

17. Port0, socket name unavailable, RMI/IIOP security

When our SCM staff tries to execute PSCS Trigger, he will face the below exception if the admin console, RMI/IIOP security should have the recommended settings as provided in the below solution.

Exception:

com.ibm.rmi.corba.ClientDelegate _createRequest:1773 P=103829:O=0:CT ORBRas[default]
org.omg.CORBA.TRANSIENT: java.net.ConnectException: **The socket name is not available on this system.**
(connect failed):host=10.31.39.151,port=0 vmcid: IBM minor code: E02 completed: No for com.ibm.rmi.IOR@48e36c99

Solution:

In CSIV2 inbound settings (Admin Console->Security->GlobalSecurity->RMI/IIOP security) and set as below:

Client certificate authentication = required

Transport = SSL-Supported

In CSIV2 outbound settings (Admin Console->Security->GlobalSecurity->RMI/IIOP security) and set as below:

Client certificate authentication = required

Transport = SSL-Supported

Screenshots

The screenshot displays the 'Global security > CSIV2 inbound communications' configuration page. The page is divided into several sections:

- CSIV2 Attribute Layer:** Includes a checkbox for 'Propagate security attributes' (checked) and 'Use identity assertion' (unchecked). There is a text field for 'Trusted identities'.
- CSIV2 Transport Layer:** Includes a dropdown for 'Client certificate authentication' set to 'Required' and a dropdown for 'Transport' set to 'SSL-supported'.
- SSL settings:** Includes radio buttons for 'Centrally managed' (selected) and 'Use specific SSL alias'. Under 'Centrally managed', there is a link to 'Manage endpoint security configurations'. Under 'Use specific SSL alias', there is a dropdown for 'CellDefaultSSLSettings' and a link to 'SSL configurations'.
- CSIV2 Message Layer:** Includes a dropdown for 'Message layer authentication' set to 'Supported'. Below it, a section 'Allow client to server authentication with:' contains checkboxes for 'Kerberos' (unchecked), 'LTPA' (checked), and 'Basic authentication' (checked).
- Additional Properties:** Includes a text field for 'Login configuration' set to 'RMI_INBOUND'.
- Related Items:** Includes a link to 'Trusted authentication realms - inbound'.

At the bottom of the page, there are buttons for 'Apply', 'OK', 'Reset', and 'Cancel'.

Global security > CSIV2 outbound communications

Use this panel to specify authentication settings for requests that are sent and transport settings for connections that are initiated by the server using the Object Management Group (OMG) Common Secure Interoperability (CSI) authentication protocol.

CSIV2 Attribute Layer

☒ Propagate security attributes

☐ Use identity assertion

☒ Use server trusted identity

☐ Specify an alternative trusted identity

Trusted identity

Password

Confirm password

CSIV2 Transport Layer

Client certificate authentication

Required

Transport

SSL-supported

SSL settings

- ☒ Centrally managed
- [Manage endpoint security configurations](#)

- ☐ Use specific SSL alias

CellDefaultSSLSettings

[SSL configurations](#)

CSIV2 Message Layer

Message layer authentication

Supported

Allow client to server authentication with:

☐ Kerberos

☒ LTPA

☒ Basic authentication

[Trusted authentication realms - outbound](#)

Additional Properties

Login configuration

RM1_OUTBOUND

☒ Stateful sessions

☐ Enable CSIV2 session cache limit

Maximum cache size
100 entries

Idle session timeout
900 seconds

☐ Custom outbound mapping