SNMP
Differences Between v2 and v3

APPLICATION NOTE

October 2015

Description: Introduction to the main differences between SNMP v2 protocol and the newer SNMP v3.

Introduction

SNMP v1 and v2 have been extensively used in the network management world, but they always lacked in our very specific area: security.

SNMP v1 and SNMP v2 rely on "community strings" as a form of plain-text password that is used to authenticate the user/system with the device they are trying to communicate with. Because these "passwords" are not protected in any way, it is very easy for someone with local network access to *sniff* them and gain access to all the data exposed through SNMP protocol.

SNMP v3 does not introduce too many changes to the protocol implementation, but rather focuses on its security weaknesses, by adding authentication and encryption mechanism.

With this latest version it is now possible to use SNMP in a more secure way. GENESIS64 supports SNMP v3 starting from version 10.90.

Configuring SNMP v3 in Workbench

In order to set up SNMP v3 to communicate with your devices, you will be using the Workbench. Browse to SNMP node under "Data Connectivity" branch and select the device you want to configure (in this case we will use an existing one).

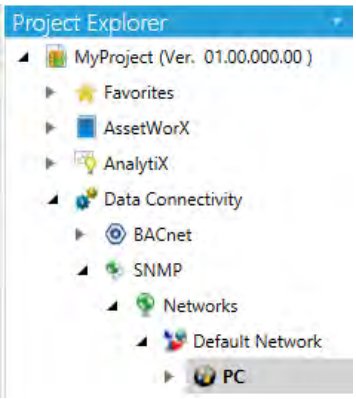

Figure 1 – Accessing an SNMP device configuration

Open the device configuration form and locate the "Device Data" section. In there you will find a dropdown menu called "SNMP Version".

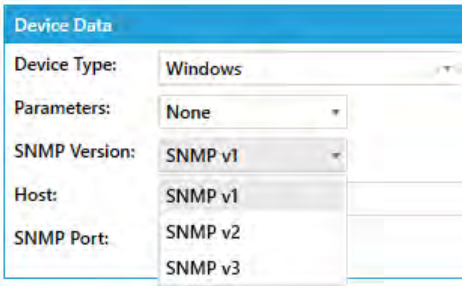

Figure 2 – Selecting SNMP version

When you select "SNMP v3" the section "SNMP v3 Settings" on the bottom of the form will be enabled.

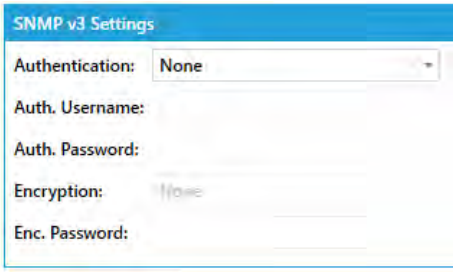

Figure 3 –SNMP v3 settings

From here you can proceed by configuring the Authentication and Encryption settings as needed.

The options for Authentication are "None", "SHA" and "MD5". By selecting an option other than "None", the "Auth. Username" and "Auth. Password" fields will be enabled, along with "Encryption".

The specified credentials will be *hashed* using the selected algorithm, either SHA or MD5. A hashing algorithm makes it easy to verify a password without having to share it directly. Hashing details are outside the scope of this document, but there's plenty of documentation on the Web, for those interested.

The Encryption settings allow to define which encryption algorithm should be used to secure communication with the device. Available options are AES 128/192/256, DES and Triple DES.

You can use these security settings in case you need to use Federal Information Processing Standards (FIPS). Please refer to the Help file accessible from the Workbench for more details on that.

Copyright 2015 ICONICS, Inc.