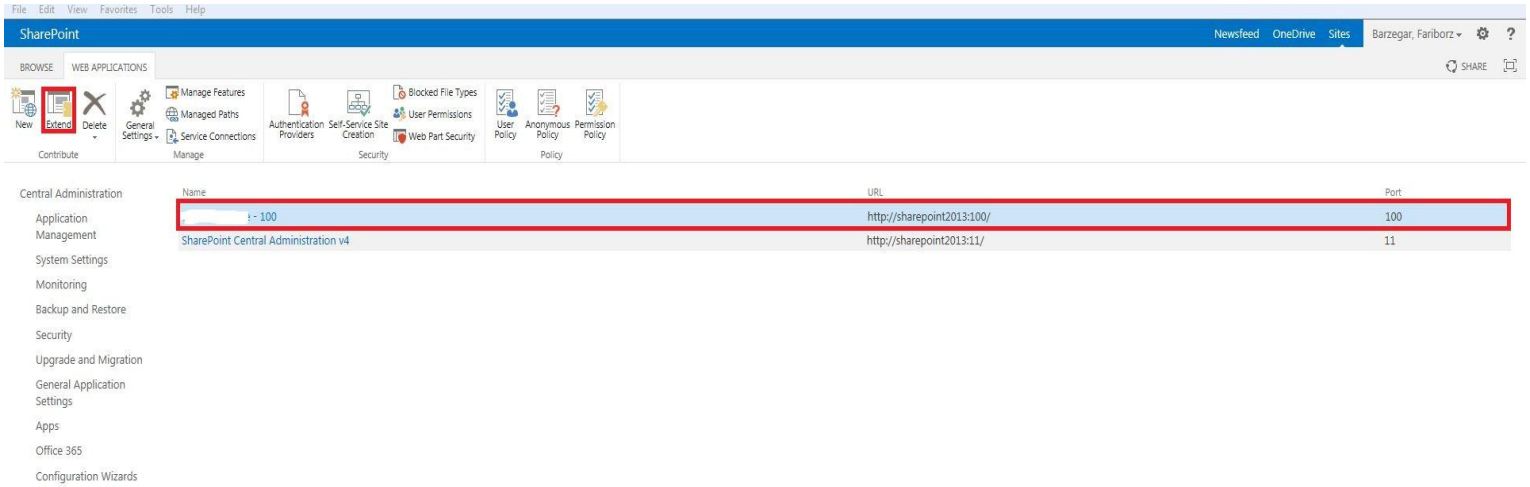


## Extend کردن یک web Application در SharePoint 2013

### Central Administration – Application Management – Manage Web Applications

انتخاب Web Application مورد نظر و کلیک بر روی دکمه Extend (مطابق شکل زیر)



The screenshot shows the SharePoint Central Administration interface. The 'WEB APPLICATIONS' section is active, and the 'Extend' button is highlighted with a red box. Below the navigation pane, a table lists the web applications. The first row is highlighted with a red box, showing the application name, URL, and port.

Name	URL	Port
:- 100	http://sharepoint2013:100/	100
SharePoint Central Administration v4	http://sharepoint2013:11/	11

بعد از کلیک بر روی Extend پنجره جدیدی باز میشود ، مطابق شکل زیر میتوان فیلدهای آن را پر کرد .

## Extend Web Application to Another IIS Web Site

### IIS Web Site

Choose between using an existing IIS web site or create a new one to serve the Microsoft SharePoint Foundation application.

If you select an existing IIS web site, that web site must exist on all servers in the farm and have the same name, or this action will not succeed.

If you opt to create a new IIS web site, it will be automatically created on all servers in the farm. If an IIS setting that you wish to change is not shown here, you can use this option to create the basic site, then update it using the standard IIS tools.

Use an existing IIS web site

Default Web Site

Create a new IIS web site

Name

extended web Application

Port

80

Host Header

portal.xyz.net

Path

C:\inetpub\wwwroot\wss\VirtualDirectories\po

### Security Configuration

If you choose to use Secure Sockets Layer (SSL), you must add the certificate on each server using the IIS administration tools. Until this is done, the web application will be inaccessible from this IIS web site.

Allow Anonymous

Yes

No

Use Secure Sockets Layer (SSL)

Yes

No

### Claims Authentication Types

Choose the type of authentication you want to use for this zone.

Negotiate (Kerberos) is the recommended security configuration to use with Windows authentication. If this option is selected and Kerberos is not configured, NTLM will be used. For Kerberos, the application pool account needs to be Network Service or an account that has been configured by the domain

any application pool account and with the default domain configuration.

Basic authentication method passes users' credentials over a network in an unencrypted form. If you select this option, ensure that Secure Sockets Layer (SSL) is enabled.

ASP.NET membership and role provider are used to enable Forms Based Authentication (FBA) for this Web application. After you create an FBA Web application, additional configuration is required.

Trusted Identity Provider Authentication enables federated users in this Web application. This authentication is Claims token based and the user is redirected to a login form for authentication.

[Learn about configuring authentication.](#)

Enable Windows Authentication

Integrated Windows authentication

NTLM

Basic authentication (credentials are sent in clear text)

Enable Forms Based Authentication (FBA)

ASP.NET Membership provider name

ASP.NET Role manager name

Trusted Identity provider

There are no trusted identity providers defined.

قسمتهایی را که با رنگ قرمز مشخص شده است را میتوانید به دلخواه تغییر دهید.

### Sign In Page URL

When Claims Based Authentication types are enabled, a URL for redirecting the user to the Sign In page is required.

[Learn about Sign In page redirection URL.](#)

Default Sign In Page

Custom Sign In Page

### Public URL

The public URL is the domain name for all sites that users will access in this SharePoint Web application. This URL domain will be used in all links shown on pages within the web application. By default, it is set to the current servername and port. <http://go.microsoft.com/fwlink/?LinkId=114854>

URL

http://portal.xyz.net:80

Zone

Intranet

OK

Cancel

بعد از این کار یک سایت به نام Extended Wep Application در IIS سرور شیروینت ساخته میشود ، و در قسمت Configure Alternate Access Mappings یک رکورد اضافه میشود .

حال برای اینکه این آدرس در سطح سازمان و توسط دیگر کاربران قابل استفاده باشد نیاز به ساختن یک Alias Record در DNS می باشد .

ممکن است بعد از این مراحل و هنگام وارد کردن URI در Internet Explorer نیاز به وارد کردن Username & Password باشد . با رفتن به Security Tab در Internet Options و انجام یک یا هر دو تنظیمات زیر (یا تنظیمات دیگری در قسمت Security) میتوان این مشکل را برطرف کرد .

