

Brodersen RTU Security Update

Overview of latest RTU32M/N security functionality

Application Note

7 April 2020 Doc. 13001



Introduction

We no longer chase enemies in long boats, but our impressive hardware and software is used to terrify our competitors and keep our products safe!

Brodersen have been manufacturing products for use in remote monitoring and control solutions for more than 50 years. Our customer base is global and our products are used in a diverse range of applications that include energy management systems, water and waste water SCADA, infrastructure monitoring, building automation and airport management systems.

This application note provides an overview of the RTU32M/N Series security functionality. RTU security is a hot topic amongst large utility companies who need to ensure their SCADA systems comply with both their own corporate security requirements and regulatory authority security standards.

Traditionally corporate IT security system standards are based around information security with focus on Confidentiality, Integrity and Availability. These focal points are typically reversed when defining SCADA system security requirements ie. Availability is most important! Most RTU vendors have struggled to adapt their products to evolving security standards that are easily implemented in devices like PCs and Smartphones that are obsolete in 2-3 years, but hard to deploy in RTUs designed to operate for 10-15 years.

A fresh start allows security to be included, rather than 'added-on'

The RTU32M/N Series are the latest generation of Brodersen RTUs – with a new architecture that allows a 'fresh start' to developing product and security functionality. Instead of trying to add on security, the RTU32M/N products have it included at multiple levels ie. adding a hard shell to a soft core seems good, until an entry point is found – a better solution is to have multiple layers of hard shells around a hard core (the Viking ancestors knew that!).

The essential components for the new RTU platform include 'future proof' hardware with guaranteed availability of the core CPU board components past 2035 and an embedded Linux operating system.



MP32A – RTU32M CPU Module



BRODERSEN
simplifying systems


RTU security features overview

The RTU32M/N Series have numerous security features that include;

- **Management of User Access and User Authentication** - limiting use of default passwords, user group passwords and user privileges managed from a central location via LDAP.
- **Firewall Implementation** – a user interface to manage which IP ports are open and whitelisting and blacklisting of ranges of IP addresses (uses iptables).
- **Management of System Services** – controls access to HHTP, HTTPS, SSH and Event Viewer services. An important requirement of any secure system is that non-essential services are disabled.
- **Secure Applications and Firmware Updates** - use of 'signed' application logic and firmware using RSA public-key cryptosystem techniques.
- **Encryption of Sensitive Data** - any files that include user or password type info. can be stored in an encrypted 'container' area of the SD card to protects against theft or incorrect transfer of SD cards.
- **Secure Network Connections and Protocols** – protecting data 'in flight' using dual VPNs and secure SCADA protocols such as DNP3 Secure.

Managing User Access – discouraging use of default passwords

The RTU32M/N Series products use a web server interface to view system information and manage the setup of the RTU. The System Overview page below shows a 'Security alert' and warns that the RTU is configured to use default passwords.



System Overview

- System Overview
- Hardware Overview
- Runtime Settings
- I/O Board Settings
- System Configuration
- Maintenance
- Utilities
- Firewall
- DNP3 Slave
- WITS-DNP3 Slave

User name: admin
User group: Administrators
Log out
2020/04/05

CPU Temp: 62 °C
CPU Load: 32.9 %
Memory Usage: 25.7 %
Board Temp: 38.5 °C
Board Type: RTU32M

Security alert.
The RTU is configured to use default passwords.

Local Area Network (LAN) settings

This section displays a summary of your LAN network settings. These settings indicate configuration of your LAN ports.

Network Settings LAN1	eth0
Obtain an IP Address via DHCP	DISABLED
Local IP Address	192.168.0.1
Subnet mask	255.255.255.0
Default gateway	
Preferred DNS Server	
Alternate DNS Server	
MAC address	F8:DC:7A:1F:72:F3
RX/TX Bytes	84.0/104.7 MiB

Network Settings LAN2	eth1
Obtain an IP Address via DHCP	ENABLED
Local IP Address	0.0.0.0
Subnet mask	0.0.0.0
Default gateway	0.0.0.0
Preferred DNS Server	
Alternate DNS Server	
MAC address	F8:DC:7A:1F:72:F2
RX/TX Bytes	0.0/0.0 MiB

Hostname: rtu32

Project Information

Project Name	modbustest_2
Project Runtime Start	2020/04/07 06:31:56.184
Project IO count	55
Project Build Time	2020/04/07 06:31:48
Project Build Version	34
Project Build CRC	16#f3348db3

RTU32 Version Information


RTU32 Firmware Version	1.65.5.168
RTU32 Firmware Date	2020/04/01
RTU32 Firmware ID	93046
Runtime Version	8.7.150121
RTU32 Image Date	2020
RTU32 Image Version	4.1.15-2.0.0.1351+g0a8cb4d
RTU32 Image Build Version	1352
RTU32 Device Tree version	1219

192.168.0.1 says

Information:

Security alert.

The RTU is configured to use default passwords, which might imply a security risk.



OK

The pop-up alert above appears every time a selection is made to advise and encourage the user to change the default password.

Administration of default passwords and creation of additional users

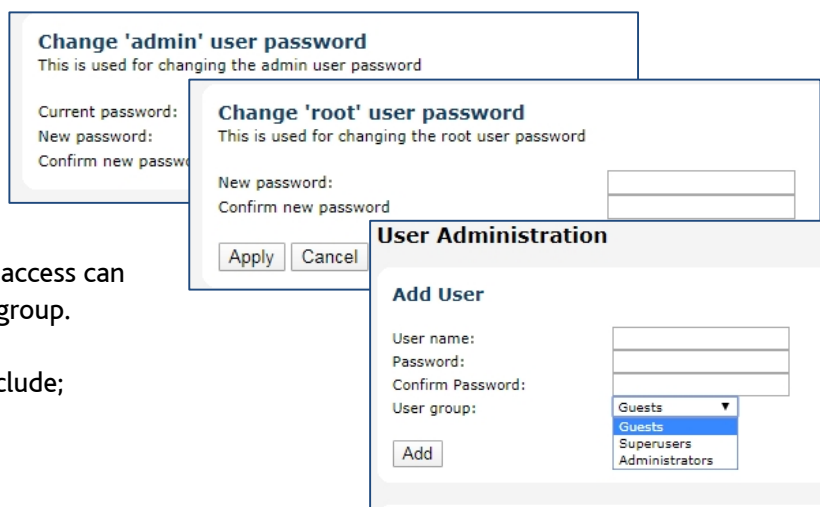
The admin user password can be changed from the default.

The root user password is not set by default to ensure root level access is only available if enabled/set.

A user with Administrators group level access can add additional users and set their user group.

Web server User group access levels include;

- Guests (read only)
- Superusers (read and some config)
- Administrators (full access).

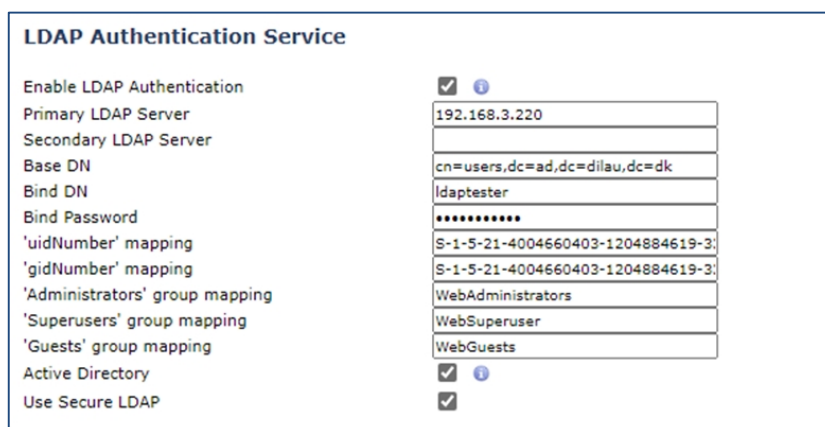


The image shows three overlapping screenshots of a web-based user administration interface. The top-left screenshot is titled 'Change 'admin' user password' and contains fields for 'Current password:', 'New password:', and 'Confirm new password:'. The top-right screenshot is titled 'Change 'root' user password' and contains fields for 'New password:' and 'Confirm new password:'. The bottom screenshot is titled 'User Administration' and features an 'Add User' section with fields for 'User name:', 'Password:', 'Confirm Password:', and 'User group:'. The 'User group:' dropdown menu is open, showing options: 'Guests', 'Guests' (highlighted), 'Superusers', and 'Administrators'. An 'Add' button is located below the dropdown.

User Authentication from a central LDAP Authentication Service

Management of user authentication from a centrally managed server is critical for large corporations and utility companies that need to respond rapidly to changes of personnel. The RTU can be configured to authenticate a user when a log in event occurs.

The example setup here shows how user groups are mapped from the RTU to the LDAP server groups.

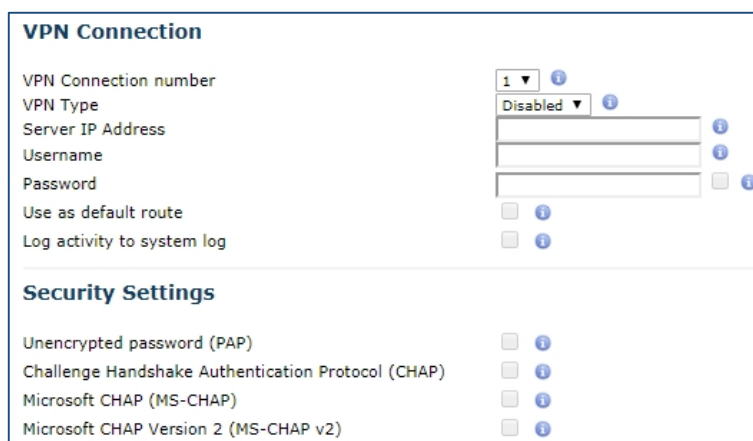


The image shows the 'LDAP Authentication Service' configuration interface. It includes a list of settings on the left and their corresponding values on the right. The settings are: 'Enable LDAP Authentication' (checked), 'Primary LDAP Server' (192.168.3.220), 'Secondary LDAP Server' (empty), 'Base DN' (cn=users,dc=ad,dc=dilau,dc=dk), 'Bind DN' (ldaptester), 'Bind Password' (masked with dots), ''uidNumber' mapping' (S-1-5-21-4004660403-1204884619-3), ''gidNumber' mapping' (S-1-5-21-4004660403-1204884619-3), ''Administrators' group mapping' (WebAdministrators), ''Superusers' group mapping' (WebSuperuser), ''Guests' group mapping' (WebGuests), 'Active Directory' (checked), and 'Use Secure LDAP' (checked).

Secure / Dual VPN Connection

The RTU supports dual VPN server connections using PPTP and L2TP/IPsec to provide secure connections to other networks. L2TP with IPsec adds security to the establishment of the connection using pre-shared keys and encapsulation of the data packets using encryption.

The RTU logic block 'CONNECTVPNEX' allows management and logging of the VPN connection process.



The image shows the 'VPN Connection' configuration interface. It includes a list of settings on the left and their corresponding values on the right. The settings are: 'VPN Connection number' (1), 'VPN Type' (Disabled), 'Server IP Address' (empty), 'Username' (empty), 'Password' (empty), 'Use as default route' (unchecked), and 'Log activity to system log' (unchecked). Below this is the 'Security Settings' section, which includes: 'Unencrypted password (PAP)' (unchecked), 'Challenge Handshake Authentication Protocol (CHAP)' (unchecked), 'Microsoft CHAP (MS-CHAP)' (unchecked), and 'Microsoft CHAP Version 2 (MS-CHAP v2)' (unchecked).

PPP Over Serial Link

Some corporate users have restrictions imposed on their field technicians that do not allow LAN ports on laptops to be used for anything other than connection to their corporate system. Use of PPP (Point to Point Protocol) allows IP connectivity with the RTU using a serial port.



The image shows the 'PPP Over Serial Link Service' configuration interface. It includes a list of settings on the left and their corresponding values on the right. The settings are: 'Enable PPP over serial link' (unchecked), 'COM Port' (COM4), 'Baud Rate' (115200), 'Local IP address' (195.0.0.14), and 'Peer IP address' (195.0.0.110). At the bottom, there is a status message: 'PPP Over Serial link Service is not started' and 'PPP Over Serial link Service is not connected to peer'.

Syslog Reporting Services

If enabled, the Syslog service sends reports of all RTU runtime events and web server events to a corporate Syslog server.

Syslog Reporting Service

Enable Syslog Reporting ☐ ⓘ

Syslog Server IP address . . .

Syslog Server Port

Management of System Services

Various system services can be enabled/disabled to restrict access to only the required services.

System Services

Enable Web Server Http Access ☒ ⓘ

Enable Web Server Https Access ☐ ⓘ

Enable SSH Server ☒ ⓘ

Allow SSH root login ☒ ⓘ

Enable RTU EventLog Server ☒ ⓘ

Enable Encrypted storage ☐ ⓘ

Encrypted Storage – with optional SD cards

The RTU is able to store any files that include user and password type information in an encrypted container area of the SD card.

Firewall Setup – Managing IP Ports and IP Addresses

The RTU Firewall allows management of the IP ports that connect services and networks to the RTU. In addition, Blacklists and Whitelists allow management of excluded/included lists of IP addresses.

Firewall Ports Configuration

On this page you can open incoming connections for your listening ports.

IP Protocol ⓘ

Starting port ⓘ

Ending port ⓘ

SSH ☐ ⓘ

Ports open

Updated successfully

- TCP Port: 22 (SSH)
- TCP Port: 80
- TCP Port: 502
- TCP Port: 20000:20002

Delete

Delete

Delete

Delete

Blacklist IP Address

Start IP Address . . .

End IP Address . . .

Whitelist IP Address

Start IP Address . . .

End IP Address . . .

IP Addresses whitelisted

Updated successfully

- 192.168.11.1-192.168.11.125
- 192.168.0.1-192.168.0.40

Delete

Delete

Applications and Firmware updates are 'signed' to keep your RTUs safe

The WorkSuite logic application includes an Application Code Signing Tool that manages the generation and storage of public and private keys and enables the signing of logic applications (with an encrypted signature). The public key and private key are used by WorkSuite to encrypt authorisation. The public key is loaded in the RTU and used to decrypt authorisation. Firmware update utilities for loading of RTU base firmware and IO module firmware also ensure that only 'signed' code/updates authorised by Brodersen will load.

RTU32 Application Code Signing Tool

RSA certificate Location: ⓘ

Public Key filename: rsa-public

Private Key filename: rsa-private

Generate

☒ Enable code signing

Application code signing in progress ...

- > Generating signature... Successfully ...
- > Validating signature... Successfully
- > No error detected

Options

☒ Use UTC time for real time clock functions ⓘ

☐ Enable Multi Task ⓘ

☒ Allow only signed Application code to run ⓘ

Public key file does not exist. Please upload

Public key file: rsa-public.pem

File uploaded successfully

Validating application code signature ...

Unable to start application because signature is invalid

Firmware Update

Firmware file: No file chosen

Installed Modules:

Index	Type	HW Version	HW Date	FW Version	FW Date	New FW Version	FW
1	PS24A	A	12-03-2018	1.1.2.2	06-06-2018	*	
2	IO14B		24-01-2019	1.1.2.6	22-01-2020		
3	IO14B		24-01-2019	1.1.2.6	22-01-2020		
4	AI08A		25-01-2018	1.1.2.6	22-01-2020		
5	IO14A		24-01-2019	1.1.2.6	22-01-2020		

Select firmware for PS24A

Available firmwares:

OK Cancel

(*) Newer Firmware available (**) Module must be updated

Additional product information is available from our website, or from the authorised distributor in your region.
<http://www.brodersen.com>

