HikCentral V.1.1.x for Windows® Hardening Guide

Contents

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 & Hybrid SANs.

The purpose of this guide is to help HikCentral 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 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 LINK

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 and get support on official website of Microsoft 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.

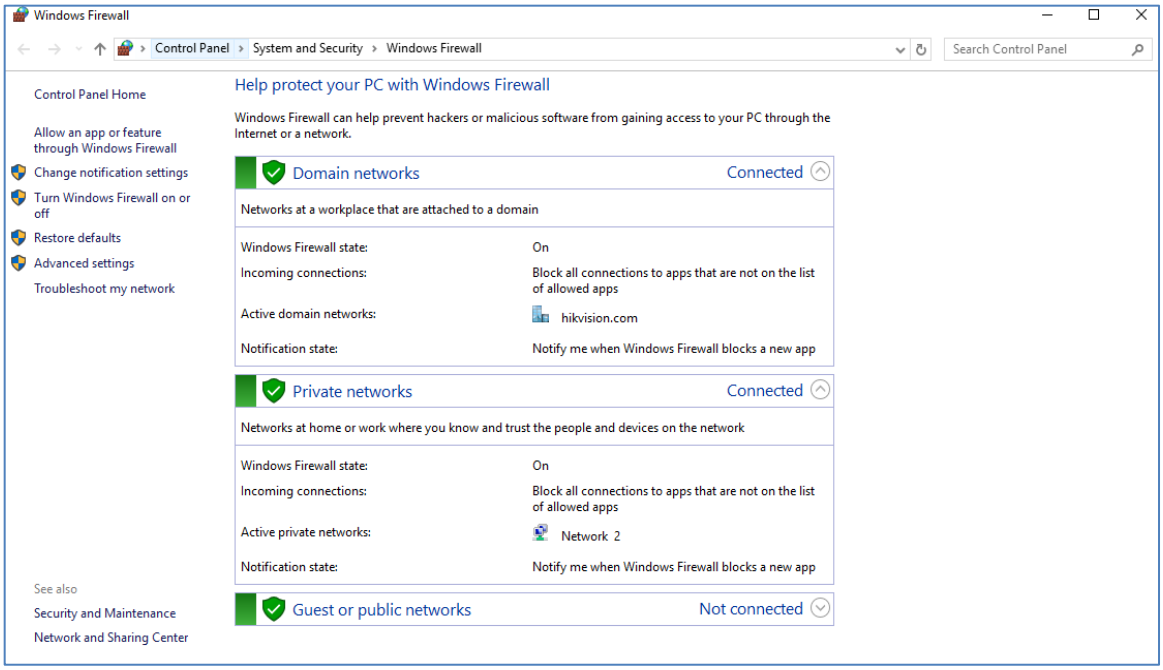
For best practices of password management for Windows, please visit the Microsoft website LINK

1.2 Turn Off Windows Remote Desktop

Disable Windows Remote Desktop to secure the Windows system safety.

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.



1.4 Turn Off Sensitive Port

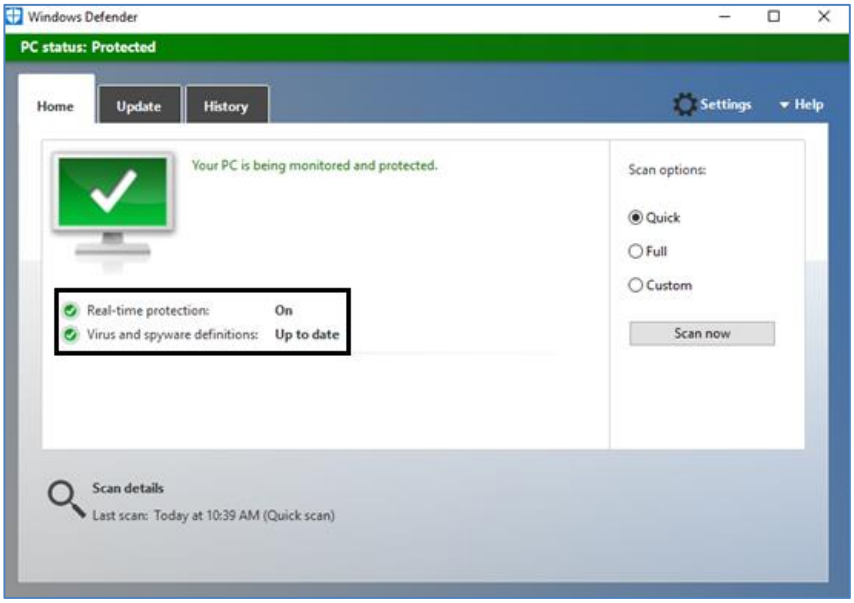
Turn off TCP Ports (135/139/445) and UDP Ports (137/138) in the Windows Security Policy.

1.5 Antivirus

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"

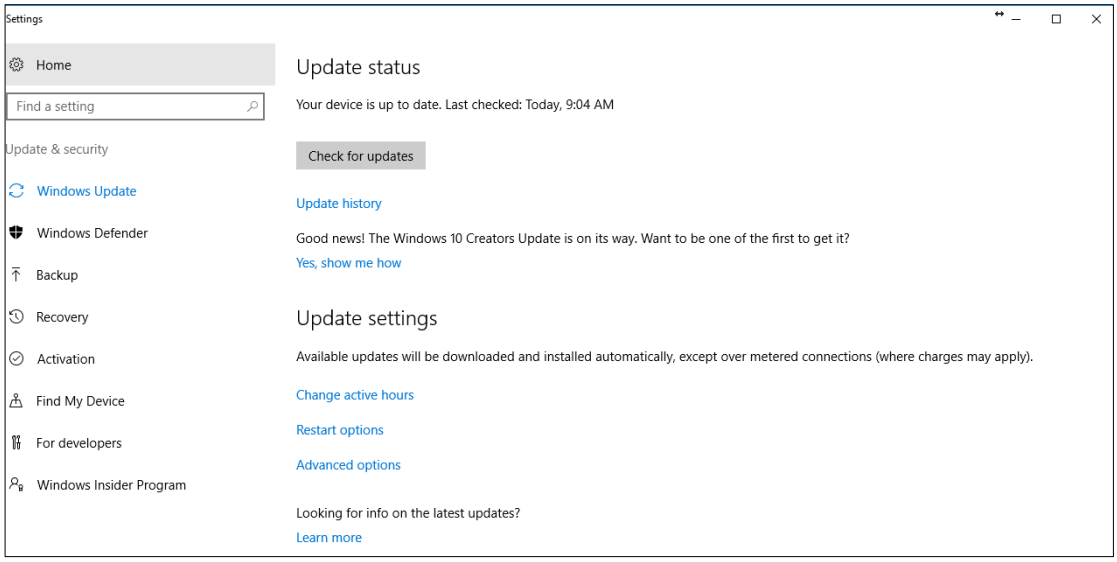
Example from Windows 10:



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 10:



2. Network Access - Protecting User's 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 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 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

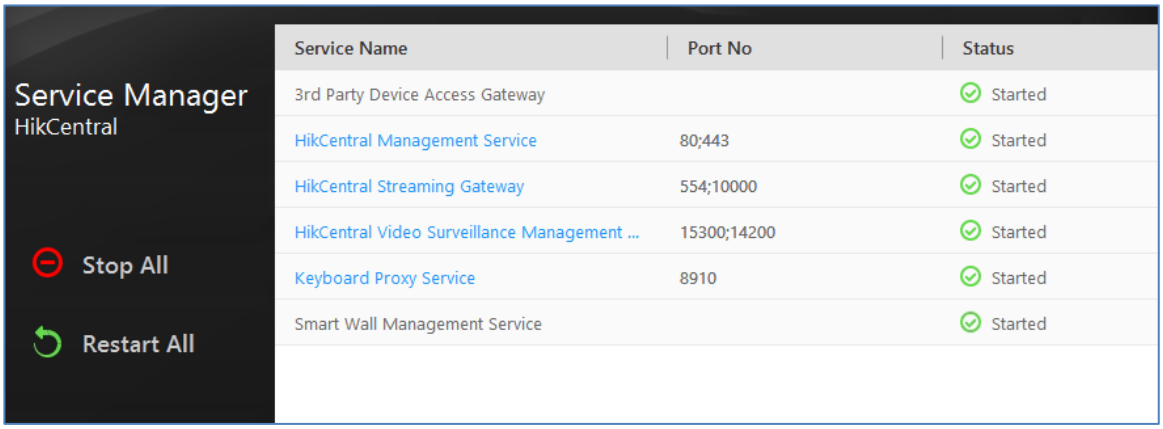
Choose proper security technologies to enhance network security, such as an intrusion Detection System (IDS), ACL (Access Control List), 802.1x, RADIUS authentication and Security Auditing.

3. Application Platform - HikCentral Security Configurations

3.1 HikCentral Port Forwarding

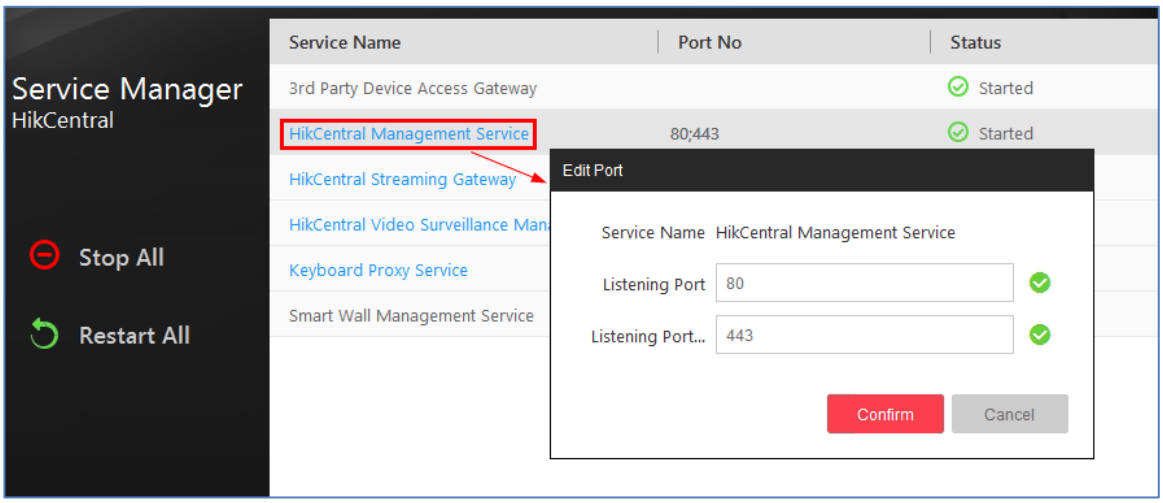
HikCentral only requires four open ports for basic functionality:

- 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)



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

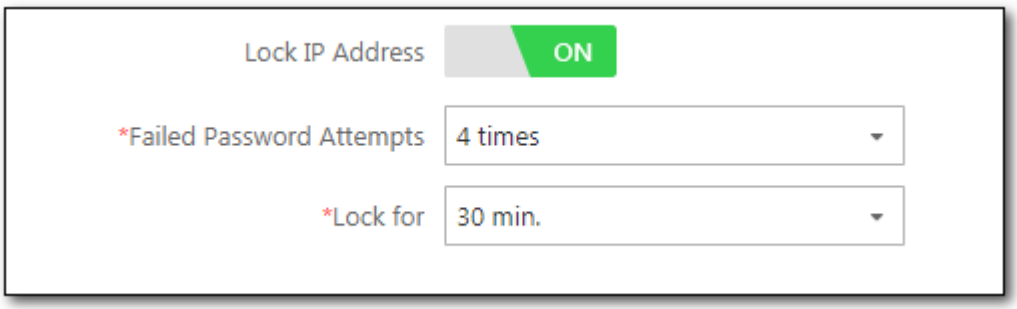
The example below shows how to change the ports in the HikCentral Service Manager,



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

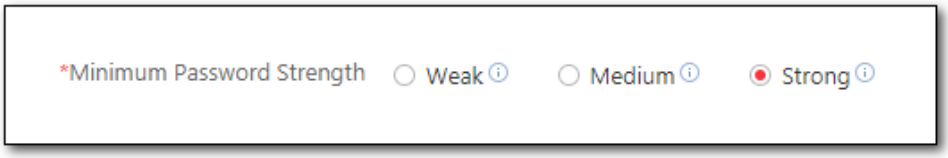
3.2 Lock IP Address: After Too Many Attempts

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



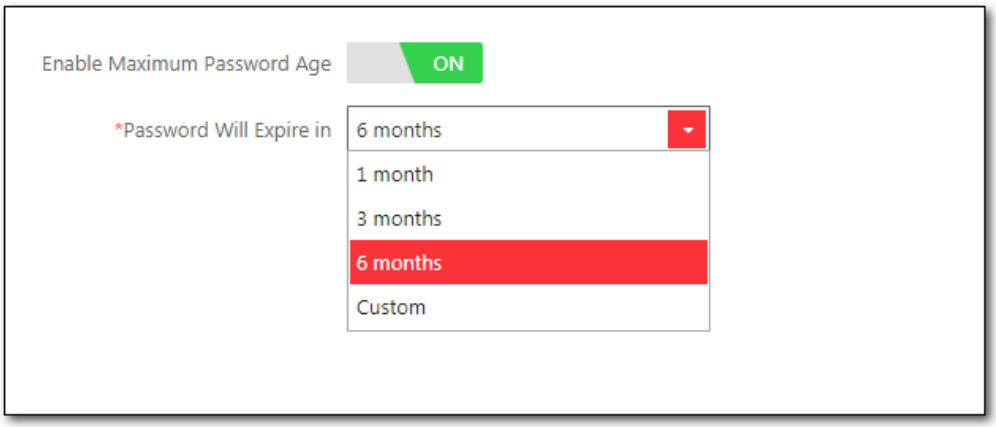
3.3 Minimum Password Strength

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



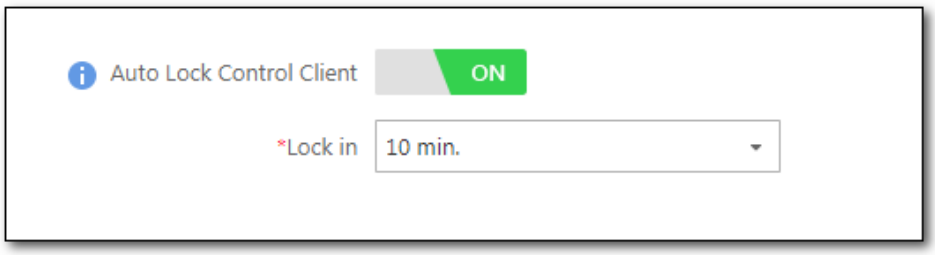
3.4 Maximum Password Age

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



3.5 Auto Lock Control Client

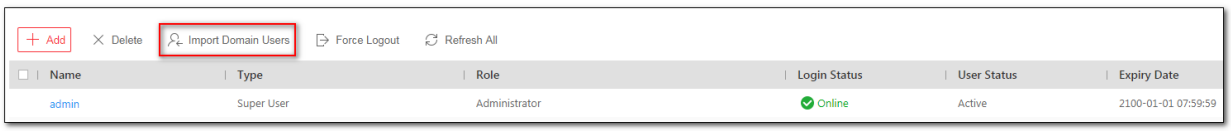
Enable **"Auto Lock Control Client"** and Set the **"Lock Time"** in the Security Settings section of the HikCentral Web Client. This locks the Control Client if it is idle for the configured period. The user is required to use the username and password to unlock the Control Client.



3.6 User Privileges

a) Active Directory Integration

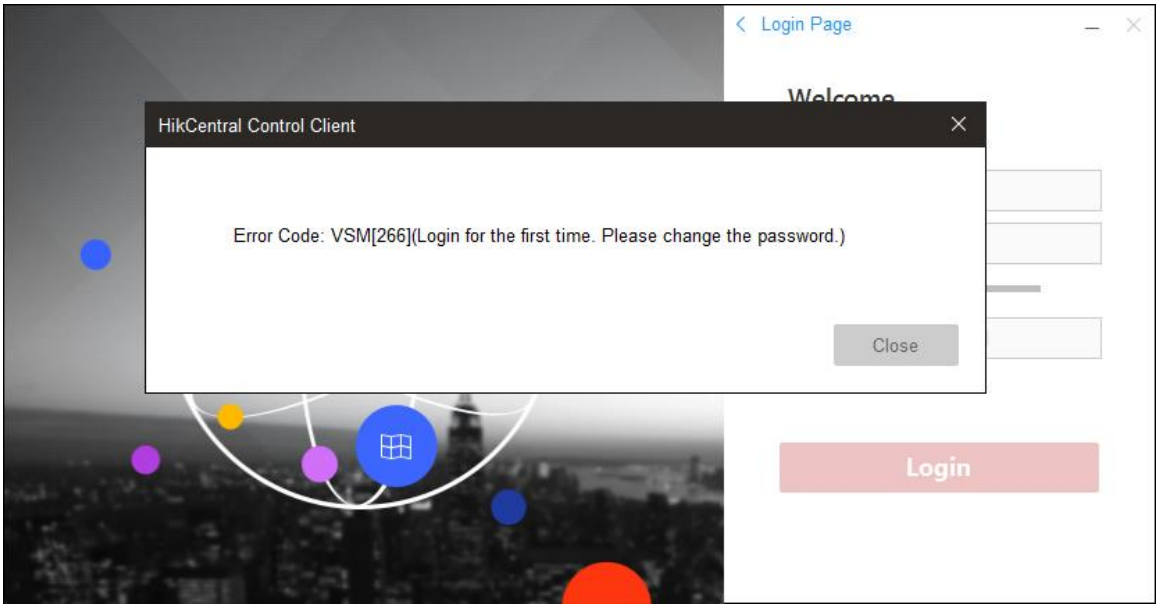
HikCentral can import Active Directory account from Windows Active Directory Server. By doing this, all the user data is stored in the Active Directory Server, making the data more secure.



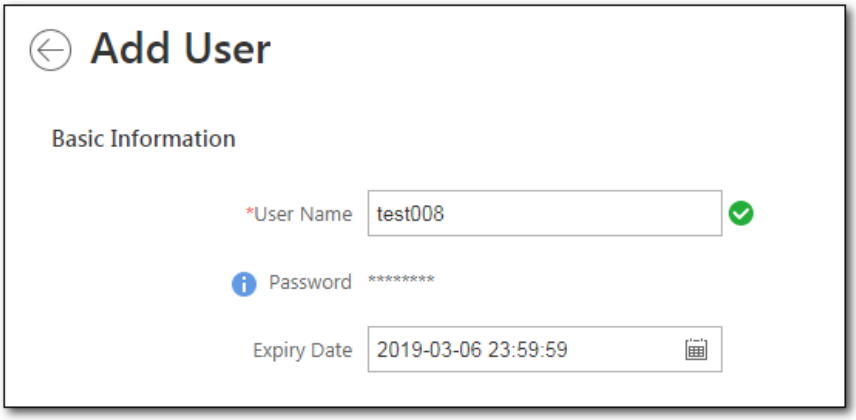
b) Strong Password

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)

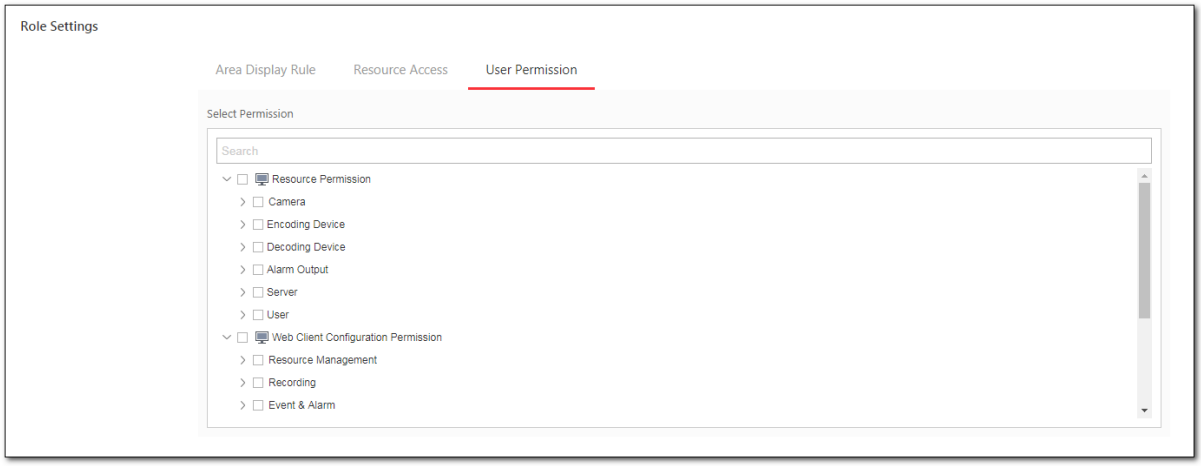


When the administrator create a new user, he/she can set an **"Expiry Date"** for the user.



c) Minimum User Privileges

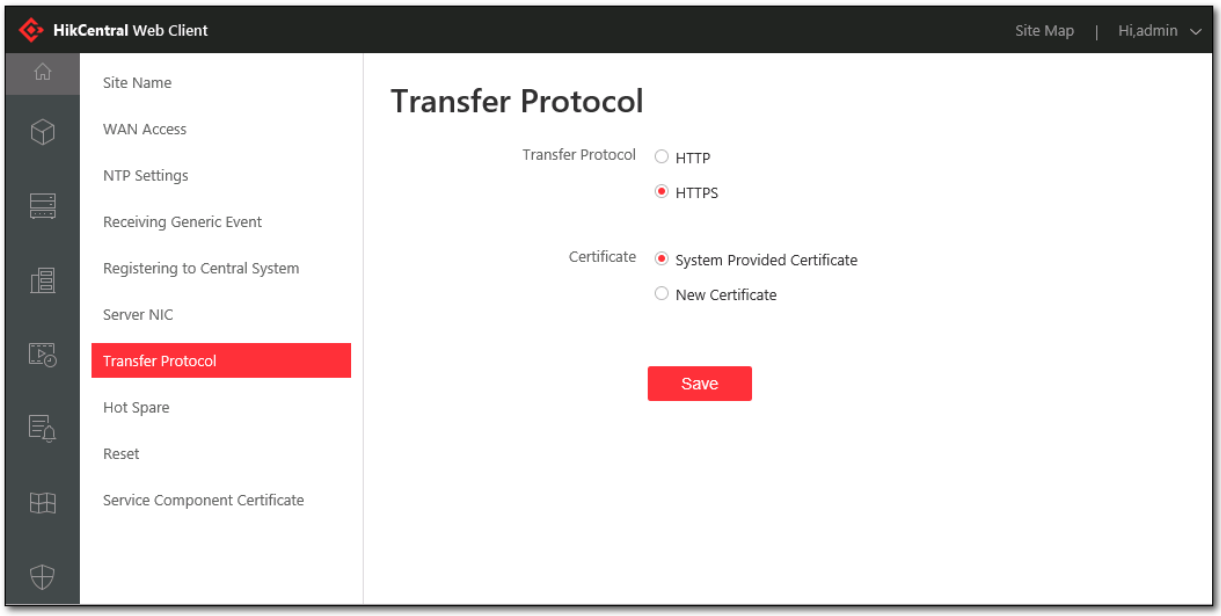
When the administrator creates a new role, he/she must **only select** the required permissions for the role.



3.7 Security Transfer Protocol

Change the Transfer Protocol **HTTP to HTTPS on the HikCentral** web client,

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



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 expose 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