

# RTU cyber Security

## Secure your RTU against attacks

Focus on cyber security has steadily increased in the electric sector over the last couple of years. ABB fully understands the importance of cyber security and has identified it as a key requirement. ABB is committed to provide customers with products and systems that clearly address cyber security and thus constantly adapts its products and systems to the latest developments in cyber security.

The electric power grid has changed significantly over the past decade and continues to change with technology enhancements. The new generation of control systems is more and more based on open standards and commercial technology, e.g. Ethernet and TCP/IP based communication protocols such as IEC 60870-5-104, DNP 3.0 or IEC 61850. This change in technology has not only brought huge benefits from an operational point of view, it also introduced cyber security concerns known from office or enterprise IT systems. ABB anticipates the security challenges and constantly adapts its systems to the latest developments in security. Our RTUs respond to the needs of the power industries and assure a high level of cyber security. User access control, security logging, hardware hardening are implemented according to NERC-CIP and IEEE 1686. Different algorithms and various encryption standards (32, 56, 128 bits) are used for password and log file storage.

### User access control

#### User account management

The RTU560 supports user authentication and authorization on an individual user level. User authentication is required and authorization is enforced for all interactive access to the device.

#### User accounts

The RTU560 allows to fully manage user accounts, i.e. creating, editing and deleting them freely. User names and passwords can be configured according to customer's requirements.



### Role Based Access Control

The RTU560 supports Role Based Access Control (RBAC). Every user account can be assigned different roles and the user roles can be added, removed and changed as needed.

### Password complexity

The RTU560 offers the possibility of enforcing password policies that can be customized by specifying minimum password length, maximum password lifetime, as well as usage of lower case, upper case, numeric and special characters.

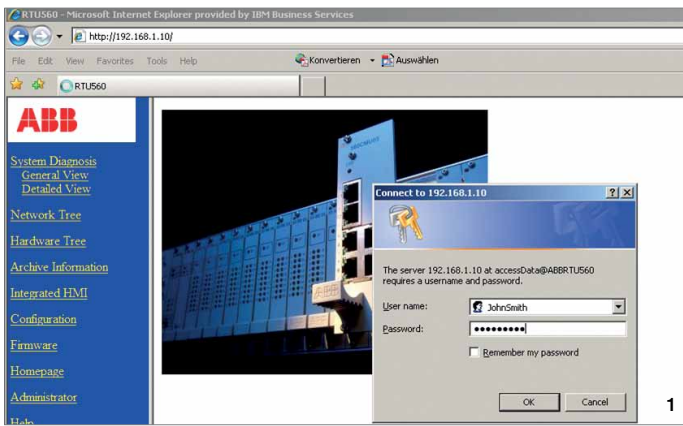
### HTTPS support

The RTU560 permits encrypted communication between the web browser and the RTU. A standard browser can be utilized such as Internet Explorer or Firefox. Furthermore the operator can select between http:// and https:// by configuration. In addition, self-signed certificates, pre-installed at web client, can be used.

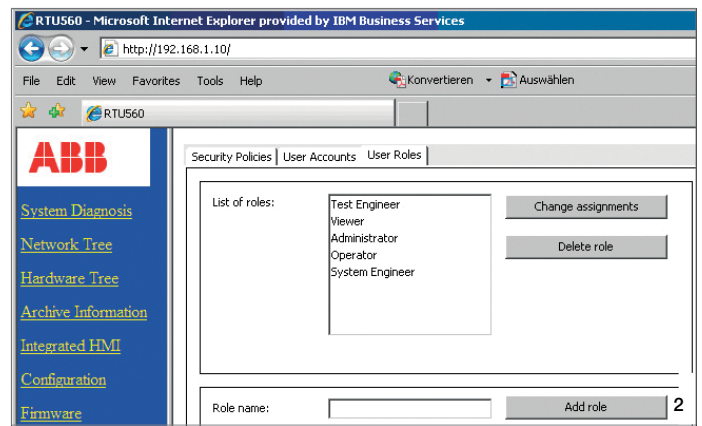
### Security logging

#### Local logging

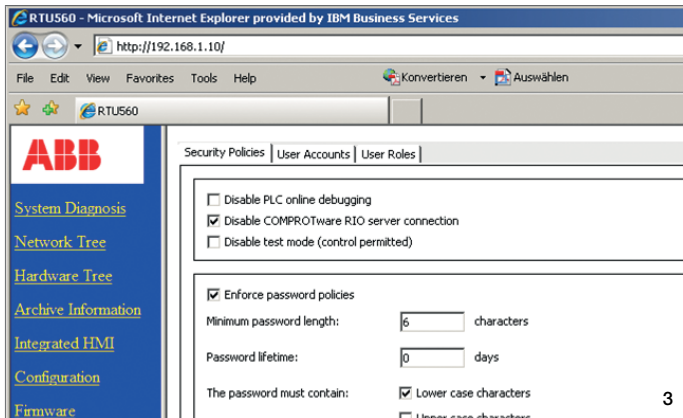
RTU560 creates audit trails (log files) of all security relevant user activities. Security events that are being logged include user login, logout, change of parameters, configurations, or updates of firmware. For each event date and time, user, event ID, outcome and source of event are logged. Access to the audit trail is available to authorized users only.



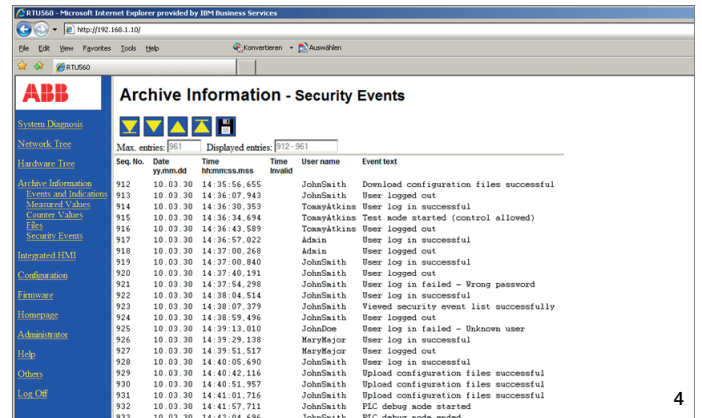
1



2



3



4

1 User access control | 2 Role Based Access Control | 3 Password complexity | 4 Security logging

### External security clients

Security events of the RTU560 can be sent to external security log clients such as the Security Event Manager (SEM) from Industrial Defender®. SEM is a monitoring and response device, which enables visibility of real time security events. Syslog UDP/TCP and ArcSight TCP - standard protocols for logging of security events - are now supported by RTU560. Furthermore up to 3 clients per ethernet port can be configured.

### Security events to control system

Security events and alarms can be sent via host protocol to the control systems. "Security indication" and "security alarm" are supported. Settings of security alarms are part of the configuration. Up to 32 security events can be mapped to one single alarm. Security events are now also available in host protocols, PLC, HMI and process archives.

### System hardening

ABB strives to improve the security and robustness of its products by performing security testing and hardening. The RTU560 has been systematically hardened, e.g. unused services have been removed and unused ports closed. Furthermore the RTU560 has been thoroughly tested at ABB's dedicated, independent security test center using state-of-the-art commercial and open-source security testing tools. Hardening steps as well as the resulting configurations, e.g. open ports and services, are documented in detail.

### VPN function

The RTU560 offers one encrypted channel between the RTU and the IPsec Router on customer's side. The VPN tunnel provides confidentiality and integrity and authenticity. A secure communication via public networks with fixed IP addresses (e.g. internet) is possible. The authentication is handled by pre-shared keys.

For more information please contact:

### ABB AG

#### Power Systems Division

P.O. Box 10 03 51

68128 Mannheim, Germany

Phone: +49 621 381-3000

Fax: +49 621 381-7622

Email: [rtu-sales-support@de.abb.com](mailto:rtu-sales-support@de.abb.com)

[www.abb.com/substationautomation](http://www.abb.com/substationautomation)

#### Note:

We reserve the right to make technical changes or modify the contents of this document without prior notice. With regard to purchase orders, the agreed particulars shall prevail. ABB AG does not accept any responsibility whatsoever for potential errors or possible lack of information in this document.

We reserve all rights in this document and in the subject matter and illustrations contained therein. Any reproduction, disclosure to third parties or utilization of its contents - in whole or in parts - is forbidden without prior written consent of ABB AG.

Copyright© 2011 ABB

All rights reserved