شرکت پردازش تصویر کمان

www.kaman.ir

پیوست الزامات امنیتی

سامانه های نظارت تصویری

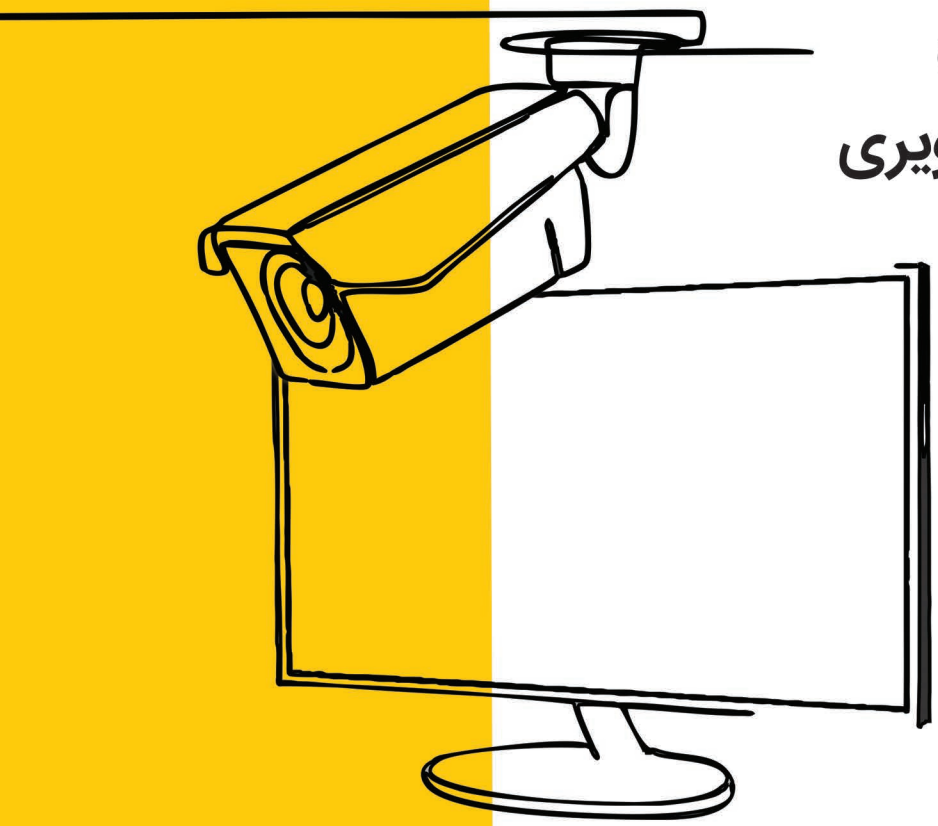
با کمان هدف در تیررس شماست

support@kaman.ir

V1.00

خرداد ۱۴۰۲

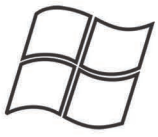
پیوست الزامات امنیتی سامانه های نظارت تصویری



نصب هر نرم افزاری مستلزم انجام یکسری اقدامات اولیه ست. در نرم افزارهای نظارت تصویر به دلیل ماهیت امنیتی شان این اقدامات بیشتر از هر نرم افزاری اهمیت دارند. نرم افزار شیردال به عنوان یک نرم افزار تخصصی نظارت و پایش تصاویر دوربین های مداربسته از این قاعده مستثنی نیست و با توجه به ساختار کلاینت و سروری آن توجه همه جانبه در نصب وراه اندازی آن ضروری است.

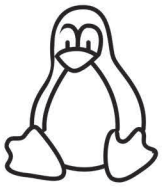
برای راه اندازی نرم افزار شیردال لازم است هم در سیستم عامل لینوکس به عنوان سرور و هم در سیستم عامل ویندوز و همچنین در شبکه دوربین ها اقداماتی به منظور امن سازی بیشتر انجام گیرد. در این سند برای هریک از این موارد راهکارهایی ارائه شده است.

امن سازی ویندوز



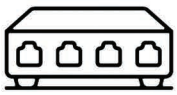
برای امن سازی سیستم عامل ویندوز مهمترین اصل انتخاب پسورد پیچیده ست. برای اینکار باید کاربر الزام به انتخاب رمز عبور پیچیده ای شود که دوره انقضا هم داشته باشد. برای این کار از پیوست یک استفاده کنید.

امن سازی سیستم عامل لینوکس



لینوکس به عنوان سیستم عامل سرور شیردال نقشی اساسی در یک پروژه نظارت تصویری مبتنی بر نرم افزار شیردال ایفا می کند. هرچند بنا بر ماهیت لینوکس و همچنین جداسازی شبکه دوربین و سرور تا حد زیادی می توان از حملات نفوذ جلوگیری کرد ولی به عنوان یک راهکار عمومی استفاده از یک رمز عبور پیچیده و با طول کاراکتر مناسب می توان از بیشتر حملات و آسیب ها جلوگیری کرد. این کار به هنگام نصب نرم افزار به صورت پیش فرض انجام می شود.

شبکه



شبکه ارتباطی یک پروژه نظارت تصویری به عنوان شریان اصلی ارتباطی که تمام اجزای سیستم را به هم وصل می کند نقشی حیاتی در امنیت و آسیب پذیری ایفا می کند. انتخاب یک توپولوژی مناسب می تواند با هزینه اندکی می توان بخش بزرگی از حملات نفوذ را خنثی کرد. با عنایت به این موضوع که یک گره شبکه می تواند به عنوان پلی برای نفوذ استفاده شود، توجه به نحوه پیکربندی و همچنین اجرای شبکه از اصلی ترین دغدغه های یک مدیر نظارت تصویری به حساب می آید. استفاده از سوئیچ های با قابلیت مدیریت برای جداسازی ترافیک دوربین ها از ترافیک کلاینت ها و همچنین هدایت ترافیک دوربین به سمت سرور مشخصی می تواند از بروز آسیبهای امنیتی تا حد زیادی جلوگیری کند.

دوربین

دوربین به عنوان نقطه شروع یک شبکه نظارت تصویری همواره مورد تهدید نفوذگران قرار دارد. از آنجایی که تنوع برند و مدل دوربین ها بسیار زیاد است همین امر در کنار مزایایی که دارد، دوربین را به عنوان یکی از دریچه های نفوذ به سیستم تبدیل کرده است. بهترین و اصلی ترین روش انتخاب یک رمز عبور با پیچیدگی زیاد و همچنین تغییر آن به صورت دوره ای است. استفاده از پیکربندی مبتنی بر vlanهای مختلف برای ارتباط دوربین ها با سرورها نیز از مواردی است که در نصب و راه اندازی سیستم نظارت تصویری توصیه می شود.

این پیوست به منظور یادآوری نکات امنیتی در ساختارهای نظارت تصویری در سازمان ها برای مشتریان این شرکت تهیه و ارسال شده است.
رعایت این نکات برای مشتریان ضروری می باشد.

۱ استفاده از زیر ساخت ارتباط کابلی/سیمی در ارتباطات بین تجهیزات نظارت تصویری به عنوان مطمئن ترین راه حل، و در صورت ضرورت در استفاده از ارتباطات بی سیم از مکانیزم های امنیتی رمزنگاری قوی TLS/AES شیردال استفاده شود و همچنین اعمال سیاستهای محدود سازی دستگاههای مجاز به شبکه از طریق لیست آی پی های مجاز، فیلترینگ Mac آدرس و ....

۲ استفاده از رمز نگاری TLS/AES در مبادی ذیربط انتقال اطلاعات، و همچنین استفاده از تجهیزاتی که از طریق پروتکل های رمزنگاری در مبدا" و مقصد اطلاعات و داده ها عمل می نمایند.

۳ حتی المقدور شبکه نظارت تصویر سازمان بصورت فیزیکی از شبکه های دیگر سازمان جدا شوند، و در غیر اینصورت با VLAN بندی از سایر شبکه های سازمانی جداسازی انجام شود.

۴ استفاده از مشاورین معتبر برای تست های نفوذ در شبکه و تجهیزات سازمان و رفع عدم انطباق ها در شبکه

۵ اعمال محدودیت و بسته شدن در پورت های ورودی و خروجی تجهیزات و ایجاد VPN های مورد اطمینان برای دسترسی ها و ارتباطات راه دور و فقط در صورت ضرورت

۶ رعایت استانداردهای امنیتی در کابل گذاری ها و نصب تجهیزات شبکه از لحاظ سهولت دسترسی فیزیکی به آنها

۷ استقرار و جانمایی دوربین ها با لحاظ شدن پوشش یکدیگر ساختار حفاظت فیزیکی

۸ پایش عملکرد شبکه و تجهیزات آن و استفاده از نرم افزارهای پایش شبکه و اعمال هشدارها در صورت بروز حوادث و یا وقایع غیر متداول از جمله تکرار دسترسی های غیر مجاز و یا .....

۹ ایجاد بک آپ لازم در صورت ایجاد بحران در شبکه برای استمرار سرویس نظارت تصویری

۱۰ بروز نگهداری نرم افزارهای شبکه و عدم استفاده از نسخ غیر قابل اطمینان و کرک شده

۱۱ استفاده از تجهیزات معتبر و آزمایش پس داده و دارای مجوز و پرهیز از برخی از دستگاههای نامشخص و یا مشکوک

۱۲ تامین برق اضطراری برای مواقع قطعی حداقل ۲ تا ۳ ساعت

۱۳ بروزرسانی دائم سیستم عامل لینوکس در سرورها و ویندوز برای کلاینت ها و firmware دوربین ها و تجهیزات شبکه

۱۴ بازنگری دوره ای در تعریف کاربران و اعمال سیاست های تغییر کلمه عبور کاربران در دوره های زمانی مشخص.

۱۵ توجه به نام و کلمه عبور دوربین ها و یا تجهیزات تازه استقرار یافته و تغییر دوره ای آنها با سیاست های کلمه عبور قوی و مطمئن

۱۶ فعالسازی تمپرینگ دوربین ها و اعلام هشدار سامانه در صورت قطعی سامانه و شبکه

۱۷ حفظ کلمه عبور و نام دوربین ها در محلی مطمئن و دور از دسترس و اعمال سیاست مشخص برای یک فرد از حفاظت از آن در سازمان و عدم در اختیار گذاری بی رویه آن به افراد دیگر.

۱۸ انجام آزمون های دوره ای تست نفوذ و ارزیابی امنیتی با استفاده از توانمندی مشاورین ذیصلاح

۱۹ استفاده از وقایع تاریخچه ای نرم افزار نظارت تصویری(لاگ ها) و بررسی آنها برای مدیریت دسترسی ها

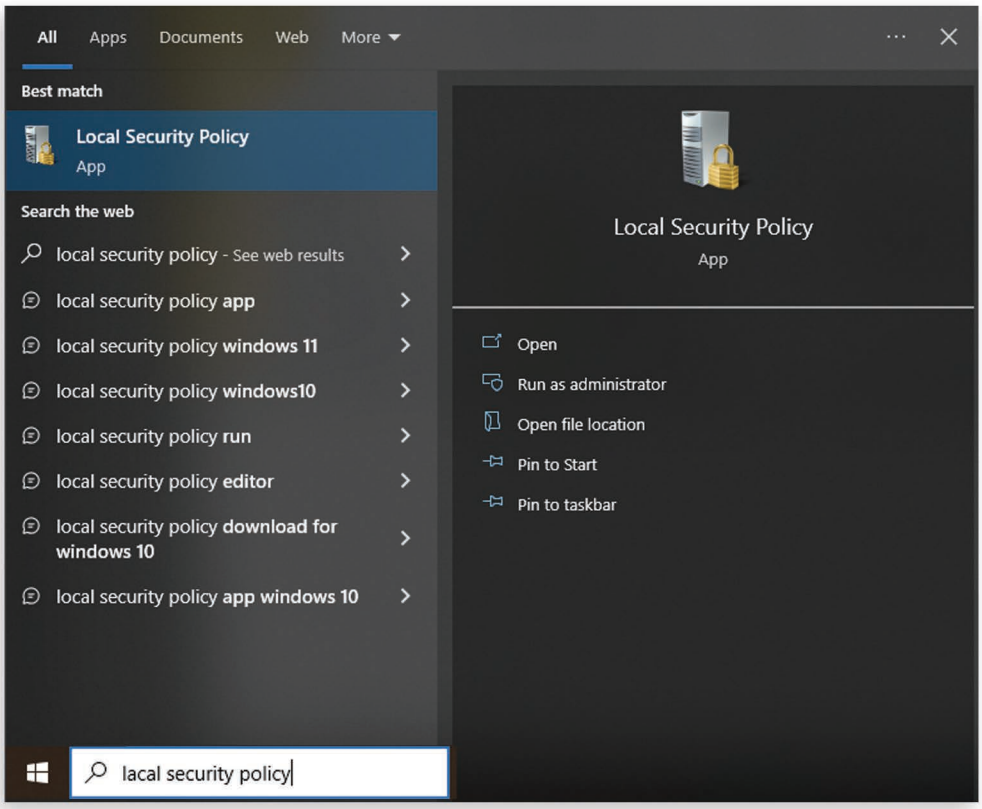
۲۰ حفظ و نگهداری تنظیمات مدیریت سامانه نرم افزاری شیردال برای بازیابی سریع دوربین ها در کلاینت ها و سرور در کوتاه ترین زمان ممکن

پیوست ۱ - نحوه تنظیمات امنیتی رمز عبور در Windows10

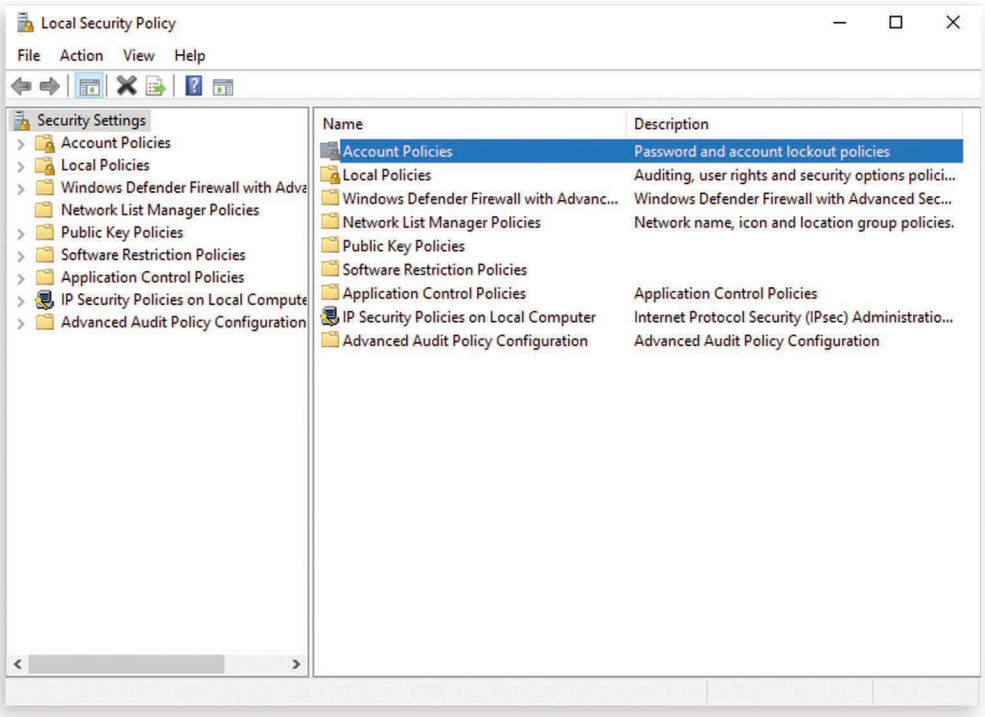
رمز عبور یکی از روش‌های متداول تأیید اعتبار هویت کاربر است. سیستم‌عامل Windows دارای گزینه‌های مختلف تأیید اعتبار مانند پین، رمز عبور، اثر انگشت و توکن است، اما برگ برنده تأیید اعتبار کاربر همچنان رمز عبور است.

تنظیمات امنیتی رمز عبور در Windows10 را می‌توان از قسمت local security policy انجام داد.

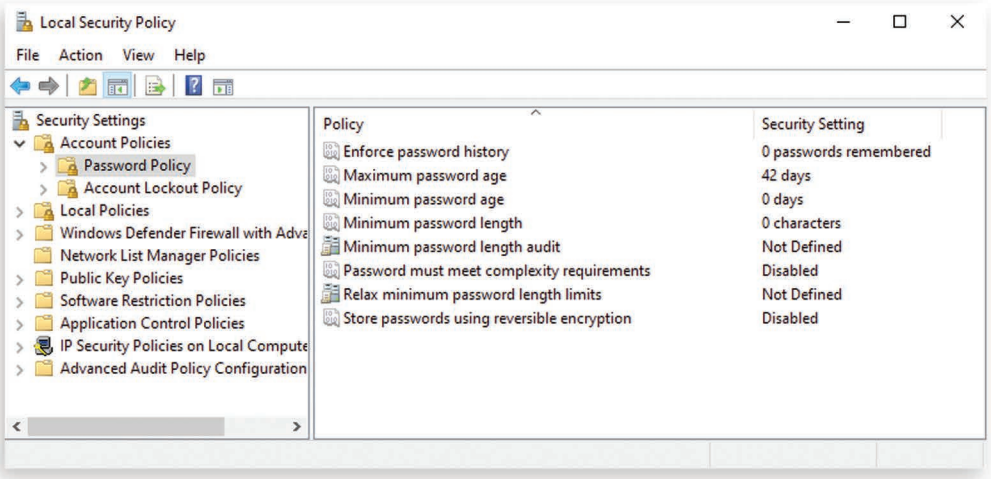
در نوار جستجوی Windows10 عبارت "Secpl" را تایپ کرده تا مانند شکل زیر به قسمت تنظیمات امنیتی Windows10 وارد شوید.



روی Account Policies setting کلیک کنید و به دنبال آن گزینه Password Policy را انتخاب کنید.



گزینه‌های Password Policy:



1- Enforce password history

این گزینه به کاربر اجازه می‌دهد تا تعداد رمزهای عبور منحصربه‌فرد مجاز برای هر کاربر را قبل از استفاده مجدد از رمز عبور قدیمی تعیین کند. برای مثال، اگر مقدار روی ۵ تنظیم شود، کاربر می‌تواند پس از ۵ تغییر رمز عبور منحصربه‌فرد، رمز عبور اول را دوباره استفاده کند. مقداری به صورت پیش‌فرض در این گزینه تنظیم‌نشده است و محدوده مقدار مجاز از ۰ تا ۲۴ می‌باشد.

2- Maximum password age

این قابلیت به کاربر این امکان را می‌دهد تا مدت اعتبار زمان رمز عبور را تنظیم کند که پس از پایان رسیدن زمان تنظیم‌شده کاربر مجبور به تغییر رمز عبور می‌شود. برای مثال، اگر مقدار روی ۳۰ تنظیم شود، از کاربر خواسته می‌شود تا رمز عبور را در روز سی و یکم تغییر دهد. در این حالت مقداری به صورت پیش‌فرض تنظیم‌نشده است. محدوده‌های مقدار مجاز زمان اعتبار رمز عبور از ۰ تا ۹۹۹ روز می‌باشد. مقدار صفر به معنای عدم انقضای رمز عبور با گذشت زمان است.

3- Minimum password age

این قابلیت به معنای این است که زودتر از زمان تعیین‌شده نمی‌توانیم رمز عبور را تغییر دهیم. به‌طور مثال اگر مقدار روی ۵ تنظیم شود، کاربر فقط می‌تواند پس از ۵ روز رمز عبور را تغییر دهد. به صورت پیش‌فرض، مقدار این قابلیت صفر می‌باشد. محدوده‌های مقدار مجاز ارزش‌دهی از ۰ تا ۹۹۸ روز متغیر می‌باشد اگر مقدار روی ۰ تنظیم شود، این بدان معناست که رمز عبور را می‌توان فوراً تغییر داد.

4- Minimum password length

این گزینه به کاربر امکان می‌دهد تا حداقل طول رمز عبور را تنظیم کند. برای مثال، اگر مقدار روی ۸ تنظیم شود، حداقل طول رمز عبور نمی‌تواند کمتر از ۸ باشد. به صورت پیش‌فرض مقداری برای این گزینه تنظیم‌نشده است. محدوده تنظیم طول کاراکتر رمز عبور از ۱ تا ۱۴ کاراکتر می‌باشد. اگر مقدار روی ۰ تنظیم‌شده باشد، این بدان معناست که دیگر رمز عبور موردنیاز نمی‌باشد.

5- Password must meet complexity requirement

اگر این گزینه فعال باشد، رمز عبور انتخابی باید حداقل شرایط زیر را داشته باشد. البته این مقدار به صورت پیش‌فرض غیرفعال می‌باشد.

۱- رمز عبور شامل user name یا بخش‌هایی از نام آن‌که بیش از دو قسمت متوالی است نباشد.

۲- حداقل شامل ۶ کاراکتر باشد.

۳-کاراکترهای تشکیل‌دهنده رمز عبور با شرایط زیر باشند

۳-۱- حروف بزرگ انگلیسی

۳-۲- حروف کوچک انگلیسی

۳-۳- اعداد از ۰ تا ۹

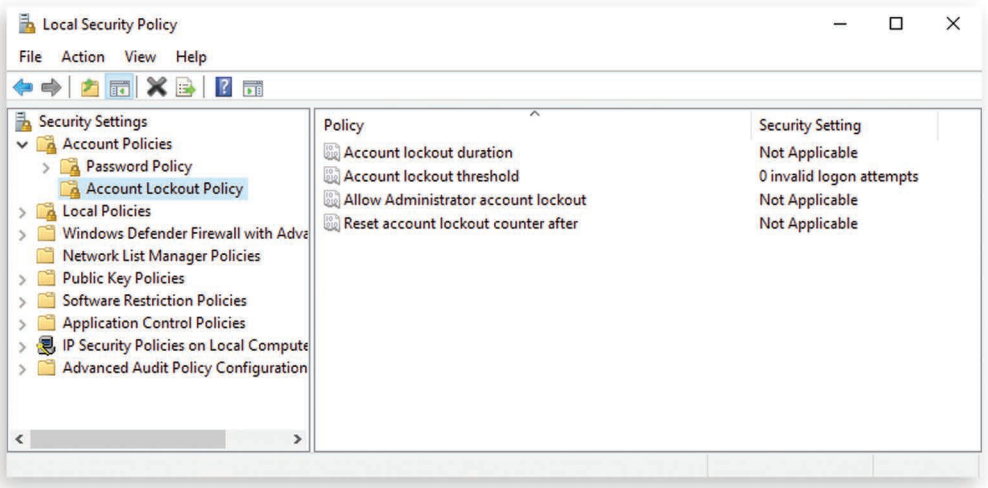
۳-۴- کاراکترهای غیر الفبایی مانند (!, $, #, %...)

۴- پیچیدگی زمانی اعمال می‌شود که رمز عبور اعمال یا تغییر داده شود.

6- Store passwords using reversible encryption

این قابلیت به معنای این است که زودتر از زمان تعیین‌شده نمی‌توانیم رمز عبور را تغییر دهیم. به‌طور مثال اگر مقدار روی ۵ تنظیم شود، کاربر فقط می‌تواند پس از ۵ روز رمز عبور را تغییر دهد. به صورت پیش‌فرض، مقدار این قابلیت صفر می‌باشد. محدوده‌های مقدار مجاز ارزش‌دهی از ۰ تا ۹۹۸ روز متغیر می‌باشد اگر مقدار روی ۰ تنظیم شود، این بدان معناست که رمز عبور را می‌توان فوراً تغییر داد.

برای امنیت بیشتر ما می‌توانیم ازطریق گزینه
Account Lockout Policy امنیت بیشتری را برقرار کنیم



1-Account lockout threshold

این گزینه تعداد تلاش‌های ناموفق مجاز ورود به سیستم قبل از قفل شدن نام کاربری است. برای مثال، اگر این مقدار روی ۵ تنظیم‌شده باشد، رمز عبور سیستم پس از ۵ تلاش غیرمجاز برای ورود، قفل می‌شود. به صورت پیش‌فرض، مقداری برای این قابلیت در نظر گرفته نشده است. محدوده‌ی مقداردهی مجاز از ۰ تا ۹۹۹ می‌باشد که اگر مقدار روی ۰ تنظیم شود، حساب هرگز قفل نخواهد شد.

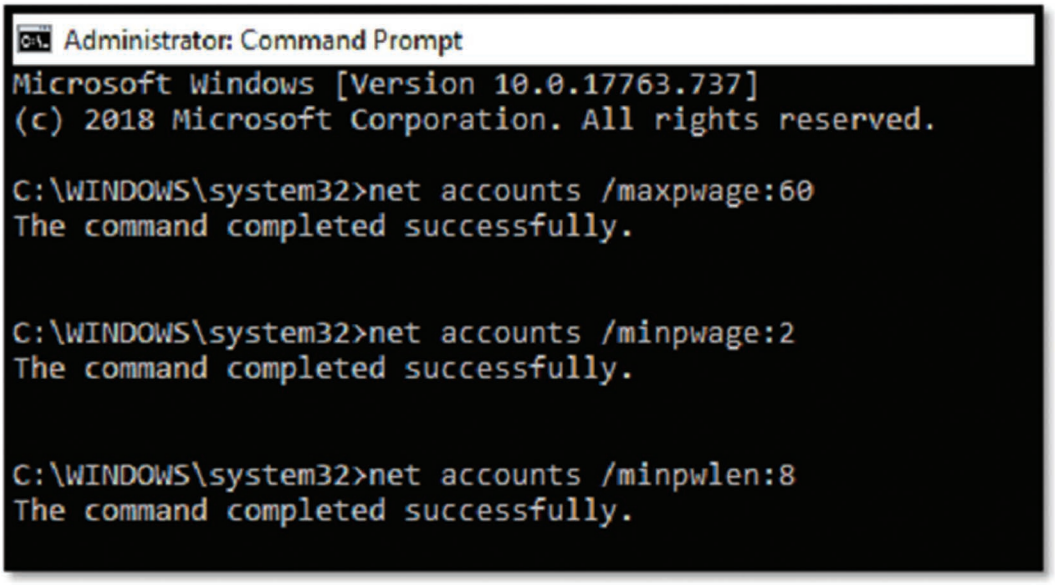
2- Account lockout duration

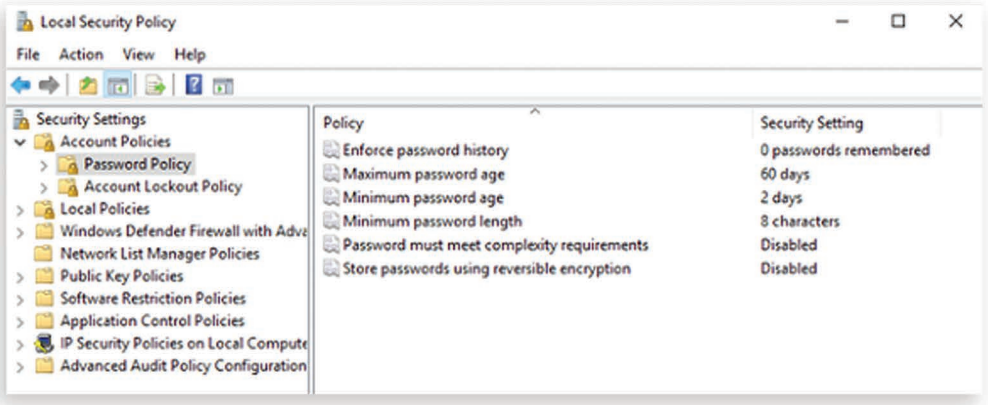
این گزینه مدت زمانی است که سیستم پس از فعال شدن به صورت خودکار قفل می شود. برای مثال، اگر مقدار روی ۵ تنظیم شود، سیستم پس از مدت ۵ دقیقه قفل می شود. به صورت پیش‌فرض، مقداری برای این گزینه تنظیم‌نشده است. مقدار مجاز از ۱ تا ۹۹۹۹ دقیقه می‌باشد. اگر مقدار روی ۰ تنظیم شود، زمانی که ادمین آن را باز کند، قفل خواهد شد.

3- Reset account lockout counter after

میزان زمانی است که پس از طی آن زمان سیستم دوباره بازنشانی می‌شود، برای مثال، اگر به ۵ تنظیم شود، سیستم پس از ۵ دقیقه به ۰ بازمی‌گردد. به صورت پیش‌فرض مقداری تنظیم‌نشده است. محدوده‌های مقدار مجاز از ۱ تا ۹۹۹۹۹. اگر مقدار روی ۰ تنظیم شود، این بدان معناست که حساب هرگز قفل نخواهد شد.
تنظیمات ذکرشده در مقاله را با مثال زیر تشریح می‌کنیم:

تنظیم حداکثر اعتبار رمز عبور تا ۶۰ روز	net accounts /maxpwage:60:
تنظیم حداقل اعتبار رمز عبور ۲ روز	net accounts /minpwage:2:
تنظیم حداقل طول رمز عبور ۸ کاراکتر	net accounts /minpwlen:8:

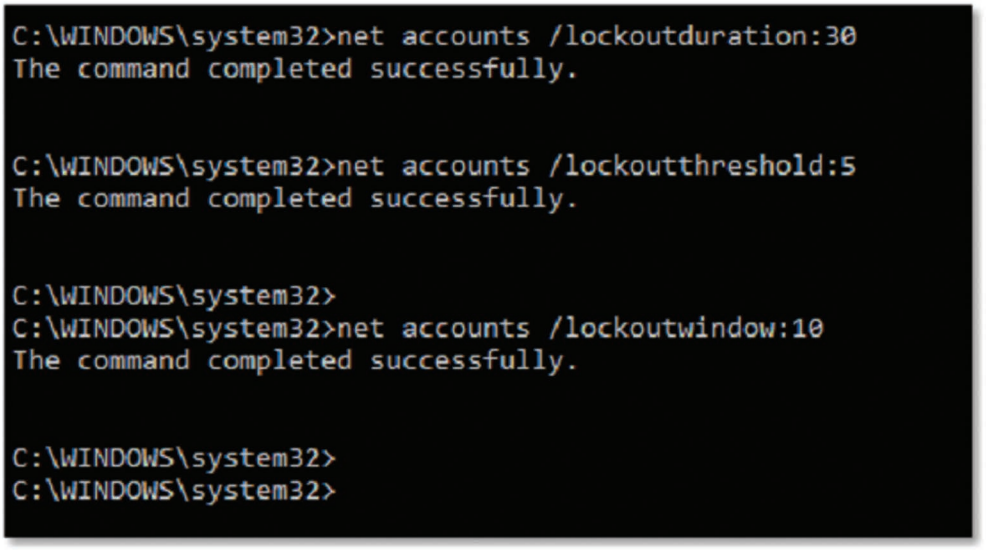


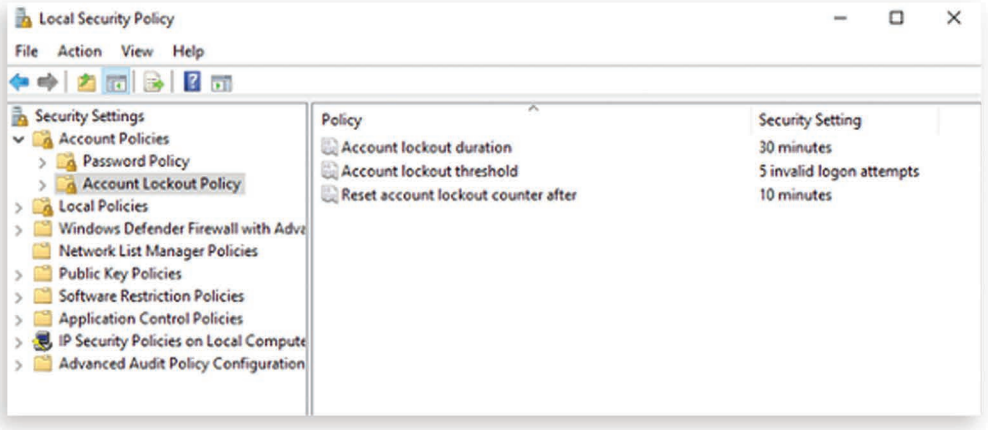


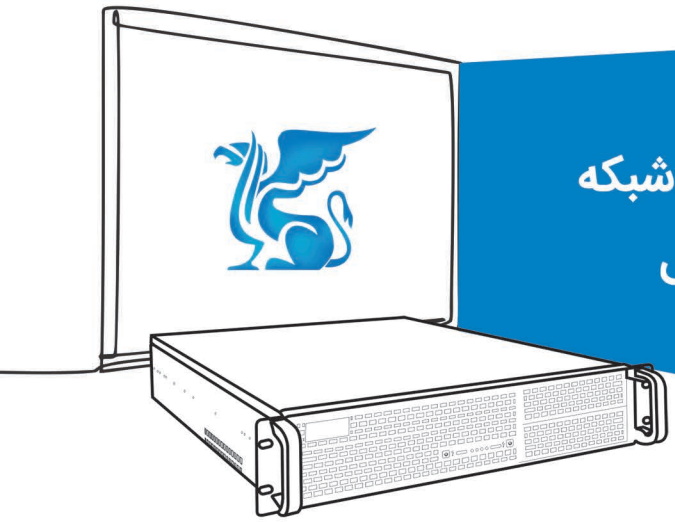
تنظیم مدت زمان قفل اکانت تا ۳۰ دقیقه net accounts /lockoutduration: 30:

حداکثر تلاش‌های قابل‌قبول غیرمجاز ۵ بار net accounts /lockoutthreshold: 5:

مدت زمان باز شدن مجدد سیستم پس از گذشت ۱۰ دقیقه net accounts /lockoutwindow:10:







پیوست ۲ - معماری پیشنهادی شبکه برای راه اندازی نرم افزار شیردال

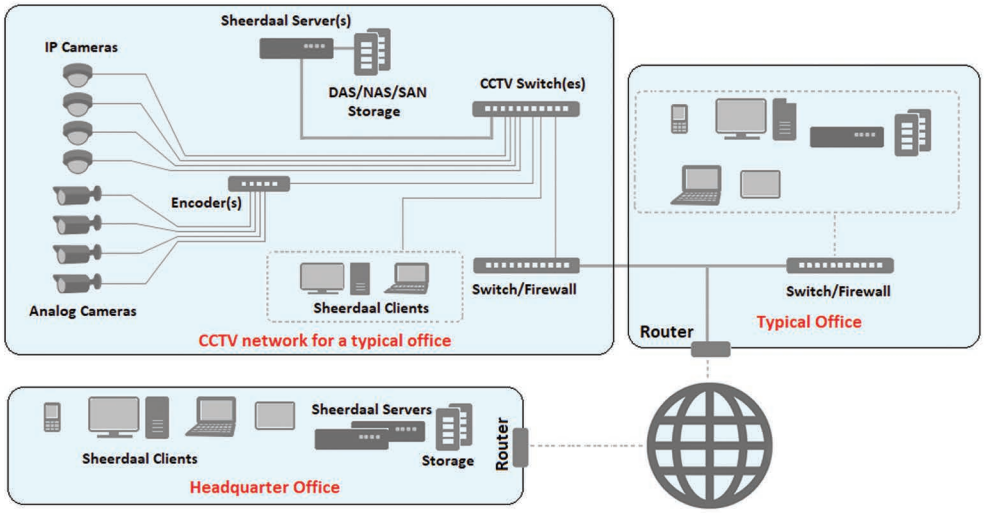
سیستم پیشنهادی براساس استفاده از نرم‌افزار شیردال در پروژه هایی با گستردگی بالا در مراکز متفاوت برای ایجاد یک سیستم جامع نظارت تصویری است. با استفاده از نرم‌افزار و ساختار پیشنهادی، عملیات هر یک از مراکز بطور مستقل و در یک محیط امن و کیفی انجام و امکان اتصال آن¬ها به واحد مرکزی برای نظارت، مدیریت و کنترل فرآهم خواهد شد. افزایش کارایی و امنیت، بهبود پشتیبانی فنی و عملیاتی، کاهش ناسازگاری، ایجاد و رعایت استاندارد همراه با کاهش هزینه‌ها به نسبت خدمات و اطلاعات دریافتی از مزایای استفاده از طرح پیشنهادی است.

با توجه به اینکه برای نقل و انتقال تصاویر دوربین‌ها اعم از آنالوگ و شبکه‌ای نیازمند استفاده از شبکه‌های ارتباطی و محلی هستیم، لذا اولین قدم، ایجاد یک شبکه مناسب، امن و مستقل برای دوربین‌ها در داخل هر ساختمان و سپس انتقال آن به مرکز/مراکز متفاوت می‌باشد. با توجه به حساس بودن خروجی دوربین ها و در عین حال نیاز به پهنای باند مناسب، بایستی شبکه‌های محلی دوربین‌ها و امور اداری از هم مستقل و در عین حال بهم مرتبط باشند. شکل ذیل شمای کلی یک شبکه محلی پیشنهادی برای دوربین های مداربسته هر ساختمان را ارایه می‌دهد.

خصوصیات امنیتی شبکه پیشنهادی

در طرح شبکه پیشنهادی برای افزایش امنیت اطلاعات و تصاویر به موارد ذیل توجه ویژه شده است:

جداسازی شبکه دوربین‌ها از شبکه اداری و مدیریتی سبب افزایش امنیت شبکه دوربین‌ها و کنترل مناسب دسترسی‌ها خواهد شد.



جداسازی شبکه دوربین‌ها از شبکه اداری و مدیریتی برای جلوگیری از بروز تداخل و مشکلات ترافیک شبکه از اهمیت زیادی برخوردار است. اگر این مهم بخوبی مورد توجه قرار نگیرد، بدلیل تولید تصاویر با حجم بالا توسط دوربین‌ها، امکان کاهش راندمان در هر دو شبکه وجود خواهد داشت.

با توجه به ماهیت امنیتی سیستم‌های نظارت و پایش تصویر و همچنین شواهد معتبر، باید امکان وجود Backdoor در دوربین‌ها را بسیار جدی گرفت. در طرح پیشنهادی جدا بودن شبکه دوربین‌ها و قرار گرفتن سرور شیردال برای مدیریت تصاویر و کاربران و وجود دیواره آتش، عوامل بازدارنده در مدیریت و کنترل این خطر بالقوه هستند.

با عنایت به ساختار شبکه و همچنین امکانات امنیتی شیردال، مشاهده و استفاده از تصاویر دوربین برای کاربران خاص در شبکه اداری و مدیریتی میسر است.

امکان اتصال و انتقال اطلاعات و تصاویر از راه دور در شبکه دیده شده است. این مهم براساس دیواره آتش و همچنین قابلیت‌های امنیتی شیردال بخوبی پوشش داده شده است.

Network Security Architecture