

NEXEDGE®

Release Notes

Information for December 2025 Update

NXR-1000 Series

R2.5

Last Updated: 16th. December. 2025

Language: English

Document No: RN-25-0003

Version: 1.00

Contents

Document Copyrights	- 2 -
Disclaimer	- 2 -
1. RELEASE INFORMATION	- 3 -
1.1. Compliance with RED Cybersecurity Requirements	- 3 -
1.2. Encrypted IP communication and password protection added	- 3 -
2. NXR-1000 FIRMWARE CHANGES	- 5 -
2.1. Initial Settings Changes	- 5 -
2.2. Add Password setting (connected PC software)	- 6 -
2.3. Add password setting (Hot Standby).....	- 8 -
3. CHANGES IN LICENSE MANAGEMENT CLIENT	- 10 -
3.1. KPT-300LMC.....	- 10 -
4. FIELD PROGRAMMING UNIT (FPU) CHANGES.....	- 11 -
4.1. KPG-D7.....	- 11 -
Revision History	- 12 -

Document Copyrights

Copyright 2025 is owned by JVCKENWOOD Corporation. All rights reserved.

No part of this manual shall be reproduced, translated, distributed or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, for any purpose without prior written consent from JVCKENWOOD Corporation.

Disclaimer

This document is intended to provide basic and general information about the specifications of the products listed above and the system configuration. The intended purpose of all technical descriptions herein shall be to improve your understanding of product specifications and system configuration. The descriptions provided in this document are carefully examined and are believed to be entirely reliable. JVCKENWOOD Corporation shall be entirely free from any responsibility and liability for inapplicability, damage or loss arising from inaccuracies in this document and reserves the right to change the product specifications herein to improve readability, function or product design. The applicability of the descriptions in this document may vary depending upon the product specifications and configurations of relevant equipment.

Furthermore, you are neither licensed nor entitled to use and/or divert any descriptions in this document to your application.

Contact JVCKENWOOD Corporation for further details.

The AMBE+2™ voice coding Technology embodied in this product is protected by intellectual property rights including patent rights, copyrights and trade secrets of Digital Voice Systems, Inc.

NEXEDGE® is a registered trademark of JVCKENWOOD Corporation in the U.S. and other countries

NXDNTM is a trademark of Icom Incorporated and JVCKENWOOD Corporation.

All other product names referenced herein are trademarks or registered trademarks of their respective manufacturers.

1. Release information

1.1. Compliance with RED Cybersecurity Requirements

The following new versions will be released in late December 2025:

- NXR-1000 series: R2.5

This update is designed to comply with the cybersecurity requirements of the European Radio Equipment Directive which came into force on August 1, 2025. After this date, radio equipment marketed in the EU market must comply with these requirements.

The changes are as follows:

- Encryption of IP communication between the repeater and PC software
- With this firmware update, the default settings of certain items are changed, and password protection is added for connected software and hot standby operation.
- Added the password for IP connection to KPT-300LMC.
- Added the password for IP connection to KPG-D7.

1.2. Encrypted IP communication and password protection added

To comply with the cybersecurity requirements specified in the European security regulations (Radio Equipment Directive), Encrypted IP communication and password protection are added between the repeater and PC software.

The following PC software can be encrypted.

< Target PC software >

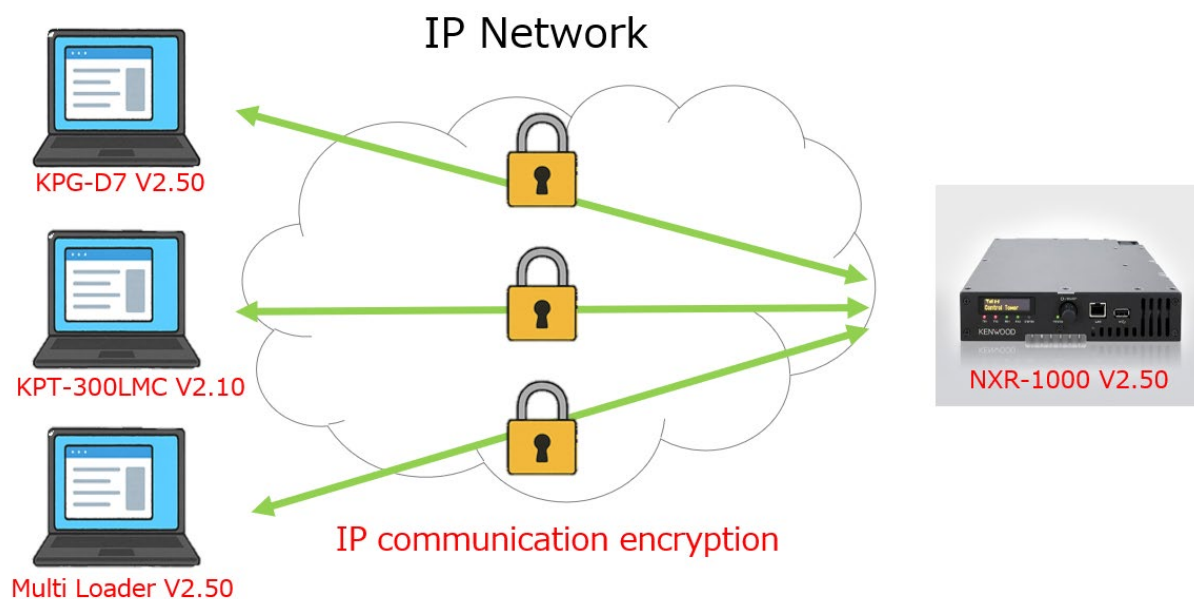
- KPT-300LMC
- KPG-D7
- Multi Loader

The following PC software and the repeater configuration Web Tool are also affected by the addition of the password. For Details, refer to " 2.2 Adding a password ", "3he repeater configuration Web Tool. License Management Client Changes," and "4. Field Programming Unit (FPU) Changes ".

< Applicable PC Software >

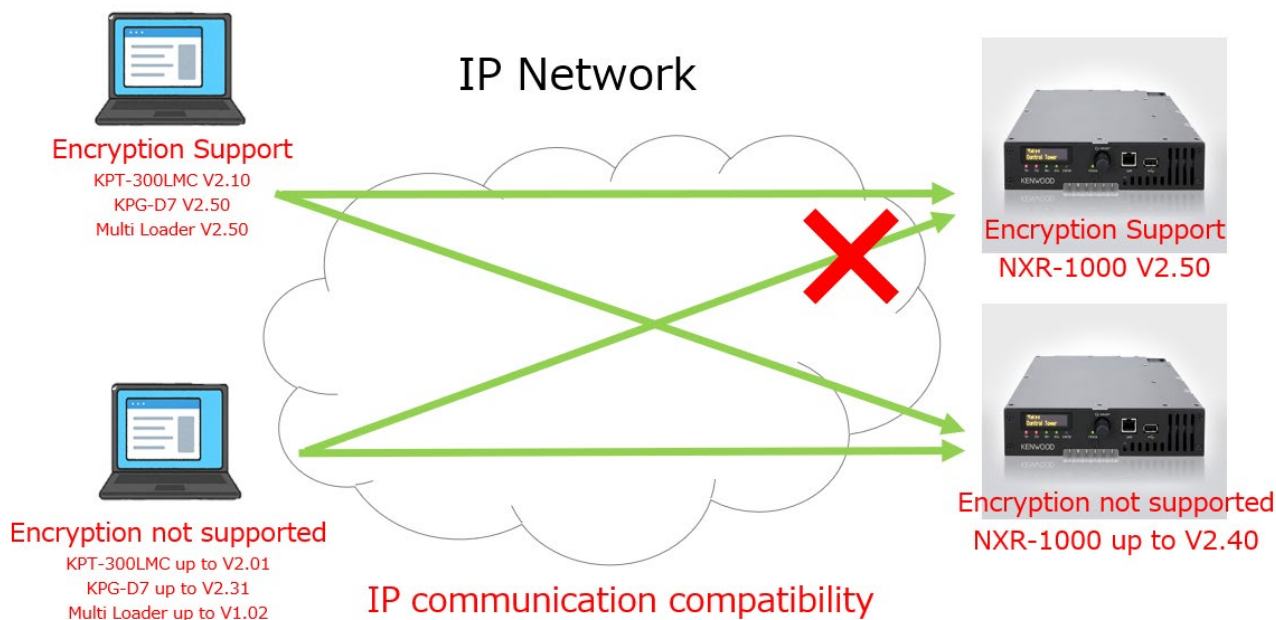
- KPT-300LMC
- KPG-D7

IP connection between the repeater and PC software is encrypted as shown below.



PC software that does not support encrypted IP communication cannot communicate with a repeater that uses encryption.

Compatibility between the old and new versions is as follows.



2. NXR-1000 Firmware Changes

2.1. Initial Settings Changes

The NXR-1000 Firmware Version is 2.50 and the following initial settings have been changed.

< Initial Settings to be Changed >

- Remote Access Control
- HTTP

<Remote Access Control>

Remote Access Control is a function that allows or prohibits network connections to a repeater.

Starting with Firmware Version 2.50, Remote Access Control is turned OFF by default value when shipped from the factory or when Factory Reset is performed.

Therefore, when connecting to Web Tool for the first time and making settings, you must first enable Remote Access Control.

If you update a repeater with Remote Access Control already enabled (ON) to Version 2.50, the current settings will be retained.

[Setting the operation of the unit]

1. Select "Control" from the OLED menu on the unit.
2. Select "Remote Access Control".
3. Change the setting from "Off" to "On".



(OLED Menu) Control > Remote Access Control

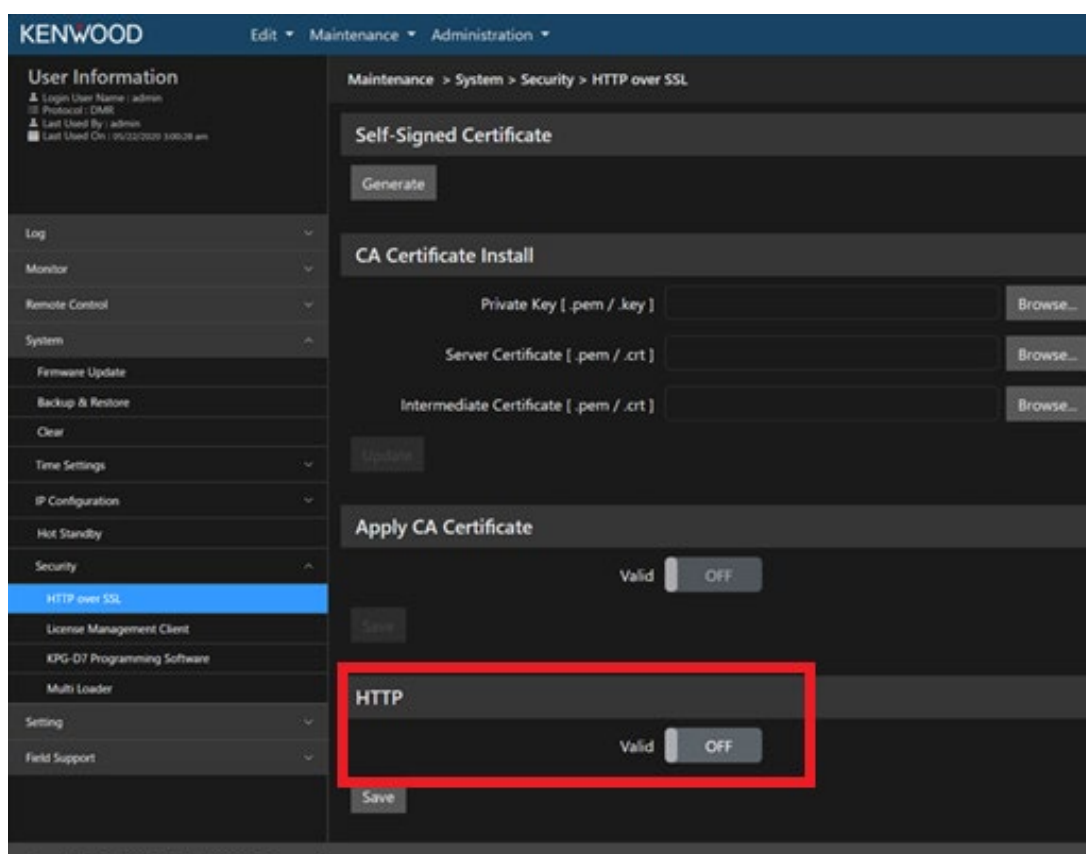


<HTTP>

From Firmware Version 2.50, at the time of shipment or Factory Reset, HTTPS connection is enabled, and HTTP connection is turned OFF by default.

If a repeater for which HTTP connection is already enabled (ON) is updated to Version 2.50, the setting in use is retained.

- HTTP setting location in Web Tool
(Maintenance > System > Security > HTTP over SSL > HTTP)



2.2. Add Password setting (connected PC software)

With Firmware V2.50, password settings are added to the Web Tool for the following PC software. This password is required to connect to the software.

For New Password (Confirm), you can confirm that the new password is correct by entering the new password again.

Note: HTTPS connection is required to set this password. Therefore, it is disabled to input a password for HTTP connection.

< PC software that requires additional password settings >

- KPT-300LMC V2.10
- KPG-D7 V2.50

• KPG-D7 Password setting location in the Web Tool

(Maintenance > System > Security > KPG-D7 Programming Software)

The screenshot shows the Kenwood Web Tool interface. On the left is a sidebar with 'User Information' and a menu including Log, Monitor, Remote Control, System, Firmware Update, Backup & Restore, Clear, Time Settings, IP Configuration, Hot Standby, Security, HTTP over SSL, License Management Client, and KPG-D7 Programming Software. The main area has a breadcrumb trail: Maintenance > System > Security > KPG-D7 Programming Software. The title is 'KPG-D7 Programming Software'. It features two input fields: 'New Password' and 'New Password (Confirm)', both highlighted with a red rectangle. A 'Save' button is located below the fields.

• KPT-300LMC (License Management Client) Password setting location in the Web Tool
(Maintenance > System > Security > License Management Client)

The screenshot shows the Kenwood Web Tool interface. On the left is a sidebar with 'User Information' and a menu including Log, Monitor, Remote Control, System, Firmware Update, Backup & Restore, Clear, Time Settings, IP Configuration, Hot Standby, Security, HTTP over SSL, License Management Client, and KPG-D7 Programming Software. The main area has a breadcrumb trail: Maintenance > System > Security > License Management Client. The title is 'License Management Client'. It features two input fields: 'New Password' and 'New Password (Confirm)', both highlighted with a red rectangle. A 'Save' button is located below the fields.

2.3. Add password setting (Hot Standby)

From firmware V2.50, it is required to set new password to be used for communication between repeaters using the Hot Standby function.

The same password must be set for the main and sub repeaters using the Hot Standby function.

- Password setting location in Web Tool
(Maintenance > System > Hot Standby)

KENWOOD Edit Maintenance Administration

User Information
 Login User Name : admin
 Protocol : DMR
 Last Modified By : admin
 Last Modified On : 05/25/2020 6:48:20 am

Log
 Monitor
 Remote Control
 System
 Firmware Update
 Backup & Restore
 Clear
 Time Settings
 IP Configuration
Hot Standby
 Security
 Setting
 Field Support

Maintenance > System > Hot Standby

Hot Standby

Valid ☐ OFF

Mode Main

Monitoring IP Address

Failsoft Mode

Failsoft Mode Wait Timer [s] 5

Failsoft Mode Wait Timer

Auto Active Status Switch

Valid ☐ OFF

Switch Time 1 : 00

Interval [day] OFF

Virtual IP Address

IP Address

Subnet Mask 255.255.255.0

Default Gateway 192.168.0.254

Save Password

- New Password setting location in Password

KENWOOD Edit Maintenance Administration

User Information
▲ Login User Name : admin
▲ Protocol : DMZ
▲ Last Modified By : admin
■ Last Modified On : 01/25/2020 6:48:20 am

Maintenance > System > Password (Hot Standby)

Password (Hot Standby)

New Password

New Password (Confirm)

Save Back

3. Changes in License Management Client

3.1. KPT-300LMC

KPT-300LMC version is 2.10.

From this version, the password setting for IP connection is added.

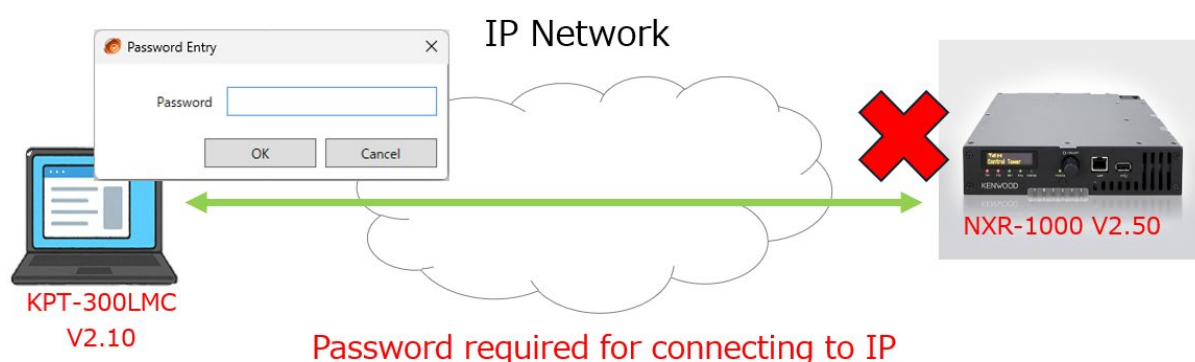
When the NXR-1000 Firmware V2.50 and KPT-300LMC V2.10 are connected via IP, the password request screen is displayed. This password is the same as the password for the KPT-300LMC previously set on the Web Tool.

KPT-300LMC can be used only when the correct password is entered.

The password is not required for serial connection.

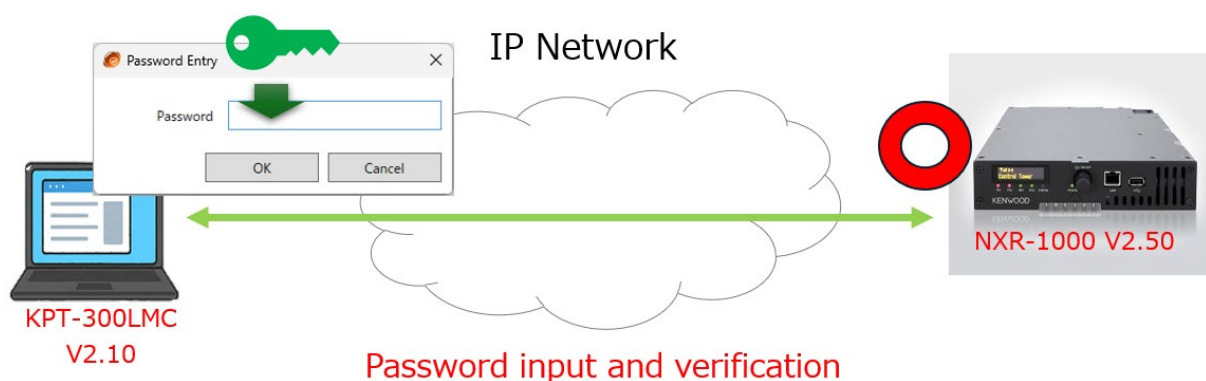
< Require password for IP connection >

KPT-300LMC cannot operate unless the correct password has been entered.



< Password input/verification >

KPT-300LMC is enabled when it matches the password set in the repeater.



4. Field Programming Unit (FPU) Changes

4.1. KPG-D7

KPG-D7 version is 2.50.

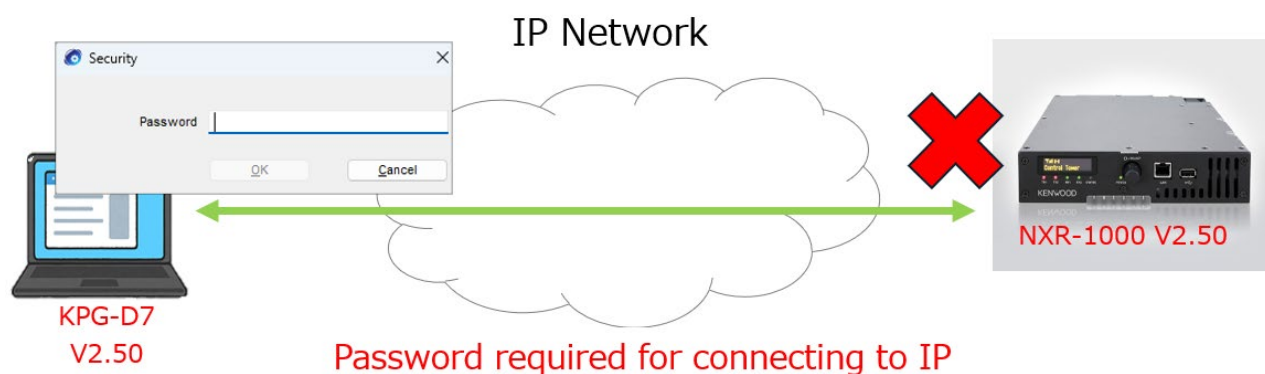
From this version, the password setting for IP connection is added.

When the NXR-1000 Firmware V2.50 and KPG-D7 V2.50 are connected via IP, the password request screen is displayed. This password is the same as the password for the KPG-D7 previously set on the Web Tool.

KPG-D7 can be used only when the correct password is entered.

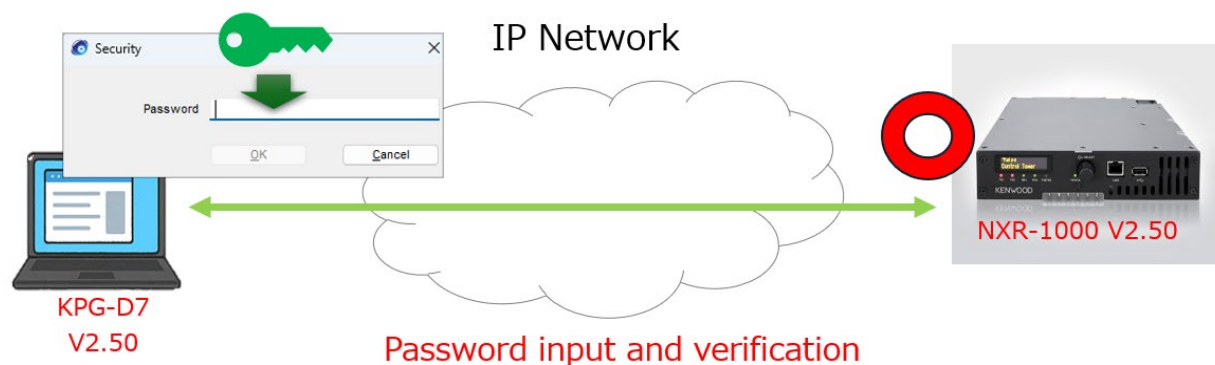
< Password request for IP connection >

KPG-D7 cannot operate unless the correct password has been entered.



< Password input/verification >

KPG-D7 is enabled when it matches the password set on the repeater.



Revision History

Version	Date of issue	Note
1.00	16th December 2025	First Release