Planning Guide for Implementing Role-Based User Accounts on an SEL ICON® Network

Ken Fodero

INTRODUCTION

This application note provides a high-level planning guide for implementing role-based user accounts on SEL ICON Integrated Communications Optical Networks.

SEL ICON systems ship from the factory configured in standalone or single user account mode. Multiuser security allows organizations to assign individual Simple Network Management Protocol (SNMP) user accounts to each ICON system operator, providing authentication, authorization, and accountability at the individual operator level. The ICON supports up to 500 individual user accounts.

Multiuser mode requires that SEL-5052 Network Management System (NMS) Server software is installed on a host Windows® computer with network access to the ICON system, as shown in Figure 1. SEL-5052 is the master repository of all data required for the ICON multiuser security system to function. Instances of SEL-5051 NMS Client software communicate with SEL-5052 via HTTPS connections to acquire and to modify the user security data stored on each ICON node.

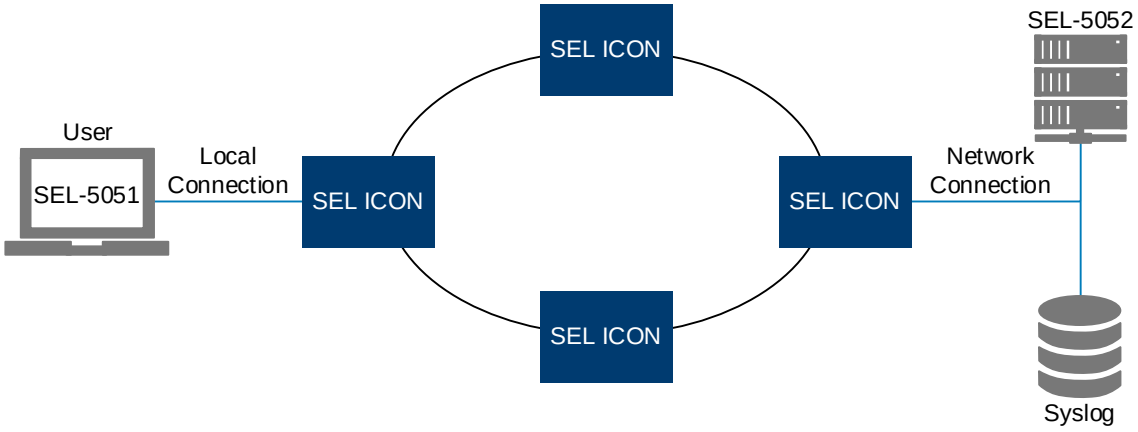

Figure 1 Network Interface Diagram

You can assign each user to one of six permission levels, or roles. These roles determine the level of access or permissions that a user has on each network. Table 1 provides an access summary of the six permission levels.

Table 1 Role Permission Levels

	Security Administrator	Administrator	Permission Level 3	Permission Level 2	Permission Level 1	Monitor
Read	Yes	Yes	Yes	Yes	Yes	Yes
User Management	Yes	No	No	No	No	No
Network Inventory	No	Yes	No	No	No	No
Firmware Upgrade, Backup, and Restore	No	Yes	Yes	Yes	No	No
Circuit Provisioning	No	Yes	Yes	No	No	No
Drop Port Management	No	Yes	Yes	Yes	Yes	No

PROBLEM

Many employees and contractors with varying skill levels need access to an ICON network. The level at which they are allowed to interact with the system varies based on their position or job function.

SEL SOLUTION

Role-based access defines the extent to which a user can change configuration settings on the system. Setting up multiple role-based user accounts in an ICON network allows you to manage the access levels of individual users and monitor their configuration changes. The implementation of multiple role-based user accounts requires cooperation and coordination with multiple departments. The conversion from single user to multiple role-based user accounts is a major change to the functionality of each ICON node and the network. The conversion process must be planned and tested to ensure a smooth transition. The following phases are recommended to ensure a successful transition.

Project Kickoff Meeting

Schedule a project kickoff meeting with all responsible departments. The purpose of this meeting is to determine the overall project owner and the action items for representatives of each group or department.

Department names and individual titles vary based on the organization, but the following roles should be included in the meeting:

- Telecom engineering (technical network support owner).
- Security analyst (network software security owner).
- System analyst (NMS or Network Operation Center [NOC] owner).
- IT representative (virtual machine or server owner).
- SEL technical representative.

The meeting goals are to:

- Determine the overall project owner.
- Determine the owner for setting up the SEL-5052 virtual machine or server. This task should include determining the network data path to the ICON network (IP address, ports, firewall rules, and so on).
- Answer relevant SEL-5052 concerns for the security group (e.g., what database structure does SEL-5052 use? [SEL-5052 uses a PostgreSQL DB and a Microsoft® SQL Server Compact Edition DB]).
- Determine who owns setting up the recommended external X.509 certificate.
- Decide who the administrators are for the system.
- Create a list of users who have access to the network.

Note that for future compatibility, you should have users select their network IDs as their usernames.

If you have a current access permission level scheme in use, match the SEL-5051 software access levels to the existing scheme.

Phase 1: Testing and Planning

The testing phase can be performed prior to the kickoff meeting to determine the steps required for implementation as long as an isolated test system is available. It is important to note that once implemented, downgrading or returning to the single user account mode requires local access to every ICON node on the affected network. Use the following steps to prepare for implementation:

- Set up a test system to verify the network operation and access for the network to SEL-5052.
- Develop a process and schedule to back up and restore the SEL-5052 database.
- Develop a process to add new nodes into existing multiuser networks.

Phase 2: Live System Implementation

Before implementing the live system, verify that the components meet the hardware, software, and SEL-5052 host requirements.

Verify that the firmware and SEL-5051 versions of all ICON nodes in the network are compatible with multiuser functionality. You can verify this through the global inventory report available in SEL-5051. The versions should be equal to or greater than the following hardware and software versions:

- Server module firmware: SEL-8030-01-R118-V0-Z013007-D20170210.
- SEL-5051 Version 2.5.0.0.
- SEL-5052 Version 1.3.0.0.

Follow the instructions in Appendix N of the ICON Instruction Manual for a step-by-step process to enable multiuser accounts. Permission levels allowed for the six defined user roles are documented in greater detail in that section.

The SEL-5052 host computer must meet the following minimum requirements:

- CPU: 32 or 64 bit at 2 GHz.
- RAM: 2 GB.
- Disk: 128 GB.

The SEL-5052 host computer must use one of the following operating systems:

- Windows 7.
- Windows 8.
- Windows 10.
- Windows Server 2012 R2.

LAN2016-04

SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 USA
Tel: +1.509.332.1890 • Fax: +1.509.332.7990
www.selinc.com • info@selinc.com