HikCentral V1.3 for Windows® Hardening Guide

Contents

Introduction.. 1
1. The Operating System - Microsoft Windows Security Configuration 2
1.1Strict Password Policy 2
1.2Turn Off Windows Remote Desktop 2
1.3Turn On Windows Firewall 2
1.4Disable Sensitive Ports 2
1.5Antivirus 3
1.6Windows Updates Must Be Turned On 3
2. Network Access - Protecting User Access to Network 4
2.1Remote Client Access 4
2.2VLANs 4
2.3Disable Unused Switch Ports 4
2.4Only Open the Minimum Required Ports on a Dedicated Router Firewall 4
2.5Network Security 4
3. Application Platform - HikCentral Security Configurations 5
3.1HikCentral Port Forwarding 5
3.2Lock IP Address: After Too Many Attempts 6
3.3Minimum Password Strength 6
3.4Maximum Password Age 6
3.5Auto Lock Control Client 7
3.6Change Device Password Periodically 7
3.7User Privileges 7
a) Active Directory Integration 7
b) Strong Password 8
c) Minimum User Privileges 9
3.8Security Transfer Protocol 9
3.9Stream Encryption 9
4. Recommendations for Additional Security Configurations 10

Introduction

HikCentral is a Central Management Software (CMS) that requires a Windows-based server. HikCentral is developed by Hangzhou Hikvision Digital Technology Co. Ltd; all rights are reserved by Hikvision. HikCentral 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.

The purpose of this guide is to help customer secure related servers and applications on their video surveillance network.

The document contains instructions, for the following,

1. The operating system
- Microsoft Windows
2. Network access
- Protecting user’s access to a network
3. The application platform
- HikCentral Security Configurations
4. Recommendations for additional security configurations

NOTE: This document focuses on HikCentral software. For best security practices for NVRs, DVRs, and IP cameras manufactured by Hikvision, please refer to the security guides on our website

Supported Operating Systems

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

- Microsoft® Windows 7 64-bit
- Microsoft® Windows 8 64-bit
- Microsoft® Windows 8.1 64-bit
- Microsoft® Windows 10 64-bit
- Microsoft® Windows Server 2008 R2 64-bit
- Microsoft® Windows Server 2012 64-bit

For recommended settings, please visit the Microsoft website LINK

1. The Operating System - Microsoft Windows Security Configuration

1.1 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 Windows Server purchased from Hikvision, a new password should be assigned to the Windows Administrator account upon first login.

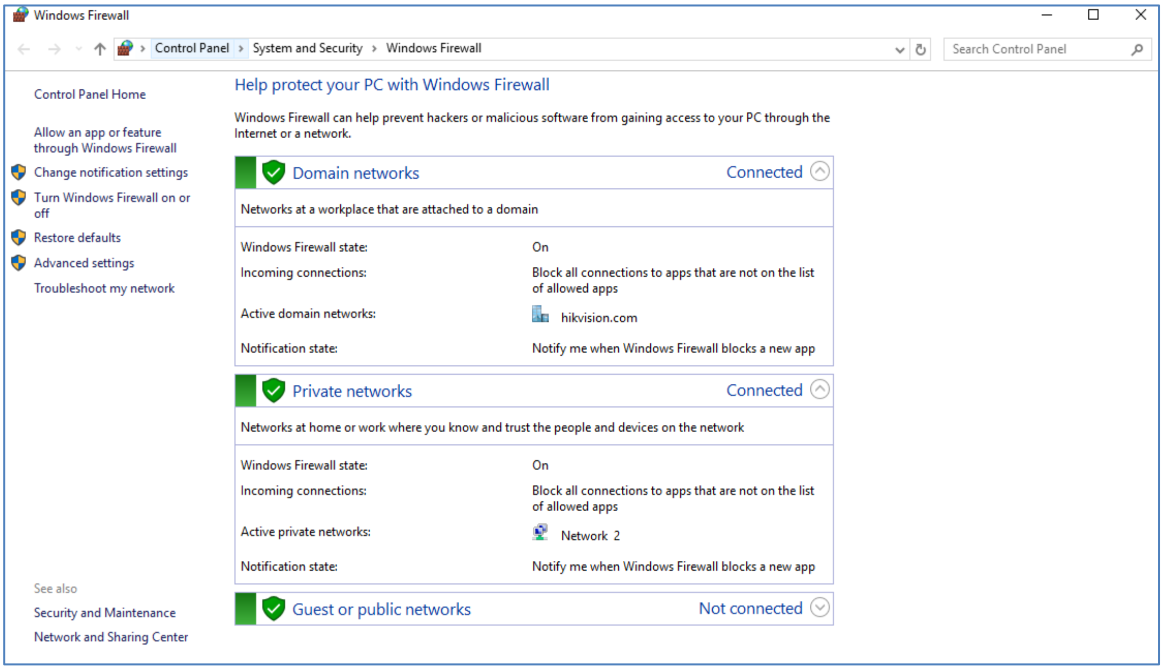
For best practices of password management for Windows, please visit the Microsoft website LINK

1.2 Turn Off Windows Remote Desktop

Disable Windows Remote Desktop to secure the Windows system.

1.3 Turn On Windows Firewall

A software firewall is the second layer of defense after the network layer firewall and will help protect your computer from outside attempts to control or gain the access. By default, the Windows firewall is turned on and should remain on at all times.



Windows Firewall

Control Panel > System and Security > Windows Firewall

Search Control Panel

Control Panel Home

Allow an app or feature through Windows Firewall

Change notification settings

Turn Windows Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

See also

Security and Maintenance

Network and Sharing Center

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Domain networks — Connected

Networks at a workplace that are attached to a domain

Windows Firewall state: On

Incoming connections: Block all connections to apps that are not on the list of allowed apps

Active domain networks: hikvision.com

Notification state: Notify me when Windows Firewall blocks a new app

Private networks — Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state: On

Incoming connections: Block all connections to apps that are not on the list of allowed apps

Active private networks: Network 2

Notification state: Notify me when Windows Firewall blocks a new app

Guest or public networks — Not connected

1.4 Disable Sensitive Ports

TCP Ports (135/139/445) and UDP Ports (137/138) in the Windows Security Policy are suggested to be disabled when you are NOT in use for RPC, NetBIOS, and SMB.

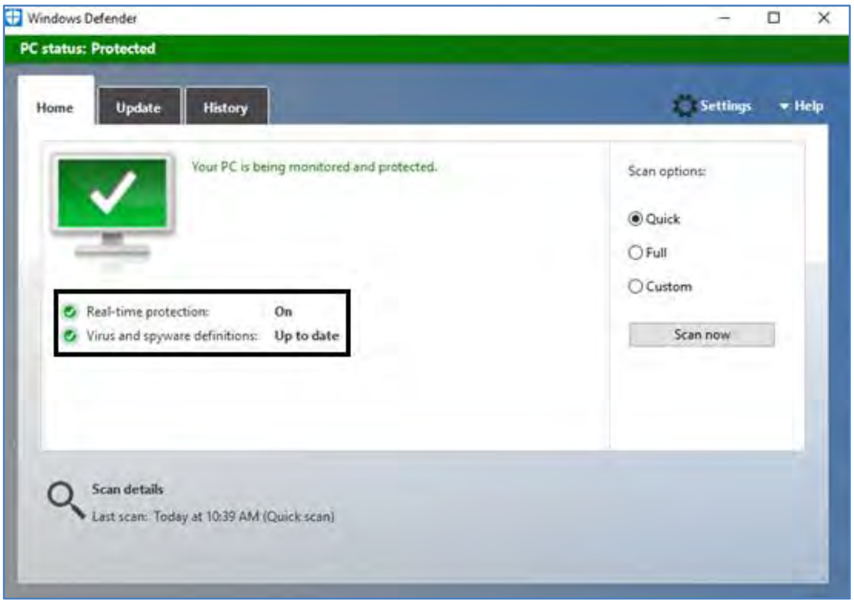
1.5 Antivirus

Please install full-featured Anti-Virus software to keep HikCentral Server in security. Antivirus must be active and automatically updated.

For example, the settings of Microsoft Windows Antivirus “Windows Defender” is as below,

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

Example from Windows 10:



PC status: Protected

Your PC is being monitored and protected.

Real-time protection: On
Virus and spyware definitions: Up to date

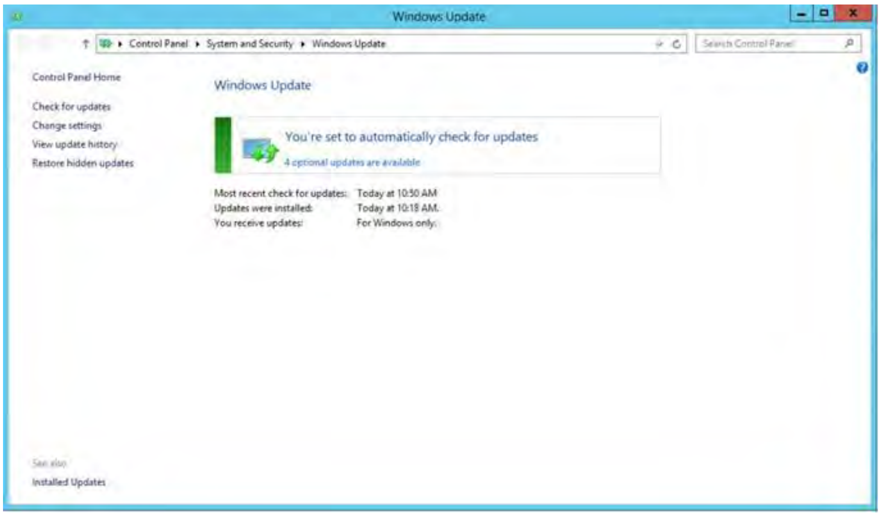
● Quick
○ Full
○ Custom

Last scan: Today at 10:39 AM (Quick scan)

1.6 Windows Updates Must Be Turned On

It is important that Windows updates are set to ‘auto install’. Normally, this is the default setting.

Ex: from Windows Server:



You're set to automatically check for updates

4 optional updates are available

Most recent check for updates: Today at 10:50 AM
Updates were installed: Today at 10:18 AM.
You receive updates: For Windows only.

2. Network Access - Protecting User Access to Network

2.1 Remote Client Access

If the HikCentral Server is on a LAN behind a NAT, it is recommended to use VPN tunneling (Configure on the Router or Firewall Settings) to remotely access the client software on PC via WAN.

A Virtual Private Network (also called 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, while also protecting privacy and increasing security within a LAN. A VPN not only adds an additional layer of protection for a surveillance system, but it also provides the additional benefit of segmenting the production networks business traffic and video traffic.

2.2 VLANs

If the HikCentral Server is on a LAN with Client PCs, it is recommended to use a Virtual LAN (VLAN).

A Virtual Lan is created by subdividing a LAN into multiple segments. The network segmentation is done through a network switch or router configuration. A VLAN can address resource needs without rewiring device network connections.

2.3 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. The option to disable specific ports is a common option in managed switches, both low cost and enterprise.

2.4 Only Open the Minimum Required Ports on a Dedicated Router Firewall

If it is not possible to use VPN among various sites, you need to make sure that the router has a firewall and only open the ports required to connect to the HikCentral Server.

2.5 Network Security

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

3. Application Platform - HikCentral Security Configurations

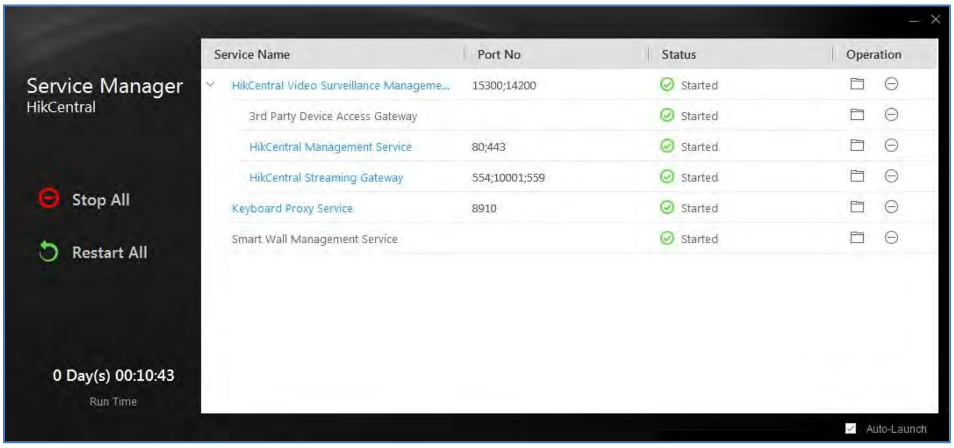
3.1 HikCentral Port Forwarding

Port mapping should only be opened when your HikCentral needs to access to a Wide Area Network. Please follow rules below to protect your data:

1) Please do the ports forwarding based on the **HikCentral Ports List** document - LINK. Don't forward any unnecessary ports.
2) Try not to use general port for other services. For example, port 80 is utilized for HikCentral Management Service by default; don't use port 80 for other services like Streaming Gateway Services.
3) Port forwarding exposes your HikCentral Server directly to the Internet on that port. Be sure to set high security passwords for all accounts and keep the network connection in security.

HikCentral only requires four open ports for basic functionality:

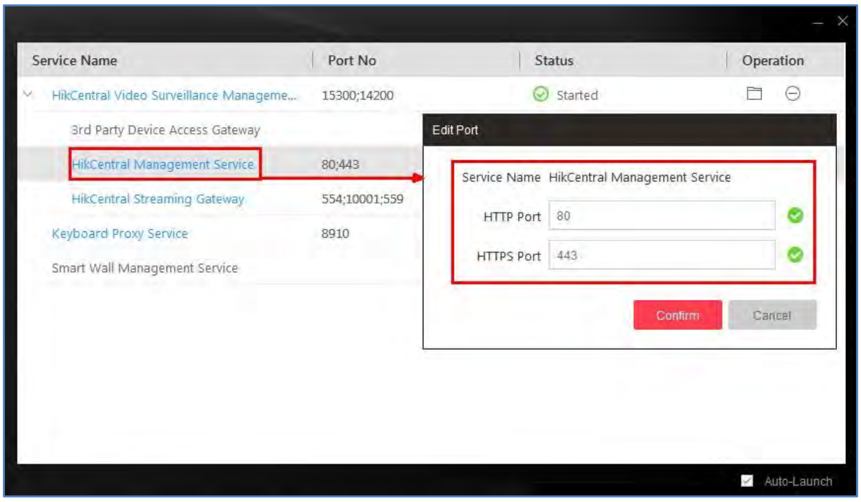
- HikCentral Streaming Gateway: 554, 10000 (used for live view and playback video streaming
- HikCentral Management Service: 80, 443 (used for connecting to Web Clients and Control Client)



Service Name	Port No	Status	Operation
HikCentral Video Surveillance Manageme...	15300;14200	✓ Started	
3rd Party Device Access Gateway		✓ Started	
HikCentral Management Service	80;443	✓ Started	
HikCentral Streaming Gateway	554;10001;559	✓ Started	
Keyboard Proxy Service	8910	✓ Started	
Smart Wall Management Service		✓ Started	

It is recommended to change the port number from the default.

The example below shows how to change the ports in the HikCentral Service Manager,



Service Name	Port No	Status	Operation
HikCentral Video Surveillance Manageme...	15300;14200	✓ Started	
3rd Party Device Access Gateway			
HikCentral Management Service	80;443		
HikCentral Streaming Gateway	554;10001;559		
Keyboard Proxy Service	8910		
Smart Wall Management Service			

Service Name HikCentral Management Service

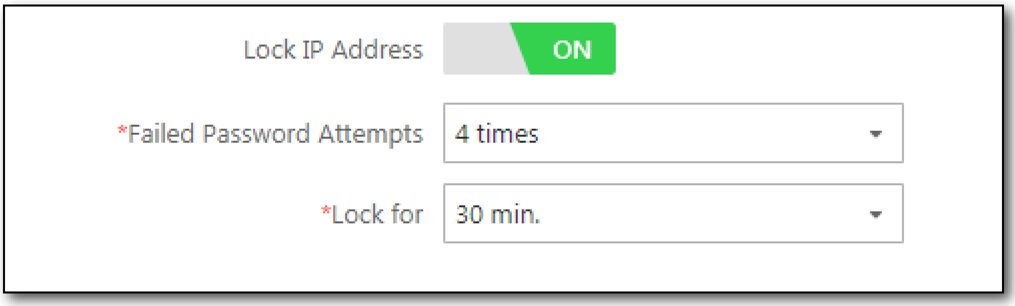
HTTP Port 80

HTTPS Port 443

Please see **HikCentral Ports List** document for information on port forwarding required for advanced applications. LINK

3.2 Lock IP Address: After Too Many Attempts

Enable the **"Lock IP Address"** function in the Security Settings section of the HikCentral Web Client. This helps protect against illegal login attempts to the HikCentral Server



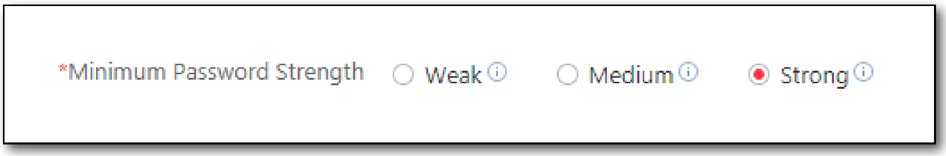
Lock IP Address ON

*Failed Password Attempts 4 times

*Lock for 30 min.

3.3 Minimum Password Strength

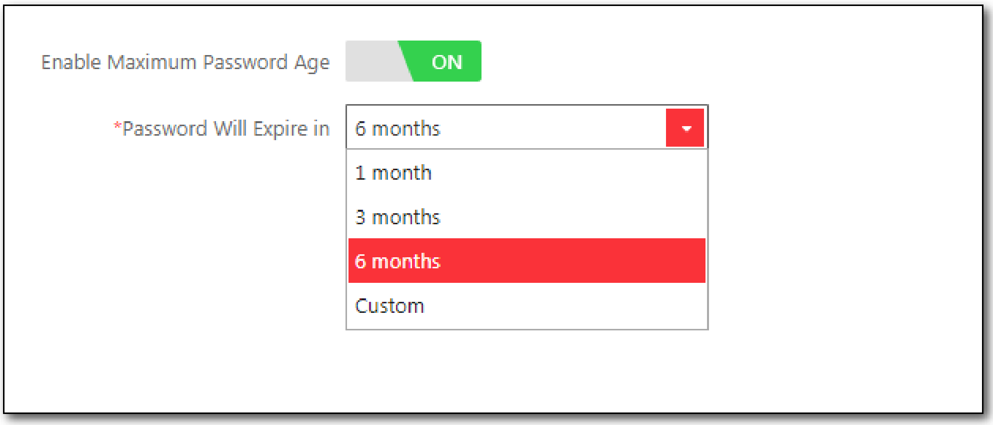
Select **Strong** as the **"Minimum Password Strength"** in the Security Settings section of the HikCentral Web Client.



*Minimum Password Strength ○ Weak ○ Medium ● Strong

3.4 Maximum Password Age

Enable **"Maximum Password Age"** and Set the **"Expire Time"** as you want in the Security Settings section of the HikCentral Web Client.

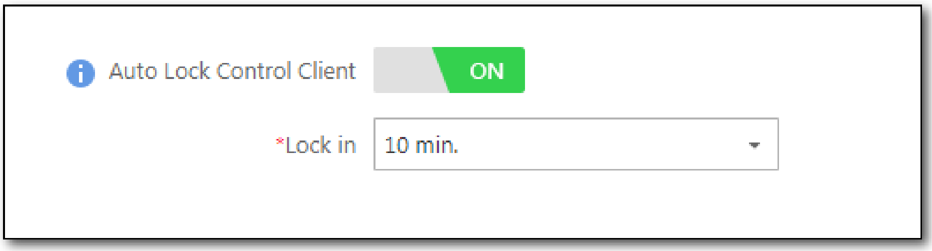


Enable Maximum Password Age ON

*Password Will Expire in 6 months

3.5 Auto Lock Control Client

Enable **"Auto Lock Control Client"** and Set the **"Lock Time"** in the Security Settings section of the HikCentral Web Client. This locks the Control Client if it is idle for the configured period. The user is required to use the username and password to unlock the Control Client.

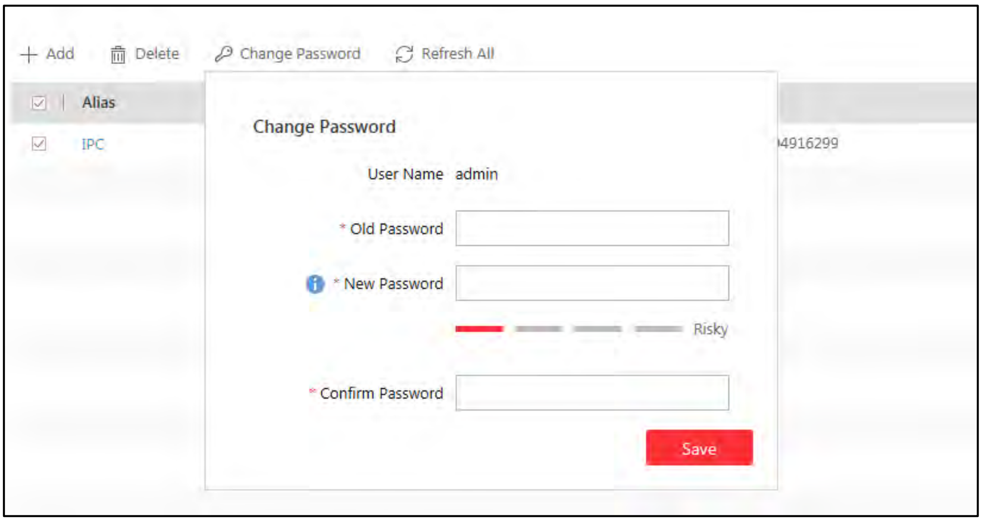


Auto Lock Control Client ON

*Lock in 10 min.

3.6 Change Device Password Periodically

Change Device Password Periodically to make the device more secure



Change Password

User Name admin

* Old Password

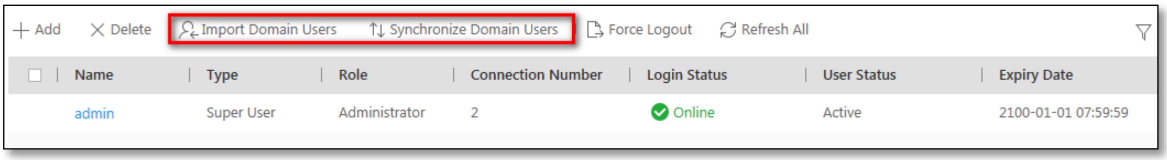
* New Password

* Confirm Password

3.7 User Privileges

a) Active Directory Integration

HikCentral can select Active Directory accounts from Windows Active Directory Server. By doing this, all the user data is stored in the Active Directory Server, making the data more secure.

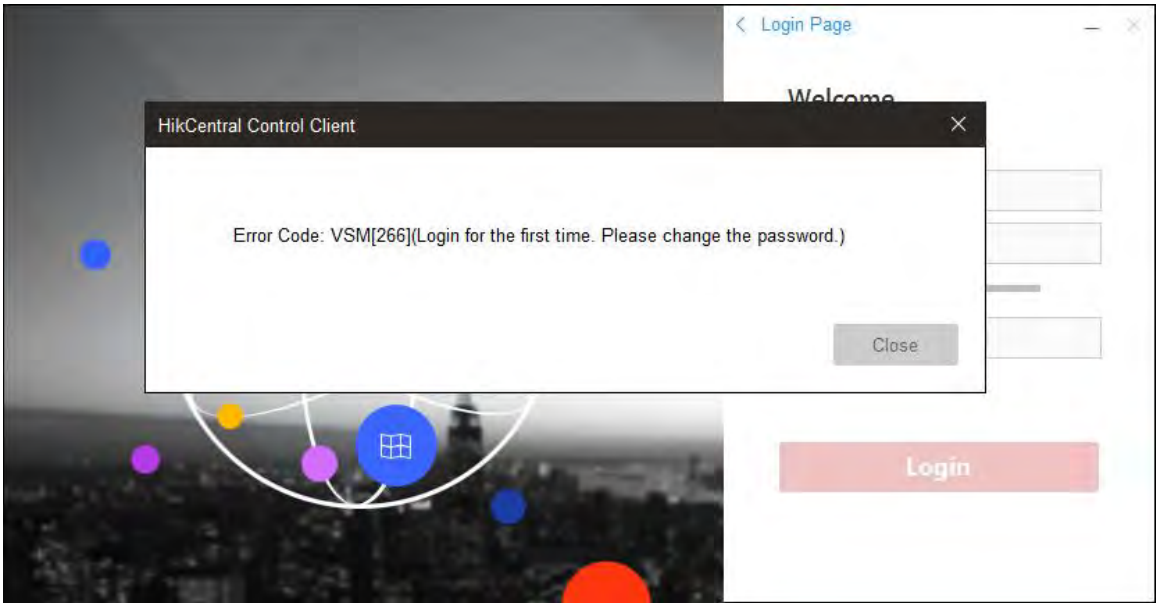


□	Name	Type	Role	Connection Number	Login Status	User Status	Expiry Date
	admin	Super User	Administrator	2	✓ Online	Active	2100-01-01 07:59:59

b) Strong Password

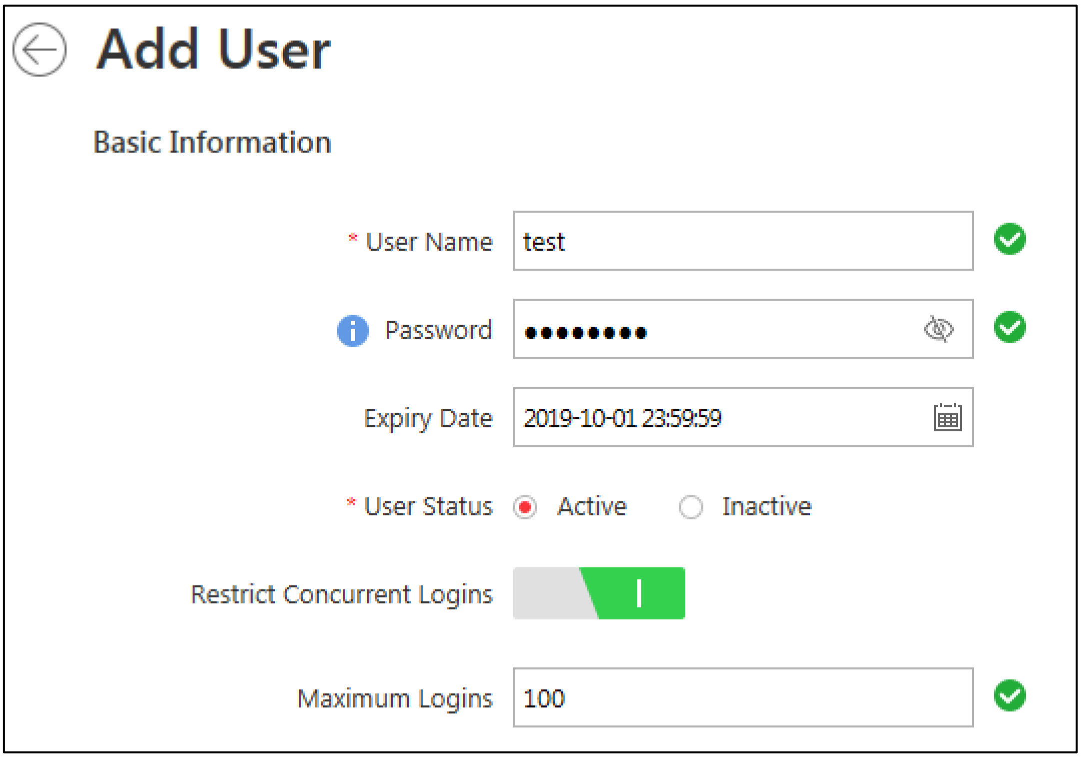
When the administrator adds a new user, the user needs to change the password, when they log in for the first time.

Please set a STRONG password (case-sensitive letters, special characters combined with numbers)



Error Code: VSM[266](Login for the first time. Please change the password.)

When the administrator creates a new user, he/she can set a **STRONG** password and an **"Expiry Date"** for the user. And the administrator can also set the Restrict Concurrent Logins to the **Suitable Number** for the user



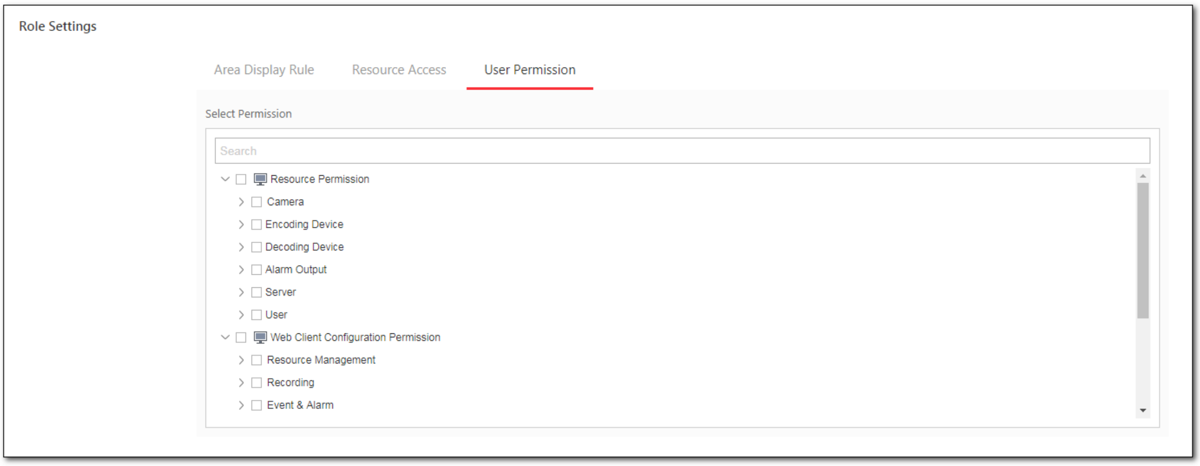
Add User

Basic Information

* User Name: test
Password: ●●●●●●●●●
Expiry Date: 2019-10-01 23:59:59
* User Status: ● Active ○ Inactive
Restrict Concurrent Logins: on
Maximum Logins: 100

c) Minimum User Privileges

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



Select Permission

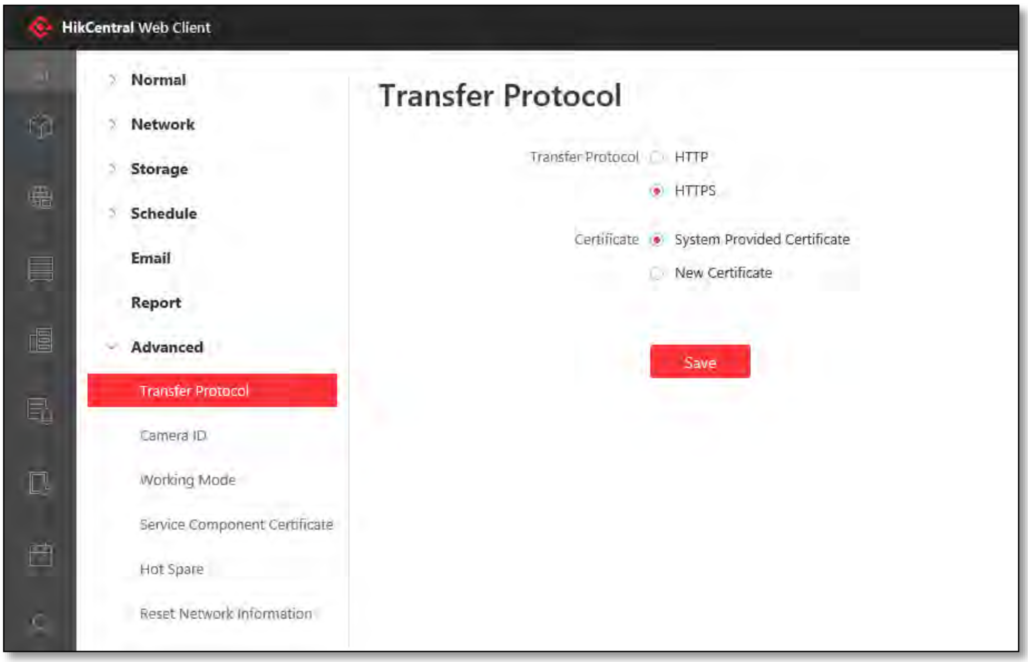
Search

- □ Resource Permission
  - □ Camera
  - □ Encoding Device
  - □ Decoding Device
  - □ Alarm Output
  - □ Server
  - □ User
- □ Web Client Configuration Permission
  - □ Resource Management
  - □ Recording
  - □ Event & Alarm

3.8 Security Transfer Protocol

1. Log into the Web Client.
2. Change the Transfer Protocol **HTTP to HTTPS on the HikCentral** web client,

The administrator is able to select **"System Provided Certificate" or "New Certificate".**



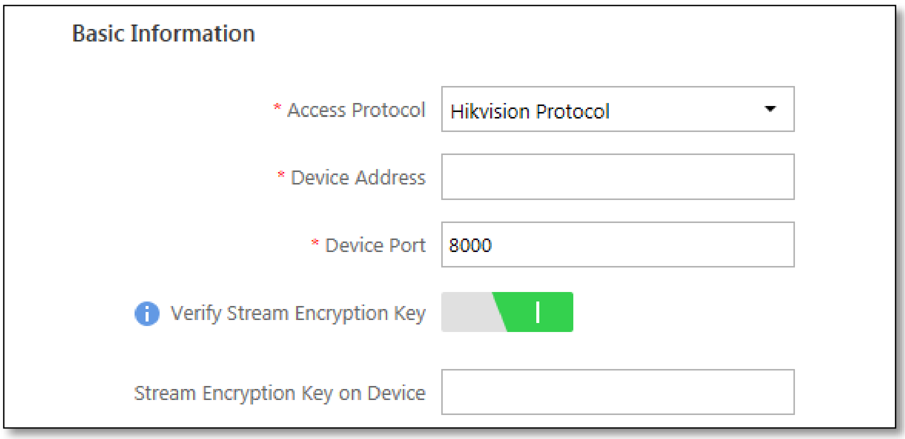
Transfer Protocol

Transfer Protocol ○ HTTP ● HTTPS

Certificate ● System Provided Certificate ○ New Certificate

3.9 Stream Encryption

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



Basic Information

* Access Protocol	Hikvision Protocol
* Device Address	
* Device Port	8000
Verify Stream Encryption Key	●
Stream Encryption Key on Device	

4. Recommendations for Additional Security Configurations

- Block unauthorized computers or devices from accessing the local network, and forbid unauthorized connection to untrusted networks on individual devices.
- If some services need to be exposed on an untrusted network, it is necessary to build a Demilitarized Zone (DMZ) to add an additional layer of security to the Local Area Network (LAN). External attackers can only access services in the DMZ instead of gaining access to the LAN.
- Create VLANs to divide the network into different broadcast domains, and apply strict security strategies for important VLANs.
- Use a Domain Controller (DC) to manage policies, users, and groups.
- Physical Access to Server

  There should be restricted physical access to the Server (or a Virtual Server hosting on HikCentral)

  a. Locked access control on the door of the Server Room;

  b. Limited access to manage the server room by the administrator-level user only.
- Restrict the use of removable media on servers

  Restrict removable media like USB disk, SD cards and cellphones on servers to help prevent malware from entering the network.

First Choice for Security Professionals

HIKVISION | www.hikvision.com