سند پیاده سازی لاگین یکپارچه در سامانه گراف

انواع لاگین در سامانه گراف:

۱- لاگین کاربران بدون استفاده از کاربر شبکه

در این حالت از ویوی لاگین سامانه گراف استفاده می شود و احراز هویت کاربر بر اساس اطلاعات درج شده در مدیریت کاربران سامانه می باشد.

۲- لاگین با کاربر شبکه (Ldap) و با استفاده ازActiveDirectory

در این حالت نیز از ویوی لاگین سامانه گراف استفاده می شود و کاربر با فعال کردن گزینه "کاربر شبکه" مشخص می کند که باید عملیات احراز هویت بر اساس اطلاعات سرور اکتیو دایرکتوری شبکه آن سازمان انجام پذیرد. روال احراز هویت به این صورت است که هر کاربری که در دامنه شبکه سازمان تعریف شده باشد، با همان اکانت کاربری وارد ویندوز سیستم خود شده و در ورود به سامانه گراف با انتخاب گزینه "کاربر شبکه" مشخص می کند که اطلاعات کاربری باید با کاربر اکتیو دایرکتوری تطبیق داده شده و لاگین انجام شود. به این منظور باید گزینه LdapDomains در تنظیمات سیستم با لیست دامنه های سیستم لاگین Ldap مقداردهی شود. می بایست دامنه ها با کارکتر کاما (لاتین) از یک دیگر جدا شوند. مانند: tso.mashhad.ir,ftm.mashhad.ir

مثال: کاربری با نام کاربری GraphUser عضو شبکه داخلی شرکت گراف می باشد و در اکتیو دایرکتوری تعریف شده است. از طریق همین نام کاربری به ویندوز سیستم خود وارد می شود و در مرورگر سامانه گراف را باز کرده و با همین اطلاعات کاربری و باز فعال کردن گزینه "کاربر شبکه"، در سامانه گراف احراز هویت می شود.

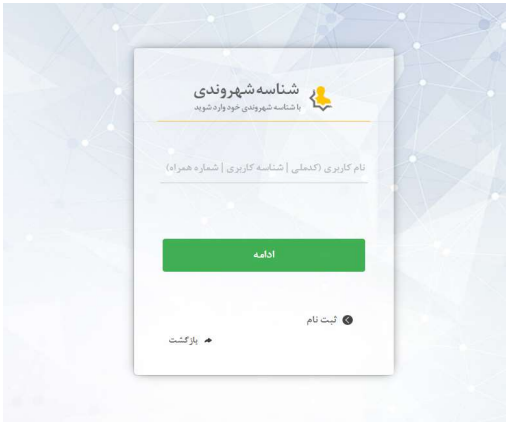
۳- لاگین یکپارچه شهروندی مشهد

برای استفاده و پیاده سازی این مورد بایستی به ازای هر کدام از سامانه ها، ابتدا آدرس UrlBack به شکل (websiteroot/login/externallogin) به سازمان فاوا ارسال شود و اطلاعات (AppClientID, AppSecretKey, AppUserName) دریافت شده و در تنظیمات سیستم اعمال شود.

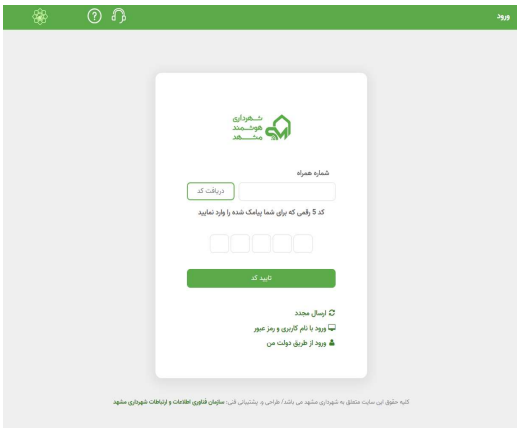
با ثبت این تنظیمات، ورود به سامانه، از طریق ویوی لاگین یکپارچه مشهد خواهد بود.اگر گزینه ISSSOV2 در تنظیمات سیستم، مقدار صفر داشته باشد، ویوی قدیمی لاگین مشهد (تصویر شماره۱) نمایش داده خواهد شد و اگر مقدار ۱ برای این گزینه تنظیم شده باشد، ویوی جدید لاگین مشهد (تصویر شماره ۲) به کاربر نمایش داده خواهد شد.

* ویوی قدیمی لاگین مشهد به زودی حذف شده و ویوی جدید جایگزین قطعی آن خواهد شد و در ادامه این تنظیمات کارایی نخواهد داشت.

تصویر شماره ۱



تصویر شماره ۲



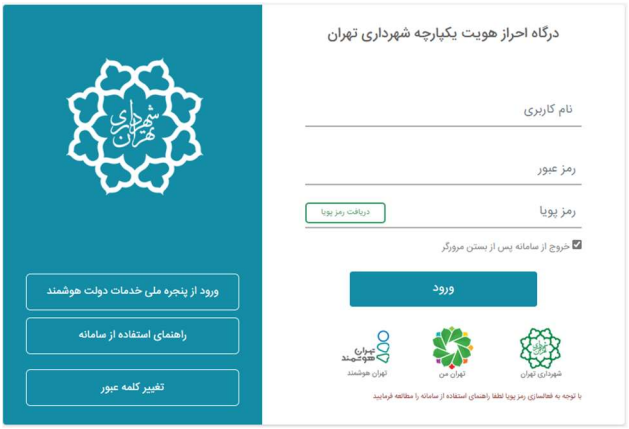
۴- لاگین یکپارچه شهروندی تهران

در این حالت اگر در webConfig کلید SSOTehranWebConfigSettingEnabled با true مقدار دهی شود، اولویت خواندن تنظیمات، از وب کانفیگ خواهد بود در غیر این صورت اطلاعات از تنظیمات سیستم خوانده می شود.

در هر کدام از دو حالت فوق مقادیر فیلدهای (AppClientID_tehran, AppSecretKey_tehran, Authority_URL_Tehran, Redirect_URL_Tehran) باید دریافت شده و در سیستم ثبت شوند.

با ثبت این تنظیمات، ورود به سامانه، از طریق ویوی لاگین یکپارچه تهران (تصویر شماره ۳) خواهد بود.

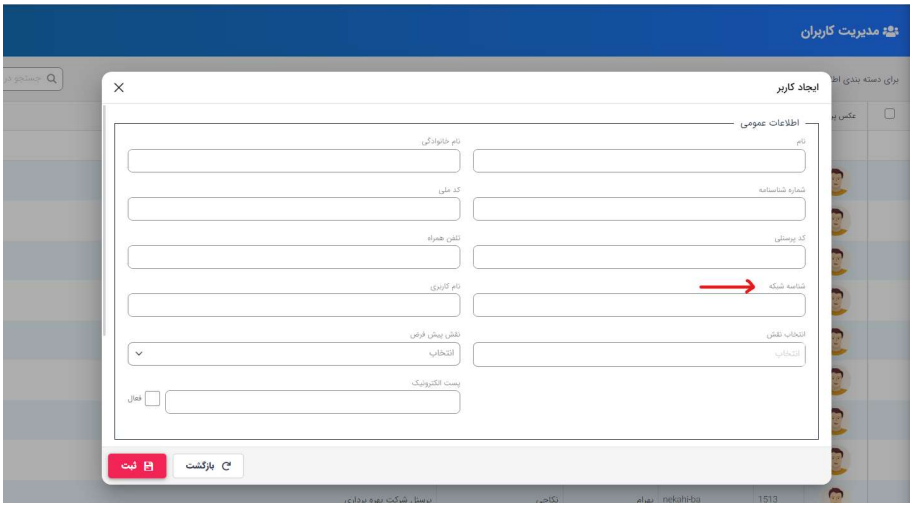
تصویر شماره ۳



روال لاگین سامانه از طریق سامانه های یکپارچه (مشهد و تهران)

بعد از لاگین فرد در سامانه یکپارچه، نام کاربری وی با شناسه کاربری تعریف شده در سامانه گراف تطبیق داده می شود (تصویر شماره ۴). چنانچه به ازای این نام کاربری، در مدیریت کاربران فردی تعریف شده باشد، کاربر با موفقیت به سامانه گراف وارد می شود. در این حالت اطلاعات کاربری فرد شامل (نام و نام خانوادگی و موبایل) نیز بروز رسانی می شود.

تصویر شماره ۴



دریافت اطلاعات لاگین می تواند از طریق یک منبع داده یا یک فرآیند در سیستم انجام شود. در هر دو حالت باید گزینه ExternalLoginConfig در تنظیمات سیستم مقداردهی شود.

چنانچه از منبع داده برای دریافت اطلاعات استفاده شده است بایستی شماره منبع داده را در قسمت Provider و بعنوان مقدار برای کلید ProviderId درج نموده و کلید های متناسب با اطلاعات دریافت شده از منبع داده، در ادامه اضافه شود.

نکته ای که وجود دارد این است که مقدار value که در این پارامترها با @@ مشخص شده است، در کوئری استرینگ برگردانده شده از سرویس لاگین خارجی جستجو می شود.

به عنوان مثال در کد زیر هنگامی که لاگین کاربر در سامانه خارجی انجام می شود و به سامانه گراف ریدایرکت می شود، برای فراخوانی منبع داده با پارامترهای username , refresh_token این ورودی ها از کوئری استرینگی که سرویس لاگین خارجی برای ما تامین کرده است، دریافت می شود. بعد از فراخوانی منبع داده، نتیجه باید شامل نام کاربری (UserName) ، نام (UserFirstName) ، نام خانوادگی (UserLastName) ، شماره تلفن همراه (UserCellPhone) ، کد ملی (NationalCode) باشد. متغیر دیگری هم در خروجی میتوان قرار داد به نام SelectedRole که به صورت اختیاری است و میتوان نقش های کاربر را تعیین کرد. اگر این پارامتر مقداردهی نشود به صورت پیش فرض این مورد از تنظیمات سیستم گزینه DefaultRole دریافت می شود.

```
{
    "Provider": {
        "ProviderId": 1021,
        "ProviderParameters": [
            {
                "Name": "username",
                "Value": "@@username"
            },
            {
                "Name": "refresh_token",
                "Value": "@@refresh_token"
            }
        ],
        "UserInfoMappingFromProviderFields": [
            {
                "Name": "UserName",
                "Value": "@username"
            },
            {
                "Name": "UserFirstName",
                "Value": "@firstname"
            },
            {
                "Name": "UserLastName",
                "Value": "@surname"
            },
            {
                "Name": "UserCellPhone",
                "Value": "@mobile"
            },
            {
                "Name": "NationalCode",
                "Value": "@nationalCode"
            },
            {
                "Name": "SelectedRole",
                "Value": "@SelectedRole"
            }
```

در صورتی که از فرآیند برای دریافت اطلاعات استفاده شده است باید قسمت Process مقداردهی شود. در این حالت شناسه گروه فرآیندی و شناسه فرآیند، برای کلید های ProcessGroup و Process باید ثبت شده و کلید های متناسب با اطلاعات دریافت شده از لاگین یکپارچه، در ادامه اضافه شود.

ورودی این روش هم مشابه روش استفاده از منبع داده است یعنی پارامترهای ورودی که در این قسمت مشخص شود در کوئری استرینگ برگشتی از سرویس لاگین خارجی جستجو می شود. خروجی فرآیند نیز مانند روش قبل باید شامل اطلاعات تکمیلی کاربر باشد.

* نمونه فایل BPMN دریافت اطلاعات لاگین، در مسیر جاری، قابل دانلود می باشد. در فایل نمونه یک ScriptTask به زبان #C پیاده سازی شده است که در آن برای دریافت مقادیر از متد آماده getConfig استفاده می شود.

در این متد ابتدا webConfig بررسی می شود. چنانچه به ازای کلیدهای احراز هویت مقداری تعیین نشده باشد، اطلاعات از تنظیمات سیستم دریافت خواهد شد.


```
"Process": {
    "ProcessGroup": 1047,
    "Process": 2255,
    "RoleID": 1,
    "UserID": 1,
    "RunType": 500002,
    "Variables": [
        {
            "Name": "username",
            "Value": "@@username"
        },
        {
            "Name": "refresh_token",
            "Value": "@@refresh_token"
        }
    ],
    "UserInfoMappingFromPocessFields": [
        {
            "Name": "UserName",
            "Value": "@username"
        },
        {
            "Name": "UserFirstName",
            "Value": "@firstname"
        },
        {
            "Name": "UserLastName",
            "Value": "@surname"
        },
        {
            "Name": "UserCellPhone",
            "Value": "@mobile"
        },
        {
            "Name": "SelectedRole",
            "Value": "@SelectedRole"
        },
        {
            "Name": "ManMailAccessToken",
            "Value": "@ManMailAccessToken"
```

ایجاد کاربر جدید در سامانه گراف به ازای کاربران لاگین یکپارچه

در صورتی که نیاز باشد در صورت عدم وجود کاربر به ازای شناسه کاربری، بصورت اتومات در سامانه گراف یک کاربر تعریف شود، بایستی گزینه CreateExternalLoginUser با مقدار یک تنظیم شود. در این حالت پسورد پیش فرض کاربر و نقش پیش فرض وی از تنظیمات DefaultPassword و DefaultRole خوانده می شود.

خطاهای ورود به سامانه گراف از طریق لاگین یکپارچه

شرایطی که کاربر نمی تواند در سامانه گراف لاگین کند، شامل موارد زیر می باشد:

۱- کاربری با این شناسه کاربری و کد ملی در سامانه گراف وجود ندارد و امکان ایجاد کاربر هم در سیستم تعریف نشده است. (CreateExternalLoginUser مقدار صفر دارد).

* اگر کد ملی از سمت سامانه یکپارچه با مقدار NULL ارسال شود، شرط کد ملی چک نخواهد شد.

۲- کاربر با این اطلاعات وجود دارد اما در سامانه گراف غیرفعال شده است.

۳- کاربر وجود ندارد و امکان ایجاد کاربر جدید در سیتم تعریف شده است اما با این نام کاربری در حال حاضر، فردی در سیستم تعریف شده است.

۴- کاربر وجود ندارد و امکان ایجاد کاربر جدید در سیتم تعریف شده است اما با این کد ملی در حال حاضر، فردی در سیستم تعریف شده است.

۵- کاربر وجود ندارد و امکان ایجاد کاربر جدید در سیتم تعریف شده است اما با این شماره موبایل در حال حاضر، فردی در سیستم تعریف شده است.

در تمامی این حالات سامانه به آدرس (websiteroot/Views/Login/CustomErrorLoginPage.cshtml) منتقل می شود.

* می توان بر اساس نیاز این فایل را شخصی سازی نمود اما باید در نظر داشت که در بروزرسانی های نگارش سامانه این فایل با فایل پیش فرض زیرساخت جایگزین خواهد شد.