FortiGate Firewall:

Status ‘0’: Failed to open TCP connection to X.X.X.X:XXX (execution expired)

1. Verify the port used for API calls

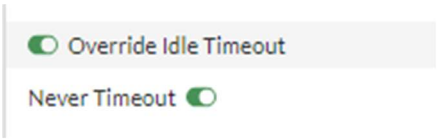
Ask the customer to verify which port is used for API calls. They must input the correct port number in the firewall SOAR settings on the CSD.

1. Navigate to **System** > **Settings > Administration Settings.**
2. Make note of the **HTTPS port**. This will be the port that is used to make API calls for SOAR.
3. The customer must input the port number in the SOAR config settings on the CSD.
4. Please have the customer test the connection from the CSD with the correct port value. If the issue persists, move on to the next troubleshooting step.

2. Check the timeout settings for the XDR admin profile

Ask the customer to enable Override Idle Timeout & Never Timeout.

1. Navigate to **System** > **Admin Profiles** > **(Your REST API Admin Profile)**
2. Scroll down to **Override Idle Timeout** and slide the toggle to **On**. Then slide **Never Timeout** to **On**.



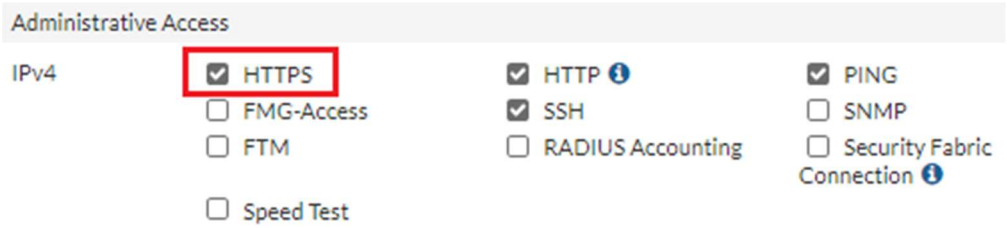
3. Once the customer makes these changes, please have them test the connection again from the CSD.

3. Create a NAT rule to permit traffic from our SOAR endpoint to the firewall

If you have a firewall placed in front of your FortiGate device, you will need to make sure there is a policy in place on that firewall to allow the traffic from our SOAR endpoint to the FortiGate device. The firewall could be blocking API requests if they do not allow admins to log in from the public IP, only the management IP of the device. If this is the case, the customer will need to make sure that they set up a NAT forwarding rule on the firewall to allow traffic from our endpoints (44.209.49.222 & 44.239.173.232) to the management IP.

4. Ensure HTTPS is enabled on the WAN Interface

Admin access from the WAN interface is needed for XDR to have remote access to the firewall device. You can manage these settings by navigating to **Network > Interfaces** and adjusting the administrative access to the interface.

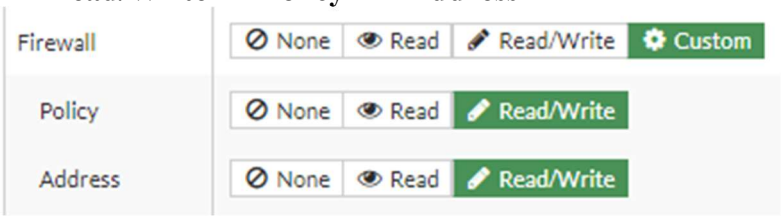


5. Ensure the SOAR IP is added as a trusted host to the system administrator account

The XDR REST API admin needs to be able to communicate and authenticate to the firewall. If you are restricting admin logins to only certain networks, you must add the SOAR IP (44.209.49.222 & 44.239.173.232) as a trusted host to the administrator account. This will make sure the

Error 401: This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required.

1. Check the REST API firewall permissions to ensure the API admin user can make the appropriate changes on the firewall.
    a. Navigate to **System** > **Admin Profiles** > **(Your REST API Admin Profile) > Access Permissions.**
    b. Under **Access Control**, go to the **Firewall** section, and make sure the API admin user can **Read/Write** for **Policy** and **Address** actions.



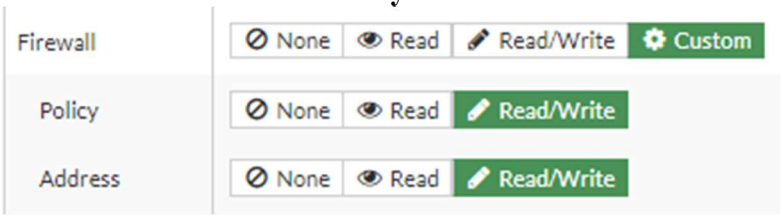
Error 403: This error occurs when the user making the API call does not have the necessary permissions.

1. Verify that the XDR admin user still has the necessary permissions to make API calls to the firewall.

Ask the customer to verify that the XDR admin user still has the necessary permissions to make API calls to the firewall. This would require checking the REST API firewall permissions (similar to the 401 error):

1. Navigate to **System** > **Admin Profiles** > **(Your REST API Admin Profile) > Access Permissions.**

2. Under **Access Control**, go to the **Firewall** section, and make sure the API admin user can **Read/Write** for **Policy** and **Address** actions.



3. Once the customer makes these changes, please have them test the connection from the CSD. If the issue persists, move on to the next troubleshooting step.

2. Regenerate a new REST API KEY

Have the customer regenerate a new API Key for the XDR admin and upload the new value to the SOAR config on the CSD.

1. Navigate to **System** > **Administrators > (Your REST API Administrator).**
2. Go to API Key and click **Regenerate**.
3. Save the new API key in a safe place.
4. Upload the new API key to the SOAR config page on the CSD.
5. Once the customer updates the SOAR data, please have them test the connection again.

Additional FortiGate References:
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/399023
https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-Rest-API-response-error-codes/ta-p/202126