

Emails sent through the Global Output Server never arrive

Last Modified on 10/06/2022 4:16 am EDT

Symptom

Emails sent through the Global Output Server never arrive.

- If sending manually from Alarm Monitoring, it might appear that the email was successfully sent, but the recipient never gets it.
- **C:\ProgramData\LnI\logs\GOSEmailAgent.log** registers:

TIME: [03/09/2019 13:09:13]

SEVERITY: Error

ERROR CODE: 0x20010001

PROGRAM: GOSServer

FILE: gosEmailAgent.cpp (LINE 275)

DETAILS: Internal logic error.: Failed to connect to SMTP server! Server's response: 221 2.0.0
Service closing transmission channel

Resolution

Check the authentication methods supported by the SMTP server by establishing a telnet session. In a command prompt, enter:

```
telnet
```

The server will greet with code **220**, to which you should respond **ehlo** to make the authentication mechanisms available. In the example below, the telnet session was started with **telnet EXCH2013.rk01k.local 587**:

```

c:\ Telnet EXCH2013.rk01k.local
220 EXCH2013.rk01k.local Microsoft ESMTPL MAIL Service ready at Sat, 9 Mar 2019 13:45:50 -0500
ehlo
250-EXCH2013.rk01k.local Hello [192.168.1.24]
250-SIZE 36700160
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
250-AUTH GSSAPI NTLM
250-8BITMIME
250-BINARYMIME
250 CHUNKING

```

The authentication methods are found after the **AUTH** command: **GSSAPI** and **NTLM**. **PLAIN** is not listed, therefore the GOS service cannot log in.

NOTE: If **AUTH** is not listed, then the server is configured to use no authentication. In this case, supplying any value in GOS email settings for username/password will also fail authentication.

Browse the SMTP server logs to verify the failed exchange. Microsoft Exchange 2013 stores the relevant log in **C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\FrontEnd\ProtocolLog\SmtpReceive**. It shows that the server closes the transmission:

```

2019-03-09T18:00:56.684Z,EXCH2013\Default Frontend
EXCH2013,08D6A4AD158BE2FF,27,127.0.0.1:25,127.0.0.1:57056,
2019-03-09T18:00:56.684Z,EXCH2013\Default Frontend
EXCH2013,08D6A4AD158BE2FF,28,127.0.0.1:25,127.0.0.1:57056,>,221 2.0.0 Service closing
transmission channel

```

Implementing the solution is specific to each SMTP server. In Microsoft Exchange 2013, this is accomplished by unchecking **Offer basic authentication only after starting TLS** in the **Exchange Admin Center > Mail flow > Receive connectors > Client Frontend > Edit > Security**:

The screenshot shows the Exchange Admin Center interface. On the left is a navigation pane with categories like recipients, permissions, compliance management, organization, protection, mail flow (highlighted), mobile, public folders, unified messaging, servers, hybrid, and tools. The main area shows the configuration for a receive connector on server EXCH2013.rk01k.local. A modal window titled 'Exchange Receive Connector - Internet Explorer' is open, displaying the configuration for 'Client Frontend EXCH2013'. The 'security' tab is active, showing authentication options: Transport Layer Security (TLS) is checked, 'Offer basic authentication only after starting TLS' is checked and highlighted in yellow, and Integrated Windows authentication is also checked. Other options like 'Enable domain security (mutual Auth TLS)', 'Basic authentication', 'Exchange Server authentication', and 'Externally secured' are unchecked. Under 'Permission groups', 'Exchange users' is checked, while 'Exchange servers', 'Legacy Exchange servers', 'Partners', and 'Anonymous users' are unchecked. 'save' and 'cancel' buttons are at the bottom right of the modal.

After submitting the change, wait approximately 5 minutes for the change to take effect, then verify it by retrieving the authentication methods again. This time **LOGIN** should be listed in the server's response to **ehlo**:

```
ca Telnet EXCH2013.rk01k.local
220 EXCH2013.rk01k.local Microsoft ESMTPL MAIL Service ready at Sat, 9 Mar 2019 13:34:57 -0500
ehlo
250-EXCH2013.rk01k.local Hello [192.168.1.24]
250-SIZE 36700160
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
250-AUTH GSSAPI NTLM LOGIN
250-8BITMIME
250-BINARYMIME
250 CHUNKING
```

The GOS service should now be able to send email successfully.

Applies To

Global Output Service

Additional Information