# Secure Access – Troubleshooting Rewrite related issues (Core/Web Based Access)

## Why do certain web-based applications have issues through the rewrite engine compared to accessing the resource directly (e.g. from within the office network without any VPN)?

One of the main features that Junos Pulse Secure Access offers is clientless Access to web-based applications. For this the Junos Pulse Secure Access platform has a Content Intermediation Engine (CIE), a highly advanced parser and rewriter. The CIE retrieves Web-based content from internal Web servers and changes URL references and Java socket calls so that all network references point back to the SA.

In order to successfully intermediate Web applications, the CIE must identify all links within a page and rewrite them accurately. The CIE supports a wide range of Web based applications which use different technologies (standard HTML, JavaScript, VBscript, Java, Flash, PDF, etc.) In order to support such wide range of web based technologies the CIE has complex and smart logic built into it.

With certain application, the CIE may not be able to identify these URL's and rewrite them as per CIE guidelines. (Note that several of these web technologies are not standards based and how the network references occur within the application depends on the way these applications were designed and developed by the application vendor). This causes most of the issues and symptoms that end users experience when accessing web based applications using the clientless Web/Core based access methods. For more information and guidelines for developing Web applications that is compliant with the IVE Content Intermediation Engine, please refer to the Content Intermediation Engine Best Practices Guid**Error! Hyperlink reference not valid.**

## What should I do when an application does not work as expected while accessing through the rewrite engine?

If you are having issues with a web based application through the rewrite engine, you may choose any one of the below routes to resolve the issue:

***Method 1: Using Secure Application Manager (SAM), Network Connect (NC) or Junos Pulse***

**Pros:** Quick resolution, easy to configure
**Cons:** Client based access

If you have users that already use an alternate access method like Network Connect (NC), Junos Pulse or Secure Application Manager (SAM) then you can use the following access method to access this specific web application (or identify a new alternate access method that suits your end users requirements)

1. Configuring VPN Tunneling (for Network Connect or Junos Pulse) or configuring JSAM
2. Create a Selective Rewrite Resource policy to **Don't Rewrite Content: Redirect to target web server**
3. Log-in as an end user, launch NC/Pulse or WSAM and attempt to access the web application

***Method 2: Use Pass-through Proxy Access Mechanism:***

**Pros:** Clientless access
**Cons:** Needs either additional public DNS entry or a high port (tcp port 11000-11099) to be opened on the firewall.

To configure pass through proxy, refer to Creating a Pass-through Proxy Resource Policy.

***Method 3: Open a case with JTAC to have the issue investigated and fixed.***

**Pros:** Clientless Access without any additional configuration.
**Cons:** Slow resolution as it involves log collection, replication and in some cases code fixes, verification, new release delivery and there after upgrade of the SA device.

## I have decided to use option #3 listed above. What logs should I collect for troubleshooting?

When opening a case with JTAC for rewrite related issues, please use any one of the below options:

1. Provide JSAM or Network Connect access to the web application for troubleshooting purposes and provide detailed steps to navigate through your customer application. This is the preferred option as it allows Juniper to replicate the issue on-demand and avoiding to gather additional logs in the future.

   **This option significantly reduce resolution times.**

2. Collect relevant log files and provide detailed steps to replicate.

   Required for all Rewriter Cases

   While replicating the issue through the Junos Pulse Secure Access:
   - Session Recording log (Dsrecord log)
   - Policy trace log
   - Event Access, Admin Access and User Access
   - HttpWatch Logs
   - Packet capture (internal port)
   - Step-by-step screenshot of each page until the problem page

   When accessing resource directly on the LAN:
   - Httpwatch logs
   - Wireshark capture (when accessing a non-https site)

   The below sections provide detailed instructions on how to collect these log files.

   Important: Please note that some of these tools may capture sensitive information like usernames, passwords and/or application data. JTAC will handle this sensitive information similar to any other troubleshooting information that is provided. The use of these logs is only for troubleshooting purposes and we do not need any username/password related information that is contained in these log files and you may obfuscate any sensitive information before providing the log files to Juniper.

### Tools required for collecting the logs:

1. **HttpWatch:** Download the latest HttpWatch Basic Edition from https://www.httpwatch.com
2. **Wireshark:** Download Wireshark from http://www.wireshark.org/download.htm**Error! Hyperlink reference not valid.**

## Prerequisites before collecting logs:

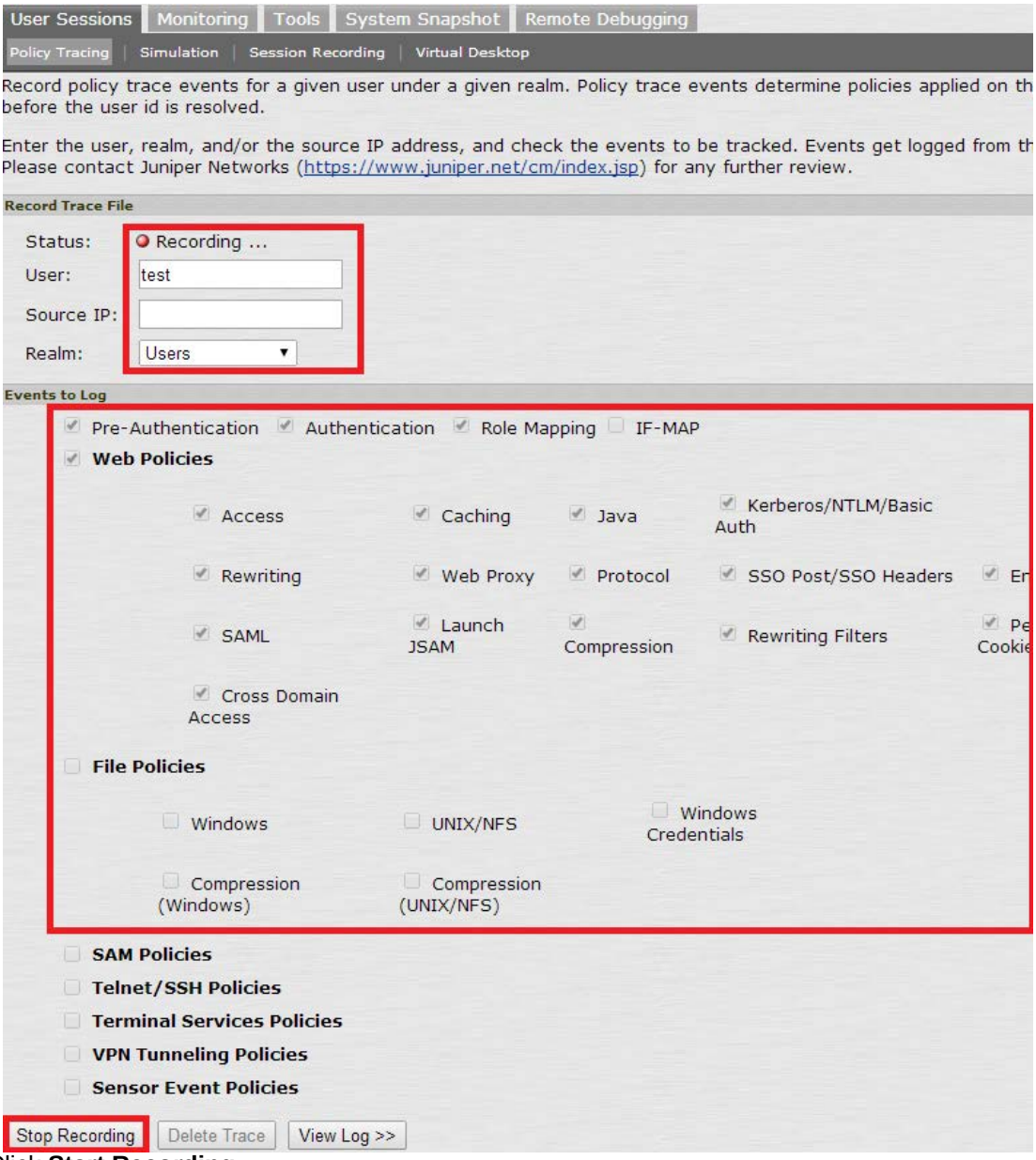
1. Clear browser cache.
2. If the application uses Active-X, clear the relevant Active-X objects from your browser.
3. If the application uses Java, clear Java cache, then disable caching

***Note:*** *The above pre-requisites are crucial in collecting these logs; if these are not followed then JTAC will not have all the information pertaining to this application and this is very important to replicate/understand the issue experienced via the SA rewrite engine.*

## How to enable logs in the SA Admin Console before replicating the issue?

**Policy Trace:**

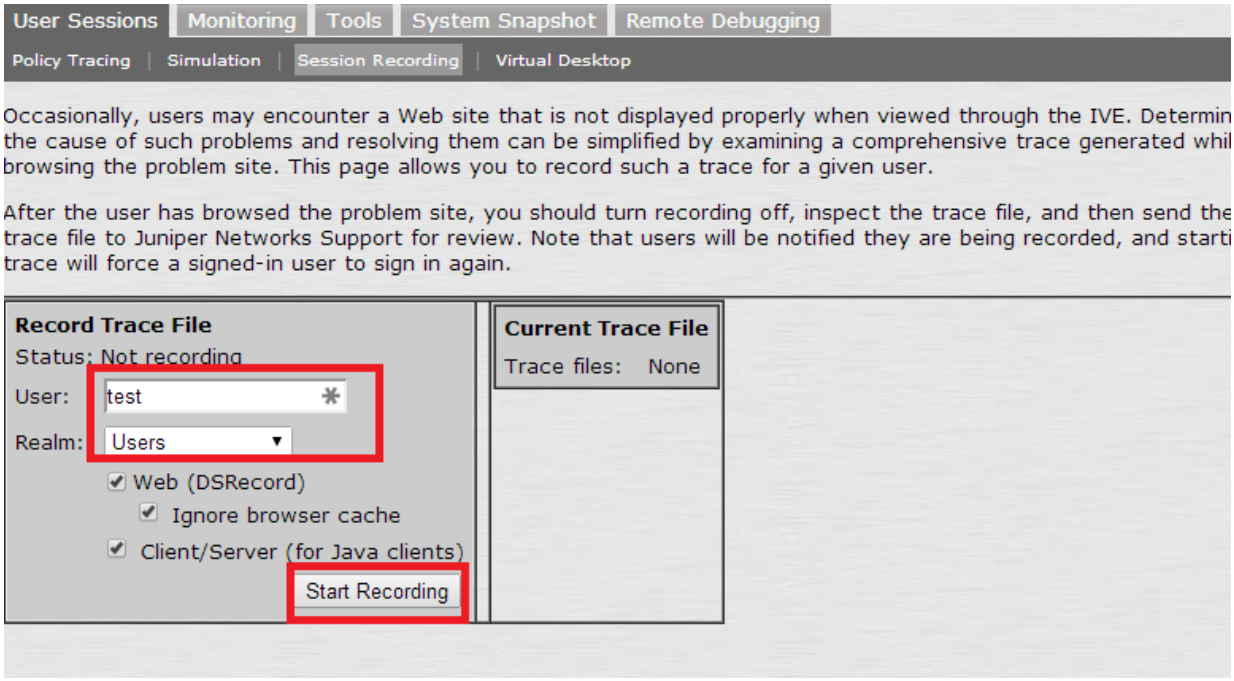
1. Navigate to **Maintenance** > **Troubleshooting** > **User Sessions** > **Policy Tracing**
2. In User field, enter the user name to monitor.
3. In Realm drop-down, select the corresponding realm.
4. Enable *Authentication Pre- Authentication*, Authentication, *Role Mapping* & *Web Policies*




5. Click **Start Recording**.

**Session Recording:**

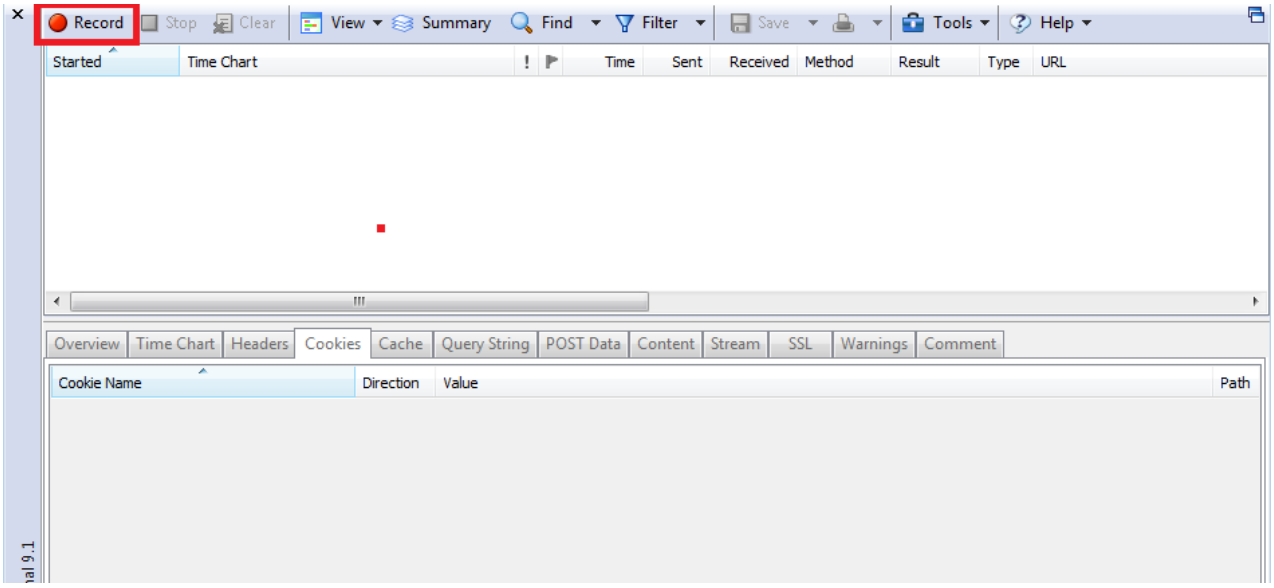
1. Navigate to **Maintenance** > **Troubleshooting** > **Session Recording**,
2. In the User field, enter the user name to monitor




3. Select the User Realm to which user belongs.

**HTTP watch log:**

1. Open the browser
2. Right click on the web page
3. Select HttpWatch Basic
4. A menu will appear on the bottom. Click **Record**.




For more detailed instructions, refer to http://help.httpwatch.com/#gettingstarted.html

## How to capture a direct TCP dump from client computer when accessing the application directly (not using SA), how does it help JTAC?

1. Use a computer that has direct access to the backend application
2. Follow the same prerequisites before capturing log as stated in the above section.
3. Using Wireshark, start packet capture on the local adapter (physical or wireless)
4. Start Httpwatch log on client browser. (After installing HTTP watch on client computer, before starting to access any URL, open browser and enable HTTP watch under View > Explorer bar > Http watch. Start recording.)
5. Access the backend application, save every web page as a screenshot on a word document. This helps in understanding how to navigate between different pages.
6. Once you reach the problematic page, stop the packet capture and httpwatch capture.
7. Save packet captured file.
8. Save httpwatch log.

A direct packet capture helps JTAC understand how the application works. This will serve as a comparable example what data is changed through the rewrite engine and help determine the root cause of the issue.

**APPENDIX I**

## Alternate Access mechanism that could solve / avoid the reported rewrite problem.

SA provides different access mechanisms other than rewrite to safely access backend resource. They are:

## 1. *Network Connect (NC)*

The Network Connect access option provides a VPN user experience, serving as an additional remote access mechanism to corporate resources using Junos Pulse Secure Access. This feature supports all Internet-access modes, including dial-up, broadband, and LAN scenarios, from the client machine and works through client side proxies and firewalls that allow SSL traffic.

Refer NC configuration guide for more details on how to configure NC to access a protected resources: http://www.juniper.net/techpubs/software/ive/guides/howtos/How_To_NC_Config.p**Error! Hyperlink reference not valid.**

## *2. Secure Application Manager (SAM)*

The Secure Application Manager option provides secure, application-level remote access to enterprise servers from client applications. You may deploy two versions of the Secure Application Manager:

***a) Windows version (WSAM)—***The Windows version of the Secure Application Manager is a Windows-based solution that enables you to secure traffic to individual client/server applications and application servers.

Refer Secure Application Manager section under latest administrator guide for more details on how to configure JSAM to access a protected resources: http://www.juniper.net/techpubs/software/ive/admin/j-sa-sslvpn-7.0-admingui**Error! Hyperlink reference not valid.**

***b) Java version (JSAM)—***The Java version of the Secure Application Manager provides support for static TCP port client/server applications, including enhanced support for Microsoft MAPI, Lotus Notes, and Citrix NFuse. JSAM also provides NetBIOS support, which enables users to map drives to specified protected resources.

Refer JSAM configuration guide for more details on how to configure JSAM to access a protected resources:
http://www.juniper.net/techpubs/software/ive/guides/howtos/How_To_JSAM.p**Error! Hyperlink reference not valid.**

**APPENDIX II**

## How can JSAM access to backend resources help JTAC in troubleshooting / fixing rewrite issue better?

- Use the following link which has step by step instruction on to provide JSAM access for a backend application resource http://www.juniper.net/techpubs/software/ive/guides/howtos/How_To_JSAM.p**Error! Hyperlink reference not valid.**
- Providing JTAC with access to same backend resource via JSAM will speed up issue identification and there after help engineering develop / test a fix that may be developed for the issue in the event a problem is identified in the SA rewrite engine.
- JSAM access is only for connectivity purposes for JTAC in order to access customer backend resources.
- With JSAM access JTAC will be able to replicate the issue using different browsers in their lab environment using various test devices, running different OS versions.
- This ensures that customer does not have to make any additional changes required for troubleshooting on their production SAs; all changes / testing will be performed on JTAC lab environment.
- Once JTAC can replicate the reported rewrite issue using customer provided JSAM access to backend resource all log collection can also be captured on the LAB environment.