

Using Integrated Windows Authentication with Websense Content Gateway, v7.6

Websense Support Webinar August 2011

Support Webinars

- Introduction to Integrated Windows Authentication
- How to configure Integrated Windows Authentication
- How to use IWA with Multiple Realm Authentication
- Web browsers and IWA
- Troubleshooting IWA



Ravi Desai

- Title: Technical Support Specialist
- Accomplishments:
 - Over 4 years supporting Websense products
- Education / Certifications:
 - B.Eng (Hons) Computer Systems and Networks
 - CCNA
 - MCP
 - WCWSA – Websense Certified Web Security Associate

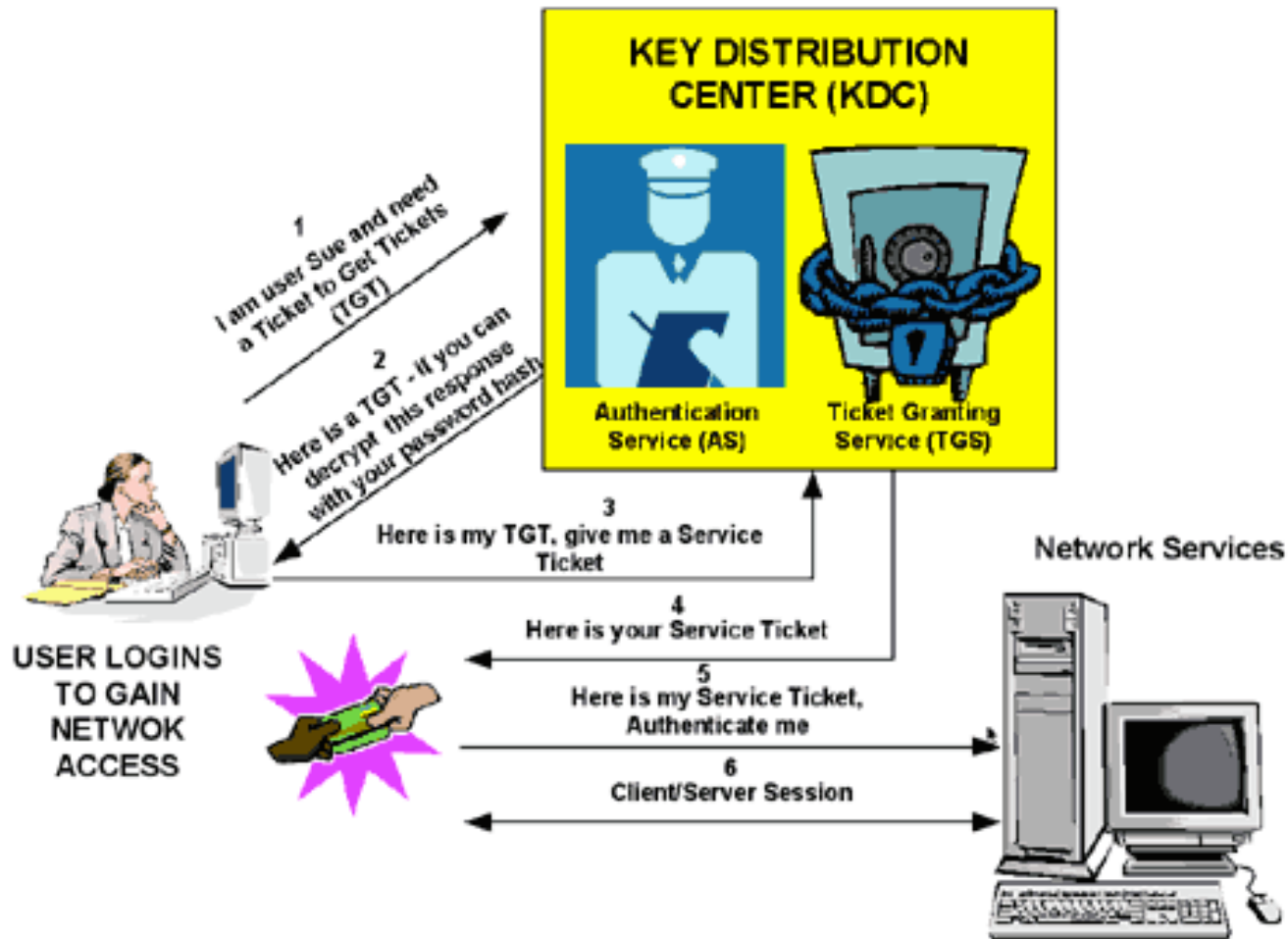
- Provides a secure and robust method of authenticating users belonging to shared-trust, Windows domains (one or many)
- Uses Kerberos
- Supports Windows Active Directory 2003 and 2008
- Supports NTLMv2 with session security and NTLMv1 with session security
- Falls back to interactive authentication on failure
- Can be used with Multiple Realm Authentication option
- All clients need to be joined to a trusted domain
- Browsers specify FQDN of the proxy as an intranet or trusted site

■ Common terms:

- KDS/KDC = Key Distribution Server/Center
- AS = Authentication Server/Service
- SS = Service Server/Service
- TGS = Ticket-Granting Server
- TGT = Ticket Granting Ticket/Ticket to Grant Ticket
- ST = Service Ticket
- SPN = service principle name
 - TYPE/principle@domain
 - HTTP/www.foo.com@foo.com

Kerberos - Microsoft's view

KERBEROS TICKET EXCHANGE



- Client requests and gets TGT using user credentials
 - TGT is good for a period of time (10 hrs by default)
- Client connects to the service
- Service challenges for Kerberos
- Client requests and gets ST for SPN using TGT
 - HTTP server/proxy always HTTP/www.foo.com
 - ST good for a period of time (10 hrs by default)
- Client presents challenge response

- Verify that time is synchronized among systems
- Enter the fully qualified proxy name in DNS
- Enable IWA in Content Gateway Manager
 - Go to Configure -> My Proxy -> Basic

Authentication	
None	<input type="radio"/>
Integrated Windows Authentication	<input checked="" type="radio"/>
LDAP	<input type="radio"/>
Radius	<input type="radio"/>
Legacy NTLM	<input type="radio"/>
Multiple Realm Authentication	<input type="radio"/>

Join Content Gateway to the domain

- Go to Configure -> Security -> Access Control -> Integrated Window Authentication

Filtering **Integrated Windows Authentication** **Global Authentication Options** **Transparent Proxy Authentication**

Single Domain Authentication

Apply Cancel

Windows Domain

User authentication is performed using the specified domain.

Domain Membership Status: **Joined** **Unjoin**

Realm Name:

Fully Qualified Domain Name:

Content Gateway DNS Hostname:

Domain Controller: Auto-detect using DNS **Test** DC name or IP address:

- Proxy clients must specify this hostname in the browser proxy settings for Kerberos authentication to occur.
- Specifies the name or IP address of the domain controller. Backup servers can be specified in a comma separated list.

Diagnose authentication problems: **Troubleshoot Authentication**

Apply Cancel

- Configure client browsers to use the FQDN of the proxy
- Kerberos authentication does not require communication between Content Gateway and the KDC at user authentication time
- Some browsers (Firefox) require that Kerberos be enabled and SPN white listed
- Browsers must connect to the service using a FQDN, else authentication falls back to NTLM, if possible

- What is Multi Realm Authentication
- Used for environments having multiple isolated domains
- Users in these domains need to be authenticated by a domain controller in their own domain. With respect to this feature, these domains are called realms
- If users in the network can be authenticated by a DC having a trust relationship then multi realm rules need not be created

Multiple Realm Authentication

- Content Gateway can authenticate users from multiple domains using this option
- Multiple realm authentication option must be selected in Configure -> My Proxy -> Basic
- Join the required domains to Content Gateway via the Configure -> Security -> Access Control -> Domains section
- Demo

Joined Domains

UKLAB-WS

Realm Name: UKLAB-WS

Fully Qualified Domain Name: uklab-ws.com

Content Gateway DNS Hostname: wibble.uklab-ws.com

Domain Controller:

Auto-detect using DNS **Test**

DC name or IP address:

Unjoin Domain

● Proxy clients must specify this hostname in the browser proxy settings for Kerberos authentication to occur.

● Specifies the name or IP address of the domain controller. Backup servers can be specified in a comma separated list.

Apply Cancel

Multiple Realm Authentication

- Before creating an IWA realm rule, each realm's domain must be joined to Content Gateway
- Rules can be specified for realms that are authenticated with IWA, Legacy NTLM, or LDAP
- Rules are stored in auth.config

■ Filtering ■ Domains ■ **Authentication Realms** ■ Global Authentication Options ■ Transparent Proxy Authentication

Multiple Realm Authentication

Apply Cancel

Authentication

The "auth.config" file lets you define rules for authenticating users by source IP address and/or proxy port. A domain must be joined before it can be specified in a Windows Authentication rule.

Rule Type	Rule Name	Source IP	Enabled	LDAP/NTLM Options	LDAP Attributes (Optional)
winauth	uklab	10.1.1.1,10.5.23.35	1		
winauth	aok	10.1.1.2	1		

Refresh Edit File

Apply Cancel

- IWA is supported with Internet Explorer 7, 8, and 9, Firefox 3 and 4, Google Chrome 6, 7, 8, 9, and 10, Windows Safari 4 and 5, Safari 4 on iPad iOS4, and Opera 10
- Browser must connect to service using a FQDN
 - Explicit – FQDN in proxy config
 - Transparent – Redirect hostname must be FQDN
 - Both – FQDN must match Content Gateway domain hostname
 - Client must be able to talk to TGT or have valid ST

■ Failure to join domain

– Prerequisites not met:

- Content Gateway must be able to resolve the domain name
- Content Gateway system time must be in sync with domain controllers to +/- 1 minute
- Must have correct domain admin credentials to join
- Must have TCP/UDP connectivity to domain controller/s (port 88, 389, 445)

The screenshot shows the 'Integrated Windows Authentication' configuration page. At the top, there are four tabs: 'Filtering', 'Integrated Windows Authentication', 'Global Authentication Options', and 'Transparent Proxy Authentication'. Below the tabs, the 'Single Domain Authentication' section is active. A red box highlights a message: 'Failed to join domain. Click here to view the failure log'. Below this, the 'Windows Domain' section is visible, with a note: 'User authentication is performed using the specified domain.' There are two input fields: 'Domain Name:' and 'Administrator Name:'. To the right of the 'Domain Name:' field is a bullet point: '• Specifies a fully qualified domain name.' To the right of the 'Administrator Name:' field is a bullet point: '• Specifies the Windows Domain Administrator user name.'

- Domain join failure messages are displayed in Content Gateway Manager
- Join failures are logged in:
`/opt/WCG/logs/smbadmin.join.log`
- Failure messages are common Kerberos and Samba error messages and codes. Use Google to find their meaning

- Clients fail to authenticate
- Testing problems between Content Gateway and the domain controllers: Use the Test button in the GUI to troubleshoot
- Prerequisites
 - Proxy clients must belong to the domain that Content Gateway belongs to, or belong to a domain that has a mutual trust relationship
 - Client system time must be in sync with the domain controller and Content Gateway
 - Explicit proxy clients must ***NOT*** be configured with the IP address of Content Gateway in the proxy config/PAC file.
 - Must use FQDN of Content Gateway or only NTLM authentication will be used
 - Content Gateway FQDN must be in DNS and resolvable by all proxy clients
 - Content Gateway must have connectivity to the domain controller(s) to join and fallback to NTLM

Client fails to authenticate

Integrated Windows Authentication Statistics

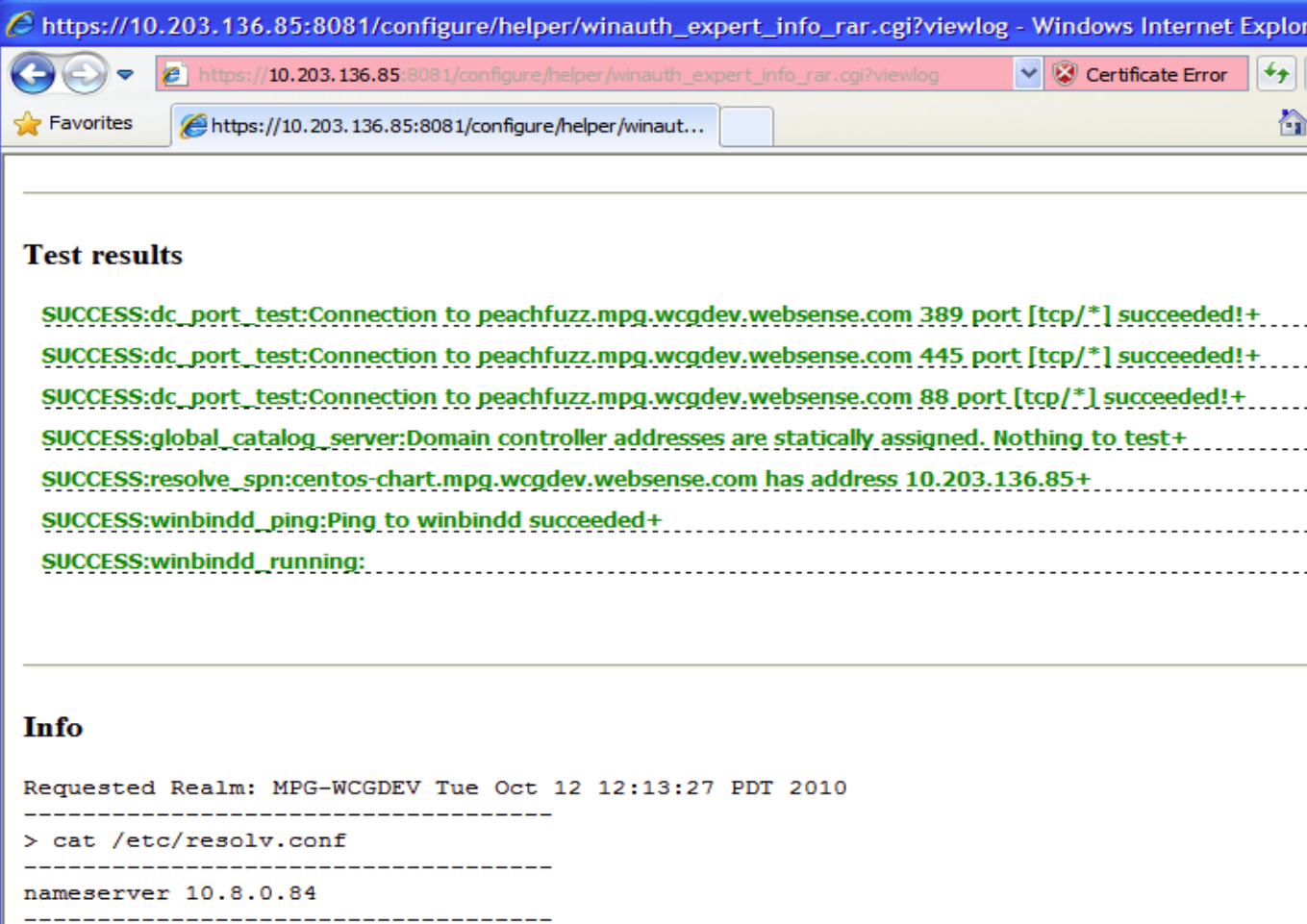
Attribute	Current Value
Kerberos request counters	
Total Kerberos requests	0
Authentication succeeded	0
Authentication failed	0
Kerberos errors	0
NTLM request counters	
Total NTLM requests	0
Authentication succeeded	0
Authentication failed	0
NTLM request errors	0
NTLM within negotiate requests	0
Basic authentication request counters	
Total basic authentication requests	0
Authentication succeeded	0
Authentication failed	0
Basic authentication request errors	0
Performance counters	
Kerberos - Average time per transaction	0.00 ms
NTLM - Average time per transaction	0.00 ms
Basic - Average time per transaction	0.00 ms
Average helper latency per transaction	0.00 ms

Diagnostic Test

MPG-WCGDEV

- Command line available but not necessary because the same output is in the UI
 - /opt/WCG/bin/SMBAdmin techsupport [REALM]
 - /opt/WCG/bin/SMBAdmin testall
- Log files involved:
 - /var/log/messages
 - /opt/WCG/logs/content_gateway.out
 - /opt/WCG/logs/smbadmin.log
 - /opt/WCG/logs/smbadmin.join.log

■ Test results in UI



https://10.203.136.85:8081/configure/helper/winauth_expert_info_rar.cgi?viewlog - Windows Internet Explorer

https://10.203.136.85:8081/configure/helper/winauth_expert_info_rar.cgi?viewlog Certificate Error

https://10.203.136.85:8081/configure/helper/winaut...

Test results

SUCCESS:dc_port_test:Connection to peachfuzz.mpg.wcgdev.websense.com 389 port [tcp/*] succeeded!+
SUCCESS:dc_port_test:Connection to peachfuzz.mpg.wcgdev.websense.com 445 port [tcp/*] succeeded!+
SUCCESS:dc_port_test:Connection to peachfuzz.mpg.wcgdev.websense.com 88 port [tcp/*] succeeded!+
SUCCESS:global_catalog_server:Domain controller addresses are statically assigned. Nothing to test+
SUCCESS:resolve_spn:centos-chart.mpg.wcgdev.websense.com has address 10.203.136.85+
SUCCESS:winbindd_ping:Ping to winbindd succeeded+
SUCCESS:winbindd_running:

Info

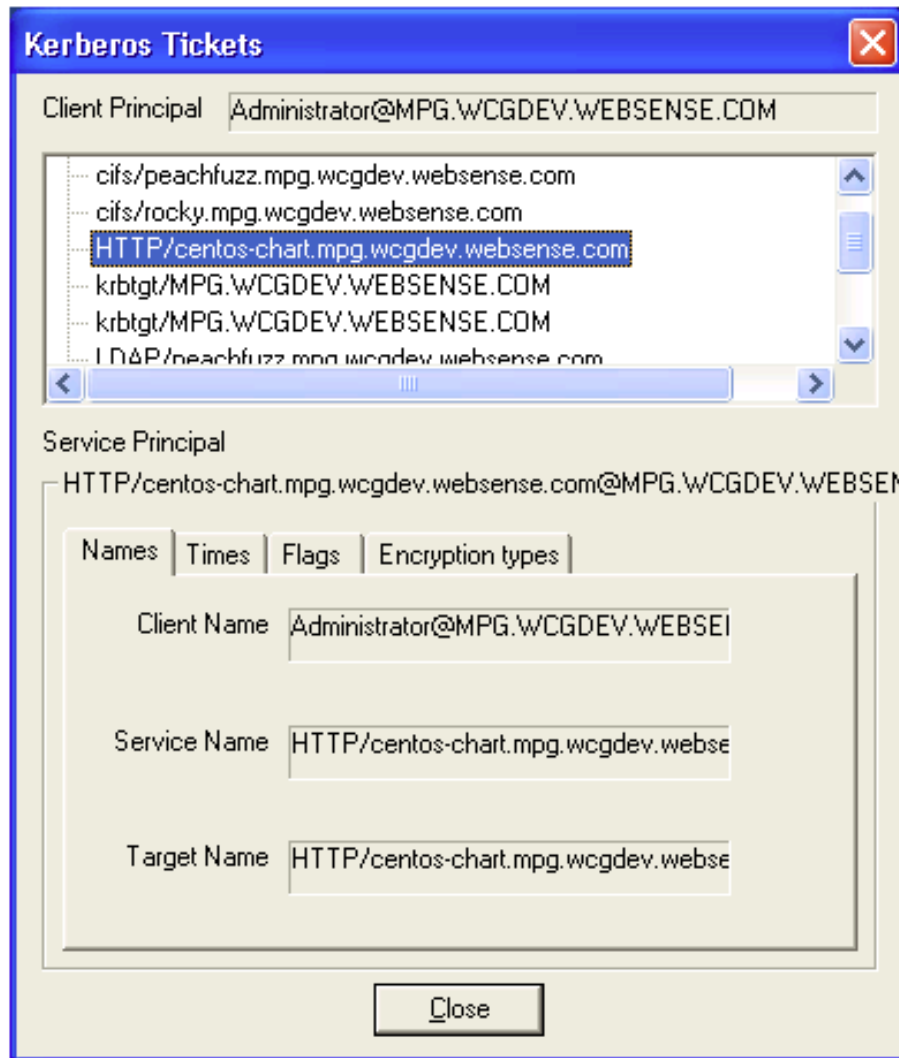
Requested Realm: MPG-WCGDEV Tue Oct 12 12:13:27 PDT 2010

> cat /etc/resolv.conf

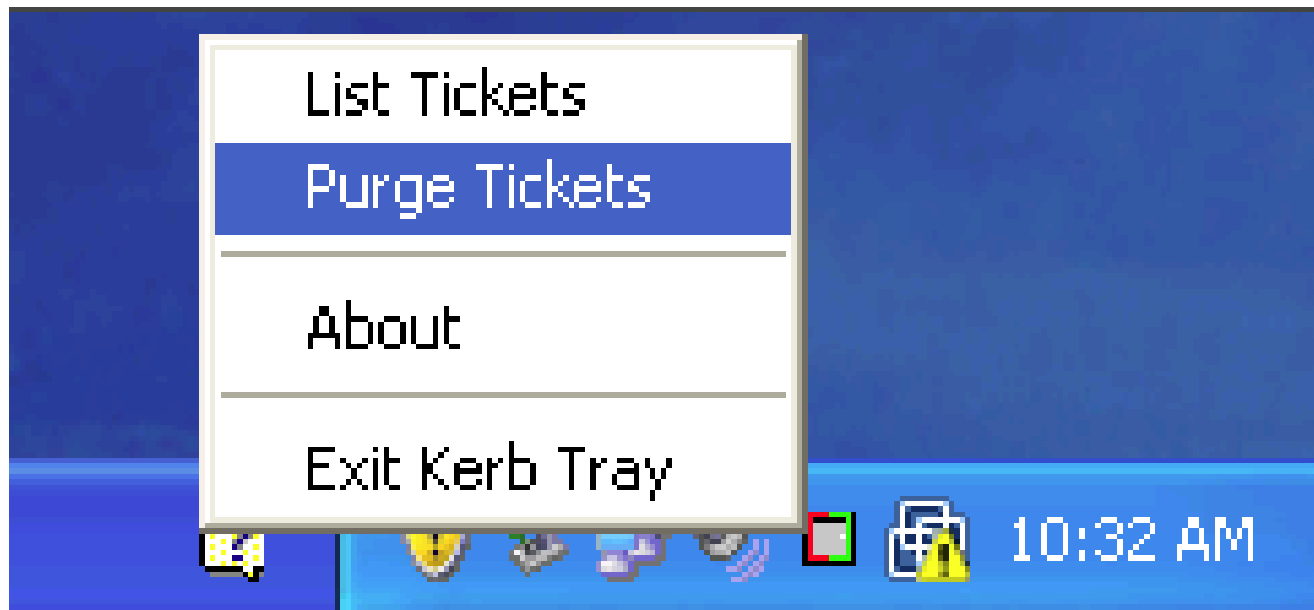
nameserver 10.8.0.84

- Testing problems between Content Gateway and clients
 - For new deployments, start with a functional Content Gateway *without* authentication turned on
 - Is the explicit proxy client configured with the FQDN of Content Gateway? If not the client will only do NTLM authentication.
 - Can the client resolve the proxy's FQDN?
 - Can the client obtain Content Gateway service tickets?

- Download the Windows utility [kerbtray.exe](http://www.microsoft.com/downloads/en/details.aspx?familyid=4E3A58BE-29F6-49F6-85BE-E866AF8E7A88&displaylang=en) from:
<http://www.microsoft.com/downloads/en/details.aspx?familyid=4E3A58BE-29F6-49F6-85BE-E866AF8E7A88&displaylang=en>
- Open a browser and send traffic through the proxy
- Look at kerbtray – You should see “HTTP/WCGFQDN”



- If all else fails, right click the kerbtray systray icon and click “Purge tickets”
- Log out of Windows and log back in again



- Run a packet capture using Wireshark
 - Purge tickets in kerbtray
 - Start capture using the correct port
 - Try to browse to a site
 - Stop the capture and analyze

- Can enable debug tags **winauth.*** and **winauthp.*** in records.config to enable debugging for Kerberos authentication (**win.*** could cover both)
- Debug output is sent to:
/opt/WCG/logs/content_gateway.out
- Samba debug can be enabled from:
/opt/WCG/contrib/samba/etc/smb.conf

- Microsoft error codes:
[http://msdn.microsoft.com/en-us/library/ms681382\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms681382(VS.85).aspx)

- Some sample error codes:

```
smb_err_desc smb_err_dos[] = {
    {SMB_ERRDOS_BADFUNC, "Invalid function"},
    {SMB_ERRDOS_BADFILE, "File not found"},
    {SMB_ERRDOS_BADPATH, "Directory invalid"},
    {SMB_ERRDOS_NOFIDS, "Too many open files"},
    {SMB_ERRDOS_NOACCESS, "Access denied, the client's context
does not"},
    {SMB_ERRDOS_BADFID, "Invalid file handle"},
    {SMB_ERRDOS_BADMCB, "Memory control blocks destroyed"},
    {SMB_ERRDOS_NOMEM, "Insufficient server memory"},
    {SMB_ERRDOS_BADMEM, "Invalid memory block address"},
    {SMB_ERRDOS_BADENV, "Invalid environment"},
    {SMB_ERRDOS_BADFORMAT, "Invalid format"},
    {SMB_ERRDOS_BADACCESS, "Invalid open mode"},
    {SMB_ERRDOS_BADDATA, "Invalid IOCTL data"},
    {SMB_ERRDOS_BADDRIVE, "Invalid drive specified"},
    {SMB_ERRDOS_REMCD, "Can not remove server's current
directory"},
    {SMB_ERRDOS_DIFFDEVICE, "Not same device"},
}
```

- Microsoft error code definitions:

<http://msdn.microsoft.com/en-us/library/aa370674%28v=vs.85%29.aspx>

```
Oct 10 05:10:08 dk-gevelwbsn02-wcg content_gateway[20936]: WARNING: DC
replied with error:2215 for user LAB01.GAAB from host 045SK-LABB38001
Oct 10 05:10:08 dk-gevelwbsn02-wcg content_gateway[20936]: WARNING: DC
replied with error:2215 for user LAB01.GAAB from host 045SK-LABB38001
Oct 10 05:10:16 dk-gevelwbsn02-wcg content_gateway[20936]: WARNING: DC
replied with error:2215 for user LAB01.GAAB from host 045SK-LABB38001
Oct 10 05:10:16 dk-gevelwbsn02-wcg content_gateway[20936]: WARNING: DC
replied with error:2215 for user LAB01.GAAB from host 045SK-LABB38001
Oct 10 05:10:18 dk-gevelwbsn02-wcg content_gateway[20936]: WARNING: DC replied with
error:2215 for user MD.PBC-SK from host 421PA-PBCPROD03
```

Kerberos Resources

- http://www.youtube.com/results?search_query=Kerberos+Authentication+Demo
- <http://technet.microsoft.com/en-us/library/bb742516.aspx>
- [http://en.wikipedia.org/wiki/Kerberos_\(protocol\)](http://en.wikipedia.org/wiki/Kerberos_(protocol))

Knowledge Base

- Search or browse the knowledge base for documentation, downloads, top knowledge base articles, and solutions specific to your product.

Support Forums

- Share questions, offer solutions and suggestions with experienced Websense Customers regarding product Best Practices, Deployment, Installation, Configuration, and other product topics.

Tech Alerts

- Subscribe to receive product specific alerts that automatically notify you anytime Websense issues new releases, critical hot-fixes, or other technical information.

ask.websense.com

- Create and manage support service requests using our online portal.

Webinar Update

Title: Installing, upgrading, and managing reporting databases for Websense Web Security v7.6

Date: September 21, 2011

Time: 8:30 A.M. PDT (GMT -7)

How to register:

<http://www.websense.com/content/SupportWebinars.aspx>

Customer Training Options

- To find Websense classes offered by Authorized Training Partners in your area, visit: <http://www.websense.com/findaclass>
- Websense Training Partners also offer classes online and onsite at your location
- For more information, please send email to: readiness@websense.com

WEBSense®
**Authorized Training
Partner**

WEBSense®
Certified Instructor



Questions?

