Bosch Security System | Video Systems

Quick Lockdown Guide

Firmware 6.4

BOSCH
Invented for life

Overview

The purpose of this technical brief is to provide easy step-by-step instructions on how to increase the security of your IP camera installation, as well as reduce the device's visibility during vulnerability scans. This is known as reducing a device's "Attack Surface".

This brief is written utilizing a Bosch IP starlight 7000 HD camera (CPP 7) in a defaulted state with Firmware 6.4 installed and Bosch Configuration Manager 5.50. The assessment tools that are referenced in this document are *Nexpose*/*Insight* by Rapid 7 and NMAP.

Prior to Starting

You should have a firm understanding of the difference between *Vulnerability Testing* and *Penetration Testing.* Vulnerability scanning is the second of the three basic phases of the hacking called *Vulnerability Analysis*. This process analyzes specific targets for a range of possible weaknesses. There are a wide range of tools used for this process to include Nexpose, Nessus, Metasploit, Spartan, and NMAP. All of these tools utilize a database of documented vulnerabilities which are typically geared towards servers, PC, and mobile devices. Remember, in most cases these tools are the same tools that hackers use.

Penetration testing, or phase three of an active attack, is the act of attempting to leverage the individual vulnerabilities found during the *Vulnerability Analysis* phase*.* This phase is time consuming on a vulnerability by vulnerability basis, and pen testing one vulnerability may take days or weeks.

The terms *Vulnerability and Penetration* testing are often used synonymously. While there are tools such as Metasploit that can perform both of these functions, they are two different processes. Both of these processes can be performed in one of three ways:

- ***White Box:*** Full knowledge of device, passwords etc. typically in a lab environment
- ***Grey Box:*** Some or partial knowledge of device and the network it resides on. Production environment, tester has limited access to the network and device.
- ***Black Box:*** No knowledge. Device is in a secure production environment. Tester has no physical access to the device or the network.

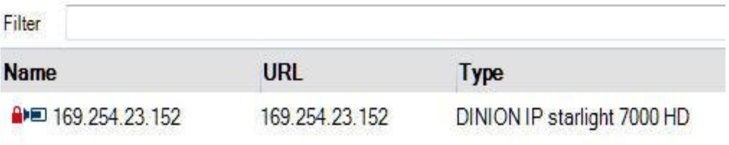
Remember the purpose of a vulnerability assessment is to show you your possible weaknesses so you can remedy any actual issues

Note: *Vulnerability Testing can also be referred to as Vulnerability Analysis and Scanning*

Initial Discovery and Configuration

All Bosch IP cameras devices with firmware 6.3 or later installed by default are configured for DHCP. If no DHCP server can be found, they will generate a unique APIPA IP Address (169.254.x.x).

A defaulted device with firmware 6.40 installed will appear with a "Lock" icon. From this state, an IP address can be assigned, but no further configuration can be performed until a password has been applied.

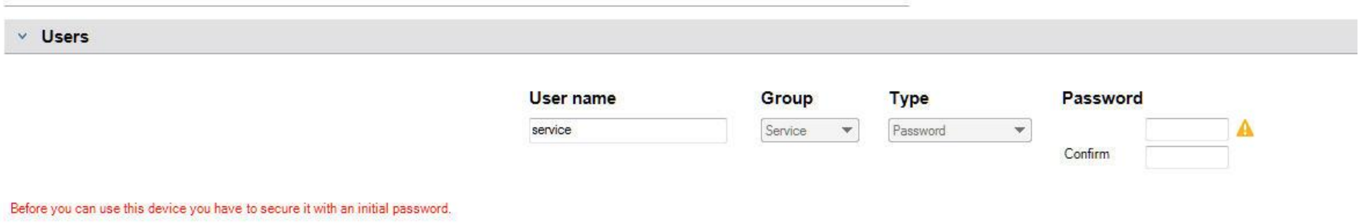


Filter

Name	URL	Type
🔒 169.254.23.152	169.254.23.152	DINION IP starlight 7000 HD

Note: *If working with a device that is already part of a configured system, the device will not be locked after you upgrade from an earlier version of firmware to 6.4 or higher.*

To apply an initial password to a defaulted device, highlight the device in Configuration Manager, and utilizing the *General, Unit Access, and Users* submenu, enter the desired password. The password must be a minimum of eight (8) characters.



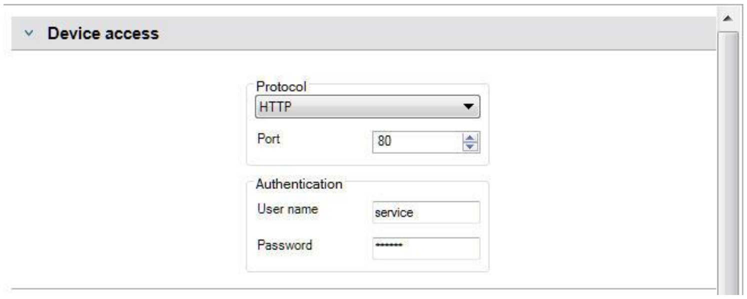
Users

User name	Group	Type	Password
service	Service	Password	
		Confirm	

Before you can use this device you have to secure it with an initial password.

After a password has been applied, the device will still appear to be protected. After adding the devices to the "My Devices" tree in Configuration Manager, select the *General, Unit Access, and Device Access menu.*

- Specify the "service" account and apply the newly-generated password to unlock the device.



Device access

Protocol: HTTP

Port: 80

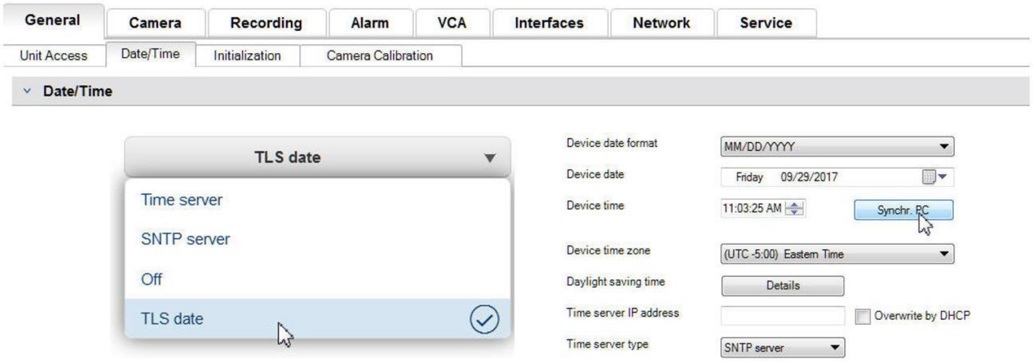
Authentication

User name: service

Password: ••••••

Time and Date

As of firmware 6.20, all devices provide a new option for time synchronization, TLS Date. Unlike *Time* and *NTP* protocols which are unsecure, the TLS-Date option can be configured using TLS protocol. Any HTTPS server can be can configured as a time provider, and time is provided via an HTTPS “Handshake”. A root certificate from the HTTPS server can also be added to the camera’s certificate store.



Device date format: MM/DD/YYYY
Device date: Friday 09/29/2017
Device time: 11:03:25 AM
Device time zone: (UTC -5:00) Eastern Time
Daylight saving time: Details
Time server IP address: □ Overwrite by DHCP
Time server type: SNTP server

From the *General, Time and Date* menu:

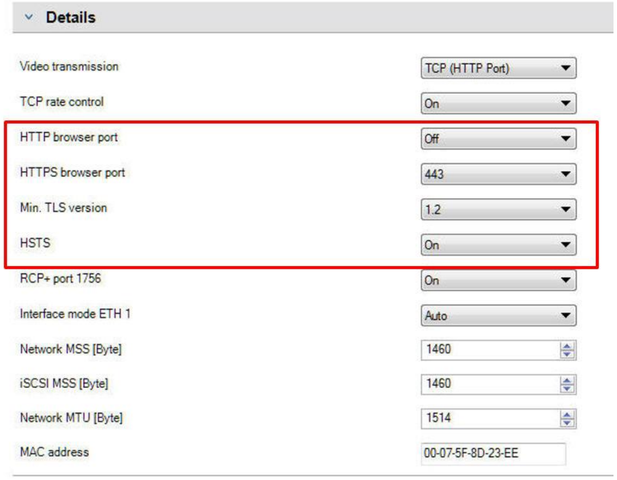
- Enter the IP address of a valid HTTPS server in your network
- Select “TLS date” in the drop down menu

Network Access and Services

All network and vulnerability scanners are designed to scan a specific range of ports and the protocols associated with those ports. By default, all unnecessary ports have been disabled in Bosch IP cameras, and certain protocols have been removed, such as Telnet.

The *Network and Network Access* menu allows you to modify how the device will communicate with the system. To further reduce the device’s presence on the network, set the following:

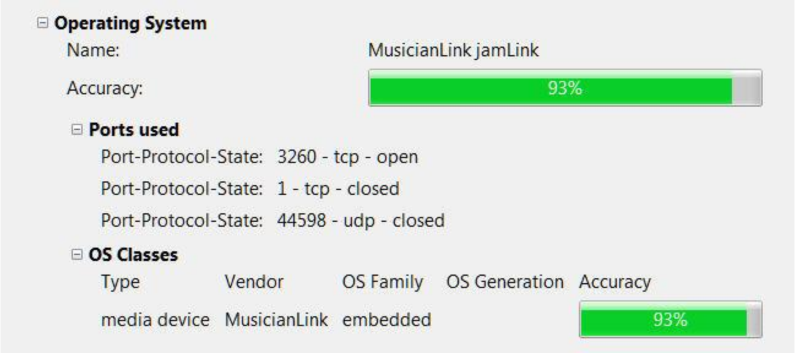
- HTTP Browser Port: OFF
- Min TLS version: 1.2
- HSTS: ON



Video transmission	TCP (HTTP Port)
TCP rate control	On
HTTP browser port	Off
HTTPS browser port	443
Min. TLS version	1.2
HSTS	On
RCP+ port 1756	On
Interface mode ETH 1	Auto
Network MSS [Byte]	1460
iSCSI MSS [Byte]	1460
Network MTU [Byte]	1514
MAC address	00-07-5F-8D-23-EE

Note: If modifying devices that will be utilized in BVMS, the devices should be scanned and added to BVMS prior to network access modification. If not, they will need to be manually entered into the system.

An optional HTTPS setting is to change the default port 443 to an alternate port starting at 10433. Since most vulnerability test tools are designed to detect specific protocols on specific ports. This basic communications port change causes the device to be either undetectable or recognizable as a valid device. In the example below, NMAP will see a Bosch camera as a “JamLink” OS device.



Operating System

Name: MusicianLink jamLink

Accuracy: 93%

Ports used

Port-Protocol-State: 3260 - tcp - open

Port-Protocol-State: 1 - tcp - closed

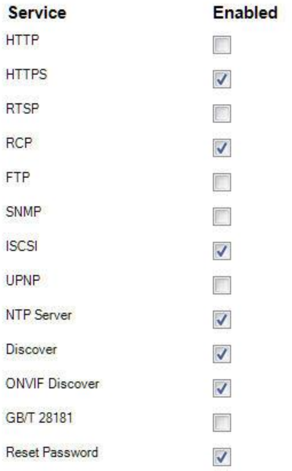
Port-Protocol-State: 44598 - udp - closed

OS Classes

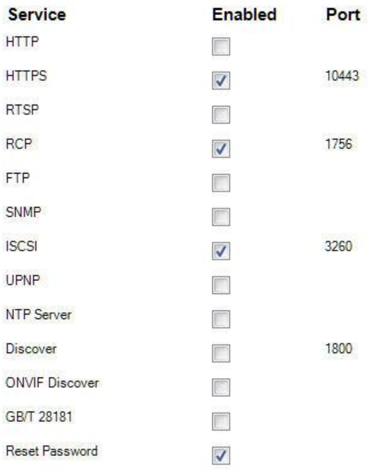
Type	Vendor	OS Family	OS Generation	Accuracy
media device	MusicianLink	embedded		93%

NMAP Scan after 443 port change

The next menu is the *Network, Network Services* menu. This menu provides the opportunity to disable any remaining ports that are not needed in a particular installation. In the example below, we have disabled everything except: HTTPS, RCP, iSCSI, and Rest Password

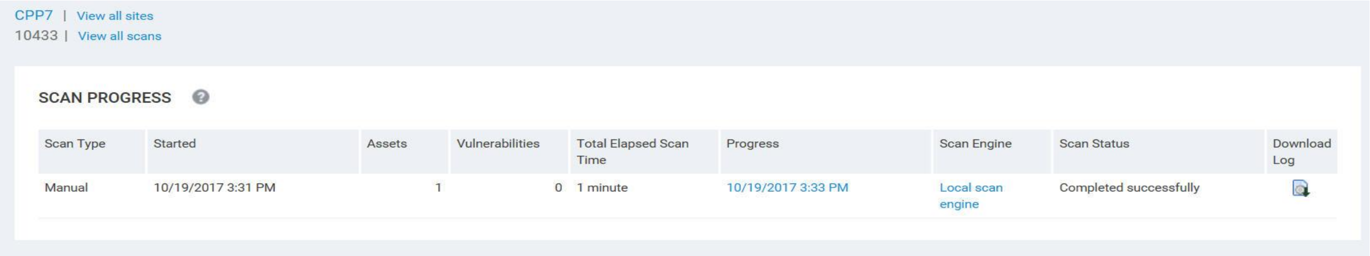


Service	Enabled	Port
HTTP	□	
HTTPS	☑	10443
RTSP	□	
RCP	☑	1756
FTP	□	
SNMP	□	
ISCSI	☑	3260
UPNP	□	
NTP Server	☑	
Discover	☑	1800
ONVIF Discover	☑	
GB/T 28181	□	
Reset Password	☑	



Service	Enabled	Port
HTTP	□	
HTTPS	☑	10443
RTSP	□	
RCP	☑	1756
FTP	□	
SNMP	□	
ISCSI	☑	3260
UPNP	□	
NTP Server	□	
Discover	□	1800
ONVIF Discover	□	
GB/T 28181	□	
Reset Password	☑	

These basic adjustments leave programs like Nexpose and Insight by Rapid 7 with basically nothing to scan, as none of the built in scan engines are programmed for “outside” the box.

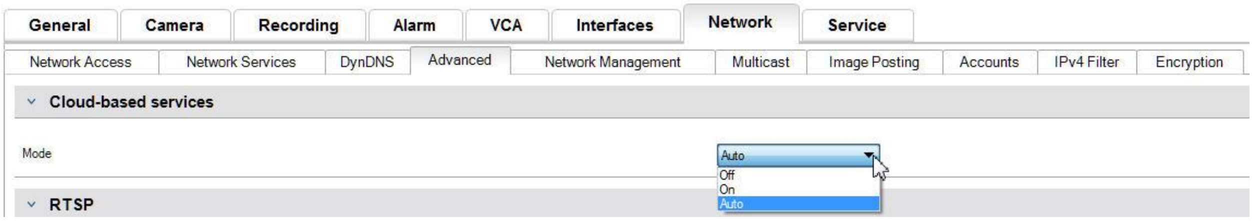


CPP7 | View all sites
10433 | View all scans

SCAN PROGRESS

Scan Type	Started	Assets	Vulnerabilities	Total Elapsed Scan Time	Progress	Scan Engine	Scan Status	Download Log
Manual	10/19/2017 3:31 PM	1	0	1 minute	10/19/2017 3:33 PM	Local scan engine	Completed successfully	

All Bosch devices can supply specified “Meta Data” to Bosch Cloud Services. The *Network and Advanced* submenu allow you to disable this feature. The default setting is “Auto”, select “Off”.



Cloud-based services

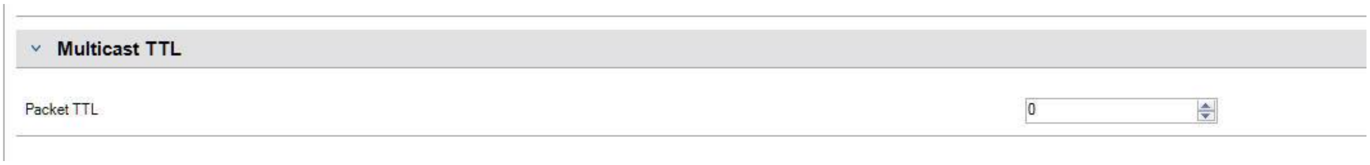
Mode: Auto

Off
On
Auto

- ***Auto (default):*** On boot up the video device will attempt to poll the Cloud Server a few times, and if unsuccessful, it will cease attempting to reach the cloud server.
- ***On:*** The video device will constantly poll the Cloud Server
- ***Off:*** No polling is performed

The *Network and Multicast* menu provides the Time-To-Live (TTL) menu, which specifies how many hops a multicast packet can traverse prior to being discarded. Below is a chart that specifies the distance a packet can survive. Even if you are not utilizing multicast at this time, the default number of “64” should be changed to either a 1 or a 0.

- TTL Value 0 = Restricted to local host
- TTL Value 1 = Restricted to same subnet
- TTL Value 15 = Restricted to same site
- TTL Value 64 (Default) = Restricted to same region
- TTL Value 127 = Worldwide
- TTL Value 191 = Worldwide with limited bandwidth
- TTL Value 255 = Unrestricted Data



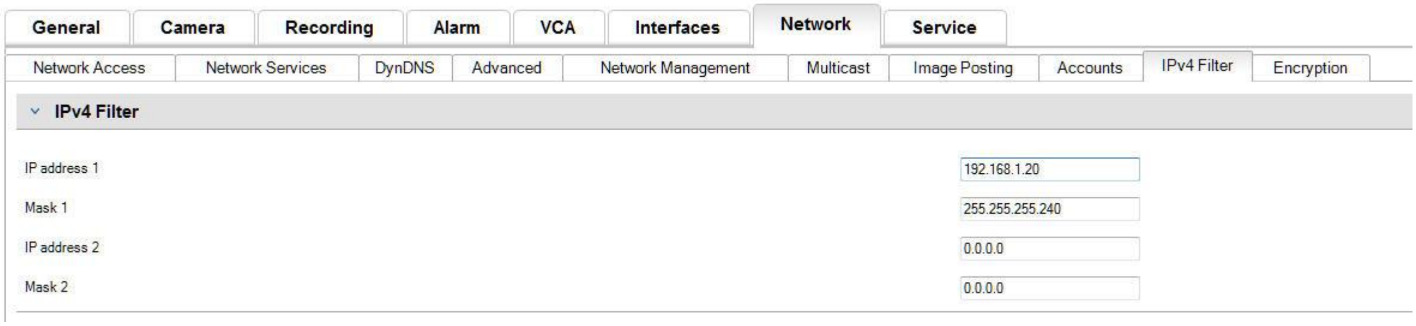
Multicast TTL

Packet TTL: 0

IPv4 Filtering

Probably the most powerful tool that is built into all Bosch video devices is the IPv4 Filtering tool. This feature allows you to restrict access to any Bosch IP video device down to a specific IP Address pool. IPv4 filtering utilizes the basic fundamentals of “subnetting” to define up to two allowable IP address ranges. Once defined, access to the devices is denied from any IP address not within the defined parameters. An example would be a small system with 50 cameras, 2 Workstations, and a DIVAR IP Recording Appliance. You could define a filter that only allows access from the Appliance and video system workstations. This eliminates any internal threats

Using Configuration Manager, with the device highlighted, select the *Network* menu and the *IPv4 Filter* submenu.



IPv4 Filter

IP address 1: 192.168.1.20
Mask 1: 255.255.255.240
IP address 2: 0.0.0.0
Mask 2: 0.0.0.0

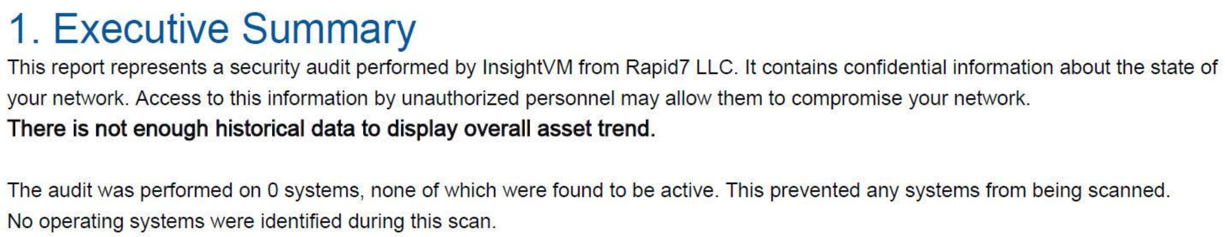
Note: To successfully configure this feature, you must have basic understanding of subnetting or have access to a subnet calculator.

When adding a filter rule, you will make two entries:

- A base IP address that falls within the subnet rule you create. The base IP address specifies which subnet you are allowing and it must fall within the desired range.
- A subnet mask that defines the IP addresses with which the IP video device will accept communication.

In the example above, we entered an “IP address 1” of 192.168.1.20 and a “Mask 1” of 255.255.255.240. This setting will restrict access from devices that fall within the defined IP range of 192.168.1.16 to .31.

This feature essentially acts as a “cloaking” device. As shown below, when the device is scanned from outside the “allowed” IP range, Insight does not see the target as “active”.



1. Executive Summary

This report represents a security audit performed by InsightVM from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

There is not enough historical data to display overall asset trend.

The audit was performed on 0 systems, none of which were found to be active. This prevented any systems from being scanned.
No operating systems were identified during this scan.

Conclusion

We live in a wired world, and every day there are thousands of new threats from every source imaginable: Rogue nations, state sponsored attacks, social engineering, script kiddies, and professional cyber criminals.

Being proactive is the best practice you can implement, not only on your production networks but on your security systems as well. While all Bosch IP devices are loaded with a closed OS that runs in limited memory space and can only be written to with digitally signed firmware, basic lock down procedures protect you from threats both external and *internal*.

More in-depth security features can be configured on Bosch devices such as the utilization and deployment of certificates in several scenarios. All units contain the built in firewall that protects from botnet attacks. For more information on these features and more, see the *BoschIPVideoDataSecurityGuidebook.pdf* which is available for download at www. boschsecurity.us