP)

3. Wie stelle ich sicher, dass die SNMP-Einstellungen zwischen PPB MANAGEMENT und USV/PDU/ATS korrekt eingerichtet sind?

Um die Trap-Benachrichtigung von der USV/PDU/ATS ständig zu erhalten, führen Sie die folgenden Schritte aus, um die SNMP-Einstellungen zu überprüfen:

- ✓ Öffnen Sie die Seite Netzwerk-/Trap-Benachrichtigung auf der Website von UPS/PDU/ATS und die Seite EINSTELLUNGEN/Sicherheit auf der Fernbedienung.
- ✓ Vergewissern Sie sich, dass die IP-Adresse der Fernbedienung auf der Seite Netzwerk-/Trap-Benachrichtigung auf der Website von UPS/PDU/ATS zu finden ist. Wenn die IP-Adresse gesucht werden kann, überspringen Sie den Schritt 3.
- ✓ Wenn die IP-Adresse des PPB MANAGEMENT nicht gefunden werden konnte, klicken Sie auf die Tastenkombination Trap Receiver auf der Seite Network/Trap Notifikation, um zur Seite Trap Konfiguration zu gelangen. Geben Sie die erforderlichen Daten ein, um einen neuen Trap-Empfänger hinzuzufügen.
- ✓ Wenn die IP-Adresse des PPB MANAGEMENT gefunden werden konnte, überprüfen Sie, ob die SNMP-Einstellungen übereinstimmen.

CyberPower

[CyberPower | USV Systeme, PDU, Überspannungsschutz | Professionelle Stromversorgung Lösungen](#)

CyberPower Systems GmbH
Edisonstr. 16,
85716 Unterschleissheim
Germany

T: +49-89-1 222 166 -0 F: +49-89-1 222 166 -29

E-mail: service@cyberpower.de

Web: www.cyberpower.de

[Home | CyberPower Wiki \(cyberpowersystems.de\)](#)

CyberPower und das CyberPower-Logo sind Marken von Cyber Power Systems, Inc. und/oder verbundenen Unternehmen, die in vielen Ländern und Regionen registriert. Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber.