Configuration Instructions for a DB4 Server on Windows Operating Systems

FPS GOLD[®] recommends that a new user, "DB4User," be set up on the DB4 server for the DB4 engine. This is for security purposes. Set up the user first before configuring the DB4 server. The user can either be a domain user or a local user.

To set up a DB4 user, complete the following steps.

- **Step 1** Click <START> on the desktop.
- Step 2 Select Control Panel, then Administrative Tools, then Computer Management.

📕 Computer Management		
■ File Action View Window He ← → € I □ □ □ 20	łp	
Computer Management (Local) System Tools Event Viewer Shared Folders Cocal Users and Groups Cocal Users and Groups Device Manager Storage Cocal Users and Groups Cocal Users Cocal Users and Groups Cocal Users Cocal Users and Groups Cocal Users Cocal Us	Name Users Groups	

Step 3 Select Local Users and Groups.

Follow procedures for adding a new User.

- We suggest the username of **DB4User**.
- Type a description in the **DESCRIPTION** field, indicating that this user is set up for the DHI DB4Engine.
- Remember the password because it will be needed later in the setup.
- Select "Password Never Expires."
- This user must be a local administrator. We also suggest limiting this user logon abilities to this computer only.

To configure the DB4 server, complete the following steps.

- **Step 1** Click <START> on the desktop.
- **Step 2** Select Run.... The Run dialog will appear.
- **Step 3** Type "dcomcnfg" in the **OPEN** field.

Run	? 🛛
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	dcomcnfg 🗸
	OK Cancel Browse

Step 4 Click OK. The Component Services dialog will appear.

Component Services		
🐌 Eile <u>A</u> ction <u>V</u> iew <u>W</u> indow <u>H</u> elp		_8×
Console Root	Console Root	
Component Services	Name	
+ Services (Local)	Component Services	
	Event Viewer (Local)	
	shares (receiv	

Step 5 Click on Component Services and open up the explorer view tree until you see My Computer



Step 6 Right Click on My Computer and select Properties and then select the Default Properties Tab. Make sure that the Enable Distributed COM on this Computer is checked. Set the Default Authentication Level to Connect Set the Default Impersonation Level to Identify

Default Protocols	MSDTC	COM Security
General	Options	Default Properties
Enable Distribute	d COM on this computer	
Enable COM Inte	met Services on this comp	uter
Default Distributed	COM Communication Prop	erties
The Authentication	Level specifies security at	the packet level.
Dofouilt Authoritie	ation Lough	
Derault Authentic	auon Level.	
Connect		
Connect	level specifies whether an	lications can determine
Connect The impersonation who is calling them using the client's id Default Imperson	level specifies whether application and whether the application of the second s	plications can determine ion can do operations
Connect The impersonation who is calling them using the client's id Default Imperson Identify	level specifies whether application and whether the application the specifies whether application the specific action the spec	plications can determine ion can do operations

Step 7 Select the Com Security Tab. You should see two new buttons called Edit Limits

General	Options	Default Properties
Default Protocols	MSDTC	COM Security
ccess Permissions -		
You may edit who is	s allowed default access	to applications. You may
also sec limits on ap	plications that determine	trieli own permissions.
\rightarrow	Edit <u>L</u> imits	Edit Default
1 11 11 11	- · ·	
aunch and Activation	n Permissions	
aunch and Activation You may edit who is activate objects. Yo	n Permissions s allowed by default to la ou may also set limits on j	unch applications or applications that
aunch and Activation You may edit who is activate objects. Yo determine their own	n Permissions s allowed by default to la ou may also set limits on opermissions.	unch applications or applications that
aunch and Activation You may edit who is activate objects. Yo determine their own	n Permissions s allowed by default to la pu may also set limits on permissions. Edit Limits	unch applications or applications that Edit Default
aunch and Activation You may edit who is activate objects. Yo determine their own	n Permissions s allowed by default to la ou may also set limits on permissions. 	unch applications or applications that Edit <u>D</u> efault
aunch and Activation You may edit who is activate objects. Yo determine their own	n Permissions s allowed by default to la pu may also set limits on permissions. Edit Limits	unch applications or applications that Edit <u>D</u> efault
aunch and Activation You may edit who is activate objects. Yo determine their own	n Permissions s allowed by default to la ou may also set limits on permissions. Edit Ljmits	unch applications or applications that Edit <u>D</u> efault
aunch and Activation You may edit who is activate objects. Yo determine their own	n Permissions s allowed by default to la pu may also set limits on permissions. Edit Ljmits	unch applications or applications that Edit <u>D</u> efault
aunch and Activation You may edit who is activate objects. Yo determine their own	n Permissions s allowed by default to la ou may also set limits on permissions. Edit Ljmits	unch applications or applications that Edit <u>D</u> efault
aunch and Activation You may edit who is activate objects. Yo determine their own	n Permissions s allowed by default to la pu may also set limits on permissions. Edit Ljmits	unch applications or applications that Edit <u>D</u> efault

Step 8 Click on the Edit Limits for Access Permissions.

Access Permission		? 🔀
Security Limits		
Group or user names:		
ANONYMOUS LOGON		
🕵 Everyone		
	A <u>d</u> d	<u>R</u> emove
Permissions for ANUNYMUUS	Allow	Deny
Local Access	>	
Hemote Access		
1		
	OK	Cancel

Make sure that **Anonymous Logon** and **Everyone** are in the group / user name with full permissions for local and remote access. Click **Add** to add them if they are not in the group

Select Users , Computers , or Groups	? 🛛
Select this object type:	
Users, Groups, or Built-in security principals	Object Types
Erom this location:	
dhi.local	Locations
Enter the object names to select (<u>examples</u>):	
ANONYMOUS LOGON	Check Names
Advanced	OK Cancel

Step 9 Click on OK and then Click on Apply

Step 10 Click on the Edit Limits for Launch and Activation Permissions.

Launch Permission		? 🛛
Security Limits		
Group or user names:	-XP\Administrato	re]
ANONYMOUS LOGON		
	Add	Remove
Permissions for Administrators	Allow	Deny
Local Launch Remote Launch Local Activation		
Remote Activation		
	ОК	Cancel

Make sure that you have **Anonymous Logon** and **Everyone** with full security for all options also in this area.

Step 11 Click on Apply and then Click on OK. You are now back to Component Services.

DHI.DB4Engine Section

Step 1 Open the Tree View for DCOM Config.

Step 2 Select "DHI.DB4Engine" from the list of available applications.



Step 3 Right Click on DHI.DB4Engine and choose Properties. The DHI.DB4Engine Properties dialog will appear.

Step 4 From the General tab choose Authentication Level <u>None</u>.



Step 5 Click on Apply.

DHI.DB4Engine Properties	? 🛛
General Location Security Endpoints Identity	
Launch and Activation Permissions	
C <u>U</u> se Default	
© Customize	<u>E</u> dit
Access Permissions	
Use Default	
C Custo <u>m</u> ize	Edit
Configuration Permissions	
C Use Default	
 Customize 	Edjt
OK Car	

Step 6 Select **Customize** for Launch and Activation Permissions.

Step 7 Click the <EDIT...> button associated with this security option. The Launch Permission dialog will appear.

ich Permission		?
surity		
oup or user names:		
Administrators (STEVENPVA	dministrators)	
ANONYMOUS LOGON		
🕺 Everyone		
2 SYSTEM		
	Add	<u>R</u> emove
ermissions for ANONYMOUS)GON	Allow	Deny
Local Launch	~	
Remote Launch	\checkmark	
Local Activation		
Remote Activation	 Image: A start of the start of	
	Οκ	Cance
	OK]_

- **Step 8** Verify that **Anonymous Logon**, **Everyone** and **System** are selected. They will be displayed in Group or user names box. These users/groups must be set up with all "Allow" security.
 - (Use the <ADD...> button if these users/groups need to be added.) NOTE: Any other users/groups that are already selected may remain. You may, however, delete "Interactive" if it is selected.

Select Users , Computers , or Groups	? 🛛
Select this object type:	
Users, Groups, or Built-in security principals	Dbject Types
From this location:	
dhi.local	Locations
Enter the object names to select (examples):	
anonymous logon; everyone	Check Names
Advanced	UK Cancel

Type in the names of the needed users. Separated with a semi-colon and space.

Step 9	Click OK	and then	on Apply.
--------	----------	----------	-----------

DHI.DB41	Engine Pr	operties	5		? 🛛
General	Location	Security	Endpoints	Identity	
Which	user accou	nt do you v	vant to use to	o run this applic	ation?
C The	interactive	user.			
C The	Jaunching	user.			
 This 	s <u>u</u> ser.				
Us <u>e</u> r:		F	STEVENP\D	B4User	Browse
Passi	word:	ŀ	****		
Co <u>n</u> fi	rm passwor	± ['	****		
C The	system ac	count (serv	vices only).		
		(OK	Cancel	

- **Step 11** Select "This user" to answer the question, "Which user account do you want to use to run this application?"
- **Step 12** Click <BROWSE...>. The Browse for Users dialog will appear.
- Step 13 Select the DB4User.
- **Step 14** Type the password associated with the DB4 user in the **PASSWORD** field.
- **Step 15** Type the password again in the **CONFIRM PASSWORD** field.
- Step 16 Click on Apply and then Click on OK. You are now back to Component Services.

DHILocate or Locater Class Section

Step 1 Select **DHILocate** from the list of available applications.



Step 2 Right Click on DHILocate and choose Properties. The DHILocate Properties dialog will appear.

Step 3 From the General tab choose Authentication Level <u>None</u>.



Step 4 Click on Apply.

DHILocate Properties	? 🛛
General Location Security E	Indpoints Identity
Launch and Activation Perr	nissions
C <u>U</u> se Default	
Customize	<u> </u>
Access Permissions	
C Use De <u>f</u> ault	
• Custo <u>m</u> ize	<u>Edit</u>
Configuration Permissions –	
C Use Defa <u>u</u> lt	
Customize	E dit
	OK Cancel Apply

Step 6 Select **Customize** for Launch and Activation Permissions.

Step 7 Click the <EDIT...> button associated with this security option. The Launch Permission dialog will appear.

unch Permission		?
ecurity		
<u>G</u> roup or user names:		
Administrators (STEVENP\Ad	dministrators)	
ANONYMOUS LOGON		
SYSTEM		
	Add	<u>R</u> emove
LOGON	Allow	Deny
Local Launch	~	
Remote Launch	~	
Local Activation		
Remote Activation	×	
	ОК	Cancel

- **Step 8** Verify that **Anonymous Logon** and **Everyone** are selected. They will be displayed in the Group or user names box. These users/groups must be set up with all "Allow" security.
 - (Use the <ADD...> button if these users/groups need to be added.) **NOTE**: Any other users/groups that are already selected may remain. You may, however, delete "Interactive" if it is selected.
- Step 9 Click OK and then Apply.

Step 10 Select Customize for Access Permissions.

DHILocate Properties	? 🛛
General Location Security Endpoints Ider	ntity
Launch and Activation Permissions	
C <u>U</u> se Default	
Customize	Edit
Access Permissions	
C Use De <u>f</u> ault	
© Custo <u>m</u> ize	E <u>d</u> it
Configuration Permissions	
C Use Defa <u>u</u> lt	
 Customize 	Edit
ОК (Cancel Apply

Step 11 Click the <EDIT...> button associated with this security option. The Registry Value Permissions dialog will appear.

Access Permission		? 🛛
Security		
Group or user names:		
🕵 Everyone		
SYSTEM		
	<u>Add</u>	<u>R</u> emove
Permissions for Everyone	Allow	Deny
Local Access	 Image: A start of the start of	
Hemote Access		
	ОК	Cancel

- **Step 12** Verify that **Everyone** is selected. It will be displayed in the Group or user names box. This user/group must be set up with all "Allow " security.
 - (Use the <ADD...> button if this user/group needs to be added.) **NOTE**: Any other users/groups that are already selected may remain. You may, however, delete "Interactive" if it is selected.
- Step 13 Click OK and then Apply.



- **Step 15** Select "This user" to answer the question, "Which user account do you want to use to run this application?"
- **Step 16** Click <BROWSE...>. The Browse for Users dialog will appear.
- Step 17 Select the DB4User.
- Step 18 Type the password associated with the DB4 user in the PASSWORD field.
- Step 19 Type the password again in the CONFIRM PASSWORD field.
- Step 20 Click Apply and then OK.

DHI.QuerySvr Section (For DB4 Servers that will also support GOLDTrakPC)

- **Step 1** Select "DHI.QuerySvr" from the list of available applications.
- **Step 2 Right** Click DHI.QuerySvr and choose **Properties**. The DHI.QuerySvr Properties dialog will appear.



Step 3 From the General tab choose Authentication Level <u>None</u>.



Step 4 Click on Apply.

DHI.QuerySvr Properties	
General Location Security Endpoints Identity	
Launch and Activation Permissions	
© Customize ▲	
Access Permissions © Use De <u>f</u> ault	
C Customize	
Configuration Permissions	
• Customize Edit	
OK Cancel Apply	

Step 6 Select **Customize** for Launch and Activation Permissions.

Step 7 Click the <EDIT...> button associated with this security option. The Launch Permission dialog will appear.

ministrators)	
ministrators)	
ministrators)	
<u>d</u> d	<u>R</u> emove
Allow	Deny
v	
ок	Cancel
	dd

- **Step 8** Verify that **Anonymous Logon, Everyone** and **System** are selected. They will be displayed in the Group or user names box. These users/groups must be set up with all "Allow " security.
 - (Use the <ADD...> button if these users/groups need to be added.) **NOTE**: Any other users/groups that are already selected may remain. You may, however, delete "Interactive" if it is selected.
- Step 9 Click OK and then Apply.

Step 10 Select Customize for Access Permissions.

DHI.QuerySvr Properties	? 🔀
General Location Security Endpoints Identity	
Launch and Activation Permissions	
Customize	
Access Permissions	
Customize	
Configuration Permissions	
C Use Defa <u>u</u> lt	4
(• CustomizeEdit	
OK Cancel Ar	oply

Step 11 Click the <EDIT...> button associated with this security option. The Registry Value Permissions dialog will appear.

Access Permission		? 🔀
Security		1
Group or user names:		
🕵 Everyone		
SELF		
MA SISIEM		
1	Add 1	Bemove
		TICHIOYC I I
Permissions for Everyone	Allow	Deny
Permissions for Everyone	Allow	Deny
Permissions for Everyone Local Access Remote Access	Allow	Deny
Permissions for Everyone Local Access Remote Access	Allow	Deny
Permissions for Everyone Local Access Remote Access	Allow	Deny
Permissions for Everyone Local Access Remote Access	Allow	Deny
Permissions for Everyone Local Access Remote Access	Allow	Deny
Permissions for Everyone Local Access Remote Access	Allow	

- **Step 12** Verify that **Everyone** and **System** are selected. It will be displayed in the Group or user names box. This user/group must be set up with all "Allow " security.
 - (Use the <ADD...> button if this user/group needs to be added.) **NOTE**: Any other users/groups that are already selected may remain. You may, however, delete "Interactive" if it is selected.
- Step 13 Click OK and then Apply.



- **Step 15** Select "This user" to answer the question, "Which user account do you want to use to run this application?"
- Step 16 Click <BROWSE...>. The Browse for Users dialog will appear.
- **Step 17** Select the DB4User.
- Step 18 Type the password associated with the DB4 user in the PASSWORD field.
- Step 19 Type the password again in the CONFIRM PASSWORD field.
- Step 20 Click Apply and then OK.
- **NOTE**: Sometimes the DCOM Configuration dialog will appear stating that "The operation completed successfully." Click <OK> to return to the desktop. The configuration will be complete.

Generally, a restart of the machine is necessary before the settings will take effect. Do not restart the machine until all steps have been completed.

DB4Server Registry changes for GOLDTrakPC



On the DB4 server paths for GOLDTrakPC must be set in the registry as shown above. For SERVERWMFS use your DB4 server name in place of SBP-VM-XPPRO.

If you have any problems or questions, contact your FPS GOLD customer service representative.

Firewall Exceptions – Windows XP only

Step 1 Right click on My Network Places and select Properties.







The firewall should be defaulted on. Leave it turned on. Click on the Exceptions tab.

🗑 Windows Firewall 🛛 🔀
General Exceptions Advanced
Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.
Name
DHI. Trace. Viewer
🗹 dlihost
File and Printer Sharing
Microsoft Management Console
Remote Assistance
Remote Desktop
UPnP Framework
Add Program Add Port Edit Delete Display a notification when Windows Firewall blocks a program What are the risks of allowing exceptions?
OK Cancel

Step 3 You need to add in a Port Exception and a Program Exception.

Click on the **Add Port** button and fill out the box for the name DCOM RPC and port 135 as shown below. Click **OK** to add to exceptions.

Edit a Port	X			
Use these settings number and protoc want to use.	to open a port through Windows Firewall. To find the port ol, consult the documentation for the program or service you			
<u>N</u> ame:	DCOM RPC			
<u>P</u> ort number:	135			
What are the risks of opening a port?				
Change scope	OK Cancel			

Step 4 Click on the Add Program to add dllhost.exe to the exception list. This program is in the C:\Windows\System32 or C:\WINNT\System32 folder. You will need to Browse to get to the file.

Add a	Program					
To allo select i	w communication the program, or cl	is with a program by a ick Browse to search	adding it to the Excep for one that is not lis	otions list, ted.		
<u>Program</u>	Programs:					
	heckWriter					
© Chang	DRe IP Configura ustomer Informati B4 Server Monito HI Trace Viewer eeCell OLDTeller® Platf OLDTrak® PC OLDTrak® PC Se earts ternet Backgamm ath: C:\Program	itor on Management r orm etup non n Files\FPSGOLD\GC	DLDTrakPC\ch	₹rowse Cancel		
rowse				? 🛛		
Look jn:	C system32		O Ø Ø	•		
My Recent Documents Desktop My Documents	arp.exe asr_fmt.exe asr_dm.exe asr_dm.exe at.exe attrib.exe auditusr.exe auditusr.exe autochk.exe autochv.exe autofmt.exe bastch.exe bootcfg.exe	bootvrfy.exe cacls.exe calc.exe calc.exe calc.exe charmap.exe chcp.com chchdsk.exe chchdsk.exe chchdsk.exe cidaemon.exe cidaemon.exe cipher.exe cisvc.exe ckcnv.exe cleanmgr.exe cliconfg.exe clipbrd.exe	Control.exe control.exe command.com comp.exe compact.exe consdupd.exe consdupd.exe consdupd.exe control.exe control.exe convert.exe cortrol.exe cortrol.exe cortrol.exe cortrol.exe cortrol.exe cortrol.exe cortrol.exe cortrol.exe cortrol.exe cortrol.exe cortrol.exe cortrol.exe cortrol.exe cortrol.exe cortrol.exe cortrol.exe cortrol.exe cortrol.exe cortrol.exe cortrol.exe cortrol.exe cortrol.exe cortrol.exe cortrol.exe cortrol.exe cortrol.exe cortrol.exe cortrol.exe cortrol.exe cortrol.exe	Image: Second		
My Computer	bootok.exe	, dipsrv.exe	dcomcnfg.exe			
My Network	Files of <u>type</u> :	Applications (*.exe;*.com	r,*.icd)	Cancel		

Click on the dllhost.exe file and then click **Open** to select the file.

Add a Program	×
To allow communications with a program by adding it to the Exceptions list, select the program, or click Browse to search for one that is not listed.	
<u>Programs:</u>	_
<u>z</u> CheckWriter	^
🙍 CORe IP Configurator	
Customer Information Management	=
🖾 DB4 Server Monitor	1
DHI Trace Viewer	
📶 dilhost.exe	
4 FreeCell	2
GOLDTeller® Platform	
GOLDTrak® PC	
GOLDTrak® PC Setup	
W Hearts	
Path: C:\WINDOWS\system32\dllhost.exe Browse	
	_
Change scope OK Cancel	

Once dllhost.exe is in your list of programs, select it and click **OK**.

 $Repeat \ Step \ 4 \ for \ DHI \ Locate.exe \ found \ in \ C:\ Program \ Files\ DHI \ Shared\ Sha$

Your list of exceptions should now include dllhost.exe, DHILocate.exe and a DCOM RPC (port 135) exceptions

Step 5 Click OK on your firewall settings to save all firewall settings.

vinitae	wys r newon s	Jettings		-
General	Exceptions	Advanced		
Window from ou Genera Window <u>What a</u>	vs Firewall is t utside sources I tab and sele vs Firewall is c <u>re the risks of</u>	urned off. Your co such as the Inter ct On. urrently using set <u>funblocking a pro</u>	omputer is at risk of a rnet. We recommend tings for the domain gram? d. baux	attacks and intrusions that you dick the network location.
Progr	am or port	on, select its crief	K DOX:	
	TS Peercachin onnect to a Ne ore Networkin COM RPC	ng etwork Projector		H
	HILocate.exe stributed Tran host.exe e and Printer	saction Coordinat	tor	
	CSI Service y Managemer togon Servic	nt Service e		
	rformance Lo	ery		•
Add p	orogram fy me when V	Add p <u>o</u> rt Vindows Firewall <u>b</u>	Properties	Delete
		-		

Firewall Exceptions – Windows 2008 Server

Step 1 Under Administrative Tools (usually found by clicking on Start or by going to Control Panel) click on Windows Firewall with Advanced Security

		🔄 Data Sources (ODBC)
	122	Event Viewer
Server Manager		😂 iSCSI Initiator
Command Prompt		🛓 Local Security Policy
		Memory Diagnostics Tool
	Steven Packer	🎯 Reliability and Performance Monitor
	Deministr	🛓 Security Configuration Wizard
		🚠 Server Manager
	Computer	🔍 Services
Notenad	Compacer	📆 Share and Storage Management
	Network	🔄 Storage Explorer
DB4 Server Monitor	~	System Configuration
	Control Panel	🕑 Task Scheduler
Ease of Access Center		I Windows Firewall with Advanced Security
	Administrative Loois	🐌 Windows Saver Backup
	Help and Support	
	Run	
	Windows Security	
All Programs		
Start Search	0 🔒 🔸	
🎝 Start 🛛 🚠 💻 🏉		

You may get the following Window. Click on Continue to bring up the Firewall Settings.





Step 2 Click on Inbound Rules

Step 3 Scroll down to find Performance Logs and Alerts (DCOM-In) Under the Domain Profile

And the second se				
hbound Rules				Actions
ame	Group 🔺	Profile	En 🔺	Inbound Rules
Network Discovery (NB-Datagram-In) Network Discovery (NB-Name-In) Network Discovery (Pub-WSD-In) Network Discovery (SSDP-In)	Network Discovery Network Discovery Network Discovery Network Discovery	Any Any Any Any	Nc Nc Nc Nc	New Rule Filter by Profile
Network Discovery (UPnP-In) Network Discovery (WSD Events-In) Network Discovery (WSD EventsSecure-In)	Network Discovery Network Discovery Network Discovery	Any Any Any	Nc Nc Nc	Image: State
Network Discovery (WSD-In) Performance Logs and Alerts (DCOM-In) Performance Logs and Alerts (TCP-In) Performance Logs and Alerts (TCP-In)	Network Discovery Performance Logs and Alerts Performance Logs and Alerts Performance Logs and Alerts	Any Domain Domain	Nc Nc Nc	Refresh
Performance Logs and Alerts (TCP-In) Remote Administration (NP-In) Remote Administration (RPC) Remote Administration (RPC) Permote Deckton (TCP-In)	Performance Logs and Alerts Remote Administration Remote Administration Remote Administration Remote Administration	Privat Any Any Any Any		Help Performance Logs and Alerts O Enable Rule Dete
	bound Rules ame Network Discovery (NB-Datagram-In) Network Discovery (NB-Name-In) Network Discovery (Pub-WSD-In) Network Discovery (WSD Events-In) Network Discovery (WSD Events-In) Network Discovery (WSD EventsSecure-In) Network Discovery (WSD EventsSecure-In) Network Discovery (WSD-In) Performance Logs and Alerts (DCOM-In) Performance Logs and Alerts (TCP-In) Performance Logs and Alerts (TCP-In) Remote Administration (RPC) Remote Administration (RPC) Perfort (TCP-In)	bound Rules ame Group Network Discovery (NB-Datagram-In) Network Discovery Network Discovery (NB-Name-In) Network Discovery Network Discovery (Pub-WSD-In) Network Discovery Network Discovery (SSDP-In) Network Discovery Network Discovery (UPNP-In) Network Discovery Network Discovery (WSD Events-In) Network Discovery Network Discovery (WSD Events-In) Network Discovery Network Discovery (WSD Events-Secure-In) Network Discovery Network Discovery (WSD Events (DCOM-In) Performance Logs and Alerts (DCOM-In) Performance Logs and Alerts (DCOM-In) Performance Logs and Alerts Performance Logs and Alerts (TCP-In) Performance Logs and Alerts Performance Logs and Alerts (TCP-In) Remote Administration (RPC) Remote Administration (RPC-EPMAP) Remote Administration Remote Administration (RPC-EPMAP) Remote Administration	bound Rules ame Group Profile Network Discovery (NB-Datagram-In) Network Discovery Any Network Discovery (NB-Name-In) Network Discovery Any Network Discovery (Pub-WSD-In) Network Discovery Any Network Discovery (SSDP-In) Network Discovery Any Network Discovery (UPnP-In) Network Discovery Any Network Discovery (WSD Events-In) Network Discovery Any Network Discovery (WSD Events-In) Network Discovery Any Network Discovery (WSD EventsSecure-In) Network Discovery Any Network Discovery (WSD-In) Performance Logs and Alerts Domain Performance Logs and Alerts (DCOM-In) Performance Logs and Alerts Domain Performance Logs and Alerts (TCP-In) Performance Logs and Alerts Domain Performance Logs and Alerts (TCP-In) Performance Logs and Alerts Privat Remote Administration (RPC) Remote Administration Any Remote Administration (RPC-EPMAP) Remote Administration Any	bound Rules ame Group Profile En Network Discovery (NB-Datagram-In) Network Discovery Any Nc Network Discovery (NB-Name-In) Network Discovery Any Nc Network Discovery (Pub-WSD-In) Network Discovery Any Nc Network Discovery (GSDP-In) Network Discovery Any Nc Network Discovery (UPnP-In) Network Discovery Any Nc Network Discovery (WSD Events-In) Network Discovery Any Nc Network Discovery (WSD Events-In) Network Discovery Any Nc Network Discovery (WSD Events-In) Network Discovery Any Nc Network Discovery (WSD-In) Network Discovery Any Nc Performance Logs and Alerts (DCOM-In) Performance Logs and Alerts Domain Nc Performance Logs and Alerts (TCP-In) Performance Logs and Alerts Domain Nc Performance Logs and Alerts (TCP-In) Remote Administration Any Nc Remote Administration (RPC) Remote Administration Any

Step 4 Click on the Performance Logs and Alerts (DCOM-In) and then click on Enable Rule.

Step 5 Click on New Rule.

🎡 Windows Firewall with Advar	nced Security			
File Action View Help				
🗢 🔿 🔰 💼 🗟 🗖				
I Windows Firewall with Advance	Inbound Rules			Actions
Inbound Rules	Name	Group 🔺	Profile En	🖌 Inbound Rules 🔺 📥
Connection Security Rules Monitoring	BITS Peercaching (Content-In) BITS Peercaching (RPC) BITS Peercaching (RPC) BITS Peercaching (RPC-EPMAP) BITS Peercaching (WSD-In) Core Networking - Destination Unreachable (ICMPv6-In) Core Networking - Destination Unreachable Fragmentati Core Networking - Destination Unreachable Fragmentati Core Networking - Internet Group Management Protocol Core Networking - Internet Group Management Protocol Core Networking - Multicast Listener Done (ICMPv6-In) Core Networking - Multicast Listener Report v2 (ICMPv6-In) Core Networking - Multicast Listener Report v2 (ICMPv6-In) Core Networking - Nulticast Listener Report v2 (ICMPv6-In) Core Networking - Nulticast Listener Report v2 (ICMPv6-In) Core Networking - Nulticast Listener Report v2 (ICMPv6-In) Core Networking - Neighbor Discovery Advertisement (I Core Networking - Neighbor Discovery Splicitation (ICMP	BITS Peercaching BITS Peercaching BITS Peercaching COM+ Network Access Core Networking Core Networking	Any Nc Any Ye Any Ye	 New Rule Filter by Prof Filter by State Filter by Group View Refresh Export List Help Performance Logs and Alerts Enable Rule X Delete

Step 6 Choose Program Rule type and Click Next.

Step 7 Choose This Program Path: and Browse to

64 Bit Operating system C:\Program Files (x86)\Common Files\DHI Shared\DHILocate.exe 32 Bit Operating system C:\Program Files\Common Files\DHI Shared\DHILocate.exe Click Next

艨 New Inbound Rule Wizard		×					
Program							
Specify the full program path and	executable name of the program that this rule matches.						
Steps:							
Rule Type	Does this rule apply to all programs or a specific program?						
Program							
 Action 	O All programs						
Profile	Pruie applies to all connections on the computer that match other fule properties.						
Name	• This program path:						
	ramFiles% (x86)\Common Files\DHI Shared\DHILocate.exe Browse						
	Example: c:\path\program.exe %ProgramFiles%\Internet Explorer\iexplore.exe						
	%Frugrammies% (miernet Explorer flexplore vexplore exe						
	Learn more about specifying programs						
	Careed Nuclear Concert						
	< Back Next> Lancel						

Step 8 Choose Allow the connection and Click Next

艨 New Inbound Rule Wizard	X					
Action						
Specify the action that is taken w	hen a connection matches the conditions specified in the rule.					
Steps:						
Bule Type	What action should be taken when a connection matches the specified conditions?					
Program						
 Action 	• Allow the connection					
Profile	Allow connections that have been protected with IPsec as well as those that have not.					
Name	xerr xerr what action should be taken when a connection matches the specified conditions? C Allow the connection					
	Allow only connections that have been authenticated and integrity-protected through the use of IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.					
	<u>Hequire the connections to be encypted</u> Bequire privacy in addition to integrity and authentication					
	Override block rules					
	Userul for tools that must always be available, such as remote administration tools. If you specify this option, you must also specify an authorized computer or computer group.					
	O Block the connection					
	Learn more about actions					
	< Back Next > Cancel					
<u>II</u>						

Step 9 Choose Domain, Private and Public (all checked is the default) for When does this rule apply? Click Next

💣 New Inbound Rule Wizard	×
Profile	
Specify the profiles for which this r	rule applies.
Steps:	
 Rule Type Program Action Profile Name 	 When does this rule apply? Domain Applies when a computer is connected to its corporate domain. Private Applies when a computer is connected to a private network location.
	Public Applies when a computer is connected to a public network location.
	< <u>B</u> ack Cancel

Step 10 Give the rule a name, usually the name of the program you are adding as an exception. Click Finish

💣 New Inbound Rule Wizar	d	>
Name		
Specify the name and descriptio	n of this rule.	
Steps:		
Rule Type		
Program		
Action		
Profile	Name:	
Name		
	Description (optional):	
	<u> < B</u> ack <u>Finish</u> Cancel	
tep 11 Repeat Steps 5 For Step 7 you 64 Bit 6	5 – 10 for the program dllhost.exe. will find the program in Operating system	
32 Bit (Operating system	

C:\Windows\System32\dllhost.exe

You should see something like the following when you have finished adding the Program Exceptions

Ele Action Yiew Help Image: Second Rules Actions Windows Firewall with Advanced S Inbound Rules Imbound Rules Anny Yes Allow Outbound Rules Anny Yes Allow Name Anny Yes Allow Monitoring Off Decisioning (contents on the content on the conten	👹 Windows Firewall with Advance	d Security							_ 🗆 ×
Image: Second	File Action View Help								
Windows Firewall with Advanced 5 Inbound Rules Actions Inbound Rules Name Group ^ Profile Enabled Action Inbound Rules Connection Security Rules OthElocate Any Yes Allow Inbound Rules Inbound Rules <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>									
Inbound Rules Name Group A Profile Enabled Action Inbound Rules Outbound Rules Other the state Any Yes Allow New Rule On outbound Rules On outbound Rules Any Yes Allow Vestate Vestate Monitoring Outbound Rules Any Yes Allow Vestate Vestate Vestate BITS Peercaching Any No Allow Vestate Vesta	Windows Firewall with Advanced S	Inbound Rules						Actions	
Connection Security Rules Monitoring Contention Security Rules Conten	Inbound Rules	Name	Group 🔺	Profile	Enabled	Action		Inbound Rules	• -
Monitoring Control reacting (contention) Differenced mig Any Yes Allow V Control reacting (RPC) Bits Peercaching Any No Allow V Filter by Profile Control reacting (RPC) Bits Peercaching Any No Allow V Filter by State Control reacting (RPC-EPMAP) Bits Peercaching Any No Allow V Filter by State	Connection Security Rules	1 DHILocate		Any	Yes	Allow		🐹 New Rule	
Constructioning (contentionin) Constructioning Any No Allow There is provide Image: state Constructioning (RPC) BITS Peercaching Any No Allow There is provide Image: state Constructioning (RPC-EPMAP) BITS Peercaching Any No Allow There is provide Image: state Construction Construction BITS Peercaching Any No Allow Image: state Construction Construction BITS Peercaching Any No Allow Image: state Construction Construction BITS Peercaching Any No Allow Image: state	🗉 🔜 Monitoring	🔮 dllhost		Any	Yes	Allow		Tihar bu Duafila	
✓ BITS Peercaching (RPC) BITS Peercaching Any No Allow ✓ BITS Peercaching (RPC-EPMAP) BITS Peercaching Any No Allow ✓ Filter by State ✓		or or or reencaching (concentern)	bit 5 Feercaching	MUY	140	MILOW		The ricer by Profile	· _
✓ BITS Peercaching (RPC-EPMAP) BITS Peercaching Any No Allow ▼ ▼ ▼ Filter by Group ▼		BITS Peercaching (RPC)	BITS Peercaching	Any	No	Allow		🕎 Filter by State	•
Y Filter by Group		BITS Peercaching (RPC-EPMAP)	BITS Peercaching	Any	No	Allow	-		
	I I	4						Y Filter by Group	· · · ·
		loste							

This step is not usually necessary

For Windows Server 2003 SP1 Only

Go to Administrative Tools. Click on Local Security Policy, Local Policies, Security Options. Find "Network access: Let Everyone permissions apply to anonymous users" Double click and click on **Enable** then click **Apply** and then click **OK**.

Local Security Settings		<u>.</u>	- 0
<u>-jie Action View H</u> elp			
- → 🗈 📧 🗙 😭 🗟 😫			
Security Settings	Policy A	Security Setting	
Account Policies	B Domain member: Maximum machine account password age	30 days	
Local Policies	BDomain member: Require strong (Windows 2000 or later) session key	Disabled	
Audit Policy	📖 Interactive logon: Do not display last user name	Disabled	
H User Rights Assignment	Interactive logon: Do not require CTRL+ALT+DEL	Disabled	
Dublic Key Policies	📆 Interactive logon: Message text for users attempting to log on		
Public Key Policies Software Destriction Policies	📖 Interactive logon: Message title for users attempting to log on	Not Defined	
3 Jortware Restriction Policies 7 ID Security Policies on Local Computer	Binteractive logon: Number of previous logons to cache (in case domain controller is not available)	10 logons	
The Sociality Policies on Eocal Compater	B Interactive logon: Prompt user to change password before expiration	14 days	
Jortware Restriction Policies	📴 Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled	
	🛍 Interactive logon: Require smart card	Disabled	
	📖 Interactive logon: Smart card removal behavior	No Action	
	BigMicrosoft network client: Digitally sign communications (always)	Disabled	
	BigMicrosoft network client: Digitally sign communications (if server agrees)	Enabled	
	Big Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled	
	Big Microsoft network server: Amount of idle time required before suspending session	15 minutes	
	Big Microsoft network server: Digitally sign communications (always)	Disabled	
	BigMicrosoft network server: Digitally sign communications (if client agrees)	Disabled	
	B Microsoft network server: Disconnect clients when logon hours expire	Enabled	
	BNetwork access: Allow anonymous SID/Name translation	Disabled	
	BNetwork access: Do not allow anonymous enumeration of SAM accounts	Enabled	
	BNetwork access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled	
	Betwork access: Do not allow storage of credentials or .NET Passports for network authentication	Disabled	
	Network access: Let Everyone permissions apply to anonymous users	Disabled	F
	BNetwork access: Named Pipes that can be accessed anonymously	COMNAP,COMNOD	
	BNetwork access: Remotely accessible registry paths	System\CurrentCon	
	Network access: Remotely accessible registry paths and sub-paths	System\CurrentCon	
	Network access: Restrict anonymous access to Named Pipes and Shares	Enabled	
	Network access: Shares that can be accessed anonymously	COMCFG,DFS\$	
	Network access: Sharing and security model for local accounts	Classic - local users	
	Network security: Do not store LAN Manager hash value on next password change	Disabled	
	Network security: Force logoff when logon hours expire	Disabled	
	Network security: LAN Manager authentication level	Send NTLM respons	
	Network security: LDAP client signing requirements	Negotiate signing	
	Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	No minimum	
	Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	No minimum	
	Recovery console: Allow automatic administrative logon	Disabled	
	μ	NILLIJ	

For Windows 7

If you have setup a Windows 7 machine as a DB4 Server and as a Client Machine the following will need to be added to the Registry.

HKEY_LOCAL_MACHINE\SOFTWARE\DHI Computing Service\DB4

Key: LocalOutProc

Value: The Name of the DB4 Server Machine

<u>Edit View Favorites H</u> elp				
	*	Name	Type	Data
SOFTWARE ATL Technologies		(Default) BORNABLESECUREFILES	REG_SZ REG_DWORD	0x00000000 (0)
D Classes		Clenor Log	REG_SZ	-
D - D Clients		LocalOutProc	REG_SZ	D4615VM3
D- CORe		100 NO TIFY PERIOD SECONDS	REG_DWORD	0x00000014 (20)
DHI Computing Service DB4 GOLDTeller GOLDTeller GOLDVision GOLDVision InstallShield	(III)	SIMULTANEOUSOPEN	REG_DWORD	0x000001f4 (500)
 Mektra ODBC Policies 				
▷ - 🌉 Sonic ▷ - 📕 Sunbelt Software				
ThinPrint	-			
· · · · · · · · · · · · · · · · · · ·	and and			