

## User Manual for Aarhus Batch Inversion Distributed

## Introduction

The Aarhus Batch Inversion Distributed (ABI) is designed to replace the older EMBI and SCEMBI systems for performing inversions within the Workbench environment. To do this there are two applications, a client application in the front named Aarhus Batch Inversion, and a service application working behind the scenes named AarhusRunner. Users will not be directly involved with AarhusRunner, which is why this document will focus on ABI. All a user needs to know about AarhusRunner is that it is operating on a number of servers in the network, waiting to perform performance-demanding computation tasks ordered by Aarhus Batch Inversion's throughout the system.

ABI is started from Workbench just like Embi and Scembi when running an inversion and is designed to resemble the user interfaces of the old systems.



Figure 1: Workbench and Importer interacts with a network of AarhusRunner services



## Workbench setup for running ABI

# Note: Aarhus GeoSoftware doesn't take any responsibility for the setup and changes in Windows to make ABI work.

Workbench and Windows need to be set up to start ABI when an inversion is launched. To do so, follow these steps:

1. go to File  $\rightarrow$  Preferences under the Misc tab and check "Run Aarhus Batch Inversion Distributed".

Preferences						Х					
Workspace	Borehole	Misc	GIS	Res2DInv							
Misc											
☑ Check for new version at start up											
Enable multi threaded database queries											
✓ Do not back import SkyTEM data before inversion											
Enabled SCI of ERT data											
Scaling factor to manipulation of data in colorscale wizard 1											
Use Sparse Formats											
Max memo	ory allowed	2500	[MB]								
Run Aarhus Batch Inversion distributed											
					OK	Cancel					

2. Open the ABI.ini in the workbench installation directory and set SharedDir to point to the shared directory.

You will need to save the ini file in another folder and copy/replace the existing ini file in the Workbench installation folder, due to Windows admin rights.





#### Windows 10 only:

Windows 10 have as default restricted the access to network drives for the user. To remove this restriction, open the "Edit Group Policy" in Control panel and go to:

- Computer Configuration →Administrative Templates → Network → Lanman Workstation
- Double click on Enable insecure guest logon
- Click Enable and OK

Local Group Policy Editor						- 🗆 ×		
File Action View Help								
← ⇒   2 📷   🗟 🖬 🛛 🐨   🦷								
Local Computer Policy	Canman Workstation							
V 👰 Computer Configuration	Enable insecure quest logons	Setting		State	Comment			
> Contrare Settings	chable insecure guest logons	E Cipher suite order		Not configured	No			
> iii Windows Settings	Edit policy setting	Copper suite order	ity Charac	Not configured	No			
Administrative lemplates		Enable incerure quert logons	ity snares	Enabled	No			
> Control Panel	At least Windows Server Windows 10	El Offline liler Availability on Continuour Av	vailability Sharer	Not configured	No			
Rackground Intelligent Transfer Service (RITS)	At least windows server, windows to	E online hies Availability on continuous A	valiability shares	Not configured	NO			
BranchCache	Description:							
DirectAccess Client Experience Settings	This policy setting determines if the							
DNS Client	logons to an SMB server.							
Fonts								
Hotspot Authentication	If you enable this policy setting or if							
Lanman Server	setting, the SMB client will allow	Enable insecure quest logons			_			
🛄 Lanman Workstation	insecure guest logons.	~ · · · · · · · · · · · · · · · · · · ·						
Link-Layer Topology Discovery	Marine disable this setime station also	Enable insecure guest logons		Provious Setting	Next Setting			
Microsoft Peer-to-Peer Networking Services	SMB client will reject insecure quest			Previous Setting	IVEXT Setting			
Network Connectivity Status Indicator	logons.	O Not Configured Comment:	-			<u> </u>		
Network Isolation	Income and Income and Income	Ondecomigated						
Network Provider	servers to allow unauthenticated	Enabled						
Offline Files	access to shared folders. While	O Disabled				✓		
> 🚆 QoS Packet Scheduler	uncommon in an enterprise	Supported on:	At least Windows Ser	rver. Windows 10				
SNMP	are frequently used by consumer							
SSL Configuration Settings	Network Attached Storage (NAS)					¥		
> TCPIP Settings	appliances acting as file servers.	Options:	Help	p:				
Windows Connect Now	authentication and do not use							
Windows connection wanager	insecure guest logons by default.		Thi	s policy setting determine	s if the SMB client will allow	N ^		
> WLAN Service	Since insecure guest logons are		inse	ecure guest logons to an S	MB server.			
> 📫 WWAN Service	features such as SMB Signing and	Strant security			If you enable this policy setting or if you do not configure this			
Printers	SMB Encryption are disabled. As a	ncryption are disabled. As a			policy setting, the SMB client will allow insecure guest logons.			
Server	result, clients that allow insecure		14		- ALL CARD ALL ALL IN ALL -			
> 🧮 Start Menu and Taskbar	variety of man-in-the-middle attacks			insecure quest logons.				
> System	that can result in data loss, data							
> Windows Components	corruption, and exposure to malware.			Insecure guest logons are used by file servers to allow				
	server using an insecure quest logon	any data written to a me unauthenticated an insecure guest logon an enterprise en			secure quest logons are fre	equently		
Software Settings	is potentially accessible to anyone on		use	d by consumer Network A	ttached Storage (NAS) app	liances		
> 🦉 Windows Settings	the network. Microsoft recommends		acti	ing as file servers. Window	s file servers require auther	ntication		
> 🧾 Administrative Templates	configuring file servers to require		and	est logons are unauthentic	ated important security fea	atures		
	authenticated access."		suc	h as SMB Signing and SM:	B Encryption are disabled. A	As a		
			resu	ult, clients that allow insec	ure guest logons are vulner	rable to a		
			dat	a corruption and exposur	e to malware. Additionally	any data		
			writ	tten to a file server using a	n insecure guest logon is	~		
		-						
					OK Cancel	Apply		
		L						

Now Workbench is ready to use ABI for inversions.



## Running an inversion

When the user starts an inversion from Workbench, ABI is launched. The program will prompt the user for a list of hosts to perform the inversion job.

The user can select all or some of the hosts for the inversion job in the server list to the left. On the right there is an overview of active inversion jobs in the network.

After the hosts have been selected, ABI will wait for one of the selected hosts to pick up and perform the inversion job. While the job is running, ABI keeps the user updated via the GUI.

The user **cannot** close the ABI window as long as the inversion job is active. However, the user may choose to cancel the inversion job via the Stop button. This will terminate the inversion process and enable ABI for closing.

The Show Jobs button opens an overview of the active inversion jobs, similar to the overview shown when selecting hosts in the start.

Once the inversion job is done, ABI will import the inversion result to your workspace.



Figure 2: Hosts selection in Aarhus Batch Inversion Distributed