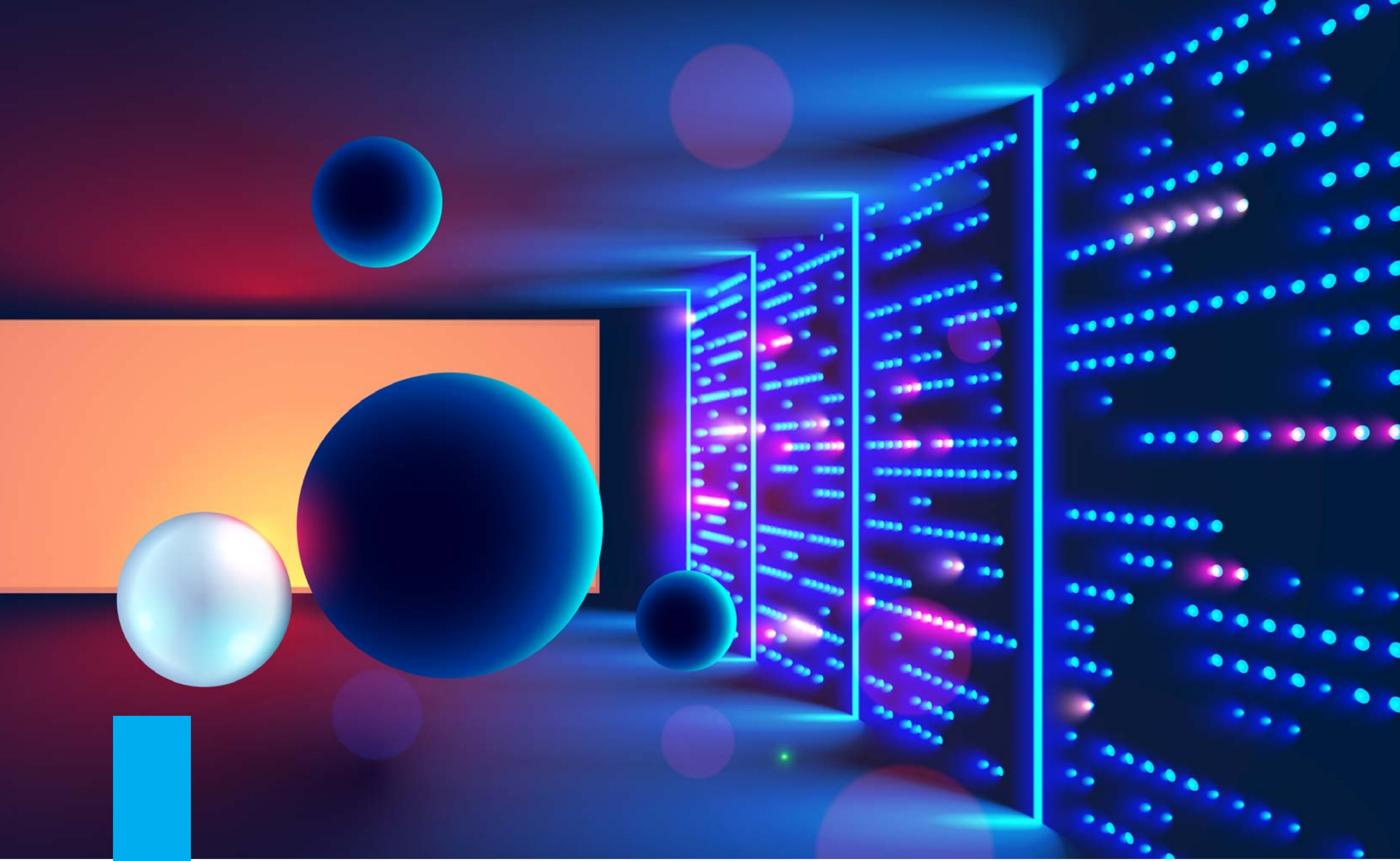


Dashboard Security Document

Ins and outs of the SecureGuard® Dashboard

speco® technologies

Table of Contents

Introduction

The SecureGuard® Dashboard is an all-in-one central management dashboard providing the ability to remotely manage an unlimited number of video surveillance systems. Swiftly diagnose recorder and camera health status before the customer notices an issue.

Password Management

Passwords are stored in a database in an encrypted format. If the database were ever compromised, original passwords remain encrypted, fortifying the defense against unauthorized access and enhancing overall data protection.

AES256 encryption algorithm is used to ensure the security of the passwords stored in our SecureGuard® Dashboard system. When the system needs to authenticate a user, the stored encrypted password is retrieved and decrypted. By using encryption and decryption techniques like AES256, the system enhances the security of the stored passwords, making it difficult for unauthorized individuals to obtain original passwords from the database.

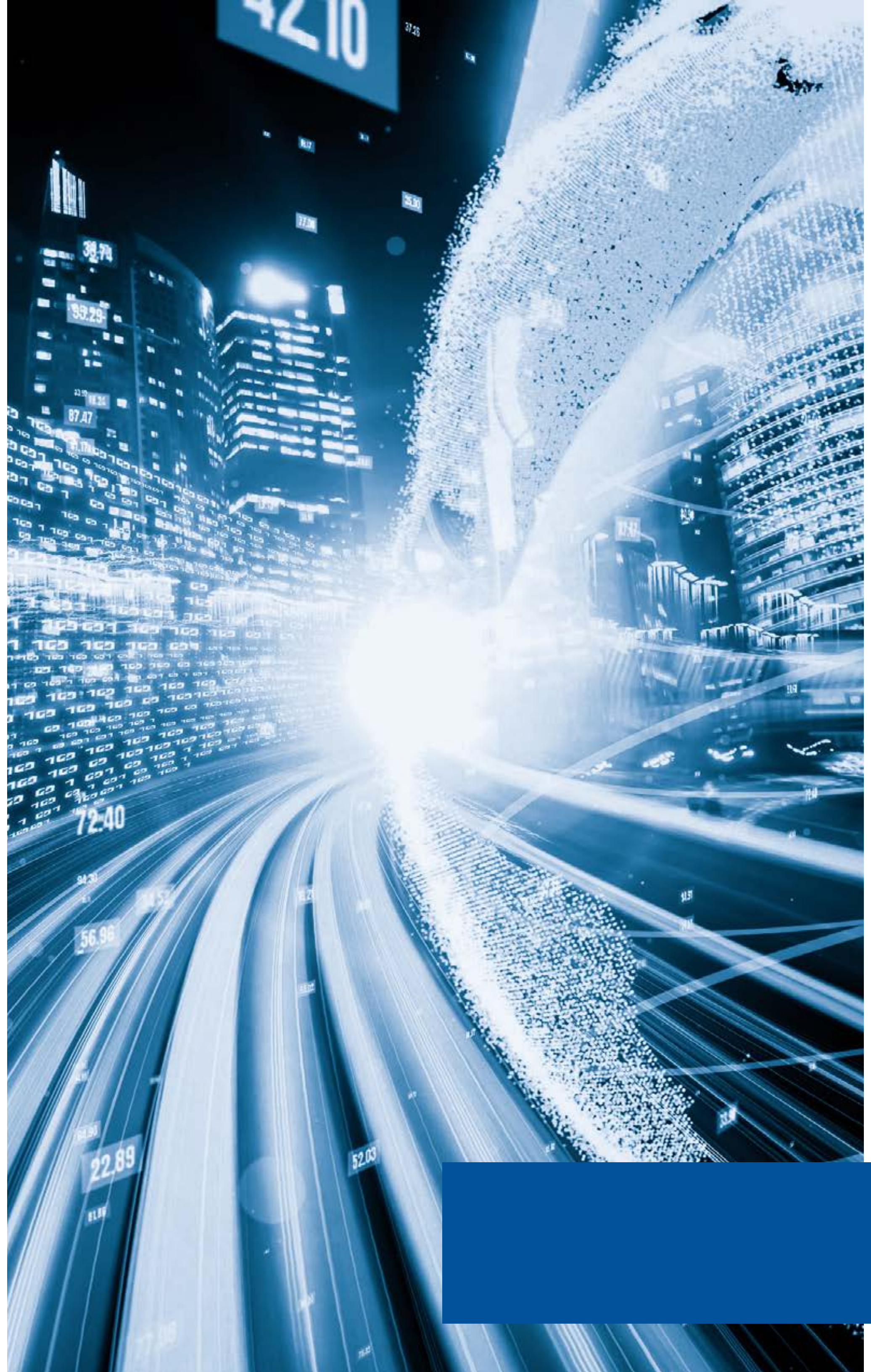
Communication

HTTPS serves as a secure standard for encrypting communication between clients and servers. The traffic between the SecureGuard® Dashboard client and the server is encrypted using HTTPS. Every incoming request from the client is passed through the secured HTTPS layer ensuring it is not an illicit entity masquerading as the source.

> **Safety, Security, and Peace**
>
> with SecureGuard® Dashboard

SQL Injection

All user inputs are validated and sanitized before incorporating them into SQL queries. This ensures that the data is properly parameterized for queries or prepared statements. When handling errors, only generic error messages are displayed to users while logging detailed errors separately, preventing attackers from gaining insights into database structure while improving incident response.



General Account Safety and Security Recommendations

Speco recommends that each user accessing the dashboard have their own account. If multiple users share a single account, there is an increased risk of a password being shared with others in the organization. Organizations should limit user access privileges to the accounts needed to perform their specific work tasks only.

Contact us at **1.800.645.5516**
or techsupport@specotech.com
to learn more about the
SecureGuard® Dashboard