**Configuration Process for allowing iOS devices to access NTLM Authenticated SharePoint 2013 Sites**

This process details how to extend a .

**SharePoint Configuration**

Verify that the target Web Application already exists and is configured to allow Active Directory NTLM Authentication on the Default zone.

Verify what Zones are available in the existing Web Application.

**Prerequisite Configuration**

Prior to making IS changes, you will need to make sure an additional IP address is associated with your web server. If running a single SharePoint server, you will need to do the following:

* Open a Command Prompt as Administrator
* Use the following command:

**Netsh int ipv4 add address <Interface Name> <ip address> <subnet mask> skipassource=true**

Example:

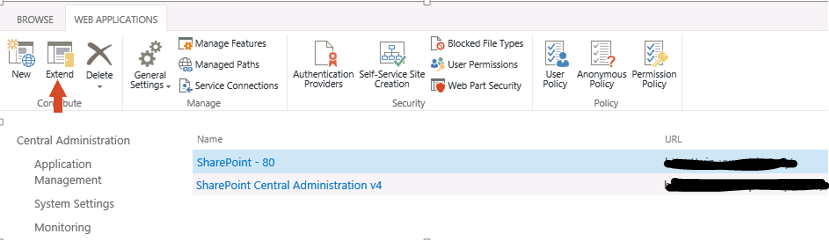
**Netsh int ipv4 add address “Local Area Connection” 192.168.1.1 255.255.255.0 skipassource=true**

This will add the secondary IP addresses to the Network Adapter without registering in DNS. See TechNet Article for additional information - <http://support2.microsoft.com/kb/975808>

If you are running a Medium-to-Large SharePoint farm with multiple WFEs, you will need to repeat this process on each server. This may also require additional configuration within the Netscalar interface to properly redirect to the additional IP addresses.

**Extend the Web Application**

On the SharePoint Central Administration Server:

1. Log in to **SharePoint Central Administration** and select the '**Application Management**' portal.
2. In the '**Web Applications**' section, select '**Manage web applications**'.
3. Select the required SharePoint site and click '**Extend**'.   
     
   

Please note that the web application will be configured to use Claims authentication.

**IIS Web Site**

1. The '**Extend Web Application to Another IIS Web Site**' screen appears. Select '**Create a new IIS web site**'
2. Fill out the details of the new site:
   * Add a meaningful name that describes the purpose of the site – for example, “Classic Web App – Extended”.
   * Ensure that the IIS web site is assigned a unique port that is not currently in use on your SharePoint server.
   * Host Header stays blank
   * Ensure that '**Allow Anonymous**' is set to '**No**'.
   * Ensure that '**Use Secure Sockets Layer (SSL)**' is set to '**Yes**' if you plan to use https, else set this to **No**.
3. Make a note of the '**Zone**' that is set for the '**Load Balanced URL**'. You will need to know this zone in point 4. of step 2
4. Click '**OK**'.

Claims Authentication Types

* Enable Windows Authentication – Check the box to select
* Integrated Windows Authentication – Uncheck the box
* Basic authentication – Check the box to select
* Enable Forms Based Authentication (FBA) – leave box unchecked
* Trusted Identity Provided – leave box unchecked

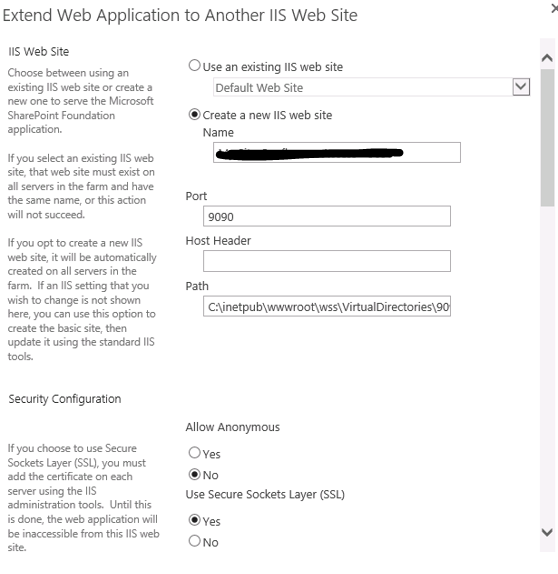
Sign In Page URL

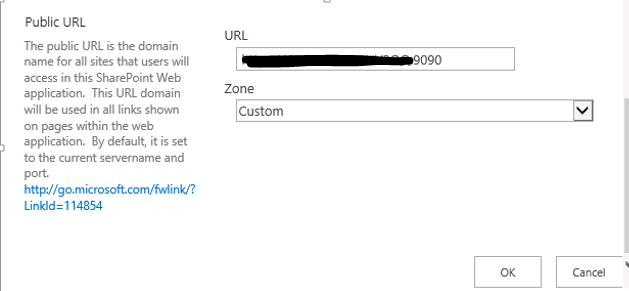
* Default Sign In Page – select

Public URL

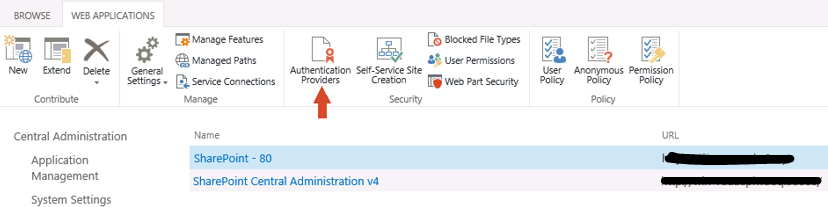
* URL – use the URL of the site being extended – ***https://classic.domain.com:<port number>***
* Zone – Custom (as available)

Click **OK**.





**Step 2: Configure the IIS Authentication Providers**

1. Go back to SharePoint's '**Manage web applications**' section.
2. Select the required SharePoint site and click '**Authentication Providers**'.   
     
   
3. The '**Authentication Providers**' screen appears. Click the name of the **Zone** (such as, 'Intranet' or 'Internet') that you used to extend the SharePoint site in step 1.
4. The '**Edit Authentication**' screen appears. Ensure that '**Integrated Windows authentication**' is not selected and '**Basic authentication (password is sent in clear text)**' is selected.
5. Click '**Save**'.

**SSL will secure the password information**

***Additional IIS Configuration***

Open IIS Manager

Verify Basic Authentication is enabled and properly configured

* In Connections pane, expand Server
* Expand Sites folder
* Click on new extended site – “Classic Web App – Extended”
* Select Authentication icon in IIS section (in center pane), then click **Open Feature** in Actions pane.
* Verify Windows Authentication is Disabled and Basic Authentication is enabled
* Select Basic Authentication, then click **Edit** in the Actions pane
* Type the Active Directory Domain in both text fields, “<domain.com>”, and click **OK**.

Update IP Address Bindings for Extended IIS Site

* Ensure the Extended Site is selected in the left Connections pane
* Click **Bindings**, in the Actions pane
* Select the https entry and click the **Edit** button
* Type in the “additional” IP address in the IP Address filed and type 443 in the Port text window
* Select the certificate that is already associated with the primary site and click **OK**.
* Click **Close**.

**Netscalar Configuration**

Netscaler Changes

1. Create new server corresponding with new IP address
2. Create new SSL service binding to corresponding server
3. Create LB VServer corresponding to the service
4. Create Content Switching Server for target URL – ***“classic.domain.com”***
5. Create Content switching policy
6. Bind LB VServer to the corresponding CS Server and policy