

**JDisc Discovery 5.0** 

**User Manual** 

#### 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.

## **Table of Contents**

1 Introduction	12
1.1 Starter Edition	12
1.2 Discovery Product Categories	12
1.3 Agent-based Products	12
1.4 Zero-Footprint Products	13
1 5 Passive Discovery Products	13
1 6 Agent-less Products	13
1 7 Product Inventory's Architecture	13
1.8 Summary	14
2 Getting Started	14
2.1 Starting the User Interface	15
2.1 Starting the User Interface	15
2.2 Understanding the User Interface	10
2.3 Initial Configuration	10
2.3.1 Define the Discovery Algorithm for Finding new Devices	
2.3.2 Select Major Platforms To Discover	
2.3.3 Configure default accounts for Unix and Mac OS X	20
2.3.4 Configure default SNMP credentials	21
2.3.5 Data Collection	22
2.3.6 Configure Microsoft Active Directory Access	23
2.3.7 The Discovery Scope	25
2.3.8 IP4 Networks And Ranges	26
2.3.9 Windows Network Neighborhood Objects	27
2.3.10 Directory Objects	28
2.4 Start the Discovery	29
2.5 Review The Result	
3 Concepts	
3.1 Pattern Matching	
3.1.1 Wildcard Matching	
3.1.2 Regular Expression Matching	
3 2 Discovery	33
3 2 1 The Discovery Process	
3.2.2 Ports and Protocols	35
3 2 3 Login Credentials	36
3.2.4 Credential Handling	
3 2 5 Pemote Login	
3.2.0 Remote Login	
2.2.1 Define your own Croune	
2.2.1.1 Create Network/Dange groups	40
3.3.1.1 Create Windows Network Neighborhood groups	
3.3.1.2 Create Windows Network Neighborhood groups	
3.3.1.3 Create Directory group	
3.3.1.4 Create a group based on device attributes	45
3.3.1.5 Groups and default accounts	
3.3.2 Groups and Reports	51
3.4 Scheduled Discovery Jobs	52
3.5 Control the discovery	55
3.5.1 Start discovery	55
3.5.2 Stop discovery	56
3.5.3 Pause discovery	56

3.5.4 Resume Discovery	56
3.5.5 Synchronize Directory	56
3.5.6 Synchronize Networks	56
3.6 The Status Panels	57
3.6.1 Devices status	58
3.6.2 Ping	59
3.6.3 Windows Network Neighborhood status	60
3.6.4 Directory Status	61
3.6.5 Status of Discovery Jobs	61
3.6.6 Data Quality	62
3.6.7 Database Status	63
4 Discovery Scenarios	64
4.1 Active Directory environments	64
4.1.1 Directories and DNS Domain Controllers	64
4.1.2 Manually Discover DNS Domain Controllers	64
4.1.3 Synchronization of Directory Objects and IP Networks	65
4.1.4 Relating Member Computers to Directory Objects	65
4.1.5 Discover directory member computers.	66
4.1.6 Simplifying configuration of Credentials	66
4.2 Discover Windows Computers	67
4.2.1 Enter Credentials for directory objects	67
4.2.2 Enter Credentials for windows Network Neighborhood Objects	68
4.2.3 Enter Windows default Accounts	69
4.2.4 Enter per device Credentials	70
4.3 Discover Unix and Apple MAC OS X Computers	71
4.4 Discover SNMP based devices	72
4.5 Virtualization technologies	73
4.5.1 Scanning VMware Environments	74
4.6 Discovery Using Jumphost	75
4.7 Discover Cloud Environments	77
4.7.1 Microsoft Azure	77
4.7.1.1 Preparation Within The Azure Portal	78
4.7.1.2 Configuration within Product Inventory	
4.7.1.3 Checking Azure Cloud Results	81
4.7.2 Amazon AWS	82
4.7.2.1 Preparation Within The AWS Portal	82
4.7.2.2 Checking Amazon AWS Cloud Results	82
4.7.3 Google Cloud Platform	83
4.7.3.1 Preparation Within The Google Cloud Platform	83
4.7.3.2 Configuration within Product Inventory	84
4.7.3.3 Review Google Cloud Platform Scan Results	84
4.7.4 Cisco Meraki	
4.7.4.1 Preparation Within The Cisco Meraki Portal	
4.7.4.2 Checking Cisco Meraki Cloud Results	85
4.8 Discover Users and User Groups	
4.8.1 Discover Local Users And User Groups	
4.8.2 Discover Active Directory Users And User Groups	
4.8.3 The User group Browser	
4.8.4 User Report	
4.8.5 User Group Report	88

4.9 Discover Databases	.89
4.9.1 Configure Database Accounts	.89
4.9.2 Review Database Discovery Results	.90
4.9.3 Discover Oracle Database Instances	.91
4.9.3.1 Discover Oracle Instances on Unix Computers	.91
4.9.3.2 Discover Oracle Instances on Windows Computers	.91
4.9.3.3 Oracle Multitenant databases from version 12c	.91
4.9.4 Discover Oracle MySQL Database Instances	.92
4.9.5 Discover IBM DB2 Database Instances	.92
4.9.5.1 Discover IBM DB2 Instances on Unix Computers	.92
4.9.5.2 Discover IBM DB2 Instances on Windows Computers	.93
4.9.6 Discover Microsoft SQL Server Instances	.93
4.9.7 Discover Postgres Database Instances	.93
4.9.7.1 Discover Postgres Instances on Unix Computers	.93
4.9.7.2 Discover Postgres Instances on Windows Computers	.94
4.9.8 Discover Sybase Database Instances	.94
4.9.8.1 Discover Sybase Instances on Unix Computers	.94
4.9.8.2 Discover Sybase Instances on Windows Computers	.94
4.10 Running Oracle LMS Scripts	.94
4.10.1 Import Oracle LMS Scripts into Product Inventory	.95
4.10.2 Review the Results	.95
4.10.3 Bulk Export	.96
4.11 JEE Server Discoverv	.96
4.11.1 IBM WebSphere.	.96
4.11.2 Oracle WebLogic	.96
4.11.3 JBoss	.96
4.12 Using Password Managers	.96
4.12.1 Paswordstate	.96
4.12.1.1 Prepare Passwordstate Server	.97
4.12.1.2 Product Inventory Configuration Steps	.97
4.12.2 Thycotic SecretServer	.98
4.12.2.1 Prepare Thycotic SecretServer	.98
4.12.2.2 Product Inventory Configuration Steps	.98
4.12.3 CyberArk	.99
4.12.3.1 Prepare CyberArk	.99
4.12.3.2 Product Inventory Configuration Steps1	103
4.12.3.3 Using CyberArk Accounts	105
4.12.4 Microsoft LAPS1	07
4.12.4.1 LAPS Architecture Overview1	07
4.12.4.2 Configure LAPS in Product Inventory	107
4.12.4.3 Configure a LAPS Account1	801
4.12.4.4 Configure Local Administrator Accounts1	801
4.13 Cluster Discovery1	801
4.13.1 Veritas Cluster1	801
4.13.2 Microsoft Cluster Services1	801
4.13.3 HP ServiceGuard Cluster1	801
4.13.4 Cisco HSRP Cluster1	109
4.13.5 VRRP Cluster1	109
4.13.6 Fortinet HA Cluster1	109
4.13.7 Juniper HP Cluster1	109

4.13.8 Unix Cluster	109
4.14 Microsoft Exchange Server Discovery	109
4.14.1 Configuration	109
4.14.2 Exchange Server Reports	110
4.15 Support Entitlement Discovery	111
4.15.1 Cisco Warranty Information	111
4.16 Multicast mDNS/UPnP Device Discovery	111
4.16.1 Discovery Process	111
4.16.1.1 IP and MAC Address Resolution	112
4.16.2 Supported Device Types	112
4.16.3 Unknown Devices	113
4.16.3.1 Unknown mDNS Devices Report	113
4.16.3.2 Unknown UPnP Devices Report	114
4.16.4 Ignoring personal devices in home office environments	
5 Discovery Configuration	117
5 1 General Tab	117
5.2 Scope Tab	118
5.2.1 Scone Tabs	119
5 2 1 1 Properties	119
5.2.1.2 IPv4 Networks	110
5.2.1.2 If V4 Networks	120
$5.2.1.3$ if $\sqrt{4}$ Address Ranges	120
5.2.1.4 If VO Network Neighborhood	122
5.2.1.6 Directory	123
5.2.1.0 Directory	124
5.2.1.7 SINVIE	120
5.2.1.0 Accounts	120
5.2.2 Root Gloup	120
5.2.3 Sub Groups	129
5.3 Directory tab.	129
5.3.1 Conligure Directory DNS Domain Controller	
5.4.1 Standard Data Collection	
5.4.1.1 Users	
5.4.1.2 Software/Hardware	
5.4.2 Virtualization Data Collection	
5.4.3 Exchange Server	132
5.4.4 Database Discovery	133
5.4.5 Custom Data Collection	134
5.4.6 File Collection	134
5.5 Discovery Jobs	135
5.5.1 Properties	137
5.5.2 Groups	137
5.5.3 Directory	138
5.5.4 Schedule	139
5.5.4.1 Run Once	139
5.5.4.2 Daily	140
5.5.4.3 Weekly	140
5.5.4.4 Monthly	140
5.5.4.5 Recurring	141
5.6 Protocols	141

5.6.1 Windows Computers	.142
5.6.1.1 WMI and Remote Registry Protocol Tunneling	143
5.6.2 Unix and Mac OS X computers	.143
5.6.3 Windows Computers	.144
5.7 Filters	.145
5.7.1 IP Exclusion Filter	146
5.7.2 Attribute Based Filters	.146
5.7.3 Filter Information	.149
5.8 Cloud	150
5.9 SSH Keys	150
6 Reporting	152
6.1 Built-in Reports	.154
6.1.1 Devices	.154
6.1.1.1 Directory Membership	.154
6.1.2 Virtualization	.155
6.1.3 Software	155
6.1.4 Networking	155
6.1.5 User	.155
6.1.5.1 Login Credentials	.155
6.1.6 Troubleshooting	.158
6.2 Common actions.	.158
6.2.1 Run immediate discovery	.158
6.2.2 Manage devices	.159
6.2.3 Compare Devices	.160
6.2.4 Connect to device	160
6.2.5 Troubleshooting	.162
6.2.6 Delete Devices	.162
6.2.7 Create Support ZIP	162
6.3 The Device Details Report	163
6.3.1 General tab	.163
6.3.2 Networking tab	.164
6.3.2.1 Interfaces	165
6.3.2.2 Networks Tab	.165
6.3.2.3 SNMP System Group	.166
6.3.3 Hardware	.167
6.3.3.1 Processors	.167
6.3.3.2 Memory Modules	.168
6.3.3.3 disks	.169
6.3.3.4 Video Controller	172
6.3.3.5 Attached Devices	173
6.3.4 Firmware	174
6.3.5 Software	175
6.3.5.1 Operating System	175
6.3.5.2 Applications	.176
6.3.5.3 Application instances	.177
6.3.5.4 Patches	178
6.3.5.5 Services	179
6.3.5.6 Drivers	179
6.3.5.7 Executables	180
6.3.5.8 Processes	181

6.3.5.9 Cluster	181
6.3.6 User	181
6.3.6.1 Logged on Users	181
6.3.6.2 Local Users	182
6.3.6.3 Logged On User History	183
6.3.7 Virtual Computers	184
6.3.8 Custom Attributes	185
6.3.9 Roles	186
6.3.10 Groups	187
6.3.11 Analyze	188
6.3.11.1 Discovery log	188
6.3.11.2 Protocols	189
6.3.11.3 Parsing Issues	190
6.3.11.4 Diagnostics	191
6.4 Virtualization Explorer	193
6.5 Send Reports via EMail	193
6.5.1 Configure The Mail Server	193
6.5.2 Scheduling a report	195
6.5.2.1 Scheduling	195
6.5.2.2 Mail Content	196
6.5.2.3 Export Settings	197
6.5.2.4 Selecting recipients of the desired report	198
6.5.3 Remove/Change your scheduled report.	199
6.6 Scheduled Report Export	200
6.6.1 Scheduling The Export	200
6.6.2 Manage Report Export Jobs	204
6.6.3 Manage Storage Locations	204
6.7 Custom reports	204
6.7.1 Create custom reports	205
6.7.2 Run Custom reports	207
6.7.3 Modify Custom reports	208
6.7.4 Remove Custom reports	208
6.7.5 Export And Import Custom reports	208
7 WMI/WBEM Browser	210
7.1 Background	210
7.2 CIM Object Model	210
7.3 Browser	210
8 Comparing Devices	213
8.1 Comparing Scalar Reports	213
8.1.1 Comparing Tables	214
9 Custom Attributes	216
9.1 Configure Custom Attributes	216
9.2 Edit Custom Attributes	217
9.3 Configure Custom Attribute Data Collection	218
9.3.1 Configure Windows Registry Collection	219
9.3.2 Configure Remote Command Execution	220
9.4 Review Custom Attributes	223
9.4.1 Device details	223
9.5 Import Custom Attributes	225
9.5.1 The Import Process	225

9.5.2 Import File Format22	27
10 Documents	28
10.1 Manage Documents22	28
10.2 Use Documents	28
10.3 Documents and Reports23	30
11 Simplified File Collection	32
11.1 Add new Collections23	33
11.2 Change or remove collections23	33
12 Custom Software Discovery	35
12.1 The XML Schema23	35
12.2 Import Software Data Collections23	36
12.3 Configure Custom Software Data Collection scripts23	37
13 Troubleshooting	39
13.1 Support ZIP	40
13.1.1 Product Support ZIP24	40
13.1.2 Device Support ZIP24	41
13.2 Data Quality Tab24	42
13.3 Protocol status	44
13.3.1 Discovery Protocol Status Report24	44
13.3.2 Device Discovery Protocol Report24	45
13.3.3 Single Device Protocol Status	46
13.4 Discovery logs24	47
13.5 Parsing issues	47
13.6 Common Windows computer Configuration Problems24	48
13.6.1 the network logon service was not started24	48
13.6.2 IO Failure and Network Path was Not found Symptoms	48
13.6.3 Logon failure and Access Denied Symptoms	49
13.7 Unknown SNMP devices24	49
13.8 Unknown telnet banners2	50
14 Open Source	52

# 1 Introduction

Automatic IT discovery is the process of finding and identifying devices on a network.

## 1.1 Starter Edition

Note that the feature-set is limited when using JDisc Discovery 's Essential Edition! The starter edition does not display all dialogues or reports described within this manual!

## **1.2 Discovery Product Categories**

The network discovery product market is segmented into four product categories:

- 1. Agent based
- 2. Zero-footprint
- 3. Passive
- 4. Agent-less

Products in these categories can create an inventory of devices on a network but follow different approaches. Products often implement techniques from theses categories.

## 1.3 Agent-based Products

Agent-based products require a proprietary data collection agent. Agents are small applications or scripts that are permanently installed and run as daemons on target computers. A central discovery or management application polls the data collection agent, collects inventory data, and finally stores inventory data in a database. The agent deployment can be either manual or automatic depending on the product.

The advantage of agent based discovery applications is that agents can collect virtually any kind of data on the target computer. Agents run locally on target computers and typically have full access to all system resources. By comparing current data with the last transmitted data, agents can minimize network utilization.

The disadvantage of agent-based systems is that many device types such as printers, routers, switches, etc. do not allow installing agents. Agent deployment can also be time consuming and might create security and performance risks unless thoroughly tested and well designed.

## 1.4 Zero-Footprint Products

Zero-footprint products do not permanently deploy agents on target computers. In many cases they rely on running system commands on target devices. Sometimes they might also deploy their own scripts or binaries on target computers for the duration of the discovery. These scripts and binaries are deleted once the discovery has completed. Thus the target computer's configuration has not changed compared to the configuration before the scan. Similar to agent-based tools, zero-footprint products can collect virtually all kind of information. Zero footprint tools share some of the disadvantages of agent-based systems, such as possible security and performance risks. However, in most cases, system commands are powerful enough to retrieve all necessary information and no proprietary scripts or binaries are used at all.

## **1.5 Passive Discovery Products**

Passive discovery products scan packets on the network. Network traffic can contain information about devices, their IP and MAC addresses, and sometimes information about running applications. Passive discovery products can create an inventory from information extracted from network packets that the discovery product receives.

The advantage of passive discovery products is the zero impact on the network. These products don't actively send network packets to target computers. However, since they rely on listening to network packets they'll not find devices that create minimal or zero network traffic. Moreover getting detailed device information is difficult if not impossible without sending packets to target devices.

## 1.6 Agent-less Products

*Agent-less products* (also called non-intrusive products) use only protocols that are available on target computers. Virtually every device on the network exposes some kind of protocol suitable to query basic configuration data. Some prominent examples for such protocols are SNMP, WMI, and WBEM.

Agent-less products can be easily deployed because they do not need to install proprietary agents on target computers. With a wide variety of protocols, they can get very detailed information.

However, as agent-less products are limited to standard protocols, they can only discover the information that the standard protocols expose. Furthermore (local) firewalls can prevent agents-less products to get detailed information from devices behind the firewall.

## 1.7 JDisc Discovery's Architecture

JDisc Discovery uses zero-footprint and agent-less technologies. It follows the client-

server architecture. The user interface client communicates via RMI with the discovery server. The discovery server runs as a Windows service in the background. The user interface client and the discovery server might also be installed on different computers.

The figure below illustrates JDisc Discovery's architecture.

Figure: JDisc Discovery architecture

The discovery server

- hosts the discovery process
- prepares reports for user interface clients
- loads and stores the discovery configuration
- provides maintenance functionality such as archive/restore of the database

The user interface client

- interacts with the user
- sends user requests to the discovery server

## 1.8 Summary

JDisc Discovery is a client-server application and it's discovery is a combination of agent-less and zero-footprint products.

The discovery process follows three concepts:

- 1. Finding active devices: JDisc Discovery uses a variety of protocols to find active devices on the network. ICMP-ping requests find devices in IP sub-networks or ranges. *Windows domain discovery* finds devices in NTLM domains. *LDAP* queries find devices in Microsoft Active Directory environments.
- 2. *Identify devices:* When JDisc Discovery has detected an active device, it attempts to identify it. Identifying a device means to query basic device information, such as manufacturer, model, and device type.
- *3. Collect data:* JDisc Discovery performs further data collection once a device has been identified. This includes a variety of hardware, software and configuration information.

*Discovering* a device using JDisc Discovery includes *identification* and *data collection*. Other products might have a different definition of discovery. Be careful when comparing JDisc Discovery with similar products!

## 2.1 Starting The User Interface

To start the JDisc Discovery client, click JDisc » JDisc Discovery 5.0 » JDisc Discovery from the Windows Start menu. JDisc Discovery uses Windows authentication.

The JDisc Discovery client brings up the login dialog, which prompts for:

- The JDisc Discovery server to connect to
- The user name. JDisc Discovery uses Windows' built-in user authentication. The first user who logs on to JDisc Discovery becomes it's primary administrator. Note: JDisc Discovery's user management allows to administer users and user groups.
- The user's Windows password
- The server's RMI port (default is 30470)

Use your Windows account to login for the first time. By default, JDisc Discovery suggests your current login name for the first login.

Connect to JDisc Discovery Ser	ver 🗖 🗖 🗙
Disc	
Server hostname	localhost
Windows user name	JAMES SMITH
Windows password	•••••
Server RMI port (default 30470)	30470
	Ok Cancel

Figure: Login to the JDisc Discovery server.

Use your Windows account to log on for the first time. By default, JDisc Discovery suggests the interactive login name.

Note: The server's and client's RMI ports can be changed. Refer to the Administration Guide for more information.

## 2.2 Understanding The User Interface

The user interface's main area displays status information. It shows information about discovery activity including devices currently being discovered, IP networks and ranges currently being pinged, Windows domains, and directory objects currently being discovered. The *Discoveries* tab lists all scheduled discoveries including their current status and schedule.

Disc Discovery [Enterprise Editio	n] - JAMES SMITH conn	ected to localhost	
Discovery Devices Software	Networking User Docu	ments Troubleshooting Administration Help	
Status Discovery i	s idle	Click for instruction to improve the da	ons on how ata quality!
Devices         Ping         Network Neighbor           Concurrent device discoveries         0           Average duration         0           Discovery jobs         0           Manually triggered         0           Devices in database         1	hood Directory Discover 1 of 10 1 of 0 pending 0 pending 18	y Jobs   Data Quality   Database	
Device	Duration	Last message	

Figure: JDisc Discovery's main window

The menu provides eight items:

- File: Exit the application
- Discovery: Configure and manually start the discovery
- Devices: Various device reports
- Software: Various software related reports
- Networking: Various network reports
- User: Various user related reports
- Documents: Document management
- Troubleshooting: Various reports to troubleshoot the discovery result
- *Administration:* Several administrative tasks such as backup, clear, and restore the database
- Help: On line help, license status, and the About dialog

## 2.3 Initial Configuration

During installation, JDisc Discovery's installation program detects and configures the local network. JDisc Discovery requires initial configuration information. Use JDisc Discovery's configuration wizard to create the initial configuration

Note: The configuration wizard does not cover all discovery configuration options. Use the *Configuration* menu item from the *Discovery* menu for detailed configuration.

Open the Configuration Wizard from the Discovery menu.

D Configuration Wizard
The configuration wizard guides you through the initial configuration and helps to customize JDisc Discovery to your needs. Use the wizard to configure:
<ul> <li>The discovery scope</li> <li>Active Directory environments</li> <li>IP4 networks and IP ranges</li> <li>Desired device types, such as Windows computers, Unix, etc.</li> </ul>
<ul> <li>Windows network neighborhood objects and Windows domain login credentials</li> <li>Active Directory objects and directory login credentials</li> </ul>
Note: The configuration wizard does not cover all possible configuration options. Experienced users should use the Advanced Configuration dialogs.
Back Next Finish Cancel

Figure: Configuration Wizard

The configuration wizard will guide you through the initial configuration. The explanation section on the bottom of the dialog informs you about important aspects of the

configuration. The dialog covers:

- Discovery scope (networks, IP ranges, Windows domains, Microsoft Active Directory objects)
- Desired platforms (such as Windows, HP-UX, Linux, ...)
- Default access credentials for each platform
- Default SNMP communities and SNMPv3 accounts.
- Data items to discover (such as processors, memory modules, software, ...)
- Microsoft Active Directory access

Click *Next* to get to the first configuration screen.

#### 2.3.1 Define The Discovery Algorithm For Finding New Devices

As a discovery product, JDisc Discovery's purpose is to find devices on the network. Depending on the purpose of the discovery exercise, a user might want to discover as many devices as possible or restrict the discovery to a well defined area. Answer the question with *yes*, if you would like to discover only a well defined part of your network. Answer with *no* to discover as many devices as possible.

Note: The discovery might also leave your company network, if it finds IP addresses outside the network in a device's ARP cache or in its IP connections. Refer to chapter 5 to learn how to configure the discovery algorithm on a finer granularity.

D Configuration Wizard	
Discovery Scope Discover only selected networks, domains, and directories?  yes  no	
JDisc Discovery offers a variety of different methods to find devices on the network. JDisc Discovery can         1. Ping IP subnetworks and IP ranges         2. Browse Windows network neighborhood objects         3. Query objects in directories         4. Lookup DNS domain servers for each DNS domain         5. Locate Windows Domain controllers         6. Find devices connected to other devices (only when the dependency mapping add-on is installed)         The first three methods described well defined areas of your network. IP subnetworks are defined by subnet base address and a subnet mask. IP ranges are defined by start and end address. Windows network neighborhood objects are defined by their path within a directory.         The last three methods find devices that are not restricted to specific IP subnetworks, IP ranges, Windows network neighborhood objects or directory objects.	
You can limit JDisc Discovery to discover only selected IP subnetworks, ranges, Windows network neighborhood objects and directory objects or discover as many devices as possible regardless where they reside on the network. Select Yes to limit JDisc Discovery's discovery to selected IP subnetworks, IP ranges, Windows network neighborhood objects and directory objects.	
Back Next Finish Cancel	]

Figure: Configure how to find new devices

## 2.3.2 Select Major Platforms To Discover

JDisc Discovery can discover a variety of devices. Select the major platforms that are of interest for your project. The wizard will adjust the discovery configuration to get an optimal discovery result.

The *Next* button will skip the default accounts screen unless at least one Unix platform or Apple's Mac OS X is selected.

D Configuration	Wizard
Device Types	
	Discover Windows server, workstations, and laptops
	☑ Discover AIX computers and workstations
	☑ Discover HP-UX server and workstations
	☑ Discover Linux computers, VMware ESX, and Oracle VM servers
	☑ Discover MacOSX server, workstations, and laptops
	☑ Discover Sun Solaris server and workstations
JDisc Discove protocols are	ery can discover many different device types and operating system using a variety of protocols. Not all relevant for all operating systems.
For instance, Enterprise Ma computers.	WMI (Windows Management Instrumentation) is Microsoft's implementation of the WBEM (Web Based anagement) standard. WMI requires administrative login credentials and is only applicable for Windows
Unix compute that, JDisc Di technique is login. JDisc D	ers often do not expose detailed information via standard protocols such as SNMP or WBEM. Because of scovery uses command line based protocols such as Telnet and SSH to execute system commands. This called <i>Remote Login</i> . You need to configure login credentials or SSH keys for each operating system to Discovery cannot discover detailed information without logging on to Unix computers.
It is a good p	ractive to only select those operating systems that you want to discover.
	Back Next Finish Cancel

Figure: Select major Device Platforms

This dialog might vary depending on the licensed edition.

## 2.3.3 Configure Default Accounts For Unix And Mac OS X

JDisc Discovery discovers Unix computers by using remote login. It logs on via SSH or telnet, then it executes system commands, and parses the output to get detailed information about a Unix or Mac OS X computer. SSH and telnet require accounts to for a successful log-on. Use this screen to enter default accounts for the selected platforms.

Note: Be careful with adding too many default accounts. Testing many default accounts (especially with SSH) can cause intrusion detection alerts!

Use JDisc Discovery's grouping mechanism to define default accounts on a much finer granularity. Refer to section 3.3 for more details on how to group devices and networks.

P-UX Sun Solaris IBN	4 AIX Linux/VMware/Xe	enServer/Oracle VI	Mac OS X			
HP-UX Accounts						
User name	Password	Туре				Add
						Remove
						Move up
Total 0 Accounts 1.0	Accounts selected					Move down
	inte laure la contra ta	- (				Move up Move down
Total 0 SSH public/pi	rivate keys   0 SSH publi	c/private keys sele	ected			
	on to Unix comput	ers and collec	t detailed har	dware and so	oftware inforr	nation using Telnet o
Discovery can log	,					

Figure: Define Default Accounts

#### 2.3.4 Configure Default SNMP Credentials

JDisc Discovery uses SNMP to discover most network devices such as routers, switches, printers, and others. SNMP requires access credentials. For the protocol version 1 and version 2c, it requires a so called SNMP community which is basically a simple password. The factory default for most devices is 'public'. Therefore this account is pre-configured JDisc Discovery's discovery. Add new communities as needed.

SNMPv3 was developed to overcome security problems<sup>1</sup> with the protocol versions 1 and 2c. Use the SNMPv3 configuration area to provide default SNMPv3 access credentials.

ault SNMP Credentials						
SNMPv1/v2c Communitie	25					
Community						Add
public						Remove
						Move up
						Move down
Total 1 SNMP communi	ty   0 SNMP communitie	es selected				
SNMPv3 Accounts						
User name	Password	Auth. protocol	Privacy password	Priv. protocol		Add
						Remove
						Modify
						Move up
						Move down
Total 0 SNMPv3 accou	nts   0 SNMPv3 accoun	ts selected				
Discourse	the ONINE (Circuit			-14-54-64		a atua du
sc Discovery uses	the SMMP (Simpl	e Network Man	agement) protoc	or to identify (	uevices on the	network.
isc Discovery supp	orts SNMPv1, SN	MPv2c, and SN	MPv3. SNMPv1	and SNMPv20	require so ca	lled communities as
on credentials. Mo	ost devices have t	een configure	d using the defai	ult community	("public") when	n they shipped from
manufacturer. SN	IMPv1 and SNMP	/2c are not sec	cure because dat	a (including l	ogon credentia	ls credentials) is

Figure: SNMP Community and Account Configuration

#### 2.3.5 Data Collection

JDisc Discovery collects hardware, software and configuration information from devices on the network. During discovery, JDisc Discovery sends to and receives data from devices being discovered. The data volume affects the network bandwidth that is utilized during discovery. The more information is collected, the more network bandwidth will be utilized.

The *Data* Collection dialog allows configuring data collection to fit to your needs. Enable or disable collection items as needed.

<sup>1</sup> SNMPv1 and v2c transmit the community unencrypted string in clear text.

Depending on the license, some items might not be available in the user interface.

✓ Discover users         Ignore       Built-in users         ✓ Delete users from logged on t         ✓ Find terminal services clients         □ Discover terminal services	▼ user history when not logged on for 30 🚖 a clients	day(s)	
Software/Hardware	Discover executable files     Oiscover processor	<ul> <li>✓ Discover disks</li> <li>✓ Discover virtual instances</li> </ul>	Discover attached devices     Joscover monitors
Discover patches	Discover memory	Discover blade enclosure components	Discover local printers/mfp
V Discover services	Discover video controllers	Discover managed devices	Discover local scanner
<ul> <li>✓ Discover drivers</li> <li>✓ Discover processes</li> <li>✓ Use pargs on Solaris</li> </ul>	[¥] Discover duster	☑ Discover VMware annotations	☑ Discover card reader
oose the hardware and softwa te: The more options you choo ose options that you need.	re options to discover.	and create more network traffic. It is	a good practice to select only

Figure: Data Collection Configuration

To reduce network utilization, limit the data collection to those items that are important for your!

#### 2.3.6 Configure Microsoft Active Directory Access

JDisc Discovery supports Microsoft Active Directory for discovery of devices that are member of a directory. A subset of directory objects will be synchronized with JDisc Discovery's database either on request or automatically when running a discovery cycle. Directory object types that can be synchronized include

- DNS domains
- Organizational units
- Containers
- Computer accounts

- User groups
- Users

JDisc Discovery queries directory member computers of enabled directory objects using the Global Catalog (GC) service and also DNS domain controllers (DC) when discovering recently logged-on computers. The resulting DNS host names of member computers are looked-up and to IP addresses and are inserted into the device queue for discovery.



Figure: Directory Access

JDisc Discovery uses the Lightweight Directory Access Protocol (LDAP) to connect to the Global Catalog (GC) service and also to DNS domain controllers (DC). The Global Catalog (GC) holds a subset replica of all directory objects across all DNS domains and trusted DNS domains.

You can configure access credentials to the Global Catalog (GC) and the Domain Controllers (DC) for each DNS Domain. JDisc Discovery uses these access credentials (service account) to synchronize directory objects but also to query directory member computers.

Select *yes* to configure Active Directory access or *no*, if Microsoft Active Directory is not installed on your network.

Configure at least one DNS domain controller / Global Catalog (GC) server for directory access and add login credentials to connect to the DNS domain controller. Click *Test* to

test the configuration. Click *Sync Networks* to synchronize IP networks configured in the directory and *Sync Directory* to synchronize the directory with JDisc Discovery's database.

Click *Test* to check the DNS domain controller connection before moving on to the next dialog!

D Configuration Wizard	
Active Directory Support	
Is Microsoft	Active Directory running on your network? 💿 yes 💿 no
DNS Domain Controller	Test Login
Service account	Sync Networks
Password	Sync Directory
	Reset
JDisc Discovery suppor 1. The directory a 2. Synchronizing I In order for JDisc Disco domain controller hostri- test the connectivity. Cl Note: This might take so You must test the conn <i>Reset</i> button to reset the	ts Microsoft Active Directory and provides these benefits: llows configuring the discovery scope with finer granularity than Windows domains. P networks from the directory reduces manual configuration or importing of IP networks. very to access a directory one DNS domain controller is required per directory. Provide a DNS name and login credentials (not necessarily an administrative account), click the <i>Test</i> button to ick the <i>Sync Directory</i> and <i>Sync Networks</i> buttons to synchronize the directory and networks. ome time depending on the size of your directory and network. ection with the <i>Test</i> button before moving on to the next screen. Alternatively, you can use the ne directory controller settings.
	Back Next Finish Cancel

Figure: Active Directory Configuration

#### 2.3.7 The Discovery Scope

The discovery scope, including

- IP4 networks
- IP4 address ranges
- Microsoft Windows network neighborhood objects
- Microsoft Active Directory objects

defines what JDisc Discovery is going to discover.

D Configuration Wizard	×
Discovery Scope	
Would you like to configure IP4 networks and rang	es? 💿 yes 💿 no
Would you like to configure Windows domains and	their administrative accounts? 💿 yes 💿 no
Configure the discovery scope. The discovery scope defined by	determines what JDisc Discovery will discover. The scope can be
Enabled IP4 networks     Enabled IP4 address ranges     Enabled Windows network neighborhood obje     Enabled Active Directory objects	cts
When the discovery starts, JDisc Discovery enabled If Windows network neighborhood objects, and queries	P4 networks and IP4 ranges, browses computers in enabled computeres in enabled Active Directory objects.
Note: Windows network neighborhood browsing dependent periodically populates the browser cache. However with several minutes until the browser cache is populated.	nds on the Windows domain browser cache. Microsoft Windows ien your computer has been started only recently, it might take
	Back Next Finish Cancel

Figure: Define the Discovery Scope

#### 2.3.8 IP4 Networks And Ranges

On the *IP4 Networks* tab add, import or change the configuration of IP4 networks. JDisc Discovery only pings enabled networks (indicated by the check mark).

Add IP4 address ranges on the *IP4 Ranges* tab. JDisc Discovery only pings enabled ranges (indicated by the check mark).

D Configuration Wizard				X
IP4 Networks IP4 Ranges				
Filter:				Enable
Case sensitive filter				Disable
Network Address	Subnet Mask	Name	Last Discovered	Add
192.168.178.0	255.255.255.0			Browse
				Remove
				Import
Total 1 network   0 networks se	elected			
Configure IP4 networks a ranges when the discover	nd IP4 address range ry is started.	es for discovery. JDis	c Discovery pings configured IP4 n	networks and IP4
			Back	Finish Cancel

Fig: Define IP4 networks and IP4 address ranges

#### 2.3.9 Windows Network Neighborhood Objects

JDisc Discovery can discover member computers of Windows domains and workgroups For each Windows domain or workgroup that is enabled for discovery, JDisc Discovery queries computer names of member computers using the Windows network neighborhood. JDisc Discovery's discovery uses WINS and DNS to convert computer names into IP addresses.

Click *Change* to enter Windows domain administrator login credentials. JDisc Discovery's uses these login credentials when discovering computers that are member of a Windows domain or workgroup.

To collect detailed information of Windows computers, administrative login credentials are required. Without administrative login credentials, JDisc Discovery will only collect basic information.

Configuring administrative login credentials for Windows domains

#### avoids configuring login credentials for each Windows computer.

D Configuration Wizard				×
Network Neighborhood				
Filter:				Enable
Case sensitive	e filter			Disable
Name	Account	Last Discovered		Update
				Add
				Browse
				Import
				Change
Total 0 Network Neighb	orhood objects   0 Network Neigh	borhood objects selected		
Configure Windows	network neighborhood of browse computers in all e	pjects that are in-scope for discov enabled Windows network neighbo	ery. When the discovery is prhood objects.	started,
				=
Provide administrati	ive login credentials for ea iscovery will discover only	ach Windows domain to improve the limited details withoutadministration	he discovery result for dom ve login credentials. In mos	ain member
hardware details su	ich as serial number, mod	el, and manufacturer will not be d	iscovered without administr	ative login
credentials.				-
			Back Next Fini	ish Cancel

Figure: Define Windows Network Neighborhood Objects

#### 2.3.10 Directory Objects

JDisc Discovery supports Microsoft Active Directory for discovery of Windows computers that are a member of a directory. Active directory permits to configure JDisc Discovery's discovery on a finer level of granularity than Windows domains allow.

On the *Directory* tab expand the directory hierarchy, select one or multiple directory objects and enable them for discovery. JDisc Discovery queries member computers of enabled directory objects. Use *Change* to configure administrative login credentials to discover member computers of enabled directory and sub-directory objects.

You can configure login credentials on different levels of the directory hierarchy. JDisc

Discovery attempts to use login credentials from the the deepest directory objects first. When a login credential fails, JDisc Discovery then tries to use login credentials from higher levels of the directory hierarchy.

Windows computers require administrative login credentials to collect detailed device information. Without administrative account privileges JDisc Discovery will get only limited device information.

Using login credentials for directory objects is a convenient way to avoid configuring login credentials for each Windows computer.

## 2.4 Start The Discovery

The *Discovery » Control* menu allows to start, stop, pause, and resume the discovery process. It also contains menu items to manually initiate a directory and network synchronization for all configured directories.



Figure: Start the Discovery

Click *Start Discovery* to start the first discovery cycle. JDisc Discovery will start pinging the local network.

The status dialog displays the current discovery status:

- The *Devices* tab displays devices and IP addresses that are currently discovered.
- The *Ping* tab displays IP4 networks and ranges currently being discovered. In this example Product discovers the network 192.168.178.0 with the subnet mask 255.255.255.0.
- The *Network Neighborhood* tab displays Windows network neighborhood objects currently being discovered.
- The *Directory* tab displays directory objects currently being discovered and the directory object/network synchronization status.

• The *Discoveries* tab displays discovery cycle status information, such as last start and finished date.

D IDisc Discovery (Enterprise Edition) - 1/	AMES SMITH connected to localhoct			
File Discovery Devices Software Netwo	rking User Documents Troubleshoo	ating Administration Help		
	TKing Oser Documents Houbleshot	ang Auministration nep		
Discovery Status				
Status				
Discovery is curre	ently running			
Devices Pipe Network Neighborhood	Diseasterne Diseasterne Jacka Daska Overliter	Detribute		
Devices (119 Network Neighborhood )	Directory   Discovery Jobs   Data Quality	Database		
Status Pinging 127 IP4 addresses in o	chunks of 64 addresses			
Item	Discov	very Job	Manually Triggered	
Networks	1 of 1	to process	0 to process	
Addresses to ping	127 of	255 to process	0 to process	
Title	IP Range	Progress		
Network 192.168.178.0/255.255.255.0	192.168.178.0 - 192.168.178.255			
				]



The discovery duration depends on the network size, utilization, access speed and also the performance of the computer running JDisc Discovery.

## 2.5 Review The Result

JDisc Discovery provides a variety of built-in reports that allow viewing different aspects of your device inventory. Reports can be run at any time while the discovery is running and reflect the current discovery result.

Open the All Devices report from the Devices menu to view all discovered devices.



Figure: Open the All IP Devices Report

The *All IP Devices* report displays a list of all devices and selected attributes such as *Name*, *IP address*, *Manufacturer*, *Model*, *Type* to name just a few.

liter							
Case sensitive filter							
Name	IP Address	Manufacturer	Model	Туре	OS Version	Patch Level	FW Ve
PortServer-1	12,216,106,31	Moxa	NPort	Port Server			3.3
Printer-1	12,216,104,75	Konica Minolta	Magicolor 2350	Printer			
rinter-2	12,216,106,180	Lexmark	T640	Printer			LS.ST.
rinter-3	12,251,240,84	Hewlett-Packard	Laser Jet 4000 Series	Printer	G.08.40		G.07.1
rinter-4	12,216,106,3	Lexmark	E240n	Printer			BR.O.F
rinter-6	12,251,240,48	Hewlett-Packard	Color LaserJet CP4005	Printer	V.33.41		none
rintServer-1	12,216,105,148	Hewlett-Packard	JetDirect	Print Server	3.51		H 07
rintServer-2	12.251.240.190	Hewlett-Packard	JetDirect 170X	Print Server	F.08.20		F.08.0
roCurve1	192, 168, 178, 18	Hewlett-Packard	ProCurve 2650	Switch	H.08.72		H.08.0
ackServer-1	12,216,105,80	IBM	eServer xSeries 336	Server (Rack)	Windows Server 2003	Service Pack 2	-TAPE 1
ackServer-2	12.251.240.164	Hewlett-Packard	rx2620	Server (Rack)	HP-UX B.11.23U		04.10
lackServer-3	12.251.240.0	Hewlett-Packard	rx6600	Server (Rack)	HP-UX B.11.23U		03.01
tackServer-4	12.251.240.233	Hewlett-Packard	rx6600	Server (Rack)	HP-UX B.11.23U		03.01
ackServer-5	12.251.240.16	Hewlett-Packard	rx2660	Server (Rack)	HP-UX B. 11.23U		03.01
olaris11-test	192.168.178.26			VMware Instance	SunOS 5.11	11.1	DevCo
iolarisZone-1	12.255.136.63			Solaris Zone			
ummit1	192.168.178.13	Extreme Networks	Summit 48i	Routing Switch	7.2.0	Build 33	
ummit2	192.168.181.2	Extreme Networks	Summit 48i	Switch	7.2.0	Build 33	
ummit3	192.168.181.3	Extreme Networks	Summit 48i	Routing Switch	7.2.0	Build 33	
SunVirtualBoxInstance-1	12.251.240.97			VirtualBox Instance	Windows Server 2008 Enterprise Edition		
witch-1	12.216.107.24	Nortel Networks	Nortel GbE Switch Module	Switch			
Witch-10	12.251.240.219	Hewlett-Packard	ProCurve 2524	Switch	F.04.08		F.02.0
witch-11	12.251.240.107	Hewlett-Packard	ProCurve 2524	Switch	F.04.08		F.02.0
Switch-2	12.216.106.203	Nortel Networks	Nortel GbE Switch Module	Switch			
٠ [							•

Figure: All Devices Report

Reports are linked to other reports. Open the context menu in the report main area to open links to other reports. JDisc Discovery maintains a history of visited reports. Reports typically have a tool bar with shortcuts to frequently used actions:

- Display all available actions for the current selection.
- Return to the previous report in the report history.
- ➡ Go to the next report in the report history.

- Refresh the current report.
- Deen a new Window with the same report.
- Export the current report to a Microsoft Excel sheet using the current sorting and filtering options.
- Export the current report to a CSV plain text file using the current sorting and filtering options.
- Display the SQL query that created the current report.
- Schedule report export.
- Display the group tree to limit the report to specific groups only (refer to section 3.3 for more details on device grouping).
- Adjust the column width to fit its content.

Use the filter field to limit the report to records that contain the filter value. Using filters is also a simple way to find data in a report. Select the 'Case sensitive filter' option to filter values in the report case sensitive.

# 3 Concepts

The *Concepts* chapter explains JDisc Discovery's discovery concepts and the user interface.

## 3.1 Pattern Matching

Pattern matching can be used to define conditions in custom reports and device groups for certain device attributes, such as model, manufacturer, etc.

JDisc Discovery offers two pattern matching algorithms:

- Wildcards
- Regular expressions

#### 3.1.1 Wildcard Matching

Regular expressions are powerful, but sometimes difficult to use. This is why JDisc Discovery offers wildcard matching similar to wildcards available in a command shell. There are two wildcards:

- '\*' matches any number of characters (including 0)
- '?' matches exactly one character

For instance, the expression 'Ci???\*' matches the string 'Cisco', 'Cisco Router', but not 'Switch Cisco'.

#### 3.1.2 Regular Expression Matching

JDisc Discovery uses Posix regular expressions. Refer to the Internet for a more detailed description of Posix regular expressions.

## 3.2 Discovery

The *Discovery* section covers the general discovery process in detail, protocols and ports, and explains why JDisc Discovery needs login credentials to work properly.

#### 3.2.1 The Discovery Process

Discovery is the process of finding and identifying devices on a network. The discovery process also covers device specific data collection once a device has been identified.

Finding a device means to detect an IP address of an active device on the network. Identifying a device is the process that determines the device type, device model, and its manufacturer.

When a device has been identified and depending on the device type, the discovery collects additional hardware, software and configuration.

JDisc Discovery defines discovery of a device as the sequence of finding its IP address(es), identifying the device, and collecting additional data.

Other software vendors define the term *Discovery* differently for their products. Take this into consideration hen comparing different discovery products.

Although the process of finding, identifying, and collecting data from a device is strictly sequential, JDisc Discovery can discover devices concurrently thus speeding up the discovery. The number of concurrent device discoveries can be configured in JDisc Discovery's discovery settings.

JDisc Discovery offers several options to find new IP addresses. Depending on the configuration finding new IP addresses can happen by:

- Pinging IP4 sub-networks
- Pinging IP4 address ranges
- Browsing computers using the Windows network neighborhood
- Querying computes in a directory
- Finding new IP addresses in a device's ARP cache<sup>2</sup>
- Finding new IP addresses in a device's connection table<sup>3</sup>

Whenever JDisc Discovery has detected an active IP address it will identify the device. Identifying a device implies sending network requests (for instance SNMP, NetBIOS, WMI, etc.) to the device to collect identifying information. Protocols can be enabled or disabled independently in JDisc Discovery's discovery settings.

When a device has been identified, JDisc Discovery will (depending on the configuration) collect hardware, software and configuration data.

Most devices require access credentials to collect hardware, software and configuration data. Without credentials, JDisc Discovery collects only basic information.

<sup>2</sup> A device's ARP cache maintains a mapping between the IP address and the MAC address of a computer on a network.

<sup>3</sup> The connection table maintains a list of ports and IP addresses to connected devices.
## 3.2.2 Ports And Protocols

Alike other agent-less discovery applications, JDisc Discovery relies on protocols that are available on devices. The following table lists all protocols including their port numbers.

Protocol	Ports
Domain Name System (DNS)	53 (TCP)
Hypertext Transfer Protocol (HTTP)	80 (TCP)
Secure Hypertext Transfer Protocol (HTTPS)	443 (TCP)
Multicast DNS (mDNS)	5353 (UDP)
Universal Plug and Play (UPnP)	1900 (UDP)
Lightweight Directory Access Protocol (LDAP)	389 (TCP)
Lightweight Directory Access Protocol (LDAPS)	636 (TCP)
Lightweight Directory Access Protocol (LDAP) (Global Catalog)	3268 (TCP)
Lightweight Directory Access Protocol (LDAPS) (Global Catalog)	3269 (TCP)
Network Basic Input/Output System (NetBIOS)	137 (UDP) 138 (UDP) 139 (TCP)
Packet Internet Grouper (PING)	n/a
Secure Shell (SSH)	22 (TCP)
Simple Network Management Protocol (SNMP)	161 (UDP)
Server Message Block (SMB)	445 (TCP)
Telnet	23 (TCP)
VMware API (VIM SDK) for VMware Server	8333 (TCP)
VMware API (VIM SDK) for VMware ESX Server	443 (TCP)
Web Based Enterprise Management (WBEM)	5989 (TCP))
Windows Remote Login	Relies on SMB

Windows Remote Registry	Relies on SMB
Windows Management Interface (WMI)	135 (TCP) and a negotiated port between 1024 and 65535 (TCP)

Table: Protocols and Ports

Firewalls (either personal firewalls installed on computers or firewalls separating networks) can block discovery traffic. In order to get proper discovery results, firewalls must be configured such to let network traffic pass the above mentioned port/protocols. Alternatively, in the case of firewalls separating networks, multiple JDisc Discovery installations might be an option to workaround the firewall restrictions.

## 3.2.3 Login Credentials

Most protocols require some kind of authentication to collect data from devices on the network. Without login credentials devices usually refuse connection attempts or do not return any data at all. Depending on the protocol and the device platform login credentials must have administrative privileges or only ordinary user privileges.

Protocol	Credentials
Domain Name System (DNS)	None
Hypertext Transfer Protocol (HTTP)	None
Secure Hypertext Transfer Protocol (HTTPS)	None
Lightweight Directory Access Protocol (Global Catalog)	Any non privileged directory user account
Network Basic Input/Output System (NetBIOS)	None
Packet Internet Grouper (PING)	None
Secure Shell (SSH)	Non root user on Unix. Some information requires root user privileges on Linux.
Simple Network Management Protocol (SNMP)	SNMP read community

	or SNMPv3 account
Server Message Block (SMB)	Either none (little information with anonymous SMB), non administrative account, or administrative account
Telnet	Non root user on Unix. Some information requires root user privileges on Linux
VMware API	Read-only user for the vCenter installation. Scanning ESX servers directly (not using the vCenter) requires root access.
Web Based Enterprise Management (WBEM)	Administrative / root account.
Windows Remote Login	Administrative account
Windows Management Interface (WMI)	Administrative account
Table: Protocols and acc	ess credentials

This is the most important rule:

### No login credentials, no or very superficial information!

# 3.2.4 Credential Handling

JDisc Discovery stores a successfully tested access credentials for each device. When a device gets discovered again, then JDisc Discovery uses the access credentials that succeeded the last time. Otherwise, it would have to test all default accounts again which can be time consuming.

JDisc Discovery tests the default accounts when the assigned access credentials do not work anymore (for instance, because an administrator has changed the password).

In some cases, you might want to clear all assigned access credentials for devices. There are two ways to accomplish this task:

1. Clear accounts (e.g. user/admin accounts or SNMP communities) for selected devices. Use the context menu *Manage* » *Change...* in order to clear selected accounts.

2. Use the context menu *Manage* » *Clear Cached Accounts...* in order to delete all cached device accounts.

D All Devices						- 0 X
⇔  ← → 🤣 🔒 📭 😫 📄	💆 🗐 🔚					
Filter:						
Case sensitive filter						
Name	IP Address			Manufacturer	Model	
				APP	LED Cinema	
				APP	Thunderbolt	
tom-laptop3.fritz.box	Properties			Apple	MacBookPro10,1	
	Discover	•				
	Manage	• <i>.</i>	Change	Accounts		
	History	10	Change	VMware Accounts		
	Compare		Change	SSH public/private Key		
	Custom Attributes	, 🔎	Change	SNMP Credentials		
	Connect with	61	Clear Ca	ched Accounts		
	Troubleshoot	3	Synchro	nize Group Assignment.		
×	Delete Devices	-				
	Create Dependency Map	_				
	Create Topology Map					
- -	Create Support ZIP					
< <u> </u>						- F
Total 6 devices   1 device selected						
		Close	e			
		_	_			

Figure: Clear Cached Access Credentials

# 3.2.5 Remote Login

Depending on the device platform, operating system and configuration, management protocols, such as SNMP, WBEM, or WMI are not available. In such a case, JDisc Discovery can use telnet and/or SSH to collect hardware, software and configuration information. Once connected, JDisc Discovery executes system commands to collect hardware, software and configuration information not available through other management protocols. The commands that are executed depend on the device's platform and operating system. When JDisc Discovery discovers Linux computers, root privileges are requires to read model, serial number and manufacturer information from the computer's BIOS. JDisc Discovery can call *su*, *sudo* or *.do* to get root privileges. The discovery settings allow choosing su, sudo or .do as preferred method. When sudo or .do fail, JDisc Discovery tries su as fallback.

Remote login is enabled by default for Windows and Unix.

Remember: Remote login is enabled by default.

Be careful when using SSH based remote login in conjunction with default accounts. Trying too many default accounts might cause security alerts.

Remote login for Windows helps to avoid WMI or remote registry access problems by tunneling the two protocols through the remote login agent.

In addition to solving access problems, tunneling WMI and remote registry can improve the discovery speed of Windows computers that are connected to slow or wide area networks.

# 3.3 Device Grouping

Device grouping is a concept that permits grouping devices by geography, organizational structure or other criteria. Group conditions can be created using any of the device attributes below:

- Membership to an IP4 network
- IP address within an IP4 address range
- Membership to a Windows network neighborhood object
- Membership to a directory object
- Device attributes such as model or manufacturer

While the discovery is running, JDisc Discovery assigns devices to group based on the group conditions. This eliminates the need to manually assigning devices to groups, which would be nearly impossible for large number of devices.

Devices are automatically assigned to groups during the discovery.

When the group hierarchy or group conditions change, devices are only reassigned to groups during the next discovery cycle. Alternatively, you might trigger manual reassignment of devices to groups by opening a device report (for instance *All Devices*), select the devices to reassign, open the context menu and select *Manage* » *Synchronize Group Assignment...* 

II Devices							
+ → &   A   [							
er:							
	24						
Case sensitive f	hiter						
*							
ame	IP Address	Manufacturer	Model	Type	OS Version	Patch Level	FW Ve
rtConvor-1	12 216 106 21	Mova	NPort	Bort Server			2.2
inter-1	12 216 104 75	Konica Minolta	Magicolor 2350	Printer			5.5
nter-2	12,216,104,75	Levmark	T640	Printer			IS ST
nter-3	12 251 240 04	Unitett-Packard	Laser let 4000 Series	Printer	G 08 40		G 07 1
inter-4	12.2 Properties	mark	F240n	Printer			BR.O.F
nter-6	12.2	lett-Packard	Color Laser let CP4005	Printer	V.33.41		none
intServer-1	12.2 Discover	Jott Dackard	JotDiract	Print Server	3.51		H 07
ntServer-2	12.2 Manage	Acceleration Ac	counts	Print Server	F.08.20		F.08.0
oCurve1	192.			Switch	H.08.72		H.08.0
ickServer-1	12.2 Compare	Change SSF	H public/private Key	Server (Rack)	Windows Server 2003	Service Pack 2	-[APE1
ckServer-2	12.2 Custom Attribu	tes 🛛 🔑 🛛 Change SNI	MP Credentials	Server (Rack)	HP-UX B. 11. 23U		04.10
ickServer-3	12.2	. C. Sunchronting	Group Arrignment	Server (Rack)	HP-UX B. 11. 23U		03.01
ckServer-4	12.2 Connect with	- Syncinol de	coroup Assignmental	Server (Rack)	HP-UX B.11.23U		03.01
ickServer-5	12.2 Troubleshoot	ett-Packard	rx2660	Server (Rack)	HP-UX B.11.23U		03.01
laris11-test	192.			VMware Instance	SunOS 5.11	11.1	DevCo
larisZone-1	12.2 👗 Delete Devices	•		Solaris Zone			
mmit1	192. 🗐 Crasta Sunnart	ZID eme Networks	Summit 48i	Routing Switch	7.2.0	Build 33	

Figure: Synchronize Group Assignments

Save time and manually reassign devices after a group configuration change.

The root group is always associated with all devices, all networks, all Windows network neighborhood objects and all directory objects. The root group's conditions are immutable.

## 3.3.1 Define Your Own Groups

Open *Discovery* » *Settings* and select *Scope*. The device group hierarchy is located in the left navigation panel. Groups can be freely organized in a hierarchy. Select a parent group, open the context menu using a right mouse click and choose a group type.

General	Scope	Directory	Data Collection	Discovery Jobs	Protocols	Тор
	mosov					
Co		Create ne	w network/rang	je group		v
		Create ne	w Windows net	work neighborh	nood group	
		Create ne	ew directory gro	up		
		Create ne	ew group			
		Delete se	lected groups			
				192, 168, 1	78.0	

Figure: Create New Group

JDisc Discovery offers four types of groups:

• *Network/range groups* assign devices based on IP4 network or IP4 address range conditions. When a device's IP address(es) matches any of the IP4

networks or IP4 ranges in the group condition the device will be assigned to the group.

- *Windows network neighborhood groups* assign devices based on membership to Windows network neighborhood objects. When a device's Windows network neighborhood matches any of the Windows network neighborhood objects in the group condition the device will be assigned to group.
- *Directory groups* assign devices based on membership to a directory object or a hierarchy of directory objects. When a device's directory object matches any of the directory objects in the group condition the device will be assigned to the group.
- *Groups* assign devices based on device attributes. Groups can be created based on the following device attributes:
  - Device model
  - Device manufacturer
  - Device type
  - Device name

The Group Info menu item displays a textual description for the group definitions.

3.3.1.1 Create Network/Range Groups

Corporate and enterprise networks are usually divided into sub-networks. Often subnetworks or a set of sub-networks belong to country, site, building or even floors in a building. Therefore network/range groups are useful to create groups that map networks to geographical locations.

To create a group, select a parent group, open the context menu and select *Create new network/range group*. Enter a group name and description and click *Ok*.

Group name	Berlin				
Description	This group contains all devices that are located in Berlin/Germany.				

Figure: Create new Network/Range Group

The new group will be added to the group hierarchy. Select the new group in the hierarchy to change the group's configuration. Note: The *Network Neighborhood* and *Directory* tabs disappears when selecting the network group.

eral Scope Directory Data	Collection Discovery Jobs Protocols Topology Jobs Filters SSH Keys	
Company L Americas	Properties Device History IPv4 Networks IPv4 Ranges IPv6 Networks SNMP Accounts	
	Filter:	Enable
🖃 🔔 France	Case sensitive filter	Disable
	Network Address Subnet Mask Name Last Discovere	Add
Munich		Browse
		Remove

Figure: Define Networks associated with this Group

The new group is not yet associated to an IP network or IP range. To associate the group with an IP network

- Click *Add* to add a new network
- Click *Browse* to browse and select existing networks
- Click *Import* to import a list of networks from a comma separated file (CSV). The file format is a string containing the network base address and subnet mask separated by a comma and a carriage return.

Enable the networks that should be discovered. JDisc Discovery will assign devices to the group regardless whether the networks in the group's condition are enabled or disabled.

The name field in the network table is editable. You may enter a name for the network for documentation purposes.

Discovery Configuration General Scope Directory Data Coll	lection Discovery Jobs Protocols T	opology Jobs   Filters   SSH Key	/5		
Company Americas Asiapacífic EMEA France Company	Properties Device History I Filter:	Pv4 Networks IPv4 Ranges I	IPv6 Networks SNMP A	ccounts	Enable
Berlin Cologne	Network Address	Subnet Mask 255,255,255,0	Name	Last Discovered	Add
					Remove Import

Figure: A Network Group with one Network

The group 'Berlin' is associated with network ('192.168.178.0 / 255.255.255.0'). Devices this network will be assigned automatically to this group during the next discovery cycle.

Specifying IP address ranges works the same way.

The name field in the network and IP address range table is editable. Use this field to provide meaningful names for IP networks and ranges.

3.3.1.2 Create Windows Network Neighborhood Groups

Using Windows network neighborhood groups is beneficial when Windows domains reflect the organizational structure such as a single domain per organization.

Select a parent group, open the context menu and select *Create new Windows network neighborhood group*. Enter a group description in the new group dialog and click *Ok*.

Group name	Development Team Berlin
Description	All devices belonging to the Windows domain BERLINDEV

Figure: Create new Network Neighborhood Group

The new Windows network neighborhood group will be added to the group hierarchy. Select the new group in the hierarchy to change the group's configuration. Note: All other tabs disappear but only the *Network Neighborhood* tab is visible.

neral Scope Directory Data Collection Dis	covery Jobs Protocols Topo	ology Jobs Filters SSH Keys		
S Company	Properties Device Histor	y Windows Network Neighbor	hood	
Asiapacífic	Filter:			Enable
France	Case sensitive	Case sensitive filter		Disable
🖨 🚽 Berlin	Name	Account	Last Discovered	Update
Cologne				Add
				Browse
				Remove
				Import

Figure: The Network Neighborhood Group

The new Windows network neighborhood group is not yet associated with any Windows network neighborhood object. To associate the new group with a Windows network neighborhood object

- Click *Add* to add a new Windows network neighborhood object that might not yet exist in JDisc Discovery's database.
- Click *Browse* to browse and select existing Windows network neighborhood objects.
- Click *Import* to import Windows network neighborhood objects from a comma separated (CSV) file.
- Click *Change* to enter login credentials for selected network neighborhood objects.

eral Scope Directory Data Collection	Discovery Jobs Protocols Topolo	gy Jobs Filters SSH Keys			
Company Americas Asiapacific	Properties Device Histor	y Windows Network Neighbor	rhood		
EMEA	Filter:			Enable	
🖻 🔔 Germany	Case sensitive	Case sensitive filter			
Berlin	Name	Account	Last Discovered	Update	
	BERLINDEV	BERLINDEV (ADMINI	ISTRATOR	Add	
				Browse	
				Remove	

Figure: Group with Associated Windows Neighborhood Objects

Enable the Windows network neighborhood objects for discovery. JDisc Discovery will assign devices to this group regardless whether the Windows network neighborhood objects in the group's condition are enabled or disabled.

It is recommended to enter administrative login credentials for Windows domains. This enables JDisc Discovery to collect detailed hardware, software and configuration information from Windows computers that belong to Windows domains.

Enter administrative login credentials for Windows domains to improve the discovery result.

#### 3.3.1.3 Create Directory Group

Using directory groups is helpful for creating groups that map the organizational or geographical structure of a corporation or an enterprise.

Select a parent group, open the context menu and select *Create new directory* 

group. Enter a group description and click Ok.



Figure: Create new Directory Group

The new directory group will be added to the group hierarchy. Select the new group in the hierarchy to change the group's configuration. Note: All other tabs disappear but only the Directory tab is visible.

Expand the directory hierarchy, select directory objects and click *Toggle* to include or exclude selected directory objects in the group's configuration.

Click *Change Account* to enter administrative login credentials for the selected directory objects. JDisc Discovery will use the login credentials to discover member computers of the selected directory objects or any subordinate directory objects. The login credentials enable JDisc Discovery to collect detailed hardware, software and configuration information from Windows computers that belong to a directory.



Figure: Directory Group with associated Directory Objects

Enter administrative login credentials for directory objects to improve the discovery result.

3.3.1.4 Create A Group Based On Device Attributes

Select a parent group, open the context menu and select *Create new group*. Enter a group description and click *Ok*.

Group name	My Dell Servers					
Description	This group contains all Dell Servers!					

Figure: Create a new Group

The new group will be added to the group hierarchy. Select the new group in the group tree to change its configuration. Select the *Specification* tab to define the group membership rules.

eneral Scope Directory Data Collection Disco	very Jobs Protocols Topology Jobs Filters SSH Keys	
Company Company Asiapacific EVIEA France Genany Ge	Properties         Device History         Specification           This group has no conditions!         Click the Change button to add new conditions!	Change

Fig: Group Specification

Initially the group specification is empty and thus no devices will be assigned to the group. Click *Change* to add group conditions or modify the group specification. On the *Group Specification* dialog select attributes from the navigation tree and build conditions.

Group conditions can use any of the attributes below:

• Device name

- Device model
- Device manufacturer
- Device type
- Operating system family
- Operating system version
- Operating system patch level

- Device Attributes	Manufacturer =
Model <mark>Manufacturer</mark> Type	Add Remove
⊡Software	Conditions (Connected with OR)
	Total 0 conditions   0 conditions selected

Figure: Change Group Specification

Select an attribute and add a new condition by selecting the operator (in this case '=') and a value (in this case 'Dell'). Click *Add* to add the condition to the group specification.

Depending on the attribute type, JDisc Discovery offers the following operators:

- equals
- not equals
- contains
- contains (case insensitive)
- greater than
- greater than or equal
- less than

- less than or equal
- between
- matches regular expression
- matches wildcard expression

Refer to chapter 3.1 for more information about pattern matching.

The *Specification* tab shows a summary of the group definition.

General Scope Directory Data Collection Discovery Jobs Protocols Topology Jobs Filters SSH Keys
Image: The ready and collection   Decovery dots   Protocols   Tappogy dots   Protocols   Protoc
Ok Cancel

Figure: Group definition summary

### 3.3.1.5 Groups And Default Accounts

Corporate and enterprise networks typically run large numbers of SNMP enabled devices and Unix computers. Often times, SNMP enabled devices and UNIX computers share the same local access and login credentials but are not member of a Windows domain or a directory (for technical or organizational reasons) that could simplify the credentials configuration.

This is why JDisc Discovery's default access and login credentials feature to reduce the

configuration effort or SNMP enabled devices and UNIX computers. JDisc Discovery attempts to authenticate configured default SNMP communities and UNIX login credentials up until one of them succeeds, associates and stores the credentials with the device in the database. The group hierarchy and order of default credentials within a group determine the order of default credentials JDisc Discovery's attempts to authenticate. Default credentials in subordinate groups are tried first and only if these fail, JDisc Discovery attempts to authenticate default credentials of superordinate groups up until it reaches the root group. JDisc Discovery's installation program adds the 'public' default SNMP community to the root group.

JDisc Discovery attempts to authenticate credentials in subordinate groups first. If credentials of subordinate groups fail, JDisc Discovery will attempt to authenticate credentials of superordinate group until the root group is reached or authentication succeeds.

Having only one global list of default credentials might cause problems in corporate and enterprise networks because JDisc Discovery will attempt to authenticate all default credentials in the worst case (if all fail) and might trigger security alerts (especially, when using SSH) and intrusion detection systems. Because of that it is important to keep the number of default credentials to a minimum. JDisc Discovery allows configuring default SNMP communities and login credentials for each group. Group based default credentials offer better granularity than a global definition of default credentials and thus reduce the risk of security alerts.

Keep default credentials to a minimum to avoid triggering security alerts (especially when using SSH) and intrusion detection systems.

Open the *Discovery Settings* dialog, select a network group and click select the *SNMP* tab.

To add default SNMP communities to a group, click *Add*. *Remove* will delete selected default SNMP communities. Click *Move Up* and *Move Down* to change the order of selected default SNMP communities.

Use the buttons in the *SNMPv3 Accounts* panel to create, delete or reorder default SNMPv3 accounts.

Discovery Configuration	
General Scope Directory Data Collectio	n Discovery Johs Protocols Topology Johs Filters SSH Keys
Americas	Properties Device History IPv4 Networks IPv4 Ranges IPv6 Networks SNMP Accounts
Asiapacific	SNMPv1/v2c Communities
France	Community
in the section of th	Remove
	Move up
	Move down
	Total 0 SNMP communities   0 SNMP communities selected
	SNMPv3 Accounts
	User name Password Auth, protocol Privacy password Priv, protocol Add
	Remove
	Modify
	Move up
	Move down
	۲
	Total 0 SNMPv3 accounts   0 SNMPv3 accounts selected
	Ok Cancel

Figure: Default SNMP Communities and SNMPv3 Accounts

Select the *Accounts* tab to create default accounts for UNIX platforms. You can help JDisc Discovery's discovery by specifying the account type (root or non-root account).

Choose default SSH public/private keys after importing keys into the JDisc Discovery application. Refer to section 5.9 on how to import SSH keys.

Discovery Configuration	X					
Ceneral SCOPE Directory Data Collection	n Diecovery John Protocole Tanology John Eiltern SCH Kave					
deneral scope Directory Data Collector						
Company	Properties Device History IPv4 Networks IPv4 Ranges IPv6 Networks SNMP Accounts					
EMEA	✓ Use default accounts from all platforms for unknown devices					
France						
international i	Clients & Servers Interconnect Devices					
	HP-UX Sun Solaris IBM AIX Linux/VMware/XenServer/Oracle VM Mac OS X					
	HP-UX Accounts					
	User name Password Type Add					
	Remove					
	Move up					
	Move down					
	Total 0 Accounts   0 Accounts selected					
	- HPU IV SSH Duhliz Ibriusta Vaur					
	Key name User name Key type Passphrase Type Adu Remove					
	Move up					
	Move down					
	< <u> </u>					
	Total 0 SSH public/private keys   0 SSH public/private keys selected					
	Ok Cancel					

Figure: Manage default Accounts for UNIX Platforms

### 3.3.2 Groups And Reports

Groups can do more than structuring devices by organizational or geographical criteria and simplifying the discovery configuration. You can use groups to restrict JDisc Discovery's reports and graphical views to devices that are member of a group or a hierarchy of groups.

In a report or graphical view click the grouping icon  $\frac{1}{2}$  to open the group tree. The group icon might be disabled in reports where grouping is not applicable.

All Devices					
፨   ← → 🤣   🖨   🛐	🗋   🔯   🕕   🚠				
Include subgroups	Filter:				
Company	Case sensitive filter				
EMEA					
- L France	Name	IP Address	Manufacturer	Model	Тур
Germany	HPE49E84	192.168.178.43	Hewlett-Packard	OfficeJet J6400 Series	Mult 🔺
Berlin	NPI3DD22D.fritz.box	192.168.178.38	Hewlett-Packard	Laser Jet CM1415fnw	Mult
Ciont Notwork	ProCurve1	192.168.178.18	Hewlett-Packard	ProCurve 2650	Swit
	teetee-pc.fritz.box	192.168.178.20	Hewlett-Packard	m8180.de	Desl
	xenserver	192.168.178.55	Hewlett-Packard	Compag dx2450	Mini
	summit1	192.168.178.13	Extreme Networks	Summit 48i	Rou
	192.168.178.7	192.168.178.7	Dell	PowerEdge T110 II	Serv
	192.168.178.73	192.168.178.73	Dell	PowerEdge T110 II	Serv
	ttrenz-PC2.fritz.box	192.168.178.75	Dell	Studio Hybrid 140g	Desl
	cisco-sw1	192.168.178.4	Cisco Systems	C2900XL	Swit
	firewalli.home.net	192.168.178.17	Cisco Systems	PIX 501	Fire
	tom-laptop3.fritz.box	192.168.178.81	Apple	MacBookPro 10, 1	Lapt
	3comtest	192.168.178.16	3COM	SuperStack 3 Switch 4300	Swit
	0005CD2D0B06.fritz.box	192.168.178.57			Unid
	192.168.178.118	192.168.178.118			Virtu

#### Figure: Report with Grouping Hierarchy

Select groups in the group hierarchy to display devices that are associated to the selected groups.

# 3.4 Scheduled Discovery Jobs

JDisc Discovery can schedule discovery jobs to start automatically. A discovery job is comprised of a set of groups define the discovery scope. In its simplest form a discovery job can be comprised of just the root group. To accommodate the discovery of more complex networks that might span across different continents and timezones, a discovery job can be comprised of a set of groups with each group defining different discovery scopes.

Discovery jobs can be scheduled using one of these schedule types:

- Not scheduled: Discovery job must be started manually
- Run once: Run once at a particular date and time
- *Run daily*: Run daily at a particular time
- *Run weekly*: Run weekly at a particular day and time
- *Run monthly*: Run monthly at a particular day of the month and time
- *Recurring*: Run recurring within a configurable interval

In it's default configuration, JDisc Discovery comes with a built-in discovery job called 'Discover all', which includes all networks, IP4 address ranges, Windows network neighborhood objects and directory objects that are enabled for discovery including all subgroups.

Discovery Configuration		×
General Scope Directory Data Collection Discovery Job	Protocols Topology Jobs Filters SSH Keys	
Discovery Name Properties	roups. Directory Schedule	
Discover all Name	Discover all	
Description	This is a built-in configuration to discover all enabled items.	
	Ok Cancel	

Figure: The 'Discover all' Discovery Job

The concept of discovery jobs is powerful and flexible. While it is easy and simple to use for small company networks, discovery jobs also fits corporate and enterprise networks with locations and sites spread across the world.

For example: A corporation would like to run JDisc Discovery to create a world wide inventory. The discovery server running JDisc Discovery is located in a data center in Europe. JDisc Discovery can only discover devices that are powered on and connected to the network. Consequently, devices that are turned off or are disconnected from the network cannot be discovered, such as the ever increasing number notebooks and PDAs. Because of that, it is essential to discover mobile devices during office hours. The JDisc Discovery administrator has already created groups for countries and sites. Now the administrator would like to schedule a discovery job for the Atlanta site. The time leap between the discovery server and the Atlanta site is 7 hours. Therefore (to discover devices during office hours in Atlanta) the discovery should start at 3pm (discovery server local time).

To create a new discovery job, open the context menu in the *Discovery Jobs* panel and choose *Add new discovery job*. Enter a meaningful discovery job name and description in the *New Discovery* dialog and click *Ok*.



Figure: Create a new Discovery Job

Select the new discovery job from the *Discovery Jobs* panel:

- Enter a meaningful name and description in the *Properties* tab.
- Select groups to associate with the discovery job in the *Groups* tab.
- Select the *Directory* tab to configure directory synchronization options. JDisc Discovery can synchronize directory hierarchies and networks from directories when a discovery job starts.
- Select the *Schedule* tab to schedule the discovery job.

Choose one of the options below:

- Not scheduled: Discoveries are not scheduled. Start a discovery manually from Discovery » Control » Start Discovery.
- *Run once*: Run the discovery job once at a particular time and date.
- *Run daily*: Run the discovery job daily at a particular time.
- *Run weekly*: Run the discovery job weekly at a particular day and time.
- *Run monthly*: Run the discovery job monthly at a particular day of the month and time.
- *Recurring*: Run the discovery job regularly.

Define blackout periods for recurring or daily schedules. A blackout period defines when not to run a discovery. Define blackout periods based on

- one or more daily intervals
- one or more days of the week
- one or more days of the month

# 3.5 Control The Discovery

JDisc Discovery's discovery can be controlled from the *Discovery* » *Control* menu or by clicking the icons from the tool bar. The discovery process can be either *running, idle, paused,* or *disabled*.

File	Disc	overy Devices Software	Ν	etwo	orking Us	er Documents	
۲	Þ	Configuration Wizard					
	Þ	Configuration	_				
	*	Control	Þ	lacksquare	Start Dis	rovery	
	Þ	Custom Data Collectors	,	•	Stop Dis Pause Di	Lor covery scovery	
	Þ	Discover Device		•	Resume	Discovery	
	J <sup>es</sup>	Import Devices	_	۲	Synchro	nize Directories	
			-	$\odot$	Synchro	nize Networks	

Figure: Control Discovery Menu

#### 3.5.1 Start Discovery

Choose *Start Discovery* or click the start icon 🕑 to start a discovery job. The discovery job starts immediately when only one discovery job is configured. JDisc Discovery' displays the *Start Discovery* dialog if more than one discovery job is configured. From the *Start Discovery* dialog select the discovery job that you want to start.

Start Discovery
Select the discovery that you would like to start
Discovery Name
Discover all Discover San Francisco Site
Total 2 discovery jobs   0 discovery jobs selected
Ok Cancel

#### 3.5.2 Stop Discovery

Choose *Stop Discovery* or click the stop discovery icon 
to stop a discovery job. JDisc Discovery prompts which discovery job to stop if more than one discovery job is running. Otherwise, if only one discovery job is running the discovery stops immediately.

#### 3.5.3 Pause Discovery

Choose *Pause Discovery or click* the pause icon (10) to pause all running discovery jobs.

Discovery jobs cannot be paused individually. JDisc Discovery can only pause all running discovery jobs at once!

#### 3.5.4 Resume Discovery

Choose *Resume Discovery* or click the start discovery icon () to resume paused discovery jobs.

### 3.5.5 Synchronize Directory

Choose *Synchronize Directory* to synchronize directory information in JDisc Discovery's database with configured directories.

Synchronizing directory information requires configuration of a DNS Domain Controller and login credentials. Refer to section 5.3.1 for how to configure directory DNS Domain Controllers.

### 3.5.6 Synchronize Networks

Choose *Synchronize Networks* to synchronize IP4 networks in JDisc Discovery's database with IP4 networks from configured directories. Refer to section 5.3.1 for how to configure directory DNS Domain Controllers.

Synchronizing IP4 networks from a directory requires configuration of a DNS Domain Controller and login credentials. Refer to section 5.3.1 for how to configure directory DNS Domain Controllers.

# 3.6 The Status Panels

JDisc Discovery's main window displays status information.

The status panel is divided into these sub-tabs:

- The *Devices* tab displays statistics about devices and IP addresses already discovered, pending IP addresses and displays devices that are currently discovered.
- The *Ping* tab displays what IP4 networks and IP4 ranges are currently pinged and the total number of IP addresses processed and pending for discovery.
- The *Windows Network Neighborhood* tab displays the Windows network neighborhood discovery current activity and the total number of Windows network neighborhood objects processed and pending for discovery.
- The *Directory* tab is divided into two panels.
  - The *Synchronization* panel displays directory and network synchronization status.
  - The Queue panel displays displays the directory discovery current activity and the total number of directory objects processed and pending for discovery.
- The *Topology Jobs* tab appears only when the 'Networking Add-On' is installed on top of JDisc Discovery. This tab lists all running network topology discovery jobs.
- The *Device History* tab appears only when the 'History Add-On' is installed on top of JDisc Discovery. This tab lists all currently running device history tasks.
- The *Data Quality* tab displays statistics about the discovered data quality. Tips on how to improve the data quality help to get the most out of JDisc Discovery.
- The *Discovery Jobs* tab lists all scheduled discovery jobs with their status.
- The *Database* tab shows statistics about the database size and the number of entries within the tables.

Jusc Discovery [Enterprise Edition] - JAMES SMITH connected to localnost	
File Discovery Devices Software Networking User Documents Troubleshooting Administration Help	
Discovery Status	
_ Ctable	
Discovery is idle	Click for instructions on how to improve the data quality!
Devices Ping Network Neighborhood Directory Discovery Jobs Data Quality Database	
Concurrent device discoveries 0 of 10	
Average duration	
Manually triggered 0 pending	
Devices in database 18	
Device Duration Last message	

Figure: The Main Window with Status Information

Icons in the Status area display the discovery's current state



The discovery is idle.



The discovery is running.



The discovery is paused.

JDisc Discovery is stopped. Only administrative tasks such as archiving and restoring the database can be executed while JDisc Discovery is stopped.

### 3.6.1 Devices Status

The *Devices* status tab displays aggregated devices statistics spanning across all running discovery jobs. In addition to that the table view displays progress for each devices currently discovered.

• *Concurrent device discoveries* displays the number of devices currently discovered concurrently. The maximum number of concurrent device discoveries

can be configured in JDisc Discovery's discovery settings.

- Average duration displays the average device discovery duration based on the average discovery duration of the last 200 devices and also an estimated device discovery rate forecast.
- *Discovery jobs* displays the total number of IP addresses pending for discovery from manually or automatically scheduled discovery jobs.
- *Manually triggered* displays the number of IP addresses that have been manually triggered for discovery.
- *Devices in database* displays the total number of devices in JDisc Discovery's database.

The table view displays device IP address, current discovery duration and discoveries activity for each device.

Devices Ping Network Neigh	borhood Directory Discov	ery Jobs Database
Concurrent device discoveries Average duration Discovery jobs Manually triggered Devices in database	8 of 10 Average discovery time: 0 8 of 8 pending 0 pending 0	10:00:19 (1849 devices per hour)
Device	Duration	Last message
192.168.178.1	00:00:04	Waiting for SMB anonymous protocol check
192.168.178.69	00:00:04	Waiting for SMB authenticated protocol check
192.168.178.75	00:00:04	Waiting for SNMP protocol check
192.168.178.78	00:00:04	Waiting for SMB anonymous protocol check
192.168.178.23	00:00:04	Waiting for SMB anonymous protocol check
192.168.178.2	00:00:04	Testing SMB anonymous
192.168.178.76	00:00:04	Waiting for SMB anonymous protocol check
192.168.178.90	00:00:04	Waiting for SMB anonymous protocol check

Figure: The Device Status Tab

The *Discovery job* and *Manually triggered* counters refer to IP addresses only. Device can have multiple IP addresses assigned and. therefore the number of IP addresses discovered might become higher than the number of devices in the database.

# 3.6.2 Ping

The *Ping* tab displays progress when pinging IP4 sub-networks and address ranges.

*Status* displays current activity. The upper table view displays overall ping progress separately for scheduled and manually triggered discovery jobs.

- The number of IP networks to ping
- The number of IP address ranges to ping
- The total number of IP addresses pending to ping

Status Pinging 127 IP4 addr	esses in chunks of 64 addresses			
em Discovery Job			Manually Triggered	
Networks	etworks 1 of 1 to process Pranges 0 of 0 to process		0 to process	
IP ranges			0 to process	
Addresses to ping	127 of 255 to proc	tess	0 to process	
Title	IP Range	Progress		
Network 192.168.178.0/255.2	55.255.0 192.168.178.0 - 192.168.178.255			

Figure: Ping Status during Discovery of a Network

The lower table view displays processing of IP networks and ranges. A progress bar indicates the progress when pinging an IP network or range.

JDisc Discovery can ping up to 10 IP networks or ranges concurrently.

## 3.6.3 Windows Network Neighborhood Status

The *Windows Network Neighborhood* tab displays Windows network neighborhood discovery progress.

- Status displays current activity.
- *Current object* displays the Windows network neighborhood object being processed.
- *Pending objects* displays the total number of Windows network neighborhood objects pending for discovery.
- *Processed objects* displays the total number of Windows network neighborhood objects discovered.

Devices	Ping	Network Neig	hborhood	Directory	Discovery Jobs	Database
Status			Idle			
Current	t <mark>o</mark> bject					
Pending Process	g objects sed obje	s 0 cts 0				

Figure: The Windows Network Neighborhood Status

### 3.6.4 Directory Status

The *Directory* tab displays directory discovery and directory synchronization status.

The *Synchronization* panel displays aggregated directory object and network synchronization statistics.

- *Added* displays the total number of directory objects and networks added to the database.
- *Removed* displays the total number of directory objects and networks removed from the database.
- *Synchronized* displays the total number of directory objects and networks synchronized with the database.
- *Status* displays current activity of the directory object and network synchronization.

The Queue panel displays directory objects discovery status.

- *Status* indicates the directory discovery's operational state, such as Running, *Idle or Paused.*
- Message displays current activity.
- Processed displays the total number of directory objects discovered.
- Pending displays the total number of directory objects to be discovered.

	Added	Removed	Synchronized	Status	Message
Directory	0		0	0 Idle	
letwork	0		0	0 Idle	
eue					
eue Status	Idle				
eue Status Message	Idle				
eue Status Message Processed	Idle 0				

#### Figure: Directory Status

#### 3.6.5 Status Of Discovery Jobs

The Discovery Jobs tab displays the status of discovery jobs. The table view displays:

- Discovery Job displays the discovery job name.
- Status displays the current status.
- *Last Started* displays when the discovery was last started. This column is empty when the discovery job was never been started.
- *Last Finished* displays when the discovery job finished. This column is empty when the discovery job never completed.
- *Duration* displays the discovery job duration. This column is empty when the discovery job never completed.
- *Next Schedule* displays the date and time for the next scheduled discovery. This column is empty when the discovery job was not scheduled.

	Status	Last Started	Last Finished	Duration	Next Schedule
Discover all	Stopped	Oct 6, 2009 5:51:32 PM	Oct 6, 2009 6:03:43 PM	00:12:11	

Figure: Discovery Jobs Status

## 3.6.6 Data Quality

The *Data Quality* tab displays data quality information on how well devices have been discovered.

The total data quality of all operating system families		
Total	33%	How to improve.
/ Operating System Family		
The data quality by operating system family		
Windows	前後	How to improve.
linux	0%	How to improve.
/Mware ESX Server	0%	How to improve.
Orade VM Server	0%	How to improve.
MAC OS X	0%	How to improve.
Sun Solaris	0%	How to improve.
HP-UX	0%	How to improve.
IBM AIX	0%	How to improve.

#### Figure: Data Quality tab

The 'Total' panel displays the data quality of all devices and operating systems whereas the 'By Operating System Family' panel displays the data quality of each operating system family individually. Click the *How to improve* link next to the quality meter to display diagnostic information on how to further improve the data quality.

### 3.6.7 Database Status

The *Database* panel displays the database size on the disk, the number of rows in each table and the size of the table on the disk (including required space for indexes)

Devices Ping Network Neighborhoo	d Directory Discovery	Jobs Database	
Database size 230.81 MB			
Table Name	Row Count	Table Size	
account	1311	3.34 MB	
application	11632	13.86 MB	
applicationinstance	23	136 KB	
applicationinstancearrayattribute	0	48 KB	
applicationinstancearrayattributec	0	16 KB	
applicationinstancearrayattributev	0	56 KB	
applicationinstanceattribute	0	128 KB	
applicationoperatingsystemrelation	19763	23.01 MB	
bios	87	400 KB	
connectortypelookup	134	32 KB	
customattribute	10	120 KB	
customattributecollectionconfig	2	56 KB	
customattributedatacollectionconfig	2	40 KB	
customattributeenum	0	8 KB	

Figure: Database status

This chapter describes common discovery scenarios and explains how to configure JDisc Discovery to best discover Windows and Unix computers. Furthermore, it also provides guidance on how to improve the discovery of other networked devices such as printers, switches, and routers.

# 4.1 Active Directory Environments

JDisc Discovery supports Active Directory environments in many ways, such as

- Automatically detect directories and DNS domain controllers on the network.
- Synchronize directory objects and IP networks with JDisc Discovery's database.
- Automatically assign member computers to directory objects.
- Discover member computers of directories that are associated with DNS domains, organizational units or containers.
- Simplify the configuration of access credentials for directory member computers.

### 4.1.1 Directories And DNS Domain Controllers

JDisc Discovery uses the SMB (Server Message Block) protocol to detect directories, Global Catalog (GC) servers DNS domain controllers (DC) on the network. Often times (depending on the security settings of target computers) this does not require entering credentials. The automatic detection of directories, Global Catalog (GC) servers and DNS domain controllers (DC) simplifies the configuration of Active Directory environments and also reveals unknown directories on the network.

You can view directories from *Networking* » *Directories*. Directories that have not yet been synchronized only have DNS domain objects. Organizational units and containers will be added underneath DNS domain objects when a directory is synchronized.

#### 4.1.2 Manually Discover DNS Domain Controllers

You can configure Gloabal Catalog (GC) servers and/or DNS domain controllers (DC) of a directory before running your first discovery job. When you do not know your Global Catalog (GC) servers or DNS domain controller (DC) host names, follow the instructions below:

• Make sure the 'Discover DNS domain controllers' option is checked on the General tab of the Discovery Configuration dialog.

- From the *Discovery* » *Discover Device* menu open the *Discover Device* dialog and enter the directory's DNS domain name.
- Wait until the discovery returns to idle state.
- Open the *Discovery Configuration dialog from Discovery* » *Configuration* and choose the *Directory* tab.
- If JDisc Discovery has discovered at least one DNS Domain Controller of the specified DNS domain name:
  - The DNS domain name is displayed in the DNS Domains panel
  - And the DNS Domain Controller is displayed in the DNS *Domain Controller* panel.
  - See section 5.3.1 for how to configure login credentials for DNS Domain Controllers.

## 4.1.3 Synchronization Of Directory Objects And IP Networks

When JDisc Discovery has detected a directory and at least one Global Catalog (GC) server or DNS domain controller (DC), you can enter login credentials (non-privileged) to access the DNS domain controller (DC) or Global Catalog (GC) servers (see section 5.3.1 for details).

JDisc Discovery uses these login credentials to run LDAP queries on the Global Catalog (GC) and DNS domain controllers (DC). Typically DNS domain controllers (DC) also run the Global Catalog (GC) service. This is why DNS domain controllers (DC) and Global Catalog (GC) servers are often user interchangeable.

When JDisc Discovery synchronizes directory objects and IP networks, it runs a series of LDAP queries against the Global Catalog (DC) service.

To synchronize directories, choose *Settings* » *Sync Directory*.

Synchronizing a directory requires at least one DNS domain controller and login credentials to run LDAP queries.

### 4.1.4 Relating Member Computers To Directory Objects

JDisc Discovery determines the directory membership of discovered computers / devices by using their:

- fully qualified host names (FQDNs)
- computer name including the NetBIOS domain name
- domain security identifier (SID)

When successful, JDisc Discovery relates directory member computers with their respective directory objects (DNS domain | organizational unit | container). JDisc Discovery uses the administrative logon credentials that are configured for the directory

object and sub-objects to log-on to directory member computers and collect hardware, software and configuration information. Relating member computers to directory objects is important to make directory groups work (see section 3.3.1.3 for details). Section 6.3.1 shows a device associated to a directory.

### 4.1.5 Discover Directory Member Computers

Alike IP networks, IP ranges and network neighborhoods/domains, directory objects can be enabled for discovery in many ways. The table below explains the different discovery modes that are applicable to directory objects.

- Discover all computers of the selected directory object.<sup>4</sup>
- Discover all computers of the selected directory object and all sub-directory objects.
- Discover recently logged-on computers of the selected directory object.<sup>5</sup>
- Discover recently logged-on computers of the selected directory object and all sub-directories.

Figure: Directory Object Discovery Modes

When the discovery is running, JDisc Discovery queries the configured Active Directory Global Catalog (GC) service or DNS domain controllers (DC) for member computers of enabled directory objects. See also section 5.2.1.6 for how to enable directory objects for discovery and section 6.1.1.1 for how to report member computers.

# 4.1.6 Simplifying Configuration Of Credentials

Login credentials can be configured for each directory object in a directory hierarchy. This enables using different login credentials for discovery of member computers, which is very important to accommodate to corporate and enterprise networks, which typically do not have single administrator credential for the entire directory.

JDisc Discovery uses configured login credentials to discover member computers of the enabled directory objects or subordinate directory objects. JDisc Discovery uses login credentials from the the deepest directory objects first. When a login credential fails, JDisc Discovery then tries to use login credentials from higher levels of the directory hierarchy. See section 5.2.1.6 for how to configure login credentials for directory objects.

<sup>4</sup> This requires only access to one Global Catalog (GC) server/service.

<sup>5</sup> This requires preferably access to all DNS Domain Controllers (DC) of the respective DNS domain.

# 4.2 Discover Windows Computers

Windows computers are very common target devices for discoveries. JDisc Discovery discovers Windows computers using protocols and technologies, such as SMB, NetBIOS, Remote registry, WMI (Windows Management Instrumentation), remote login, SNMP or vendor specific agents.

Protocols including SMB, NetBIOS and SNMP (without vendor specific agent extensions<sup>6</sup>) return only limited, but important information, such as operating system version.

Other protocols and technologies, such as WMI and remote login collect detailed hardware, software and configuration information such as hardware serial number, model, manufacturer, or installed applications.

Starting with Windows 2000, Microsoft has included WMI in the Windows operating systems. Although a WMI implementation for Windows NT 4.0 exists, it is not installed by default. WMI is using DCOM (Distributed Component Object Model) technology (which is based on DCE/RPC) for WMI client to server communication. Using WMI requires administrative credentials.

JDisc Discovery discovers most hardware information using WMI. WMI requires administrative credentials to collect hardware, software and configuration information.

Therefore:

No administrative WMI credentials, no detailed hardware information from Windows computers!

Enable remote login for Windows in cases where a firewall blocks WMI and remote registry traffic. JDisc Discovery tunnels WMI and remote registry access through its remote login agent.

JDisc Discovery allows configuring administrative credentials for

- Directory objects including DNS domains, organizational units or containers
- Windows domains
- Individual computers

### 4.2.1 Enter Credentials For Directory Objects

When you run Microsoft Active Directory on your corporate network, you can configure

<sup>6</sup> Most manufacturers (including Hewlett-Packard, Dell and IBM) enhance SNMP agents with proprietary vendor specific agents providing detailed hardware information. The standard Windows SNMP agent does not expose detailed hardware and software information.

administrative credentials for Directory objects that can contain computers, such as DNS domains, organizational units and containers.

#### Figure: Change Directory Object Credentials

JDisc Discovery logs on to computers that are member of a directory using credentials configured for directory objects. When JDisc Discovery logs on to a computer, it will use credentials from directory objects on the lowest applicable hierarchy level first. If no access credentials are configured or if access credentials fail, JDisc Discovery will begin using access credentials from superior directory objects.

Directory objects allow configuring credentials more granular than Windows domains permit. Refer to section 5.2.1.6 for detailed instructions on how to configure credentials for directory objects.

#### 4.2.2 Enter Credentials For Windows Network Neighborhood Objects

Even though Active Directory is around since the year 2000, corporate networks still run LAN Manager Windows domains. LAN Manager Windows domains have a flat structure in contrast to Active Directory's object hierarchy.

Enter administrative credentials for a Windows network neighborhood object to discover member computers.



Figure: Configure Windows Network Neighborhood Object Credentials

Configuring administrative credentials for Windows domains eliminates the need to configure administrative credentials for each computer. All Windows domain member will be discovered using the administrative credentials configured for the respective Windows network neighborhood object.

Refer to section 5.2.1.5 for how to configure administrative credentials for Windows network neighborhood objects.

### 4.2.3 Enter Windows Default Accounts

When JDisc Discovery tries to get access to a Windows computer, it must use an administrative account. Otherwise, it only gets limited information. The last two chapters explained how to configure administrative accounts for the network neighborhood (Windows Domain) or for organizational units within Microsoft's Active Directory.

However, there are situations, where JDisc Discovery can't determine the network neighborhood name or the OU within the directory. For instance, when firewalls block
the required protocols or when the device does not register within the directory.

For those cases (and only for those cases), JDisc Discovery provides the possibility to add a list of Windows default accounts.

Discovery Configuration					Σ
General Scope Directory Data Collection Discover	y Jobs Protocols Topology J	lobs Filters	SSH Keys		
Company Propertie	s Device History IPv4Netw default accounts from all platf & Servers Interconnect Dev dows IHP-UX Oracle Solaris. Use the default ac possible. Otherwise read more	orks IPv4 Ra orms for unkno ices IBM AIX Lini ounts for Wind , you risk that	nges   IPv6 Netwo wm devices ux/Oracle VM   VM ows only, if the co the accounts get	orks Network Neighborhood Directory ware ESX,VCenter Citrix XenServer Fr nfiguration via the network neighborhood odeed or that intrusion detection systems	SNMP Accounts
L L L L L L L L L L L L L L L L L L L	Vindows Accounts	Password	Type	Comment	Add
	user name administrator administrator		rype root/enable root/enable	Comment Account for workgroup 1 Account for workgroup 2	Remove Change Move up Move down
	Total 2 Accounts   0 Accounts	selected			
		Ok	Cancel		

Figure: Default Windows Accounts

Use the list of Windows default accounts only if the configuration via network neighborhood or organizational units from the directory do not succeed.

### 4.2.4 Enter Per Device Credentials

Standalone computers that are not member of a directory or a Windows domain require configuration of individual administrative credentials.

Per device administrative credentials is the only solution for directory and Windows domain member computers that do not trust the directory's or Windows domains global Administrators group because it has been removed from the computer's local Administrators group.

Open the context menu in any device report and choose Manage » Change Accounts

to configure credentials of selected devices.

	8 6 9				
Filter:					
Case sensitive filte	Modify Accounts			×=]	
Name	User Account			ype	OS Version
BladeServer-1				erver (Blade)	Windows Server 2003 Star
BladeServer-10				erver (Blade)	
BladeServer-11	User name			erver (Blade)	Windows Server 2003
BladeServer-12	Password			erver (Blade)	-
BladeServer-13				erver (Blade)	Windows Server 2003
BladeServer-14				erver (Blade)	
BladeServer-15				erver (Blade)	
BladeServer-16	Admin/Root Acc	ount		erver (Blade)	
BladeServer-17				erver (Blade)	
BladeServer-2	User name	administrator		erver (Blade)	Windows Server 2003 Ente
BladeServer-3	User name	administrator		erver (Blade)	Windows Server 2008 Star
BladeServer-4	Password	•••••		erver (Blade)	Windows Server 2003
BladeServer-5				erver (Blade)	Windows Server 2003 Ente
BladeServer-6				erver (Blade)	Windows Server 2003
BladeServer-7				erver (Blade)	Windows Server 2003 Star
BladeServer-8				erver (Blade)	
BladeServer-9		ОК	ancel	erver (Blade)	Windows Server 2003
RackServer-1		45		erver (Rack)	Windows Server 2003
	_	Hewlett-Packard	HP ZR24w	Monitor	
		Hewlett-Packard	LaserJet 4100 Series	Printer	
Desktop-8	12.255.136.208	Hewlett-Packard	m8180.de	Desktop	Windows Vista Home Prem
HPE49E84	192.168.178.43	Hewlett-Packard	OfficeJet J6400 Series	Multifunctional Device	
Laptop-4	12.255.136.191	Hewlett-Packard	Pavilion HDX9000	Laptop	Windows Vista Home Prem
ManagementDevice-1	12.251.240.235	Hewlett-Packard	Management Processor for HP I	n Management Device	
MultifunctionalDevice-?	12 255 136 171 III	Hewlett-Packard	Office let 16400 Series	Multifunctional Device	+
Total 333 devices   1 device	selected				

Figure: Change Device Credentials

Refer to section 6.2.2 for how to configure credentials for individual devices.

## 4.3 Discover Unix And Apple MAC OS X Computers

JDisc Discovery supports these Unix and Unix based operating systems:

- HP-UX
- Sun Solaris
- Linux (all major distributions)
- VMware ESX server
- Citrix XenServer
- Oracle VM Server
- IBM AIX
- Apple Mac OS X

All of the above Unix flavors typically do not have standard management protocols, such as SNMP or WBEM installed out-of-the-box or if installed, often do not provide detailed hardware, software and configuration information.

JDisc Discovery can overcome the lack of standard management protocols by logging on using telnet, executing selected system commands, and parsing the command output to retrieve hardware, software and configuration information. Ordinary user privileges are sufficient in most cases except of Linux and VMware ESX server), which require root access to collect hardware information from the BIOS.

To properly discover Unix computers:

- Enable the remote login for desired operating system platforms. Remote login is disabled for all operating system platforms by default. To enable remote login, open the *Configuration* dialog from the *Discovery* menu. Refer to section 5.6 for more details.
- Enable remote login for *unknown devices*. This option is important for hardened systems. JDisc Discovery then first logs on the computer, performs a uname command to determine the device platform. If the uname command has succeeded, the device is being discovered according to the device platform's configuration.
- Configure default credentials for desired operating system platforms. If using default credentials is not an option, configure per-device credentials. Refer to section 5.2.1.8 for more details on how to configure default credentials.

When discovering a computer, JDisc Discovery logs all commands that have been executed in the discovery log.

JDisc Discovery can use telnet or SSH to discover Unix computers correctly.

Remote login is disabled by default.

Enter default credentials in the discovery configuration or configure per-device credentials.

Root privileges are not required except for Linux and VMware ESX server.

## 4.4 Discover SNMP Based Devices

SNMP is the most common and important protocol to discover networked devices, such as routers, switches, or network printers. Network devices typically support SNMP as their primary protocol. Unlike computers, network devices often provide detailed hardware, software and configuration information in their private SNMP MIB (Management Information Base) area.

As most protocols, SNMP requires access credentials. SNMPv1 and SNMPv2c use so called 'community' as access credentials. Most manufacturers configure 'public' as their factory default community. Therefore JDisc Discovery uses 'public' as default community. You can add more default communities when needed. SNMPv3 is the security enabled version of the SNMP protocol. SNMPv3 does no longer use communities but comes with an user model that offers user authentication and password encryption.

Filter:					
Case sensitive filter					
Name	IP Addr	ess M	lanufacturer	Model	Туре
ProCurve1	192.168	.178.18 H	ewlett-Packard	ProCurve 2650	Switch
RackServer-2	12.251.	240.164 H	ewlett-Packard	rx2620	Server (Rad
RackServer-3	12.251.	240.0 H	ewlett-Packard	rx6600	Server (Rad
RackServer-4	12.251.	240.233 H	ewlett-Packard	rx6600	Server (Rac
RackServer-5	12.251.	240.16 H	ewlett-Packard	rx2660	Server (Rad
Switch-10	12.251.	240.219 H	ewlett-Packard	ProCurve 2524	Switch
Switch-11	12.25	Modify SNMP Credentia	ls	Property lies	witch
Switch-5	12.21	would stand the creating	13		witch
Switch-6	12.25				witch
Switch-7	12.25	Read Community			witch
Switch-8	12.25				witch
Switch-9	12.25	CNIMD road commun	ity tennorot		witch
teetee-pc.fritz.box	192.1	Siver reau commun	topsecret		esktop
xenserver	192.1				lini Tower
Desktop-4	12.25				lesktop
Desktop-5	12.25	SNMPv3 Account			lesktop
summit1	192.1				outing Sw
summit2	192.1	A. 46			witch
summit3	192.1	Authentication prot	ocol SHA V		outing Sw
		User name	test		Ionitor
192.168.178.7	192.1	Decemend			erver
192.168.178.73	192.1	Passworu			erver
Desktop-9	12.25	Privacy protocol	DES 👻		esktop
ttrenz-PC2.fritz.box	192.1	Privacy password			esktop
	102.1	Filvacy password			uit-h
· [	-				

Figure: Change SNMP Access Credentials

Refer to section 5.2.1.7 for how to add new default SNMP communities and accounts.

If using default SNMP communities or accounts is not an option, configure SNMP access credentials for each device individually.

## 4.5 Virtualization Technologies

JDisc Discovery supports these virtualization technologies:

- VMware ESX server (including ESXi) and VMware server running on Linux and Windows
- Oracle VM Server
- Xen
- Sun Solaris Zones
- Sun Solaris LDoms
- HP Integrity virtual machines
- Microsoft Hyper-V
- Sun VirtualBox

JDisc Discovery discovers all active virtual computer instances on a host server and

creates relations between the host server and the virtual computer instances it runs. Inactive virtual computer instances are ignored.

To return optimal results:

- VMware Tools should be installed on each VMware virtual machine. Without VMware Tools being installed, JDisc Discovery cannot discover important virtual machine attributes, such as IP address.
- Login credentials are required for each Hyper-V server to discover Hyper-V instances.

VMware Tools improves the discovery result. If VMware Tools is absent on VMware virtual machines, JDisc Discovery cannot discover the virtual machine's IP address.

The Medium Business or Enterprise Edition is required to discover virtual computers and the relationship to host computers except of Microsoft Hyper-V discovery which is part of the Small Business Edition.

### 4.5.1 Scanning VMware Environments

JDisc Discovery scans VMware environments and creates a list of VMware clusters, the physical servers, virtual machines and managing vSphere installations.

Without any access credentials, JDisc Discovery uses the HTTP or HTTPS protocol in order to identify VMware server installations. In that case, we can at least identify the operating system version even though we don't get detailed hardware and software information.

Once you provide access to the ESX(i) servers, JDisc Discovery uses the VMware API to retrieve the hardware, software and virtual machine information. Using the VMware API, JDisc Discovery can get hardware and operating system information for the ESX servers and basic information (such as IP address, mac address and configured operating system) for the virtual machines.

JDisc Discovery requires direct access to virtual machines in order to get detailed hardware and software information. The VMware API does not expose detailed information about the virtual machine's software configuration.

al Scope Directory Data Colleg	ion Discovery Jobs Protocols Filters SSH	Kevs	NG.		
Company	Description   10 addictional of   10 addicate	- muchanester bienester	-	and the Acco	nte
	Propercies 1PV4 Networks 1PV4 Range	s I IPV6 Networks   Network N	eighborhood   Direc	ubry Siximp Acco	2113
	Use default accounts from all platfor	ms for unknown devices			
	Clients & Servers Database				
	Windows   HP-UX   Oracle Solaris   I	IBM AIX   Linux/Oracle VM   VM	ware ESX/VCenter	Citrix XenServer	FreeBSD Mac OS X
	VMware ESX/VCenter Accounts				
		Deserved Trees	Comment		Add
	administrator@vsphere_local	Password Type	Comment		
	root	v root/enable			Remove
					Change
					Move up
					Move down
		III		F	
	Total 2 Accounts To Accounts s	Betteu			
	- VMware ESX/VCenter SSH Public/	Private Keys			
	Key name User i	name Key type	Passphrase	Туре	Add
					Remove
					Move up
					Move down
				+	
	Total U SSH public/private keys	1 0 Som public/private keys sele	rcteu		

Figure: VMware Default Accounts

JDisc Discovery makes use of information that is stored within the vCenter installation. The discovery process reads cluster, physcial server and virtual machine information out of the vCenter installation. Direct access to the ESX servers is no longer required. Vmware's vCenter is often installed on Windows computers. Simply enter the vCenter access credentials into JDisc Discovery's default accounts in order to let JDisc Discovery gather information from the vCenter installation.

JDisc Discovery can read information about clustering, physical hosts and their virtual machines from the vSphere installation. Root access to the physical ESX servers is not required!

# 4.6 Discovery Using Jumphost

There are cases, where you don't have direct access to a server. In many cases, administrators use a dedicated so called *jumphost* to access the server. In order to logon to the server, you connect first via SSH to the jumphost and then use the ssh client to access the actual server.



Figure: Scan a device via Jumphost

Define a jumphost for a dedicated network or IP range. In order to scan a device within this network or range, JDisc Discovery will connect to the jumphost first and then connect to the final server.

JDisc Discovery will also make use of the jumphost to ping the target network because ping to those protected networks is often blocked by a firewall.

There are two options on how to use the jumphost:

- try first a direct connection. If that fails, then use the jumphost.
- always use the jumphost.

Define a jumphost for an IP4 subnetwork or for an IP4 range from within the discovery configuration dialog.

 Properties Device History	IPv4 Networks IPv4 Ranges	IPv6 Networks Devices N	etwork Neighborhood Director	Y SNMP Accounts	
Filter:					Enable
Case sensitive ni	ter				Ping all Protocols
Means: use only ping Means: use all protoc	to find active devices ols to find active devices (signi	ificantly slower than pinging :	IPs)		Disable
Network Address	Subnet Mask	Name	Jumphost	# IP Addresses	Add
10.0.0.0	255.255.255.0		51.144.39.121		Browse
192.168.178.0	255.255.255.0				Remove
					Jump Host
					Import
					Export
<				>	

Figure: Jumphost Configuration

Click on the *Jumphost* button in order to define a jumphost for a specific IP4 network or range. Configure the jumphost access credentials and the jumphost mode.

-			
	BORNELSBOOK	*X*:0044-38.00000.000000000000000000000000000000	
3 <b>3</b> 1000	and date have		
Constant			

Figure: Jumphost Configuration Dialog

Use the *Test* button in order to test access to the jumphost.

## 4.7 Discover Cloud Environments

JDisc Discovery discovers cloud infrastructures for selected cloud provider.

#### 4.7.1 Microsoft Azure

JDisc Discovery can gather information about Microsoft's Azure cloud. That includes information about Office 365 deployments as well as virtual machines and database services.

JDisc Discovery basically requires the following rights:

- DeviceManagementManagedDevices.Read.All (Type Application) for Intune
- Directory.Read.All (Type Application) in order to read directory information
- User.Read.All (Type Application) in order to read user information.
- Furthermore, you need read access to each and every subscription that you would like to read.

### 4.7.1.1 Preparation Within The Azure Portal

You need to create an application within the Azure portal in order to collect Microsoft Azure information. Basically, you have to

- Register a new application
- Create a secret key
- Grant read access to users with the User.Read.All permission within the Microsoft

Graph API

- Grant read access to Azure Active Directory with the *Directory.Read.All* permission within the Microsoft Graph API.
- •
- Grant reader permissions to the individual subscriptions from the Access Control (IAM) dialog for each subscription.
- Grant permissions to Intune by adding the permission DeviceManagementManagedDevices.Read.All permission within the Microsoft Graph API

Follow the steps below to create an application with the required permissions:

- Connect to the Azure portal
- Open Azure Active Directory > App Registrations
- Click on New application registration
- Enter a name (e.g. JDisc Discovery)
- Enter <u>https://localhost</u> as Sign-on URL
- Once the application is created copy the *Application ID* to a Notepad window
- Now, we need to configure the api secret and the permissions
- In the application properties click on the Settings button
- Then click in the right menu on Keys
- Enter a new description for the key and a duration
- Once it is saved, copy the key secret to your notepad. The key secret is only visible once. If you don't have the key secret anymore, then you need to delete the key and create a new one
- Within the application settings click on the Required permissions item
- Click on Add and then select the Microsoft Graph API.
- Select Application Permissions and select the item *Read Directory Data* (*Directory.Read.All*)
- Select Application Permissions and select the item *Read Domain Data* (*Domain.Read.All*)
- Select Application Permission and select the item *Read all users' full profiles* (User.Read.All)
- In addition add the permission *Read Microsoft Intune Devices* (*DeviceManagementManagedDevices.ReadAll*) when you are using Microsoft Iontune.
- Click on Grant admin consent for <directory name>
- Finally, you need to grant read access to every subscription that you would like to discover:
- Open your subscriptions (e.g. from the Cost Management + Billing

- Select the desired subscription.
- Now select the item *Access Control (IAM)* in the left hand menu
- Click on Add a role assignment
- Select the role reader
- In the *Select* input field enter the name for the registered application, select the application and save your settings.

4.7.1.2 Configuration Within JDisc Discovery

Configure Microsoft Azure cloud access within JDisc Discovery once you have completed the preparation steps from the previous chapter. You will need:

- The so called *tenant id*. The tenant id might also be called *directory id*
- The application id
- The key secret

You can get the tenant id from the Azure portal within the Active Directory/Properties tab. The application id and the key secret is available from the your steps when you registered the application.

Enter the Azure cloud information in the configuration dialog.

Name	Tenant ID		Application ID	Add Change Remov
		D Add new A	zure API Key	Test
		Tom's MSDN Cloud           Tenant ID         51305350-1962-4456-858e-766232e604fc           Application ID         40bba1df-0b59-4854-9f1e-46c58d27ae7a           Key Secret         Ok		

Figure: Add access credentials for an Azure cloud directory

You might enter access credentials to more than one Azure cloud directory!

Define for each discovery job whether cloud information should be updated within this job or not.

eneral Scope Directory Data	ollection Discovery Jobs Protocols Topology Jobs Measurement Filters Cloud SSH Keys	
Name Name More Stower all	Directory     Settings     Settings       Properties     Croups     Settings       Syndronize directories     Syndronize users       Syndronize users     Syndronize users       Syndronize computer accounts     Syndronize networks       Odud Services     Odud Services       Device Discovery     Discover devices only once within	

Figure: Enable Cloud Synchronization for a Discovery Job

Not every discovery job needs to update the cloud information. In some cases, a separate job which updates the cloud information on a daily or weekly base might be sufficient!

Check the cloud discovery state from within the cloud status tab once the discovery job has started.

D JDisc Discovery [Professional Edition	n] - THOMAS TRENZ connected to loc	alhost		– 🗆 X
File Discovery Devices Software	Cloud Networking Measurement L	lsers Maps Documents	Troubleshooting Administration SHI Help	P
• • • • • • • • • • • • • • • • • • •				
Discovery Status				
Status				
Discovery is ci Getting network	irrently running interfaces			Check out how to improve the data suality!
Devices Ping Network Neighborho	d Directory Cloud Topology Jobs De	ice History Discovery Jobs	Measurement Data Quality Database	
Status Running		,,		
Current activity Scanning Azure - T	om's MSDN Cloud			
Name	Discovery Job Name	Туре	Last message	Percentage
Tom's MSDN Cloud	Discover all	Azure	Discover Office 365 Cloud	
Ulisc Azure Cloud	Discover all	Azure	waiting	

Figure: Cloud Discovery Status

#### 4.7.1.3 Checking Azure Cloud Results

The Microsoft Azure discovery performs two major tasks:

- it reads Office 365 subscriptions
- for each subscription, JDisc Discovery gets the list of subscribed services (e.g. database services, virtual machines)

Review the list of Office 365 subscriptions from the report *Cloud* » Office 365 » Office 365 Subscriptions. Open the report *Cloud* » Office 365 » Office 365 User Subscriptions in order to list of Azure directory users together with their Office 365 subscriptions.

The *Cloud Explorer* which is available through *Cloud » Cloud Explorer* organizes the cloud information in a tree. The top level item defines the Cloud technology, the next level determines the tenant (the owner of the cloud). Below the tenant there is information about the Office 365 subscriptions as well as the Azure subscritpions and their assigned resource groups and resources.

Л	Cloud Explorer							-	o ×
-									
	O O Q Q	Iter:							
	E Azure	Case sen	sitive filter						
	Default Directory	State	Name	IP Address	Manufacturer	Model	Туре	OS Version	Patch Le
	Pay-As-You-Go Dev/Test	Deallocated	windows10-1709	10.0.1.4			HyperV Instance	Windows 10 Professional	
	Thomas's Pay-As-You-Go Subscription	Deallocated	Windows2016DC	10.0.1.5			HyperV Instance	Windows Server 2016 Datacenter	
	Stoli Stoli Professional with MSDN	Deallocated	Windows2016R2	10.0.1.6			HyperV Instance	Windows Server 2012 R2 Datacenter	
	- 📃 Databases	Running	jaiscaj server database windows net	40.68.37.158	Microsoft	Microsoft DRfs/RectoreCOL	Cloud Service	10	
	Virtual Machines	🔊 Kunning	pg10.postgres.database.azure.com	191-237-232-75	Microsoft	MicrosofcobiorPostgresqu	cioud service	10	
	B DiscResources								
	⊡ <u>I</u> JDisc UG (haftungsbeschränkt)								
	Office 365     Office 365								
	Office 365 User Subscriptions								
		<							>
	·	otal 5 devices   0 i	devices selected						
				C	lose				

Figure: The Cloud Explorer

### 4.7.2 Amazon AWS

JDisc Discovery can gather information about Amazon's AWS cloud. That includes information about virtual machines.

4.7.2.1 Preparation Within The AWS Portal

You need to create an application API key and an API key secret within the Amazon AWS portal in order to collect cloud information:

- Open the IAM service within your AWS portal.
- Go to the users
- Create a new user and select the Security credentials tab.
- Within this tab use the button *Create access key* and remember the *Access key ID* and the Secret access key.

The Secret access key is displayed only during the key creation and cannot be recovered afterwards. So make sure to take a note of the key.

#### 4.7.2.2 Checking Amazon AWS Cloud Results

JDisc Discovery checks all AWS regions and collects all virtual machine resources assigned to the region together with the resource groups. Furthermore, it discovers all tags attached to a VM and stores them within the custom attribute section.

D Cloud Explorer ⇒ ⇒ ⇒ ⇒  ⊕  ₽  ₽  ₽  ₽  0							- 0 ×
	Filter: Case sen	sitive filter					
E 2015 Amazon AWS	State	Name	IP Address	Manufacturer	Model	Time	05
i⊟- <u>id</u> isc (076232821529)	Stopped	ec2-35-156-236-69 eu-central-1 compu-	35,156,236,69	Amazon	t2micro	Xen Instance	Libr
If a visit (visit) (used).	Stopped	Tom's test 1	172.31.43.43	Amazon	12.micro	Xen Instance	
	<		_				>
	Total 2 devices   0	devices selected					-
		Close					

#### Figure: Amazon AWS Results

### 4.7.3 Google Cloud Platform

JDisc Discovery can gather information about the Google Cloud Platform. That includes information about the cloud structure (folders, projects, regions, and zone) as well as information about the hosted virtual machines.

4.7.3.1 Preparation Within The Google Cloud Platform

First, enable the required APIs for your projects:

- Compute Engine API
- Cloud Resource Manager API

Create a *Service Account* within the API section. The service account requires the following permissions on the organization and the projects:

- Browser
- Viewer

Finally, create a Key for the service user. Use the JSON format when creating the key.

4.7.3.2 Configuration Within JDisc Discovery

Open the discovery configuration and select the *Google Cloud Platform* tab within the *Cloud* section.

Click on add and provide the following information:

- *name:* Choose a name for this connection
- *domain name/directory customer id:* provide the google domain name or the directory customer id
- *api key*: Past the JSON key created in the Google Cloud Platform configuration.

Use the *Test* button in order to test your configuration.

4.7.3.3 Review Google Cloud Platform Scan Results

After a successful scan review your cloud information using the Cloud Explorer.

D Cloud Explorer							- 🗆 ×
	* • • • • • •						
00000	Filter:						
	Case s	ensitive filter					
Azure							
Google Cloud Platform	State	Name	IP Address	Manufacturer	Model	Туре	OS V
in	📑 Running	scantest	10.156.0.58	Google	e2-micro	GCP Instance	
🖶 🔚 devs	Stopped	instance-1	10.182.0.2	Google	e2-micro	GCP Instance	
🖨 🔚 devs-germany	Stopped	jdisc-scanner	10.156.15.214	Google	e2-medium	GCP Instance	
Gisco Meraid Hettmer	< Total 3 devices J	0 devices selected					>
			Close				

Figure: Google Cloud Platform Scan

#### 4.7.4 Cisco Meraki

JDisc Discovery can gather information about the Cisco Meraki cloud. That includes information about the managed network devices, organizations and networks.

4.7.4.1 Preparation Within The Cisco Meraki Portal

You need to create an application API key within your Meraki portal. Configure this account within the Cloud configuration tab.

D Discovery Configuration General Scope Directory Data Collection Discovery Jobs Protocols Top	ology Jobs Filters Ooud SSH Keys	×
Azure Amazon AWS Cisco Merals Timeout 120 € second(s)		
Name ^	Add new Cisco Meraki API Key X Nome Disc API Key	Add Change Remove Test
	Ok Cancel	

Figure: Configure the API key for the Cisco Meraki Discovery

#### 4.7.4.2 Checking Cisco Meraki Cloud Results

Cisco Meraki devices can be scanned directly via SNMP or via the cloud using Meraki's REST API. The REST API gets information that is not available via the SNMP protocol such as serial numbers for access points, assigned organizations or Meraki networks.

Cloud Explorer						- 0
$  \leftarrow \rightarrow \diamondsuit   \bigtriangleup   \boxdot   \boxdot   \bigcirc   \odot   .$	ሐ 💷 🔕 📥 🖄					
Г						
0 0 Q Q	Filter:					
	Case sensitive filter					
Azure	_					
Amazon AWS	Name	IP Address	Manufacturer	Model	Type	Serial N
Cisco Meraki	JDISC-TEST-40G-01	ALC: 10 ALC: 10	Cisco Systems	MS225-48FP	Switch	
- Marshi Disc Cloud	JDISC-TEST-40G-02	an 10, 100, 100	Cisco Systems	MS225-48FP	Switch	1.000
1. Testnetwork	JDISC-TEST-AP-01	a	Cisco Systems	MR33	Access Point	1000
. 1. Datacenter Stuttoart	JDISC-TEST-AP-02	40-10-1000 Jan	Cisco Systems	MR33	Access Point	1.000 - 0
- A Datacenter Berlin	JDISC-TEST-AP-03	a 11 ma	Cisco Systems	MR33	Access Point	1000
- A. Datacenter Hamburg	JDISC-TEST-AP-04	41-12-280, perc	Cisco Systems	MR33	Access Point	(20) 40
- J. Datacenter Paris	JDISC-TEST-AP-05	a	Cisco Systems	MR33	Access Point	0.000
- Jabacenter London	JDISC-TEST-AP-06	an - 12 - 286 - 274	Cisco Systems	MR33	Access Point	1000
L. Datacenter Madrid	JDISC-TEST-EG-01	a	Cisco Systems	MS225-48FP	Switch	1000
	<					>
	Total 10 devices   0 devices sel	ected				
		Clos	e			



# 4.8 Discover Users And User Groups

JDisc Discovery discovers local user and user groups from computers and global users and user groups from Microsoft Active Directory. Moreover JDisc Discovery also gathers additional user and user group information including group members.

User and user group discovery is enabled by default. Two settings allow to to enable or disable the discovery of users and user groups.

Most reports that display users and user groups provide buttons on the right pane. These buttons simplify the navigation from user groups to their members or displaying effective permissions when the Security add-on is installed and licensed.

JDisc Discovery Discovers users, user groups and user group membership from computers and Microsoft Active Directory.

#### 4.8.1 Discover Local Users And User Groups

JDisc Discovery discovers local users and user groups for Windows and Unix computers. The discovery f local users and user groups is enabled by default and can be disabled from the discovery settings in the *Data Collection* tab.

neral Scope Directory Data Collection Discovery Jobs Protocols Topology Jobs Filters SSH Keys	
Standard Custom File Collection	
└User / User Groups	
☑ Discover user groups	
V Discover users	
☑ Delete users from logged on user history when not logged on for 30 → day(s)	
☑ Detect remote connections via RDP, SSH or telnet	
Create new devices for user connections from remote devices	

Figure: User / User Group Data Collection Settings

### 4.8.2 Discover Active Directory Users And User Groups

When Microsoft Active Directory access has been configured (refer to chapter 4.1 for more details), JDisc Discovery discovers all users and user groups that exist in Active Directory. Furthermore, JDisc Discovery assigns all users and user groups to their respective directory object and builds the user group membership of all users and user groups.

To discover Active Direcory users, user groups and user group membership, the *synchronize users* and *synchronize user groups* options must be enabled in the

Discovery Jobs directory tab.

Discovery Configuration	Discovery Jobs Protocols Topology Jobs Filters SSH Keys	×
Discovery Name Discover all	Properties       Groups       Directory       Schedule         Synchronize directories       Synchronize users       Synchronize user groups         Synchronize networks       Synchronize networks	

Figure: Directory Synchronization Settings

### 4.8.3 The User Group Browser

JDisc Discovery's user group browser displays the group hierarchy in a tree view. A report in the main area shows all users and user groups that belong to the selected group in the tree.

User Group Browser								
🔘 🖨 🔍 🔌 📄 Recursive user list	Pitter:	Olua Áltar						
JDISC Allowed RODC Password Replication Group								
-JDISC (Compliance Management JDISC (Delegated Setup	User Name	Login	Status	User Group Count	Canonical Name	Distinguished Name	User Id	34 Delete
JDISC \Denied RODC Password Replication Group (*)	Karl Napp	JDISC/KARL NAPP			1 JDISC.local/Users/Karl Napp	CN=Karl Napp,CN=Users,DC=3DISC,DC=local	S-1-5-21-3914981214-36492245-3201	Logged on Device(s)
								Looped on Mittory Design(c)
JDISC\Schema Admins (*)								Eugged of Faller y Device(a)
-JDISC/Domain Admins (*)								User Groups
-JDISC/Centerprise Admins (*) -JDISC/Cent Publishers								
JDISC/Read-only Domain Controllers								
JDISC/Development (*)								
-JDISC/DrsAdmins								
JDISC/DrsUpdateProxy								
- JDISC Domain Computers								
JDISC\Domain Users								
- JDISC Exchange Trusted Subsystem								
-JDISC/Help Desk								
JDISC Hygiene Management								
⊖-JDISC Layer 1Group ⊖-JDISC Layer 2 Group								
i⊟-JDISC\Layer3Group								
⊕-JDISC/Layer2 Group								
□-JDISC (organization Management ( ) □-JDISC ParentGroup (*)								
- JDISC(Sales (*))								
-JDISCIRAS and IAS Servers								
-JDISC\RA_AllowAddInAccess (*)								
JDISC (RA_AllowComputerAccess (*) JDISC (RA_AllowDashboardAccess (*)								
-JDISC/RA_AllowHomePageLinks (*)								
-JDISCIRA_AllowNetworkAlertAccess (*)								
JDISC RA AlowShareAccess (*)								
-JDISC Redplent Management								
DISC/Records Management     DISC/Server Management								
JDISC\UM Management								
JDISC Wew-Only Organization Management								
JDISC (WISSUSERS (~) JDISC (WinRMRemote/WMIUsers_								
	Total Luser LOurse	rs selected						
1	Total Loser To use	o operies						
					Close			
L								

Figure: User Group Browser

## 4.8.4 User Report

Open the Users » Users menu item to display global Active Directory users.

	L						
eri							
Case sensitive filter							
er Name	Login	Status	User Group Count	Canonical Name	Distinguished Name	User Id	🗶 Delete
nin	JDISC/ADMIN		12	JDISC.local/Users/Admin	CN=Admin,CN=Users,DC=JDISC,DC=local	S-1-5-21-3914981214-36492245-3201528148-1111	Longed on Design(c)
ninistrator	JDISC\ADMINISTRATOR		4	JDISC.local/Users/Administrator	CN=Administrator,CN=Users,DC=JDISC,DC=local	S-1-5-21-3914981214-36492245-3201528148-500	
overy Search Mailbox	JDISC\SM_BE4521298E5645EB9		0	JDISC.local/Users/DiscoverySearchMalbox {D9198A	CN=DiscoverySearchMailbox {D9198A05-46A6-415f-80AD-7E0933488852},CN=	S-1-5-21-3914981214-36492245-3201528148-6116	Logged on History Device
nange Online-ApplicationAccount	JDISC\\$ANR 100-U6R8HS6MI 1KP		0	JDISC.local/Users/Exchange Online-ApplicationAccount	CN=Exchange Online-ApplicationAccount,CN=Users,DC=JDISC,DC=local	S-1-5-21-3914981214-36492245-3201528148-6116	all the course
at	JDISC\GUEST		0	JDISC.local/Users/Guest	CN=Guest,CN=Users,DC=JDISC,DC=local	S-1-5-21-3914981214-36492245-3201528148-501	B User Groups
thMailbox1401c8e3dd134661bfcc1b700b0a0542	JDISC\SM_1009DB8643FB4F50A		0	JDISC.local/Users/HealthMalbox1401c8e3dd134661	CN=HealthMalbox1401c8e3dd134661bfcc1b700b0a0542,CN=Users,DC=JDISC,	S-1-5-21-3914981214-36492245-3201528148-6117	
thMailbox79732a72b1ce459982660481687d2a8b	JDISC\SM_CC56F858D8FA42888		0	JDISC.local/Users/HealthMalbox79732a72b1ce4599	CN=HealthMalbox79732a72b1ce459982660481687d2a8b,CN=Users,DC=JDISC,	S-1-5-21-3914981214-36492245-3201528148-6117	
thMalboxcab64115cc8d4f6dacfacd4a289e688c	JDISC\SM_F3D98CE292174EF79		0	JDISC.local/Users/HealthMalboxcab64115cc8d4f6da	CN=HealthMailboxcab64115cc8d4f6dacfacd4a289e688c,CN=Users,DC=JDISC,D	S-1-5-21-3914981214-36492245-3201528148-6117	
Napp	JDISC (KARL NAPP		1	3DISC.local/Users/Karl Napp	CN=Karl Napp,CN=Users,DC=JDISC,DC=local	5-1-5-21-3914981214-36492245-3201528148-1124	
р. 	JUISC WRBTGT		1	JUSC.ioca/disers/krbtgt	un=nrotgt, un=users, DC=JDISC, DC=local	5-1-5-21-3914981214-36492245-3201528148-502	
soft Exchange	JUISC (SM_AESSA IFDADFD488AB		0	JUISC.Iocal/Users/systemelalbox(bb558c35-97f1-4c	LTV=SystemMaiDox(DDSS8C35-971-4CD9-8ff7-d53741dc928c),CN=Users,DC=JD	5-1-5-21-3914981214-36492245-3201528148-6116	
isoft Exchange	JUISC (pM_6373830237CF42689		0	JUSK.Ioca/Users/SystemMailbox (e0dc1c29-89c3-40	UN=SystemMailbox(eUdc1c29-89c3-4034-b678-e6c29d823ed9), CN=Users, DC=J	5-1-5-21-3914981214-36492245-3201528148-6116	
isoft Exchange Approval Assistant	JDISC(SM_FEB580A9E0BF460F9		0	JDISC.local/Users/SystemMailbox{1f05a927-fb30-48	CN=SystemMalbox(100a927-fb30-46d0-ac59-2dddc22c6738),CN=Users,DC=J	5-1-5-21-3914961214-36492245-3201528148-6116	
sort Exchange negeration Malbox	JUISC (94 /0450ADC05340249		0	JUDC. loca/Users/nederatedbmail. 4c114d3b-8179-41	UV=Pederateotmail.+c1t+000-01/9-41+d-9301-00a95fa1e042,CN=Users,DC=JD	5-1-5-21-3914961214-30492245-3201528148-6116	
sort Exchange Migration	3015C (5M_773837700P6140979		0	JUDIC. local Jusers / Migration. 813e7716-2011-43e4-96	UN=Mgradon.atile //16-2011-Hister-9601-aba62d229136/CN=Users,DC=3DISC,	5-1-5-21-3914981214-36492245-3201528148-6116	
e su, rester	aption private replies			2010C local Common Development/share st. Tester	Cive-onare st. rester, ou exercision and cive-bernany, bc estimation of the cive of the ci	5-1-5-21-3514961214-36492245-3201528146-6113	
15.05	JDISC (IESIER			2010C local View Thomas Tonna	Civitest tester, oo - Development, oo - demany, oc - Jossi, oc - local	5-1-5-21-5914961214-56492245-5201528146-1125	
Here Here	ADDOLT INDIA		9	approximately of the second se	Champer in Trans Cit, Development Cit, Company DO, 20100 DO, Incl.	5-1-5-2 - 5-2 - 5-2 - 4-90 12 14-30 492245-320 1528148-1112	
1 20 users ( 0 users selected							

Figure: User Report

Use the buttons on the right side to display the user groups of which the user is a member.

### 4.8.5 User Group Report

Open the *Users » User Groups* menu item in to display allglobal Active Directory users groups.

+→◇ ≙ ⊑ ≅ ⊇ ⊙ ◎	- A-						
ters							
Case sensitive filter							
Jser Group Name	Description	User Group Count	User Count	Canonical Name	Distinguished Name	Unique Id	X Delete
DISC\Allowed RODC Password Replication Group	Members in this group can have their passwords replicated to all read-only domai	0		0 JDISC.local/Users/Allowed RODC Password Replicatio	CN=Allowed RODC Password Replication Group, CN=Users, DC=JDISC, DC=local	S-1-5-21-3914 +	B. Linere
DISC\Cert Publishers	Members of this group are permitted to publish certificates to the directory	0		0 JDISC.local/Users/Cert Publishers	CN=Cert Publishers, CN=Users, DC=JDISC, DC=local	S-1-5-21-3914	00015
DISC\Compliance Management	This role group will allow a specified user, responsible for compliance, to properly	0		0 JDISC.local/Microsoft Exchange Security Groups/Com	CN=Compliance Management,OU=Microsoft Exchange Security Groups,DC=JDI5	S-1-5-21-3914	Groups
DISC Delegated Setup	Members of this management role group have permissions to install and uninstall	0		0 JDISC.local/Microsoft Exchange Security Groups/Dele	CN-Delegated Setup, OU-Microsoft Exchange Security Groups, DC-JDISC, DC-loca	S-1-5-21-3914	
DISC /Denied RODC Password Replication Group	Members in this group cannot have their passwords replicated to any read-only d	7		1 JDISC.local/Users/Denied RODC Password Replicatio	CN=Denied RODC Password Replication Group.CN=Users.DC=JDISC.DC=local	S-1-5-21-3914	Group Bro
DISC/Development		0		1 JDISC.local/Users/Development	CN=Development.CN=Users.DC=JDISC.DC=local	S-1-5-21-3914	
DISC/Discovery Management	Members of this management role group can perform searches of malboxes in th	0		0 JDISC.local/Microsoft Exchange Security Groups/Disc	CN=Discovery Management, OU=Microsoft Exchange Security Groups, DC=JDISC	S-1-5-21-3914	
DISC DrisAdmins	DNS Administrators Group	0		0 JDISC.local/Users/DnsAdmins	CN=DnsAdmins.CN=Users.DC=JDISC.DC=local	5-1-5-21-3914	
DISC/Dog IndateProxy	DNS clients who are permitted to perform dynamic updates on behalf of some oth			0 IDISC local / isers/Dosi IndateProvy	CN=Dosi IndateProvy CN=I Isers DC=IDISC DC=Incal	5-1-5-21-3914	
DISC\Domain Admins	Designated administrators of the domain	0		2 IDISC local Alsers/Domain Admins	CN=Domain Admins.CN=Lisers.DC=JDISC.DC=local	S-1-5-21-3914	
DISC/Domain Computers	All workstations and servers joined to the domain	0		0 IDISC.localAlsers/Domain Computers	CN=Domain Computers, CN=Users, DC=IDISC, DC=local	S-1-5-21-3914	
DISC/Domain Controllers	All domain controllers in the domain			0 IDISC local / isers/Domain Controllers	CN=Domain Controllers, CN=Users, DC=1DISC, DC=local	S-1-5-21-3914	
DISC/Domain Guests	All domain quests	0		0 IDISC local / isers/Domain Guests	CNaDomain Guests CNaLIsers DC a IDISC DC aloral	\$-1-5-21-3914	
DISC/Domain Lisers	All domain users			0 IDISC local lisers Domain Lisers	CN=Domain Lisers CN=Lisers DC=IDISC DC=local	5-1-5-21-3914	
DISC Enterprise Admine	Deciman data a			2 IDIEC local / Isace Enterprise Admine	CN-Externation Admine CN-Linear DC-2019C DC-local	C.1.C.21.2014	
DISC Enterprise Rend only Densis Controllers	Members of this ora: a two Dand Only Demain Controllers in the enterprise			0. IDIEC Jacob I Inser Enterprise Rend only Dennis Cont	Ch-Enterprise Rend only Demain Controllers (Net Inter DC = IDISC DC -local	0.1.0.01.0014	
NEClEuchannel annu/lateren	This are a is far intercontribity with Euclidean 2002 accurs within the same fare			0 1015C local Microsoft Evolutions Security Contain Contra-	CN-Enterprise Read-only Contain Controllers, CN-Ose 5, CC-2015C, CC-1018	C 1 E 21 2014	
DISC Exchange Canvar	This group is for the operating of the Exchange accurate This group should be delated			0.1015C local Mission D Evolutions Security Groups/Exc.	Chillion and Chill	C 1 E 21 2014	
MCC Exchange To stard Colorators	This group contains all the Exchange servers. This group should not be beliefed.	0		o source local Microsoft Exchange Security Groups/Exc	CN=Exchange Servers, oo = Ho ason Exchange Seconcy & oops, oc = 30150, oc = 1.	C 1 5 21 3014	
DESC Exchange Hosted Bobsystem	This group contains exchange servers that are Exchange unders on behalf of us			o obtactional/Microsoft Exchange Security Groups/Exc	CN-Exchange Hosted Sobsystem, od = Hid oson Exchange Security Groups, DC=	5-1-5-21-3914	
DISC exchange windows Permissions	This group contains exchange servers traction exchange unders on behall of us			<ul> <li>3015C local/Pictosoft Exchange Security Groups/Exc</li> <li>3015C local/Company/Company/Company</li> </ul>	Children ange windows Permissions, oo wind oson exchange security droops, oc	5-1-5-21-3914	
Drsc (or oup 1		0		o obiscioca/demany/droop1	cn=aroop1,00=aermany,0C=J015C,0C=0cal	2-1-2-51-20146 E	
DISC (group 2		1		0 JDISC Jocal/Germany/Group2	CN=Group2,OU=Germany,DC=JDISC,DC=local	\$-1-5-21-3914	
DISC/Group Policy Creator Owners	Members in this group can modify group policy for the domain	0		1 JDISC local/Users/Group Policy Creator Owners	CN#Group Policy Creator Owners, CN#Users, DC#JDISC, DC#local	5-1-5-21-3914	
DISC yielp Desk	Members of this management role group can view and manage the configuration f	0		0 JDISC.local/Microsoft Exchange Security Groups/Help	CN=Heip Desk,OU=Microsoft Exchange Security Groups,DC=JDISC,DC=local	5-1-5-21-3914	
USC wygiene Management	members of this management role group can manage exchange anti-spam featur	0		U JUISC Jocal/Microsoft Exchange Security Groups/Hygl	CN#Hygiene Management, OU#Microsoft Exchange Security Groups, DC#JUISC, D	5-1-5-21-3914	
UISC (Layer IGroup		1		U JUISC Jocal/Germany/Development/Layer 1Group	CN=Layer turoup, OU=Development, OU=Germany, DC=JD15C, DC=local	5-1-5-21-3914	
DISC (Layer2 Group		1		U JDISCJocal/Germany/Development/Layer2 Group	CN=Layer2 Group,CU=Development,CU=Germany,DC=JDISC,DC=local	5-1-5-21-3914	
DISC (Layer 3Group		1		0 JDISC Jocal/Germany/Development/Layer 3Group	CN=Layer 3Group, OU=Development, OU=Germany, DC=JDISC, DC=local	\$-1-5-21-3914	
DISC Warketing		0		1 JDISC.local/Germany/Marketing	CN=Marketing,OU=Germany,DC=JDISC,DC=local	5-1-5-21-3914	
DISC (Organization Management	Members of this management role group have permissions to manage Exchange o	0		1 JDISC.local/Microsoft Exchange Security Groups/Org	CN=Organization Management, OU=Microsoft Exchange Security Groups, DC=JDI	5-1-5-21-3914	
DISC/ParentGroup		2		1 JDISC.local/Germany/ParentGroup	CN=ParentGroup,OU=Germany,DC=JDISC,DC=local	5-1-5-21-3914	
DISC\Public Folder Management	Members of this management role group can manage public folders. Members can	0		0 JDISC.local/Microsoft Exchange Security Groups/Publ	CN=Public Folder Management,OU=Microsoft Exchange Security Groups,DC=JDI	S-1-5-21-3914	
DISC/RA_AllowAddInAccess		0		2 JDISC.local/Users/RA_AllowAddInAccess	CN=RA_AllowAddInAccess,CN=Users,DC=JDISC,DC=local	S-1-5-21-3914	
DISC/RA_AllowComputerAccess		0		2 JDISC.local/Users/RA_AllowComputerAccess	CN=RA_AllowComputerAccess,CN=Users,DC=JDISC,DC=local	S-1-5-21-3914	
DISC\RA_AllowDashboardAccess		0		1 JDISC.local/Users/RA_AllowDashboardAccess	CN=RA_AllowDashboardAccess,CN=Users,DC=JDISC,DC=local	S-1-5-21-3914	
DISC\RA_AllowHomePageLinks		0		2 JDISC.local/Users/RA_AllowHomePageLinks	CN=RA_AllowHomePageLinks,CN=Users,DC=JDISC,DC=local	S-1-5-21-3914	
DISC\RA_AllowNetworkAlertAccess		0		1 JDISC.local/Users/RA_AllowNetworkAlertAccess	CN=RA_AllowNetworkAlertAccess,CN=Users,DC=JDISC,DC=local	S-1-5-21-3914	
DISC\RA_AllowRemoteAccess		0		2 JDISC.local/Users/RA_AllowRemoteAccess	CN=RA_AllowRemoteAccess,CN=Users,DC=JDISC,DC=local	S-1-5-21-3914	
DISC\RA_AllowShareAccess		0		2 JDISC.local/Users/RA_AllowShareAccess	CN=RA_AllowShareAccess,CN=Users,DC=JDISC,DC=local	S-1-5-21-3914	
DISCIRAS and IAS Servers	Servers in this group can access remote access properties of users	0		0 JDISC.local/Users/RAS and IAS Servers	CN=RAS and IAS Servers, CN=Users, DC=JDISC, DC=local	S-1-5-21-3914	
DISC\Read-only Domain Controllers	Members of this group are Read-Only Domain Controllers in the domain	0		0 JDISC.local/Users/Read-only Domain Controllers	CN=Read-only Domain Controllers,CN=Users,DC=JDISC,DC=local	S-1-5-21-3914	
DISC\Recipient Management	Members of this management role group have rights to create, manage, and rem	0		0 JDISC.local/Microsoft Exchange Security Groups/Red	CN=Recipient Management, OU=Microsoft Exchange Security Groups, DC=JDISC,	S-1-5-21-391#	
DISC\Records Management	Members of this management role group can configure compliance features such	0		0 JDISC.local/Microsoft Exchange Security Groups/Rec	CN=Records Management, OU=Microsoft Exchange Security Groups, DC=JDISC, D	S-1-5-21-3914	
DISC\Sales		0		1 JDISC.local/Germany/Sales	CN-Sales,OU-Germany,DC-JDISC,DC-local	S-1-5-21-39146	
DISC\Schema Admins	Designated administrators of the schema	0		2 JDISC.local/Users/Schema Admins	CN=Schema Admins, CN=Users, DC=JDISC, DC=local	S-1-5-21-3914	
DISC\Server Management	Members of this management role group have permissions to manage all Exchang	0		0 JDISC.local/Microsoft Exchange Security Groups/Ser	CN=Server Management,OU=Microsoft Exchange Security Groups,DC=JDISC,DC	S-1-5-21-3914 _	
All and the second seco				a search to addition and the colored as the first sound the sound of	All Testandificancies All Pandemosk All Caman Dr. 19866 An Last		
otal 52 user groups   0 user groups selected							

Figure: User Group Report

Use the buttons on the right side to display member users and user groups.

The user report does not display local user groups but only global Active Directory user groups.

## 4.9 Discover Databases

JDisc Discovery detects database installations together with the list of running instances, databases, its sizes and tables for a variety of database products.

The database discovery is split into two phases. Within the first phase, we are going to identify the database installations by looking at processes, installed applications or the Windows registry.

Once, we have determined the database installations and the ports that the instances are running on, we connect via JDBC to the database and determine information about the database itself. We collect information about its size, the schemas and tables defined within the database.

### 4.9.1 Configure Database Accounts

As for scanning devices, we need access credentials in order to connect to a database instance. Open the *Discovery Configuration* dialog and select the *Accounts* tab within the *Scope*. There, you can define default accounts for the currently supported

databases. Note that JDisc Discovery uses the database's JDBC driver to connect to the database.

If the connection succeeds, then we remember the username and password of the last success. This avoids to test the whole default list for each and every scan. The discovery will be faster and security logs shorter.

Database instances can be scanned without direct access to the database while more detailed information such as database size, schemas and tables requires database access via JDBC.

The database discovery requires to leave the process discovery enabled because some databases can only be identified based on their processes.

Discovery Configuration				<b>X</b>	
		Leeuur			
General Scope Directory Data Collection Discover	y Jobs   Protocols   Filters	SSH Keys			
Company Properti	es IPv4 Networks IPv4 P	Ranges IPv6 Netw	orks Network Neighborhood Directory SNMP Acco	unts	
Usi	e default accounts from all p	platforms for unknow	vn devices		
Client	s & Servers Database				
			Destance Destatues		
150	1DB2   ManaDB   Microsoft	SQL Server   MySQ	L Orace Database Posigres Database SAP MaxDB	Sybase Database	
	Postgres Database Account	5			
	User name	Password	Comment	Add	
	postgres			Remove	
				Change	
				Move up	
				Move down	
	Total 1 Account 10 Account	II nts selected	۰ ۲۰۰۰ ۲۰۰۰ ۲۰		
	Forder 1 Account   o Account				
		Ok	Cancel		

Figure: Configure Default Database Accounts

The default accounts will be used to connect to a database for the given database system.

#### 4.9.2 Review Database Discovery Results

JDisc Discovery assigns the discovered database information to the corresponding devices. Database information is available from within the device details dialog.

Networking Hardware Firmware Software User Vir	tualization Custom Attr	ibutes Roles Group	s Analyze	Features Certificates Clus	ter Services
rarchy Flat					
0000	Filter:				
	Case sensi	tive filter			
MariaDB [10.1.21]		1			
	DB Table	DB Table Size	DB Table Max Size	DB Table Row Count	
- in test	account	80.00 KB			
Microsoft SQL Server 2005 Express Edition [	accounttypelookup	16.00 KB			=
MySQL Community Server [5.7.17]	aceaccessmasklo	16.00 KB			-
PostgreSQL [9.2.4]	aceflagslookup	16.00 KB			
PostgreSQL [9.3.3]	application	576.00 KB			
E C: (program files (x86) (postgresql)(9.3)da	applicationinstance	128.00 KB			
E- Wentery [66.10 Mb]	applicationinstanc	48.00 KB			
account [80,00 KB]	applicationinstanc	16.00 KB			
accounttypelookup [16.00 K]	applicationinstanc	32.00 KB			
aceaccessmasklookup [16.00	applicationinstanc	48.00 KB			
aceflagslookup [16.00 KB]	applicationinstanc	40.00 KB			
application [576.00 KB]	applicationoperati	272.00 KB			
applicationinstance [128.00 I	attributetypelookup	16.00 KB			
applicationinstancearrayattri	availablewianmac	56.00 KB			
applicationinstancearrayattri	DIOS	176.00 KB			
applicationinstancearrayattri	ceruncate	1/6.00 KB			
application instanceattribute	duster	48.00 KB			
applicationoperatingsystem	dusterdevicerelat	16.00 KB			
attributetypelookup [16.00 K	dusterservice	40.00 KB			
< III +	Tetal 240 databases	10 databases selects	4		-
	l otal 240 databases	0 databases selecte	a		

Figure: Database Details

JDisc Discovery offers a tree version for the database report and a flat version which lists all database information in one single table.

### 4.9.3 Discover Oracle Database Instances

JDisc Discovery discovers Oracle database instances on Unix and Windows operating systems and stores them as application instances of type 'Database'.

#### 4.9.3.1 Discover Oracle Instances On Unix Computers

JDisc Discovery requires remote login to discover Oracle database instances. Make sure you have enabled remote login for the desired platform and have entered access credentials. Root access is required to query all Oracle database instances.

Root access is required to query all Oracle database instances.

4.9.3.2 Discover Oracle Instances On Windows Computers

JDisc Discovery requires

- Windows Remote Login
- WMI
- SMB

protocols to collect Oracle database instances. Make sure you have enabled these protocols and entered access credentials.

4.9.3.3 Oracle Multitenant Databases From Version 12c

Since Oracle Database version 12c Release 1, oracle introduced the concept of

multitenant architecture which enables an Oracle database to function as a multitent container database (CDB).

In order to be able to scan Oracle multitenant databases in JDisc Discovery, you need to add '*sys as dba'* account to JDisc Discovery in configuration under Scope > Accounts > Database > Oracle Database.

יכ	Device Details for 'Inte	grityVM-4'					
\$	$ \leftarrow\rightarrow\diamondsuit \textcircled{0} $	à   🗃 🗋   👮	0 14 0				
	General Networking	Hardware Firmware	Software User Conr	ections Virtua	Computers Custom	Attributes Roles Groups Analyze	
	deneral methoniang h						
	Operating System A	Applications Application	ion Instances Patches	Services Drive	ers Executables Pro	ocesses Cluster Services	
	Filter:						
	Case ser	nsitive filter					
	Instance Name	Instance Type	Application	Version	Manufacturor	Dath	
	Instance Name	Instance Type	Orado Database 10a	10.2.0.1	Orado	Paul	
	< Total 1 application	instance   0 applicati	ion instances selected		III.		•
					Close		

Figure: Database Instances

Administrative remote login, WMI and SMB is required to collect Oracle database instances.

### 4.9.4 Discover Oracle MySQL Database Instances

JDisc Discovery discovers Oracle MySQL database instances on Unix and Windows operating systems and stores them as application instances of type 'Database'.

#### 4.9.5 Discover IBM DB2 Database Instances

JDisc Discovery discovers IBM DB2 database instances on Unix and Windows operating systems and stores them as application instances of type 'Database'.

#### 4.9.5.1 Discover IBM DB2 Instances On Unix Computers

JDisc Discovery requires remote login to query DB2 database instances. Make sure you have enabled remote login for the desired platform and have entered access credentials.

Root access is required to query all DB2 database instances.

4.9.5.2 Discover IBM DB2 Instances On Windows Computers

JDisc Discovery requires

- Windows Remote Login
- WMI
- SMB (authenticated)

protocols to collect IBM DB2 database instances. Make sure you have enabled these protocols and entered access credentials.

Administrative remote login, WMI and SMB is required to collect IBM DB2 database instances.

#### 4.9.6 Discover Microsoft SQL Server Instances

JDisc Discovery discovers SQL Server database instances and stores them as application instances of type 'Database'.

JDisc Discovery requires

- SMB (authenticated)
- WMI

to collect Microsoft SQL Server instances. Make sure you have enabled these protocols and have entered access credentials.

SMB or WMI access is required to collect Microsoft SQL server instances.

### 4.9.7 Discover Postgres Database Instances

JDisc Discovery discovers Postgres database instances on Unix and Windows and stores them as application instances of type 'Database'.

#### 4.9.7.1 Discover Postgres Instances On Unix Computers

JDisc Discovery requires remote login to query Postgres database instances. Make sure you have enabled remote login for the desired platform and have entered access credentials. Root access is required to query all Postgres database instances.

Root access is required to query all Postgres database instances.

4.9.7.2 Discover Postgres Instances On Windows Computers

JDisc Discovery requires

- Windows Remote Login
- WMI
- SMB

protocols to discover Postgres database instances. Make sure you have enabled these protocols and entered the required access credentials.

Administrative remote login, WMI, SMB access is required to discover Postgres database instances.

### 4.9.8 Discover Sybase Database Instances

JDisc Discovery discovers Sybase database instances on Unix and Windows computers and stores them as application instances of type 'Database'.

4.9.8.1 Discover Sybase Instances On Unix Computers

JDisc Discovery requires remote login to discover Sybase database instances. Make sure you have enabled remote login for the desired platform and have entered access credentials.

4.9.8.2 Discover Sybase Instances On Windows Computers

JDisc Discovery requires SMB or WMI to query Sybase database instances. Make sure you have enabled at least one of those protocols and that you have entered access credentials.

# 4.10 Running Oracle LMS Scripts

JDisc Discovery can run Oracle's LMS scripts in order to help collecting the data when audited by Oracle. Oracle usually provides the LMS scripts within a ZIP package. The ZIP package includes some documentation and the Unix shell and Windows command scripts.

JDisc Discovery cannot prepackage Oracle's scripts because of Oracle's licensing terms. However, if you are audited by Oracle, then you are entitled to receive the scripts. Once you receive the scripts, you can integrate the scripts into JDisc Discovery. JDisc Discovery will then copy the scripts to a target machine that has an Oracle database installed, runs the scripts and collects the output files as custom attributes within our database.

### 4.10.1 Import Oracle LMS Scripts Into JDisc Discovery

Copy the Oracle LMS scripts to your JDisc Discovery server. Then open the configuration dialog and navigate to *Data Collection » Database* in order to import the Oracle LMS scripts into JDisc Discovery. First enable the Oracle LMS collection by selecting the checkbox *Run Oracle LMS scripts*. Then click on the *Browse* button and select the Oracle LMS zip file.

JDisc Discovery is now prepared to run Oracle's LMS scripts.

andard Networking Virtualization Exchange	Server Database Support Entitlements Custom File Collection	
Settings		
☑ Discover database details		
Discover schemas within database		
Discover tables within schema		
limeout		
IBM DB2 database connect timeout	10 ÷ seconds	
Informix database connect timeout	10 ÷ seconds	
Microsoft SQL Server database connect timeo	ut 10 2 seconds	
MongoDB connect timeout	10 🗘 seconds	
MySQL/MariaDB database connect timeout	10 🗧 seconds	
Oracle database connect timeout	10 ÷ seconds	
Postgres connect timeout	10 ÷ seconds	
SAP MaxDB connect timeout	10 ÷ seconds	
Sybase connect timeout	10 🗘 seconds	
Oracle LMS		
JDisc Discovery can deploy and run Oracle's I	MS scripts.	
Configure the Oracle LMS ZIP location and er	able Oracle LMS.	
Run Oracle LMS scripts	and captare are output main castorn denotees.	
ZIP file location (must be on the discovery	server) Browse	

Figure: Configuring Oracle LMS Data Collection

### 4.10.2 Review The Results

You find the output for the Oracle LMS collection within our custom attribute section once a server with an Oracle database installation has been scanned.

Figure: Oracle LMS Results

As a result of an Oracle LMS script execution, you get a hierarchy of folder below the *Oracle LMS* root folder. The folder structure below is that we create a new folder for each result ZIP file that comes from the LMS scripts. Then, we create the exact same folder structure as it is within the result ZIP files from Oracle's scripts.

### 4.10.3 Bulk Export

When the Oracle LMS data has been imported into JDisc Discovery's database, then you can select any number of devices and use the context menu *Oracle LMS » Export Oracle LMS Data*. The export creates a ZIP file with a folder for each device. Each device folder contains all files collected for this particular device.

## 4.11 JEE Server Discovery

JDisc Discovery detects the most common Java Enterprise Edition (JEE) application server. In addition to finding the application server software installation, JDisc Discovery also discovers all deployed JEE applications. JEE applications are represented as application instances in JDisc Discovery's reports.

### 4.11.1 IBM WebSphere

JDisc Discovery requires remote login access on Unix and Windows systems to discover IBM WebSphere installations (starting with WS 7.0).

#### 4.11.2 Oracle WebLogic

JDisc Discovery requires remote login access on Unix and Windows to discover Oracle WebLogic installations. On Unix, root access is required due to restrictive permissions configured by Oracle's installer program.

#### 4.11.3 JBoss

JDisc Discovery requires remote login access on Unix and Windows to discover JBoss installations.

# 4.12 Using Password Managers

JDisc Discovery can use password managers to obtain the current username and password for a specific device during the scan process.

#### 4.12.1 Paswordstate

Clickstudios' password manager *Passwordstate* offers a wide range of functionality to manage your passwords, rotate passwords on defined intervals.

4.12.1.1 Prepare Passwordstate Server

In order to obtain data from the Passwordstate solution via its API, you need to define API keys. There are two kind of API keys:

#### • Systemwide API Keys

There can only be one systemwide API key in Passwordstate. With this API key, users can obtain data from all shared password lists.

#### • API Keys for single Password Lists

API keys for single password lists can be defined when you would like to grant access only to this particular password list.

#### 4.12.1.2 JDisc Discovery Configuration Steps

In order to configure access to the Passwordstate solution, you need to have the following information:

- The Passwordstate's server name (e.g. passwordstate.testcompany.com)
- The port that the API is reachable on (usually 443)
- A systemwide API key or a list API key together with the numeric list id.

When configuring access to a single Password list then you need the API key for the list and the internal list id from Passwordstate. The list ids are hidden by default. Enable displaying the list id by using the *List Administrator Actions...* within the list properties and choose the option *Toggle Visibility of WEB API IDs*.

Once you have this information, you can add a Passwordstate connection in JDisc Discovery's user interface via *Administration* » Password Managers » Passwordstate.

Figure: Configure Passwordstate Connections

The menu item opens a new dialog with the list of currently configured connections.

Add a new connection via the Add button.

Figure: Add a systemwide Connection

Once, you have added the new connection, you can use the *Test* button to check whether the connection works or not.

Choose the credentials you would like to use within the discovery when the connection to the Thycotic SecretServer has been established.

Choose Accounts from the Passwordstate Password Manager

#### 4.12.2 Thycotic SecretServer

Thycotic's SecretServer is a password management product which is frequently used by companies to manage their credentials in a secure way.

4.12.2.1 Prepare Thycotic SecretServer

In order to use the Thycotic's REST API, you will need to define a user with a username and password which has the permissions for API access. Follow the Thycotic instructions on how to achieve this.

4.12.2.2 JDisc Discovery Configuration Steps

Once the Thycotic SecretServer is properly configured, you can add the Thycotic SecretServer connection to JDisc Discovery.

Open the Thycotic SecretServer connection management dialog via *Administration* » *Password Managers* » *Thycotic*.

		×
Discovery Devices Software Cloud Networking Measurement Users Maps Documents Troubleshootin	ting Administration SHI Help	
overy Status	<ul> <li>User Management</li> <li>Change Master User</li> </ul>	
Status	Database >	
Discovery is idle	Password Managers > CyberArk	4
	Manage Mail Accounts       Image Scheduled Mail Report Jobs	
Devices Pring Network Neighborhood Directory Cloud Device History Discovery Jobs Measurement Data Quality Data Concurrent device discoveries 0 of 10 Average duration Discovery jobs 0 of 0 pending Manually triggered 0 pending Devices Indathabae 0	atabé     Manage Storage Locations       Image Scheduled Report Export Jobs       Image Start Application	
Device Name Type Duration Progress	Start Application - Reporting Mode  L     Stop Application	

Figure: Configure Thycotic Secret Server Connections

This menu item opens a new dialog which allows users to manage your Thycotic SecretServer connections.

Figure: Add a new Thycotic SecretServer Account

Choose the credentials you would like to use within the discovery when the connection to the Thycotic SecretServer has been established.



Figure: Choose Credentials

JDisc Discovery will query the Thycotic SecretServer for the current login and password when the credentials are needed for the device scan. JDisc Discovery does not store the username or passwords in its database!

### 4.12.3 CyberArk

CyberArk is a password management application which is frequently used to store and manage access credentials for devices or domains. In order to use the CyberArk

password manager, you need to prepare the CyberArk server and configure access for the JDisc Discovery solution.

#### 4.12.3.1 Prepare CyberArk

Follow the steps below in order to provide access to the credentials stored within CyberArk.

#### **Step 1: Define an Application ID**

To define the application, define it manually through the CyberArk Password Vault Web Access (PVWA) interface:

- Log in as user allowed to manage applications (it requires Manage Users authorization)
- In the Applications tab, click Add Application. The Add Application page appears.

There is no special requirement for the APPID name. Specify the following information:

- in the *Name* box, specify the unique name (ID) of the application. The recommended Application ID for this integration is:APP ID = Jdisc
- in the *Description* box, specify a short description of the application that will help you identify it.
- in the *Business owner* section, specify contact information about the application's business owner.
- in the *Location* box, specify the location of the application in the Vault hierarchy. If a location is not selected, the application will be added in the same location as the user who is creating this application.

ame:	JDisc		
Description:	Used to obtain credentials while scanning devices using JDisc		
Business owner			
First Name: Last Name: Email: Phone:			
Location:	1	~	
Time Restrictions: Expiration Date:	From: To: V		

Figure: Adding an Application

Click Add and the application is added to the list of applications.



Figure: Application Configuration

- check the *Allowing extended authentication restrictions* box. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.
- Specify the application's *Authentication* details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password.

#### **Step 2: Specify Authentication Details**

Specify the application's Authentication details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password. You need to create a client certificate and you have to have the root certificate for the client certificate.

- in the Authentication tab, click *Add*. A drop-down list of authentication characteristics is displayed.
- Select Certificate Serial Number
- Specify the Certificate Serial Number.

#### **Optional Step 3: Specify the Allowed Machines**

Specify the application's Allowed Machines. This information enables AAM to make sure that only applications that run from specified machines can access their passwords.

• In the *Allowed Machines* tab, click *Add*. The Add allowed machine window is displayed.

dd allowed ma	chine		×
Address:			
	Enter IP/host name/DNS		
		bbA	Cancel

Figure: Enter allowed machine

• In the *Address* box, specify the IP/hostname/DNS of the machine where the application will run and will request passwords, then click *Add*. The IP address is listed in the Allowed Machines tab.

#### **Step 4: Provisioning Accounts and setting Permissions for Application Access**

For the application to perform its functionality or tasks, the application must have access to particular existing accounts, or new accounts to be provisioned in CyberArk Vault.

In the Password Safe, provision the privileged accounts that will be required by the application. You can -do this in either of the following ways:

- **Manually** Add accounts manually one at a time, and specify all the account details.
- **Automatically** Add multiple accounts automatically using the Password Upload feature.

For this step, you require the Add accounts authorization in the Password

Safe.

For more information about adding and managing privileged accounts, refer to the Privileged Access Security Implementation Guide.

Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application.

Add the provider user (where the Central Credential Provider is installed) and application users as members of the Password Safes where the application passwords are stored. This can either be done manually in the Safes tab, or by specifying the Safe names in the CSV file for adding multiple applications.

Add the Provider user as a Safe Member with the following authorizations:

- List accounts
- Retrieve accounts
- View Safe Members

When installing multiple Providers for this integration, it is recommended to create a group for them, and add the group to the Safe once with the above authorization.

Add Safe Member			
Search:	Search In:	Vault 💽	Search
Selected Search: Vault			
Name	Business Email	Full Name	
Access			-
Use accounts			
Retrieve accounts			
✓ List accounts			
Account Management			
Safe Management			
Monitor			
View Audit log			
View Safe Members			-
The same memory			
		ſ	Add Close

Add the application (the APPID) as a Safe Member with the following authorizations:

Retrieve accounts

If the Safe is configured for object level access, make sure that both the provider user and the application have access to the password(s) to retrieve.

For more information about configuring Safe Members, refer to the *Privileged Access Security Implementation Guide*.

4.12.3.2 JDisc Discovery Configuration Steps

Once your CyberArk Instance is configured, you have to configure the CyberArk access within the JDisc Discovery application. JDisc Discovery can use as many CyberArk servers as needed. Each server instance has its own access credentials and configured application. Follow the steps below in order to add a new CyberArk server instance to JDisc Discovery's configuration:

Open the CyberArk server configuration dialog via *Administration* > *Password Managers* > *CyberArk*.

Figure: Open the CyberArk Server Configuration Dialog

This is going to open the CyberArk Server Configuration dialog. The dialog lists all currently configured CyberArk servers.

Figure: CyberArk Servers Dialog

Click on the *Add* button in order to add an additional CyberArk server. Then enter a name for the server, the server address (hostname or IP address), the port (default it HTTPS port 443). Finally configure the *application id* configured in the CyberArk preparation.

Furthermore import the client certificate by clicking on the *click to import certificate file*. The file must be in the .p12 format and include the client certificate and the certificate's private key.

The root certificate for the client certificate must be imported into

certificate store on the server where JDisc Discovery is installed.

Add Cyberark Serve	×	
Name	JDisc CyberArk Test Server	
Cyberark Server Addre	cyberark.jdisc.com	
Cyberark Server Port	443	
Cyberark App ID	JDisc	
Client Certificate	click to import certificate file	
JDisc Discovery utilizes Authentication type	the following credentials to browse safes and passwords in order to select existing passwords in JDisc Discovery's credentials dialog.	
Credential type	Jsername/Password 🗸	
CyberArk API user	admin	
CyberArk API passwe	rd ••••••	
	Ok Cancel	

Figure: Add a new CyberArk Server Connection

The App-ID and the client certificate is used to retrieve the current credentials. In order to list the CyberArk accounts and the safes, you need to specify an additional user.

Depending on the user configuration within CyberArk, you can choose an authentication type:

- CyberArk
- Windows
- LDAP
- Radius

In order to get the username and password for this user, you can specific the username and password directly or you can specify a CyberArk safe and object name to define the credentials.

Finally, you can use the *Test* button to check the connectivity. In order to check the connectivity, you need to provide a safe and object name to test the access with.

4.12.3.3 Using CyberArk Accounts

Once the connection has been established successfully, you can use CyberArk accounts from virtually anywhere where you configure access credentials (just a few exceptions).

All credential dialogs supporting password managers have now a radio button to choose whether you would like to enter a username/password combination or whether you would like to choose credentials managed by a password manager.
D Add new Windows Accou	nt	×
Account	O Use password manager	
User name Password		
Comment		
	Ok Cancel	

Figure: Credential Dialog supporting Password Managers

Either enter a username and password or select the *User password manager* radio button in order to select credentials managed by a password manager.

🕽 Add new Windows Account	×
Account	
O Use login/password	nager
Managed Passwords	
undefined - dick to modify	
Comment	
Ok Ci	ancel

Figure: Select Password Manager Credentials

The *Managed Passwords* area contains the selected password from a password manager. Click on the *undefined* – *click to modify* link in order to select the desired credentials.

This will open a selection dialog where you can see the configured password managers on the left and once you select a safe the list of the actual passwords on the right side.

Figure: Select the desired Credentials

Finally, the credentials dialog displays the password name.

Add new Windows Account	×
Account	
JDisc Test Server - Safe: 'Test' Object: 'Operating System-WinDomain-jdisc-adn Comment	
Ok Cancel	

Figure: The selected Credentials

From now on, the discovery will use this account and query the current username and password from the CyberArk server when the account is needed.

#### 4.12.4 Microsoft LAPS

Microsoft LAPS (Local Administrator Password Solution) is a solution from Microsoft to manage local administrator account passwords for computers that are member of a Active Directory. LAPS makes local administrator accounts more secure since it is using different passwords for local administrators on different computers and it is able to change the passwords frequently.

Find more information on Microsoft's LAPS download page: <u>https://www.microsoft.com/en-us/download/details.aspx?id=46899</u>

#### 4.12.4.1 LAPS Architecture Overview

Legacy LAPS	To use LAPS, you need to install the software on one of your servers. As a second step, you need to extend your directory structure with the LAPS related attributes. Finally, you need to install a software on all the client computers that are managed through LAPS.
Native LAPS	Natively Integrated on Windows 11, Windows 10, and Windows Server (starting in April 2023)

When configured properly, LAPS updates the local administrator user's password in the Active Directory computer account property that is accessible only for specific users. Native LAPS also supports encrypted storage of the local administrator passwords in

Active Directory.

4.12.4.2 Configure LAPS In JDisc Discovery

JDisc Discovery's discovery configuration dialog includes the *LAPS* tab within the top level group. When the Active Directory structure has been synchronized you can view all directory objects in the tree view. To make use of LAPS for a directory object, you need

- a user account having access rights for reading the local administrator's password for computer accounts. This user account can be assigned on any level in the directory and is valid for all sub-directory objects.
- **for Legacy LAPS installations only:** optionally a list of common local administrator account names. This list can be assigned on any level in the directory and is valid for all sub-directory objects. This is important, since the local administrator account names can be renamed and also depend on the Windows operating system language. If omitted, *Administrator* is used as local account name.

JDisc Discovery uses LAPS only when discovering computers that are a member of a directory object that has been enabled for LAPS (either directly or indirectly via one of its parents).

4.12.4.3 Configure A LAPS Account

To access the local administrator password of a computer account in Active Directory, a user is required having at least read permissions.

To configure a LAPS account,

- Open the *Discovery Configuration* dialog-box and switch to the LAPS tab.
- Then select a directory object and click the *Change LAPS Account* button.
- From the *Modify Directory Object Account* dialog-box enter the user account and password.



For native LAPS the LAPS account must also be privileged to run process on the domain controllers that serves the Active Directory domain.

JDisc Discovery uses its Zero-footprint agent on domain controllers to decode/decrypt the local LAPS account/password cipher-text that is stored in the Active Directory computer account object.

_			
ompany		Properties Device History IPv4Networks IPv4Ranges IPv6Networks Devices NetworkNeighborhood Directory LAPS SNM	P Accounts
		Microsoft Local Administrator Password Solution (LAPS) provides management of Local Administrator account passwords for domain joined computers. Passwords are saved ACL protected in Active Directory for authorized users only. Enable directory	Toggle
		objects for which you want JDisc Discovery to query Local Administrator account passwords for domain joined computers.	Change LAPS Account
		DDISC.Cocl (*)     Domain Controllers     Domain Controllers	Local Administrator Accounts

igure: Enter a LAPS Account

## 4.12.4.4 Configure Local Administrator Accounts

Without extra configuration, JDisc Discovery uses *ADMINISTRATOR* as default login for the local administrator.

You must enter a different local administrator account name (or a list of local administrator account names) if the local administrator login is localized or has been intentionally renamed.

To enter local administrator account names,

- select a directory object and click the *Local Administrator Accounts* button to manage the list of local administrator account names.
- from the *LAPS Local Administrator Account Names* dialog-box, click *Add* to add a new local administrator account name or Remove to delete an existing local administrator account name.

D LAPS Local Administrator Account Names	×
Microsoft Local Administrator Password Solution (LAPS) provides management of Local Administrator account passwords for domain joined computers. However, LAPS does not save the Local Administrator account name.	
To support your Windows language versions and Local Administrator account names, add the appropriate Local Administrator account names. If you don't add Local Administrator account names, JDisc Discovery defaults to the 'ADMINISTRATOR' account name.	
Local Administrator Account	Add
JDISC	Remove
	Move up
	Move down
Ok Cancel	

Figure: Manage LAPS local Administrator account names

# 4.13 Cluster Discovery

JDisc Discovery identifies several cluster technologies.

#### 4.13.1 Veritas Cluster

JDisc Discovery requires remote login access on Unix and Windows to discover Veritas cluster installations. JDisc Discovery identifies the cluster name and the cluster services including their status.

#### 4.13.2 Microsoft Cluster Services

JDisc Discovery requires WMI access to identify Microsoft Cluster Services installations. JDisc Discovery identifies the cluster name and the cluster services including their status.

#### 4.13.3 HP ServiceGuard Cluster

JDisc Discovery requires remote login access to detect HP ServiceGuard cluster installations. JDisc Discovery identifies the cluster name and the cluster services including their status.

# 4.13.4 Cisco HSRP Cluster

JDisc Discovery requires SNMP access to detect Cisco's HSRP Cluster.

## 4.13.5 VRRP Cluster

JDisc Discovery requires SNMP access to identify VRRP cluster for switches and routers.

## 4.13.6 Fortinet HA Cluster

JDisc Discovery requires SNMP access to identify Fortinet HA cluster for switches and routers.

#### 4.13.7 Juniper HP Cluster

JDisc Discovery requires SNMP access to identify Juniper HP cluster for switches and routers.

### 4.13.8 Unix Cluster

JDisc Discovery requires SSH or telnet access in order to identify Solaris, Redhat, Citrix, VMware, KVM, AIX and Pacemaker clusters.

# 4.14 Microsoft Exchange Server Discovery

JDisc Discovery discovers Microsoft Exchange Server using its zero-footprint agent. Once the discovery process has deployed the agent on the exchange server, it runs some powershell scripts to retrieve exchange server editions and mailboxes.

#### 4.14.1 Configuration

Microsoft Exchange mailbox discovery is enabled by default. You might modify the settings from the *Exchange Server* tab within the *Data Collection* area. Gathering the mailboxes with their configuration can take some time and the default remote login execution timeout might be too short to run the script on weak hardware or on heavily loaded servers. Therefore there is a separate timeout value *Powershell script execution timeout*. Its default is 30 minutes. Increase the timeout if you our powershell scripts need more time.

eneral Scope Directory Data	Collection Discovery Jobs Proto	cols Topology Jobs Filte	rs SSH Keys	
Standard Exchange Server	Custom File Collection			
Discover exchange mailbo	kes			
Powershell script execution tim	eout 30 🚔 minutes			

Figure: Exchange Server Discovery Configuration

Exchange Server Discovery requires the remote login protocol (zero-footprint agent) for Windows. Otherwise, it is not possible to run the powershell script locally on the exchange server.

Exchange Server Discovery powershell scripts might need some time to retrieve mailbox information on heavily loaded or large Microsoft Exchange installations.

Use the *Powershell script execution timeout* in order to configure the timeout for Exchange data collection scripts.

# 4.14.2 Exchange Server Reports

Open the Microssoft Exchange server menu item in order to retrieve the list of Exchange servers and mailboxes.

JDisc Discovery [Enter File Discovery Devices	rprise Edition] - THOMAS TRI Software Networking User	NZ connected to localhost
) () () () Discovery Status	Applications     Application Instances     Patches	
Status	🔅 Services	
Di Di	Drivers     Executable Files     Processes     Windows Features	Check out how to improve the data quality!
Devices Ping Networ	e Clusters	y Jobs Device History Discovery Jobs Data Quality Database
Concurrent device disc	Microsoft Exchange	Microsoft Exchange Server
Average duration Discovery jobs Manually triggered Devices in database	0 of 0 pending 0 pending 394	Microsoft Exchañge Mailboxes

Figure: Exchange Server Menu Item

The *Microsoft Exchange Server* menu item lists all Exchange server, the currently used Exchange edition and version together with statistics about the managed mailboxes.

Figure: Exchange Server Report

The *Microsoft Exchange Mailboxes* report lists all mailboxes found in server farms. For each mailbox, it gathers status and configuration information about

- Web Access configuraiton
- Active Sync configuration
- quota information
- mailbox size

Figure: Exchange Mailboxes

# 4.15 Support Entitlement Discovery

JDisc Discovery gathers warranty and support entitlement information for vendors that offer a web based interface to query this information. For most vendors, this does not even require access credentials. However for some vendors, this requires an API key and API secret or username and password.

## 4.15.1 Cisco Warranty Information

With your company specific Cisco Client ID and Client Secret keys you can gather Cisco devices support entitlements about warranty information and coverage. Add your access credentials in *Scope > Accounts > Support Entitlement > Cisco Support Entitlement > Cisco* as 'User name' and 'Password' respectively.

# 4.16 Multicast MDNS/UPnP Device Discovery

Many home networking and Internet of Things (IoT) devices do not support typical management protocols such as SNMP or SSH command shells.

As a result, such devices often are not found or identified by a central discovery server. However, many home networking and Internet of Things (IoT) devices support the mDNS or UPnP protocols, which can help discover and identify such devices.

## 4.16.1 Discovery Process

When JDisc Discovery discovers remote (Windows) computers it can send mDNS and UPnP protocol multicast requests on local IPv4 and IPv6 networks and receive

multicast replies from mDNS and UPnP-enabled devices.



Figure: Multicast mDNS/UPnP Discovery Process

The figure above shows the typical multicast-based mDNS/UPnP discovery process from the discovery server to a home or branch office.

- [1] The discovery scans a Windows computer (using remote login) and collects the configured data items.
- [2] Next it sends a mDNS and UPnP multicast discovery request to all local IPv4 and IPv6 networks.
- [3] mDNS and UPnP enabled devices reply by sending multicasts and the Windows computer in the home- or branch office picks device information and returns it to the discovery server.

#### 4.16.1.1 IP And MAC Address Resolution

The mDNS and UPnP protocols work on the network layer and thus do not know MAC addresses. However, MAC addresses are important for discovery as they identify devices (among other attributes).

Therefore, MAC addresses of mDNS and UPnP-enabled devices are resolved using the local IPv4 ARP and IPv6 Network Neighbor caches on Windows computers in home- or branch offices.

## 4.16.2 Supported Device Types

Many types of devices can be identified using the mDNS and UPnP protocols. At the time of writing the following device types are supported by JDisc Discovery.

Audio Receiver (Denon)

- Dishwasher (Siemens)
- Home Automation Controller (Elero Centero Home Gateway)
- Home Environment Controller (tado°)
- Home Lighting Controller (Philips Hue)
- Laptop (Apple MacBook)
- Multifunctional Device (Brother, Hewlett-Packard)
- NAS (QNAP, Synology)
- Radio Alarm Clock (Philips Wake-up Light)
- Smart TV (LG, Samsung)
- Smart TV Receiver (Apple TV, Telekom)
- Smart Speaker (Bang & Olufsen Beoplay)
- Tablet Computer (Apple iPad)
- Weather Station (Netatmo)
- Wireless DSL Router (AVM Fritz!Box)
- Wlan Repeater (AVM)

#### 4.16.3 Unknown Devices

The mDNS and UPnP protocols are largely based on text information that is processes by the discovery using rules. These rules associate the textual information to device types, models, and manufacturers. Because of that, text information from devices that are not yet known (for which no rules exist) are set to Unidentified Device.

To support unidentified mDNS and UPnP devices faster, JDisc Discovery includes two new reports. These reports display textual information from the mDNS and UPnP protocols for which no rules exist yet.

Support ZIPs include the content of the two reports and help to develop and improve mDNS and UPnP device discovery rules.

#### 4.16.3.1 Unknown MDNS Devices Report

The device information returned by the mDNS protocol consists of service types and properties as shown in the next screenshot.

	2   🔁 🛄   😳   💷   🚠 💷 💷 💷	018			
Service Types	Properties	Creation Date	Last Discovered		
_haptcp.local	c#=3 ci=2 ff=0 id=0E:E6:9C:88:F9:66 md=SchnuffelBridge pv=1.1 s#=1 sf=0	23.02.2022, 11:56:31	24.02.2022, 11:03:24		
_httptcp.local		23.02.2022, 12:07:31	23.02.2022, 12:07:31		
_httptcp.local	path=/config/authentication_page.htm	23.02.2022, 11:56:32	24.02.2022, 11:03:24		
_nvstream_dbdtcp.local		23.02.2022, 11:56:32	24.02.2022, 11:03:20		
_nvstream_dbdtcp.local _teamviewertcp.local	DyngateID=647654641 Token=MoMfz3zKkSOqLPPS UUID=b113674c-514d-421f-b898-4d28c49	24.02.2022, 10:17:09	24.02.2022, 10:41:05		
_sshtcp.local		23.02.2022, 11:56:23	24.02.2022, 11:02:46		
Total 7 devices   1 device s	selected				

Figure: Unknown mDNS Devices Report

The service types and properties, including the values they contain, do not always allow a clear assignment to device type, model and manufacturer.

4.16.3.2 Unknown UPnP Devices Report

The UPnP protocol returns more structured data compared to the mDNS protocol. Because of this, creating rules for the UPnP protocol is easier.

Common attributes are Manufacturer, Model Name, Model Description, Model Number and Service Types as shown in the next screenshot.

J	Unknown UPn	P Devices						
	$ \Rightarrow   \leftarrow \rightarrow \diamondsuit   \textcircled{a}   \textcircled{b}   \textcircled{a} [ \textcircled{b}   \textcircled{a}   \textcircled{b}   \textcircled$							
	Filter:							
	Case sensitive filter							
	Manufacturer	Model Name	Model Description	Model Number	Service Types	Locations	Crea	
	AVM Berlin	FRITZ!WLAN Repeater 1750E	FRITZ!WLAN Repeater 1750E	av m	upnp:rootdevice urn:schemas-any-com:service:fritzbox:1 urn:schemas-upnp-org:device:fritzbox:1	49000/fboxdesc.xml	25 Fe	
	Total 1 device	1 device selected						
					Close			

Figure: Unknown UpnP Devices Report

Consequently, it can happen that devices for which the UPnP protocol is successful (but no rules exist) are displayed as *Unidentified Device* but model and manufacturer are set.

J	Devices with	Discovery Status	'Success'							
1	# ← →     →     →     ▲									
	Filter:	sensitive filter								
	Name	IP Address	Manufacturer	Туре	Model	OS Version	Patch Level	FW Version	Serial Number	La
	fritz.repeater	192.168.32.21	AVM	Unidentified Device	FRITZ!WLAN Repeater 1750E					25
	fritz.repeater	192.168.32.23	AVM	Unidentified Device	FRITZ!WLAN Repeater 1750E					25
	Total 2 devices	0 devices select	ed							
					Close					

Figure: Unidentified UPnP Devices

The *Devices with Discovery Status 'Success'* report shows two UPnP capable devices that have no rules yet.

#### 4.16.4 Ignoring Personal Devices In Home Office Environments

Due to the detection of mDNS and UPnP devices, it may now happen that companyowned and personal devices are included in the company inventory.

To avoid mixing corporate and personal devices, the discovery of mDNS and UPnP enabled devices can be automatically disabled when computers are connected to a corporate VPN in a home office environments.

D Discovery Configuration	×
General Scope Directory Data Collection Discovery Jobs Protocols Filters Cloud SSH Keys	
Standard Software Virtualization Exchange Server Database Support Entitlements Custom File Collection Policies	
If users work from home with privately owned devices (e.g. monitors, UPNP and mDNS enabled devices), these can be added to the database during scanning. To avoid this, the discovery can ignore such devices when a notebook or desktop is connected to the corporate network via VPN.	
Ignore directly attached, mDNS and UPnP enabled devices when connected via VPN	
Ok Cancel	

Figure: Discovery Configuration Data Collection Policies

The new '*Don't discover...'* policy setting is enabled by default and avoids mixing corporate and personal devices in the inventory.

# 5 Discovery Configuration

The discovery configuration chapter explains the *Discovery Configuration* dialog in detail. Open the *Discovery Configuration* dialog from *Discovery » Configuration*.

The *Discovery Configuration* consists of eight tabs:

- The *General* tab allows to configure the maximum number of devices being discovered concurrently, global DNS discovery options, ARP cache reading, and ignoring recently discovered devices.
- Use the *Scope* tab to configure IPv4 networks, IPv4 ranges, IPv6 networks, Windows network neighborhood objects and directories. Create new groups and configure default accounts for SNMP, telnet and SSH.
- Configure DNS domain controllers and credentials in the *Directory* tab.
- The *Data Collection* tab allows choose what objects (hardware and software) JDisc Discovery should discover.
- The *Discovery Jobs* tab allow creating, deleting and configuring discovery jobs including directory synchronization options. Discovery Jobs can also be scheduled.
- Use the *Protocols* to enable and disable protocols, configure protocol timeouts and retries.
- Make use of the *Filters* tab to restrict the discovery on selected device types and exclude IPv4 address ranges.
- Import SSH keys to access devices from the SSH Keys tab.

# 5.1 General Tab

The general tab hosts these global discovery settings:

- The max. number of devices being discovered concurrently. JDisc Discovery can discover devices concurrently speeding up the discovery process. Discovering devices concurrently increases network utilization.
- The timeout to abort discovery of devices that do not respond to JDisc Discovery's discovery.
- *Discover DNS domain controllers* is useful for corporate networks running Active Directory. If turned on, JDisc Discovery also discovers DNS domain controllers and DNS domains when discovering Windows computers. This way JDisc Discovery can find unknown Active Directories on the network.
- *Discover DNS servers*, if turned on, also discovers DNS servers based on DNS domain names of discovered devices. Turn on this option if you are interested in what DNS servers exist on the network.
- Discover devices found in ARP caches of routers and switches enables JDisc

Discovery to find IP addresses by reading ARP cache entries of routers and switches. Every device running TCP/IP does have an ARP cache. The ARP cache maps MAC addresses to IP addresses. Routers typically have high numbers of IP addresses in their ARP caches and are a good source to find devices on the network.

• Jumphost configuration for improved device and manufacturer identification. JDisc Discovery can use jump hosts to identify a device's mac address using the ping and arp command on the jumphost.

D Discovery Configuration
General Scope Directory Data Collection Discovery Jobs Protocols Topology Jobs Filters Cloud SSH Keys
General
JDisc Discovery discovers devices in parallel to speed up the discovery process. Adjust the maximal number of parallel discovered devices according your network speed.
Discover not more than 10 🚖 devices in parallel
Ping networks and IP ranges with 4 🔿 threads in parallel
Abort device discovery when inactive for more than 60 🚔 minutes
Find New Devices
Discover DNS domain controllers
Discover DNS servers
Discover devices found in ARP caches of routers and switches
Device Naming
Set device name and Normal (no changes) 🗸
Aging Out
Age out devices after 40 + day(s)
Age out JDisc Discovery application events after 60 🖨 day(s)
Track device deletion
- Jumphost for improved Device and Manufacturer Identification
JDisc Discovery automatically selects a Jumphost server or client for every remote network.
Enable remote ARP Jumphost
Max. Jumphost worker threads for each remote network 5 🚖
Ok Cancel

Figure: Discovery Settings General Tab.

# 5.2 Scope Tab

The Scope tab allows

- Configuring groups including sub-groups
- Assigning IP networks, IP ranges, Windows network neighborhood objects and

directory objects to groups

• Assigning default credentials to a group

Chapter 3.3 explains JDisc Discovery's grouping concept.

Create groups and sub-groups to fit your need and configure the discovery scope and default credentials.

# 5.2.1 Scope Tabs

This section explains the sub-tabs within the *Scope* tab.

#### 5.2.1.1 Properties

The *Properties* tab allows changing a group's name and description.

Discovery Configuration	tion Discovery Job	as Protocols Filters SSH Keys	x
Company EMEA France Germany Cologne Munich	Properties I Name Description	Pv4Networks IPv4Ranges IPv6Networks SNMP Accounts Berlin	



#### 5.2.1.2 IPv4 Networks

The *IPv4 Networks* tab displays IPv4 networks belonging to the selected group. Enable IPv4 networks (indicated with the check mark) to ping all IP addresses in the network when running a discovery job. Devices will be assigned to selected groups regardless if IPv4 networks are enabled or disabled for discovery.

Use the context menu or the buttons to

- Enable (using ping), enable (using all protocols) or disable network discovery
- Add new networks
- Browse existing networks
- Remove networks
- Import networks

IP network numbers are not easy to understand, especially in large corporate and enterprise networks that are comprised of hundreds to thousands IP networks. JDisc Discovery allows naming networks. Select a network and enter a name in the name column.

JDisc Discovery uses ping in order to find active addresses. However, some networks or servers might block ICP ping requests. Devices which do not reply to ping do not appear in the database. In this cases, you might enable the network discovery using all protocols. JDisc Discovery will then use all protocols (e.g. WMI, HTTP, HTTPS, SMB, SSH, telnet...) in order to find active devices. A black square in the checkmark's upper left area indicates that a full protocol scan is used.

eral Scope Directory Data	a Collection   Discovery Jobs   Protocols	Topology Jobs   Filters   SSH H	eys			
Company		IDud Naturalia III. 4 P				
L Erance	Properties Device History	IPV4 Networks IPV4 Ranges	IPv6 Networks   Network	Neighborho	od   Directory   SNMP   Accou	unts
. Germany	Filter:					Enable
						Citable
	Case sensitive nit	er				Ping all Protocols
						Disable
	means: use only ping	to find active devices	Sanathu alauwan tihana minainan	TD=)		
	Thearis: use all protoco	ois to find active devices (signi	icanuy slower trian pinging.	IPS)		Add
	Network Address	Subnet Mask	Name		Last Discovered	Browse
	TVEWORK Address	200101010	Name		Last Discovered	Remove
	111.0.0.0	255.0.0.0				
	111.0.0.0	255.0.0.0 255.255.0.0				Import
	111.0.0.0 134.170.0.0 157.55.0.0	255.0.0.0 255.255.0.0 255.255.0.0				Import
	111.0.00 134.170.0.0 157.55.0.0 157.56.0.0	255.0.0.0 255.255.0.0 255.255.0.0 255.255.0.0				Import
	111.0.00 134.170.0.0 157.55.0.0 157.56.0.0 168.63.0.0	255.0.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0				Import
	111.0.0.0 134.170.0.0 157.55.0.0 157.56.0.0 168.63.0.0 169.254.0.0	255.0.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0				Import
	111.0.0.0 34.170.0.0 57.55.0.0 55.56.0.0 58.30.0 169.254.0.0 73.194.0.0	255.0.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0				Import
	111.0.0.0 134.170.0.0 157.55.0.0 157.55.0.0 158.63.0.0 169.254.0.0 173.194.0.0 178.255.0.0	255.0.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0				Import
	111.0.0 134.170.0.0 157.55.0.0 157.55.0.0 157.55.0.0 158.63.0.0 169.254.0.0 173.194.0.0 178.255.0.0 191.234.0.0	255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0				Import
	111.0.0.0 134.170.0.0 157.55.0.0 157.55.0.0 158.53.0.0 169.254.0.0 173.194.0.0 173.255.0.0 191.234.0.0 192.165.0.0	255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0				Import
	111.0.0 134.70.0.0 157.55.0.0 157.55.0.0 157.55.0.0 159.254.0.0 173.194.0.0 173.255.0.0 191.234.0.0 192.168.6.0 192.168.6.5.0	255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0		N		Import
	111.0.0 134.170.0.0 157.55.0.0 157.55.0.0 159.254.0.0 173.194.0.0 178.255.0.0 191.234.0.0 192.168.0.0 192.168.137.0	255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0				Import
	111.0.0.0 134.170.0.0 157.55.0.0 157.55.0.0 157.55.0.0 158.63.0.0 169.254.0.0 173.194.0.0 173.255.0.0 191.234.0.0 192.168.0.0 192.168.57.0 192.168.177.0	255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0 255.255.0 255.255.0 255.255.0 255.255.0		<u>∑</u> s	Feb 29, 2016 12:55:05 PM	Import
	111.0.0 134.170.0.0 157.55.0.0 157.55.0.0 157.55.0.0 157.55.0.0 157.55.0.0 157.55.0.0 159.254.0.0 173.194.0.0 173.255.0.0 191.234.0.0 192.168.65.0 192.168.65.0 192.168.177.0 ✓ 192.168.177.0	255.0.0. 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.0.0 255.255.250.0 255.255.255.0 255.255.0 255.255.0		ß	Feb 29, 2016 12:55:05 PM	Import

Figure: IPv4 Networks Tab

Using all protocols to find active devices takes significantly longer than simply pinging a network.

Enter a name in the network table's name column.

#### 5.2.1.3 IPv4 Address Ranges

The *IPv4 Ranges* displays IP4 address ranges belonging to the selected group. Enable IPv4 address ranges (indicated with the check mark) to ping all IP addresses in the network range when running a discovery job. Devices will be assigned to selected groups regardless if IPv4 address ranges are enabled or disabled for discovery.

Use either the context menu or the buttons to

- Enable or disable address ranges
- Add new address ranges
- Browse existing address ranges
- Remove address ranges

• Import address ranges

JDisc Discovery allows naming IP address ranges. Select an address range and enter a name in the name column.

Brai Scope Directory Data C	ollection Discovery Jobs Protocols	Filters SSH Keys			
Company	Properties IPv4 Networks	IPv4 Ranges IPv6 Networks	SIMP Accounts		
Germany	Filter:				Enable
Berlin	Case sensitive fi	lter			Disable
	From Address	To Address	Name	Last Discove	Add
	192.168.180.0	192.168.180.53			Browse
					Change
					Remove
					Import
					Import IPs





#### 5.2.1.4 IPv6 Networks

The *IPv6 Networks* displays IPv6 networks belonging to the selected group. IPv6 networks cannot be enabled for discovery. There is because the address range of an IPv6 network can become huge and there would be no point to ping all addresses in the range. However, devices having IPv6 addresses that are in the scope of configured IPv6 networks will be assigned to the selected group.

Use the context menu or the buttons to

- Add new networks
- Browse existing networks
- Remove networks
- Import networks

IP network numbers are not easy to understand, especially in large corporate and enterprise networks that are comprised of hundreds to thousands IP networks. JDisc Discovery allows naming networks. Select a network and enter a name in the name column.

eral Scope Directory Data Collec	ction   Discovery Jobs   Prote	ocols Filters SSH Keys			
Company Lefter Emergence	Properties IPv4 Net	vorks IPv4 Ranges IPv6 Netwo	rks Network Neighborhoo	d Directory SNMP Accounts	]
🖃 🔔 Germany	Filter:				Add
Erlin	Case sensi	tive filter			Browse
Client Network	Network	Name			Remove
					Import
UK					Import

Enter a network name in the network table's name column.

#### 5.2.1.5 Network Neighborhood

The *Network Neighborhood* tab displays Windows network neighborhood objects belonging to selected groups. Enable Windows network neighborhood objects (indicated with the check mark) to discover member computers. Computers will be assigned to selected groups regardless if Windows network neighborhood objects are enabled for discovery.

Windows network neighborhood discovery depends on the Computer Browser service that maintains an updated list of computers on the network. If the Computer Browser service is stopped or disabled, Windows network neighborhood discovery will not work properly. To resolve computer names to IP addresses the Windows Internet Naming Services (WINS) must be installed and configured.

Use the context menu or the buttons to

- Enable or disable Windows network neighborhood objects
- Add new Windows network neighborhood objects
- Browse existing Windows network neighborhood objects
- Remove Windows network neighborhood objects
- Import new Windows network neighborhood objects from file
- Configure administrative credentials for Windows network neighborhood objects

Click *Update* to display Windows network neighborhood objects available on the computer running JDisc Discovery.

eneral Scope Directory Data Collect	tion Discovery Jobs Protocols	Filters SSH Keys		
Company EMEA France Granny Germany France Germany Company	Properties IPv4 Networks Filter:	IPv4Ranges IPv6 Networks 1	Network Neighborhood Directory SNMP	Accounts Enable
Jug Client Network	Name V DISC MSHOME TSTDOM1 TSTDOM2 TSTDOM3 TSTDOM4	Account JDISC \ADMIN TSTDOM3\Administrator	Last Discovered	Update Add Browse Remove
	TSTDOM5 TSTDOM5 TSTDOM6 TSTDOM7		Mar 4, 2014 5:25:22 PM	Change

Figure: Network Neighborhood Tab

Enter administrative credentials for selected Windows network neighborhood objects to improve discovery results.

The Windows Internet Naming Services (WINS) must be installed and configured for the Windows network neighborhood discovery to function properly.

## 5.2.1.6 Directory

The *Directory* tab displays the directories hierarchy. The directories hierarchy serves two purposes:

- Associate directory objects to a group
- Configure login credentials with directory objects. JDisc Discovery's discovery uses these login credentials to access computers that are member of a directory

To enable directory discovery:

- Select a group
- Select directory objects, open the context menu and choose any of the flowing options:
  - Discover all computers of the selected directory object.
    - This requires only access to one Global Catalog (GC) server/service.
  - Discover all computers of the selected directory object and all sub-directory objects.
  - Discover recently logged-on computers of the selected directory object.

This requires access to DNS Domain Controllers (DC) of the respective DNS domain. To cover all logged-on computers, make sure all DNS Domain Controllers (DC) are configured (either manually or automatically discovered).

Discover recently logged-on computers of the selected directory object and all sub-directories.

You can also use the *Toggle* or the *Space* key to toggle between these discovery modes

Discover all computers of the selected directory object.

This requires only access to one Global Catalog (GC) server/service.

- Discover all computers of the selected directory object and all sub-directory objects.
- Discover recently logged-on computers of the selected directory object.

This requires access to DNS Domain Controllers (DC) of the respective DNS domain. To cover all logged-on computers, make sure all DNS Domain Controllers (DC) are configured (either manually or automatically discovered).

Discover recently logged-on computers of the selected directory object and all sub-directories.

Click *Change Account* to configure administrative login credentials for selected directory objects. Directory object's having login credentials display the user name in brackets next to the directory object's name.

Figure: Directory Object with Login Credentials

#### 5.2.1.7 SNMP

The *SNMP* tab displays default SNMP communities and SNMP accounts for the selected group. The *SNMP* tab is divided into the *SNMPv1/v2c communities* and *SNMPv3 accounts* panels.

JDisc Discovery uses SNMP protocols and default SNMP communities/accounts in this order when accessing a device:

- 1. SNMPv3 accounts in the order as they appear in the SNMPv3 accounts panel
- 2. SNMPv1/v2c communities in the order as they appear in the SNMPv1/v2c *communities* panel

When an SNMPv3 account or SNMP v1/v2 community succeed, JDisc Discovery associates and stores the account or community with the device. JDisc Discovery will not try default SNMP accounts or communities in subsequent discoveries but uses the associated SNMP account or community. Only if these fail, default SNMP accounts and communities will be tried again.

Discovery Configuration						×
General Scope Directory Data Collectio	n Discovery Jobs Protocol	ls Filters SSH Keys ks IPv4 Ranges IPv6	Networks Network	k Neighborhood   Dire	ectory SNMP Act	counts
Germany Germany Cologne Client Network Munich UK	SNMPv1/v2c Communit Community public secret topsecret Total 3 SNMP commun SNMPv3 Accounts	nities   0 SNMP communi	ties selected			Add Remove Move up Move down
	User name admin	Password	Auth, protocol SHA	Privacy password	Priv. protocol AES128	Add Remove Modify Move up Move down
	Total 1 SNMPv3 acco	unt   0 SNMPv3 account	III s selected		4	
		Ok	Cancel			

Figure: Default SNMPv1/v2c Communities and SNMPv3 Accounts

Use *Add* to add new SNMP v1/v2 communities and SNMPv4 accounts in the respective panel. Click *Remove* to delete communities and accounts. Use *Move Up* and *Move Down* to change the order of communities and accounts.

#### 5.2.1.8 Accounts

The *Accounts* tab displays default login credentials for computers running Windows, Unix and MAC OS X. Depending on the protocol configuration (remote login with telnet, or SSH) you might need to configure default SSH login credentials based on public/private keys.

Discovery Configuration					Σ	
General Scope Directory Data Collection Disco	overy Jobs Protocols Topo	ology Jobs Filters	SSH Keys			
Company Company Company Propu Company Compo	erties Device History IPv-	4 Networks   IPv4 Ra	nges   IPv6 Netw wn devices	orks SNMP Accounts		
Ci	Clients & Servers Interconnect Devices           Windows         HP-UX         Oracle Solaris         IBM ADX         Linux/Oracle VM         VMware ESX/VCenter         Clirix XenServer         FreeBSD         Mac OS X					
	Use the defat possible. Oth read more	ult accounts for Wind erwise, you risk that	ows only, if the co the accounts get	onfiguration via the network neighborhood or locked or that intrusion detection systems crea	the directory is not te alarms!	
	User name	Password	Туре	Comment	Add	
	administrator administrator	V	root/enable root/enable	admin account for workgroup1 in france admin account for workgroup2 in france	Remove Change Move up Move down	
	Total 2 Accounts   0 Acc	counts selected				
		Ok	Cancel			

Figure: Default Accounts

This dialog might vary depending on the licensed edition.

Use the list of Windows default accounts only if the configuration via network neighborhood or organizational units from the directory do not succeed.

Click *Add* to add new login credentials including public/private keys. Specify if the login credentials hold root or ordinary user privileges. If in doubt, choose *user*. JDisc Discovery Checks – if needed - if login credentials hold root privileges during the discovery process.

Account	
User name	root
Account type	root/enable 👻
Password	••••

Figure: Add new Default Account

Use Add in the public/private key panel to add new login credentials for SSH.

Import SSH public/private keys for use as default credentials in the *Public/Private Keys* panel. Refer to section 5.9 for more information on how to import SSH keys.

ser name		
Account type user 👻		
elect a SSH to use with this account	•	
ilter:		
Case sensitive litter		
Name	Туре	Passphrase
Discovery User Key	RSA	

Figure: Add new public/private Key Account

# 5.2.2 Root Group

The root group (named 'Company') is created by JDisc Discovery's installation program and contains all IPv4, IPv6 networks, all IPv4 ranges, all Windows network neighborhood objects and all directory objects. You cannot delete the root group but you might change its name from the root group's property tab. Networks, address ranges, Windows network neighborhood objects and directory objects that have been created in subgroups also appear in the root group.

The root group is associated to the 'Discover all' discovery job, which always exists. Whenever you select *Discovery* » *Control* » *Start Discovery* and have not created

additional discovery jobs, JDisc Discovery starts the 'Discover All' discovery job. This way JDisc Discovery discovers all enabled IPv4 networks, IPv4 address ranges, Windows network neighborhood objects and directory objects.

# 5.2.3 Sub Groups

Create new subgroups as described in the grouping section 3.3. Depending on the sub group type, JDisc Discovery displays different tabs:

- Network groups include the *Properties*, *Networks*, *Ranges*, *SNMP* and the *Accounts* tabs.
- Windows network neighborhood groups include *Properties* and the *Network Neighborhood* tabs.
- Directory groups include *Properties* and the *Directories* tabs.

# 5.3 Directory Tab

The *Directory* tab displays directories (by DNS domain) and DNS domain controllers for each directory. JDisc Discovery automatically detects directories and associated DNS domain controllers using the Server Message Block (SMB) protocol. Directories can also be added indirectly by adding and configuring a DNS domain controller and login credentials.

# 5.3.1 Configure Directory DNS Domain Controller

To synchronize directory information and networks, a directory must be configured having at least one DNS Domain Controller and login credentials to run Lightweight Directory Access Protocol (LDAP) queries. To configure a DNS Domain Controller and login credentials:

- Open the Discovery Configuration dialog from Discovery » Configuration.
- From the *Discovery Configuration* dialog, choose the *Directory* tab and select a directory by DNS Domain from the *DNS Domains* panel.
- If the *DNS Domain Controller* panel is empty, click *Add* to add a DNS Domain Controller and login credentials for the selected DNS Domain.

If the local computer running JDisc Discovery is a member of a directory, the *Add DNS Domain Controller* dialog always defaults to a DNS Domain Controller for this directory.

If you have selected a directory different from the local computer's directory, override the DNS Domain Controller as appropriate.

- If the DNS Domain Controller panel contains at least one host name, click Change to open the Directory Service Account dialog and enter login credentials for the directory's DNS Domain Controllers.
- Finally click *Test* to test the connection to all configured DNS Domain Controllers for the directory.

# 5.4 Data Collection

The data collection tab specifies what details to discover from devices, defines custom scripts used for software data collection and defines a set of simplified file collections for various devices.

## 5.4.1 Standard Data Collection

The *Data Collection* tab allows choosing what details to discover from devices on the network.

Discovery Configuration			X					
General Scope Directory Data Collection	Discovery Jobs Protocols Filters SSH K	leys						
Standard Custom File Collection								
User / User Groups								
Discover user groups								
Discover users								
☑ Delete users from logged on user history when not logged on for 30 → day(s)								
Detect remote connections via	RDP, SSH or telnet							
Create new devices for us	er connections from remote devices 🛛 🔞							
Discover remote clients								
Software/Hardware	Discover executable files	Discover dicks	Discover TPM modules					
	Discover executable files							
Discover patches	Discover memory	Discover blade enclosure components	Discover monitors					
Discover services	Discover video controllers	Discover managed devices						
Discover drivers	Ulscover cluster							
		V Discover shares	V Discover card reader					
Use pargs on solaris								
	Ok	Cancel						

#### 5.4.1.1 Users

JDisc Discovery's user discovery distinguishes

- Local users that exist locally on a computer
- Logged on users that have been logged on to a computer at the time of the discovery

JDisc Discovery stores users that have been logged on to a computer for a configurable period. Use the 'Delete users from logged on user history when not logged on for <n> days' option to automatically delete users from the logged on user history when they have not logged on for the designated number of days.

Change the selection for ignored users to suppress built-in and service users.

Terminal services client sessions (either Windows RDP or Citrix ICA) can be detected when the 'Find terminal services clients' option is enabled and Windows remote login is also enabled. Moreover, JDisc Discovery also detects client computers from which terminal services session has been established. Enable the 'Discover terminal services clients' option to automatically discover terminal services client computers.

Terminal services client detection requires the Windows remote login protocol.

When discovering locally attached devices such as USB printers, scanners or card readers, JDisc Discovery takes the device type filters into account. So JDisc Discovery will not discover local printers, when printers are disabled within the type filters even if the discovery for local printers is enabled.

#### 5.4.1.2 Software/Hardware

Enable or disable any of the items below as appropriate:

- Applications / license keys
- Patches
- Services<sup>7</sup>
- Drivers
- Processors
- Memory modules
- Video controller<sup>8</sup>

<sup>7</sup> For Windows and Solaris

<sup>8</sup> For Windows and Linux

- Clusters (Microsoft, HP, and Veritas clusters)
- Physical, logical disks and disk partitions
- Attached devices (for example printers attached to print servers or monitors attached to a computer<sup>9</sup>)
- Blade enclosure components (for example blade servers or blade switches)
- Managed devices (such as servers managed by a server management processor)

Disable data collection items that you do not need. This saves database disk space, reduces network traffic and speeds up discovery jobs.

# 5.4.2 Virtualization Data Collection

Use the Virtualization tab to configure the details for scanning virtual environments.

Configure whether to scan offline instances, VMware annotations and virtual machine motion events.

Discovery Configuration	
eneral Scope Directory Data Collection Discovery Jobs Protocols Topology Jobs Filters SSH Keys	
Standard Virtualization Exchange Server Custom File Collection	
V Discover virtual instances	
☑ Discover offline instances	
V Discover VMware annotations	
Discover motion events	
Collect motion events for the last 90 🜩 days	
Purge older motion events	
Ok Cancel	

Figure: Virtualization Data Collection

<sup>9</sup> Monitor discovery is supported only on Windows

# 5.4.3 Exchange Server

JDisc Discovery can collect detailed information for Microsoft Exchange server. It runs Powershell scripts on the target computer in order to retrieve the list of exchange mailboxes with their sizes.

Discovery Configuration
General Scope Directory Data Collection Discovery Jobs Protocols Filters SSH Keys
Standard Virtualization Exchange Server Database Custom File Collection
V Discover exchange malboxes
Powershell script execution timeout 30 🔶 minutes
Ok Cancel

Figure: Exchange Server Discovery Configuration

## 5.4.4 Database Discovery

JDisc Discovery can collect detailed information for several databases. Use the *Database* tab in order to configure the collectibles for databases.

Timeout IBM IDE2 database connect timeout D S seconds Mororoft SQL Server database connect timeout My/SQL Maristil database connect timeout D S seconds Portgres connect timeout D S seconds Postgres connect timeout D S seconds	ral   Scope   Directory   Data Collection   g andard   Witualization   Exchange Server Settings	overy Jobs   Protocols   Filters   SSH Keys   atabase   Quatom   File Collection	
	Timeout IBM DB2 database connect timeout SAP MaxDB connect timeout Microsoft SQL Server database connect to Microsoft SQL Server database connect timeout Orade database connect timeout Postgres connect timeout	10 ⊕ seconds       30 ⊕ seconds	

Figure: Database Discovery Settings

# 5.4.5 Custom Data Collection

The *Custom* tab allows configuring the custom data collection.

Ustom Attributes			
ustom Software Data Collection			
Platforms			
All Windows versions			
Windows NT 4.0	Windows Server 2008		
Windows 2000	Windows 7		
Windows 2000 Server	Windows 8		
Windows XP	Windows Server 2012		
Windows Server 2003			
Windows Vista			
			Add
Data Collection     Execute 'Unix Custom Collection	Script' for Sup Solaris, MAC OS X. Linux, IBM AD	(	Fashla
Execute 'Software Collection Scr	of for Windows	•	Disable
			Disable
			Reset
Total 2 collections 1.1 collection color	ed		

Figure: Custom Data Collection Configuration

# 5.4.6 File Collection

JDisc Discovery can collect configuration files or command outputs from system commands from various operating systems. When the network add-on is installed, JDisc Discovery even collects configuration files from various routers and switches.

D Discovery Configuration           General         Scope         Directory         Data Collection         Discovery Job           Standard         Custom         File Collection         Discovery Job	bs Protocols Filters SSH Keys		×
Windows	Filter:		bbA
	Case sensitive filter		Remove
	Name	Command	Change
	winfo command	/usr/sbin/hwinfo	Enable
			Disable
	Total 1 collection   0 collections	selected	•
	Ok	Cancel	

Figure: File Collections

Select an operating system platform and click *Add* to add new file collection. Refer to chapter 11 for more details on the file collection mechanism.

# 5.5 Discovery Jobs

Discovery jobs provide a means to partition the discovery of large enterprise networks. Refer to chapter 3.4 for a detailed description of scheduled discovery jobs.

Discovery Configuration		x	
General Scope Directory Data Collection Discovery Jobs Protocols Filters SSH Keys			
Discovery Name		_	
Discover all Discover San Francisco Site	Properties Groups Directory Schedule		
	Name Discover San Francisco Site Description	-	
۰ III ا			
	Ok Cancel		

Figure: Discovery Jobs Tab

The 'Discover all' discovery job is created by JDisc Discovery's installation program and is permanently associated to the root group. You cannot change the group assignment or delete this discovery job. However, you might change the directory synchronization options or and define a schedule.

Create new discovery jobs by using the context menu in the left panel.

- Enter a name and description in the New Discovery Job dialog and click Ok.
- Select the new discovery job and adjust the discovery settings as needed.

Name	Discover San Francisco Site			
Description	Discover the San Francisco site during local business hours.			
	L			

Change a discovery job's settings in any of theses tabs:

- Change the discovery job name and description in the *Properties* tab.
- Use the *Groups* tab to associate groups to the discovery job. Groups define the discovery scope in terms of IP networks, IP ranges, Windows network neighborhood objects and directory objects.
- Choose directory synchronization options in the *Directory* tab.
- Schedule the discovery job from the Schedule tab

#### 5.5.1 Properties

The properties displays the discovery job name and a description.

Properties	Groups	Directory	Schedule	
Name	Disco	ver San Fra	ncisco Site	
Description	Disco	ver the San	Francisco S	Site during office hours

Figure: Properties Tab

#### 5.5.2 Groups

Groups define the scope of a discovery job. Discovery jobs can be associated to one or more groups.

The built-in discovery job 'Discover all' cannot be altered and therefore the *Groups* tab is disabled.

In the group tree, choose any of the options below:

- Enable to explicitly associate the selected group only.
- Enable Subgroup to associate the selected group including its subgroups.
- *Reset* to remove the association of the selected group and its subgroups.

S Company (*)	Enable
Golden Jacky (*)      Golden Jacky (*)	Enable Subgroup Reset

Figure: The Groups Tab

The check mark next to the group name indicates if a group is associated to a discovery job.

- Groups with black check marks 🗹 are explicitly enabled.
- Groups with a gray check mark 🗹 are implicitly enabled through one of their parent groups.
- Groups without check mark are disabled.
# 5.5.3 Directory

The *Directory* tab provides directory and networks synchronization options. When enabled, JDisc Discovery will synchronize directory objects and IPv4 networks from all (configured) directories when the discovery job is started.

Synchronizing IPv4 networks can also provide location information for each network when the directory administrator maintains network location information in the directory.



Figure: Directory Synchronization Options

# 5.5.4 Schedule

Every discovery job can be individually scheduled and runs independently from other (scheduled) discovery jobs. By default, discovery jobs are created set to *Not scheduled*. Not scheduled discovery jobs can be started manually from *Discovery* » *Control* » *Start Discovery*.

JDisc Discovery can run discovery jobs using any of the schedule types below:

- Run Once
- Daily
- Weekly

- Monthly
- Recurring
- 5.5.4.1 Run Once

Choose Run Once to run a discovery job only once at the specified date and time.

Properties	Groups	Directory	Schedule		
Schedule t	type Ru	in once	] -		
	-				
Date	3/5/10				
Time 7	7:00 PM 🗧				

Figure: Run Discovery once

#### 5.5.4.2 Daily

Choose *Daily* to run the discovery every day at the specified time. When a discovery runs longer than a full day the discovery job starts the next day at the specified time.

roperties Groups Directory Schedule
Schedule type Daily
Run every day at 12:00 PM 😓

### Fig: Run discovery daily

#### 5.5.4.3 Weekly

Choose *Weekly* to run a discovery job once every week. Specify the day and time when to start the discovery job.

Figure: Run Discovery weekly

### 5.5.4.4 Monthly

Choose *Monthly* to run a discovery job every month. Specify the day of the month and time when to start the discovery job.

Properties Gro	ups Directory	Schedule		
Schedule type	Monthly	•		
-				
Run on Mont	h's last day 👻			
At 12:0	00 PM ≑			

Figure: Run Discovery monthly

#### 5.5.4.5 Recurring

Choose *Recurring* to run a discovery job periodically. In addition to specifying the interval, you can also set the date and time when to run the discovery job for the first time.

Properties	Groups Directory	Schedule				
Schedule t	ype Recurring	•				
Run eve	ry 3 📥 day(s)	0 🔷 hour(s)	0 🌲 minute(s	s) 0 🔶 second	(s)	
First exe	cution at 3/5/10 4:00 PM					

Fig: Run recurring discovery

# 5.6 Protocols

The *Protocols* tab displays all available protocols employed by JDisc Discovery's discovery. You can enable and disable any protocol except of ICMP ping.

Change the timeout values as appropriate. Higher timeout values generally improve protocol detection but might also slow down the discovery process.

Disabling important protocols, such as SNMP or WMI might degrade the discovery result.

Disabled protocols and too low timeout values might affect the quality of the discovery result.

Discovery Drotocols	y   Data Collection   Discovery	Jobs Protocols Filters SH Keys	
Ping		2000 🔶 milliseconds 2 🔶 retries	
V DNS		2000 $\Rightarrow$ milliseconds 2 $\Rightarrow$ retries	
SNMP (v1/v2c/v3)		2000 — milliseconds 2 — retries	
VetBIOS		10 seconds	
SMB (Server Mess	age Block)	120 🔷 seconds	
WMI (Windows Ma	anagement Instrumentation)	120 🔷 seconds	
WBEM (Web Base	d Enterprise Management)	10 🕞 seconds	
Telnet banner par	sing	7000 🗇 milliseconds 🗸 Store unknown telnet banners in database	
HTTP based identi	fication	3000 — milliseconds	
HTTPS based iden	tification	5000 💭 milliseconds	
VMware VIM API		120 seconds	
Domoto Login			
Windows Unix & VN	Iware		
Windows Unix & VM	Iware Remote login method	Connect timeout Execute timeout	
Windows Unix & VM Platform Windows	Remote login method	Connect timeout     Execute timeout       5 + minute(s)     15 + minute(s)	
Windows Unix & VM Platform Windows WMI Tunneling	Remote login method Windows remote login 👻 Use tunnel when native acc	Connect timeout     Execute timeout       5 v     15 v       ess fails v	
Windows Unix & VM Platform Windows WMI Tunneling Registry Tunneling	Remote login method Windows remote login  Use tunnel when native acc Use tunnel when native acc	Connect timeout     Execute timeout       5 v     15 v       ess fails v     ess fails v	
Windows Unix & VM Platform Windows WMI Tunneling Registry Tunneling Agent uninstalls a	Remote login method Windows remote login v Use tunnel when native acc Use tunnel when native acc utomatically after an idle period	Connect timeout     Execute timeout       5 vminute(s)     15 vminute(s)       ess fails v       ess fails v       lof 0 vm/s0 and 1 vminute(s)	
Windows Unix & Vi Platform Windows WMI Tunneling Registry Tunneling Agent uninstalls a	Remote login method           Windows remote login           Use tunnel when native account           Use tunnel when native account           utomatically after an idle period	Connect timeout     Execute timeout       5 v     15 v       ess fails v     15 v       ess fails v     11 v       lof 0 v     1 v	
Windows Unix & V Platform Windows WMI Tunneling Registry Tunneling Agent uninstalls a	Remote login method Windows remote login  Use tunnel when native acc Use tunnel when native acc utomatically after an idle period	Connect timeout     Execute timeout       5 minute(s)     15 minute(s)       ess fails v     is minute(s)       is f 0 minute(s) and 1 minute(s)	

### Figure: Protocols Tab

This dialog might vary depending on the licensed edition.

JDisc Discovery's installation program configures defaults timeout values that should fit most corporate networks. If needed, you might change timeout values if these do not accommodate to your network and systems.

### 5.6.1 Windows Computers

JDisc Discovery's Windows remote login agent is a Windows service that is temporarily deployed to target Windows computers from the JDisc Discovery server. The JDisc Discovery server communicates with the agent using a Windows named pipe which is restricted to members of the local administrators of the computers running the agent. Furthermore all named pipe communication is compressed and securely encrypted. The remote login agent automatically uninstalls after a configurable idle period when it has not been accessed by a JDisc Discovery server. When you periodically re-discover your network, set the idle period to a value longer than the discovery schedule so that the agent is still running when JDisc Discovery discovers it the next time. This way you can increase the discovery speed and reduce network traffic.

### 5.6.1.1 WMI And Remote Registry Protocol Tunneling

When firewalls block WMI or remote registry traffic, JDisc Discovery's WMI and remote registry tunneling feature can improve the discovery result. When tunneling is enabled, JDisc Discovery tunnels WMI and registry requests through its remote login agent. Native access refers to accessing a protocol without using the remote login tunnel.

JDisc Discovery offers these WMI and remote registry protocol tunneling options:

- 1. *Disabled*: JDisc Discovery does not use any tunneling.
- 2. Use always: The tunnel is always used no matter if native access succeeds or fails.
- 3. Use tunnel when native access fails: JDisc Discovery uses the tunnel only, if native access fails (e.g. when WMI is blocked by a firewall).
- 4. Use native access when tunnel fails: JDisc Discovery prefers using the tunnel and uses native access only when the tunnel fails.

Make sure to configure tunneling WMI and remote registry protocols via remote login when remote login for Windows is enabled!

# 5.6.2 Unix And Mac OS X Computers

Remote login is needed to properly discover Unix and Mac OS X computers. Refer to section 4.3 for more information on how to discover Unix computers.

Configure remote login for Unix and Mac OS X platforms in the *Remote Login* panel. JDisc Discovery can log-in using:

- Secure Shell (SSH)
- Telnet

Remote login provides these options:

- Remote login disabled
- Use telnet only
- Use SSH and then telnet
- Use SSH only

SSH logins in conjunction with too many default credentials can cause intrusion detection systems to raise alerts!

In few cases JDisc Discovery requires root access - for instance when reading BIOS information on Linux computers. Whenever possible, JDisc Discovery tries to avoid using root/administrative privileges. When root/administrator access is needed, JDisc Discovery offers three methods to execute commands with root/administrator privileges:

- Call the 'su' command to switch to the root user.
- Call 'sudo' to execute commands with root access.
- Call '.do' to execute commands with root access.

Specify the *Connect timeout* for establishing a connection and the *Execute timeout* for executing system commands. JDisc Discovery sends CTRL-C to abort command execution when running longer than the configured timeout value permits.

Configuring remote login for *Unknown* platforms is important for security-hardened systems. For instance, many Linux distribution disable telnet and SNMP per default. In such cases, JDisc Discovery cannot determine the operating system using agent-less protocols.

When remote login for *Unknown* devices is enabled and login credentials are configured (either individually assigned to the device or default credentials), JDisc Discovery logs to the system using telnet or SSH and executes the 'uname' command. JDisc Discovery parses the 'uname' command output to determine the operating system and finally utilizes the platform's login method to identify the device and to collect inventory information.

Enable remote login for *Unknown* devices to identify the operating system version of security-hardened systems.

# 5.6.3 Windows Computers

*Windows remote login* is an alternate method to discover device details on computers running:

- Windows NT 4.0 that do not have Windows Management Instrumentation (WMI) or proprietary vendor specific SNMP agent extensions installed.
- Windows NT 4.0 and better that have personal firewalls installed or firewalls on the network blocking DCOM/DCE RPC traffic.

*Windows remote login* requires administrative login credentials to push JDisc Discovery's zero-footprint remote execution agent on Windows computers that runs as a service and uses a named pipe (encrypted data transmission) to communicate with the JDisc Discovery server. JDisc Discovery's zero-footprint remote execution agent

offers SSH like functionally, such as command execution, command output capture and file transfer. JDisc Discovery's zero-footprint remote execution agent automatically deletes itself 60 seconds after being accessed last by a JDisc Discovery server.

# 5.7 Filters

JDisc Discovery can filter devices based on several device attributes and by IP address exclusion ranges. The discovery process only discovers and stores devices in the database that pass the filter criteria.

JDisc Discovery allows to create multiple filter configurations which are optionally being applied to only a part of the network (e.g. specific IP ranges or devices belonging to groups). Each filter configuration can be enabled or disabled separatley.

There are two basic filter types:

- IP exclusion filters exclude single IP addresses or IP ranges with IP exclusion filters.
- Attribute based filters exclude devices based on attributes such as model, manufacturer, type, os version.

Attribute filters can be restricted to specific IP ranges or device groups. Note that attribute based filters require the discovery of at least the identifying attributes such as model, type, or manufacturer.

There is a pre-defined IP exclusion filter called 'Built-in IP Filter'. This filter is being used for devices which are permanently excluded when deleted. The pre-defined filter cannot be removed.

iscovery Configuration neral   Scope   Directory   Data Collection   Discove reate, modify or delete device exclusion configuration	ery Jobs Protocols Topology Jobs Filters SSH Ker	YS	
Name Built-in IP Filter	Type IP Exclusion Filter	Scope Global Filter	Add Change Remove
			Clone

### Figure: Filter Tab

Use the Info button to display the filter definition.

There are two different filter types: IP exclusion filters and filters based on device attributes. There can be multiple filter configurations which can be enabled invidually.

# 5.7.1 IP Exclusion Filter

Create a new IP exclusion filter by clicking he *Add* button. Choose 'IP Filter' as filter type. The Wizard guides you through the filter definition which includes a name and description and on the second panel the list of IP filters.



Figure: Choose the Filter Type

IP Filters exclude devices by IP address ranges or single IP addresses. configurations which can be enabled invidually.

You might see multi-homed devices in reports having IP addresses within excluded IP addresses ranges. However this does not mean JDisc Discovery has accessed the IP address within the exclusion range!

# 5.7.2 Attribute Based Filters

Attribute based filters filter devices by matching device attributes such as model, manufacturer, type or operating system version. Click the *Add* button and select 'Attribute Filter' in order to create a new attribute based filter.



Figure: Create a new attribute based filter

A wizard guides you through the three steps of the filter configuration:

- define the filter name and optionally provide a description
- define the scope for the filter (either global, IP range, or device group)
- define the filter criterias for selected fields

The filter name and the description helps to identify filters.

lame	Ignore Cisco Devices in Server Network
Description	Ignores all Cisco devices in the IP range 192.168.178.0 - 192.168.178.255
	Back Next Finish Cancel

Figure: Define filter name and description

The next step defines the scope for the filter. Choose between

- the global scope (apply the filter to all IP ranges)
- the IP range based scope (apply the filter to devices which have an IP address that belongs to a specific IP range)
- the device group based scope (apply the filter to devices which have an IP address that belongs to the network list for a defined device group)

<ul> <li>Global Scope - apply t</li> <li>IP Range Scope - appl</li> <li>Device Group Scope -</li> </ul>	he exclusion rules to all devi ly the exclusion rules to a sp Apply the exclusion rules to	ces. ecific list of IP ranges.			
IP Range Scope - app. Device Group Scope -	ly the exclusion rules to a sp Apply the exclusion rules to	ecific list of IP ranges.			
Device Group Scope -	Apply the exclusion rules to				
1.170		devices which belong to specific ne	twork device groups.		
a in ranges where to ap	oply the filter.				
From IP	To IP	Name			Add
192.168.178.0	192.168.178.255				Remove
					Browse
					Import
Total 1 range   0 ranges	s selected				
			Back	Next N Finish	Cance

Figure: Define the Filter Scope

Use the filter scope to limit the filter to specific network areas.

Define the filter criteria in the last step. Define filter criteria for at least one field. When using filter criterias for multiple fields, then the device gets only filtered, if it matches the criterias for all fields.

Add Attribute based Filter Con     Exclude all devices which match the	figuration 📃 🔀
Oevice Attributes (*)     Name     Model     Manufacturer (*)     Type	Manufacturer =  Add Remove
	Conditions (Connected with OR)
	Manufacturer = 'Cosco'
	Total 1 condition   1 condition selected
	Back Next Finish Cancel

Figure: Define Filter Criteria

Click *Finish* to complete the filter defintion.

Using attribute based filters speeds up the discovery, lowers the network bandwidth usage and reduces the database size by ignoring devices which are not relevant for your inventory

JDisc Discovery creates discovery events when a device does not pass the attribute filter. This helps to troubleshoot filter issues.



Figure: Attribute Filter Events

# 5.7.3 Filter Information

Filter definitions can become complex. Use the *Info* button in order to display a filter definition overview.



Figure: Filter Configuration Summary

# 5.8 Cloud

Configure Microsoft Azure cloud access within JDisc Discovery once you have completed the preparation steps from the previous chapter. You will need:

- The so called tenant id. The tenant id might also be called directory id
- The application id
- The key secret

You can get the tenant id from the Azure portal within the Active Directory/Properties tab. The application id and the key secret is available from the your steps when you registered the application.

Enter the Azure cloud information in the configuration dialog.



Figure: Add access credentials for an Azure cloud directory

You might enter access credentials to more than one Azure cloud directory!

# 5.9 SSH Keys

JDisc Discovery supports using SSH (Secure Shell) public/private keys for login authentication. To use existing SSH keys for authentication on SSH enabled devices, import your SSH keys into JDisc Discovery's configuration.

Seneral Scope Directory Data Co	lection Discovery Jobs Pro	tocols Filters SSH Keys	
Case sensitive filter			Import Remove
Name	Туре	Passphrase	
Uncluvery User Ney	ACA		
Total 1 SSH key   0 SSH keys selecter	1		
		Ok Cancel	

Figure: Private Keys

Click *Import* to import existing private SSH keys. Private keys must use the OpenSSH format!

Private SSH keys are stored safely in JDisc Discovery's database. Refer to the 'Security' chapter of the 'Administration and Security Guide' for information on how JDisc Discovery stores login credentials.

Private SSH keys must use the OpenSSH format!

JDisc Discovery's reporting system provides a variety of built-in reports. Most reports display tabular data.

Tabular reports have a:

- Toolbar
- Filter field (including a case sensitive check box)
- Table header
- Content area
- Footer line

Case sensitive	filter				
Case sensitive	linter				
Name	IP Address	Manufacturer	Model	Туре	OS Version
rahinh-i	12,210,107,10	LEHOVO	HIIINFOURJ2	Laptop	WILLOWS AF FLOTESSIONAL
Desktop-1	12.216.104.46	Lenovo	ThinkCentre A51	Desktop	Windows XP Professional
Printer-2	12.216.106.180	Lexmark	T640	Printer	
		Samsung	SyncMaster	Monitor	
		Samsung	SyncMaster	Monitor	
3comtest	192.168.178.16	3COM	SuperStack 3 Switch 4300	Switch	
summit1	192.168.178.13	Extreme Networks	Summit 48i	Routing Switch	7.2.0
summit2	192.168.181.2	Extreme Networks	Summit 48i	Switch	7.2.0
summit3	192.168.181.3	Extreme Networks	Summit 48i	Routing Switch	7.2.0
Desktop-9	12.255.136.228	Dell	Studio Hybrid 140g	Desktop	Windows Vista Home Premi
ttrenz-PC2.fritz.box	192.168.178.75	Dell	Studio Hybrid 140g	Desktop	Windows Vista Home Premi
Desktop-7	12.251.240.215	Shuttle Inc	SS58V20	Desktop	Windows Server 2003 Ente
RackServer-3	12.251.240.0	Hewlett-Packard	rx6600	Server (Rack)	HP-UX B. 11.23U
RackServer-4	12.251.240.233	Hewlett-Packard	rx6600	Server (Rack)	HP-UX B. 11.23U
RackServer-5	12.251.240.16	Hewlett-Packard	rx2660	Server (Rack)	HP-UX B. 11.23U
RackServer-2	12.251.240.164	Hewlett-Packard	rx2620	Server (Rack)	HP-UX B. 11.23U
Switch-5	12.216.105.229	Hewlett-Packard	ProCurve 5308xl	Switch	E.11.03
ProCurve1	192.168.178.18	Hewlett-Packard	ProCurve 2650	Switch	H.08.72
Switch-6	12.251.240.162	Hewlett-Packard	ProCurve 2626	Switch	H.07.50
Switch-8	12.251.240.145	Hewlett-Packard	ProCurve 2626	Switch	H.08.54
Switch-10	12.251.240.219	Hewlett-Packard	ProCurve 2524	Switch	F.04.08
Switch-11	12.251.240.107	Hewlett-Packard	ProCurve 2524	Switch	F.04.08
Switch-7	12.251.240.182	Hewlett-Packard	ProCurve 2524	Switch	F.05.17
Switch-9	12.251.240.141	Hewlett-Packard	ProCurve 2524	Switch	F.05.50
192.168.178.7	192.168.178.7	Dell	PowerEdge T110 II	Server	VMware ESXi 5.0
•	111				4

Figure: A typical JDisc Discovery Device Report

Use the filter filed to only display lines that contain the filter value. The report filters its content as you type.

The tool bar provides these following icons:

Display the context menu

- Return to the previous report
- ➡ Go to the next report
- Reload the current report
- Den a new Window with the same report
- Create an Microsoft Excel export for the current report
- Create a CSV plain text export for the current report
- Schedule automatic report exports
- Show the SQL query that created the current report
- B Open the grouping tree view to restrict the report on groups

Table headers are in most cases sortable. Click on a header column to change the table's sort order.

The table footer displays the table's total number of lines, the number of selected, and filtered lines.

Use the right mouse button to open the context menu for the report. The context menu items depend on the actual report.

Case sensitive fi	lter				
Name	IP Address	Manufacturer	Model	Туре	OS Version
ւզիտի.լ	12,210,107,10	LEHUVU	HIIINFOURJ2	Laptop	WITHOWS AF FLOTESSIONAL
Desktop-1	12.216.104.46	Lenovo	ThinkCentre A51	Desktop	Windows XP Professional
Printer-2	12.216.106.180	Lexmark	T640	Printer	i and i a
		Sar 😑 Propertie	s N	Monitor	
		San	3	Monitor	
3comtest	192.168.178.16	3C(Discover	3 Switch 4300	Switch	
summit1	192.168.178.13	Ext Manage	•	Routing Switch	7.2.0
summit2	192.168.181.2	Ext		Switch	7.2.0
summit3	192.168.181.3	Ext Compare	•	Routing Switch	7.2.0
Desktop-9	12.255.136.228	Del Custom A	Attributes 🕨 🛛 140g	Desktop	Windows Vista Home Premi
ttrenz-PC2.fritz.box	192.168.178.75	Del	d 140g	Desktop	Windows Vista Home Premi
Desktop-7	12.251.240.215	Shi Connect	with 🕨	Desktop	Windows Server 2003 Ente
RackServer-3	12.251.240.0	Hev Travislast		Server (Rack)	HP-UX B. 11. 23U
RackServer-4	12.251.240.233	Hey	1001	Server (Rack)	HP-UX B. 11. 23U
RackServer-5	12.251.240.16	Hev 💢 Delete De	vices	Server (Rack)	HP-UX B. 11. 23U
RackServer-2	12.251.240.164	Hev		Server (Rack)	HP-UX B. 11. 23U
Switch-5	12.216.105.229	Hev 🖳 Create Su	pport ZIP 08xl	Switch	E.11.03
ProCurve1	192.168.178.18	Hewlett-Packard	ProCurve 2650	Switch	H.08.72
Switch-6	12.251.240.162	Hewlett-Packard	ProCurve 2626	Switch	H.07.50
Switch-8	12.251.240.145	Hewlett-Packard	ProCurve 2626	Switch	H.08.54
Switch-10	12.251.240.219	Hewlett-Packard	ProCurve 2524	Switch	F.04.08
Switch-11	12.251.240.107	Hewlett-Packard	ProCurve 2524	Switch	F.04.08
Switch-7	12.251.240.182	Hewlett-Packard	ProCurve 2524	Switch	F.05.17
Switch-9	12.251.240.141	Hewlett-Packard	ProCurve 2524	Switch	F.05.50
192.168.178.7	192.168.178.7	Dell	PowerEdge T110 II	Server	VMware ESXi 5.0
•					4

### Figure: Report Context Menu

Use copy-paste to copy report content to the clipboard.

# 6.1 Built-in Reports

JDisc Discovery offers a variety of predefined reports for all discoverable objects and diagnostic information.

# 6.1.1 Devices

The *Devices* menu contains device oriented reports. Devices can be grouped by

- Model
- Туре
- Manufacturer
- Operating system family and version
- Device roles and groups.

Double click a device to display device details.

6.1.1.1 Directory Membership

The 'Explorer-like' Computer Accounts (Devices » Directory menu item) report displays

- Active Directory instances (including the directory hierarchy) in the left navigation panel
- Directory member computers / accounts on the right side

When you select the *Include computer accounts from sub directories* option, all computer accounts of the selected directory object and sub directory objects will be displayed.

Figure: Directory Computer Accounts

Note: The two numbers in parentheses next to the directory object name indicate

- · number of computer accounts that exist in the directory
- number of computers / devices that have been discovered and matched against existing computer accounts.

When the parentheses contain only a single number the directory object and none of its sub directory objects have been discovered. However a computer / device that is member of the directory objects or any of its sub directory objects has been discovered and assigned to the directory.

# 6.1.2 Virtualization

The Virtualization menu item contains virtualization related reports including host servers and virtual instances.

### 6.1.3 Software

The *Software* menu contains application, application instances, patch, and services reports that span across all devices.

### 6.1.4 Networking

The Networking menu contains network oriented reports including

- IPv4 networks
- IPv4 address ranges
- IPv6 networks
- Windows network neighborhood (Windows domains and workgroups)
- Directories (Microsoft Active Directory)

#### 6.1.5 User

The *User* menu item provides user, user group (including group membership) and login credentials (including SSH keys) reports.

#### 6.1.5.1 Login Credentials

The *All Login Credentials* report shows all occurrences of login credentials for devices and Windows Domain Controller (DC) or Global Catalog (GC) servers.

#### Figure: All Login Credentials

The All Login Credentials report has got several columns as described below:

- Login is the login (user / account) name.
- Password Count contains the number of different passwords of the Login.
  - Configuring more than one password for a global login can result in user lockout. This can happen when the discovery process repeatedly uses incorrect passwords to establish a connection to a device.

If a global login is assigned more than one password, select the *Login* in the report and use the *"Change password..."* context menu to set the correct password for all occurrences of the global login.

- *Device Count* is the number of devices for which the *Login* is configured.
- *Network Neighborhood* shows the Windows domains / Workgroups for which the *Login* is configured.
- *DNS Domain* displays the Active Directory forests for which the *Login* is configured.

• *Login* is used only to connect to Domain Controllers (DC) or Global Catalog (GC) servers and performing read-only LDAP/S queries.

• The *Directory Object* column shows the Active Directory objects (DNS Domain, Organizational Unit or Container) for which the *Login* is configured.



• The *Default Account Device Platform* states for what operating system platform (I.e. Windows, Linux, etc.) the *Login* has been configured.

You can use the All Login Credentials report for a selected Login to

- Change a Login password
- Change a *Login* & password
- Delete a *Login*

When you change the password or *Login* name, or when you delete a *Login*, all occurrences of the *Login* in the database are updated.

### Change a Login Password...

To change a *Login's* password, select the *Login* in the *All Login Credentials* report and click *Change password...* from the context menu.

Modify Password	×
Login	JDISC-INTERNAL\ADMINISTRATOR
Use this dialog box to replace Enter the Old password to rep	all occurrences of the login's Old password with the New password in the database. place only those occurrences in the database with the New password that matches the Old password.
Old password New password	
New password confirmation	
	Ok Cancel

Figure: Modify Password

If you want to set a *New password* for all occurrences of the selected *Login*, leave the *Old password* field empty.

You can also set a *New password* only for occurrences of the selected *Login* that have been assigned the *Old password*. In this case simply enter the Login's *Old password*.

#### Change Login and Password...

To change a *Login* and password, select the *Login* in the *All Login Credentials* report and click *Change login and password...* from the context menu.

Figure: Modify Login & Password

This works similarly to *Change a Login's Password* from above. However, you can also change the login name for all occurrences of *Login*.

#### Delete a Login

To delete a *Login*, select the *Login* in the *All Login Credentials* report and click *Delete...* from the context menu.



Figure: Delete Logins

You can either delete *All* occurrences of the selected Login or only those occurrences where the password matches. If you chose *By Password*, enter the password in the *Delete Login* dialog.

🔎 Delete Lo	gin	×
Delete login v	vith the specified password.	
Login Password	JDISC-INTERNAL\ADMINISTRATOR	
	Ok Cancel	

Figure: Delete Login

# 6.1.6 Troubleshooting

*The Troubleshooting* menu item contains troubleshooting and diagnostic reports that help finding common discovery problems discovery and permit modifying the discovery queues.

Most reports provide a context menu for management and discovery tasks or to simply display detailed information. Open the context menu with the right mouse button.

# 6.2 Common Actions

JDisc Discovery's reports provide context menus to perform frequently used actions.

# 6.2.1 Run Immediate Discovery

JDisc Discovery can run an immediate discovery of devices, IPv4 networks, IPv4 address ranges and directory objects. The table below illustrates the discover menus in the respective reports.

Report	Discovery menu
Device reports	Click <i>Discover</i> » <i>Selected Devices</i> to discover selected devices. JDisc Discovery will perform a DNS lookup to find IP addresses of selected devices. This is useful for devices using DHCP or that change their IP address frequently.
	Click <i>Discover</i> » Selected IP Addresses to discover selected devices via their IP addresses. This is not

	recommended for devices and networks using DHCP, because the IP address might have changed.
IPv4 network report	Click <i>Discover</i> » <i>Selected Network(s)</i> to discover selected IPv4 networks.
IPv4 address range report	Click <i>Discover</i> » <i>Selected Range(s)</i> to discover selected IPv4 ranges.
Windows Network Neighborhood report	Click <i>Discover » Windows Network Neighborhood</i> to discover selected Windows domains and workgroups.
Directory report	Click <i>Discover Directory</i> to discover selected directory objects.

Case sensitive fil	ter				
Name	IP Address	Manufacturer	Model	Туре	OS Version
ahinh.i	12,210,107,10	LEHUVU	HIIINFOU KJ2	Lahinh	WILLOWS AF FLUICSSIONAL
)esktop-1	12.216.104.46	Lenovo	ThinkCentre A51	Desktop	Windows XP Professional
rinter-2	12.216.106.180	Lexmark	T640		
		Samsung	SyncMast 🗁 Properties		
		Samsung	SyncMast Discover	Selected Devices.	
comtest	192.168.178.16	3COM	SuperSta		
ummit1	192.168.178.13	Extreme Networks	Summit 48 Manage	Selected IP Addresses	7.2.0
ummit2	192.168.181.2	Extreme Networks	Summit 48 Compare	•	7.2.0
ummit3	192.168.181.3	Extreme Networks	Summit 48	vitch	7.2.0
esktop-9	12.255.136.228	Dell	Studio Hy Custom Att	ributes 🕨	Windows Vista Home Premi
trenz-PC2.fritz.box	192.168.178.75	Dell	Studio Hy Connect wit	th 🕨	Windows Vista Home Premi
esktop-7	12.251.240.215	Shuttle Inc	SS58V20		Windows Server 2003 Ente
ackServer-3	12.251.240.0	Hewlett-Packard	rx6600 Troublesho	ot 🕨 ick)	HP-UX B.11.23U
ackServer-4	12.251.240.233	Hewlett-Packard	rx6600	ick)	HP-UX B. 11. 23U
lackServer-5	12.251.240.16	Hewlett-Packard	rx2660 🐥 Delete Devic	ces ick)	HP-UX B.11.23U
lackServer-2	12.251.240.164	Hewlett-Packard	rx2620 Create Supr	out ZIP (ck)	HP-UX B. 11. 23U
witch-5	12.216.105.229	Hewlett-Packard	ProCurve ProCurve		E.11.03
roCurve1	192.168.178.18	Hewlett-Packard	ProCurve 2650	Switch	H.08.72
witch-6	12.251.240.162	Hewlett-Packard	ProCurve 2626	Switch	H.07.50
witch-8	12.251.240.145	Hewlett-Packard	ProCurve 2626	Switch	H.08.54
witch-10	12.251.240.219	Hewlett-Packard	ProCurve 2524	Switch	F.04.08
witch-11	12.251.240.107	Hewlett-Packard	ProCurve 2524	Switch	F.04.08
witch-7	12.251.240.182	Hewlett-Packard	ProCurve 2524	Switch	F.05.17
witch-9	12.251.240.141	Hewlett-Packard	ProCurve 2524	Switch	F.05.50
92.168.178.7	192.168.178.7	Dell	PowerEdge T110 II	Server	VMware ESXi 5.0
4	111				4

Figure: Discover selected Devices

# 6.2.2 Manage Devices

Device reports allow changing a device's login credentials including SSH public/private keys. Select a single or multiple device and open the context menu. The *Manage* menu offers these sub menu items:

- Click *Change Accounts* to configure login credentials.
- Click Change SSH public/private Key to configure SSH keys.
- Click Change SNMP credentials to configure SNMP communities and accounts.
- Click *Synchronize Group Assignment* to manually reassign devices to groups based on information in the database. This is useful when group conditions have changed and you want to prevent running a discovery job, which would automatically assign devices to groups.

Case sensitive	filter						
Name	IP Address	Manufacturer	Mode			Туре	
)esktop-1	12,216,104,46	Lenovo	Think	entre A51		Desktop	Windows XP Professional
rinter-2	12,216,106,180	Lexmark	T640			Printer	
3comtest	192, 168, 178, 16	Samsung Samsung 3COM	Prop Disco	erties ver		Monitor Monitor Switch	
summit1 summit2	192.168.178.13 192.168.181.2	Extreme Networ Extreme Networ	Mana	ge 🍡	>	Change Accounts	7.2.0
summit3	192, 168, 181, 3	Extreme Networ	Com	oare 🧃	$\geqslant$	Change SSH public/private Key	7.2.0
Desktop-9 trenz-PC2.fritz.box	12.255.136.228 192.168.178.75	Dell	Custo	m Attributes 🔰 🤞		Change SNMP Credentials	Windows Vista Home Premi Windows Vista Home Premi
Desktop-7	12.251.240.215	Shuttle Inc	Conr	ect with	3	Synchronize Group Assignment	Windows Server 2003 Ente
RackServer-3	12.251.240.0	Hewlett-Packarc				Server (Rack)	HP-UX B. 11.23U
RackServer-4	12.251.240.233	Hewlett-Packard	Trou	oleshoot 🕨 🕨		Server (Rack)	HP-UX B. 11. 23U
RackServer-5	12.251.240.16	Hewlett-Packarc	C Delet	e Devices		Server (Rack)	HP-UX B. 11.23U
RackServer-2	12.251.240.164	Hewlett-Packard	• Deret	e berrees		Server (Rack)	HP-UX B. 11.23U
Switch-5	12.216.105.229	Hewlett-Packarc	Creat	e Support ZIP		Switch	E.11.03
ProCurve1	192, 168, 178, 18	Hewlett-Packard	Procu	Ve 2650		Switch	H.08.72
Switch-6	12.251.240.162	Hewlett-Packard	ProCu	ve 2626		Switch	H.07.50
Switch-8	12.251.240.145	Hewlett-Packard	ProCu	ve 2626		Switch	H.08.54
Switch-10	12.251.240.219	Hewlett-Packard	ProCu	ve 2524		Switch	F.04.08
Switch-11	12.251.240.107	Hewlett-Packard	ProCu	ve 2524		Switch	F.04.08
Switch-7	12.251.240.182	Hewlett-Packard	ProCu	ve 2524		Switch	F.05.17
Switch-9	12.251.240.141	Hewlett-Packard	ProCu	ve 2524		Switch	F.05.50
192.168.178.7	192.168.178.7	Dell	Power	Edge T110 II		Server	VMware ESXi 5.0
•				-			•



# 6.2.3 Compare Devices

Select the Compare menu item to compare two devices with each other.

### 6.2.4 Connect To Device

Open the context menu and choose *Connect with* to connect to a device. JDisc Discovery can connect to a device using:

• Telnet

- SSH
- Microsoft Terminal Services
- HTTP
- HTTPS

When connecting to a device JDisc Discovery does not pull login credentials from the database for security reasons. You will be prompted to specify login credentials manually.

ilter:	filter				
Name	IP Address	Manufacturer	Model	Туре	OS Version
aptop-1	12,210,107,10	LEHUVU	HIIINFOURJ2	Laptop	WINDOWS AF FLORESSIONAL
Jesktop-1	12.216.104.46	Lenovo	ThinkCentre A51	Desktop	Windows XP Professional
rinter-2	12.216.106.180	Lexmark	1640	Printer	E
		Samsung	Sync Properties	or	
		Samsung	Discover	or	
Bcomtest	192.168.178.16	3COM	Supe	h	
ummit1	192.168.178.13	Extreme Networks	Sum Manage	▶ ng Switch	7.2.0
ummit2	192.168.181.2	Extreme Networks	Sum	h	7.2.0
ummit3	192.168.181.3	Extreme Networks	Sum Compare	ng Switch	7.2.0
Desktop-9	12.255.136.228	Dell	Stud Custom Attribute	es kop	Windows Vista Home Premi
trenz-PC2.fritz.box	192.168.178.75	Dell	Stud		Windows Vista Home Premi
)esktop-7	12.251.240.215	Shuttle Inc	SS58 Connect with	SSH SSH	Windows Server 2003 Ente
RackServer-3	12.251.240.0	Hewlett-Packard	rx66 Troubleshoot	🖬 Telnet 😼	HP-UX B.11.23U
RackServer-4	12.251.240.233	Hewlett-Packard	rx66		HP-UX B.11.23U
RackServer-5	12.251.240.16	Hewlett-Packard	rx26 💢 Delete Devices	Microsoft Terminal Services	HP-UX B. 11.23U
RackServer-2	12.251.240.164	Hewlett-Packard	rx26	IN HTTP	HP-UX B.11.23U
Switch-5	12.216.105.229	Hewlett-Packard	Proc 🛄 Create Support 2		E.11.03
ProCurve1	192.168.178.18	Hewlett-Packard	ProCurve 2650	Swit HTTPS	H.08.72
Switch-6	12.251.240.162	Hewlett-Packard	ProCurve 2626	Switch	H.07.50
Switch-8	12.251.240.145	Hewlett-Packard	ProCurve 2626	Switch	H.08.54
Switch-10	12.251.240.219	Hewlett-Packard	ProCurve 2524	Switch	F.04.08
Switch-11	12.251.240.107	Hewlett-Packard	ProCurve 2524	Switch	F.04.08
Switch-7	12.251.240.182	Hewlett-Packard	ProCurve 2524	Switch	F.05.17
Switch-9	12.251.240.141	Hewlett-Packard	ProCurve 2524	Switch	F.05.50
192.168.178.7	192.168.178.7	Dell	PowerEdge T110 II	Server	VMware ESXi 5.0
•					P.

Figure: Connect to a Device

# 6.2.5 Troubleshooting

Click *Perform SNMP Walk* from the *Troubleshooting* menu to dump all SNMP variables of a SNMP enabled device.

ilter:							
Case sensitive	filter						
Name	IP Address	Manufacturer	Model		Туре	OS Version	
ցիւրի. т	12,210,107,10	LEHUVU	HILLINF OU RUZ		Laptop	WILLOWS AF FLUTESSIULIDI	í,
)esktop-1	12.216.104.46	Lenovo	ThinkCentre A51		Desktop	Windows XP Professional	1
Printer-2	12.216.106.180	Lexmark	T640		Printer		F
		Samsung	SyncMaster		Monitor		-
		Samsung	SyncMaster		Monitor		
Bcomtest	192.168.178.16	3COM	SuperStack 3 Sw	itch 4300	Switch		
summit1	192.168.178.13	Extreme Networks	Summit 48i		Routing Switch	7.2.0	
summit2	192.168.181.2	Extreme Networks	Summit 48i		Switch	7.2.0	
ummit3	192.168.181.3	Extreme Networks	Summit 48i		Routing Switch	7.2.0	
Desktop-9	12.255.136.228	Del 💼 👝		)q	Desktop	Windows Vista Home Prem	
trenz-PC2.fritz.box	192, 168, 178, 75	Dell Prop	perties	)a	Desktop	Windows Vista Home Prem	1
Desktop-7	12.251.240.215	Shuttle Disc	over 🕨	-	Desktop	Windows Server 2003 Ente	e
RackServer-3	12.251.240.0	Hewlett			Server (Rack)	HP-UX B.11.23U	
RackServer-4	12.251.240.233	Hewlett Mar	nage 🕨 🕨		Server (Rack)	HP-UX B. 11. 23U	
RackServer-5	12,251,240,16	Hewlett Con	nnare 🕨		Server (Rack)	HP-UX B.11.23U	
RackServer-2	12,251,240,164	Hewlett	ipure		Server (Rack)	HP-UX B. 11. 23U	
Switch-5	12,216,105,229	Hewlett Cust	tom Attributes 🔸		Switch	E.11.03	
ProCurve1	192, 168, 178, 18	Hewlett Con	nact with		Switch	H.08.72	
Switch-6	12,251,240,162	Hewlett	The curve of the second s			H.07.50	
Switch-8	12.251.240.145	Hewlett Trou	ubleshoot 🔹 🕨	🔍 Perf	orng SNMP Walk	H.08.54	
Switch-10	12,251,240,219	Hewlett 🖌 p. i		O Prov	BUREAA (AVIAL Data	F.04.08	
Switch-11	12,251,240,107	Hewlett K Dele	ete Devices	S Brov	vse vydelvi/ vyivii Data	F.04.08	
Switch-7	12,251,240,182	Hewlett	ate Support 7IP	🥖 Ping	J	F.05.17	
Switch-9	12.251.240.141	Hewlett-range	THE Support ZIP	🦪 т		F.05.50	
192, 168, 178, 7	192, 168, 178, 7	Dell	PowerEdge T11	/ Irac	erouten	VMware ESXi 5.0	
4			, oncluge (110		berrer	A MORE EDVI 010	
							-

Figure: SNMP Walk

Click *Ping* to ping IP addresses of selected devices. Enter the timeout and retry parameters and press *Ok*. JDisc Discovery will ping all active IPv4 and IPv6 IP addresses and display the results.

Click*Browse WBEM/WMI Data* in order to review WBEM or WMI information for the selected device.

Click *Traceroute* in order to view the traceroute output for the selected device.

# 6.2.6 Delete Devices

JDisc Discovery does not automatically delete devices from the database that have been disconnected from the network or which do no longer exist. Click *Delete Devices* to delete selected devices from the database.

# 6.2.7 Create Support ZIP

JDisc Discovery can pack the information required by our support to help troubleshooting discovery problems. To create a support ZIP file, select a set of devices and click *Create Support* ZIP to create a support ZIP file.

# 6.3 The Device Details Report

The *Device Details* report displays detailed device information. Double click a device or choose *Properties* from the device's context menu to open the *Device Details* report.

JDisc Discovery does not always collect all device details. Data quality greatly depends on the device type, platform, available protocols and the network infrastructure (firewalls).

The Device Details report consists of the nine tabs:

- The *General* tab displays basic device information such as name, manufacturer, model, type, serial number, etc.
- The *Networking* tab displays network interfaces, IPv4 networks to which the device is connected and the SNMP system group variables.
- The *Hardware* tab displays processors, memory modules, physical/logical disk information and attached devices.
- The *Firmware* tab displays firmware version, manufacturer and the SMBIOS version for Intel based systems.
- The *Software* tab displays operating system information, installed application and patches.
- The User tab displays local user, logged on user and logged on user history.
- The *Virtual Computers* tab displays virtual (computer) instances running on the selected device.
- The *Roles* tab displays device roles assigned by the discovery.
- The *Groups* tab displays all groups to which the device belongs.
- The *Analyze* tab displays the discovery log, protocol status, parsing issues, and rule based diagnostics.

### 6.3.1 General Tab

The *General* tab displays the following device information:

• Name

- Manufacturer
- Model
- Туре
- Serial number
- Hardware version
- Part number
- Windows computer name
- Windows network neighborhood name (if member of a Windows domain or Workgroup)
- Directory object name (if member of a directory)
- Creation date (first discovery date)
- Last discovery date
- Discovery duration (Device identification and device data collection)
- Database duration (Database update transaction)
- If the device is a virtual (computer) instance, JDisc Discovery can display the physical host server on which the virtual (computer) instance runs.



Figure: Device Details » General Tab

# 6.3.2 Networking Tab

The *Networking* tab displays network interfaces, IPv4 networks to which the device belongs and SNMP system group variables.

#### 6.3.2.1 Interfaces

The interfaces table displays all interfaces including interface type, description, speed, assigned DNS names, IP addresses and subnet masks.

neral Networki	ng Hardware Firmware	Software User Virtual Co	mputers Custom Attributes Roles Groups Analyze	
nterfaces Net	works SNMP System Group	2		
Filter:				
Ca	se sensitive filter			
	Physical Address	Type	Description	Speer
	Physical Address	i ype	WAN Minimuck (CCTD)	opeer
	1	unknown coffwarol oopback	Software Loopback Interface 1	Â
	1	SUITWATELOOPDACK	Software Eoopback Internace 1	
	2	unknown	WAN Miniport (L2TP)	
	3	unknown	WAN Miniport (PPTP)	=
	4	unknown	WAN Miniport (PPPOE)	_
1	5	unknown	WAN Miniport (IPv6)	
	5	unknown	WAN Miniport (Network Monitor)	
	3	unknown	WAN Miniport (IP)	
	9	unknown	Microsoft-ISATAP-Adapter	
1	20:41:53:59:4e:ff	unknown	RAS Async Adapter	
1	1 00:1b:fc:b4:f9:82	ethernetCsmacd	Intel(R) 82566DC-2 Gigabit Network Connection	
1	2 00:c0:a8:f3:3f:b0	ethernetCsmacd	USB Wireless 802.11 b/g Adaptor	S
1	3	unknown	Microsoft-ISATAP-Adapter	
1	4	unknown	Microsoft-ISATAP-Adapter	
1	5 00:ff:a9:b8:29:9d	ethernetCsmacd	TAP-Win32 Adapter V9	
•	III			•
Total 31 inte	faces   0 interfaces selecte	d		

Figure: Interfaces Table

### 6.3.2.2 Networks Tab

The *Networks* tab displays IPv4 networks to which the device belongs. To display all devices in the networks displayed, select a network and open the context menu and choose a report.

	are Firmware Software User	Virtual Computers Cus	stom Attributes Roles Groups Analyze
Interfaces Networks SNN	1P System Group		
Filter:			
Case sensitive	filter		
Network Address	Subnet Mask	Name	Last Discovered
192.168.178.0	255.255.255.0		Mar 4, 2014 5:30:40 PM
•		III	4

### Figure: Networks Table

# 6.3.2.3 SNMP System Group

If a device supports SNMP, the SNMP system group displays standard SNMP variables such as System Object ID, System Description, etc.

D Davies Dateils for 'Drinter 1'
General Networking Hardware Firmware Software User Virtual Computers Custom Attributes Roles Groups Analyze
Interfaces Networks SNMP System Group
System Name         System Object ID       1.3.6.1.4.1.2590.1.1.1.1.1.26         System Description       KONICA MINOLTA magicolor 2350         System Location       B1 Room 32c         System Contact       Jim Smith
LIOSE

Figure: SNMP System Group Tab

# 6.3.3 Hardware

The Hardware tab displays processors, memory modules, disks and attached devices.

#### 6.3.3.1 Processors

The *Processors* tab displays physical processors. Dual core and hyper-threaded processors appear as one row. The core count and the thread count columns describe a physical processor in more detail.

Gene	eral Netwo	rking Hardware	box	e User Virtual Cor	mputers Custon	n Attributes	Roles Grou	ips Analyze		
	Filter:									
	Slot	Model	Manufacturer	Current Speed	Max Speed	Cores	Threads	Address Width		
	CPU 1	Core2 Ouad	Intel	2,39 GHz	2.39 GHz	4	4	4	e	
				1						
	Total 1 pro	cessor   0 processo	rs selected	1					4	



### 6.3.3.2 Memory Modules

The *Memory Modules* tab displays memory modules including size, model, and manufacturer. When JDisc Discovery cannot discover memory modules the total memory size will be displays instead. In this case the memory module slot is named 'Total'.

J) Devic	e Details fo → 🏂   eral   Networ rocessors   M	or 'teetee-pc.fritz.box'	)   ===================================	omputers Custom Attribute:	Roles Groups Analyze	
	Total memo	ry 3.00 GB Case sensitive filter				
	Slot	Model	Manufacturer	Size		
	BANKO	Physikalischer Speicher	7E7E7E7E7E510000	E10 M	2	
	BANK1	Physikalischer Speicher	7676767676510000	1.00 GE	2	
	BANK2	Physikalischer Speicher	7E7E7E7E7E510000	512 ME	3	
	BANK3	Physicalischer Speicher	7E7E7E7E7E510000	1.00 GE	-	
	Total 4 mer	mory modules   0 memory modu	les selected			
			C	lose		

Figure: Memory Modules Tab

#### 6.3.3.3 Disks

The *Disks* tab is separated into these tabs *Physical Disks*, *Disk Partitions*, and *Logical Disks*.

### **Physical Disks**

The *Physical Disks* tab displays all physical disks including model, manufacturer, serial number and total size.

Device Details for 'teetee-pc.fritz.box'				x
General Networking Hardware Firmware Processors Memory Modules Disks Via Physical Disks Disk Partitions Logical Total Physical Disk Space 467.65 (	e Software User deo Controller Atta Disks Disk Arrays	Virtual Computers Custom A	ttributes Roles Groups Analyze	
Filter:				
Model	Manufacturer	Serial Number	Size	
Generic- SD/MMC USB Device		<b>\$</b>	1.89 GB	
HDT725050VLA360 ATA Device	Hitachi	VFK401R4195LAK	465.76 GB	
Total 2 physical disks   0 physical dis	sks selected			
		Close		

Figure: Physical Disks Tab

The Total Physical Disk Space displays the sum of all physical disks.

**Disk Partitions** 

The *Disk Partitions* tab displays all partitions on the computer.

Device Details for 'teetee-pc.fritz.box'		- 0 <b>X</b>
General Networking Hardware Firmware Software User	Virtual Computers Custom Attributes Roles Groups Analyze	
Processors Memory Modules Disks Video Controller Atta	ached Davieer	
Physical Disks Disk Partitions Logical Disks Disk Arrays		
Total Partition Space 467.65 GB		
Filter:		
Case sensitive hiter		
Name	Size	
Disk #0, Partition #0 Disk #0, Partition #1	457.64 GB 8.12 GB	
Disk #3, Partition #0	1.89 GB	
Total 3 disk partitions   0 disk partitions selected		
	Close	

Figure: Disk Partitions Tab

### Logical Disks

The *Logical Disks* tab displays mounted logical disks on the computer. Logical disks have these attributes:

- Name
- Mount point
- Total size
- Used size
- Free size
- Serial number

Gener	→ 🕏   🔓   🗅	ardware Firmware S	Software User N	/irtual Computer	s Custom Attr	ibutes Roles	Groups Analyze	
Pro	cessors Memory M	odules Disks Video	Controller Attack	ned Devices				
F	Physical Disks Disk F	Partitions Logical Disk	s Disk Arrays					
	Total disk space Total used space Total free space Filter:	467.65 GB 358.24 GB 109.41 GB						
	Case se	nsitive filter						
	Name	Mount Point	File System	Size	Used	Free	Serial Number	
		H:	FAT	1.89 GB	520.50 MB	1.38 GB	65663833	
	RECOVERY	D:	NTES	457.64 GB 8, 12 GB	7,11 GB	1.01 GB	187D0FFC	
			m					4
	✓ Total 3 logical disk	s   0 logical disks selec	ted					



The *Total disk space, Total used space, and Total free space* fields list the accumulated number for all logical drives.

### **Attached Disk Arrays**

JDisc Discovery discovers attached disk arrays for HP-UX computers.

6.3.3.4 Video Controller

The Video Controller tab displays a computer's video controllers.

Gene	e Details for 'teetee-	pc.fritz.box'	ware User Vi	rtual Computers C	Custom Attributes	Roles Groups An	alyze	
	Slot	Model	Manufa	Serial Number	RAM	Horiz Resolution	Vert Resolution	
	PCIVEN 10DE&DE	GeForce 8600 GT	NVIDIA	ochar Hamber	512 00 MR	1 020	1 201	
	Total 1 video controlle	er   0 video controllers se	elected	III			•	
				Close				

Figure: Video Controllers

### 6.3.3.5 Attached Devices

The Attached Devices tab displays directly attached devices. JDisc Discovery discovers

- printers attached to print servers
- tape drives attached to tape libraries
- monitors attached to a computer
- blade workstations, servers, switches and power supplies mounted in a blade enclosure
- rack or blade servers connected to a management device
| General Networking | Hardware Firmware Sc    | ftware User Virtual Co   | omputers Custom Attribute | es Roles Groups Anal | yze        |
|--------------------|-------------------------|--------------------------|---------------------------|----------------------|------------|
| Processors Memory  | Modules Disks Video C   | ontroller Attached Devic | tes                       |                      |            |
| Filter:            |                         |                          |                           |                      |            |
| Case se            | sitive filter           |                          |                           |                      |            |
| Manufacturer       | Model                   | Туре                     | Name                      | IP Address           | OS Version |
| Dell               | 2407WFP                 | Monitor                  |                           |                      |            |
|                    |                         |                          |                           |                      |            |
|                    |                         |                          |                           |                      |            |
| <                  | III<br>levices selected |                          |                           |                      | A          |

Fig: Attached monitor

## 6.3.4 Firmware

The *Firmware* tab displays firmware version information. Firmware includes

- Name (BIOS manufacturer name for Intel/AMD based systems)
- Manufacturer
- Version (BIOS version for Intel/AMD based systems)
- Release Data
- SMBIOS Version

Device Details for 'teet	tee-pc.fritz.box'	- 0 X
$  \leftarrow \rightarrow \mathcal{O}   \bigcirc  $		
General Networking	Hardware Firmware Software User Virtual Computers Custom Attributes Roles Groups Analyze	
Name Manufacturer Unique Id FW Version Release Date SMBIOS Version	BIOS Date: 08/02/07 17:24:08 Ver: 08.00.14 American Megatrends Inc. 9F873458-4727-11DC-8DF2-28ED466C6CD8 5.6 Thu Aug 02 01:00:00 CEST 2007 2.5	
	Close	

Figure: Firmware Tab

#### 6.3.5 Software

The *Software* tab displays operating system, applications, application instances, patches and services.

#### 6.3.5.1 Operating System

The Operating System tab displays

- OS Family classification of operating systems into families, such as Windows, HP-UX, etc
- OS Version operating system name including version information
- OS System Type the system type (such as x86, x64, ia64 and Sparc)
- Patch Level Service Pack on Windows platforms
- Install Date
- System Uptime
- Owner
- Unique Id
- Product Key
- Locale language locale on Windows platforms

Device Details for 'teetee $  \leftarrow \rightarrow   \bigcirc   \bigcirc   \bigcirc$	pc.fritz.box'	
General Networking Ha Operating System App	rdware Firmware Software User Virtual Computers Custom Attributes Roles Groups Analyze	
OS Family OS Version OS System Type Patch Level Install Date Uptime Owner Unique Id Product Key Locale	Windows 7 Professional x64 Service Pack 1 Thu Mar 29 21:52:19 CEST 2012 01:29:27 ttrenz 00371-OEM-9308645-37138 0407	

Figure: Operating System Information

# 6.3.5.2 Applications

The *Applications* tab displays installed applications.

eneral Networking Hardware Firmware S	oftware User Virt	ual Computers   Custom Attribu   Services   Drivers   Executab	utes Roles Groups Analyze	
<b>Filmer</b>				_
Filter:				
				_
Application	Version	Manufacturer	Path	
iTunes	11.1.4.62	Apple	c:\program files (x86)\itunes\itunes.exe	
jacoZoom 1.5	1.5.1.5	infoZoom		
Java (Sun)	5.0.5000			
Java(TM) Web Start Launcher	10.51.2.13	Oracle	c:\program files (x86)\java\jre7\bin\java	
Java 6 Runtime, Standard Edition	6.0.220	Sun Microsystems	c:\program files (x86)\java\jre1.6.0 22	
Java 6 Runtime, Standard Edition	6.0.350	Sun Microsystems	c:\program files (x86)\java\jre6	_
Java 6 SDK, Standard Edition	1.6.0.310	Sun Microsystems	c:\program files (x86)\java\jdk1.6.0 31	-
Java 6 SDK, Standard Edition	1.6.0.350	Sun Microsystems	c:\program files (x86)\java\jdk1.6.0_35	
Java 7 Update 25	7.0.250	Oracle	c:\program files (x86)\java\jre7	
Java 7 Update 51	7.0.510	Oracle	c:\program files (x86)\java\jre7	
Java Auto Updater	2.1.9.8	Sun Microsystems		
JavaFX 2.1.0	2.1	Oracle	c:\program files (x86)\oracle\javafx 2.1	
Java SE Development Kit 7 Update 13	1.7.0.130	Oracle	c:\program files (x86)\java\jdk1.7.0_13	
Java SE Development Kit 7 Update 25	1.7.0.250	Oracle	c:\program files (x86)\java\jdk1.7.0_25	
Java SE Development Kit 7 Update 7	1.7.0.70	Oracle	c:\program files (x86)\java\jdk1.7.0_07	
JoomlaPack Native Tools 2009.3		JoomlaPack Developers	c:\program files (x86)\joomlapack native	
ManageEngine MihBrowser 5				- I.
•			4	
Total 236 applications   0 applications sele	cted			
				_
				_

Figure: Applications Tab

## 6.3.5.3 Application Instances

The *Application Instances* tab displays installed application instances such as database instances, JEE application server instances or web server instances.

Dev	vice Details for 'Integ	grityVM-4'					
<b>\$</b> +	- → 🌫 🔒 🖣	à 🛛 🔊 🗋 💓 🛛					
Ge	neral Networking H	Hardware Firmware	Software User Conn	ections Virtua	al Computers Custom	Attributes Roles Groups Analyze	
	Operating System A	pplications Applicati	on Instances Patches	Services Driv	ers Executables Pro	ocesses Cluster Services	
	Filter:						
	Case ser	nsitive filter					
	Instance Name	Instance Type	Application	Version	Manufacturer	Path	
	customers	Database	Oracle Database 10g	10.2.0.1	Oracle	/opt/oracle/product/10.2.0.1	
	costonero	o diababe	order batababe rog		0.000	lobilo and board to the t	
	•				m		+
	Total 1 application	instance   0 applicati	on instances selected				
					Close		

# Figure: Application Instances

## 6.3.5.4 Patches

The *Patches* tab displays installed patches.

		1
General Networking Hardware Firmware Software User Virtual Computers Cus	tom Attributes   Roles   Groups   Analyze	
Operating System   Applications   Application Instances   Patches   Services   Drivers	Executables   Processes   Cluster Servic	es
Filter:		
Case sensitive filter		
<b>v</b>		
Patch	Manufacturer	
microsoft visual studio 2008 standard edition - deu Service Pack 1 (kb945140)	Microsoft	
microsoft visual studio 2008 remote debugger light (x64) - deu Service Pack 1 (kb	Microsoft	
microsoft office sharepoint designer 2007 Service Pack 3 (sp3)	Microsoft	
microsoft office 2007 Service Pack 3 (sp3)	Microsoft	
KB982018		
KB976902		
KB976002		
КВ972222	Microsoft	
KB971092	Microsoft	
KB967642	Microsoft	
KB958488		
KB950424	Microsoft	
KB950278	Microsoft	
KB948484	Microsoft	
KB947888	Microsoft	
KB946733	Microsoft	
KB946729	Microsoft	
KB945140	Microsoft	<b>T</b>
Total 263 patches   0 patches selected		

## 6.3.5.5 Services

The Services tab displays installed services including important service attributes.

eral Networking Hardware Firmware S	oftware User Virtual Computers Custom Attributes Roles Gr	oups Analyze	
perating System Applications Application	Instances Patches Services Drivers Evenutables Processes	Cluster Services	
per a ung System   Applications   Application	Instances Fatches Convers Executables Frocesses	Cluster Services	
-1			
Filter:			
Case sensitive filter			
<b>^</b>			
Service	Display Name	Status	
Dthserv	Bluetooth-Unterstutzungsalenst	Stopped	
c2cautoupdatesvc	Skype Click to Call Updater	Running	
c2cpnrsvc	Skype Click to Call PNR Service	Running	
CertPropSvc	Zertifikatverteilung	Running	=
clr_optimization_v2.0.50727_32	Microsoft .NET Framework NGEN v2.0.50727_X86	Stopped	
clr_optimization_v2.0.50727_64	Microsoft .NET Framework NGEN v2.0.50727_X64	Stopped	
clr_optimization_v4.0.30319_32	Microsoft .NET Framework NGEN v4.0.30319_X86	Stopped	
clr_optimization_v4.0.30319_64	Microsoft .NET Framework NGEN v4.0.30319_X64	Stopped	
COMSysApp	COM+-Systemanwendung	Stopped	
CryptSvc	Kryptografiedienste	Running	
CscService	Offlinedateien	Running	
DcomLaunch	DCOM-Server-Prozessstart	Running	
defragsvc	Defragmentierung	Stopped	
Dhcp	DHCP-Client	Running	
Dnscache	DNS-Client	Running	
dot3svc	Automatische Konfiguration (verkabelt)	Stopped	
DPS	Diagnoserichtliniendienst	Running	-
< III			•
Total 192 convices   0 convices calested			
Total 172 Services   U services Selected			

#### Figure: Installed Services

#### 6.3.5.6 Drivers

The *Drivers* tab displays installed drivers including important driver attributes.

Filter:       Case sensitive filter         Driver       Display Name         1394ohd       OHCI-konformer: 1394-Hostcontroller         ACP1       Microsoft ACPI-Treiber         AFD       Ancillary Function Driver for Winsock         amdxata       amdxata         Asynchroner RAS -Medientreiber       atapi         atapi       IDE-Kanal         avgnftht       avgntfit         avgnftb       avgntfit         avgnftb       avgntfit         bibdrive       bibdrive         bibdrive       bibdrive         bibdrive       bibdrive         cdrom       CD-ROM-Laufwerktreiber         cLFS       Gemeinsames Protokoll (CLFS)         CNG       CNG         CNG       CNG         ChristeRus       Busenumeratortreiber für Verbundneräte         ital 131 drivers  0 drivers selected       ital 131 drivers  0 drivers selected	→ 🌮   🖨   ि   🟝 🕞   👮   🙃   👬 al Networking Hardware Firmware Software rating System Applications Application Instance	User Virtual Computers Custom Attributes Roles Groups Analyze es Patches Services Drivers Executables Processes Cluster Services	
Driver     Display Name       1394ohci     OHCI-Konformer 1394-Hostcontroller       ACP1     Microsoft ACPI-Treiber       AFD     Ancillary Function Driver for Winsock       amdxata     amdxata       AsyndMac     Asyndroner RAS -Medientreiber       atapi     IDE-Kanal       avgntfit     avgntfit       avipbb     avipbb       avipbb     avipbb       avimgr     Beep       bibdrive     bibdrive       bibdrive     bibdrive       cdrom     CD-ROM-Laufwerktreiber       CLFS     Gemeinsames Protokoll (CLFS)       CNG     CNG       CMG     CNG       Total 131 drivers   0 drivers selected	ilter:		
1394ohd     OHCI konformer 1394Hostcontroller       ACPI     Microsoft ACPI-Treiber       AFD     Andilary Function Driver for Winsock       amdxata     amdxata       AsyndMac     Asyndroner RAS -Medientreiber       atapi     IDE-Kanal       avipbb     avipbb       avipbb     avipbb       avingtht     aughtfit       avipbb     avipbb       avingth     Beep       bibdrive     bibdrive       bibdrive     bibdrive       cdrom     CD-ROM-Laufwerktreiber       CLFS     Gemeinsames Protokoll (CLFS)       CNG     CNG       CnonositeBus     Busenumeratortreiber für Verbundneräte       *     111	Driver	Display Name	
ACPI     Anclary Function Driver for Winsock       amdxata     amdxata       andxata     amdxata       atapi     IDE-Kanal       avgntfit     avgntfit       avkmgr     avkmgr       Beep     Beep       bibdrive     bibdrive       bibdrive     bibdrive       bibdrive     Beep P       Browser Derosuporttreiber     CommositeFus       cdrom     CD-ROM-Laufwerktreiber       CLFS     Gemeinsames Protokoll (CLFS)       CNS     CNS       Claid     10	1394obci	OHCI-konformer 1394-Hostcontroller	
AFD     Andlary Function Driver for Winsock       amdxata     amdxata       Asynchroner RAS -Medientreiber     atapi       atapi     IDE-Kanal       avgntfit     avgntfit       avight     avgntfit       avight     avight       avight     blodrive       blodrive     blodrive       blodrive     blodrive       blodrive     blodrive       cdrom     CD-ROM-Laufwerktreiber       cdrom     CD-ROM-Laufwerktreiber       CLFS     Gemeinsames Protokoll (CLFS)       CNG     CNG       COMO     CNG       ComositeRus     Busenumeratortreiber für Verbundneräte       Total 131 drivers   0 drivers selected		Microsoft ACPI-Treiber	- AL
amdxata andxata andxata Asynchroner RAS -Medientreiber atapi DE-Kanal DE-Kanal DE-Kanal avgntfit avgntfit avgntfit avgntfit avgntfit avgntfit avgntfit Beep Beep Beep Beep Blodrive blodrive blodrive blodrive blodrive blodrive CD-ROM-Laufwerktreiber CLFS Gemeinsames Protokoll (CLFS) CNG CompositeRus Busenumeratortreiber für Verbundneräte Total 131 drivers le 0 drivers selected	AED.	Aprillary Eurotion Driver for Winsock	E
AsyncMac     Asynchroner RAS -Medientreiber       atapi     IDE -Kanal       avgntfit     avgntfit       avipbb     avipbb       avkmgr     avkmgr       bibdrive     bibdrive       bibdrive     bibdrive       bibdrive     bibdrive       cardow     CD -ROM-Laufwerktreiber       CLFS     Gemeinsames Protokoll (CLFS)       CNG     CNG       CnanositeBus     Busenumeratorkreiber für Verbundneräte       Total 131 drivers  0 drivers selected     III	amdxata	amdxata	
atapi     IDE-Kanal       avgntfit     avgntfit       avipbb     avipbb       avimgr     avimgr       Beep     Beep       bibdrive     bibdrive       bowser     Browsersupporthreiber       cdrom     CD-ROM-Laufwerktreiber       CLFS     Gemeinsames Protokoll (CLFS)       CNG     CNG       CompositeBus     Busenumeratortreiber für Verhundneräte       III     Total 131 drivers  0 drivers selected	AsyncMac	Asynchroner RAS -Medientreiber	
avgnfft avgnff	atani	IDE-Kanal	
avipbb avipbb avimgr avimgr avimgr avimgr Beep Beep bibdrive bibdrive bibdrive bowser Browsersupporttreiber camdrv42 Philog SPC 900NC PC Camera cdrom CD-ROM-Laufwerktreiber CLPS Gemeinsames Protokoll (CLPS) CNG CNG CommositeBus Busenumeratorkreiber für Verbundneräte	avontfit	avontfit	
avkmgr avkmgr avkmgr Beep Beep bibdrive bibdrive bowser Browsersupporttreiber camdrv42 Philips SPC 900NC PC Camera cdrom CD-ROM-Laufwerktreiber CLFS Gemeinsames Protokoll (CLFS) CNG CNG CNG CompositeRus Busenumeratortreiher für Verhundneräte < III Total 131 drivers  0 drivers selected	avipbb	avipbb	
Beep     Beep       blbdrive     blbdrive       bowser     Browsersupporttrelber       candrv42     Philps SPC 900KC PC Camera       cdrom     CD-ROM-Laufwerktrelber       CLFS     Gemeinsames Protokoll (CLFS)       CNG     CNG        CNG        Total 131 drivers selected	avkmar	avkmgr	
bibdrive     bibdrive       bowser     Browsersupporttreiber       camdrv42     Philps PC 900NC PC Camera       cdrom     CD-ROM-Laufwerktreiber       CLFS     Gemeinsames Protokoll (CLFS)       CNG     CNG       C onnositeBus     Busenumerator/treiber für Verbundneräte       Total 131 drivers   0 drivers selected     III	Been	Been	
bowser Browsersupporttreiber camdrv42 Philips SPC 900NC PC Camera cdrom CD-ROM-Laufwerktreiber CLFS Gemeinsames Protokoll (CLFS) CNG CNG CNG C CMG CNG CNG Total 131 drivers   0 drivers selected	blbdrive	blbdrive	
camdrv42     Philips SPC 900NC PC Camera       cdrom     CD-ROM-Laufwerktreiber       CLFS     Gemeinsames Protokoll (CLFS)       CNG     CNG       CommositeBus     Busenumeratortreiher für Verhundneräte       ✓     III       Total 131 drivers   0 drivers selected	bowser	Browsersupporttreiber	
cdrom     CD-ROM-Laufwerktreiber       CLPS     Gemeinsames Protokoll (CLFS)       CNG     CNG       CNG     CNG       Charles     Busenumerator/treiher für Verbundneräte       Total 131 drivers   0 drivers selected     III	camdrv42	Philips SPC 900NC PC Camera	
CLFS     Gemeinsames Protokoll (CLFS)       CNG     CNG       CommositeBus     Busenumeratortreiher für Verbundneräte       <	cdrom	CD-ROM-Laufwerktreiber	
CNG CNG CompositeBus Busenumeratortreiher für Verhundneräte ✓ III Total 131 drivers   0 drivers selected	CLFS	Gemeinsames Protokoll (CLFS)	
ComnositeBus Busenumeratortreiher für Verbundneräte  Total 131 drivers   0 drivers selected	CNG	CNG	
	CompositeBus	Busenumeratortreiber für Verbundgeräte	-
Total 131 drivers   0 drivers selected	< III		•
	Total 131 drivers   0 drivers selected		

Figure: Installed Drivers

## 6.3.5.7 Executables

The *Executables* tab displays the list of all executables found on local harddrives.

perating System   Applications   Application I	instances Patches Services Drivers Executables Processes	Cluster Services
Filter:		
Case sensitive filter		
Binary	Name	Version
4hitmanibroker eve		
6feff9b68218417f98f549 eve		<u> </u>
853f67d554f05449430e7e.exe		
isdel.exe	InstallShield®	5.51.138.0
isdel.exe	InstallShield®	5.51.138.0
isdel.exe	InstallShield®	5.51.138.0
regsvr32.exe	Microsoft(R) Win32 SDK	4.0.1381.0
33.0.1750.117_32.0.1700.107_chrome_up	odater.exe	
3dvision_306.97.exe	NVIDIA 3D Vision driver	4.0.0.0
3dvision_306.97.exe	NVIDIA 3D Vision driver	4.0.0.0
3dvision_311.06.exe	NVIDIA 3D Vision driver	2.11.15.0
3dvision_311.06.exe	NVIDIA 3D Vision driver	2.11.15.0
64bitmapibroker.exe		
7z.exe	7-Zip	9.20.0.0
7zfm.exe	7-Zip	9.20.0.0
7zg.exe	7-Zip	9.20.0.0
acrobroker.exe	Adobe PDE Broker Process for Internet Explorer	11.0.0.379
· · · · · · · · · · · · · · · · · · ·		4
	and the second se	

Figure: The list of all local executables

#### 6.3.5.8 Processes

The Processes tab displays running processes including important process attributes.

operativ	Networking	Hardware Firr	nware Software Us	er Virtual Computers Custom Attr	ibutes Roles Groups Analyze	
operation	.g 0 / 0 to	- appression - A				11
Filter	:					
	Case	sensitive filter				
	~					
Proc	tess Id	Parent Proc Id	Binary	User Name	Login	Path
	304	ł	smss.exe	TEETEE-PC\SYSTEM	TEETEE-PC\SYSTEM	c: \winc 🔺
	324	ł	svchost.exe	TEETEE-PC/LOKALER DIENST	TEETEE-PC/LOKALER DIENST	c: wind
	344	ł	svchost.exe	TEETEE-PC\SYSTEM	TEETEE-PC\SYSTEM	c:\winc ≡
	432	2	csrss.exe	TEETEE-PC\SYSTEM	TEETEE-PC\SYSTEM	c: wind
	512	2	csrss.exe	TEETEE-PC\SYSTEM	TEETEE-PC\SYSTEM	c: \wind
	520	)	wininit.exe	TEETEE-PC\SYSTEM	TEETEE-PC\SYSTEM	c: winc
	584	ł	winlogon.exe	TEETEE-PC\SYSTEM	TEETEE-PC\SYSTEM	c: \wind
	624	ł	services.exe	TEETEE-PC\SYSTEM	TEETEE-PC\SYSTEM	c:\winc
	632	2	lsass.exe	TEETEE-PC\SYSTEM	TEETEE-PC\SYSTEM	c: \wind
	640	)	lsm.exe	TEETEE-PC\SYSTEM	TEETEE-PC\SYSTEM	c: \winc
	716	i	svchost.exe	TEETEE-PC/WETZWERKDIENST	TEETEE-PC/WETZWERKDIENST	c: \wind
	740	)	svchost.exe	TEETEE-PC\SYSTEM	TEETEE-PC\SYSTEM	c:\winc
	808	8	nvvsvc.exe	TEETEE-PC\SYSTEM	TEETEE-PC\SYSTEM	c:\wind
	832	2	nvscpapisvr.exe	TEETEE-PC\SYSTEM	TEETEE-PC\SYSTEM	c:\prog
	868	1	taskeng.exe	TEETEE-PC\SYSTEM	TEETEE-PC\SYSTEM	c: \wind
	876	i	svchost.exe	TEETEE-PC WETZWERKDIENST	TEETEE-PC/NETZWERKDIENST	c:\winc
	964	4	lononui.exe	TEETEE-PC\SYSTEM	TEETEE-PC\SYSTEM	c:\wint
•			1			4
Tota	82 proces	sses   0 processes	selected			

#### Figure: Running Processes

#### 6.3.5.9 Cluster

The *Clusters* tab lists all cluster services running on a member of a cluster. Additionally, it lists the cluster name that the device belongs to.

#### 6.3.6 User

The *User* tab is divided into three sub-tabs.

6.3.6.1 Logged On Users

Displays users that have been logged on when the device has been discovered.

	e Software USET Virtual Computers Oustom A	ttributer Poles Groups Apalyze
Logged on Users Local Users Logged	on User History	
-1		
Filter:		
Case sensitive filter		
User Name	Login	Logon Type
100	100	
102	102	
Postfix Daemon	postfix	
root	root	
Thomas Trenz	ttrenz	
< III		4
Total 6 logged on users   0 logged on	users selected	



6.3.6.2 Local Users

Displays local users.

	Itware User Virtual Computers   Custom Attrib	utes Roles Groups Analyze
ogged on Users Local Users Logged on Use	r History	
<b>-</b> 1		
Filter:		
Case sensitive filter		
User Name	Login	User Id
Batch iobs daemon	at	25
bes	bes	1002
bin	bin	1
Daemon	daemon	2
dev2	dev2	1001
dnsmasg	dnsmasg	104
FTP account	ftp	40 =
Games account	games	12
Mailer daemon	mail	8
Manual pages viewer	man	13
News system	news	9
nobody	nobody	65534
Novell Customer Center User	suse-ncc	103
NTP daemon	ntp	74
PolicyKit	polkituser	101
Postfix Daemon	postfix	51
Printing daemon	İn	4
•	III	P.
Total 25 users   1 user selected		

Figure: Local Users

# 6.3.6.3 Logged On User History

Displays users that have been logged within a configurable number of days.

	Device Details for 'teetee-pc.fritz.box'										
alle	* · · · * W · · · · · · · · · · · · · ·										
	General Networking Hardware Firmware Software User Virtual Computers Custom Attributes Roles Groups Analyze										
Learned on Linear Learning Logard on Linear History											
Logged on Users   Local Users   Logged on User history											
		Filter:									
		Case se	ensitive filter								
		_									
		User Name	Login	Logon Type	Client Name	User Id	Last Seen At				
		TTRENZ	TEETEE-PC\TTRENZ	Interactive		S-1-5-21-149989641-1482761726-481798120-1000	Feb 18, 2014 3:58:24 Pf				
		Total 4 look loops	d an una 10 la bland an un	an anlanta d			4				
		Total Tlast logge	a on user   0 last logged on use	rs selected							
					Close						

Figure: Logged on User History

# 6.3.7 Virtual Computers

The *Virtual Computers* tab displays virtual computers (for example VMware) running on a host server.

Device Details for '192.168.178.73'            ← →							
General Networking Hardware Firmware Software User Virtual Computers Custom Attributes Roles Groups Analyze							
1		1985	0.05.44.5		c o		
invicvs	192.168.178.25	VMware Instance	openSuSE 11.2	2.6.31.14-0.8-desktop	6.0	VMware-56 4d d	
jboss7.fritz.box	192.168.178.76	VMware Instance	CentOS 6.4	2.6.32-358.el6.i686	6.0	VMware-56 4d 0	
jbossas5.fritz.box	192.168.178.70	VMware Instance	CentOS 6.4	2.6.32-358.el6.i686	6.0	VMware-56 4d 7	
jbossas6.fritz.box	192.168.178.72	VMware Instance	CentOS 6.4	2.6.32-358.el6.i686	6.0	VMware-56 4d ct	
JDiscServer	192.168.178.74	VMware Instance					
JDisc Web Site - Joomla Ubuntu		VMware Instance	Ubuntu 64-bit				
solaris11-test	192.168.178.26	VMware Instance	SunOS 5.11	11.1	DevConf 2.0		
weblogic.fritz.box	192.168.178.64	VMware Instance	CentOS 6.4	2.6.32-358.el6.i686	6.0	VMware-56 4d 4	
websphere800.fritz.box	192.168.178.66	VMware Instance	CentOS 6.4	2.6.32-358.el6.i686	6.0	VMware-56 4d 3	
		11					
Total 9 Virtual computers   0 Virtu	ual computers selected					· · · · · · · · · · · · · · · · · · ·	
			Close				

#### Fig: Virtual Computers tab

## 6.3.8 Custom Attributes

The *Custom Attributes* tab displays the custom attribute hierarchy including the attributes for the selected folder.

Device Details for 'teetee-period	fritz.box'							
General Networking Hardware Firmware Software User Virtual Computers Custom Attributes Roles Groups Analyze								
Custom Attributes								
Location	Building	Building 01						
	Collection date: Sep 30, 2014 6:27:33 PM							
	Collection date: Sep 30, 2014 6:27:33 PM	101						
Close								

Figure: Custom Attributes Tab

## 6.3.9 Roles

JDisc Discovery assigns roles (for example 'database server', 'domain controller', etc.) to device during discovery. The *Roles* tab displays roles assigned to a device.

Device Details for 'teetee-pc.fritz.box'	
General Networking Hardware Firmware Software User Virtual Computers Custom Attributes Koles Groups Analyze	
-	
riter:	
Case sensive men	
Role	
Database server	
Total 1 role 1 0 roles selected	
Close	

#### Fig: Roles tab

#### 6.3.10 Groups

During the discovery process, JDisc Discovery assigns devices to groups (Refer to the Grouping chapter 3.3 for more details. The *Groups* tab displays groups to which a device it assigned.

Device Details for 'teetee-pc.fritz.box'	
General Networking Hardware Firmware Software User Virtual Computers Custom Attributes Roles Groups Analyze	
Filter:	
Group Name	
Company » EMEA » Germany » Cologne » Client Network	
Total 2 device groups   0 device groups selected	



## 6.3.11 Analyze

The *Analyze* tab consists of four sub-tabs that focus on troubleshooting and diagnosing the discovery.

- Discovery Log
- Protocols
- Parsing Issues
- Diagnostics

6.3.11.1 Discovery Log

The *Discovery Log* tab displays the sequence of activity during discovery of a device including errors and warnings when encountering unexpected results. The *Discover Log* is the most important tool to troubleshoot discovery problems.

Device Details for 'teetee-pc.fritz.box'       □ </th							
Discovery Log Protocols Parsing Issues Diagnostics							
	Timestamp	102					
	2014-03-04 17:25:22.758 2014-03-04 17:25:22.758	Discover device 192. 168. 178. 20 Version	<u>^</u>				
Anonymous NetBIOS detection     SMB anonymous protocol test     ■	2014-03-04 17:25:22.758 2014-03-04 17:25:22.758	Product: JDisc Discovery Version: 3.0					
Telnet banner detection SNMP protocol test	2014-03-04 17:25:22.758 2014-03-04 17:25:22.758 2014-03-04 17:25:43.19	Build: 3027 Check Protocols Identify device: StandardDeviceIdentifier					
WBI protocol test	2014-03-04 17:25:43.19 2014-03-04 17:25:43.19	Devices with mac addresses: 1 found Device 1: teetee-pc.fritz.box					
DNS detection Getting Basic Information	2014-03-04 17:25:43.19 2014-03-04 17:25:43.19	Devices with IP4 addresses: 1 found Device 1: teetee-pc.fritz.box					
	2014-03-04 17:25:43.19 2014-03-04 17:25:43.19 2014-03-04 17:25:43.19	Devices with computer name: 1 round Device 1: teetee-pc.fritz.box Devices with IP6 addresses: 0 found					
	2014-03-04 17:25:43.19 2014-03-04 17:25:22.762	devices to delete: 0 found Anonymous NetBIOS detection					
	2014-03-04 17:25:22.805 2014-03-04 17:25:22.805	Successful anonymous NetBIOS connection Type: Computer					
Discover Device     Device	2014-03-04 17:25:22.805 2014-03-04 17:25:22.805 2014-03-04 17:25:22.805	Computer Name: TEETEE-PC Operating System OS Family: Windows	-				
Correction 17.23.22.003 Correling, windows							
Close							

Figure: Discovery Log Tab

## 6.3.11.2 Protocols

The *Protocols* tab displays all protocols including the protocol status. The protocol status can help finding discovery problems, such as firewalls, incorrect credentials, etc.

Device Details for 'teetee-pc.fritz.box'   General Networking Hardware Firmwar  Discovery Log Protocols Parsing Issue	Software User Virtual Computers Custom Attributes Roles Groups Analyze     Softwares	
Filter:		
Case sensitive filter		
Protocol	Protocol Status	
DNS	Timeout	
нттр	Timeout	
HTTPS	Timeout	
NetBIOS anonymous	Success	
Remote login	Protocol not tested	
Remote login admin	Success	
SMB anonymous	Multiple connections to a server or shared resource b	
SMB authenticated	Success	
SNMPv1	Timeout	
SNMPv2c	Timeout	
SNMPv3	Access credentials missing	
SSH	Protocol not tested	
Telnet	Protocol not tested	
Telnet banner parsing	Protocol not supported	
VMware VIM API	Port unreachable	
WBEM	Port unreachable	
WMI	Success	
Total 17 device protocols   0 device p	rotocols selected	
	Close	

Figure: Protocols Tab

### 6.3.11.3 Parsing Issues

To retrieve hardware, software and configuration information, JDisc Discovery executes system commands on Unix and MAC OS X computers, parses the command output and stores the information in the database.

The output format of system commands often depends on the operating system version. Though JDisc Discovery detects many system commands outputs on supported platforms, operating system updates can change the system command output formats unexpectedly. In such a case, JDisc Discovery might fail to parse the command output. Therefore JDisc Discovery stores system command output in the database, when parsing fails. The system command output is then visible in the *Parsing Issues* tab and helps JDisc Discovery's support to integrate the new format in future product versions.

D Device Details for 'RackServer-4'							
General Networking Hardware Firmware Software User Virtual Computers Custom Attributes Roles Groups Analyze							
Discovery Loa Protocols Parsing Issues Diagnostics							
-Parsing issues							
Unknown Command Outputs     Iname is non-existent for this module     The list of the same 12							
Close							
UUSC							

#### Figure: Parsing Issues Tab

#### 6.3.11.4 Diagnostics

JDisc Discovery features a rule based expert system to help troubleshooting discovery problems. Built-in rules (based on experience) help identifying and resolving discovery problems quickly.

Choose the *Diagnostics* tab to display problems and recommendations for the selected device. Double click on an item in the *Diagnostics* tab to display detailed information.

\$\f → \$\@\D \$\U \$\U \$\U \$								
General Networking Hardware Firmware Software User Virtual Computers Custom Attributes Roles Groups Analyze								
Discovery Log Protocols Parsing Issues Diagnostics								
Filter:								
Case sensitive filter								
Description								
Enter Windows domain login credentials								
и и и и и и и и и и и и и и и и и и и								
Total 1 diagnostic message   0 diagnostic messages selected								
Close								

Figure: Diagnostics Tab

# 6.4 Virtualization Explorer

Use the JDisc Discovery *virtualization explorer* in order to browse your virtual environments. The virtualization explorer provides a tree with the different virtualization technologies together with their topology (including datacenters, cluster, physical hosts and virtual machines).

Fig: Virtualization Explorer

The virtualization explorer lists the virtualization technologies within a tree:

- **I**: Management servers for a virtualization technology (for instance vCenter installations)
- 💷: Virtual datacenters
- 둼: Cluster
- I Physical server hosting virtual machines

# 6.5 Send Reports Via EMail

JDisc Discovery allows automatic and scheduled emailing of any report into comma separated value or Microsoft Excel formatted files. Often time administrators want to share the most recent inventory information with their colleagues from other organizations. The simple CSV or Microsoft Excel formats make the inventory information directly usable for IT personnel that is not used to run or do not have access to JDisc Discovery.

JDisc Discovery can automatically send out any report table as an attachment file to desired recipients email addresses. To break down the feature components, the following steps show how the feature can be utilized.

## 6.5.1 Configure The Mail Server

As in regular email services, there must be an email address for the server. In order to do that, the sender's email address properties must be configured. To do so, under *Administration* menu, choose *Manage Mail Accounts* menu item.

D Manage Mail Accounts							
Mail accounts are used to se							
Name	Sender E-Mail	Add					
		Remove					
		Change					
		Test					
<		>					
	Ok Cancel						

Fig: Manage your mail servers and accounts

Clicking on *Add* buttons takes you to the dialog where you can setup the reports sender email address.

D Add New Mail Acco	unt X
New Mail Account	
Name	
Sender E-Mail	
Password	
Port	587
Mail Server	
Authentication Protocol	password ~
Encryption Protocol	STARTTLS ~
	Ok Cancel

Fig: Add a new mail server and account

Once a sender is added to the list, it can be tested using the *Test* button to make sure that its credentials are correct and a successful connection can be established.

## 6.5.2 Scheduling A Report

Now that you have a working sender email, you can send any scheduled report. For instance, open the report *Devices* » *Virtualization* » *Virtual Instances* and select the clock icon:

🕽 Virtual Computers 🛛 🕂				_		$\times$			
Filter: Case sensitive filter									
Name	IP Address	Туре	OS Version						

Fig: Schedule a Report Export or Mail Message

From the appeared dialog, select Send report via email option.



Fig: Send Report via EMail

Now a wizard will walk you through four steps in order to configure your scheduling, email content, report file properties and report email recipients.

## 6.5.2.1 Scheduling

Here you decide how often you would like to send your report to the corresponding recipients. In the following screenshot you see that it is set to be sent every 2 minutes starting from 6 PM, second of February 2016 which is relatively a high frequency of

sending.

D Mail Wizard	$\times$
Mail Schedule	
Specify the time and the date of the report in order to be mailed.	
Schedule type Recurring ~	
Run every 0 day(s) 0 hour(s) 2 minute(s)	
First execution at 2/2/16	
6:00 PM	
Back Next Finish Cano	el

Fig: Schedule Mail Messages

#### 6.5.2.2 Mail Content

The second page allows you to select the sender's email address among the list of senders that you had setup in the first step (*Configuring a sender*) and there fields to choose the subject and the message content of your email to the recipients.

丿 Mail W	/izard	×
Mail Config	guration	
Enter sub	pject of the mail and the corresponding message.	
Sender	pedram.khoshdani@jdisc.com ~	
Subject		
Message		
		1
	Back Next Finish Cancel	

#### Fig: Configure the Mail Message

#### 6.5.2.3 Export Settings

In the third section, the report file must be given a name and you can choose Excel or CSV as the file format. If CSV is chosen as the file format, you can freely choose your desired column separator. Other options such as *Multiple lines per item* and *Human readable values* help you better organize your data format. If the report is empty and contains no entry, you are still able to send it by checking the *Send empty report* checkbox. Otherwise, JDisc Discovery discards the mail.

🕽 Mail Wizard		×
Attachement File Configuration		
Specifiy the export format and configur	ation.	
File name		]
Export format	Excel 🖂	
Column separator	~!~	
Multiple lines per item (if needed)		
Human readable values (e.g. 4.5Mb	instead of 4718592 bytes)	
Send empty report (empty reports	are also sent)	
Zipping and Encryption		
Unzipped		
◯ Zipped		
OZipped & Encrypted		
Password		1
Repeat password		
	De de	Can I
	Back Next	Finish Cancel

Fig: Configure the Export Settings

Optionally, you might choose a ZIP file for compression and encryption.

6.5.2.4 Selecting recipients of the desired report

On the last page, you can add the recipient list. There are three ways to do so. You can add your recipients by clicking on the *Add* button which this is handy when doing for the first time or sending to only a few number of recipients. But you can also add them using the *Import* button which essentially allows you to import a text file with recipients email addresses on each line.

If this is not your first time adding your recipients, then you can take advantage of browse feature. Click on the *Browse* button in order to select the list of recipients from the list of already existing email addresses.

D Mail Wizard	×
Recipients Email Addresses	
Recipient Mail(s)	Add
	Remove
	Change
	Import
	Browse
Total 0 Mail account infos   0 Mail account infos selected	
Back Next Fit	nish Cancel

Fig: Add the Mail Recipients

By choosing *Finish*, the scheduled report is done and your recipients should receive automated emails containing the corresponding report based on the scheduled set.

## 6.5.3 Remove/Change Your Scheduled Report

If you intent to modify or remove your existing scheduled reports, you can simply choose *Administration* » *Manage Scheduled Mail Report Jobs* in order to modify existing scheduled mail jobs.

D Mail Report Jobs			- D >	<
Filter:				
Case sensitive filter				
Report Title	Filename	Schedule	Exp Remove	
Virtual Computers	Demo	run every 2 minutes	Exc Change	
<			>	
Total 1 mail report job   1 m	ail report job selected			
		Close		

Fig: Manager your scheduled Mail Jobs

Choose *Remove* in order to remove the scheduled report job or *Change* in order to modify its configuration.

# 6.6 Scheduled Report Export

JDisc Discovery allows automatic and scheduled exporting of any report into comma separated value or Microsoft Excel formatted files. Often time administrators want to share the most recent inventory information with their colleagues from other organizations. The simple CSV or Microsoft Excel formats makes the inventory information directly usable to IT personnel that are not used to run or do not have access to JDisc Discovery.

JDisc Discovery can automatically and scheduled export any table based report to a defined network location (e.g. a network share or a local directory on the discovery server).

## 6.6.1 Scheduling The Export

The scheduled report export preserves the column sort order and all selected filters.

Click the schedule report icon 🖾 from the report's toolbar to configure the automatic and scheduled export.

🕽 Virtual Computers				_	$\times$
⇔ ←→¢ ≙ ∿ ₹∎ <mark>©</mark> ₀ ∴					
Filter:					
Name	IP Address	Туре	OS Version		

Fig: Schedule report export

And then from the opened menu select the *Export report to disk* option.



Fig: Export report options menu

The Scheduled Report Export configuration wizard allows adjusting these settings:

- The report export schedule
- The export options (such as export format, separator characters, etc.)
- The export destination (where to export the report to e.g. a Windows share or a local folder on the discovery server)

Configure the report export schedule in the *Export Schedule* group.



Fig: Report Export Schedule Panel

Enter a descriptive name in the *Export job name* field. This name will help you to locate the report export job later on to modify parameters or to delete the job.

JDisc Discovery creates the report file name from the *Base filename* and appends the time when exporting the report to file. This way you can keep multiple revisions of the report in the same directory.

The export options are

- Use multiple lines per device or item
- Create human readable values (e.g. 4.5Mb instead of 4718592 bytes)
- Keep a history of exported report files
- The export format (Comma Separated Values or Microsoft Excel)

Report Export Wiz	zard				×
Export Configuration					
Specifiy the file prope	erties and configurations.				
Export job name	Monthly All Devices Report				
Base filename	AllDevicesMonthly				
Multiple lines per Human readable v Create a new file f Keep at most	item (if needed) values (e.g. 4.5Mb instead of 4718592 bytes) for every export 30 ♀ revisions				
Export format Column separator Null value	Excel v       r <null></null>				
		Back	Next	Finish	Cancel

Fig: Export Configuration

The export destination designates where to store exported report files. Two storage destination options are available:

- A local directory on the discovery server (type *Local Disk*)
- A Windows network share (type *Windows Shared Drive*)

A user name and password are required to access a Windows networks share during the export.

Click the *Test* button to check if the write access to the destination directory succeeds.

Enable the *Use existing* storage location option in the *Export Destination* group to export the report into an existing storage location. It is a good practice to use meaningful and descriptive names when creating new storage locations.

D Report Export Wizard				×
Export Destination				
• Create a new storage location				
O Use existing storage location				
Descriptive name Accounting Report Share				
Type Windows Shared Drive $\sim$				
Enter a network location				
Network Incetion Viaccounting/Reports/Inventory				
Login COMPANY (ADMINISTRATOR				<b>T</b> 1
Password				Test
Comment				
	Back	Next	Finish	Cancel

Fig: Export Destination

## 6.6.2 Manage Report Export Jobs

You can manage your existing report export jobs from the *Administration* menu. Select *Administration* » *Manage Scheduled Report Export Jobs* to change settings or delete existing report export jobs.

Fig: Open the Manage Scheduled Report Export Jobs DialogThis opens the *Report Export Jobs* dialog that displays all existing report export jobs. Select a report export job to and click *Change* to modify its settings or *Remove* to delete the report export job. Refer to chapter 6.6.1 for how to configure report export jobs.

#### 6.6.3 Manage Storage Locations

Storage locations describe a directory and required access credentials to store reports. While storage locations can be created when scheduling new report export jobs, you can also add, change and delete existing storage locations from the *Manage Storage Locations* dialog.

# 6.7 Custom Reports

JDisc Discovery offers a variety of built-in reports. However, if these do not fit your needs, you can create your own reports using JDisc Discovery custom reporting feature.

Custom reports can be created with three levels of visibility to other users:

• *Private* custom reports can only be executed by the creating user.

- *Group* custom reports can be executed by all users in the same group.
- *Global* custom reports can be executed by all users.

Custom reports can be organized in a hierarchy.

### 6.7.1 Create Custom Reports

Select Devices » Custom Reports to open the Custom Reports dialog.

Custom Reports	
Private Reports	Add
Group Reports	Add Folder
	Clone
	Remove
	Change
	Run
	Export
	Import
Close	

Figure: Custom Reports Dialog

Click Add Folder to add a new folder to the report hierarchy.

Select a visibility category in the left panel of the dialog and click *Add* to create *a* new custom report. Enter a report name and description and click *Next*.

leport Prope	rbes
Name	Devices with part number
Description	This report contains a device list with part numbers.
	Back Next Finish Cancel

Select attributes to display in the custom report. Attributes are categorized into:

- *Device Attributes* include Windows computer name, IP address, model, manufacturer, etc.
- *Software* attributes are comprised of operating system information, applications, application instances, patches, services, drivers, and processes.
- *Firmware* attributes include firmware information, such as BIOS name, version, etc.
- Hardware attributes represent hardware, such as processor, memory, disks, etc.
- *Networking* attributes include IP and MAC addresses, Windows network neighborhood and SNMP system group information.
- User attributes include logged on users, local users and logged on user history.
- Virtualization attributes include virtual computers and physical host details.
- *Attached Devices* represent attributes of directly attached devices (such as monitors).
- *Custom Attributes* include the folder hierarchy and attribute names of existing custom attributes.

Most of the attributes can serve as filter criteria to restrict the report to devices that match the specified criteria. If you do not enter any filter, all devices will be displayed in the custom.

Computer Name     Organization     Organization	Â	Name contains
Type     Wodel     Wanufacturer     Serial Number     Part Number     Roles     Last Discovered     Discovery Duration     Database Duration     Software	Е	Conditions (Connected with OR)
al-Hardware ∃Networking al-User alVirtualization	-	Total 0 conditions   0 conditions selected

Figure: Custom Report Attributes

Click *Next* to change the attribute order, if desired. Use *Move up* and *Move down* to change the attribute order as desired.

Move down

Figure: Attribute Order

## 6.7.2 Run Custom Reports

Open the *Custom Reports* dialog from *Devices » Custom Reports,* select a report and click *Run*. The custom report will be displayed in a new window.

Private Reports Group Reports Global Reports L Devices with part number	This report contains a device list with part numbers.	Add Add Folder
		Clone
		Remove
		Change
		Run
		Export
		Import

Figure: Run a Custom Report

#### 6.7.3 Modify Custom Reports

Open the *Custom Reports* dialog from *Devices » Custom Reports,* select a report and click *Change* to modify the report.

Clone
Remove
Change
Run
Export
Import



## 6.7.4 Remove Custom Reports

Open the *Custom Reports* dialog from *Devices » Custom Reports,* select a report and click *Remove* to delete the selected report.

## 6.7.5 Export And Import Custom Reports

Custom reports can be exported into XML formatted text files that can be imported into another JDisc Discovery installation. This way custom reports can be exchanged easily.

Select a report to export, click *Export*, select a file name and click *Save* to export the report.

Private Reports Group Reports Global Reports	This report contains a device list with part numbers.	Add
		Add Folder
		Clone
		Remove
		Change
		Run
		Export
		Import

Figure: Export a Custom Report

To import a custom report from file, select a visibility category (*Private Reports, Group Reports,* or *Global Reports*) in the left panel *and* click *Import* to select the custom report file to import.

Private Reports	Add
Group Reports	Add Folder
±	Clone
	Remove
	Change
	Run
	Export
	Import
	h

Figure: Import a Custom Report
# 7.1 Background

The WBEM (Web Based Enterprise Management) defines a set of standard to simplify network management in heterogeneous network environments. The WBEM protocol is based on the Common Information Model (CIM) which defines the schema for your IT infrastructure. WBEM is widely used on many Unix operating systems, but also on infrastructure components such as routers or switches.

WMI (Windows Management Instrumentation) is Microsoft's technology which is not compatible with WBEM, but widely uses the same information model. WMI is the primary source for hardware, configuration and software information on Windows computers.

## 7.2 CIM Object Model

The data model of WMI and WBEM consists of classes (comparable to classes in modern programming languages), instances and relations. Classes identify the information schema by defining attributes (state) and methods (behavior) of classes. For instance a class that defines a process might have the process id, the process name, the user starting the process and the command line parameters as properties. The method 'kill' let's users kill a specific process. Classes are usually derived from base classes and share their state and behavior.

WBEM and WMI organize classes in so called 'namespaces' that organize classes in a hierarchy. There exist also manufacturer specific namespaces.

### 7.3 Browser

JDisc Discovery provides a WBEM/WMI browser that allows displaying raw WMI and WBEM information. The navigation tree in the browser's left panel displays the hierarchy of namespaces and all classes that belong to the selected namespace.

The browser supports the WMI on Windows as well as the WBEM protocol on Unix operating systems.

Choose the *Troubleshooting* » *WBEM/WMI Browser* context menu from within any device report to open the WBEM/WMI Browser for the selected device.

Filter:								
Case sensitive filter								
Name		IP Addres	s	Manufacturer		Model	Туре	
XenInstance-9							Xen Instan	έ.
3comtest		192.168.1	78.16	3COM		SuperStack 3 Switch 4300	Switch	1
				APP		Color LCD	Monitor	
tom-laptop3.fritz.box		102 100 1	70.01	Apple		MacBookPro 10, 1	Laptop	L
FibreChannelSwitch-1		Properties		Brocade		IBM_2005_16B	Fibre Chan	ł.
FibreChannelSwitch-2		Discover		Brocade		IBM_2005_16B	Fibre Chan	ł .
cisco-sw1		DISCOVER	-	Cisco Systems		C2900XL	Switch	
Firewall-1		Manage	•	Cisco Systems		PIX 501	Firewall	
firewalli.home.net		-		Cisco Systems		PIX 501	Firewall	
		Compare		Dell		2407WFP	Monitor	
192.168.178.7		Custom Attribut	es 🕨	Dell		PowerEdge T110 II	Server	
192.168.178.73				Dell		PowerEdge T110 II	Server	
Desktop-9		Connect with		Dell		Studio Hybrid 140g	Desktop	
ttrenz-PC2.fritz.box		Troubleshoot	ÞQ.	Perform SNMP Walk		Studio Hybrid 140g	Desktop	
summit1				-		Summit 48i	Routing Sw	i.
summit2	×	Delete Devices	4	Browse WBEM/WMI Data	·	Summit 48i	Switch	
summit3	<b>a</b>	<u> </u>	21D	Ping		Summit 48i	Routing Sw	i.
Desktop-4		Create Support 2				P35-DS3L	Desktop	
Desktop-5		12.251.24	0.241 🌌	I raceroute	:o	P35-DS3L	Desktop	÷
				Hewlett-Packard		HP ZR24w	Monitor	Ľ
				Hewlett-Packard		LaserJet 4100 Series	Printer	
Desktop-8		12.255.13	6.208	Hewlett-Packard		m8180.de	Desktop	
HPE49E84		192.168.1	78.43	Hewlett-Packard		OfficeJet J6400 Series	Multifunctio	)
Laptop-4		12.255.13	6.191	Hewlett-Packard		Pavilion HDX9000	Laptop	
ManagementDevice-1		12.251.24	0.235	Hewlett-Packard		Management Processor for HP Integrity and HP 9000.	Manageme	r 7
•							•	

Figure: Open WMI/WBEM Browser from the device report's context menu

This menu item opens the browser window.

Browse WBEM/WMI Data for 'tom-lap	otop3.fritz.box'		
e internet interne	Filter:		
CIMV2     Generations	Case sensitive filter		
. Security			
TerminalServices	Caption	Description	GroupName
	Logical program group "Default:Start Menu"	Logical program group "Default:Start Menu"	Start Menu
CIM_Action	Logical program group "Default:Start Menu\Programs"	Logical program group "Default:Start Menu\Programs"	Start Menu\Programs
CIM_AdjacentSlots	Logical program group "Default:Start Menu\Programs	Logical program group "Default:Start Menu\Programs	Start Menu\Programs\Accessories
CIM_AggregatePSEXte CIM_AggregateRedun CIM_AlarmDevice	Logical program group "Default:Start Menu\Programs	Logical program group "Default:Start Menu\Programs	Start Menu\Programs\Accessories\A
CIM_AllocatedResourc	Logical program group "Default:Start Menu\Programs	Logical program group "Default:Start Menu\Programs	Start Menu \Programs \Accessories \S
CIM_ApplicationSystem	Logical program group "Default:Start Menu\Programs	Logical program group "Default:Start Menu\Programs	Start Menu\Programs\Maintenance
CIM_AssociatedCoolin CIM_AssociatedMemor	Logical program group "Public:Start Menu"	Logical program group "Public:Start Menu"	Start Menu
CIM_AssociatedProces CIM_AssociatedSensor	Logical program group "Public:Start Menu\Programs"	Logical program group "Public:Start Menu\Programs"	Start Menu\Programs
CIM_AssociatedSupply -	< III		F.
( <u> </u>	Total 95 items   0 items selected		
	Clos	e	

Figure: WMI/WBEM browser window

When you expand a namespace from the WBEM/WMI Browsers' namespaces navigation panel will load all class definitions in the background. Depending on the connection speed and the number of classes existing in the namespace this might take a while .

Class definitions are represented by a capital 'C'. When you select a class the WBEM/WMI Browser will display all instances of the class in main content panel. Each instance is represented as a row within the instances table. The columns within the instances table represent the attributes of the instances' class definition.

As in any other report, you can use the toolbar icons to export WBEM/WMI class instance information to Microsoft Excel or CSV formats.

The export icon offers a convenient way to export a classes or even namespaces (including or excluding subordinate namespaces).

The export process creates a ZIP file contains a set of XML files and directories:

- Directories represent namespaces
- XML files represent instances

The WMI/WBEM export helps JDisc to extend its discovery capabilities alike SNMP walks from SNMP enabled devices.

# 8 Comparing Devices

JDisc Discovery can compare two devices and highlight the changes. Select two devices from any device report and select *Compare* » *Devices* to review the changes.

ilter:				
Case sensitive filter				
Name	IP Address	Manufacturer	Model	Туре
Jesktop-5	12.251.240.241	Gigabyte Lechnolo	gy Co P35-DS3L	Desktop
Laptop-4	12.255.136.191	Hewlett-Packard	Pavilion HDX9000	Laptop
Firewall-1	12.255.136.17	Cisco Systems	PIX 501	Firewall
firewalli.home.net	192.168.178.17	Cisco Systems	PIX 501	Firewall
192.168.178.7	192.168.178.7	Dell	PowerEdge T110 II	Server
192.168.178.73	192.168.178.73	D-1	PowerEdge T110 II	Server
Switch-11	12.251.240.107	Properties	ProCurve 2524	Switch
Switch-9	12.251.240.141	Discover	ProCurve 2524	Switch
Switch-7	12.251.240.182	Discover	ProCurve 2524	Switch
Switch-10	12.251.240.219	Manage 🕨	ProCurve 2524	Switch
Switch-8	12.251.240.145	-	re 2626	Switch
Switch-6	12.251.240.162	Compare •	Devices /e 2626	Switch
ProCurve1	192.168.178.18	Custom Attributes 🕨	ProCurve 2650	Switch
Switch-5	12.216.105.229		ProCurve 5308xl	Switch
RackServer-2	12.251.240.164	Connect with	rx2620	Server (Rac
RackServer-5	12.251.240.16	Troubleshoot	rx2660	Server (Rac
RackServer-3	12.251.240.0	riodbicshoot	rx6600	Server (Rac
RackServer-4	12.251.240.233 🗙	Delete Devices	rx6600	Server (Rac
Desktop-7	12.251.240.215	C	SS58V20	Desktop
Desktop-9	12.255.136.228	Create Support ZIP	Studio Hybrid 140g	Desktop
ttrenz-PC2.fritz.box	192.168.178.75	Dell	Studio Hybrid 140g	Desktop
summit1	192.168.178.13	Extreme Networks	Summit 48i	Routing Swi
summit2	192.168.181.2	Extreme Networks	Summit 48i	Switch
summit3	192.168.181.3	Extreme Networks	Summit 48i	Routing Swi
3comtest	192.168.178.16	3COM	SuperStack 3 Switch 4300	Switch
< III				4

Fig: Open the device compare dialog

This opens a new device details dialog that displays and highlights changes using different colors.

## 8.1 Comparing Scalar Reports

The figure below shows the device details compare dialog for two devices. Strikeout red colored text has been removed from the first device and green colored text has been added in the second device.

D Comparing Device Deta	ils for '192.168.178.7' with 'ttrenz-PC2.fritz.box'	
General Networking H	ardware   Firmware   Software   User   Virtual Computers   Custom Attributes   Roles   Groups   Analyze	
Name	192.168.178.7	
Manufacturer	Dell	
Model	PowerEdge T110 IIStudio Hybrid 140g	
Type Carriel Number	ServerDesktop	
HW Version		
Part Number	ō	
Computer Name	TTRENZ-PC2	
Directory Name	RE WORKGROUP	
Directory nume		
Creation Date	2012-0 <mark>4-19-19:25:23</mark> 1-24 07:48:36.0	
Last Discovered	201 <mark>4-03-04</mark> 2-04-19 1 <mark>7</mark> 9:2 <mark>8:04</mark> 3:56.0	
Uptime	6 days 11:57:32	
Discovery Duratio	n 00:01: <mark>5420</mark>	
Database Duration	00:00:0 <mark>0</mark> 2	
	Close	

Fig: Compare report of the operating system tab

#### 8.1.1 Comparing Tables

When comparing table based reports, JDisc Discovery adds two columns at the beginning of the table to display the comparison status. JDisc Discovery displays

- identical rows using two check-marks
- missing rows in any of the two snapshot by omitting the check-mark in the respective columns.
- a red cross for rows that contain differences and highlights the cells that contain the differences using red background color.

) Compari	ing Device Details for 'Desktop-9' with 'ttr → 🤣 🚔 I 🔁 😹 📄 I 👹 I 🗃 I 👬 I Networking Hardware Firmware Softwa	enz-PC2.fritz.box'	omputers Custom Attr	ibutes Roles Groups Analyze	
Fil	Applications Application Instant Iter: Case sensitive filter	nces   Patches   Ser	vices   Drivers   Execut	ables   Processes   Cluster Services	
	Application	Version	Manufacturer	Path	
	/ v DocProcOFolder	1.0	Hewlett-Packard	1001	
	Dvnamic HTML Data Binding	9.0.8112.16421			
	Dynamic HTML Data Binding	8.0.6001.18943			
~	/ 🗸 Fax	100.0.272	Hewlett-Packard		
	Firefox	11.0.0.4454	Mozilla Corporation	c:\program files\mozilla firefox\firefox.exe	
	GPBaseService	100.0.187	Hewlett-Packard		E
3	Google Toolbar for Internet Explorer	1.0	Google	c:\program files\google\google toolbar	
	🔀 Google Toolbar for Internet Explorer	1.0	Google	c:\program files\google\installers	
	🗸 🗸 Google Toolbar for Internet Explorer	1.0	Google	c:\program files\google\installers	
	Google Toolbar for Internet Explorer	7.3.2710.138	Google	c:\program files\google\google toolbar	
~	Google Toolbar for Internet Explorer	1.0	Google	c:\program files\google\google toolbar	
	🗸 Google Update Helper	1.3.21.111	Google		
-	Google Update Helper	1.2.183.29	Google		
	HP Customer Participation Program 10.0	10.0	Hewlett-Packard		
	HP Imaging Device Functions 10.0	10.0	Hewlett-Packard		· · ·
	initial 149 applications L0 applications selected	,			
	otal 146 applications   0 applications selected				
			Close		

Fig: Differences in a table based report

Custom attributes extend JDisc Discovery's device data model to store additional device attributes that are not included in the standard device data model. Custom attributes can either be edited manually or filled by reading values from the Microsoft Windows registry or by executing commands, scripts or binaries on Windows and Unix computers. Custom attributes can be configured to preserve the version history. JDisc Discovery then keeps track of custom attribute value changes and can display changes between different revisions.

## 9.1 Configure Custom Attributes

To configure custom attributes, open the *Custom Attributes* configuration dialog from *Devices » Custom Attributes » Configuration*. Custom attributes can be organized hierarchical allowing to group attributes that belong together.

1 C 100	Add
E-Cation	Add Folder
Room Number	Change
Guiding     Support Information     Support Contract Name     Support Provider	Remove

Figure: Custom Attributes Configuration Dialog

Click:

- Add Folder to add a new folder into the hierarchy.
- Change to modify attributes..
- *Remove* to delete attributes or folders.
- *Add* to create a new custom attribute.

JDisc Discovery supports eight custom attribute types:

- Text: text attributes can contain text of any size.
- Multiline text: multiline text attributes contain text of any size including line breaks.
- Date: attributes of type date contain date information.
- Time: attributes of type time contain time information.
- Enumeration: Define attributes having a fixed set of values.
- Integer: a number
- Currency: a currency value
- Document: An imported document

To add a custom attribute:

- Choose a type from the drop-down box.
- Define a name and optionally enter a description.
- Optionally configure to automatically collect the custom attribute..

## 9.2 Edit Custom Attributes

To edit custom attributes

- Select a device or multiple devices in any device aware report and open the *Custom Attributes » Edit context menu*.
- Select the attribute or multiple attributes to edit and click *Ok*.

Name	IP Address	Manufacturer	Model	Room Number	Building	
Desktop-2	12.251.240.197	To Be Filled By O.E.M.	To Be Filled By 🔺	Room Nr. 23	Buildung Nr. 12	
Desktop-3	12.251.240.85	To Be Filled By O.E.M.	To Be Filled By	Roo		
Desktop-6	12.251.240.37	To Be Filled By O.E.M.	To Be Filled By			
Computer-18	12.251.240.77	Sun Microsystems				
Laptop-3	12.255.136.102	Sony	VGN-SR29VN_5			
Desktop-7	12.251.240.215	Shuttle Inc	SS58V20			
		Samsung	SyncMaster			
		Samsung	SyncMaster			
FibreChannelSwitch-3	12.216.105.117	QLogic	4Gb Fibre Char			
ibreChannelSwitch-4	12.216.104.224	QLogic	4Gb Fibre Char			
Switch-1	12.216.107.24	Nortel Networks	Nortel GbE Swi' =			
Switch-2	12.216.106.203	Nortel Networks	Nortel GbE Swit			
Switch-3	12.216.105.210	Nortel Networks	Nortel GbE Swit			
Switch-4	12.216.104.37	Nortel Networks	Nortel GbE Swi			
PortServer-1	12.216.106.31	Moxa	NPort			
MultifunctionalDevice-1	12.216.106.164	Lexmark	X642e			
Printer-2	12.216.106.180	Lexmark	T640			
Printer-4	12.216.106.3	Lexmark	E240n			
Desktop-1	12.216.104.46	Lenovo	ThinkCentre As			
.aptop-1	12.216.104.16	Lenovo	ThinkPad R52			
.aptop-2	12.216.104.82	Lenovo	ThinkPad R61			
Printer-1	12.216.104.75	Konica Minolta	Magicolor 2350			
RadeEnclosure-1	12 216 106 213	TRM	BladeCenter F			

You can edit multiple custom attributes for multiple devices at once!

The *Edit Custom Attributes* dialog is divided into two panels:

- 1. The device panel on the left side displays the selected devices.
- 2. The attribute panel on the right side displays selected attributes and values.

To enter attribute values:

- Select a cell in the attribute panel and edit the cell value.
- Click the save icon 🔚 to save your attribute value changes.
- Click the cross icon × to clear values of selected cells.

When an attribute value has been changed by a different user while you have been editing the same value, JDisc Discovery displays the conflicts and prompts whether to overwrite the other user's changes or to discard your changes.

## 9.3 Configure Custom Attribute Data Collection

In addition to manually editing custom attribute values, JDisc Discovery can automatically populate custom attribute values by

- Reading the Microsoft Windows registry
- Executing binaries, scripts or system commands on target computers

Registry based custom attribute data collection is an easy way to collect attributes that JDisc Discovery does not collect out of the box. Moreover, JDisc Discovery can also populate custom attributes with command and script output.

A custom attributes' data collection method can be configured differently for each platform. You might use this flexibility to collect a computer's owner custom attribute from the registry on Windows computers but execute system commands on Unix.

Data collections can be enabled or disabled individually.

A custom attributes' data collection method can be configured differently for each platform. The platforms also include the different Windows versions such as Windows Vista or Windows XP. Only text, multiline text and integer types can be automatically populated!

Select *Keep change history for at least <n> days* to enable the change history for a custom attribute. JDisc Discovery will keeps any number of revisions for at least <n> days. Older revisions will be deleted.

Select *Automatically populate value* to turn on automatic data collection for a custom attribute.

	1
Туре	Multiline text 💌
Name	/etc/passwd file
Description	Collects the /etc/passwd file on Unix computers.
History Keep cha Data Collection	ange history for at least 10 🚖 days
Automat     Data C	ically populate value ollection Add Change Remove

Figure: Enable automatic Data Collection

The Data Collection table displays configured data collection methods for the selected custom attribute. Click *Add* or *Remove* to add new or to remove data collection methods.

#### 9.3.1 Configure Windows Registry Collection

Select Windows Registry from the Collection Method drop-down box. You can configure

registry keys and values on per Windows operating system version. For convenience, you might select *All Windows versions* to configure the same registry key and value for all Windows versions.

Select a value from the *HKEY* drop-down box and enter a registry key. To read the default value, leave the value name blank . Otherwise enter the value name.

Alternorms   Collection Method   Windows Registry   Value name   CommonFilesDir				
Collection Method Windows Registry   Platforms  All Windows Versions  Windows 2000 Windows Server 2008  Windows 2000 Windows 7  Windows 2000 Server Windows 8  Windows 2000 Server Windows 8  Windows XP  Windows Server 2012  Windows Version  Registry Data Collection  HKEY HKEY_LOCAL_MACHINE  Key name SoFTWARE/Microsoft/Windows/CurrentVersion Value name CommonFilesDir	lethod & Platfor	rms		
Platforms         ✓ All Windows versions         Windows NT 4.0       Windows Server 2008         Windows 2000       Windows 7         Windows 2000 Server       Windows 8         Windows XP       Windows Server 2012         Windows Server 2003       Windows Vista         Registry Data Collection	Collection Me	thod Windows Regi	stry -	
Windows versions         Windows NT 4.0       Windows Server 2008         Windows 2000       Windows 7         Windows 2000 Server       Windows 8         Windows XP       Windows Server 2012         Windows Server 2003       Windows Vista	Platforms			
Windows NT 4.0       Windows Server 2008         Windows 2000       Windows 7         Windows 2000 Server       Windows 8         Windows XP       Windows Server 2012         Windows Server 2003       Windows Vista	All Wind	dows versions		
Windows 2000       Windows 7         Windows 2000 Server       Windows 8         Windows XP       Windows Server 2012         Windows Vista       Windows Vista         Registry Data Collection       HKEY         HKEY       HKEY_LOCAL_MACHINE           Key name       SOFTWARE/Microsoft/Windows/CurrentVersion         Value name       CommonFilesDir		Vindows NT 4.0	Windows Server 2008	
Windows 2000 Server       Windows 8         Windows XP       Windows Server 2012         Windows Server 2003       Windows Vista         Registry Data Collection       HKEY         HKEY       HKEY_LOCAL_MACHINE ▼         Key name       SOFTWARE/Microsoft/Windows/CurrentVersion         Value name       CommonFilesDir	V	Vindows 2000	Windows 7	
Windows XP Windows Server 2012 Windows Server 2003 Windows Vista  Registry Data Collection  HKEY HKEY_LOCAL_MACHINE  Key name SOFTWARE/Microsoft/Windows/CurrentVersion Value name CommonFilesDir	V	Vindows 2000 Server	Windows 8	
Windows Server 2003 Windows Vista  Registry Data Collection  HKEY HKEY_LOCAL_MACHINE Key name SOFTWARE/Microsoft/Windows/CurrentVersion Value name CommonFilesDir	V	Vindows XP	Windows Server 2012	
Windows Vista  Registry Data Collection  HKEY HKEY_LOCAL_MACHINE Key name SOFTWARE/Microsoft/Windows/CurrentVersion Value name CommonFilesDir	V	Vindows Server 2003		
HKEY     HKEY_LOCAL_MACHINE       Key name     SOFTWARE/Microsoft/Windows/CurrentVersion       Value name     CommonFilesDir	V	Vindows Vista		
Value name CommonFilesDir	Registry Data Co	ollection		
	Registry Data Co HKEY Key name	HKEY_LOCAL_MACH		
	Registry Data Co HKEY Key name Value name	HKEY_LOCAL_MACH SOFTWARE Wicrosof	INE   IWindows \CurrentVersion	
	Registry Data Co HKEY Key name Value name	HKEY_LOCAL_MACH SOFTWARE\Microsof CommonFilesDir	INE  IWindows \CurrentVersion	
	Registry Data Co HKEY Key name Value name	Illection HKEY_LOCAL_MACH SOFTWARE\Vicrosof CommonFilesDir	INE	
	Registry Data Co HKEY Key name Value name	Illection [HKEY_LOCAL_MACH SOFTWARE(Vicrosof CommonFilesDir	INE	
	Registry Data Co HKEY Key name Value name	Ilection HKEY_LOCAL_MACH SOFTWARE (Vicrosof CommonFilesDir	INE	
	Registry Data Co HKEY Key name Value name	Ilection HKEY_LOCAL_MACH SOFTWARE (Microsof CommonFilesDir	INE	
	Registry Data Co HKEY Key name Value name	Ilection HKEY_LOCAL_MACH SOFTWARE (Microsof CommonFilesDir	INE	
	Registry Data Co HKEY Key name Value name	Illection HKEY_LOCAL_MACH SOFTWARE (Microsof CommonFilesDir	INE	

Figure: Windows Registry Custom Attribute Data Collection

#### 9.3.2 Configure Remote Command Execution

Custom attribute data collection can use JDisc Discovery's remote login capabilities. When remote login is enabled, JDisc Discovery can log on to target computers, optionally copy data collection scripts or binaries and finally execute commands. When a command has been executed successfully the console output is captured and stored in the custom attribute. When a command fails to execute the console output appears in the *Parsing Issues* tab of the Device Details dialog.

JDisc Discovery supports the following command execution types:

- Execute a built-in system shell command (such as Is on Unix, or dir on Windows) or a standard system command.
- Execute custom binaries (.exe files or binary executables for Unix)

- Execute custom Visual Basic Scripts (.vbs)
- Execute custom Windows batch files (.bat)
- Execute custom Windows CMD files (.cmd)
- Execute custom Windows Powershell scripts (.ps1)
- Execute custom Unix shell scripts

To import scripts or binaries, open the *Custom Attribute Data Collection* dialog from *Discovery* » *Custom Data Collection* » *Custom Attribute Data Collection*. Imported binaries and scripts are stored in JDisc Discovery's database and will be preserved when archiving and restoring databases.

Name	^		Command lin	ne		Add
etc passwd			cat /etc/pas	swd		Remove
						Change
						ų
						Export
						port
•					Þ	
∢	III ary   1 script or bina	ry selected			Þ	
∢ otal 1 script or bina	III ary   1 script or bina	ry selected			+	
<ul> <li>Total 1 script or binal</li> </ul>	III ary   1 script or bina	ry selected			•	
< ☐ otal 1 script or bina	ווו ary   1 script or bina	ry selected			4	
<	ווו ary   1 script or bina	ry selected			• E	
< ☐ iotal 1 script or bin	ייי	ry selected			• 	
< otal 1 script or bin	ייי	ry selected			4	
< Total 1 script or bin	ייי	ry selected			4	

Figure: Configure Custom Attribute Data Collections

#### IIIII BE CARFUL IIIII

Always be careful when importing scripts or binaries into JDisc Discovery. Make sure your scripts and binaries are checked by your favorite anti-virus software. Otherwise you might risk to spread viruses over your network!

Make sure your homegrown scripts or executables run as fast as possible and do not hang in any case. Intensive testing is recommended before deploying your own scripts or binaries to your productive environment.

Each custom attribute data collection delays the discovery of a device while the script or binary runs (or until the timeout kills the

To add a new data collection script or binary supply these attributes:

- Type
- Name: The name that identifies this data collector.
- Description: An optional description.
- Filename: The file name that references the script or binary to be copied to target computers.
- Command line: The command line to execute after the binary or script has been transferred to target computers.
- Script code: This field contains the script code when one of the script options is selected.

Scripts and binaries can be used for custom attribute data collection.

Select *Execute Command* from for the *Collection Method* drop-down box. The *Execute* area displays configured custom data collections. For convenience, you can add new scripts or binaries by clicking *Add*.

Select the operating systems and data collectors as appropriate.

ethod & Platforms				
Collection Method Execute Comm	nand 👻			
Platforms				
All Windows versions		V HP-UX		
Windows NT 4.0	Windows Server 2008	AIX		
Windows 2000	Windows 7	Linux		
Windows 2000 Server	Windows 8	MAC OS X		
Windows XP	Windows Server 2012	Solaris		
Windows Server 2003		VMware ESX Server		
Windows Vista		Oracle VM Server		
		Citrix YenServer		
xecute	elected platforms			
	elected platforms		Ture	Add
Name 'show startus' for Cisco IOS	d	command line	l ype	Auu
show version' for Cisco ASA	si	how version	Sytem	
	s	how version	Sytem	
show version' for Cisco IOS		how version	Sytem	
'show version' for Cisco IOS 'show version' for Cisco PIX OS 'show version' for ProCurve	SI	how version	SVID-00	
'show version' for Cisco IOS 'show version' for Cisco PIX OS 'show version' for ProCurve Command 'show tech'	sr sl sl	how version how tech	Sytem -	
'show version' for Cisco IOS 'show version' for Cisco PIX OS 'show version' for ProCurve Command 'show tech' etc passwd	si si ci	how version how tech at /etc/passwd	Sytem - Sytem -	
show version' for Cisco IOS 'show version' for Cisco PIX OS 'show version' for ProCurve Command 'show tech' etc passwd ∢	si si ci III	how version how tech at /etc/passwd	Sytem Sytem Sytem ▼	
show version for Cisco IOS show version for Cisco PIX OS 'show version' for ProCurve Command 'show tech' etc passwd 4 [ Total 11 scripts or binaries   1 script of	si si m m pr binary selected	how version how tech at /etc/passwd	Sytem Sytem	
show version for Cisco IOS show version for Cisco PIX OS 'show version' for ProCurve Command 'show tech' etc passwd 4 Total 11 scripts or binaries   1 script of	si si si mi si binary selected	how version how tech at /etc/passwd	Sytem ← Sytem ← Sytem ←	

Figure: Configure Custom Attribute Data Collection

When a script or binary is referenced by more than one custom attribute it will be copied only once to a target system saving network bandwidth and speeding up the discovery process.

The working directory for script or binary execution is a directory within the temporary session directory.

#### 9.4 Review Custom Attributes

The *Device Details* dialog displays the values of all successfully collected custom attribute from within the *Custom Attributes* tab. Furthermore custom attributes can be used from custom reports as any other device attribute.

#### 9.4.1 Device Details

Open the *Device Details* dialog and select the *Custom Attributes* tab. The navigation tree in the left panel displays the custom attribute hierarchy. Select a folder to display custom attributes. Each custom attribute is identified by its name, its last modification date and in case of multiple revisions the number of revisions.

Device Details for 'invicvs'		
	🔊 📄 👹 🗊 🚠	
General Networking Hards	ware   Firmware   Software   User   Virtual 0	Computers Custom Attributes Roles Groups Analyze
		avahi:x:105:107:User for Avahi:/var/run/avahi-daemon:/bin/false
		bin:x:1:1:bin:/bin:/bin/bash
		daemon:x:2:2:Daemon:/sbin:/bin/bash
		dnsmasq:x:104:65534:dnsmasq:/var/lib/empty:/bin/false
		ftp:x:40:49:FTP account:/srv/ftp:/bin/bash
		games:x:12:100:Games account:/var/games:/bin/bash
		haldaemon:x:102:105:User for haldaemon:/var/run/hald:/bin/false
		lp:x:4:7:Printing daemon:/var/spool/lpd:/bin/bash
		mail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/false
	Collection date: Oct 1 2014 2:45:15 PM	man:x:13:62:Manual pages viewer:/var/cache/man:/bin/bash
	Collection date: Oct 1, 2014 2.45.15 PM	messagebus:x:100:101:User for D-Bus:/var/run/dbus:/bin/false
		news:x:9:13:News system:/etc/news:/bin/bash
		nobody:x:65534:65533:nobody:/var/lib/nobody:/bin/bash
		ntp:x:/4:103:NIP daemon:/var/11D/ntp:/bin/raise
		poixituser:x:101:104:Poiicykit:/var/run/Poiicykit:/bin/false
		postik.x.si.si.postik baemon./va/spool/postik./bin/iaise
		robt.x.0.0.100t./fot./bin/bash
		ssnd:X:/I:65:55H daemon:/Var/IID/ssnd:/Din/Taise
		suse-ncc.x.103.106.Noveri Customer Center Oser./var/115/14312/Suse-ncc-Taken
		www.unrw.30.8:WWW daemon anache:/war/lib/wwwrunr/bin/false
	•	( III )
		Close

Click the revisions link to open a new dialog displaying all collected revisions including heir values. Select a date to review the custom attribute value from that time.

Versions for Custom Attribute	ite 'Show Tech'				X
Collection Time		Mwe 0026d0dd 0097930c	0056ed50	0 009753a4	1606 🔺
Sep 21, 2010 2:46:34 PM		Lwe 0030cad6 00a2ba1c	00585368	0 00a2aba4	3704
Sep 21, 2010 2:44:52 PM		Lwe 0030cd0e 00a2cacc	00585a98	0 00a2bc54	3704
		Hwe 0011fa67 00a368cc	0051bc10	0 00a32ee4	1450
		Csi 003048fb 00a37eec	0056ed50	0 00a36f94	3540
		Hwe 002ef791 00a620cc	0054e100	0 00a5e244	1588
		Hwe 003fdf05 00a641cc	007fc208	0 00a622f4	7896
		Hwe 0041553a 00a6531c	00567c88	0 00a643a4	3960
		Hsi 001e7d4e 00a66fdc	0056ed50	0 00a66064	3928
	Show Tech	Crd 001e7d03 00a6809c	0056f1c8 1104313	0 00a67114	3584
	Collection date: Sep 21, 2010 2:46:34 PM	Lsi 001e7dbd 00a6913c	0056ed50	0 00a681c4	3848
		Cwe 001f2705 00a7f284	008392b8	0 00a7d31c	8040
		Mwe 004152aa 00a80324	00837340	0 00a7f3ec	3896
		Msi 003ba8a1 00a81434	0056ed50	0 00a804bc	3888
		Cwe 001e99a9 00a8763c	0076f9d8 56	0 00a85744	7212
		Mwe 004152aa 00a8874c	008372f8	0 00a87814	3896
		Msi 003ba8a1 00a8985c	0056ed50	0 00a888e4	3888
		Hwe 004152aa 00aa5184	00837268 31	0 00aa47dc	904
		Hwe 004152aa 00aa5dbc	00837260	0 00aa5a74	840
		Hwe 003fe199 00aa6924	007e7800	0 00aa62dc	1196
		Hwe 003fe199 00aa722c	007e7708	0 00aa6be4	1196
		MWe 0038707e 00aa97ac	0056ed50	0 00aa7834	7960
		H- UUSIEDA/ UU091120	00566038 8	0 00a2ee04	3364
					-
	•				•
L]		Close			
		CIUSE			

Figure: Versions with Collection Data for Attribute 'Show Tech'

Select two revisions and click the Compare button he from the toolbar to open a new dialog displaying the differences between the two revisions.

Changed lines are highlighted with red background. Missing lines on either side are highlighted with yellow background. You can use the toolbar buttons or these keyboard strokes: F3 (next diff) and Shift-F3 (previous diff) to jump to the next or previous difference.





## 9.5 Import Custom Attributes

JDisc Discovery can import custom attributes from a comma separated text file.

#### 9.5.1 The Import Process

An import file can contain values for exactly one custom attribute, but for multiple devices. Each line consists of a *device identifier* and the actual custom attribute value. The device identifier and the custom attribute value are separated by a comma (',').

A device identifier can be one of the following:

- An IP4 address
- An IPv6 address
- A fully qualified hostname
- A Windows computername (with or without domain)
- A hostname (without full domain information)
- A device's serial number

JDisc Discovery attempts to match the device in the database that uniquely matches the device identifier in the import file. If JDisc Discovery finds more than a single device that matches the device identifier it will ignore the line from the import file and does not assign any value to the custom attribute. To import custom attribute values, select the *Devices* » *Custom Attributes* » *Import...* menu.



Figure: Import Custom Attribute values

Select the custom attribute that you would like to import.



Figure: Select a Custom Attribute to import

Finally select the import file containing the device identifier and the custom attribute values. The import process opens a new report that displays if the import was successful or not for each line of the import file.

auccessful imports       375         alled imports       325         Device       Status       Line       Result         192.168.178.17       Image: Constraint of the state of the	
Device         Status         Line         Result           192.168.178.17         Image: Constraint of the state o	
192.168.178.4       Image: Successfully identified 'cisco-sw1         192.168.178.17       Image: Successfully identified 'frewalli.home.net         192.168.178.18       Image: Successfully identified 'trenz-PC2.fritz.box         trenz-pc       Image: Successfully identified 'trenz-PC2.fritz.box         Diddel Daddel       Image: Successfully identified 'trenz-PC2.fritz.box         Image: Successfully identified 'trenz-PC2.fritz.box       Successfully identified 'trenz-PC2.fritz.box         Image: Successfully identified 'size-sw1       Image: Successfully identified 'size-sw1         Image: Successfully identified 'size-sw1       Image: Successfully identified 'frewalli.home.net         Image: Successfully identified 'size-sw1       Image: Successfully identified 'trenz-PC2.fritz.box         Image: Successfully identified 'trenz-PC2.fritz.box       Image: Successfully identified 'trenz-PC2.fritz.box         Image: Successfully identified 'trenz-PC2.fritz.box       Image: Successfully identified 'trenz-PC2.fritz.box         Image: Successfully identified 'trenz-PC2.fritz.box       Image: Successfully identified 'trenz-PC2.fritz.box	
192.168.178.17       Image: Constraint of the second	
192.168.178.18       Image: Solution of the device with where hostname 'Diddel Daddel'. Could not find device with where hostname 'Diddel Daddel'. Could not find device with where solution and the solution of the solution of the device with where solution of the solution of the device with where solution and the solution of the device with where solution and the solution of the device with where solution and the solution of the device with where solution and the solution of the device with where solution and the solution of the device with where solution and the solution of the device with where solution and the solution the solution and the solution of the solution and	
trenz-pc2       Image: Constraint of the second secon	
trenz-pc       Image: Sourcessfully identified "trenz-PC2.fritz.box         biddel Daddel       Image: Sourcessfully identified "trenz-PC2.fritz.box         biddel Daddel       Image: Sourcessfully identified "trenz-PC2.fritz.box         could not find device with Windows computer name 'Diddel Daddel'. Could not find device with Windows computer name 'Diddel Daddel'. Could not find device with Windows computer name 'Diddel Daddel'.         con identifier >       Image: Sourcessfully identified 'isco-sw1         192.168.178.17       Image: Sourcessfully identified 'isco-sw1         192.168.178.18       Image: Sourcessfully identified 'irreaver12.box         trenz-pc       Image: Sourcessfully identified 'irreaver2.fritz.box         trenz-pc       Image: Sourcessfully identified 'trenz-PC2.fritz.box         could not find device with Windows computer name 'Diddel Daddel'. Could not find device with where hostname starts	
Diddel Daddel <ul> <li>Could not find device with hostname 'Diddel Daddel', Could not find device with Windows computer name 'Diddel Daddel', Could not find device with where hostname 'Diddel Daddel', Could not find device with where hostname starts with 'Diddel Daddel', Could not find device with where hostname starts with 'Diddel Daddel',</li> <li>No device value pair found!</li> </ul> <li>Start 178.4</li> <li>Successfully identified 'disco-sw1</li> <li>Successfully identified 'disco-sw1</li> <li>Successfully identified 'broCurve1</li> <li>Successfully identified 'threnz+PC2.firitz.box</li> <li>Successfully identified 'threnz+PC2.firitz.box</li> <li>Successfully identified 'threnz+PC2.firitz.box</li> <li>Successfully identified 'with obstame 'Diddel Daddel', Could not find device with Windows computer name 'Diddel Daddel', Could not find device with Windows computer name 'Diddel Daddel', Could not find device with where hostname 'Diddel Daddel', Could not find device with where hostname starts with 'Diddel Daddel', Could not find device with where hostname starts with 'Diddel Daddel', Could not find device with where hostname starts with 'Diddel Daddel', Could not find device with where hostname starts with 'Diddel Daddel', Could not find device with where hostname starts with 'Diddel Daddel', Could not find device with where hostname starts with 'Diddel Daddel', Could not find device with where hostname starts with 'Diddel Daddel', Could not find device with where hostname 'Diddel Daddel', Could not find device with where hostname starts with 'Diddel Daddel', Could not find device with where hostname starts with 'Diddel Daddel',</li>	
Kno identifier>     Image: Transmission of the second	Jeľ.
cno identifier>     8     No device value pair found!       192.168.178.14     9     Successfully identified 'cisco-sw1       192.168.178.17     0     10     Successfully identified 'frewalli.home.net       192.168.178.18     11     Successfully identified 'frewalli.home.net       192.168.178.18     11     Successfully identified 'trenz-PC2.fritz.box       trenz-pc2     12     Successfully identified 'trenz-PC2.fritz.box       Diddel Daddel     14     Could not find device with Nothame 'Diddel Daddel'. Could not find device with where hostname starts with 'Diddel Daddel'. Could not find device with where hostname starts with 'Diddel Daddel'.        15     No device value pair found!	
192.168.178.4     9     Successfully identified 'cisco-sw 1       192.168.178.17     0     10     Successfully identified 'frewalli.home.net       192.168.178.18     11     Successfully identified 'frewalli.home.net       192.168.178.18     11     Successfully identified 'trenz-PC2.fritz.box       trenz-pc2     12     Successfully identified 'trenz-PC2.fritz.box       Diddel Daddel     14     Could not find device with hostname 'Diddel Daddel'. Could not find device with where hostname starts with 'Diddel Dadde'.       coid not find device with where hostname starts with 'Diddel Dadde'.     Could not find device with where hostname starts with 'Diddel Dadde'.       coid not find device with where hostname starts with 'Diddel Dadde'.     Could not find device with where hostname starts with 'Diddel Dadde'.	
192.168.178.17     Image: 10     Successfully identified 'freewalli.home.net       192.168.178.18     11     Successfully identified 'freewalli.home.net       192.168.178.18     11     Successfully identified 'freewalli.home.net       trenz-pc2     Image: 12     Successfully identified 'trenz-PC2.fritz.box       trenz-pc     13     Successfully identified 'trenz-PC2.fritz.box       iddel Daddel     14     Could not find device with Nostname 'Diddel Daddel'. Could not find device with Windows computer name 'Diddel Daddel'. Could not find device with where hostname starts with 'Diddel Dadde'. <no identifier="">     15     No device value pair found!</no>	
192.168.178.18     Image: State St	
ttrenz-pc2 © 12 Successfully identified 'ttrenz-PC2.fritz.box ttrenz-pc © 13 Successfully identified 'ttrenz-PC2.fritz.box Diddel Daddel 14 Could not find device with hostname 'Diddel Daddel'. Could not find device with where hostname 'Diddel Daddel'. Could not find device with where hostname 'Diddel Daddel'. Could not find device with where hostname starts with 'Diddel Daddel'.	
trenz-pc © 13 Successfully identified 'trenz-PC2.fritz.box Diddel Daddel U 14 Could not find device with hostname 'Diddel Daddel'. Could not find device with Windows computer name 'Diddel Daddel'. Could not find device with where hostname 'Diddel Daddel'. Could not find device with where hostname starts with 'Diddel Dadde'. So identifier> U 15 No device value pair found!	
Diddel Daddel     14     Could not find device with hostname 'Diddel Daddel'. Could not find device with Windows computer name 'Diddel Daddel'. Could not find device with were hostname starts with 'Diddel Dadde'. <no identifier="">     15     No device value pair found!</no>	
<no identifier=""> () 15 No device value pair found!</no>	Jeľ.
<no identifier=""> () 16 No device value pair found!</no>	
192.168.178.4 📀 17 Successfully identified 'cisco-sw1	
192.168.178.17 📀 18 Successfully identified 'firewalli.home.net	
192. 168. 178. 18 📀 19 Successfully identified 'ProCurve1	
trenz-nc? 🔊 20 Successfully identified 'ttrenz-PC'2 fritz hav	
	4

Figure: Custom Attributes Import Result

Each line in the Custom Attributes Import result report displays detailed information about the import process.

#### 9.5.2 Import File Format

Each line of the import file represents a single device and one custom attribute value. Custom attribute values must not span across a single line. Carriage return characters must be escaped using the '\n' character representation. JDisc Discovery supports different data types such as date, time, integer or text for custom attribute values:

- A simple text field: JDisc Discovery simply copies the value following the comma into the text field.
- A multiline text field JDisc Discovery replaces all '\n' meta-characters with a new feed character, all '\r' meta-characters with a carriage return character and all '\t' meta-characters with a tabulator character.
- An integer field JDisc Discovery parses integer values and stores them when parsed successfully.
- A date field Date fields must comply to this format: 'YYYY-MM-DD'.
- A time field

Time fields must comply to this format: 'HH:MM:SS'.

• An enumeration field The value must be one of the valid enumeration values.

# 10 Documents

JDisc Discovery can manage documents, such as device user manuals, support contracts, warranty information or any other document. You can import your documents into JDisc Discovery's database and assign them to devices.

Documents are stored in JDisc Discovery's database and are included in a database archive when you use the archive and restore functions.

## 10.1 Manage Documents

Select *Documents » Manage Documents* to add, remove or change documents. You can use folders to organize your documents in folder hierarchy.



Figure: Manage Documents Dialog

Double-click the document icon to open the document. Click *Export to* export selected documents to the local computer's file system.

### 10.2 Use Documents

You can use custom attributes to assign documents to devices. Define a custom attribute of type *Document* to hold document assignments.

ield Definitio		
Туре	Document 🗸	
Name	User Manual	
Description		

Figure: Add a new Custom Attribute of Type Document

Open the context menu from any device report and select *Custom Attributes* » *Edit* to edit custom attributes. Select the new custom attribute and click ok.

D Edit Custom Attributes			_ 0	23
Name	IP Address	User Manual		
BladeServer-3	12.216.106.32	Documents		
BladeServer-4	12.216.104.22	Hanuals		
BladeServer-5	12.216.104.88	Microsoft		
BladeServer-6	12.216.105.135	- Oracle		
BladeServer-7	12.216.106.70	Oracle Server License		
BladeServer-8		13		
BladeServer-9	12.216.104.146			
cisco-sw1	192.168.178.4			
Computer-1	12.216.105.21			
Computer-10	12.216.107.245			ŀ
				,
	Ok	Cancel		

Figure: Edit Document Custom Attributes

JDisc Discovery opens the document hierachy when editing a document attribute. Select the desired attribute and hit the *Enter* key.

Assigning documents to devices does not duplicate the document. JDisc Discovery creates an association between the document and

## 10.3 Documents And Reports

You can use custom attributes of type *Document* as any other custom attribute in your custom reports or in the device details dialog.

Double-clicking the document icon in a custom report opens the associated document.

ilter:				
Case sensitive filter				
Name	IP Address	Model	User Manual	
Laptop-3	12.255.136.102	VGN-SR29VN_S	📆 Sony laptop User Manual	-
192.168.178.7	192.168.178.7	PowerEdge T110 II	📆 Oracle Server License	-
BladeServer-3	12.216.106.32	BladeCenter HS20	📆 Oracle Server License	
		Color LCD		
		HP ZR24w		
		SyncMaster		
		SyncMaster		
		2407WFP		
		LaserJet 4100 Series		
0005CD2D0B06.fritz.box	192.168.178.57			
122.225.109.102	122.225.109.102			
128.36.47.32	128.36.47.32			
157.55.133.142	157.55.133.142			
17.172.232.128	17.172.232.128			
173.194.69.125	173.194.69.125			
173.194.69.16	173.194.69.16			
173.194.70.101	173.194.70.101			
173. 194. 70. 125	173.194.70.125			
184.91.67.19	184.91.67.19			
188.108.188.172	188.108.188.172			
188.193.131.102	188.193.131.102			
₹ <u>200,000,000,000</u>	III 100 102 200 201			
	III III			F

Figure: Custom Report with a Document

Double-click the document icon cell to open the document. Documents appear as any other custom attribute in the *Custom Attributes* tab.



Figure: Document Custom Attribute within the Device Details Dialog

# 11 Simplified File Collection

JDisc Discovery can collect the content of ASCII files and can capture text output of command line applications on Windows and Unix platforms. When the Networking Add-On is installed, JDisc Discovery can also collect configuration files and command output from many Cisco router and switches and HP ProCurve switches.

Open the *Discovery Configuration* dialog, select the *Data Collection* tab and select the *File Collection* tab from within the data collection tab..

JDisc Discovery supports two flavors of file collections:

- 1. Collect the content of ASCII files
- 2. Capture the output of command line tools

Discovery Configuration			×
General Scope Directory Data Collection Discovery Jobs	Protocols Filters SSH Keys		
Standard Custom File Collection			
Windows	Filter:		Add
	Case sensitive filter		Remove
	Name	Command	Change
	hwinfo command	/usr/sbin/hwinfo	Enable
			Disable
	Total 1 collection   0 collections	selected	
		ancel	
		ance	

Figure: File Collections

The navigation tree in the right panel displays available operating system families. To review the current collection configuration, to add new collections or to remove existing collections, select one of the platforms in the navigation tree.

Each collection can be individually enabled or disabled. Click *Enable* or *Disable* to toggle the configuration of selected collections.

## 11.1 Add New Collections

Select a platform from the navigation tree and click *Add*. Choose the desired platforms, configure history settings and select *File collection* to collect ASCII files on the hard drive or *Command execution* to capture a command's output. Enter a collection name and the full path name of the file or command. Enable *Requires administrative access* if the command or the file access requires privileged user rights.

Platforms	
All Windows versions	
Windows NT 4.0	Windows Server 2008
Windows 2000	Windows 7
Windows 2000 Server	Windows 8
Windows XP	Windows Server 2012
Windows Server 2003	
Windows Vista	
listory Veep change history for at lease File Collection	ast 90 📩 days
istory Veep change history for at lease ile Collection File collection	ast 90 💌 days
istory Very Keep change history for at lease File Collection File collection Command execution	ast 90 📩 days
iistory Keep change history for at lea ile Collection File collection Command execution Collection name hosts file	ast 90 丈 days
iistory Veep change history for at lea Veep collection Veep collection Veep collection Command execution Collection name hosts file Full path name VeSystemRoo	ast 90 days
istory Veep change history for at lease Collection Collection Collection name hosts file Full path name VecSystemRoo Requires administrative access	ast 90 days

Figure: Add Windows File Collection

JDisc Discovery supports the use of path variables such as %SystemRoot% when specifying the file name.

Always specify the full path name for file names or binaries!

## 11.2 Change Or Remove Collections

Select a platform from the navigation tree and click Change or Remove to modify or

remove the collection. Note: Built-in collections cannot be deleted. However, the history configuration can be changed for built-in collections.

# 12 Custom Software Discovery

JDisc Discovery already collects installed applications, patches, and services. However it only collects software that has been installed using the platforms standard installation procedure. Software that has just been copied to a computer will not be detected.

JDisc Discovery can be enhanced by custom scripts or binaries to improve the software discovery of non-standard installed applications. Alike custom attribute collection, custom software discovery is also copying scripts or binaries to target computers and executes them remotely. When the console output matches a well-defined XML schema, JDisc Discovery parses the output and adds the contained software entries to the device.

JDisc Discovery's built in duplicate suppression takes care about removing duplicate software entries.

#### 12.1 The XML Schema

Custom software scripts or binaries must conform to a well-defined XML schema. The XML schema consists of sections for applications (including application instances), patches and services.

For your reference: The XML schema definition is located in your installation directory within the 'schemas' directory. Refer to the schema file for a full description of all attributes!

The example below shows a XML example output :

```
<?xml version="1.0" encoding="UTF-8"?>
<software>
  <app>
    <name>Demo Application</name>
    <version>1.5</version>
    <vendor>Demo Vendor</vendor>
    <path>c:\Program Files\Demo Vendor\Demo Application</path>
    <user>testuser</user>
    <installdate>2017-12-24</installdate>
    <license>
     <productid>123455</productid>
     <productkey>ABC-DEF-GHI</productkey>
     <expires>2019-12-24</expires>
     <status>licensed</status>
     <comment>This is a temporary license</comment>
    </license>
    <instance>
     <name>Demo Applciation Instance</name>
      <type>db</type>
    </instance>
  </app>
```

```
<patch>
    <name>Demo Patch</name>
    <vendor>Demo Vendor</vendor>
  </patch>
  <svc>
    <name>DemoServiceName</name>
    <dispname>Demo Service Display Name</dispname>
    <version>5.0</version>
    <vendor>Demo Vendor</vendor>
    <path>c:\Program Files\Demo Service</path>
    <binary>c:\Program Files\Demo Service\Demo.exe</binary>
    <params>-p -q -d</params>
    <startupmode>auto</startupmode>
    <status>running</status>
    <failure>none</failure>
  </svc>
</software>
```

Simply repeat the 'app', 'patch', or 'svc' sections to add multiple applications, patches and services if returned in a single data collection execution.

## 12.2 Import Software Data Collections

Open the *Custom Software Data Collection* dialog from *Discovery* » *Custom Data Collection* » *Custom Software Data Collection* to import scripts or binaries .

Name	^	Command line	8	Add
Software Collection Scri	pt	test		Remove
Jnix Custom Collection S	Script	test		Change
				Export
< Total 2 scripts or binarie	III s   1 script or binary sele	cted	4	
			E	
4			-	

Figure: Configure Custom Software Data Collection

#### !!!!! BE CAREFUL (Part 2) !!!!!

Always be careful when importing scripts or binaries into JDisc

Discovery. Make sure your scripts and binaries have been checked by your favorite anti-virus software. Otherwise you might risk to spread viruses over your network

Make sure your homegrown scripts or executables run as fast as possible and do not hang in any case. Intensive testing is recommended before deploying your own scripts or binaries to your productive environment.

Each custom attribute data collection delays the discovery of a device while the script or binary runs (or until the timeout kills the execution).

Make sure your scripts or binaries create the proper XML schema. Otherwise, the output will be rejected!

## 12.3 Configure Custom Software Data Collection Scripts

Custom collection scripts must be configured to be executed. Once, they are imported into JDisc Discovery, they can be configured in JDisc Discovery's discovery settings.

To configure custom software data collection scripts and binaries, open the *Discovery Configuration* dialog from Discovery » Configuration, select the *Data Collection* » *Custom* tab. The *Data Collection* table displays configured custom software data collections. Enable or disable custom software data collections by using the check box. Select a custom software data collection and choose the operating system platforms for which the custom software data collection is targeted.

ndard Custom File Collection		
Custom Attributes		
Custom Software Data Collection		
Platforms		
All Windows versions		
Windows NT 4.0	Windows Server 2008	
Windows 2000	Windows 7	
Windows 2000 Server	Windows 8	
Windows XP	Windows Server 2012	
Windows Server 2003		
Windows Vista		
Data Collection		Add
Execute 'Unix Custom Collection	rript' for Sun Solaris, MAC OS X, Linux, IBM AIX	Enable
V Execute Software Collection Scr	t for Windows	Disable Reset
	u	

Figure: Configure Custom Software Data Collection

You can run multiple custom software data collection scripts for a operating system platform.

The troubleshooting chapter explains how to troubleshoot JDisc Discovery if it does not discover devices properly or does not collect device details as expected.

The most common problems for incomplete discovery results are:

- Firewalls (either personal or network firewalls) blocking protocols. Refer to the protocols section 3.2.2 to review protocols and ports.
- Mis-configured/incorrect credentials prevent the discovery from identifying devices properly and collecting device details.
- Without credentials the discovery uses only anonymous protocols that do not require credentials and collect only basic device details.
- Mis-configured device type filters might exclude devices that should be discovered.

We keep all information provided by you confidential and will not disclose any information to other companies.

JDisc Discovery offers multiple ways to assist troubleshooting:

- The support ZIP file provides all information that our support engineers need to resolve product and device discovery issues.
- The *Data Quality* tab shows how well the devices within your network have been discovered and provides help on how to improve the data quality.
- The *Discovery Protocol Status* report displays the overall status of all protocols for a all devices. This report allows to quickly identify class problems, such as incorrect login credentials, or firewalls block network traffic. In addition to that, the *Device Details* dialog offers the *Analyze » Protocols* tab displays more detailed protocol information for a single device.
- The *Discovery Log* tab displays the sequence of all activity during the discovery of a device.
- The *Diagnostics* tab features a rule based expert system helping to identify issues that prevent a device from being discovered properly. Moreover the *Diagnostics* tab provides hints on how to resolve common problems.
- The *Parsing Issues* tab displays the output of system commands that could not be parsed correctly. This output can help JDisc Discovery's support to integrate new versions of system commands or operating system versions.
- The Unknown SNMP Devices report displays all devices supporting the SNMP protocol, which JDisc Discovery could not identify. The output of the Unknown SNMP Devices report can help JDisc Discovery's support to improve the discovery by adding those unknown devices to future versions of JDisc Discovery.
- The Unknown Telnet Banners report displays all devices supporting the telnet

protocol, which JDisc Discovery could not identify. The output of the *Unknown Telnet Banners* report can help JDisc Discovery's support to improve the discovery by adding those unknown devices to future versions of JDisc Discovery.

## 13.1 Support ZIP

The support ZIP function simplifies the interaction with JDisc's support and provides a single file containing all server log files, discovery logs and related support information.

To accommodate to different problems, JDisc offers two support ZIP file types:

- 1. The product support ZIP
- 2. The device support ZIP

#### 13.1.1 Product Support ZIP

The product support ZIP contains the license file and server log files. If your installation is not working properly, choose the *Administration* » *Create Support ZIP* menu item.

JD JDisc Discovery - JAMES SMITH connected to local	host	
File Discovery Devices Software Networking User [	Documents Troubleshooting Administration Help	
O      Discovery Status	Devices Discovery	
Status Discovery is idle	Create Support	Click for instructions on how to improve the data quality

Figure: Create a product support ZIP file

From the *Export Support ZIP* dialog, choose a file name to store the product support ZIP file. Optionally you can enter a message for JDisc's support that describes the problem.

Export Support ZIP	×
creates a zip file containing diagnostic information for JDisc's support.	
upport ZIP destination file c:\temp\support.zip	Browse
lessage to JDisc's support team	
Dear Support,	
am having a problem scanning	
Ok Cancel	

Figure: Export a Support ZIP file

#### 13.1.2 Device Support ZIP

The device support ZIP contains the license file, server log files, device details including the discovery log of selected devices. Choose the device support ZIP when you are facing issues when discovering one or multiple devices.

To create a device support ZIP, select one or more devices from a device report and chose the context menu item *Create Support ZIP*. The information in the device support ZIP is important for JDisc's support to resolve device specific discovery issues.

ilter:					
Case sensitive filter					
Name	IP Address	Manufacture	r M	Iodel	Туре
Switch-2	12.216.106.203	Nortel Networ	ks N	ortel GbE Switch Module	Switch
Switch-3	12.216.105.210	Nortel Networ	ks N	ortel GbE Switch Module	Switch
Switch-4	12.216.104.37	Nortel Networ	ks N	ortel GbE Switch Module	Switch
PortServer-1	12.216.106.31	Moxa	N	Port	Port Server
MultifunctionalDevice-1	12.216.106.164	Lexmark	X	642e	Multifunctio
Printer-2	12.216.106.180	Lexmark	те	640	Printer
Printer-4	12.216.106.3	Lexmark	E	240n	Printer
Desktop-1	12.216.104.46	Lenovo	T	hinkCentre A51	Desktop
Laptop-1	12.216.104.16	Lenovo	T	hinkPad R52	Laptop
Laptop-2	12.216.104.82	Lenovo	T	hinkPad R61	Laptop
Printer-1	12.216.104.75	Konica Minolta			Printer
BladeEnclosure-1	12.216.106.213	IBM	Prope	rties	Blade Enclo
BladeEnclosure-2	12.119.74.240	IBM	Discov	ver 🕨	Blade Enclo
BladeEnclosure-3	12.216.107.252	IBM			Blade Enclo
BladeServer-1	12.216.105.92	IBM	Mana	ge 🕨	Server (Bla
BladeServer-10		IBM	Comp	oare 🕨	Server (Bla
BladeServer-11	12.216.106.37	IBM			Server (Bla
BladeServer-12		IBM	Custo	m Attributes 🕨	Server (Bla
BladeServer-13	12.216.105.103	IBM	Conne	ect with	Server (Bla
BladeServer-14		IBM			Server (Bla
BladeServer-15		IBM	Troub	leshoot 🕨	Server (Bla
BladeServer-16		IBM	Y Delete	Devices	Server (Bla
BladeServer-17		IBM	~ Delete	Devices	Server (Bla
BladeServer-2	12.216.106.198	IBM	Create	E Support ZIP	Server (Black
A	10 010 100 00	TOM		2	C (D)-

Figure: Create a device support ZIP file

Finally, from the *Export Support ZIP* dialog, choose a file name to store the device support ZIP file. Optionally you can enter a message for Company's support that describes the problem.

### 13.2 Data Quality Tab

Click on the Data Quality tab within the status area in order to review the current data quality. Red quality bars indicate a poor quality, yellow an fair quality and green a good data quality.

U P		neip	
atus			
Discov	rery is idle		Click for instructions on how to improve the data quality!
uisas Ding Naturak Na	abbabaad Diractaay Discovery John Data Quality, Database		
vices   Ping   Network Ne	gnbornood   Directory   Discovery Jobs		
Total			
The total data quality of	all operating system families		
Total	80%		How to improve
By Operating System Fam	dy		
The data quality by oper Windows	ating system family		How to improve
The data quality by oper Windows	ating system family		How to improve
The data quality by oper Windows	ating system family 경험원 		How to improve How to improve How to improve
The data quality by oper Windows Linux VMware ESX Server Orade VM Server	ating system family 30% 30% 100% 0%		How to improve How to improve How to improve How to improve
The data quality by oper Windows	ating system family		How to improve How to improve How to improve How to improve How to improve
The data quality by oper Windows Linux Comment Windows Comment Unux Comment Oracle VM Server Comment Citrix XenServer Comment MAC OS X	ating system family		How to improve How to improve How to improve How to improve How to improve How to improve
The data quality by oper Windows Linux Control of the data quality by oper Unux Control of the data quality of the data quality by oper Oracle VM Server Control of the data quality of the data quality by oper Oracle VM Server Control of the data quality of the data quality by oper Citrix XenServer Control of the data quality of the data quality by oper MAC OS X Control of the data quality by operating the data quality by o	ating system family		How to improve How to improve How to improve How to improve How to improve How to improve
The data quality by oper Windows	ating system family		How to improve How to improve
The data quality by oper Windows	ating system family		How to improve How to improve

Figure: Data Quality Tab

Follow the *How to improve...* link in the right area in order to open a new diagnostics report. This report displays a list of tasks on how to improve the data quality.

D Diagnostics				
riha.				
riter:				
Description				
Enable Windows remote login to improve the discovery result				
Enable Cisco IOS remote login to improve the discovery result				
Enable Linux/VMware ESX/Orade VM Devices with selected recommendation(s)				
Enable HP ProCurve remote login to i				
· 0_				
	+			
Iotai 5 diagnostic entris   1 diagnostic entry selected				
Close				

#### Figure: Diagnostics Report

Use the context menu to open the list of devices to which a diagnostic entry applies or use the *Explain* option in order to get more details on the diagnostic entry.

### 13.3 Protocol Status

The protocol status is the first place to start troubleshoot discovery problems as it provides a quick overview of all devices. The protocols used by JDisc Discovery's depend on the device type and operating system. The Discovery Scenarios chapter presents an overview on how JDisc Discovery discovers the most important device types and operating systems and also explains the protocols.

#### 13.3.1 Discovery Protocol Status Report

Open the *Discovery Protocol Status* report from the *Troubleshooting* » *Devices* » *Protocol Status* menu. The *Discovery Protocol Status* report displays an overview of all protocols including the number of devices in the *Success*, *Warning* and *Failed* category. Select protocols and use the context menu to display all devices in any of the three categories.
Case sensitive filter				
Protocol	Success	Warning	Error	
DNS	7	212	33	
нттр	0	148	104	
HTTPS	0	96	38	
NetBIOS anonymous	63	51	138	
Remote login	37	166	49	
Remote login admin	42	202	8	
SMB anonymous	78	51	123	
SMB authenticated	44	193	15	
SNMPv1	67	51	134	
SNMPv2c	50	68	134	
SNMPv3	0	251	1	
SSH	55	197	0	
Telnet	4	247	1	
Telnet banner parsing	28	51	173	
VMware VIM API	8	171	73	
WBEM	17	56	179	
WMI	40	88	124	

#### Figure: Discovery Protocol Status Report

The protocol *Warning* category indicates configuration problems, such as missing passwords.

### 13.3.2 Device Discovery Protocol Report

The *Device Protocol Status* report displays all devices including the status of selected protocols.

elect Discovery Protocols
Discovery Protocols
SNMPv1 Select All
SNMPv2c Disable All
SNMPv3
WMI
V Telnet
SSH
Telnet banner parsing
SMB anonymous
SMB authenticated
☑ HTTP
WBEM
📝 Remote login
🔽 Remote login admin
VetBIOS anonymous
VMware VIM API
V DNS
✓ HTTPS
Ok Cancel

Figure: Discovery Protocols Selection Dialog

Click *Ok* to open the *Device Discovery Protocol Status* report displaying the status of the selected protocols for all devices.

13.3.3 Single Device Protocol Status

From the *Device Details* dialog select *Analyze* » *Protocols* to displays the status of all protocols for the selected device.

Filter: Case sensitive filter Protocol DNS HTTP HTTPS NetBIOS anonymous Remote login admin SMB anonymous DNS Protocol Remote login admin SMB anonymous	Protocol Status Timeout Timeout Timeout Success Protocol not tested Success	
Case sensitive filter  Protocol  DNS HTTP HTTPS NetBIOS anonymous Remote login admin SMB anonymous	Protocol Status Timeout Timeout Success Protocol not tested Success	
Protocol DNS HTTP HTTPS NetBIOS anonymous Remote login admin SMB anonymous	Protocol Status Timeout Timeout Success Protocol not tested Success	
Protocol DNS HTTP HTTPS NetBIOS anonymous Remote login Remote login admin SMB anonymous	Protocol status Timeout Timeout Success Protocol not tested Success	
DNS HTTP HTTPS NetBIOS anonymous Remote login Remote login admin SMB anonymous	Timeout Timeout Success Protocol not tested Success	
HTTP HTTPS NetBIOS anonymous Remote login Remote login admin SMB anonymous	Timeout Timeout Success Protocol not tested Success	
HTTPS NetBIOS anonymous Remote login Remote login admin SMB anonymous	Timeout Success Protocol not tested Success	
NetBIOS anonymous Remote login Remote login admin SMB anonymous	Success Protocol not tested Success	
Remote login Remote login admin SMB anonymous	Protocol not tested Success	
Remote login admin SMB anonymous	Success	
SMB anonymous	and the second sec	
	Multiple connections to a server or shared resource b	
SMB authenticated	Success	
SNMPv1	Timeout	
SNMPv2c	Timeout	
SNMPv3	Access credentials missing	
SSH	Protocol not tested	
Telnet	Protocol not tested	
l einet banner parsing	Protocol not supported	
VMWare VIM API	Port unreachable	
VVDEM	Port unreachable	
VVIMI	SUCCESS	
Total 17 device protocols 1.0 device protocols select	ted	
Total 17 device protocola jo device protocola aciet	~~~	

Figure: Protocols Tab displaying the Protocol Status for a single Device

## 13.4 Discovery Logs

JDisc Discovery logs discovery activity during discovery and data collection of a device. The discovery log also includes protocol information and data collected for each protocol.

From the *Device Details* dialog select *Analyze* » *Discovery Log* to display the discovery log.

The navigation tree in the left panel represents high-level discovery activity. Select an item in the left panel to limit the log output in the content panel. Errors and warnings are highlighted with icons.

## 13.5 Parsing Issues

To collect device details JDisc Discovery's discovery executes system commands on Unix and MAC OS X computers. System command output often depends on the operating system version. Though JDisc Discovery supports many operating system versions, system commands might generate output that JDisc Discovery cannot parse. To improve troubleshooting and support, JDisc Discovery stores unknown system command output in the database. This information helps JDisc Discovery's support to integrate new system command output formats into the product. From the *Device Details* dialog select *Analyze* » *Parsing Issues* to display unknown system command outputs.

# 13.6 Common Windows Computer Configuration Problems

Windows computer protocols, services and local policies can be configured in many ways to fit corporate security guidelines. However, some configuration settings, such as:

- Client for Microsoft Networks is not installed
- File and Printer Sharing for Microsoft Networks is not installed or disabled
- Simple File Sharing is enabled
- Sharing and security model for local accounts is set to Guest only local users authenticate as Guest
- Server service is stopped

negatively affect JDisc Discovery's ability to accurately discover Windows computers.

This section describes common configuration problems and symptoms to detect these problems based on JDisc Discovery's protocol status values.

### 13.6.1 The Network Logon Service Was Not Started

Protocol	Protocol Status
SMB authenticated	An attempt was made to logon, but the network logon service was not started
Remote login admin	An attempt was made to logon, but the network logon service was not started
WMI	Access denied

Table: The network logon service was not started

Can be caused by these Windows configuration options:

- Client for Microsoft Networks is not installed
- Netlogon service is stopped

### 13.6.2 IO Failure And Network Path Was Not Found Symptoms

Protocol	Protocol Status

NetBIOS anonymous	IO Failure
SMB anonymous	The network path was not found
SMB authenticated	The network path was not found
Remote login admin	The network path was not found

Table: IO Failure and Network Path was Not found Symptoms

Can be caused by these Windows configuration options:

- File and Printer Sharing for Microsoft Networks is not installed or disabled
- Server service is stopped

13.6.3 Logon Failure And Access Denied Symptoms

Protocol	Protocol Status
SMB authenticated	Logon failure: unknown user name or bad password
Remote login admin	Logon failure: unknown user name or bad password
WMI	Access denied

Table: Logon failure and Access Denied Symptoms

The symptoms might be caused by an invalid logon credential / password combination but also by these Windows configuration options:

- Simple File Sharing is enabled
- Sharing and security model for local accounts is set to Guest only local users authenticate as Guest

## 13.7 Unknown SNMP Devices

JDisc Discovery supports many SNMP based devices. When manufacturer ship new devices the discovery's internal lookup tables and classes must be updated in order to support them. SNMP based devices that JDisc Discovery does not identify are classified as *Unknown SNMP device*. In such a case JDisc Discovery can access the device via SNMP but does not know how to discover the device including assigning a device type and model.

You can help improving JDisc Discovery's device coverage when you send the

*Unknown SNMP Devices* report to JDisc Discovery's support. The development team can then add those unknown SNMP devices to future product versions.

Open the Unknown SNMP Devices report from Troubleshooting » Devices » Unknown SNMP Devices.

Submit the *Unknown SNMP Devices* report to JDisc Discovery's support email-address. The development team can then add those unknown devices to future product versions.

In addition to the *Unknown SNMP Devices* report, SNMP walks can also help to support unknown device.

To start a SNMP walk:

- Download the SNMP Walk Tool from our web site: www.jdisc.com/downloads/SnmpWalk.zip
- The SNMP walk tool already produces the output format that we need for our SNMP simulator.
- Run the tool according the instructions and submit the result file to our support. Depending on your corporate policies, you might send model, manufacturer and serial number along with the SNMP walk to JDisc Discovery's support emailaddress. This additional information helps JDisc Discovery's support to better identify relevant SNMP variables in the SNMP walks.

Performing SNMP walks on unknown SNMP devices helps JDisc Discovery's support team to add these unknown devices in future product versions. Include (if possible) model, manufacturer and serial number. This helps JDisc Discovery's support to identify relevant SNMP variables in the SNMP walks.

## 13.8 Unknown Telnet Banners

If all other protocols fail, JDisc Discovery uses telnet to identify devices. In such a case the discovery connects to a device using telnet and attempts to match the console banner output against well known banners. If a banner cannot be recognized, it will be stored in the database for later troubleshooting.

The *Unknown Telnet Banners* report displays all devices including the unknown telnet banner (if applicable).

- Open the Unknown Telnet Banners report from Troubleshooting » Devices » Unknown Telnet Banners.
- Double click a device in the *Unknown Telnet Banners* report to display the *Device Details* dialog.

- From the *Device Details* dialog select Analyze » *Parsing Issues*.
- From the *Parsing Issues* tab, select the *Unknown Telnet Banner* from the left navigation panel to display the unknown telnet banner.

<ul> <li>Image: Image: Im</li></ul>
General       Networking       Hardware       Firmware       Software       User       Virtual Computers       Custom Attributes       Roles       Groups       Analyze         Discovery Log       Protocols       Parsing Issues       Diagnostics
General       Networking       Hardware       Firmware       Software       User       Virtual Computers       Custom Attributes       Roles       Groups       Analyze         Discovery Log       Protocols       Parsing Issues       Diagnostics       Diagnostics       Diagnostics
Discovery Log Protocols Parsing Issues Diagnostics
Parsing issues     iname is non-existent for this module
for a list of valid names, use name '?'
Close

Figure: Unknown Telnet Banner Report

Submit the *Unknown Telnet Banner* report to JDisc Discovery's support email-address. The support team can then add this unknown telnet banner to future product versions.

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 (http://acs.lbl.gov/~hoschek/colt).
- 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/).