

Application Notes

NXR-1000 series Installing a Server Certificate

Last Updated:	17 th February 2023
Language:	English
Document No.:	AN-23-0002
Version:	1.00

CONTENTS

Document Copyrights2

Disclaimer2

1. Introduction3

2. Applying a Server Certificate to NXR-1700.....4

2.1. Issuance and Application of the Self-Signed Certificate..... 4

2.2. HTTPS Connection with the Self-Signed Certificate 5

2.3. Applying the Server Certificate 6

2.4. Validating the Server Certificate 7

3. Confirmation of Application of the Server Certificate ...8

4. Invalidating the HTTP Connection.....9

Revision History10

Document Copyrights

Copyright 2023 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 and system configuration of NXR-1000 Series. The intended purpose of all technical descriptions herein shall be, to improve your understanding of the 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 in order to improve readability, function or product design. 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.

1. Introduction

This document introduces a method and approach to issue a Self-Signed Certificate and validate an HTTPS connection by applying a Server Certificate issued by a Certificate Authority (CA).

Note that we do not name any specific companies as the Certificate Authority in this document and shall leave it to your decision as to which one to choose.

Accordingly, this document does not contain any general description of a Private Key, which is necessary when obtaining a Server Certificate, and how to issue a Certificate Signing Request. Please ask and follow the guidance of your Certificate Authority regarding the Private Key and the Certificate Signing Request.

2. Applying a Server Certificate to NXR-1700

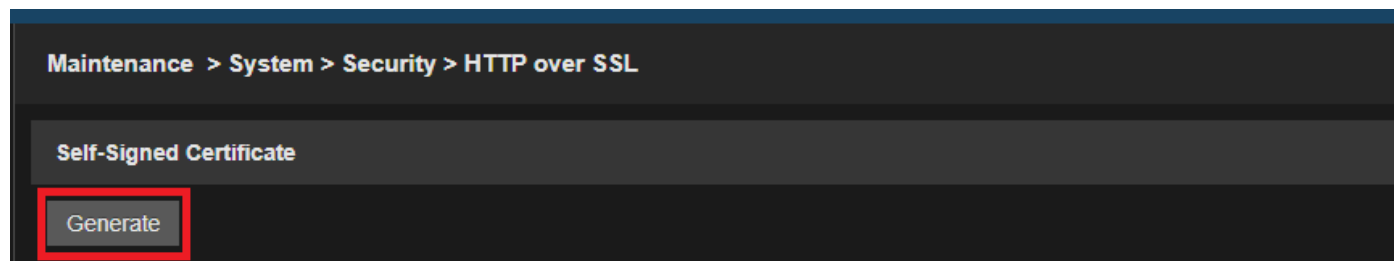
This section describes a method for validating HTTPS communication through the Web Tool of the NXR-1700. And it requires the followings that are issued by the Certificate Authority:

Item	Outline	Necessity
Private Key	Private Key Passphrase is NOT supported	Must
Server Certificate	Server Certificate	Must
Intermediate Certificate	Intermediate CA Certificate	Unnecessary when the Server Certificate includes the intermediate Certificate

2.1. Issuance and Application of the Self-Signed Certificate

The NXR-1700 requires the issuance and application of the Self-Signed Certificate before validating HTTPS communication authorized by the Certificate Authority. This enables an HTTPS connection with the Self-Signed Certificate to be available. The Server Certificate of the Certificate Authority is configured using the HTTPS connection with the Self-Signed Certificate.

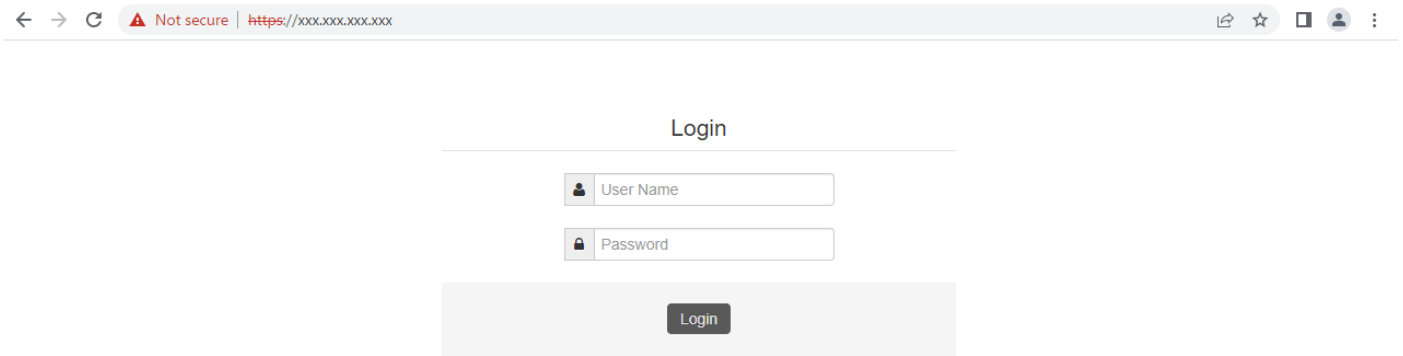
Click the “Generate” button and the Self-Signed Certificate will be issued and applied.



2.2. HTTPS Connection with the Self-Signed Certificate

Use the HTTPS connection to Login into the Web Tool after applying the Self-Signed Certificate.

The operations which will be introduced in Section 2.3 and thereafter are conducted using the HTTPS connection.



The screenshot shows a web browser window. The address bar at the top displays a red warning icon followed by 'Not secure' and the URL 'https://xxx.xxx.xxx'. Below the address bar, the page title 'Login' is centered. The main content area contains two input fields: the first is labeled 'User Name' with a user icon, and the second is labeled 'Password' with a lock icon. Below these fields is a dark gray button labeled 'Login'.

2.3. Applying the Server Certificate

The Private Key, the Server Certificate, and the Intermediate CA Certificate (as needed) that are obtained from the Certificate Authority should be configured on this page.

Click the “Update” button after completing the configuration and apply the configured files.

The screenshot displays a web interface for configuring SSL settings. At the top, a breadcrumb trail reads 'Maintenance > System > Security > HTTP over SSL'. Below this, there are two main sections: 'Self-Signed Certificate' and 'CA Certificate Install'. The 'Self-Signed Certificate' section contains a 'Generate' button. The 'CA Certificate Install' section contains three rows of input fields and buttons. The first row is for the 'Private Key [.pem / .key]' with the value 'server.key' and a 'Browse...' button. The second row is for the 'Server Certificate [.pem / .cert]' with the value 'server.crt' and a 'Browse...' button. The third row is for the 'Intermediate Certificate [.pem / .cert]' with an empty field and a 'Browse...' button. At the bottom left of the 'CA Certificate Install' section is an 'Update' button. All four buttons ('Generate', 'Browse...', 'Browse...', and 'Update') are highlighted with red rectangular boxes.

Maintenance > System > Security > HTTP over SSL

Self-Signed Certificate

Generate

CA Certificate Install

Private Key [.pem / .key] server.key Browse...

Server Certificate [.pem / .cert] server.crt Browse...

Intermediate Certificate [.pem / .cert] Browse...

Update

2.4. Validating the Server Certificate

Go to “Apply CA Certificate” on the settings menu and change the slide switch control to “ON”, then click the “Save” button to validate the Server Certificate.

Maintenance > System > Security > HTTP over SSL

Self-Signed Certificate

Generate

CA Certificate Install

Private Key [.pem / .key] server.key Browse...

Server Certificate [.pem / .cert] server.crt Browse...

Intermediate Certificate [.pem / .cert] Browse...

Update

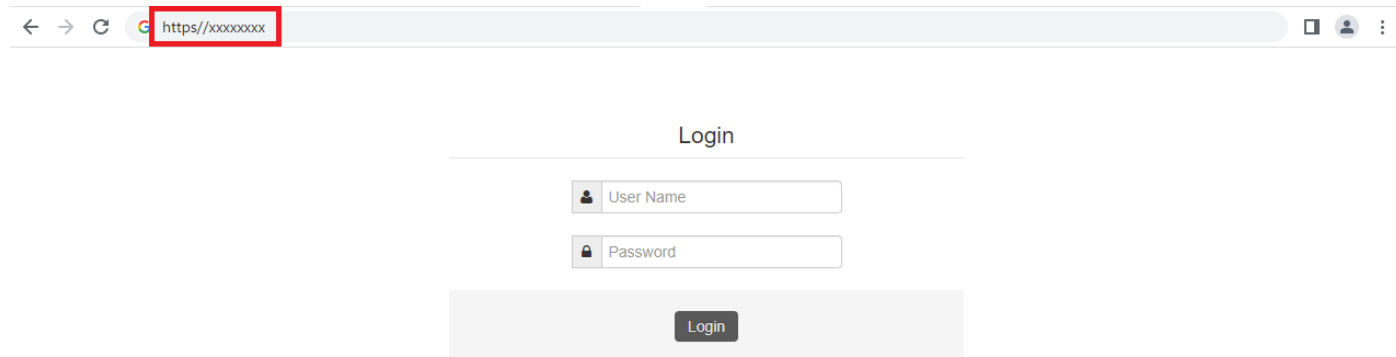
Apply CA Certificate

Valid ☒ ON

Save

3. Confirmation of Application of the Server Certificate

Enter "https://" followed by the Common Name that is designated when applying the Server Certificate in the web browser and establish the HTTPS connection.



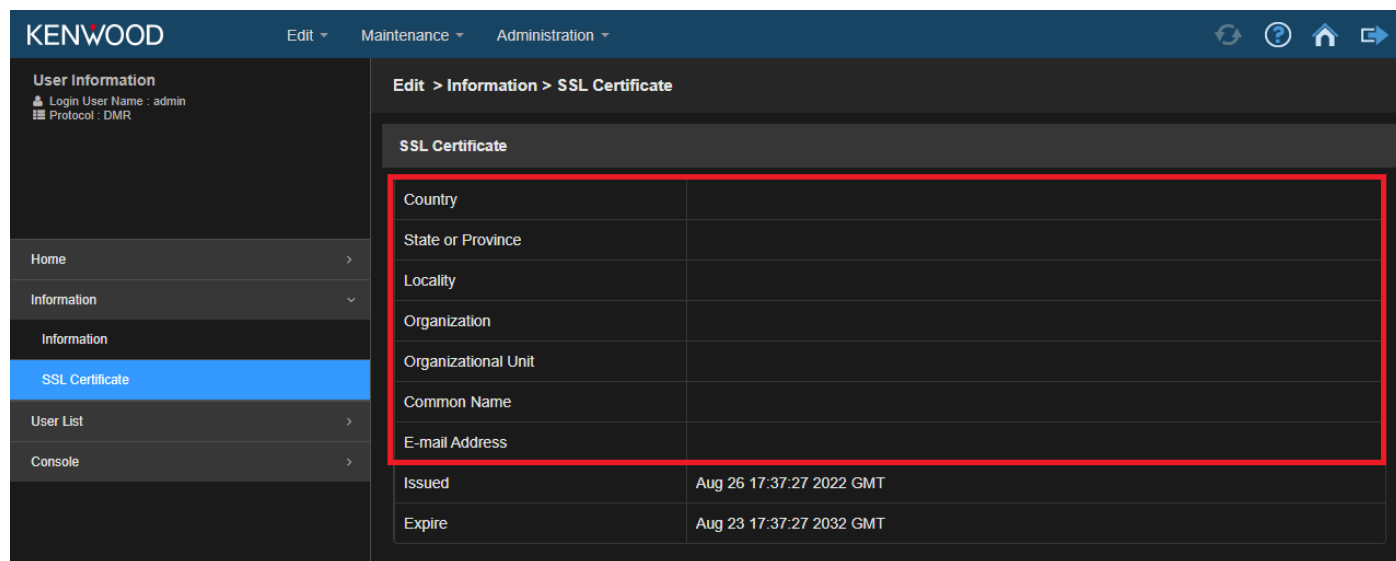
Login

User Name

Password

Login

Go to the “SSL Certificate” page and confirm whether the information given by the Certificate Authority is listed after the successful login.



KENWOOD

Edit Maintenance Administration

User Information

Login User Name : admin

Protocol : DMR

Home

Information

Information

SSL Certificate

User List

Console

Edit > Information > SSL Certificate

SSL Certificate

Country	
State or Province	
Locality	
Organization	
Organizational Unit	
Common Name	
E-mail Address	

Issued Aug 26 17:37:27 2022 GMT

Expire Aug 23 17:37:27 2032 GMT

4. Invalidating the HTTP Connection

Go to “HTTP” on the settings menu and change the slide switch control to “OFF”, then click the “Save” button to invalidate the HTTP Connection.

Upon completion of this invalidation, the NXR-1700 series only supports HTTPS access.

The screenshot displays a settings interface with a dark theme. It is divided into several sections:

- Self-Signed Certificate**: Contains a "Generate" button.
- CA Certificate Install**: Includes three rows for file selection:
 - Private Key [.pem / .key] with a text input containing "server.key" and a "Browse..." button.
 - Server Certificate [.pem / .cert] with a text input containing "server.crt" and a "Browse..." button.
 - Intermediate Certificate [.pem / .cert] with an empty text input and a "Browse..." button.Below these is an "Update" button.
- Apply CA Certificate**: Features a "Valid" label and a slide switch currently set to "ON". A "Save" button is located below.
- HTTP**: At the bottom, it has a "Valid" label and a slide switch currently set to "OFF". A "Save" button is located below this section.

Red rectangular boxes highlight the "Save" button in the HTTP section and the "OFF" position of the HTTP slide switch.

Revision History

Version	Date of issue	Note
1.00	17 th February 2023	First edition