**WCG NTLM Authentication failures**

Symptoms:

1. Clients can’t authenticate after entering credentials in an auth prompt
2. Clients are presented with an authentication prompt when they should be authenticated transparently

Actions and Data to gather:

1. Reference KB Article: <https://emea.salesforce.com/kA5200000004CY8>
2. Search KB articles and relevant release notes to identify a match with any existing known issues.
3. WCG Config Uploader files
4. Explicit or WCCP
5. AD 2008 or AD 2003, NTLMv2 or NTLMv1
6. Client OS and browser type and version
7. When did the issue start occurring?  Right after a fresh install?  After a specific action or change to the environment? New DC added? New firewall, or other hardware device?
8. Reproduce issue with the following enabled:
   1. NTLM debug tags
   2. Pcaps capturing client, proxy and targeted DC
9. Check content\_gateway.out NTLM debug for any signs of maxing out on DC connections.  Ensure load balancing is enabled as appropriate and increase dc max connections in records.config to 30 from default of 10.  Retest and recheck content\_gateway.out.
10. Gather client and DC LM settings, ie NTLMv2, session security See the how to below.
11. If NTLM cache is disabled, determine why it’s disabled, and re-enable if appropriate.  A common reason for disabling NTLM cache is a NAT’ed environment.
12. What is the current load?
13. Gathering LM settings on both client and DC:
    1. NTLMv2 discussion:

<http://forums.websense.com/topic.asp?TOPIC_ID=8441>

* 1. DC settings:
     1. Open up “Start->Administrative Tools->Domain Controller Security Policy”
     2. Navigate to “Security Settings->Local Policies->Security Options
     3. Network security: LAN Manager authentication level should be set to one of the following (non NTLMv2 settings):
        1. Send LM & NTLM responses
        2. Send LM & NTLM – Use NTLMv2 sessions security if negotiated
        3. Send NTLM Responses only
  2. Client settings:
     1. Start->Run->secpol.msc
     2. Navigate to “Security Settings->Local Policies->Security Options
     3. Network security: LAN Manager authentication level should be set to one of the following (non NTLMv2 settings):
        1. Send LM & NTLM responses
        2. Send LM & NTLM – Use NTLMv2 sessions security if negotiated
        3. Send NTLM Responses only