



BOSCH

Invented for life

BVMS 7.5 - Single Port (SSH) Connectivity

www.boschsecurity.com

Author: Verhaeg Mario (ST-ESS/MKP1)

Date: 06-Oct-2017 12:46

Document information

| | |
|---------------|-------------------------------|
| Project | Bosch video management system |
| Reference | BVMS |
| Version | 6 |
| Last modified | 06 October 2017 |

Version history

| Version | Date | Who | Description |
|---------|-----------------|-------------|-------------|
| 6 | 06 October 2017 | David Brent | Final |

Introduction

When working with previous versions of BVMS, remote connectivity was cumbersome due to the amount of port mapping that needed to be configured. BVMS 7.5 provides a new method of remote connectivity utilizing Secure Shell (SSH) Tunnelling.

SSH Tunnelling constructs an encrypted tunnel established by an SSH protocol/socket connection. This encrypted tunnel can provide transport to both encrypted and un-encrypted traffic. The Bosch SSH implementation also utilizes Omni-Path protocol, which is a high performance low latency communications protocol developed by Intel.

Key management

The BVMS SSH service generates a private and public key when it is started for the first time. Both keys are saved in an encrypted file. When the BVMS SSH service restarts this file is detected and the private key is read.

Content

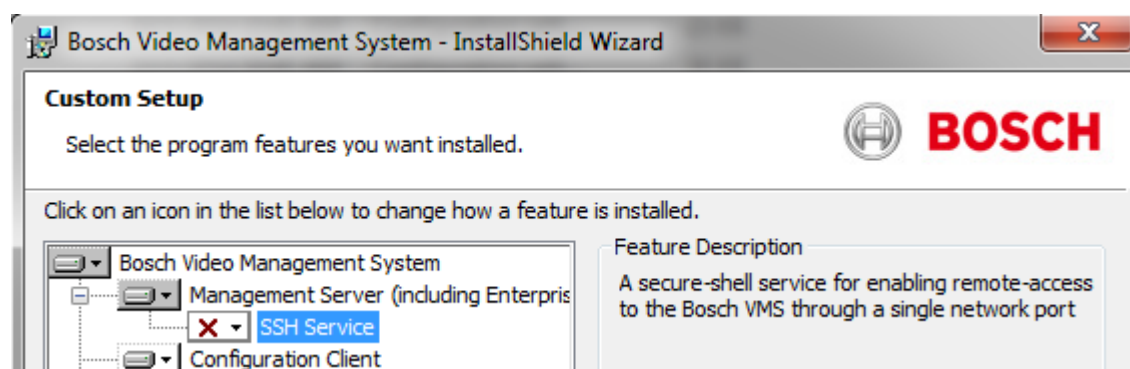
- Document information
 - Version history
- Introduction
- - Key management
- Content
- 1. Configuration
 - 1.1. Installation
 - 1.2. Port mapping entry
- 2. Operation
 - 2.1. Login with the Operator Client
- 3. Verification

1. Configuration

1.1. Installation

There is little to no configuration required for this feature to function.

- The SSH Service must be installed and running. If deploying a BVMS Pro system, insure the SSH Service is part of the installation process.
- Recording Appliances that ship with BVMS 7.5 should have the service pre-installed. Check your “Services”.



If the service has not been installed, the install package can be run from the BVMS 7.5 downloadable install package. If working with a DIVAR IP Recording Appliance, the appliance “Installer Package” must be used.

1.2. Port mapping entry

The primary configuration step is to configure one (1) port forwarding for the BVMS Central Server to utilize port 5322 for both internal and external connections. This is the only port mapping entry that needs to be made for the entire system.

Note

BVMS Port Mapping is not required!

The image below shows a sample configuration.



Copyright Robert Bosch GmbH.

2. Operation

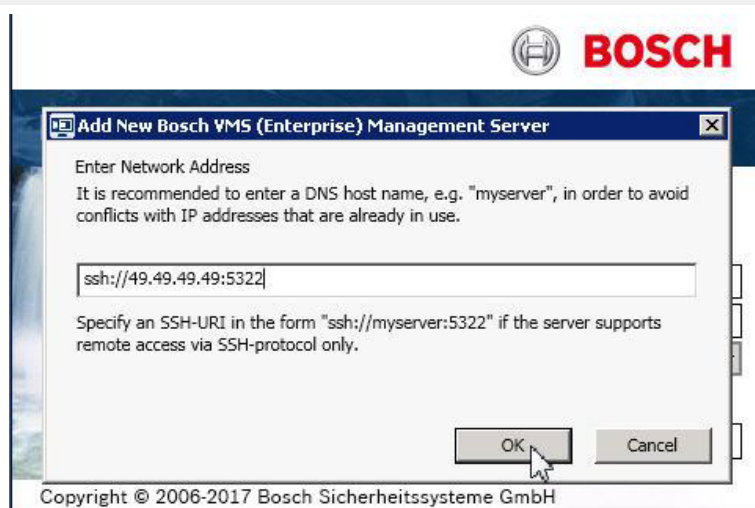
2.1. Login with the Operator Client

After the basic configuration is done, logging in via Operator Client is very intuitive:

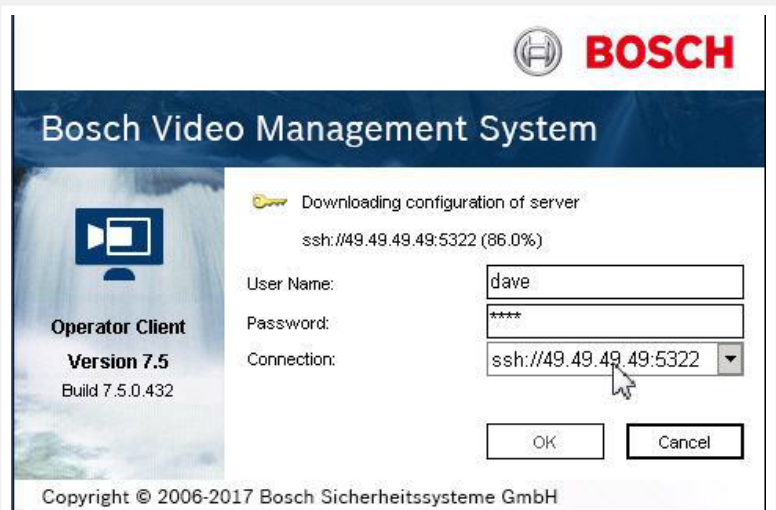
From the log menu, select the "Connection" drop down menu, then Select <New...>



You will be prompted to enter an IP address or DNS host name. You will also notice a cheat guide below the entry menu that will assist with address entry. Addressing must be in the following format: `ssh://IP or servername:5322`. In the example we used: `ssh://49.49.49.49:5322`.



After entering a properly formatted address, enter a valid user name and password. SSH users **MUST** have a password associated with their BVMS account. User accounts without a password cannot log in utilizing an SSH Connection.




The screenshot shows the Bosch Video Management System Operator Client login interface. At the top right is the Bosch logo. The title bar reads "Bosch Video Management System". On the left, there is a graphic of a monitor with a play button icon, labeled "Operator Client Version 7.5 Build 7.5.0.432". The main area displays a progress bar for "Downloading configuration of server" at "ssh://49.49.49.49:5322 (86.0%)". Below this, there are input fields for "User Name:" (containing "dave"), "Password:" (containing "****"), and "Connection:" (a dropdown menu showing "ssh://49.49.49.49:5322"). At the bottom right are "OK" and "Cancel" buttons. The footer text reads "Copyright © 2006-2017 Bosch Sicherheitssysteme GmbH".

3. Verification

After connection is established via an SSH Tunnel, all communications between the BVMS Server (192.168.1.19) and a remote client (49.49.49.48) are encrypted. Below is a Wireshark Capture taken from the BVMS Server after a connection is established.

| Time | Source | Destination | Protocol | Length | Info |
|------------|--------------|--------------|-----------|--------|---|
| 1 0.000000 | 192.168.1.51 | 192.168.1.19 | TLSv1.2 | 507 | Application Data |
| 2 0.000112 | 192.168.1.19 | 49.49.49.48 | Omni-Path | 614 | |
| 3 0.002428 | 49.49.49.48 | 192.168.1.19 | Omni-Path | 198 | |
| 4 0.002492 | 192.168.1.19 | 192.168.1.51 | TLSv1.2 | 139 | Application Data |
| 5 0.003725 | 192.168.1.51 | 192.168.1.19 | TCP | 60 | 443→49390 [ACK] Seq=454 Ack=86 Win=1579 Len=0 |
| 6 0.031465 | 192.168.1.51 | 192.168.1.19 | TLSv1.2 | 507 | Application Data |
| 7 0.031577 | 192.168.1.19 | 49.49.49.48 | Omni-Path | 614 | |
| 8 0.033776 | 49.49.49.48 | 192.168.1.19 | Omni-Path | 198 | |
| 9 0.033824 | 192.168.1.19 | 192.168.1.51 | TLSv1.2 | 139 | Application Data |



Bosch Sicherheitssysteme GmbH
ST/ESS-MKP1
Postfach 11 11
85626 Grasbrunn
GERMANY