Configuring your browser for Windows Authentication

In order to be able to use Windows Authentication to log into the IDERA Dashboard, you have to configure your browser settings.

Internet Explorer 9,10,11

To configure these versions of Internet Explorer , follow these steps:

- 1. Go to Internet Options.
- 2. Click Security.
- 3. Click Internet and then Custom Level.

Internet Options						
General Security Privacy Content Connections Programs Advanced						
Select a zone to view or change security settings.						
Internet Local intranet Trusted sites Restricted sites						
Internet						
This zone is for Internet websites, except those listed in trusted and restricted zones.						
Security level for this zone						
Allowed levels for this zone: Medium to High						
Medium-high Appropriate for most websites Prompts before downloading potentially unsafe content Unsigned ActiveX controls will not be downloaded						
Enable Protected Mode (requires restarting Internet Explorer)						
Custom level Default level						
Reset all zones to default level						
OK Cancel Apply						

4. Go to Scripting/Active scripting and make sure **Enable** is selected.

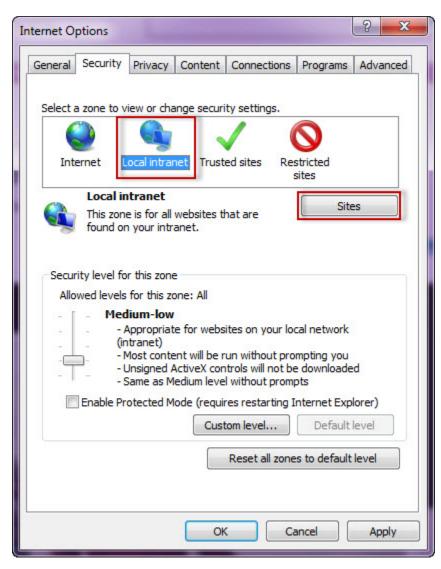
5. Then go to User Authentication/Logon and make sure Automatic logon with current user name and password is selected.

6. Click OK.

ttings		
	O Disable	
	Enable	
	Websites in less privileged web content z	one can navigate in
	Disable	
	Enable	
1.00	Prompt	
SC SC	ripting	
Ş	Active scripting	
	O Disable	
	Enable	
-	Prompt	
	Allow Programmatic clipboard access Disable	
	Enable	
	Prompt	
(=e	Allow status har undates via script	-
٠ 📃	III	
Takes	effect after you restart your computer	
set cu	stom settings	
set to	: Medium-high (default)	 Reset
	(Hedidin High (denadic)	Resettin
		K Cancel
	0	Cancel

ettings			
) Disable		
0	Enable		
\$ E	nable XSS filter		
0	Disable		
	Enable		
\$ S	cripting of Java applets		
0	Disable		
	Enable		
0) Prompt		
	Authentication		
86 L	ogon		
0	Anonymous logon		
	Automatic logon only in In		1
			password
0	Prompt for user name and	u password	-
•			•
*Takes eff	fect after you restart your co	omputer	
eset custo	m settings		
eset to:	Medium-high (default)	•	Reset
		C	
		OK	Cancel

7. Click Local intranet and then Sites.



8. Type the URL you are going to use (e.g. http://sqlj01) and click $\boldsymbol{Add}.$

9. Click Close.

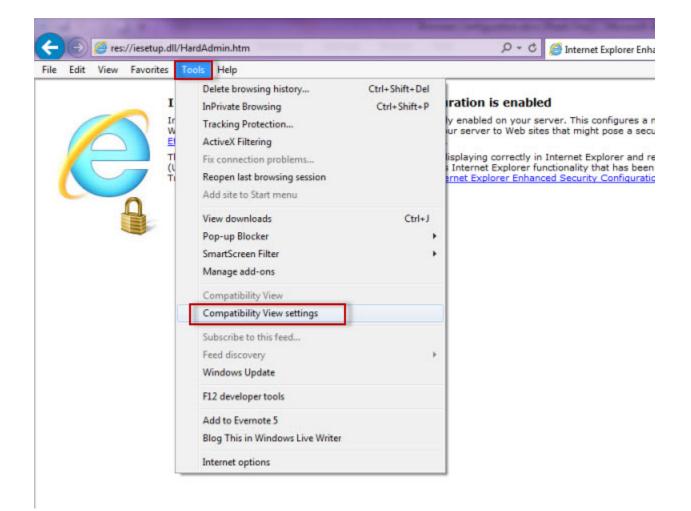
Local intranet					
You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.					
Add this website to the zone: http://sqlj01 Websites:					
Remove					
Require server verification (https:) for all sites in this zone					
Close					

10. Go to Advanced and make sure Enable Integrated Windows Authentication is selected.

11. Click **OK**.

Internet Options					? ×
General Security	Privacy	Content	Connections	Programs	Advanced
Settings					
Check	for signal t save end Tempora DOM Sto Enhance Integrat SmartSci Strict P3	tures on do crypted pag ry Internet orage <u>d Protecte</u>	Files folder wh d Mode* S Authenticatio pport	nen browser	is dc
	SL 2.0 SL 3.0				E
	LS 1.0				-
 Use I 	LS 1.1				•
*Takes effect	after you	restart you	r computer		
Reset Internet Ex	plorer set	tings	Restore	advanced s	ettings
Resets Interne condition. You should only				Kes	et
		Ok	Ca	ancel	Apply

12. Go to Tools in the menu bar, and select Compatibility View Settings.



13. In the Compatibility View Settings window make sure Display intranet sites in Compatibility View is selected.

14. Click Close.

You can add and remove websites to be disp Compatibility View.	layed in
Add this website:	Add
	Auu
Websites you've added to Compatibility View:	_
 Display all websites in Compatibility View Display intranet sites in Compatibility View 	
Download updated compatibility lists from Microsof Learn more by reading the <u>Internet Explorer priva</u>	
	Close

Configuring Google Chrome and Mozilla Firefox

To configure Google Chrome, you can go to the following link: http://dev.chromium.org/developers/design-documents/http-authentication.

To configure Mozilla Firefox, view the following steps:

- 1. Open your Mozilla Firefox browser and type about:config .
- 2. Click I'll be careful, I promise!.

about:config × +		
Firefox about:config		V C S - about:config
	Char appl	is might void your warranty! nging these advanced settings can be harmful to the stability, security, and performance of this cation. You should only continue if you are sure of what you are doing. Show this warning next time

3. Search and double click network.negotiate-auth.delegation-uris.

about:config × +			V
Search:			
Preference Name	▲ Status	Туре	Value
network.negotiate-auth.allow-insecure-ntlm-v1	default	boolean	false
network.negotiate-auth.allow-insecure-ntlm-v1-https	default	boolean	true
network.negotiate-auth.allow-non-fqdn	default	boolean	false
network.negotiate-auth.allow-proxies	default	boolean	true
network.negotiate-auth.delegation-uris	default	string	
network.negotiate-auth.gsslb	default	string	
network.negotiate-auth.trusted-uris	default	string	
network.negotiate-auth.using-native-gsslib	default	boolean	true

4. Type https://localhost:9291. Click OK .

5. Search network.automatic-ntlm-auth.trusted-uris, double-click it and type the same value as before: https://localhost:9291. Click OK.

6. Close all instances of the Firefox browser to make the changes effective. Launch the browser again and access the application.

IDERA Dashboard provides an integrated user experience for the IDERA products in your environment.

IDERA | Products | Purchase | Support | Community | Resources | About Us | Legal