**WCG SSL decryption**

Please search KB articles and relevant release notes to identify a match with any existing known issues before escalating.

General SSL debugging steps:

1. Logs: – set inbound and outbound logs to level 7 and enable access logs.
2. SSL logs can roll over quickly in high load environments, so logs should be captured ASAP after the problem happens.
3. With level 7 logging, collect the entire /opt/WCG/sxsuite/log folder (Configuploader only gives the most recent logs and may only have a few minutes of traffic).
4. Remember – inbound is browser<->proxy, outbound is proxy<->web server
5. To check if a connection is tunneled, look for Next Proxy messages in inbound.log (level 7 needed) – tHTTPS is tunneled, HTTPS is decrypted
6. Decryption bypass for explicit proxy does NOT go through Microdasys, transparent proxy does.

Symptom:

Decryption disabled alert.

Actions:

* This alert can happen when configuration changes are made and should be ignored in that case.
* In addition to normal logging (see above) enable CAS logging:

oemtool globalconfig cas\_log yes

* Also collect /var/log/messages
* Again logs must be gathered immediately after the alert or the required data will be lost.

Symptom:

VERIFY DENY page displayed

Actions:

* ‘Verify deny’ is a generic error. You need to look at the specific error message.
* Certificate errors (self-signed, untrusted, expired etc):

There is a validation problem with the server certificate. If the customer thinks this is a mistake, they should inspect the certificate (use a non-proxy connect to get the certificate) and decide if it should be trusted. To trust a certificate with an error, find the incident for that URL and change to “Allow”.

* Handshake errors:

This indicates a problem establishing an SSL connection to the server.

Check outbound encryption settings – protocol or cipherlist may be incompatible

For some obsolete servers, setting disable\_SNI yes MAY be required. Don’t use this as a catch-all fix unless you are sure it resolves a problem.

Symptom:

Browser/Client errors

Actions:

* Check inbound protocol and cipher settings to make sure these are compatible.
* Make sure root CA certificate is installed as a trusted root CA
* Some browsers and applications have their own root CA store, check their docs if available
* Some applications will never accept our certificates – if all else fails, tunnel.