Configuring Chrome and Firefox for Windows Integrated Authentication

Windows Integrated Authentication allows a users' Active Directory credentials to pass through their browser to a web server. Windows Integrated Authentication is enabled by default for Internet Explorer but not Google Chrome or Mozilla Firefox. Users who use the non-Microsoft browsers will receive a pop-up box to enter their Active Directory credentials before continuing to the website. This adds additional steps and complexity for users.

How to enable Windows Integrated Authentication for Google Chrome and Mozilla Firefox:

Configuring Delegated Security for Mozilla Firefox

To configure Firefox to use Windows Integrated Authentication:

1. Open Firefox.
2. In the address bar type about:config
3. You will receive a security warning. To continue, click I'll be careful, I promise.

4. You will see a list of preferences listed. Find the settings below by browsing through the list or searching for them in the search box. Once you have located each setting, update the value to the following:

Setting	Value **
network.negotiate-auth.delegation-uris	IISServer.domain.com or just the server name
network.automatic-ntlm-auth.trusted-uris	IISServer.domain.com or just the server name
network.automatic-ntlm-auth.allow-proxies	True
network.negotiate-auth.allow-proxies	True

** MyIISServer.domain.com should be the fully qualified name of your IIS server that you are setting up the Windows Integrated Authentication too.

Negotiate authentication is not supported in versions of Firefox prior to 2006.

Configuring Delegated Security in Google Chrome

You can use three methods to enable Chrome to use Windows Integrated Authentication. Your options are the command line, editing the registry, or using ADMX templates through group policy. If you choose to use the command line or edit the registry, you could use Group Policy Preferences to distribute those changes on a broader scale. Below are the steps for the three methods:

To use the command line to configure Google Chrome:

Start Chrome with the following command:

```
Chrome.exe –auth-server-whitelist=”IISSERVER.DOMAIN.COM”
–auth-negotiate-delegatewhitelist=”IISSERVER.DOMAIN.COM”
–auth-schemes=”digest,ntlm,negotiate”
```

To modify the registry to configure Google Chrome:

Configure the following registry settings with the corresponding values:

Registry

AuthSchemes

Data type: String (REG_SZ)

Windows registry location: SoftwarePoliciesGoogleChromeAuthSchemes

Mac/Linux preference name: AuthSchemes

Supported on: Google Chrome (Linux, Mac, Windows) since version 9

Supported features: Dynamic Policy Refresh: No, Per Profile: No

Description: Specifies which HTTP Authentication schemes are supported by Google Chrome. Possible values are ‘basic’, ‘digest’, ‘ntlm’ and ‘negotiate’. Separate multiple values with commas. If this policy is left not set, all four schemes will be used.

Value: “basic,digest,ntlm,negotiate”

AuthServerWhitelist

Data type: String (REG_SZ)

Windows registry location: SoftwarePoliciesGoogleChromeAuthServerWhitelist
Mac/Linux preference name: AuthServerWhitelist
Supported on: Google Chrome (Linux, Mac, Windows) since version 9
Supported features: Dynamic Policy Refresh: No, Per Profile: No
Description: Specifies which servers should be whitelisted for integrated authentication. Integrated authentication is only enabled when Google Chrome receives an authentication challenge from a proxy or from a server which is in this permitted list. Separate multiple server names with commas. Wildcards (*) are allowed. If you leave this policy not set Chrome will try to detect if a server is on the Intranet and only then will it respond to IWA requests. If a server is detected as Internet then IWA requests from it will be ignored by Chrome.
Value: "IISSERVER.DOMAIN.COM"

AuthNegotiateDelegateWhitelist
Data type: String (REG_SZ)
Windows registry location: SoftwarePoliciesGoogleChromeAuthNegotiateDelegateWhitelist
Mac/Linux preference name: AuthNegotiateDelegateWhitelist
Supported on: Google Chrome (Linux, Mac, Windows) since version 9
Supported features: Dynamic Policy Refresh: No, Per Profile: No
Description: Servers that Google Chrome may delegate to. Separate multiple server names with commas. Wildcards (*) are allowed. If you leave this policy not set Chrome will not delegate user credentials even if a server is detected as Intranet.
Example Value: "IISSERVER.DOMAIN.COM"

***To use ADM/ADMX templates through Group Policy to configure Google Chrome*:**

1. Download Zip file of ADM/ADMX templates and documentation from: http://www.chromium.org/administrators/policy-templates.
2. Add the ADMX template to your central store, if you are using a central store.

3. Configure a GPO with your application server DNS host name with **Kerberos Delegation Server Whitelist** and **Authentication Server Whitelist** enabled.

Each of these three methods achieve the same results for configuring Google Chrome for Windows Integrated Authentication. The method that is best for you will depend on how your organization is set up. Personally, I would use the command line or the registry if you are deploying across an enterprise. You can easily distribute a shortcut on the user's desktop with the command and distribute that with Group Policy preferences. If you choose to use the registry method, that is able to be distributed with Group Policy.

With a variety of third-party browsers available, many users will receive a pop-up box to enter their Active Directory credentials before continuing to an IIS hosted web application. This leads to additional steps, complexity and confusion for many end-users. By setting up Windows Integrated Authentication into Chrome and Firefox, you will be able to give your users the greatest amount of flexibility for their choice of browser as well as ease of use with your web-based applications.