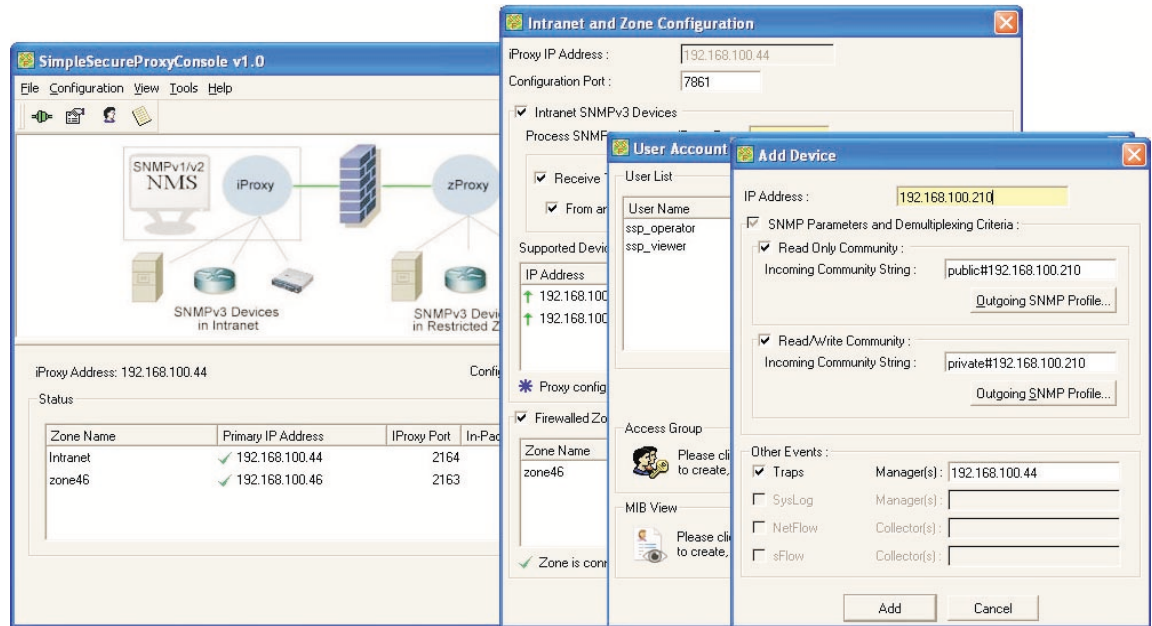


# SimpleSecureProxy™

Securely manage SNMPv3 devices with existing SNMPv1/v2 NMS.



## Overview

Network Management Systems (NMS) using the Simple Network Management Protocol (SNMP) are widely deployed to manage today's corporate networks. **SNMPv3**, the most recent version of SNMP, adds authentication and encryption to the protocol, to make the management of the devices more secure. While many networking devices have SNMPv3 support built-in, widely deployed NMS systems do not support SNMPv3.

**SimpleSecureProxy** is an easy-to-deploy software solution that allows you to leverage your existing SNMPv1/v2 NMS to **securely** manage SNMPv3 devices in your network. Critical resources within your intranet and/or in cordoned-off zones like the DMZ can now be managed in a secure manner using SNMPv3 without upgrading or replacing your NMS. **SimpleSecureProxy** not only does protocol translation between the different versions of SNMP, but it also configures and updates the Users, Passwords and Access privileges in the SNMPv3 devices.

**Intranet:** You can enable SNMPv3 on just a few critical devices or on all your intranet devices, and manage them using your existing SNMPv1/v2 NMS. Users and passwords can also be periodically updated as desired.

**Restricted Zones:** Firewalls are typically used to break up corporate networks into zones with varying levels of security. Due to heightened security concerns, these firewalls are often set up to block UDP/SNMP traffic, making the resources in the cordoned off zones like the DMZ, invisible to the NMS that manages the rest of your network. These resources can also be managed via the SimpleSecureProxy.

**SimpleSecureProxy** is made up of the "iProxy" that runs on the intranet side. It does the protocol translation and demultiplexing when communicating with intranet devices. For managing devices in a restricted zone, the "iProxy" communicates over an **encrypted TCP connection** with a "zProxy" that runs within the restricted zone. Openssh port forwarding or a single port/rule in the firewall, enables UDP based management traffic like SNMP, NetFlow, sFlow and Syslog to be securely forwarded to the management and collector systems in the intranet over this secure TCP connection.

## Features & Benefits

**SimpleSecureProxy** is an easy-to-deploy, software solution whose benefits include:

- Leveraging your existing SNMPv1/v2 NMS to securely manage critical resources via SNMPv3.
- Built-in configuration and updating of SNMPv3 parameters like Users, passwords and privileges.
- Management visibility to critical resources in firewalled zones like the DMZ.

**SimpleSecureProxy** features include:

- Supports translation between all SNMP versions (SNMPv1/v2c/v3) and SNMPv3 USM/VACM configuration.
- Updates users, passwords and privileges on all SNMPv3 devices.
- iProxy can be co-located on the same machine as the NMS. Redundant zProxies are also supported.
- DES based encryption is included. Use of SSL with stunnel/openssh is also easily configurable.
- A local, easy to use graphical utility is included for configuration along with a command line utility.

## System Requirements

**SimpleSecureProxy** is available on

- Microsoft Windows 2000/XP/2003, RedHat Linux 9.0+ and Solaris 2.6+.



Simplifying  
Network  
Management

SimpleSoft  
257 Castro Street  
Suite 220  
Mountain View,  
CA 94041  
650.965.4515  
650.965.4505 fax  
sales@simplesoftinc.com  
www.simplesoftinc.com  
www.snmpstest.com