SIEMENS

FAQ • 06/2016

How to Regenerate Keys and Certificates

RUGGEDCOM RX1000/RX1000P/RX1100/RX1100P

https://support.industry.siemens.com/cs/ww/en/view/109738241

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, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit http://www.siemens.com/industrialsecurity.

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit http://support.industry.siemens.com.

Table of contents

1 Overview

By default, RUGGEDCOM ROX devices include static cryptographic keys and certificates for SSH and SSL. These cryptographic keys and certificates should be updated regularly to avoid security related issues.

This procedure describes how to remove the existing certificates and generate new certificates.

1.1 Regenerating Keys and Certificates

To regenerate the keys and certificates on the device, do the following:

1. Log in to the device as root via an SSH or serial console connection. For more information about logging in to the device, refer to the *ROX User Guide* for the device.
2. Delete the current HTTPS key by the typing the following command, then press **Enter**:

   ```
   rm /etc/webmin/miniserv.pem
   ```

3. Generate a new HTTPS key by typing the following command, then press **Enter**:

   ```
   /var/lib/dpkg/info/webmin.postinst configure
   ```

   The following message will appear:

   md5sum: miniserv.pem: No such file or directory

   Starting webmin: webmin

4. Restart the Web server by typing the following command, then press **Enter**:

   ```
   /etc/init.d/webmin restart
   ```

   The following message will appear:

   Restarting webmin: webmin

5. Delete the current SSH key by typing the following command, then press **Enter**:

   ```
   rm /etc/ssh/ssh_host_*_key*
   ```

6. Generate a new SSH key and restart SSH by typing the following command, then press Enter:

   For ROX v1.13 and newer

   ```
   /var/lib/dpkg/info/openssh-server.postinst configure.
   ```

   For ROX v1.12 and older

   ```
   /var/lib/dpkg/info/ssh.postinst configure
   ```

2 Customer Support

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' 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

3 History

Table 3-1

Version	Date	Modifications
1	6/2016	Initial release