به نام خدا

**سند راهنما**

شهرسازی وب نسخه ؟؟؟

تحلیلگران آمارد

نسخه 1.7

مرداد ماه 1401**فهرست**

[1 شرح کلی 4](#_Toc137904157)

[2 راهنمای کاربر................................................................................................................4](#_Toc137904158)

[1.2 معرفی............................................................................................................. 4](#_Toc137904159)

[1.1.2 مشخصات هدف ارزیابی 4](#_Toc137904160)

[2.1.2 پیکربندی 5](#_Toc137904161)

[3.1.2 محیط عملیاتی هدف ارزیابی 5](#_Toc137904162)

[4.1.2 مدهای عملیات 5](#_Toc137904163)

[2.2 نقشهای کاربر.................................................................................................... 5](#_Toc137904164)

[1.2.2 انواع نقش‌ها 6](#_Toc137904165)

[2.2.2 شرح کارکردهای امنیتی 6](#_Toc137904166)

[3.2 شرح واسط‌ها .....................................................................................................8](#_Toc137904167)

[1.3.2 تولید داده ممیزی 8](#_Toc137904168)

[2.3.2 بازبینی داده‌های ممیزی 8](#_Toc137904169)

[3.3.2 انتخاب داده‌های ممیزی 9](#_Toc137904170)

[4.3.2 ذخیره رویدادهای ممیزی 9](#_Toc137904171)

[5.3.2 ازبین‌رفتن داده‌های ممیزی 10](#_Toc137904172)

[6.3.2 عملیات رمزنگاری 10](#_Toc137904173)

[7.3.2 خط‌مشی و عملیات مهار دسترسی 11](#_Toc137904174)

[8.3.2 ورود داده کاربری به محصول با مشخصه امنیتی 11](#_Toc137904175)

[9.3.2 خروج داده کاربری به محصول با مشخصه امنیتی 12](#_Toc137904176)

[10.3.2 صحت داده کاربری ذخیره‌شده 12](#_Toc137904177)

[11.3.2 مدیریت احراز هویت ناموفق 13](#_Toc137904178)

[12.3.2 تعریف مشخصات کاربر 13](#_Toc137904179)

[13.3.2 مدیریت کلمه عبور 14](#_Toc137904180)

[14.3.2 احراز هویت کاربر 14](#_Toc137904181)

[15.3.2 سازوکار احراز هویت چندگانه 15](#_Toc137904182)

[16.3.2 انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر 16](#_Toc137904183)

[17.3.2 مدیریت مشخصه‌های امنیتی 16](#_Toc137904184)

[18.3.2 حفظ وضعیت امن در زمان شکست و تحمل خطا 17](#_Toc137904185)

[19.3.2 محدودیت برروی چندین نشست هم‌زمان 17](#_Toc137904186)

[20.3.2 خاتمه دادن به نشست‌ها 18](#_Toc137904187)

[21.3.2 سوابق دسترسی به محصول 18](#_Toc137904188)

[22.3.2 سوابق دسترسی به محصول 19](#_Toc137904189)

[23.3.2 برقراری نشست 19](#_Toc137904190)

[4.2 رخدادها.........................................................................................................19](#_Toc137904191)

[5.2 اقدامات امنیتی.................................................................................................20](#_Toc137904192)

[6.2 پیشنهادات برای استفاده امن هدف ارزیابی 20](#_Toc137904193)

[3 فرآیند آمادهسازی هدف ارزیابی 21](#_Toc137904194)

[1.3 روال پذیرش..................................................................................................... 21](#_Toc137904195)

[2.3 روال نصب و راه اندازی 21](#_Toc137904196)

[1.2.3 فراهم سازی محیط عملیاتی 21](#_Toc137904197)

[2.2.3 نصب هدف ارزیابی 22](#_Toc137904198)

[3.2.3 راه اندازی هدف ارزیابی 42](#_Toc137904199)

# شرح کلی

سند راهنمای کاربری توسط تولیدکننده محصول برای تمامی نقش­های کاربری در نظر گرفته شده است. این سند در دو بخش راهنمای آماده سازی (آنچه که باید انجام گیرد تا محصول به پیکربندی مطرح شده در محیط عملیاتی سند هدف امنیتی منتقل گردد، این پیکربندی شرایطی است که محصول در آزمایشگاه ارزیابی شده است) و بخش راهنمای کاربر (آنچه که در طول عملکرد هدف ارزیابی در پیکربندی ارزیابی شده، صورت می­گیرد) ویژگی­هایی را شرح می­دهد.

ملزومات موجود در بخش راهنمای کاربر تضمین می‌کند، تمامی کاربران با توجه به نقش­ها و مجوزهای تعریف شده برای آنها، قادر به انجام عملیات بر روی هدف ارزیابی به صورت امن می­باشند. در بخش راهنمای کاربری مواردی چون کارکردهای امنیتی ارائه شده توسط توابع امنیتی هدف ارزیابی، دستورالعمل­ها و راهنماهای ارائه شده (شامل هشدارها)، اطلاعات مهم امنیتی و اقداماتی که برای کاربرد امن محصول لازم می­باشد، مطرح می­گردد.

روال آماده­سازی بیانگر روال­های برای تحویل محصول به صورت امن و نصب و راه اندازی آن به صورت نمونه ارزیابی شده می­باشد.

# راهنمای کاربر

## معرفی

### مشخصات هدف ارزیابی

|  |  |
| --- | --- |
| **نام محصول** | **شهرسازی آمارد** |
| **نسخه** | 1.1401.03.21 |
| **مدل** | - |
| **نام شرکت** | تحلیلگران آمارد |
| **نوع محصول** | تحت وب |
| **سطح ارزیابی** | EAL1 |
| **نام پروفایل حفاظتی** | **برنامه کاربردی تحت شبکه اسفند ماه 96** |

### پیکربندی

در این قسمت پیکربندی محصول که در آزمایشگاه مورد ارزیابی قرار گرفته، شرح داده می­شود. همچنین سخت افزار و نرم افزار پشتیبانی شده توسط محصول در قالب جدول زیر مشخص می­گردد.

|  |  |  |
| --- | --- | --- |
| **کامپوننت هدف ارزیابی** | **سخت افزار** | **نرم افزار** |
| **برنامه‌ی تحت وب** | - | Iis , windows server 2016 |
| **وبسرویس ارائه خدمات sms** | - | iis |
| **وبسرویس نقشه gis** | - | Iis,arcgis server |

### محیط عملیاتی هدف ارزیابی

|  |  |
| --- | --- |
| **کامپوننت محیط عملیاتی** | **هدف یا کاربرد آن برای هدف ارزیابی** |
| **windows server** | اجرای محیط عملیات |
| **Iis** | اجرای منابع داده |
| **Sql server** | نگهداری مقادیر داده |
| **arcgis** | نگهداری مقادیر نقشه و موقعیت مکانی |

### مدهای عملیات

محصول شامل مدهای نرمال و توسعه بوده که توسط سوپروایزر میتوان بین این مد‌ها تغییر اعمال نموده و از آن‌ها استفاده کرد.

## نقش­های کاربر

با توجه به پشتیبانی محصول از نقش­های مختلف، (همانند کاربران نهایی، ممیز، مدیر اجرایی، سرپرست، برنامه نویس و ...) لازم است در سند راهنما برای هریک از نقش­ها «کارکرد امنیتی مربوطه» و «واسط­های در دسترس آنها» مشخص گردد.

کاربران ممکن است نقش­های متفاوتی داشته باشند و با توجه به نقش در رابطه با محصول نیز وظایف و مسئولیت­های متفاوتی برعهده داشته باشند. به عنوان مثال، غالباٌ کاربران نهایی با سرویس‌ها و کارکرد‌های هدف ارزیابی در ارتباط بوده و سرپرستان با عملیاتی همچون پیکربندی، سرپرستی و نظارتی سروکار دارند. در این قسمت لازم است نقش­ها به صورت دسته بندی شده در نظر گرفته شوند.

### انواع نقش‌ها

* کاربر مدیر سیستم (admin): در سامانه تنها کاربر admin با دسترسی به منوی پنل کاربری تعریف شده است و از دسترسی سایر کاربران به این منو محافظت شده است و بنابراین هیچ یک از کاربران به جز کاربر admin در واسط کاربری سامانه امکان اعمال تغییرات در تنظیمات امنیتی سامانه را ندارند.
* کاربر توسعه‌گر (developer): این کاربر تمامی دسترسی‌های کاربر مدیر سیستم را داراست و بخاطر انجام پشتیبانی فنی استفاده‌می‌شود.
* نقش‌های پیش‌فرض: نقش‌های پیش‌فرض در این سامانه عبارت است از: شهرداری مرکزی، که با تعریف کاربر جدید به طور پیش فرض در این گروه قرار می‌گیرد. همچنین به صورت پیش فرض در سامانه هنگام تعریف کاربر باید یک سِمَت سازمانی برای کاربر انتخاب شود که مجوزی برای سمت تعریف نشده است و صرفا با انتخاب سمت، دسترسی و مجوز خاصی به کاربر داده نمی‌شود و تخصیص سمت برای کاربر فقط یک تعریف و عنوان در حال حاضر می‌باشد که جهت ایجاد کاربر و ورود کاربر به سامانه است و پس از تعریف کاربر می‌توان برایش مجوز و دسترسی‌های خاصی تعیین نمود و همچنین می‌توان با تعریف کاربر در یکی از گروه‌های شهرداری مرکزی، دسترسی‌های پیش فرضی به همه کاربران آن گروه اعطا نماید.
* همچنین می‌توان مامور بازدید، از افراد تعریف شده در سامانه، تعریف نمود.
* امکان تعریف کاربر مهندس و دیگر نقش‌ها نیز در سامانه وجود دارد. که این نقش‌ها مانند سمت سازمانی صرفا یک فیلد هستند و دسترسی خاصی برایشان درنظرگرفته‌نشده‌است.
* در باقی موارد، کاربر بر اساس دسترسی‌هایی که مدیر سیستم به او می‌دهد، می‌تواند به بخش‌های مختلف سامانه دسترسی داشته و تغییراتی را در داده‌های محصول انجام دهد.

### شرح کارکردهای امنیتی

کارکردهای امنیتی میان نقش‌های مختلف تفاوتی ندارند. درنتیجه تمامی مشروحات زیر برای تمامی نقش‌ها صادق هستند:

* + کاربر امکان مشاهده تلاش‌های موفق و ناموفق خود را بعد از ورود به سامانه دارد.
  + اگر تعداد تلاش‌های ناموفق از حد خاصی بیشتر شود، حساب کاربری کاربر غیرفعال می‌شود. تنها مدیر سیستم می‌تواند کاربری را فعال نماید. ویا اینکه بعد از مدت زمان تعیین‌شده در سیستم، حساب کاربر از حالت تعلیق درآمده و کاربر مجدد با واردکردن رمزعبور صحیح می‌تواند وارد حساب خود شود.
  + در صورتیکه به هر دلیلی در بار اول، اعتبارسنجی با مشکل روبرو شود، در دفعات بعدی (تا زمان ورود موفق) کاربر باید علاوه بر نام کاربری و کلمه عبور، کد Captcha نمایش داده شده را نیز وارد نماید.
  + بر اساس قوانینی که مدیریت سیستم فراهم می‌نماید، این امکان وجود دارد که نیاز باشد کاربر علاوه بر نام کاربری و کلمه عبور، کد اعتبارسنجی که به شماره تلفن همراه وی پیامک می‌شود را نیز در فرم ورود، وارد نماید.
  + کاربر با توجه به دسترسی‌هایی که برایش تعریف شده، امکان ورود به بخش‌های مختلف نرم افزار و همچنین انجام عملیات در آن بخش‌ها را دارد.
  + کاربر امکان تغییر کلمه عبور را دارد. کلمه عبور باید از یک تعداد کاراکتر بیشتر بوده و از قوانین حاکم بر کلمه عبور پیروی کند.
  + کلمه عبور می‌تواند هر ترکیبی از حروف کوچک و بزرگ، اعداد و کاراکترهای خاص (شامل \* و & و ^ و % و $ و # و @ و فاصله) باشد. این سیاست‌ها توسط کاربران مجازی که دسترسی ویرایش تنظیمات امنیتی سامانه را دارند، قابل ویرایش هستند.
  + درصورتی که تعداد نشست‌های همزمان کاربر از مقداری که توسط مدیر سیستم تنظیم می‌شود، عبور کند، به کاربر اجازه ورود داده‌نشده و کاربر اخطاری مرتبط دریافت می‌کند.
  + درصورت ورود کاربر جدید به یک حساب که نشست‌های فعال دیگری دارد، به کاربر آغازگر اولین نشست ازطریق پیامک اطلاع داده‌می‌شود.
  + امکان دسترسی به واسطه‌هایی چون: احراز هویت و خروج کاربر از سامانه
* **هشدارها**
  + با توجه به دسترسی‌هایی که برای کاربر تعریف شده، حفاظت از کلمه عبور از اهمیت ویژه‌ای برخوردار است.
  + کاربر باید پس از اتمام کار با سامانه، به نشست خود خاتمه دهد تا جلوی سوءاستفاده از کاربری وی گرفته شود.
  + کاربر سطح مدیر باید حد آستانه تعداد نشست‌های همزمان را دقیقا برحسب نیاز تنظیم‌کند. حد آستانه‌ی بالاتر منجر به همزمانی بیشتر نشست‌ها می‌شود و ممکن است بستر سوءاستفاده را فراهم آورد.

## شرح واسط‌ها

### تولید داده ممیزی

* روش فراخوانی: بوسیله کنش‌های هر کاربر قبل و/یا هنگام و/یا بعد از هر عمل در سامانه.
* پارامترهای قابل تنظیم:
  + شناسه کاربر: شناسه‌ی یکتایی که هر کاربر داراست.
  + نام کاربر: نام و شهرت کاربر که در سامانه ثبت است.
  + نوع عمل: نوع کلی عمل مانند مشاهده، ویرایش، ایجاد، بارگیری و ...
  + نام بخش: بخشی از سامانه که کاربر عمل خود را صورت‌داده مانند بخش مدیریت کاربران.
  + شرح عملیات: شرح دقیق عملی که رخ‌داده با جزئی‌ترین اطلاعات.
  + تاریخ و ساعت: تاریخ و زمان عملی که کاربر انجام‌داده‌است.
  + نشانی IP: شناسه‌ی IP دستگاه کاربر که درون شبکه‌ قراردارد.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + نتیجه: عدم‌توانایی ثبت رویداد بدلیل خالی‌نبودن فضای ذخیره‌سازی اطلاعات ممیزی در پایگاه داده
  + نتیجه: ثبت موفق رویداد

### بازبینی داده‌های ممیزی

* روش فراخوانی: کاربر مجاز ازطرق زیر دسترسی به داده‌های ممیزی دارد:
  + منو > رویدادهای ممیزی > لاگین‌های کاربران
  + منو > امکانات > گزارش کاربران سیستم
  + منو > امکانات > بررسی پیام‌های سیستم
  + منو > امکانات > بررسی پیام‌های IIS
* پارامترهای قابل تنظیم:
  + ‌شناسه کاربر: برای تشخیص اینکه آیا این کاربر اجازه دسترسی به بخش مشاهده اطلاعات ممیزی دارد یا خیر.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + پیام خطا: عدم امکان خواندن اطلاعات ممیزی برای کاربران غیرمجاز

### انتخاب داده‌های ممیزی

* روش فراخوانی: کاربر مجاز (دارای دسترسی "تعاریف > فیلتر رویدادهای ممیزی" می‌تواند بین مواردی که در مسیر "تعاریف > فیلتر رویدادهای ممیزی" وجود دارد، انتخاب نماید که کدام رویداد ممیزی ثبت شود.
* پارامترهای قابل تنظیم:
  + شناسه کاربر: برای بررسی دسترسی‌های کاربر
  + الزام ثبت رویدادهای فعالیت کاربران: درصورت انتخاب شدن رویدادهای فعالیت کاربران ثبت می‌شوند.
  + الزام ثبت رویدادهای ورود/خروج کاربران: درصورت انتخاب شدن رویدادهای ورود/خروج کاربران ثبت می‌شوند.
  + الزام ثبت رویدادهای پیام‌های سیستم: درصورت انتخاب شدن رویدادهای پیام‌های سیستم ثبت می‌شوند.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + پیام خطا: نمایش خطا درصورت عدم دسترسی کاربر به بخش مذکور
  + نتیجه موفق: ویرایش سیاست‌های فیلتر رویدادهای ممیزی

### ذخیره رویدادهای ممیزی

* روش فراخوانی: بوسیله کنش‌های هر کاربر قبل و/یا هنگام و/یا بعد از هر عمل در سامانه.
* پارامترهای قابل تنظیم:
  + شناسه کاربر: برای تشخیص اینکه آیا این کاربر اجازه دسترسی به بخش مشاهده اطلاعات ممیزی دارد یا خیر.
  + رکورد ممیزی: بمنظور بازدرهم‌سازی رکورد که درنهایت این مقدار درهم جدید با مقدار درهم موجود در پایگاه‌داده سنجیده‌شده و نتیجه این سنجش به کاربر نمایش‌داده‌می‌شود.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + نتیجه موفق: سنجش اعتبارسنجی به کاربر نمایش‌داده می‌شود.
  + نتیجه ناموفق: عدم‌توانایی ثبت رویداد بدلیل خالی‌نبودن فضای ذخیره‌سازی اطلاعات ممیزی در پایگاه داده
  + پیام خطا: درصورت عدم دسترسی کاربر به بخش مذکور

### ازبین‌رفتن داده‌های ممیزی

* روش فراخوانی: درصورت تجاوز دنباله‌ی ممیزی از حد آستانه هشدار ویا از حد آستانه بحران.
* پارامترهای قابل تنظیم:
  + شماره تماس کاربر: شماره تماسی که برای فرستادن پیامک اطلاع‌رسانی استفاده می‌شود.
  + نام جدول ممیزی پُرشده: جدول ممیزی پرشده که قصد خالی‌سازی فضای آنرا داریم.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + نتیجه ناموفق: درصورت ثبت‌نبودن شماره تماس کاربر مربوطه، یک رکورد ممیزی با همین مضمون ثبت می‌گردد.
  + نتیجه ناموفق: درصورت عدم توانایی فرستادن اعلان پیامکی، یک رکورد ممیزی با همین مضمون ثبت می‌گردد.
  + نتیجه موفق: درصورت موفق‌آمیز بودن، فضای خالی برای ثبت رکوردهای ممیزی جدید فراهم می‌گردد.

### عملیات رمزنگاری

* روش فراخوانی:
  + هنگام استفاده از الگوریتم رمزنگاری برای صحت‌سنجی داده‌های احراز هویت، داده‌های ممیزی و داده‌های رکورد
  + هنگام استفاده از الگوریتم رمزنگاری برای تولید داده‌های درهم‌شده (Hash)
* پارامترهای قابل تنظیم:
  + نوع الگوریتم: نوع الگوریتم درهم‌ساز را مشخص می‌کند.
  + متن ساده: حاوی یک رکورد ممیزی ویا یک رمز عبور کاربر است که قرار است روی آن درهم‌سازی صورت گیرد.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + نتیجه موفق: یک مقدار درهم‌شده خواهد بود.

### خط‌مشی و عملیات مهار دسترسی

* روش فراخوانی: به‌ازای هر کنش کاربر در سامانه، دسترسی‌های او به موجودیت‌های فعال ویا غیرفعال درخواستی کنترل و مهار می‌شود. کاربر مجاز سطح مدیر توانایی افزودن یا کاستن دسترسی‌های کاربران دیگر را ازطرق زیر دارا هستند:
  + منو > مدیریت کاربران > سطح دسترسی
  + منو > مدیریت کاربران > دسترسی و گروه‌بندی کاربران
* پارامترهای قابل تنظیم:
  + شناسه کاربر: برای شناسایی اینکه آیا کاربر به بخش درخواستی خود دسترسی دارد یا خیر استفاده می‌شود.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + پیام خطا: درصورتی که کاربر به بخش درخواستی خود دسترسی نداشته باشد.
  + نتیجه موفق: درصورتی که کاربر بخش مذکور دسترسی داشته باشد، عملیات صورت می‌گیرد.
  + نتیجه: در هر دو حالت قبل یک رویداد ممیزی مرتبط ثبت می‌شود.
  + نتیجه: درصورتی تجاوز از حد آستانه تعداد نشست‌های هم‌زمان، پیامکی ارسال می‌شود.

### ورود داده کاربری به محصول با مشخصه امنیتی

* روش فراخوانی: کاربر می‌تواند به مسیر زیر رفته و پس‌از انتخاب شماره پرونده اقدام به بارگذاری داده کند: منو > آرشیو > آرشیو الکترونیک > آپلود

درنهایت رویکرد ممیزی شامل شناسه و نام کاربر و دیگر مشخصه‌های امنیتی و حائز اهمیت ثبت می‌گردد.ب ایست خاطرنشان کرد که سامانه فعلی از سازوکار امضای دیجیتال پشتیبانی نمی‌کند.

* پارامترهای قابل تنظیم:
  + شناسه کاربر: بابت شناسایی او و اینکه چه دسترسی‌هایی دارد.
  + داده بارگذاری‌شده: هر آنچه که کاربر قصد بارگذاری آن را دارد.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + نتیجه موفق: درصورت موفقت‌آمیز بودن، داده کاربر در سرور ذخیره می‌شود.
  + پیام خطا: درصورت بروز مشکل اعم‌از عدم دسترسی ویا موارد دیگر.
  + نتیجه: در هر دو حالت قبل رویداد ممیزی ثبت می‌گردد.

### خروج داده کاربری به محصول با مشخصه امنیتی

* روش فراخوانی: ‌کاربر می‌تواند درصورت داشتن دسترسی بارگیری در بخش‌های دارای این دسترسی (مثلا دکمه‌هایی با متن "خروجی اکسل")، اقدام به بارگیری (download) کند. درنهایت رویکرد ممیزی شامل شناسه و نام کاربر و دیگر مشخصه‌های امنیتی و حائز اهمیت ثبت می‌گردد.
* پارامترهای قابل تنظیم:
  + شناسه کاربر: بابت شناسایی او و اینکه چه دسترسی‌هایی دارد.
  + داده قابل‌بارگیری: هر آنچه که کاربر قصد بارگیری آن را دارد.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + پیام خطا: درصورت بروز مشکل اعم‌از عدم دسترسی ویا موارد دیگر.
  + نتیجه: رویداد ممیزی مرتبط شامل اطلاعات حائز امنیت ثبت می‌گردد.

### صحت داده کاربری ذخیره‌شده

* روش فراخوانی: کاربر مجاز با مراجعه به بخش‌های زیر می‌تواند از معتبر بودن یا نبودن داده‌‌ مطلع گردد:
  + منو > رویدادهای ممیزی > لاگین‌های کاربران
  + منو > امکانات > گزارش کاربران سیستم
  + منو > امکانات > بررسی پیام‌های سیستم
  + منو > امکانات > بررسی پیام‌های IIS
* پارامترهای قابل تنظیم:
  + نوع الگوریتم: نوع الگوریتم درهم‌ساز را مشخص می‌کند.
  + متن ساده: حاوی یک رکورد ممیزی ویا یک رمز عبور کاربر است که قرار است روی آن درهم‌سازی صورت گیرد.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + نتیجه: نتیجه یکی از دو حالت "معتبر" یا "نامعتبر" است که به کاربر نمایش‌داده‌می‌شود.

### مدیریت احراز هویت ناموفق

* روش فراخوانی: کاربری که نشست فعال نداشته‌باشد، هنگام واردکردن اطلاعات احراز هویت خود در صفحه ورود به سامانه دچار خطا شود و نتواند به سامانه ورود پیدا‌کند. درصورت تکرار این خطا، رویه ورود پیچیده‌تر شده و از کد کپچا استفاده می‌گردد.
* پارامترهای قابل تنظیم:
  + حد آستانه تلاش ناموفق ورود: عددی مثبت که کاربر سطح مدیر وارد سامانه می‌کند.
  + کد کپچا: یک عبارت تصادفی که برای پیچیده‌سازی فرآیند ورود بکار می‌رود.
  + داده‌های احراز هویت کاربر: نام کاربری و رمزعبوری که کاربر برای ورود استفاده می‌کند.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + پیام خطا: درصورت تجاوز از حد آستانه، پیام مرتبط به کاربر نمایش‌داده‌می‌شود.
  + نتیجه ناموفق: درصورت تجاوز از حد آستانه، کد کپچا فعال می‌شود.

### تعریف مشخصات کاربر

* روش فراخوانی: بمحض ورود موفق کاربر به سامانه و ایجاد نشست فعال، فراخوانی می‌شود. و داده‌های زیر از کاربر فعال ذخیره می‌شود:
  + شناسه کاربر
  + متد احراز هویت مورد استفاده
  + داده احراز هویت
  + وضعیت حساب کاربری
* پارامترهای قابل تنظیم:
  + شناسه کاربر: نام کاربری که در سامانه تعریف‌شده‌باشد.
  + متد احراز هویت: روش ورود کاربر به سامانه. مانند ورود با رمزعبور، ورود با کد یکبارمصرف و ...
  + داده احراز هویت: شامل نام کاربری و رمزعبور کاربر.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + ‌نتیجه موفق: داده‌ها و مشخصه‌های امنیتی کاربر ذخیره می‌شوند.

### مدیریت کلمه عبور

* روش فراخوانی: ‌کاربر سطح مدیر می‌تواند تمامی این سیاست‌ها را در مسیر "تعاریف > پنل کاربری > تنظیمات پسورد" تعیین کند.
* پارامترهای قابل تنظیم:
  + شامل عدد بودن: الزامی بودن وجود ارقام در کلمه عبور را مشخص می‌کند.
  + شامل حروف بودن: الزامی بودن وجود حروف در کلمه عبور را مشخص می‌کند.
  + شامل علائم بودن: الزامی بودن وجود نویسه‌های خاص در کلمه عبور را مشخص می‌کند.
  + طول پسورد: حداقل طول کلمه عبور را مشخص می‌کند.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + نتیجه موفق: درصورت موفقیت‌آمیز بودن، تنظیمات جدید ثبت می‌شوند.
  + نتیجه: رویداد ممیزی ثبت می‌شود.
  + پیام خطا: بدلیل عدم دسترسی کاربر به بخش موردنظر.

### احراز هویت کاربر

* روش فراخوانی: در صفحه ورود کاربران (LOGIN) کاربر می‌تواند اقدامات میانی زیر را بدون نیاز به احراز هویت انجام دهد:
  + بازیابی رمزعبور

باقی موارد و امکانات سامانه نیازمند به احراز هویت موفق کاربر هستند. کاربری می‌تواند احراز هویت کند که از قبل هیچ نشست فعالی نداشته‌باشد. در شرایطی که احراز هویت دو مرحله ای فعال باشد، کاربر باید اقدام به دریافت رمز یکبار مصرف از طریق پیامک و ورود آن در پارامتر مربوطه نماید.

* پارامترهای قابل تنظیم:
  + داده احراز هویت: نام کاربری و رمزعبور کاربر بمنظور ورود موفق به سامانه
  + شماره تماس کاربر: بمنظور بازیابی رمزعبور
  + کد تایید دومرحله‌ای: درصورتی که این تنظیمات فعال باشد، کاربر بایست کد تاییدی که دریافت کرده است را وارد سامانه نماید.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + پیام خطا: درصورت عدم انطباق شماره تماس کاربر با اطلاعات ذخیره‌شده در سامانه
  + پیام خطا: درصورت ورود ناموفق کاربر
  + نتیجه موفق: ورود موفق درصورت تصدیق داده‌های هویتی کاربر

### سازوکار احراز هویت چندگانه

* روش فراخوانی: در صفحه ورود کاربران (LOGIN) کاربری می‌تواند احراز هویت کند که از قبل هیچ نشست فعالی نداشته‌باشد. در شرایطی که احراز هویت دو مرحله ای فعال باشد، کاربر باید اقدام به دریافت رمز یکبار مصرف از طریق پیامک و ورود آن در پارامتر مربوطه نماید.

کاربر می‌تواند از طرق مختلف احراز هویت صورت‌دهد. مانند:

* + نام کاربری و رمزعبور
  + تایید دومرحله‌ای
  + استفاده از رمز یکبارمصرف
* پارامترهای قابل تنظیم:
  + نام کاربری و رمزعبور: اطلاعاتی که کاربر برای ورود نیاز دارد.
  + شماره تماس: بمنظور ارسال کد تایید در سازوکار ورود با شماره تماس
  + کد تایید دومرحله‌ای: یک دنباله تصادفی برای تایید گام دوم ورود کاربر
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + پیام خطا: درصورت اشتباه‌بودن کد تایید، نام کاربری و رمزعبور.
  + نتیجه موفق: کاربر باموفقیت وارد سامانه می‌شود.

### انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر

* روش فراخوانی: پس‌از ورود موفق کاربر به سامانه و ایجاد نشست فعال، در ازای هر درخواست http که از سمت کاربر می‌آید، سامانه وجود انقیاد مشخصه‌ها را با موجودیت فعلی کاربر سنجیده و درصورت بروز عدم تطابق یا عدم انقیاد، نشست کاربر فعلی خاتمه‌می‌یابد.
* پارامترهای قابل تنظیم:
  + شناسه کاربر: شناسه‌ی یکتایی که هر کاربر داراست.
  + نشانی IP: شناسه‌ی IP دستگاه کاربر که درون شبکه‌ قراردارد.
  + جزئیات واسط کلاینت: اطلاعاتی ازقبیل نام مرورگر، نسخه‌ی آن و ...
  + متد احراز هویت: روش ورود کاربر به سامانه. مانند ورود با رمزعبور، ورود با کد یکبارمصرف و ...
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + ‌نتیجه: درصورت تغییر مرورگر یا دستگاه کاربر فعال، او از حساب خود خارج می‌گردد.

### مدیریت مشخصه‌های امنیتی

* روش فراخوانی: کاربر سطح مدیر می‌تواند مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر را ویرایش، حذف یا مشاهده کند. این امکان برای دیگر کاربران فراهم نیست و جلوی آن گرفته می‌شود.

برای مثال می‌تواند به رجوع به بخش "منو > مدیریت کاربران > تعریف کاربران" داده‌های احراز هویت کاربر هدف را ویراسته و ذخیره نماید. درصورت وجود نشست فعال برای کاربر هدف، این نشست خاتمه‌یافته و کاربر مذکور نیازمند ورود مجدد خواهد بود.

* پارامترهای قابل تنظیم:
  + شناسه کاربر: برای تشخیص اینکه آیا این کاربر دسترسی سطح مدیر دارد یا خیر.
  + مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر: داده‌هایی که مدیر می‌تواند آنرا دستخوش تغییر کند.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + پیام خطا: درصورت دسترسی غیرمجاز، کاربر خطای مرتبط دریافت می‌کند.
  + نتیجه موفق: درصورت موفقیت‌آمیز بودن، نشست کاربری که مشخصه‌های امنیتی او تغییر کرده است، منقضی شده و لازم است تا دوباره به سامانه وارد شود.

### حفظ وضعیت امن در زمان شکست و تحمل خطا

* روش فراخوانی: هنگام بروز خطای نرم‌افزاری و سخت‌افزاری
* پارامترهای قابل تنظیم:
  + ‌رخداد شکست: هرگونه رخدادی که باعث اختلال در عملکرد سامانه گردد.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + نتیجه: وضعیت امن حفظ شده و یک رویداد ممیزی مرتبط با آن که شامل اطلاعات خطای پیش‌آمده است، ثبت می‌گردد. درنهایت شماره‌ی خطای پیش‌آمده به کاربر نمایش‌داده می‌شود تا بعدا قابل ردگیری کاربر باشد.

### محدودیت برروی چندین نشست هم‌زمان

* روش فراخوانی: کاربر سطح مدیر می‌تواند به رجوع به مسیر "منو > تعاریف > پنل کاربری > تنظیمات لاگین" اقدام به ویرایش تنظیمات محدودیت نشست‌های همزمان کند.
* پارامترهای قابل تنظیم:
  + حد آستانه تعداد نشست‌های همزمان
  + شناسه کاربر: برای شناسایی او و دسترسی‌هایش
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + پیام خطا: درصورت دسترسی غیرمجاز به حد آستانه تعداد نشست‌های همزمان، خطایی مرتبط نمایش داده می‌شود و رویداد ممیزی مرتبط ثبت می‌گردد.
  + نتیجه موفق: درصورت موفقیت‌آمیز بودن رویه، حد آستانه جدید ذخیره می‌گردد.
  + نتیجه: ثبت رویداد ممیزی مرتبط

### خاتمه دادن به نشست‌ها

* روش فراخوانی: به خواست خود کاربر و از مسیر "منوی سمت چپ، بالا > خروج" می‌توان از سامانه خارج شد. ویا اگر کاربر به مدت معینی که آن را کاربر مدیر سیستم تعیین می‌کند، بیکار بماند، نشست مرتبط با او خاتمه می‌یابد.
* پارامترهای قابل تنظیم:
  + ‌بازه‌ زمانی مرتبط با خاتمه نشست غیرفعال: عددی که براساس آن سامانه حدود زمانی مجاز برای ماندن درحالت بی‌کار (IDLE) را برای کاربر جایز می‌داند.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + نتیجه: درصورت تجاوز از بازه زمانی مذکور، کاربر پیام با مضمون مرتبط دریافت‌کرده و نیازمند ورود مجدد به سامانه است.
  + نتیجه: درصورت فشردن دکمه خروج از حساب، کاربر داوطلبانه به نشست خود خاتمه می‌دهد.

### سوابق دسترسی به محصول

* روش فراخوانی: به خواست خود کاربر و از مسیر "منوی سمت چپ، بالا > خروج" می‌توان از سامانه خارج شد. ویا اگر کاربر به مدت معینی که آن را کاربر مدیر سیستم تعیین می‌کند، بیکار بماند، نشست مرتبط با او خاتمه می‌یابد.
* پارامترهای قابل تنظیم:
  + ‌بازه‌ زمانی مرتبط با خاتمه نشست غیرفعال: عددی که براساس آن سامانه حدود زمانی مجاز برای ماندن درحالت بی‌کار (IDLE) را برای کاربر جایز می‌داند.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + نتیجه: درصورت تجاوز از بازه زمانی مذکور، کاربر پیام با مضمون مرتبط دریافت‌کرده و نیازمند ورود مجدد به سامانه است.
  + نتیجه: درصورت فشردن دکمه خروج از حساب، کاربر داوطلبانه به نشست خود خاتمه می‌دهد.

### سوابق دسترسی به محصول

* روش فراخوانی: کاربر می‌تواند از مسیر "منوی سمت چپ، بالا > تاریخچه فعالیت" به سوابق دسترسی خود دسترسی داشته باشد.
* پارامترهای قابل تنظیم:
  + ‌شناسه کاربر: برای شناسایی او و واکشی سوابق ورود او از پایگاه داده
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + نتیجه: نمایش سوابق ورود موفق و ناموفق

### برقراری نشست

* روش فراخوانی: ‌کاربر مجاز می‌تواند با مراجعه به مسیر "منو > تعاریف > پنل کاربری > محدودسازی لاگین" تنظیمات مرتبط با محدودسازی ورود را ویرایش‌کند.
* پارامترهای قابل تنظیم:
  + از تاریخ – تا تاریخ: بازه زمانی مجاز برای ورود کاربران را نگه‌می‌دارد.
  + از آی‌پی – تا آی‌پی: بازه نشانی IP مجاز برای ورود کاربران را نگه‌می‌دارد.
  + از پورت – تا پورت: بازه مقادیر پورت مجاز برای ورود کاربران را نگه‌می‌دارد.
* پاسخ هدف ارزیابی، پیام‌ها و كد‌های بازگردانده شده:
  + پیام خطا: درصورت دسترسی نداشتن به بخش تنظیمات، خطای مرتبط به کاربر نشان‌داده‌می‌شود.
  + نتیجه موفق: درصورت موفقیت‌آمیز بودن، تنظیمات جدید ثبت می‌گردد. نتیجه‌ی این تنظیمات به محدودشدن شرایط ورود کاربر منجر می‌شود.
  + نتیجه: رویداد ممیزی مرتبط ثبت می‌شود.

## رخدادها

* سر‌ریز حافظه‌ی تخصیص داده شده به رویداد‌های ممیزی
* وارد کردن بیش از حد نام کاربری و کلمه عبور اشتباه.
* ورود مقادیر ناصحیح ورودی فرم‌های نرم افزار.
* ثبت شدن رویداد‌های ممیزی خاص كه می‌تواند نمایانگر تلاش ‌برای نفوذ به سیستم باشد.
* خروج پرسنل از یك سازمان كه نیازمند حذف حساب كاربری و یا غیر‌فعال‌سازی آن خواهد بود.

## اقدامات امنیتی

جهت اجرای اهداف امنیتی که برای محیط عملیاتی در سند هدف امنیتی بیان شده، موارد ذیل جهت فراهم نمودن آن انجام خواهد شد:

* ارائه لیست موارد امنیتی شبکه برای فراهم نمودن موارد امنیتی نفوذ شامل استفاده از فایروال فیزیکی و تنظیم رول‌های مختلف امنیتی برای جلوگیری از نفوذ.
* ارائه آموزش‌های جامع به پرسنل و افراد دخیل در نرم افزار توسط شرکت برای افزایش بهره بری و امنیت نرم افزار.
* شرکت تحلیلگران آمارد سازو کار آموزش‌های لازم برای تیم توسعه دهنده خود برای فراهم کردن امنیت کامل پروژه را نیز ایجاد کرده است.
* تمامی مراحل نصب و راه اندازی محصول توسط تیم مجرب شرکت تحلیلگران انجام شده تا تمامی موارد امنیتی موجود در چک لیست بررسی و مورد پیگیری قرار بگیرد.
* نسخه پشتیبان خودکار سیستم توسط تیم پشتیبان شرکت برای ارائه خدمات بهتر و امنیت بالا تحویل کاربر نهایی خواهد شد.

## پیشنهادات برای استفاده امن هدف ارزیابی

* به مدیر سامانه توصیه می‌شود در سامانه با فراهم کردن بسته امنیتی HTTPS برای سازوکار امن اقدام نماید.
* به مدیر سامانه توصیه می‌شود تا دسترسی بخش‌های مهم سامانه از جمله مدیریت سطوح دسترسی و تعریف کاربر جدید را محدود کرده و در اختیار همه کاربران قرار ندهد.
* به کاربران توصیه می‌شود نام کاربری و کلمه عبور خود را در اختیار شخص دیگری قرار نداده و هر چند مدت نسبت به تغییر کلمه عبور خود اقدام نمایند.

# فرآیند آماده­سازی هدف ارزیابی

## روال پذیرش

* تحویل‌گیرنده باید بررسی كند كه تمامی بخش‌های هدف ارزیابی همان طور كه در ST نشان داده شده است با ورژن صحیح تحویل داده شده است(منظور تطابق با همان ورژنی است که در آزمایشگاه مورد ارزیابی قرارگرفته و گواهی نامه امنیتی کسب کرده است و همان نسخه در اختیار کاربران قرارگرفته است.)
* تحویل گیرنده می‌بایست علاوه بر نرم افزار لایسنس با اعتبار طبق قرارداد را نیز از تیم پشتیبانی تحویل بگیرد.

## روال نصب و راه اندازی

* برای نصب امن نرم افزار باید حداقل موارد زیر فراهم و بررسی شود:
* سامانه باید حداقل از ویندوز سرور 2012 پشتیبانی نماید.
* امکان نصب پایگاه داده sql حداقل نسخه 2012 فراهم باشد.
* بعد از ارسال اطلاعات نسخه وب به iis میبایست اتصال نرم افزار با پایگاه داده برقرار شود.
* ارائه شماره شناسه نرم افزار به شرکت و دریافت لایسنس استفاده از محصول.
* اپراتور میبایست بعد از اجرا برنامه (در url تنظیم شده) نام کاربری و کلمه عبور مدیر سیستم را تعیین و ثبت نماید.
* بعد از ثبت مدیر سیستم و لاگین اولین مرحله راه اندازی سیستم ورود به تنظیمات و تنظیم اطلاعات اولیه شامل نام شرکت و اطلاعات تماس آن و همچنین تعریف کاربران و سطوح دسترسی میباشد.

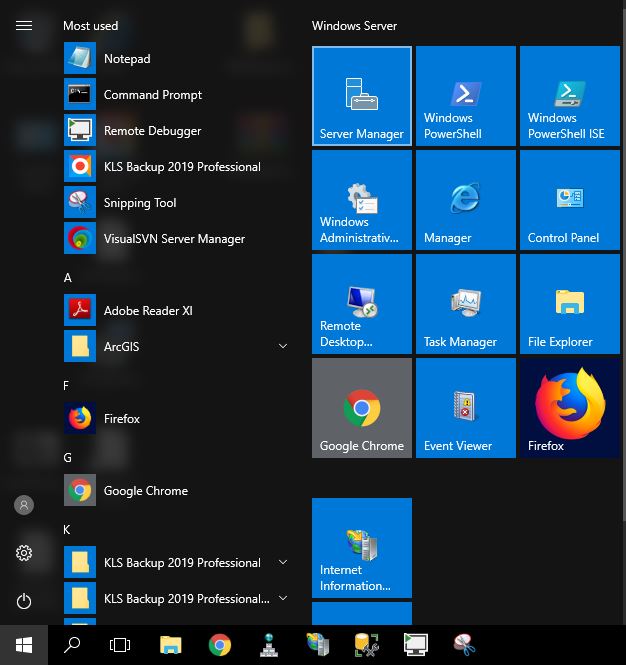
### فراهم سازی محیط عملیاتی

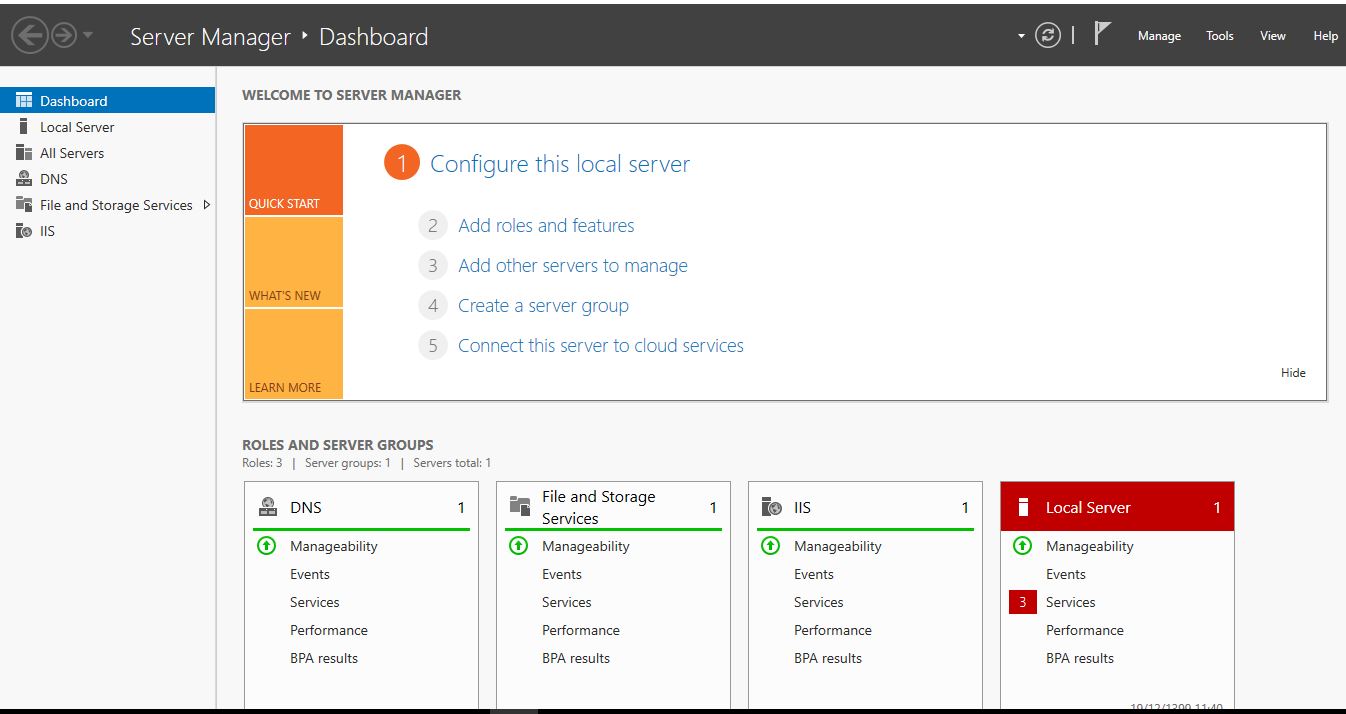
* انجام تنظیمات مربوط به پورت‌ها و نقش‌ها در فایروال سیستم عامل.
* تنظیمات مربوط به iis و تست نقاط امنیتی آن.
* تست نفوذ به بخش فایروال فیزیکی سیستم.
* آموزش نحوه تنظیم، رفع خطا و کنترل امنیت سیستم به اپراتور اصلی نرم افزار.
* آموزش روال نرم افزار به سایر افراد دخیل در نرم افزار.
* تهیه سیستم پشتیبان خودکار و فراهم سازی سامانه ذخیره سازی آخرین نسخه دیتابیس.

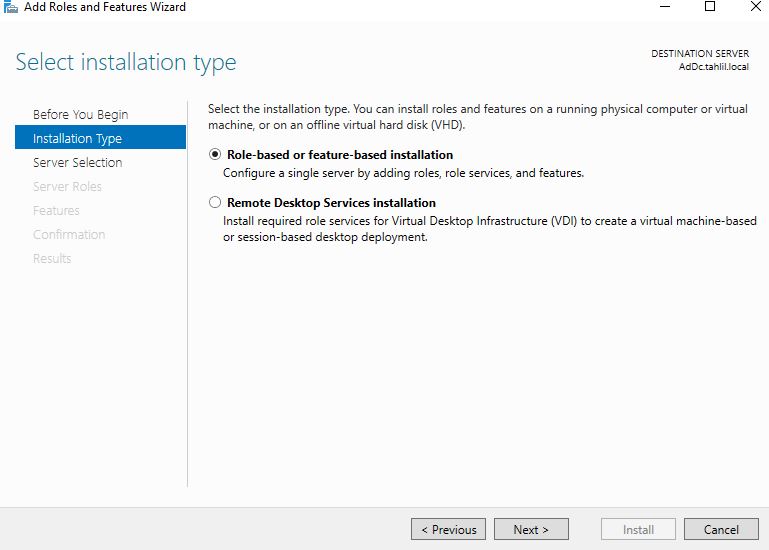
### نصب هدف ارزیابی

برای استفاده از نرم افزار شهرسازی تحت وب ابتدا باید سرویس IIS را بر روی سرور فعال کنیم .

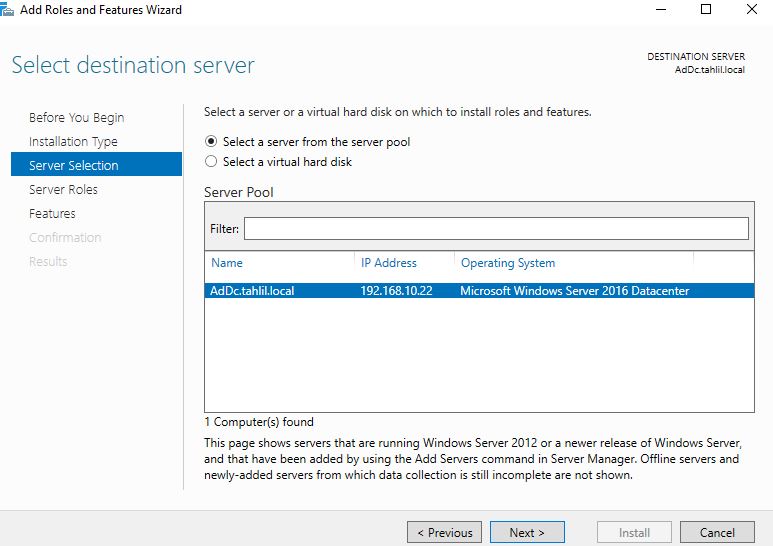
1. روی سرور روی نوار start کلیک کرده و server manager را اتنخاب می‌کنیم .



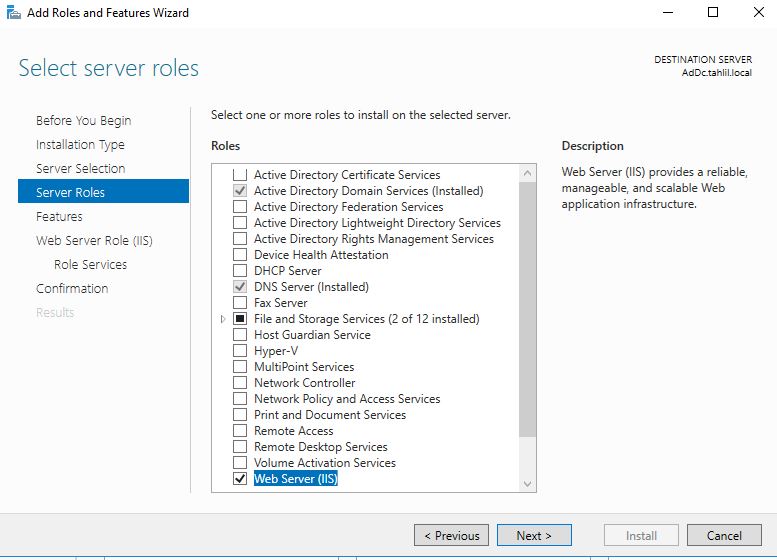
1. در این صفحه روی گزینه add role and featuresکلیک می‌کنیم .
2. روی Next کلیک می‌کنیم .

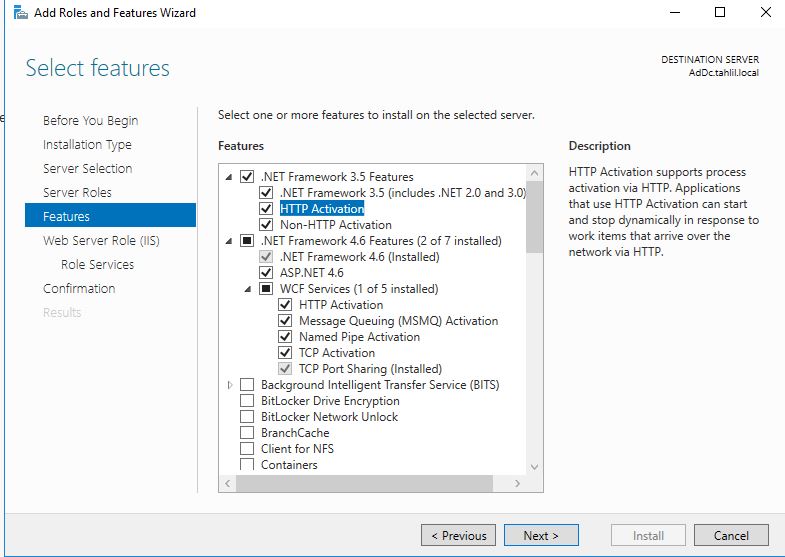


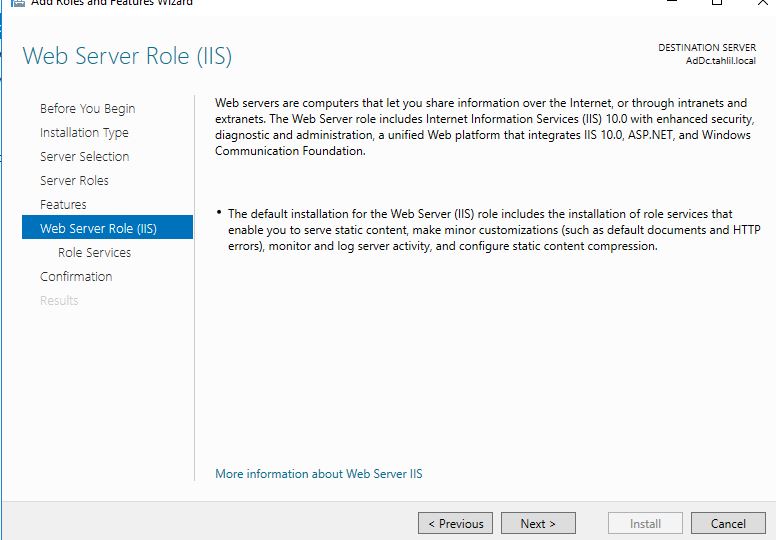
1. در این صفحه نام کامپیوتر سرور به همراه آدرس IP و نوع سیستم عامل سرور نمایش داده میشود. بر روی Next کلیک می‌کنیم .



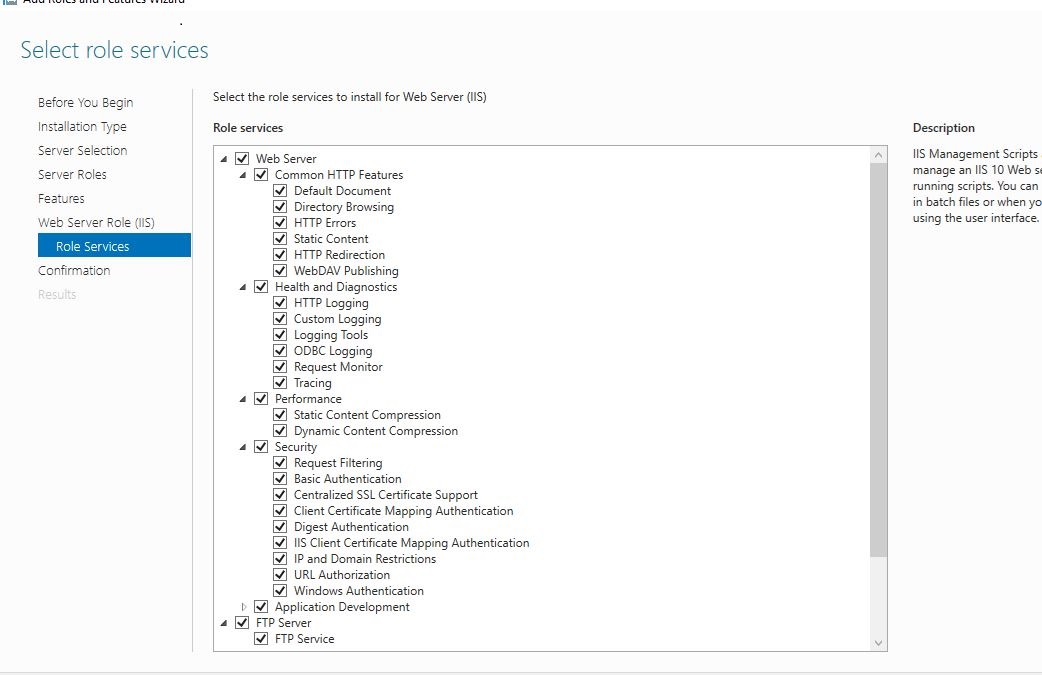
1. در این صفحه تیک مربوط به گزینه Web server (IIS) را فعال می‌کنیم و در پنجره‌ای که نمایش داده میشود روی add features کلیک می‌کنیم .



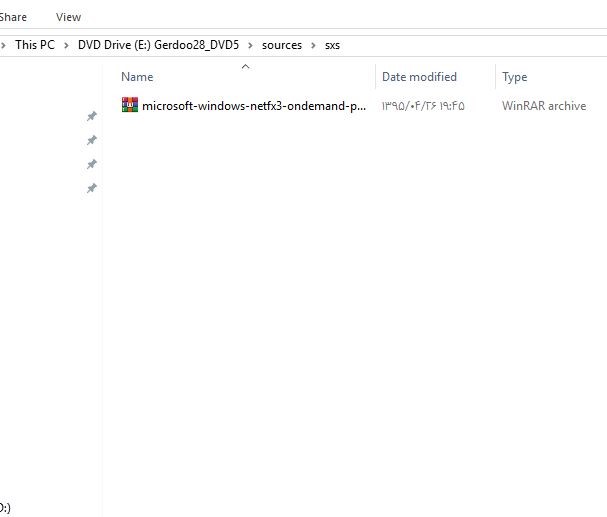
1. در این صفحه تیک مربوط Net Framework 3.5 features و Net Framework 4.6 features به همراه گزینه‌های مربوط به آنها را فعال میکنیم .
2. بر روی گزینه Next کلیک می‌کنیم .



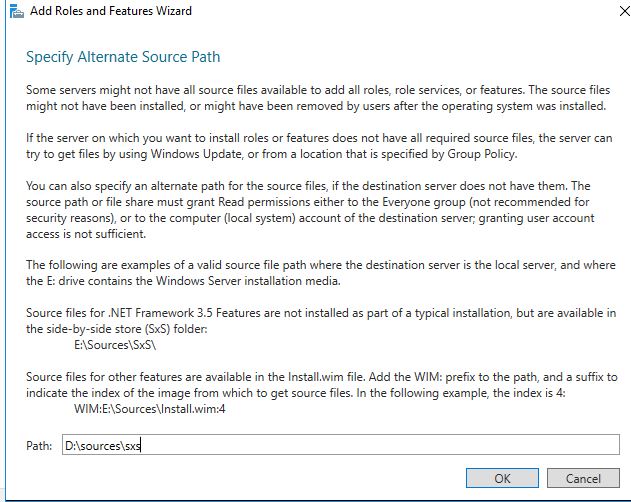
1. در صفحه ظاهر شده تیک همه گزینه‌ها را فعال می‌کنیم .



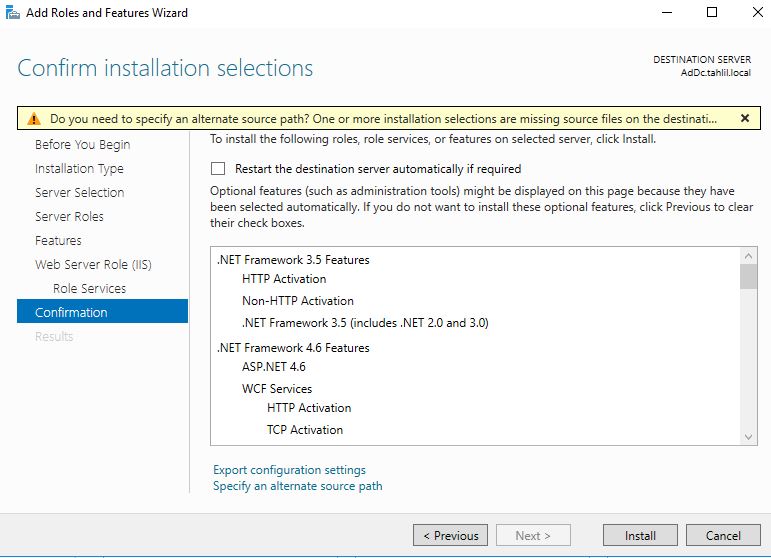
1. در صفحه ظاهر شده روی گزینه Specify an alternate source path کلیک می‌کنیم حال به سراغ DVD نصبی ویندوز سرور می‌رویم آدرس زیر را کپی می‌کنیم .



1. آدرس کپی شده را در این قسمت Paste می‌کنیم .



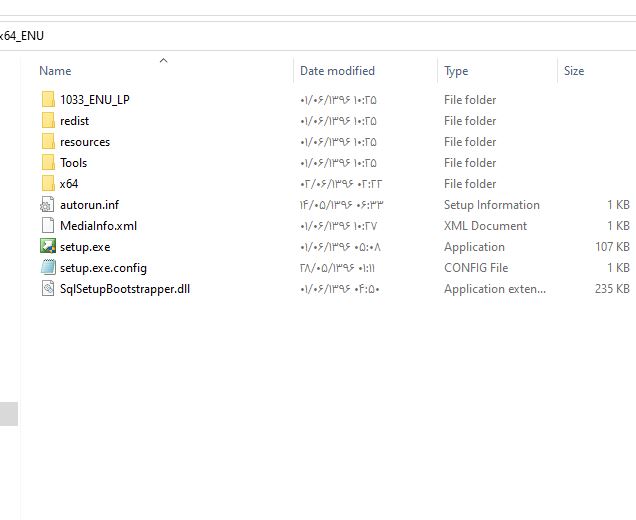
1. در صفحه ظاهر شده بر روی گزینه install کلیک می‌کنیم .



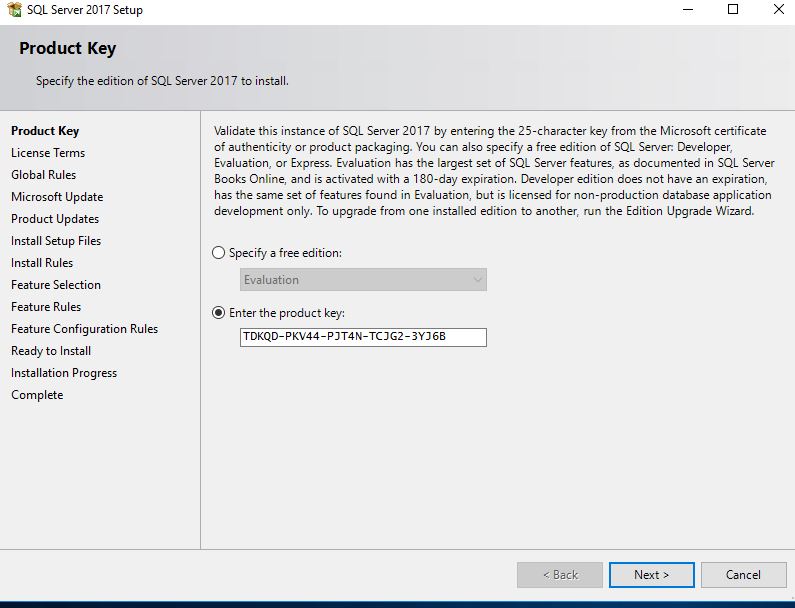
**نـصـب Sql server 2017 :**

جهت راه اندازی نرم افزار ابتدا باید نرم افزار Sql Server 2017 را نصب کنیم . نسخه نصبی Sql Server 2017 به صورت فایل iso می‌باشد بنابراین برای باز کردن آن ابتدا باید نرم افزار UltraISO.Premium یا نرم افزار WinMountرا نصب کنیم . فرض نرم افزار UltraISO.Premium را نصب کرده ایم . بر روی فایل iso راست کلیک می‌کنیم روی Ultro Iso رفته سپس گزینه Mount to Drive X را انتخاب میکنیم . (یک درایو مجازی در My computer ساخته می‌شود که به عنوان مثالX نام درایو مجازی ساخته شده می‌باشد ) .

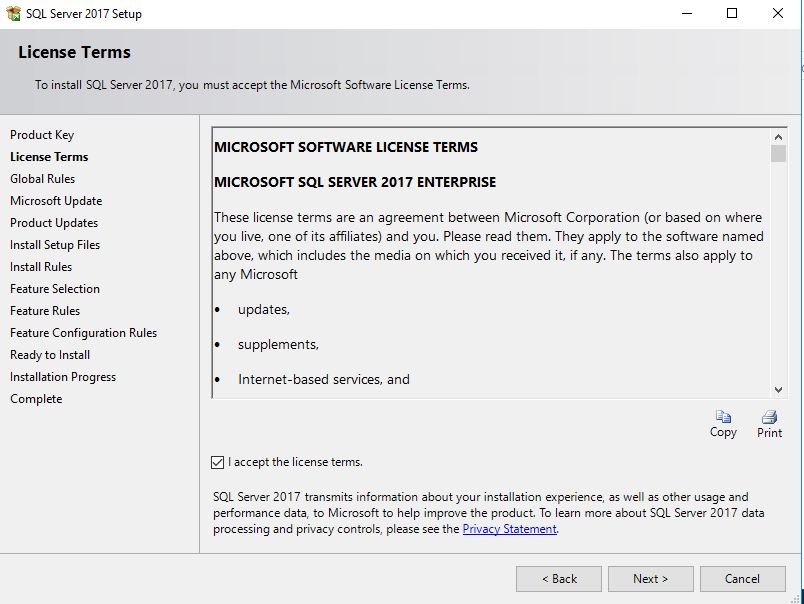
1. روی درایو مجازی راست کلیک و open را انتخاب می‌کنیم . بر روی setup.exe دبل کلیک می‌کنیم .



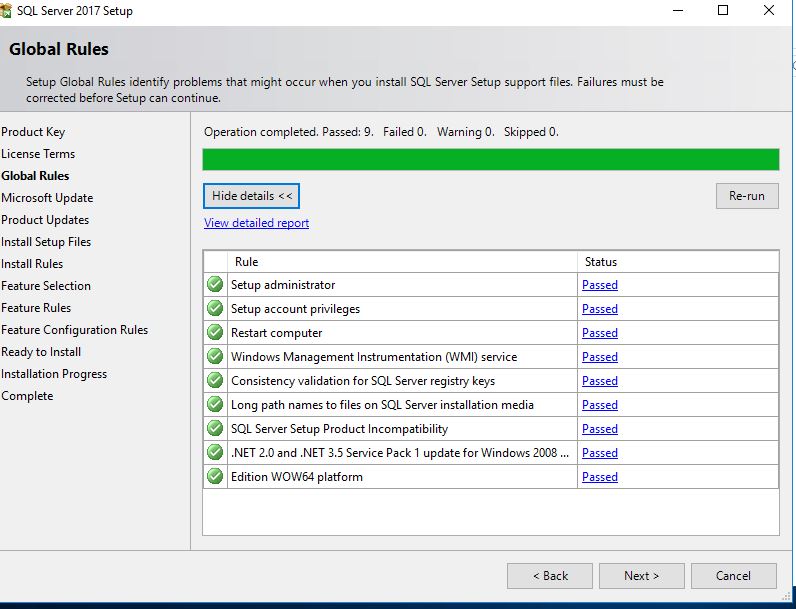
1. در صفحه ظاهر شده بر روی Next کلیک می‌کنیم .



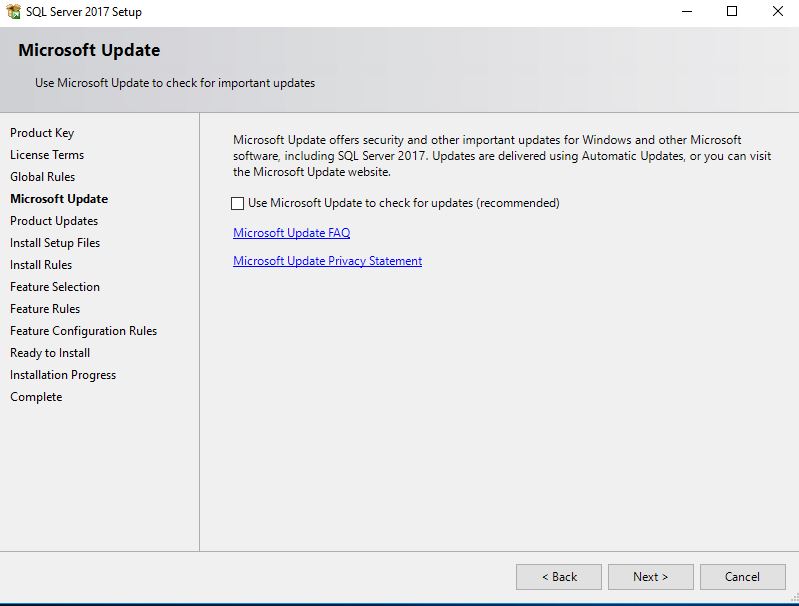
1. در این صفحه تیک مربوط به I accept the licence را پذیرفته و بر روی Next کلیک می‌کنیم .

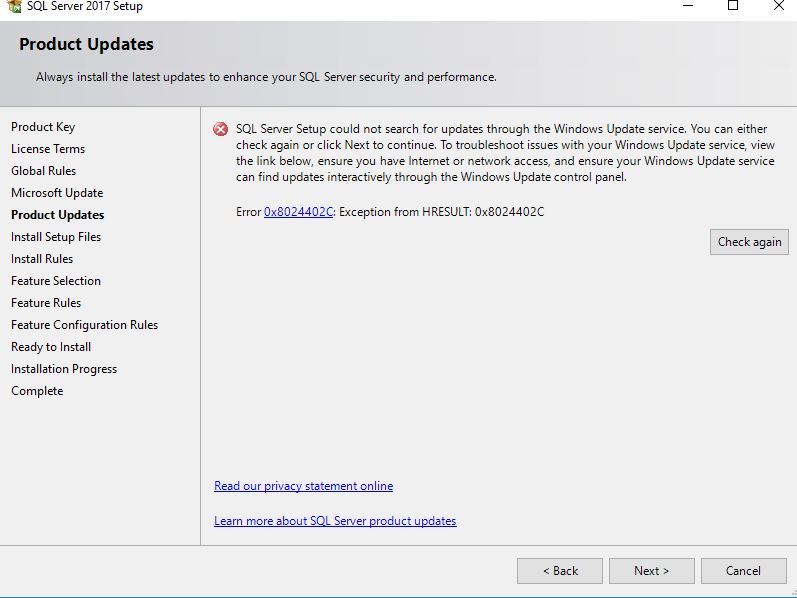


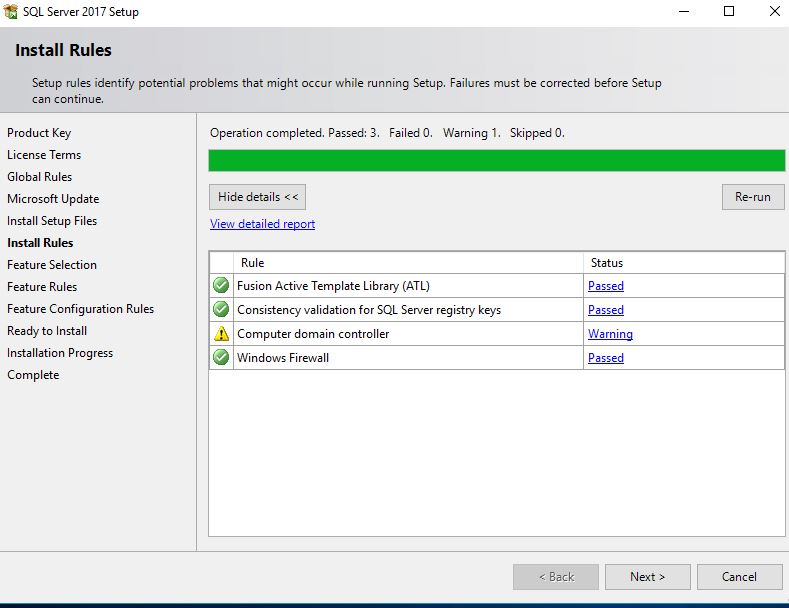
1. در این صفحه بر روی Show Detailes کلیک کرده و پس از چک کردن گزینه‌ها بر روی Next کلیک می‌کنیم .

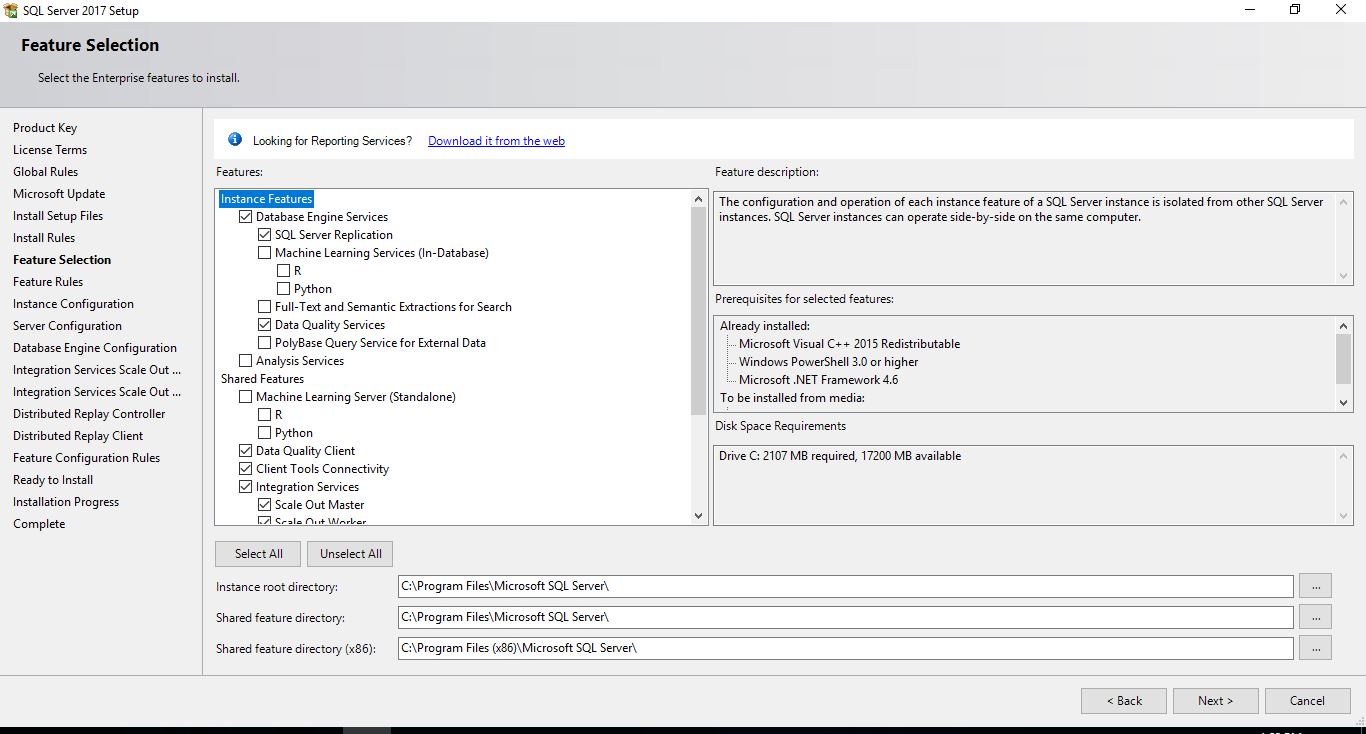


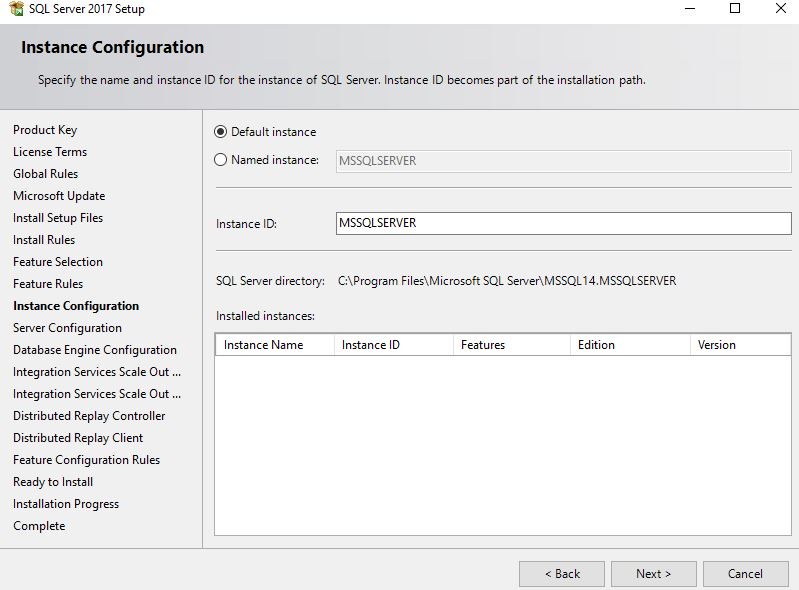
1. در صفحه ظاهر شده تیک مربوط به use Microsoft update را بر می‌داریم و بر وری Next کلیک می‌کنیم .

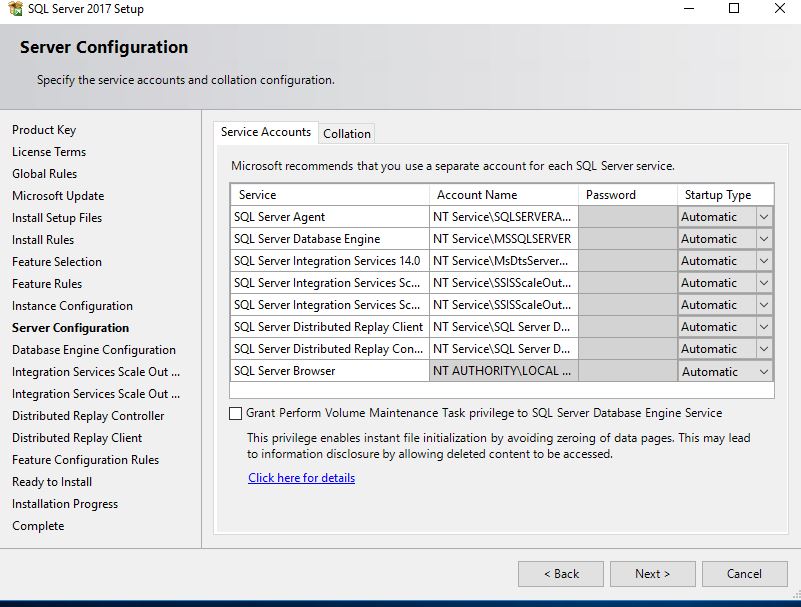
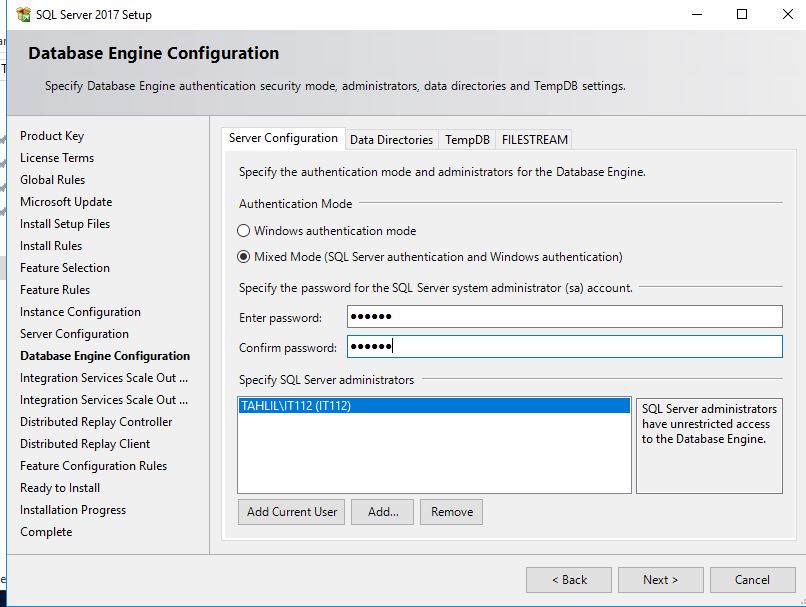


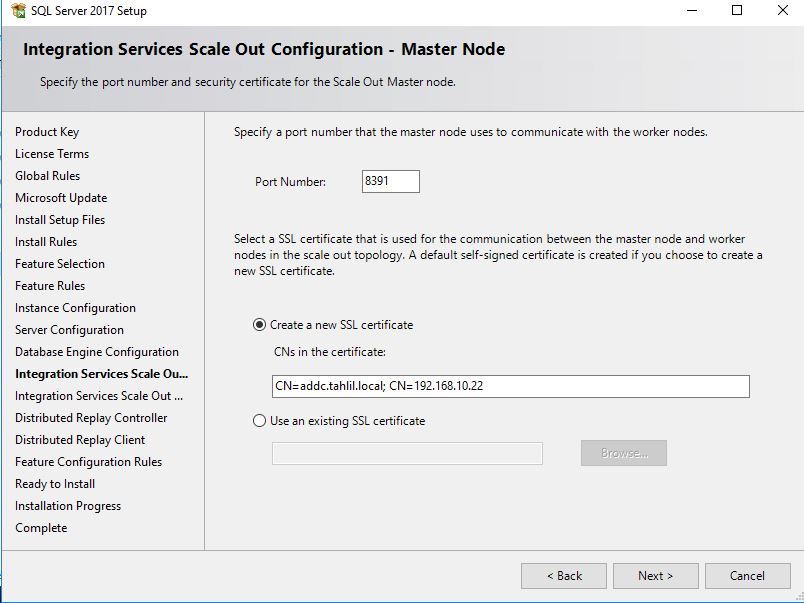
1. در صفحه ظاهر شده به دلیل بروز خطا چند بار بر روی گزینه Back و Next کلیک می‌کنیم تا صفحه مربوط به خطا برطرف گردد .
2. در صفحه ظاهر شده بر روی Next کلیک می‌کنیم .



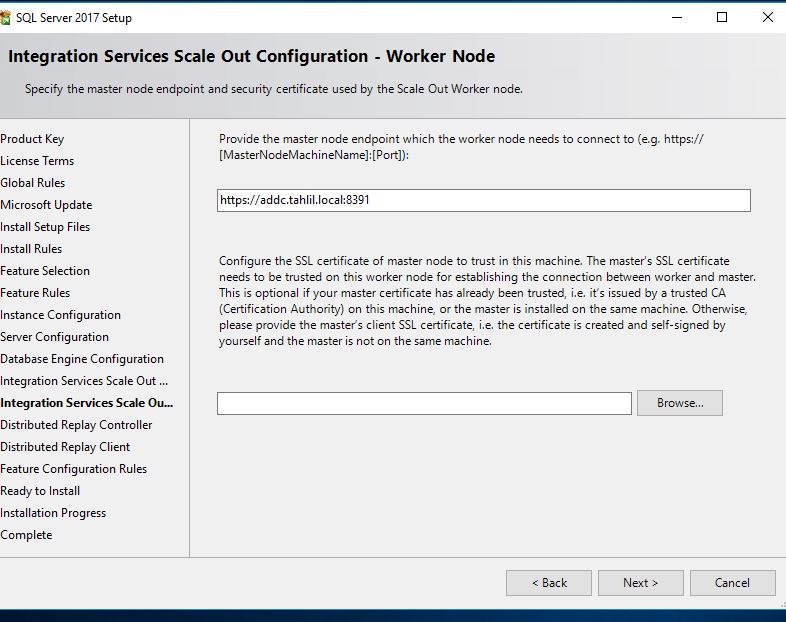
1. در صفحه ظاهر شده طبق شکل فقط تیک مربوط به گزینه‌های زیر فعال می‌کنیم و بر روی Next کلیک می‌کنیم
2. در این صفحه هم می‌توانیم Default instance را انتخاب کنیم و هم گزینه Named Instance که در صورت انتخاب گزینه ی دوم باید یک نام برای آن انتخاب کنیم .



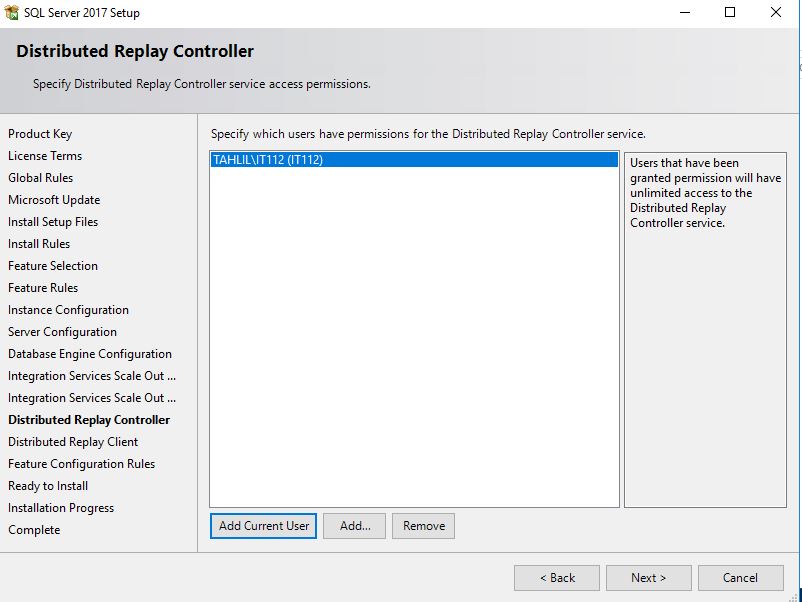
1. در صفحه ظاهر شده در قسمت Start type همه ی گزینه‌ها را بر روی Automatic تنظیم می‌کنیم ضمنا در تب collation زبان موردنظر حتما روی Arabic \_CI\_AS تنظیم گردد .
2. در این صفحه ابتدا روی گزینه Add Current User کلیک می‌کنیم تا یوزر مورد نظر جهت احراز هویت در sql server اضافه گردد سپس روی گزینه Mixed Mode کلیک کرده و یک پسورد اختیاری وارد می‌کنیم .(این قسمت جهت احراز هویت تحت شبکه می‌باشد )
3. در صفحه ظاهر شده بر روی Next کلیک می‌کنیم .



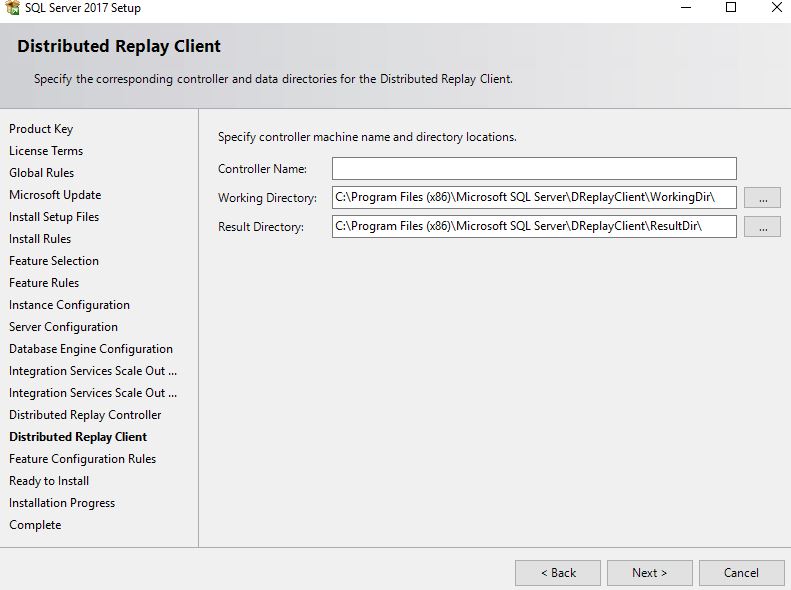
1. در صفحه ظاهر شده بر روی Next کلیک می‌کنیم .

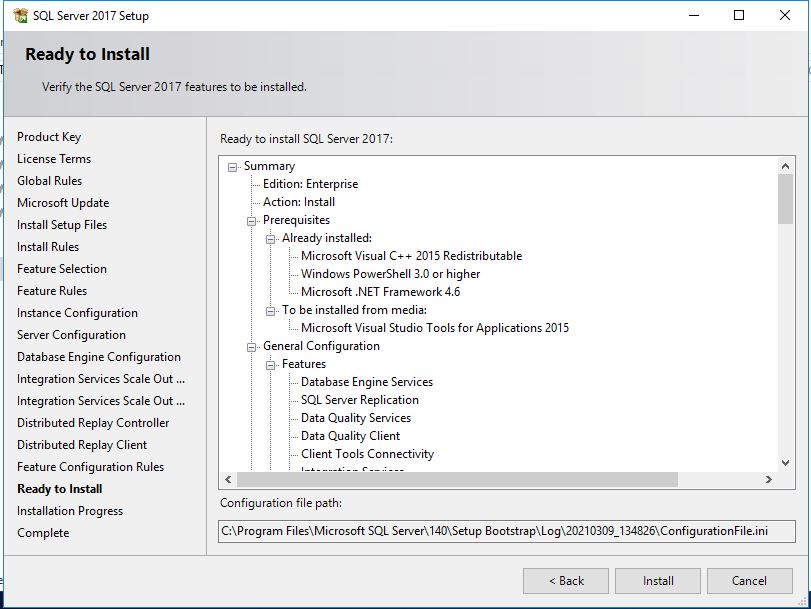


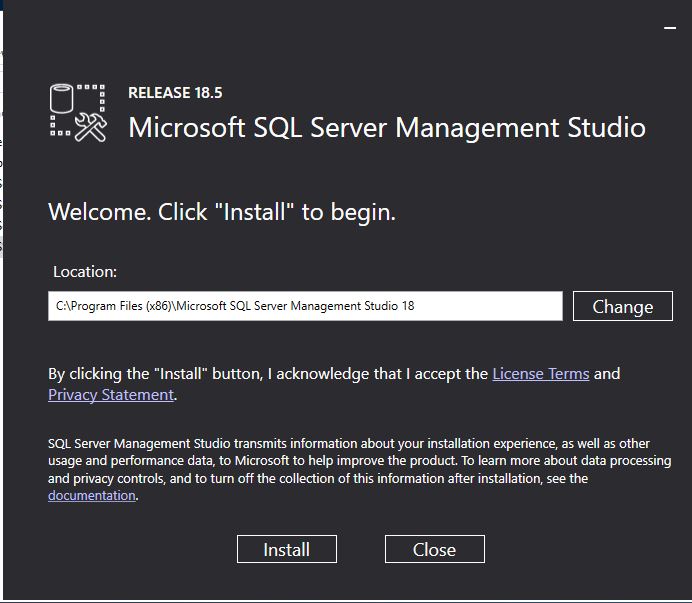
1. در این صفحه بر روی گزینه Add Current user کلیک کرده و سپس Next را انتخاب می‌کنیم .

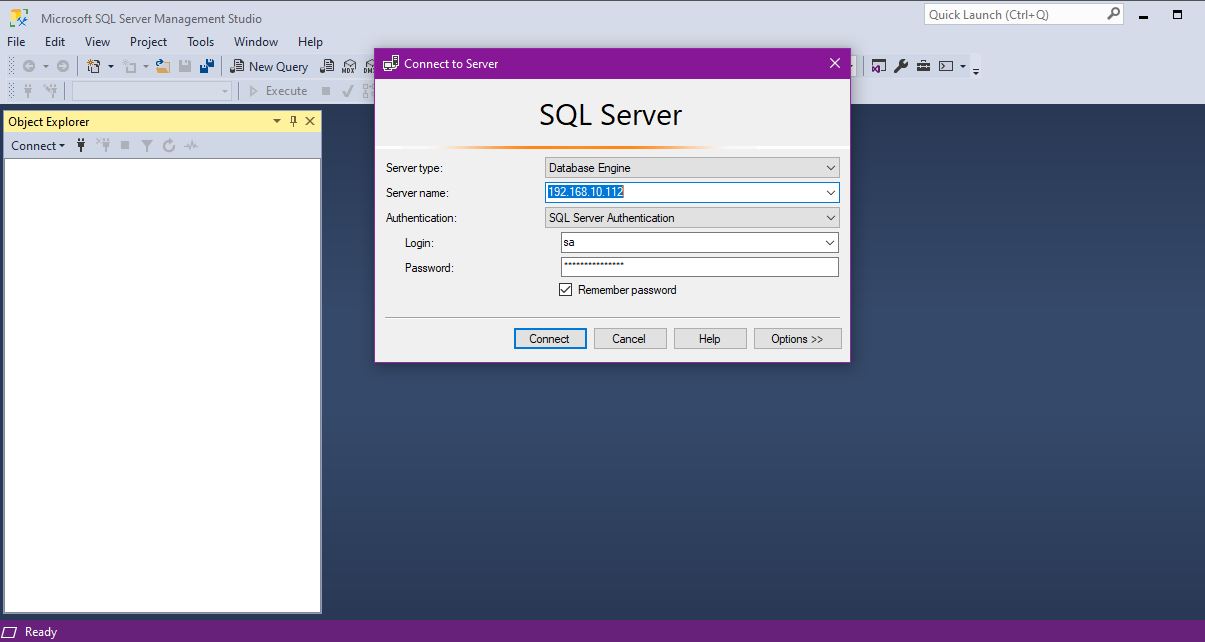


1. در صفحه ظاهر شده بر روی Next کلیک می‌کنیم .



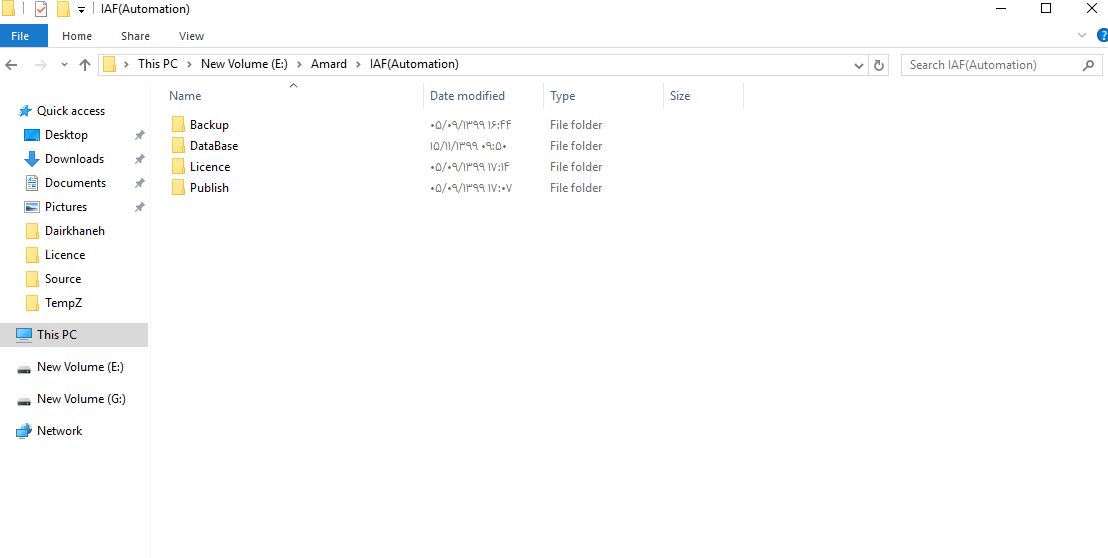
1. در صفحه ظاهر شده install را انتخاب می‌کنیم
2. حال به سراغ نصب Sql server Management studio می‌رویم . بر روی فایل نصبی دبل کلیک و install را انتخاب می‌کنیم .



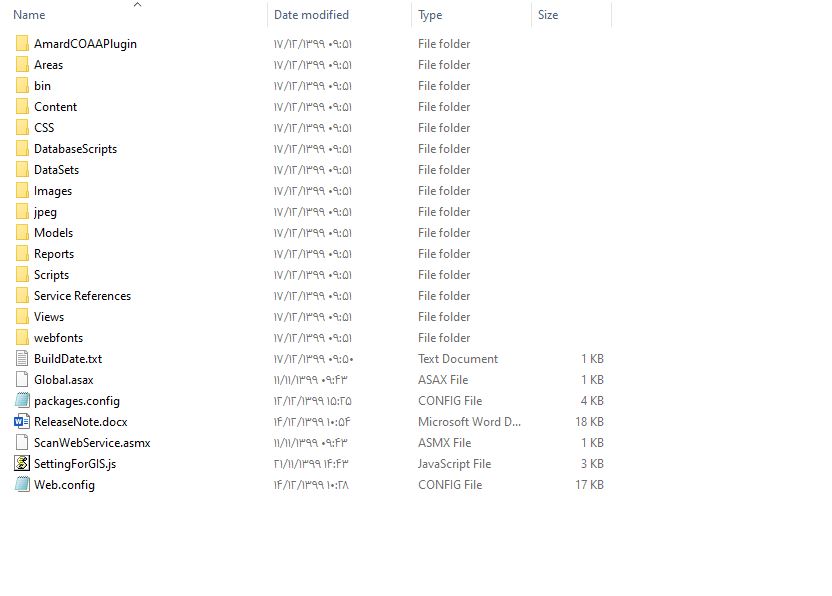
بعد از نصب Sql Server حال به سراغ Attach کردن دیتابیس‌های مربوطه می‌رویم . روی نوار start کلیک کرده و از قسمت Microsoft Sql Server Tools گزینه Sql server Management studio را انتخاب می‌کنیم .

پس از لاگین شده به Sql Server دیتابیس‌های مورد نظر را attach می‌کنیم .

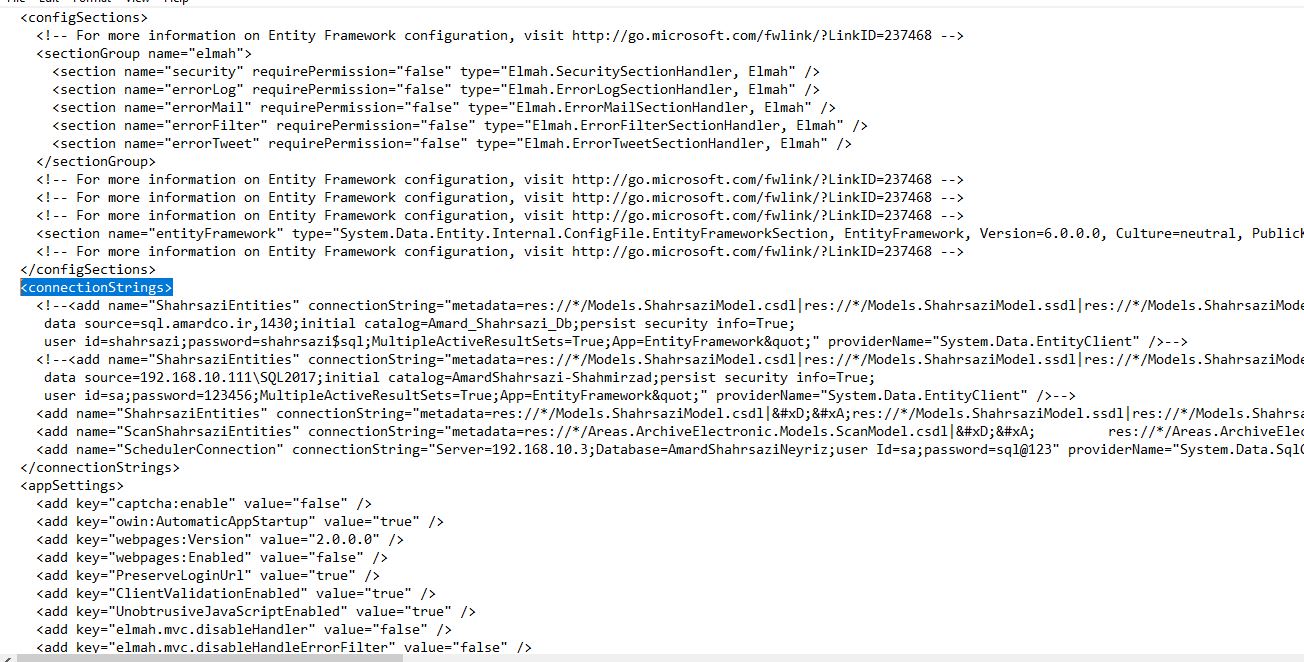
فرض فایل‌های مورد نظر جهت نصب نرم افزار را در درایو E سرور کپی کرده ایم .



به پوشه ی Publish وارد شده و به سراغ فایل Web.config می‌رویم . (فایلی جهت ایجاد ارتباط بین نرم افزار با Sql server )

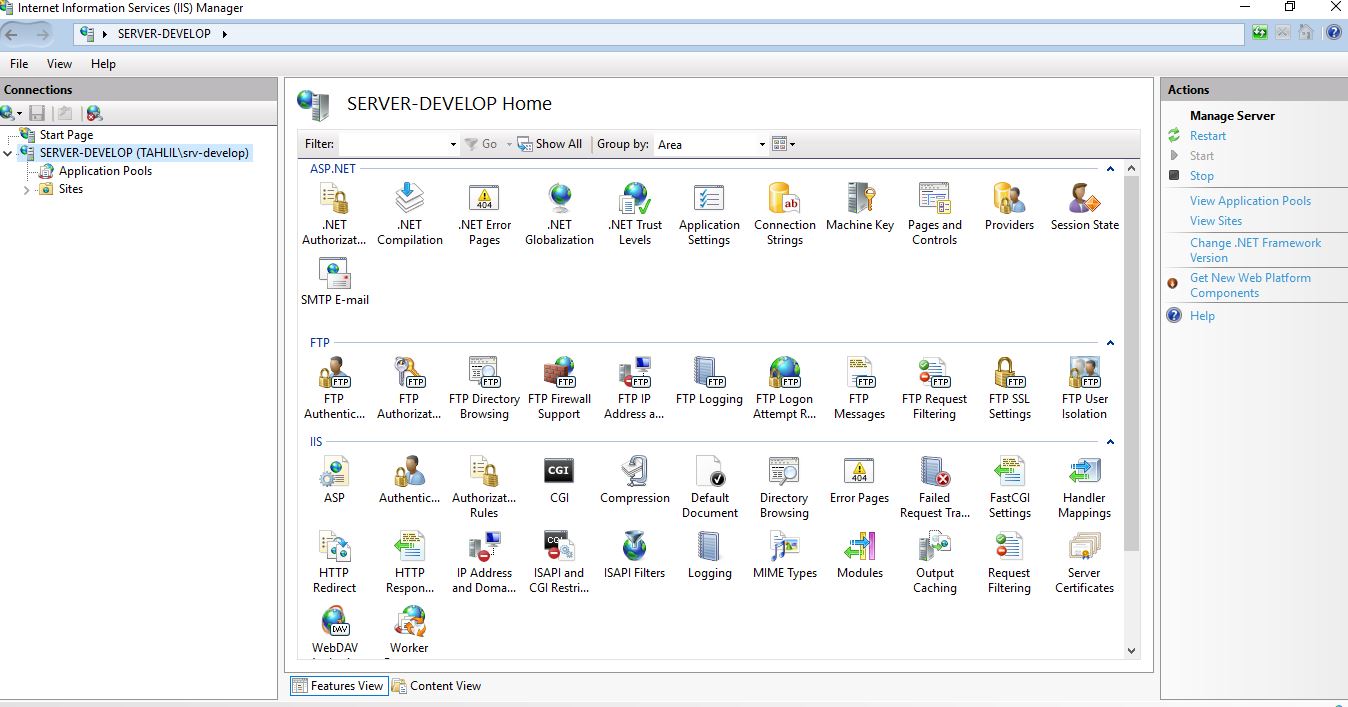


فایل web.config را باز می‌کنیم و به قسمت Connection string می‌رویم

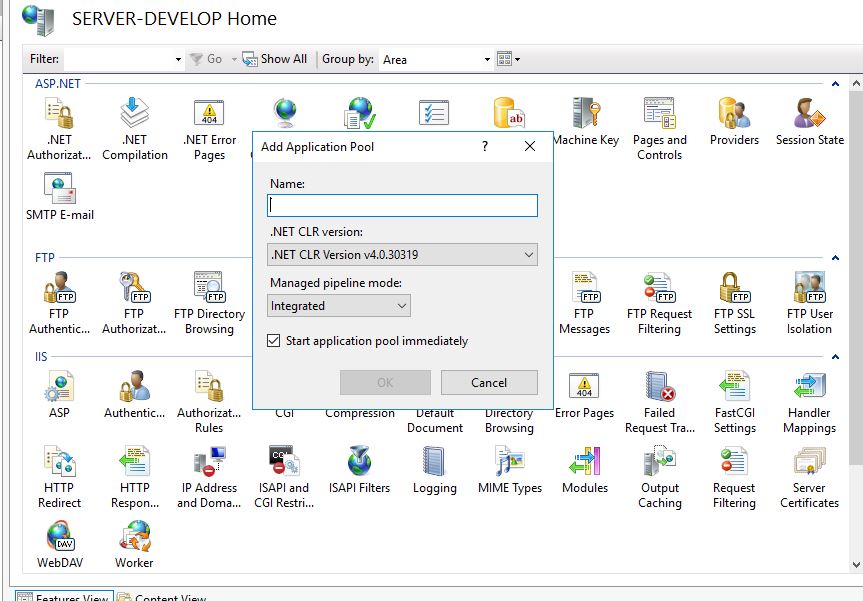


1. در قسمت Data Source باید نام instance نصب شده را وارد کنیم .
2. در قسمت catalog باید نام دیتابیس‌های مورد نظر را وارد کنیم .
3. در قسمت ID باید یوزر sa را وارد کنیم .
4. در قسمت password باید پسورد وارد شده در هنگام نصب sql را وارد کنیم .

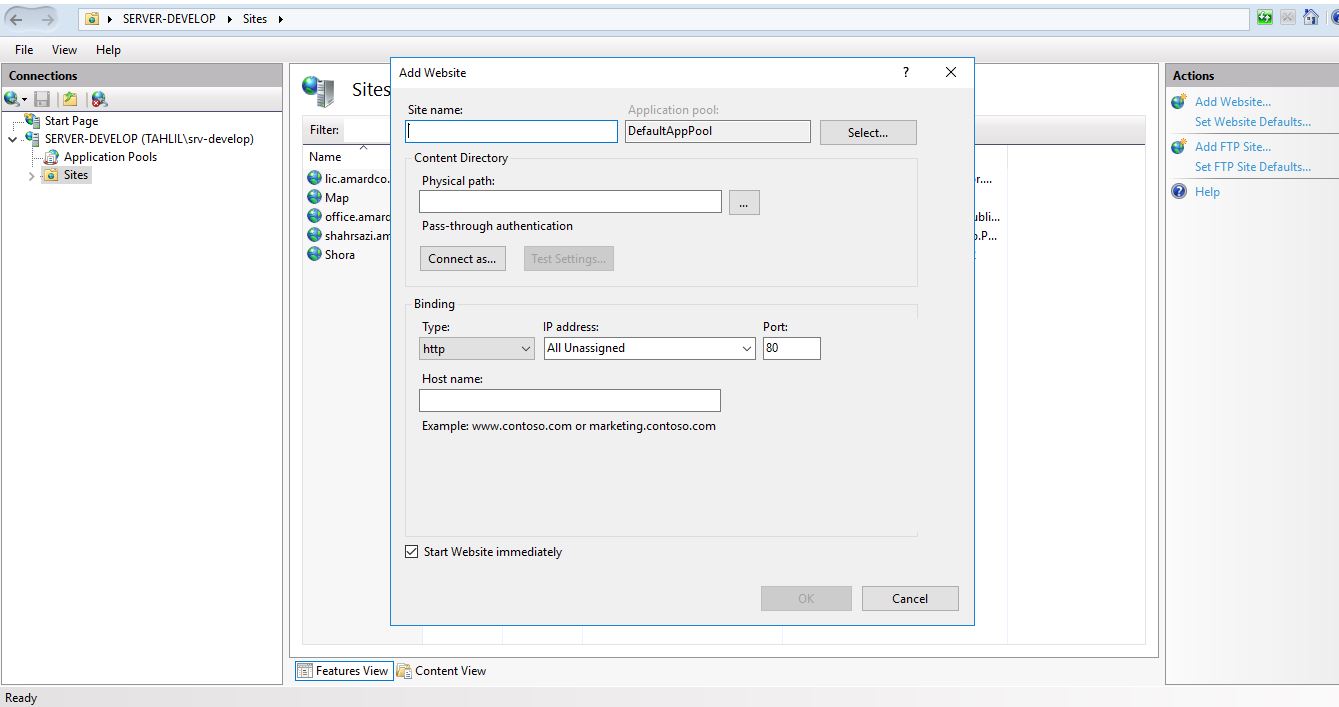
حال به control panel رفته و گزینه Administrative tools را انتخاب کرده و روی Internet information Service (IIS) manager را انتخاب می‌کنیم .



ابتدا روی Application pool راست کلیک کرده و گزینه Add Application pool را انتخاب می‌کنیم .

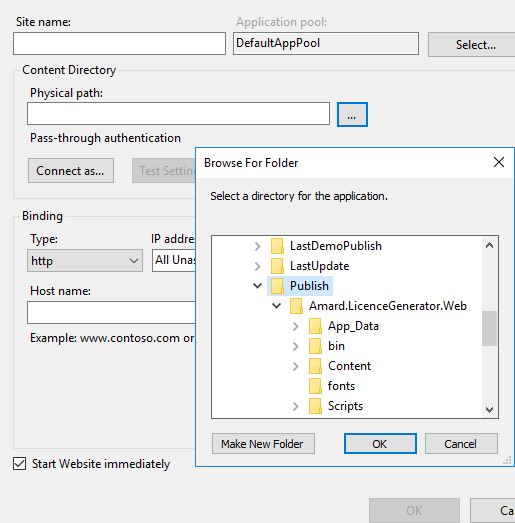


حال بر روی Site کلیک کرده و یک سایت جدید ایجاد می‌کنیم .

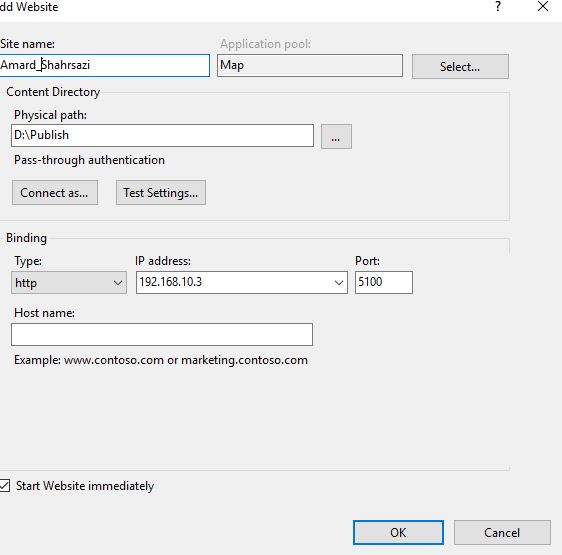


در قسمت pool، pool تعریف شده را انتخاب می‌کنیم

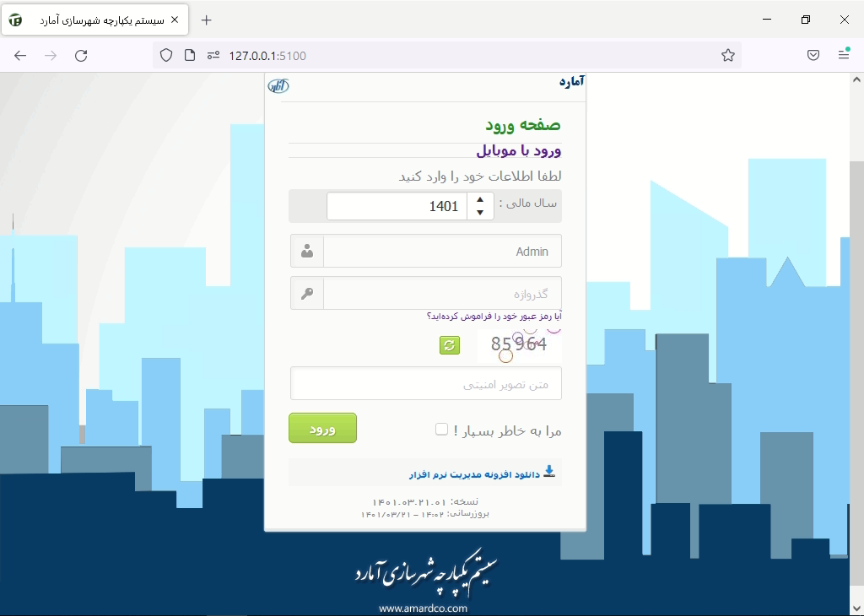
در قسمت physical path آدرس پوشه ی Publish را انتخاب می‌کنیم



در قسمت Ip Address، IP سرور را وارد می‌کنیم و یک شماره port به دلخواه وارد می‌کنیم



پس از راه اندازی سایت مورد نظر روی مرورگر رفته و آدرس تعریف شده به همراه شماره پورت موردنظر را وارد می‌کنیم. به عنوان مثال روی مرورگر فایرفاکس آدرس <http://192.168.10.3:5100> را وارد می‌کنیم .



### راه اندازی هدف ارزیابی

* تغییر كلمه‌ی عبور پیش‌فرض مدیر سامانه
* تنظیم سال مالی
* تنظیم تنظیمات اولیه شامل نام چاپ و اطلاعات پایه