شرکت مهندسی طلوع پردیس
www.TolueTech.com

شرکت مهندسی طلوع پردیس
www.TolueTech.com

راهنمای استفاده از نرم افزار

Unis

تهران،خیابان کریمخان زند،پلاک۷۶،طبقه چهارم تلفن : ۸۸۳۱۲۰۱۰
www.TolueTech.com

فهرست مندرجات

۱. نکاتی قبل از شروع برنامه ۴
۱.۱. معرفی محصول ۴
۱.۱.۱. رئوس مطالب ۴
۱.۱.۲. پیکربندی محصول ۴
۱.۲. نصب نرم افزار ۵
۱.۳. انواع اعتبارسنجی ۵
۱.۴. مراحل استفاده از سنسور تشخیص اثر انگشت ۶
۱.۵. مراحل ثبت اثر انگشت ۹
۲. راهنمای کاربری نرم افزار Unis Manager ۱۱
۲.۱. شروع برنامه ۱۱
۲.۲. پیکربندی منو ۱۲
۲.۲.۱. نظارت ۱۲
۲.۲.۱.۱. پاک کردن همه آیتمهای لیست ۱۲
۲.۲.۲. مدیریت ترمینال ۱۳
۲.۲.۲.۱. افزودن ترمینال ۱۵
۲.۲.۲.۲. تنظیمات گزینه ترمینال ۱۶
۲.۲.۲.۳. تعیین مدیر برای ترمینال ۲۰
۲.۲.۲.۴. ارتقاء Firmware ترمینال ۲۰
۲.۲.۳. مدیریت کاربری ۲۱
۲.۲.۳.۱. افزودن کاربر ۲۲
۲.۲.۳.۲. ارسال اطلاعات کاربر به ترمینال ۲۴
۲.۲.۳.۳. مدیریت کاربری ترمینال ۲۴
۲.۲.۴. مدیریت میهمان ۲۵
۲.۲.۴.۱. اضافه کردن میهمان ۲۶
۲.۲.۵. کنترل تردد ۲۸
۲.۲.۵.۱. افزودن منطقه زمانی ۲۸

۲.۲.۵.۲. افزودن زمان تردد ۳۰
۲.۲.۵.۳. افزودن ناحیه تردد ۳۱
۲.۲.۵.۴. افزودن گروه تردد ۳۲
۲.۲.۵.۵. حذف ۳۲
۲.۲.۵.۶. ارسال به ترمینال ۳۳
۲.۲.۶. سیستم ۳۳
۲.۲.۶.۱. تغییر رمزعبور اصلی ۳۳
۲.۲.۷. مدیریت داده ها ۳۴
۲.۲.۷.۱. مدیریت ثبت وقایع ۳۴
۲.۲.۷.۱.۱. ثبت وقایع تردد ۳۴
۲.۲.۷.۱.۲. ثبت وقایع بازبینی سرور ۳۶
۲.۲.۷.۱.۳. ثبت وقایع بازبینی ترمینال ۳۷
۲.۲.۷.۱.۴. ثبت ورود مدیر ۳۹
۲.۲.۷.۲. مدیریت سازمان ۴۰
۲.۲.۷.۲.۱. مدیریت شاخه ۴۰
۲.۲.۷.۲.۲. مدیریت بخش ۴۱
۲.۲.۷.۲.۳. مدیریت عنوان شغلی ۴۲
۲.۲.۷.۳. مدیریت تعطیلات ۴۳
۲.۲.۷.۴. مدیریت اختیارات مدیر ۴۴
۲.۲.۷.۵. مدیریت Untipass back ۴۵
۲.۲.۸. ابزار ۴۶
۲.۲.۸.۱. راه اندازی طرح بندی کارت ۴۶
۲.۲.۸.۲. صدور کارت هوشمند ۵۰
۲.۲.۸.۳. تنظیمات محیطی ۵۱
۲.۲.۸.۳.۱. تنظیمات محیطی شبکه محلی ۵۱
۲.۲.۸.۳.۲. تنظیمات محیطی سرور ۵۳
۲.۲.۹. شکل دهی موقعیت(E-map) ۵۴
۲.۲.۹.۱. تنظیم موقعیت ترمینال ۵۵
۲.۲.۹.۲. تنظیم موقعیت نقشه ۵۶
۲.۲.۹.۳. نظارت شکل دهی موقعیت ۵۷
۲.۲.۱۰. سایرموارد ۶۱
۲.۲.۱۰.۱. Tray icon ۶۱
۲.۲.۱۱. اطلاعات برنامه ۶۱

۱. نکاتی قبل از شروع برنامه

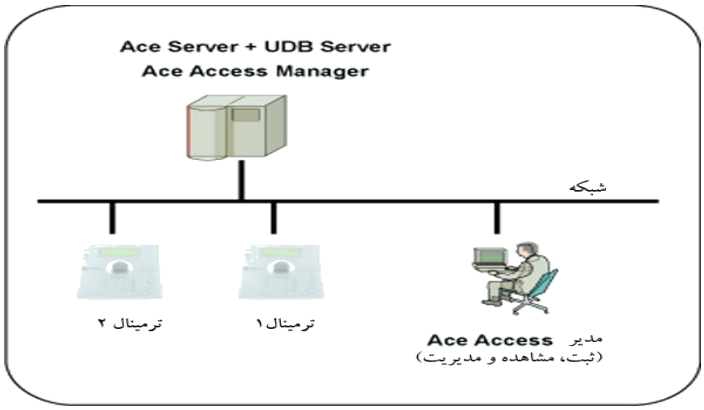
۱.۱. معرفی محصول

۱.۱.۱. رئوس مطالب

Unis برنامه ای کارآمد جهت کنترل عملکرد ترمینال تشخیص اثر انگشت و کـــــارت محسوب می شود. این برنامـه هریـک از ترمینال ها و کاربران را از طریق شبکه، مدیریت و هماهنگ می کند. مدیریت اعتبار سنجی کاربران در لحظه ورود و نیز جسـتجو و نمایش ترددهای انجام شده قبلی، توسط این برنامه امکان‌پذیر است.

این راهنما به تشریح نحوه نصب برنامه Unis می پردازد که قادر است از طریـق برقـراری ارتبـاط بـا ترمینـال، امکـان مـدیریت و مشاهده آن را فراهم نماید.

۱.۱.۲. پیکربندی محصول



۱.۲. نصب نرم‌افزار

پس از قرار دادن CD برنامه، فرایند نصب بطور خودکار آغاز خواهد شد. در غیر این صورت، جهت شروع عملیات نصب به طور دستی، فایل Setup.exe موجود در CD را اجرا نمایید.

۱.۳. انواع اعتبارسنجی

اعتبارسنجی‌کاربران به صورت های ذیل قابل انجام است؛ همچنین می‌توان از ترکیب این حالت ها استفاده کرد.

- اعتبارسنجی اثر انگشت : روشی است که با استفاده از اثرانگشت، صحت اعتبارسنجی را تایید می کند و به یکی از دو طریق زیر انجام می‌گردد.

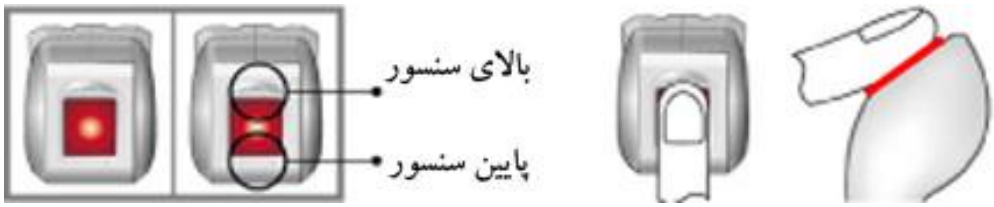
- اعتبارسنجی ۱:۱ : در این حالت ابتدا برای هر کاربر شناسه‌ای را وارد می‌کنیم، سپس انگشت را قرار می‌دهیم. اثر انگشت وارد شده تنها با انگشت ثبت شده این کاربر (با شناسه وارد شده) مقایسه می‌شود. این روش زمان بسیار کمی را صرف می‌کند.
- اعتبارسنجی ۱:N : در این حالت اثر انگشت وارد شده که بدون شناسه کاربر است، با تمام اثر انگشت‌های ثبت شده مقایسه می‌گردد. این روش بسیار ساده است و در مقایسه با حالت قبل و زمانی‌که تعداد کاربران زیاد باشد، زمان بیشتری صرف می‌نماید.
- اعتبارسنجی کارت اثر انگشت: پس از وارد نمودن اطلاعات اثر انگشت کاربر در کارت هوشمند، اثر انگشت وارد شده طی اعتبارسنجی با اثر انگشت ثبت شده در کارت هوشمند مقایسه می‌گردد. از آنجایی که در این روش هیچ وسیله ی ذخیره سازی به غیر از کارت هوشمند مورد استفاده قرار نمی‌گیرد، امنیت سیستم به میزان قابل توجهی ارتقاء پیدا خواهد کرد.
- اعتبارسنجی رمز ورود: در این روش، اعتبارسنجی با ورود و مقایسه یک رمز ۴ تا ۸ رقمی انجام می‌شود. زمانی که استفاده از اثر انگشت مقدور نباشد، از رمز ورود استفاده می‌نماییم.
- اعتبارسنجی کارت: در این روش کارت RF کاربران مورد اعتبارسنجی قرار خواهد گرفت. ابتدا بایستی شماره کارت را در سیستم ثبت نمود تا بتوان از آن استفاده کرد.

۱.۴. مراحل استفاده از سنسور تشخیص اثر انگشت

- ثبت ابتدایی اثر انگشت: ثبت ابتدایی اثر انگشت، مهمترین بخش در فرایند تشخیص توسط سنسور شناسایی اثر انگشت است. انگشت باید به دقت و درستی ثبت گردد تا در اعتبارسنجی به سهولت قابل تشخیص باشد.
- انگشت‌های مورد استفاده در مرحله ثبت: استفاده از انگشت سبابه و انگشت های میانی جهت ثبت بهتر است؛ همچنین استفاده از انگشت شست یا انگشت کوچک توصیه نمی شود؛ زیرا قرار دادن صحیح شست و انگشت کوچک روی محفظه سنسور تشخیص اثرانگشت مشکل است و این امر دریافت تصویر دقیقی از اثر انگشت را دشوار می سازد.
- مراحل ورود صحیح اثر انگشت:

۱- وقتی سنسور شروع به چشمک زدن می‌کند، انگشت را روی آن قرار دهید.

۲- پس از قرار دادن نوک انگشت روی سنسور، به بالای پنجره سنسور که در شکل زیر نشان داده شده است، دقت کنید. انگشت را بدون حرکت اضافه طوری روی پنجره سنسور قرار دهید که نوک آن بین قسمت بالایی و پایینی سنسور باشد.



۳- انگشت خود را با فشار مناسب روی سنسور قرار دهید؛ مانند زمانی که روی استامپ انگشت می‌زنید. فشار خیلی کم یا زیاد به سنسور وارد نکنید.

۴- انگشت نباید به بالا، پایین، چپ یا راست متمایل شود؛ همچنین نباید تنها نوک انگشت را روی سنسور گذاشت و یا اینکه در حال اسکن انگشت را حرکت داده یا چرخاند. شکل زیر حالت های نادرست را نشان داده است.

- روش صحیح ثبت اثر انگشت: وقتی اثر انگشت وارد گردید، پس از مشاهده تصویر اثر انگشت وارد شده، می‌توان آن را تغییر داد. اگر وضعیت نمایش داده شده مناسب نبود، می‌توان اثر انگشت دیگری از کاربر را ثبت نمود. رعایت موارد زیر در اثر انگشت ثبت شده الزامی است.
  - محل مرکز اثر انگشت: مرکز اثر انگشت جایی است که بیشترین خمیدگی را دارد. در شکل زیر، قسمت داخلی دایره آبی، ناحیه مرکز اثر انگشت را نشان می‌دهد. عموماً این ناحیه، در مرکز اثر انگشت قرار گرفته است. توجه به ناحیه مرکزی اثر انگشت به ثبت درست آن کمک می‌کند. این ناحیه مرکزی باید در وسط محفظه سنسور قرار گیرد. اثرانگشت‌های ثبت شده نبایستی نسبت به محور عمودی دوران داشته باشند، بلکه باید کاملاً عمودی واقع شوند. توجه به شکل های زیر ضروری است.

محل صحیح قرار دادن ناحیه مرکزی انگشت

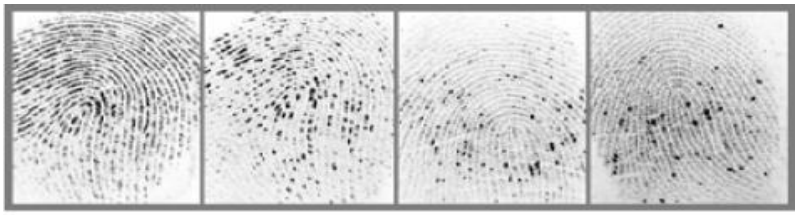
قرار دادن نادرست ناحیه مرکزی انگشت روی صفحه سنسور

مسیر نادرست ورودی(دوران عمودی)

- کیفیت تصویر اثر انگشت: وضعیت انگشت الگو و ساختار شیارهای آن، کیفیت تصویر اثر انگشت را تعیین می‌کنند. انگشت های دارای جای زخم یا ترکهای عمیق، انگشت های واجد شیارهای کم در اثر بیماری، انگشت های خیلی خشک یا انگشت های خیس، معمولاً کیفیت تصویر نامناسبی ایجاد می‌نمایند.

اثر انگشتهای خیس

اثر انگشت هایی که در بالا نشان داده شده‌اند، توسط انگشت های خیس یا در اثر اعمال فشار زیاد در هنگام ثبت ایجاد شده‌اند. راه حل این مشکل، کاهش اعمال فشار در حین ثبت یا خشک کردن انگشت با یک حوله می‌باشد. انجام این کارها به تولید اثر انگشت با کیفیت مناسب کمک می‌کند.



اثر انگشتهای خشک

اثر انگشت هایی که در بالا نشان داده شده، به علت وارد آوردن فشار کم انگشت در هنگـــــام ثبت یا خشک‌بودن انگشـت ایجـاد شده‌اند. برای حل این مشکل هنگام ثبت، انگشت خود را کمی بیشتر روی صفحه سنسور فشار داده یا در آن بدمیـد. (بـه خصـوص در زمستان)

انگشتهای دارای ترک

تصاویراثر انگشت های بالا به دلیل وجود ترک یا آثار زخم و یا بیماری هایی مانند سودا ایجاد شده‌اند. در صورت ثبت این انگشتان، پس از بهبود زخم یا بیماری، اعتبارسنجی ممکن نبوده و دسترسی این کاربران با مشکل روبرو خواهد شد؛ بنابراین از ثبـت نمـودن این انگشتان خودداری کرده و از انگشت دیگری استفاده نمایید.

رعایت این سه شرط برای ایجاد یک اثر انگشت با تصویر مناسب لازم است:

ناحیه مرکزی اثر انگشت در وسط پنجره سنسور قرار گیرد.

نقش اثر انگشت تمام تصویر را پر نماید.

خطوط برآمده (خطوط مشکی) و خطوط مربوط به فرورفتگیها و شیارهای (خطوط سفید) اثر انگشت به وضـوح از یکـدیگر متمـایز باشند.

دسترسی نادرست و رد کردن نادرست: کیفیت نامناسب تصویر اثر انگشت، عدم ثبت مشخصات صحیح انگشت یا عدم انطباق ناحیه مرکزی انگشت و مرکز صفحه سنسور در هنگام ثبت، سبب بروز مشکلات زیادی می‌گردد. برخی از این مشکلات عبارتند از:

رد نادرست: این اتفاق حالتی را نشان می‌دهد که تست اعتبارسنجی یک انگشت ثبت شده ناموفق بوده و کاربر شناسایی نمی‌شود. اگر شرایط اثر انگشت ثبت شده نامناسب باشد، اعتبارسنجی به احتمال زیاد ناموفق بوده و کاربر شناسایی نمی‌شود. باید به این نکته نیز توجه کرد که ثبت اولیه اثر انگشت شرط لازم برای اعتبارسنجی موفق است ولی کافی نیست. به عبارت دیگر حتی اگر ثبت اولیه به درستی انجام شود ولی در دفعات بعدی انگشت کاربر وضعیت خوبی نداشته باشد، احتمال عدم تشخیص اثر انگشت وی وجود دارد. عواملی مانند شرایط ورود اثر انگشت و کیفیت تصویر انگشت در بروز این اتفاق مؤثرند.

۱- تایید نادرست: این مسئله زمانی رخ می دهد که اثر انگشت شخص دیگری به جای کاربر ثبت شده تأیید می‌شود. بطور کلی این اتفاق اغلب زمانی روی می‌دهد که اثر انگشت با مشخصات ناقص و ناکافی یا بدون ثبت صحیح محدوده مرکزی اثر انگشت ثبت شده باشد. همچنین گاهی شباهت بین ساختار اثر انگشت ها موجب بروز این اتفاق می‌گردد.

۲- سطح امنیت اعتبارسنجی: این عدد مبین میزان دقت در مقایسه بین اثر انگشت وارد شده با اثر انگشت ثبت شده می باشد. وقتی سطح امنیت اعتبارسنجی کاهش پیدا می‌کند، از میزان رد کردن‌های نادرست کاسته می‌شود. این در حالیست که تأییدهای نادرست افزایش می‌یابد؛ بالعکس اگر سطح امنیتی افزایش یابد، رد کردن نادرست زیاد شده و تأیید نادرست کاهش پیدا می‌کند. به همین دلیل، هر جا با هر سیستم اعتبار سنجی اثر انگشت از یک سطح امنیتی مناسب خود استفاده می‌کند. تنظیم سطح امنیتی پیش فرض می‌تواند برای اعمال مقاصد عمومی سیستم اعتبارسنجی به کار گرفته شود.

۱.۵. مراحل ثبت اثر انگشت:

این مراحل برای ثبت اثر انگشت از طریق سنسور تشخیص اثر انگشت (درایو رومیزی یا اصطلاحاً Hamster) با برنامه Unis انجام می‌شود.

1- این پنجره ابتدایی ثبت اثر انگشت است . برای عدم نمایش آن در دفعات بعدی، تیک موجود در باکس را بردارید

2- یک انگشت برای ثبت کردن انتخاب نمایید.

3- انگشت خود را روی صفحه سنسور بگذاید.

4- سپس انگشت خود را از روی سنسور بردارید.

5- مجدداً انگشت خود را روی صفحه سنسور بگذارید.

6- اگر اثر انگشت به درستی وارد شده باشد، عبارت OK نمایش داده می شود تا به مرحله بعد بروید.

7- اثر انگشت های ثبت شده به رنگ سبز نمایش داده می شوند اگر ثبت اثر انگشت ها به پایان رسید، دکمه NEXT را بزنید تعداد اثر انگشت ها در نرم افزار از قسمت [Server Option Setting] قابل تنظیم است.

8- ورود اثر انگشت ها به پایان رسید.
برای اتمام دکمه Finish را بزنید..

۲. راهنمای کاربری نرم‌افزار Unis Manager

۲.۱. شروع برنامه

تنها کاربرانی که به عنوان مدیر ثبت شده باشند، می‌توانند از این برنامه استفاده نمایند. پس از نصب و در اولین اجرا که هنوز کاربری به عنوان مدیر تعریف نشده است، می‌توان به عنوان مدیر اصلی وارد برنامه شد. رمز ورود اولیه مدیر اصلی پس از نصب به صورت پیش فرض عدد «۱» است.

برای اجرای برنامه روی آیکون موجود در دسکتاپ دو بار کلیک نمایید. وقتی پنجره ورود باز شد، طبق شکل مقابل مربع کنار عبارت «ورود مدیر اصلی سیستم» را علامت زده و عبارت ۱ را در قسمت رمز وارد نمایید. پس از نصب برنامه، رمز ابتدایی را با انتخاب «تغییر رمز اصلی» از منوی «سیستم» تغییر دهید.

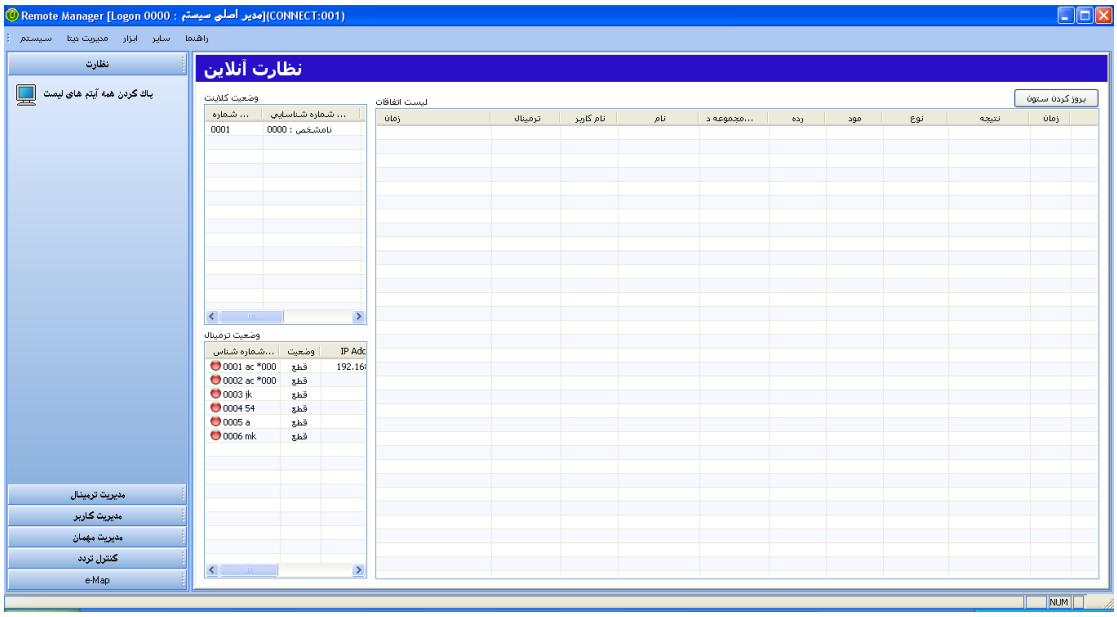
۲.۲. پیکربندی منو

۲.۲.۱. نظارت

نظارت بر وضعیت اعتبارسنجی و اطلاعات تردد کاربران ثبت شده، وضعیت اتصال ترمینال‌ها به سرور و وضعیت دسترسی به سرور Unis به لحظه قابل کنترل است.

۲.۲.۱.۱. پاک کردن همه آیتم‌های لیست

با فشردن این گزینه اطلاعات تمام ترددها پاک خواهد شد.



فهرست ترددهای انجام شده کاربران نمایش داده می‌شود. ستونهای این جدول عبارتند از:

- **زمان**: تاریخ و ساعت دسترسی نمایش داده می‌شود.

- **شماره شناسایی ترمینال**: شماره ترمینالی که اعتبارسنجی را انجام داده نمایش داده می‌شود.

- **شماره شناسایی کاربر**: شناسه کاربر اعتبارسنجی شده نمایش داده می‌شود.

- **نام شخص**: نام کاربر اعتبارسنجی شده نمایش داده می‌شود.

- **مُد**: در صورت ثبت مُدهای F۱، F۲، F۳ یا F۴ ، مُد اعتبارسنجی نمایش داده می‌شود.

- **نوع** : نوع اعتبارسنجی که یکی از موارد کارت، رمز، کارت اثر انگشت، ۱:۱، N:۱ است نمایش داده می‌شود.

- **نتیجه**: نتیجه اعتبارسنجی که موفقیت یا شکست می‌باشد، نمایش داده می‌شود.

وضعیت کلاینت

وضعیت کلاینتی که به سرور متصل شده، در این قسمت نشان داده می‌شود. این اطلاعات شامل موارد زیر است:

- **شناسه کلاینت**: شناسه کلاینتی که به سرور متصل شده نمایش داده می‌شود.

- **شناسه مدیر**: شناسه مدیری که از این کلاینت استفاده می‌کند نمایش داده می‌شود.

- **آدرس IP** : IP کامپیوتری که کلاینت از طریق آن متصل شده، نمایش داده می‌شود.

- **نسخه** : نسخه کلاینتی که به سرور متصل شده، نمایش داده می‌شود.

وضعیت ترمینال

وضعیت ارتباط ترمینال با سرور قابل مشاهده بوده و شامل موارد زیر است:

- **نام ترمینال**: شناسه و نام ترمینال ثبت شده نمایش داده می‌شوند.

- **وضعیت**: وضعیت اتصال یا عدم اتصال ترمینال مشخص می‌گردد. اگر ترمینالی متصل باشد، چراغ سبز نمایش داده می‌شود و در صورت عدم برقراری ارتباط، چراغ قرمز در این قسمت ظاهر می‌گردد.

- **آدرس IP** : IP ترمینال متصل شده، نمایش داده می‌شود.

- **نسخه**: نسخه ترمینال که شامل اطلاعاتی از قبیل Firmware، پروتکل، و کارتخوان هستند، نمـــایش داده می‌شود.

۲.۲.۲. مدیریت ترمینال

اضافه کردن، حذف، تغییر و اعمال تنظیمات ترمینال‌ها، برای هر ترمینال قابل انجام است.

یک ترمینال جهت اتصال به سرور نخست بایستی ثبت گردد.

◄ افزودن ترمینال: در منوی[مدیریت ترمینال] گزینه[افزودن ترمینال] را انتخاب کنید.

◄تغییر ترمینال: در پنجره فهرست ترمینال ها روی نام ترمینال مورد نظر جهت تغییردادن آن دوبارکلیک کنید.

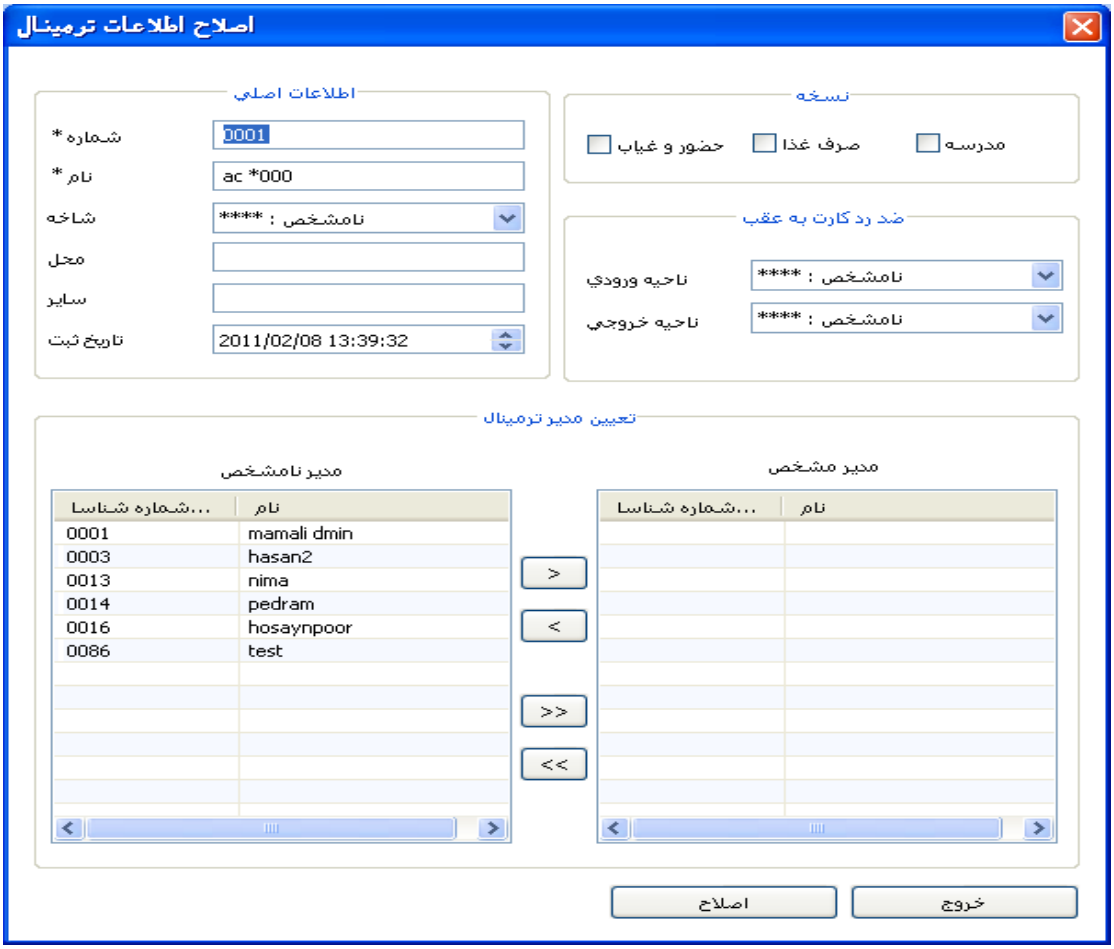
◄حذف ترمینال: در پنجره فهرست ترمینال ها، در کادر مقابل نام ترمینال موردنظر جهت حذف آن علامتگذاری و گزینه [حذف ترمینال] را انتخاب کنید.

ستونهای این جدول عبارتند از:

- شناسه: شناسه ترمینال نمایش داده می شود.
- نام: نام ترمینال نمایش داده می شود.
- شاخه: شاخه نصب ترمینال نمایش داده می شود.
- عملکرد: مجموعه عملکرد موجود در ترمینال عبارتند از: مدیریت حضور و غیاب، مدیریت سرویس غذا و مدیریت مدرسه به نمایش درمی آید.
- Anti pass back: استفاده یا عدم استفاده از آپشن«عدم رد کارت به عقب» در ترمینال به نمایش در می آید.
- منطقه ورود: منطقه ورود «Anti pass back» ترمینال به نمایش در می آید.
- منطقه خروج: منطقه خروج «Anti pass back» ترمینال به نمایش در می آید.

- موقعیت: محل نصب ترمینال به نمایش در می آید.
- آدرسIP: آدرسIP ترمینال به نمایش در می آید.
- نسخه: نسخه میان افزاری ترمینال به نمایش در می آید.

۲.۲.۲.۱. افزودن ترمینال



- اطلاعات پایه
- شناسه: تخصیص شماره شناسه به ترمینال را در این قسمت انجام دهید.
- نام: در این بخش نام ترمینال را وارد کنید.
- شاخه: از میان شعبی که در منوی[مدیریت شعبه] ثبت گردیده، یک شاخه را انتخاب نمایید.
- موقعیت: محل نصب ترمینال را در این قسمت وارد کنید.
- سایرموارد: در اینجا سایر آیتم های موجود در ترمینال را وارد کنید.
- تاریخ ثبت: تاریخ و ساعت ثبت ترمینال را در اینجا تنظیم نمایید.

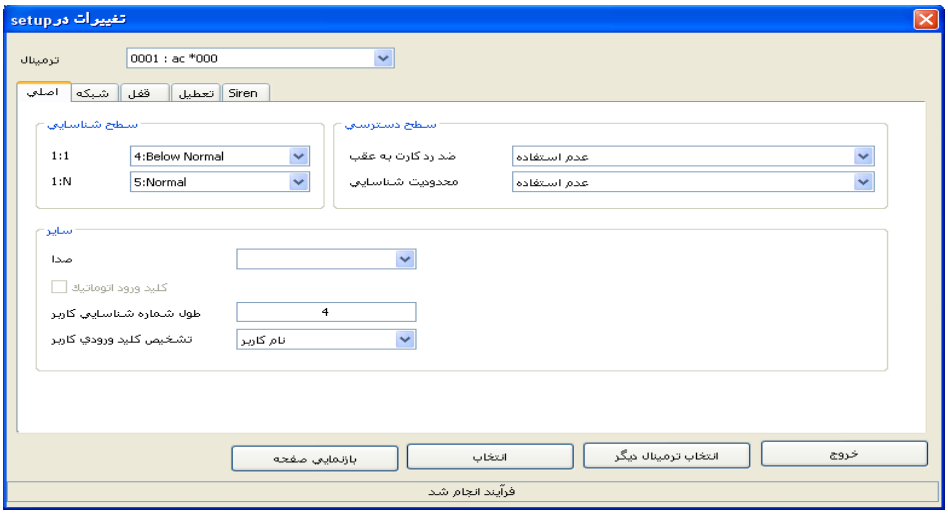
- تعیین کارکرد ترمینال
- حضور و غیاب: چنانچه کارکرد ترمینال حضور و غیاب می باشد، کادر مقابل این گزینه را علامتگذاری کنید.
- وعده غذایی: چنانچه کارکرد ترمینال مدیریت سرویس غذا می باشد، کادر مقابل این گزینه را علامتگذاری کنید.
- مدرسه: چنانچه کارکرد ترمینال مدیریت مدرسه می باشد، کادر مقابل این گزینه را علامتگذاری کنید.
- عدم رد کارت به عقب
- منطقه ورود: در این قسمت کد ثبت شده در منوی[ثبت Anti pass back] را قرار دهید.
- منطقه خروج: در این قسمت کد ثبت شده در منوی[ثبت عدم رد کارت به عقب] را قرار دهید.
- تعیین مدیر ترمینال
- در این قسمت یک مدیر برای ترمینال تعریف می شود.
- فهرستی از کاربرانی که صلاحیت مدیریت ترمینال دارند و در حوزه کنترل تردد در منوی [ثبت مدیریت] ثبت شده اند، در قسمت «مدیر نامعین» به نمایش گذاشته می شود.
- پس از انتخاب یک کاربر به عنوان مدیر، با استفاده از دکمه > نام کاربر منتخب را به لیست «مدیر معین» انتقال دهید.

۲.۲.۲.۲. تنظیمات گزینه ترمینال

با اتصال ترمینال، تنظیمات گزینه های انتخابی آن تایید و اعمال می گردد.

پس از انتخاب ترمینال مورد نظر از پنجره فهرست ترمینال ها، دکمه Setup Options را فشار دهید.

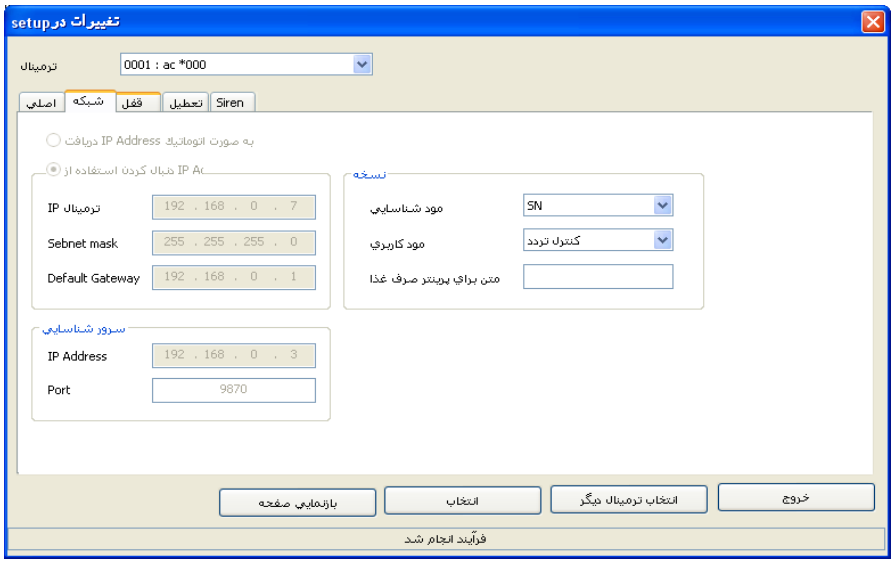
- تنظیمات اولیه



- سطح اعتبارسنجی
- ۱:۱: مقدار سطحی است که در طول اعتبارسنجی۱:۱ در ترمینال تشخیص اثرانگشت استفاده می شود.
- N:۱: مقدار سطحی است که در طول اعتبارسنجیN:۱ در ترمینال تشخیص اثرانگشت استفاده می شود.
- سطح دسترسی
- Anti pass back: مقداری است که به عدم رد کارت به عقب اختصاص می یابد.
  - -عدم استفاده: در این حالت، گزینه Anti pass back در ترمینال تنظیم نشده است.
  - -اجازه دسترسی در هنگام قطع ارتباط: در موقع قطع ارتباط، امکان دسترسی برای همه کاربران فراهم است.
  - ممنوعیت دسترسی در هنگام قطع ارتباط: در موقع قطع ارتباط، امکان دسترسی برای هیچ یک ازکاربران فراهم نیست.

- محدودیت اعتبارسنجی: در این قسمت، وجود و یا عدم وجود محدودیت اعتبارسنجی در ترمینال تعیین می شود.
- سایر موارد
- بکارگیری پیغام صوتی: ترمینال با استفاده از پیغـــام صوتی موفقیت اعتبارسنجی را اعـــلام می نماید.
- بکارگیری کلید ورود اتوماتیک: پس از وارد نمودن شناسه کاربری در ترمینال، بدون کلید ورود امکان استفاده از آن وجود دارد.
- طول شناسه کاربری(۸-۱): در این قسمت طول شناسه کاربری تعیین می شود.
- کلید کاربری: تعیین نوع شماره شناسه ای که بایستی حـین اعتبارسـنجی ۱:۱ وارد گـردد؛ شناسـه کـاربری یـا شناسـه اختصاصی در این بخش انجام می پذیرد. شناسه کاربری کلید پیش فرضی است که در برنامـه اسـتفاده مـی شـود و ایـن مقدار حداکثر یک عدد ۸ رقمی می تواند باشد. اگر یک کلید بیش از ۹رقمـی موردنیـاز باشـد، از شناسـه اختصاصـی بـه عنوان کلید استفاده نمایید.

تنظیمات شبکه



- استفاده از آدرس IP خودکار: در این صورت ترمینال با IP دینامیک تنظیم می گردد.
- استفاده از آدرس IP زیر:
  - IP ترمینال: IP ثابتی که به ترمینال تخصیص یافته، در این قسمت به نمایش در می آید.
  - subnet mask :subnet mask ترمینال به نمایش گذاشته می شود.
  - Gateway پیش فرض: Gateway ترمینال نمایش داده می شود.
  - IP سرور اعتبارسنجی: آدرس IP مربوط به سرور اعتبارسنجی جهت اتصال ترمینال نشان داده می شود.
  - پورت سرور اعتبارسنجی: پورت مربوط به سرور اعتبارسنجی جهت اتصال ترمینال نشان داده می شود.
  - مد اعتبارسنجی: مد اعتبارسنجی ترمینال به نمایش گذاشته می شود.

-NS: نخست، اعتبارسنجی با سرور انجام می شود. در صورتی که سرور قطع باشند، اعتبارسنجی با ترمینال انجام می گردد.

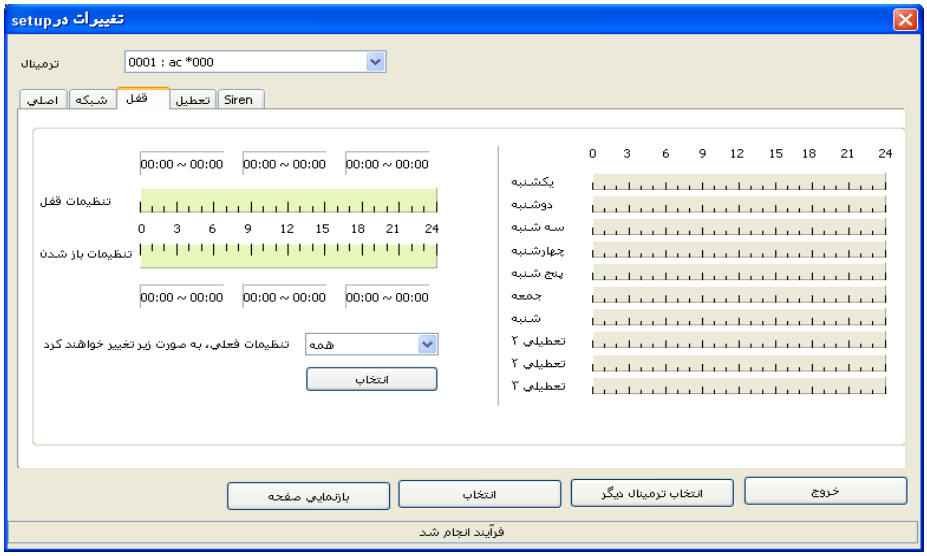
-SN: نخست، اعتبارسنجی با ترمینال انجام می شود. چنانچه کاربر اعتبارسنجی شده در ترمینال موجود نباشد، اعتبارسنجی با سرور انجام می گردد.

-NO: اعتبارسنجی فقط با سرور انجام می شود.

- حالت عملیاتی: حالت عملیاتی انتخاب شده از میان کنترل تردد، مدیریت حضور و غیاب و مدیریت سرویس غذا، نمایش داده می شود.
- متن برای چاپگر غذا: در این قسمت، متنی که با پرینتر متصل به ترمینال چاپ می شود، تنظیم می گردد.

⊙تنظیمات قفل

این عملکرد در ترمینال ورودی-خروجی ، باز یا قفل بودن آن را تنظیم می کند.



- تنظیمات قفل: برای محدود کردن دسترسی کاربر (اعتبارسنجی) بوسیله ترمینال از این گزینه استفاده می شود.
- تنظیمات باز: این قسمت بدون محدودیت اعتبارسنجی، برای باز گذاشتن ترمینال استفاده می شود.
- مراحل تنظیم زمان:

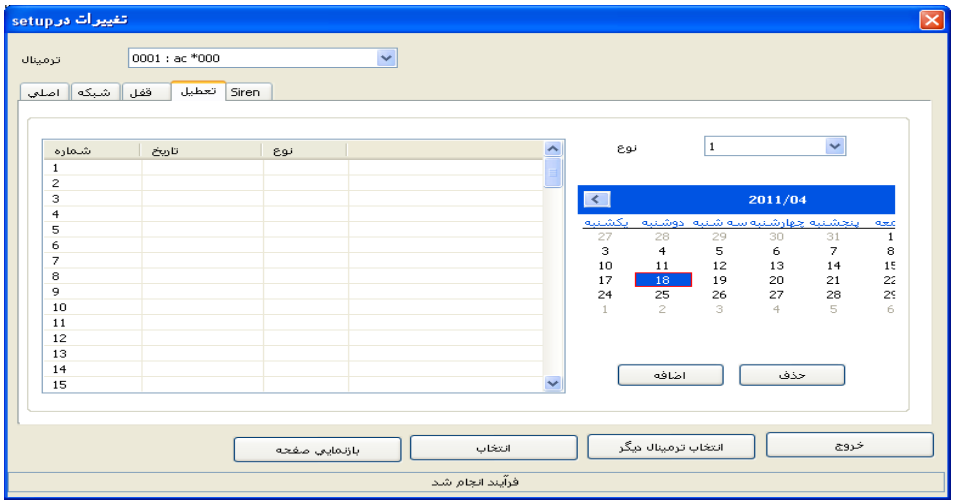
۱)پس از کلیک کردن دکمه موس اسلایدری ظاهر می شود که می توانید با درگ کردن خطوط مرزی آن به چپ و راست، زمان را تنظیم نمایید (این کارحداکثر ۳ بار امکانپذیر است). تنظیمات زمان در واحد ۵ دقیقه ای انجام می شود. ضمناً زمان قفل و بازشدن نمی تواند یکسان باشد.

۲) وقتی پس از انتخاب یک روز هفته، دکمه "اجرا" کلیک شود، روز مربوطه اعمال می شود.

- تعطیلات نیز قابلیت تنظیم داشته و به صورت تعطیلات ۳-۱ معین می گردند.

⊙ تنظیم تعطیلات

این قسمت جهت ثبت تعطیلات برای تنظیمات قفل یا بازشدن به کار می رود.



۱) از لیست عددی را برای تنظیم کردن انتخاب نموده و نوع تعطیلی را مشخص کنید.
۲) نوع تعطیلی به صورت ۱ تا ۳ طبقه بندی و تعیین می شود.
۳) تاریخ تعطیلی را انتخاب و دکمه [ثبت] را بفشارید تا آن را به عنوان تاریخ تعطیلی اختصاص دهد. می توانید حداکثر تعداد۱۰۰ تعطیلی را ثبت نمایید.

۲.۲.۲.۳. تعیین مدیر برای ترمینال

ترمینال توسط هر مدیری که برای آن تعریف شده، اداره می شود. مدیر ترمینال کاربری است که توانایی استفاده از منوهای ترمینال را دارد. در مواقعی که بیش از یک مدیر برای ترمینال ثبت گردد، روند اعتبارسنجی مدیر برای وارد شدن به منوی تنظیمات ضرورت می یابد.

پس از انتخاب یک مدیر از لیست موجود، یک ترمینال را از فهرست«ترمینالهای تخصیص داده نشده» انتخاب کنید تا ثبت گردد. سپس دکمه [>] را بفشارید تا به لیست« ترمینال های تخصیصی» انتقال یابد.

فهرستی از کاربرانی که صلاحیت مدیریت ترمینال را دارا می باشند، در قسمت[ثبت حق مدیریت] به نمایش در می آید.

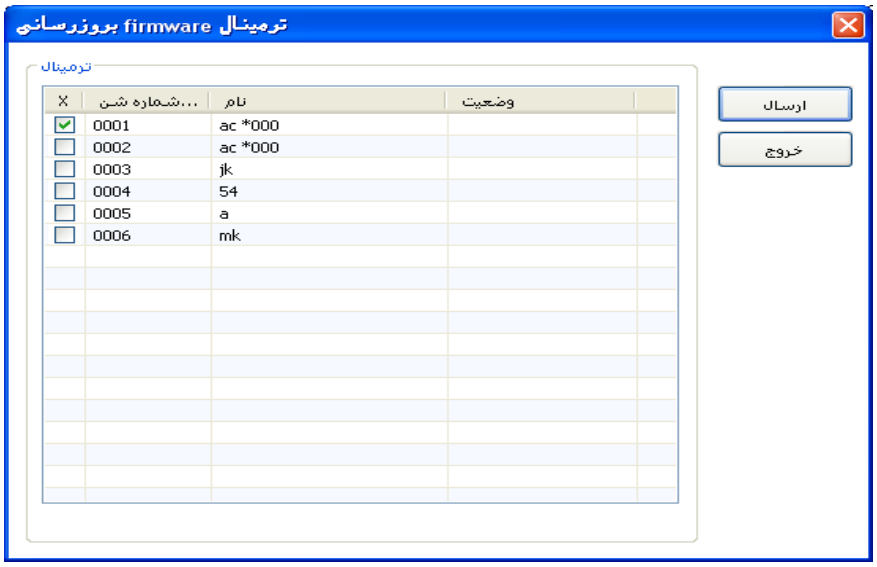
۲.۲.۲.۴. ارتقاء Firmware ترمینال

Firmware ترمینال قابلیت ارتقاء یافتن دارد.

دکمه [Upgrade Firmware] را بفشارید تا مسیر فایل Firmware را بیابید. آنگاه دکمه [Open] را فشار دهید.

ترمینال موردنظر را جهت ارتقاء انتخاب و دکمه [Send] را بفشارید تا Firmware را ارتقا دهد.

※اگر شما طی انجام عملیات ارتقاء Firmware ، ترمینال را خاموش کنید، عملکرد داخلی نرم افزار متوقف شده و ترمینال غیرقابل استفاده می شود. بنابراین حین ارتقاء Firmware احتیاطهای لازم را بعمل آورید.



۲.۲.۳. مدیریت کاربری

این قسمت شامل فهرستی از کاربران ثبت شده است.

◄افزودن کاربر: در بخش [مدیریت کاربر] گزینه[افزودن کاربر] را انتخاب کنید.

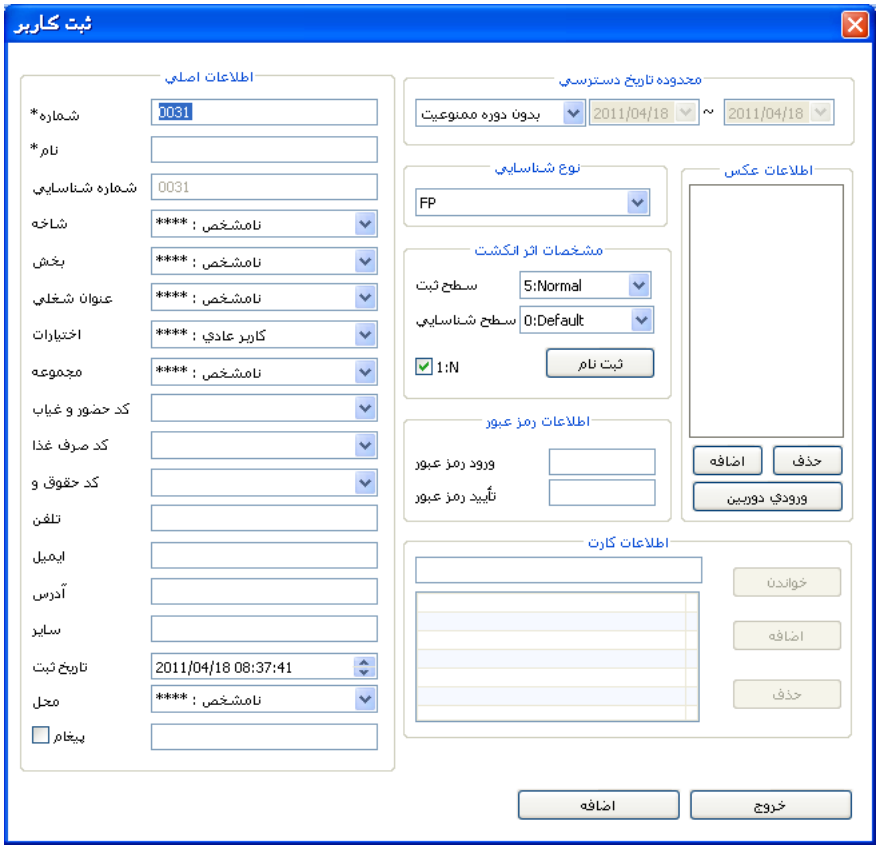
◄ویرایش کاربر: در پنجره لیست کاربران، برای تغییر کاربر روی آن دوبار کلیک کنید.

◄حذف کاربر: به منظور حذف یک کاربر، آن را از لیست کاربران انتخاب و سپس گزینه[حذف کاربر] را انتخاب نمایید.

عناوین ستونهای این جدول عبارتند از:

- شناسه: شناسه کاربری نمایش داده می شود.
- نام: نام کاربری نمایش داده می شود.
- شناسه اختصاصی: شناسه اختصاصی کاربر نمایش داده می شود.
- شاخه: وضعیت شغلی کاربر مربوطه را نشان می دهد.
- گروه: گروه کاربر مربوطه نشان داده می شود.
- سمت: عنوان کاربر در شرکت نشان داده می شود.
- گروه دسترسی: گروه کنترل دسترسی کاربر نشان داده می شود.
- اختیارات: اختیارات مدیر کاربر نمایش داده می شود.
- T/A: کد حضور و غیاب کاربر نمایش داده می شود.
- لیست پرداختی: کد دستمزد ساعتی کاربر نمایش داده می شود.
- وعده غذایی: کد سرویس غذای کاربر نمایش داده می شود.

۱.۳.۲.۲. افزودن کاربر



- اطلاعات اولیه
- شناسه: در این بخش شناسه کاربر را تخصیص دهید.

- نام: نام کاربر را وارد کنید.
- شناسه اختصاصی: شناسه اختصاصی کاربر را وارد کنید.
- شاخه: در اینجا کد وضعیت شغلی ثبت شده در [ثبت شاخه] را قرار دهید.
- گروه: در این محل کد گروهی را که در منوی [ثبت گروه] ثبت گردیده، تخصیص دهید.
- سمت: در اینجا کد عنوانی [ثبت سمت] بگذارید.
- اختیارات: کد اختیارات مدیر را که در قسمت [ثبت اختیارات مدیر] ثبت گردیده، قرار دهید.
- گروه دسترسی: کد گروه دسترسی ثبت شده در منوی[تنظیمات گروه دسترسی] را تخصیص دهید.
- کد T/A: کد حضور و غیاب را قرار دهید.
- کد لیست پرداختی: کد لیست پرداختی را بگذارید.
- تلفن: شماره تلفن را وارد نمایید.
- آدرس ایمیل: آدرس ایمیل را وارد کنید.
- سایر: آیتم های دیگر را وارد کنید.
- تاریخ ثبت شده: تاریخ و ساعت ثبت کاربر، بطور خودکار وارد می شود.
- موقعیت: محل فعلی کاربر در قسمت[ثبت عدم رد کارت به عقب]
- محدوده تاریخ تردد:
- عدم محدودیت زمانی: در این حالت یک کاربر می تواند به همه آیتم ها دسترسی داشته باشد.
- دوره زمانی مجاز: در این حالت می توانید دوره زمانی مجاز جهت تردد کاربر را تعیین کنید.
- دوره زمانی محدود: در این حالت می توانید دوره زمانی محدود جهت تردد کاربر را مشخص نمایید.
- انواع اعتبارسنجی:
- FP: اعتبارسنجی اثرانگشت
- FP –کارت: اعتبارسنجی کارت-اثرانگشت
- PW: اعتبارسنجی رمزعبور
- کارت: اعتبارسنجی کارت
- کارت یا FP: اعتبارسنجی اثر انگشت یا کارت
- کارت و FP: اعتبارسنجی اثر انگشت و کارت
- کارت یا PW: اعتبارسنجی رمزعبور یا کارت
- کارت و PW: اعتبارسنجی رمزعبور و کارت
- (شناسه یا کارت) و FP: اعتبارسنجی شناسه یا کارت و اعتبارسنجی اثرانگشت
- (شناسه یا کارت) و PW: اعتبارسنجی شناسه یا کارت و اعتبارسنجی رمزعبور
- FP و PW: اعتبارسنجی رمزعبور و اثر انگشت
- FP یا PW: اعتبارسنجی رمزعبور یا اثر انگشت

اطلاعات اثرانگشت: دکمه Enroll را بفشارید تا یک اثرانگشت ثبت شود. برای کسب اطلاعات بیشتر در خصوص مراحل ثبت اثرانگشت، به بخش [مراحل ثبت اثرانگشت] مراجعه کنید.

اجازه اعتبارسنجی N:۱ : در این حالت، اعتبارسنجی فقط با اثرانگشت و بدون وارد کردن شناسه در ترمینال تشخیص اثرانگشت انجام می گیرد.

اطلاعات رمزعبور: یک رمزعبور ثبت کنید تا برای اعتبارسنجی استفاده گردد.

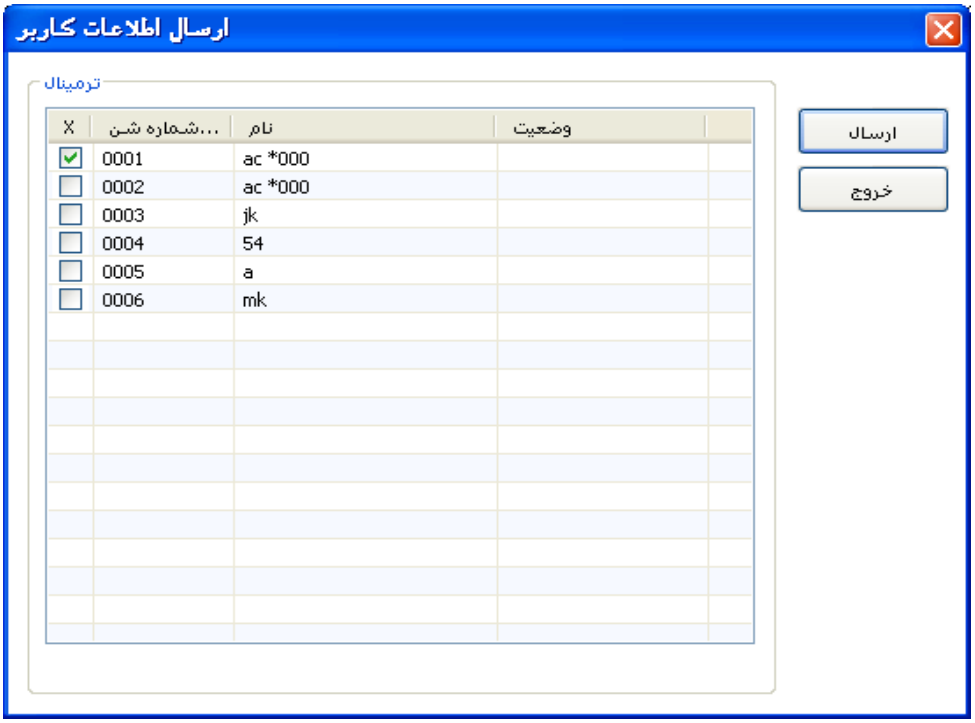
اطلاعات کارت: دکمه Reading را بفشارید و یک کارت را در ریدر هوشمند اثرانگشت بخوانید.

وقتی شماره کارت در READING... نشان داده می شود، دکمه Add را بفشارید تا کارت ثبت گردد.

اطلاعات عکس: به منظور ثبت یک تصویر دلخواه، دکمه ثبت را بفشارید(اندازه پیشنهادی: ۲۴۰*X۱۸۰)

۲.۲.۳.۲. ارسال اطلاعات کاربر به ترمینال

در این حالت، اطلاعات کاربری که از فهرست کاربران انتخاب گردیده به ترمینال ارسال می شود.



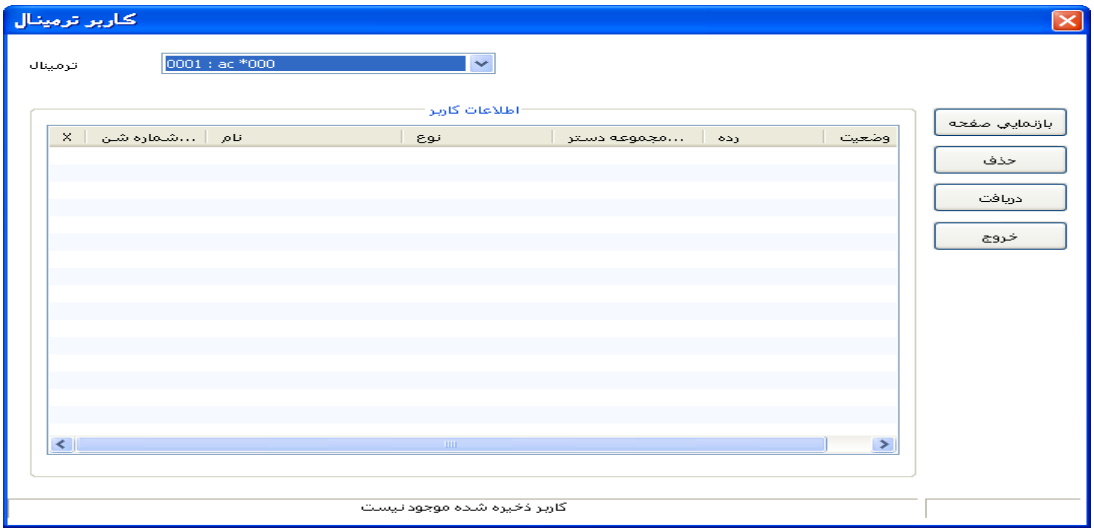
یک ترمینال را جهت دریافت اطلاعات انتخاب و آنگاه دکمه ارسال را بفشارید.

۲.۲.۳.۳. مدیریت کاربری ترمینال

اطلاعات کاربری ذخیره شده در یک ترمینال، قابلیت جستجو و بارگذاری در سرور را داراست.

اطلاعات کاربری ذخیره شده در یک ترمینال شامل نام کاربر نمی شود.

اطلاعات کاربری که قبلاً در سرور ثبت شده، قابل بارگذاری نیست.



بازنمایی صفحه: اطلاعات کاربری ذخیره شده در ترمینال را بارگذاری مجدد می کند.

حذف: کاربری را که در ترمینال انتخاب شده، حذف می کند.

دریافت: اطلاعات کاربر منتخب را در سرور بارگذاری می کند.

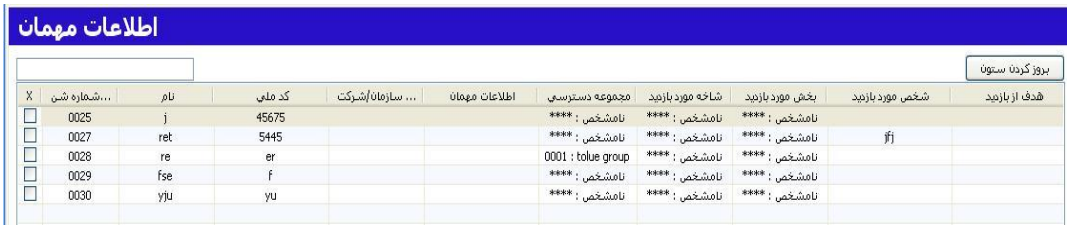
۲.۲.۴. مدیریت میهمان

این قسمت فهرستی از بازدیدکنندگان ثبت شده را ارائه می کند.

◄اضافه کردن بازدیدکننده: در بخش[مدیریت بازدیدکننده] گزینه[اضافه کردن بازدیدکننده] را انتخاب نمایید.

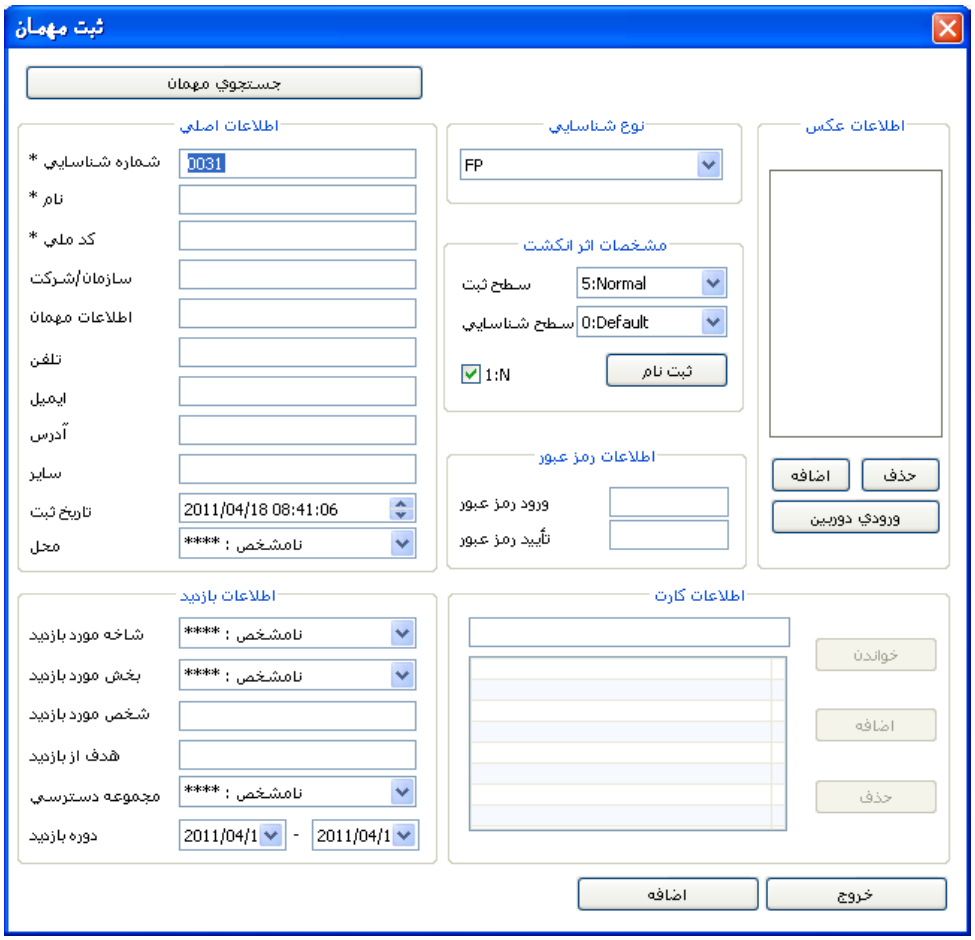
شناسه بازدیدکننده از شناسه کاربر قابل تمیز بوده و می تواند در منوی [گزینه سرور] تنظیم گردد.

◄حذف بازدیدکننده: از پنجره حاوی لیست بازدیدکنندگان، بازدیدکننده موردنظر را جهت حذف انتخاب و گزینه[حذف بازدیدکننده] را انتخاب کنید.



- شناسه: در این قسمت شناسه بازدیدکننده به معرض نمایش در می آید.
- نام: در این بخش نام بازدیدکننده ارائه می گردد.
- شماره اجتماعی: شماره اجتماعی بازدیدکننده نمایش داده می شود.
- شخص مورد بازدید: شخص مورد بازدید نمایش داده می شود.
- اطلاعات بازدیدکننده: اطلاعات بازدیدکننده نمایش داده می شود.
- گروه دسترسی: گروه دسترسی بازدیدکننده عرضه می شود.
- شاخه بازدید: شاخه بازدید بازدیدکننده عرضه می شود.
- گروه بازدید: گروه بازدید بازدیدکننده عرضه می شود.
- هدف بازدیدکننده: هدف بازدید بازدیدکننده نمایش داده می شود.
- مقصود از بازدید: مقصود از بازدید بازدیدکننده ارائه می گردد.

۲.۲.٤.۱ اضافه کردن میهمان



- اطلاعات اولیه
- شناسه: در این قسمت شناسه بازدیدکننده را تعیین کنید.
- نام: نام بازدیدکننده را وارد کنید.
- شماره اجتماعی: شماره اجتماعی بازدیدکننده را وارد نمایید.
- شرکت بازدیدکننده: نام شرکت بازدیدکننده را وارد کنید.
- اطلاعات بازدیدکننده: اطلاعات بازدیدکننده را وارد کنید.
- تلفن: شماره تلفن بازدیدکننده را وارد کنید.
- آدرس ایمیل: آدرس ایمیل بازدیدکننده را واردکنید.
- آدرس: آدرس پستی بازدیدکننده را واردکنید.
- سایر: دیگر موارد موردنیاز را وارد نمایید.
- تاریخ ثبت: تاریخ و ساعت ثبت بازدیدکننده بطور خودکار وارد می شود.
- اطلاعات بازدید
- محل کار بازدید: محل کاری را که در بخش[ثبت شاخه] ثبت گردیده، تعیین کنید.
- گروه بازدید: یک گروه از آنچه که در بخش [ثبت گروه] درج گردیده، تعیین نمایید.
- شخص مورد بازدید: شخص مورد بازدید بازدیدکننده را وارد نمایید.
- مقصود از بازدید: مقصود از بازدید بازدیدکننده را وارد نمایید.
- گروه دسترسی: یک گروه دسترسی از آنچه که در بخش [ثبت گروه دسترسی] درج گردیده، اختصاص دهید.
- دوره زمانی بازدید: دوره زمانی بازدید بازدیدکننده را تعیین کنید. تنها طی مدت زمان تخصیص داده شده امکان بازدید وجود دارد.
- انواع اعتبارسنجی
- FP: اعتبارسنجی اثرانگشت
- FP –کارت: اعتبارسنجی کارت-اثرانگشت
- PW: اعتبارسنجی رمزعبور
- کارت: اعتبارسنجی کارت
- کارت یا FP: اعتبارسنجی اثر انگشت یا کارت
- کارت و FP: اعتبارسنجی اثر انگشت و کارت
- کارت یا PW: اعتبارسنجی رمزعبور یا کارت
- کارت و PW: اعتبارسنجی رمزعبور و کارت
- (شناسه یا کارت) و FP: اعتبارسنجی شناسه یا کارت و اعتبارسنجی اثرانگشت
- (شناسه یا کارت) و PW: اعتبارسنجی شناسه یا کارت و اعتبارسنجی رمزعبور
- FP و PW: اعتبارسنجی رمزعبور و اثر انگشت
- FP یا PW: اعتبارسنجی رمزعبور یا اثر انگشت

اطلاعات اثرانگشت: دکمه ثبت نام را بفشارید تا یک اثرانگشت ثبت شود. برای کسب اطلاعات بیشتر در خصوص مراحل ثبت اثرانگشت، به بخش [مراحل ثبت اثرانگشت] مراجعه کنید.

اجازه اعتبارسنجی N:۱ : در این حالت، اعتبارسنجی فقط با اثرانگشت و بدون وارد کردن شناسه در ترمینـال تشـخیص اثرانگشـت انجام می گیرد.

اطلاعات رمزعبور: یک رمزعبور ثبت کنید تا برای اعتبارسنجی استفاده گردد.

اطلاعات کارت: دکمه خواندن را بفشارید و یک کارت را در ریدر هوشمند اثرانگشت بخوانید.

وقتی شماره کارت در READING... نشان داده می شود، دکمه اضافه را بفشارید تا کارت ثبت گردد.

اطلاعات عکس: به منظور ثبت یک تصویر دلخواه دکمه ثبت را بفشارید(اندازه پیشنهادی: ۲۴۰*X۱۸۰)

۲.۲.۵. کنترل تردد

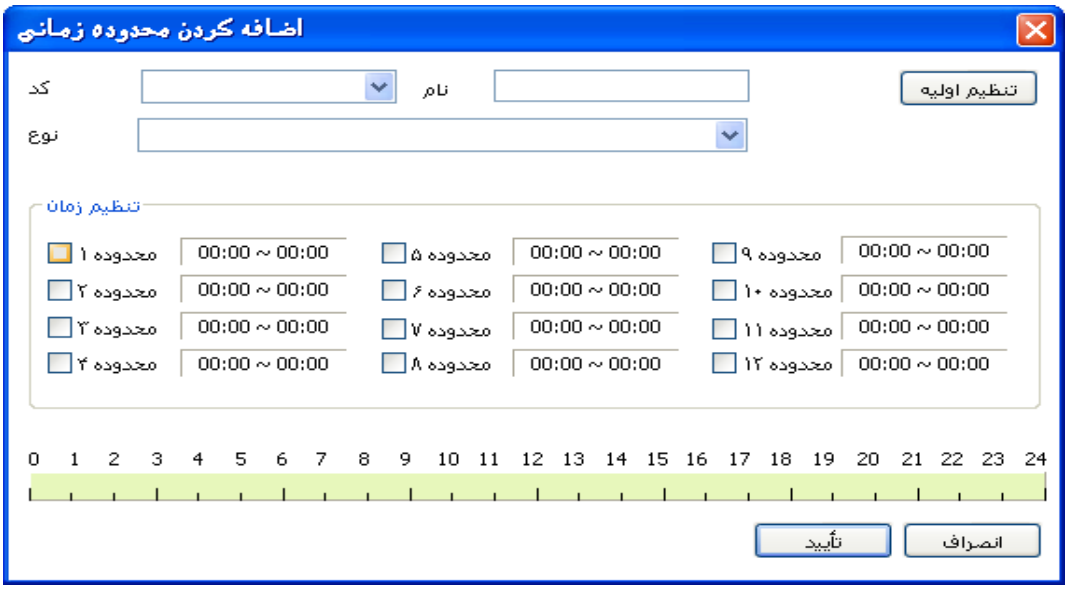
یک مدیر از کارکرد کنترل تردد استفاده می کند تا با تاریخ هفتگی دسترسی کاربر را محدود نماید.

تنظیم منطقه زمانی، تنظیم ساعت تردد، تنظیم منطقه تردد و تنظیم گروه تردد که نسبت به کنترل تردد کارکرد کمتری دارند به صورت تب پیکربندی می شوند تا مقادیر تنظیمی خود را نشان دهند.

برای تنظیم کنترل تردد، یک گروه دسترسی با عملکرد نسبتاً کمتری ایجاد می شود.

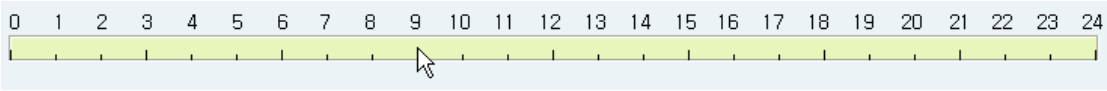
۲.۲.۵.۱. افزودن منطقه زمانی

روزانه حداکثر ۱۲ منطقه زمانی مجاز جهت تردد، طبق کدها تنظیم می شوند.

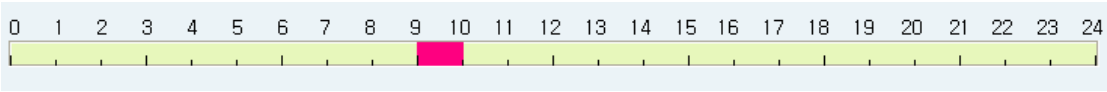


مراحل ثبت

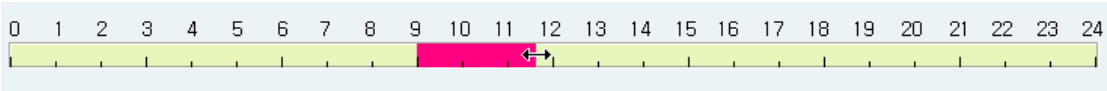
۱)یک نام و شماره رمز دلخواه (۴ رقمی ثابت) وارد کنید.



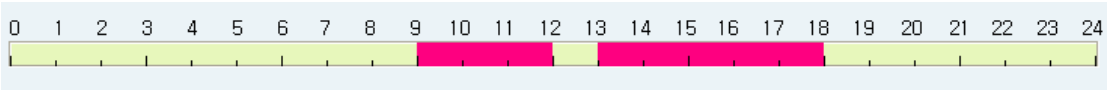
همانند شکل بالا روی منطقه زمانی دلخواه کلیک کنید.



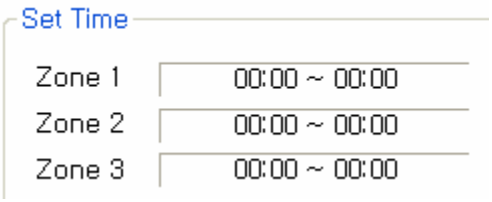
همانند شکل بالا یک نوار قرمز رنگ در محل کلیک ایجاد می شود.



۴)اشاره گر موس را به لبه نوار قرمز حرکت داده و آن را به موقعیت دلخواه درگ کنید.



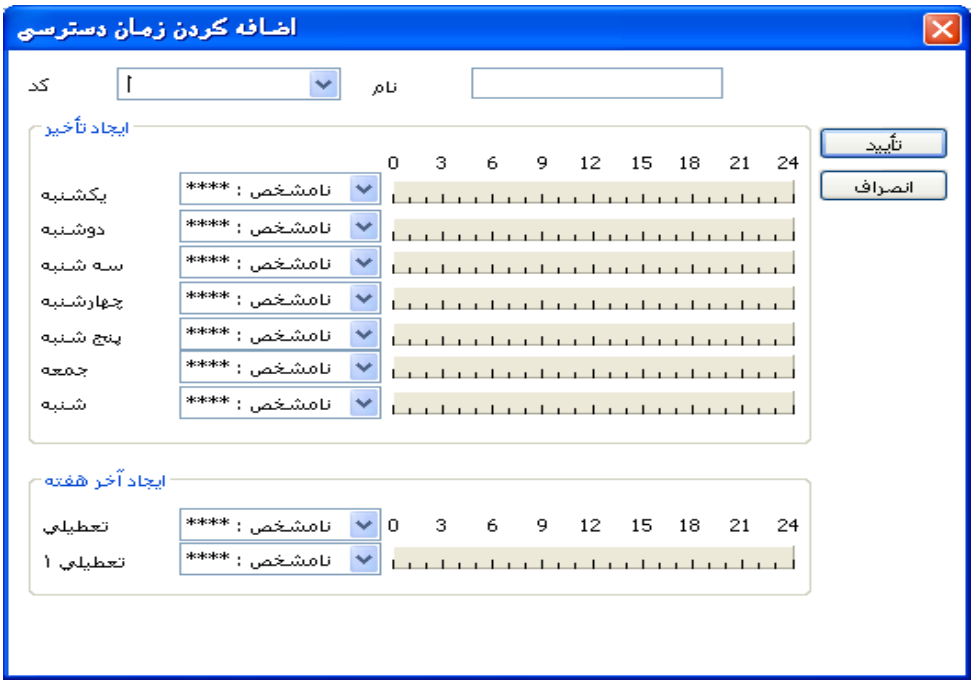
۵)همانند مراحل فوق مناطق زمانی دیگری را ایجاد کنید.



در صورت تعیین منطقه زمانی، زمان دقیق منطقه زمانی در تنظیمات منطقه زمانی نمایش داده می شود.

۲.۲.۵.۲. افزودن زمان تردد

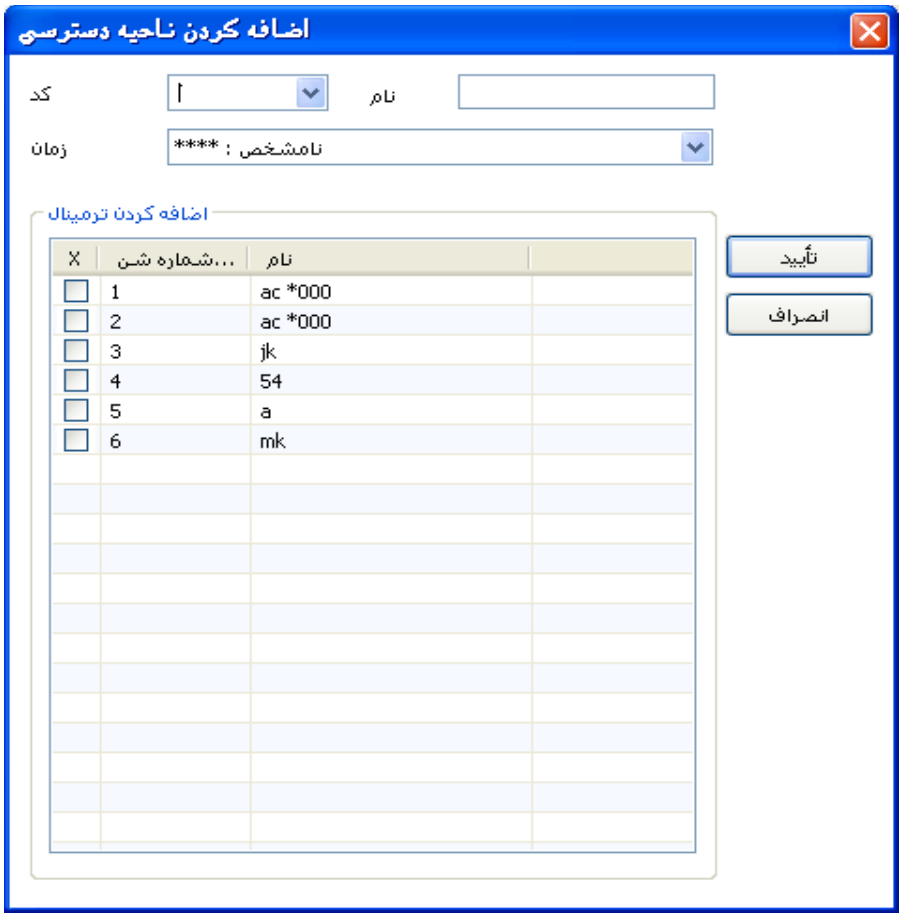
ساعات تردد ایام هفته و تعطیلات براساس کد تنظیم می گردند. این ساعات تردد برای تنظیمات گروه دسترسی بکار می روند.



نام و کد دلخواه را وارد نموده، کد منطقه زمانی را در بخش[افزودن منطقه زمانی]براساس تاریخ هفته و تعطیلات تنظیم نمایید.

۲.۲.۵.۳. افزودن ناحیه تردد

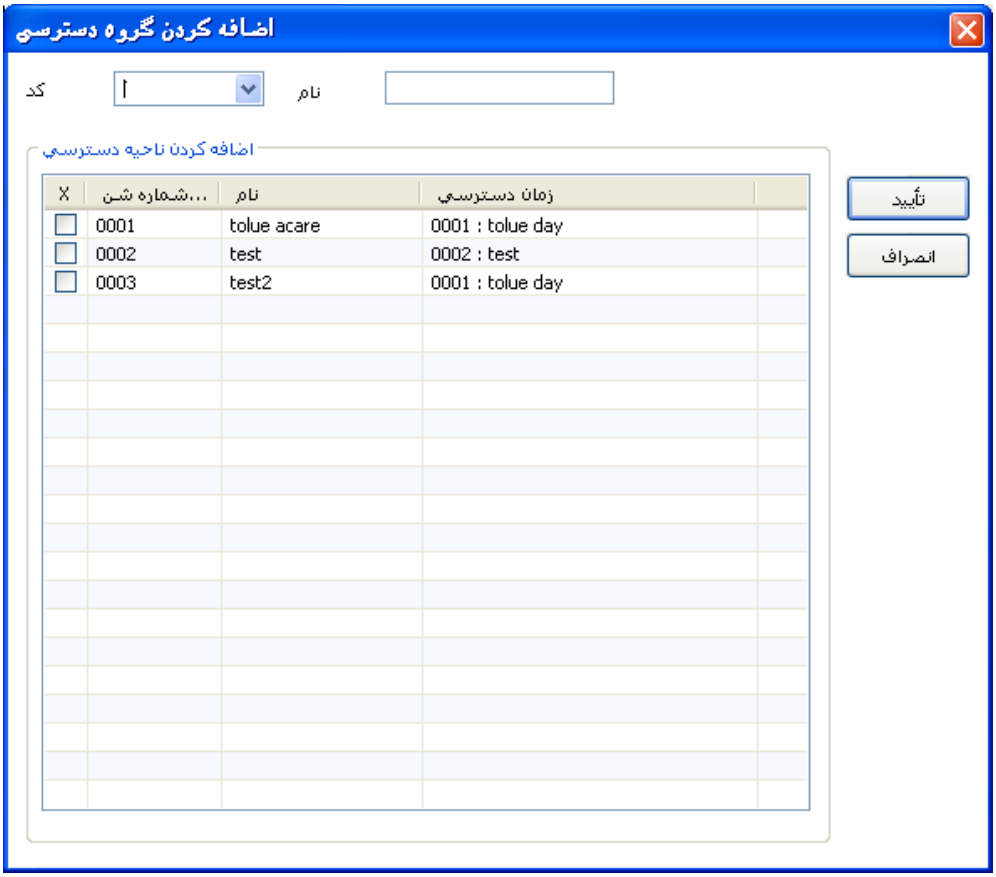
ترمینال براساس کد تنظیمی اجازه دسترسی را می دهد. این مقادیر تنظیمی جهت تنظیمات گروه دسترسی استفاده می شود.



پس از وارد نمودن نام و کد دلخواه، ترمینال و زمانی را که قرار است اجازه دسترسی بدهد انتخاب کنید.

۲.۲.۵.۴. افزودن گروه تردد

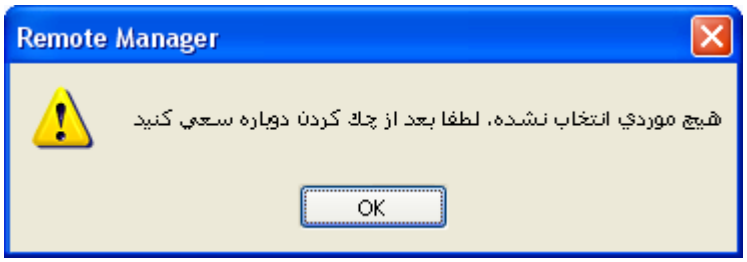
گروه دسترسی با ادغام منطاق تردد تنظیم می گردد.



پس از وارد نمودن نام و کد موردنظر، کد دلخواهی را از میان کدهایی که در بخش[افزودن زمان تردد] ثبت گردیده اند، انتخاب کنید. سپس، کد دلخواهی را از بین کدهای ثبت شده در بخش[افزودن منطقه تردد] برگزینید.

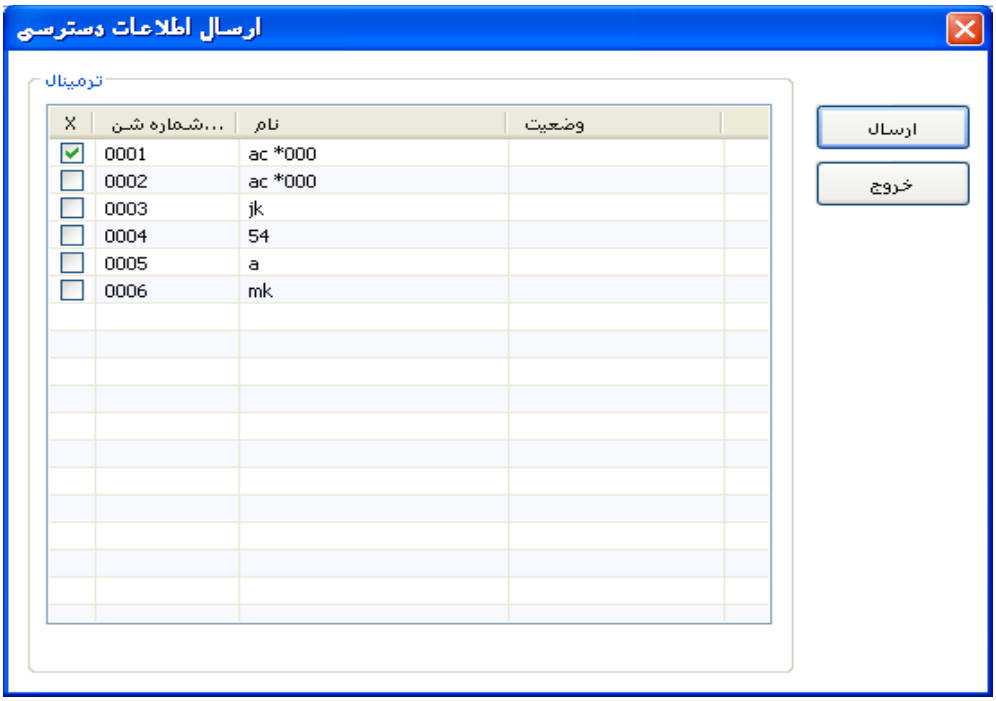
۲.۲.۵.۵. حذف

این عملکرد اطلاعات حق تردد را که از پنجره فهرست کنترل دسترسی انتخاب گردیده، حذف می نماید.



۲.۲.۵.۶. ارسال به ترمینال

پس از تکمیل تنظیمات حق تردد، مقدار تنظیمی به ترمینال ارسال و اعمال می گردد.



ترمینالی را که قرار است اطلاعات را دریافت کند، انتخاب و آنگاه دکمه ارسال را بفشارید.

۲.۲.۶. سیستم

۲.۲.۶.۱. تغییر رمزعبور اصلی

این عملکرد رمزعبور مدیر اصلی سیستم را تغییر می دهد.

۲.۲.۷. مدیریت داده ها

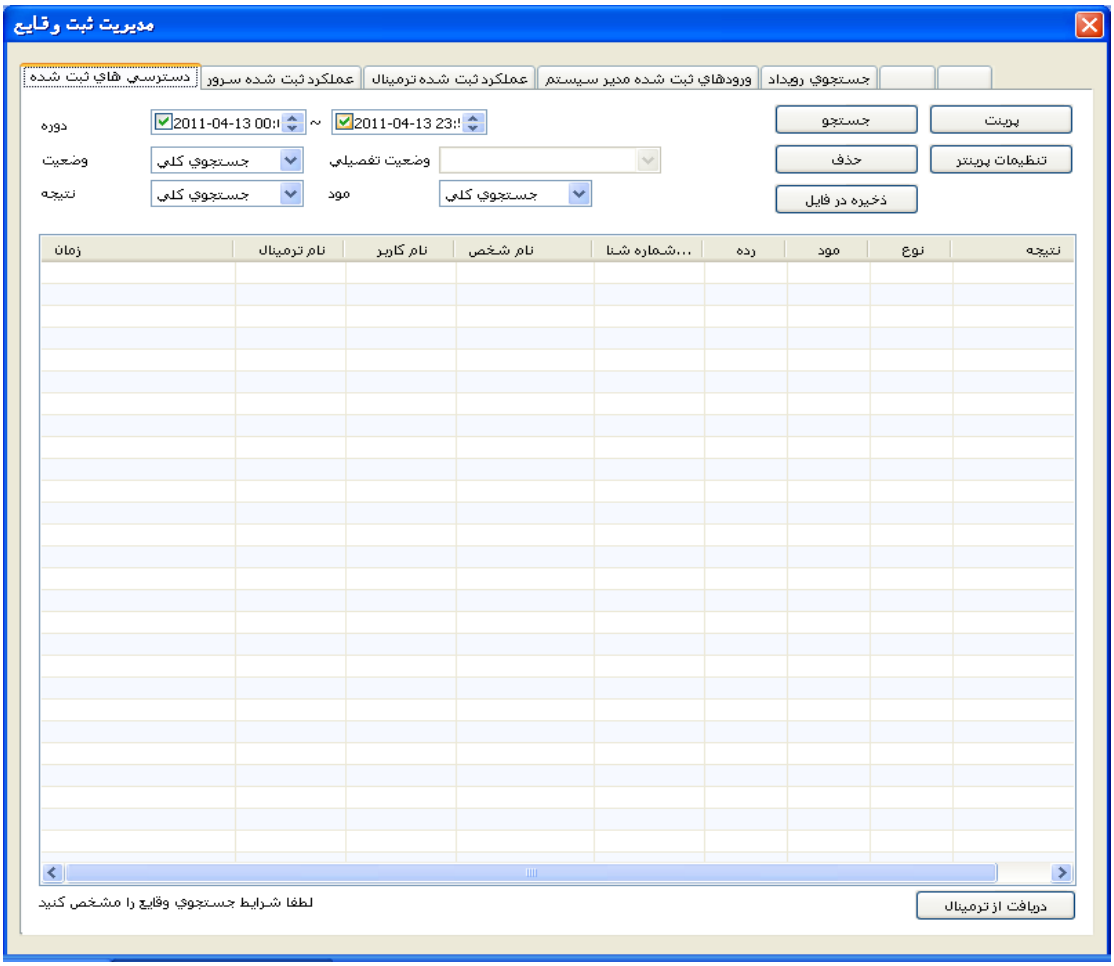
۲.۲.۷.۱. مدیریت ثبت وقایع

این عملکرد، ترمینال تشخیص اثرانگشت و ترددهای ثبت شده مربوط به آن را مدیریت می کند.

این عملکرد عبارتند از: جستجوی سابقه اعتبارسنجی، جستجوی سابقه ورود به سیستم، جستجوی جزئیات عملیات سرور، جستجوی جزئیات عملیات ترمینال، اخذ وقایع ثبت شده اعتبارسنجی و به دست آوردن جزئیات عملیات ترمینال.

۲.۲.۷.۱.۱. ثبت وقایع تردد

این عملکرد، سابقه اعتبارسنجی بعمل آمده از کاربر را جستجو می کند.



دوره زمانی: دوره زمانی جستجو در این قسمت تنظیم می شود. به منظور جستجوی کل دوره ها علامت داخل کادر 2008-08-25 00:00 را بردارید .

وضعیت: شرایط جستجو در این بخش تنظیم می شود. شرایط موردنظر را از بین گزینه های: جستجوی همه/جستجوی ترمینال/جستجوی پرسنل/جستجوی بازدیدکننده، تنظیم نمایید.

وضعیت تفضیلی: جزییات شرایط جستجوی بعمل آمده در این جا تنظیم می گردد. تخصیص جزئیات به منظور جستجو از طریق شناسه بکار می رود.

نتیجه: شرایط جستجو برای هرکدام از نتایج اعتبارسنجی در این قسمت و بصورت جستجوی همه/موفقیت و یا شکست نتایج اعتبارسنجی، تنظیم می شوند.

جستجو: این دکمه بر اساس شرایط جستجو، سوابق اعتبارسنجی بعمل آمده را جستجو می نماید.

حذف: این دکمه بر اساس شرایط جستجو، سوابق اعتبارسنجی بعمل آمده را حذف می نماید.

※چون سابقه اعتبارسنجی حذف شده قابلیت بازیابی ندارد، لطفاً در این خصوص احتیاط لازم را به عمل آورید.

ذخیره در فایل: سوابق جستجو شده را به عنوان فایل CSV ذخیره می نماید.

پرینت: با استفاده از چاپگر از سوابق مورد جستجو خروجی می گیرد.

کاغذ: چاپگر و کاغذ چاپ را تنظیم می کند.

دریافت از ترمینال: سوابق اعتبارسنجی ذخیره شده در ترمینال را در سرور بارگذاری می کند.

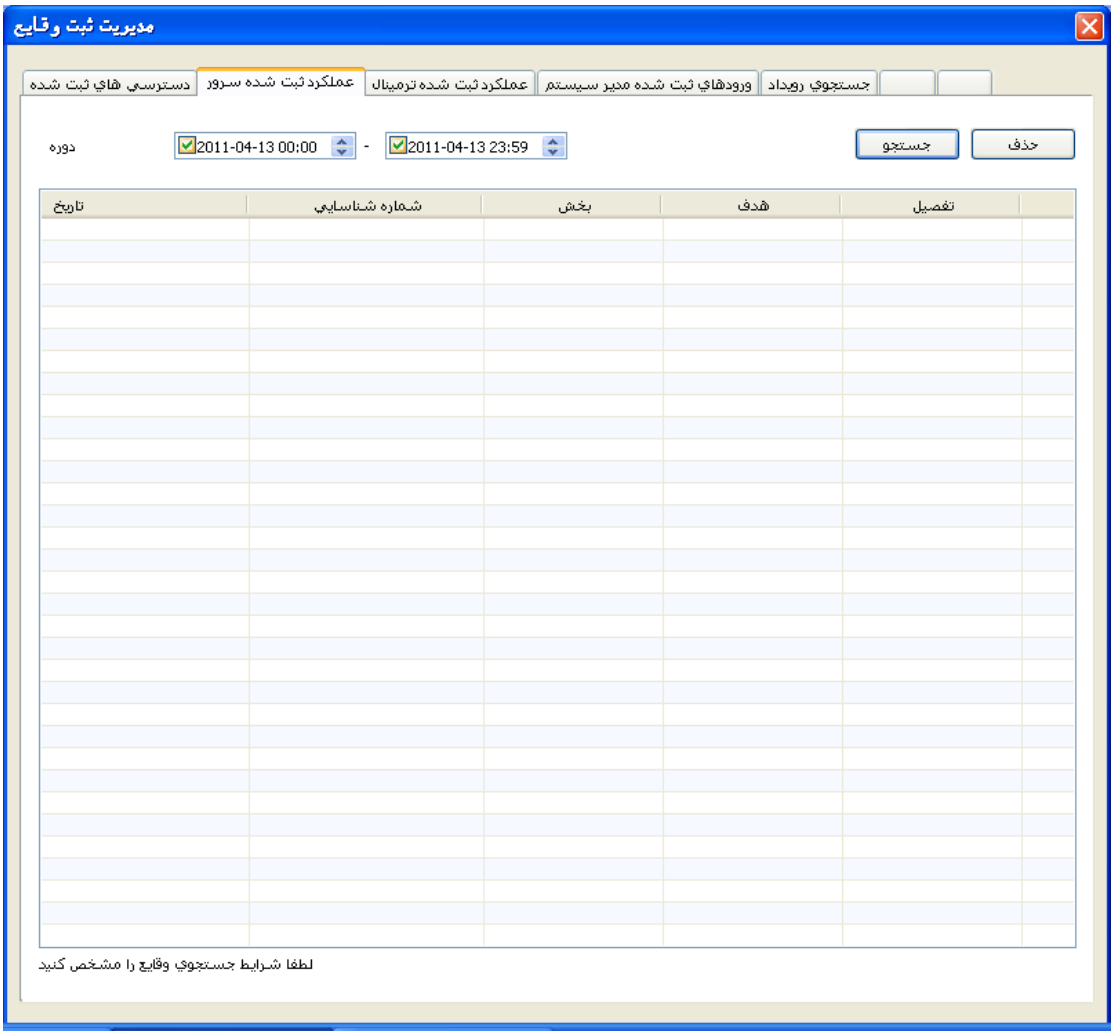
وقتی که ترمینال در مد S/N و یا N/S عمل می کند، اگر ارتباط با سرور قطع شده باشد، سوابق اعتبارسنجی در حافظه داخلی ترمینال ذخیره می شود.

پس از انتخاب ترمینال موردنظر، دکمه[اخذ] را بفشارید تا سوابق اعتبارسنجی را بدست آورید.

دریافت دوباره همه وقایع: این بخش تمامی وقایع ثبت شده اعتبارسنجی را که در ترمینال ذخیره گشته دوباره اخذ می کند.

۲.۲.۷.۱.۲. ثبت وقایع بازبینی سرور

مدیری که وارد سیستم UNIS می شود، قادر به جستجوی جزییات کاری همچون حذف، اضافـه و تغییر می باشد.



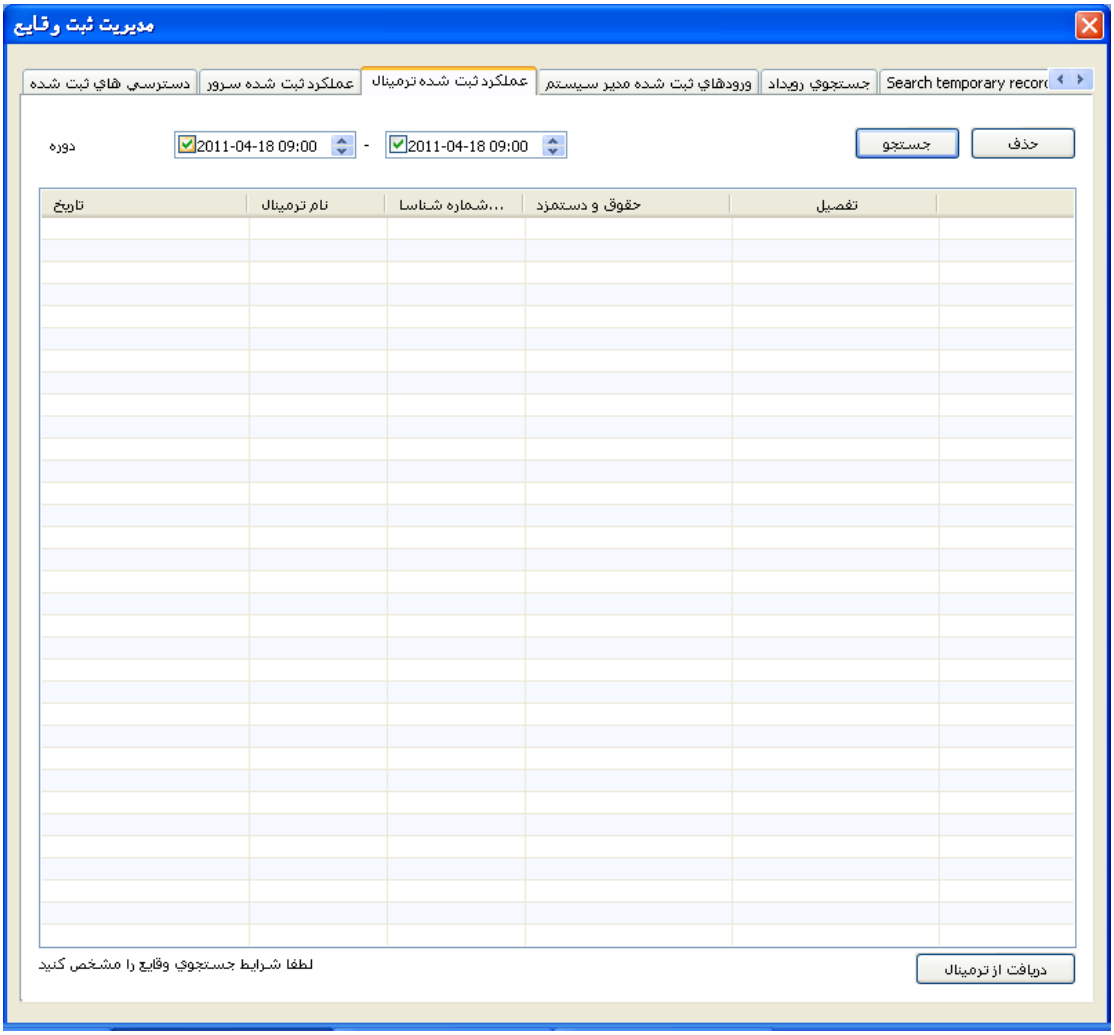
- تاریخ: زمان انجام عملیات توسط مدیر را نشان می دهد.
- شناسه: شناسه مدیری را نشان می دهد که وارد سیستم شده است.
- بخش: قسمت عملیاتی به نمایش در می آید.
- هدف: آیتم های تفصیلی در بخش عملیاتی نمایش داده می شوند.
- (اگر بخش عملیاتی مربوط به ترمینال باشد، شناسه ترمینال به نمایش در می آید.)
- جزئیات: حذف، اضافه، تغییر و سوابق جستجو به نمایش در می آیند.

جستجو: جزئیات عملیات را در دوره تعیین شده جستجو می کند.

حذف: جزئیات عملیات را در دوره تعیین شده حذف می کند.

۲.۲.۷.۱.۳. ثبت وقایع بازبینی ترمینال

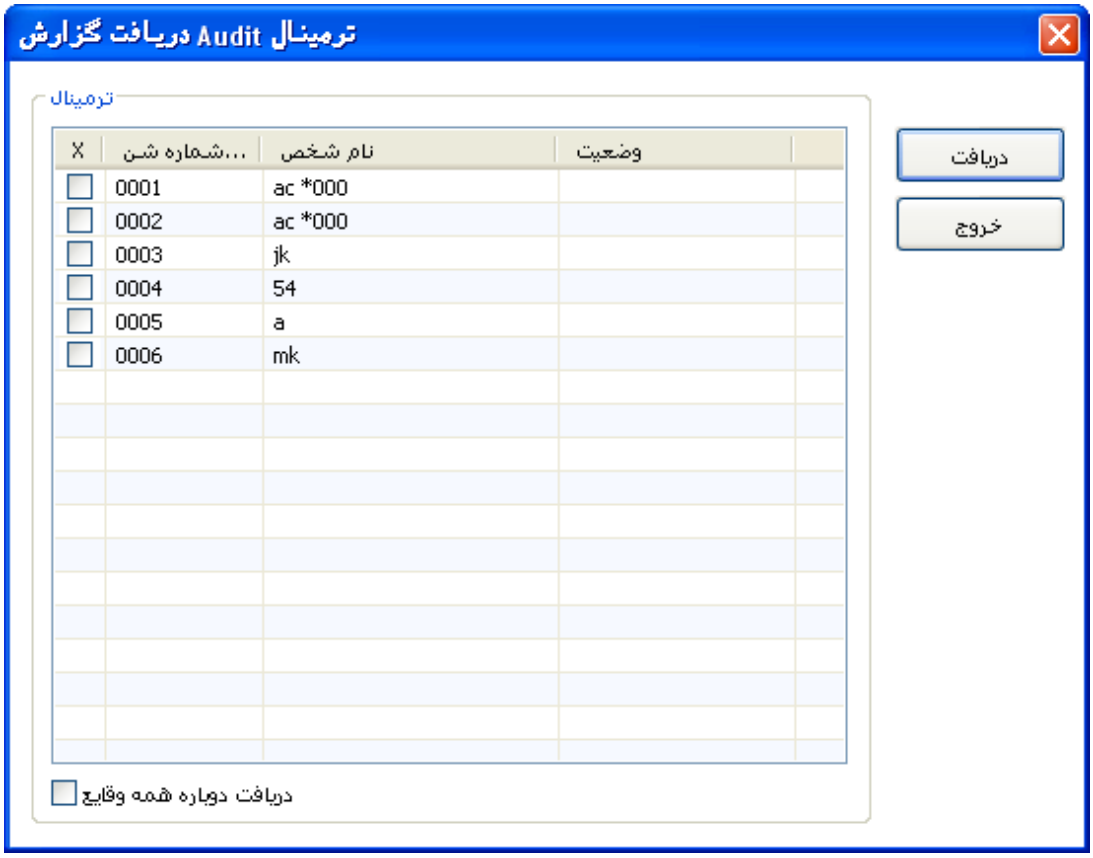
مدیر ترمینال، جزئیات عملیات اجرا شده در ترمینال را جستجو می کند.



- تاریخ: زمان وقوع عملیات توسط مدیر را نشان می دهد.
- شناسه ترمینال: شناسه ترمینالی را نشان می دهدکه مدیر بوسیله آن به انجام عملیات پرداخته است.
- شناسه مدیر: شناسه مدیری را نشان می دهد که وارد سیستم ترمینال شده است.
- نام مدیر: نام مدیری را نشان می دهد که وارد سیستم ترمینال شده است.
- جزئیات: جزئیات عملیات صورت گرفته توسط مدیر در این قسمت به نمایش در می آید.

- جستجو: جزئیات عملیات صورت گرفته را در دوره تعیین شده جستجو می کند.
- حذف: جزئیات عملیات صورت گرفته را در دوره تعیین شده حذف می کند.

دریافت از ترمینال: رویداد بازبینی ذخیره شده در ترمینال را در سرور بارگذاری می کند.

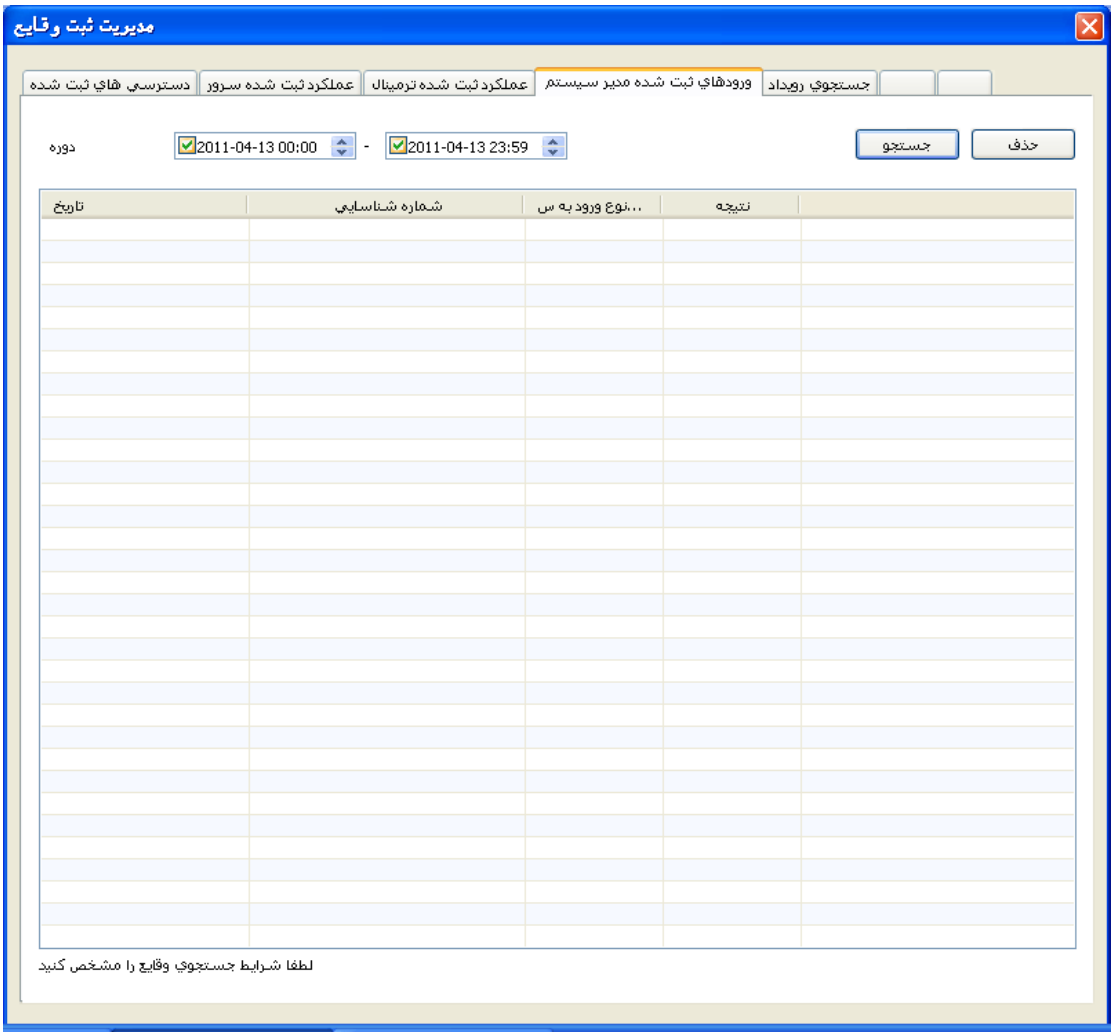


پس از انتخاب ترمینال موردنظر، دکمه[دریافت] را فشرده و سوابق اعتبارسنجی را اخذ نمایید.

اخذ مجدد همه وقایع ثبت شده: تمامی وقایع اعتبارسنجی را که در ترمینال ذخیره شده دوباره اخذ می کند.

۲.۲.۷.۱.۴. ثبت ورود مدیر

سوابق ورود مدیر به سیستم UNIS را جستجو می کند.



- تاریخ: تاریخ و ساعتی را نشان می دهد که مدیر وارد سیستم شده است.
- شناسه: شناسه مدیری را نشان می دهد که وارد سیستم شده است.
- نوع ورود: یکی از حالتهای ورود، خروج، آیکن، فعال نمایش داده می شود.
- نتیجه: موفقیت یا شکست عملیات اعتبارسنجی به نمایش گذاشته می شود.

جستجو: سوابق ورود مدیر را در دوره ای معین جستجو می کند.

حذف: سوابق مورد جستجو را حذف می نماید.

۲.۲.۷.۲. مدیریت سازمان

۲.۲.۷.۲.۱. مدیریت شاخه

مواردکاربرد شاخه ها در هنگام وارد نمودن اطلاعات کاربر، ترمینال و بازدیدکننده می باشد.

- اطلاعات ورودی
- کد: یک شماره منحصربفرد ۴رقمی را وارد نمایید.
- نام: نام محل کار را وارد کنید.
- اضافه: دکمه ثبت اطلاعات محل کار
- اصلاح: دکمه تغییر اطلاعات محل کار
- حذف: دکمه حذف اطلاعات محل کار

۲.۲.۷.۲.۲. مدیریت بخش

بخشها در هنگام وارد کردن اطلاعات پرسنل و بازدیدکننده کارایی دارند.

- اطلاعات ورودی
- کد: یک شماره منحصربفرد ۴رقمی را وارد نمایید.
- نام: نام گروه را وارد کنید
- اضافه: دکمه ثبت اطلاعات گروه وارد شده
- اصلاح: دکمه تغییر اطلاعات گروه
- حذف: دکمه حذف اطلاعات گروه

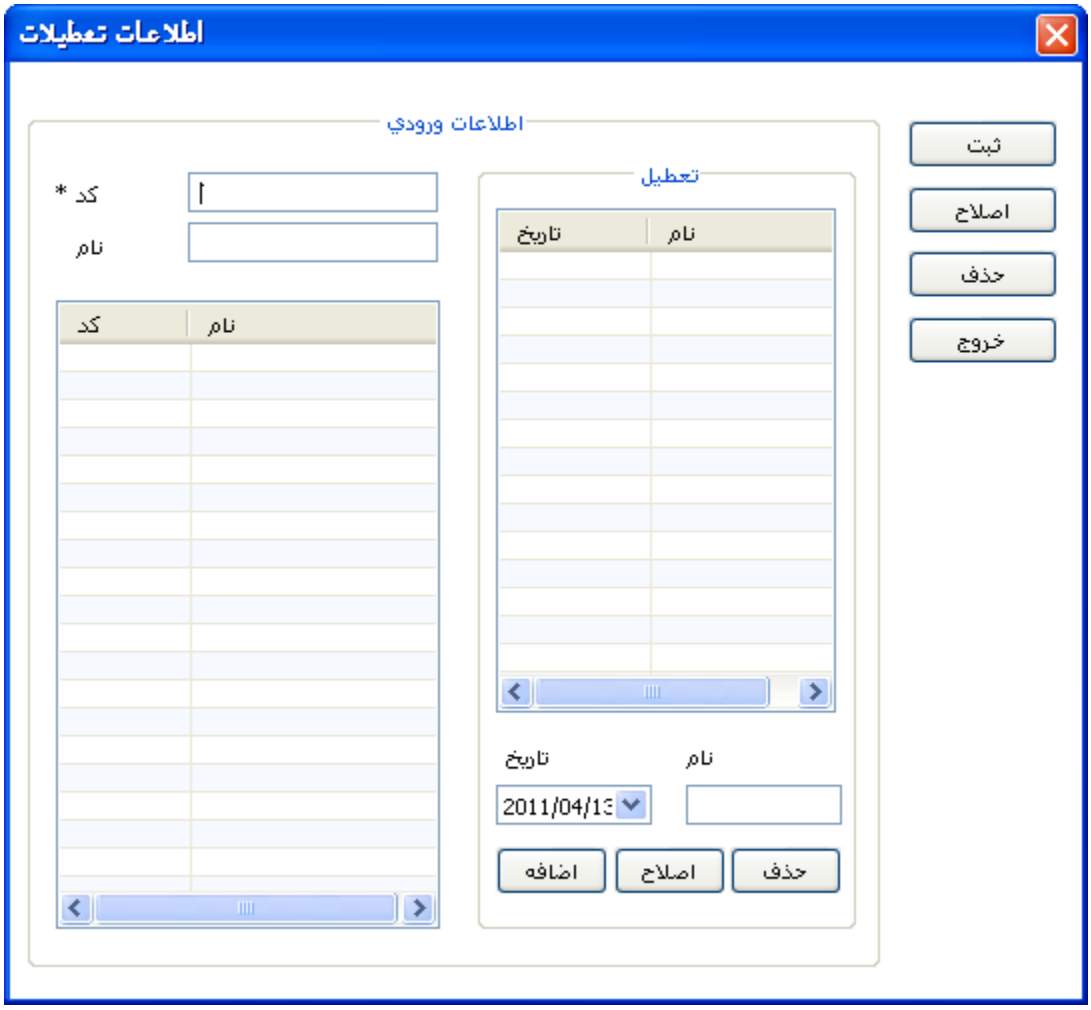
۲.۲.۷.۲.۳. مدیریت عنوان شغلی

پس از ثبت مشاغل، موارد استفاده آنها در هنگام وارد کردن اطلاعات پرسنل و بازدیدکننده می باشد.

- اطلاعات ورودی
- کد: یک شماره منحصربفرد ۴رقمی را وارد نمایید.
- نام: نام شغل را وارد کنید.
- اضافه: دکمه ثبت اطلاعات شغل وارد شده
- اصلاح: دکمه تغییر اطلاعات شغلی
- حذف: دکمه حذف اطلاعات شغلی

۲.۲.۷.۳. مدیریت تعطیلات

در این بخش تعطیلات ثبت می گردند. تعطیلات تعیین شده در مدیریت حضور و غیاب و کنترل تردد نیز کاربرد دارند.



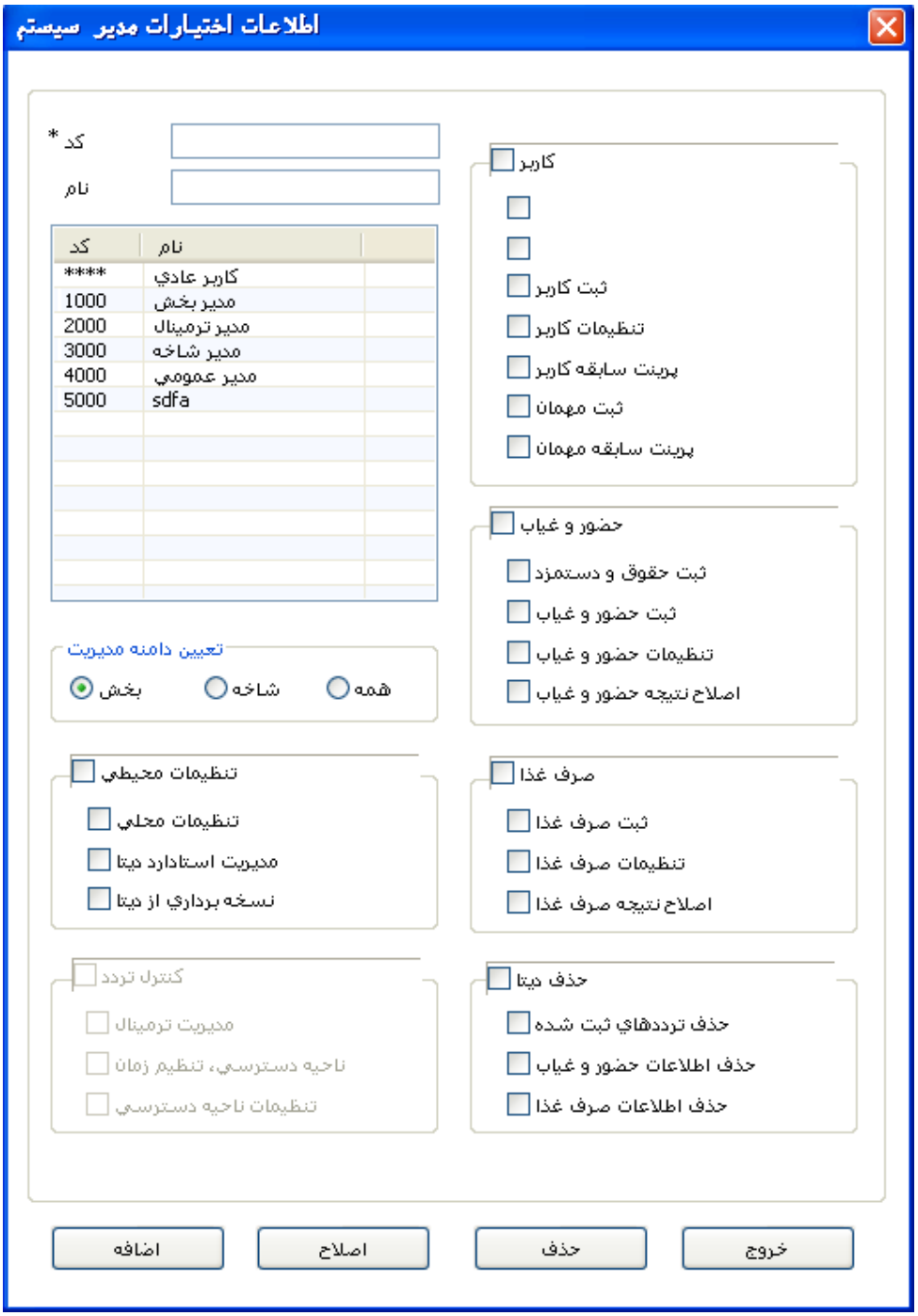
- اطلاعات ورودی
- کد: یک شماره منحصربفرد ۴رقمی را وارد نمایید.
- نام: نام مناسب برای کد وارد کنید.
- حذف و اضافه کردن تعطیلات

پس از وارد کردن یک کد، Name: Chrismas Date: 2009/12/25 را وارد و دکمه اضافه را بفشارید. پس از وارد نمودن تمامی تعطیلات، دکمه ثبت را فشرده تا تعطیلات به کدهای قابل اجرای خود اختصاص یابند.

※از آنجا که برخی تعطیلات از قبیل اولین روز سال نو و روز شکرگزاری هرسال در تقویم شمسی تغییر می یابند، لازمست این تعطیلات همه ساله تنظیم شوند.

۲.۲.۷.۴. مدیریت اختیارات مدیر

این عملکرد اختیارات مدیر را جهت استفاده از "مدیریت از راه دور" محدود می کند.



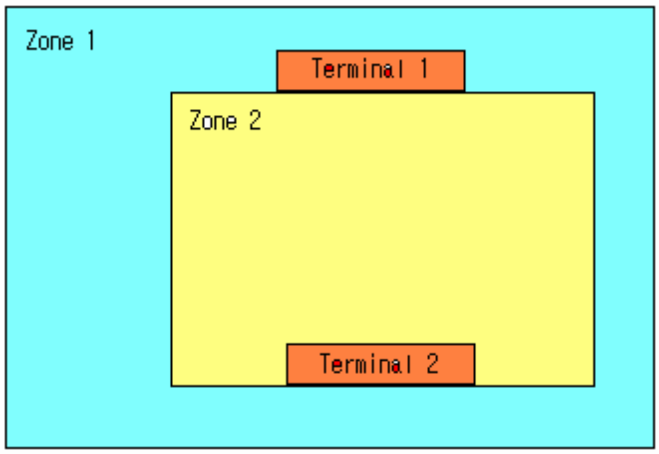
بعد از تنظیم نمودن حیطه مدیریتی در بخش"تعریف حوزه مدیریت" ، موارد تفصیلی را تنظیم کنید.

****یک کاربر عمومی نمی تواند تغییرات را اعمال نماید. ضمناً تنظیمات پیش فرض به تمامی کاربران اختصاص می یابد.

تمام مدیران قادرند کاربران عمومی را جستجو نمایند؛ لیکن تنها مدیر سطح بالا می تواند تغییرات را اعمال نماید.

۲.۲.۷.۵. مدیریت Anti Pass back

در صورت فعال شدن Anti Pass Back در یک منطقه ای که ورودی و خروجی وجود داشته باشد، تنها شخصی که از طریق ورودی وارد شده می تواند از طریق خروجی خارج شود.



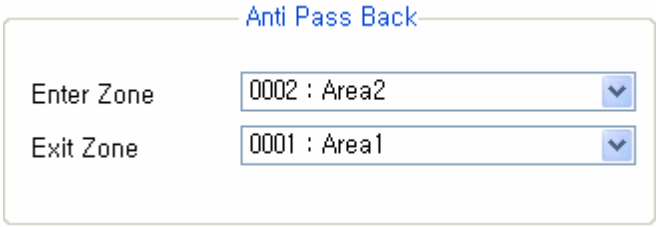
برای نمونه، وقتی یک شخص از منطقه۱ به منطقه ۲ حر کت می کند، آن فـرد از Terminal 1 می گذرد. در اینجا، ترمینال ۱ هم خروجی منطقه ۱ و هم ورودی منطقه ۲ محسوب می شود. تنها فردی که از Terminal 1 وارد می شود مـی توانـد از Terminal 2 خارج شود.

"منو-> مدیریت داده ها->Anti Pass Back " را انتخاب کنید.

کد "Antipass back " ثبت می گردد.

- اطلاعات ورودی
- کد: یک شماره منحصربفرد ۴رقمی را وارد نمایید.
- نام: نام عدم رد کارت به عقب را وارد کنید.
- اضافه: دکمه ثبت اطلاعات عدم رد کارت به عقب
- اصلاح: دکمه تغییر اطلاعات عدم رد کارت به عقب
- حذف: دکمه حذف اطلاعات عدم رد کارت به عقب

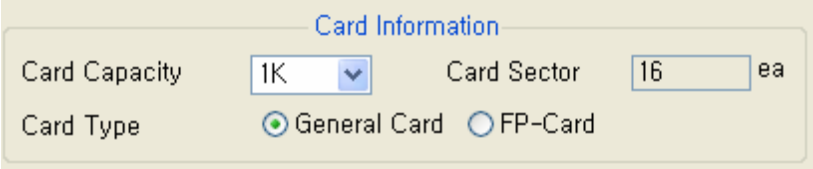
اطـــلاعات عدم رد کـــــارت به عقب ثبت شده، طی ثبت ترمینال به عنوان ورودی منطقه و خروجی منطقه ثبت می گردد.



۲.۲.۸. ابزار

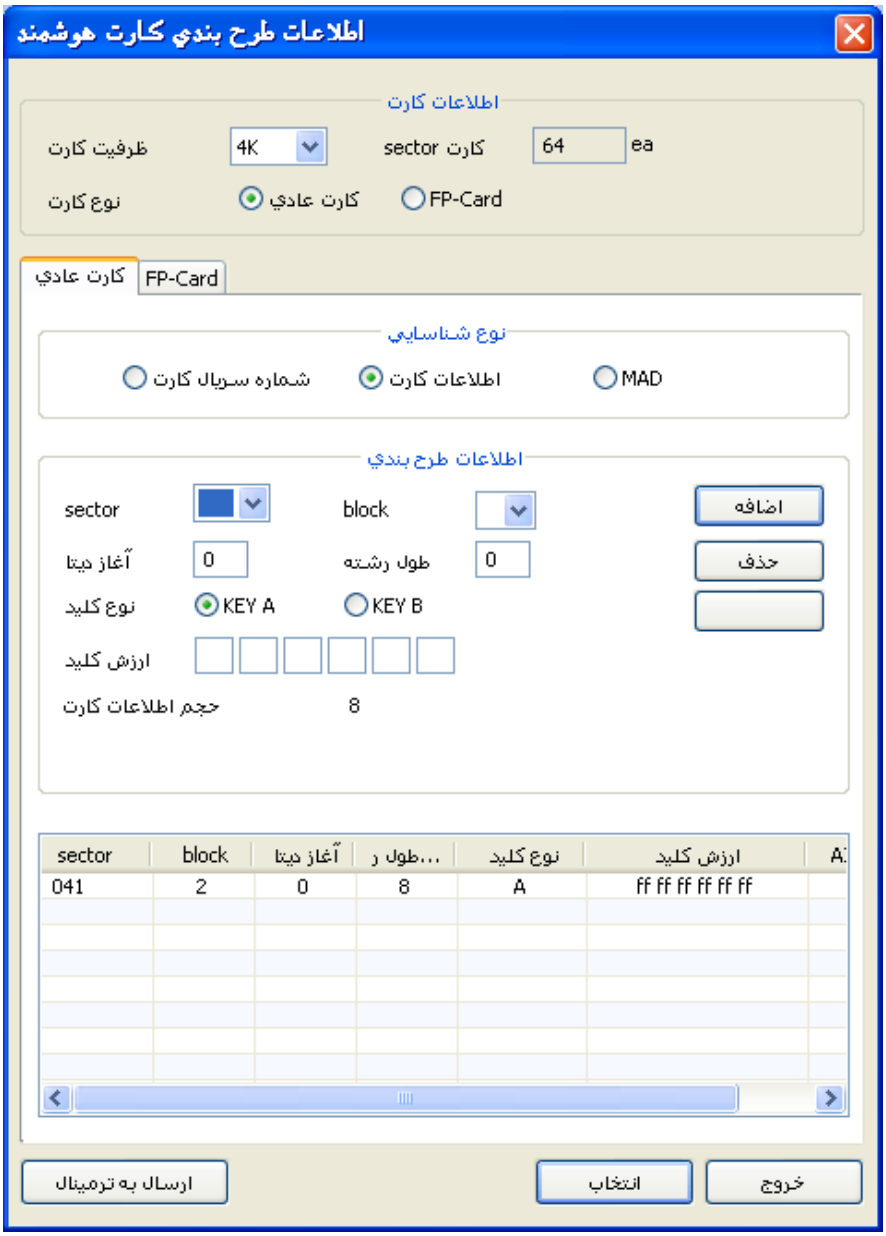
۲.۲.۸.۱. راه اندازی طرح بندی کارت

نظر به اینکه این منو به اختیارات مدیراصلی نیازمند است، طرح کارت هوشمند را تنظیم می نماید.



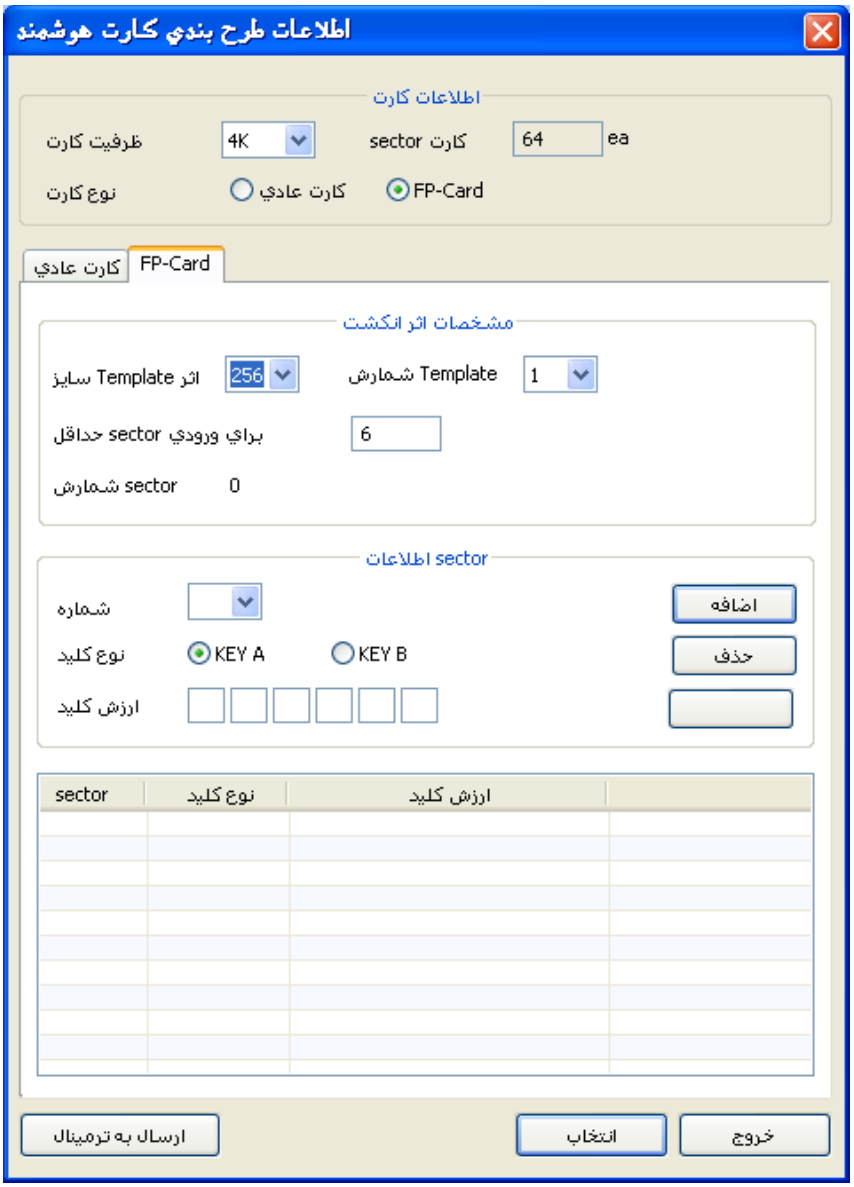
- **اطلاعات کارت**

در این بخش ظرفیت و نوع کارت تنظیم می گردد.



تنظیمات کارت عمومی

- انواع اعتبارسنجی
- سریال کارت: هنگام اعتبارسنجی با سریال کارت هوشمند این گزینه را انتخاب نمایید.
- داده کارت: هنگام اعتبارسنجی با استفاده از اطلاعات خاص کارت هوشمند این گزینه را انتخاب کنید.
- اطلاعات طرح بندی
- در این بخش طرح بندی داده های کارت تنظیم می گردد. تنها وقتی که شیوه اعتبارسنجی[تشخیص اطلاعات کارت] باشد، از این قسمت استفاده می گردد.



تنظیم کارت اثرانگشت

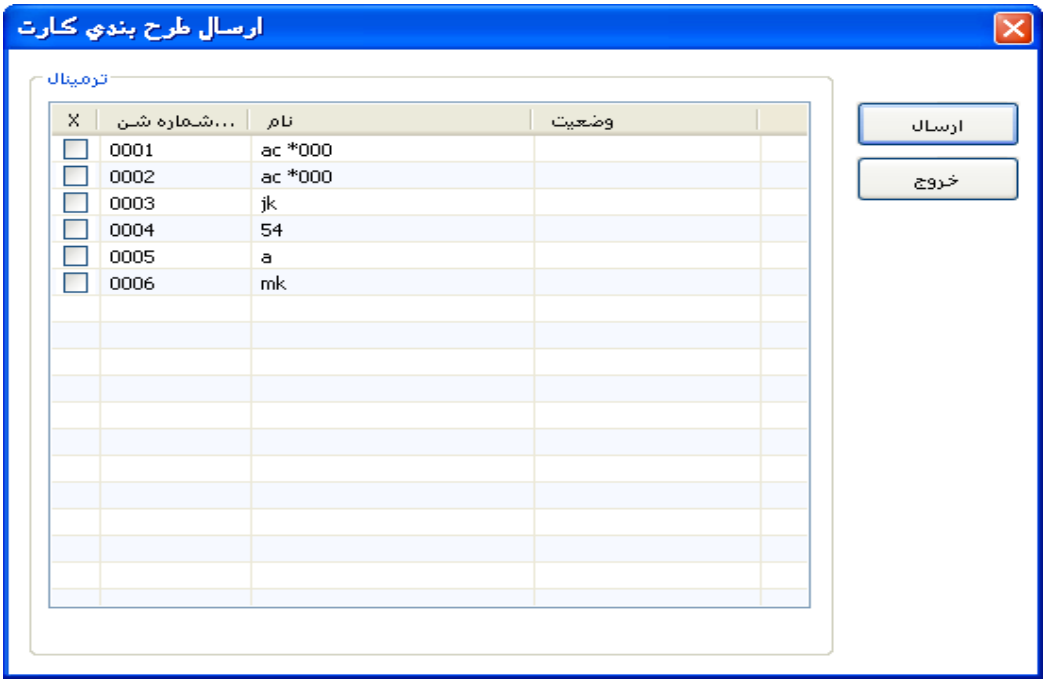
- اطلاعات اثرانگشت

اندازه و تعداد اثرانگشت های الگو را جهت استفاده انتخاب کنید.

- اطلاعات سکتور

اطلاعات سکتور را تنظیم کنید تا به اطلاعات اثرانگشت دسترسی بیابید.

دکمه ارسال به ترمینال اطلاعات طرح کارت را به ترمینال ارسال می کند.



ترمینال مقصد را جهت دریافت اطلاعات، انتخاب و دکمه ارسال را بفشارید.

۲.۲.۸.۲. صدور کارت هوشمند

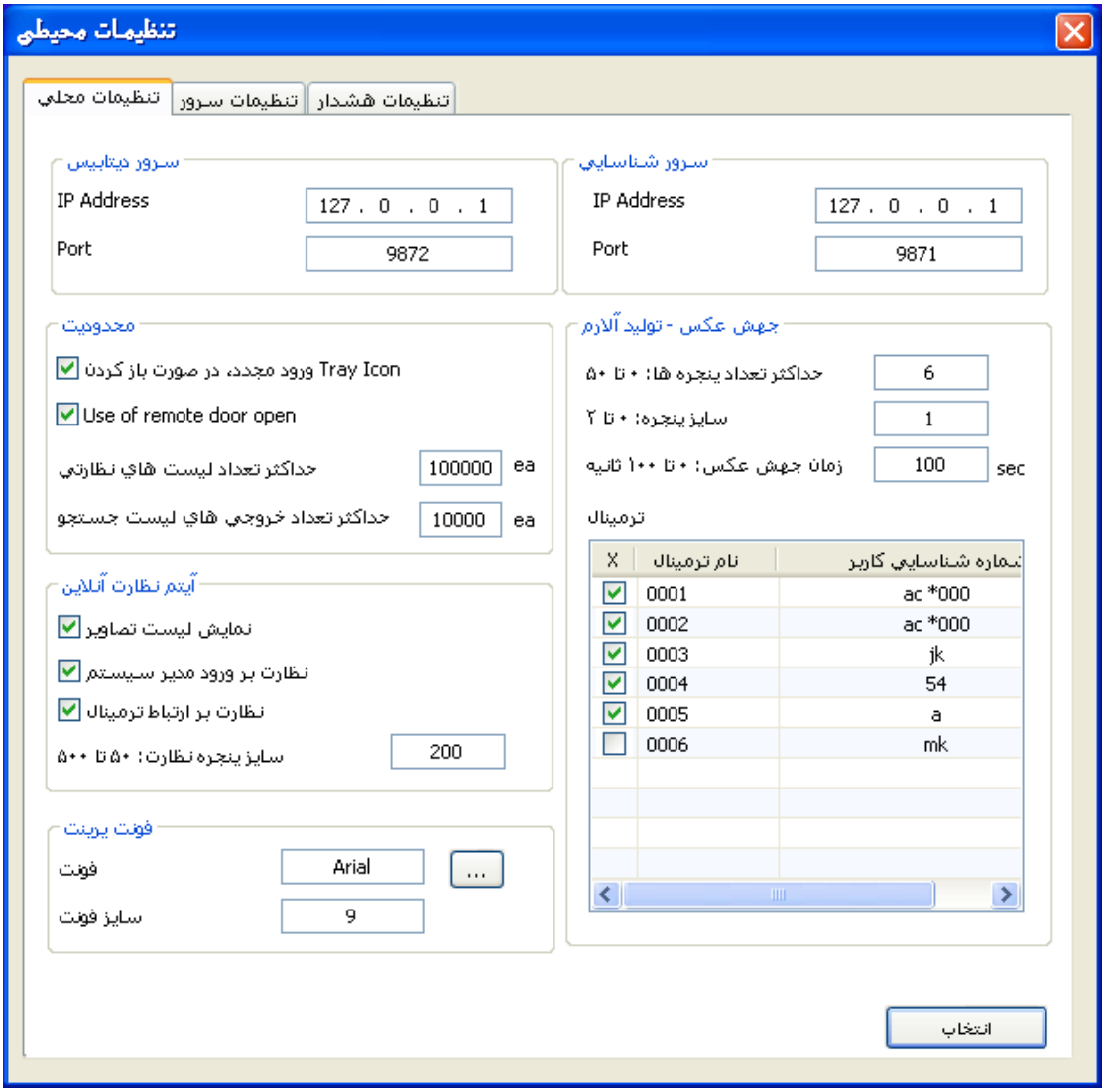
طرح بندی کارت اثرانگشت ثبت شده، یک کارت اثرانگشت صادر می کند.

۲.۲.۸.۳. تنظیمات محیطی

۲.۲.۸.۳.۱. تنظیمات محیطی شبکه محلی

گزینه های شبکه محلی برای سیستم Unis تنظیم می گردند.

مقادیر انتخابی تعیین شده تنها روی سیستم Unis عامل در یک کامپیوتر محلی، صحیح و معتبر می باشند.



بانک اطلاعاتی سرور

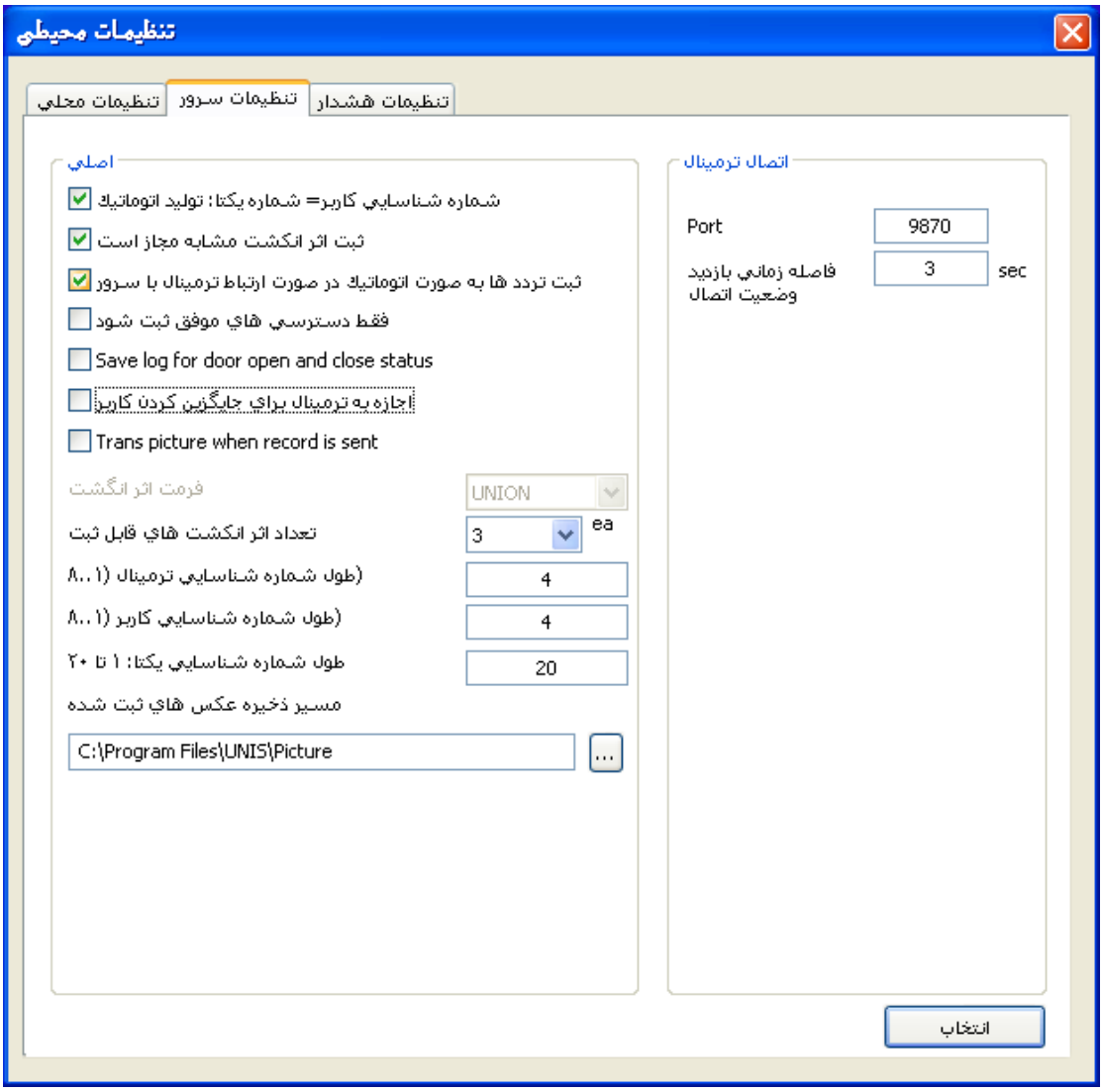
- آدرس IP: آدرس IP بانک اطلاعاتی سرور(آدرس IP کامپیوتری که در طول نصب برنامه بعنوان سرور تعیین گردیده)
- پورت: شماره پورت سوکت را جهت اتصال به بانک اطلاعاتی سرور وارد کنید.
- محدودیت
- مشاهده لیست کامل نقشه: در صفحه نظارت شکل دهی موقعیت، هر نقشه بعنوان یک لیست و نه بعنوان یک نقشه کامل نظارت شده است (برای کسب اطلاعات بیشتر، به بخش ۲.۲.۹. شکل دهی موقعیت رجوع شود).
- ورود دوباره در هنگام باز کردن tray icon: هنگام فعال بودن برنامه ای که با tray icon در حال اجراست، به عنوان مدیر وارد سیستم شوید.
- حداکثر تعداد لیست های نظارت: حداکثر تعداد لیست ها را وارد کنید تا در صفحه مانیتورینگ به نمایش گذاشته شود. اگر تعداد لیست ها از حداکثر میزان آن فراتر رود، لیست ها بطور خودکار جمع می شوند.
- حداکثر تعداد خروجی های لیست جستجو: حداکثر تعداد لیست ها را وارد کنید تا در صفحه جستجوی سوابق اعتبارسنجی نمایش داده شود.

بخش مانیتورینگ آنلاین

- ورود مدیر به سیستم مانیتورینگ: وضعیت ورود مدیر در نمایشگر ظاهر می گردد.
- مانیتورینگ اتصال ترمینال: وضعیت ترمینال در مانیتور نشان داده می شود.
- مانیتورینگ همزمان اندازه پنجره(۵۰۰~۵۰): اندازه افقی پنجره مانیتورینگ کلاینت/ترمینال تعیین شده است.
- فونت چاپ: برای خروجی چاپ فونت نصب می گردد.
- سرور اعتبارسنجی
- آدرس IP: آدرس IP سرور اعتبارسنجی را وارد نمایید (آدرس IP کامپیوتر سرور در طول نصب برنامه).
- پورت اتصال: شماره پورت سوکت سرور اعتبارسنجی را وارد کنید.
- پنجره pop up: تنظیم پنجره pop up تصویر هنگام موفقیت اعتبارسنجی در ترمینال اثرانگشت.
- حداکثر تعداد پنجره pop up (۶~۰): حداکثر تعداد پنجره pop up را جهت نمایش وارد کنید.
- مدت زمان ظهور پنجره pop up (۱۰۰~۰): مدت زمانی را که طول می کشد تا پنجره pop up باز شود بر حسب ثانیه وارد کنید.
- اندازه پنجره pop up (۲~۰): اندازه پنجره pop up را تعیین کنید.
- انتخاب ترمینال قابل اجرا: پنجره pop up تنها در روی ترمینال منتخب قابل تنظیم است.

۲.۲.۸.۳.۲. تنظیمات محیطی سرور

گزینه های انتخابی برای اینکه توسط سرور و تمام سیستم های unis به اشتراک گذاشته شوند، تنظیم می گردند.



مقدماتی

- شناسه کاربر به عنوان شناسه منحصربفرد استفاده می گردد (ایجاد خودکار): اگر شناسه اختصاصی بطور مجزا استفاده نگردد، با شناسه کاربری جایگزین می شود.
- امکان ثبت اثرانگشت مشابه: حین ثبت اثرانگشت کاربر، اثرانگشت مشابه بدون انتخـــاب ثبت می گردد.
- به محض اتصال ترمینال، بطور خودکار وارد سیستم دسترسی شوید: پس از قطع اتصال ترمینال، سابقه اعتبارسنجی که در ترمینال باقی مانده، در هنگام اتصال مجدد ترمینال، به سرور ارسال می شود.
- تنها ورود اعتبارسنجی موفق را ذخیره کنید: رویداد اعتبارسنجی ناموفق فقط می تواند در مانیتور انتخاب گردد، اما ذخیره نمی شود.

- همزمانی خودکار تغییر اطلاعات کاربری در ترمینال: در صورتی که اطلاعات کاربری تغییرکند، اطلاعات کاربری ذخیره شده در ترمینال نیز تغییر کرده است.
- تعداد اثرانگشتی که قابل ثبت است: (۱۰~۱)
- طول شناسه ترمینال(۸~۱): تعداد رقمهای مورد نظر را برای شناسه تعیین کنید.
- طول شناسه کاربر(۸~۱): تعداد رقمهای مورد نظر را برای شناسه تعیین کنید.
- طول شناسه اختصاصی(۲۰~۱): تعداد رقمهای مورد نظر را برای شناسه تعیین کنید.
- دامنه شناسه بازدیدکننده: محدوده شناسه ای را که باید به بازدید کننده داده شود، تعیین کنید.
- تنظیمات اتصال ترمینال
- پورت: شماره پورت سوکت را جهت اتصال ترمینال به سرور وارد کنید.
- مدت زمان بررسی وضعیت اتصال: وضعیت اتصال بین ترمینال و سرور در یک فاصله زمانی معین بررسی می شود.

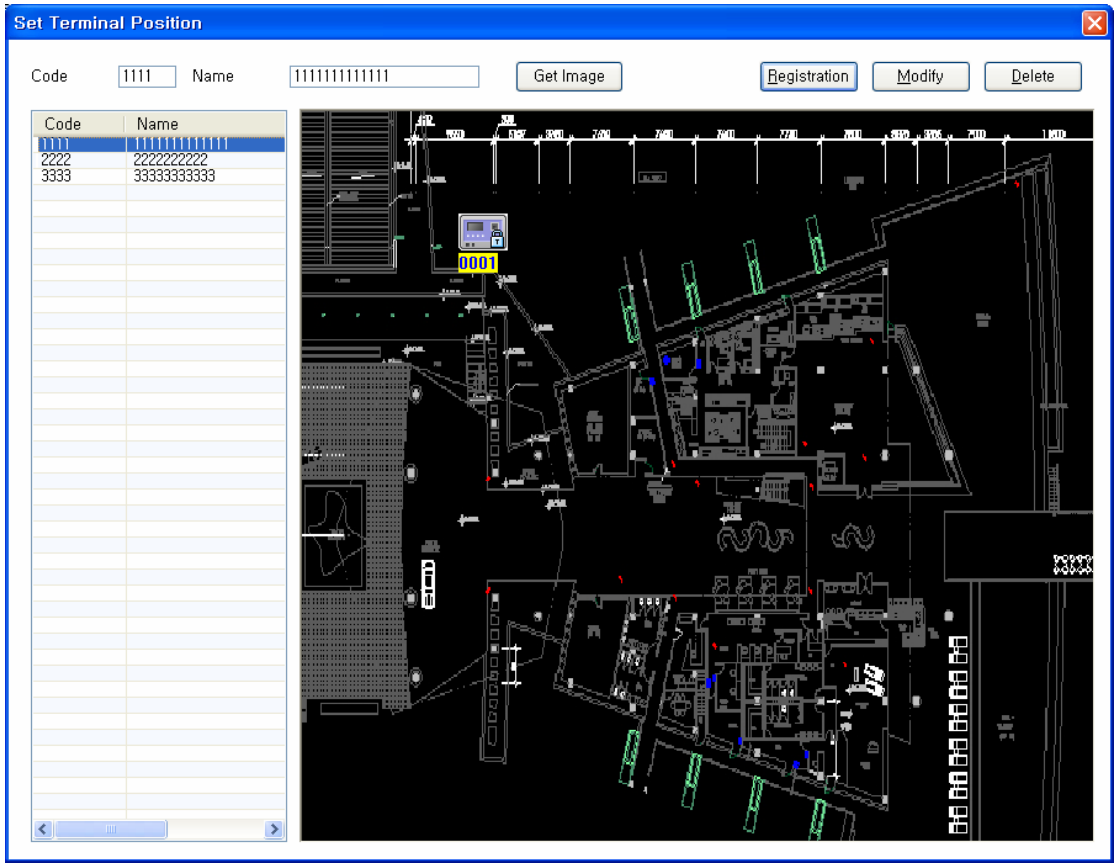
۲.۲.۹. شکل دهی موقعیت(e-map)

وضعیت ترمینال از یک موقعیت ترسیمی ثبت شده همزمان قابل رویت است.

جهت انجام این کار، موقعیت تمام ترمینال ها به همراه نقشه ها بایستی تعیین گردد. تنها فایلهای تصویری با فرمت JPEGوBMP می توانند در شکل دهی موقعیت ثبت شوند. به منظور عملکرد DB بهتر است در صورت امکان از فایلهای با فرمتJPEG استفاده گردد.

(برای انواع دیگر فایلهای تصویری، پیش از استفاده لازم است با کمک ابزار گرافیکی، فایل را به فرمت JPEG ذخیره نمایید.)

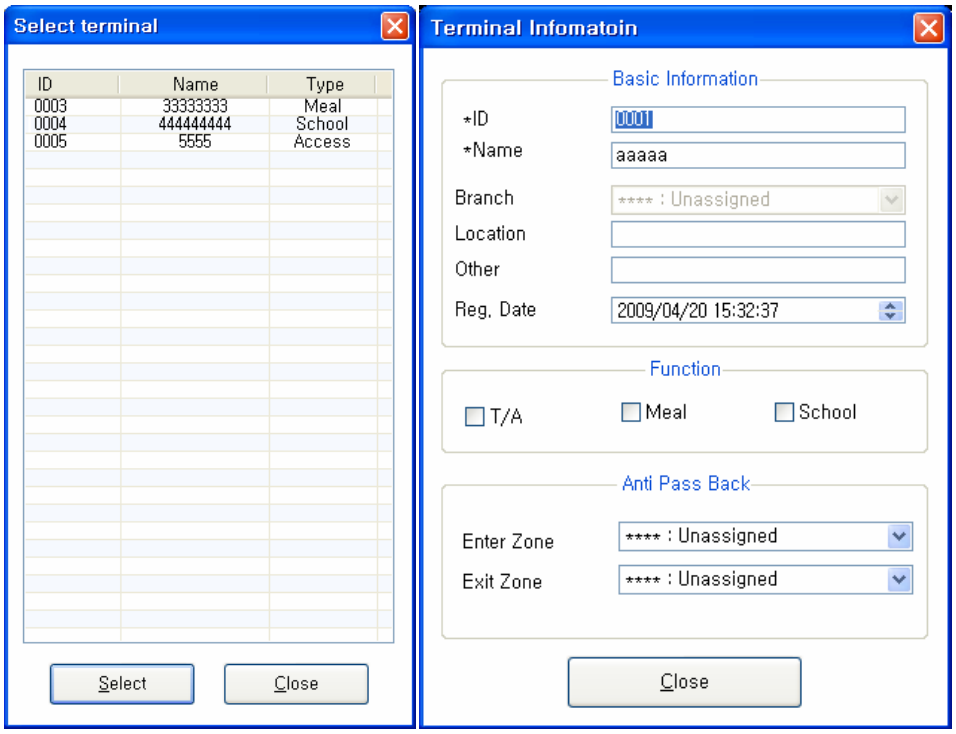
۲.۲.۹.۱. تنظیم موقعیت ترمینال



از منوی[شکل دهی موقعیت] موجود در سمت چپ صفحه اصلی، بر روی گزینه [تنظیم موقعیت ترمینال] کلیک کنید تا صفحه ای همانند شکل فوق ظاهر شود. برای انتخاب طراحی پس زمینه، بر روی گزینه[انتخاب تصویر] کلیک نموده و تصویر پس زمینه را انتخاب کنید.

اگر شما با موس بر روی نقشه مربوطه کلیک راست انجام دهید، لیستی از ترمینالها جهت انتخاب ظاهر می شوند. ترمینالی را انتخاب نموده و آن را در بالای تصویر پس زمینه بگذارید. هنگامی که تعیین موقعیت ترمینال به اتمام رسید، کد و نام نقشه مربوطه را وارد و آن را ثبت کنید.

در صورت نیاز به هرگونه تغییر، یک نقشه را از لیست موجود در سمت چپ انتخاب و تغییرات لازم را اعمال نمایید. دکمه[اصلاح] را بفشارید تا مقادیر تغییر یافته ذخیره گردد.



در صورت ضرورت تغییر مکان، آیتم ترمینال مربوطه را با استفاده از موس کلیک و درگ نموده و آن را در یک موقعیت مناسب قرار دهید.

شما می توانید اطلاعات جزئی ثبت ترمینال را با دوبار کلیک کردن بر روی آیکون ترمینال موردنظر مشاهده نمایید.

۲.۲.۹.۲. تنظیم موقعیت نقشه

اگر موقعیت هر نقشه در کل نقشه تعیین شده باشد، محل قرارگیری نقشه حین مانیتورینگ در یک نظر اجمالی قابل رویت است.

تعیین موقعیت نقشه تنها برای یک نقشه با یک موقعیت ترمینال تعیین شده، قابل ثبت است.

در صورت عدم ثبت تعیین موقعیت نقشه، بهتر است مشاهده و نظارت لیست تمام نقشه را فقط با استفاده از یک لیست و بدون ترسیم کامل آن بررسی کنید.

پس از آنکه با کلیک کردن بر روی دکمه تصویر، تصویر پس زمینه را انتخاب نمودید، می توانید به ادامه کار بپردازید.

با انجام کلیک راست موس بر روی نقشه کامل، یک نقشه را جهت قرار گرفتن انتخاب کنید. برای تغییر مکان یک آیتم، در حالیکه روی آن کلیک کرده اید، آن را حرکت دهید.

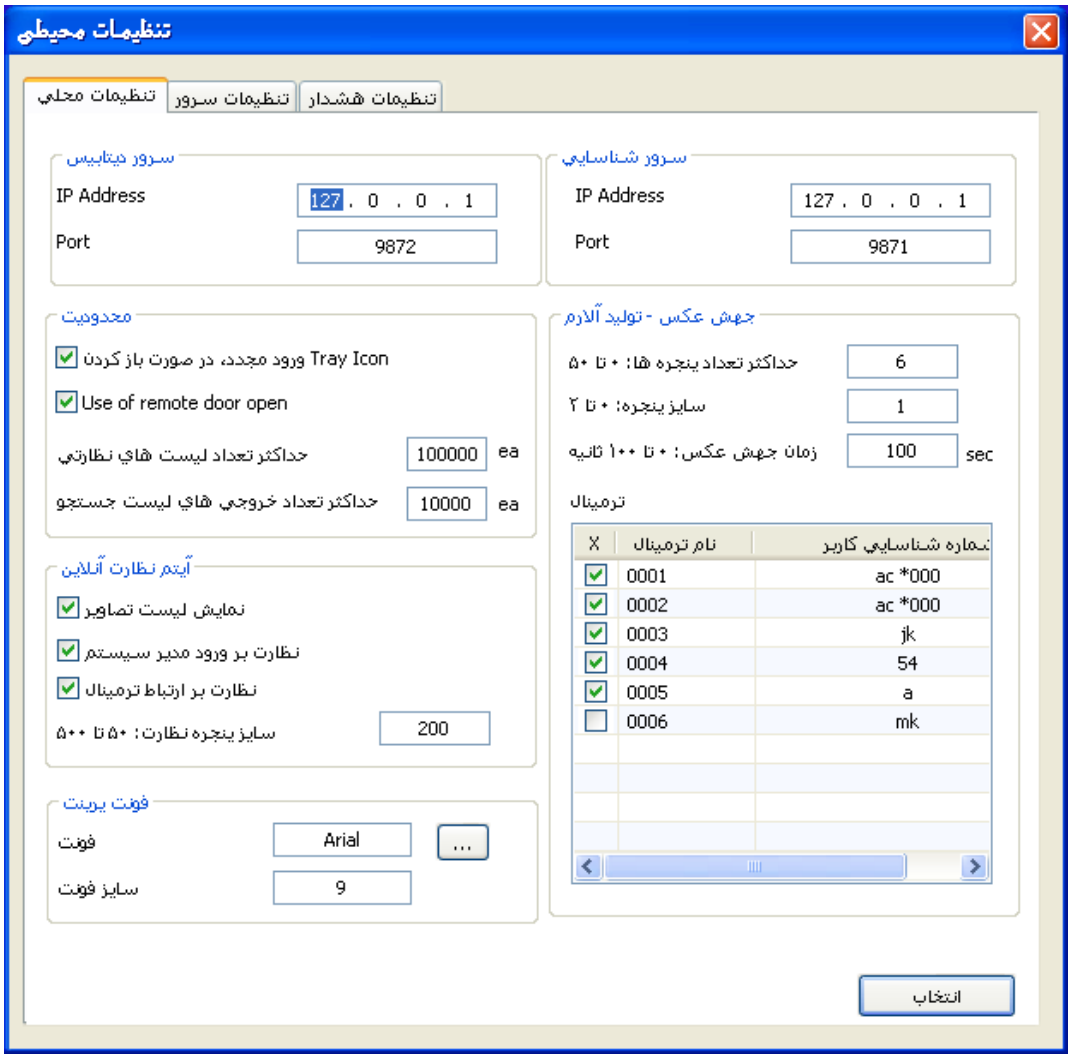
اگر بر روی آیتمی دوبار کلیک شود، اطلاعات مربوطه به نمایش در می آید.

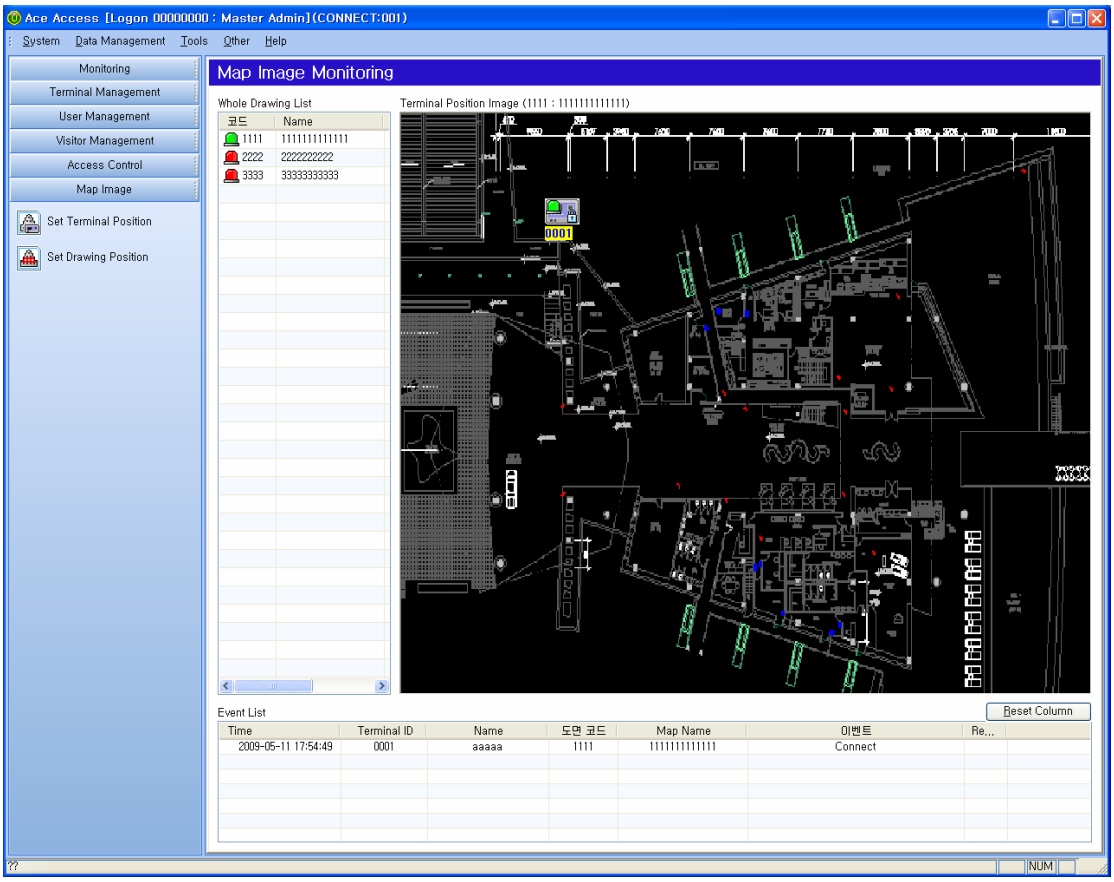
وقتی تعیین موقعیت نقشه خاتمه یافت، جهت ذخیره نمودن عملیات، دکمه ذخیره را بفشارید.

۲.۲.۹.۳. نظارت شکل دهی موقعیت

هنگامی که همه کارهای ترسیم به اتمام رسید، سیستم نیاز به راه اندازی مجدد دارد تا کارهای صورت گرفته بـر روی شـکل دهـی موقعیت را کارآمد نماید.

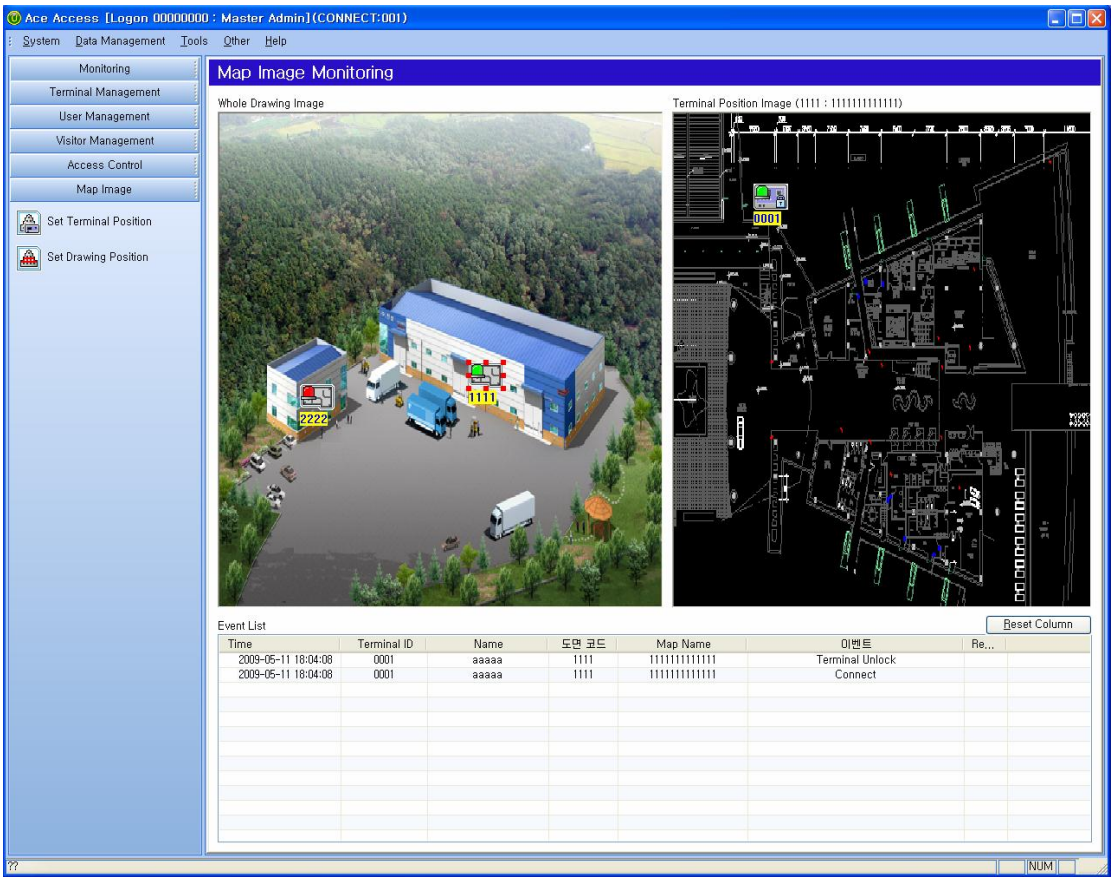
صفحه مانیتورینگ دو نوع فرم طرح بندی دارد. انتخاب طرح بندی در [تنظیمات محیطی] از منوی[ابزار] انجـــام مـی شـود. اگـر شما در تنظیمات محیطی محلی، مشاهده لیست نقشه کامل را انتخاب کنید، می توانید نقشـه کامـل را بـه صـورت یـک لیسـت و جزییات نقشه را در یک فرم مبسوط ببینید.





هنگام مشاهده نوع لیست نقشه کامل، یک نقشه را از لیست موجود در سمت چپ انتخاب و روی آن دوبار کلیک نمایید. سپس جزییات نقشه مربوطه در سمت راست ظاهر می گردد و موقعیت تمام ترمینالهای وابسته نشان داده می شود.

اگر شما روی لیست رویداد در قسمت تحتانی پنجره دوبار کلیک کنید، نقشه ی جایی که ترمینال رویداد مربوطه وجود دارد، نشان داده می شود و ترمینال مربوطه بعنوان ترمینال منتخب به نمایش در می آید.



اگر شما روی یک آیتم ترسیمی در نقشه کامل موجود در سمت چپ دوبارکلیک کنید، آیتم مربوطه بعنوان یک آیتم منتخب نمایش داده می شود. جزییات نقشه مربوطه در سمت راست نشان داده شده و همه ترمینالهای وابسته به این نقشه به نمایش در می آیند.

اگر روی لیست وقایع در قسمت تحتانی پنجره دوبار کلیک کنید، موقعیت ترمینال رویداد ذیربط نمایان شده و ترمینال مربوطه به عنوان یک ترمینال منتخب به نمایش در می آید.

موارد ذیل تصاویر و توضیحات آیتم ها می باشند:

آیتم معرف یک نقشه

آیتم معرف یک ترمینال کنترل تردد(مانیتورینگ ورودی/خروجی امکانپذیر است)

آیتم معرف یک ترمینال حضور و غیاب(مورد استفاده در مدیریت حضور و غیاب)

آیتم معرف یک ترمینال ساعت حضور و غیاب(مورد استفاده در مدیریت ساعت حضور وغیاب)

آیتم معرف یک ترمینال آب آشامیدنی(مورد استفاده در مدیریت نوشیدن آب)

مطالب زیر توضیحاتی راجع به سیگنالهای به نمایش در آمده بر روی ترمینال ارائه می دهند:

قطع ارتباط شبکه را اعلام می کند (به عنوان هشدار در نقشه نمایش داده می شود).

باز بودن پوشش ترمینال را اعلام می دارد (به عنوان هشدار در نقشه نمایش داده می شود).

اعلام حریق در ترمینال (به عنوان هشدار در نقشه نمایش داده می شود).

اعلام بازبودن در متصله به ترمینال (به عنوان اخطار در نقشه نمایش داده می شود).

اعلام قفل بودن ترمینال (به عنوان اخطار در نقشه نمایش داده می شود).

اعلام وضعیت سیگنال خارجی مانند پیشگیری از جرم (به عنوان اخطار در نقشه نمایش داده می شود).

اعلام وضعیت عادی در ترمینال (در حالت عادی در یک نقشه نشان داده می شود).

موارد ذیل توضیحاتی پیرامون سیگنالهای به نمایش درآمده بر روی یک نقشه هستند:

اعلام وضعیت هشدار

اعلام وضعیت اخطار

اعلام وضعیت عادی

سیگنالهای اولیه ای که در نقشه نشان داده می شوند بصورت هشدار>اخطار>عادی تعریف می گردند. اگر حداقل یک ترمینال بسته به وضعیت ترمینالهای مربوط به نقشه به وضعیت اولیه تبدیل شود، بنابراین علامت نقشه تغییر یافته است.

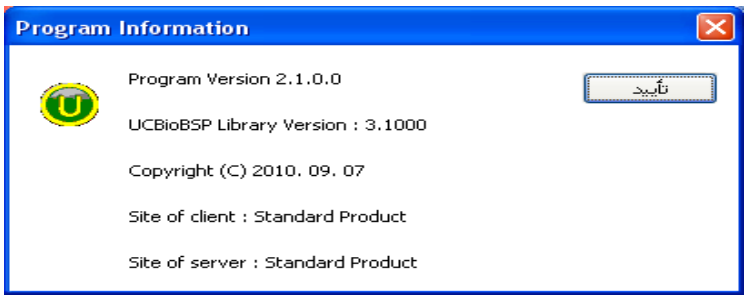
۲.۲.۱۰.سایر موارد

۲.۲.۱۰.۱ tray icon

برنامه unis می تواند به صورت tray icon کوچک شود.

برای باز کردن مجدد برنامه unis، روی tray icon موجود در گوشه راست پایین ترین نقطه پنجره دوبار کلیک کنید.

اگرجهت ورود مدیر به سیستم رمز عبور تنظیم شده باشد، شناسه و رمز عبور لازم است.

۲.۲.۱۱. اطلاعات برنامه

این بخش، نسخه برنامه unis و نسخه برنامه اثرانگشت را نشان می دهد.