PARS ERTEBAT
پارس ارتباط

HIKVISION®
See Far, Go Further

راهنمای امنیت شبکه

هایک ویژن

شرکت پارس ارتباط افزار پیشرو در تولید، تأمین، توزیع، آموزش و خدمات پس از فروش
تجهیزات حوزه فناوری اطلاعات و ارتباطات (ICT)، سیستم‌های نظارت تصویری و حفاظت پیرامونی

۰۲۱ - ۸ ۹۳ ۹۵ www.pars-e.com parsertebatchannel pars.ertebat.afzar pars ertebat afzar

فصل اول: مقدمه

دوربین های مداربسته و دستگاه های ذخیره ساز NVR یا DVR تحت شبکه هنگام اتصال به شبکه در معرض ریسک‌های امنیتی قرار می‌گیرند.

شرکت هایک ویژن، برای حفاظت از تجهیزات نظارتی و ذخیره ساز خود در برابر حملات احتمالی، امکانات و دستورالعملی را جهت ارتقای سطح امنیت انواع دوربینهای مداربسته و دستگاه های ذخیره ساز NVR یا DVR تحت شبکه خود فراهم کرده است؛ از جمله ایجاد امنیت در عملیات راه اندازی اولیه، الزام به استفاده از رمزهایی قوی، غیرفعال کردن بعضی از سرویس‌های شبکه بر حسب تقاضا و ...

شما هم به عنوان کاربر شبکه، باید با اهمیت استفاده از راهکارهای امنیتی آشنا بوده و کارهای لازم از جمله بررسی لاگ‌های سیستم و تغییر منظم رمزعبور را انجام دهید.

فصل دوم: امنیت در عملیات راه اندازی اولیه

۱.۲ فعال سازی دوربینهای مداربسته و دستگاه های ذخیره ساز NVR یا DVR تحت شبکه با تنظیم یک رمز قوی

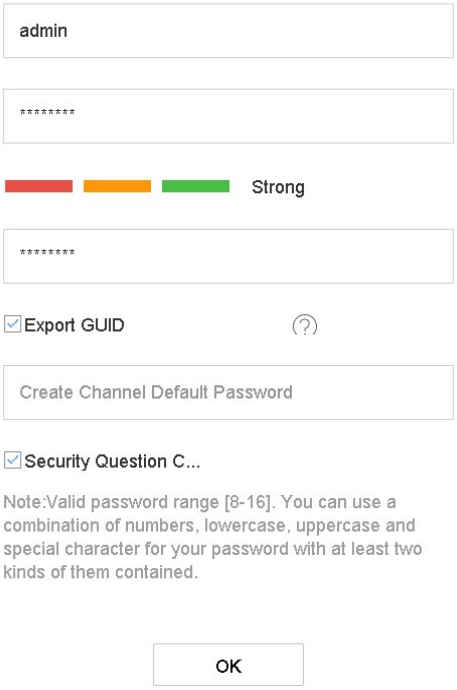
هنگام اولین دسترسی، باید دستگاه و دوربین‌های دوربینهای مداربسته و دستگاه های ذخیره ساز تحت شبکه را با تنظیم یک رمز ادمین قوی، فعال کنید. پیش از این فعال سازی، اجازه انجام هیچ کار دیگری را نخواهید داشت.

می‌توانید دستگاه را از طریق GUI محلی، مرورگر وب، SADP یا نرم‌افزار کلاینت فعال کنید.

در بخش بعدی، روش فعال سازی از طریق GUI محلی و SADP را توضیح می‌دهیم.

۱.۱.۲ فعال سازی از طریق GUI محلی

گام اول: در هر دو فیلد Create New Password و Confirm New Password یک رمز یکسان را وارد کنید.



شکل ۲-۱ تنظیم رمز ادمین

هشدار

به شدت توصیه می‌کنیم که برای ارتقای سطح امنیت محصولات، یک رمز قوی انتخاب کنید (رمزی که حداقل متشکل از ۸ کاراکتر و شامل حداقل سه مورد از این موارد باشد: حروف بزرگ، حروف کوچک، اعداد و کاراکترهای ویژه). بهتر است که رمز عبور را به صورت منظم تغییر دهید، به ویژه برای سیستم‌های به شدت امنیتی که ریست کردن ماهیانه یا هفتگی رمز عبور، به حفاظت هر چه بیشتر از آنها کمک می‌کند.

گام دوم: در فیلد Create Channel Default Password یک رمز پیش فرض برای دوربین های متصل به شبکه تعریف کنید.

گام سوم: Export GUID و Security Question Configuration را بررسی کنید.

Export GUID: GUID را برای ریست کردن رمز در آینده استخراج کنید.

Security Question Configuration: سوالات امنیتی را که برای ریست کردن رمز استفاده می‌شوند، تنظیم کنید.

گام چهارم: روی OK کلیک کنید.

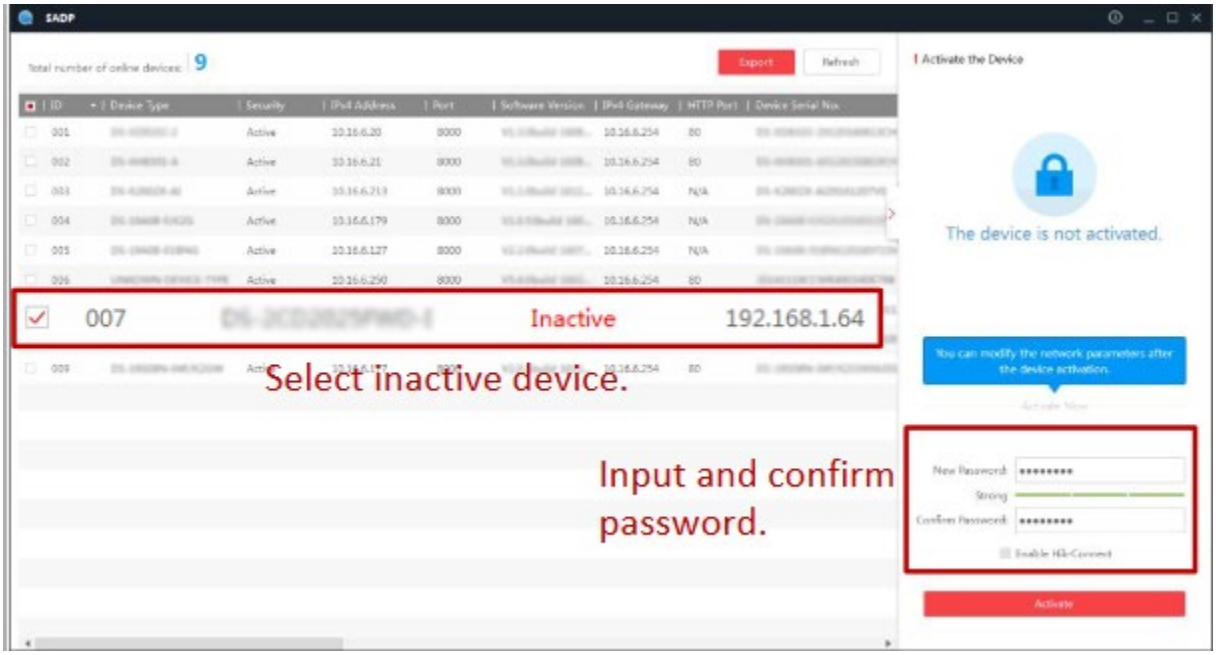
۲.۱.۲ فعال سازی از طریق نرم‌افزار SADP

از نرم‌افزار SADP برای تشخیص دستگاه‌های آنلاین، فعال سازی دستگاه و ریست کردن رمز استفاده می‌شود.

می‌توانید این نرم‌افزار را از دیسک ارایه شده در داخل بسته بندی برخی از تجهیزات یا از سایت رسمی دانلود کرده و آن را نصب کنید. لطفا برای فعال سازی دستگاه، مراحل زیر را دنبال کنید.

گام اول: نرم‌افزار SADP را برای جستجوی کلیه تجهیزات Hikvision تحت شبکه آنلاین اجرا کنید.

گام دوم: وضعیت دستگاه را از لیست دستگاه‌ها بررسی کرده و دستگاه غیرفعال را انتخاب کنید.



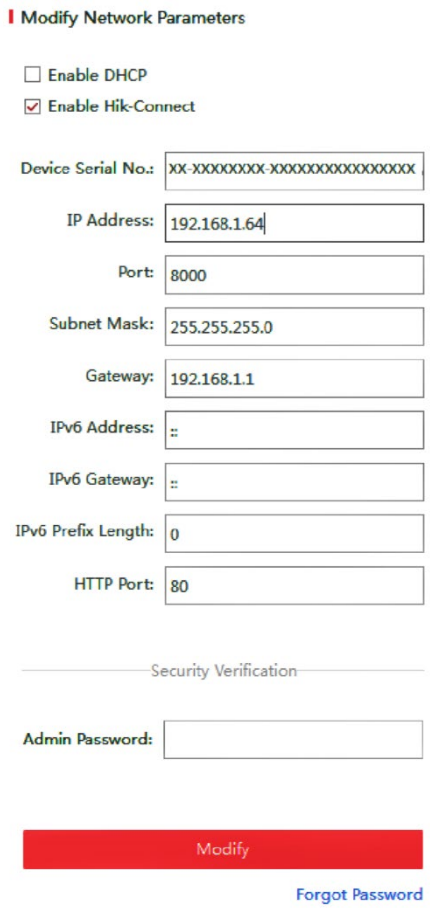
شکل ۲-۲ رابط کاربری SADP

گام سوم: رمز مناسب را ایجاد کرده و در فیلد پسورد وارد کنید. سپس رمز را تأیید کنید.

گام چهارم: برای شروع فعال سازی، روی Activate کلیک کنید.

در پنجره پاپ-آب باز شده، می‌توانید مشاهده کنید که فعال سازی تکمیل شده است یا خیر. در صورت شکست فرایند فعال سازی، مطمئن شوید که رمز شما با الزامات تعیین شده همخوانی داشته و دوباره امتحان کنید.

گام پنجم: با تغییر دادن IP به صورت دستی یا انتخاب تیک گزینه Enable DHCP، IP دستگاه‌ها را به یک سابنت مشترک با کامپیوتر تغییر دهید.



شکل ۲-۳ تغییر آدرس IP

گام ششم: رمز را وارد کرده و برای فعال کردن تغییر IP، روی دکمه Modify کلیک کنید.

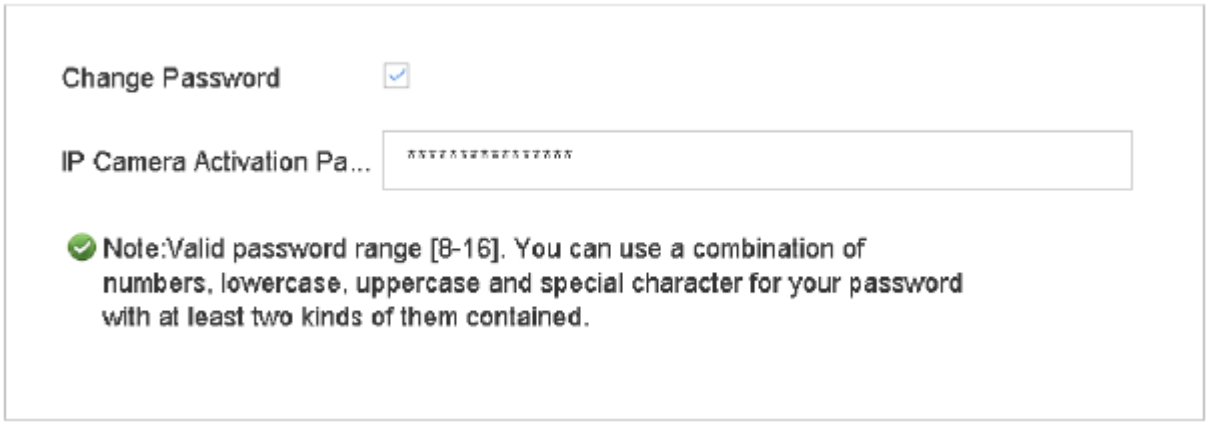
۲.۲ مدیریت دوربین تحت شبکه

زمانی که دستگاه را برای اولین بار فعال می‌کنید، می‌توانید رمز فعال سازی دوربین‌های تحت شبکه را هم تنظیم کنید. برای انجام این کار به فصل ۱.۲ فعال سازی دستگاه با تنظیم یک رمز قوی مراجعه کنید. همچنین، می‌توانید رمز را برای ارتقای امنیت هم مدیریت کنید.

گام اول: مسیر Menu > Maintenance > System Service > IP Camera Activation را طی کنید.

گام دوم: برای فعال کردن مجوز، تیک گزینه Change Password را بزنید.

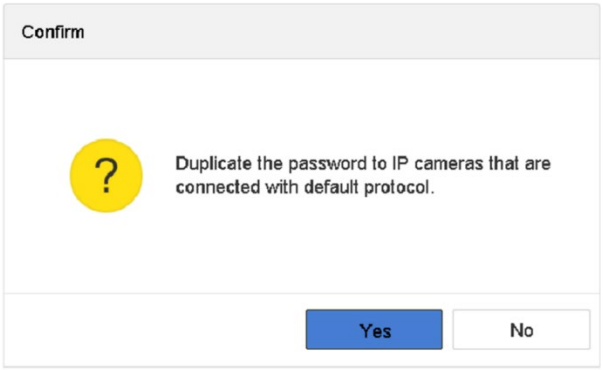
گام سوم: برای به دست آوردن مجوز دسترسی، رمز ادمین دستگاه را وارد کنید.



شکل ۲-۴ تغییر دادن رمز فعال سازی دوربین تحت شبکه

گام چهارم: در فیلد متنی IP Camera Activation Password رمز قوی جدید دوربین‌ها را وارد کنید. برای آشنایی با الزامات رمز قوی، به فصل ۱.۲ امنیت پسورد مراجعه کنید.

گام پنجم: روی Apply کلیک کنید تا کادر زیر باز شود:



شکل ۲-۵ توجه!

گام ششم: جهت استفاده از رمز عبور فعلی برای دوربین‌های تحت شبکه‌ای که با پروتکل پیش فرض متصل شده‌اند، روی Yes کلیک کنید.

۳.۲ امنیت رمز عبور

۱.۳.۲ تنظیمات رمز عبور

الزامات رمز قوی

به شدت توصیه می‌شود که در مراحل فعال سازی دستگاه و تغییر رمز، یک رمز قوی برای دستگاه انتخاب کنید تا امنیت آن افزایش پیدا کند. همچنین، توصیه می‌شود که این رمز را به صورت منظم تغییر دهید. به ویژه در سیستم‌های امنیتی که تغییر ماهیانه یا هفتگی رمز عبور، به حفاظت هر چه بیشتر از آنها کمک می‌کند.

رد شدن رمز عبور اشتباه!!

اگر کاربر ادمین، ۷ بار نام کاربری/رمز عبور را اشتباه وارد کند (که این رقم برای اپراتور/کاربر ۵ بار است)، آدرس IP قفل می‌شود.

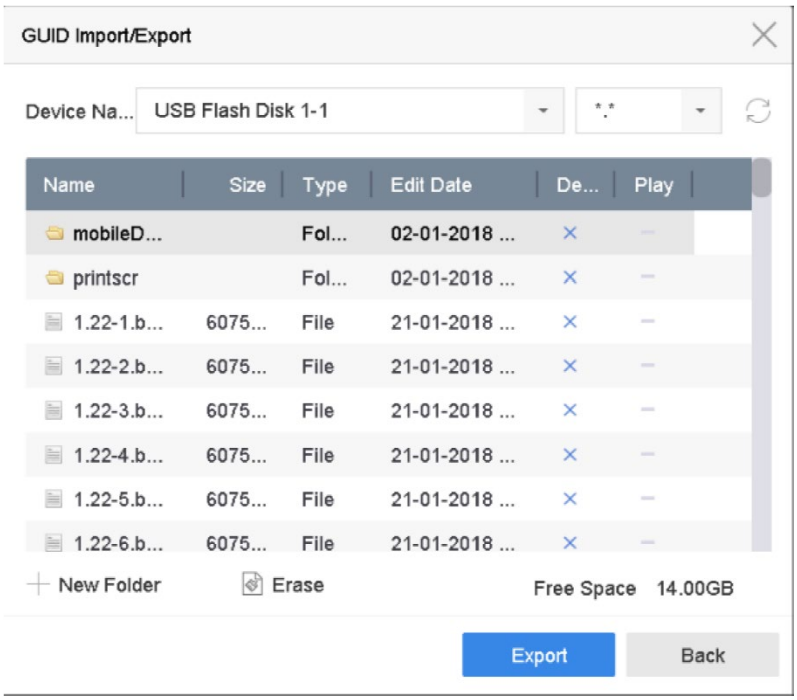
۴.۲ تنظیم امنیت رمز عبور

۱.۴.۲ استخراج فایل GUID

فایل GUID به شما برای ریست کردن پسورد هنگام فراموش کردن آن کمک می‌کند.

گام اول: هنگام فعال سازی دستگاه یا ویرایش حساب کاربری ادمین، گزینه استخراج به فایل GUID را انتخاب کنید.

گام دوم: فلش دیسک U را در دستگاه قرار داده و فایل GUID را روی آن استخراج کنید.



شکل ۲-۶ استخراج فایل GUID

نکته: برای ریست کردن رمزعبوردر آینده از فایل GUID مراقبت کنید.

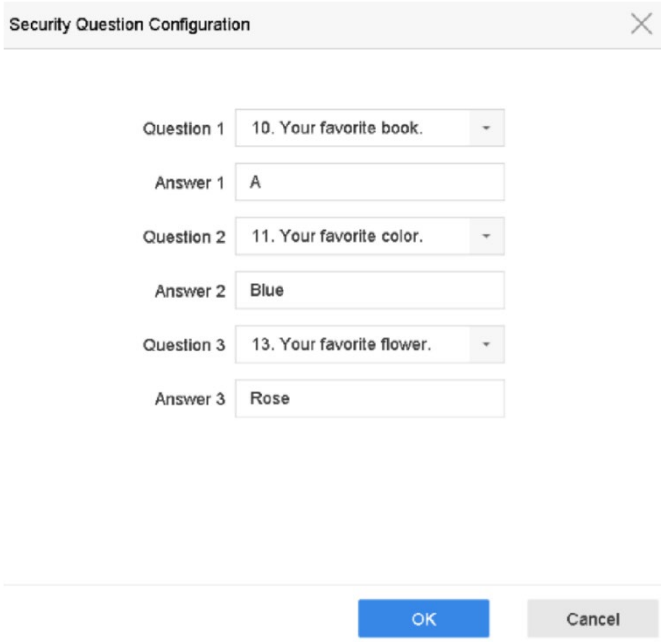
۲.۴.۲ پیکربندی سوالات امنیتی

هنگامی که رمزعبورتان را فراموش کرده یا با مشکلات امنیتی روبرو می‌شوید، پیکربندی سوالات امنیتی به شما برای ریست کردن رمزعبورکمک می‌کند.

گام اول: هنگام فعال سازی دستگاه یا ویرایش حساب کاربری ادمین، روی Security Question Configuration کلیک کنید.

گام دوم: سه سوال امنیتی را از لیست انتخاب کرده و پاسخ‌ها را وارد کنید.

گام سوم: روی OK کلیک کنید.



شکل ۲-۷ پیکربندی سوالات امنیتی

۵.۲ ریست رمزعبور

در صورت فراموش کردن پسورد ادمین، می‌توانید پسورد را با وارد کردن فایل GUID یا پاسخ دادن به سوالات امنیتی ریست کنید.

۱.۵.۲ ریست کردن رمزعبور با GUID

پیش از شروع

پس از فعال سازی دستگاه یا ویرایش حساب کاربری ادمین، باید فایل GUID را استخراج کرده و روی فلش دیسک U ذخیره کنید (به فصل ۱.۴.۲ استخراج فایل GUID مراجعه کنید).

گام اول: در رابط کاربری لاگین، روی Forgot Password کلیک کنید.

گام دوم: نوع ریست رمزعبور را به Verify by GUID تغییر دهید.

نکته:

لطفاً قبل از ریست کردن رمز عبور، فلش دیسک حاوی فایل GUID را در NVR قرار دهید.

گام سوم: فایل GUID را از فلش دیسک انتخاب کرده و برای وارد کردن آن به دستگاه، روی Import کلیک کنید.

نکته:

اگر ۷ بار، فایل GUIE اشتباه را وارد کرده باشید، تا ۳۰ دقیقه اجازه ریست کردن رمزعبور را ندارید.

گام چهارم: پس از وارد کردن فایل GUID، برای تنظیم کردن رمز جدید ادمین وارد رابط کاربری پسورد شوید.

گام پنجم: برای تنظیم رمز جدید، روی OK کلیک کنید. می‌توانید برای ریست کردن رمزعبوردر آینده، فایل GUID جدید را به فلش دیسک وارد کنید.

نکته:

پس از تنظیم رمز جدید، فایل GUID اصلی نامعتبر خواهد شد. برای ریست کردن رمزعبوردر آینده، باید فایل GUID جدید را استخراج کرد. همچنین، می‌توانید برای ویرایش کاربر ادمین و استخراج فایل GUID، وارد رابط کاربری User>User Management شوید.

۲.۵.۲ ریست کردن رمز عبور با استفاده از سوالات امنیتی

باید هنگام فعال سازی دستگاه یا ویرایش حساب کاربری ادمین، سوالات امنیتی را پیکربندی کرده باشید (به فصل ۲.۴.۲ پیکربندی سوالات امنیتی مراجعه کنید)

گام اول: در رابط کاربری لاگین، روی Forgot Password کلیک کنید.

گام دوم: نوع ریست رمزعبور را Verify by Security Question انتخاب کنید.

گام سوم: پاسخ درست سه سوال امنیتی را وارد کنید.

گام چهارم: روی OK کلیک کنید.

نکته:

در صورت تطبیق نداشتن پاسخ‌ها، عملیات اعتبارسنجی با شکست روبرو می‌شود.

می‌توانید در رابط کاربری Reset Password یک رمز جدید برای ادمین تعریف کنید.

۳.۵.۲ لاگ اوت خودکار از منو

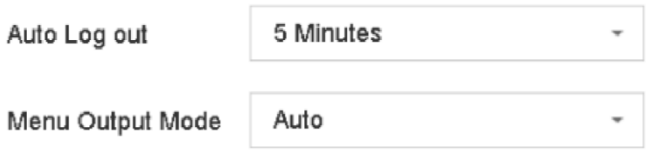
می‌توانید قابلیت لاگ اوت خودکار را تنظیم کنید تا پس از مدتی غیرفعال ماندن، کاربر از سیستم لاگ اوت شود. برای بازیابی عملیات، باید دوباره به سیستم وارد شوید.

گام اول: به مسیر Menu > System > General بروید.

گام دوم: Auto Logout را روی ۱/۲/۵/۱۰/۲۰/۳۰ دقیقه تنظیم کنید.

گام سوم: روی Apply کلیک کنید.

مثال: وقتی زمان خروج خودکار، بر روی ۵ دقیقه تنظیم شده باشد، پس از ۵ دقیقه غیر فعال بودن، سیستم از منوی عملیات جاری وارد صفحه نمایش لایو می‌شود.



شکل ۲-۸. خروج خودکار

فصل سوم مدیریت حساب کاربری

۱.۳ تنظیم مجوزهای کاربر

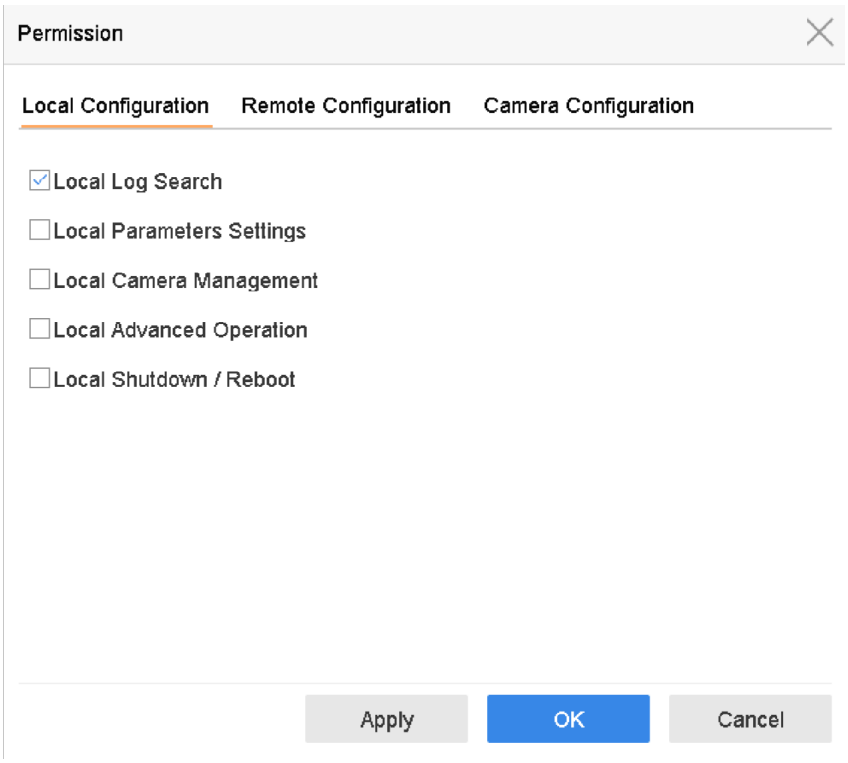
۱.۱.۳ تنظیم مجوزها برای کاربران چند سطحی

حساب کاربری administrator می‌تواند دو سطح حساب کاربری ایجاد کند: اپراتور و مهمان. و می‌توان برای کاربران مختلف، مجوزهای عملیاتی مختلفی را تنظیم کرد. در حالت پیش فرض، کاربران اپراتور و مهمان مجوزهای متفاوتی دارند.

گام اول: وارد مسیر Menu > System > User شوید.

گام دوم: یک کاربر (اپراتور/مهمان) را از لیست انتخاب کنید.

گام سوم: برای ورود به صفحه تنظیمات دسترسی، روی کلیک کنید.



شکل ۳-۱ رابط کاربری تنظیمات دسترسی کاربران

گام چهارم: می‌توانید مجوزهای عملیات پیکربندی محلی، پیکربندی از راه دور و پیکربندی دوربین را برای کاربر تنظیم کنید.

گام پنجم: برای ذخیره تنظیمات، روی OK کلیک کنید.

۲.۱.۳ تنظیم مجوزهای مشاهده تصویر زنده محلی، برای کاربران غیر ادمین

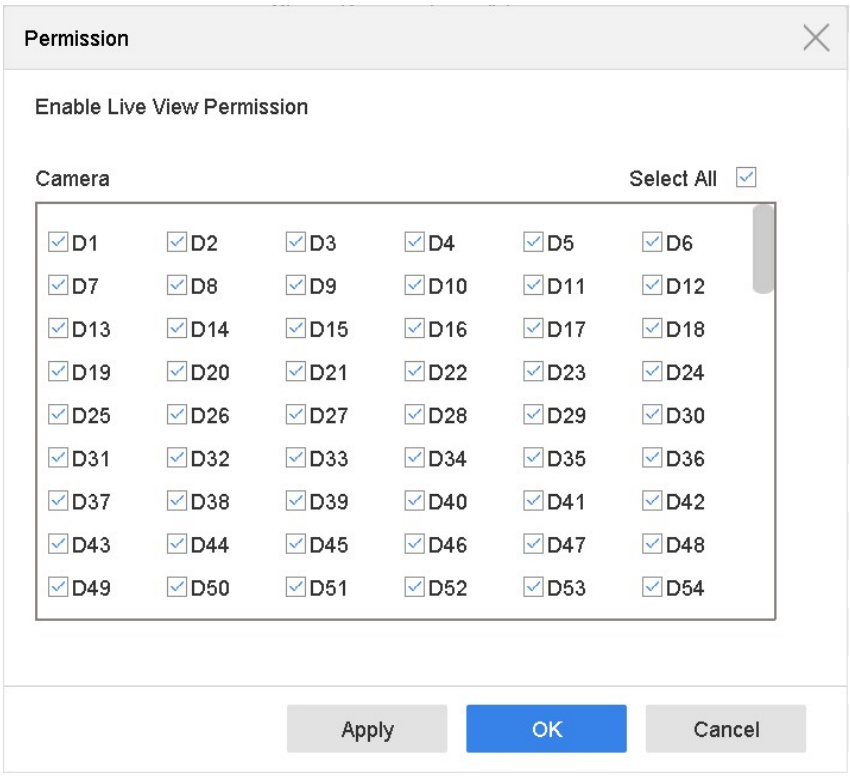
کاربر ادمین، می‌تواند مجوزهای نمایش لایو را برای دوربین‌های خاصی به کاربران معمولی (اپراتور یا مهمان) اختصاص دهد.

گام اول: به مسیر System > User بروید.

گام دوم: روی کاربر ادمین کلیک کنید.

گام سوم: رمز ادمین را وارد کرده و روی OK کلیک کنید.

گام چهارم: دوربین‌هایی را که یک از کاربران غیر ادمین می‌تواند به صورت محلی مشاهده کند، انتخاب کرده و روی OK کلیک کنید.



شکل ۳-۲ تنظیم مجوزهای مشاهده تصویر زنده

گام پنجم: روی کاربر غیر ادمین کلیک کنید.

گام ششم: روی تب Camera Configuration کلیک کنید.

گام هفتم: تنظیمات Camera Permission را به Local Live View تغییر دهید.

گام هشتم: دوربین‌های مورد نظر را برای نمایش پخش زنده انتخاب کنید.

گام نهم: روی OK کلیک کنید.

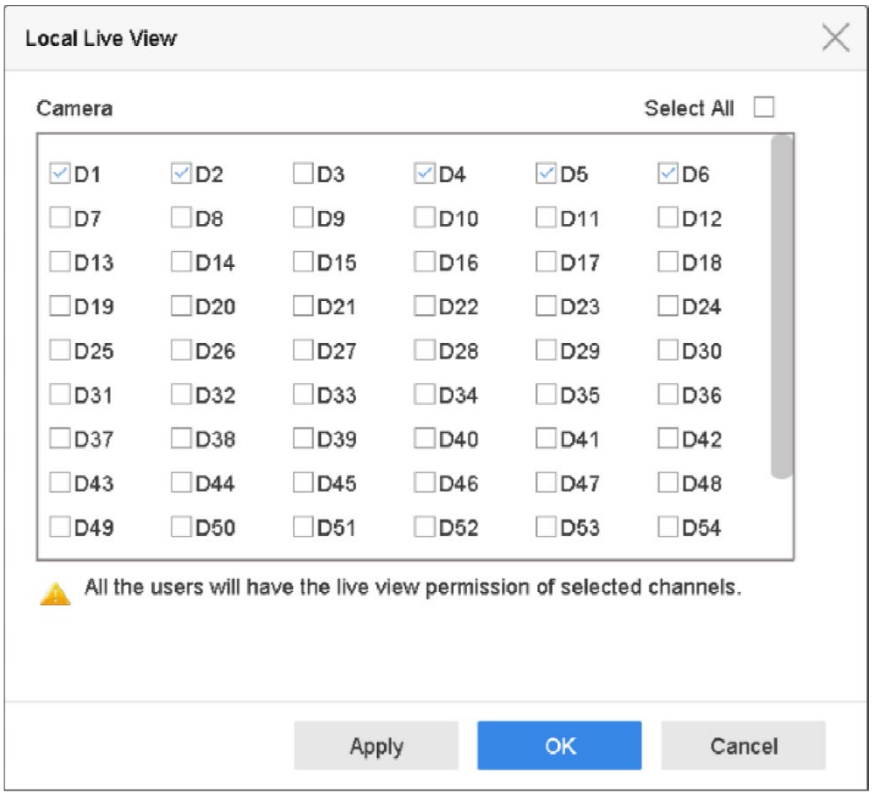
۳.۱.۳ تنظیم مجوزهای نمایش زنده در صفحه قفل

کاربر ادمین می‌تواند مجوزهای نمایش زنده را برای دوربین‌هایی خاص در صفحه قفل دستگاه تعیین کند.

گام اول: به مسیر System > User بروید.

گام دوم: روی Live View Permission on Lock Scree کلیک کنید.

گام سوم: پسورد ادمین را وارد کرده و روی Next کلیک کنید.



شکل ۳-۳ تنظیم مجوزهای نمایش زنده

گام چهارم: تنظیم مجوزها

- دوربین‌هایی را که مایل هستید کاربر جاری در وضعیت لاگ اوت بتواند تصویر زنده آنها را مشاهده کند، انتخاب کنید.
- دوربین‌هایی را که مایل نیستید کاربر جاری بتواند در وضعیت لاگ اوت تصویر زنده آنها را مشاهده کند، از حالت انتخاب خارج کنید.

گام پنجم: روی OK کلیک کنید.

نکته:

- کاربر ادمین می‌تواند این مجوزها را برای حساب‌های کاربری تنظیم کند.
- وقتی کاربر معمولی (اپراتور یا مهمان) مجوز نمایش زنده محلی را برای دوربین‌هایی خاص نداشته باشد (به بخش ۲.۱.۳ تنظیم مجوزهای نمایش زنده محلی برای کاربران غیر ادمین مراجعه کنید)، نمی‌توان مجوز نمایش تصویر زنده چنین دوربین‌هایی را برای صفحه قفل تنظیم کرد (در حالت پیش فرض، امکان مشاهده تصویر زنده وجود ندارد).

۲.۳ حذف کاربر غیرفعال

توصیه می‌کنیم که در صورت وجود حساب‌های کاربری غیرفعال روی دستگاه، برای پیشگیری از اجرای یکسری عملیات غیرضروری، چنین حساب‌هایی را به صورت منظم حذف کنید.

گام اول: به مسیر Menu > System > User بروید.

گام دوم: یک کاربر را برای حذف از لیست انتخاب کنید.

شکل ۳-۴ فهرست کاربران

گام سوم: برای حذف حساب کاربری انتخاب شده، روی Delete کلیک کنید.

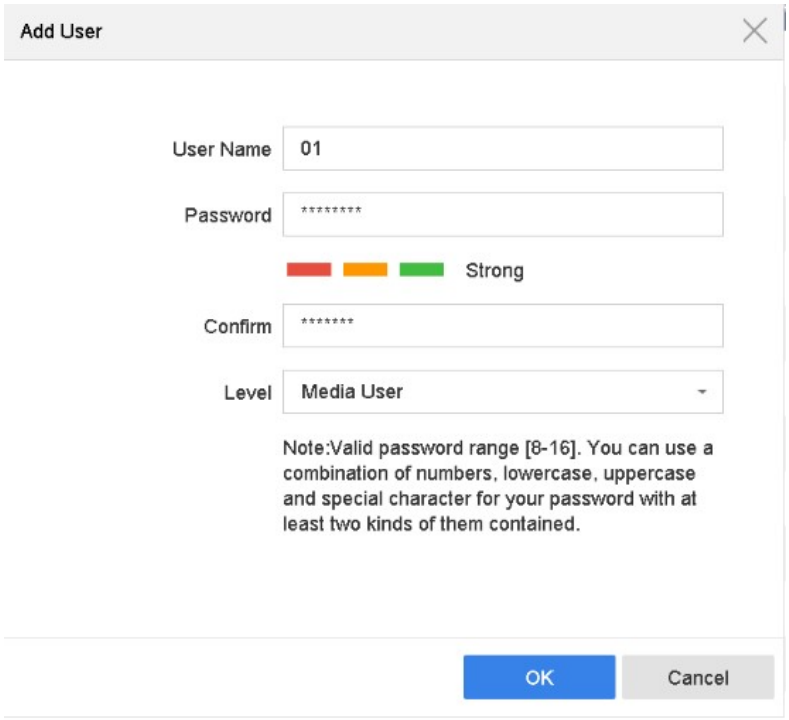
۳.۳ انتقال حساب‌های کاربری ONVIF

برای اتصال دوربین شخص ثالث به دستگاه از طریق ONVIF، می‌توانید این قابلیت را فعال کرده و حساب‌های کاربری را مدیریت کنید.

گام اول: به مسیر Menu > Maintenance > System Service > ONVIF بروید.

گام دوم: برای فعال کردن مدیریت دسترسی ONVIF روی Enable ONVIF کلیک کنید.

گام سوم: برای ورود به صفحه Add User روی Add کلیک کنید.



شکل ۳-۵ اضافه کردن کاربر

گام چهارم: نام کاربری را ویرایش کرده و یک رمز قوی وارد کنید.

گام پنجم: سطح کاربر را انتخاب کنید (Media User، Operator، Admin).

گام ششم: برای ذخیره تنظیمات روی OK کلیک کنید.

نتیجه: حساب‌های کاربری اضافه شده، مجوز اتصال سایر دستگاه‌ها به DVR/NVR را از طریق پروتکل ONVIF دارند.

نکته:

پروتکل ONVIF در حالت پیش فض غیرفعال است.

فصل چهارم کنترل دسترسی از راه دور

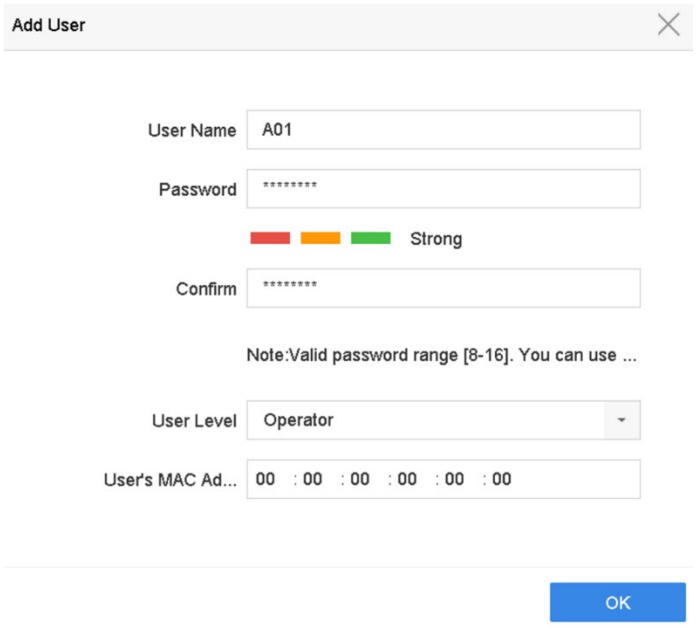
۱.۴ تنظیم مک آدرس کاربر

مک آدرس کاربر، در واقع مک آدرس کامپیوتر راه دوری است که به دستگاه ورود می‌کند. در صورت پیکربندی و فعال کردن این گزینه، فقط کاربر راه دوری با همین مک آدرس تایید شده اجازه دسترسی به دستگاه را خواهد داشت.

گام اول: به مسیر Menu > Configuration > User بروید.

گام دوم: برای ورود به صفحه Add User روی Add کلیک کنید.

گام سوم: اطلاعات کاربر جدید از جمله نام کاربری، رمز ادمین، رمز تأیید، سطح و مک آدرس کاربر را وارد کنید.



شکل ۴-۱ منوی اضافه کردن کاربر و مک آدرس

گام چهارم: برای ذخیره تنظیمات روی OK کلیک کنید.

۲.۴ قفل کردن دسترسی غیرمجاز

در صورت ۷ بار تلاش ناموفق برای وارد کردن نام کاربری/ رمز عبور ادمین (که این رقم برای اپراتور/ کاربر ۵ بار است)، حساب کاربر قفل خواهد شد.

نکته:

در صورت قفل شدن حساب کاربر، می‌توانید حدود ۳۰ دقیقه بعد، دوباره برای ورود به دستگاه تلاش کنید.

فصل پنجم سرویس‌های سیستمی

۱.۵ حذف سرویس‌ها

سرویس‌ها و قابلیت‌های زیر برای حفظ امنیت شبکه حذف شده‌اند

- Telnet
- سرور PSIA
- دسترسی PSIA IPC
- SSH

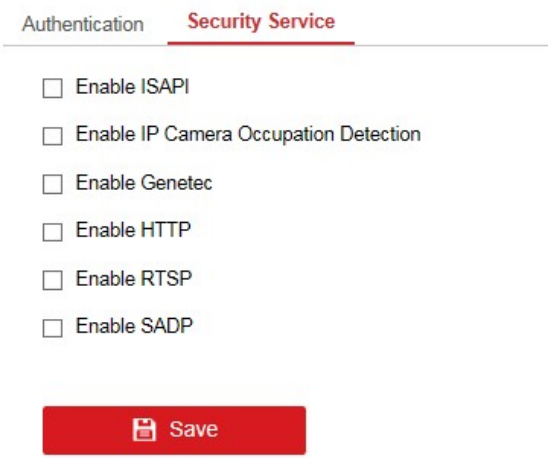
۲.۵ غیرفعال سرویس‌ها

می‌توانید برای ارتقای امنیت دسترسی، مثلاً در مواقعی که در محیط شبکه‌ای غیرقابل اطمینان قرار دارید، قابلیت‌های زیر را غیرفعال کنید.

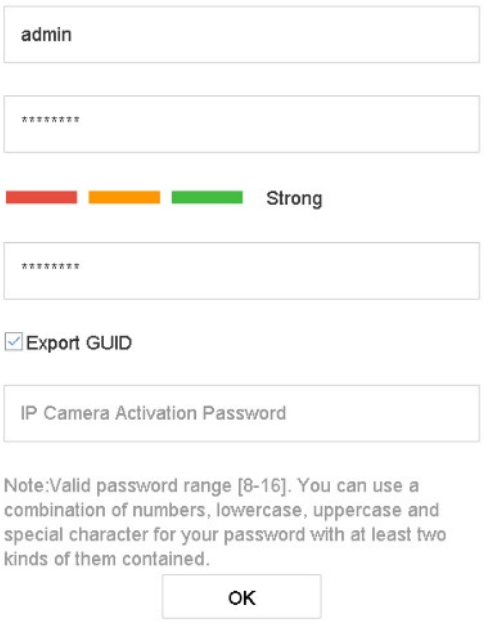
- Multicast
- Genetec
- ISAPI[1]
- SADP

گام اول: از GUI محلی به مسیر Menu > Maintenance > System Service رفته یا از مرورگر وب وارد مسیر Configuration > System > Security > Authentication شوید.

[1] Internet Server Application Program Interface



شکل ۵-۱ غیرفعال کردن سرویس‌ها (مرورگر وب)



شکل ۵-۲ غیرفعال کردن سرویس‌ها (GUI محلی)

گام سوم: برای غیرفعال کردن سرویس‌ها، تیک گزینه Enable Genetec/Enable ISAPI/Enable SAD را بردارید.

HTTPS ۳.۵

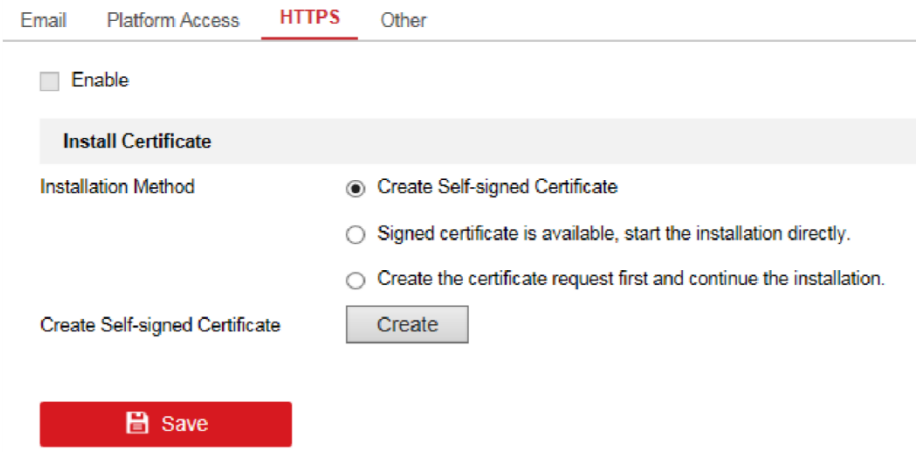
HTTPS برای احراز هویت سایت‌ها و سرورهای وب آنها کاربرد دارد و از کاربران در برابر حملات مرد میانی حفاظت می‌کند.

برای تنظیم شماره پورت HTTPS، مراحل زیر را طی کنید.

نکته: اگر شماره پورت را ۴۴۳ تنظیم کردید و آدرسIP ۱۹۲.۱۶۸.۱.۶۴ است، می‌توانید با تایپ کردن آدرس https://192.168.1.64:443 از طریق مرورگر وب، به دستگاه دسترسی پیدا کنید.

گام اول: (از مرورگر وب) به مسیر Configuration > Network > Advanced Settings > HTTPS بروید.

گام دوم: برای فعال کردن این قابلیت، تیک گزینه Enable را بزنید.



شکل ۵-۳ صفحه پیکربندی HTTP

گام سوم: گواهینامه اعطاء شده یا خود امضاء شده (self-signed) را ایجاد کنید.

- ایجاد گواهینامه self-signed

۱. روش نصب را Create Self-signed Certificate انتخاب کنید.
۲. برای ورود به صفحه ایجاد گواهینامه، روی Create کلیک کنید.

شکل ۵-۴ ایجاد گواهینامه Self-signed

۳. کشور، نام میزبان/IP، اعتبار و سایر اطلاعات را وارد کنید.
۴. برای ذخیره تنظیمات روی OK کلیک کنید.

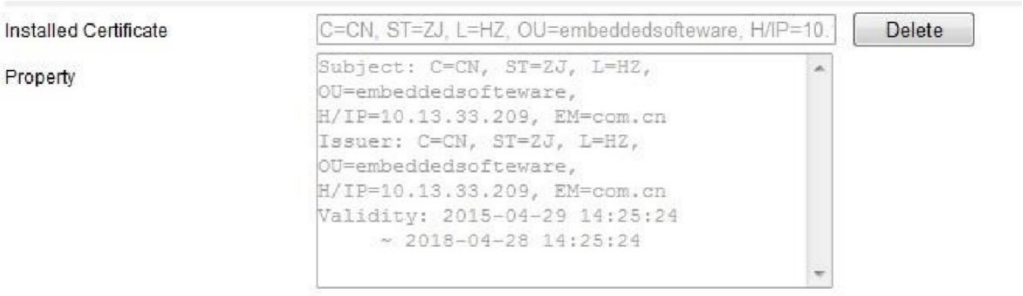
نکته:

اگر از قبل یک گواهینامه نصب شده باشد، گزینه Create Self-signed Certificate غیرفعال (خاکستری رنگ) خواهد بود.

- ایجاد گواهینامه اعطاء شده

۱. گزینه Create the certificate request first and continue the installation را به عنوان روش نصب انتخاب کنید.
۲. برای ایجاد درخواست گواهینامه، روی Create کلیک کنید. در پنجره باز شده، اطلاعات لازم را وارد کنید.
۳. درخواست گواهینامه را دانلود کرده و آن را برای امضاء به مرجع صدور گواهینامه ارسال کنید.
۴. پس از دریافت گواهینامه امضاء شده معتبر، آن را به دستگاه وارد (import) کنید.

گام چهارم: پس از ایجاد و نصب گواهینامه، اطلاعات آن قابل مشاهده خواهد بود.



شکل ۵-۵ گواهینامه نصب شده

گام پنجم: برای ذخیره تغییرات روی Save کلیک کنید.

HTTP ۴.۵

می‌توانید HTTP را غیرفعال کنید یا برای ارتقای سطح امنیت دسترسی، مشخص کنید که احرازهویت HTTP چه موقع فعال شود.

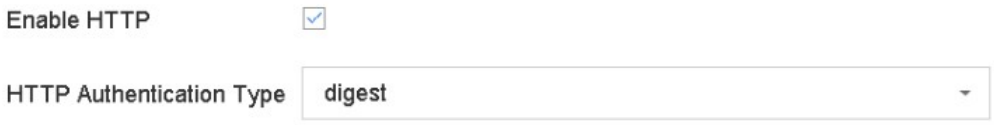
نکته:

در حالت پیش فرض، سرویس HTTP فعال است.

تنظیم احرازهویت HTTP

اگر نیاز به فعال سازی سرویس HTTP دارید، می‌توانید برای ارتقای امنیت احرازهویت HTTP را فعال کنید.

گام اول: از GUI محلی وارد مسیر Menu > Maintenance > System Service شده یا از مرورگر وب وارد مسیر Configuration > System > Security > Authentication شوید.



شکل ۵-۶ احرازهویت HTTP

گام دوم: برای فعال کردن سرویس HTTP روی Enable HTTP کلیک کنید.

گام سوم: در لیست دراپ-داون، نوع digest را برای HTTP Authentication انتخاب کنید.

گام چهارم: برای ذخیره تنظیمات، روی Save کلیک کنید.

نکته:

انواع احرازهویت قابل انتخاب شامل digest و digest/basic هستند. به دلایل امنیتی، توصیه می‌شود که نوع احرازهویت را digest انتخاب کنید.

غیرفعال کردن HTTP

حساب کاربری ادمین می‌تواند سرویس HTTP را از مرورگر تحت وب یا GUI غیرفعال کند.

پس از غیرفعال کردن HTTP، همه سرویس‌های مرتبط به آن از جمله HTTP، UPnP، ISAPI، Onvif و Gennetc هم خاتمه پیدا می‌کنند.

گام اول: از GUI محلی وارد مسیر Menu > Maintenance > System Service شده یا از مرورگر وب وارد مسیر Configuration > System > Security > Authentication شوید.

گام دوم: برای غیرفعال کردن سرویس HTTP تیک گزینه Enable HTTP را بردارید.

۵.۵ احرازهویت وب / RTSP

می‌توانید با تنظیم احرازهویت وب و RTSP، جریان داده‌های تصویر لایو را ایمن سازی کنید.

گام اول: از GUI محلی وارد مسیر Menu > Maintenance > System Service شده یا از مرورگر وب وارد مسیر Configuration > System > Security > Authentication شوید.

شکل ۵-۷ احرازهویت RTSP (GUI محلی)

شکل ۵-۸ احرازهویت RTSP (مرورگر وب)

گام دوم: نوع احراز هویت را انتخاب کنید.

- از لیست دراپ-داون، نوع RTSP Authentication را digest انتخاب کنید.
- از لیست دراپ-داون، نوع Web Authentication را digest انتخاب کنید.

نکته:

انواع احرازهویت قابل انتخاب شامل digest و digest/basic هستند. اگر گزینه digest را به عنوان احرازهویت RTSP انتخاب کنید، فقط درخواست‌هایی با احرازهویت digest قابلیت دسترسی به جریان ویدیوی ارسال شده با پروتکل RTSP از طریق آدرس آی‌پی را دارند. به دلایل امنیتی، توصیه می‌شود که نوع احرازهویت را، digest انتخاب کنید.

گام سوم: برای ذخیره تنظیمات، روی Save کلیک کنید.

۶.۵ غیرفعال کردن UPnP

UPnP[2] یک معماری شبکه است که امکان سازگاری دستگاه‌ها، نرم‌افزارها و انواع تجهیزات سخت‌افزاری را فراهم می‌کند. پروتکل UPnP به دستگاه‌ها امکان می‌دهد که به صورت روان و بی وقفه با یکدیگر ارتباط برقرار کنند و پیاده سازی شبکه‌ها را در محیط‌های شرکتی و خانگی آسان‌تر می‌کند.

گام اول: از GUI محلی وارد مسیر Menu > Maintenance > System Service شده یا از مرورگر وب وارد مسیر Configuration > Network > Basic Settings > NAT شوید.

گام دوم: برای غیرفعال کردن قابلیت UPnP، تیک گزینه Enable UPnP را بردارید.

۷.۵ غیرفعال کردن Control4

پروتکل Control4 امکان جستجوی دستگاه‌های هایک ویژن از طریق SDDP، دریافت پارامترهای ساده شبکه، اطلاعات دستگاه و یا دسترسی به بعضی از عملیات مربوط به دستگاه را فراهم می‌کند.

[2] Universal Plug and Play

گام اول: وارد مسیر Menu > Maintenance > System Service > More Settings > Control4 شوید.

گام دوم: تیک گزینه Enable SDDP و Enable CGI را بردارید.

گام سوم: روی Apply کلیک کنید.

۸.۵ غیرفعال کردن گزارش دهی I-VIEW-NOW UPNP

سرویس گزارش دهی I-VIEW-NOW UPNP به سیستم امکان می‌دهد که پارامترهای شبکه دستگاه را از طریق ایمیل برای دریافت کننده‌های مجاز ارسال کند.

گام اول: وارد مسیر Menu > Maintenance > System Service > More Settings > I-VIEW-NOW UPNP Reporting شوید.

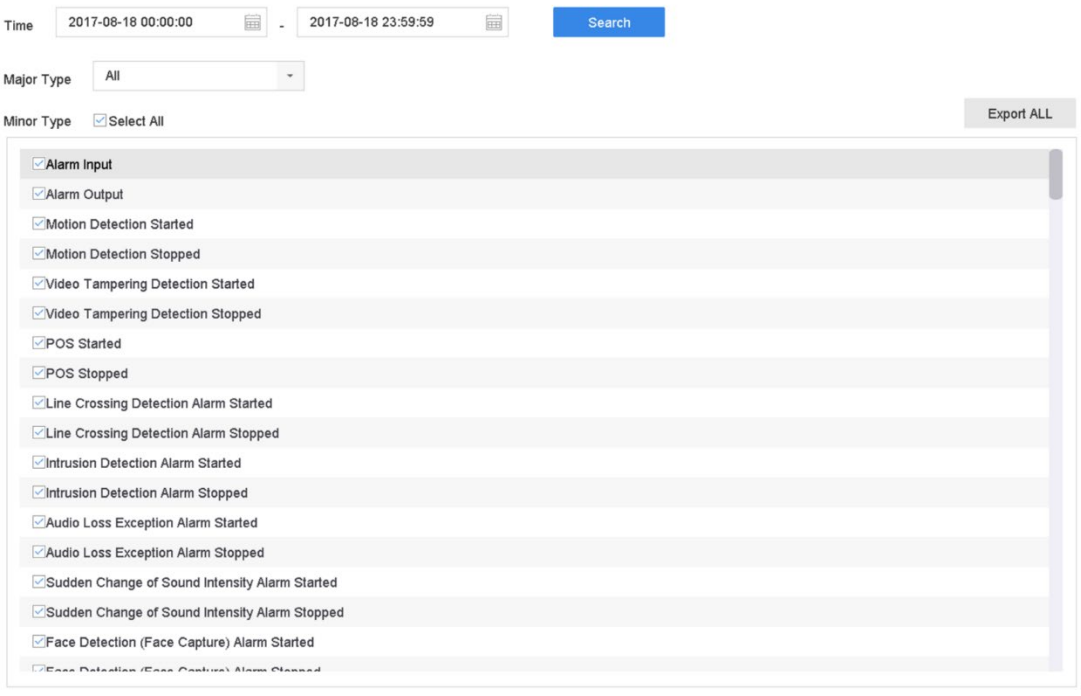
گام دوم: تیک گزینه I-VIEW-NOW UPNP Reporting را بردارید.

گام سوم: روی Apply کلیک کنید.

فصل ششم لاگ‌های سیستم

سیستم، اطلاعات دستگاه، عملیات، هشدارها و استثناءها را در فایل‌های لاگ ذخیره می‌کند که می‌توان آنها را در هر زمان دلخواهی مشاهده و استخراج کرد. می‌توانید برای نظارت بر امنیت سیستم، لاگ‌ها را به صورت منظم بررسی و استخراج کنید.

گام اول: وارد مسیر Menu > Maintenance > Log Information شوید.

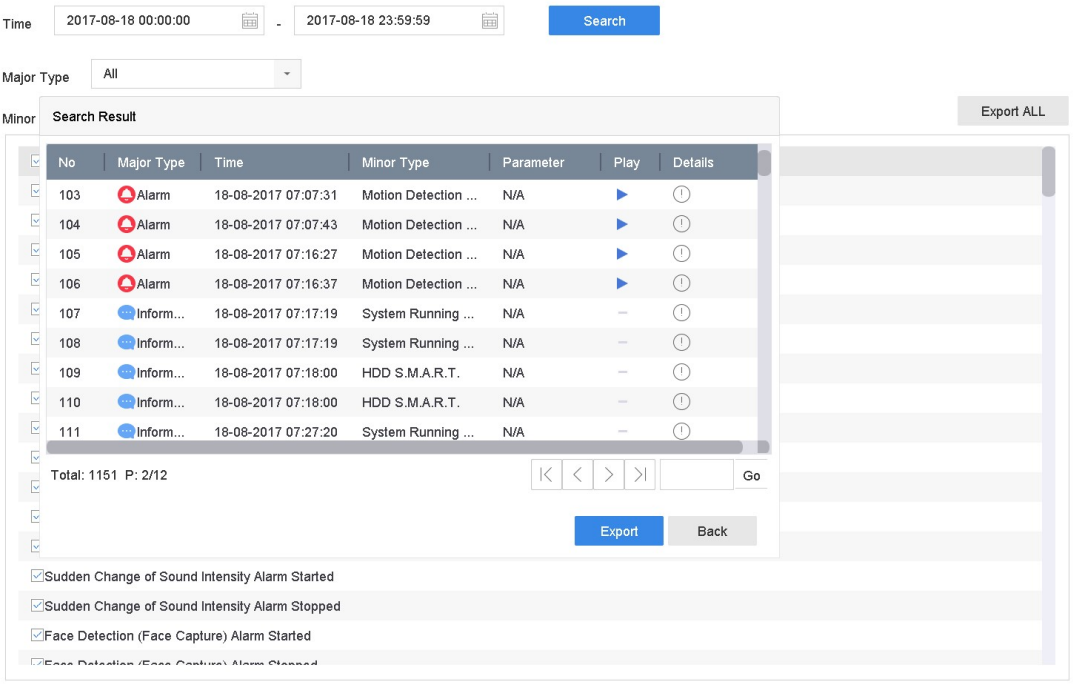


شکل ۶-۱ جستجوی لاگ

گام دوم: شرایط جستجوی لاگ از جمله زمان، نوع اصلی و نوع فرعی را مشخص کنید.

گام سوم: برای شروع جستجوی فایل‌های لاگ، روی Search کلیک کنید.

همانطور که در تصویر زیر مشاهده می‌کنید، فایل‌های لاگ تطبیق یافته نمایش داده می‌شوند.



شکل ۶-۲ نتایج جستجوی لاگ

نکته:

هر بار حداکثر ۲۰۰۰ فایل لاگ نمایش داده می‌شود.

عملیات مرتبط:

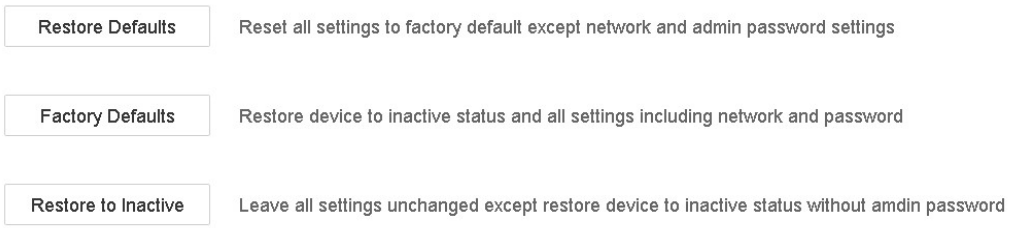
- روی دکمه کلیک یا دابل کلیک کنید تا اطلاعات جامع آن را ببینید.
- برای مشاهده فایل ویدیویی مربوطه، روی دکمه کلیک کنید.

فصل هفتم ارتقاء و بازیابی تنظیمات سیستم

در مواقعی که ریسک امنیتی برای شبکه وجود دارد، بهتر است دستگاه را ارتقاء داده یا تنظیمات پیش فرض را بازیابی کنید.

۱.۷ بازیابی تنظیمات پیش فرض

گام اول: وارد مسیر Menu > Maintenance > Default شوید.



شکل ۷-۱ بازیابی تنظیمات پیش فرض

گام دوم: نوع بازیابی را بر اساس گزینه‌های زیر انتخاب کنید:

بازیابی تنظیمات پیش فرض (Restore Defaults): این گزینه همه پارامترها را به غیر از پارامترهای حساب کاربری و شبکه (از جمله آدرس آی‌پی، ماسک ساب‌نت، درگاه، MTU، حالت کاری NIC، مسیر پیش فرض، پورت شبکه و غیره) به تنظیمات پیش فرض کارخانه برمی‌گرداند.

تنظیمات پیش فرض کارخانه (Factory Defaults): این گزینه همه پارامترها را به تنظیمات پیش فرض کارخانه برمی‌گرداند.

برگشت به حالت غیرفعال (Restore to Inactive): این گزینه دستگاه را به وضعیت غیرفعال برمی‌گرداند.

گام سوم: برای برگشتن به تنظیمات پیش فرض، روی OK کلیک کنید.

۲.۷ ارتقای سیستم

همیشه برای دریافت همه آپدیت‌های امنیتی، از جدیدترین نسخه میان‌افزار استفاده کنید. می‌توانید سیستم را از طریق GUI محلی، مرورگر وب یا نرم‌افزار کلاینت به روزرسانی نمایید.

پایان

HIKVISION®

See Far, Go Further

پارس ارتباط
گارانتی

PARS ERTEBAT
پارس ارتباط

با ۲۴ مـاه گارانتی
پارس ارتباط افزار

tp-link MikroTik TELTONIKA QNAP HUAWEI

PLANET Networking & Communication | Hewlett Packard Enterprise | ASUS | SEAGATE | WD Western Digital

HARES | HIKVISION | dahua | HiLook | Teledataone

ASENWARE | AUS electronics | Alcatel·Lucent Enterprise | BenQ

دفتر مرکزی: تهران، خیابان ولیعصر، خیابان زعفرانیه، خیابان اعجازی، ساختمان ۳۹

مرکز آموزش و خدمات پس از فروش: تهران، خیابان شهید بهشتی، خیابان سرافراز، کوچه سوم، ساختمان ۱۲

کارخانه: شهر قدس، شهرک صنعتی زاگرس، خیابان صنعت، کوچه صنایع یکم، پلاک ٤

تلفن: ۸۹۳۹۵ ۰۲۱ **فکس:** ۸۹۳۹۵ ۰۲۱ (داخلی ۰) **ایمیل:** info@pars-e.com

www.pars-e.com pars.ertebat.afzar parsertebatchannel pars ertebat afzar