How to Install CA-signed Certificates

RUGGEDCOM NMS v2.1 for Windows

https://support.industry.siemens.com/cs/ww/en/view/109760439

Siemens Industry Online Support

This entry is from the Siemens Industry Online Support. The general terms of use (http://www.siemens.com/terms_of_use) apply.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.
In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement—and continuously maintain—a holistic, state-of-the-art, industrial security concept. Siemens's products and solutions only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens's guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity.

Siemens's products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported and failure to apply latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under http://www.siemens.com/industrialsecurity.

Table of Contents

1 Introduction

The RUGGEDCOM NMS User Guide outlines how to create and install a new certificate. However, some users may want to use a CA-signed certificate on RUGGEDCOM NMS. For example, a corporation that runs its own certificate authority (CA) infrastructure may want to use its own trusted CA-signed certificate on RUGGEDCOM NMS.

This document outlines how to install a CA-signed certificate on RUGGEDCOM NMS v2.1 for Windows.

NOTE Self-signed certificates are flagged by browsers as insecure.

NOTE The procedure outlined in this document does not apply to RUGGEDCOM NMS v2.1 for Linux.

2 Obtaining the Shell Script

A proprietary shell script is needed install a CA-signed certificate. To obtain the script, submit a Service Request to Siemens Customer Support asking for a copy of the script to install a CA-signed certificate.

For more information, refer to Section 5, “Customer Support”.

3 Configuring the CA-signed Certificate

To be used with RUGGEDCOM RNMS, PEM-format keys and certificates must be saved in a Java KeyStore. For instructions, refer to the following subsections.

3.1 Preliminary Steps

First, do the following:

1. Generate a new private key.
2. Request a new CA-signed certificate for the private key.
3. Save the private key, certificate, and CA certificate to one directory.
4. Make sure that OpenSSL is installed. If necessary, download OpenSSL from `<https://www.openssl.org/source/>` and install it.

3.2 Packaging PEM Files in a PKCS KeyStore

The PEM-format key and certificates cannot be directly saved in a Java KeyStore; they must first be packaged in a PKCS KeyStore. To package the PEM files in a PKCS KeyStore, do the following:

1. Execute the following command:

   ```
   openssl pkcs12 -export -in <server.cert.pem> -inkey
   <private.key.pem> -certfile <CA.cert.pem> -name
   "<your.domain.com>" -out <your.domain.com>.p12
   ```

   Where:

   - **<server.cert.pem>** is the name of the server certificate file.

- **<private.key.pem>** is the name of the private key.
- **<CA.cert.pem>** is the name of the CA-signed certificate file.
- **<your.domain.com>** is the complete domain name of the RNMS server (e.g. rnms.ruggedcomnms.com).

2. When prompted, enter a password for the PKCS KeyStore.

3.3 Converting a PKCS KeyStore to a Java KeyStore

Once the PEM-format key and certificates are packaged in a PKCS KeyStore, the PCKS KeyStore must be converted to a Java KeyStore. To convert a PCKS KeyStore a Java KeyStore, do the following:

1. Execute the following command:

```
keytool -importkeystore -srckeystore <your.domain.com.p12> -
srcstoretype PKCS12 -destkeystore <your.domain.com>.jks -
deststoretype jks
```

   Where:

   - **<your.domain.com.p12>** is the name of the PKCS KeyStore.
   - **<your.domain.com>** is the complete domain name of the RNMS server (e.g. rnms.ruggedcomnms.com).

2. When prompted, enter the password configured in step 2 of Section 3.2, "Packaging PEM Files in a PKCS KeyStore".

4 Installing the RNMS Server Certificate

To install the RNMS server certificate, do the following:

1. Rename the Java KeyStore from Section 3.3, "Converting a PKCS KeyStore to a Java KeyStore" as *ruggednms.jks.*
2. Copy the Java KeyStore to the following folder: `C:\ruggednms\share`.
3. Save the script from Section 2, "Obtaining the Shell Script" to the following folder: `C:\ruggednms\scripts`.
4. Navigate to `C:\ruggednms\scripts` and execute the script.
5. Follow the on-screen prompts to install the RNMS server certificate on RUGGEDCOM NMS.

5 Customer Support

Siemens Customer Support is available 24 hours, 7 days a week for all Siemens customers. For technical support or general information, please contact Siemens Customer Support through any one of the following methods:

- **Online**

  Visit http://www.siemens.com/automation/support-request to submit a Support Request (SR) or check on the status of an existing SR.

- **Telephone**

  Call a local hotline center to submit a Support Request (SR). To locate a local hotline center, visit http://www.automation.siemens.com/mcms/aspa-db/en/automation-technology/Pages/default.aspx.

- **Mobile App**

  Install the Industry Online Support app by Siemens AG on any Android, Apple iOS or Windows mobile device and be able to:

  - Access Siemens's extensive library of support documentation, including FAQs, manuals, and much more
  - Submit SRs or check on the status of an existing SR
  - Find and contact a local contact person
  - Ask questions or share knowledge with fellow Siemens customers and the support community via the forum

6 History

Version	Date	Modifications
1	09/2018	Initial release.
2	11/2018	Updated terminology and added instructions for converting the CA-signed certificate into a Java KeyStore.