PANDUIT™ infrastructure for a connected world

smartzone™

Technical Reference 88-SZ

Published: **7/25/18**

SmartZone: JACE Security

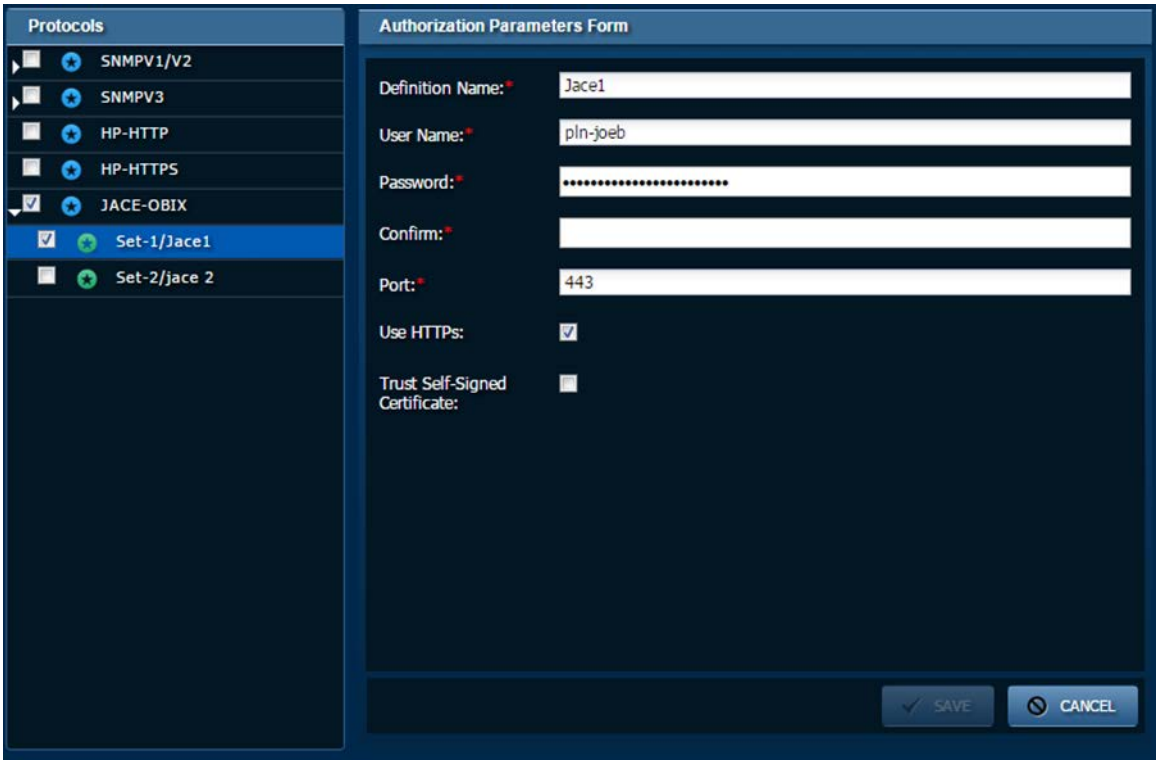
Applies to:	SmartZone JACE
Objective:	Configure Authorization for JACE devices in SmartZone DCIM.
Documentation Reference:	SmartZone DCIM User Manual, Admin Topics/Discovery/General Settings
Pre-Requisites:	At least one JACE device

IMPORTANT: SmartZone only uses Read access and does not in any way write back to the JACE.

Panduit SmartZone software communicates with JACE devices using oBIX. oBIX (Open Building Information Exchange) is a standard of RESTful APIs for building control systems.

SmartZone reads data over a network of devices using XML and URIs, within a framework specifically designed for building automation.

The communication uses the standard HTTP or HTTPS protocols. As far as security is concerned, HTTPS ensures privacy and server authentication. Authorization for resources on the JACE is controlled through user/password credentials. These are defined on the JACE and are then specified as a configuration in SmartZone (see screenshot below).


Protocols
SNMPV1/V2
SNMPV3
HP-HTTP
HP-HTTPS
JACE-OBIX
Set-1/Jace1
Set-2/jace 2
Authorization Parameters Form
Definition Name:*
Jace1
User Name:*
pln-joeb
Password:*
Confirm:*
Port:*
443
Use HTTPs:
Trust Self-Signed Certificate:
SAVE
CANCEL