HikCentral Access Control V2.0 Hardening Guide (Windows)

Legal Information

About this Document

Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Document is subject to change, without notice, due to updates or other reasons.

Please use this Document with the guidance and assistance of professionals trained in supporting the Product.

LEGAL DISCLAIMER

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE DOCUMENT IS PROVIDED "AS IS" AND “WITH ALL FAULTS AND ERRORS”. HIKVISION MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. IN NO EVENT WILL HIKVISION BE LIABLE 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), OR OTHERWISE, IN CONNECTION WITH THE USE OF THE DOCUMENT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

Contents

Chapter 1 Overview

1.1 Introduction

HikCentral Access Control is a software that requires a Microsoft® Windows-based server. HikCentral Access Control is able to manage and control distributed access control devices and video intercom devices.

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 Access Control can provide better service to users.

The instructions of this document are listed as follows:

1. HikCentral Access Control Program Security-HikCentral Access Control 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 Access Control security. For best security practices about access control devices and video intercom devices, refer to the corresponding security guides on Hikvision official website.

1.2 Supported Operating Systems

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

- Microsoft® Windows 11 64-bit
- Microsoft® Windows 10 64-bit
- Microsoft® Windows 8.1 64-bit
- Microsoft® Windows 7 SP1 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 2008 R2 SP1 64-bit

For Windows 8.1 and 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.

Browser Version:

- Google Chrome® 90 and above
- Firefox® 90 and above
- Safari® 11 and above
- Microsoft® Edge 89 and above
- Internet Explorer® 11 and above

Database: PostgreSQL V11.8
OS for Mobile Client:

- iOS 10.0 and later
- Android phone OS version 6.0 or later

Chapter 2 HikCentral Access Control Program Security

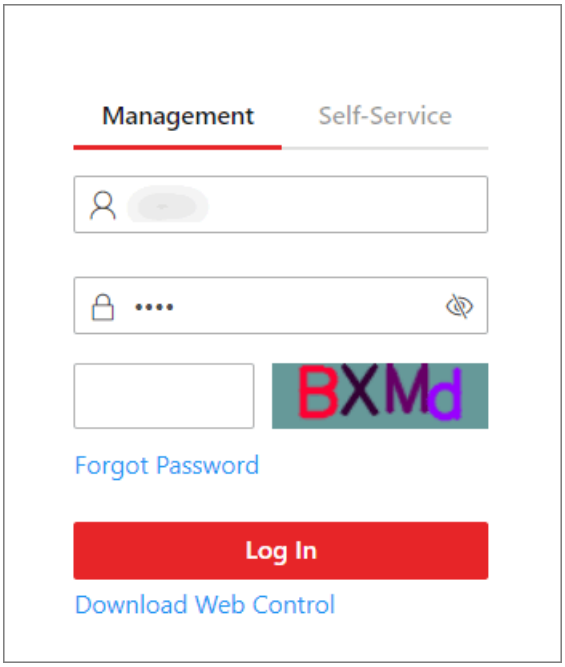
This section describes the security measures taken by HikCentral Access Control from the perspective of program security.

2.1 Brute Force Attack Prevention

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

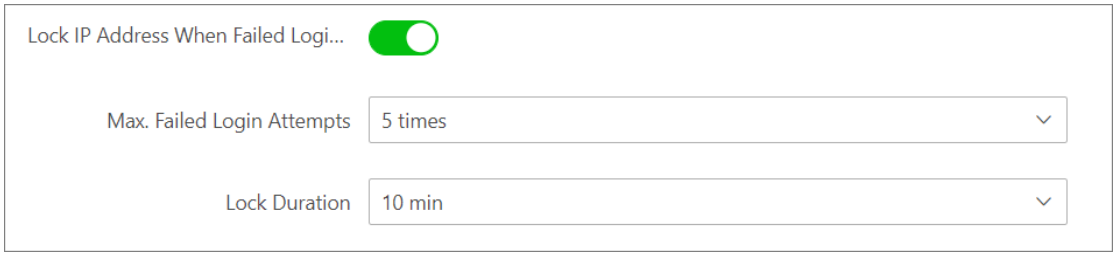
2.1.1 Verification Code Mechanism

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



2.1.2 Lock IP Address: After Too Many Attempts

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



2.2 Identity Authentication

Identity verification means that the HikCentral Access Control service will allocate a session ID to all request clients and verify the session validity of each request. For the inactive client within 15 minutes, the server will clear the session information. If the client wants to continue the request, it needs to log in to the HikCentral Access Control service again.

The account password information allocated by the platform is required when the client wants to log in to the HikCentral Access Control service. After the server verified the password, it will allocate an effective session ID to the client. Therefore, the security of account password is important. HikCentral Access Control suggests that the account password should be composed of digits, letters, and special characters, and the length should be more than 8 characters.

HikCentral Access Control also supports setting the password strength of the lowest security level allowed for login. The operations are as follows:

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

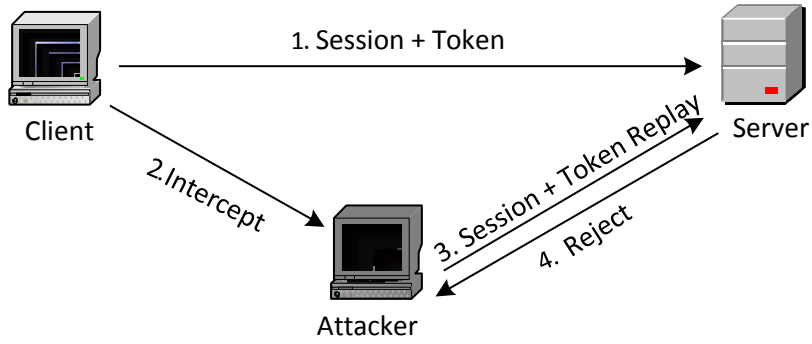
Once this option is configured, the account whose password is lower than this password strength will not be allowed to log in.

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

2.4.1 Transmission Protection

1. Transmission security of HikCentral Access Control client and server

In the HTTP mode, after the HikCentral Access Control client connects to the server, both sides will negotiate a dynamic AES key with a length of 128 bits. The private and sensitive information transferred on the link is encrypted by the negotiated key. As the key is dynamically negotiated between the server and the client, it can ensure that the AES keys negotiated on each link are mutually independent.

Currently, HikCentral Access Control will encrypt and transfer sensitive information such as personnel information, license plate information, and password to reduce the risk of data leakage.

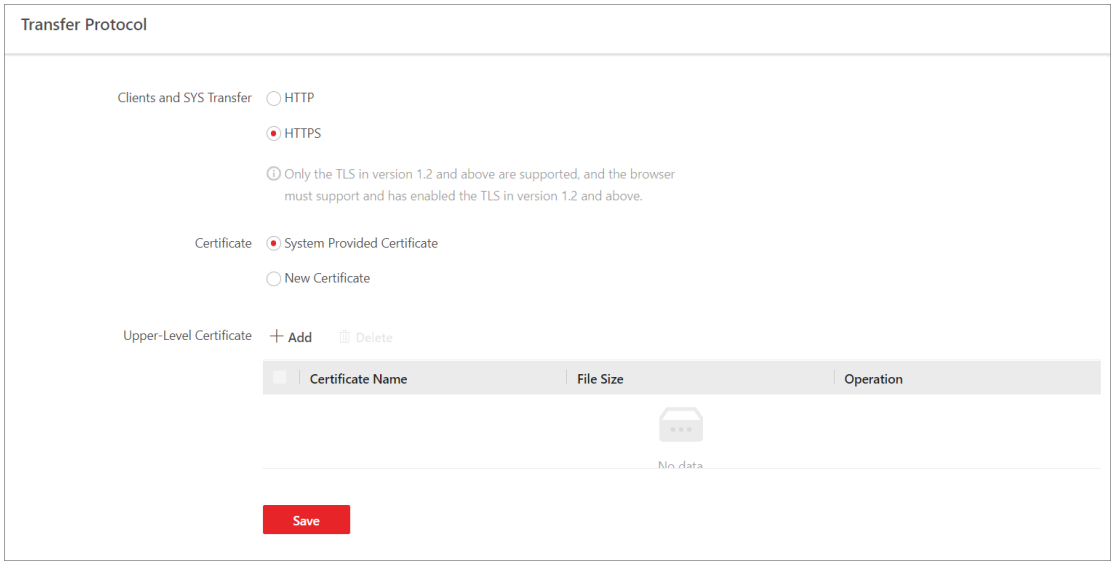
In the cases with high security requirements, it is recommended to switch to HTTPS, which is also supported by HikCentral Access Control. The operation steps are as follows:

1) Log in to HikCentral Access Control via the Web Client

2) Enter the System Configuration page and select the HTTPS as the transfer protocol.

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

Note: To reduce the risk, the above operations are only allowed to be performed locally on the server by the admin user, and users are allowed to use the platform certificates or import new certificates when switching to HTTPS.



2. Transmission Security Between HikCentral Access Control and Devices or Other Servers

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

(2) The transmission between HikCentral Access Control and facial recognition server supports HTTPS to ensure that the communication channel is encrypted.

2.4.2 HikCentral Access Control Storage Protection

According to the property and performance requirements of private and sensitive information storage, HikCentral Access Control 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 *Chapter 2.6* for database security description.

2. Disk Storage

Disk storage mainly refers to the case where HikCentral Access Control is configured as a picture storage server. HikCentral Access Control supports configuring picture storage server by channel. When the HikCentral Access Control service is configured as the picture storage server, the event pictures reported by the channel will be stored on the HikCentral Access Control 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 used for picture storage. Pictures are stored in accordance with certain storage security rules.

2.5 Database Security

HikCentral Access Control 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 Access Control database service only reserves one user for the HikCentral Access Control connection database service to reduce the risk of account cracking.
2. The password of HikCentral Access Control database can be updated. If you change the admin password of HikCentral Access Control administrator, 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 Access Control 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 p protected from network access.

2.5.2 Database Storage Security

1. Some private and sensitive information, such as device password, is required by HikCentral Access Control 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 Access Control 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 Access Control server, which can reduce the risk of leakage caused by transmission.
3. HikCentral Access Control supports regular backup of configuration database to reduce the risk of data loss.
4. HikCentral Access Control database only opens necessary ports by default to reduce the risk of being attacked.

2.5.3 Database Version Update

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

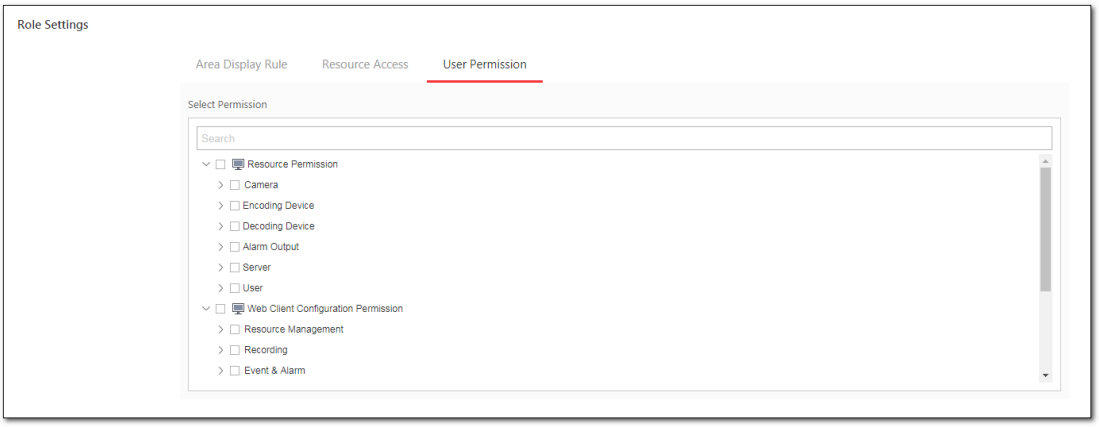
2.6 Device Anti-Hijacking

Although safty measures have been taken, there is still a risk that the devices will be hijacked, that is, the devices will be replaced without users' perception. HikCentral Access Control 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 Access Control.

2.7 Access Control

HikCentral Access Control 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 Access Control 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.



2.8 Device Firmware Upgrade

HikCentral Access Control manages the devices, such as access control devices, video intercom devices, and so on. Once the vulnerabilities appear in device firmware, upgrading firmware one by one will cause large workload, low efficiency and security. HikCentral Access Control provides two methods of firmware upgrade, which can upgrade the firmware of device in a batch and strengthen the system security.

(1) HikCentral Access Control Firmware Upgrade

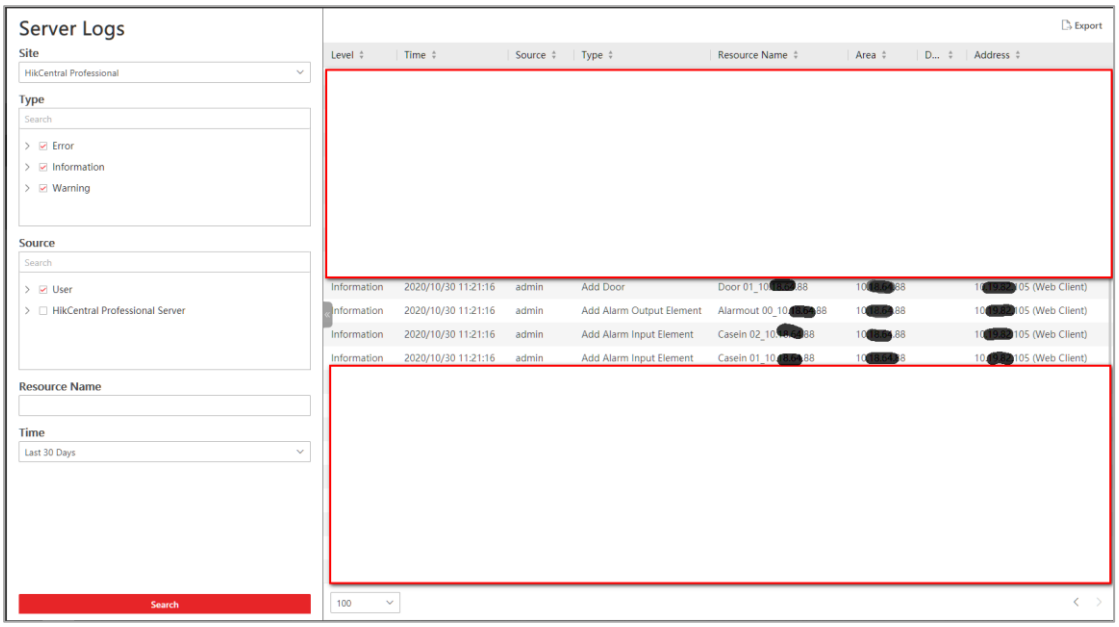
After users obtain the new firmware package released by the Hikvision device, they can directly upload it to HikCentral Access Control, and the HikCentral Access Control service can independently upgrade the firmware of the device.

(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 Access Control detects that there is a new firmware package in Hik-Connect, HikCentral Access Control will prompt and guide the users to upgrade.

2.9 Audit Log

HikCentral Access Control 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.



2.10 Digital Signature and Anti-Tamper Protection of Product Information

The plug-in of HikCentral Access Control 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 Access Control and refused to load.

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

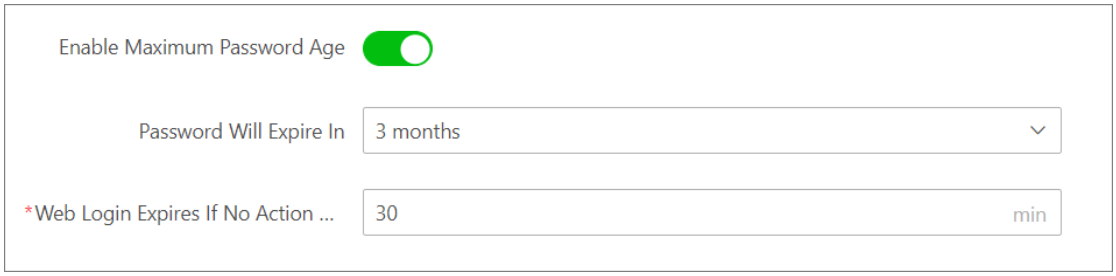
2.11 HikCentral Access Control Version Update

The version of HikCentral Access Control will be updated continuously, and the security problems or vulnerabilities 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 Access Control pay attention to the vulnerability information disclosed by dominant security companies and update the version of HikCentral Access Control.

2.12 Other Security Measures

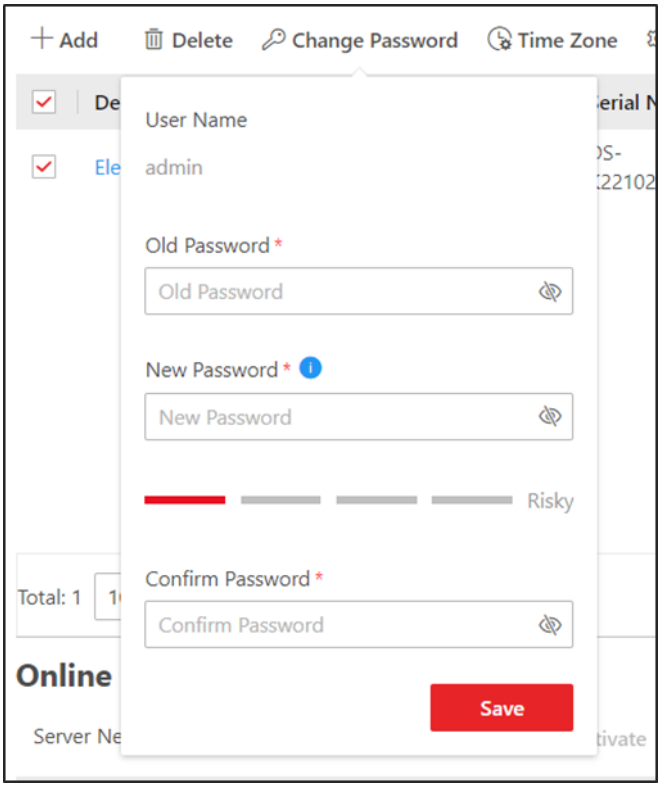
2.12.1 Maximum Password Age

Switch on **Enable Maximum Password Age** and Set the **Password Will Expire In** as you want on the Security page of the HikCentral Access Control Web Client.



2.12.2 HikCentral Access Control Changes Device Password Periodically

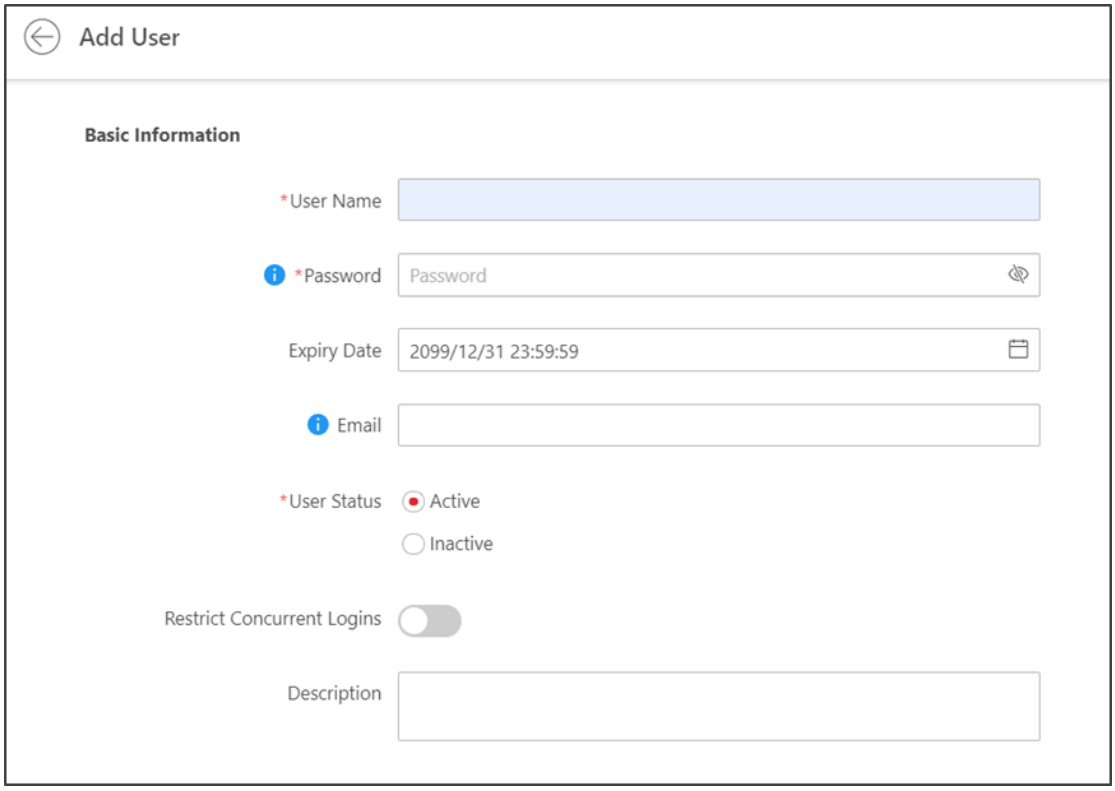
Change device password periodically to make the device more secure.



2.12.3 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.



Chapter 3 Operating System Security of Server and Client

HikCentral Access Control service and clients are deployed in Microsoft® Windows which supports many security policies. This section describes the security settings of the HikCentral Access Control 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.

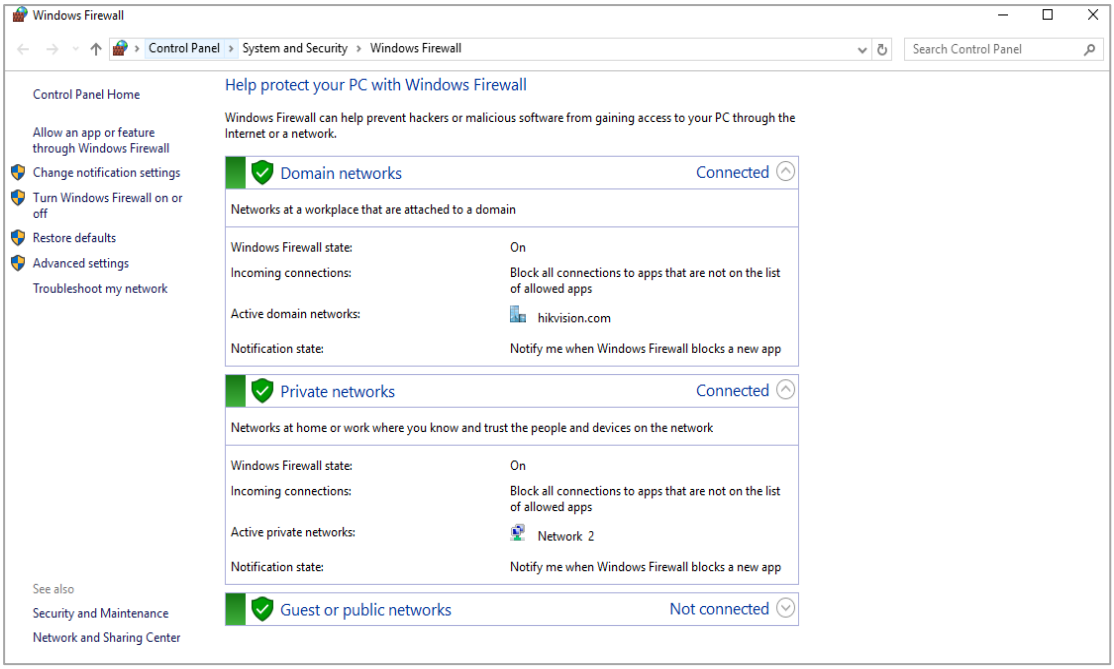
For the best practices of password management on Windows, visit the Microsoft® official website.

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 defense 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

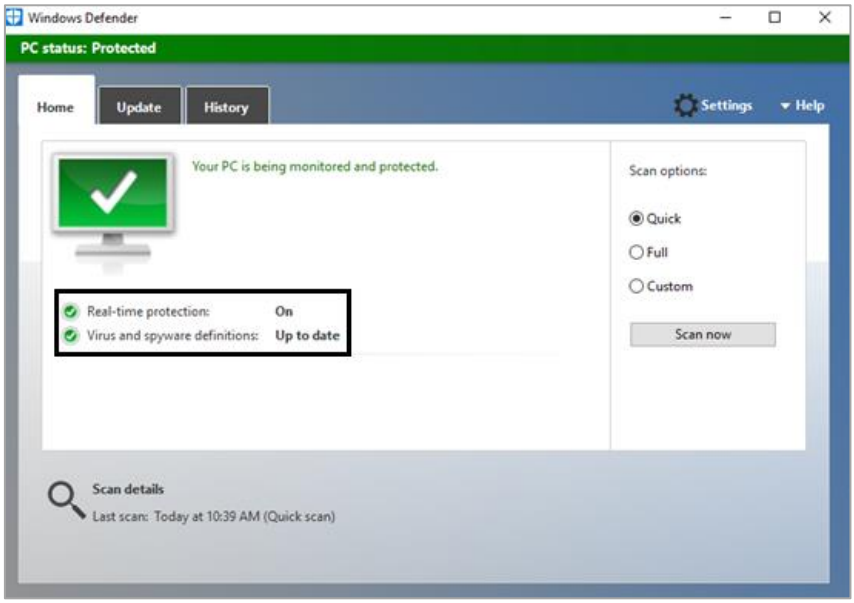
are suggested to be disabled when RPC, NetBIOS, and SMB are NOT used.

3.5 Antivirus

Install full-featured Anti-Virus software to keep HikCentral Access Control 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”

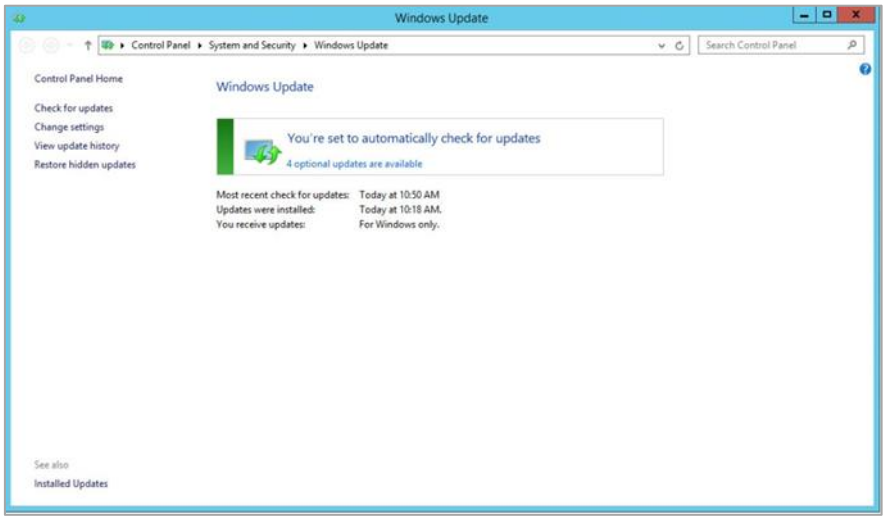
Example from Microsoft® Windows 10:



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 Access Control 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

The devices deployed in the front-end are responsible for the data collection of the whole system. The security of these devices is highly important. Set a strong password for each device to reduce the risk of device password leakage. The recommended password should be composed of digits, letters and special characters, and the length should not be less than 8 characters.

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 Access Control

It is recommended to create an exclusive account on the device if this device is to be added to HikCentral Access Control for management. For example, you can create an account named HikCentral Access Control, and then add the device to HikCentral Access Control with this user name. Similarly, other users can access the device by the name of HikCentral Access Control. 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 Access Control service.

5.1 Server Physical Security

The deployment server of HikCentral Access Control 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 Access Control 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 Access Control 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 Access Control. Only authorized users are allowed to use mobile storage media when necessary.

5.4 Allocate Different Accounts for Facilitate Audit

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

to know clearly in the HikCentral Access Control 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 Access Control also supports Active Domain (AD) users. AD server has high security and can verify the validity of users.

5.5 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.

5.6 Prohibit Risky Protocols and Services

Regularly use security tool to scan HikCentral Access Control 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.

5.7 Prohibit Remote Database Access

HikCentral Access Control uses PostgreISQL 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.

5.8 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 Access Control server.

5.9 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