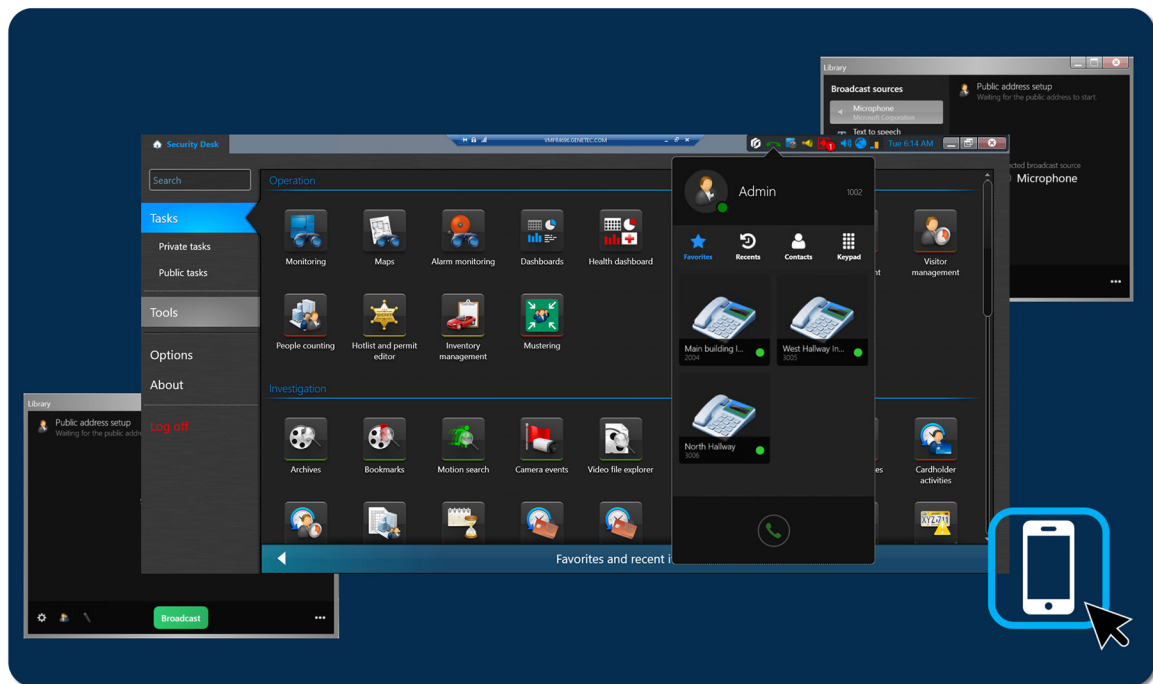


مدیریت کاربران (User Management) در جتک بخشی حیاتی از نرم افزار است که کنترل می کند چه افرادی می توانند وارد سیستم شوند و هر کاربر به چه امکانات و منابعی دسترسی دارد. به عبارت ساده تر، User Management تضمین می کند که هر فرد تنها به اندازه وظیفه و مسئولیت خود از سیستم استفاده کند و دسترسی اضافی یا غیرمجاز نداشته باشد. هر کاربر در جتک نماینده یک شخص واقعی است و با نام کاربری و رمز عبور مخصوص به خود وارد سیستم می شود. این ویژگی باعث می شود همه کاربران بتوانند به صورت مستقل و امن وارد نرم افزار شوند و هیچ کاربری مجبور به اشتراک گذاری اطلاعات ورود خود با دیگران نباشد.

اهمیت مدیریت کاربران در سیستم های امنیتی و نظارتی بسیار بالاست زیرا همه کاربران نباید دسترسی یکسان داشته باشند. به عنوان مثال، یک اپراتور نظارت تصویری فقط نیاز دارد تصاویر زنده یا ضبط شده را مشاهده کند و تغییرات مدیریتی یا تنظیمات کلی سیستم برای او غیرضروری است. از طرف دیگر، مدیر سیستم یا مسئول امنیت نیاز دارد به تنظیمات، گزارش ها و بخش های مدیریتی دسترسی داشته باشد تا بتواند عملکرد سیستم را کنترل کند. User Management در جتک باعث می شود که دسترسی ها کنترل شده و امن باشند، از تغییرات ناخواسته جلوگیری شود و مسئولیت هر کاربر مشخص باشد. این کار نه تنها امنیت سیستم را افزایش می دهد، بلکه در صورت بروز خطا یا سوءاستفاده، می توان دقیقاً مشخص کرد که کدام کاربر چه عملی انجام داده است.

سطح دسترسی ها در جتک بر اساس نقش ها و وظایف تعریف می شود. می توان تعیین کرد که هر کاربر به کدام دوربین ها دسترسی داشته باشد، آیا می تواند تصویر زنده یا ضبط شده را مشاهده کند یا خیر، امکان تغییر تنظیمات را داشته باشد یا نه و به گزارش ها و بخش های مدیریتی دسترسی داشته باشد یا خیر. علاوه بر این، سیستم امکان تعریف گروه های کاربری (User Groups) را فراهم می کند تا مدیریت دسترسی ها ساده تر و سازمان یافته تر شود. برای مثال، همه اپراتورهای نظارت تصویری می توانند در یک گروه قرار بگیرند و دسترسی مشابهی به تصاویر زنده و ضبط شده داشته باشند، در حالی که مدیران سیستم در گروه دیگری قرار می گیرند و دسترسی کامل به تمامی بخش ها خواهند داشت.



ویژگی‌های کلیدی User Management:

- کنترل دقیق سطح دسترسی‌ها: در این مدل، می‌توان به‌صورت کاملاً جزئی مشخص کرد که هر کاربر به کدام بخش‌ها، تجهیزات، ماژول‌ها و تنظیمات سیستم دسترسی داشته باشد یا نداشته باشد. این کنترل بدون وابستگی به سایر کاربران انجام می‌شود و امکان پیاده‌سازی سیاست «حداقل دسترسی لازم» را فراهم می‌کند.
- افزایش امنیت کلی سیستم: زمانی که هر کاربر فقط به امکانات مرتبط با وظیفه خود دسترسی دارد، احتمال سوءاستفاده عمدی یا سهوی، نفوذ داخلی و ایجاد تغییرات ناخواسته در سیستم به‌طور قابل توجهی کاهش پیدا می‌کند.
- کاهش خطای انسانی: محدود بودن محیط کاری هر کاربر به ابزارهای موردنیازش باعث می‌شود عملیات حساس یا تنظیمات حیاتی به اشتباه تغییر داده نشوند و ریسک خطاهای انسانی به حداقل برسد.
- امکان تغییر سریع سیاست‌های دسترسی: در صورت تغییر سیاست‌های امنیتی یا ساختار سازمانی، کافی است Role مربوطه ویرایش شود تا تغییرات به‌صورت خودکار روی تمام کاربران مرتبط اعمال گردد.

❖ جلوگیری از دسترسی‌های غیرضروری: با حذف دسترسی‌های اضافی، کاربران تنها بخش‌هایی از سیستم را مشاهده یا کنترل می‌کنند که واقعاً به آن نیاز دارند، که این موضوع هم امنیت و هم تمرکز کاری را افزایش می‌دهد.

❖ افزایش سرعت و دقت در مدیریت کاربران: افزودن کاربر جدید یا جابه‌جایی کاربران بین بخش‌ها تنها با تخصیص یا تغییر Role انجام می‌شود. این روش علاوه بر صرفه‌جویی در زمان، احتمال خطا در تنظیم مجوزها را نیز به‌طور محسوسی کاهش می‌دهد.

در نهایت، User Management در جنتک هسته اصلی کنترل دسترسی نرم‌افزاری سیستم است و تعیین می‌کند چه کسی، در چه زمانی و با چه سطحی از اختیار بتواند به بخش‌های مختلف سامانه دسترسی داشته باشد. این مازول امکان تعریف کاربران، تخصیص نقش‌ها، محدودسازی دسترسی به دوربین‌ها، درب‌ها، مازول‌ها و تنظیمات سیستمی را به‌صورت کاملاً جزئی و مبتنی بر سیاست‌های سازمانی فراهم می‌کند. با استفاده از User Management، هر کاربر فقط به اطلاعات و قابلیت‌هایی دسترسی دارد که برای انجام وظایفش ضروری است، نه بیشتر. این ساختار باعث افزایش امنیت کلی سیستم، کاهش خطای انسانی، بهبود پاسخ‌گویی اپراتورها و امکان ردیابی کامل فعالیت کاربران از طریق لاگ‌ها می‌شود.