SIEMENS

FAQ • 08/2014

How to Secure RUGGEDCOM ROS® Devices Before and After Field Deployment

RUGGEDCOM ROS

http://support.automation.siemens.com/WW/view/en/99858806

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit http://www.siemens.com/industrialsecurity.

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit http://support.automation.siemens.com.

Table of Contents

1 Overview

RUGGEDCOM ROS®

RUGGEDCOM ROS® is the embedded software running on RUGGEDCOM Ethernet Switches and Media Converters. RUGGEDCOM devices run in mission-critical environments and are often used for allowing access to devices critical to public infrastructure and safety. It is very important that customers and clients understand how to protect a ROS® device from unauthorized access. The following describes a few simple steps that will help secure a ROS® device before and after it is deployed in the field.

Intended Audience

This document is intended for Network Design Specialists, Cyber-Security Specialists, Network Management personnel and Network Technical Support personnel.

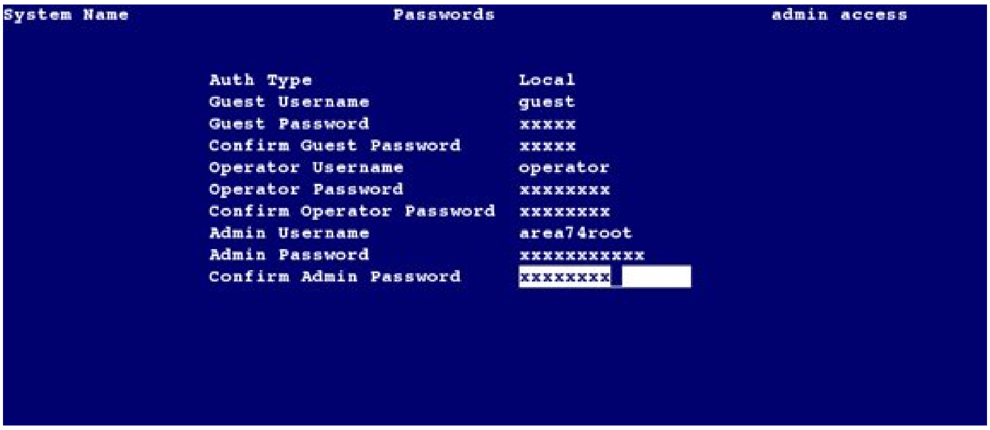
2 Securing ROS® Devices Before Deployment

2.1 Change the Username and Password from their Defaults

It is critical that unauthorized users or malicious attackers do not have access to the device and its settings. The default username and password are well known and, if left unchanged, will leave the device and its settings easily available for misuse/attacks.

Within ROS®, there are three user types: Admin, Operator and Guest. Privileges are highest for Admin and lowest for Guest. The usernames can and should be changed as needed. Changing the username will make sure the default usernames can no longer be used for login purposes. The corresponding user permissions for the user type will remain the same.

Figure 2-1: Change the Username and Password



```
System Name                     Passwords                       admin access

                 Auth Type                  Local
                 Guest Username             guest
                 Guest Password             xxxxx
                 Confirm Guest Password     xxxxx
                 Operator Username          operator
                 Operator Password          xxxxxxxx
                 Confirm Operator Password  xxxxxxxx
                 Admin Username             area74root
                 Admin Password             xxxxxxxxxxx
                 Confirm Admin Password     xxxxxxxx_
```

When choosing a password, choose one that will be hard to crack and follows well established organizational guidelines or best practices. When the password is first saved, ROS will verify the strength of the password and will warn the user through the alarms table if it finds the password to be too weak. Although, the alarm can be disabled from the Alarms form, this is not recommended. Instead, choose a stronger password.

There are several guidelines for selecting a good password. The most common include:

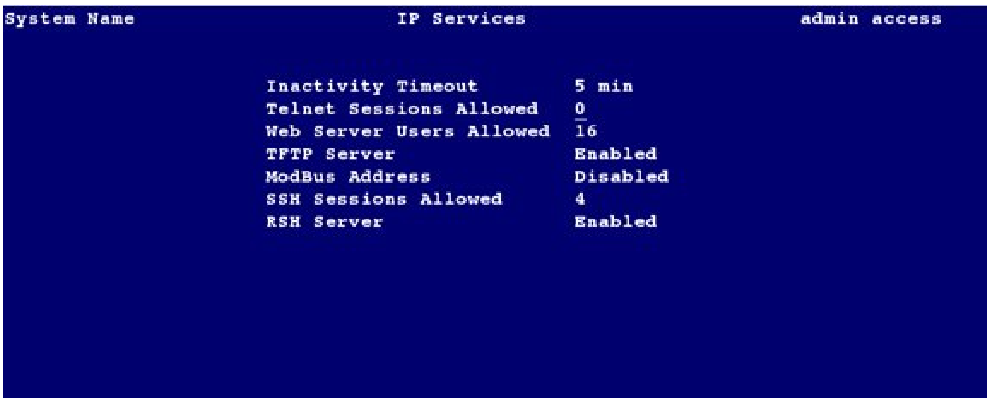
- Select a password that is at least 8 characters in length.
- Use a combination of alphabetical, numeric and special characters.
- Use a combination of uppercase and lowercase letters.
- Do not use single dictionary words. If using a combination of words, do not combine predictable words.
- Do not use local or organizational terms.
- Do not use predictable sequences such as ‘12345’ (numbers are incrementing orderly) or ‘mkonhy’ (keys are equally spaced and moving in a predictable direction).

Note that the Admin user profile is intended to be used by very few personnel and only when settings need to be changed. This username and its password are not meant to be used by personnel for normal access to check status or view settings. Use the Operator profile for this purpose instead. In general, the higher the privileges are for a user profile, the less people should know the username and password for the profile.

2.2 Turn Off Services that Are Vulnerable

ROS® supports protocols such as RSH, Telnet, SNMP[1] and TFTP. These services are *not secure* and send passwords over cleartext or, as in the case of TFTP, require no passwords at all. These services are available for historical reasons and are meant for backward compatibility with customer equipment or services that rely on these services. It is highly recommended that these services be turned off. Secure alternatives such as SSH and SFTP are also supported and will greatly minimize the r*i*sk posed by remotely accessing devices.

Figure 2-2: Disabling IP Services



```
System Name                       IP Services                        admin access


                      Inactivity Timeout        5 min
                      Telnet Sessions Allowed   0
                      Web Server Users Allowed  16
                      TFTP Server               Enabled
                      ModBus Address            Disabled
                      SSH Sessions Allowed      4
                      RSH Server                Enabled
```

2.3 Turn Off Services that are Not Required

ROS® supports RCDP (RUGGEDCOM Discovery Protocol) and LLDP (Link Layer Discovery Protocol).

RCDP provides an easy way to configure multiple devices with basic settings such as System Name and IP addresses before initial deployment. It is recommended that as soon as the configuration of the unit is complete, RCDP be turned off.

LLDP is an IEEE 802.1 protocol that allows devices to discover each other. It is useful for Network Management Systems to have a ‘map’ of the network and helps to troubleshoot in networks with a large number of devices. However, the protocol communicates frequently and advertises device identification parameters such as System Names and IP addresses used by the device. Unless a Network Management System is in use, LLDP should be turned off before deployment.

[1] SNMPv1 and SNMPv2 are not secure. SNMPv3 is secure. SNMP is disabled by default on all ROS® devices.

3 Making Sure Devices Stay Secure

3.1 Protect the Configuration Files

Configuration files for ROS® are CSV (comma separated values) formatted and are meant for ease of use and the portability of configuration parameters. Although they may be of no use to a hacker, all of the device settings are recorded in the configuration file (including password hashes) . It is recommended that these files be kept in a secure place if downloaded from the device. The configuration files should also be password encrypted before distributing them over e-mail or other such forms of communication.

3.2 Use Real Servers Whenever Possible

AAA servers are a great way to secure passwords and authorize logins. ROS® supports RADIUS and TACACS+ services.

ROS is meant for embedded devices and does not support the features of a full operating system. AAA servers run on real Operating systems that can be hardened against malicious attacks and provide a secure environment for password maintenance.

ROS® can support both Local and Remote authentication at the same time. However, if the remote authentication is trusted, local authentication can be disabled.

Secure Access Management Servers, such as RUGGEDCOM's Crossbow Server, hide the device from any external network. The device can only be accessed through these servers.

4 Conclusion

Securing a ROS® device is as simple as modifying a few parameters. This will go a long way in making it difficult to attack or access the device with malicious intent.

In summary, security for ROS® devices can be greatly increased by following the below mentioned suggestions:

- Change the username and password as soon as the device has been received
- Configure passwords that adhere to good password guidelines
- Provide only minimum access to users based on their role
- Turn off services that are not needed or serve no purpose
- Protect configuration files and store them securely