Only SA or SA delegate users can log in or Log in as SA to configure open access

Last Modified on 04/04/2023 4:22 pm EDT

Symptom

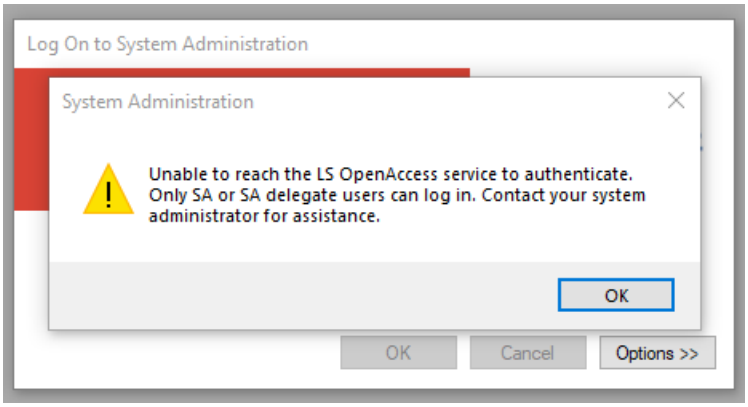
When logging into OnGuard 7.5 or later, the error “Unable to reach the LS OpenAccess service to authenticate. Only SA or SA delegate users can log in.” error is shown. This typically happens when the Message Broker can't configure the connections correctly.

Resolution

On the server

This error indicates that the settings are not correct for communication with the Message Broker. If the customer is using SSO, interrupt it and use a local login to see if the following message is shown:

"Unable to reach the LS OpenAccess service to authenticate. Only SA or SA delegate users can log in. Contact your system administrator for assistance."



If you see this error, perform the following troubleshooting procedure:

Verify that the Message Broker and OpenAccess are configured, and that OpenAccess is running:

1. Log into System Administration using the SA user.
2. Navigate to **Administration** > **System Options** and verify that Message Broker and OpenAccess are configured and have the same entry (should be the Fully Qualified Domain Name (FQDN) of the OnGuard server).
3. Go to Services and verify that the LS OpenAccess service is running. If not, start it and try to log in.
4. If you get the same error, perform the steps below.

Update the Message Broker Host Name (Upgrade migrations only)

1. Go to the Message Broker host table.

2. Update the Message Broker host name to the new FQDN and update the port to 5657.
   Note: For OnGuard 7.5, port 5671 is the default and should not have to be added.
3. Run Setup Assistant. This will create the NGINX certificates and create the correct connections for RabbitMQ. If this does not resolve the error, perform the steps below.

Verify that the Host Name is correct

1. Log in to the SQL Server.
2. Navigate to **Database** > **AccessControl database** > **tables**, then locate the message_broker_host table and right-click and select **edit top 200**.
3. Expand the Host name column to the right so that you can see the full information. Verify that the host name is correct with **:5657** (or, for OnGuard 7.5, with **:5671** and should not have to be changed) at the end. If not, click in the space and enter the correct FQDN and port.
4. Click on any Null to set the change.
5. Run Setup Assistant and see if that resolves the issue. If this does not resolve the error, perform the steps below.

Verify Ls_server_cert.pem and Ls_server_cert_key.pem certificates

1. Navigate to **C:\ProgramData\LnI\nginx\conf** and verify that you see the **ls_server_cert.pem** and **ls_server_cert_key.pem** files.
   - If the files are missing, run the script from the Installation Guide, making sure to copy the script to Notepad and backspace until it is one long line, and insert the information shown in System Options for the **Server name**.
   - If the files are there, make a copy of the **ls_server_cert.pem** file and paste the script in the lower white area. Rename the file to **ls_server_cert-Copy.pem.crt** and ignore the pop-up error.
2. Open the certificate and note the “issued to” value. If this is different from what is in Message Broker, update Message Broker with this value. Also verify the actual machine name by right-clicking on computer name of this PC in Windows Explorer and selecting **Properties**. If the name does not match what is configured for the Message Broker host, recreate the certificates in step 1 and update the Message Broker and OpenAccess settings.
3. Verify that the certificates are correct and match the machine name.
4. Verify the System Options and the port are correct.
5. Run Setup Assistant and verify that it completes.
6. Log in again. If this does not resolve the error, perform the steps below.

Check in Microsoft Management Console (MMC) under Certs that the Prism certificate (OnGuard 7.5) or the LenelS2 certificate (OnGuard 7.6 or later) is installed

1. Open the Start menu and type **MMC**. You should see **MMC.exe**. Run as an Administrator.
2. Select **File** > **Add/remove snap in**.
3. Click on the **Certificates** on the left and select **Add in the middle**. Select **Computer account** > **Next** > **Finish**, then click **OK** in the lower right.
4. In the upper left, expand **Certificates** and expand the **Trusted Root Certification Authorities**, and then click on the **Certificates** folder below it.
5. On the right, scroll down to the P entries (alphabetical) and verify if the Prism SOA (for OnGuard 7.5) or the LenelS2 (OnGuard 7.6 and later) Common Trusted Root is in place. If it is there, continue

with step 6. If it is missing, do the following:
    - Navigate to the installation location of OnGuard. Default is**C:\Program Files (X86)\OnGuard**. Locate the **Certificate** folder.
    - Run the **lnl_app_root_certificate_installer.exe** file as administrator. If the certificate is not created in the Certificate store (MMC), then there is a policy or permission issue. Work with your IT department to get this certificate installed.
6. If you are still getting the error message, reboot the workstation.
7. If you are still getting the message, contact LenelS2 OnGuard technical support.

On a client

1. Verify there is no issue on the server.
2. If the customer cannot log in due to a license issue, run Setup Assistant on the server and check the logs. If all steps pass, then continue this procedure.
3. Check that the **RabbitMQ.Client.dll** file is in the root of the OnGuard folder (normally located in **C:\Program Files (x86)\OnGuard**). If not, copy the **RabbitMQ.Client.dll** file from server, add the file to the OnGuard folder, re-open System Administration, and then try to log in again.
4. Check in MMC under Certs that the Prism certificate (OnGuard 7.5) or the LenelS2 certificate (OnGuard 7.6 and later) is installed.
5. Use the Start menu and type **MMC**, then run **MMC.exe**.
6. Select **File** > **Add/remove snap in**.
7. Click on the **Certificates** on the left and select **Add in the middle**. Choose **Computer account** > **Next** > **Finish**, and then select **OK** in the lower right.
8. In the upper left, navigate to **Certificates** > **Trusted Root Certification Authorities** > **Certificates**.
9. On the right, scroll down to the P entries (alphabetical) and verify if the Prism SOA (for OnGuard 7.5) or the LenelS2 (for OnGuard 7.6 and later) Common Trusted Root is in place. If it is there, continue with step 10. If it is missing, do the following
    - Navigate to the install location of OnGuard, which is**C:\Program Files (X86)\OnGuard** by default. Locate the **Certificate** folder.
    - Run the **lnl_app_root_certificate_installer.exe** file as administrator. If the certificate is not created in the Cert store (MMC), then there is a policy or permission issue. Work with your IT department to get this certificate installed.
10. If you are still having an issue, contact LenelS2 OnGuard technical support.

Applies To

OnGuard 7.5 and later

Additional Information