سند راهنمای امن سازی

نرم‌افزار مدیریت حوادث برق و ثبت خاموشی (مهنا ۱۲۱)

مهندسی هرمزان نیروی ایرانیان (مهنا)
MAHNA

مشخصات سند	
موضوع	سند راهنمای امن سازی نرم افزار مدیریت حوادث برق و ثبت خاموشی
نسخه سند	۲.۱
تاریخ	۱۴۰۱/۱۲/۰۲
تهیه کنندگان	شرکت مهندسی هرمزان نیروی ایرانیان (مهنا) – امین علی‌بلندی
طبقه‌بندی	عادی

مقدمه:

با توجه به اهمیت بالای امنیت در محصولات شرکت مهندسی هرمزان نیروی ایرانیان (مهنا) و راه‌کارهای مناسب و به روز افزایش امنیت مطابق با استانداردهای جهانی، این سند با هدف راهنمایی در امن سازی نرم افزار مدیریت حوادث برق ایجاد شده است تا مدیران سیستم و کاربران با اطمینان خاطر بیشتری از محصول استفاده نمایند.

این سند دارای دو رویکرد است:

۱- رویکرد امن‌سازی نرم افزار
۲- رویکرد امن‌سازی محیط عملیاتی نرم افزار

معرفی محصول:

سامانه مدیریت حوادث برق و ثبت خاموشی (مهنا ۱۲۱)، یک نرم‌افزار کاربردی دسک‌تاپی (Desktop Application) برای ثبت حوادث است. اصلی ترین کاربرد نرم افزار ثبت خاموشی، ثبت درخواست‌ها و خاموشی‌های مشترکین برق می‌باشد. تفکیک و پالایش به موقع این اطلاعات و هدایت آن به مسیر درست، باعث افزایش بهره‌وری در استفاده از منابع در سازمان‌های هدف می‌گردد.

این نرم افزار دارای بخش‌های مختلف زیر است:

- واحد اپراتوری، شامل زیربخش‌های: ایجاد پرونده / اعلان‌های عمومی و پیام‌های اضطراری / مرکز تماس / مشاهده وضعیت مناطق و شبکه برق / سوابق پرونده‌ها / و غیره
- واحد اتفاقات، شامل زیربخش‌های: مدیریت و پیگیری خاموشی‌ها / ارجاع و پیگیری ارجاعات بین واحدهای مربوطه / ثبت تجهیزات مصرفی / و غیره
- بخش شبکه و بارگیری‌ها، دارای زیربخش‌های: ساختار شبکه برق / بارگیری شبکه / بارگیری فشار متوسط / و غیره
- بخش آمار، جهت دریافت آمار از امور مختلف: اقدام شده، تعداد اکیپ‌های اعزام شده و ... با قابلیت فیلتر زمان و تاریخ.
- بخش گزارش‌گیری، شامل زیربخش‌های: گزارش‌های کنترلی / گزارش‌های خاموشی / گزارش عملکرد کاربران / و غیره

شرح عملکرد نرم‌افزار:

پس از ثبت رکوردها توسط اپراتورهای سامانه، کار توسط اپراتورهای مناطق مشاهده می شود که وظیفه برنامه ریزی و رسیدگی به آنها را دارند تا اگر مشترک بی برق شده با اعزام مامور و رفع مشکل، برق دار شود.

همچنین در صورت نیاز به تعمیرات یا تغییرات در شبکه برق، واحد دیسپاچینگ با برنامه ریزی با اطلاع قبلی، شبکه را بی برق میکند تا ماموران بتوانند اقدامات لازم را انجام دهند. برای اطلاع رسانی خاموشی های بابرنامه و پیگیری آن از پنل "با برنامه" استفاده میشود.

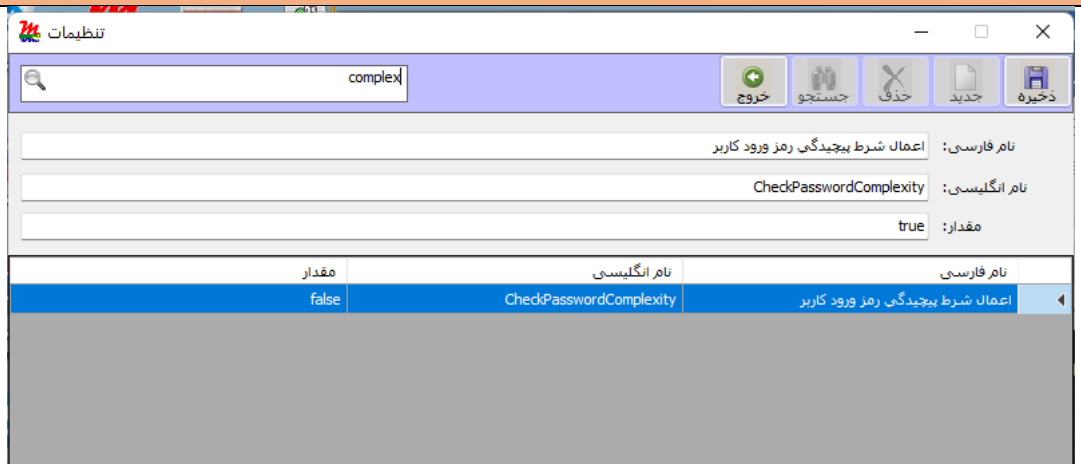
تمامی رکوردها قابلیت جستجو و فیلتر شدن را دارند و همچنین از قابلیت‌های دیگر نرم افزار میتوان به گزارش گیری اشاره کرد که شامل گزارش حوادث، گزارش بارگیری ها، گزارش تجهیزات از قبیل پست توزیع و فیدر، گزارش عملکرد پرسنل و... می باشد.

اطلاعات شبکه و بارگیری در نرم افزار ثبت شده و قابلیت بروزرسانی را دارد و امکان انجام محاسبات در بخش شبکه فشار ضعیف شبکه برق را در نرم افزار فراهم میسازد.

تنظیمات بسیار متعدد و متنوعی در نرم افزار وجود دارد که فرایندهای مربوط به بیزینس اپلیکیشن توسط مدیر سیستم پیکربندی می گردد. مدیر سیستم امکان تعریف/ویرایش و همچنین اختصاص نقش‌های مشخص شده به کاربران را دارد. دسترسی های مختلف نیز به نقش‌ها و به کاربران داده می شود.

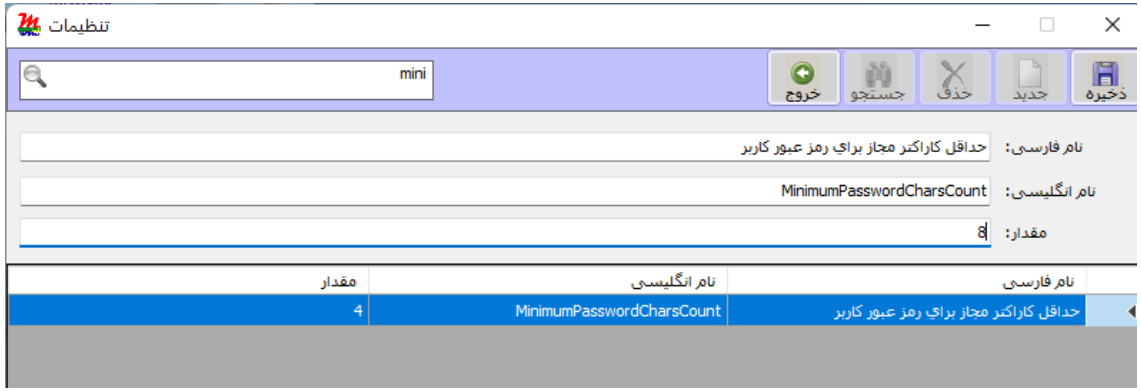
جدول موضوعات و راهنمای امن سازی نرم افزار

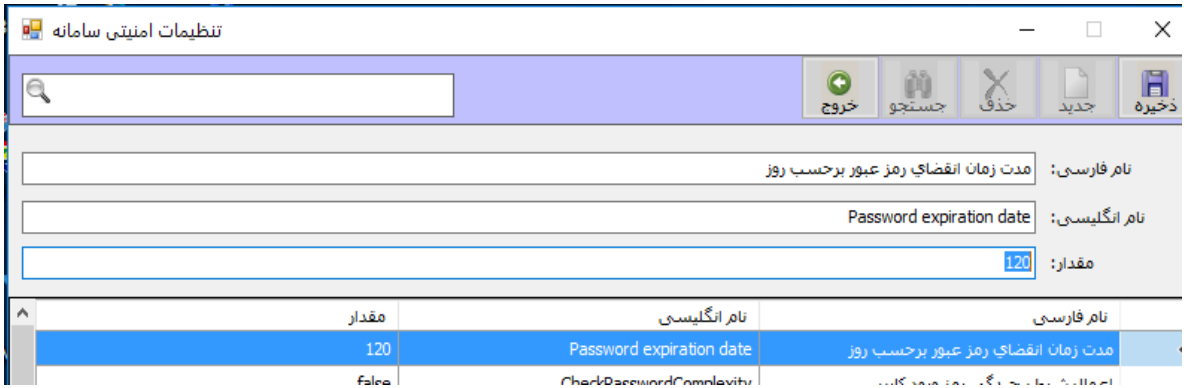
ردیف	موضوع	توضیحات و روش امن سازی
۱.	**پیچیدگی پسورد** (Password Complexity)	برای افزایش امنیت نرم افزار و استفاده از کلمه های عبور قوی و امن، لازم است طول کلمه عبور حداقل ۸ کاراکتر و به صورت پیچیده باشد. برای امن سازی نرم افزار در خصوص کلمات عبور مراحل زیر انجام شود: - مدیر سیستم (admin) از قسمت تنظیمات – تنظیمات امنیتی، گزینه تنظیمات کلی را انتخاب کند  - گزینه ی **اعمال شرط پیچیدگی رمز ورود کاربر** را انتخاب نموده و مقدار آن را true کرده و سپس ذخیره شود.

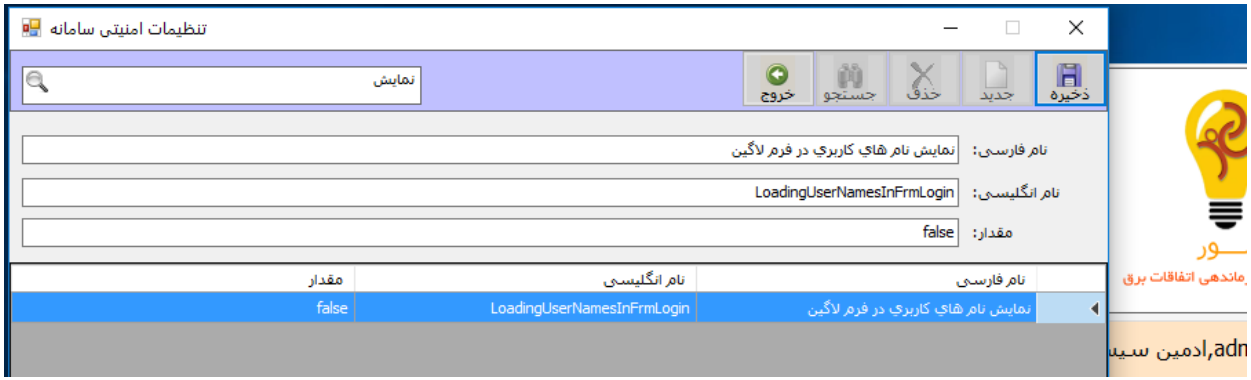
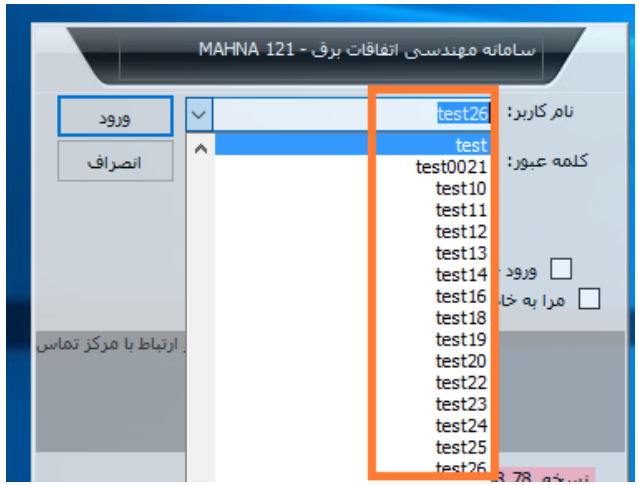
ردیف	موضوع	توضیحات و روش امن سازی
		 پس از این تنظیمات، کلمه عبورهای ساده قابل استفاده نبوده و می بایست از حروف کوچک، بزرگ، اعداد و علائم اختصاری در تعیین کلمه عبور استفاده شود.
۲.	**طول کلمه عبور**	طبق استانداردهای امنیتی، حداقل طول کلمه عبور می بایست بیش از ۸ کاراکتر باشد. لذا برای افزایش امنیت نرم افزار در خصوص کلمات عبور ، مراحل زیر انجام شود: - مدیر سیستم (admin) از قسمت تنظیمات – تنظیمات امنیتی، گزینه تنظیمات کلی را انتخاب کند.

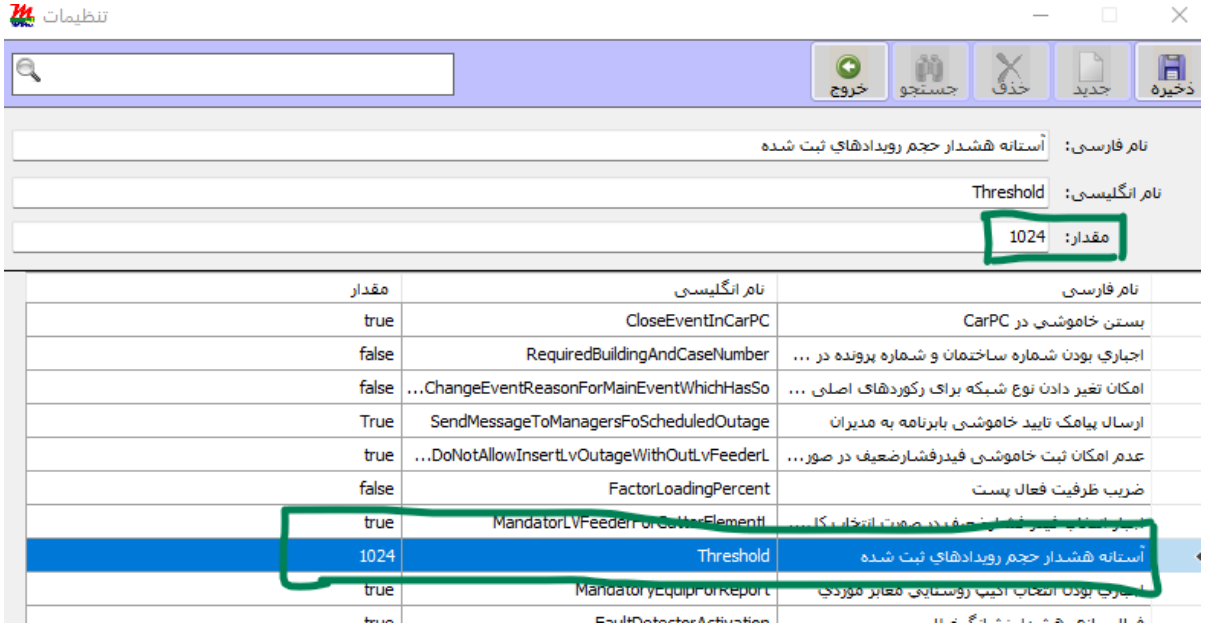
ردیف	موضوع	توضیحات و روش امن سازی

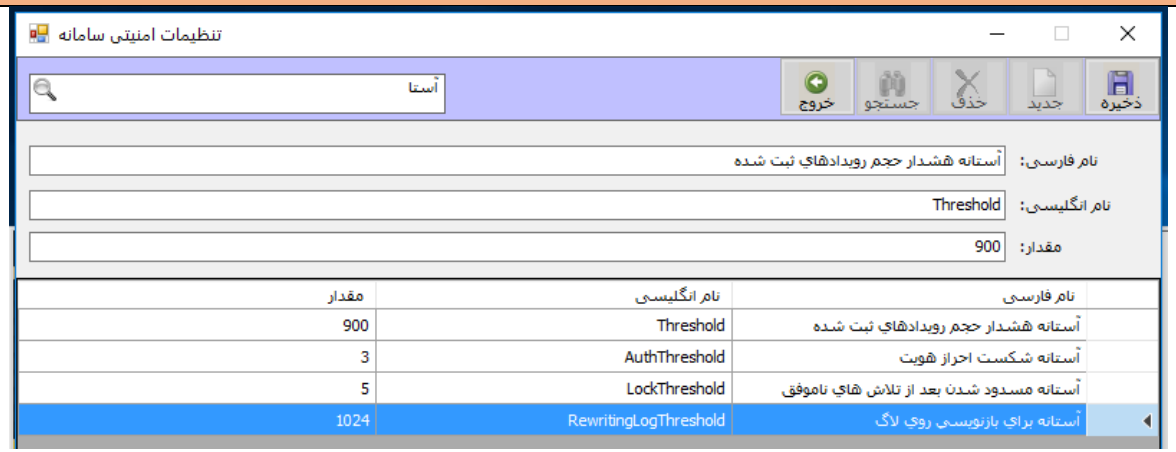
- گزینه ی **<u>حداقل کاراکتر مجاز برای رمز عبور کاربر</u>** (MinmumPasswordCharsCount) را انتخاب نموده و مقدار آن را ۸ و یا بیشتر قرارداده و سپس ذخیره شود.



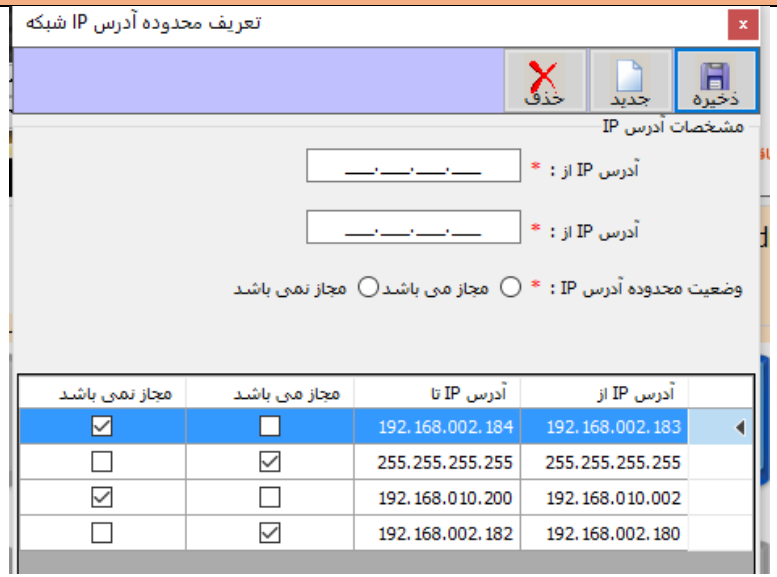
ردیف	موضوع	توضیحات و روش امن سازی
۳.	**مدت زمان انقضای Password**	از دیدگاه امنیت، لازم است کلمه عبور کاربران بعد از یک مدت مناسبی (حداکثر هر ۱۸۰ روز یکبار)، تغییر کند. لذا در قسمت تنظیمات، گزینه پیکربندی نرم‌افزار، بخش تنظیمات امنیتی سامانه، امکان تعیین "مدت زمان انقضای رمز عبور کاربر بر حسب روز" ایجاد شده است. 
۴.	**حد آستانه تلاش ناموفق احراز هویت**	در این محصول، در بخش تنظیمات قسمت تنظیمات کلی، گزینه هایی برای تعیین حد آستانه تلاش ناموفق احراز هویت وجود دارد تا از ورود کاربر غیرمجاز که طی حمله Brute force قصد یافتن اطلاعات لاگین کاربران را دارد، جلوگیری شود. آستانه شکست احراز هویت: AuthThreshold = 3 آستانه مسدود شدن بعد از تلاش هاي ناموفق: LockThreshold = 5 - اولین پارامتر، آستانه شکست احراز هویت است که باید مقدار آن بزرگتر از ۲ باشد. در این حالت پس از تلاش های ناموفق کاربر برای ورود به نرم افزار، Captcha فعال می شود. - دومین پارامتر، آستانه مسدود شدن پس از تلاش های ناموفق است که اگر کاربر به تعداد تعیین شده برسد، حساب کاربری وی مسدود خواهد شد.

ردیف	موضوع	توضیحات و روش امن سازی
۵.	**عدم نمایش نام های کاربری در فرم لاگین**	بر اساس نیاز سازمان می توان در تنظیمات امنیتی نرم افزار، قابلیت نمایش یا عدم نمایش نام‌های کاربری را فعال یا غیرفعال نمود. بر اساس دیدگاه امنیت، لازم است نام های کاربری در فیلد نام نمایش داده نشوند، لذا در قسمت " **نمایش نام‌های کاربری در فرم لاگین**" مقدار False قرار داده شود.  تصویر زیر مربوط به زمانی است که مقدار true باشد، در فیلد نام کاربر، نام‌های کاربری موجود نمایش داده می شوند. 

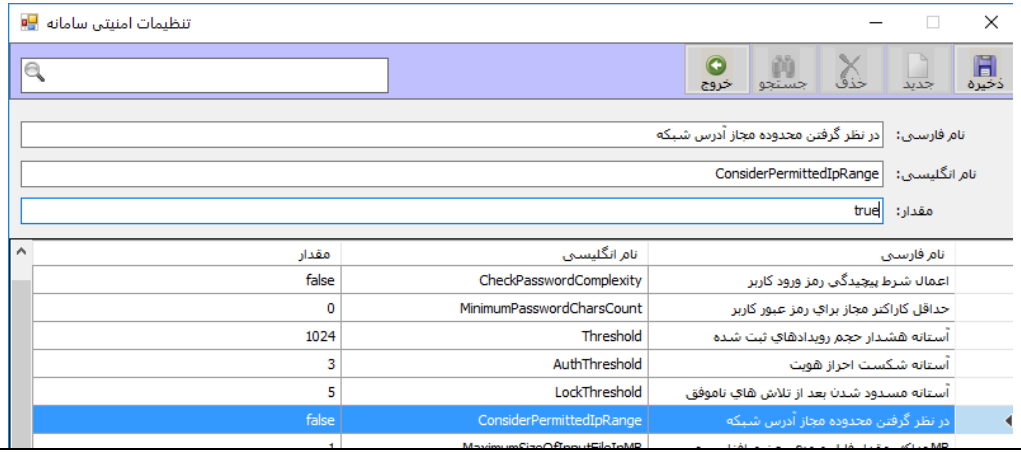
ردیف	موضوع	توضیحات و روش امن سازی
۶.	**آستانه هشدار حجم رویدادهای ثبت شده**	با توجه به اینکه پرشدن فضای ذخبره سازی لاگ ممیزی (ثبت رویدادها) مشکل مهم و بزرگی محسوب می شود، لذا باید آستانه ای را برای ایجاد هشدار قبل از پر شدن فضای ذخیره سازی دریافت نمود تا اقدام مناسب در زمان مناسب صورت گیرد. لذا در بخش تنظیمات کلی نرم افزار، می بایست مقدار Threshold را تعیین نمود. این مقدار بر حسب MB است. 
۷.	**آستانه برای بازنویسی روی لاگ**	با توجه به محدودیت در فضاهای ذخیره‌سازی داده، این امکان در نرم افزار ایجاد شده است تا مدیر سامانه، مقدار حجمی را برای ذخیره سازی لاگ ها در نظر بگیرد. این قابلیت مدیریت صحیحی را فراهم خواهد ساخت. برای این منظور، در بخش تنظیمات، تنظیمات امنیتی سامانه، گزینه‌ای با عنوان آستانه برای بازنویسی لاگ وجود دارد. توصیه می شود این مقدار کمتر از 1G (1024 MB) نباشد. پس از رسیدن حجم داده های لاگ به مقدار تعیین شده، عملیات بازنویسی بر روی قدیمی ترین لاگ آغاز می شود. مقدار قابل تعیین در تنظیمات، بر حسب MB است.

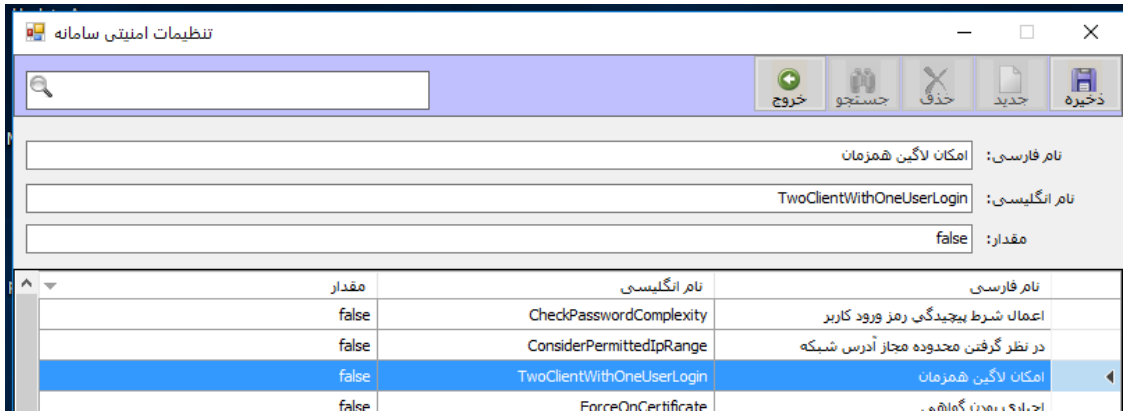
ردیف	موضوع	توضیحات و روش امن سازی
		
۸.	**ذخیره‌سازی اطلاعات لاگین (مرا به خاطر بسپار)**	در فرم لاگین نرم افزار OMS، گزینه ای با عنوان "**مرا به خاطر بسپار**" وجود دارد که به صورت پیش فرض تیک ندارد تا اطلاعات کاربر به صورت ناخواسته در نرم افزار ذخیره نباشد. توصیه می شود در زمان ورود کاربر، در صورتیکه کاربر مایل به ذخیره سازی اطلاعات لاگین خود باشد، این گزینه را انتخاب نماید. در مراکزی که از یک ایستگاه کاری چندین کاربر متفاوت استفاده می نمایند، بهتر است اطلاعات لاگین ذخیره نشود.
۹.	**تعیین محدوده آدرس IP شبکه**	برای کنترل و محدود سازی دسترسی و استفاده از نرم افزار، امکان تعیین محدوده آدرس شبکه در بخش تنظیمات نرم افزار برای ادمین وجود دارد. با تعریف آدرس مورد نظر و تعیین گزینه مجاز می باشد یا مجاز نمی باشد، از دسترسی غیرمجاز به نرم افزار جلوگیری خواهد شد.

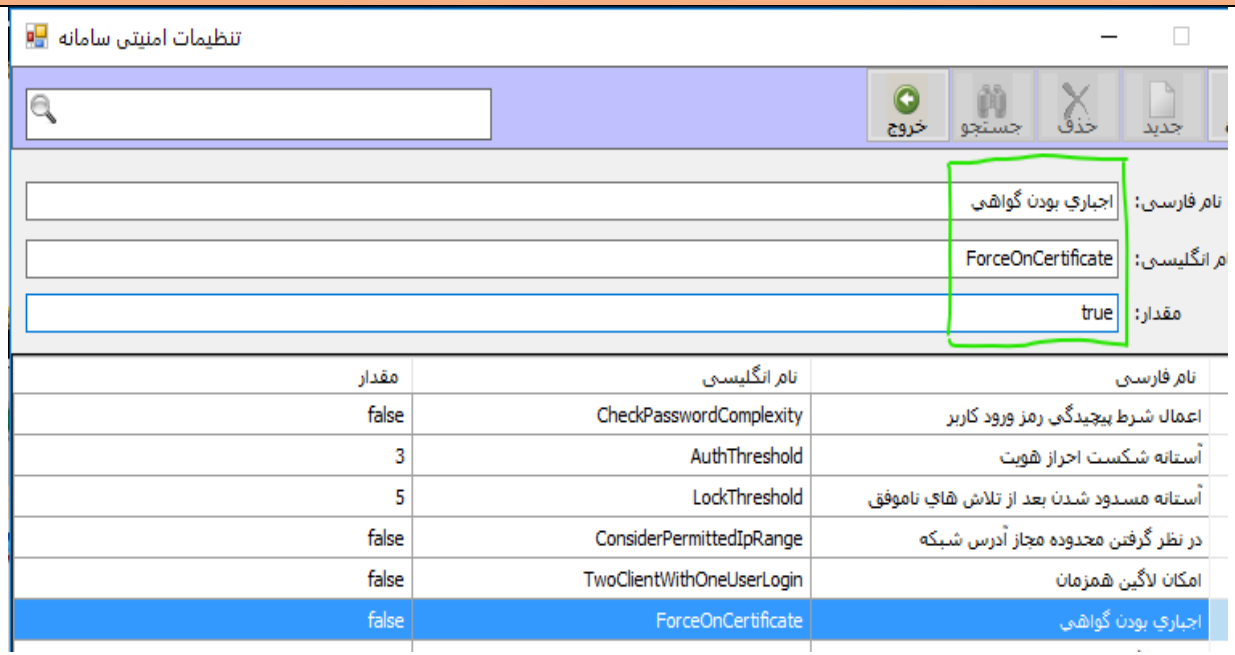
ردیف	موضوع	توضیحات و روش امن سازی



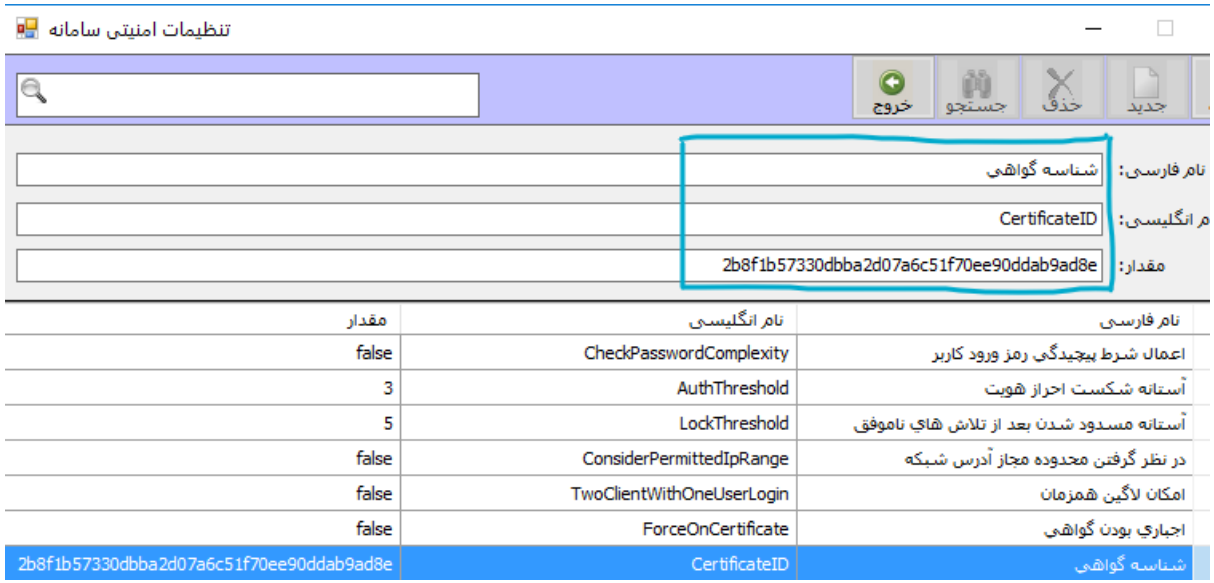
همچنین لازم است برای اجرای این محدودیت، در بخش تنظیمات کلی، مقدار گزینه ی **"در نظر گرفتن محدوده مجاز آدرس شبکه"** (ConsiderPermittedIpRange) ، True شود.

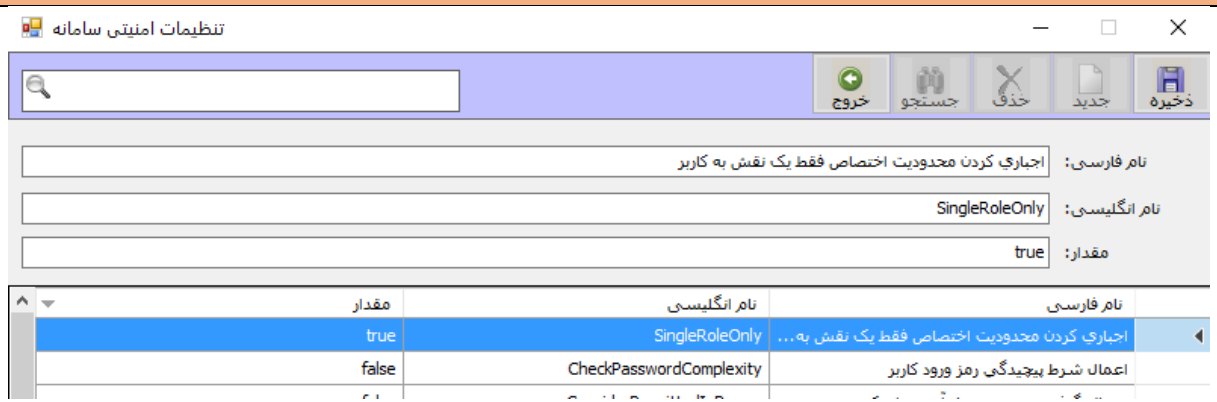
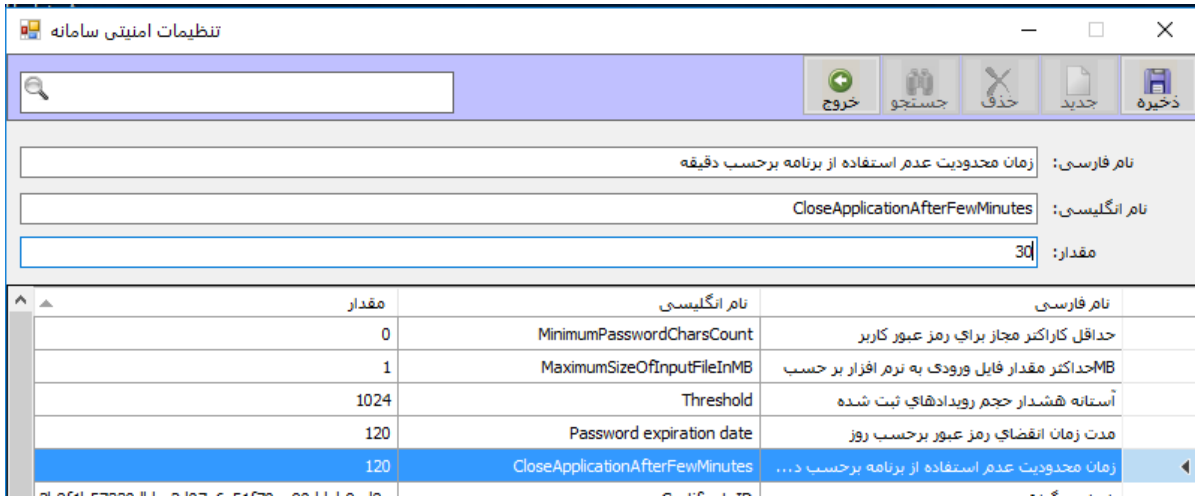


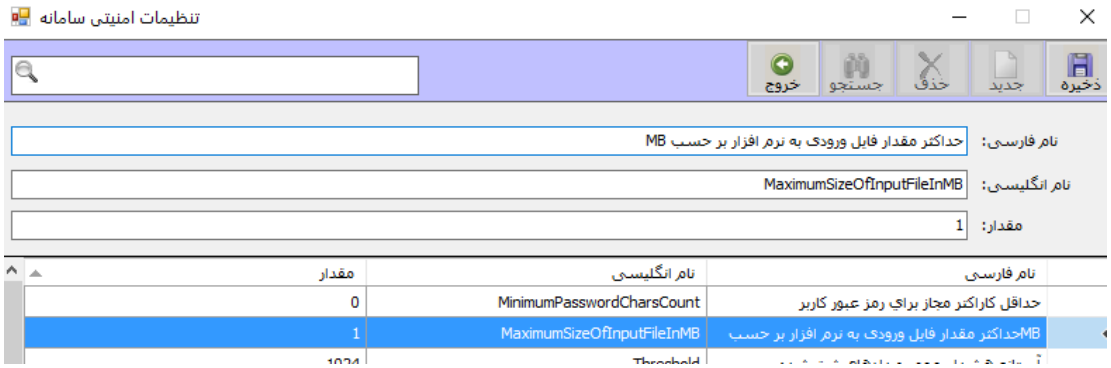
ردیف	موضوع	توضیحات و روش امن سازی
۱۰.	**مدیریت نشست همزمان**	به صورت پیش‌فرض امکان نشست همزمان با یک نام کاربری در نرم‌افزار مهنا۱۲۱ وجود ندارد. در صورت نیاز بیزینس برای وجود این امکان، لازم است در بخش تنظیمات امنیتی سامانه، گزینه امکان لاگین همزمان تنظیم گردد. اگر مقدار آن true باشد، نشست همزمان بدون محدودیت امکان پذیر خواهد بود (که از نظر امنیتی توصیه نمی شود) ، و اگر مقدار آن false باشد، در زمان ایجاد نشست همزمان، یک پیام مبنی بر لاگین بودن فرد دیگری با همین نام نمایش داده می شود، و سپس نشست اول اتوماتیک بسته می شود. (البته به کاربر اول پیامی مبنی بر ایجاد نشست با همین نام و با ذکر آدرس IP نمایش داده می شود). 
۱۱.	**بروزرسانی نرم افزار**	نرم افزار مهنا ۱۲۱ به صورت پیش فرض دارای تنظیمات و قابلیت بروزرسانی امن است. با توجه به اینکه قابلیت بروزرسانی دستی نیز وجود دارد، می بایست از محل تهیه فایل بروزرسانی و مورد اعتماد بودن آن اطمینان حاصل شود و سپس فایل بروزرسانی در محل نصب نرم‌افزار جایگزین گردد.
۱۲.	**استفاده از گواهینامه (Certificate) برای ارتباط امن (Over TLS)**	با توجه به اینکه ارتباط بین نرم‌افزار با سرور پایگاه داده با استفاده از گواهینامه معتبر، به صورت رمزشده برقرار می شود، لذا باید در تنظیمات امنیتی نرم‌افزار، مقدار اجباری بودن استفاده از گواهی True باشد تا هیچگاه کلاینت ها بدون داشتن گواهینامه قادر به برقراری ارتباط نباشند.

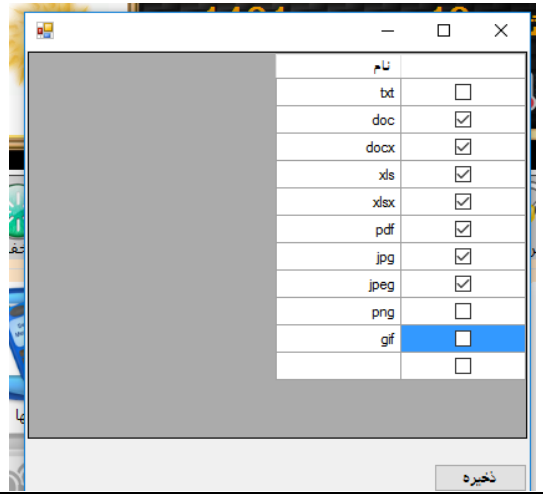
ردیف	موضوع	توضیحات و روش امن سازی
		

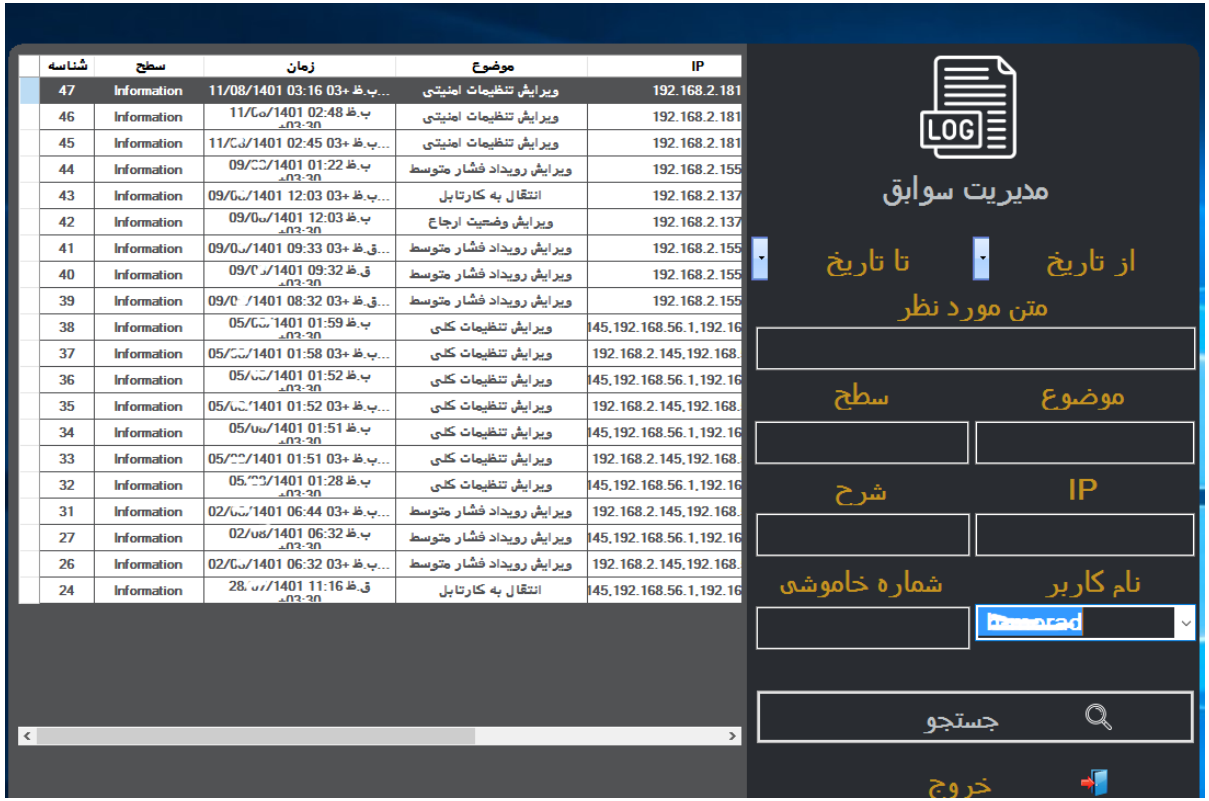
زمانی که مقدار تنظیمات این بخش با عنوان اجباری بودن گواهی، true باشد، کاربر بدون داشتن گواهینامه معتبر قادر به استفاده از نرم افزار و لاگین نخواهد بود.

ردیف	موضوع	توضیحات و روش امن سازی
۱۳.	**تنظیمات مربوط به گواهینامه مجاز در نرم‌افزار**	 نام فارسی / نام انگلیسی / مقدار اعمال شرط پیچیدگی رمز ورود کاربر / CheckPasswordComplexity / false آستانه شکست احراز هویت / AuthThreshold / 3 آستانه مسدود شدن بعد از تلاش های ناموفق / LockThreshold / 5 در نظر گرفتن محدوده مجاز آدرس شبکه / ConsiderPermittedIpRange / false امکان لاگین همزمان / TwoClientWithOneUserLogin / false اجباری بودن گواهی / ForceOnCertificate / false شناسه گواهی / CertificateID / 2b8f1b57330dbba2d07a6c51f70ee90ddab9ad8e
۱۴.	**مدیریت اختصاص نقش به کاربر**	در قسمت تنظیمات، پیکربندی نرم افزار، بخش تنظیمات امنیتی، گزینه ای با عنوان " **اجباری کردن محدودیت اختصاص فقط یک نقش به کاربر**" وجود دارد که اگر مقدار آن true باشد، در زمان ایجاد کاربر جدید و یا ویرایش کاربر، امکان اختصاص بیش از یک نقش به یک کاربر وجود نخواهد داشت و در صورتی که این مقدار false باشد، ادمین میتواند بیش از یک نقش را به کاربر اختصاص دهد (بر اساس نیاز بیزینس)

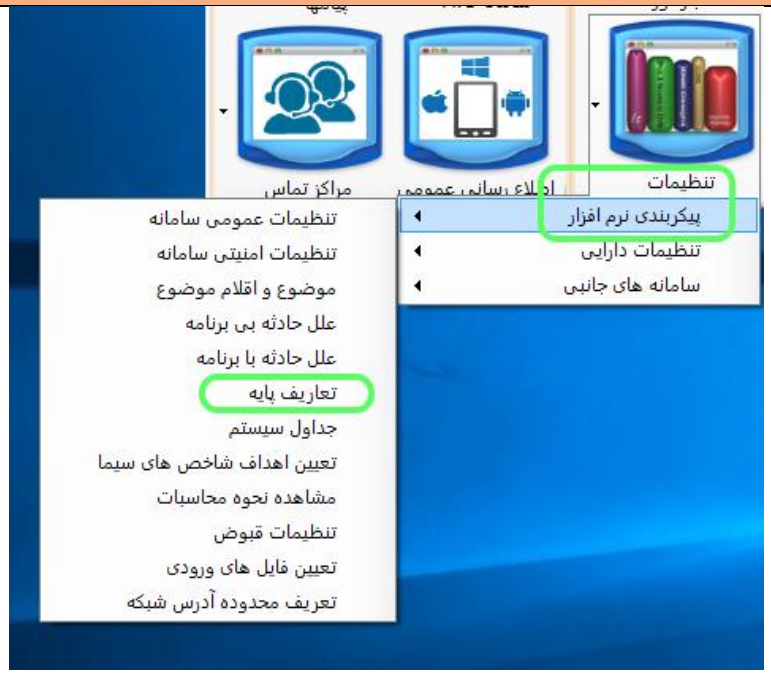
ردیف	موضوع	توضیحات و روش امن سازی
		
۱۵.	**زمان محدودیت عدم استفاده از برنامه**	یکی از موارد مهم در امنیت، مدیریت نشست های غیرفعال است. در صورتی که کاربر برای مدتی از نرم افزار استفاده نکند و هیچ عملکردی روی سیستم نداشته باشد، نشست وی به صورت اتوماتیک غیرفعال خواهد شد. به صورت پیش فرض این مقدار ۳۰ دقیقه است و در صورتی که مدیرمجاز مایل باشد مقدار آن را بر حسب دقیقه تغییر دهد، در تنظیمات امنیتی، در گزینه زمان محدودیت عدم استفاده از برنامه بر حسب دقیقه، مقدار آن را تعیین می نماید. 

ردیف	موضوع	توضیحات و روش امن سازی
۱۶.	**مدیریت حجم فایل‌های ورودی به نرم افزار**	برای جلوگیری از ورود فایل‌های حجیم به نرم‌افزار و ذخیره‌سازی آنها در پایگاه داده که منجر به پر شدن حافظه ذخیره‌سازی سمت سرور می‌شود، در این نرم‌افزار بخشی در تنظیمات امنیتی با عنوان: **" حداکثر مقدار فایل ورودی بر حسب** MB " تعبیه شده است تا حداکثر مقدار حجم فایل جهت آپلود و import در سامانه مدیریت شود. 
۱۷.	**مدیریت فرمت و نوع داده ورودی به نرم افزار**	یکی از نکات مهم در امنیت، جلوگیری از ورود (import) و یا آپلود فایل با فرمت غیرمجاز به داخل نرم افزار است. لذا در نرم افزار مهنا ۱۲۱، قابلیت مدیریت و تعیین فرمت مجاز تعبیه شده است.

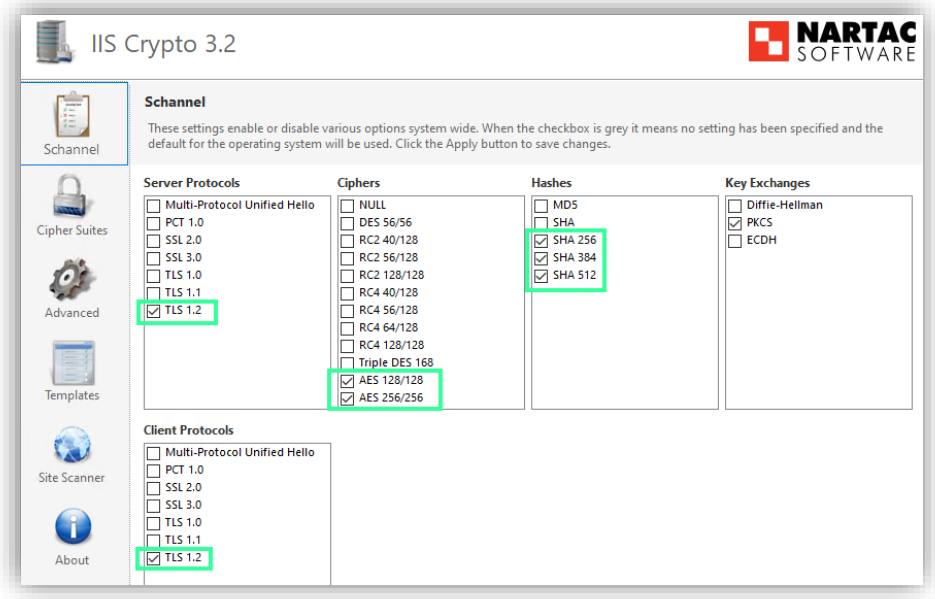
ردیف	موضوع	توضیحات و روش امن سازی
		 تصویر زیر مربوط به مدیریت تعیین فرمت مجاز است: 

ردیف	موضوع	توضیحات و روش امن سازی
۱۸.	**مشاهده لاگ‌های ممیزی**	برای مشاهده لاگ‌ها (رویدادهای ممیزی) در نرم‌افزار، کاربرانی که اجازه دسترسی به بخش مانیتورینگ به آنها داده شده باشد، با ورود به بخش مدیریت سوابق ، امکان مشاهده لاگ ها را خواهند داشت. همچنین امکان فیلترینگ بر اساس نام کاربر، آدرس IP، تاریخ وساعت رویداد و ... نیز وجود دارد. 
۱۹.	**عدم استفاده از کلمه عبورهای قبلی**	با رویکرد امنیتی، لازم است کاربران امکان استفاده از ۳ کلمه عبور قبلی خود را نداشته باشند. یعنی در زمان تغییر کلمه عبور، نسبت به استفاده از رمز عبوری که در ۳ دوره اخیر استفاده کرده است، خطا نمایش داده شود.

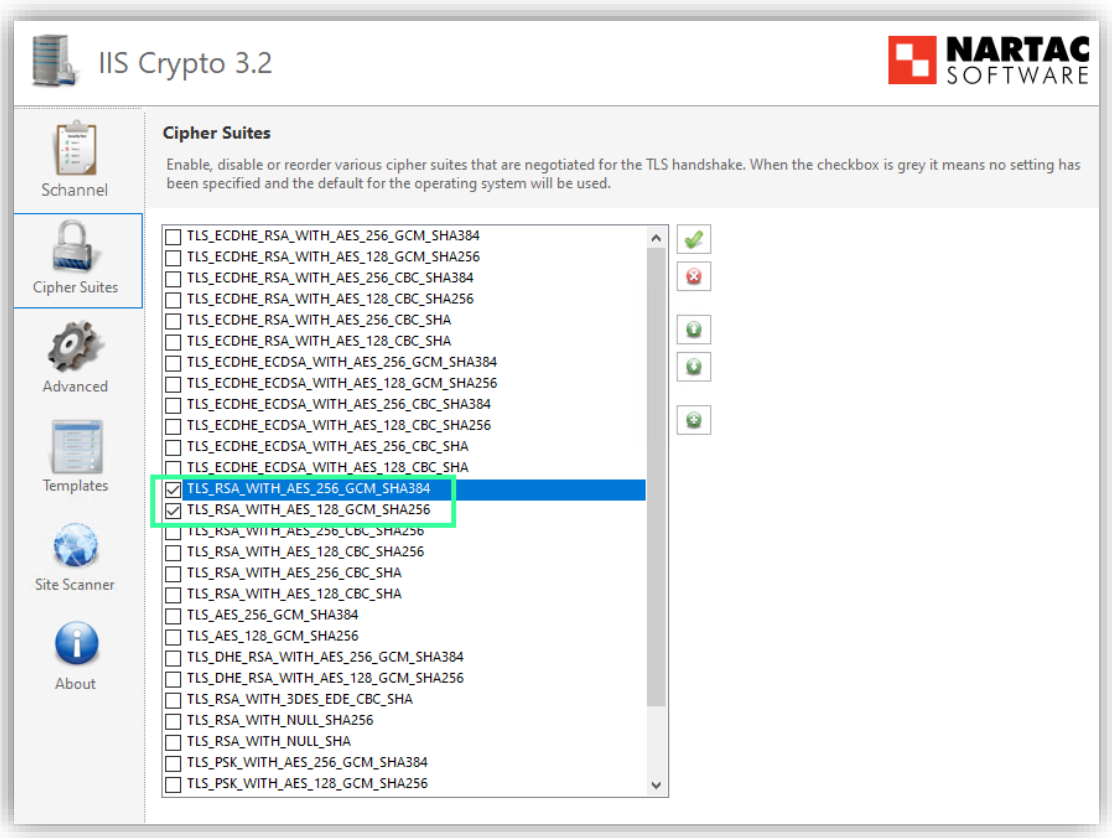
ردیف	موضوع	توضیحات و روش امن سازی
۲۰.	**استفاده از .Net Framework 4.8**	برای افزایش کارایی و امنیت نرم افزار مهنا ۱۲۱، می بایست نسخه .Net سیستم عامل کلاینت ها، نسخه 4.8 باشد.
۲۱.	**حداکثر فضای جدول لاگ**	در تنظیمات عمومی نرم افزار، قسمتی برای تعیین حداکثر فضای جدول لاگ (سری لاگ / SeriLog) وجود دارد، که تعیین کننده حجم ذخیره سازی رویدادهای ممیزی است. ادمین سیستم بر اساس فضای خالی سرور نرم افزار، این مقدار را تعیین می نماید و طبق عملکرد امنیتی محصول، زمانی که حجم لاگ های ذخیره شده به آستانه هشدار و بازنویسی لاگ ها نزدیک شود، اقدام لازم را برای ارسال هشدار و انجام عملیات بازنویسی روی قدیمی ترین لاگ ها صورت می دهد. 
۲۲.	**تعریف نقش، اختصاص ماژول و تعیین دسترسی ها به هر نقش**	در بخش **تنظیمات -> پیکربندی نرم افزار -> تعاریف پایه -> نوع : نقش** امکان تعریف یک نقش جدید، سپس تخصیص ماژول و تعیین دسترسی ها به بخش های مختلف، در نرم افزار در مسیر بالا وجود دارد.

ردیف	موضوع	توضیحات و روش امن سازی
		 

جدول موضوعات و راهنمای امن سازی محیط عملیاتی نرم افزار

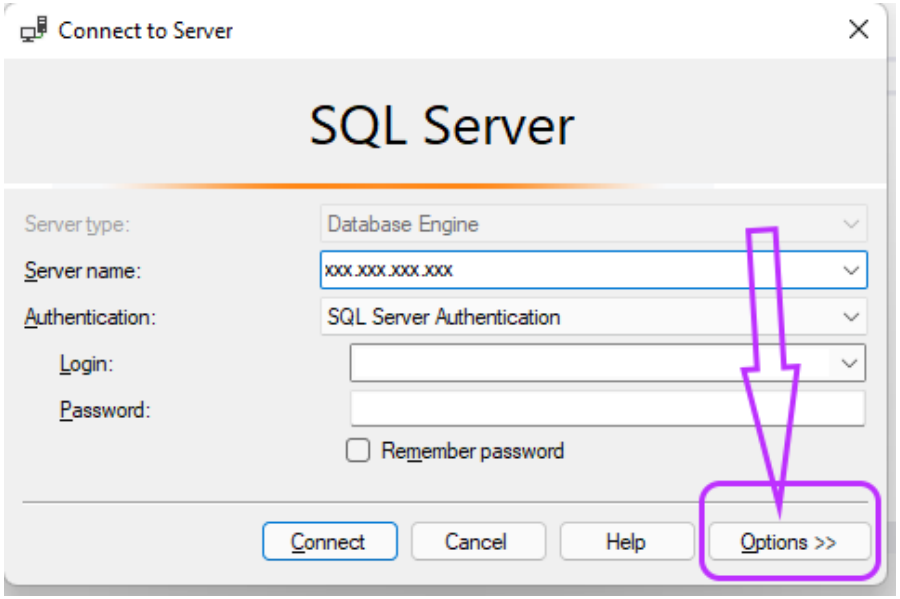
ردیف	موضوع	توضیحات و روش امن سازی
۱.	**دنباله های ممیزی[1] امن سمت سرور**	با توجه به امن بودن ارتباطات بین سرور و کلاینت در سامانه مدیریت حوادث برق و ثبت خاموشی با استفاده از پروتکل TLS 1.2، لازم است امن-سازی های لازم بر روی سیستم عامل ویندوز صورت گیرد. یکی از این امن‌سازی‌ها، غیرفعال کردن دنباله های ممیزی ضعیف و ناامن است که به صورت پیش فرض در سیستم عامل ها ممکن است فعال باشند. برای این کار می توان در Registry سیستم عامل سرور و یا با استفاده از نرم‌افزارهای جانبی (مانند IIS Crypto) ، این عملیات را صورت داد. دنباله های ممیزی مورد استفاده در ارتباطات امن نرم افزار شامل موارد زیر است: TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_GCM_SHA256 در تصاویر زیر، گزینه های مورد تایید استاندارد در تنظیمات نرم‌افزار جانبی نمایش داده شده است: 

[1] - Cipher Suites

ردیف	موضوع	توضیحات و روش امن سازی
		تنظیمات Cipher Suites : 
۲.	**دنباله های ممیزی امن سمت کلاینت**	طبق توضیحات فوق (دنباله های ممیزی امن سمت سرور)، همان روش‌ها در سیستم عامل ویندوز کلاینت نیز کاربرد دارد و قابل استفاده و پیاده سازی هستند.

ردیف	موضوع	توضیحات و روش امن سازی
۳.	**شناسایی فایل های مخرب و ویروسی**	جهت شناسایی و حذف فایل‌های مخرب سمت سرور، می بایست از آنتی‌ویروس‌های قوی که دارای لایسنس بوده و قابلیت بروزرسانی دارند، استفاده شده باشد تا در صورت آپلود فایل مخرب و ویروسی از سمت Client، کنترل‌های لازم جهت جلوگیری از اجرا شدن و فعالیت فایل مخرب در سرور صورت گیرد.

راهنمای ارتباط امن با پایگاه داده

ردیف	موضوع	توضیحات و روش امن سازی
۱.	**ارتباط امن با پایگاه داده از طریق Microsoft SQL server Management Studio**	جهت برقراری ارتباط امن با پایگاه داده از طریق نرم افزار Management Studio لازم است قبل از لاگین، از طریق گزینه options در management studio، گزینه های Encrypt Connection و Trust server certificate در تب Connection Properties تیک زده شده باشد. مطابق با تصویر زیر:  در تب Connection Properties گزینه های مذکور انتخاب شوند :

ردیف	موضوع	توضیحات و روش امن سازی