Article Number

000009081

Title

Proxy error “Error during SSL Handshake with remote server”

Summary

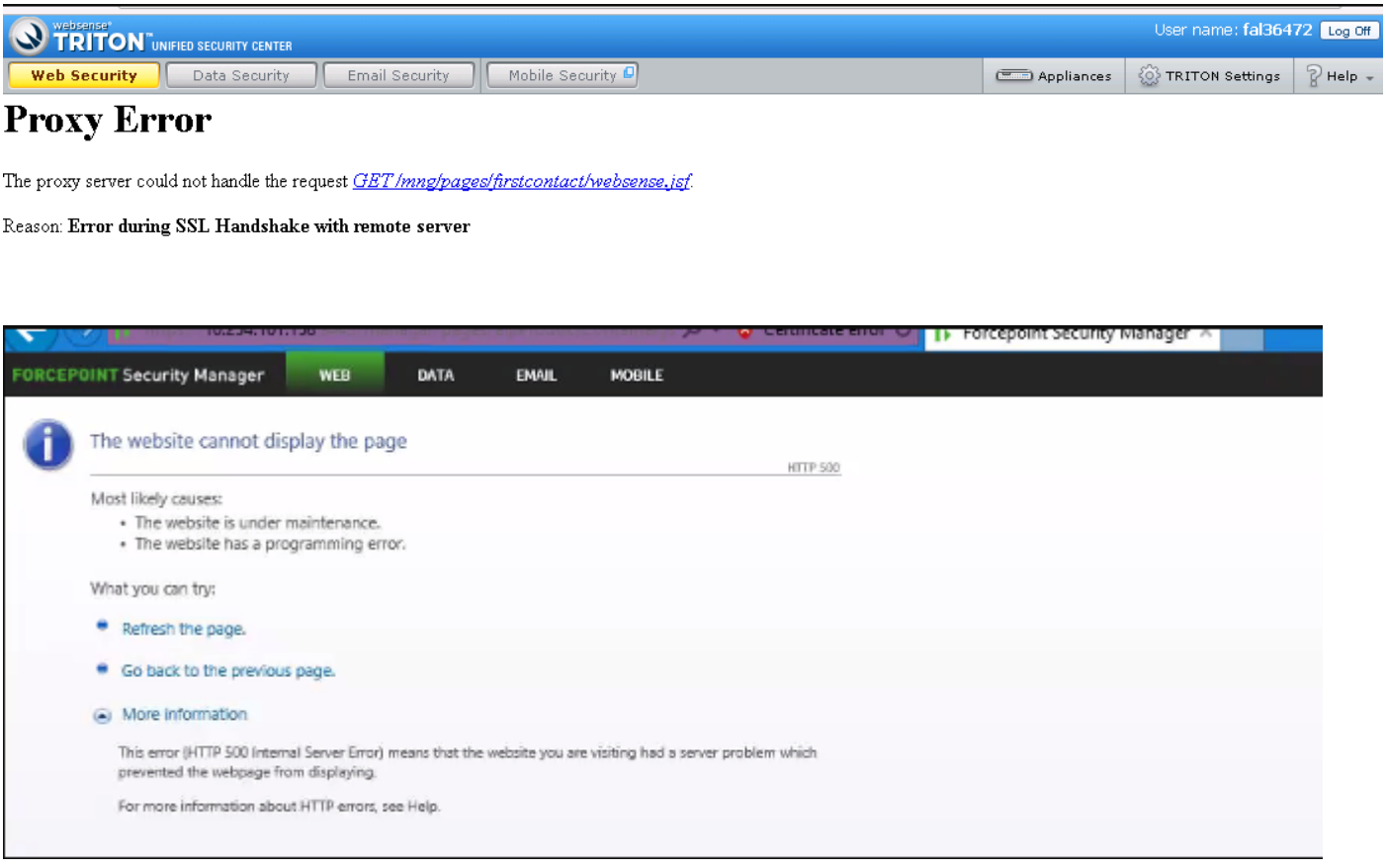
Unable to login to Triton - Error during SSL Handshake with remote server

Problem

When trying to log on to the Forcepoint Security Manager (formerly TRITON), the following error message is displayed:

"*Proxy Error*

The proxy server could not handle the request GET /mng/pages/firstcontact/websense.jsf.
Reason: Error during SSL Handshake with remote server"



Solution

This error may be caused by a certificate issue. There are a few options listed below to resolve the issue.

Replace the current key files with new files

1. Log on to the server where the TRITON Web Security service is installed.
2. Open Windows Explorer and navigate to the **Program Files (x86)\Websense\Web Security\apache\conf\ssl\automation** directory.
3. Run the following batch files. **Note** If the dates in **Program Files (x86)\Websense\Web Security\apache\conf\ssl\output** do not change to today's date after doing this step, try again with by running the files as administrator.
    a. s1_newreq.bat
    b. s2_server_key.bat
    c. s3_server_crt.bat
    d. s4_server_p12.bat
    e. s5_server_cert_txt.bat
4. Copy the **server.key** file from the **Program Files (x86)\Websense\Web Security\apache\conf\ssl\output** directory to the **Program Files (x86)\Websense\Web Security\apache\conf\ssl\ssl.key** directory.
5. Copy the **server.crt** file from the **Program Files (x86)\Websense\Web Security\apache\conf\ssl\output** directory to the **Program Files (x86)\Websense\Web Security\apache\conf\ssl\ssl.crt** directory.
6. Copy the **cakey.pem** file from the **Program Files (x86)\Websense\Web Security\apache\conf\ssl\output** directory to the **Program Files (x86)\Websense\Web Security\apache\conf\ssl\private** directory.
7. Copy the **manager.p12** file from the **Program Files (x86)\Websense\Web Security\apache\conf\ssl\output** directory to the **Program Files (x86)\Websense\Web Security\tomcat\conf\keystore\tomcat** directory.
8. Copy the **cert.txt** file from the **Program Files (x86)\Websense\Web Security\apache\conf\ssl\output** directory to the **Program Files (x86)\Websense\Web Security\Manager\OnlineHelp\en\certificateSupport** directory.
9. Restart the services listed below in the following order:

a. Websense TRITON - Web Security

b. Websense Web Reporting Tools

c. Websense RTM Client

Re-install the TRITON Web Security Component

1. Log off TRITON Manager.
2. Log on to the server where TRITON components are installed.
3. Search for **Websense TRITON Setup** and open this installer.
4. Next to the Web module, click **Remove**.
5. Go through the wizard and uninstall only the **TRITON Web Security** service.
6. Restart the server.
7. Search for **Websense TRITON Setup** and open this installer.
8. Next to the Web module, click **Modify**.
9. Install the **TRITON Web Security** service.
10. Log on to TRITON Manager.

Note Re-installing this component creates a new certificate without having to manually edit files.

The TRITON Manager certificate has expired

Review the Generating a custom Websense Manager SSL certificate KB article on creating a new certificate.

keywords: ssl error; proxy error; cert; certificate; expired; security manager not working; cannot log into security manager; fsm; handshake; unable to login to triton

URL Name

Unable-to-login-to-Triton-Error-during-SSL-Handshake-with-remote-server