Secure by default
Increasing the default level of IP camera security
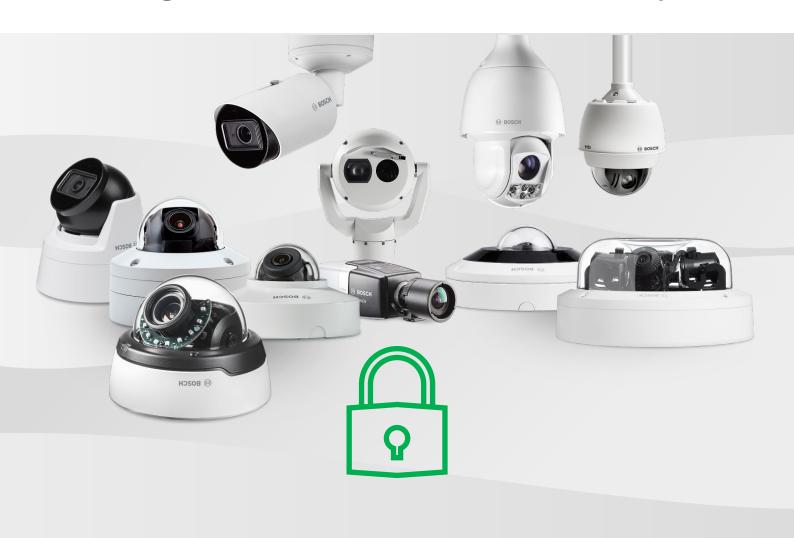
Table of contents

1   Introduction

At Bosch, we were always aiming for best possible security of our IP cameras as well as other devices and solutions. Numerous documents, like security-related tech notes as well as a hardening guide, our Data Security Guidebook, had been created, published, and marketed to create the necessary education and awareness.
Since security features are evolutionary advancements that are not immediately applied to and usable in existing installations, remaining backward compatible with new firmware releases and cameras was long considered more important than achieving the best security by default.

With increasing demand for better default security, in accordance with our security certifications, and with more and more systems having evolved into using increased security measures, now is the time to finally do the switch to stronger default settings and not only rely on education and documentation.

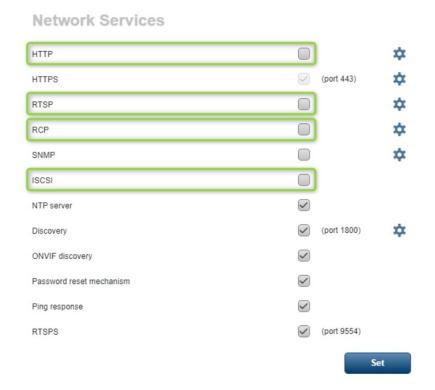# 2   New secure default settings

Bosch will undertake a cybersecurity best practice by disabling certain ports on the camera by default. This best practice is being undertaken to reduce potential attack surfaces and limit the exposure of sensitive services, as mentioned in our Data Security Guidebook since years.
This new secure default behavior will be standard with new firmware releases as mentioned below, applies to cameras that are produced with these firmware versions, and will also apply to all cameras that are being upgraded in the field to one of these or future firmware versions.

Platform	Firmware version	Expected release date
CPP14	9.0	October 2023
CPP13	8.90	July 2023
CPP7.3, CPP7, CPP6	7.88	December 2023

The following ports will be disabled by default:
- RCP+   ports 1756
- HTTP   port 80
- RTSP   port 554
- ISCSI Server   port 3260

2.1   What is the immediate impact of this?

- RCP+ is the native communication interface to the camera. On a secured camera, this protocol needs to go through an HTTPS tunnel.
- Most web browsers have moved to use HTTPS instead of HTTP for initially connecting to URLs, so the impact of closing the HTTP port is considered irrelevant for browser applications.
  For installations that use HTTP as the main communication protocol, though, this may have a major impact since communication to the cameras from a VMS using default HTTP settings is interrupted.
- Modern video decoders and viewers provide means of using secure RTSP connections but need to be configured to do so. If solely relying on RTSP, such clients will not receive video anymore.
- Bosch IP cameras provide a possibility to expose their local storage medium as an iSCSI drive. Access to local storage is not possible anymore, and as a result, direct iSCSI replay is not functional anymore as well.

2.2   How do default settings work in Bosch IP cameras?

The configuration of a Bosch IP camera comes with default settings that evolved over the years to reflect the best practice settings for standard applications.

If configuration settings have not been changed or touched, their values remain at their default states. Such settings will receive the new default values with the firmware update and immediately assume the new behavior.

A setting that had been modified, or even overwritten with the same value, is considered a changed value, intentionally set, and thus not considered default anymore. Such settings will not be affected when the default values are changed by a firmware update. New default values would then only apply to these settings after a factory reset.

- The RCP+ port 1756 is typically not changed to another port, or disabled and re-enabled, so will most likely remain at its default. Thus, if never being changed, it will receive its new default, being switched off.

- HTTP is typically used with port 80, so will most likely also remain at its default.
  Thus, if never being changed, it will receive its new default, being switched off.

- RTSP is typically used with port 554, with no need to be changed or switched off, so will most likely also remain at its default. Thus, if never being changed, it will receive its new default, being switched off.

- The iSCSI server is typically used with port 3260, with no need to be changed or switched off, so will most likely also remain at its default. Thus, if never being changed, it will receive its new default, being switched off.

A camera that is used out of the box without changing anything, which is likely due to the effort we spent on making the camera's default values the most appropriate for standard use cases, will see the full effect from the changed security defaults.

2.3   How can the settings be reverted?

Quite easily, the closed-off ports can be re-enabled through:
- the camera webpage, using HTTPS in the browser,
- the Bosch Configuration Manager, using HTTPS as the selected communication protocol,
- an RCP+ integration in a video management system, using a secure tunnel with RCP-via-HTTPS.

Re-enabling the ports is considered an intentional configuration and will remain during future firmware updates until a factory reset.

Note: Reverting the port closure lowers the security level of the system and shall only be considered if there is no way to improve the overall security settings of the system.
Take it as a chance to improve security where possible.

2.4   How can negative impact be avoided?

Wherever possible, security measures should be in place to a necessary extend before the firmware is updated.

With video management systems that support secure connections, they should be configured to make use of that before the cameras are updated with one of the secured firmware versions.
Where this is not possible, it could make sense to update in smaller batches, then re-configure the cameras to have them working again in the non-secure environment to keep downtimes of the surveillance system low and partial.

A web browser cache might need to be cleared, especially if the browser "learned" to use HTTP to a camera instead of trying HTTPS first.

2.5   Why are other ports still open?

The discovery ports are kept open to allow configuration tools to detect the device on the network. These two ports do not provide an attack surface due to their limited purpose, and do not need to be closed.

The NTP server port and the Ping response (ICMP) also have limited purpose and do not provide an attack surface, so do not need to be closed.

The password reset mechanism is a service using a browser connection, now secure, that does not use an own port.

Client connections going out of the camera may open their required ports. These are using services on other servers or devices but do not provide attackable services themselves.