Application Note

Setting up to use HTTPS

Software From
V08_20_04

Revision
v1.0

Publish Date
December 2017

CUBIC | vocality

AN315 SETTING UP TO USE HTTPS

HTTPS requires the Security software (RTUSEC)
at VOS07_44.01 or later
and a Feature Key on all products.

1 Overview

This Application Note explains how you can configure CA-signed certificates, which may be needed because newer web-browsers no longer support self-signed certificates.

Overview: Certificates for HTTPS

Certificates are associated with a specific address or addresses. These could be DNS addresses, an FQDN such as www.vocality.com or one or more IP addresses.

You are able to install a single certificate on your Vocality unit. That certificate must be associated with the IP address(es) from which HTTPS access is required.

Each certificate is associated with a Private Key, stored on your Vocality unit.

2 Summary of steps for installing the certificate from a CA

1. Choose a Certificate Authority (CA) and follow their instructions to generate a Private Key and a Certificate Signing Request, which applies to the IP address(es) that your Vocality unit will be using for HTTPS.
2. Submit your certificate request following the CA's instructions.
3. Install the Certificate and Private Key into your Vocality unit (see **Section 3**). If the certificate is provided in PEM format you can use it as it is, otherwise you will need to run a utility to convert a PKCS12 or DER format certificate to PEM format.
4. Reboot your Vocality unit.
5. Test HTTPS operation with the browsers you intend to use. (In some cases, you may need to ensure that your CA's root certificate is installed on the PC running the browser as well as installing the private key and certificate on the Vocality unit.)

3 Installing a PEM format key and certificate on your Vocality unit

Access your Vocality unit on the M&C/SerialTelnet interface. This cannot be done through the web interface.

1. On the **HTTPS and SSH > HTTPS menu** set HTTPS CERTIFICATE MODE to Config.
2. Type **<Ctrl>E** to return to the main banner page.
3. From the **Banner page** type (uppercase):

   D D D

   M

   This will take you to the debug command prompt 'Dbg>'.
4. Type **HTTPS CERT**. This will take you to the HTTPS Shell with command prompt 'HTTPS Certificate

Shell>'. (If you need reminders about the commands available here just type **HELP**).

5. Type **KEY** then paste in the private key for your Vocality unit in PEM format. (Just open the PEM format files with a text editor such as Notepad or vi, to copy the contents as required.)

   Press **<Enter>** then paste the private key in again for confirmation.

   Press **<Enter>** to leave a blank line.

6. Type **CERT** then paste in the certificate for your Vocality unit in PEM format. (Just open the PEM format files with a text editor such as Notepad or vi, to copy the contents as required.)

   Press **<Enter>** then paste the certificate in again for confirmation.

   Press **<Enter>** to leave a blank line.

7. If no errors have been reported, type **SAVE**.

   The KEY and CERT values are only held locally as '(new) - Not Set' values until you commit them to be stored in encrypted form as the '(current config)' by typing SAVE.

8. You now need to reboot unit to cause change to take effect: type **EXIT** to leave the HTTPS Certificate Shell, then type **BOOT**.

   Until the unit is rebooted you the **HTTPS and SSH > HTTPS menu** will not show that this data has been set.

4 Checking whether a valid key and certificate are stored on your Vocality unit

1. From the **Banner page** type (uppercase):

   D D D

   M

   This will take you to the debug command prompt 'Dbg>'.

2. Type **HTTPS CERT**. This will take you to the HTTPS Shell with command prompt 'HTTPS Certificate Shell>'. (If you need reminders about the commands available here just type **HELP**).

3. Type **SHOW**.

   You would expect valid Private Keys to show as:
   -----BEGIN RSA PRIVATE KEY-----
   << data hidden >>
   -----END RSA PRIVATE KEY-----

   You would expect valid Certificates to show as:
   -----BEGIN CERTIFICATE-----
   << data hidden >>
   -----END CERTIFICATE-----

   If any of these visible headers or footers have been entered incorrectly you will be warned of a **Suspect format** when they are loaded.

5 Checking whether the correct key and certificate are stored on your Vocality unit

Go through the steps in **Section 3** over again, up to step 6, without a SAVE, to enter key and/or certificate details that you want to test. At this point type **COMP** to compare the '(new) - Not Set' values with the '(current config)' values.

If the '(new) - Not Set' and '(current config)' values are different you can then go on to choose **SAVE** to commit your newly entered values, then **EXIT** and **BOOT**.

6 Erasing old key and certificate data stored on your Vocality unit

1. From the **Banner page** type (uppercase):

   D D D

   M

   This will take you to the debug command prompt 'Dbg>'.

2. Type **HTTPS CERT**. This will take you to the HTTPS Shell with command prompt 'HTTPS Certificate Shell>'. (If you need reminders about the commands available here just type **HELP**).

3. Type **CLEAR**.

4. Type **SAVE** to commit your newly entered null values, then **EXIT** and **BOOT**.

Alternatively, a factory default will erase any stored key and certificate.

7 About Application Notes

Application Notes are intended as a supplement to, rather than a substitute for, your User Manual. Should you have queries which are not answered by our current documentation, your local Vocality support team would be happy to hear from you.
E-mail **support@vocality.com**.