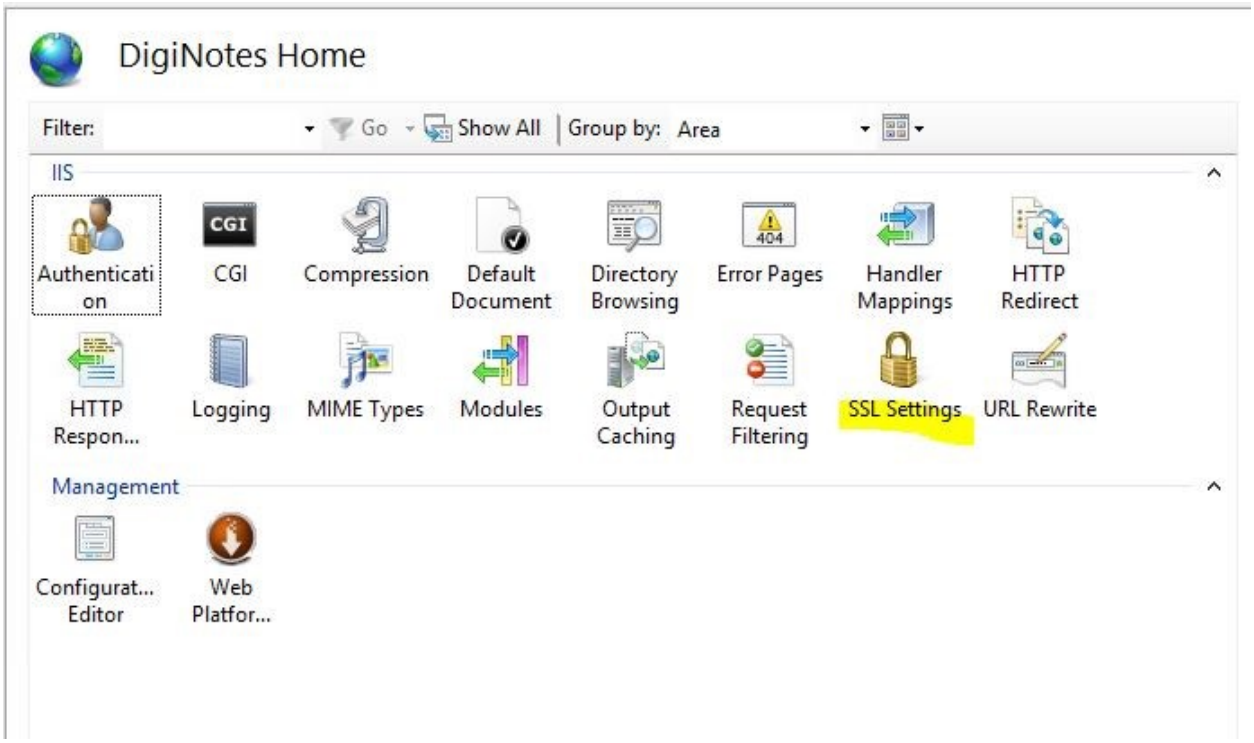
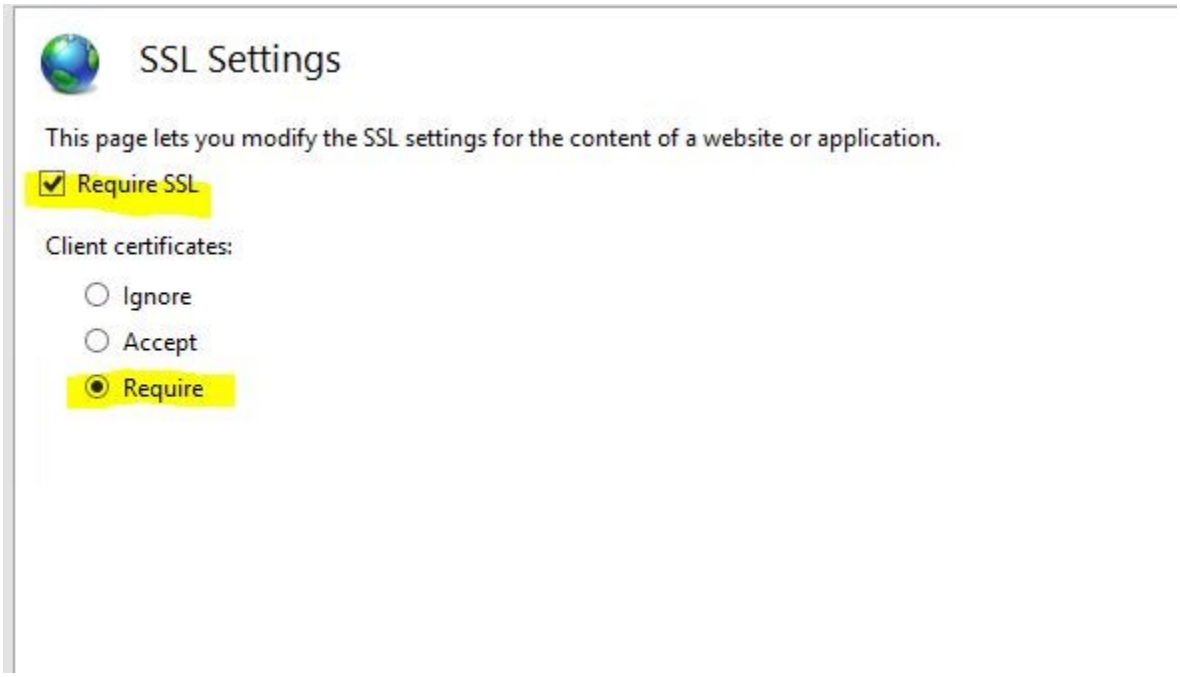
Client Authentication With IIS 8 (Windows Server 2012) Many to One Mapping.

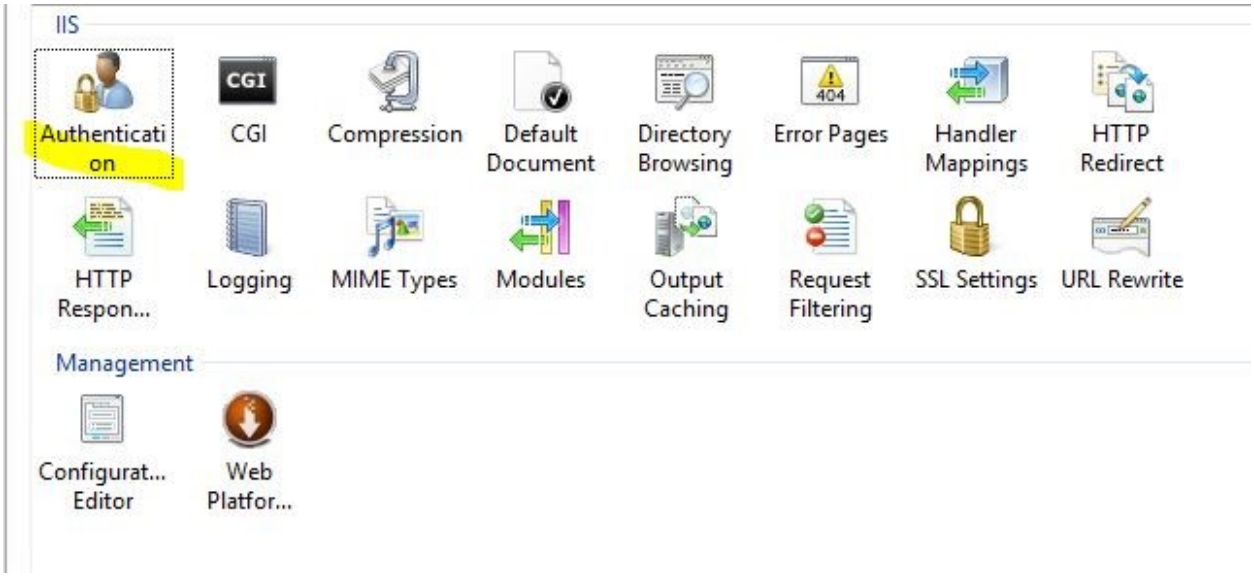
When setting up Client Authentication I did IIS Specific rather than Active Directory. To set this up, you will first need to set your site to require SSL. Open IIS and expand the server until you see your website. Select your site, and then select SSL Settings.



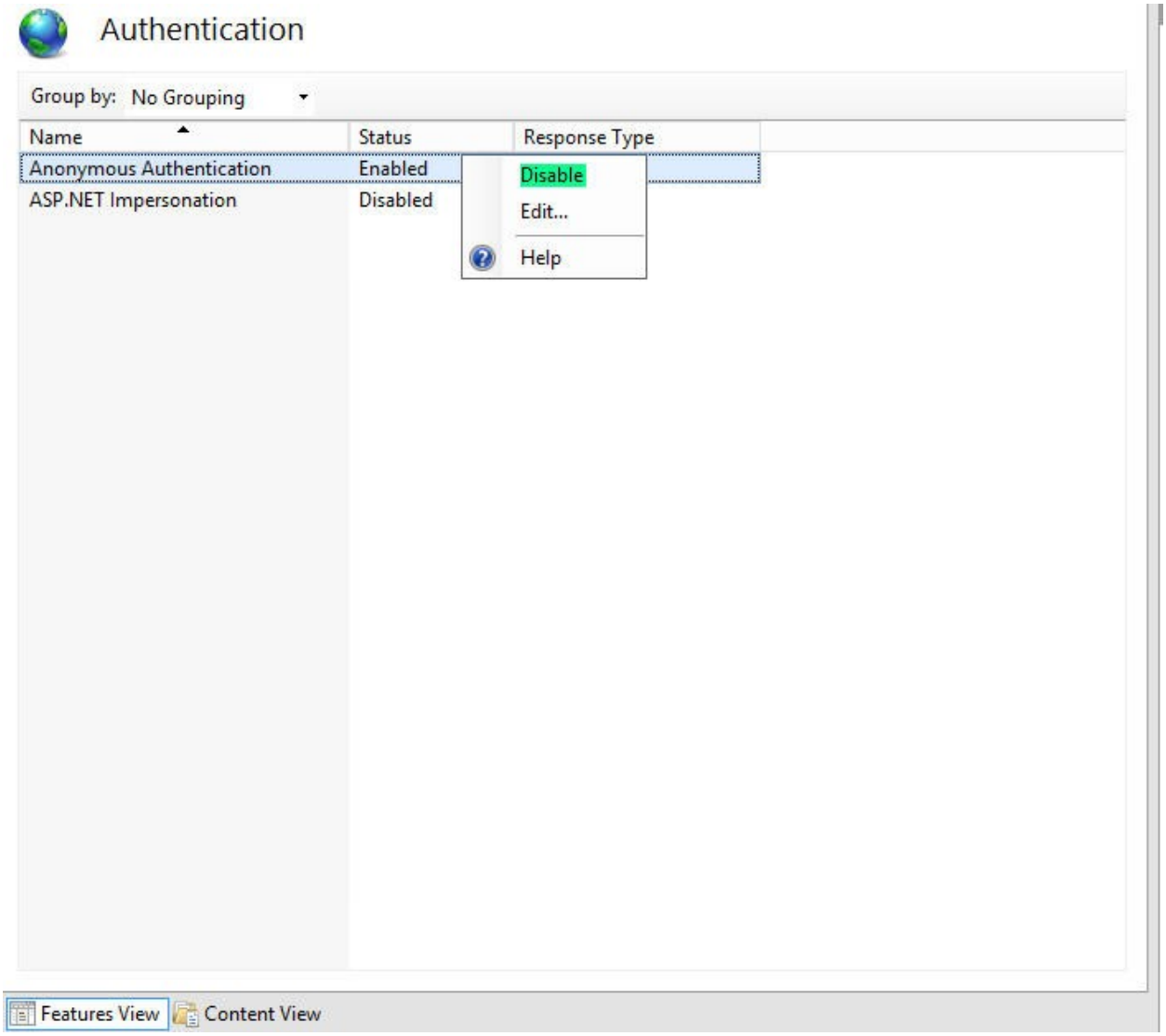
Then select the check box to Require SSL, then under Client certificates, select Require. This forces the site to require Client authentication in order to access the contents.



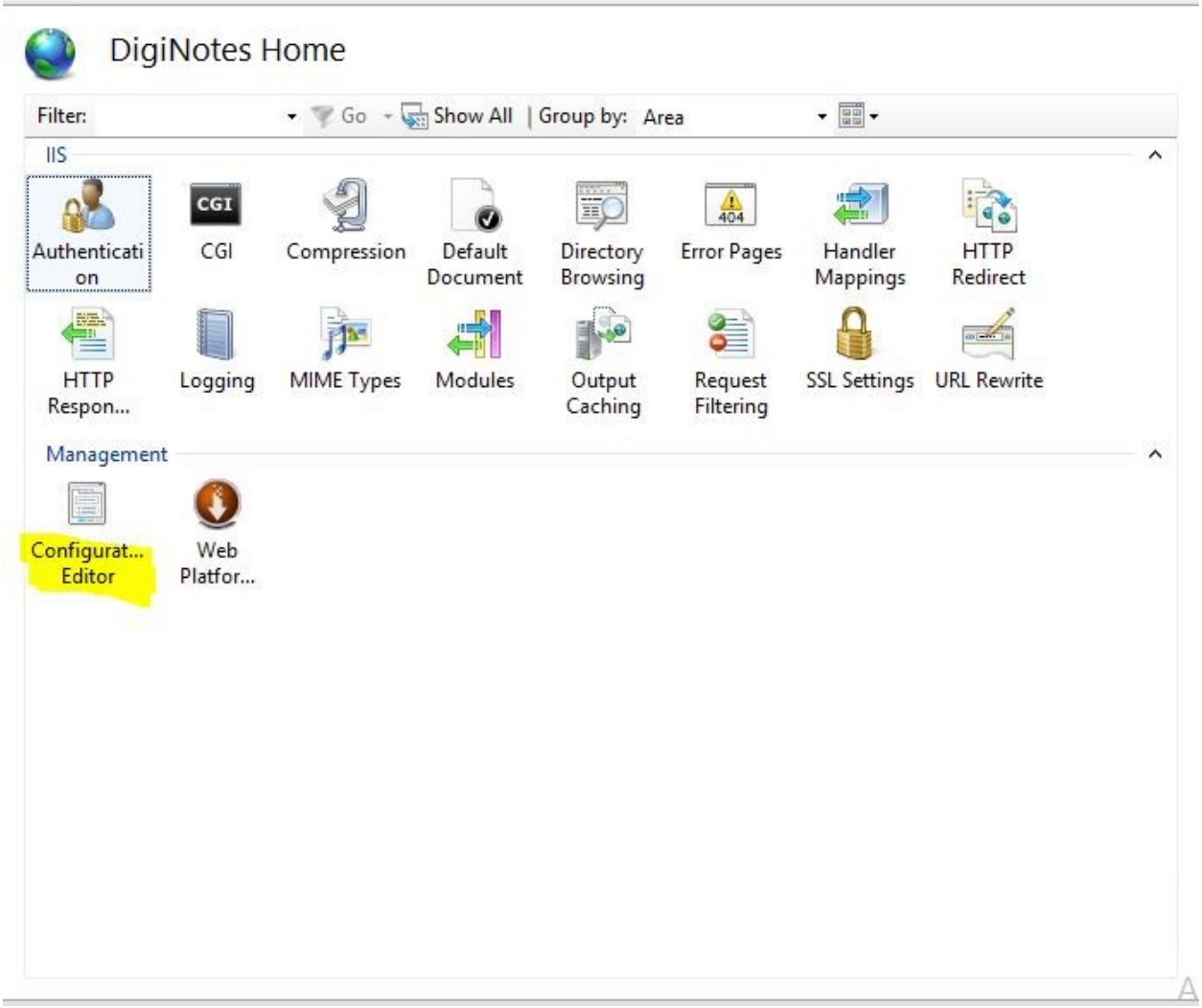
By default your site has Anonymous Authentication enabled. This allows anyone to access the site. So you will need to disable this. Go back to your site management section and select Authentication.



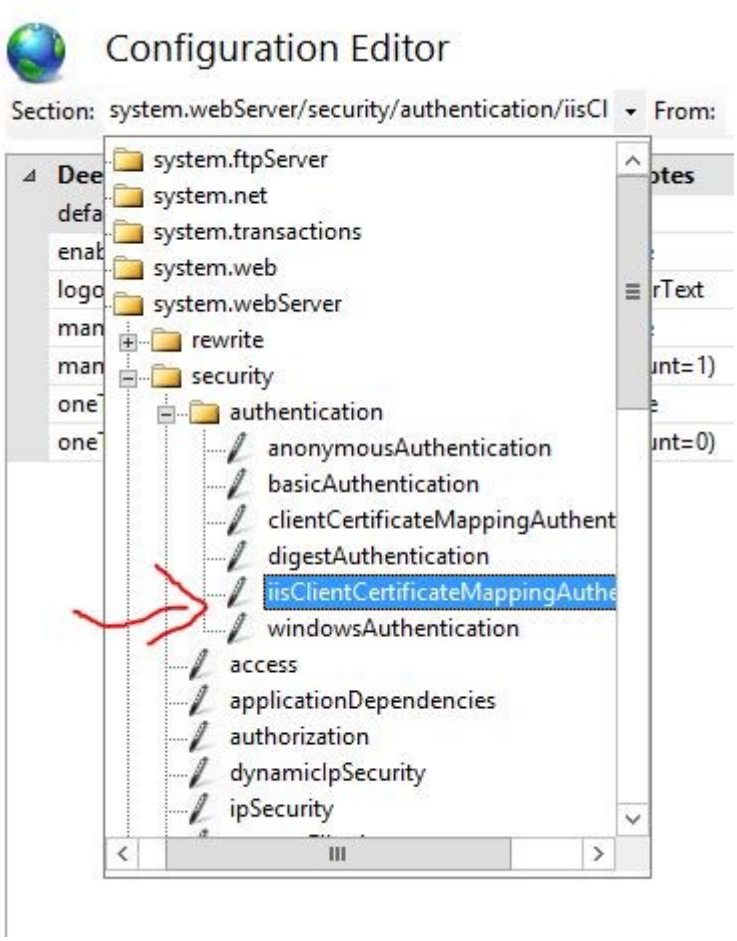
Right click Anonymous Authentication and then select Disable.



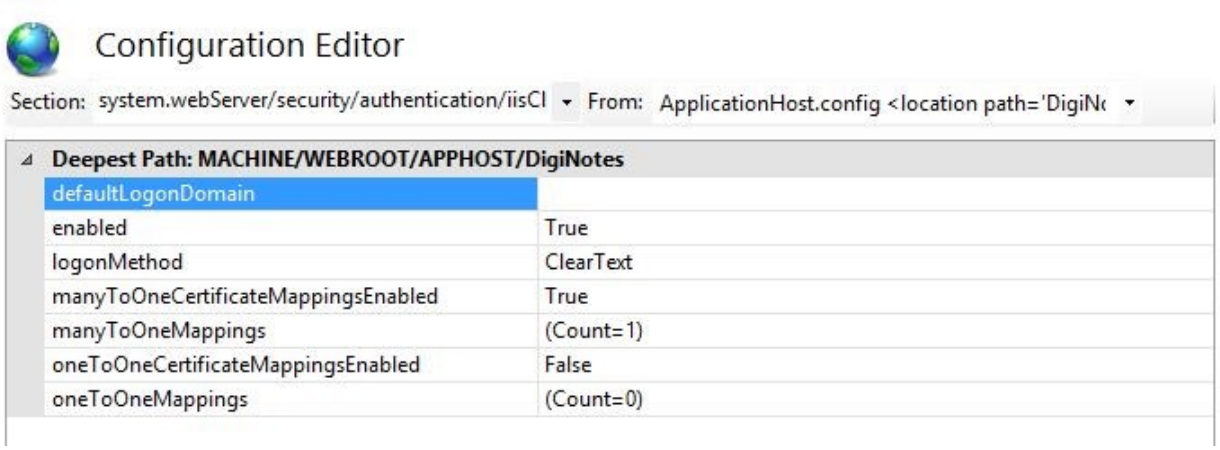
Now the basics are set up. At this point you need to tell the server what to allow, or if it's easier what not to allow. Go to your site's management page in IIS and select Configuration Editor.



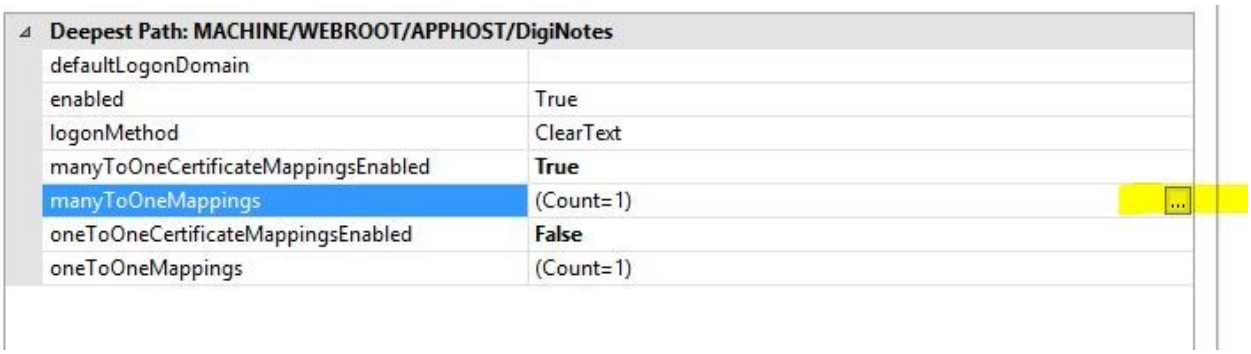
In the Configuration Editor you can select any security sections. For this specific tutorial we want to go to the system.webServer>security>authentication>iisClientMappingAuthentication.



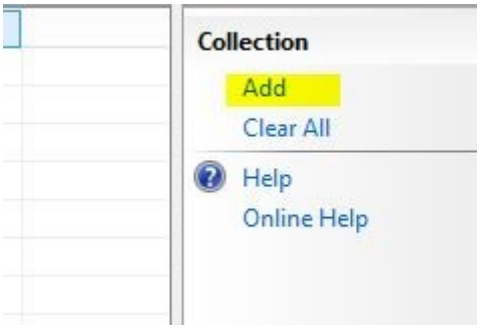
For Many to One authentication, set oneToOneCertificateMappingsEnabled to false, and manyToOneCertificateMappingsEnabled to true.



Next to manToOneMappings (Count=0) select the "..." button.



The to the right of the new window select "Add".

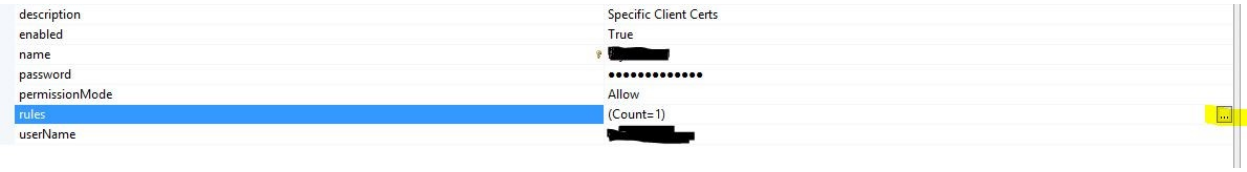


At the bottom of the window are new fields to enter information into:

- The Description is an identifier of the rule.
- The enabled field is to specify whether the rule should be used or not.
- The name is the name of the given rule (Another identifier)
- The password is the password for a valid Windows User on the server
- The permissionMode is used for whether you want to grant access to those that meet the given roles in "rules" or you want to deny them access.
- The rules section is where you define the specific criteria that this Mapping needs to look for.
- The usernName is the valid Windows users for this Mapping.

description	
enabled	True
name	
password	
permissionMode	Allow
rules	(Count=0)
userName	

Now that you have the Mapping created, it's time to create some rules for the Mapping. Select the "..." button next to rules.



Again select "Add" in the new window, and you will be presented with a few options.

- The certificateField can be either Subject or Issuer
- The certificateSubField is used to dictate which field on a certificate that will be used for filtering. Any of the Active Directory fields can be used
    1. CN = commonName (for example, "John Doe")
    2. OU = organizationalUnitName (for example, "Support")
    3. O = organizationName (for example, "Digicert")
    4. L = localityName (for example, "Lehi")
    5. S = stateOrProvinceName (for example, "UT")
    6. C = countryName (for example, "US")
- The compareCaseSensitive is a way to enable strict comparison to the matchCriteria, or make it less strict.
- The matchCriteria is where you dictate what should be matched for this rule. If you were requiring a specific CN in the certificateSubField this is where the exact CN is dictated.

certificateField	Subject
certificateSubField	CN
compareCaseSensitive	True
matchCriteria	

At this point you can close both new windows and select Apply in the Configuration Editor to apply the rules. And you are done. You have successfully enabled Client Authentication for your IIS server using Many to One Mapping. The advantage to this is that you can restrict or enabled access to a range of clients. If you rather restrict to one or few individuals then you may want to consider One to One Mapping.