

سامانه مدیریت هویت و دسترسی آیدیمنت



از سال ۱۳۸۸ اراده‌مان را متمرکز کردیم تا میهنمان را به اوج قله‌های پیشرفت در فناوری اطلاعات و ارتباطات برسانیم و در این مسیر ناب‌ترین استعدادها به شوق حل پیچیده‌ترین مسائل با ما همراه شده‌اند. اکنون بسیاری از سازمان‌های بزرگ در بخش دولتی و خصوصی، مهیمن را شریکی توانمند و قابل اتکا در مسیر هوشمندسازی و تحول دیجیتال یافته‌اند و آنچه با همکاری هم ساخته‌ایم برای کسب و کارها و جامعه ارزش‌آفرینی می‌کند.

حرکت به سوی قله ادامه دارد ...



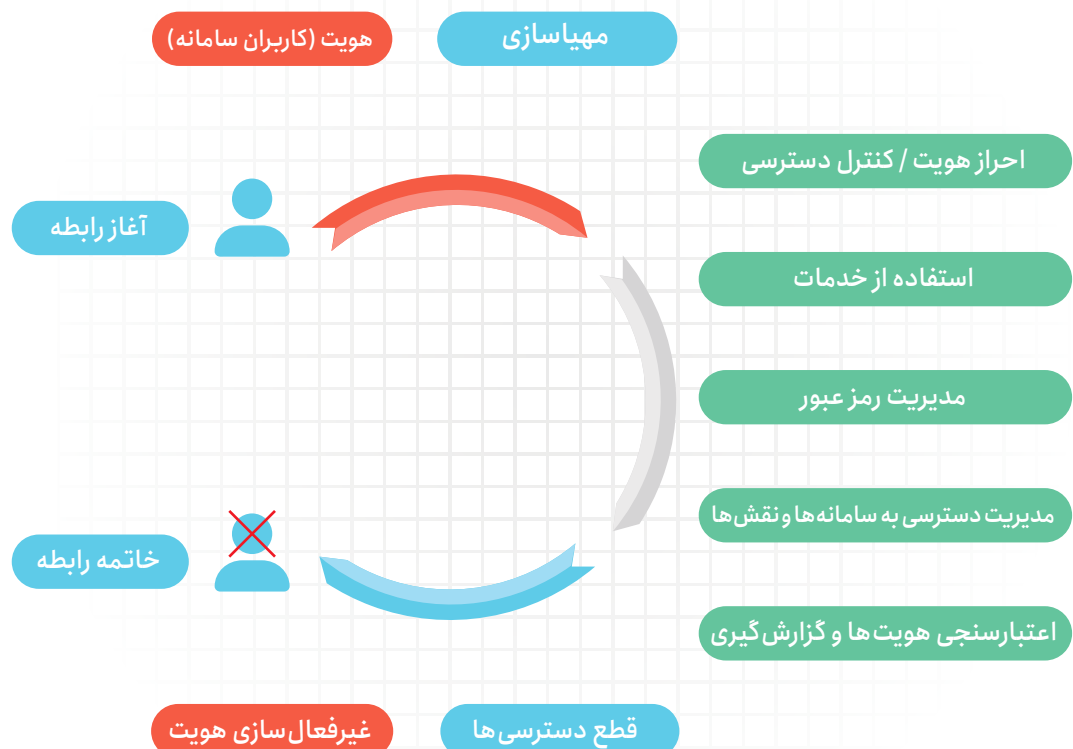
- ۲ آیدیمت چه کاری انجام می دهد؟
- ۳ چرا آیدیمت مهم است؟
- ۴ گواهی افتای محصول
- ۵ نگاه کلی به محصول
- ۷ ویژگی های کلیدی



آیدیمنت چه کاری انجام می دهد؟

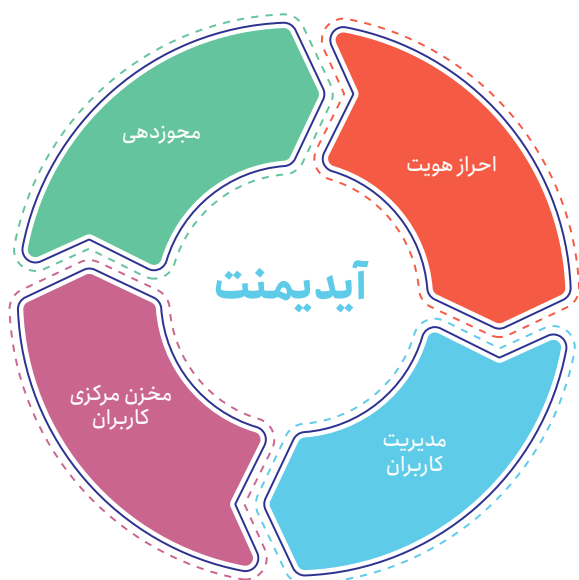
آیدیمنت یک سامانه‌ی مدیریت هویت و دسترسی (IAM (Identity and Access Management) است. آیدیمنت این اطمینان خاطر را برای سازمان‌ها به وجود می‌آورد که افراد و موجودیت‌هایی که دارای هویت‌های دیجیتال هستند، سطح درستی از دسترسی را به منابع سازمان از جمله داده‌ها، شبکه‌ها و سامانه‌های نرم‌افزاری دارند. با این سامانه می‌توان مدیریت چرخه‌ی حیات هویت کاربران از جمله تعریف یا حذف کاربر، اعطا، سلب و یا تنظیم دسترسی یا نقش کاربر، ردیابی فعالیت و ارائه گزارش‌های متنوع مدیریتی، اعمال سیاست‌های امنیتی دلخواه و نهایتاً احراز هویت کاربران را در نهایت دقت، سرعت و امنیت انجام داد.

چرخه حیات مدیریت هویت و دسترسی

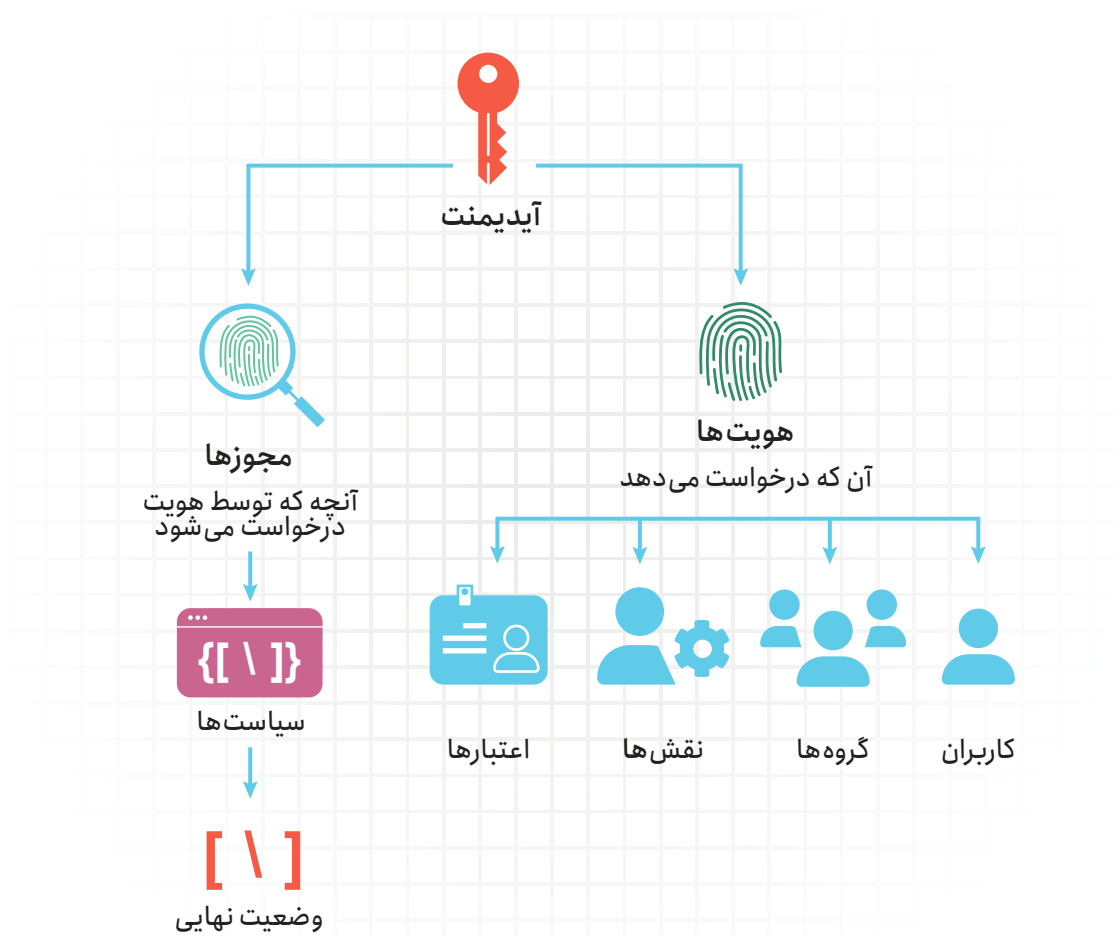




چرا آیدیمنت مهم است؟



نیاز به مدیریت بهینه هویت‌ها و دسترسی‌های اعضای سازمان از دغدغه‌های اصلی سازمان‌های در حال رشد و بزرگ‌مقیاس محسوب می‌شود. در مواجهه با این نیاز و پیچیدگی‌های آن، وجود سامانه‌ای یکپارچه و کارآمد که بتواند علاوه بر رفع نیازها، نگرانی‌های امنیتی را نیز رفع نماید ضروری است. با سامانه یکپارچه مدیریت هویت و دسترسی آیدیمنت، به سهولت می‌توان انواع تنظیمات و نیازمندی‌های مربوطه را انجام داد.





گواهی افتای محصول

در چشم‌انداز امنیت سایبری امروز، سازمان‌ها نیازمند اطمینان از این موضوع هستند که راهکارهای نرم‌افزاری مورد استفاده، به‌ویژه در حوزه زیرساختی مانند مدیریت هویت و دسترسی، از بالاترین سطوح امنیتی و کیفی برخوردار باشند. صرف ادعا برای تأمین امنیت کافی نیست؛ بلکه این امنیت باید توسط نهادهای معتبر ملی ارزیابی و تأیید گردد.

مرکز مدیریت راهبردی افتا به عنوان مرجع رسمی ارزیابی و صدور گواهی‌نامه‌های امنیتی برای محصولات حوزه فناوری اطلاعات در کشور، نقشی حیاتی در این زمینه ایفا می‌کند. دریافت گواهی افتا برای یک محصول، نشان‌دهنده انطباق کامل آن با الزامات امنیتی تعریف‌شده و گذراندن موفقیت‌آمیز آزمون‌های دقیق نفوذ و ارزیابی‌های عملکردی است.

سامانه مدیریت هویت و دسترسی آیدیمنت، در راستای تعهد خود به ارائه محصولی امن، پایدار و قابل اعتماد و با هدف ایجاد اطمینان خاطر کامل برای مشتریان خود، مفتخر است که پس از طی فرایندهای ارزیابی فنی و امنیتی دقیق، موفق به اخذ گواهی‌نامه افتا گردیده است. این دستاورد، گواهی بر این مدعاست که آیدیمنت نه تنها بر اساس استانداردهای بین‌المللی طراحی شده، بلکه با تمامی سیاست‌ها و الزامات امنیتی ملی نیز سازگار است. این گواهی به سازمان‌ها تضمین می‌دهد که حفاظت از دارایی‌های دیجیتال و مدیریت دسترسی کاربران آن‌ها در بستری کاملاً تأیید شده و امن صورت می‌پذیرد.





نگاه کلی به محصول

آیدیمنت سامانه‌ای برای مدیریت یکپارچه هویت در فرایندهای سازمانی است که قادر است فرایند مدیریت چرخه‌ی حیات و دسترسی کاربر را در سازمان هوشمند و کارآمد کند. استفاده از این محصول، این ارمغان را برای سازمان به همراه خواهد داشت که میزان دسترسی همه کاربران به تمامی منابع سازمان منطبق بر سیاست‌های امنیتی مدنظر سازمان است.

ورود به حساب کاربری

چنانچه اپلیکیشن آتین را بر روی گوشی خود نصب داشته باشید، بعد از ثبت نام نسخه موبایل می‌توانید این QR کد را اسکن کنید و وارد حساب کاربری خود شوید.

Login *

رمز عبور *

ورود

رمز عبور خود را فراموش کرده‌اید؟

ورود و خروج یکپارچه

با یکپارچگی سامانه‌های نرم‌افزاری سازمان با آیدیمنت، کاربران سامانه‌ها می‌توانند به جای استفاده از هویت‌ها و رمزهای عبور متفاوت (که به دلیل تنوع در سطوح دسترسی و مخازن هویتی رخ می‌دهد) از یک نام کاربری و رمز عبور واحد برای ورود به تمامی سامانه‌ها استفاده کنند.

اعتبارسنجی هویت

مدیر سامانه می‌تواند با مدیریت رمز عبور کاربران و اعمال سیاست‌های احراز هویتی و نقش‌ها و گروه‌های متفاوت و انتصاب سیاست دلخواه به هرکدام از کاربران، از صحت اعتبارسنجی کاربر بر مبنای سیاست تعیین شده سازمان اطمینان حاصل نماید.

ثبت نام کاربر

با استفاده از این قابلیت، سازمان‌ها از جریان‌های نامحدود ثبت نام بهره برده و ضمن امکان تعریف جریان مبتنی بر نوع کاربر، از سازگاری کامل با سرویس تأیید هویت برخوردار است.

اعطا و کنترل مجوز

آیدیمنت از پیاده‌سازی‌های خاص و روش‌های متفاوت کنترل دسترسی پشتیبانی کرده و امکان کنترل دسترسی به محتوا و فرم‌های داخل سامانه‌ها مبتنی بر قوانین و سیاست‌های سازمان را برای کاربر فراهم می‌آورد. همچنین با فراهم آوردن امکان «تحویل برنامه» ضمن استقرار در لبه‌ی شبکه، اقدام به جلوگیری از دسترسی به برنامه‌ها بدون احراز هویت قبلی می‌نماید.



خصیصه‌های کاربران برای سامانه فراهم است. همچنین امکان اتصال به انواع مخازن هویتی سازمانی در سامانه پیش‌بینی شده است.

احراز هویت بر مبنای RADIUS

یکپارچه‌سازی اندپوینت‌های RADIUS با SSO و احراز هویت VPN به صورت یکپارچه با سایر سامانه‌های سازمانی، یکی از نقاط قوت آیدیمنت است. همچنین به دلیل یکپارچه بودن تمامی سرویس‌ها، امکان راه‌اندازی احراز هویت چندعاملی نیز برای اندپوینت‌های RADIUS مهیا است.

پایش و گزارش‌دهی

با توجه به حساسیت عملکرد محصول آیدیمنت در سازمان‌ها، لاگ تمامی رفتارهای کاربران ثبت شده و با استفاده از داشبورد مدیریت، امکان استخراج انواع متفاوت گزارش‌های مورد نیاز برای مدیر سامانه فراهم است.

احراز هویت چندعاملی (MFA)

با استفاده از احراز هویت چندعاملی یا MFA، سازمان‌ها می‌توانند سطح امنیت سامانه‌های خود را تا حد زیادی بالاتر ببرند. استفاده از Email، SMS، تماس تلفنی و push notification به عنوان فاکتور هویت‌سنجی و فراهم آوردن فاکتورهای احراز هویت متفاوت به ازای هر سیاست و اعمال تنظیمات متفاوت روی سیاست‌های امنیتی گوناگون این بخش، حداکثر امنیت را برای حراست از ورود امن سازمان‌ها فراهم می‌آورد.

مدیریت دسترسی به API‌ها

از مدیریت دسترسی به API‌ها می‌توان برای ایمن‌سازی API‌های سازمان استفاده کرد. این سرویس با سایر بخش‌های محصول یکپارچه است. کاربر ادمین، امکان مدیریت دسترسی و مجوز مرکزی و همچنین مدیریت دامنه‌ها و ادهای قابل تنظیم را دارد.

دایرکتوری مجازی

با ارائه پروتکل LDAP، امکان احراز هویت و دریافت





ویژگی‌های کلیدی

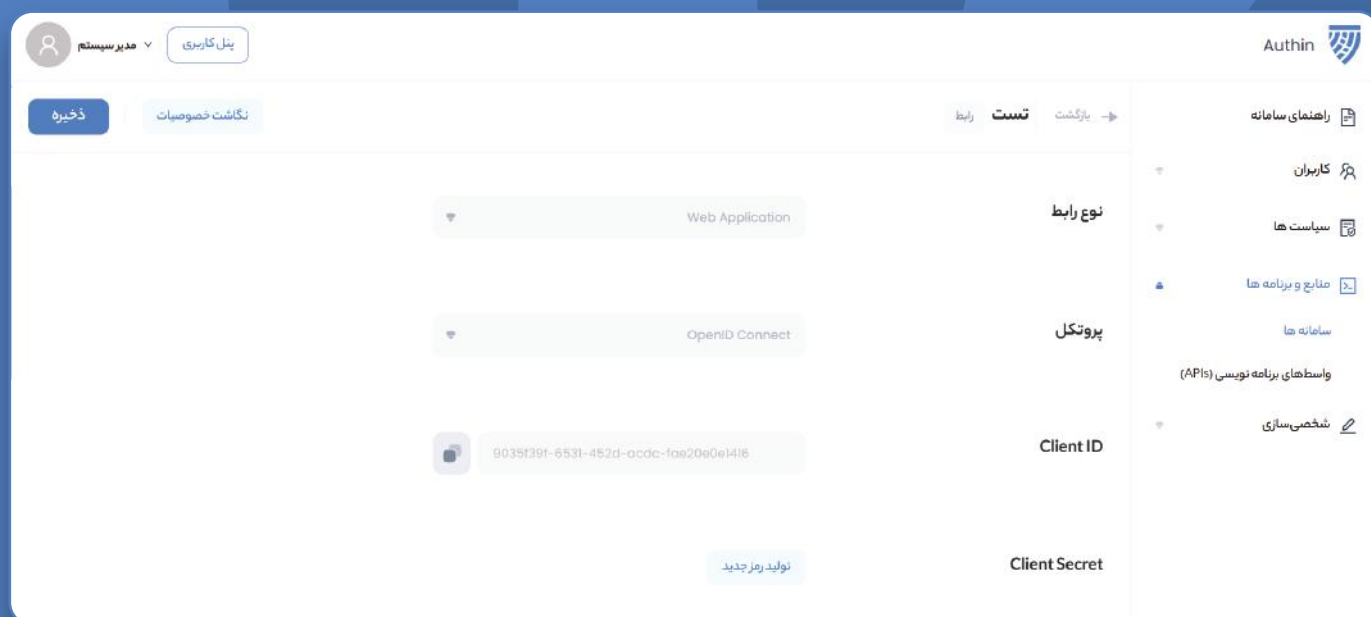
ورود و خروج یکپارچه

- احراز هویت نامحدود SAML و OIDC
- مدیریت سیاست‌های رمز عبور
- بازنشانی رمز عبور
- شخصی‌سازی پنل و صفحات
- گزارش‌های استاندارد و شخصی‌سازی شده
- یکپارچگی با SIEM
- قابلیت تعیین محدوده‌های IP
- مدیریت یکپارچه سیاست‌های امنیتی
- دارای سازوکار مناسب جهت مدیریت Session
- امکان تعریف کاربران و گروه کاربران به تعداد نامحدود
- امکان تعریف ساعات کاری برای هر کاربر و یا گروه کاربری
- امکان تعریف گروه‌های کاری
- امکان تعریف نقش‌ها و گروه‌های وابسته
- امکان تعریف سیاست‌های احراز هویت
- امکان تعریف سیاست‌های مورد نظر سازمان بدون محدودیت و در قالب استانداردهای امنیتی

- امکان تعیین کلیه سیاست‌های رمز عبور مانند بازنشانی، تغییر و ...

اعتبارسنجی هویت

- User Provisioning
- User Deprovisioning
- خصیصه‌های سفارشی
- همگام‌سازی دایرکتوری و هویت
- یکپارچه‌سازی تعداد نامحدود دایرکتوری
- نگاشت سفارشی
- پشتیبانی از SCIM
- یکپارچه‌سازی با سامانه منابع انسانی
- گزارش‌های دسترسی
- جلوگیری از دسترسی به برنامه‌ها بدون احراز هویت قبلی
- توسعه و استقرار در لبه شبکه





ویژگی‌های کلیدی

ثبت نام کاربر

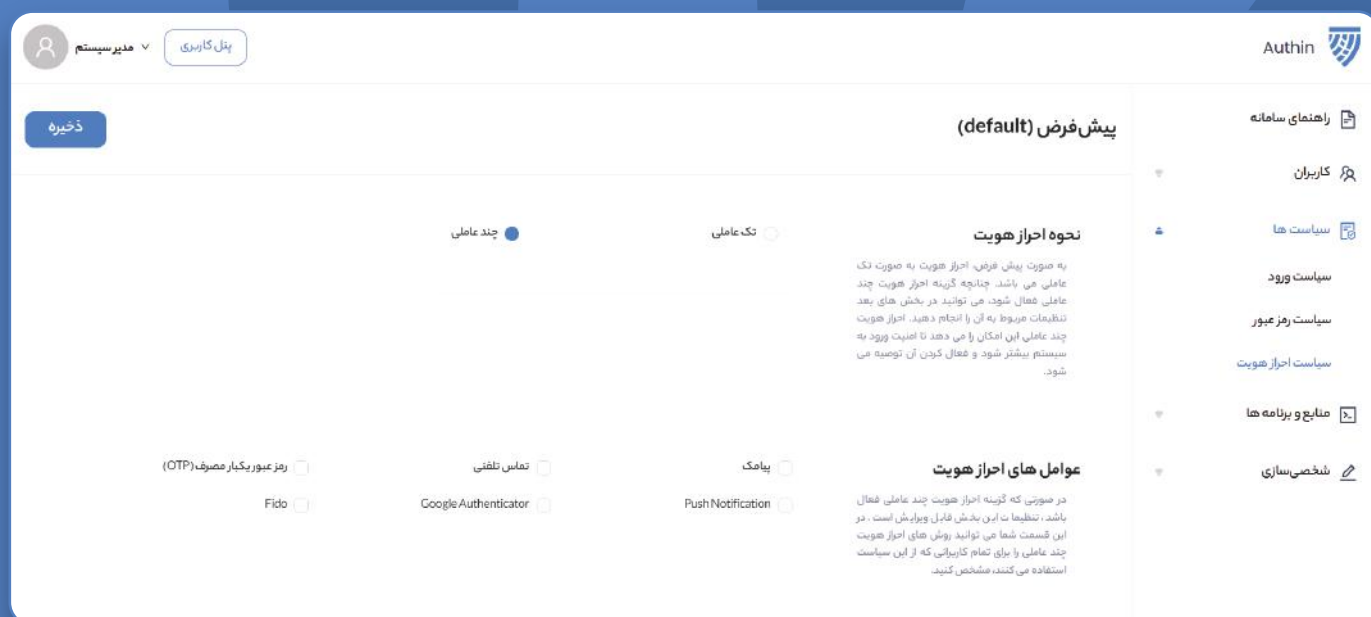
- جریان‌های نامحدود ثبت نام
- سازگاری با سرویس تأیید هویت
- تعریف جریان مبتنی بر نوع کاربر

اعطا و کنترل مجوز

- سازگاری با OAuth 2.0 و OIDC
- کنترل دسترسی به برنامه‌های کاربردی
- امکان کنترل دسترسی به محتوا و فرم‌های داخل سامانه‌ها مبتنی بر قوانین و سیاست‌های سازمان

احراز هویت چندعاملی (MFA)

- قابلیت تنظیم احراز هویت چندعاملی
- پشتیبانی از دستگاه‌های هویت سنج متفاوت
- فاکتورهای احراز هویت متفاوت به ازای هر سیاست
- پشتیبانی از توکن‌های TOTP و سخت افزاری
- اپلیکیشن موبایلی هویت سنج
- قابلیت تنظیم سیاست پیچیدگی رمز عبور
- استفاده از Email SMS، تماس تلفنی و push notification به عنوان فاکتور هویت سنجی





ویژگی‌های کلیدی

◀ مدیریت دسترسی به APIها

- ◀ سازگاری با OAuth2.0 و OIDC
- ◀ مدیریت دسترسی و مجوز مرکزی
- ◀ دامنه‌ها و ادعاهای قابل تنظیم دسترسی

◀ احراز هویت بر مبنای RADIUS

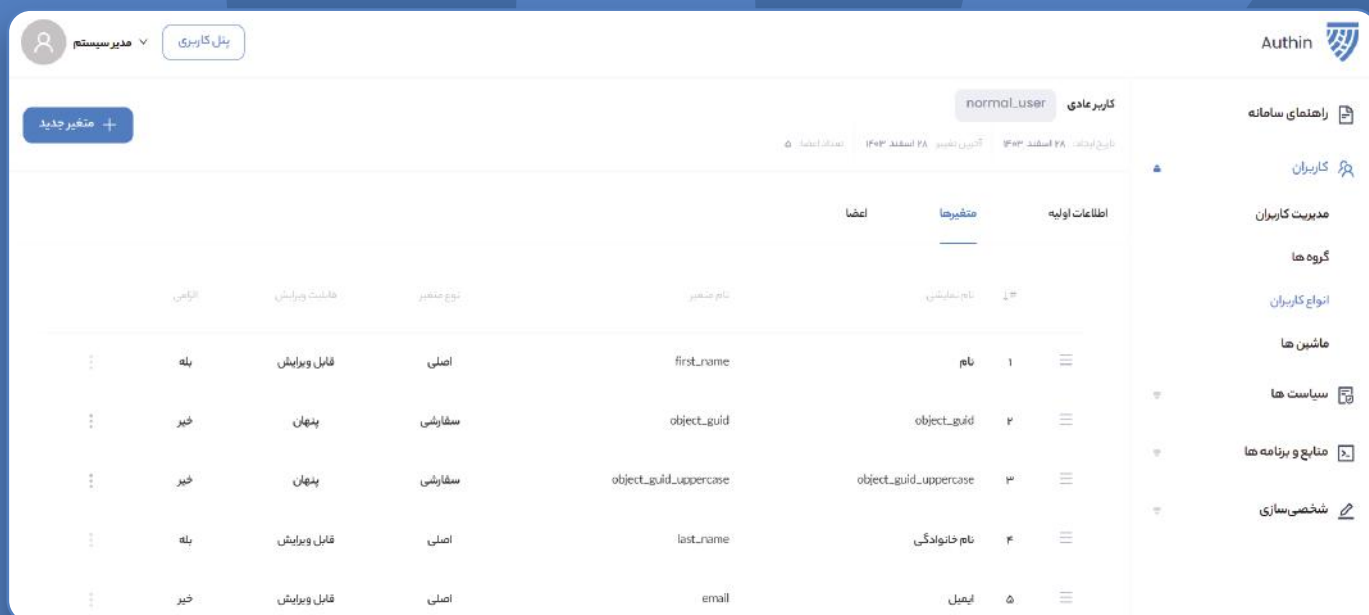
- ◀ احراز هویت VPN و WIFI
- ◀ یکپارچه سازی اندپوینت‌های RADIUS با SSO
- ◀ راه اندازی احراز هویت اندپوینت‌های RADIUS با MFA

◀ دایرکتوری مجازی

- ◀ ارائه پروتکل LDAP برای احراز هویت کاربران
- ◀ امکان دریافت خصیصه‌های کاربران به واسطه پروتکل LDAP
- ◀ نگاشت و تبدیل خصیصه‌ها
- ◀ پشتیبانی از مخازن هویتی سازمانی متفاوت

◀ پایش و گزارش دهی

- ◀ مدیریت لاگ و مانیتورینگ عملکرد کاربران
- ◀ گزارش رویدادها
- ◀ دارای ابزار مدیریت/کنسول، پشتیبانی و نگهداری و...
- ◀ داشبورد مدیریت





تهران، خیابان شهید بهشتی، بین خیابان
شهید علی اکبری و شهید مفتح، پلاک ۲۷۶
ساختمان مهام



۰۲۱۸۸۰۱۹۰۰۱



www.mohaymen.ir



info@mohaymen.ir



Mohaymen ICT Group

