Application Note

Configuring SSH on Vocality units

Software From
V07_04_01

Revision
v1.5

Publish Date
November 2017

CUBIC | vocality

AN309 CONFIGURING SSH

SSH requires the Security software (RTUSEC) and a Feature Key on all products.

1 Overview

This Application Note explains how you can configure an SSH server on Vocality units (with software VOS06_03.01C or later, RTUSEC versions only from VOS07_44.01 onwards). You will need to configure either **Password mode SSH** or **Pre-shared key mode SSH**.

Overview: SSH Server

Secure Shell (SSH) is a network protocol, which allows data exchange using a secure channel between two network devices. SSH is an alternative to remote shells which send information, in particular passwords, in plain text, posing a security risk. SSH encryption offers confidentiality and data integrity over unsecured networks.

The SSH server is present in all nodes that support IP – so on a chassis based system (V150 or V200), there will be a separate SSH client on each slot that supports IP.

Vocality does not provide an SSH client. Commercial and freeware SSH clients (such as PuTTY) are available for several platforms. Any client that supports the standard SSH-2 protocols and provides a subset of common cryptography, message digest, key exchange and authentication mechanisms with the server is suitable.

2 Pre-requisites

Your unit should be running the RTUSEC software variant, with a Feature Key loaded, to enable SSH.

If you plan to use keys, you will also need:

- Free software such as PuTTYgen, or a similar package, to generate SSH key pairs;
- Free software such as PuTTY, or a similar SSH client, which can accept SSH keys.

The IP address, or network, of units permitted to access your unit needs to be specified in the **IP > Access Table**, shown in Figure 1 .

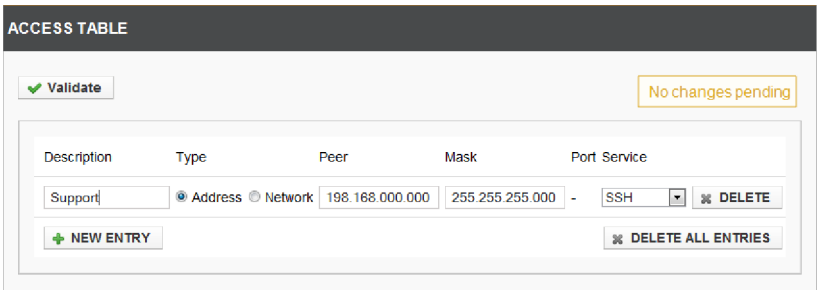

Figure 1 IP > Access Table menu

3 Password mode SSH

In the **HTTPS and SSH > SSH Server >Key and Authentication menu** set AUTH MODE to **`Password`**.

Log in via SSH using your usual VOS user account credentials. You will be prompted for these twice. (If user accounts are disabled it will be possible to log in with any or no username and password.)

4 Pre-shared key mode SSH

Use PuTTYgen or similar to generate a public/private key pair. Please note the following points:

- VOS supports RSA or DSA keys
- VOS supports 512-2048 bits with a default of 1024, while PuTTYgen defaults to 2048 bits.
- The Key Passphrase is optional. If a Passphrase is not entered, the device can be accessed via SSH by just using the Private Key and Node Name. Your VOS Username and Password will be required after connection, if VOS User Accounts are enabled.

Save your private key (.ppk) file.

In the **HTTPS and SSH > SSH Server >Key and Authentication menu** set AUTH MODE to **`Key`**.

Copy the Public Key string shown in the PuTTYgen window and paste it into the AUTH PUBLIC KEY space on the **HTTPS and SSH > SSH Server >Key and Authentication menu** and press **<Enter>**. When your changes to this menu are saved the CURRENT HOST KEY STATE should show Valid.

Load the private key (.ppk) file into your SSH client. In PuTTy this is done by choosing to **<Browse>** for the private key file, in the window shown in Figure 2 .

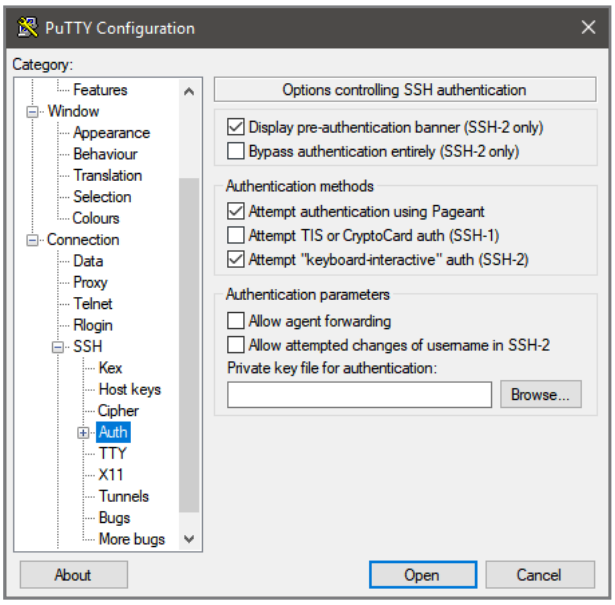

Figure 2 PuTTy v0.70 configuration

When you choose **<Open>** to start the SSH connection to your unit:

- Login using the Vocality Node Name. (If you have not changed it, the default is Node Name is **`Node1`**.)
- Your password is the Passphrase configured in PuTTYgen, if any. (If a Passphrase has not been configured in PuTTYgen you will not be asked for one.)
- You will then be prompted to enter your VOS Username and Password, if VOS User Accounts are enabled. If not, you will have access the menus structure straightaway.

5 Diagnostics

Two user-level diagnostics commands may be of use.

The **`ssh info`** command reports information about any connected clients (client address, crypto and HMAC algorithms used). For example, with a single client connected:

```
Dbg> ssh info

SessionID: 4097

Client address: 192.168.000.021

InCipher: aes256-ctr

InMAC: hmac-sha1

OutCipher: aes256-ctr

OutMAC: hmac-sha1
```

The session ID supplied may be used to force the disconnection of this client. The **`ssh disconnect`** *session ID* command can be used for this. You will need to specify the Session ID of the client to disconnect. For example:

```
Dbg> ssh disconnect 4097

Closing SSH session 4097...

Complete
```

6 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**.

A MENUS

A.1 SSH Server menu

The feature is only available in the secure variant of software.

The SSH Server menu allows generation of the host key, configuration of the user authentication mechanism (password or pre-shared key-based), selection of the crypto algorithms available and selection of the HMAC algorithms available.

A.1.1 SSH > Key & Authentication menu

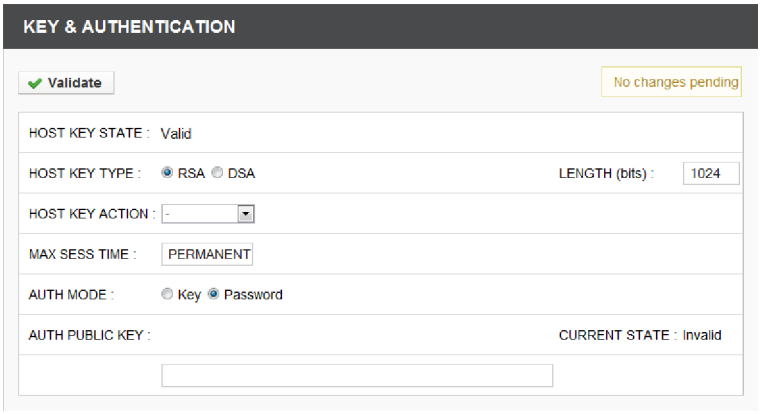

Figure 3 SSH > Key & Authentication menu - Password mode

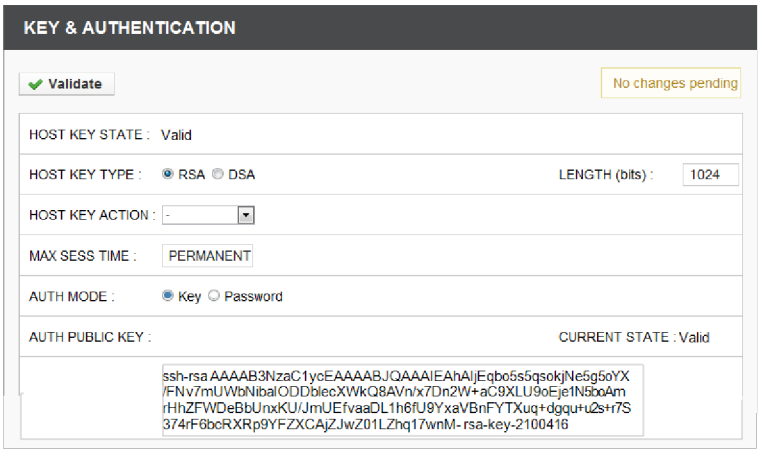

Figure 4 SSH > Key & Authentication menu - Key mode

The SSH Key & Authentication menu presents configuration parameters and controls for host keys used during asymmetric cryptography, session timeouts, and session authentication settings. Please refer to your User Manual for information about how user passwords are used with SSH.

Parameter	Range	Default	Use
Host Key Control			
HOST KEY STATE	Valid/Invalid	-	Read-only. Reports the state of the current host key. There must be a valid host key present for the SSH to work.
HOST KEY TYPE	RSA/DSA	RSA	Type of host key to use. (Note: The host key will be regenerated when this field is changed.)
LENGTH (bits)	512-40962048	1024	Length of key to generate in bits. This must be a multiple of 128 bits – will be rounded down to nearest multiple on entry if incorrect. (Note: The host key will be regenerated when this field is changed.)
HOST KEY ACTION	- / Regenerate / Zeroize	-	Regenerate the host key or zero it (Note: When the key is regenerated or zeroed, only subsequent SSH connections made will be affected – existing connections will use the host key that was present when they connected.)
Session Control			
MAX SESS TIME	10-1440 or PERMANENT	PERMANENT	Maximum session time in minutes. Use PERMANENT for unlimited session time
Authentication Control			
AUTH MODE	Password/Key	Key	Authentication mode required
AUTH PUBLIC KEY	String entry	-	The public key to use for key authentication mode
CURRENT STATE	Valid/Invalid	-	Read-only. Reports the state of the current authentication key.

Table A-1 Parameters in the SSH > Key & Authentication menu

When configuration changes are saved, a new host key will be generated and stored if any of the following conditions occur:

- current host key is invalid;
- host key type has been changed;
- host key length has been changed;
- host key action is set to regenerate.

Host key generation can be a lengthy operation. A progress indicator shows elapsed time against an estimated worst case. For RSA keys longer than 1024-bits this process can take minutes, or even tens of minutes to complete. Please wait for the key generation and save mechanism to complete. You cannot interrupt the key generation mechanism. Unit configuration may be corrupted and lost if you switch power off before key generation is complete.

Note: On the first connection following key generation, or regeneration, there will be a warning. This indicates that the server host key has changed from a previously cached value.

If the client is attempting to authenticate the server, then the client will need to be updated with the server's host public key following any key regeneration.

A.1.2 SSH Server > Crypto menu

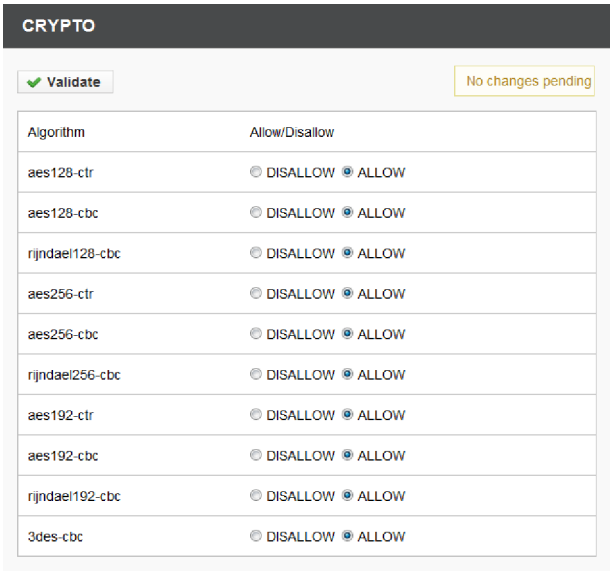

Figure 5 SSH Server > Crypto menu

The Crypto menu controls which symmetric cryptographic algorithms are advertised to the client during SSH protocol negotiation. By default all algorithms are allowed. This can be used to ensure a minimum strength of encryption is used. A row is presented for each crypto algorithm supported. Each can be set to ALLOW or DISALLOW.

A.1.3 SSH Server > HMAC menu

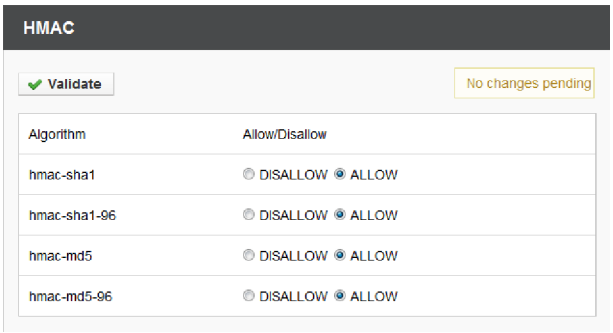

Figure 6 SSH Server > HMAC menu

The HMAC menu controls which message digest (hash-based message authentication code) algorithms are advertised to a client during SSH protocol negotiation. A row is presented for each mechanism supported, providing a parameter to ALLOW or DISALLOW each option. By default all algorithms are allowed to provide maximum interoperability.