

## Runtime Infrastructure - Bug #2860

Support # 2696 (New): security review

### implement proper server certificate validation in spawned clients

11/19/2015 02:10 PM - Greg Shah

<b>Status:</b> Closed	<b>Start date:</b>
<b>Priority:</b> Normal	<b>Due date:</b>
<b>Assignee:</b>	<b>% Done:</b> 0%
<b>Category:</b>	<b>Estimated time:</b> 0.00 hour
<b>Target version:</b>	<b>case_num:</b>
<b>billable:</b> No	<b>version:</b>
<b>vendor_id:</b> GCD	
<b>Description</b>	
<b>Related issues:</b>	
Related to User Interface - Bug #2778: ./ask-gui.p fails if "Program name" is... <b>Closed</b> <b>10/23/2015</b>	

#### History

##### #1 - 11/19/2015 02:14 PM - Greg Shah

The current web client disables server certificate validation when connecting. This is insecure and makes our code vulnerable to man-in-the-middle (MITM) attacks. The solution is to provide the server's certificate and/or proper CA in a truststore that is sent down to the client via the temporary client session. Or, if the already existing keystore is enough, to make it work properly.

For more details, see [#2778-97](#).

At a minimum this security issue affects the web client.

##### #2 - 11/19/2015 04:25 PM - Greg Shah

- Status changed from New to Closed

Fixed in task branch 2677a revision 11065.