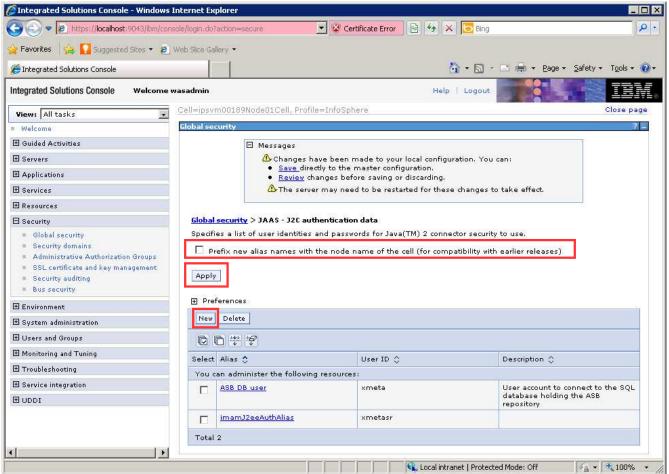
CREATING AUTHENTICATION DATA

Standardization Rules Designer data sources use JAAS (Java Authentication and Authorization Service) J2C (Java 2 Connector) authentication data for connection credentials. This data must be created before configuring Standardization Rules Designer data sources. Complete the following steps to create the JAAS J2C authentication data:

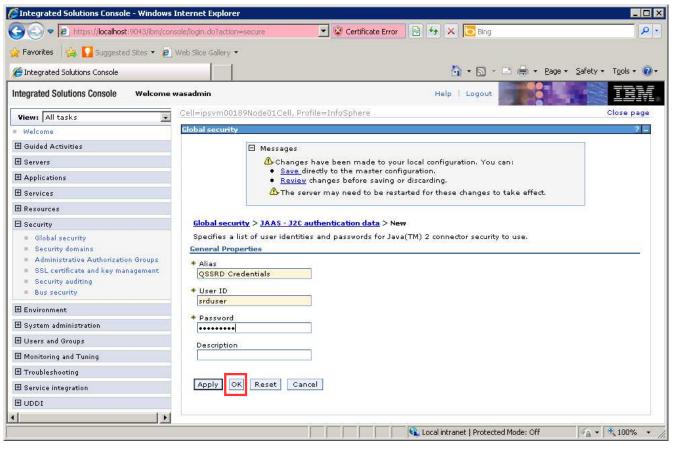
- 1. Login to the IBM WebSphere Application Server Administrative Console.
- 2. Expand the **Security** node in the left pane.
- 3. Click Global Security.
- 4. Expand the Java Authentication and Authorization Service node in the right pane.
- 5. Click J2C authentication data.

Favorites 🛛 🙀 🚺 Suggested Sites 👻 🔊	Web Slice Gallery 🕶	
Integrated Solutions Console		🟠 🔹 🔂 🔹 📾 🔹 Page 🔹 Safety 🔹 Tools 🔹 🌘
tegrated Solutions Console Welcome	wasadmin	Help Logout
View: All tasks	Cell=ipsvm00189Node01Cell, Profile=InfoSphere	Close page
Welcome	Global security	
B Guided Activities	Global security	
8 Servers	Use this panel to configure administration and the default application securi	ity policy. This security configuration applies to the secu
8 Applications	functions and is used as a default security policy for user applications. Security domains can be defined to override and customize the applications.	
] Services		
B Resources	Security Configuration Wizard Security Config	juration Report
3 Security	Administrative security	Authentication
Global security Security domains Administrative Authorization Groups SSL certificate and key management Security auditing	Enable administrative security Administrative user roles Administrative aroup roles. Administrative authentication	Authentication mechanisms and expiration C LTPA C Kerberos and LTPA
 Bus security 	Enable application security	Kerberos configuration
] Environment	Java 2 security Authentication cache se □ Use Java 2 security to restrict application access to local resources	C SWAM (deprecated): No authenticated comm Authentication cache settings
B System administration		₩eb and SIP security
E Users and Groups		RMI/IIOP security
B Monitoring and Tuning		Java Authentication and Authorization Service
9 Troubleshooting		
B Service integration	User account repository	 System logins J2C authentication data
	Current realm definition Standalone custom registry	Use realm-qualified user names
	Available realm definitions Standalone custom registry 🗸 Configure Set as current	Security domains External authorization providers

- 6. Uncheck Prefix new alias names with the node name of the cell...
- 7. Click Apply. Do not click Save at this time.
- 8. Click New.



- 9. Enter QSSRD Credentials in the Alias field.
- 10. Enter the Standardization Rules Designer database user name in the User ID field.
- 11. Enter the Standardization Rules Designer database user password in the **Password** field.
- 12. Enter an optional description in the **Description** field if desired.
- 13. Click **OK**.
- 14. Click Save.



The Standardization Rules Designer authentication data creation step is now complete.