



HikCentral Professional V2.6.1 Hardening Guide (Windows)

Legal Information

© About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use this Document with the guidance and assistance of professionals trained in supporting the Product.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- **HIKVISION** and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS.

YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

Contents

Chapter 1	Overview	1
1.1	Introduction	1
1.2	Supported Operating Systems	1
Chapter 2	HikCentral Professional Program Security	2
2.1	Brute Force Attack Prevention	2
2.1.1	Verification Code Mechanism	2
2.1.2	Lock IP Address: After Too Many Failed Attempts	2
2.2	Identity Authentication	3
2.3	Replay Attack Prevention	4
2.4	Private and Sensitive Data Protection	4
2.4.1	Transmission Protection	4
2.4.2	Storage Protection	6
2.4.3	Data Protection	6
2.5	Database Security	6
2.5.1	Database Password Security	6
2.5.2	Database Storage Security	7
2.5.3	Database Version Update	7
2.6	Private Data Security	7
2.6.1	The Face Data Security of Access Control Devices	7
2.6.2	The Face Data Security of Encoding Devices	8
2.6.3	The Personal Data Security	10
2.7	Stream Encryption	11
2.8	Device Anti-Hijacking	12
2.9	Access Control	12
2.10	Device Firmware Upgrade	13
2.11	Audit Log	13
2.12	Digital Signature and Anti-Tamper Protection of Product Information	14
2.13	HikCentral Professional Version Update	14
2.14	Application Market Security Mechanism	14
2.15	Other Security Measures	15
2.15.1	Maximum Password Validity Period	15
2.15.2	Auto Lock Control Client	15
2.15.3	Change Device Password Periodically	15
2.15.4	Strong Password	16

2.15.5	Encryption of Exported Video File	17
2.15.6	Encryption of Exported Person Information	18
Chapter 3	Operating System Security of Server and Client	18
3.1	Strict Password Policy.....	18
3.2	Disable Windows Remote Desktop	19
3.3	Enable Windows Firewall.....	19
3.4	Disable Sensitive Ports	19
3.5	Antivirus.....	19
3.6	Enable Windows Update	20
3.7	Application Program Security.....	20
Chapter 4	Security Deployment of Device and Network	21
4.1	Set Strong Password for Device.....	21
4.2	Stop or Disable Irrelevant Device Services or Protocols.....	21
4.3	Set Exclusive Account for HikCentral Professional	21
4.4	Use Firewall.....	21
Chapter 5	Security Deployment of Server and Network.....	23
5.1	Server Physical Security	23
5.2	Use Encrypted Channels for Communication	23
5.3	Strictly Control Using Removable Storage Media on Server.....	23
5.4	Allocate Different Accounts for Facilitate Audit.....	23
5.5	VLANs	24
5.6	Disable Unused Switch Ports	24
5.7	Prohibit Risky Protocols and Services	24
5.8	Prohibit Remote Database Access	24
5.9	Only Enable the Minimum Required Ports on a Dedicated Router Firewall	24
5.10	Network Security.....	24

Chapter 1 Overview

1.1 Introduction

HikCentral Professional is a Central Management Software (CMS) that requires a Microsoft® Windows-based server.

HikCentral Professional is able to manage and control distributed monitoring points or massive deployments of video cameras and their recordings on a series of NVRs, DVRs, and Hybrid SANs.

This document informs users of the factors affecting the system security and provides security suggestions for users in terms of system overall security. The safe and reliable running environment and the security mechanism of HikCentral Professional can provide better service to users.

The instructions of this document are listed as follows:

1. HikCentral Program Security-HikCentral Security Configurations
2. Operating System Security of Server and Client
Security Configurations Based on Microsoft® Windows Operating System
3. Device and Network Security Deployment
4. Server and Network Security Deployment

Note: This document focuses on HikCentral Professional security. For best security practices about NVRs, DVRs, and network cameras, refer to the corresponding security guides on Hikvision official website.

1.2 Supported Operating Systems

HikCentral Professional is compatible with any of the following Microsoft® Windows Operating systems:

- Microsoft® Windows 11 64-bit
- Microsoft® Windows 10 64-bit
- Microsoft® Windows Server 2019 64-bit
- Microsoft® Windows Server 2016 64-bit
- Microsoft® Windows Server 2012 R2 64-bit
- Microsoft® Windows Server 2012 64-bit
- Microsoft® Windows Server 2022

**For Windows Server 2012 R2, make sure it is installed with the rollup (KB2919355) updated in April, 2014.*

For recommended settings, visit the Microsoft® official website.

Chapter 2 HikCentral Professional Program Security

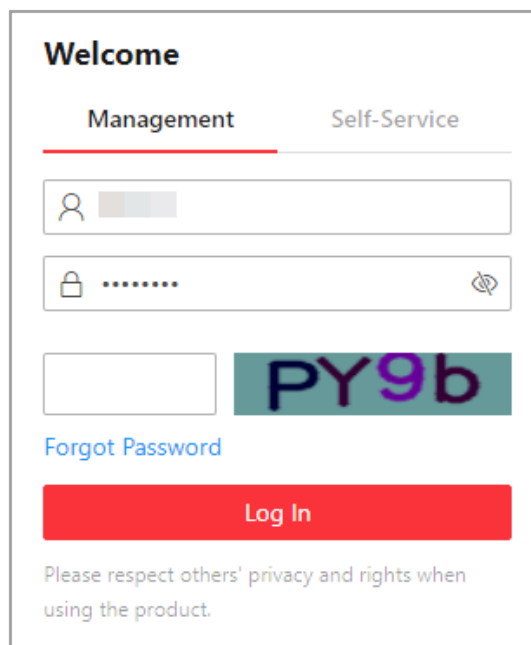
This section describes the security measures taken by HikCentral from the perspective of program security.

2.1 Brute Force Attack Prevention

HikCentral Professional service supports multiple mechanisms of preventing the force attack to protect the account from being cracked.

2.1.1 Verification Code Mechanism

The verification code is required as shown below when the password is wrong:



The screenshot shows the HikCentral Professional login page. At the top, there is a 'Welcome' header and two tabs: 'Management' (selected) and 'Self-Service'. Below the tabs, there are two input fields: a username field with a person icon and a password field with a lock icon and a toggle for visibility. Below the password field, there is a verification code field with a box and a green box displaying the code 'PY9b'. Below the verification code field, there is a 'Forgot Password' link. At the bottom, there is a red 'Log In' button. Below the button, there is a disclaimer: 'Please respect others' privacy and rights when using the product.'

2.1.2 Lock IP Address: After Too Many Failed Attempts

Enable the “**Lock IP Address**” function in the Security Settings module of the HikCentral Professional Web Client. This helps protect against invalid attempts to log in to the HikCentral Professional Server.



The screenshot shows the Security Settings module of the HikCentral Professional Web Client. It contains two settings: 'Max. Failed Login Attempts' set to '5 times' and 'Lock Duration' set to '10 min'. Both settings have a dropdown arrow on the right.

2.2 Identity Authentication

Identity authentication refers to the process that ensures only authorized clients can access the HikCentral Professional service. The service assigns a unique session ID to each client request and checks its validity before responding. If a client connection remains inactive for 15 minutes, the session information will be cleared. To continue making requests, the client needs to log in again.

The security of login credentials is crucial. Clients must provide their account and password assigned by the server to log in to the service. The server verifies the credentials and grants a valid session ID to the client. For the first login, both user accounts and employee accounts are required to change the passwords. Starting from version 2.5, the login functionality for employee accounts is disabled by default and needs to be manually enabled. HikCentral Professional supports three password strength levels - low, medium, and high.

A low strength password must meet the following requirements:

- Must be at least 8 characters long, including a combination of two or more of the following: numbers [0-9], lowercase letters [a-z], uppercase letters [A-Z], and special characters (@, #, !, /, <, ?, %).
- Must not contain "123" and "admin" (in any case).
- Must not contain more than 3 consecutive identical characters, such as "1111" and "aaaa".
- Must not contain more than 3 consecutive numbers, such as "1234" and "4321".
- Must not contain your login ID or its reverse order.
- Must not use easily guessed passwords, such as "1qaz2wsx" "1qaz@WSX" "!@#\$QWER" "p@ssword" "passw0rd", and "p@ssw0rd".

A medium strength password must meet the following requirements:

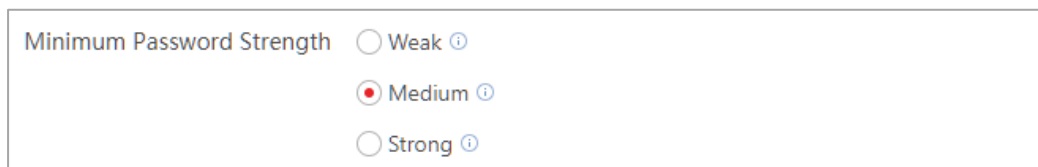
- Must be at least 8 characters long, including a combination of two or more of the following: numbers [0-9], lowercase letters [a-z], uppercase letters [A-Z], and special characters (@, #, !, /, <, ?, %).
- Must not consist of digits and letters of the same case, such as "123abc" or "456XYZ".
- Must not contain "123" and "admin" (in any case).
- Must not contain more than 3 consecutive identical characters, such as "1111" and "aaaa".
- Must not contain more than 3 consecutive numbers, such as "1234" and "4321".
- Must not contain your login ID or its reverse order.
- Must not use easily guessed passwords, such as "1qaz2wsx" "1qaz@WSX" "!@#\$QWER" "p@ssword" "passw0rd", and "p@ssw0rd".

A high strength password must meet the following requirements:

- Must be at least 8 characters long, including a combination of two or more of the following: numbers [0-9], lowercase letters [a-z], uppercase letters [A-Z], and special characters (@, #, !, /, <, ?, %).
- Must not contain "123" and "admin" (in any case).
- Must not contain more than 3 consecutive identical characters, such as "1111" and "aaaa".
- Must not contain more than 3 consecutive numbers, such as "1234" and "4321".
- Must not contain your login ID or its reverse order.
- Must not use easily guessed passwords, such as "1qaz2wsx" "1qaz@WSX" "!@#\$QWER" "p@ssword" "passw0rd", and "p@ssw0rd".

The default minimum password strength is Medium. To set the minimum password strength, follow these steps:

1. Log in to HikCentral Professional via the Web Client.
2. Enter the Security page to configure the minimum password strength, as shown in the figure below.



Minimum Password Strength

☐ Weak ⓘ

☒ Medium ⓘ

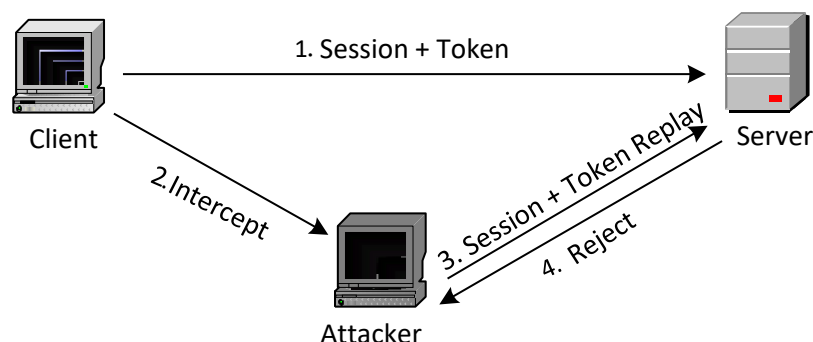
☐ Strong ⓘ

Once this option is configured, the account whose password is lower than this password strength will not be allowed to log in.

A session ID and a dynamic token are required when the client connects to the server.

2.3 Replay Attack Prevention

Replay is a common attack on the network. HikCentral Professional server uses a dynamic token with each client. The server will verify the token according to certain rules for each request. If the token in a request expires, the server will take the request as a replay attack, and then it will refuse the service to reduce the risk of platform replay attack. Refer to the following figure for replay attack model and HikCentral Professional anti-replay method.



2.4 Private and Sensitive Data Protection

The protection of privacy data mainly refers to two aspects:

1. The protection of privacy data in the transmission process between HikCentral Professional client and server, and the transmission security in the communication process of between HikCentral Professional and devices or other servers.
2. Storage protection of privacy data by HikCentral Professional server.

2.4.1 Transmission Protection

1. Transmission security of HikCentral Professional client and server

The HikCentral Professional client and server communicate with each other over HTTPS. HTTPS

uses TLS/SSL encryption and identity authentication over HTTP to secure communications. The HikCentral Professional client and server can also communicate with each other over HTTP. When both sides connect, they will negotiate a dynamic 128-bit AES key that is unique for each session. This key encrypts privacy-sensitive data such as personal, license plate, and password information to prevent data leakage.

Before version 2.5, the HikCentral Professional client and server communicates with each other over HTTP by default. Starting from version 2.5, the communication protocol will not automatically switch to HTTPS.

To switch to HTTPS for enhanced security needs, follow these steps:

- 1) Log in to HikCentral Professional via the Web Client
- 2) Enter the System Configuration page and select the HTTPS as the transfer protocol.

In HikCentral Professional 2.0, the encryption protocol version used in the HTTPS is TLSv1.2 or later, which has higher security.

Note: To reduce the risk, only the admin user can take these steps locally on the server. Users are allowed to use the platform certificates or import new certificates when using HTTPS.

The screenshot shows the 'Transport Protocol' configuration interface. It includes radio buttons for selecting the transfer protocol (HTTP or HTTPS) and the certificate type (Platform Provided Certificate or New Certificate). There is a warning message about browser TLS support. Below, there are buttons to add or delete upper-level certificates, and a table to manage them. A red 'Save' button is at the bottom.

2. Transmission Security Between HikCentral Professional and Devices or Other Servers

(1) To reduce the risk of data leakage in the interaction process, the communication between HikCentral Professional and the devices is based on Hikvision private protocol. Sensitive information transmission is encrypted based on the dynamic key negotiated by HikCentral Professional and the devices. The key length is 128 bits, and the encryption algorithm is AES.

(2) The transmission between HikCentral Professional and recording server supports HTTPS to ensure that the communication channel is encrypted.

3. Stream Encryption Transmission

The stream transmitted between HikCentral Professional and the devices supports being encrypted, and the encryption key supports being defined by users. When configuration completed, the stream from device will be encrypted to transmit to HikCentral Professional. HikCentral Professional needs to use the key to decrypt the stream before checking the stream information.

2.4.2 Storage Protection

According to the property and performance requirements of private and sensitive information storage, HikCentral Professional supports data storage in database, disk, and external storage servers.

The contents stored in different storage methods and the safety measures adopted are as follows:

1. Database Storage

Refer to the chapter of Database Security.

2. Disk Storage

Disk storage mainly refers to the case where HikCentral Professional is configured as a picture storage server. HikCentral Professional supports configuring picture storage server by channel. When the HikCentral Professional service is configured as the picture storage server, the event pictures reported by the channel will be stored on the HikCentral Professional server disk. This rule ensures the efficiency of pictures reading and the security of storage, that is, pictures cannot be browsed directly.

3. External Storage Server

External storage server mainly refers to pStor, CVR, and cloud storage used for picture and video storage. Pictures and videos are stored in accordance with certain storage security rules.

2.4.3 Data Protection

Exporting sensitive information such as fingerprint, face, and ID card requires authentication by the password of the current account.

2.5 Database Security

HikCentral uses PostgreSQL to record private and sensitive information to ensure data security through three aspects.

2.5.1 Database Password Security

1. By default, the HikCentral Professional database service only reserves one user for the HikCentral Professional connection database service to reduce the risk of account cracking.
2. The password of HikCentral Professional database can be updated. If you change the admin password, the database password will be automatically updated in the background. The database password is encrypted by AES128 algorithm and stored in the configuration file. The secret key component is generated randomly and unpredictable.
3. HikCentral Professional only allows local access to the database on the server by default, and cannot connect to the database service outside. Ensure that the data is protected from network access.

2.5.2 Database Storage Security

1. Some private and sensitive information, such as device password and private data (phone, email, face, and fingerprint), is required by HikCentral Professional client, so AES128 algorithm is used to encrypt and store in the database, and the secret key component is generated randomly and unpredictable.
2. Some private and sensitive information, such as HikCentral Professional account password, is stored after it is added with salt value and processed by the SHA256 algorithm. The correctness of these information is verified at the HikCentral Professional server, which can reduce the risk of leakage caused by transmission.
3. HikCentral Professional supports regular backup of configuration database to reduce the risk of data loss.
4. HikCentral Professional database only opens necessary ports by default to reduce the risk of being attacked.

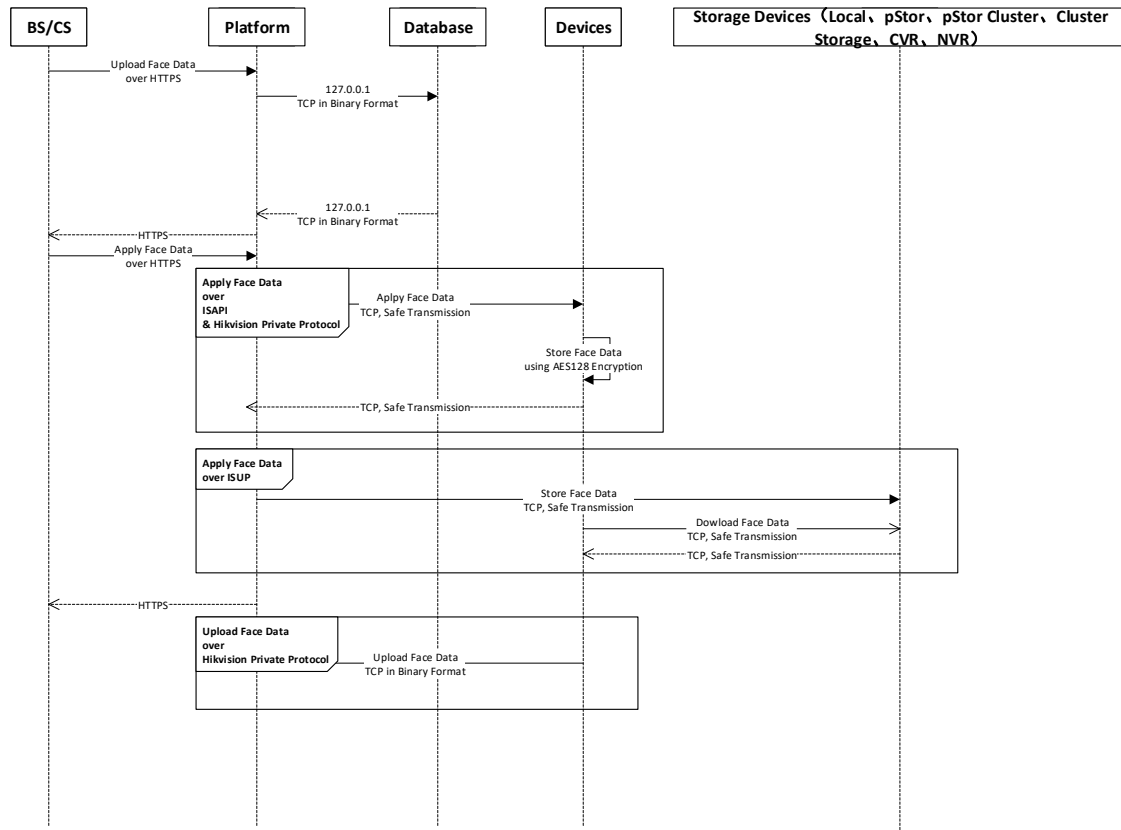
2.5.3 Database Version Update

1. HikCentral Professional will use the dominant security scanning tools before release, including PostgreSQL database. For serious flaws, HikCentral Professional will update the version in time according to the official breach repair situation of PostgreSQL. Please follow the HikCentral Professional version update instructions.
2. When HikCentral Professional is upgraded, PostgreSQL will be upgraded to a version with higher security (depending on the timeliness of breach official release from PostgreSQL).

2.6 Private Data Security

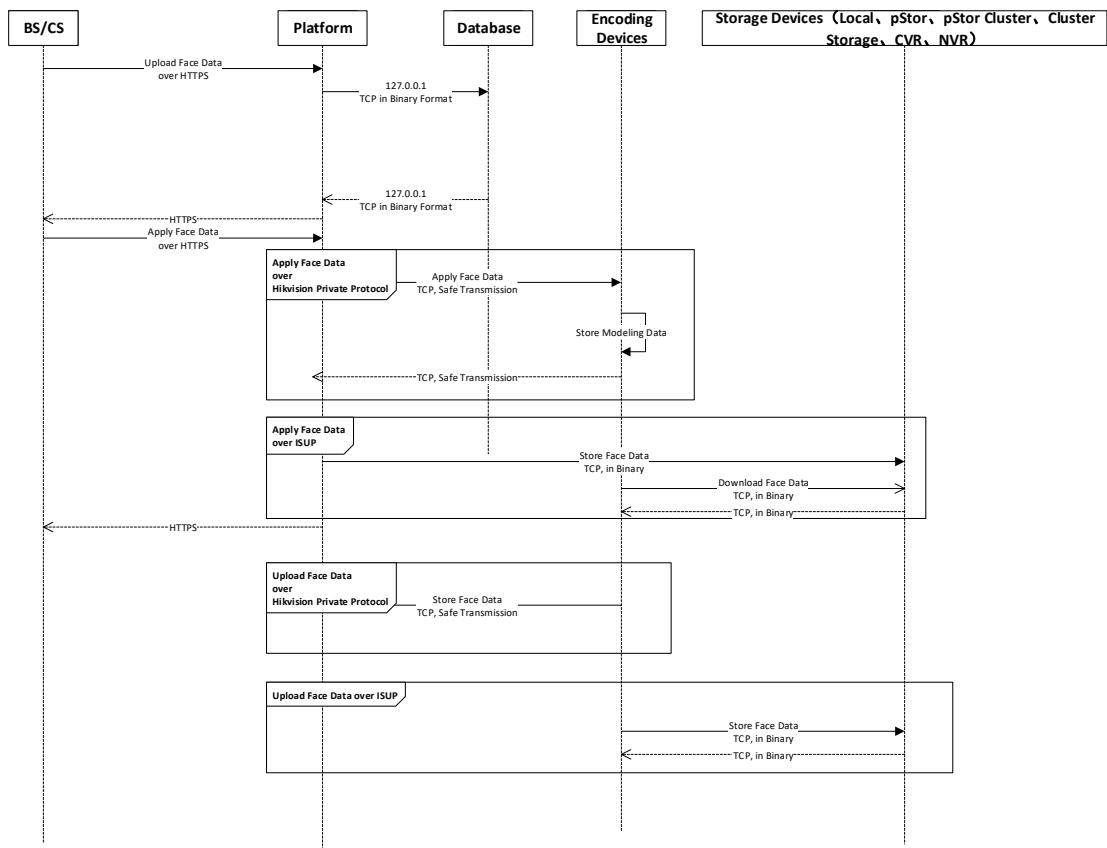
2.6.1 The Face Data Security of Access Control Devices

You can apply the face data collected and stored in the database to specific access control devices. The devices use these data to recognize and authenticate individuals. During the authentication process, the captured facial data is stored either locally on the device or on a storage server. The following diagram illustrates the sequence of data transmission and storage.

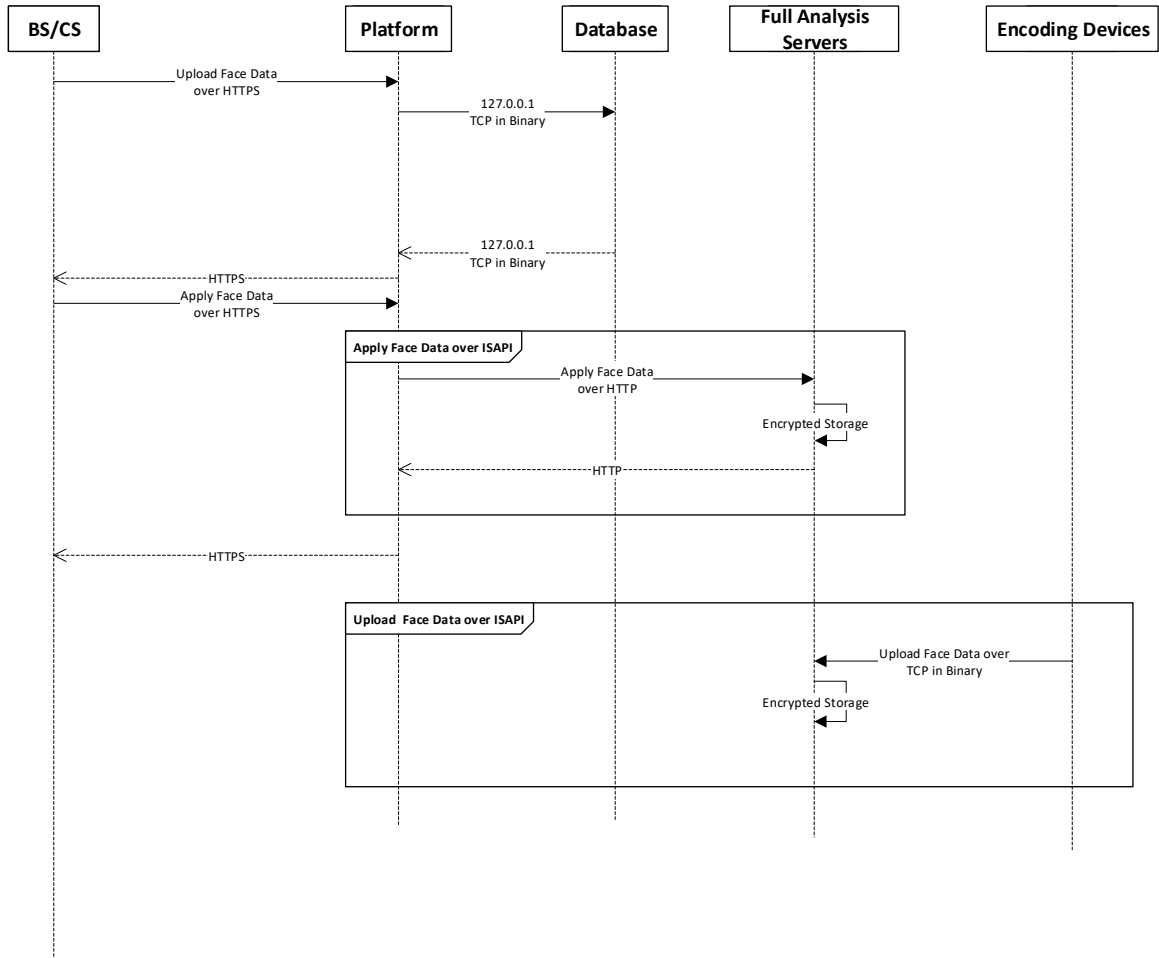


2.6.2 The Face Data Security of Encoding Devices

The encoding devices with facial recognition capabilities will capture face pictures and create a model of face data from the HikCentral Professional platform. These devices will recognize and compare captured pictures with the modeling data. The following diagram illustrates the sequence of data transmission and storage.

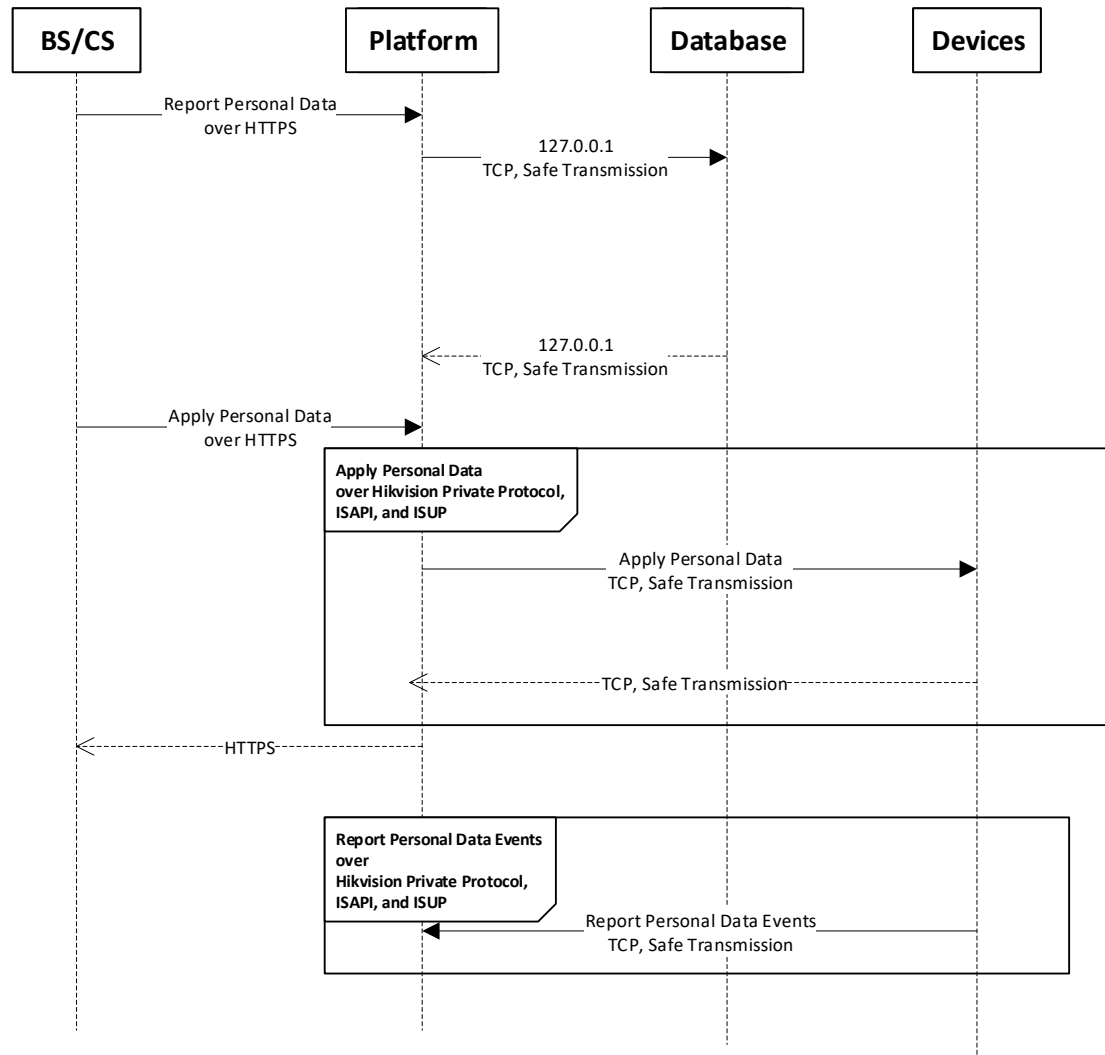


The encoding devices without facial recognition capabilities capture face pictures and upload them to the Full Analysis server. The server will recognize, compare, and store face pictures based on the face data from the HikCentral Professional platform. The following diagram illustrates the sequence of data transmission and storage.



2.6.3 The Personal Data Security

Personal data include the information of cards, license plates, fingerprints, and irises. The following diagram illustrates the sequence of personal data transmission.



2.7 Stream Encryption

When adding encoding device, Stream Encryption can be selected to prevent video stream being stolen and play on condition that this function has been enabled on device webpage.

Add Encoding Device

Basic Information

Access Protocol

Hikvision Private Protocol

Adding Mode

☒ IP Address/Domain
 ☐ Hik-Connect DDNS ⓘ
 ☐ IP Segment
 ☐ Port Segment
 ☐ Batch Import

*Device Address

ⓘ Add via TLS Protocol
☐

*Device Port

8000

ⓘ Mapped Port

☐

ⓘ Verify Stream Encryption Key

☒

*Stream Encryption Key on Device

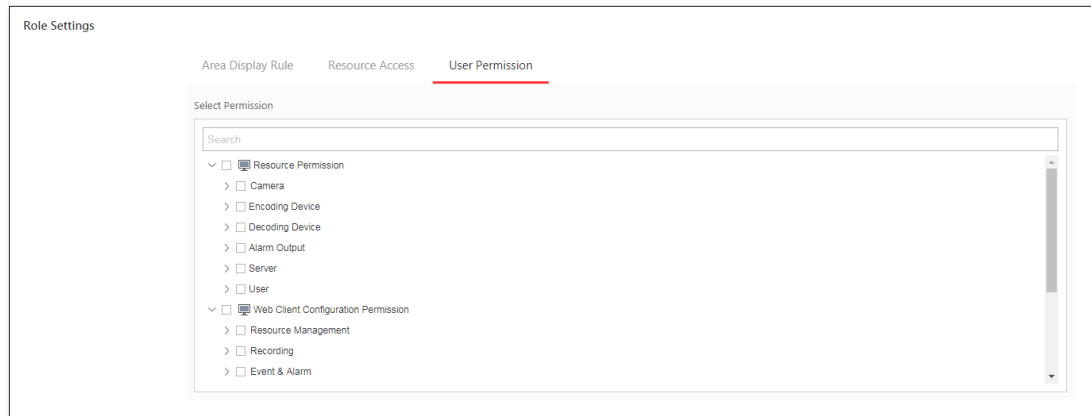
2.8 Device Anti-Hijacking

The devices connected to HikCentral Professional are deployed in different monitoring points. Although managed by the center, there is still a risk that the devices will be hijacked, that is, the devices will be replaced without users' perception. HikCentral Professional will record the feature data of the accessed devices. Once the feature data changes, it will immediately stop the relevant functions of the device in HikCentral Professional.

2.9 Access Control

HikCentral Professional supports permission allocation of different levels for different users. The user permission of each request from the client or server will be verified. Users without permission cannot operate or access resources. HikCentral Professional recommends that users be assigned minimum permissions.

When the administrator creates a new role, he/she must **only select** the required permissions for the role.



2.10 Device Firmware Upgrade

HikCentral Professional manages the devices, such as network cameras, NVRs, and so on. Once the vulnerabilities appear in device firmware, upgrading firmware one by one will cause large workload, low efficiency and security. HikCentral Professional provides two methods of firmware upgrade, which can upgrade the firmware of device in a batch and strengthen the system security.

(1) HikCentral Professional Firmware Upgrade

After users obtain the new firmware package released by the Hikvision device, they can directly upload it to HikCentral Professional, and the HikCentral Professional service can independently upgrade the firmware of the device.

(2) Firmware Upgrade via Hik-Connect

After users purchase the Hik-Connect service, once Hikvision releases new device firmware, it will be automatically updated to Hik-Connect. When HikCentral Professional detects that there is a new firmware package in Hik-Connect, HikCentral Professional will prompt and guide the users to upgrade.

2.11 Audit Log

HikCentral Professional has corresponding logs for all kinds of resource access and operation, especially for the access of private and sensitive information, which can be followed up afterwards.

Level	Time	Source	Event	Resource	Area	Description	Address
Information	2024/05/28 15:55:04	admin	User Login	--	--	--	(Web Client)
Information	2024/05/28 15:38:46	admin	User Logout	--	--	--	(Web Client)
Information	2024/05/28 15:09:42	admin	User Logout	--	--	--	(Web Client)
Information	2024/05/28 15:06:01	admin	User Login	--	--	--	(Web Client)
Information	2024/05/28 14:53:54	admin	Search Parking Rec...	--	--	--	(Web Client)
Information	2024/05/28 14:53:54	admin	Search Parking Rec...	--	--	--	(Web Client)
Information	2024/05/28 14:53:48	admin	Search Parking Rec...	--	--	--	(Web Client)
Information	2024/05/28 14:53:48	admin	Search Parking Rec...	--	--	--	(Web Client)
Information	2024/05/28 14:28:23	admin	User Login	--	--	--	(Web Client)

2.12 Digital Signature and Anti-Tamper Protection of Product Information

The plug-in of HikCentral Professional 2.0 supports digital signature verification. When the program starts, the digital signature of plug-in will be verified. Only plug-ins whose signature are verified are allowed to be loaded. Any tampered or fake plug-ins will be recognized by HikCentral Professional and refused to load.

HikCentral Professional 2.0 supports anti-tamper protection for product description files and other configuration files. Any edit to the configuration can be recognized by HikCentral Professional. Once tampering is detected, the HikCentral Professional will not start automatically until the edit is restored.

2.13 HikCentral Professional Version Update

The version of HikCentral Professional will be updated continuously, and the security problems or breach exposed in the iteration process will be repaired to ensure the continuous improvement of the overall product strength. It is recommended that users of HikCentral Professional pay attention to the breach information disclosed by dominant security companies and update the version of HikCentral Professional.

2.14 Application Market Security Mechanism

HikCentral Professional Application Market is deployed on the server of Amazon Web Services (AWS) Singapore. If Application Market is enabled, the platform will test the connection of the AWS server every 3 minutes. Application Market is disabled by default, you can enable/disable it after confirming your needs. After it is enabled, HikCentral Professional synchronizes the latest versions of applications with Application Market.

Security authentication is required for communications between HikCentral Professional and

Application Market. HikCentral Professional synchronizes and downloads applications via HTTPS, and it performs integrity verification for downloaded applications.

2.15 Other Security Measures

2.15.1 Maximum Password Validity Period

Switch on **Enable Maximum Password Validity Period** and Set the **Password Will Expire In** as you want on the Security page of the Web Client.

Enable Maximum Password Validity Period ☒

Password Will Expire In 3 months ^

1 month
3 months
6 months
Custom

*Days to Remind Before Password Expiration

*Web Login Expires If No Action Within

2.15.2 Auto Lock Control Client

Switch on **Auto Lock Control Client** and Set the **Lock In** on the Security page of the HikCentral Professional Web Client. The Control Client will be locked after a time period of inactivity. The user should enter the user name and password to unlock the Control Client.

Auto Lock Control Client ☒

No Operation In 10 min v

2.15.3 Change Device Password Periodically

Change device password periodically to make the device more secure.

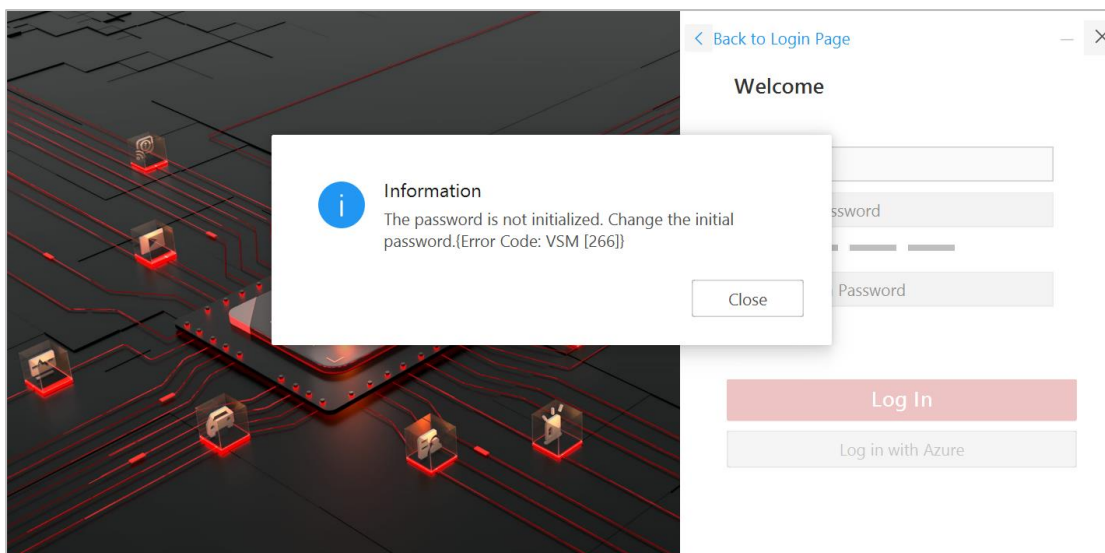
The screenshot shows the HikCentral Professional user management interface. A modal window is open for editing a user. The modal contains the following fields and elements:

- User Name:** admin
- Old Password:** A password field with a lock icon and a toggle for visibility.
- New Password:** A password field with a lock icon, a toggle for visibility, and an information icon.
- Confirm Password:** A password field with a lock icon and a toggle for visibility.
- Password Strength:** A visual indicator showing a red bar and the word "Risky".
- Save:** A red button at the bottom right of the modal.


The background interface shows a list of users with checkboxes and status icons. At the bottom, there is a "Total: 10" and a dropdown menu set to "100".

2.15.4 Strong Password

The new user needs to change the password when they log in for the first time.
Set a **STRONG** password (case-sensitive letters, special characters combined with digits).




When the administrator adds a new user, he/she can set a **STRONG** password and an **Expiry Date** for the user. The administrator can also set the **Restrict Concurrent Logins** to limit the maximum IP addresses logged in to the platform using the user account.


 Add User


Basic Information


* User Name

test

 * Password







Strong 

Expiry Date

2099/12/31 23:59:59



 Email

* User Status

☒ Active


☐ Inactive

Description

Login Protection

Restrict Concurrent Logins

☒

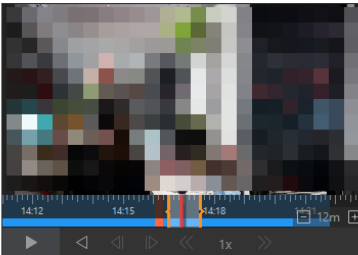
 * Maximum Login Times

100

2.15.5 Encryption of Exported Video File

When exporting video file, a password can be set for file in MP4 or EXE format. Then the password is needed when playing the video file on VSPlayer.

Export All



☒ Synchronize Downloading Time

<input checked="" type="checkbox"/>	Camera Name	Download Time
<input checked="" type="checkbox"/>		19/07/09 14:16:30-19/07/0...

File Format

☒ MP4

☐ AVI

☐ EXE

2.15.6 Encryption of Exported Person Information

When exporting information about persons, the user password is required for identity verification. See 2.4.3.

Chapter 3 Operating System Security of Server and Client

HikCentral Professional service and clients are deployed in Microsoft® Windows which supports many security policies. This section describes the security settings of the HikCentral Professional server and clients based on the operating system.

3.1 Strict Password Policy

1. Always adhere to the end-user's IT department policy for password management
2. Assign a complex password.
 - a) If using a WorkStation purchased from Hikvision, a new password should be assigned to the administrator for the first login.

For the best practices of password management on Windows, visit the Microsoft® official

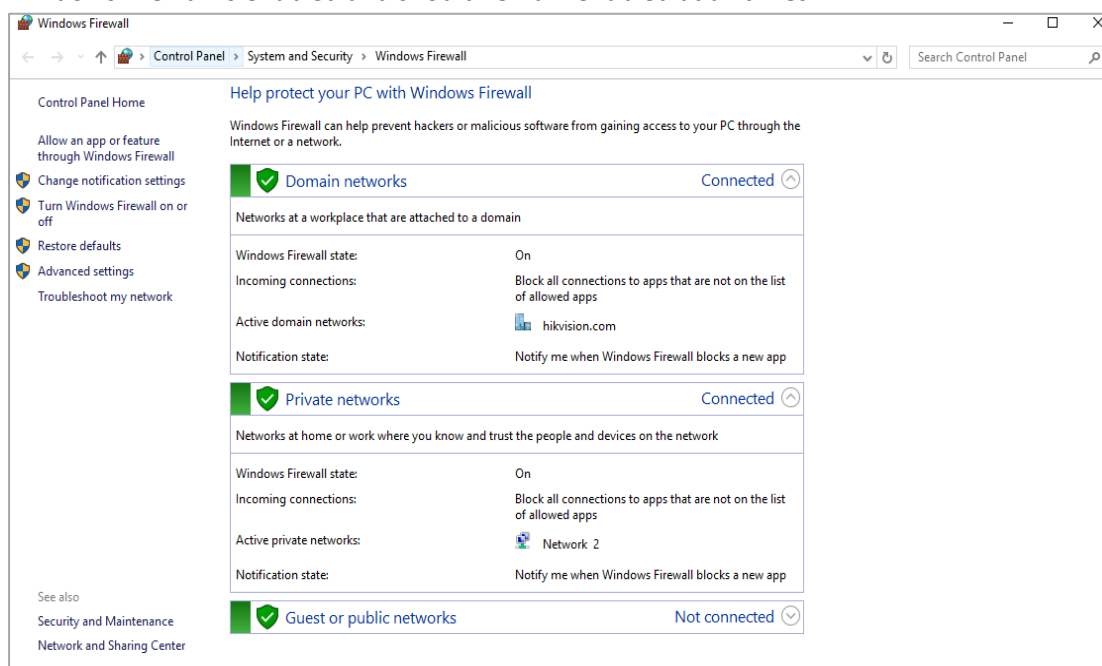
website.

3.2 Disable Windows Remote Desktop

Disable Windows remote desktop to secure the operating system.

3.3 Enable Windows Firewall

A software firewall is the second layer of protection behind the network layer firewall. It will help you protect the computer from outside attempts of control or access. By default, Windows firewall is enabled and should remain enabled at all times.



3.4 Disable Sensitive Ports

TCP ports (135/139/445) and UDP ports (137/138) in the Microsoft® Windows Security Policy are suggested to be disabled when RPC, NetBIOS, and SMB are NOT used.

3.5 Antivirus

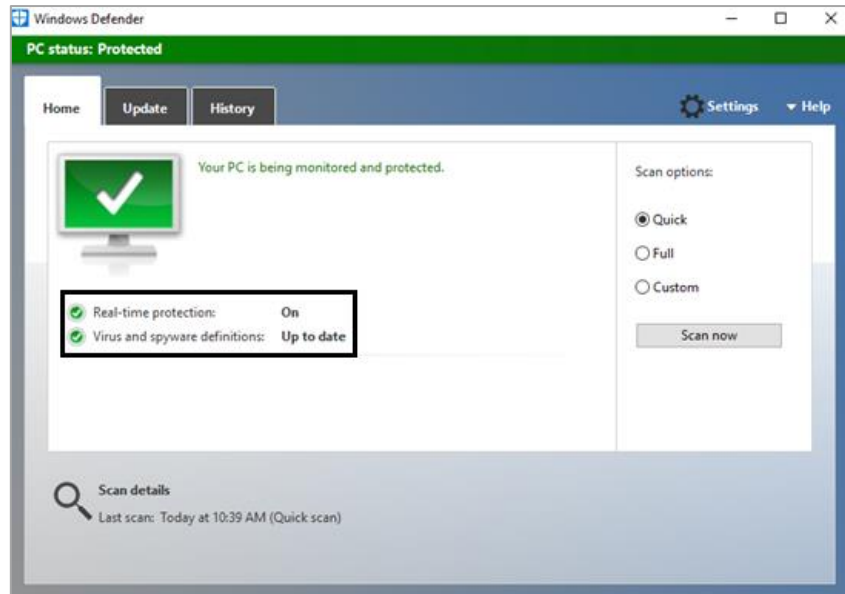
Install full-featured Anti-Virus software to keep HikCentral Professional Server secure.

Antivirus must be active and automatically updated.

For example, the settings of Windows antivirus Windows Defender are as below.

- Real-time protection must be “On”
- Virus and spyware definitions must be “Up to date”

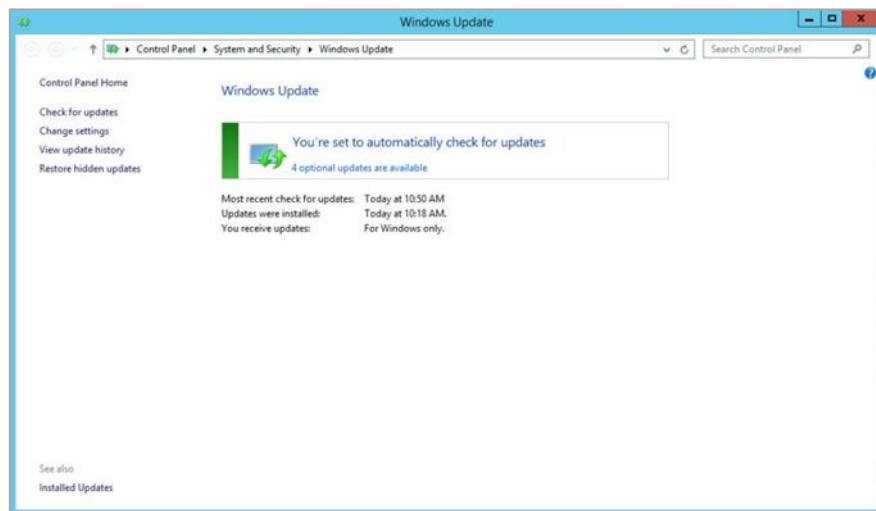
Example from Microsoft® Windows 10:



3.6 Enable Windows Update

It is important that Windows update is set to **auto install**. Normally, this is the default settings.

Ex: from Microsoft® Windows Server:



3.7 Application Program Security

HikCentral Professional Mobile Client should run on a reliable device, which means that the other applications on the device are secure.

Chapter 4 Security Deployment of Device and Network

4.1 Set Strong Password for Device

Camera products that collect data are crucial in a security system. Setting a strong password for these products can reduce the risk of data leakage.

A strong device password must meet the following requirements:

- Must be at least 8 characters long, including a combination of two or more of the following: numbers [0-9], lowercase letters [a-z], uppercase letters [A-Z], and special characters (@, #, !, /, <, ?, %).
- Must not contain “123” and “admin” (in any case).
- Must not contain more than 3 consecutive identical characters, such as “1111” and “aaaa”.
- Must not contain more than 3 consecutive numbers, such as “1234” and “4321”.
- Must not contain your login ID or its reverse order.
- Must not use easily guessed passwords, such as “1qaz2wsx” “1qaz@WSX” “!@#\$QWER” “p@ssword” “passw0rd”, and “p@ssw0rd”.

4.2 Stop or Disable Irrelevant Device Services or Protocols

By default, the device may start or enable many services or protocols to meet the needs of different cases. Users need to stop or disable useless services or protocols according to the actual needs. Since if these default started or enabled services or protocols have flaws, they will be vulnerable to network or local attacks, resulting in serious consequences such as device down and data leakage.

For those cases with high security requirements, security services or protocols on the device can be started or enabled, such as HTTPS.

4.3 Set Exclusive Account for HikCentral Professional

It is recommended to create an exclusive account on the device if this device is to be added to HikCentral Professional for management. For example, you can create an account named HikCentral, and then add the device to HikCentral Professional with this user name. Similarly, other users can access the device by the name of HikCentral Professional. This method is mainly for easy review afterwards, that is, you can quickly find out the users who have accessed the device, resources or functions that have been accessed, whether other external users have accessed the device, and so on, via the device logs. All above information is used to analyze whether the device has been hijacked.

4.4 Use Firewall

Try not to expose the devices directly to the Wide Area Network (WAN) because the devices

are vulnerable to be attacked in this case. Use a firewall between the device network and the WAN if necessary. The firewall can control the permissions of WAN to access internal resources and reduce the risk of attack on devices.

Chapter 5 Security Deployment of Server and Network

This section mainly introduces how to improve the server and network security to deploy the HikCentral Professional service.

5.1 Server Physical Security

The deployment server of HikCentral Professional is one of the core hardware in the whole system. It is recommended that the server be physically deployed in server room, and the access records of the server should be maintained. Monitoring the server room is also a preventive measure.

5.2 Use Encrypted Channels for Communication

If the HikCentral Professional server is on a Local Area Network (LAN) behind a Network Address Translation (NAT), it is recommended to use Virtual Private Network (VPN) tunneling (configure on the Router or Firewall Settings page) to remotely access the clients on computer via Wide Area Network (WAN).

A VPN is a private distributed network that often extends across public networks or the Internet.

Various protocols are available to create a VPN, typically a tunnel that carries the protected traffic. VPNs can be deployed with encrypted communications, or merely rely on secure communication within the VPN itself.

VPN is used to connect remote sites via WAN connections, protect privacy, and increase security within a LAN. A VPN not only adds an additional layer of protection for a video security system, but it also provides the additional benefit of segmenting the production networks into business traffic and video traffic.

Even if the HikCentral service is deployed on a security network, it is recommended to switch to HTTPS to configure the service.

5.3 Strictly Control Using Removable Storage Media on Server

Mobile storage media, such as USB flash drive and SD card may carry viruses. If they are used on the server without control, malicious programs may enter the local server or even the network where the server is located, thus polluting the running environment of HikCentral Professional. Only authorized users are allowed to use mobile storage media when necessary, such as copying HikCentral Professional's video as evidence.

5.4 Allocate Different Accounts for Facilitate Audit

HikCentral Professional supports creating roles with different permissions. Administrators can allocate different accounts to those who need to log in to HikCentral Professional so as to know

clearly in the HikCentral Professional audit log module which account uses what type of client and which location (IP address) operates what resources in the system afterward. Audit logs help the administrator locate the one who caused the system exception.

HikCentral also supports Active Domain (AD) users. AD server has high security and can verify the validity of users.

5.5 VLANs

If the HikCentral Professional server is on a Local Area Network (LAN) with Control Clients, it is recommended to use a Virtual LAN (VLAN).

A VLAN is created by subdividing a LAN into multiple segments. The network segmentation is done through a network switch or router configuration. A VLAN can access resource without rewiring device network connection.

5.6 Disable Unused Switch Ports

Disabling unused network ports ensures that unauthorized devices do not get access to the network. This mitigates the risk of someone trying to access a security subnet by plugging a device into a switch or unused network socket. Disabling specific ports is a common option in managed switches, both low cost and enterprise.

5.7 Prohibit Risky Protocols and Services

Regularly use security tool to scan HikCentral Professional deployment server. Disable or stop the protocols or services that the tool considers risky on the server. Irrelevant programs or services running on the server should be prohibited without special need.

5.8 Prohibit Remote Database Access

HikCentral Professional uses PostgreSQL database. By default, remote access is disabled after the installation. It is recommended that remote access should also be disabled to reduce the risk of database password leakage.

5.9 Only Enable the Minimum Required Ports on a Dedicated Router Firewall

If it is not possible to use Virtual Private Network (VPN) among various sites, you need to make sure that the router has a firewall and only the required ports are enabled to connect to the HikCentral Professional server.

5.10 Network Security

Choose proper security technologies to enhance network security, such as the Intrusion Detection System (IDS), ACL (Access Control List), 802.1x, RADIUS Authentication, and Security Auditing.



See Far, Go Further