



# NCAISS: User Receiving “Page Cannot Be Displayed” Error when Registering a Certificate or Attempting PKI Authentication into NCAISS

## Background

When registering a certificate with an NCAISS account, or attempting to authenticate into NCAISS, a user may receive a “Page Cannot be Displayed” error message. In most cases, the “Page Cannot Be Displayed” error is indicative of a problem that occurred before the user reached the NCAISS application (i.e., between the user’s workstation and the DSS infrastructure components that validate PKI certificates). Such issues are most likely caused by the user’s workstation, browser, or network settings. To resolve the issue the user will have to work with their local IT Helpdesk, and possibly the DSS Network Team.

## Information to Identify Cause of Error

When a user is working with the DSS Call Center or local IT helpdesk to resolve the issue of receiving a “Page Cannot Be Displayed” error there is certain information that is beneficial in identifying the cause of the issue (e.g., workstation settings, certificate, DSS F5 infrastructure). Answers to the questions below will aid in the identification of the root cause of the issue:

1. What behavior is the user experiencing when trying register a certificate or authenticate to NCAISS?
2. Is the user prompted to select their certificate?
3. Is the user’s certificate displayed in the certificate selection window?
4. Is there an error message on the page, and specifically what does it say?
5. What is the URL of the failed webpage?
6. What is the issuing authority of the certificate?

## Possible Causes of Error

There can be many possible causes of the “Page Cannot Be Displayed” error. The user should work with their local IT helpdesk to check the following on their workstation:

1. Incompatibility settings defined by administrative/group policies.
2. The browser is in “private mode,” and cookies are blocked.
3. Mixed/unprotected content is blocked (e.g., unsecure/unencrypted images).
4. Specific header attributes are blocked.
5. Certain add-ins/plugins are incompatible.
6. Root certificates are not properly configured on the DSS infrastructure.
7. Issue with DoD Interoperability root certificate. Note: see section below for instructions on how to remove the certificate.

In some cases the reinstallation of the internet browser may be required.

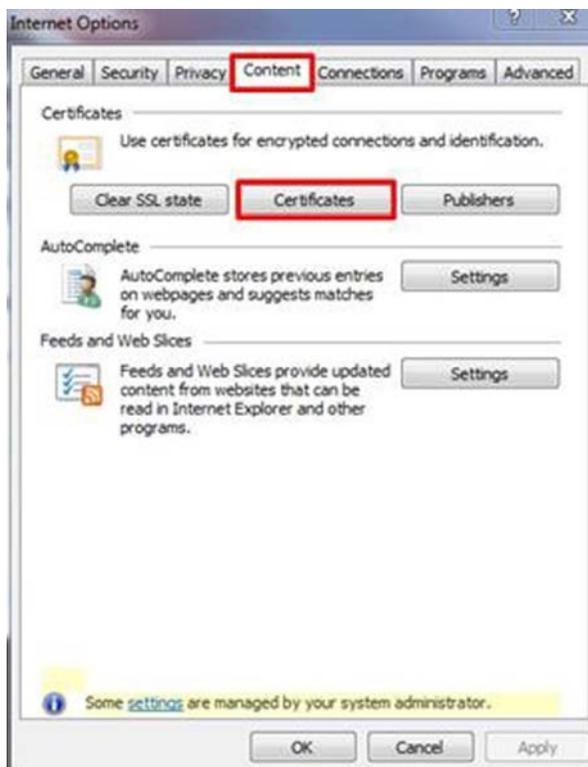
Additionally, the issue may be caused by the user’s Windows’ certificate path not following the DoD direct-trust path. A way to have the user’s Windows use the standard DoD direct-trust path is to have the user install and run the DoD InstallRoot Tool v4.1. This tool can be found on DISA’s IASE site: <http://iase.disa.mil/pki-pke/Pages/tools.aspx>



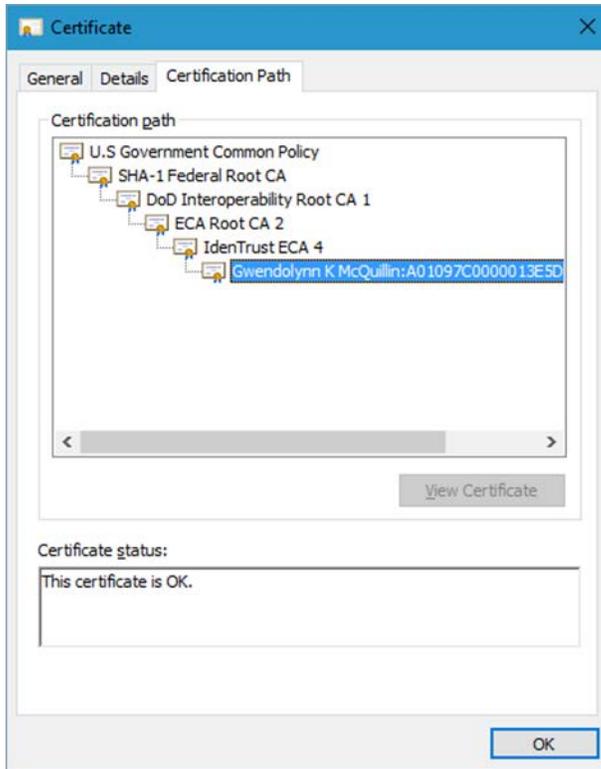
## Removing the DoD Interoperability Certificate

As highlighted above, one potential cause for the “Page Cannot Be Displayed” error, is an issue with a DoD interoperability root certificate. To resolve this issue, the certificate must be removed via the user’s browser (i.e., Internet Explorer). Take the following steps to verify if this certificate issue is the cause of the error, and if so, resolve the issue.

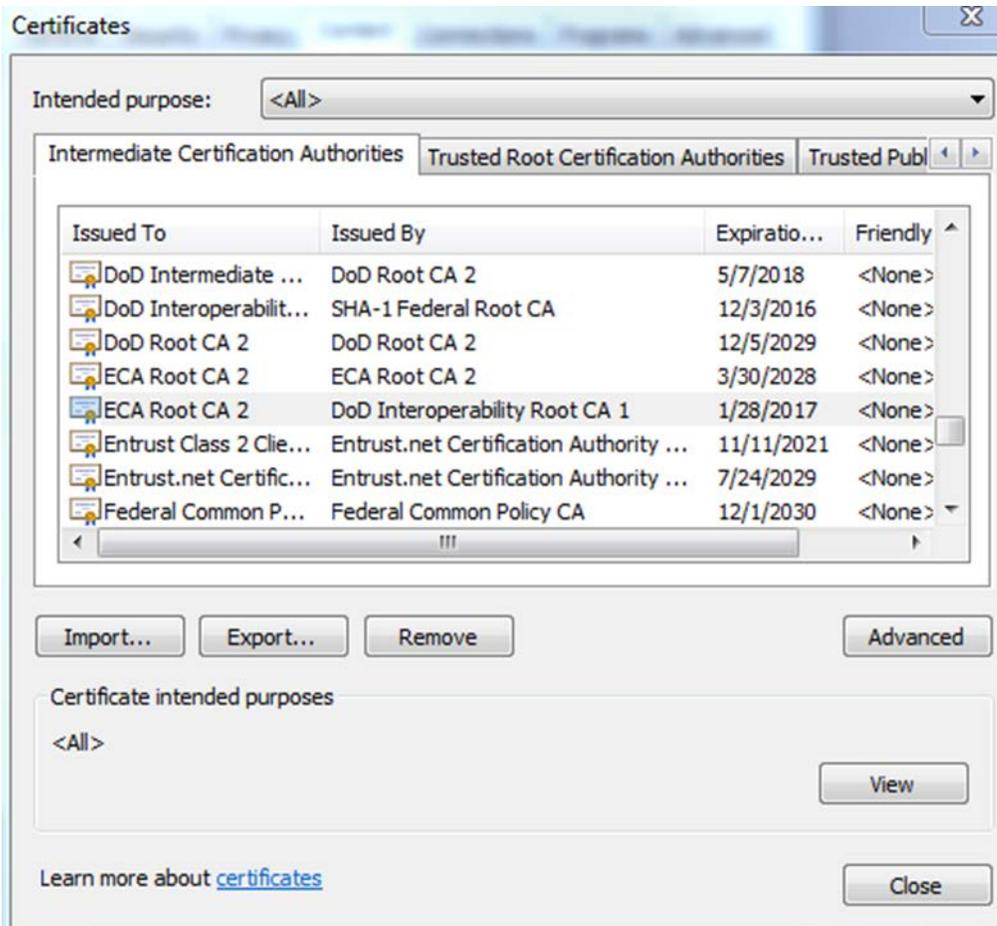
1. Attempt to log into NCAISS and verify the “Page Cannot Be Displayed” error message.
2. Close Internet Explorer and open a new browser window.
3. Open the **Tools** menu via clicking the gear icon or by pressing the Alt key on the keyboard.
4. Go to **Internet Options**.
5. Click on the **Content** tab.
6. Click the **Certificates** button.
7. Double click on the certificate being used to access NCAISS.



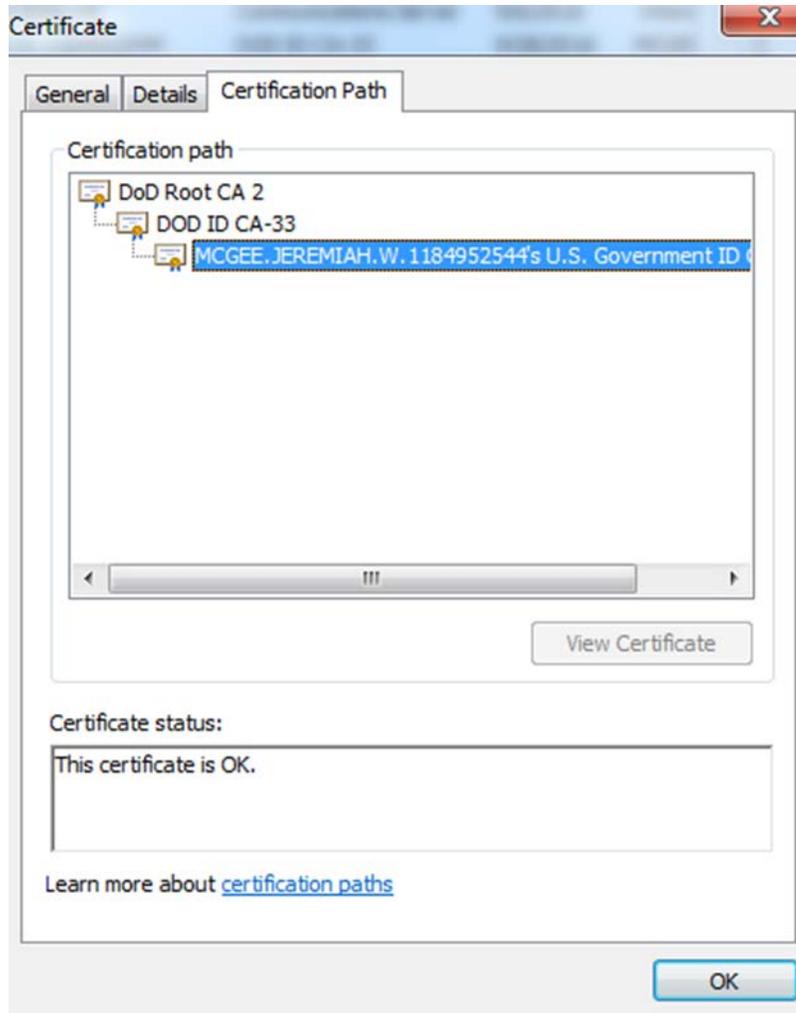
8. Verify the Certification Path is six levels. The third level will be DoD Interoperability Root CA 1. If the path is six levels, continue to Step 9. If the path is three levels, the issue is not with the interoperability certificate. Contact your local IT Helpdesk, and/or the DSS Knowledge Center.



9. Go to the **Intermediate Certification Authorities** tab
10. Click on **ECA Root CA 2**.
11. Under the Issued By column, select the certificate issued by “DoD Interoperability Root CA 1”. Note: If there are more than one with different expiration dates, select them all.
12. Click the **Remove** button.



13. Return to the **Personal** tab on the Certificates Pane.
14. Double click on the certificate being used to access NCAISS.
15. Verify the Certification Path is down to three levels as shown below.



16. Try to log into NCAISS again.