

SOLARWINDS TECHNICAL REFERENCE

Implementing SNMPv3

Why SNMPv3?	3
SNMPv3 Security	4
General Implementation	6
SolarWinds Product-Specific Implementation....	7
SolarWinds SNMPv3 input mapped to IOS ..	7

This paper examines the steps required to implement SNMPv3 and how to use SNMPv3 in SolarWinds Products.

Copyright© 1995-2010 SolarWinds. All rights reserved worldwide. No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of SolarWinds. All right, title and interest in and to the software and documentation are and shall remain the exclusive property of SolarWinds and its licensors. SolarWinds Orion™, SolarWinds Cirrus™, and SolarWinds Toolset™ are trademarks of SolarWinds and SolarWinds.net® and the SolarWinds logo are registered trademarks of SolarWinds All other trademarks contained in this document and in the Software are the property of their respective owners.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Document Revised: 03/31/2010

Why SNMPv3?

SNMP version 1 and version 2 provide a very simple model for device management communications. Unfortunately, they also lack some critical features in the areas of security and flexibility, including the following:

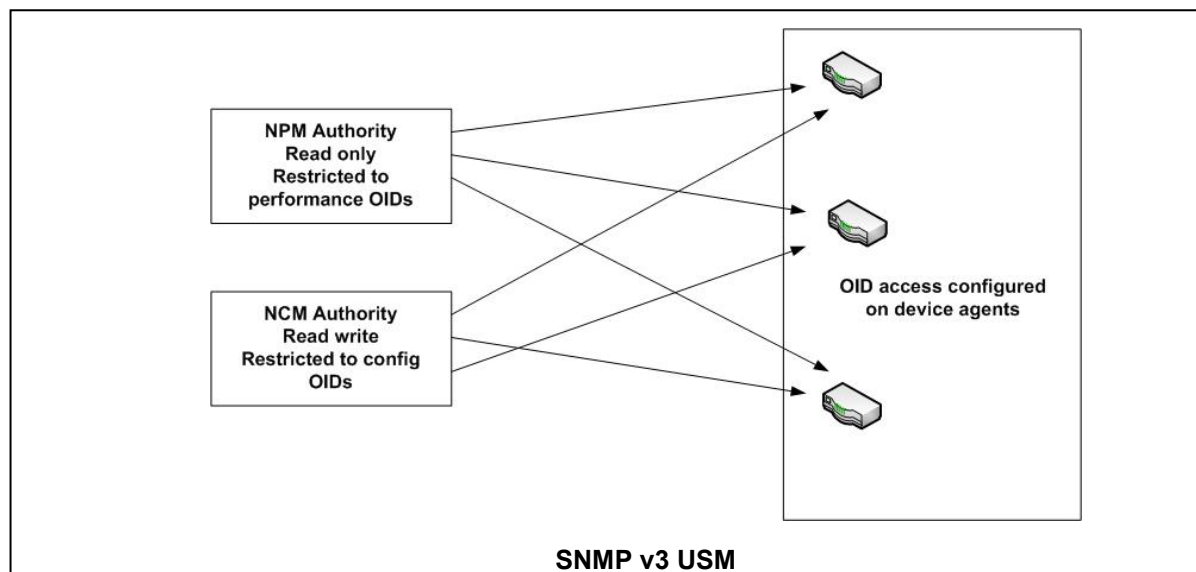
- **Weak Authentication Security.**
 - Community strings are transmitted in clear text. A packet capture will expose read-only and read/write community.
 - Only two roles are allowed, read only and read/write.
 - Default community strings for read only (public) and read/write (private) can be easily implemented in production networks, allowing access to devices by rogue SNMP managers.
 - Provides no ability to authenticate the source of an SNMP request.
- **Weak Privacy.**
 - Requests and replies are easily decoded, exposing entire SNMP conversations, including aspects of system configurations.
- **No Access Control Model.**
 - SNMP v1 and v2 do not define access control mechanisms, so once a device gains access to the device using v1 or v2 that device has unrestricted access.

SNMPv3 Security

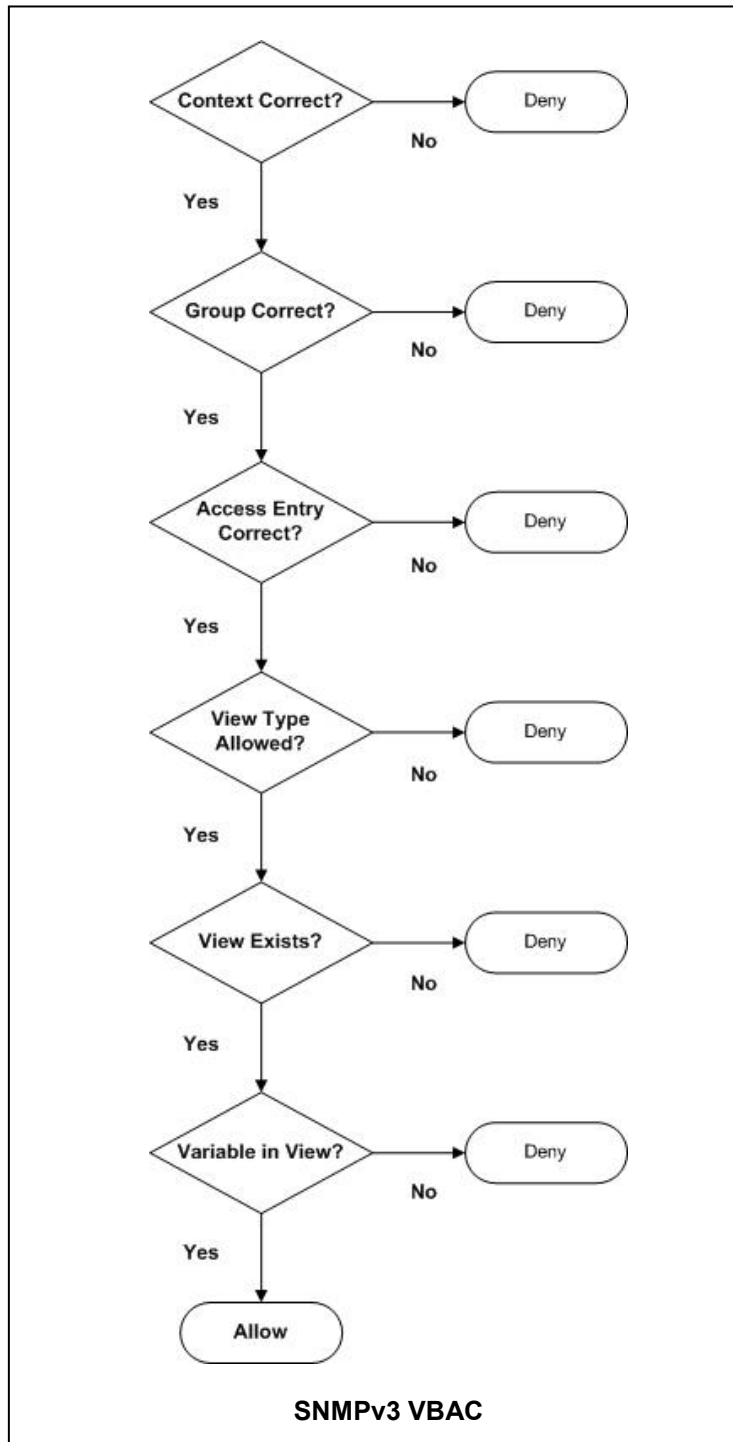
The three problems with SNMP version 1 and version 2 listed above are addressed in SNMPv3 through the implementation of the following enhancements:

- **Authentications Enhancements – User-Based Security Model (USM).**
 - Individual messages can be authenticated to known SNMP authorities, such as a particular Network Management System (NMS).
 - Messages contain multiple timing mechanisms preventing capture and replay. These include
 - SNMP authority engine uptime. The time since the last reset of the authority's SNMP engine.
 - SNMP authority up time. The uptime of the NMS.

Because this information is passed in encrypted form, a device attempting to mimic the authority has no way of knowing these details. Below is a depiction of SNMPv3 USM.



- **Strong Privacy.**
 - Data encryption options strengthen message privacy.
- **Access Control - View-Based Access Control (VBAC)**
 - VBAC allows the configuration of SNMP agents to restrict the authority access to the following:
 - Access certain portions of a MIB or deny access to all of a MIB on a per-authority basis.
 - Define the rights to the level of access, read, read/write, and notify (trap) on a per OID per authority basis.
 - VBAC creates a six step process for gaining access to MIB variables. Here is how this is accomplished:



General Implementation

Implementation of SNMPv3 is not difficult if it is done with proper planning. Here are the steps:

1. The following should be considered when planning the deployment.
 - a. Mapping the authority (NMS), access to devices and MIBs. groups, views, contexts and users needs to be planned and documented before configuring managed devices. If this is not done in advance, chances are you will have to configure devices multiple times to provide access for all authorities.
2. Configure the device to be managed for SNMPv3 management according to the manufacturer's documentation and the planned authority access.
3. Add the device to the Authority (NMS) using the SNMPv3 configuration parameters from step 1.
4. Test the SNMPv3 communications from the NMS.
5. If the test fails review the device configuration, NMS configurations, and any firewall or ACL rules that may be interfering.
6. Create a record of the NMS SNMP users and associated passwords and store them in a secure location. Because this information is not recorded in the running configuration of most devices it cannot be backed up or restored.

SolarWinds Product-Specific Implementation

Once the planning and implementation of SNMPv3 on the managed devices is complete you will need to enter the proper information into the SolarWinds product to allow SNMPv3 polling and traps. Here is how to map the SNMPv3 configured on the managed device to the required fields in your SolarWinds products.

SNMP Info

SNMP Version: SNMPv3 is a secure version of the SNMP protocol, adding authentication and encryption. SNMPv3 may require configuration on your network devices. Orion NPM can store SNMPv3 credential sets in the Orion database.

SNMP Port:

Allow 64 bit counters

SNMPv3 Credentials

SNMPv3 Username:

SNMPv3 Context:

SNMPv3 Authentication

Method:

Password / Key:

SNMPv3 Privacy / Encryption

Method:

Password / Key:

Credential Set Library

Name:

Saved Credential Sets

Read / Write SNMPv3 Credentials

SNMPv3 Username:

SNMPv3 Context:

SNMPv3 Authentication

Method:

Password / Key:

SNMPv3 Privacy / Encryption

Method:

Password / Key:

Credential Set Library

Name:

Saved Credential Sets

Orion Add Node SNMPv3 Screen

SolarWinds SNMPv3 input mapped to IOS

SNMP Credentials Area – Used to set read credentials

SNMP Read/Write Credentials Area – Used to set read/write credentials

Authentication

- SNMP v3 Username = user defined in `snmp-server user` command.
- SNMP v3 Context = context defined in `snmp-server group` command.

- SNMP v3 Authentication Method = method defined in `snmp-server group` command.

Password/Key = you have the option of entering the password defined in `snmp-server user` command or a defined key. If you use a password, we will convert the password to a shared key. If you use a key, we will simply use that key

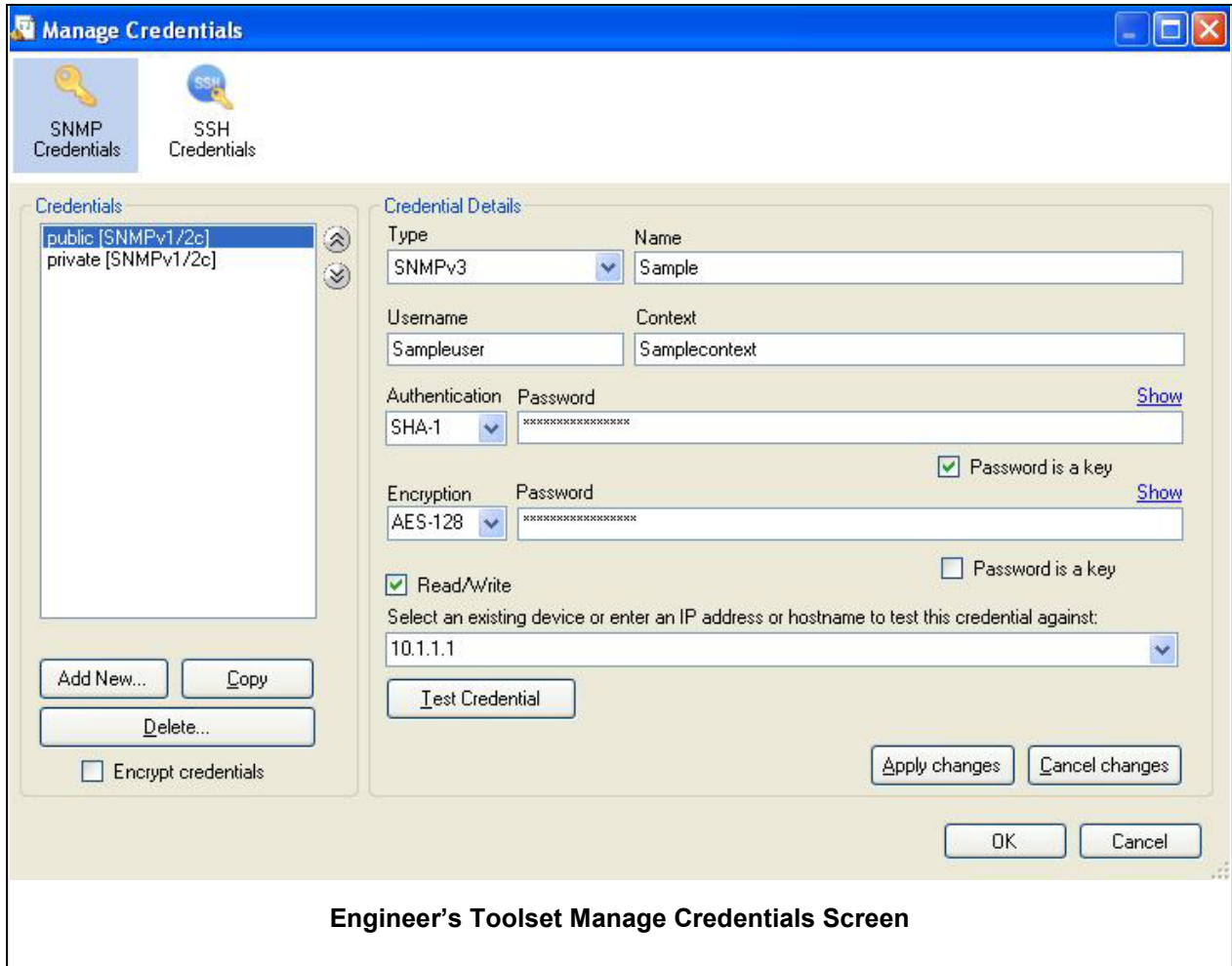
Privacy

- SNMP v3 Privacy/Encryption = as defined in `snmp-server user` command.
- Password/Key = you have the option of entering the password defined in `snmp-server user` command or a defined key.

Credential set Library

- Name you choose to save the credential set on the SolarWinds Product. This is not communicated to the managed devices or configured in IOS.

Minor differences exist in the exact order of these fields or the implementation method, such as in Engineer's Toolset read/write is specified with a check box rather than a separate input area.



Engineer's Toolset Manage Credentials Screen

