Application Note

nVent SCHROFF

Guardian Management Gateway Security

Revision 1.3

01 / 12 / 2022 (Month / Day / Year)

Table of contents:

1 Document revision history 4

2 Purpose 4

3 Guardian Management Gateway Security Overview 4

3.1 User Model 4

3.2 System Restrictions 5

3.3 Serial Port Access 5

3.4 Network Access 5

3.4.1 SNMP 5

3.4.2 Secure Shell (SSH) 6

3.4.3 Telnet (NOT SECURE, DISABLED BY DEFAULT) 6

3.4.4 Web Interface 6

3.4.5 Management of SSL Certificates 6

3.4.6 IP Firewall 7

3.4.7 Role-Based Access Control 8

3.4.8 Login and Password Policy Settings 8

3.4.9 Restricted Service Agreement 9

3.4.10 Communication Matrix 9

3.4.11 Remote Access Protocol Versions 11

3.5 Firmware Upgrade Security 11

3.6 LCDUI 11

3.7 Security Scanning 11

3.8 Maximum Security Configuration 11

Table of figures:

No table of figures entries found.

1 Document revision history

Rev.	Date	Author	Verified by	Description of changes
R1.0	2019.10.18	D.P.		Initial release
R1.1	2020.03.05	D.P.		Minor edits, name change
R1.2	2020.09.14	D.P.		Update to reflect the latest security enhancements
R1.3	2022.01.11	D.P.		Merge contents from another internal security document

2 Purpose

This application note describes the security aspects of the nVent SCHROFF Guardian Management Gateway device.

3 Guardian Management Gateway Security Overview

The Guardian Management Gateway device firmware is based on a recent version of Linux (4.1.15), which supports a number of secure protocols for remote access. Most remote access methods are built around the user/password model, in which a login is required before accessing the corresponding service. In addition, each user account is associated with a privilege level, which specifies the services and resources accessible by the user. The desired level of security can be achieved by configuring the Guardian Management Gateway firmware as required (i.e. by making sure that all non-secure protocols are disabled).

The security aspects of the Guardian Management Gateway device firmware are discussed in more detail in the following sub-sections.

3.1 User Model

The Guardian Management Gateway device maintains a common database of user credentials (username, password, access rules, etc), which is used across most remote access methods (web interface, serial port, remote command line access). Other remote access methods (such as SNMP) use their own authentication mechanisms. It is therefore not possible to access the Guardian Management Gateway device without entering a valid user name and password (with the exception of the LCD interface – see section 3.6**Error! Reference source not found.** below). In addition to the local user database, the Guardian Management Gateway device can be configured to enable remote authentication using LDAP. The LDAP authentication uses secure communication to a user database stored on a remote server.

IMPORTANT: all new Guardian Management Gateway devices are shipped with three user accounts: “admin”, “user” and “guest”. The default passwords for these accounts match the user names. Only the “admin” account is enabled by default, the two other ones are disabled. The “admin” account is configured with the maximum privilege level, and when logging as “admin”, the user is requested to change the default password on the first login. Also, a user with administrative privileges can change the password for the “admin” account at any time by running the following command from the serial console:

```
cli> user password admin <new_password>
```

Alternatively, the admin user password can be changed from the web interface (USER MANAGEMENT -> Change Password). The passwords for the non-privileged “user” and “guest” accounts can be changed in a similar way.

3.2 System Restrictions

To prevent unauthorized access to the system files and resources, the production version of the Guardian Management Gateway firmware does not allow access to the Linux shell for any user account. When logging on to a device via a command line interface (serial or SSH), the user sees a restricted CLI shell that only supports Guardian-specific commands. As a consequence, neither a regular user nor an administrator has access to the underlying file system or other system resources that are not exposed by the main application.

3.3 Serial Port Access

The Guardian Management Gateway serial port can be used for diagnostics and for command line access to the Guardian Management Gateway device. After the device boots up, a login prompt is displayed on the serial console. A valid username and password are required to access the Guardian Management Gateway Command Line Interface.

3.4 Network Access

The Guardian Management Gateway supports multiple remote access methods, which are described in the following sub-sections.

3.4.1 SNMP

Using SNMP, it is possible to monitor Guardian Management Gateway sensors and to toggle Guardian Management Gateway controls. The Guardian Management Gateway software supports the SNMPv3 protocol, which uses MD5/SHA authentication and AES/DES encryption to ensure secure communication. While the less secure SNMP protocols (v1 and v2) are also supported, they are disabled in the Guardian Management Gateway software configuration by default (DEVICE SETTINGS -> Network Services -> SNMP).

The Guardian Management Gateway firmware supports the following pre-defined SNMPv3 user templates:

SNMP USER	AUTHENTICATION TYPE	PRIVACY PROTOCOL	ACCESS CONTROL
baseusermd5	MD5	None	read/write
baseusersha	SHA-1	None	read/write
baseusermd5des	MD5	DES	read/write
baseusermd5aes	MD5	AES	read/write
baseusershades	SHA-1	DES	read/write
baseusershaaes	SHA-1	AES	read/write

Other SNMP users are created from the pre-defined SNMPv3 user templates listed above.

3.4.2 Secure Shell (SSH)

The Guardian Management Gateway firmware supports remote access to the Guardian command line interface via the Secure Shell protocol (SSH version 2).

The SSH settings can be viewed and changed via the “Device Settings” -> “Network Services” -> “SSH” menu item. By default, the SSH service is enabled on port 22, and both the password authentication and the public key authentication methods are enabled. The Guardian administrator can disable or enable the SSH service, change the SSH port, or change the authentication type. There are three SSH authentication types supported by the Guardian: password authentication only, public key authentication only, password and public key authentication (default).

A user can change their public keys via the “User Management” -> “Change User SSH Key” menu item. A user can add a public key or clear their set of public keys. Also, the Guardian administrator can add a public key or clear the set of public keys for another user via the “User Management” -> “Users” menu item and the “Edit user” button.

In addition, the Guardian administrator can enable an option to allow multiple SSH logins with the same user name.

3.4.3 Telnet (NOT SECURE, DISABLED BY DEFAULT)

In addition to SSH, the Guardian Management Gateway firmware supports the Telnet protocol for accessing the command line interface. This method provides a simple non-secure remote access to the Guardian Management Gateway command line interface. It is intended for use in isolated environments, and is disabled in the default configuration. It can be enabled using the DEVICE SETTINGS -> Network Services -> Telnet dialog.

3.4.4 Web Interface

The Guardian Management Gateway firmware supports remote access via a Web interface. To access the web interface, a login and password is required. If secure communication (TLS) is enabled, all communication with the iPDU is encrypted. The Guardian Management Gateway device supports the following HTTPS ciphers: TLS 1.2 with AES 128/ 256-bit encryption. It is possible to configure the Guardian Management Gateway device to disable non-secure web access (DEVICE SETTINGS -> Network Services -> HTTP -> Force HTTPS for Web Access).

3.4.5 Management of SSL Certificates

The Guardian Management Gateway software uses the X.509 certificate model to provide trusted access via the web interface. To enable secure web communication, a valid X.509 certificate must be installed on the Guardian Management Gateway device

An SSL certificate can be installed via the “Device Settings” -> “Security” -> “SSL Certificate” menu item (see Section 19.4 in the 63972-383 User Manual).

An SSL certificate is a file that is needed for secure HTTP (HTTPS) access to the Guardian; this file is issued by some certificate authority and confirms the identity of a specific HTTPS server, in our case, this is the identity of the Guardian device.

By default, the Guardian uses a self-signed certificate, which is generated automatically when the network configuration is changed. However, a user can install a certificate that is specific to the company and domain/host name used by the specific customer (if secure HTTP communication with the Guardian is needed); the Guardian device provides the necessary tools for that.

There are three kinds of certificates and certificate-related objects that the Guardian software can deal with:

- A certificate signed by a certificate authority (CA). This certificate must come from outside, and can be downloaded to the Guardian, stored there and installed as the active certificate
- A self-signed certificate. This certificate is generated on the Guardian and can be stored there and installed as the active certificate. When the active certificate is a self-signed one, Web browsers normally issue a warning when establishing an HTTPS session with the target server; the Web user must acknowledge the security risks to continue the communication
- A certificate sign request (CSR). This is a file that is generated on the Guardian and should be sent to a certificate authority to obtain a valid certificate. This file contains the necessary information about the Guardian, its location and ownership.

Self-signed certificates and certificates sign requests can be generated via the “Device Settings” -> “Security” -> “Create SSL Certificate” menu item.

3.4.6 IP Firewall

The Guardian Management Gateway firmware supports the IP firewall functionality, which can be configured to disable remote access based on the IP address of the remote system. This functionality is implemented using the standard Linux firewall mechanism (netfilter/iptables).

The IP Firewall can be configured using the DEVICE SETTINGS -> Security -> Firewall dialog of the web interface (see Section 19.1 in the 63972-383 User Manual).

The IP Firewall settings are separate for the IPv4 and IPv6 protocols, but have the same structure. The global firewall settings include:

- Enable firewall: true if the firewall is enabled for the given protocol, false otherwise
- Default firewall policy for incoming packets: *ACCEPT* or *DROP* packets

By default, the IP Firewall is disabled.

Each rule defines a network address (a host or subnet address) and the policy that applies to the packets originating from this address. The policy can be *ACCEPT*, *REJECT* or *DROP*. The order of rules is significant: for each incoming packet, the rules are examined in that order and the first matching rule determines the policy to be applied. If no rules match, the default policy is applied.

3.4.7 Role-Based Access Control

The Guardian Management Gateway software implements access control rules based on "roles". A role defines the operations that are allowed for all user accounts associated with this role. The "administrator" role provides full access to the Guardian Management Gateway functionality, including user creation/removal and role assignment. Using this mechanism, it is possible to limit certain critical functionality to "trusted" users.

The global role-based firewall can be managed by the "Device Settings"->"Security"->"Role-Based Firewall" menu item in the Web interface (see Section 19.3 in the 63972-383 User Manual). This firewall allows or denies logins for specific users from specific IP address ranges. The firewall settings are separate for the IPv4 and IPv6 protocols, but have the same structure. The global role-based firewall settings include:

- Enable role-based firewall: true if the role-based firewall is enabled for the given protocol, false otherwise
- Default role-based firewall policy: *ALLOW* or *DENY* login

By default, the role-based firewall is disabled.

Each rule defines a range of network addresses (IPv4 or IPv6 addresses), the list of roles and the policy that applies to the login attempt of a user belonging to one of the specified roles, from an IP address belonging to the specified range. The policy can be *ALLOW* or *DENY*. The order of rules is significant: for each login attempt, the rules are examined in that order and the first matching rule determines the policy to be applied. If no rules match, the default policy is applied.

3.4.8 Login and Password Policy Settings

The password and login policy can be managed by the "Device Settings" -> "Security" -> "Login Settings & Password Policy" menu item in the Web interface (see Section 19.2 in the 63972-383 User Manual).

The password and login policy on the Guardian is enforced by Pluggable Authentication Modules (PAM). The following PAM modules are involved:

- *pam_cracklib* is used to determine if the new password meets the criteria set out in the Guardian configuration. When the "Strong Passwords" feature is enabled in the Guardian configuration, the password is checked for length, characters used (uppercase, lowercase, numerical, special characters), and the ease with which the password may be guessed. It works for local system accounts only.
- *pam_pwhistory* saves the previously used passwords for each user in order to force password change history and prevent the user from alternating between the same passwords too frequently. When the Guardian "Password History Depth" configuration parameter is set to *N*, the module prohibits the reuse of the last *N* passwords.
- *pam_tally2* denies access if too many login attempts fail. The Guardian administrator can set the "Lock after failed attempts" and "Lock timeout (seconds)"

configuration parameters. They are propagated to the *pam_tally2* module as *deny* and *unlock_time* options, respectively. It works for local system accounts as well as for LDAP accounts.

- *pam_ldap* is used when the LDAP is enabled on the Guardian device.

The Password Aging interval can be set by the Guardian administrator (note that it only works for local system accounts). The PASS_WARN_AGE setting is *7*. It indicates how many days prior to the password expiration that warning notices will be sent to users (i.e., when they log in). The PASS_MIN_DAYS setting is *0*. It indicates how many days need to pass before the user is allowed to change their password since the last password change.
A Guardian user can be manually locked and unlocked by the Guardian administrator via the "User Management" -> "Users" menu item. When a local user is locked / unlocked, the changes are propagated to */etc/shadow* and The Guardian administrator can set a timeout interval in seconds after which if no data has been received within a SSH session, the session is closed.. If the "Idle Timeout Period (seconds)" is set to *0*, this feature is disabled.

A Guardian user can set the "Idle Timeout (seconds)" and "Delay Before Disconnect (seconds)" intervals for a Web Session via the "User Management" -> "Change User Preferences" menu item. In this case, a Web session of the user is closed if no data has been received with the Web session during the "Idle Timeout" interval. A warning is generated the "Delay Before Disconnect" seconds before the session closes. Also, the "Idle Timeout" and "Delay Before Disconnect" intervals for a Web session can be specified for a user by the Guardian administrator via the "User Management" -> "Users" menu item, when the user is created or edited. The default values of the "Idle Timeout" and "Delay Before Disconnect" intervals can be set via the "Device Settings" -> "Settings", the "User Defaults" tab.. The factory settings of the parameters are *600* (seconds) and *15* (seconds), respectively.

3.4.9 Restricted Service Agreement

The restricted service agreement can be managed by the "Device Settings" -> "Security" -> "Restricted Service Agreement Banner" menu item in the Web interface (see Section 19.5 in the 63972-383 User Manual).

A restricted service agreement (a special security banner) can be shown to a user during the logon in the Web interface. In addition, the restricted service agreement can be enforced, which means that the user should explicitly acknowledge it in order to be able to log in.

The following attributes are specified for the restricted service agreement:

- Show flag (*TRUE*/*FALSE*)
- The text of restricted service agreement
- Enforce flag (*TRUE*/*FALSE*)

3.4.10 Communication Matrix

The following tables summarize the network ports/services supported by the Guardian Management Gateway firmware:

PORT NUMBER / TYPE	NETWORK SERVICE DESCRIPTION
22/tcp *22/tcp6*	SSH server. A secure communication protocol, protected with data integrity and encryption algorithms.
23/tcp	Telnet server. An insecure protocol with every character passed as plain text in a separate packet. It is safer to use SSH instead of Telnet. This service is disabled by default.
80/tcp	HTTP server. This service is insecure. It can be disabled by setting the "Enforce HTTPS" flag.
161/udp *161/udp6*	SNMP server. The SNMP server supports both secure SNMP v3 and insecure v1/v2c access. It is possible to disable support of insecure versions and only support encryption for SNMP v3 connections.
443/tcp	HTTPS server. This service is secure.
47809/udp *47808/udp6*	BACnet server. This service is disabled by default.
443/tcp	RedFish server. This service shares the port with the HTTPS server but is disabled by default.

PORT NUMBER / TYPE	NETWORK CLIENT DESCRIPTION
67/udp *68/udp*	DHCP client. This client is running by default.
123/udp	NTP client. This client is running by default.
<dynamic>	SMTP client. This client is started by request when sending mail.
<dynamic>	LDAP client. This client is not running by default.
<dynamic>	IoT client. This client is running by default. The remote port 8883 on the IoT broker (AWS cloud or Azure cloud or AWS Greengrass) is accessed. If the "Use Web Sockets" flag is set, the remote port is 443.

3.4.11 Remote Access Protocol Versions

The following table summarizes the network communication protocols used by the Guardian Management Gateway device:

Protocol	*Version*
SSH	V2
NTP	V4
SNMP	V1,V2,V3
TLS	V1.2
HTTP/HTTPS	V1.1
LDAP	V3
Telnet	V1
BACnet	V1.19
MQTT	V3.1.1
Redfish	V1.6

3.5 Firmware Upgrade Security

The firmware upgrade mechanism uses a digital signature (SHA256 digest) to verify the integrity and authenticity of upgrade images. This ensures that it is not possible to program a corrupted image or an image that has not been approved and signed by nVent.

3.6 LCDUI

The LCD interface provides mostly read-only access to the Guardian Management Gateway device (i.e. obtaining device-specific information, sensor readings, etc), but it can also be used to acknowledge alarms and to update the device firmware/configuration from a USB Flash drive. Even though the environment in which a Guardian Management Gateway device is installed is expected to be secure, the LCDUI functionality can be further restricted by disabling front panel alarm acknowledgement and/or firmware and configuration updates using the corresponding configuration options accessible through the web interface (DEVICE SETTINGS -> Settings -> LCD UI SETTINGS).

3.7 Security Scanning

Each release of the Guardian Management Gateway firmware is scanned for security vulnerabilities using the Nexpose tool by Rapid7. All recent releases of the Guardian Management Gateway firmware have 0 reported vulnerabilities.

3.8 Maximum Security Configuration

To provide maximum protection of the Guardian Management Gateway device from unauthorized access, nVent recommends the following steps:

- Verify that the Telnet access method is disabled (DEVICE SETTINGS -> Network Services -> Telnet).
- Change the default administrator password before connecting the device to the network (USER MANAGEMENT -> Change Password).

- Set the login and password restrictions according to the desired level of protection (DEVICE SETTINGS -> Security -> Login Settings & Password Policy).
- Enable and configure the firewall to provide restricted access to authorized IP addresses only (DEVICE SETTINGS -> Security -> Firewall).
- If desired, enable and configure the role-based firewall to set up role-based access restrictions (DEVICE SETTINGS -> Security -> Role-based Firewall).
- Generate and upload a custom X.509 certificate (refer to section 3.4.8 above).
- Disable HTTPS access (DEVICE SETTINGS -> Network Services -> HTTP -> Force HTTPS for Web Access).
- Review the list of users (USER MANAGEMENT -> Users) and make sure that only the required user accounts are enabled, and that each user account is assigned the correct role.
- Review/change the restricted service agreement banner, if required (DEVICE SETTINGS -> Security -> Restricted Service Agreement Banner).