

JDisc Discovery 5.0

Security Add-On

Legal Notice

JDisc GmbH shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material. The information herein is subject to change without notice and is provided "as is" without warranty of any kind. The entire risk arising from the use of this information remains with the user. In no event shall JDisc GmbH be liable for any direct, consequential, incidental, special, punitive, or other damages whatsoever (including - without limitation - damages for loss of business profits, business interruption or loss of business information), even if JDisc GmbH has been advised of the possibility of such damages. The foregoing shall apply regardless of negligence or any other fault on behalf of either party and regardless of whether such liability sounds in contract, negligence, tort, or any other theory of legal liability, and notwithstanding any failure of essential purpose of any limited remedy. The limited warranties for JDisc GmbH products are exclusively set forth in the documentation accompanying such products. Nothing herein should be construed as constituting a further or additional warranty.

Copyright

JDisc GmbH may hold patents or pending patent applications covering the subject matter of this document. The furnishing of this document does not imply any license for these patents. You can send license inquiries, in writing, to:

JDisc GmbH Kuppinger Weg 25 D-71116 Gärtringen Germany

This document is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced, or translated to another language without prior written consent of JDisc GmbH.

All other registered trademarks are the property of their respective owners.

© Copyright JDisc GmbH, 2023.

Contents

1 Introduction	4
2 Share Permissions	5
2.1 Configuration	5
2.2 Shares Per Computer	
2.3 Displaying All Shares	
2.4 Shared Resources Per User	
3 Open Source	

1 Introduction

JDisc Discovery's Security Add-On extends JDisc Discovery's discovery with network share discovery and access permission related features:

- 1. Discovery of Network Shares
 - Windows computers the discovery queries all share permissions and maps them to local / global user and user groups.
 - Unix/Linux computers running SAMBA
- Displaying Effective Access Permissions Specialized reports display all users that can access a network share either through direct access permissions on the share or indirectly by user group membership.

The JDisc Discovery Security Add-On discovers all network shares of Windows and Unix/Linux computers. For Windows computers the discovery queries all access permissions and maps them to local/global users and user groups.

2.1 Configuration

To discover network shares and share permissions on Windows computers, JDisc Discovery requires administrative WMI or SMB protocol access.

Enable or disable the "Discover share" option in the *Data Collection* | *Standard* tab of the discovery configuration dialog.

al Scope Directory Data Collection	Discovery Jobs Protocols Topology Jobs Filter	rs SSH Keys	
dard Custom File Collection			
lser / User Groups			
Discover user groups			
Discover users			
Ignore	ser history when not logged on for 30 🚔 da	-(-)	
 Delete users from logged on us Find terminal services clients 	ser history when not logged on for30 🚔 da	y(s)	
Discover terminal services			
Discover terminal services	clients		
oftware / Hardware / Networking			
Discover applications	Discover executable files 🛛 😣	Discover disks	Discover attached devices
Discover licenses	Discover processor	Discover virtual instances	Discover monitors
Discover patches	Discover memory	Discover blade enclosure compon	Discover local printers/
Discover services	Discover video controllers	Discover managed devices	Discover local scanner
Discover drivers	V Discover cluster	Discover VMware annotations	Discover card reader
Discover processes	🔽 Discover wlans 🛛 🔞	✓ Discover shares	
🔽 Use pargs on Sol 🔞	Identify VLANs by VLAN id only 👻	13	
ependency Mapping			
Find dependencies between compu	iters		
Discover connected devices			
Delete inactive dependencies b	etween computers when older than 7 🔿 c	lay(s)	

Figure: Enable/Disable Share Discovery

2.2 Shares Per Computer

The Device Details dialog displays network shares in the *Networking* |*Shares* tab. The Shares tab displays all network shares including the share permissions.

evice Details for 'tom-lap ← → 🤣 🔐 📭		# @					
Seneral Networking Haro				Custom Attributes	Roles Groups Analyze		
Filter:	ve filter						
Share Name	Description	Туре	Max Connections	Path	Trustee	Access	Effective Permissions
ADMINS	Remote Admin	Disk Drive Admin		C:\Windows			4
C\$	Default share	Disk Drive Admin		C:\			
D\$	Default share	Disk Drive Admin		D:\			
diddeldaddel		Disk Drive		C:\temp	TOM-LAPTOP3\LAYER2GROUP	 Full control Read 	
E\$	Default share	Disk Drive Admin		E:\			
IPC\$	Remote IPC	IPC Admin					
temp		Disk Drive		C:\temp	TOM-LAPTOP3\ADMINISTRATORS TOM-LAPTOP3\LAYER2GROUP TOM-LAPTOP3\EVERYONE TOM-LAPTOP3\EVERYONE	✓ Full control ✓ Full control ✓ Full control	
tmp		Disk Drive		C:\tmp	TOM-LAPTOP3/4DMINISTRATORS TOM-LAPTOP3/EVERYONE	 ✓ Full control ✓ Full control 	
Total 8 shared resource	es 1 shared resource :	selected]
					Close		

Figure: Network Shares per Computer

The *Effective Permissions* button displays all users that can access the selected share.

Access permissions can be granted either directly on the share or indirectly by user group membership.

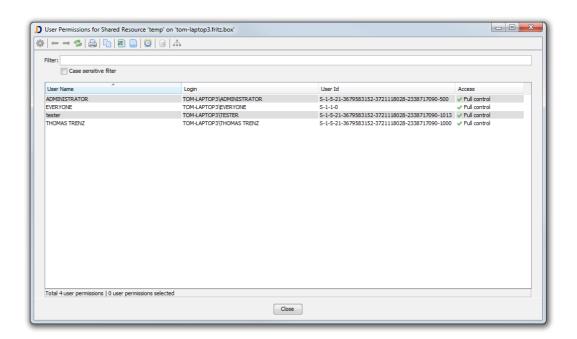


Figure: User Permissions per Shared Resource

2.3 Displaying All Shares

Open the *Shares* report from the *Networking* menu to display all devices and networks shares including their access permissions.

JDisc Discovery [Enterprise Edit	on] - T	HOMAS TREN	Z connecte	d to loc	alhost	
File Discovery Devices Software	Netwo	orking Users	Maps Doc	uments	Troub	leshootir
🕑 🖲 🕕 🥜	🧭 I	Pv4 Networks				
Discovery Status	V6 I	Pv6 Networks				
	⇔∣	Pv4 Ranges				
Status Discovery		Network Neigh	borhood			
(Part)	<i>»</i> (Connections		•		
	a 1	Fopology		•		
	📄 V	/LANs				
Devices Ping Network Neighbo	🙊 v	WLAN		• evice H	listory	Discover
Concurrent device discoveries		Shares .				
Average duration		e aiscover Jame	: 00:01:06 (545 devi	ces per	hour)
Discovery jobs	0 of 0 pe	-				
Manually triggered Devices in database	0 pendir 26	ng				
Devices in udtabase	20					

Figure: Global Shares Report

To display also administrative shares, check the "Include administrative shares" in the report's filter panel.

iter:										
Case sensitive f	fiter									
Include administrati	ive shares									
										Effective Permissions
Name	IP Address	Туре	Share Name	Share Type	Path	Description	Trustee	Access V Read	Manufacturer	Cilective Permosuro
DISCSERVER	192, 168, 178, 74	Whikare Instance	temp	Disk Drive	C1/temp		JDISC (Domain Users JDISCSERVER VADMINISTRATORS	Read Full control		
DISCREVER	192, 168, 178, 74	Where Instance	Users	Disk Drive	D:\Server#olders\Users	Users	A EVERYONE	Full control		
DISCSERVER	192, 168, 178, 74	Where Instance	SYSVOL	Disk Drive	C:\Windows\ayavol\ayavol	Logon server share	JDISCSERVER JADMINISTRATORS	 Full control 		
							AUTHENTICATED USERS	✓ Pul control ✓ Read		
IDISCSERVER	192, 168, 178, 74	Whikare Instance	Business	Disk Drive	D:\Share\Business		DUSC (Development DUSC SERVER WOMENISTRATORS EVERYONE Thomas Tranz	✓ Read ✓ Full control ✓ Full control ✓ Read		
ID(SCSERVER	192, 168, 178, 74	Where Instance	ShareTest	Disk Drive	D:\6hareTest		A Share st. Tester	Full control		
DISCSERVER	192, 168, 178, 74	VMware Instance	Software	Disk Drive	D:\Share\Software		2015CSERVER (ADMINISTRATORS	✓ Full control ✓ Full control		
DESCSERVER	192, 168, 178, 74	VMware Instance	NETLOGON	Disk Drive	C:\Windows\øysvol\øysvol\JDESC.local\@CR3PTS	Logon server share	A JOISCSERVER WOMENESTRATORS	✓ Full control ✓ Read		
DISCSERVER	192, 168, 178, 74	VMisare Instance	Private	Disk Drive	D: (Share Private		DISCSERVER WOMINISTRATORS SEVERYONE	✓ Full control ✓ Pull control		
DISCSERVER	192. 168. 178. 74	VMware Instance	EveryoneFolder	Disk Drive	D:\\$hareTest\EveryoneFolder		ADDISCSERVER VADMINISTRATORS	Full control		
DISCSERVER	192, 168, 178, 74	VMware Instance	Company	Disk Drive	D:\ServerFolders\Company	Company	A EVERYONE	 Ful control Ful control 		
om-laptop3.fritz.box	192, 168, 178, 125	Laptop	temp	Disk Drive	C:\benp		TOM-LAPTOP3'ADMINISTRATORS	 Full control Full control 	Apple	
om-laptop3.fritz.box	192, 168, 178, 125	Laptop	trp	Disk Drive	C:\tmp		TOM-LAPTOP3(ADMINISTRATORS	✓ Pul control ✓ Ful control	Apple	
om-laptop3.fritz.box	192, 168, 178, 125	Laptop	diddeidaddel	Disk Drive	C1/temp		A TOM-LAPTOP3'LAYER2GROUP	✓ Full control ✓ Read	Apple	
										5

Figure: All Shared Resources



To display all *administrative shares, check the "Include administrative shares" check-box.*

2.4 Shared Resources Per User

JDisc Discovery can display all network shares which the selected user has access to. Select the *Effective Permissions* context menu item or button to display all network shares that can be accessed by the selected user.

Case sensitive filter					
User Name	Login	Status	User Group Count	Canonical Name	🔀 Delete
Admin	JDISC\ADMIN		. 12	2 JDISC.local/Users/Admin	Langed on Device (c)
Administrator	JDISC\ADMINISTRATOR			JDISC.local/Users/Administrator	Logged on Device(s)
Discovery Search Mailbox	JDISC\SM BE4521298E5645EB9		C	JDISC.local/Users/DiscoverySearchMailbo	Logged on History Device(s)
Exchange Online-ApplicationAccount	JDISC\\$ANR 100-U6R8HS6MI 1KP		C	JDISC.local/Users/Exchange Online-Applic	
Guest	JDISC\GUEST			JDISC.local/Users/Guest	📣 User Groups
HealthMailbox 140 1c8e 3dd 13466 1bfcc 1b 700b0a0	542 JDISC\SM_1009DB8643FB4F50A		0	JDISC.local/Users/HealthMailbox1401c8e	Effective Permissions
HealthMailbox79732a72b1ce459982660481687d	2a8b JDISC\SM_CC56F858DBFA4288B		0	JDISC.local/Users/HealthMailbox79732a7	
HealthMailboxcab64115cc8d4f6dacfacd4a289e6	38c JDISC\SM_F3D98CE292174EF79		0) JDISC.local/Users/HealthMailboxcab64115	
Karl Napp	JDISC WARL NAPP		1	JDISC.local/Users/Karl Napp	
krbtgt	JDISC WRBTGT			I JDISC.local/Users/krbtgt	
Microsoft Exchange	JDISC\SM_AE58A 1FDADFD488AB		0	JDISC.local/Users/SystemMailbox{bb558c	
Microsoft Exchange	JDISC\SM_6373B30237CF42689) JDISC.local/Users/SystemMailbox{e0dc1c	
Microsoft Exchange Approval Assistant	JDISC\SM_FEB680A9E0BF460F9			JDISC.local/Users/SystemMailbox{1f05a9	
Microsoft Exchange Federation Mailbox	JDISC\SM_F7B45DADCD534D249) JDISC.local/Users/FederatedEmail.4c1f4d	
Microsoft Exchange Migration	JDISC\SM_773B37700F614D979			JDISC.local/Users/Migration.8f3e7716-20	
Share st. Tester	JDISC\SHARETESTER) JDISC.local/Germany/Development/Share	
test tester	JDISC\TESTER			JDISC.local/Germany/Development/test te	
Thomas Trenz				JDISC.local/Users/Thomas Trenz	
Thomas tt. Tre 🗙 Delete			0) JDISC.local/Germany/Development/Thoma	
Dispaly devices where us	er is logged on				
Display devises where w	er is within logged on history				
Display user group mem	berships				
Effective permissions					
13					
< III.					

Figure: Display network shares per user

The *Effective Permissions* menu item opens a new report that displays all network shares that are accessible for the selected user.

Filter:									
Case sensitive f	iter								
Name	IP Address	Manufacturer	Model	Туре	OS Version	Serial Number	Share Name	Path	Access
tom-laptop3.fritz.box	192.168.178.81	Microsoft	MacBookPro10,1	Laptop	Windows 7 Professional	C02JR3LHDKQ5	diddeldaddel temp tmp	C:\temp C:\temp C:\tmp	 ✓ Read ✓ Full control ✓ Full control

Figure: Accessible networks shares per user

This software includes software developed by various open-source projects and organizations as listed below. The corresponding files and components are copyright to the corresponding organization or vendor and all rights reserved. The software files and components distributed under the open-source licenses are distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the license of the corresponding project for specific rights and limitations under the license. Depending on the license, any product derived from the products may not be called with the name of the project nor may the name of the project appear in their name, without prior written permission. For written permission, please contact the corresponding project owner by visiting the corresponding project home page as listed below.

All license files can be found in the installation directory 'Licenses'.

- This product includes software developed by the Apache Foundation (<u>http://www.apache.org</u>). These are 'Axis', 'Commons Collections', 'Commons Net', 'CXF', 'log4j', and 'POI', 'Drools', 'log4j'.
- This product includes the 'SBLIM' WBEM implementation (http://sourceforge.net/projects/sblim/files/sblim-cim-client2/)
- This product includes icons from 'FAMFAMFAM' icon gallery 'SILK' (<u>http://www.famfamfam.com/lab/icons/silk</u>).
- This product includes Kai Toedter's 'Jcalendar' (<u>http://www.toedter.com/en/jcalendar/index.html</u>).
- This product includes the JUNG layout library (<u>http://jung.sourceforge.net</u>).
- This product includes the COLT numeric library (<u>http://acs.lbl.gov/~hoschek/colt</u>).
- This product uses the Postgres database (<u>http://www.postgresql.org</u>).
- This product uses SNMP4J (<u>http://www.snmp4j.org</u>).
- This product uses the Ganymed SSH library (http://www.ganymed.ethz.ch/ssh2).
- This product uses the drools rule engine (<u>http://jboss.org/drools</u>).
- This product uses the janino compiler (<u>http://www.janino.net</u>).
- This product uses Jyhton (<u>http://www.jython.org/Project</u>).
- The product calls the dmidecode binary (<u>http://www.nongnu.org/dmidecode</u>).
 Find the source code in the 'sources' directory.
- This product uses icons from 'Crystal Clear' (<u>http://commons.wikimedia.org/wiki/Crystal_Clear</u>).
- This product uses the 'PUTTY' ssh client.
- This product uses the dom4j library (<u>http://dom4j.sourceforge.net/dom4j-1.6.1</u>).
- This product uses the Jaxen library (<u>http://jaxen.org/</u>)

- This product uses the Jcalendar library (<u>http://toedter.com/jcalendar/</u>).
- This product uses the Jdom library (<u>http://www.jdom.org/</u>).
- This product uses the saxpath library (<u>http://www.saxpath.org/</u>).
- This product uses the miglayout library (<u>http://www.miglayout.com/</u>).
- This product uses the taskdialog library (<u>https://code.google.com/p/oxbow/</u>).
- This product uses the vijava library (<u>http://vijava.sourceforge.net/</u>).
- This product uses the dnsjava library (<u>http://www.dnsjava.org/</u>).
- This product uses the trove library (http://trove.starlight-systems.com/).