Question 1:

Case: 15288890
The client received the error.
Q: Error: upstream connect error or disconnect/reset before headers. retried and the latest reset reason: connection termination

A: When users access envelopes via the email notification link, their device must establish a stable connection to our servers. If that connection is disrupted or fails to establish properly, the request is terminated, which can result in the error you're seeing.

We recommend checking the user's internet connection and any firewall or proxy settings that might interfere with server communication. In some cases, retrying after a short period or using a different network can help resolve the issue.

You can try performing this action over mobile data.
If that continues, please provide us with the browser HAR. Capturing a HAR File in your Browser

Question 2:

Q: How do I determine if a recipient used the Print and Sign feature?
A: There is an optional column in the **Envelope Recipient Report** called **Signed on Paper**.
Link: https://docusign.lightning.force.com/lightning/r/Knowledge__kav/ka81W000000PJhjQAG/view

Question 3:

Q: How do I set Reminders and Expirations for documents sent from my account?
A: These settings are the default behavior for all documents sent from your account. You can choose to enforce these settings for all documents, or allow users to modify the values for each document they send.
To allow users to change these values, select **Allow users to override these settings**.
Reminders: (Default: Off)
You can turn on reminders to send follow up emails to signers automatically. When you enable reminders, you specify when and how often to send notifications.
Expiration: (Default: 120 days; no warning)
You can modify this value as desired. You can also add the option to send signers an expiration warning. When a document expires, the status changes to Voided and it can no longer be viewed or signed by recipients.
When an in process document reaches five days to expiration, an expiration countdown appears under the document status in the Documents list.

Link:https://docusign.lightning.force.com/lightning/r/Knowledge__kav/ka81W000000PE6XQAW/view

Question 4:

Q: NDSE - Error when uploading brand - "Requested value 'JPE' was not found"
A: Issue: A customer is trying to upload a brand they previously exported. On uploading the brand, they see an error message.

The logs will show you the following error message:

{"errorCode":"BRAND_CREATE_FAILED","message":"Brands could not be created. Unable to upload brand, error: Requested value 'JPE' was not found."}

Solution:
Open the brand in a text editor
Find all occurrences of JPE   like <Logo type="JPE">
Replace JPE with JPEG
Link: https://docusign.lightning.force.com/lightning/r/Knowledge__kav/ka81W000000PC0AQAW/view

Question 5:

Case: 15190767
Q: Why does Okta show this error when provisioning a user to DocuSign?
Error: `Automatic provisioning of user "" to app DocuSign failed: Error while trying to push profile update for "": Username and email combination already exists for this account.`

A:
This issue occurs because the Okta User Provisioning API integration with DocuSign is outdated and not officially supported by DocuSign. It often causes conflicts with DocuSign's user model, leading to errors like duplicate email/username conflicts or failed API calls.

Key Details:

- DocuSign does **not recommend** using Okta's API provisioning integration as it’s based on **SSO v1**, which is outdated.
- The integration attempts to create or modify users even if the user already exists in DocuSign, which can cause conflicts.
- Instead, DocuSign recommends using **Just-In-Time Provisioning (JIT)** via SSO v2.

- In cases where you must use Okta for user management, consider **disabling the API integration** or managing users manually in DocuSign.

Recommended Solutions:

1. **Disable API integration** in Okta (recommended by DocuSign):
   - Go to: `Okta Admin > Applications > DocuSign > Provisioning > API Integration`
   - Uncheck "Enable API Integration" and save.
2. **Use JIT Provisioning** instead:
   - When a user logs in via SSO for the first time, they will be created/activated in DocuSign.
   - Guide: Just in Time Provisioning Setup
3. **Manual provisioning (if API must remain enabled)**:
   - Create or activate users in DocuSign Admin with the "Automatically activate memberships" option.
   - Alternatively, activate Pending memberships manually via the Org Admin interface.

Link:

- SSO v2 Okta Auto Provisioning Integration - Activation Issues
- Okta error "Could not connect to the API; service not available"

Question 6:

Case: 15295262
Q: Can users still access a shared DocuSign account (e.g., `peopleteam@node4.co.uk`) using their individual SSO logins after switching to SSO via Microsoft Entra?

A:
No, users cannot access a shared DocuSign account using their individual SSO credentials unless that shared email is explicitly federated in the IdP (e.g., Microsoft Entra). However, DocuSign offers a **bypass** configuration that allows specific accounts—like shared email addresses—to log in using **DocuSign credentials** even when the organization enforces SSO.

Key Details:

- Shared accounts like `peopleteam@node4.co.uk` are not typically mapped in SSO environments and will not be accessible via individual user SSO logins.
- DocuSign provides a **Federated Authentication Bypass (FedAuthBypass)** which enables password-based login for selected users while SSO is active.
- This is useful for service accounts, test users, or shared logins where SSO enforcement should be bypassed.

Recommended Solutions:

Enable SSO Bypass (FedAuthBypass):

1. Go to: **Admin > Organization > Users**
2. Locate the user `peopleteam@node4.co.uk`
3. Under Security settings, change login policy to:
   "Log in with SSO, password, or passwordless options"
4. Save changes.

Optional – Disable password reset (if desired):

1. Go to: **Admin > Address Book > User Profile**

2. Set **“Allow Password Login for SSO Users”** to **“No”**

3. Save.

This prevents users from resetting the shared password, helping to enforce tighter control over access.

Important Note:
Shared accounts are not a best practice due to audit and security concerns. For long-term security and compliance, consider creating individual accounts or SSO-enabled service accounts instead.

Link:
[DocuSign Admin Guide – FedAuthBypass Setup (internal use only)]
[DocuSign SSO v2 Setup – Best Practices]

Question 7: Q: How do I resolve an SSO lockout for an Org Admin? A: This issue occurs when a DocuSign Organization (ORG) Admin is unable to log into DocuSign due to Single Sign-On (SSO) issues, such as an expired certificate or Identity Provider (IdP) problems. The process involves verifying the user's ORG Admin status and then applying a Federated Authentication Bypass (FedAuthBypass) to allow them to log in with a password.

Keywords used by customers in this situation include: “Locked out”, “Can’t log in because of a SSO cert update”, “No one has access”. Other names for the password login policy are: FedAuthBypass, SSO bypass, federated bypass, “Log in with SSO (if an identity provider is mapped to the domain), password, or passwordless login options”.

Solution Steps:

1. **Confirm the user is an ORG Admin:**

    ○ Copy the domain of the impacted user’s email address.
    ○ Navigate to Account Admin for the relevant environment (Production or Demo).
    ○ On the Organizations page, change "Search By" to Domain, paste the domain (without @), and search.
    ○ Find the Organization ID and select Actions > Edit.
    ○ Scroll to the “User Id” “User Name” section to see the Org Admins. Verify the case contact's name is listed and note their UserID.
    ○ Copy the User ID and perform a global search in Badmin. Open the Site Name link.

    - Select View Membership and verify the user's Name, Email, and User ID match the Org Admin details from Account Admin. If they don't match, escalate to eSign Specialized.
2. **Verify the Org Admin's Federation Status:**

    - In Account Admin, select Users from the left menu.
    - Change "Search By" to Email or User ID, paste the user's email or User ID, and search.
    - Review the Federation Status column.
        - Blank means the user is on the domain's default login policy.
        - FedAuthBypass means the user can log in via username and password, bypassing domain policies.
    - If the user is confirmed Org Admin and Federation Status is blank (No FedAuthBypass), they are locked out due to SSO settings.
    - If the user is confirmed Org Admin and Federation Status is FedAuthBypass, they must log in via password. Offer to send a password reset if needed.
3. **Adjusting the Login Policy - FedAuthBypass:**

    - **Internal Admin Console (Preferred):**
        - Send an email via the case confirming the customer's approval to adjust their individual user login.
        - Log into the IAC server associated with the user’s account.
        - Select Open, then View Membership, then Permissions.
        - Scroll to the Federated Status drop-down and select “Fed Auth Bypass”.
        - Select Save.
        - Send a password reset to the ORG Admin.
        - Include the updated user id in your case comment. Transfer to eSign Specialized for assistance with other users or account login policy updates.
    - **Account Admin (If Internal Admin Console permissions are not available):**
        - Navigate to Account Admin for the relevant environment.
        - Select Users from the left menu.
        - Change "Search By" to Email or User ID, paste the user's email or User ID, and search.
        - Select the Actions drop-down and “Edit Federation Status.”
        - In the drop-down, set the status to “FedAuthBypass” and select Save.
        - Optionally, send a password reset request.

Link: https://docusign.lightning.force.com/lightning/articles/Knowledge/SSO-2-0-Bypass-Exemption

Question 7:

Case: 15315062
Q: How do I resolve an issue where the DocuSign Print Driver is not allowing documents to be printed and displays the error: “An error has occurred. Please try again”?

A:
This issue may be caused by:

- **Internet connectivity problems**, which can prevent proper authentication or driver communication.
- **An outdated version of the DocuSign Print Driver** — versions prior to 3.6 are no longer supported.

Recommended Solutions:

1. **Reinstall the latest version of the Print Driver (3.6.3)**
   Provide the customer with appropriate links based on their system:
   - 32-bit EXE: Download
   - 64-bit EXE: Download
   - 32-bit MSI: Download
   - 64-bit MSI: Download
2. **Confirm the system is connected to the internet** during login and when attempting to print.
3. **Follow up with troubleshooting** if the issue persists after reinstalling:
   - Check firewall and antivirus settings that could block the driver.
   - Run as administrator.
   - Test printing to a different printer or device.

Key Details:

- This issue is not classified as a system degradation but as a **local issue**.

- DocuSign support should continue working directly with the user if reinstalling doesn't resolve the problem.

Optional Step:
Provide a **Calendly link** to schedule a meeting for further troubleshooting:
Luciano’s Calendly

Tags: Print Driver, Error Message, Driver Compatibility, Local Issue, Driver Reinstall

Question #:
Q:
A:
Link:

Question #:
Q:
A:
Link:

Question #:
Q:
A:
Link:

Question #:
Q:
A:
Link: