راهنمای نصب و راه اندازی درگاه امضای دیجیتال (ISG)

شرکت پندار کوشک ایمن

واحد امنیت اطلاعات و زیرساخت کلید عمومی

نسخه:	**۱,۰**
تاریخ:	**شهریور ۱۴۰۰**
شناسه:	**PKI-ISG-Deployment-Guide**
طبقه‌بندی:	**عمومی**

تاریخچه گزارش

نسخه	تاریخ	تهیه‌کننده/گان	مرور کننده/گان	توضیحات
۱,۰	۱۴۰۰/۰۶/۲۲	کارشناس نصب و راه اندازی	مدیر فنی	آماده سازی سند

فهرست مطالب

۱. مقدمه

این مستند به صورت اختصاصی برای کارشناسان نصب و راه اندازی سامانه‌های تحت IIS تهیه شده است و قدر مسلم نیاز به دانش اولیه مرتبط با نصب و راه اندازی سامانه‌های تحت وب دارد.

در این مستند مراحل انتقال برنامه نصب به IIS و اعمال تنظیمات مربوط، به صوررت گام به گام توضیح داده شده است.

درگاه امضای دیجیتال شامل ۴ سامانه مستقل است:

۱. سامانه درگاه امضای دیجیتال (ISG UI)
۲. سرویس REST درگاه امضا (ISG REST)
۳. سرویس SOAP درگاه امضا (ISG SOAP)
۴. سامانه مدیریت درگاه امضا (ISG Admin)

نکته: سرویس‌های درگاه امضا می‌توانند به صورت سامانه‌ای مستقل یا به صورت یک برنامه کاربردی درون سامانه درگاه امضا نصب شوند. تصمیم گیری در این مورد وابسته به سیاست‌های سازمانی بهره بردار است.

۲. نیازمندی‌های نرم افزاری

<table>
<tr><th colspan="3">مشخصات نرم افزاری سرور</th></tr>
<tr><th colspan="2">OS</th><th>Web Server</th></tr>
<tr><td colspan="2">Windows Server 2016 or upper (64-bit)</td><td>Server Roles: IIS
Features:
• .NET Framework 4.6.1 (or higher features, depend on OS version)
• WCF Services
  ○ HTTP Activation
  ○ Named Pipe Activation
  ○ TCP Activation
  ○ TCP Port Sharing
• IIS Hostable Web Core</td></tr>
<tr><td colspan="3">مشخصات پایگاه داده</td></tr>
<tr><th>DB Engine</th><th>Features</th><th>User</th></tr>
<tr><td>MS SQL 2019</td><td>Instance Features:
• Database Engine Services
• Full-Text and Semantic Extractions for Search
Shared Features:
• Client Tools Connectivity
• SQL Client Conectivity SDK</td><td>A login to a database called ISG, that has:
Owned Schemas: db_owner
Membership: db_owner</td></tr>
</table>

سایر نرم افزارهای مورد نیاز	
Softwate	**Version**
SQL Server Management Studio	18 or Upper
Notepad++	Any version with Compare Plugins

۳. سایر نیازمندی‌ها

- **دسترسی‌های دایم اینترنت**

از مبدا	به مقصد	پورت‌ها	توضیحات
آی پی سرور ISG	۲۱۲,۱۶,۷۰,۲۱	۸۰ ۴۴۳	سرور مقصد متعلق به شرکت پندار بوده و ارایه دهنده خدمات اطلاع رسانی توسط تلفن همراه است.
از هر نشانی اینترنتی	آی پی سرور ISG	۸۰ ۴۴۳	جهت مراجعه امضا کنندگان به درگاه امضا
از هر نشانی اینترنتی یا نشانی شبکه داخلی	آی پی سرور ISG	۸۰۸۰ ۸۰۸۱	جهت مراجعه مدیر درگاه امضا
آی پی سرور ISG *	https://accounts.google.com/o/oauth2/auth		Google Auth
آی پی سرور ISG *	https://oauth2.googleapis.com/token		Google Ttoken
آی پی سرور ISG *	https://www.googleapis.com/oauth2/v1/certs		Google Auth Provider X509 Cert
آی پی سرور ISG *	https://www.googleapis.com/robot/v1/metadata/x509/firebase-adminsdk-zn8t9%40pendarnotification.iam.gserviceaccount.com		Google Client X509 Cert

* سرویس‌های گوگل به منظور پیام رسانی به تلفن‌های همراه اندروید استفاده می‌شود. در ارتباط با این سرویس‌ها ۳ رویکرد امکان پذیر است:

I. ایجاد حساب کاربری بهره بردار در مجموعه سرویس‌های Firebase برای بهره بردارانی که امکان دسترسی به این سرویس‌ها را دارند. مالک این حساب کاربری، بهره بردار خواهد بود.

II. استفاده از حساب کاربری شرکت پندار کوشک ایمن برای بهره بردارانی که امکان دسترسی به این سرویس‌ها را دارند اما مایل به داشتن حساب کاربری در Firebase نمی‌باشند. مالک این حساب کاربری، شرکت پندار است.

III. استفاده از سرویس ویژه شرکت پندار کوشک ایمن برای بهره بردارانی که در دسترسی به این سرویس‌ها با مانع مواجه هستند.

- **مشخصات binding سامانه‌ها**

درگاه امضای دیجیتال در sub-domain های مجزایی برای ارایه سرویس‌ها، رابط کاربری و دسترسی مدیر درگاه میزبانی می‌شود. به عنوان مثال:

isg.Your_Organization.**ir**
isgREST. Your_Organization.**ir** or **isgREST**.Your_Organization.**Local**
isgSOAP. Your_Organization.**ir** or **isgSOAP**.Your_Organization.**Local**
isgAdmin.Your_Organization.**ir** or **isgAdmin**.Your_Organization.**Local**

به صورت پیش فرض، سرویس‌های ISG در همان درگاه امضای دیجیتال نصب می‌شوند. در صورت تمایل بهره بردار به نصب هر یک از سرویس‌ها در سامانه‌ای مجزا، با ارایه مشخصات رکورد DNS آن سامانه، تفکیک سرویس‌ها امکان پذیر است.

لذا می‌بایست رکوردهای DNS مربوط به تمامی sub-domainها ایجاد و اعلام گردند. همچنین لازم است گواهینامه SSL هر سامانه بر روی سرور نصب و مشخصات آن ارایه شود.

- **مدیریت درگاه امضا**

دسترسی به سامانه مدیریت درگاه، مبتنی بر SSL دوطرفه می‌باشد. توصیه اکید می‌شود به منظور حفظ امنیت بیشتر، گواهینامه سمت کلاینت (ISG Admin) بر روی توکن سخت افزاری نگهداری شود. برای شناسایی کاربر مجاز (مدیر درگاه)، ارایه فایل cer (کلید عمومی) به همراه زنجیره این گواهینامه الزامی است.

۴. نصب گام به گام

۴,۱ پیش نیازهای نصب

با توجه به مطالب ذکر شده، پیش از آغاز فرآیند نصب، می‌بایست اطمینان حاصل کنید که نیازمندی‌های لازم فراهم شده‌اند:

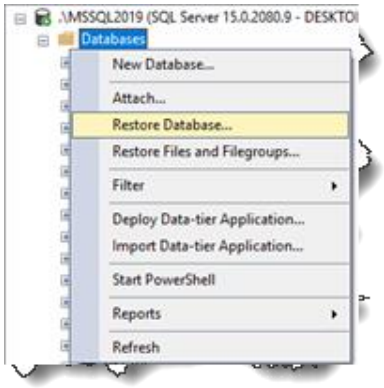
- SQL Server طبق مشخصات ذکر شده در بند ۲ نصب شده است.
- حساب کاربری لازم برای دسترسی به SQL Server ایجاد شده است.
- فایل backup پایگاه داده ISG دریافت شده است.
- IIS طبق مشخصات ذکر شده در بند ۲ نصب شده است.
- برنامه نصب هر یک از درگاه‌ها دریافت شده است.
- دسترسی‌های اینترنتی مطابق جدول بند ۳ وجود دارد.
- حساب کاربری Firebase ایجاد و فایل json آن دریافت شده است.
- رکوردهای DNS به تعداد سامانه‌های مورد نیاز ساخته شده است.
- گواهینامه مدیر درگاه صادر شده و فایل cer (کلید عمومی) آن به همراه زنجیره این گواهی دریافت شده است.
- زنجیره انواع گواهینامه‌هایی که امضا کنندگان استفاده خواهند کرد، موجود است. به عنوان مثال اگر امضا کنندگان می‌بایست از گواهینامه‌های سطوح برنزی تا پلاتینیم مرکز توسعه استفاده نمایند، می‌بایست زنجیره این نوع گواهینامه‌ها موجود باشد.

۴,۲ نصب پایگاه داده

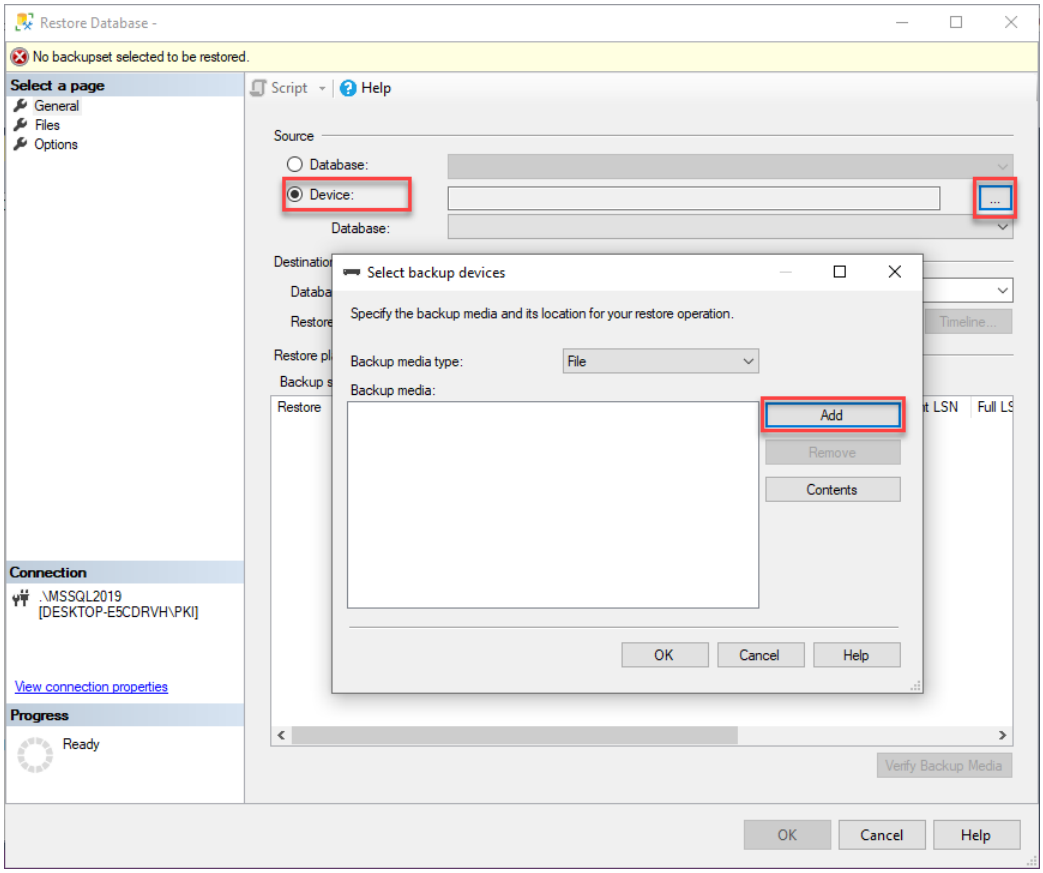
۱. فایل backup را به مسیر پیش فرض SQL Server منتقل کنید.

C:\Program Files\Microsoft SQL Server\<INSTANCE NAME>\MSSQL\Backup

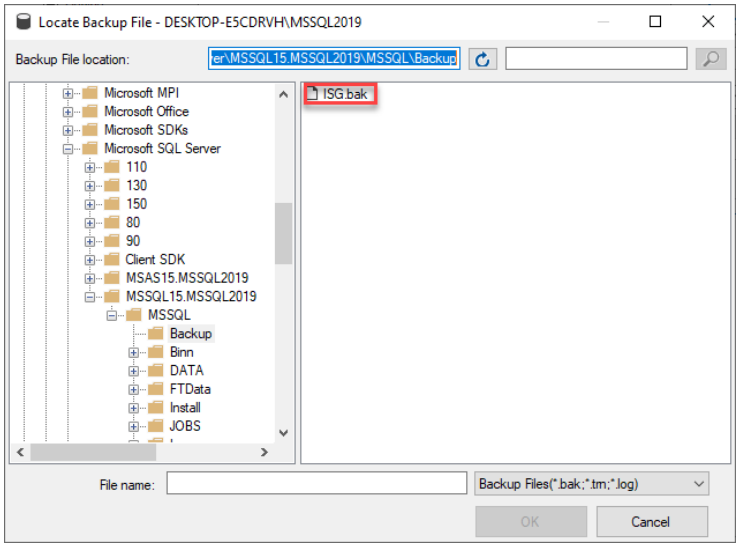
۲. در محیط Management Studio در بخش Databases، آیتم Restore Database را انتخاب کنید.



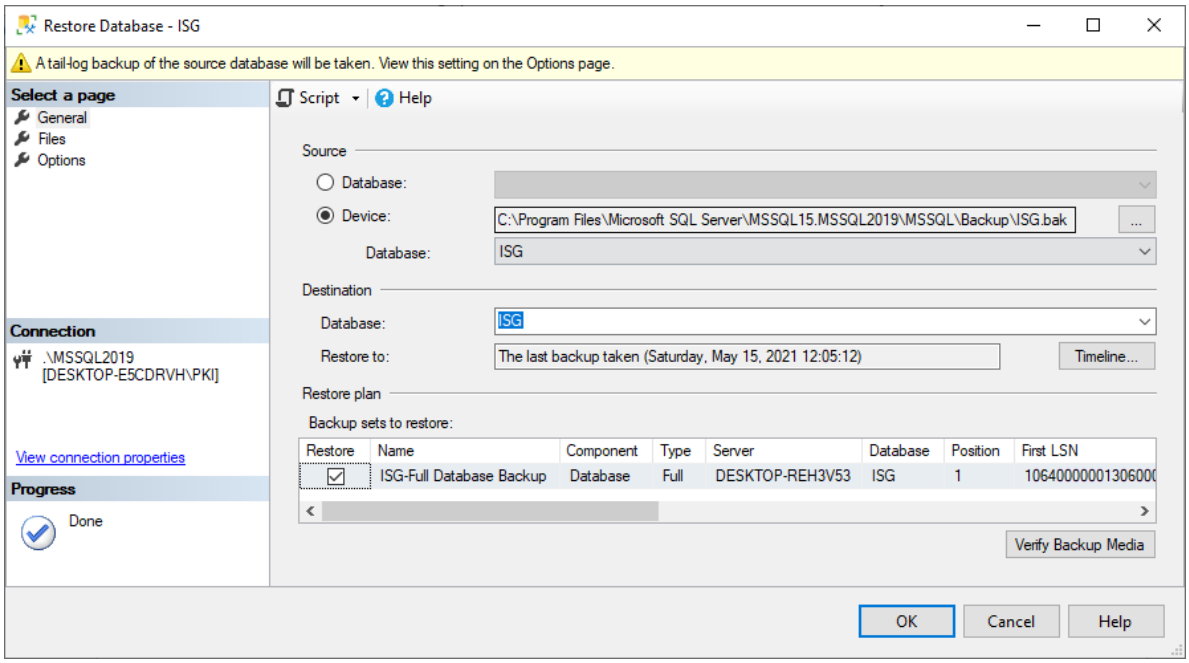
۳. در پنجره Restore Database گزینه Device را انتخاب کرده، روی دکمه مقابل (...) کلیک کنید تا پنجره Select backup devices را باز شود.



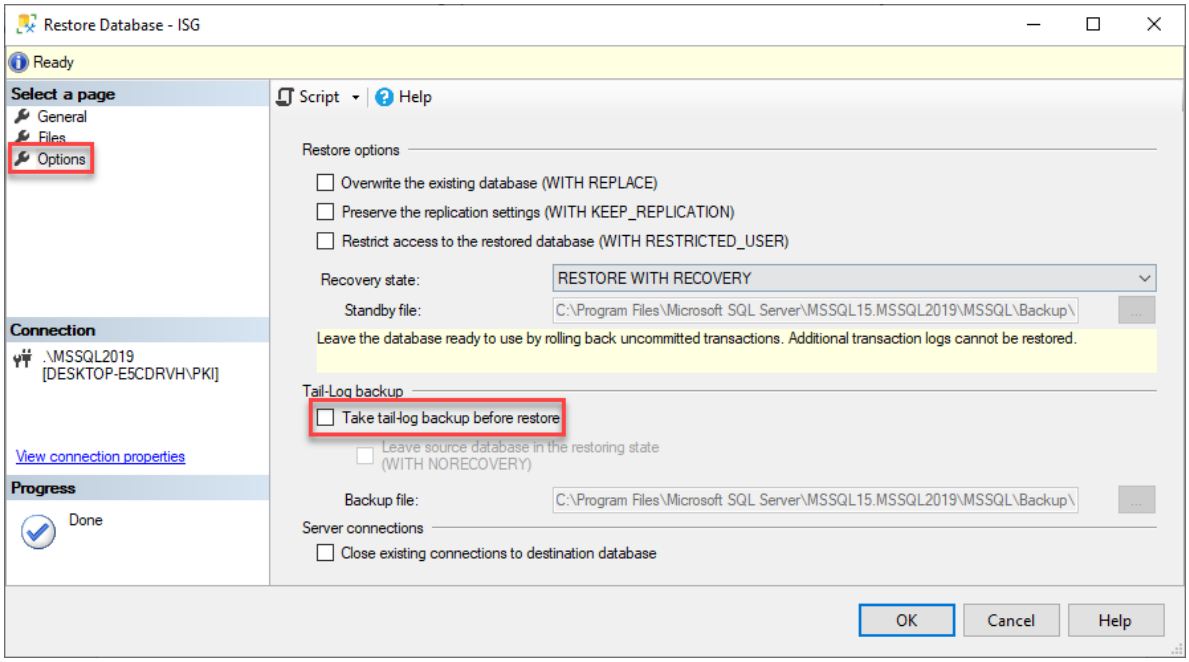
۴. روی دکمه Add در تصویر قبل کلیک کنید تا پنجره Locate Backup File گشوده شود. سپس فایل پشتیبان پایگاه داده ISG را انتخاب کنید.



۵. با کلیک روی دکمه OK در پنجره‌های گشوده شده به پنجره Restore Database باز گردید.



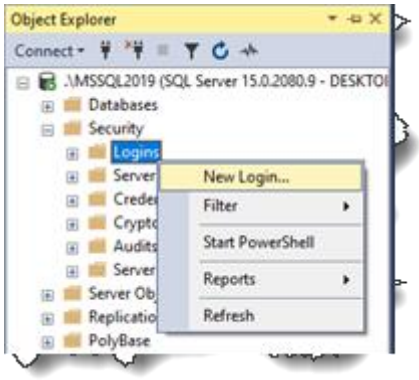
۶. در پانل سمت چپ پنجره فوق، گزینه Options را انتخاب نموده و تیک مربوط به Take tail-log backup before restore را بردارید.



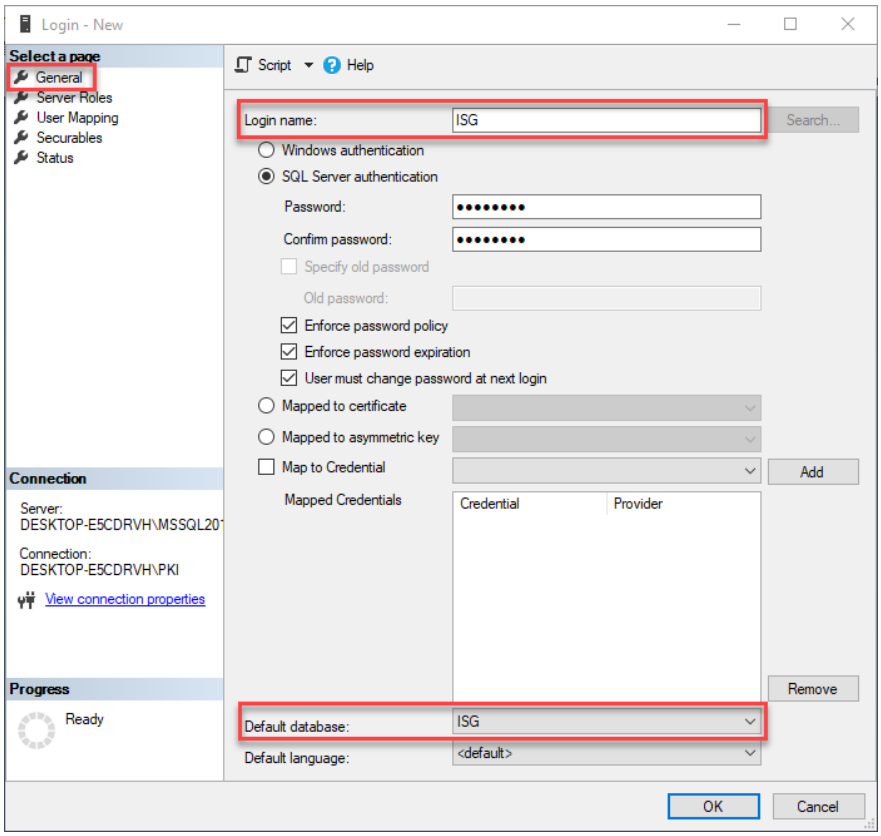
۷. بر روی دکمه OK کلیک کنید و تا پایان مرحله ساخت پایگاه داده از روی فایل backup و دریافت پیام success تامل نمایید.

۴,۳ تنظیمات دسترسی به پایگاه داده

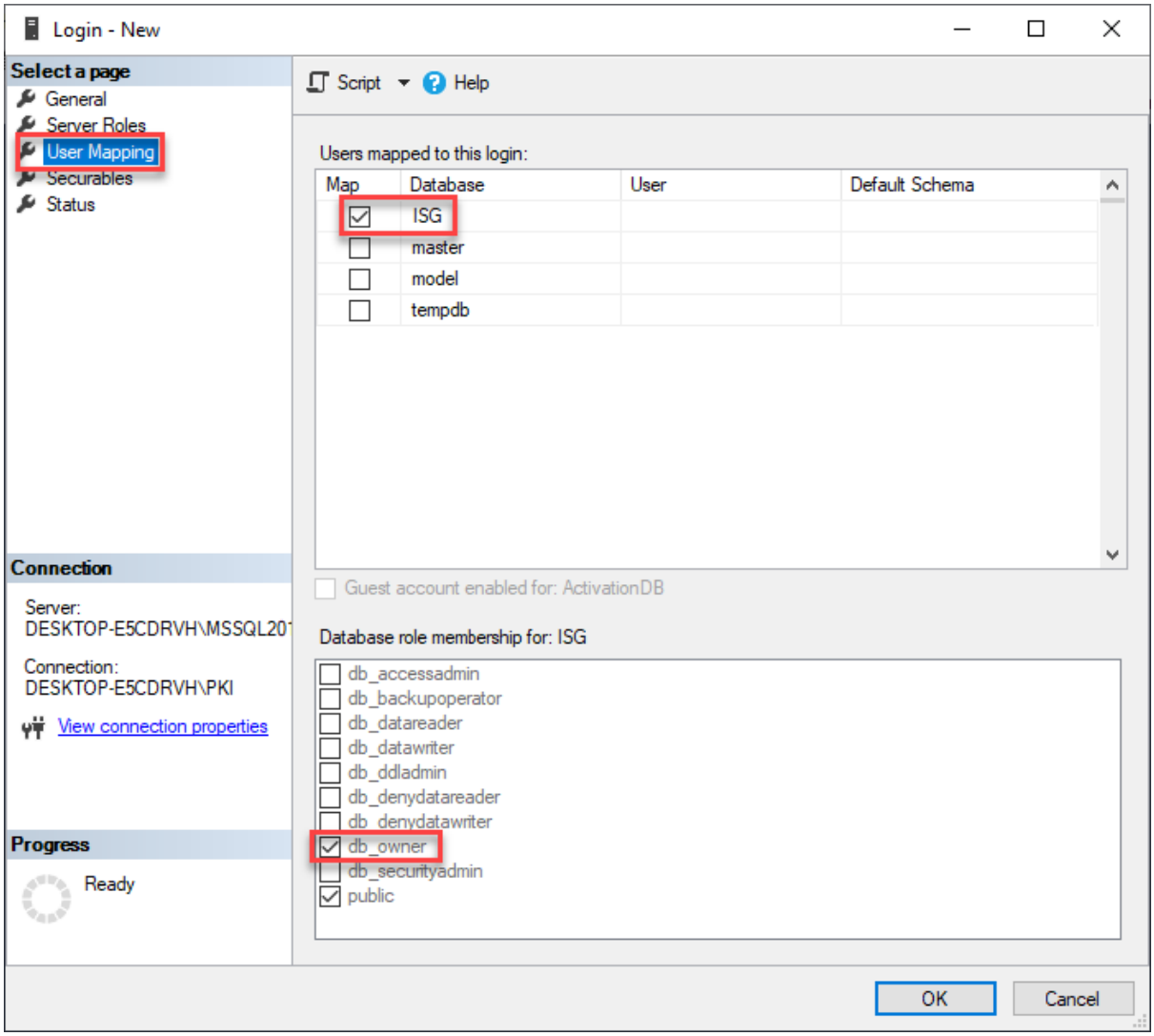
۱. اگر لاگین مربوط به دسترسی به پایگاه داده ISG وجود دارد، می‌توانید از این قسمت صرفنظر کنید. در غیر این صورت در پنجره Object Explorer قسمت مربوط به Security را بازکرده و برای ساخت یک لاگین جدید اقدام نمایید.



۲. یک login به نام ISG تعریف کرده، گذرواژه آن را تعیین کنید. سپس پایگاه داده پیش فرض را ISG قرار دهید.



۳. سپس به قسمت User Mapping رفته، در قسمت Users mapped to this login پایگاه داده ISG را انتخاب کنید و در قسمت Database role membership هر دو role مربوط به db_owner و public را برگزینید.

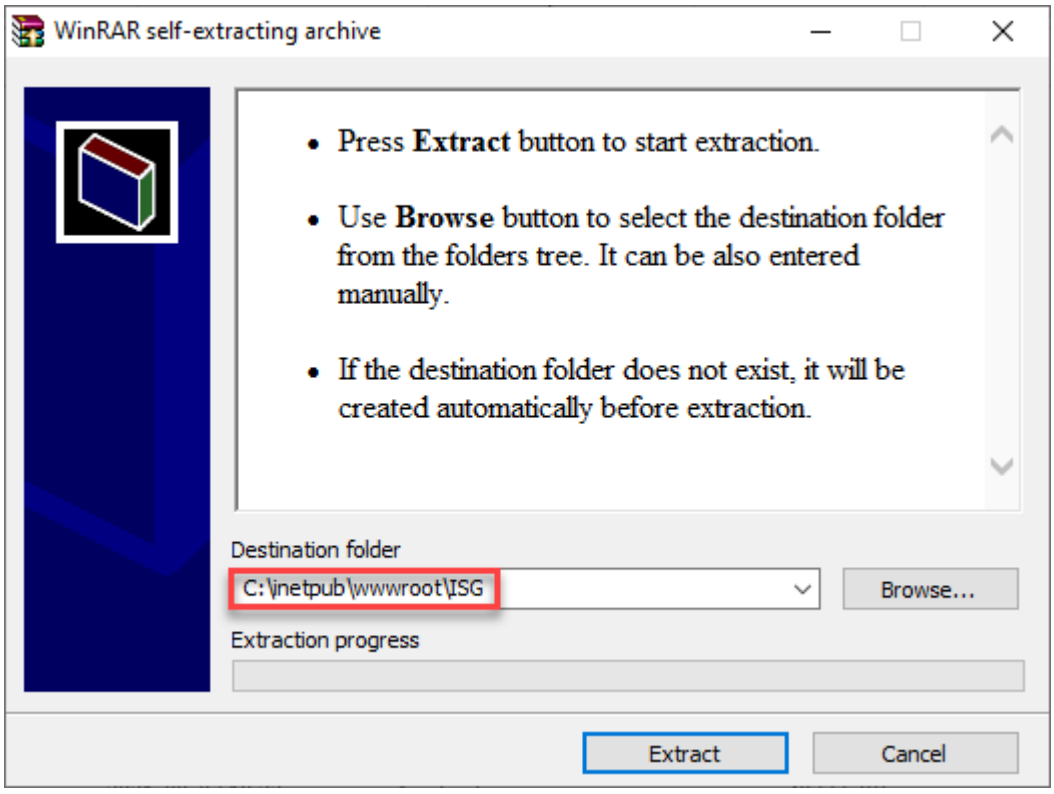


۴. روی دکمه OK کلیک کنید تا login مربوط به ISG ایجاد شود.

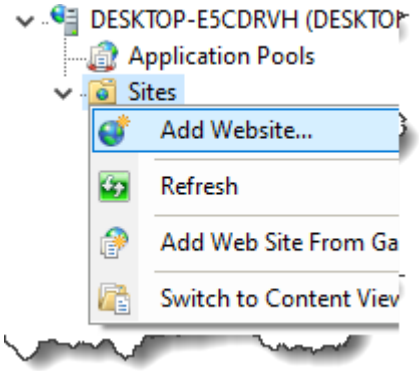
۴,۴ ایجاد سامانه جدید در IIS

در این بخش مراحل ایجاد یک سامانه در IIS توضیح داده می‌شود. از سامانه ISG به عنوان یک سامانه نمونه استفاده شده است اما مراحل شرح داده شده، برای ایجاد هر سامانه دیگری کاربرد دارد.

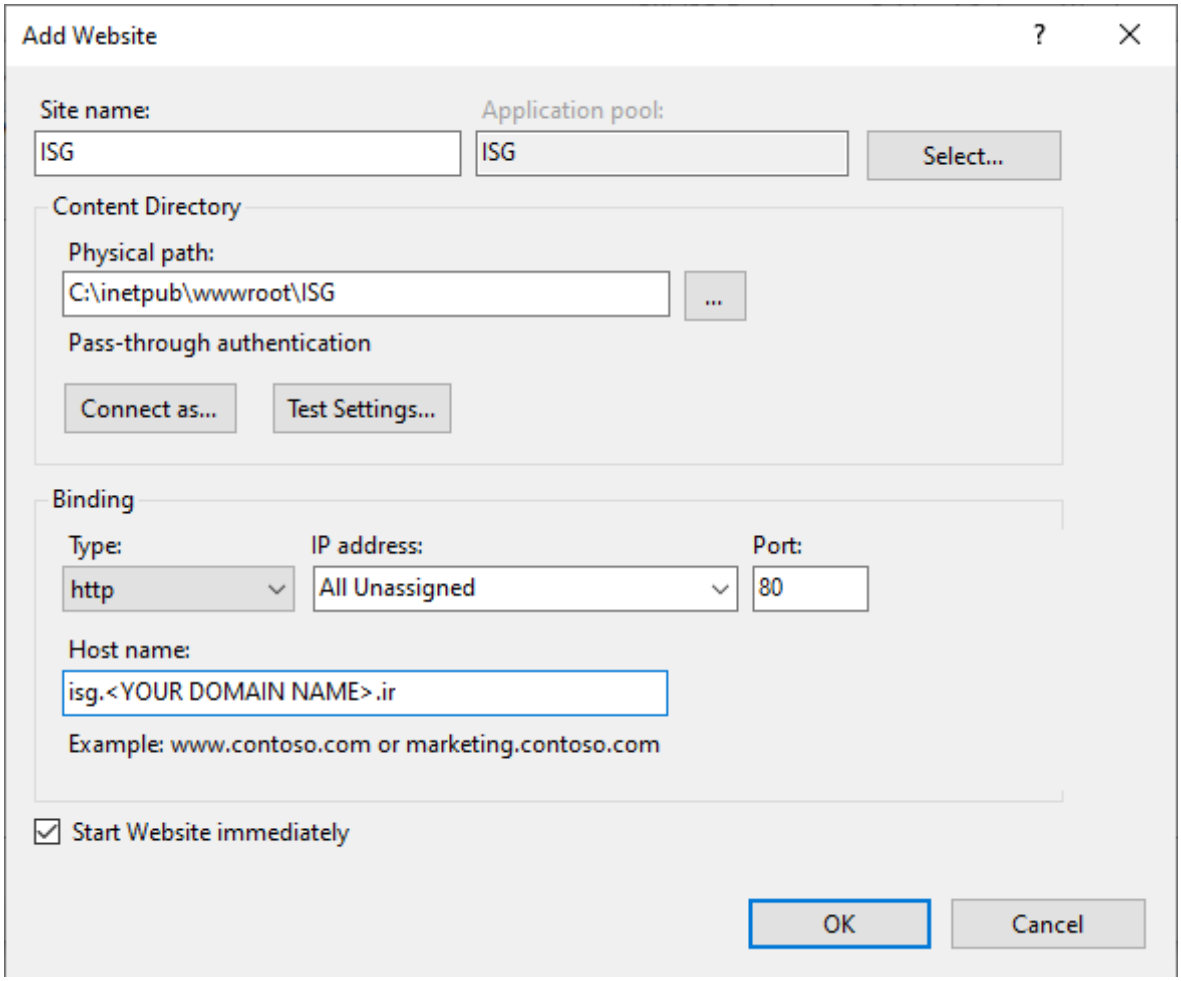
۱. پوشه‌ای برای دسترسی سامانه مورد نظر به نرم افزار مربوط ایجاد کنید. پیشنهاد می‌شود پوشه مذکور در این مسیر باشد:
C:\inetpub\wwwroot\ISG
سپس نرم افزار ISG را که در فایل ISG_UI_Vx.x.x.exe فشرده شده است، در مسیر پوشه ایجاد شده بازگشایی کنید.



۲. کنسول IIS Manager را باز کرده و در قسمت Sites اقدام به ایجاد سامانه جدید نمایید.



۳. در پنجره Add Website مشخصات سامانه را مطابق شکل زیر درج کنید.



در قسمت Host name به جای عبارت isg.<YOUR DOMAIN NAME>.ir مشخصات رکورد DNS سامانه خود را وارد نمایید.
سپس روی دکمه OK کلیک کنید تا سامانه جدید ایجاد و پنجره بسته شود.

۴. برای اعمال تنظیمات SSL باید از قبل گواهینامه SSL سایت مورد نظر بر روی سرور نصب شده باشد.

۴,۱. در بخش Sites در پانل سمت چپ، سایت ISG را انتخاب کنید.

۴,۲. در پانل سمت راست روی آیتم Bindings کلیک کنید تا پنجره Site Bindings گشوده شود.

۴,۳. در پنجره Site Bindings روی Add کلیک کنید تا پنجره Add Site Binding گشوده شود.

۴,۴. آیتم Type را https قرار دهید.

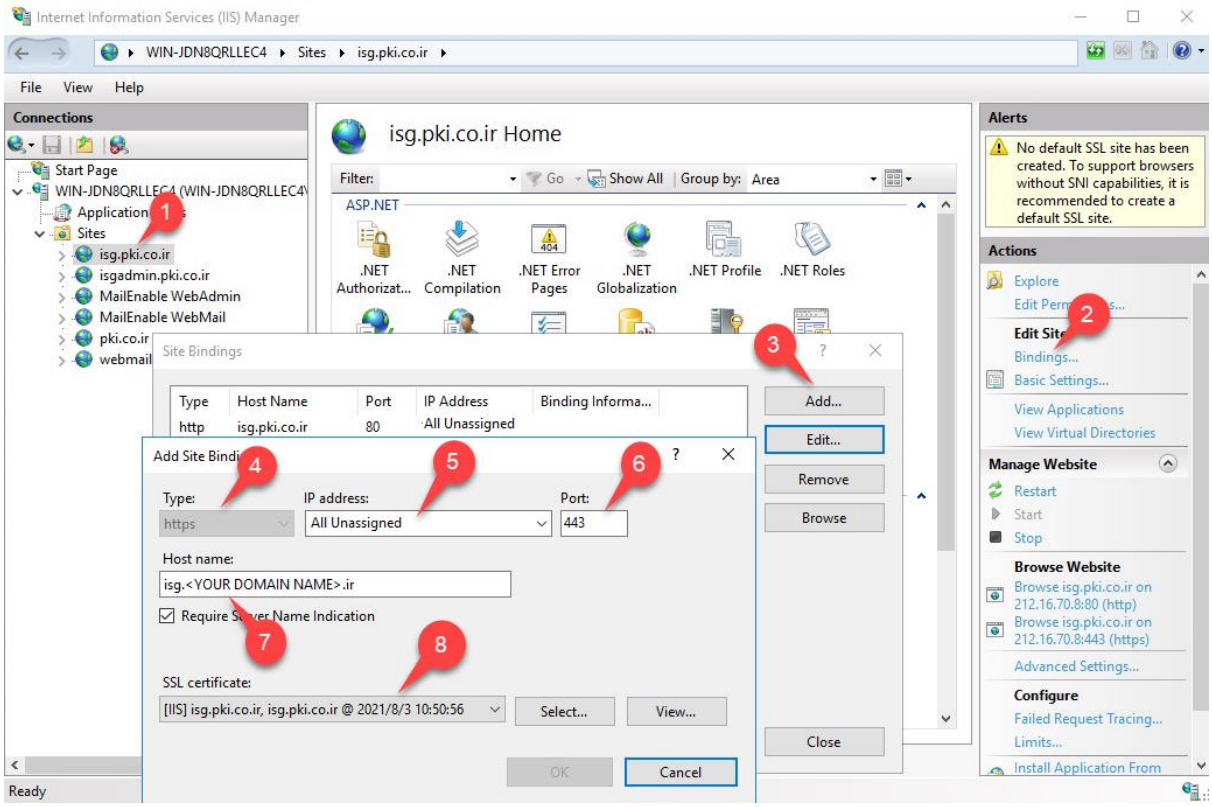
۴,۵. نشانی IP را مطابق IP سرور قرار داده یا به صورت پیش فرض در وضعیت All Unassigned رها کنید.

۴,۶. پورت پیش فرض SSL پورت 443 است. اگر پورت خاصی مد نظر شماست، شماره پورت را درج کنید.

۴,۷. در قسمت Host name به جای عبارت isg.<YOUR DOMAIN NAME>.ir مشخصات رکورد DNS سامانه خود را وارد نمایید.

۴,۸. گواهینامه SSL سامانه را از فهرست SSL Certificate انتخاب کنید.

۴,۹. روی دکمه OK پنجره‌های گشوده شده کلیک کنید تا بسته شوند.



۵. در این مرحله حساب کاربری‌ای که Applicatin Pool تحت آن اجرا می‌شود را مطابق شکل بعد تغییر دهید.

۵,۱. در پانل سمت چپ Application Pools را انتخاب کنید تا فهرست آن دیده شود.

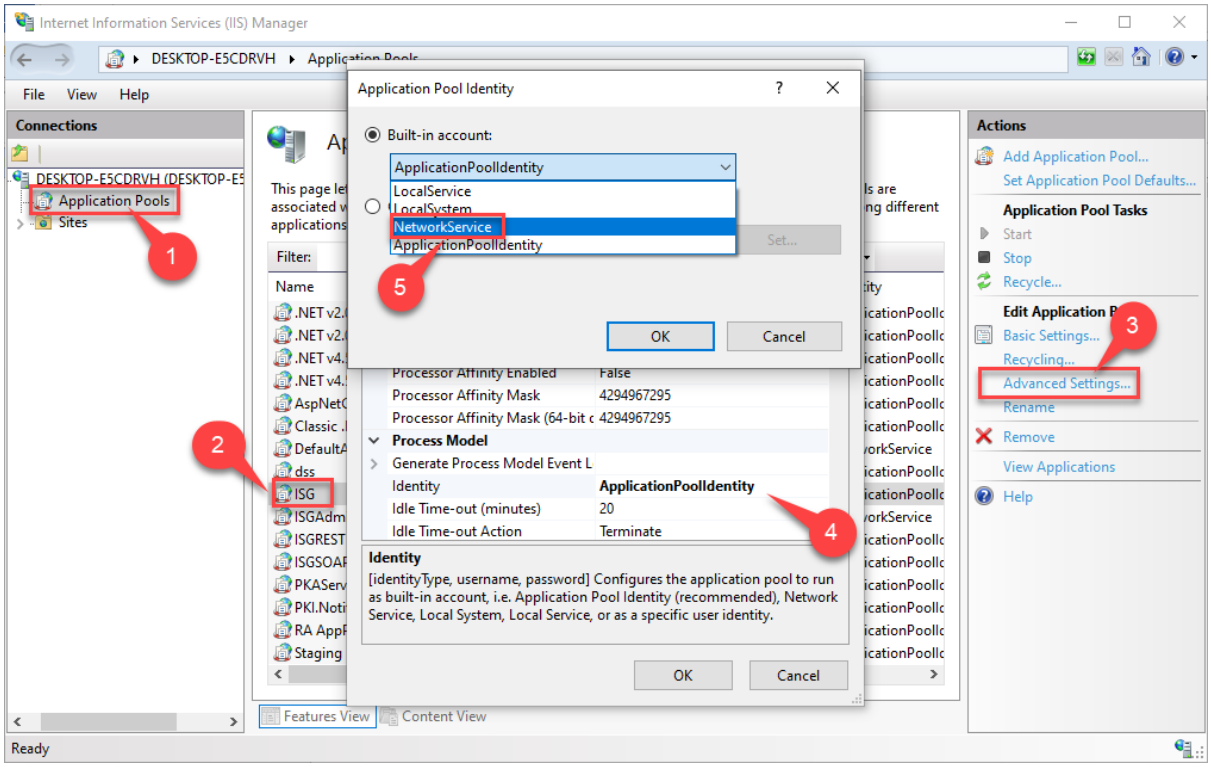
۵,۲. از فهرست ISG را انتخاب کنید.

۵,۳. سپس در پانل سمت راست روی Advanced Settings کلیک کنید.

۵,۴. در پنجره Advanced Settings از قسمت Process Model ویژگی Identity را تغییر دهید. مقدار این ویژگی به صورت پیش فرض ApplicationPoolIdentity است. روی آن کلیک کنید تا پنجره Application Pool Identity گشوده شود.

۵,۵. در قسمت Built-in account آیتم NetworkService را برگزینید.

۵,۶. سپس روی دکمه OK پنجره‌های گشوده شده کلیک کنید تا بسته شوند.



۶. اکنون به پوشه محل نصب نرم افزار ISG بروید و اگر داخل آن پوشه‌ای به نام logs وجود ندارد، آن را ایجاد کنید.

۶,۱. روی پوشه logs کلیک راست کنید و از منو Properties را انتخاب کنید.

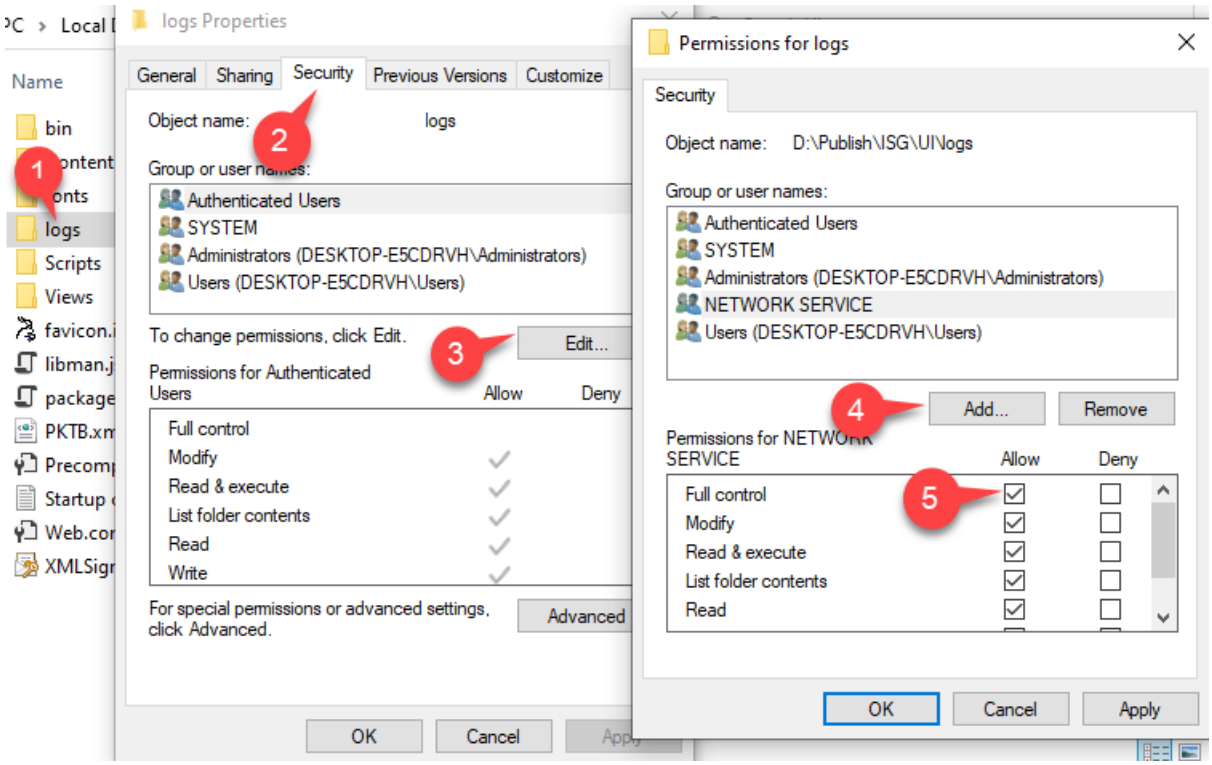
۶,۲. در پنجره logs Properties به برگه Security بروید.

۶,۳. روی دکمه Edit کلیک کنید تا پنجره Permissions for logs گشوده شود.

۶,۴. در پنجره Permissions for logs روی Add کلیک کنید و گروه NETWORK SERVICE را اضافه نمایید.

۶,۵. در بخش Permissions for NETWORK SERVICE آیتم Full Control را در ستون Allow تیک بزنید.

۶,۶. روی دکمه OK پنجره‌های گشوده شده کلیک کنید تا بسته شوند.



۴,۵ ایجاد برنامه کاربردی در یک سامانه

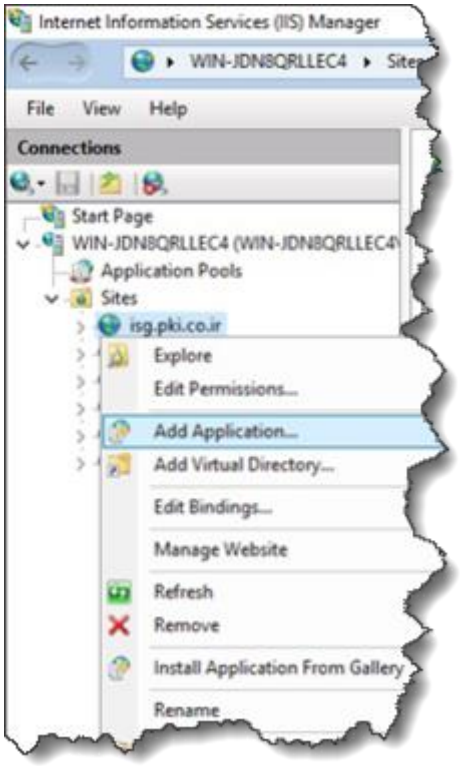
در این بخش مراحل ایجاد یک Application در IIS توضیح داده می‌شود. از برنامه ISG.REST به عنوان یک Application نمونه استفاده شده است اما مراحل شرح داده شده، برای ایجاد هر Application دیگری کاربرد دارد.

۱. پوشه‌ای برای دسترسی Application مورد نظر به نرم افزار مربوط ایجاد کنید. پیشنهاد می‌شود پوشه مذکور در این مسیر باشد:

C:\inetpub\wwwroot\ISG_REST

۲. سپس نرم افزار سرویس REST را که در فایل ISG_REST_Vx.x.x.exe فشرده شده است، در مسیر پوشه ایجاد شده بازگشایی کنید.

۳. روی سایت مورد نظر در IIS Manager کلیک راست کرده و Add Application را برگزینید.

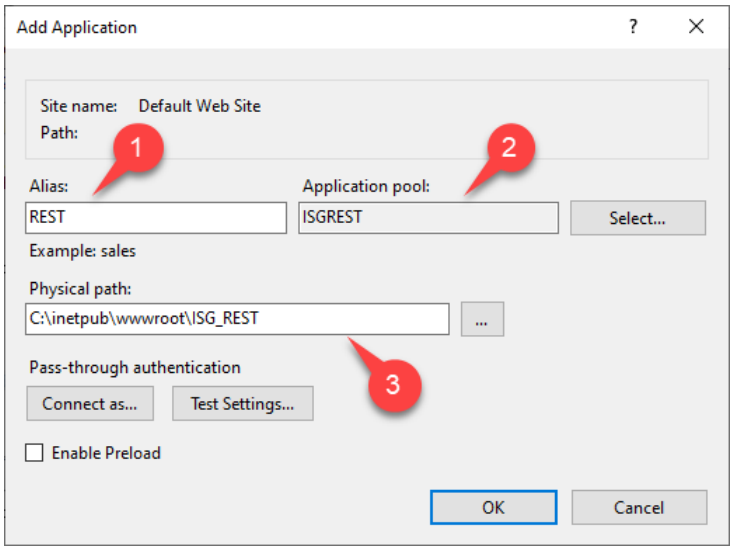


۴. اطلاعات لازم در پنجره Add Application را مطابق شکل بعد مشخص نمایید.

۴,۱. نام Alias را درج کنید.

۴,۲. با کلیک بر روی Select می‌توانید Application Pool مختص به Application مورد نظر را معرفی کرده یا از Application Pool سایت اصلی استفاده نمایید.

۴,۳. در قسمت Physical path مسیری که فایل‌های Application را قرار داده‌اید، معرفی نمایید.



۵. با کلیک بر روی OK پنجره بسته شده و Application مورد نظر شما ساخته می‌شود.

۴,۶ اعمال تنظیمات سامانه‌ها

پس از تکرار مراحل ایجاد Site و Application برای ایجاد تمامی سامانه‌های مورد نیاز، می‌بایست هر سامانه را تنظیم کنید.

۱. تنظیم سامانه ISG

- فایل web.config سامانه را در یک ویرایشگر متن باز نموده و به قسمت appSettings بروید. مقادیر پیش فرض مطابق شکل زیر است:

```
<appSettings>
    <add key="webpages:Version" value="3.0.0.0" />
    <add key="webpages:Enabled" value="false" />
    <add key="ClientValidationEnabled" value="true" />
    <add key="UnobtrusiveJavaScriptEnabled" value="true" />
    <add key="logToFile" value="true" />
    <add key="CRLAndOCSPValidation" value="false" />
    <add key="ServiceLogIsEnabled" value="true" />
</appSettings>
```

logToFile: در صورتی که مقدار logToFile برابر با true باشد، هنگام بروز خطا در برنامه، جزییات خطا در یک فایل متنی در پوشه logs بر اساس تاریخ رخداد خطا ذخیره خواهد شد.

CRLAndOCSPValidation: در صورت true بودن مقدار این تنظیم، گواهینامه‌های امضا کنندگان به صورت آنلاین بر اساس نشانی‌های مندرج در گواهینامه با صادر کننده گواهینامه چک خواهد شد. اگر مقدار این تنظیم false باشد، فقط ویژگی‌هایی از گواهینامه اعتبار سنجی می‌شوند که نیاز به دسترسی آنلاین ندارند. مانند تاریخ انقضا و ...

ServiceLogIsEnabled: در صورت true بودن این تنظیم، تمامی عملیات از جمله خطاهای رخداده در پایگاه داده ذخیره خواهند شد.

- در فایل web.config به قسمت connectionStrings بروید و آیتم ISGConnectionString را مطابق بند ۴,۳ (تنظیمات دسترسی به پایگاه داده) ویرایش کنید. نام ISGConnectionString را ویرایش نکنید.

۲. تنظیمات Site یا Application مربوط به سرویس REST

سرویس REST درگاه امضا را می‌توانید هم به صورت یک Site و هم یک Application نصب نمایید. متناسب با نوع نصب انتخاب شده، تنظیمات دسترسی به پایگاه داده متفاوت خواهد بود که در ادامه توضیح داده می‌شود.

- فایل web.config مربوط را در یک ویرایشگر متن باز نموده و به قسمت appSettings بروید. مقادیر پیش فرض مطابق شکل زیر است:

```
<appSettings>
    <add key="webpages:Version" value="3.0.0.0" />
    <add key="webpages:Enabled" value="false" />
    <add key="ClientValidationEnabled" value="true" />
    <add key="UnobtrusiveJavaScriptEnabled" value="true" />
    <add key="logToFile" value="true" />
    <add key="ServiceLogIsEnabled" value="true" />
    <add key="homePage" value="https://pki.co.ir/" />
    <add key="gateway" value="https://isg.pki.co.ir" />
    <add key="pendarNotificationServiceURL" value="http://ntf.pki.co.ir" />
    <add key="usePendarNotification" value="true" />
</appSettings>
```

logToFile: در صورتی که مقدار logToFile برابر با true باشد، هنگام بروز خطا در برنامه، جزییات خطا در یک فایل متنی در پوشه logs بر اساس تاریخ رخداد خطا ذخیره خواهد شد.

ServiceLogIsEnabled: در صورت true بودن این تنظیم، تمامی عملیات از جمله خطاهای رخداده در پایگاه داده ذخیره خواهند شد.

homePage: تنظیم مقدار این آیتم اختیاری می‌باشد. هر نشانی اینترنتی که در این تنظیم درج شود، به عنوان صفحه اصلی نمایش داده خواهد شد.

gateway: نشانی اینترنتی سامانه ISG است. این نشانی را بدون کاراکتر / در آخر آن درج کنید.

pendarNotificationServiceURL: نشانی سرویس ویژه اطلاع رسانی شرکت پندار کوشک ایمن است. تغییر در این نشانی، موجب بروز خطا، در هنگام ارسال پیام اطلاع رسانی خواهد شد. بدون هماهنگی با شرکت پندار این نشانی را تغییر ندهید.

usePendarNotification: اگر مقدار true تنظیم شود، پیام‌های اطلاع رسانی از طریق سرویس ویژه شرکت پندار ارسال شده و در غیر این صورت، پیام‌ها از طریق سرویس Firebase گوگل ارسال خواهند شد.

نکته: پیام‌های اطلاع رسانی فقط به تلفن همراه امضا کنندگانی ارسال خواهد شد که برنامه mKeyOne را روی گوشی هوشمند خود نصب و مراحل ثبت نام را طی کرده باشند.

- اگر سرویس REST را به صورت یک Site نصب کرده‌اید، در فایل web.config به قسمت connectionStrings بروید و آیتم ISGConnectionString را مطابق بند ۴,۳ (تنظیمات دسترسی به پایگاه داده) ویرایش کنید. در این حالت می‌بایست قسمت defaultConnectionFactory از بخش entityFramework را مطابق شکل زیر کامنت کرده یا حذف نمایید.

```
<add name="ISGConnectionString" connectionString="Integrated Security=SSPI;Initial Catalog=ISG;Data Source=(local)\MSSQL2019" providerName="System.Data.SqlClient" />
/connectionStrings>
entityFramework>
<!--<defaultConnectionFactory type="System.Data.Entity.Infrastructure.SqlConnectionFactory, EntityFramework">
<parameters>
<parameter value="ISGConnectionString" />
</parameters>
</defaultConnectionFactory>-->
<providers>
<provider invariantName="System.Data.SqlClient" type="System.Data.Entity.SqlServer.SqlProviderServices, EntityFramework.SqlServer" />
</providers>
```

- اگر سرویس REST را به صورت یک Application در سامانه ISG نصب کرده‌اید، می‌بایست تنظیمات مربوط به دسترسی به پایگاه داده را برعکس مورد قبل انجام دهید. یعنی بخش connectionStrings را کامنت نموده یا حذف کنید و قسمت defaultConnectionFactory را به بخش entityFramework بیافزایید.

```
<add name="ISGConnectionString" connectionString="Integrated Security=SSPI;Initial Catalog=ISG;Data Source=(local)\MSSQL2019" providerName="System.Data.SqlClient" />
/connectionStrings>-->
entityFramework>
<defaultConnectionFactory type="System.Data.Entity.Infrastructure.SqlConnectionFactory, EntityFramework">
<parameters>
<parameter value="ISGConnectionString" />
</parameters>
</defaultConnectionFactory>
<providers>
<provider invariantName="System.Data.SqlClient" type="System.Data.Entity.SqlServer.SqlProviderServices, EntityFramework.SqlServer" />
</providers>
```

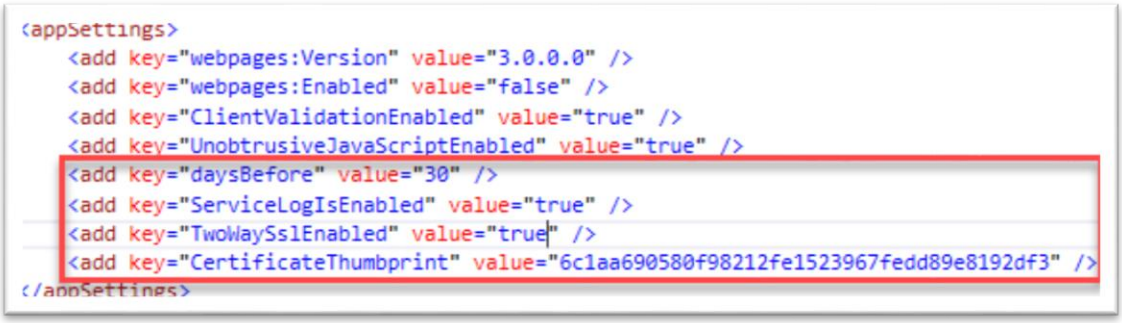
نکته: استفاده از کلید واژه ISGConnectionString در هر دو حالت از تنظیمات فوق الزامی است. به هیچ عنوان این کلید واژه را تغییر ندهید.

۳. تنظیمات Site یا Application مربوط به سرویس SOAP

سرویس SOAP درگاه امضا را می‌توانید مانند سرویس REST، هم به صورت یک Site و هم یک Application نصب نمایید. تمامی تنظیمات لازم برای سرویس SOAP همانند تنظیمات سرویس REST است. تنها تفاوت این است که در بخش appSettings به آیتم homePage نیازی نیست.

۴. تنظیم سامانه ISG Admin

- فایل web.config سامانه را در یک ویرایشگر متن باز نموده و به قسمت appSettings بروید. مقادیر پیش فرض مطابق شکل زیر است:



daysBefor: مقدار این تنظیم به صورت پیش فرض ۳۰ روز قرار داده شده است. با استفاده از این مقدار به مدیر درگاه پیام داده می‌شود که در صورت تمایل، لاگ‌های قدیمی‌تر سامانه از پایگاه داده حذف شوند.

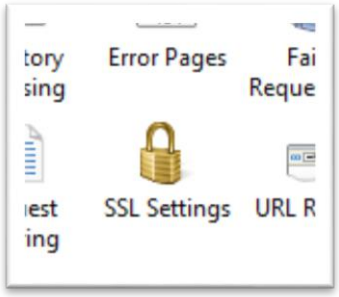
ServiceLogIsEnabled: در صورت true بودن این تنظیم، تمامی عملیات از جمله خطاهای رخداده در پایگاه داده ذخیره خواهند شد.

TwoWaySslEnabled: مقدار true، دسترسی به این سامانه از طریق کانال SSL را الزامی می‌نماید.

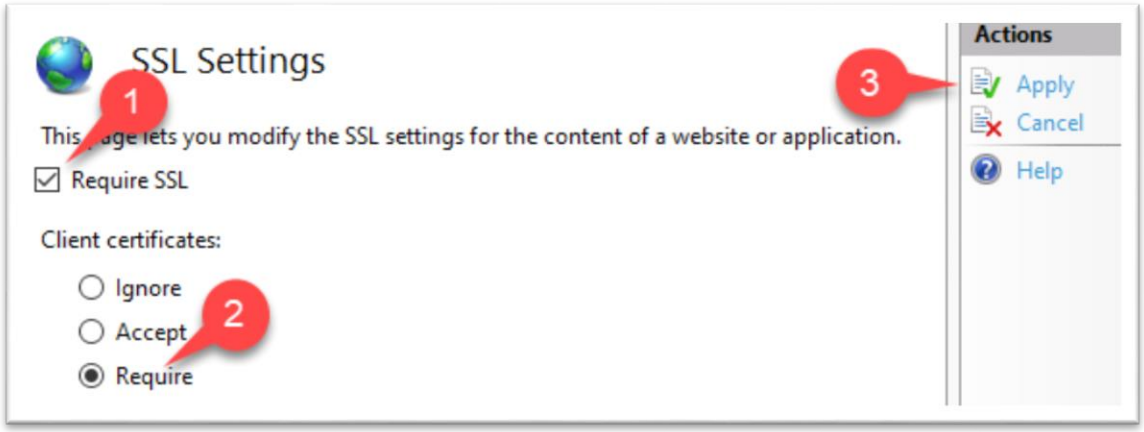
CertificateThumbprint: در صورتی که مقدار TwoWaySslEnabled برابر با true باشد، فقط گواهینامه‌ای برای سمت کلاینت پذیرفته خواهد شد که مقدار thumbprint آن برابر با مقدار درج شده در این تنظیم است. برای درج مقدار صحیح این تنظیم می‌بایست فایل cer (کلید عمومی) گواهینامه مدیر سایت را در اختیار داشته باشید.

- در فایل web.config به قسمت connectionStrings بروید و آیتم ISGConnectionString را مطابق بند ۴،۳ (تنظیمات دسترسی به پایگاه داده) ویرایش کنید. نام ISGConnectionString را ویرایش نکنید.

- در IIS Manager سایت ISGAdmin را انتخاب کرده و تنظیمات SSL را باز کنید.



- در بخش SSL Settings تنظیمات را مطابق شکل زیر اعمال کنید.



- ابتدا با تیک زدن Required SSL استفاده از کانال SSL را الزامی نمایید.
- سپس در بخش Client certificates آیتم Require را انتخاب کنید.
- در پایان با کلیک روی Apply، تغییرات را اعمال نمایید.

نکات عمومی:

- در صورت بهره برداری از امکان پیام رسانی به تلفن همراه، فایل json حساب کاربری Firebase را به سامانه‌های REST و SOAP در مسیری که فایل web.config وجود دارد، منتقل نمایید.
- زنجیره‌های انواع گواهینامه‌هایی که امضا کنندگان استفاده می‌نمایند، همچنین زنجیره گواهینامه مدیر درگاه امضا را در Certificate Store مربوط به Local Machine نصب کنید.
- پس از اعمال تنظیمات در هر Site یا Application، یکبار آن Site را Restart نموده و Application Pool مربوط را نیز Recycle کنید.