



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.....	15
2.1 Starting the User Interface.....	15
2.2 Understanding the User Interface.....	15
2.3 Initial Configuration.....	16
2.3.1 Define the Discovery Algorithm for Finding new Devices.....	18
2.3.2 Select Major Platforms To Discover.....	19
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.....	30
3 Concepts.....	33
3.1 Pattern Matching.....	33
3.1.1 Wildcard Matching.....	33
3.1.2 Regular Expression Matching.....	33
3.2 Discovery.....	33
3.2.1 The Discovery Process.....	34
3.2.2 Ports and Protocols.....	35
3.2.3 Login Credentials.....	36
3.2.4 Credential Handling.....	37
3.2.5 Remote Login.....	38
3.3 Device Grouping.....	39
3.3.1 Define your own Groups.....	40
3.3.1.1 Create Network/Range groups.....	41
3.3.1.2 Create Windows Network Neighborhood groups.....	42
3.3.1.3 Create Directory group.....	44
3.3.1.4 Create a group based on device attributes.....	45
3.3.1.5 Groups and default accounts.....	48
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.....	79
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.....	84
4.7.4.1 Preparation Within The Cisco Meraki Portal.....	84
4.7.4.2 Checking Cisco Meraki Cloud Results.....	85
4.8 Discover Users and User Groups.....	86
4.8.1 Discover Local Users And User Groups.....	86
4.8.2 Discover Active Directory Users And User Groups.....	86
4.8.3 The User group Browser.....	87
4.8.4 User Report.....	87
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 Discovery.....	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 Passwordstate.....	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 Steps.....	103
4.12.3.3 Using CyberArk Accounts.....	105
4.12.4 Microsoft LAPS.....	107
4.12.4.1 LAPS Architecture Overview.....	107
4.12.4.2 Configure LAPS in Product Inventory.....	107
4.12.4.3 Configure a LAPS Account.....	108
4.12.4.4 Configure Local Administrator Accounts.....	108
4.13 Cluster Discovery.....	108
4.13.1 Veritas Cluster.....	108
4.13.2 Microsoft Cluster Services.....	108
4.13.3 HP ServiceGuard Cluster.....	108
4.13.4 Cisco HSRP Cluster.....	109
4.13.5 VRRP Cluster.....	109
4.13.6 Fortinet HA Cluster.....	109
4.13.7 Juniper HP Cluster.....	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.....	116
5 Discovery Configuration.....	117
5.1 General Tab.....	117
5.2 Scope Tab.....	118
5.2.1 Scope Tabs.....	119
5.2.1.1 Properties.....	119
5.2.1.2 IPv4 Networks.....	119
5.2.1.3 IPv4 Address Ranges.....	120
5.2.1.4 IPv6 Networks.....	122
5.2.1.5 Network Neighborhood.....	123
5.2.1.6 Directory.....	124
5.2.1.7 SNMP.....	125
5.2.1.8 Accounts.....	126
5.2.2 Root Group.....	128
5.2.3 Sub Groups.....	129
5.3 Directory tab.....	129
5.3.1 Configure Directory DNS Domain Controller	129
5.4 Data Collection.....	130
5.4.1 Standard Data Collection.....	130
5.4.1.1 Users.....	130
5.4.1.2 Software/Hardware.....	131
5.4.2 Virtualization Data Collection.....	132
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 Format.....	227
10 Documents.....	228
10.1 Manage Documents.....	228
10.2 Use Documents.....	228
10.3 Documents and Reports.....	230
11 Simplified File Collection.....	232
11.1 Add new Collections.....	233
11.2 Change or remove collections.....	233
12 Custom Software Discovery.....	235
12.1 The XML Schema.....	235
12.2 Import Software Data Collections.....	236
12.3 Configure Custom Software Data Collection scripts.....	237
13 Troubleshooting.....	239
13.1 Support ZIP.....	240
13.1.1 Product Support ZIP.....	240
13.1.2 Device Support ZIP	241
13.2 Data Quality Tab.....	242
13.3 Protocol status.....	244
13.3.1 Discovery Protocol Status Report.....	244
13.3.2 Device Discovery Protocol Report.....	245
13.3.3 Single Device Protocol Status.....	246
13.4 Discovery logs.....	247
13.5 Parsing issues.....	247
13.6 Common Windows computer Configuration Problems.....	248
13.6.1 the network logon service was not started.....	248
13.6.2 IO Failure and Network Path was Not found Symptoms.....	248
13.6.3 Logon failure and Access Denied Symptoms.....	249
13.7 Unknown SNMP devices.....	249
13.8 Unknown telnet banners.....	250
14 Open Source	252

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 these 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 its 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 Getting Started

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 its 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.

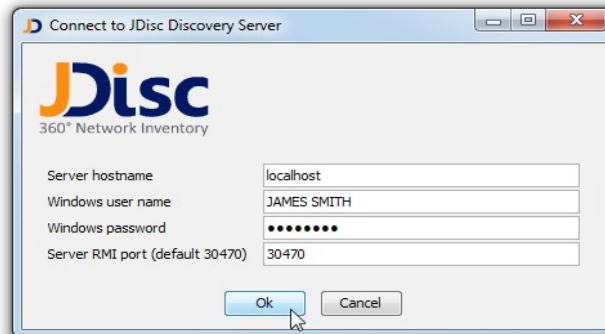


Figure: Login to the JDisc Discovery server.

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.

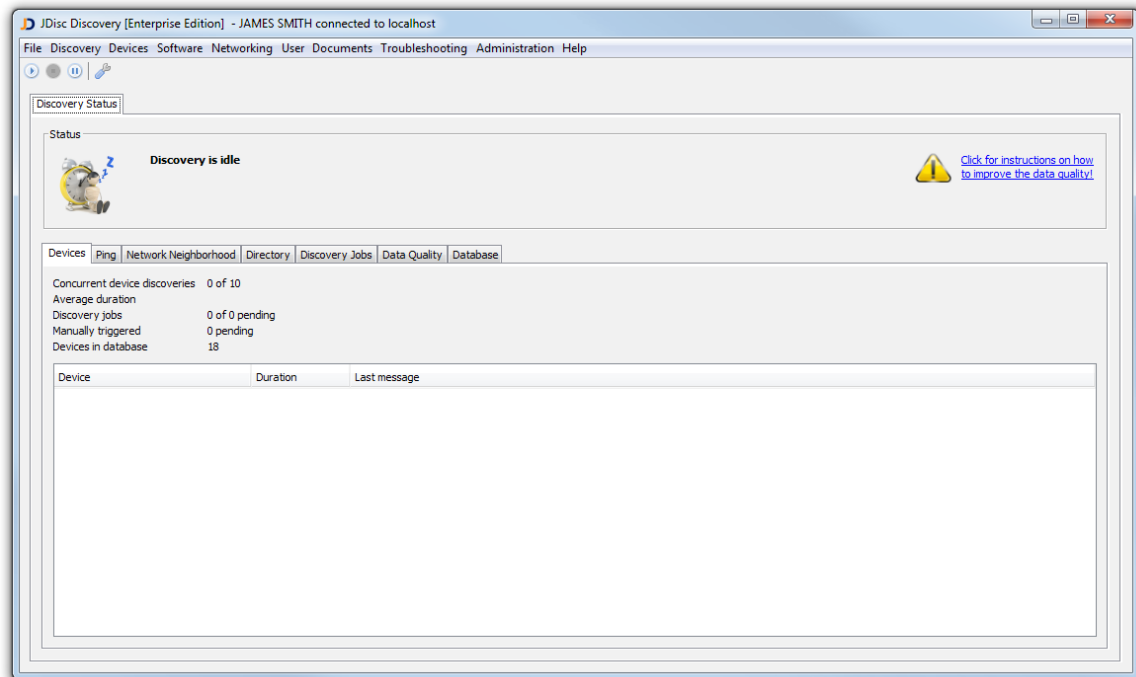


Figure: JDisc Discovery's main window

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.

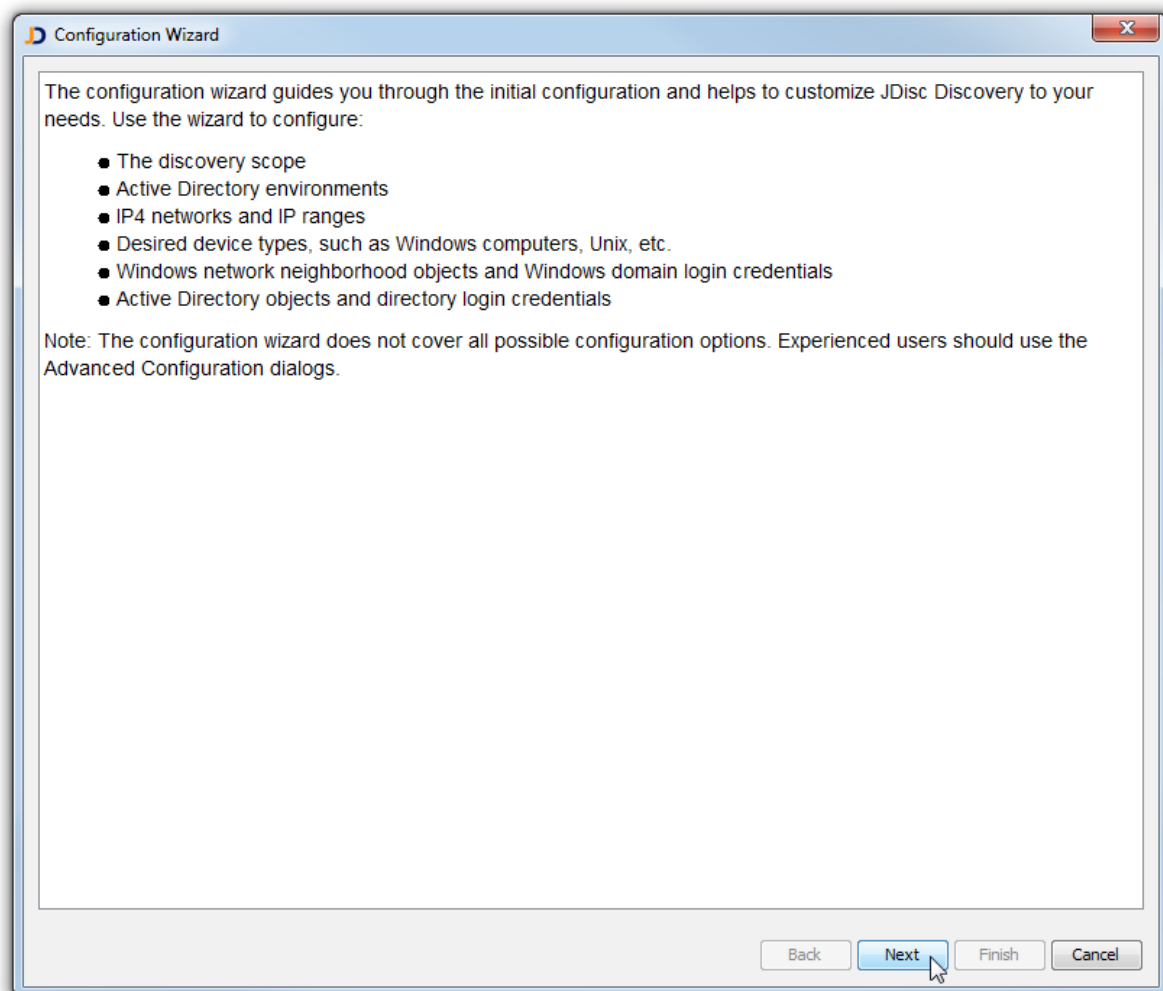


Figure: Configuration Wizard

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.

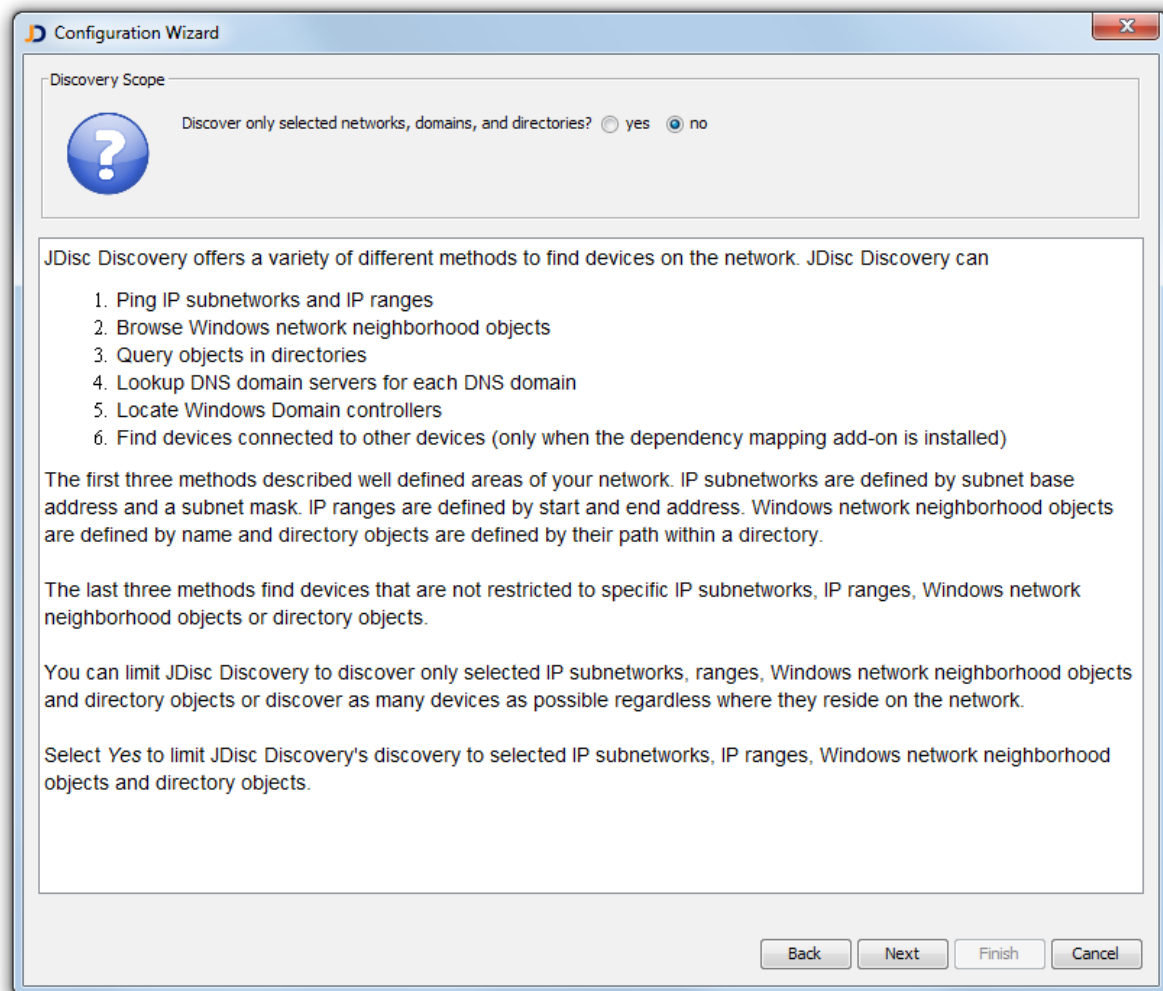


Figure: Configure how to find new devices

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.

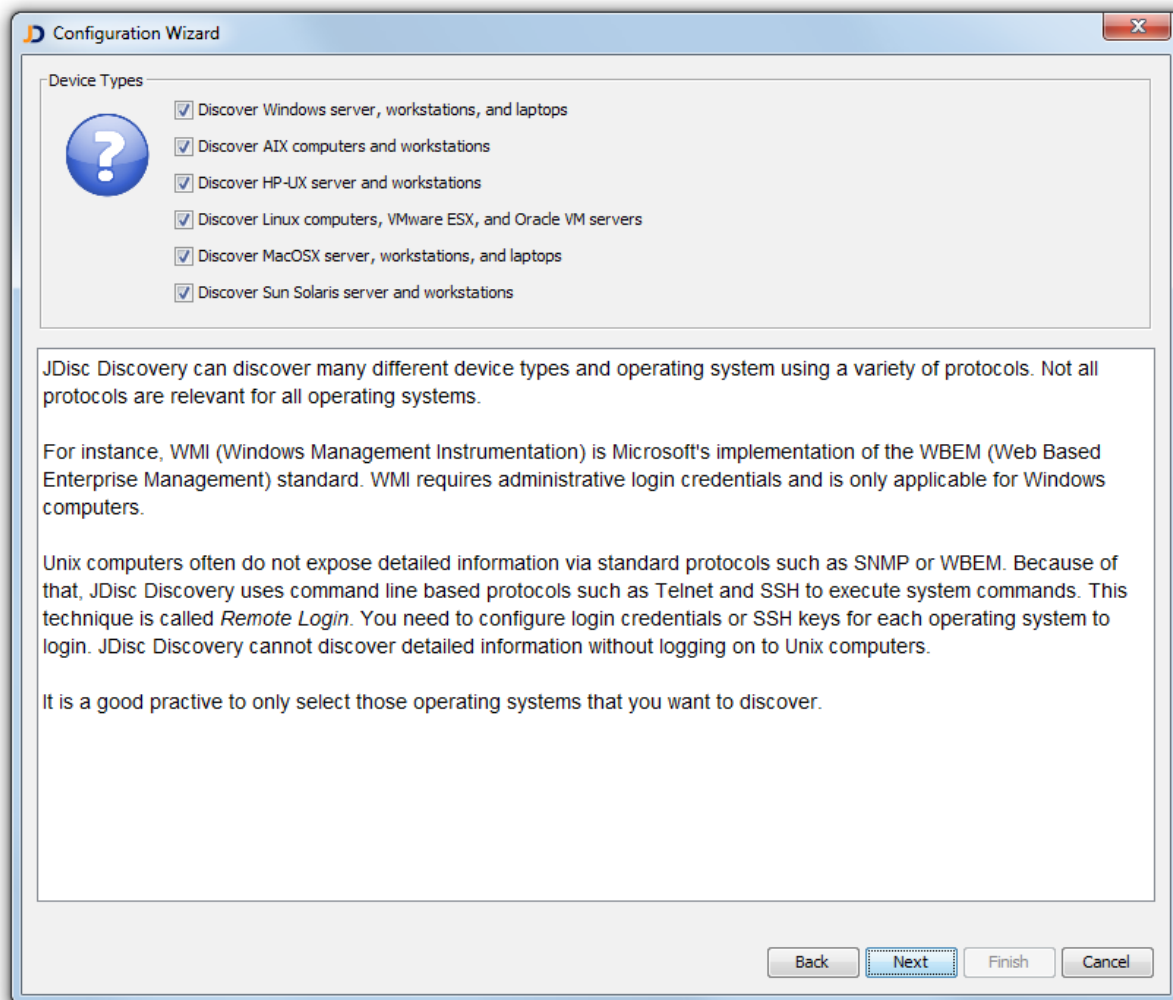


Figure: Select major Device Platforms

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.

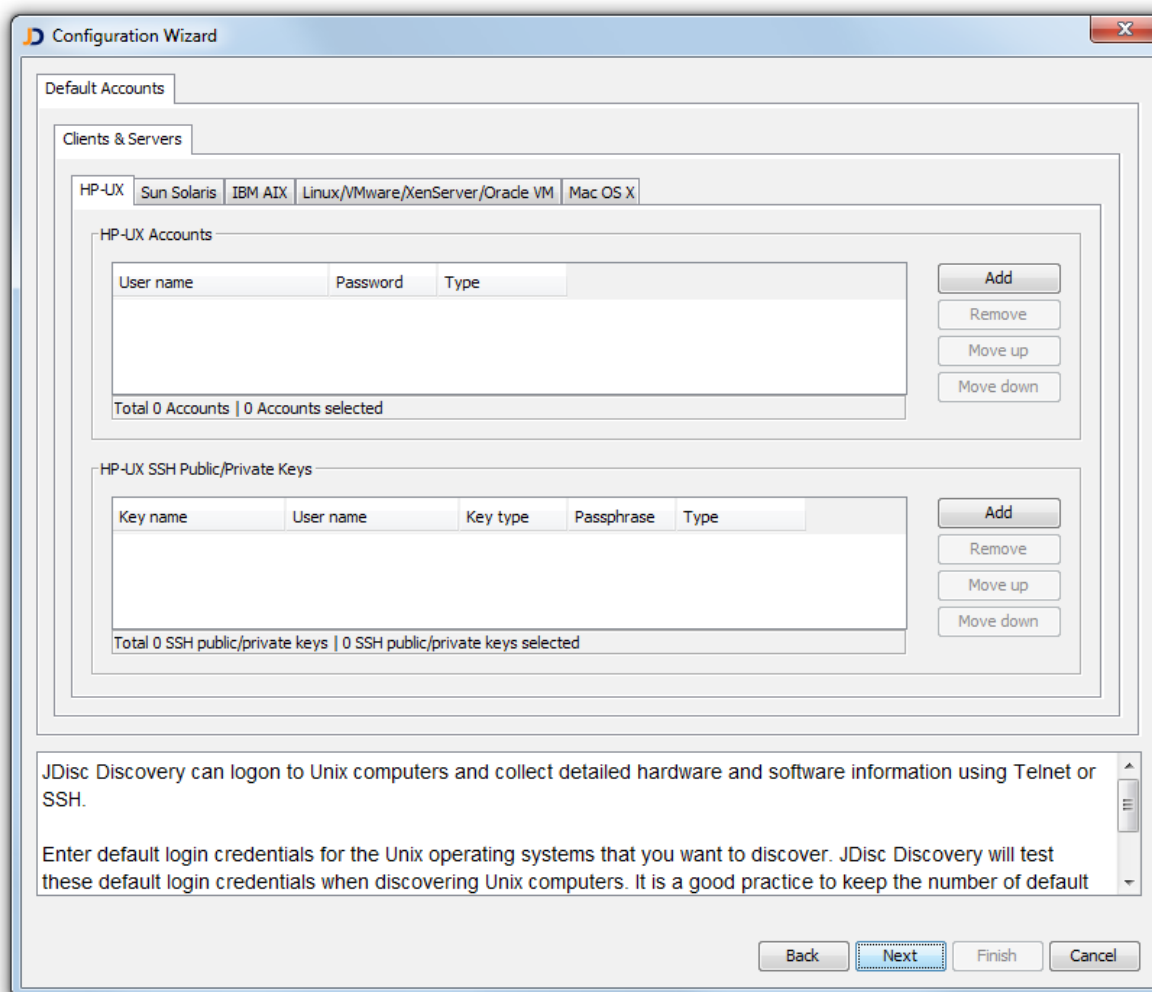


Figure: Define Default Accounts

This dialog might vary depending on the licensed edition.

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 problems¹ with the protocol versions 1 and 2c. Use the SNMPv3 configuration area to provide default SNMPv3 access credentials.

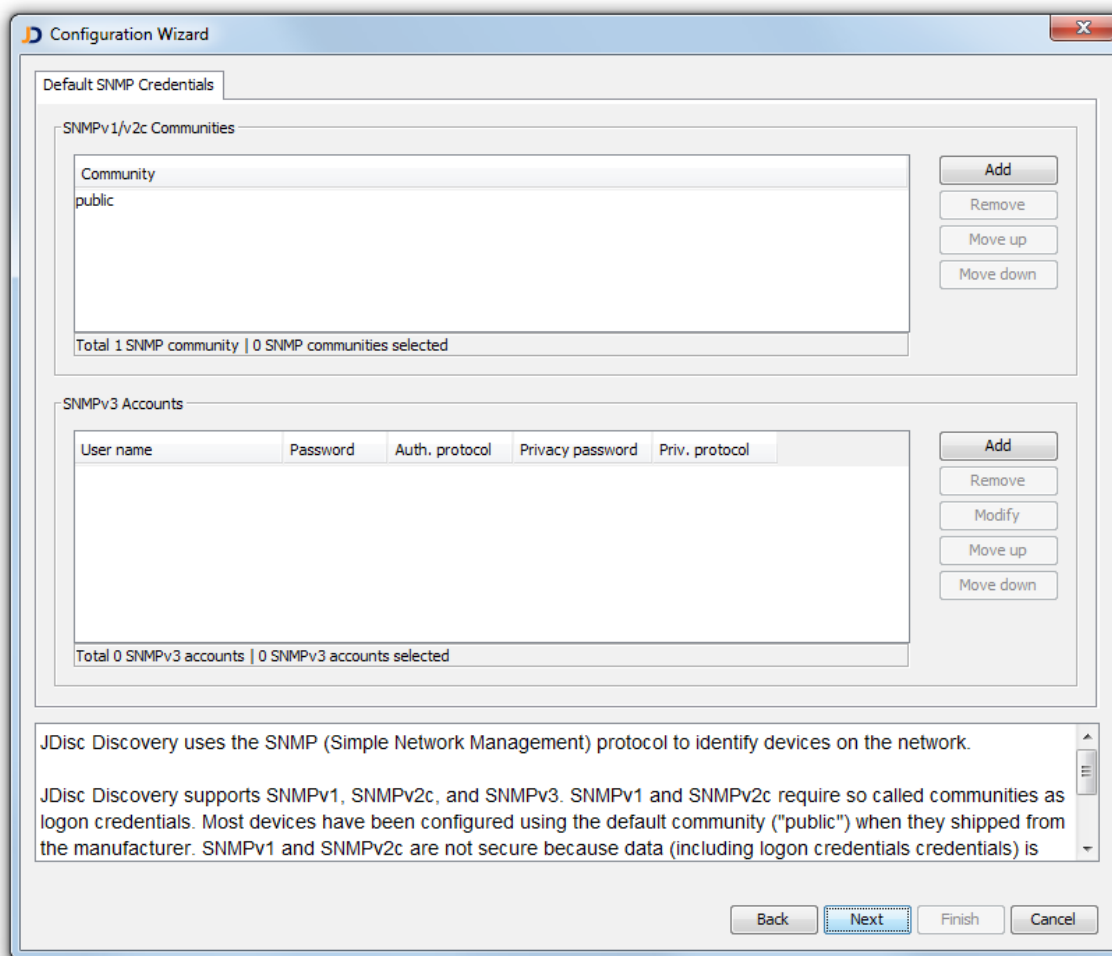


Figure: SNMP Community and Account Configuration

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.

¹ 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.

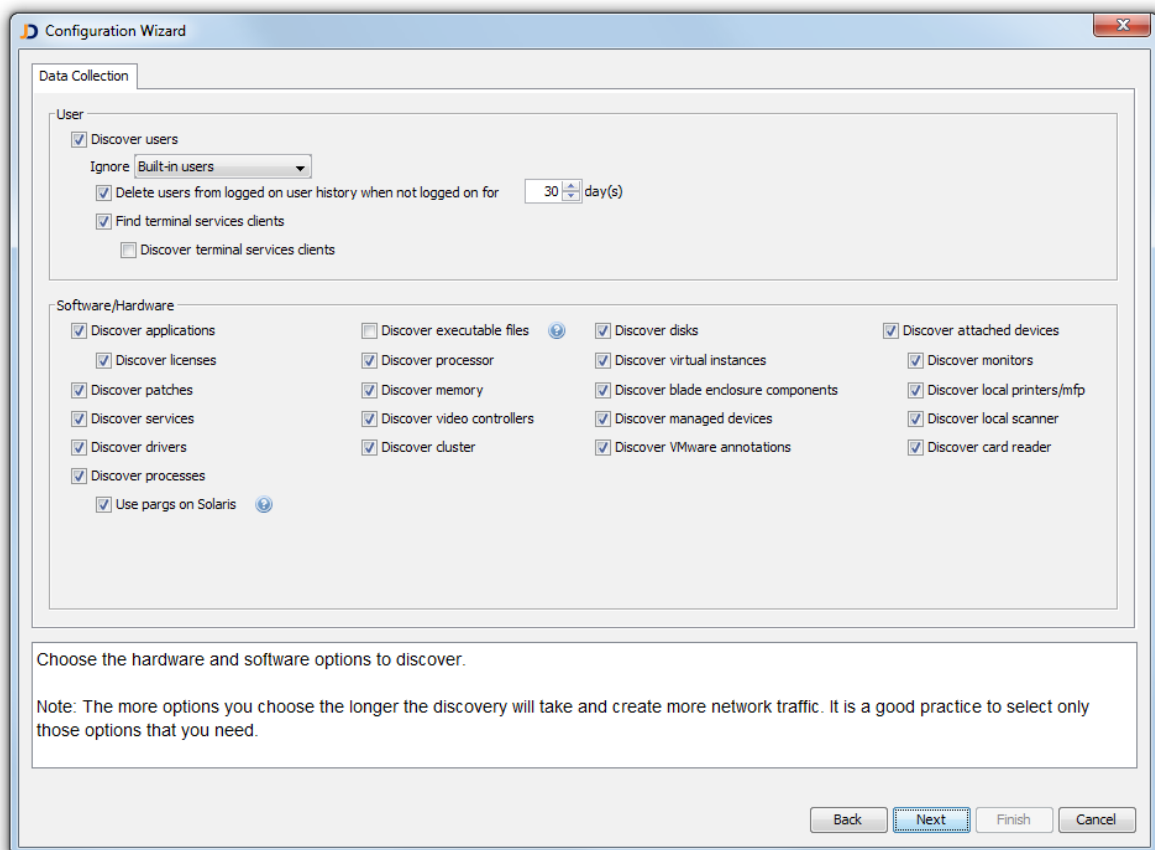


Figure: Data Collection Configuration

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.

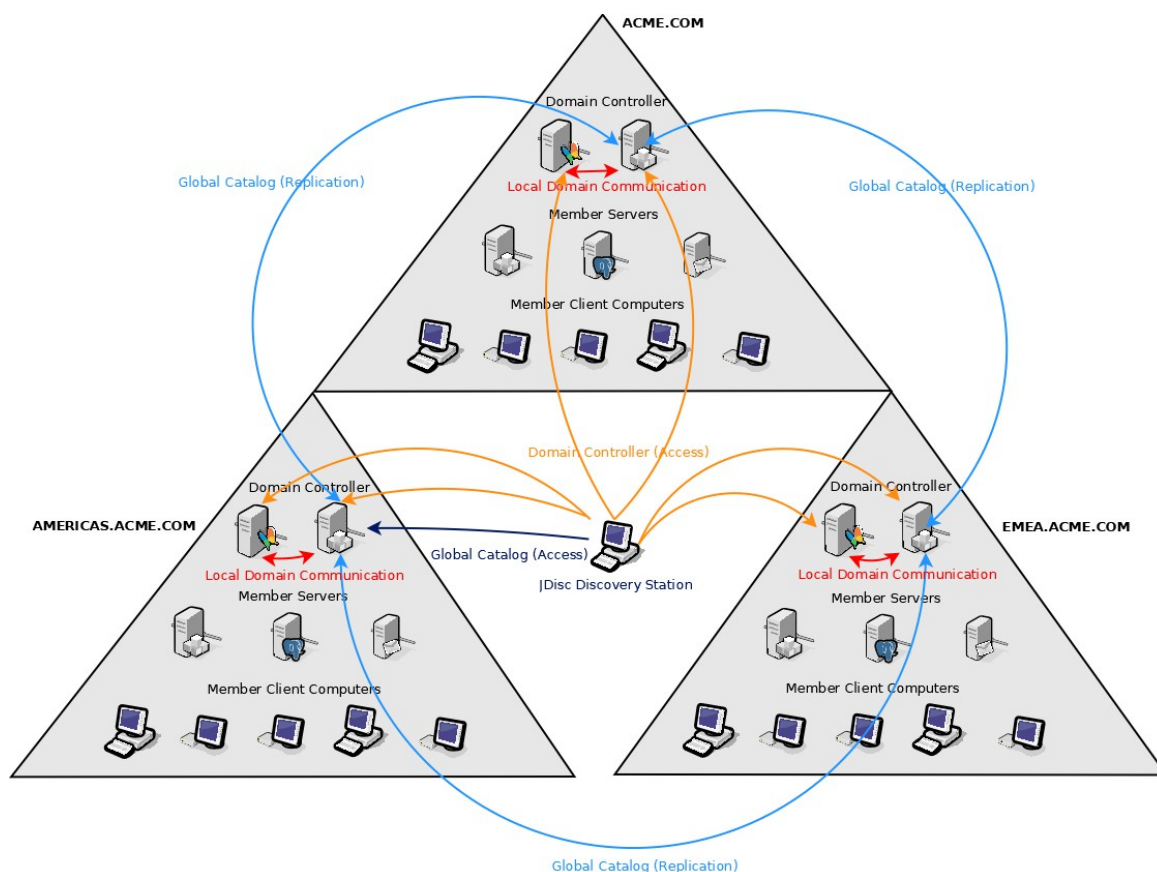


Figure: Directory Access

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!

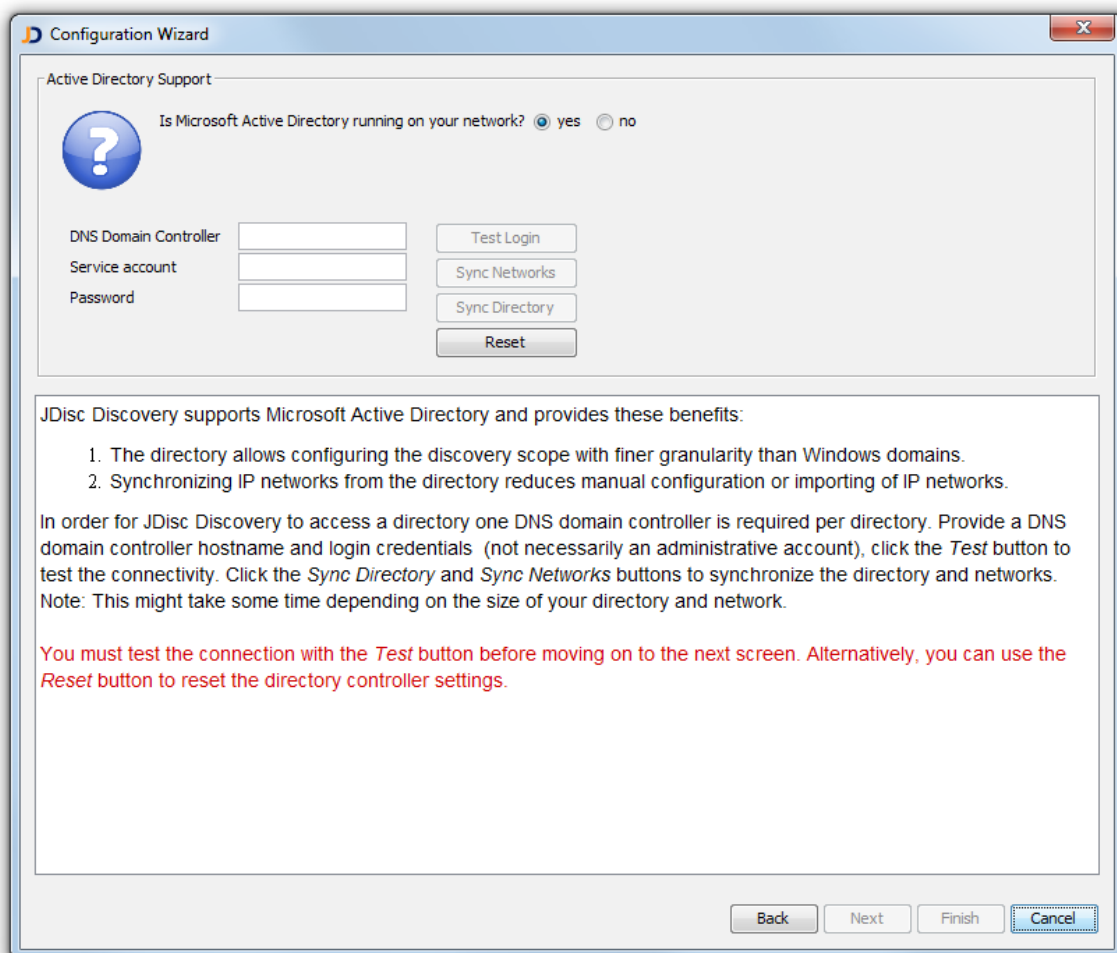


Figure: Active Directory Configuration

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.

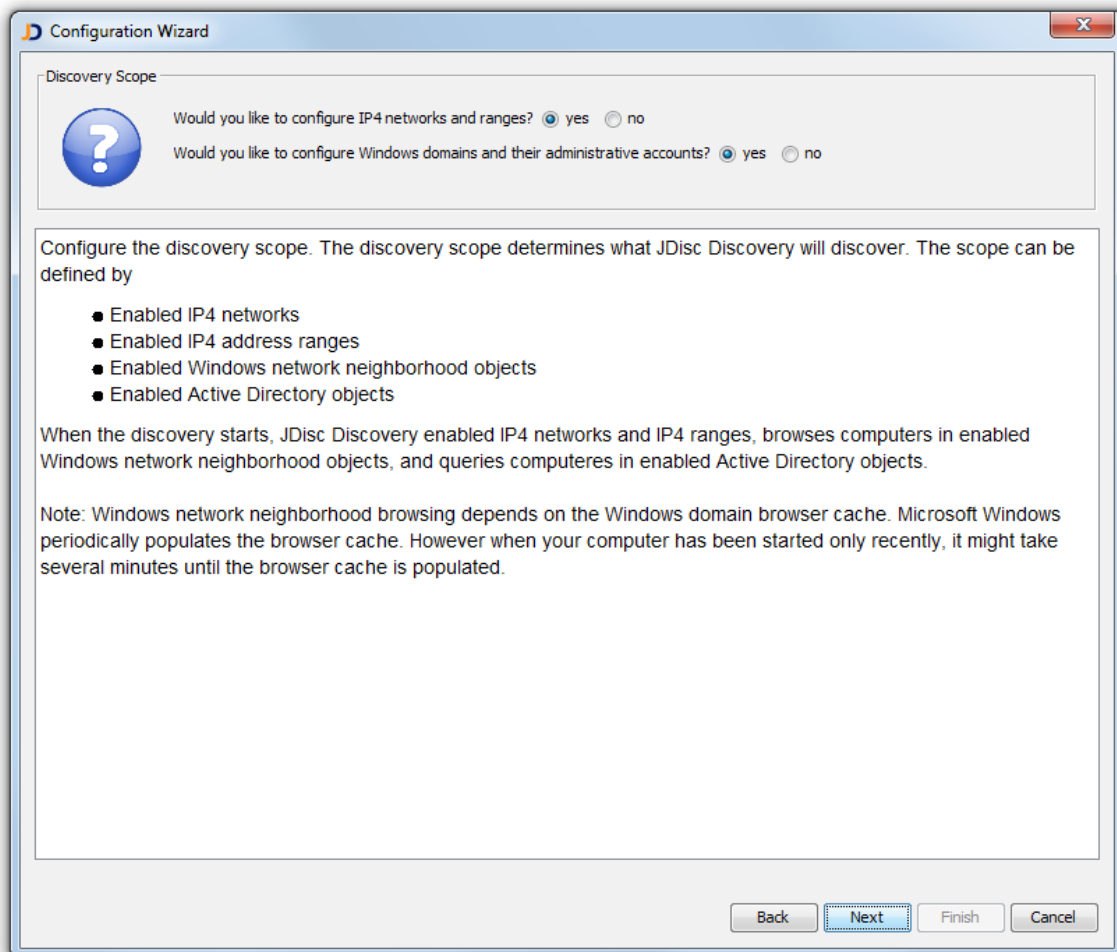


Figure: Define the Discovery Scope

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).

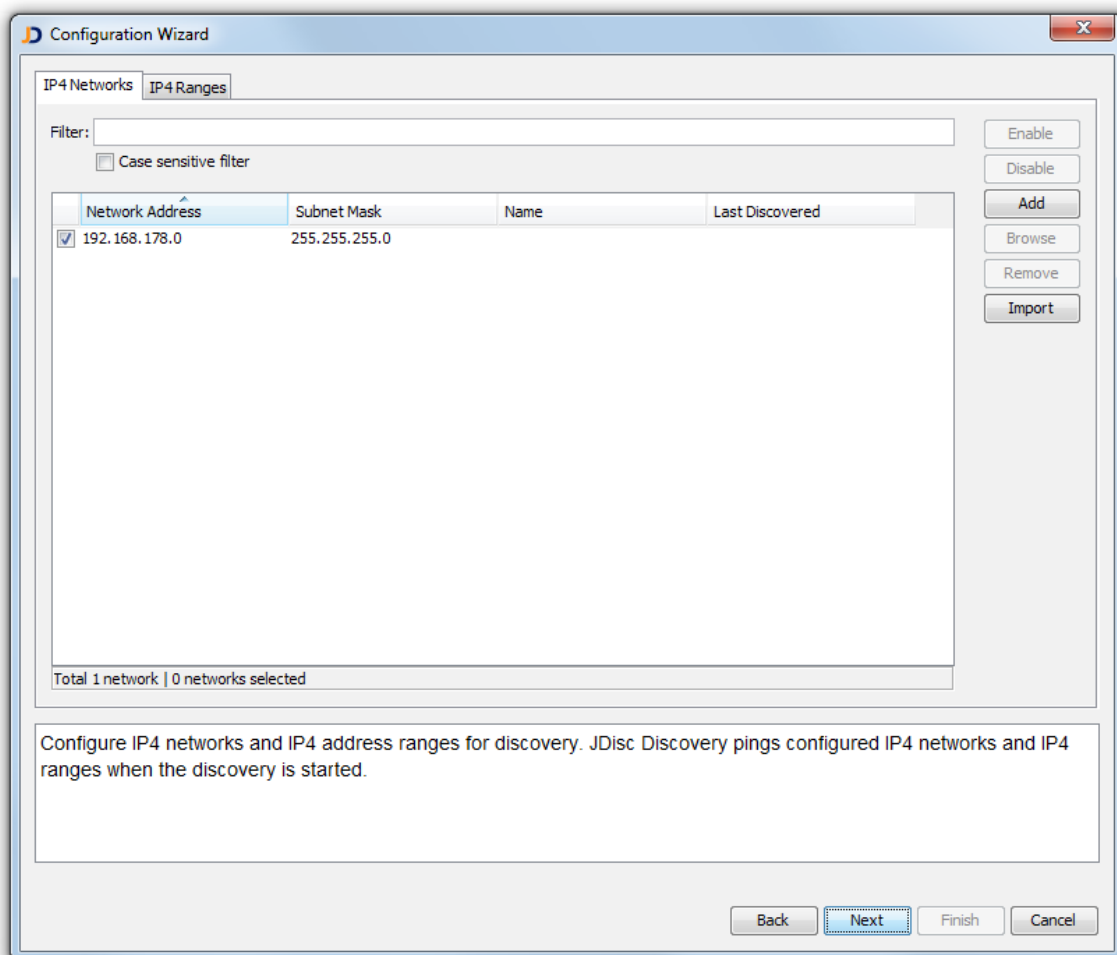


Fig: Define IP4 networks and IP4 address ranges

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.

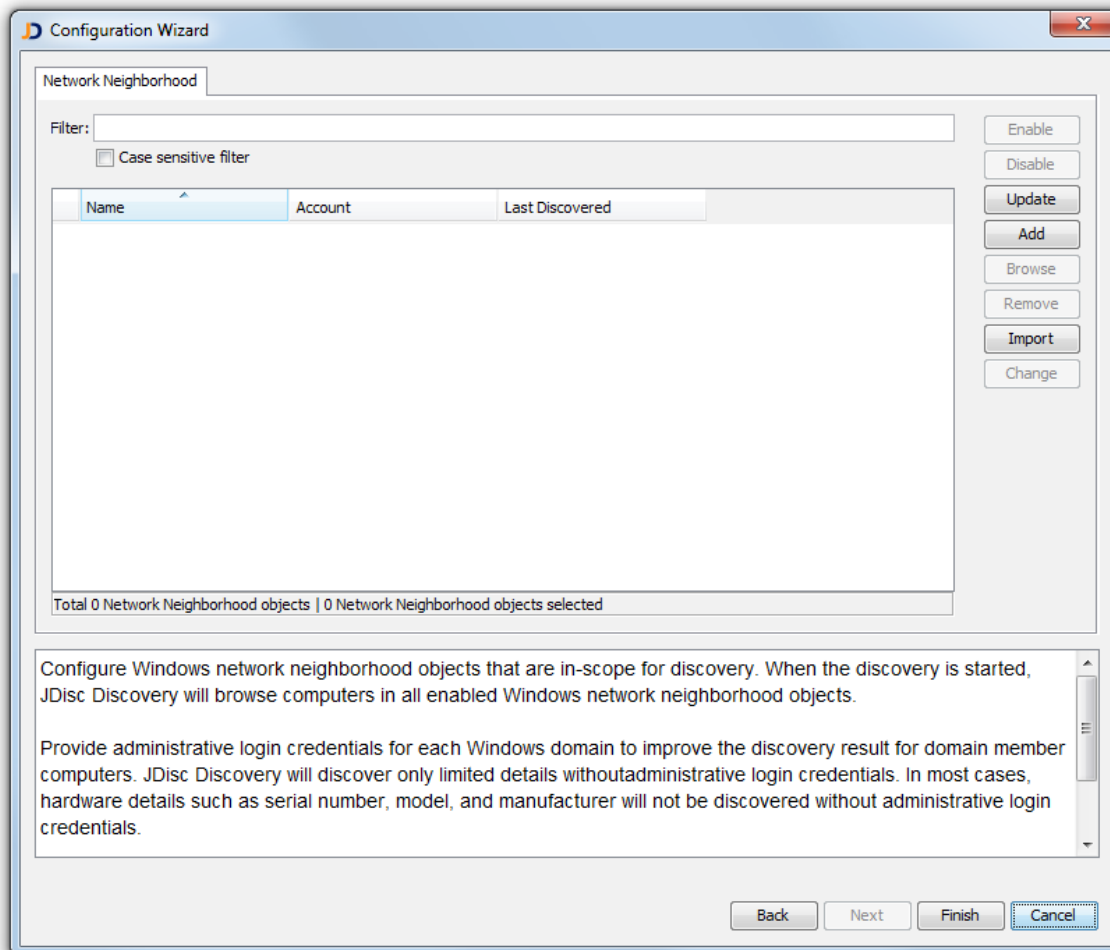


Figure: Define Windows Network Neighborhood Objects

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.

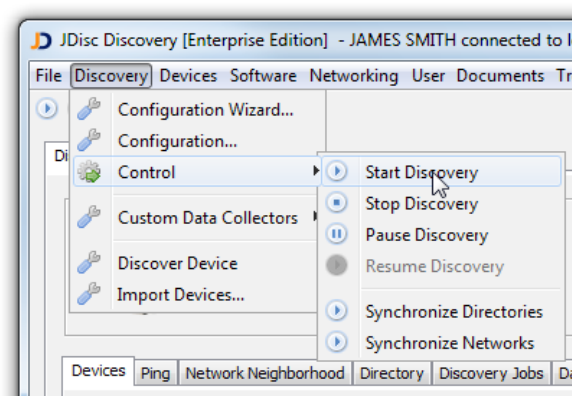


Figure: Start the Discovery

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.

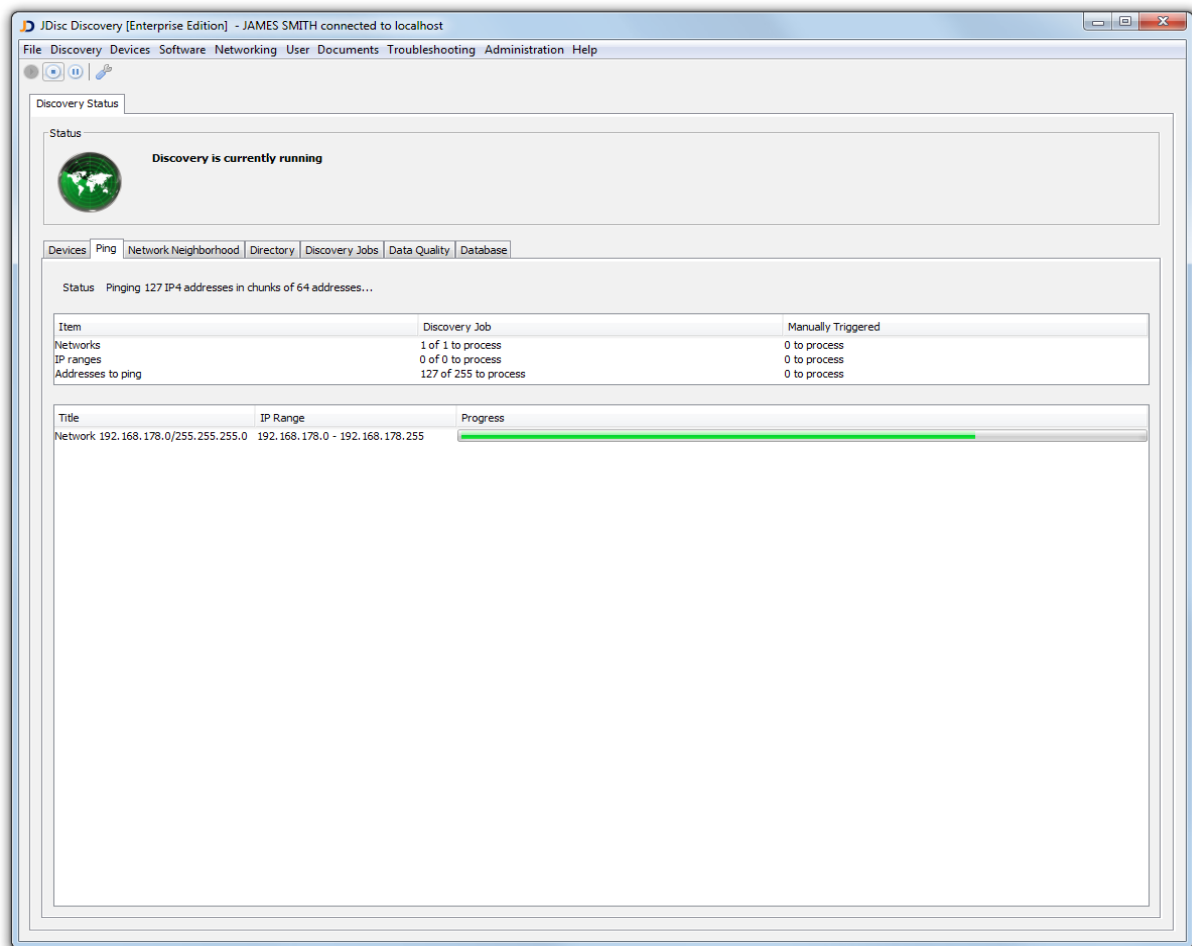


Figure: The Discovery Status

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.

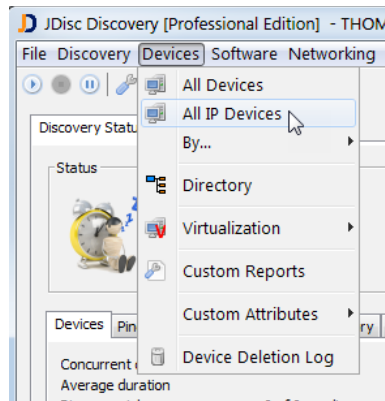


Figure: Open the *All IP Devices* Report




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.

Name	IP Address	Manufacturer	Model	Type	OS Version	Patch Level	FW Version
PortServer-1	12.216.106.31	Moxa	NPort	Port Server			3.3
Printer-1	12.216.104.75	Konica Minolta	Magicolor 2350	Printer			
Printer-2	12.216.106.180	Lexmark	T640	Printer			LS-ST
Printer-3	12.251.240.84	Hewlett-Packard	LaserJet 4000 Series	Printer	G.08.40		G.07.1
Printer-4	12.216.106.3	Lexmark	E240n	Printer			BR.Q.f
Printer-6	12.251.240.48	Hewlett-Packard	Color LaserJet CP4005	Printer	V.33.41		none
PrintServer-1	12.216.105.148	Hewlett-Packard	JetDirect	Print Server	3.51		H.07.
PrintServer-2	12.251.240.190	Hewlett-Packard	JetDirect 170X	Print Server	F.08.20		F.08.0
ProCurve1	192.168.178.18	Hewlett-Packard	ProCurve 2650	Switch	H.08.72		H.08.0
RadServer-1	12.216.105.80	IBM	eServer xSeries 336	Server (Rack)	Windows Server 2003	Service Pack 2	-[APE]
RadServer-2	12.251.240.164	Hewlett-Packard	rx2620	Server (Rack)	HP-UX B.11.23U		04.10
RadServer-3	12.251.240.0	Hewlett-Packard	rx6600	Server (Rack)	HP-UX B.11.23U		03.01
RadServer-4	12.251.240.233	Hewlett-Packard	rx6600	Server (Rack)	HP-UX B.11.23U		03.01
RadServer-5	12.251.240.16	Hewlett-Packard	rx2660	Server (Rack)	HP-UX B.11.23U		03.01
solaris11-test	192.168.178.26			VMware Instance	SunOS 5.11	11.1	DevCo
SolarisZone-1	12.255.136.63			Solaris Zone			
summit1	192.168.178.13	Extreme Networks	Summit 48i	Routing Switch	7.2.0	Build 33	
summit2	192.168.181.2	Extreme Networks	Summit 48i	Switch	7.2.0	Build 33	
summit3	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		
Switch-1	12.216.107.24	Nortel Networks	Nortel GBE Switch Module	Switch			
Switch-10	12.251.240.219	Hewlett-Packard	ProCurve 2524	Switch	F.04.08		F.02.0
Switch-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			

Total 333 devices | 0 devices selected

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.



Open 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 when 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 computers in a directory
- Finding new IP addresses in a device's ARP cache²
- Finding new IP addresses in a device's connection table³

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.

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

³ 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 access 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.

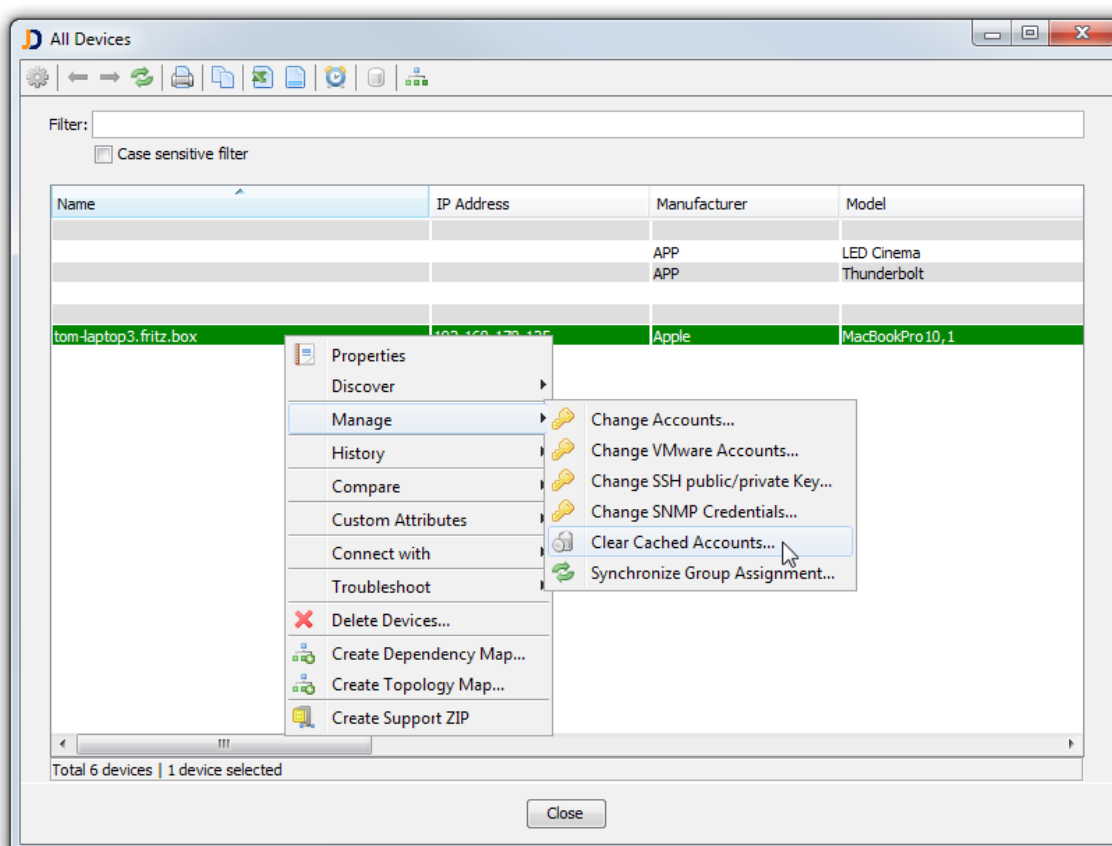


Figure: Clear Cached Access Credentials

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 required 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...*

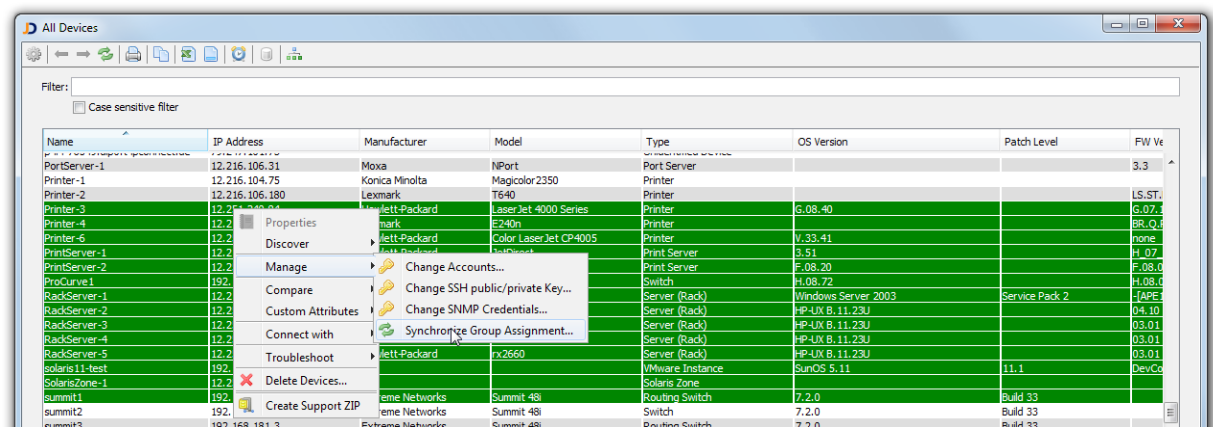


Figure: Synchronize Group Assignments

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.

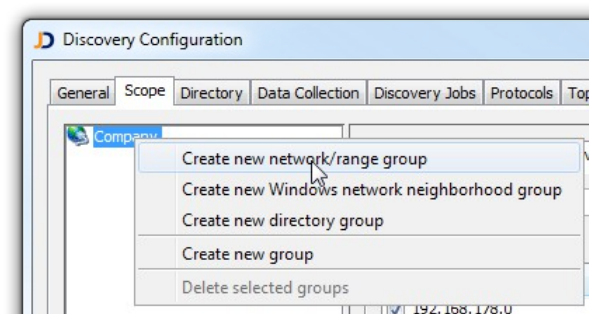


Figure: Create New Group

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 sub-networks 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*.

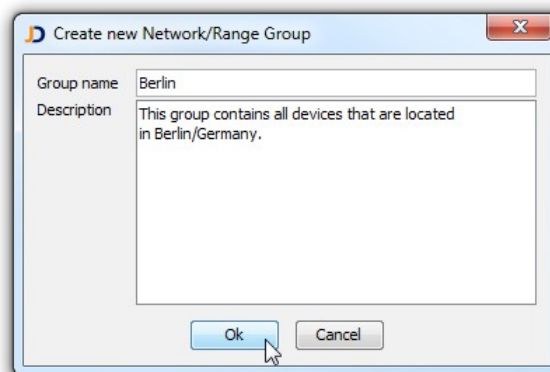


Figure: Create new Network/Range Group

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.

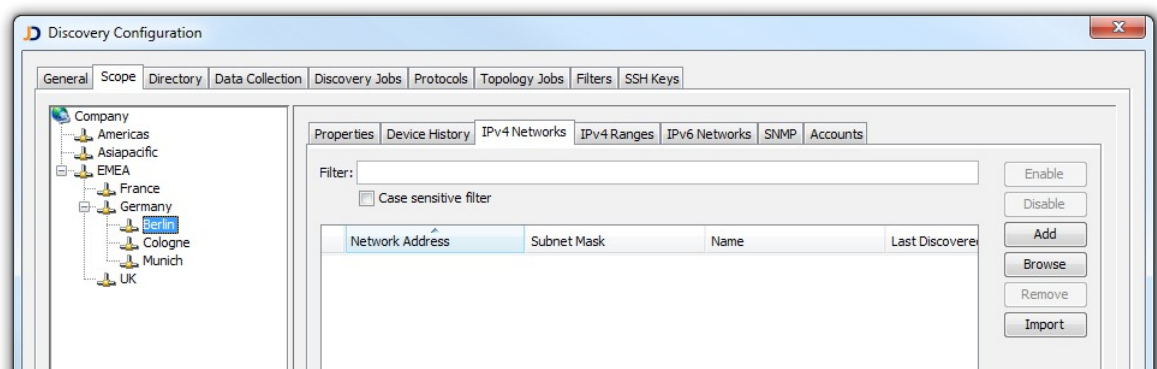


Figure: Define Networks associated with this Group

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.

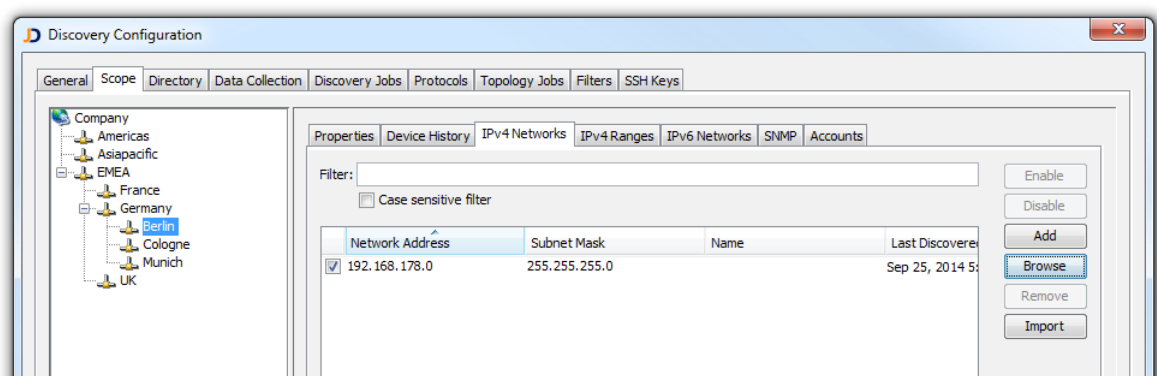


Figure: A Network Group with one Network

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*.

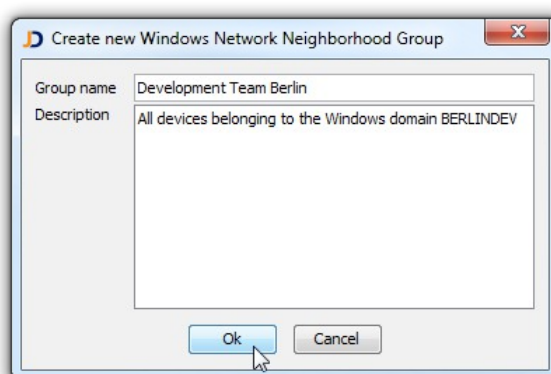


Figure: Create new Network Neighborhood Group

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.

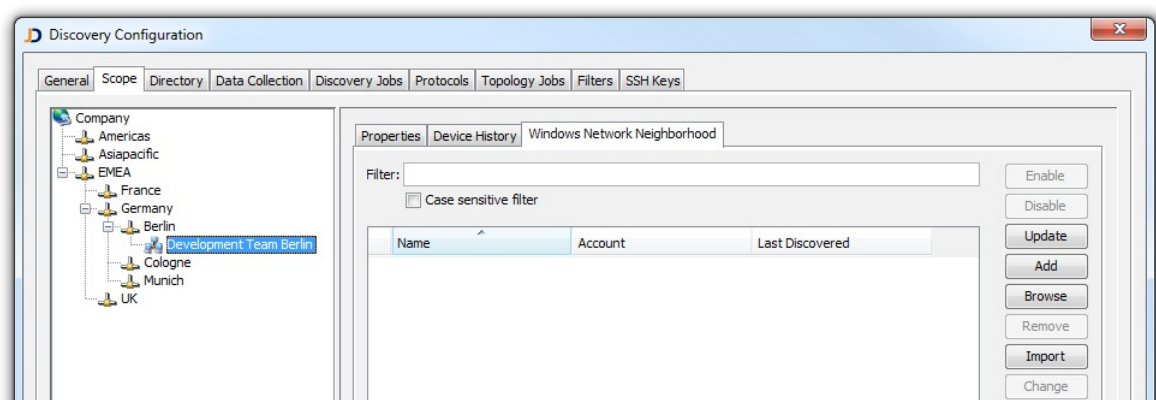


Figure: The Network Neighborhood Group

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.

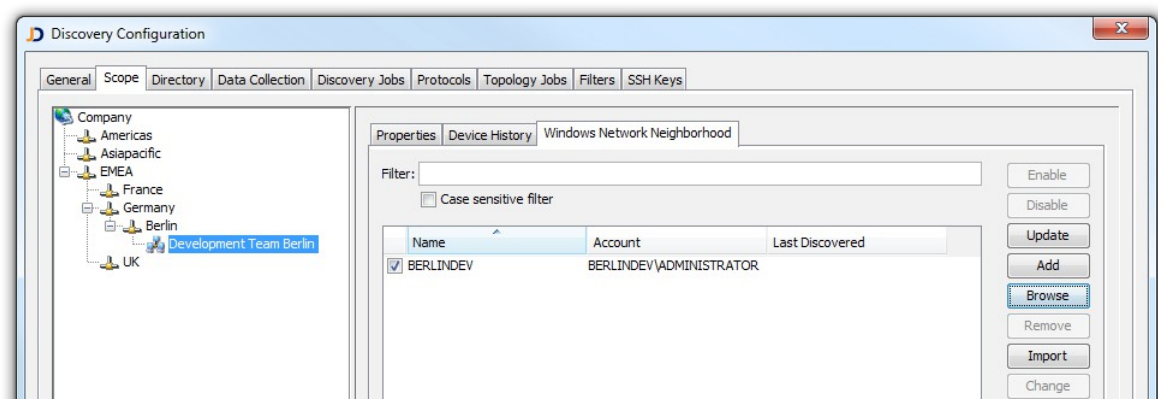


Figure: Group with Associated Windows Neighborhood Objects

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*.

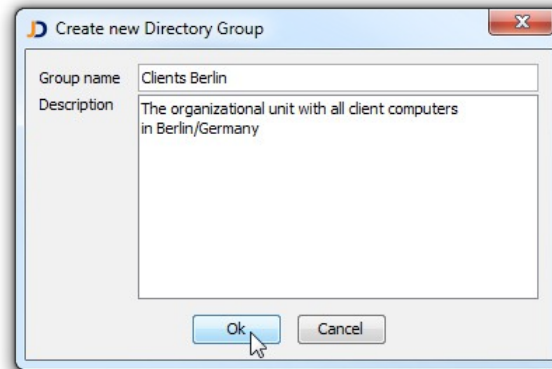


Figure: Create new Directory Group

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.

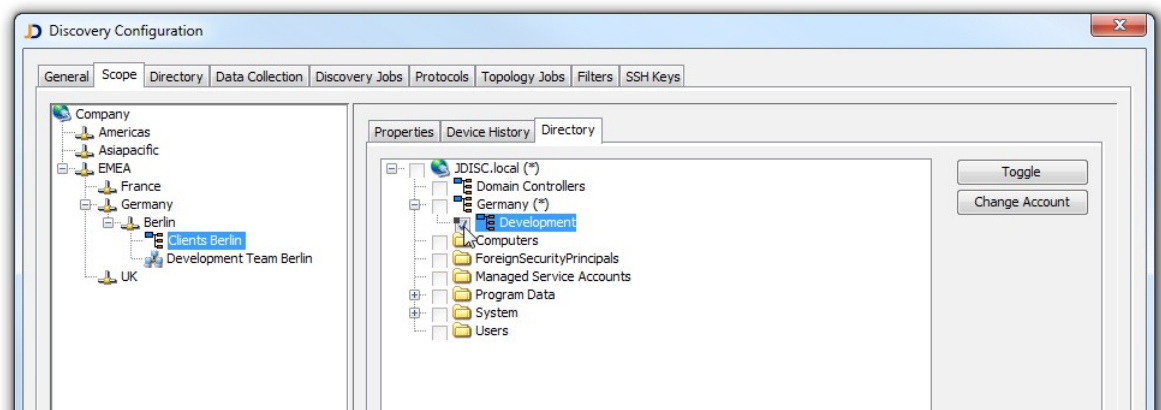


Figure: Directory Group with associated Directory Objects

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*.

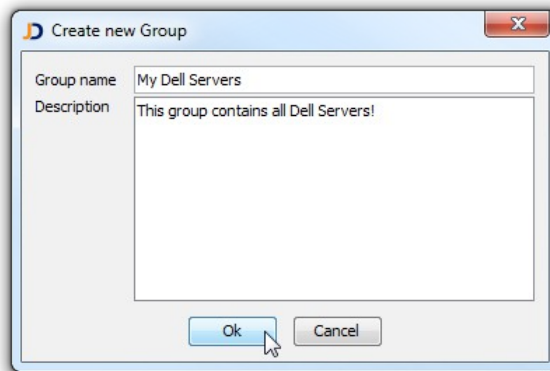


Figure: Create a new Group

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.

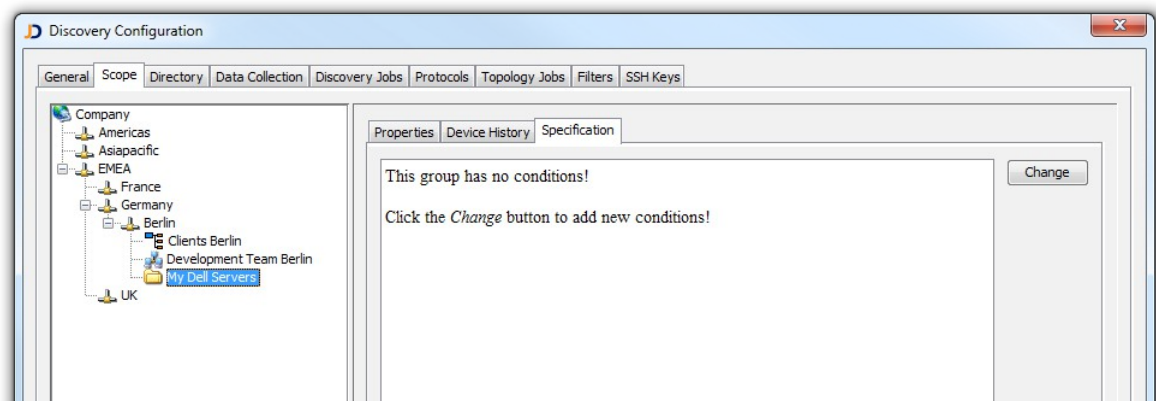


Fig: Group Specification

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

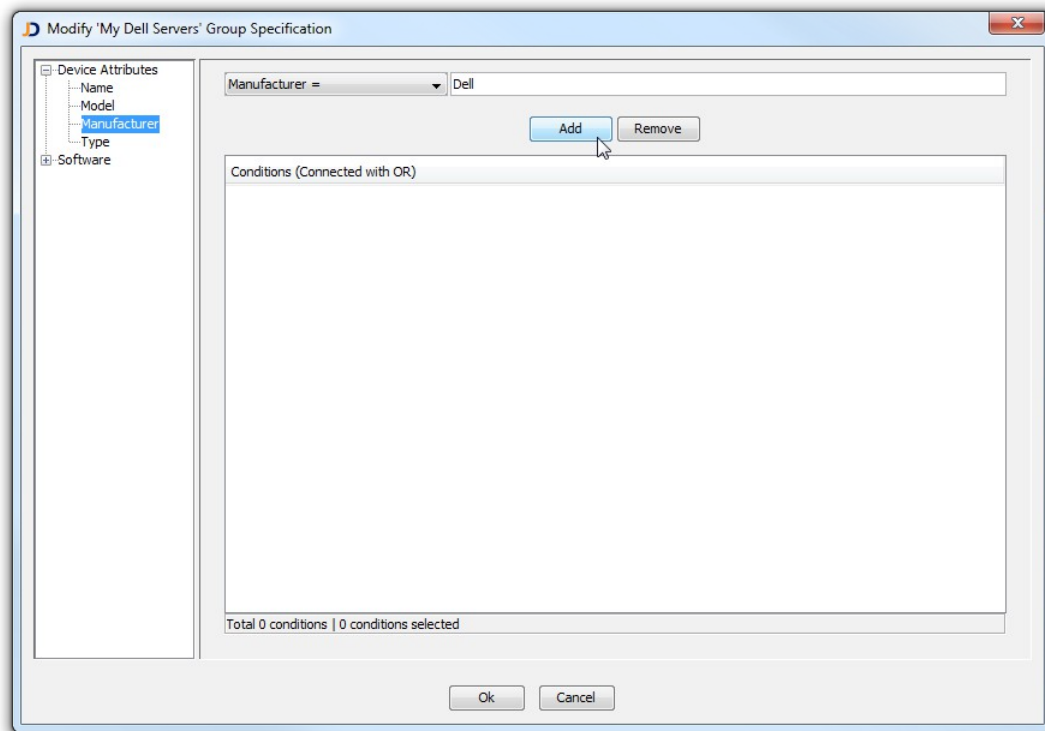


Figure: Change Group Specification

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.

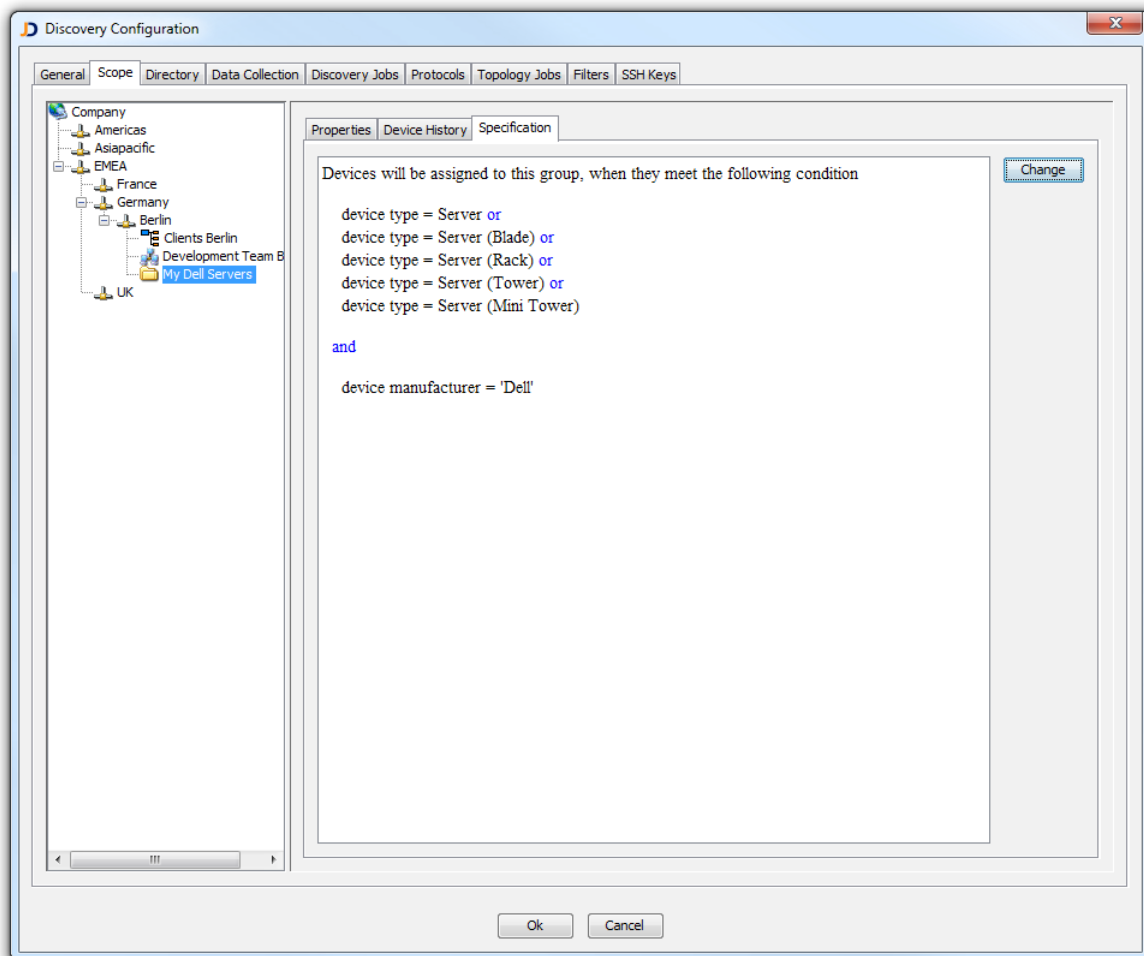


Figure: Group definition summary

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.

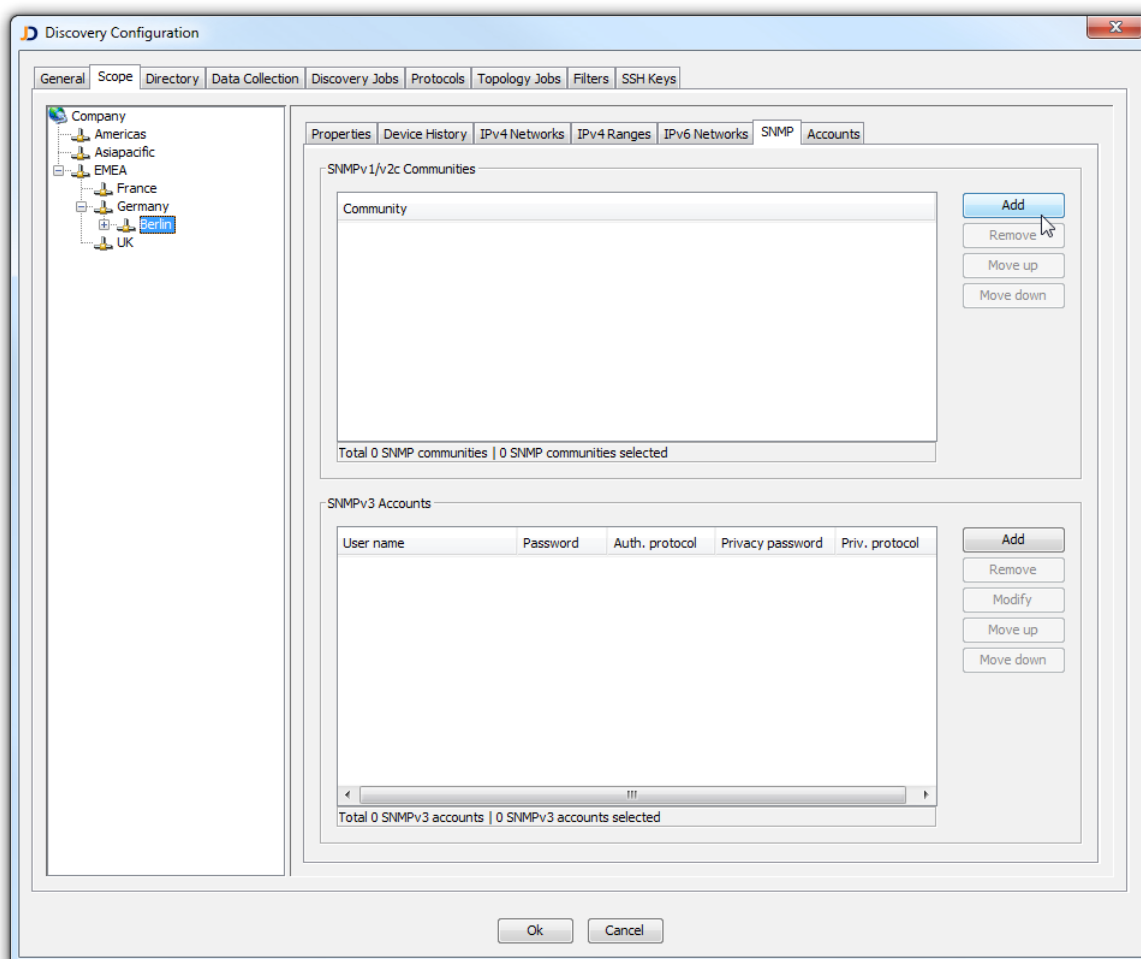


Figure: Default SNMP Communities and SNMPv3 Accounts

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.

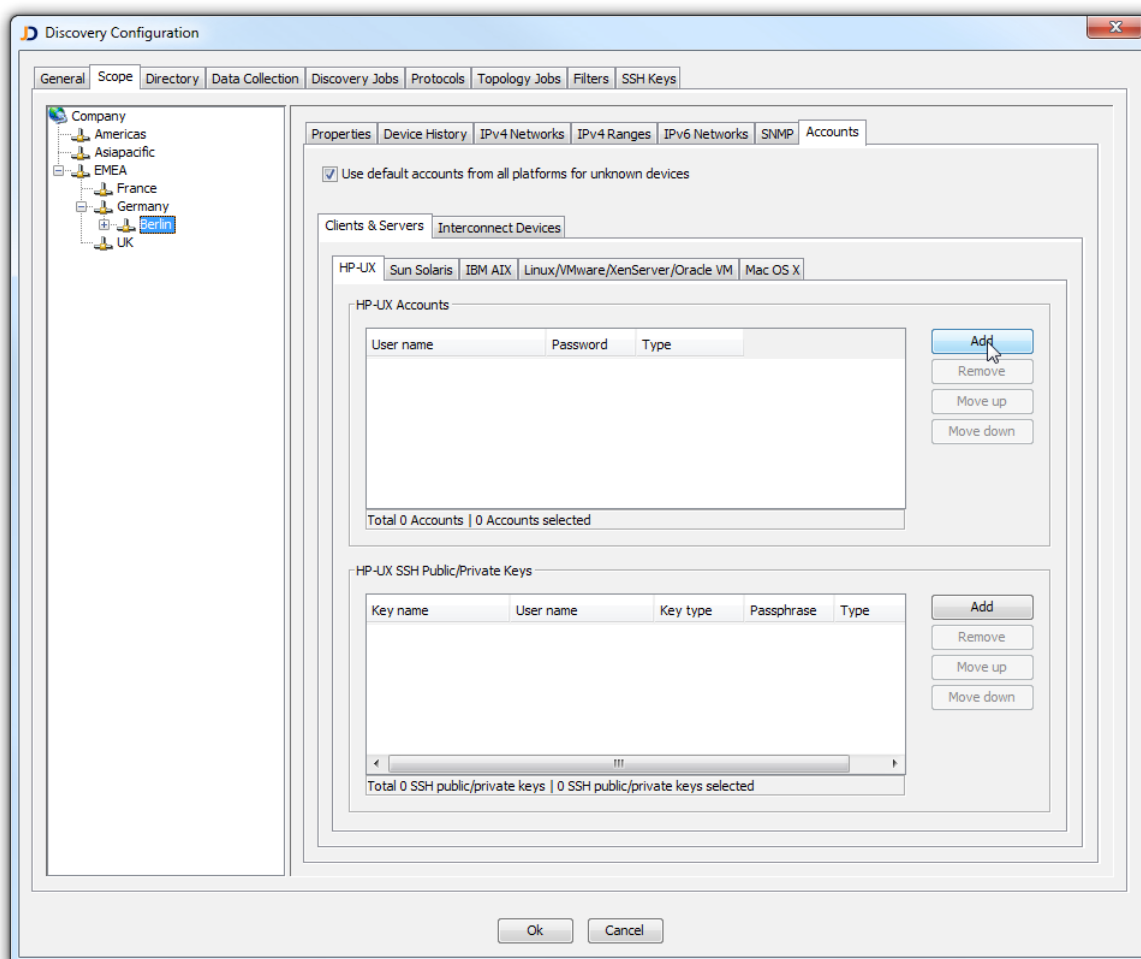



Figure: Manage default Accounts for UNIX Platforms

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  to open the group tree. The group icon might be disabled in reports where grouping is not applicable.

Name	IP Address	Manufacturer	Model	Type
HPE49E84	192.168.178.43	Hewlett-Packard	OfficeJet J6400 Series	Mult
NP130D220.fritz.box	192.168.178.38	Hewlett-Packard	LaserJet CM1415fhw	Mult
ProCurve1	192.168.178.18	Hewlett-Packard	ProCurve 2650	Swit
teetee-pc.fritz.box	192.168.178.20	Hewlett-Packard	m8180.de	Desi
xenserver	192.168.178.55	Hewlett-Packard	Compaq dx2450	Mini
summit1	192.168.178.13	Extreme Networks	Summit 48i	Rou
192.168.178.7	192.168.178.7	Dell	PowerEdge T110 II	Seri
192.168.178.73	192.168.178.73	Dell	PowerEdge T110 II	Seri
ttrenz-PC2.fritz.box	192.168.178.75	Dell	Studio Hybrid 140g	Desi
cisco-sw1	192.168.178.4	Cisco Systems	C2900XL	Swit
firewall.home.net	192.168.178.17	Cisco Systems	PIX 501	Fire
tom-laptop3.fritz.box	192.168.178.81	Apple	MacBookPro10,1	Lapt
3comtest	192.168.178.16	3COM	SuperStack 3 Switch 4300	Swit
0005CD0D0806.fritz.box	192.168.178.57			Umc
192.168.178.118	192.168.178.118			Virt.

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.

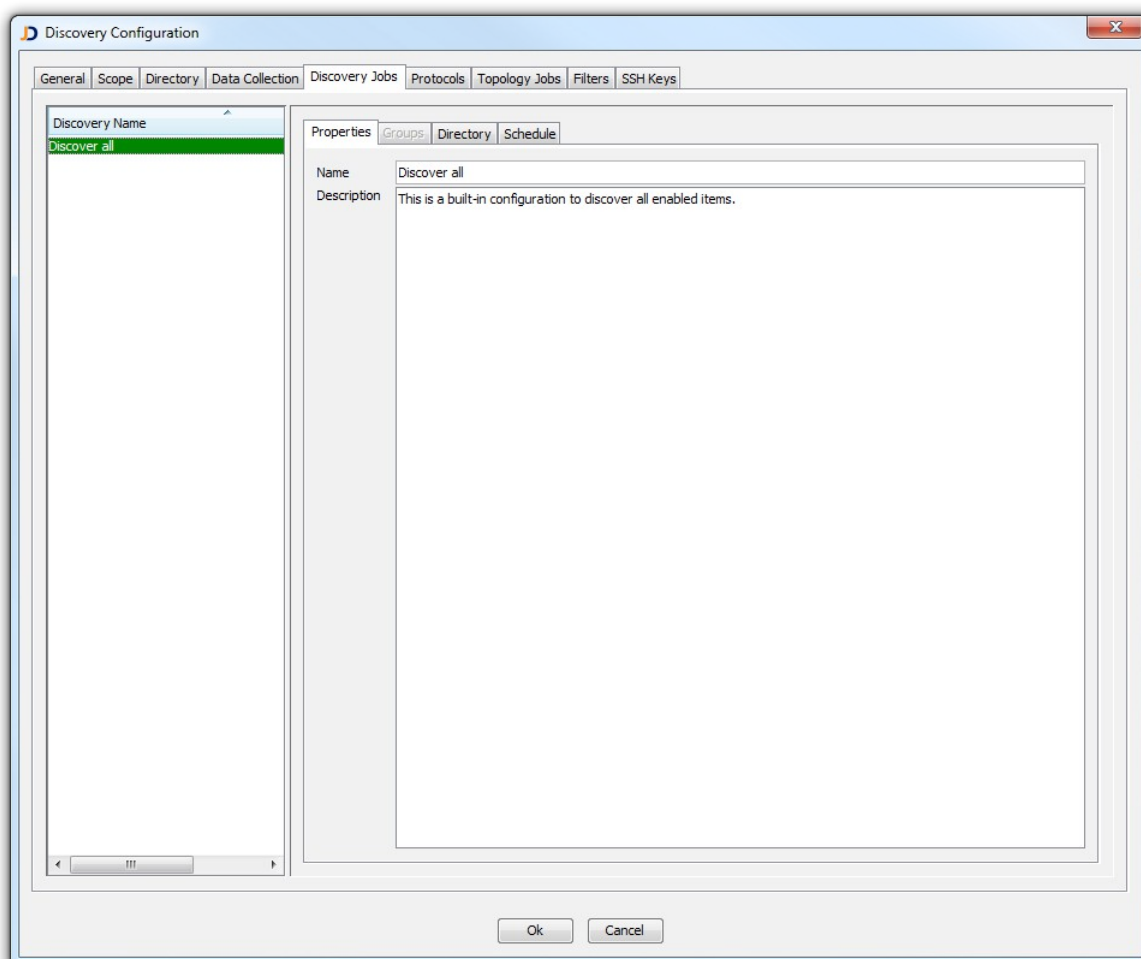


Figure: The 'Discover all' Discovery Job

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*.

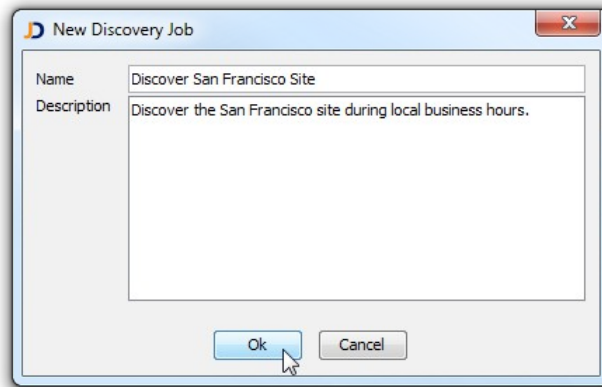


Figure: Create a new Discovery Job

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*.

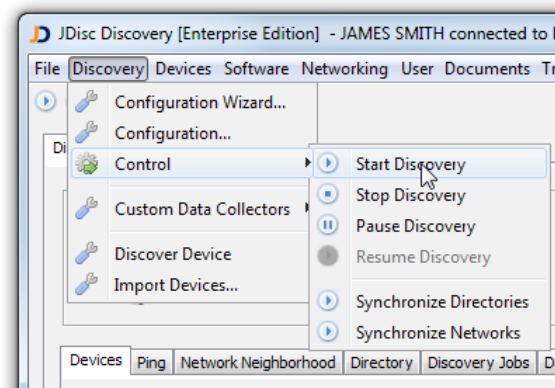


Figure: Control Discovery Menu

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.

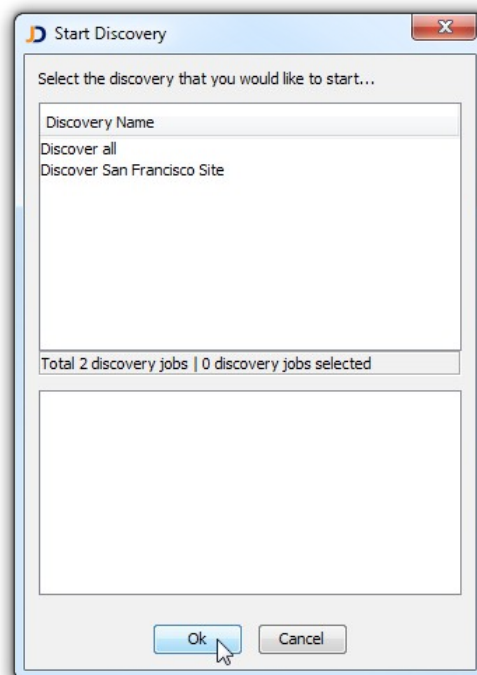




Figure: Select and start a Discovery Job

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  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 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.

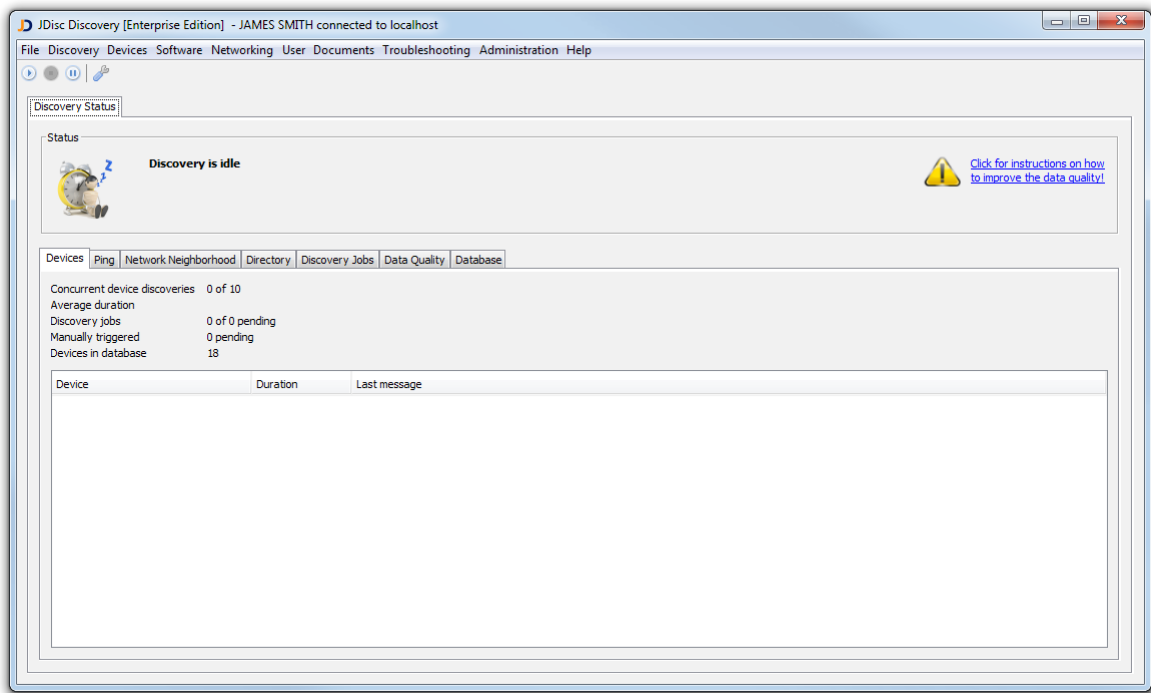


Figure: The Main Window with Status Information

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 Neighborhood	Directory	Discovery Jobs	Database
Concurrent device discoveries 8 of 10					
Average duration Average discovery time: 00:00:19 (1849 devices per hour)					
Discovery jobs 8 of 8 pending					
Manually triggered 0 pending					
Devices in database 0					
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

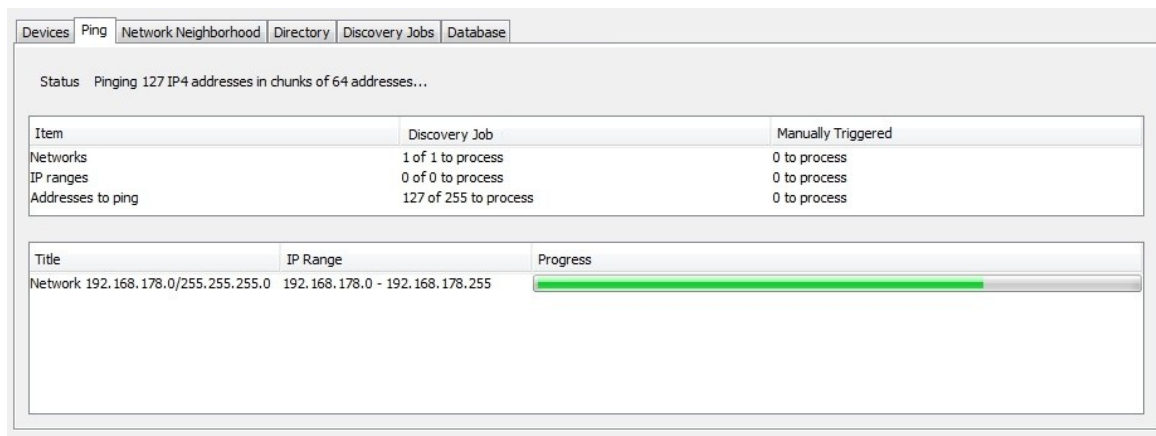


Figure: Ping Status during Discovery of a Network

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.

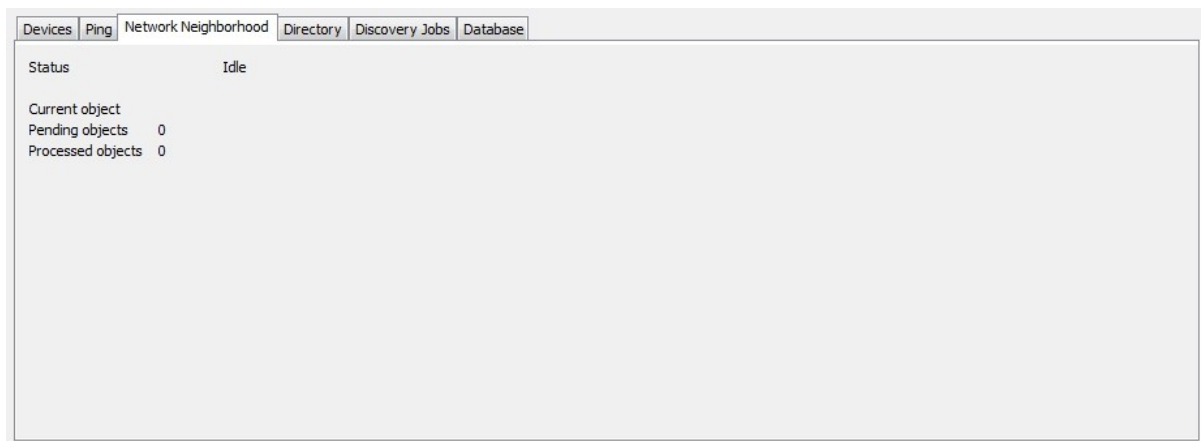


Figure: The Windows Network Neighborhood Status

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.

Devices	Ping	Network Neighborhood	Directory	Discovery Jobs	Database
Synchronization					
	Added	Removed	Synchronized	Status	Message
Directory	0	0	0	Idle	
Network	0	0	0	Idle	
Queue					
Status	Idle				
Message					
Processed	0				
Pending	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.

Devices	Ping	Network Neighborhood	Directory	Discovery Jobs	Database
Discovery Job	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.

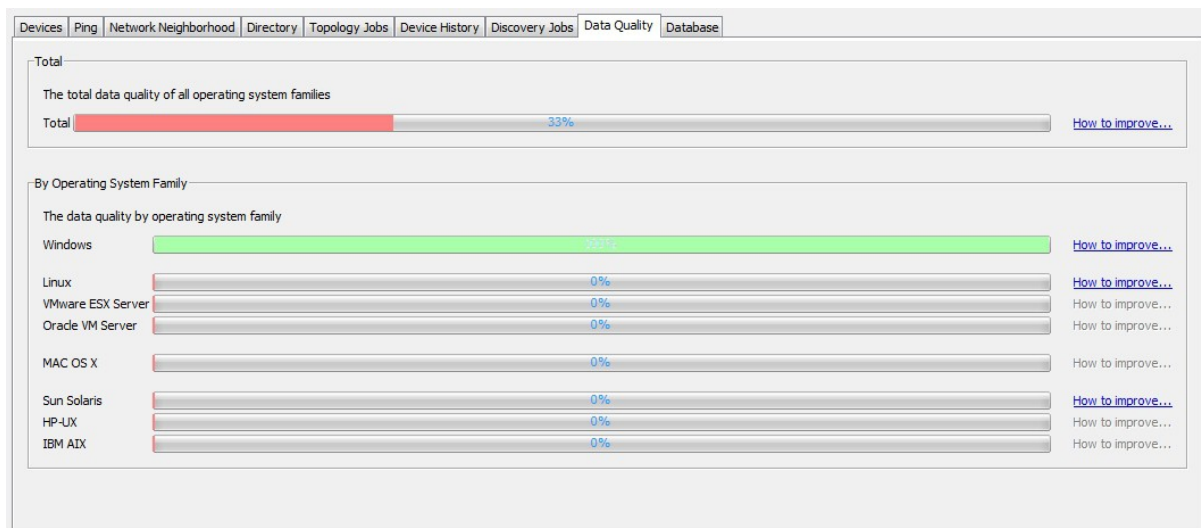


Figure: Data Quality tab

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)

The screenshot shows the 'Database' tab with a 'Database size' of 230.81 MB and a table listing database tables, their row counts, and their sizes.

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

4 Discovery Scenarios

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 Global 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.⁴
- ☒ Discover all computers of the selected directory object and all sub-directory objects.
- ☐ Discover recently logged-on computers of the selected directory object.⁵
- ☐ 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.

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

⁵ 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 extensions⁶) 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

⁶ 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.

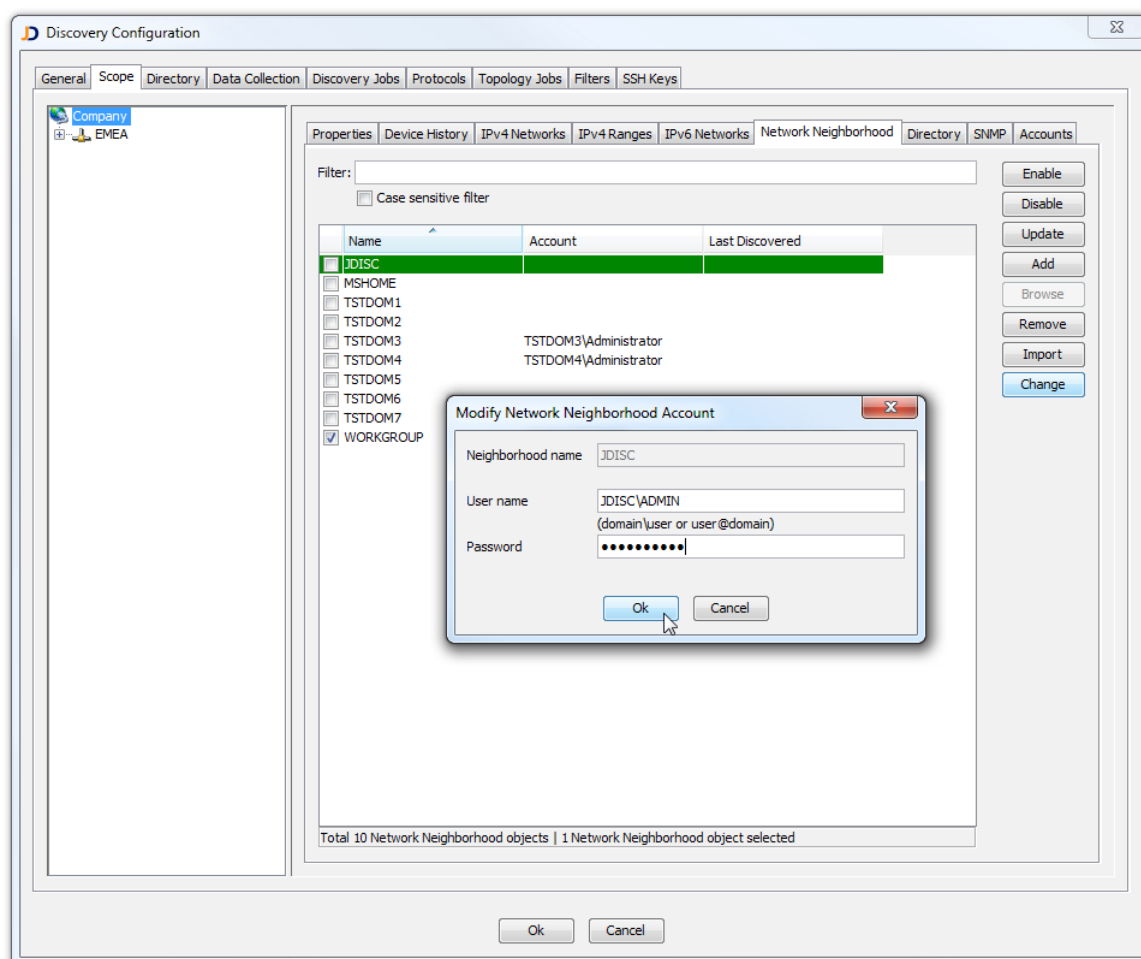


Figure: Configure Windows Network Neighborhood Object Credentials

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.

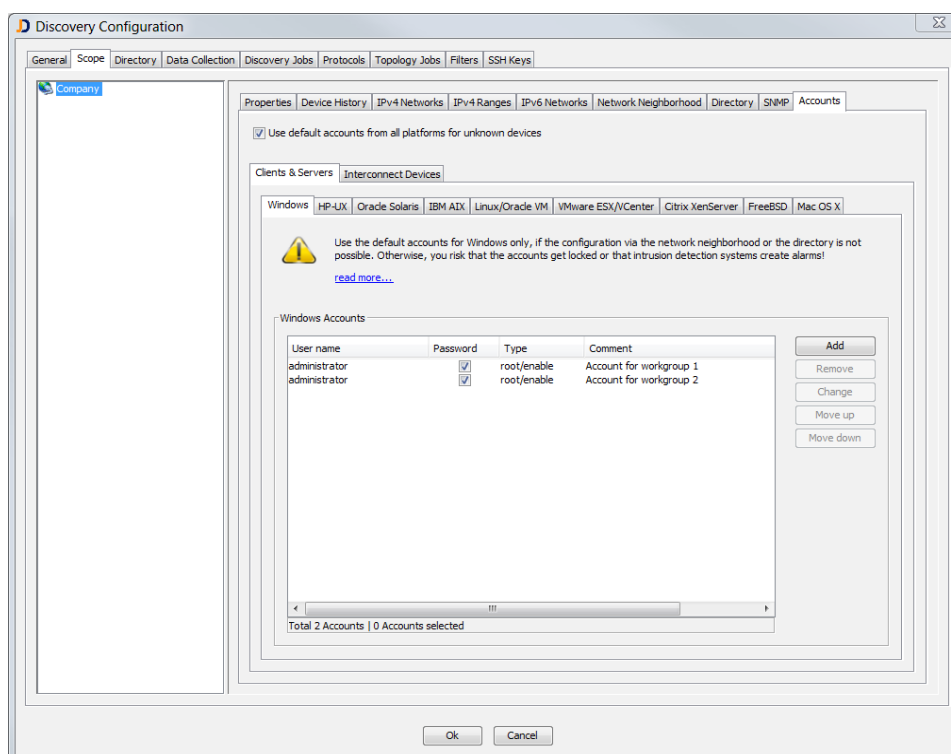


Figure: Default Windows Accounts

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.

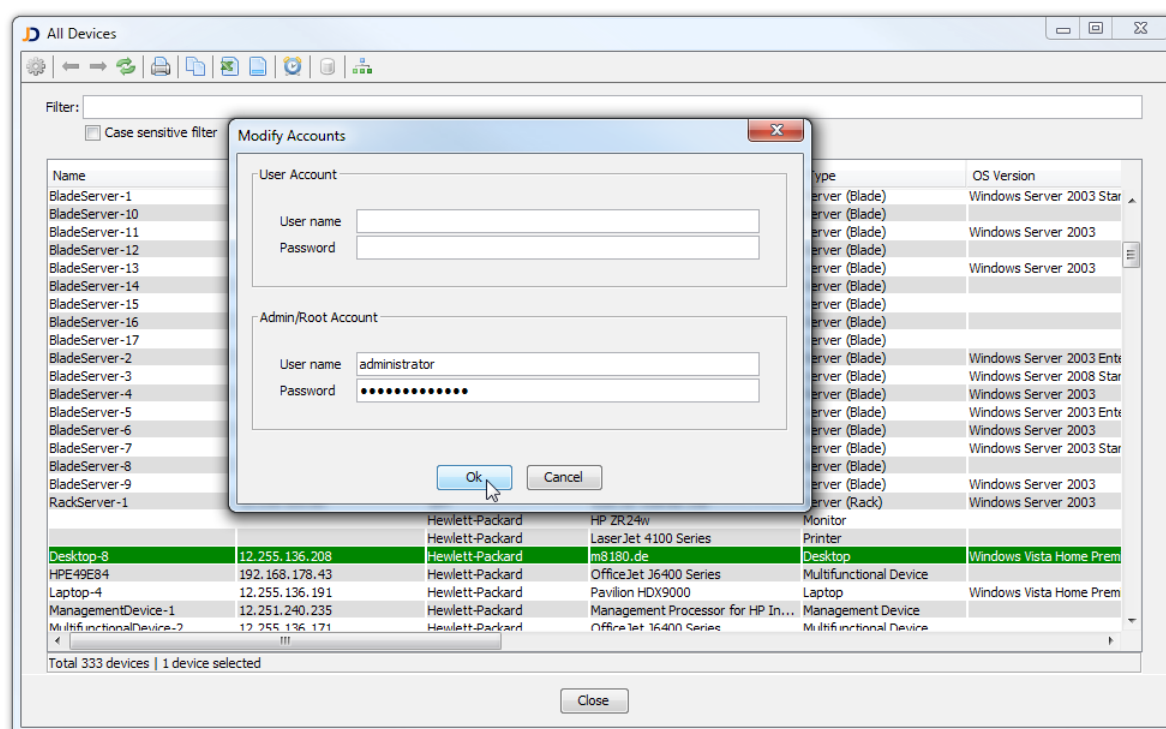


Figure: Change Device Credentials

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.

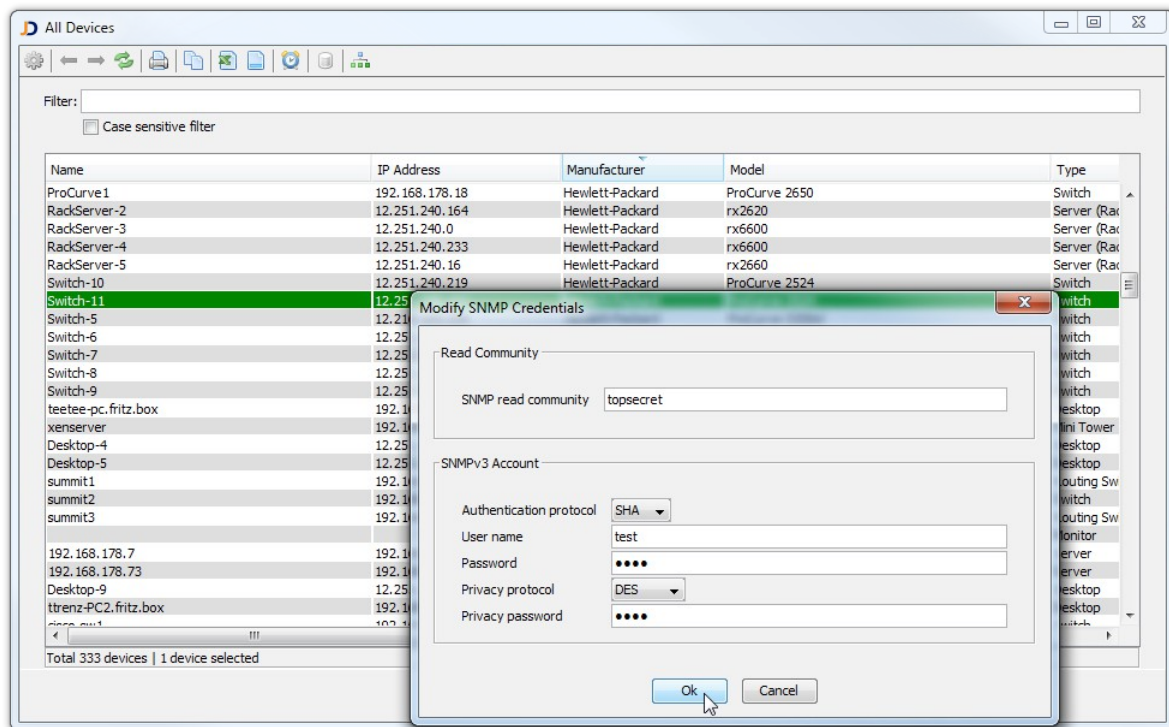


Figure: Change SNMP Access Credentials

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

JDisk 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

JDisk 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.

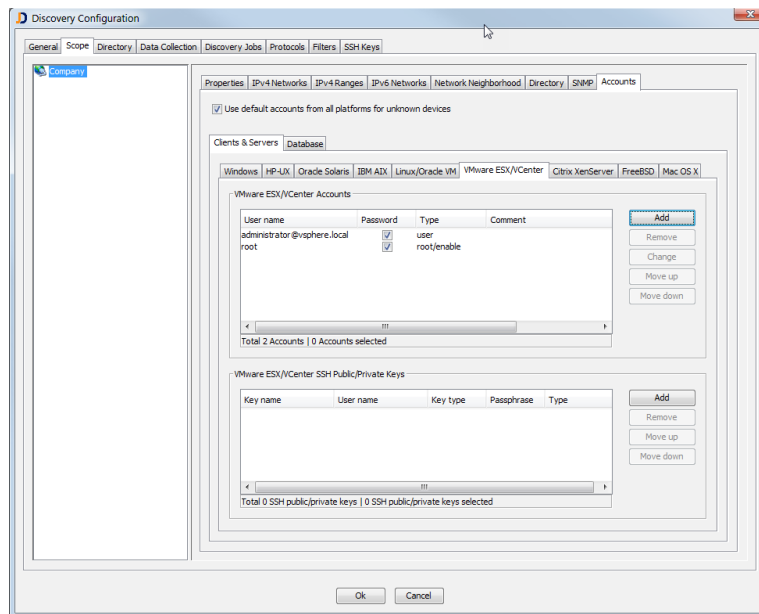


Figure: VMware Default Accounts

JDisc Discovery makes use of information that is stored within the vCenter installation. The discovery process reads cluster, physical 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.

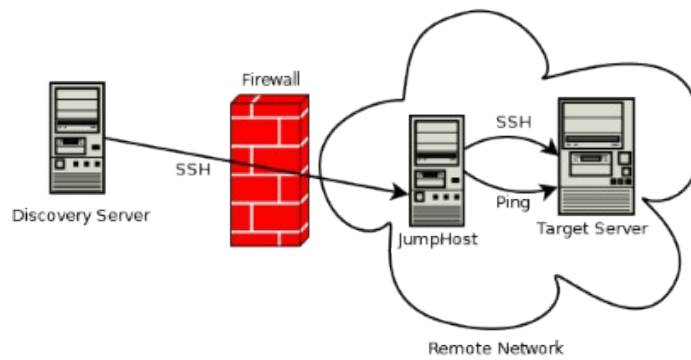


Figure: Scan a device via JumpHost

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.

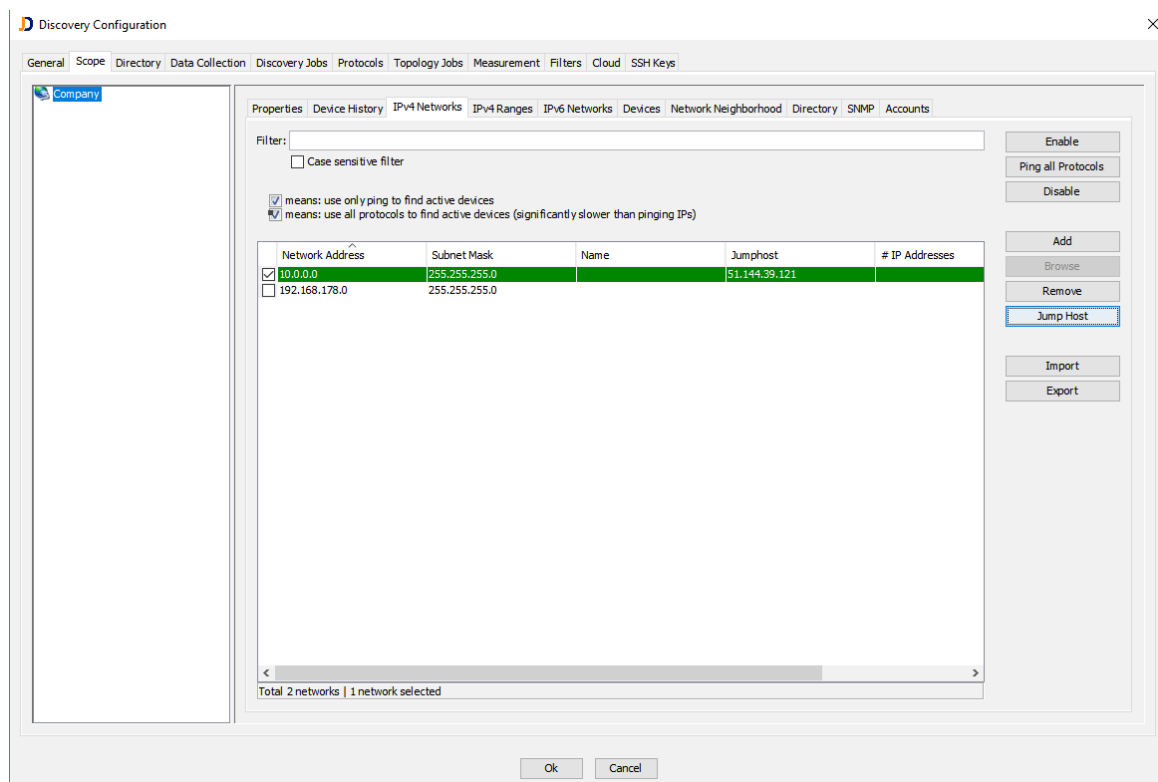


Figure: Jumphost Configuration

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.

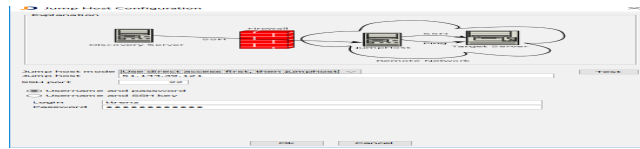


Figure: Jumphost Configuration Dialog

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 <https://localhost> 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 Intune.
- 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.

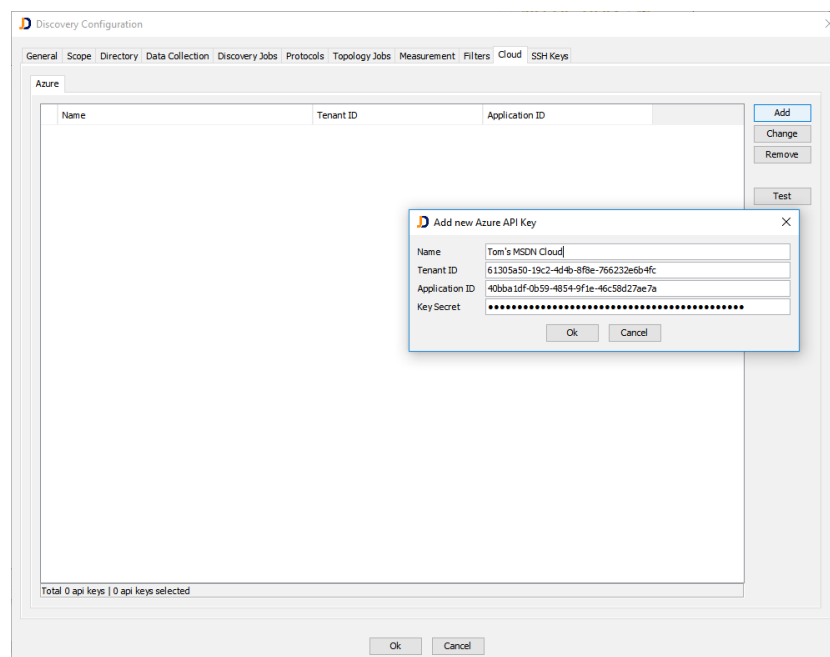


Figure: Add access credentials for an Azure cloud directory

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.

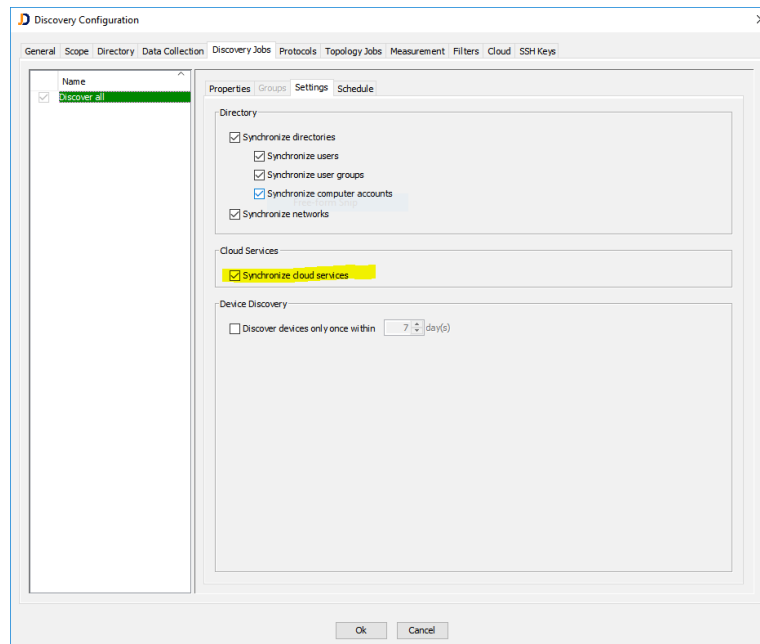


Figure: Enable Cloud Synchronization for a Discovery Job

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.

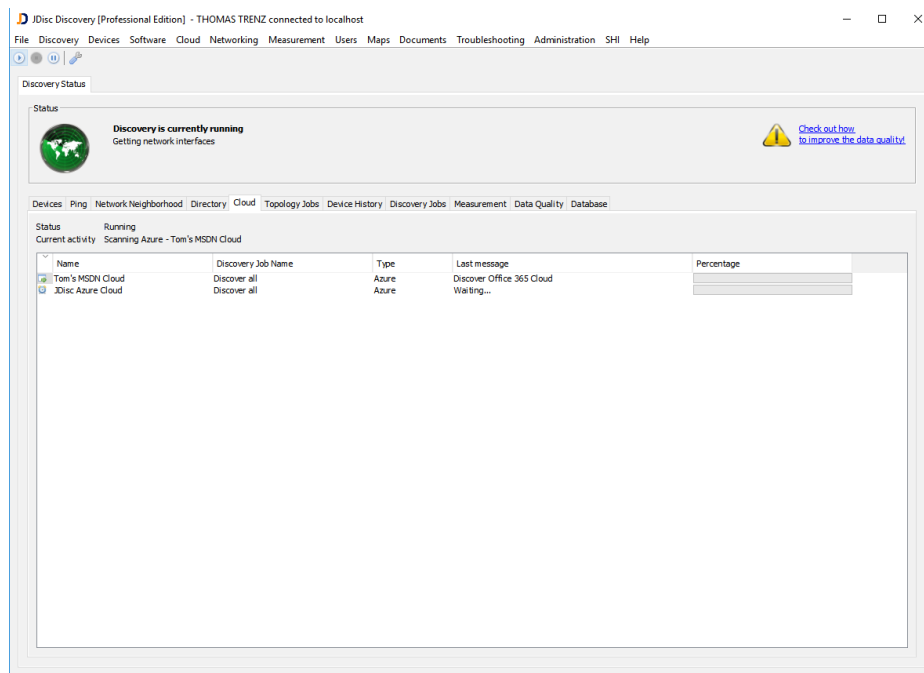


Figure: Cloud Discovery Status

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 subscriptions and their assigned resource groups and resources.

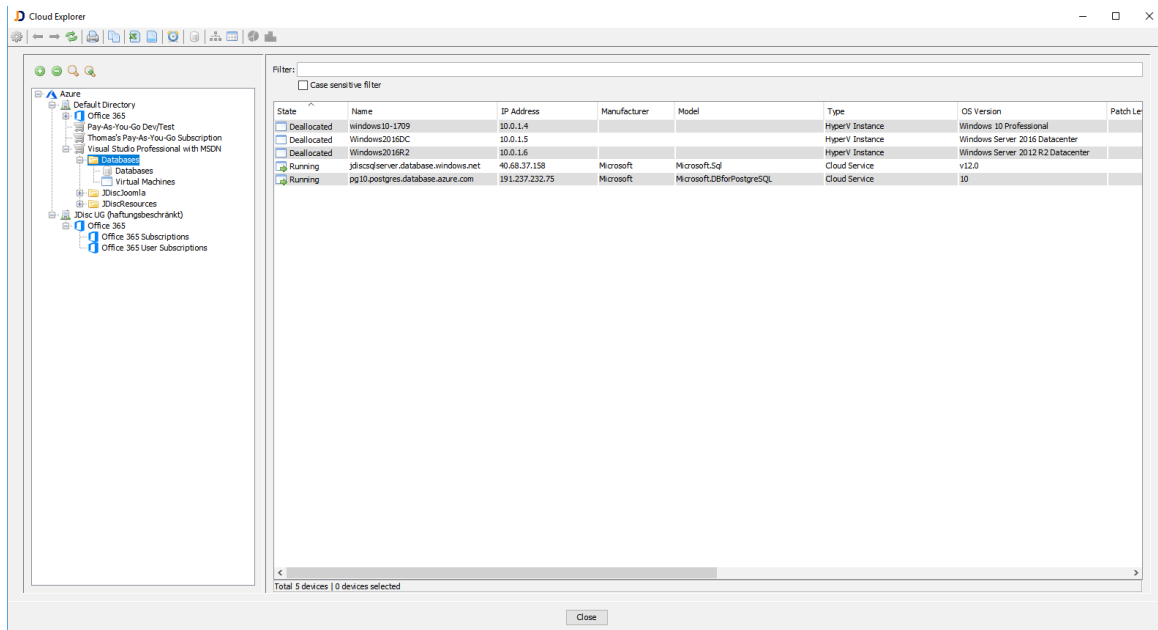


Figure: The *Cloud Explorer*

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.

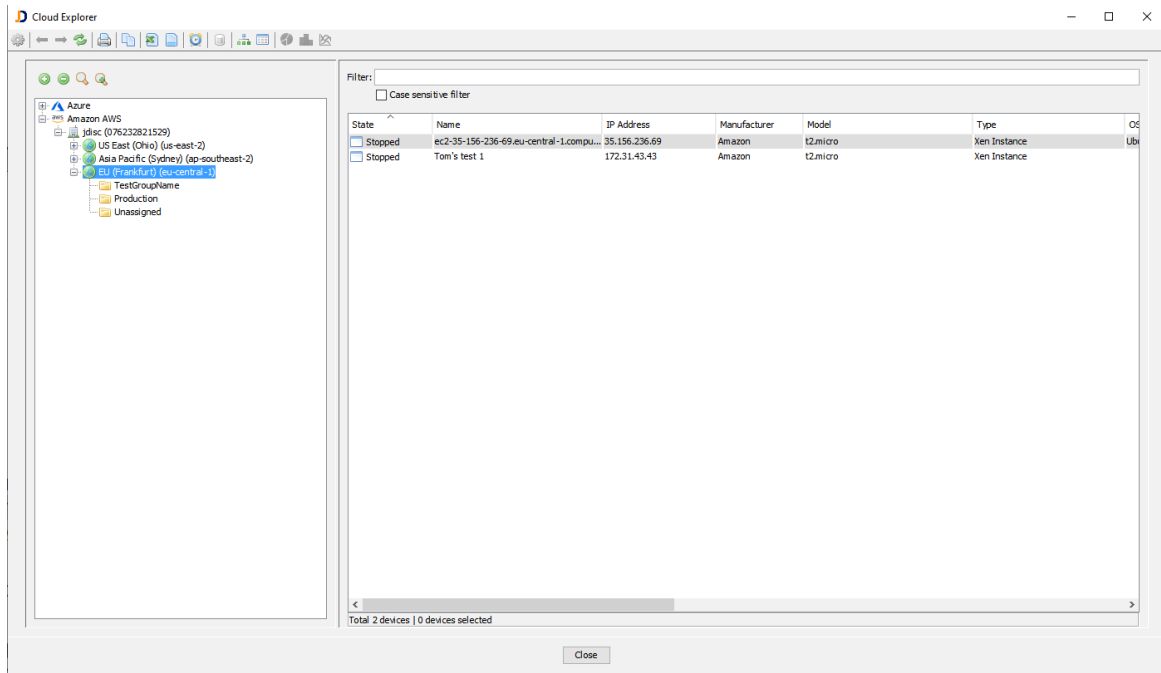


Figure: Amazon AWS Results

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*.

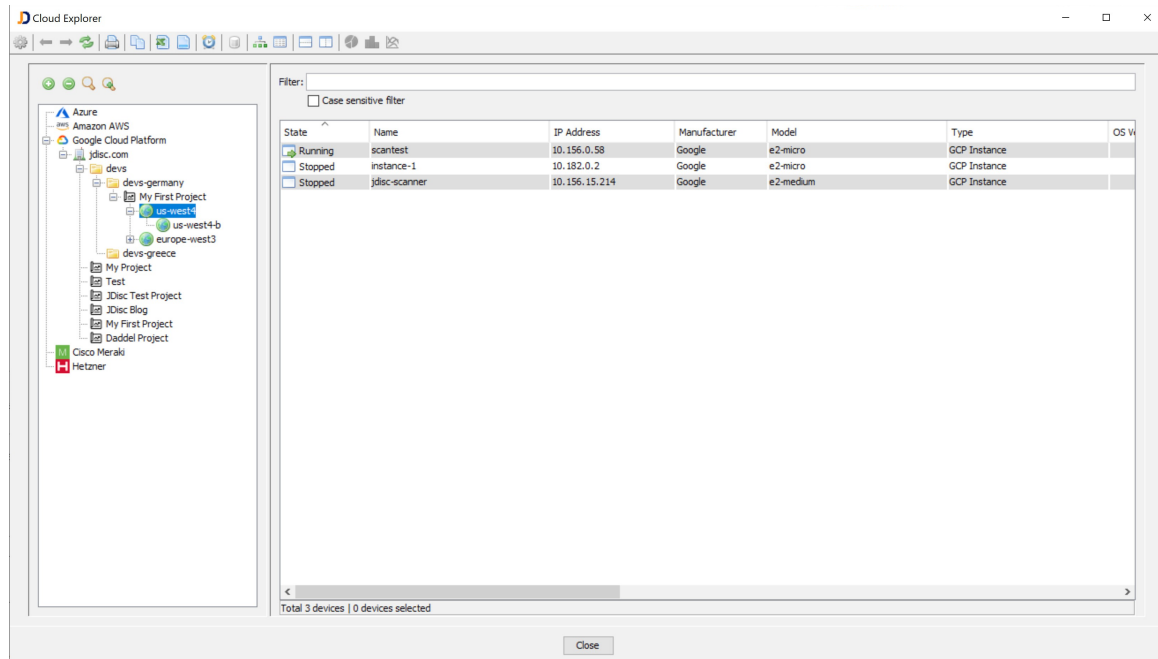


Figure: Google Cloud Platform Scan

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.

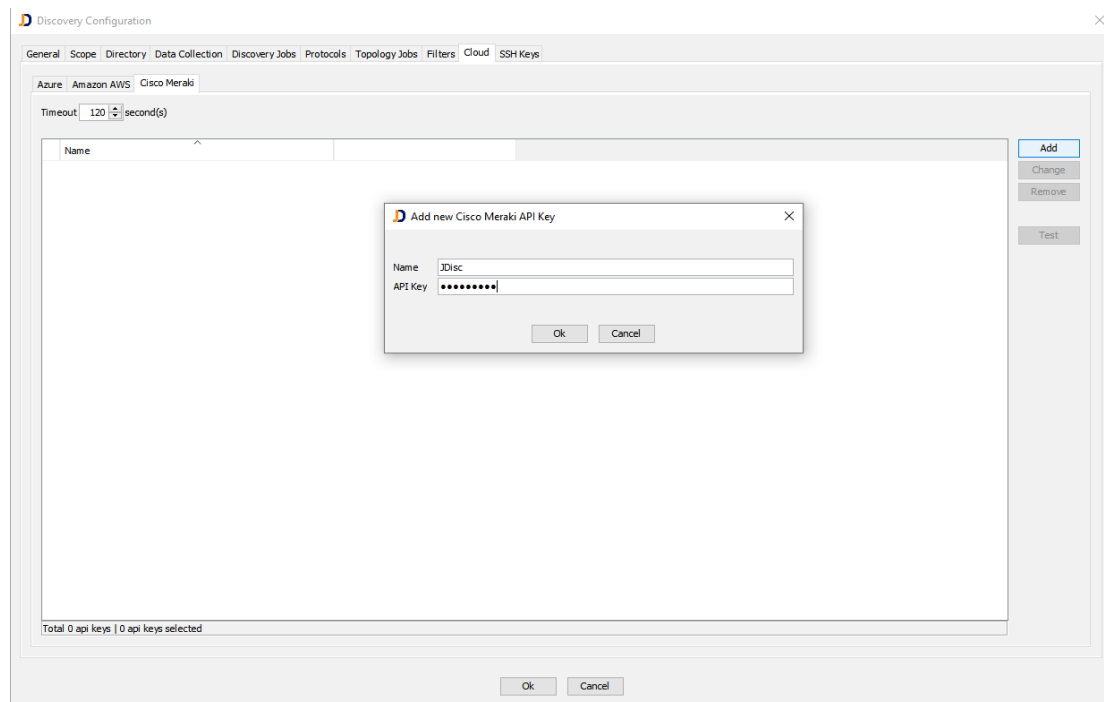


Figure: Configure the API key for the Cisco Meraki Discovery

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.

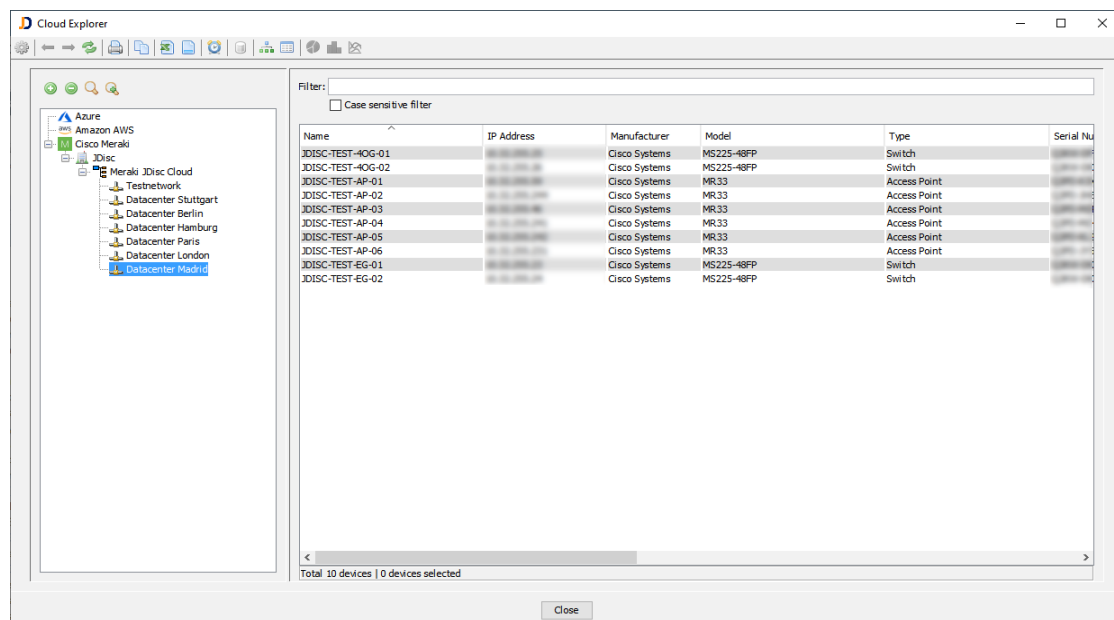


Figure: Meraki Discovery Results

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 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 of local users and user groups is enabled by default and can be disabled from the discovery settings in the *Data Collection* tab.

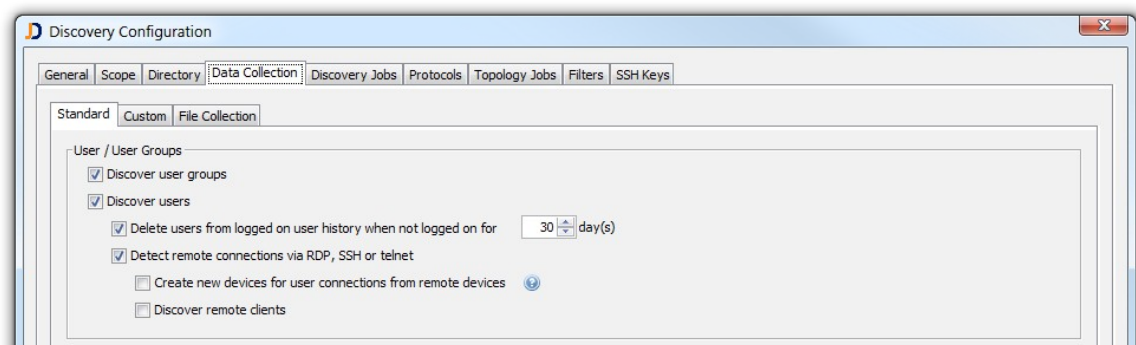


Figure: User / User Group Data Collection Settings

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 Directory users, user groups and user group membership, the *synchronize users* and *synchronize user groups* options must be enabled in the

Discovery Jobs directory tab.

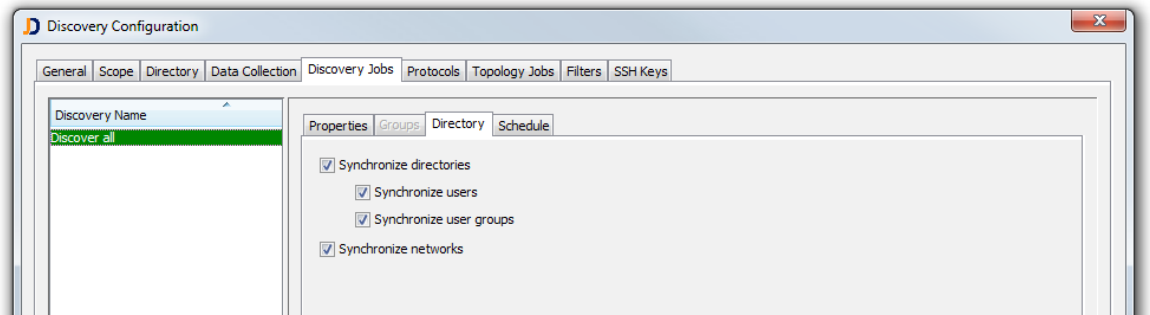


Figure: Directory Synchronization Settings

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.

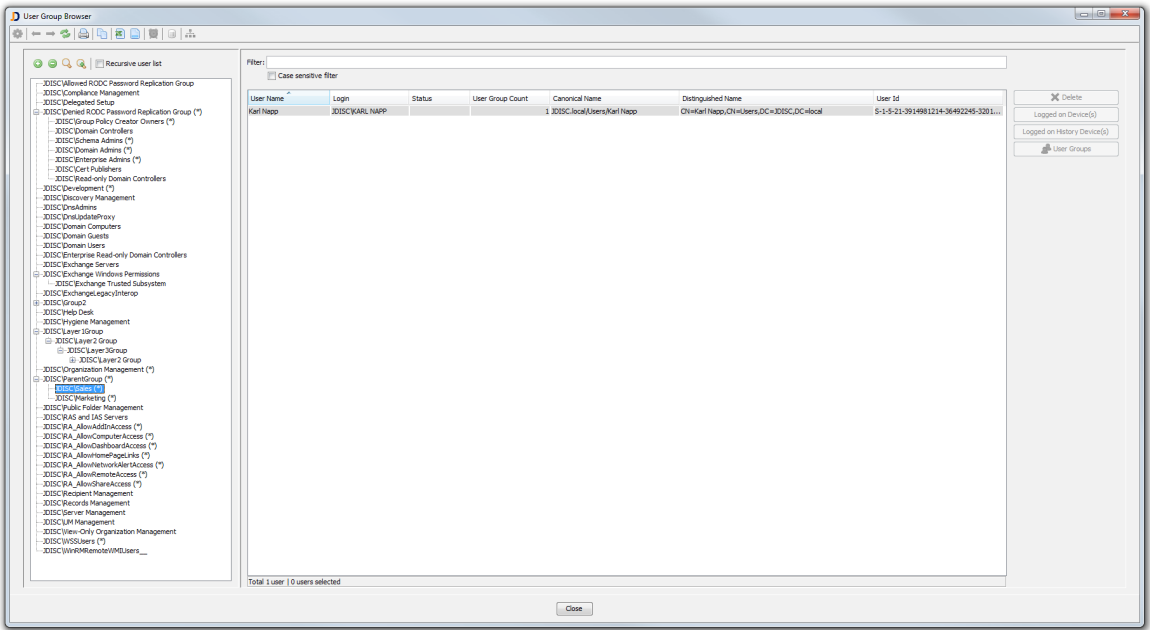
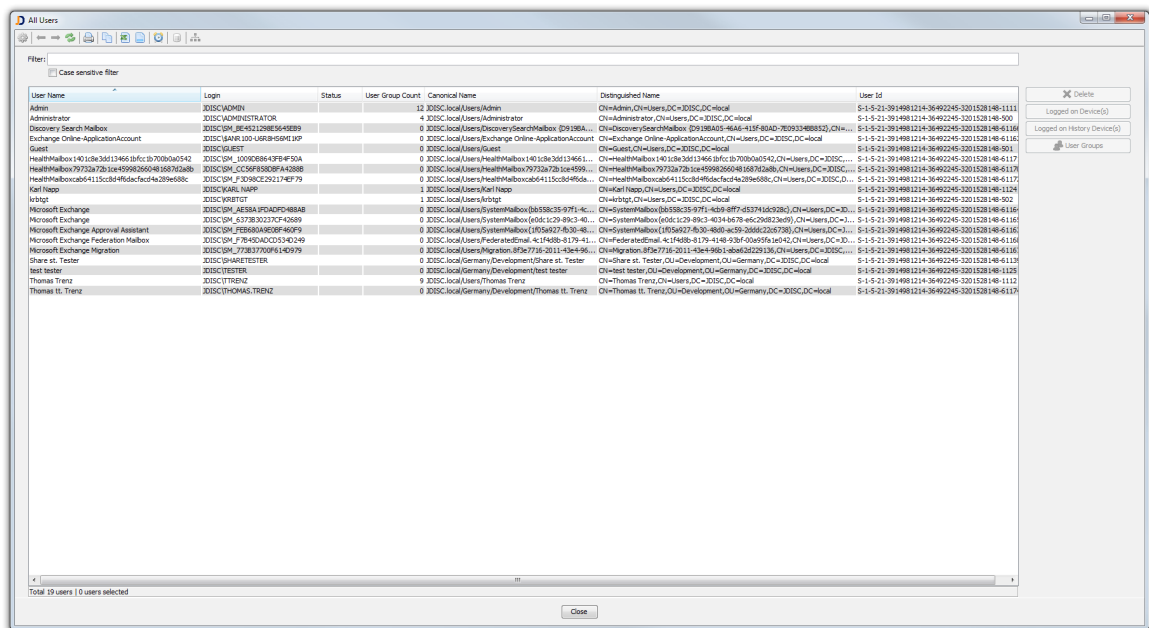


Figure: User Group Browser

4.8.4 User Report

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



User Name	Login	Status	User Group Count	Canonical Name	Distinguished Name	User ID
Admin	JOISC\ADMIN		12	JOISC.local/Admin	CN=Admin,CN=Users,DC=JOISC,DC=local	S-1-5-21-3914981214-36492245-3201528148-1111
Administrator	JOISC\ADMINISTRATOR		4	JOISC.local/Users/Administrator	CN=Administrator,CN=Users,DC=JOISC,DC=local	S-1-5-21-3914981214-36492245-3201528148-500
Discovery Search Mailbox	JOISC\DISCOVERYSEARCHMAILBOX		0	JOISC.local/Users/DiscoverySearchMailbox	CN=DiscoverySearchMailbox,CN=Users,DC=JOISC,DC=local	S-1-5-21-3914981214-36492245-3201528148-6186
Exchange Online-ApplicationAccount	JOISC\EXCHANGEONLINEAPPLICATIONACCOUNT		0	JOISC.local/Users/Exchange Online-ApplicationAccount	CN=Exchange Online-ApplicationAccount,CN=Users,DC=JOISC,DC=local	S-1-5-21-3914981214-36492245-3201528148-6186
Guest	JOISC\GUEST		0	JOISC.local/Users/Guest	CN=Guest,CN=Users,DC=JOISC,DC=local	S-1-5-21-3914981214-36492245-3201528148-501
HealthMailbox 1401c8a3d1196518fc1b7020a0542	JOISC\HEALTHMAILBOX1401C8A3D1196518FC1B7020A0542		0	JOISC.local/Users/HealthMailbox 1401c8a3d1196518fc1b7020a0542	CN=HealthMailbox 1401c8a3d1196518fc1b7020a0542,CN=Users,DC=JOISC,DC=local	S-1-5-21-3914981214-36492245-3201528148-6117
HealthMailbox 79732a72b15a4599826648156762a8b	JOISC\HEALTHMAILBOX79732A72B15A4599826648156762A8B		0	JOISC.local/Users/HealthMailbox 79732a72b15a4599826648156762a8b	CN=HealthMailbox 79732a72b15a4599826648156762a8b,CN=Users,DC=JOISC,DC=local	S-1-5-21-3914981214-36492245-3201528148-6117
HealthMailboxcab4115c8d4f6dcfcd4a289e688c	JOISC\HEALTHMAILBOXCAB4115C8D4F6DCFCD4A289E688C		0	JOISC.local/Users/HealthMailboxcab4115c8d4f6dcfcd4a289e688c	CN=HealthMailboxcab4115c8d4f6dcfcd4a289e688c,CN=Users,DC=JOISC,DC=local	S-1-5-21-3914981214-36492245-3201528148-6117
Karl Hopp	JOISC\KARL.HOPP		1	JOISC.local/Users/Karl Hopp	CN=Karl Hopp,CN=Users,DC=JOISC,DC=local	S-1-5-21-3914981214-36492245-3201528148-1124
Urbtst	JOISC\URBTST		1	JOISC.local/Users/Urbtst	CN=Urbtst,CN=Users,DC=JOISC,DC=local	S-1-5-21-3914981214-36492245-3201528148-902
Microsoft Exchange	JOISC\MICROSOFT EXCHANGE		0	JOISC.local/Users/SystemMailbox (b558c35-9771-4d59-8977-4537465928c2)	CN=SystemMailbox (b558c35-9771-4d59-8977-4537465928c2),CN=Users,DC=JOISC,DC=local	S-1-5-21-3914981214-36492245-3201528148-6186
Microsoft Exchange	JOISC\MICROSOFT EXCHANGE		0	JOISC.local/Users/SystemMailbox (6081c29-8b3c-40...	CN=SystemMailbox (6081c29-8b3c-40341678-efc29832a05),CN=Users,DC=JOISC,DC=local	S-1-5-21-3914981214-36492245-3201528148-6186
Microsoft Exchange Approval Assistant	JOISC\MICROSOFT EXCHANGE APPROVAL ASSISTANT		0	JOISC.local/Users/SystemMailbox (1f5a927-8c30-4650-ac59-3268c2267380)	CN=SystemMailbox (1f5a927-8c30-4650-ac59-3268c2267380),CN=Users,DC=JOISC,DC=local	S-1-5-21-3914981214-36492245-3201528148-6186
Microsoft Exchange Federation Mailbox	JOISC\MICROSOFT EXCHANGE FEDERATION MAILBOX		0	JOISC.local/Users/FederatedMailbox (1f468b-6179-4148-93af-0a09fa3e42)	CN=FederatedMailbox (1f468b-6179-4148-93af-0a09fa3e42),CN=Users,DC=JOISC,DC=local	S-1-5-21-3914981214-36492245-3201528148-6186
Microsoft Exchange Migration	JOISC\MICROSOFT EXCHANGE MIGRATION		0	JOISC.local/Users/Migration (8f778-3811-4e4e-46...	CN=Migration (8f778-3811-4e4e-4638d329138),CN=Users,DC=JOISC,DC=local	S-1-5-21-3914981214-36492245-3201528148-6186
Share st. Tester	JOISC\SHARESTESTER		0	JOISC.local/Users/Development/Share st. Tester	CN=Share st. Tester,OU=Development,OU=Germany,DC=JOISC,DC=local	S-1-5-21-3914981214-36492245-3201528148-6112
Test Tester	JOISC\TESTER		0	JOISC.local/Users/Development/Test Tester	CN=Test Tester,OU=Development,OU=Germany,DC=JOISC,DC=local	S-1-5-21-3914981214-36492245-3201528148-1126
Thomas H. Trenz	JOISC\THOMAS.TRENZ		0	JOISC.local/Users/Thomas H. Trenz	CN=Thomas H. Trenz,CN=Users,DC=JOISC,DC=local	S-1-5-21-3914981214-36492245-3201528148-1112
Thomas H. Trenz	JOISC\THOMAS.TRENZ		0	JOISC.local/Users/Development/Thomas H. Trenz	CN=Thomas H. Trenz,OU=Development,OU=Germany,DC=JOISC,DC=local	S-1-5-21-3914981214-36492245-3201528148-6117

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 all global Active Directory users groups.

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.

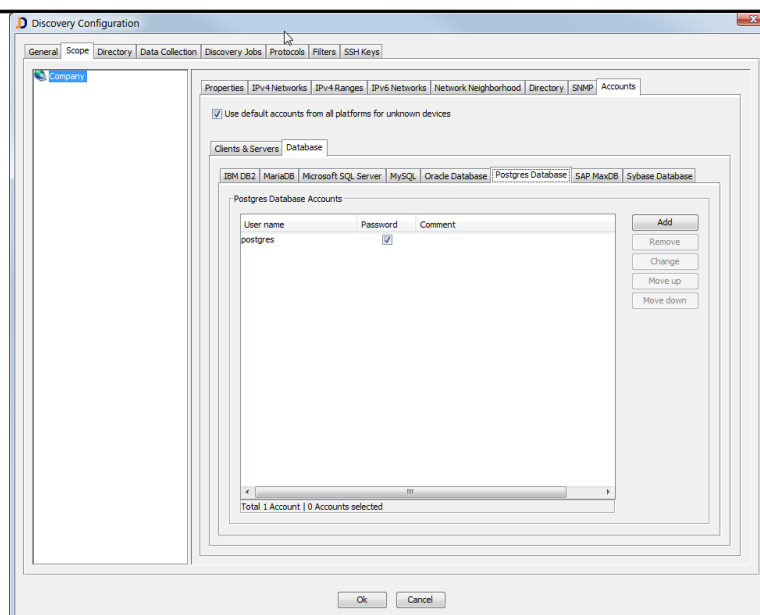


Figure: Configure Default Database Accounts

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.

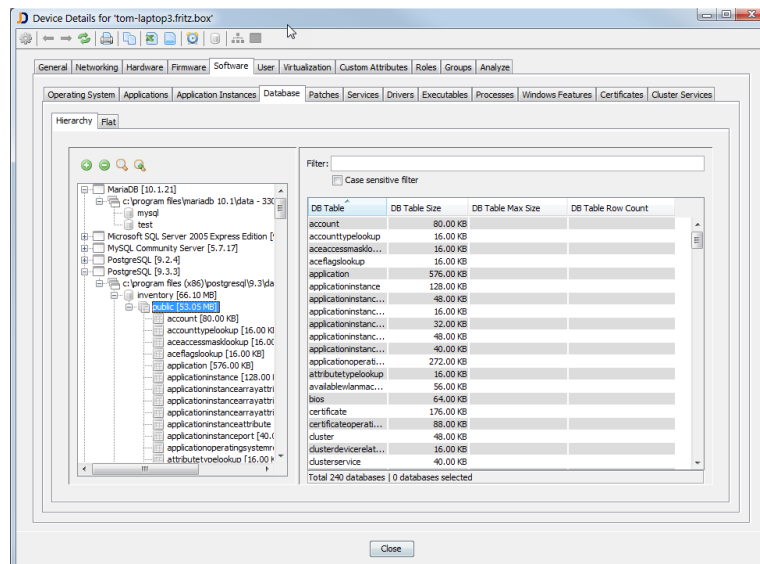


Figure: Database Details

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 multitenant 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.

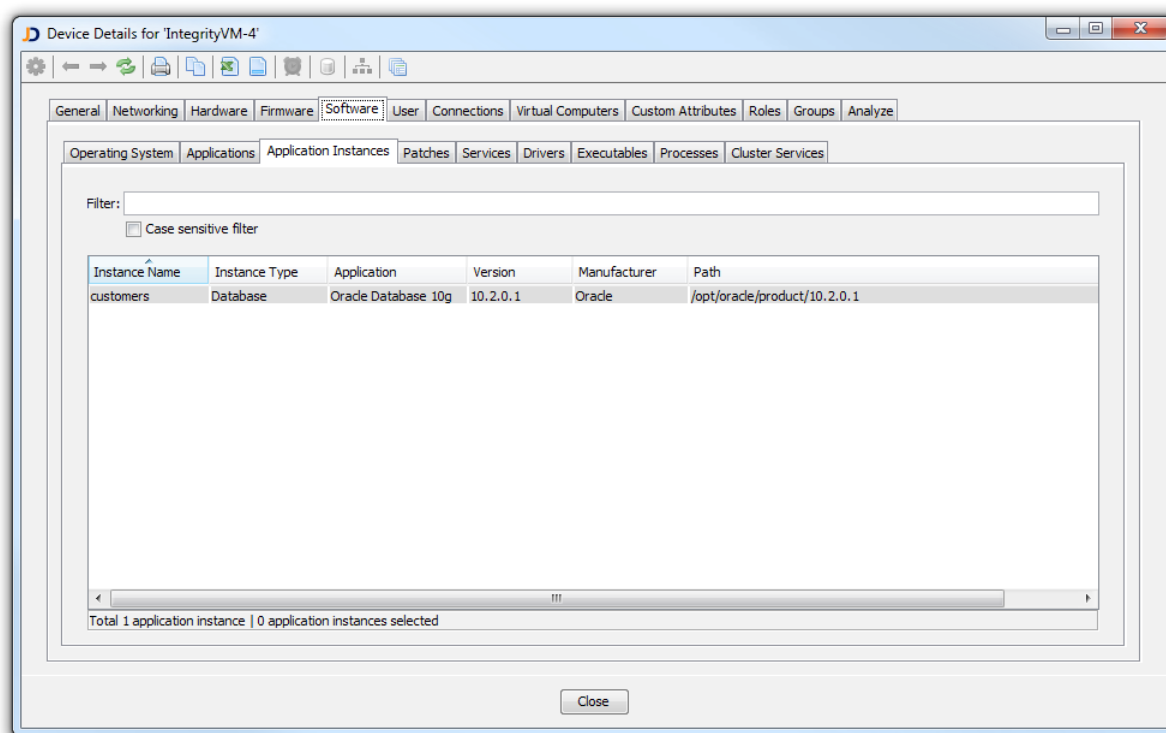


Figure: Database Instances

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.

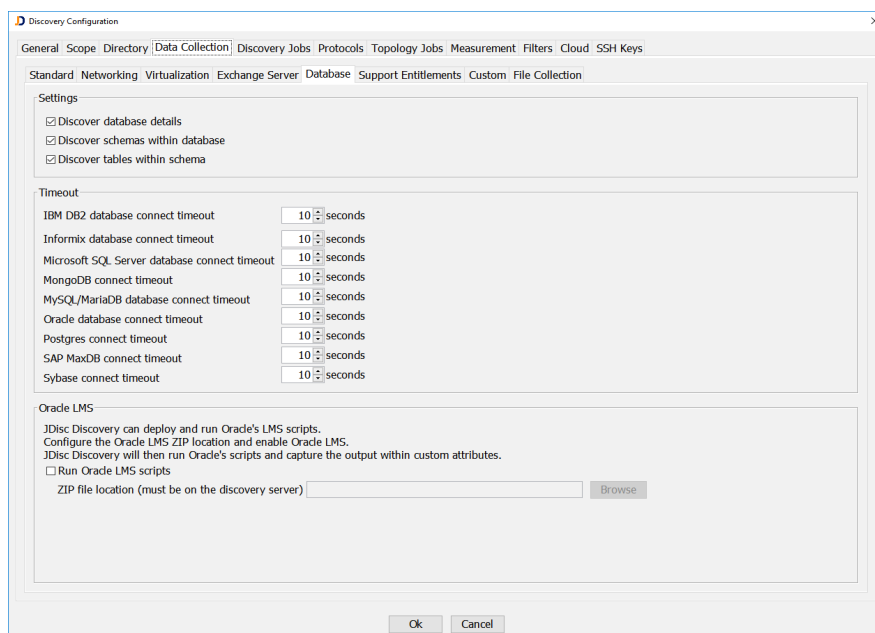


Figure: Configuring Oracle LMS Data Collection

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 Passwordstate

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*.

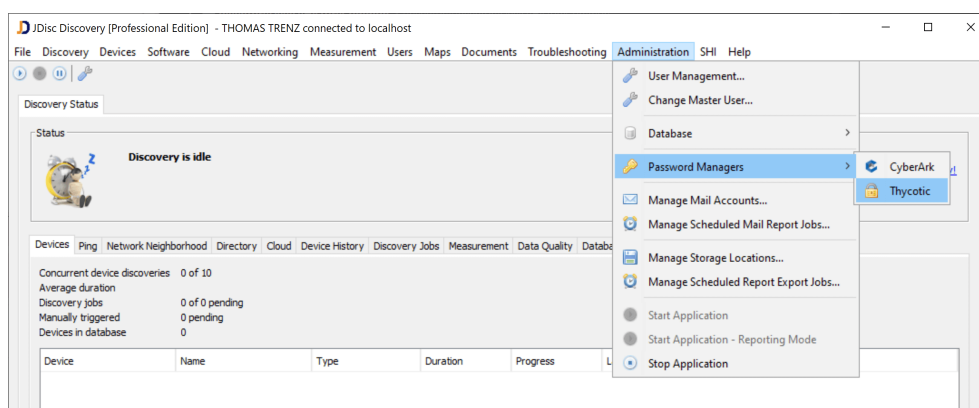


Figure: Configure Thycotic Secret Server Connections

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.

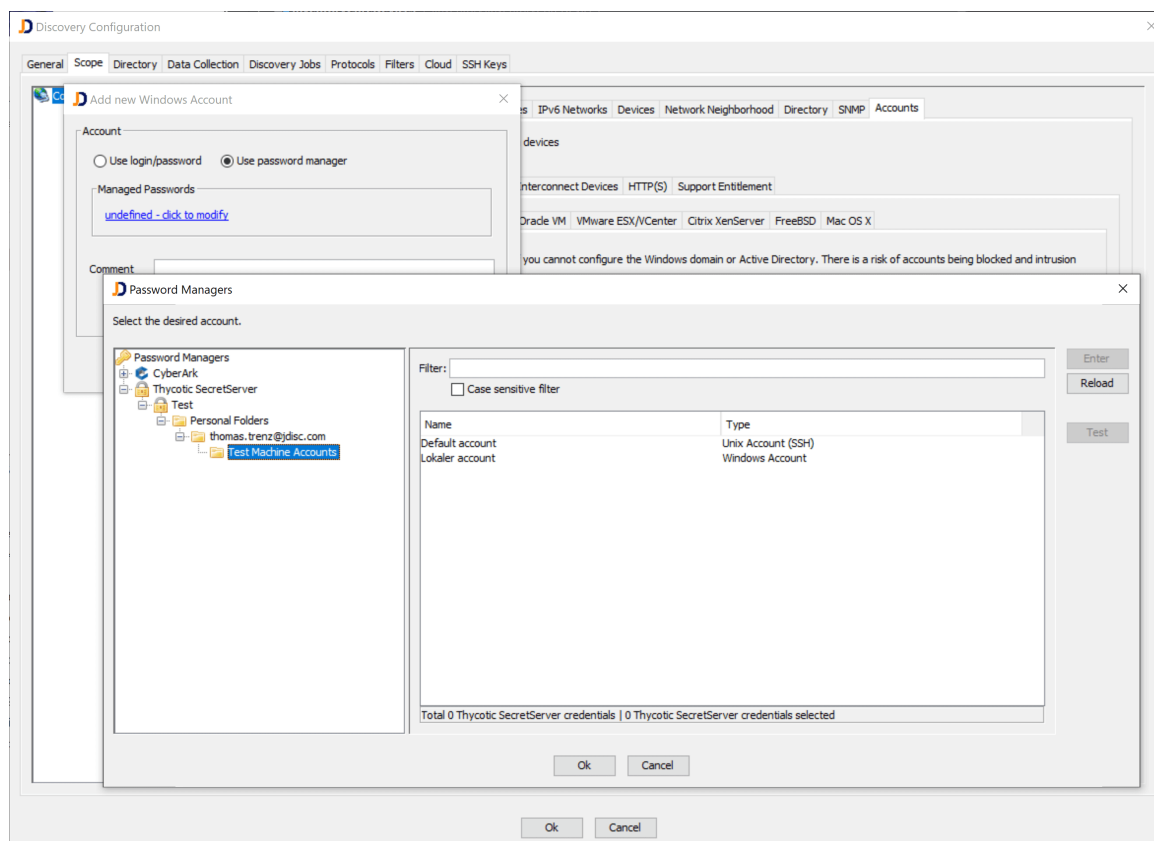


Figure: Choose Credentials

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.

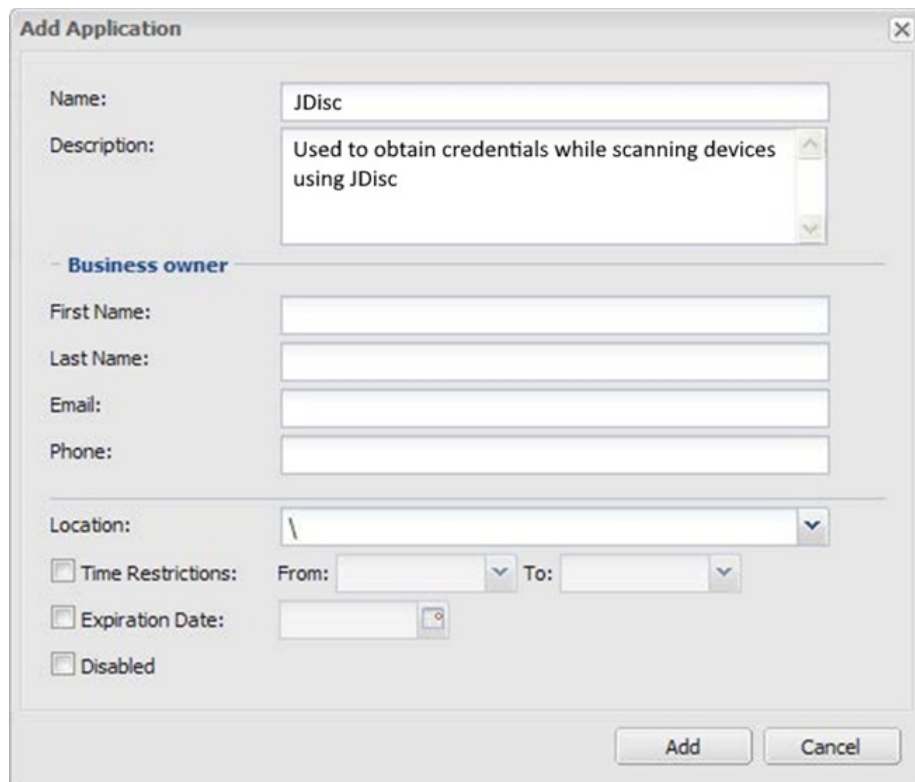
Step 1: Define an Application ID

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.



Add Application

Name: JDisc

Description: Used to obtain credentials while scanning devices using JDisc

Business owner

First Name:

Last Name:

Email:

Phone:

Location: \

☐ Time Restrictions: From: To:

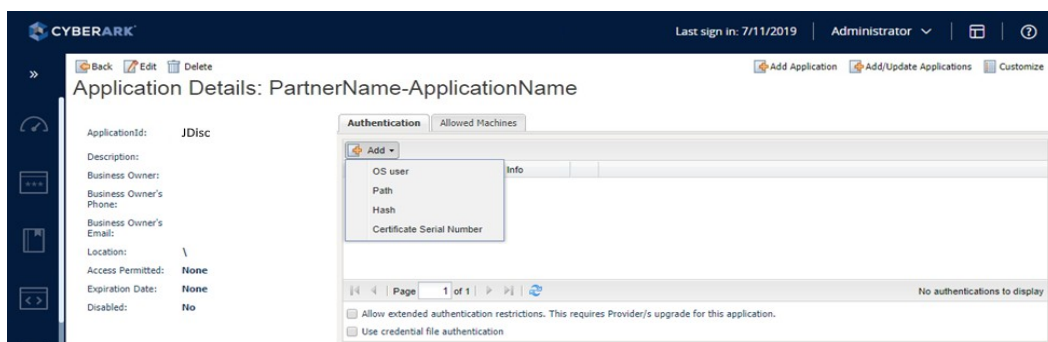
☐ Expiration Date:

☐ Disabled

Add Cancel

Figure: Adding an Application

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



CYBERARK Last sign in: 7/11/2019 Administrator

Application Details: PartnerName-ApplicationName

ApplicationId: JDisc

Description:

Business Owner:

Business Owner's Phone:

Business Owner's Email:

Location: \

Access Permitted: None

Expiration Date: None

Disabled: No

Authentication Allowed Machines

Add

OS user

Path

Hash

Certificate Serial Number

Page 1 of 1

No authentications to display

☐ Allow extended authentication restrictions. This requires Provider's upgrade for this application.

☐ Use credential file authentication

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.

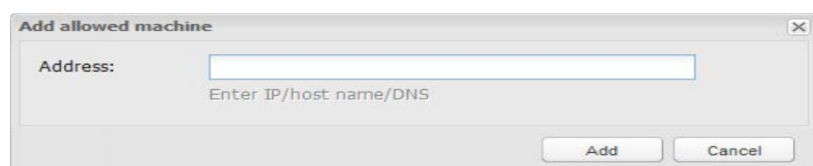


Figure: Enter allowed machine

- 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:

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

Configuring Application Permissions

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.

The screenshot shows a window titled "Add Cyberark Server". It contains several input fields and dropdown menus. The "Name" field is filled with "JDisc CyberArk Test Server". The "Cyberark Server Address" field is filled with "cyberark.jdisc.com". The "Cyberark Server Port" field is filled with "443". The "Cyberark App ID" field is filled with "JDisc". The "Client Certificate" field has a link that says "click to import certificate file". Below these fields, there is a note: "JDisc Discovery utilizes the following credentials to browse safes and passwords in order to select existing passwords in JDisc Discovery's credentials dialog." Below the note, there are two dropdown menus: "Authentication type" set to "CyberArk" and "Credential type" set to "Username/Password". Below these are two more input fields: "CyberArk API user" filled with "admin" and "CyberArk API password" filled with masked characters (dots). At the bottom right, there are "Ok" and "Cancel" buttons.

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 specify 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.

Add new Windows Account

Account

☒ Use login/password ☐ Use password manager

User name/Password

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

☐ Use login/password ☒ Use password manager

Managed Passwords

[undefined - click to modify](#)

Comment

Ok Cancel

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.

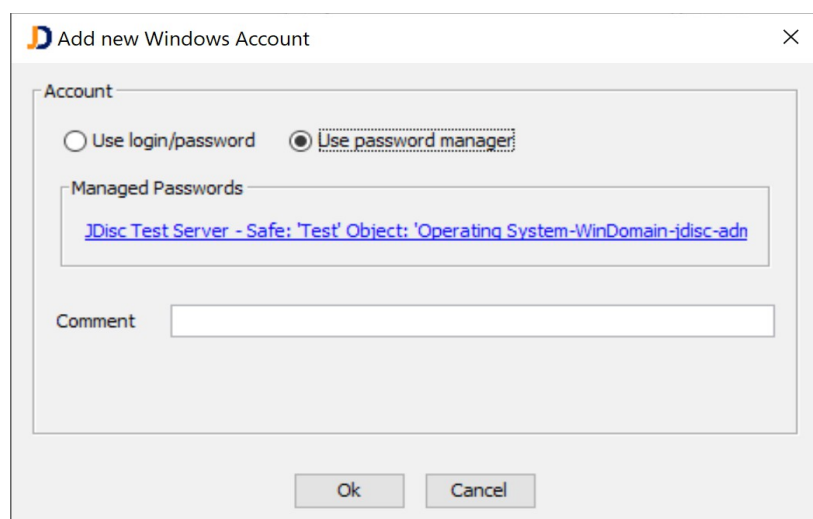


Figure: The selected Credentials

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:

<https://www.microsoft.com/en-us/download/details.aspx?id=46899>

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.

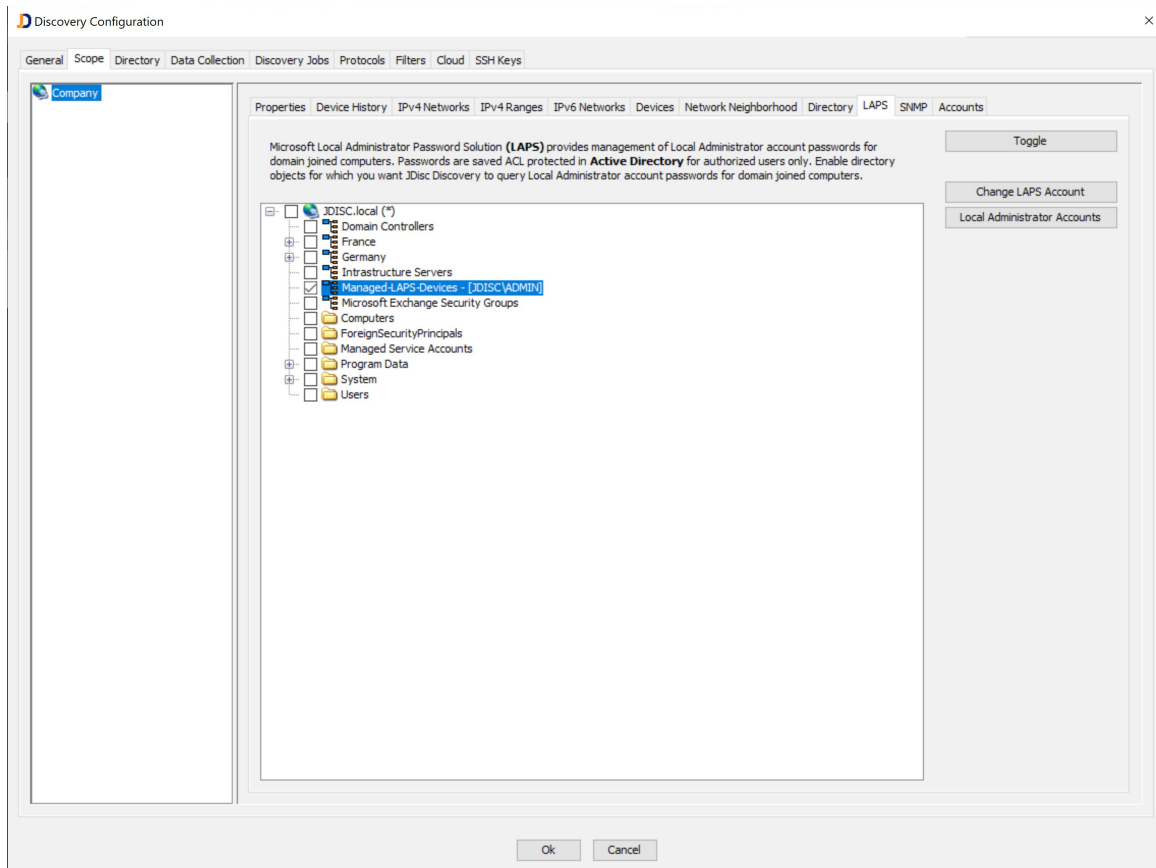


Figure: Enter a LAPS Account

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.

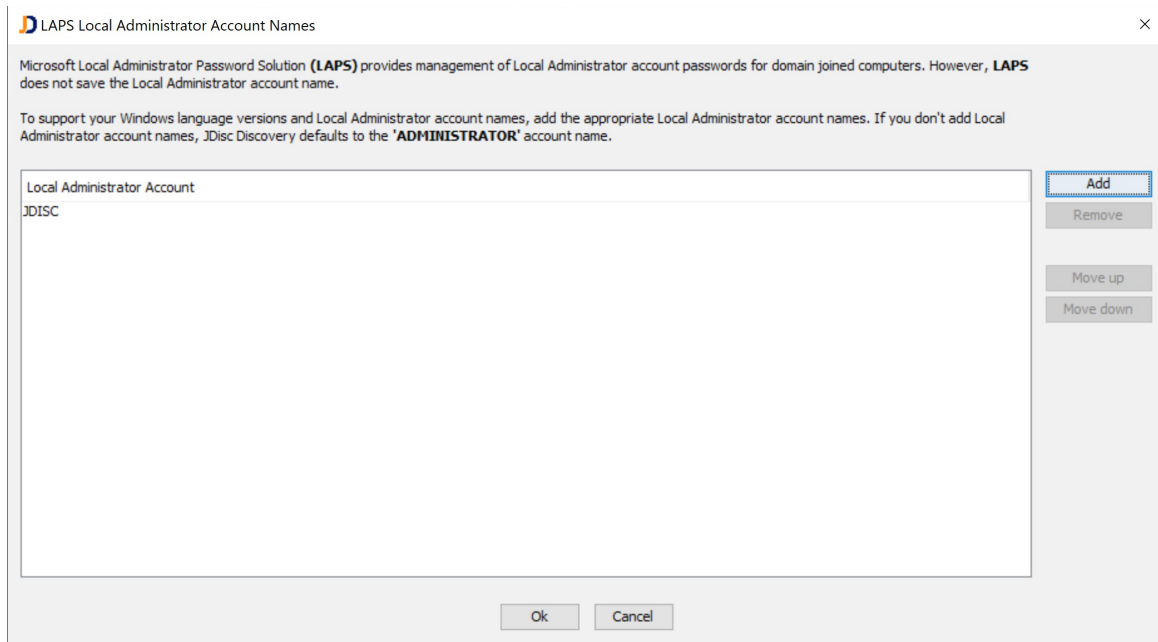


Figure: Manage LAPS local Administrator account names

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.

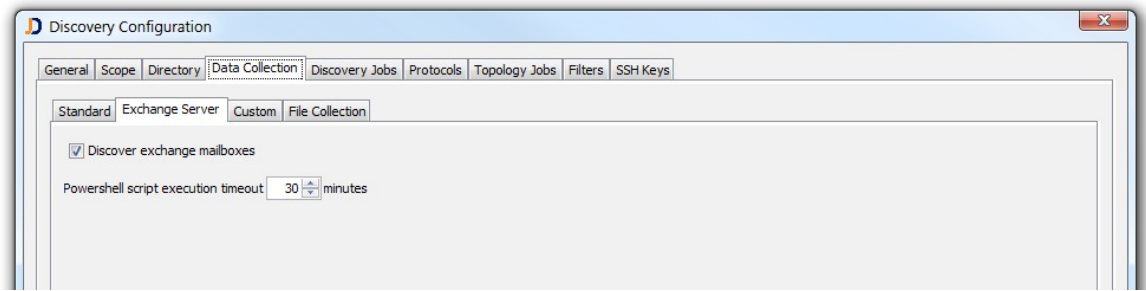


Figure: Exchange Server Discovery Configuration

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

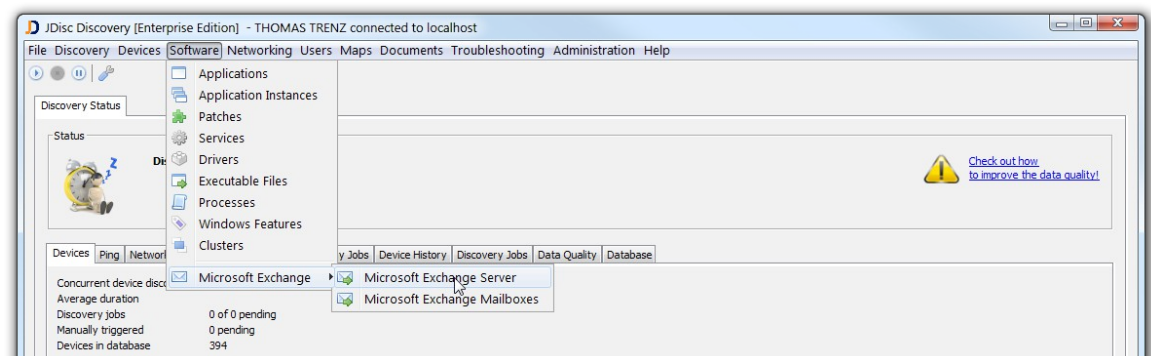


Figure: Exchange Server Menu Item

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.

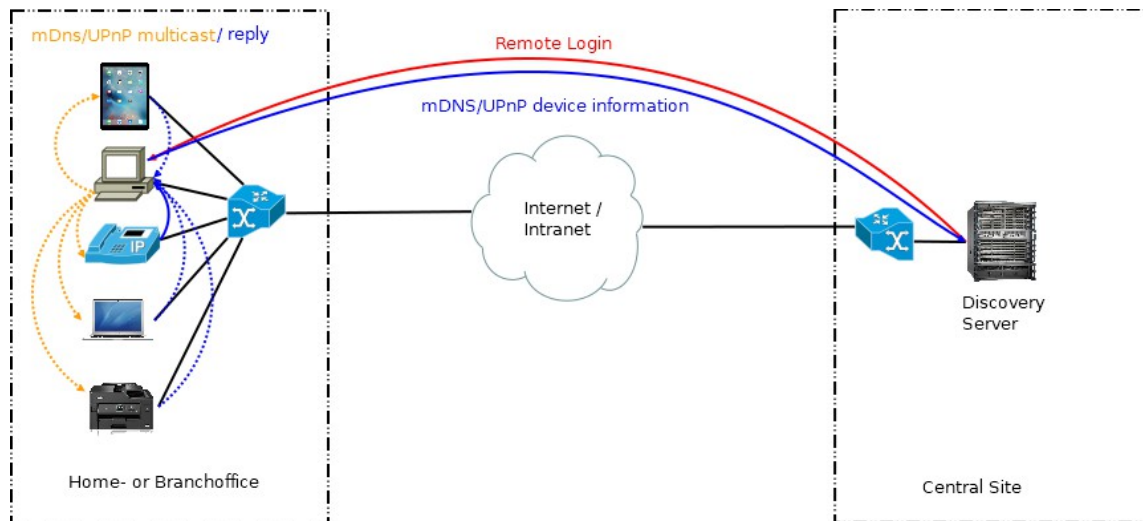


Figure: Multicast mDNS/UPnP Discovery Process

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 Centro 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

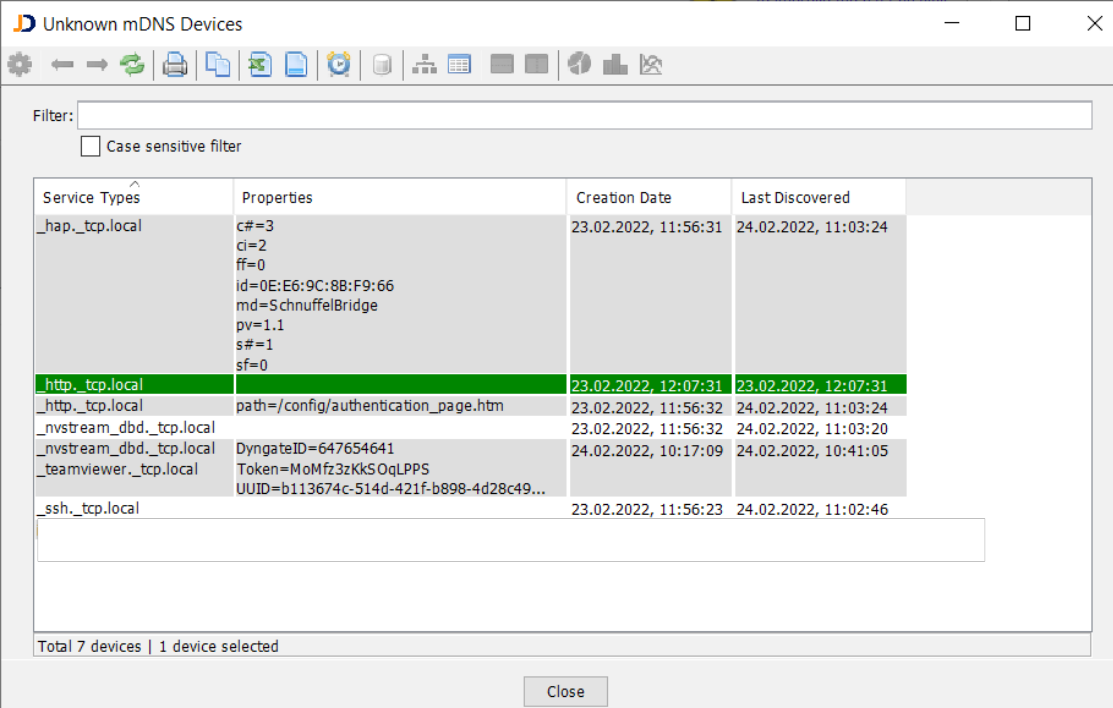
The mDNS and UPnP protocols are largely based on text information that is processed by the discovery using rules. These rules associate the textual information to device types, models, and manufacturers. Because of that, text information from devices that are not yet known (for which no rules exist)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



Unknown mDNS Devices

Filter:

☐ Case sensitive filter

Service Types	Properties	Creation Date	Last Discovered
_hap._tcp.local	c#=3 ci=2 ff=0 id=0E:E6:9C:8B:F9:66 md=SchnuffelBridge pv=1.1 s#=1 sf=0	23.02.2022, 11:56:31	24.02.2022, 11:03:24
_http._tcp.local	path=/config/authentication_page.htm	23.02.2022, 12:07:31	23.02.2022, 12:07:31
_http._tcp.local		23.02.2022, 11:56:32	24.02.2022, 11:03:24
_nvstream_dbd._tcp.local		23.02.2022, 11:56:32	24.02.2022, 11:03:20
_nvstream_dbd._tcp.local	DyngateID=647654641	24.02.2022, 10:17:09	24.02.2022, 10:41:05
_teamviewer._tcp.local	Token=MoMfz3zKkSOqLPPS UUID=b113674c-514d-421f-b898-4d28c49...		
_ssh._tcp.local		23.02.2022, 11:56:23	24.02.2022, 11:02:46

Total 7 devices | 1 device selected

Close

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.

Unknown UPnP Devices						
Filter:						
<input type="checkbox"/> Case sensitive filter						
Manufacturer	Model Name	Model Description	Model Number	Service Types	Locations	Created
AVM Berlin	FRITZ!WLAN Repeater 1750E	FRITZ!WLAN Repeater 1750E	avm	upnp:rootdevice urn:schemas-any-com:service:fritzbox:1 urn:schemas-upnp-org:device:fritzbox:1	49000/fboxdesc.xml	25 Feb 2015
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.

Devices with Discovery Status 'Success'										
Filter:										
<input type="checkbox"/> Case sensitive filter										
Name	IP Address	Manufacturer	Type	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 selected										
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 company-owned 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.

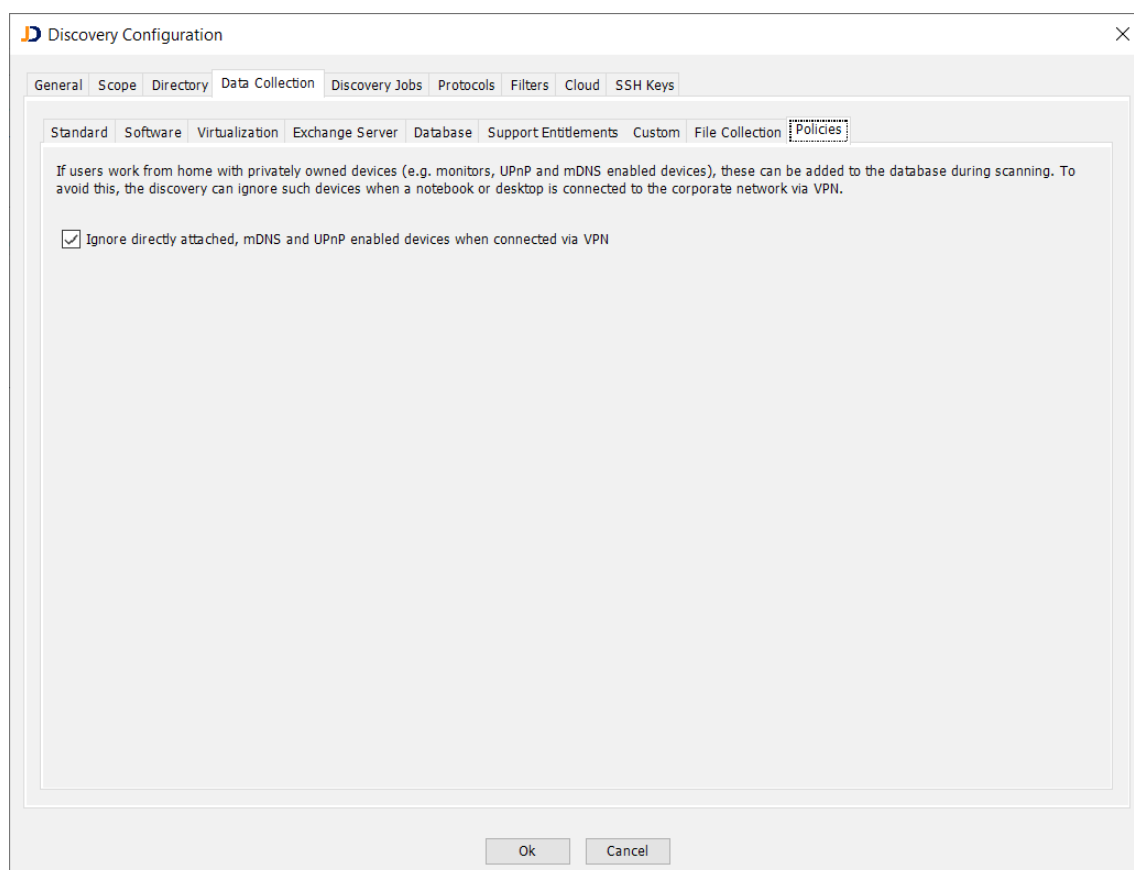


Figure: Discovery Configuration Data Collection Policies

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.

The screenshot shows the 'Discovery Configuration' window with the 'General' tab selected. The window has a title bar with a close button and a tab bar with options: General, Scope, Directory, Data Collection, Discovery Jobs, Protocols, Topology Jobs, Filters, Cloud, and SSH Keys. The 'General' tab contains several sections:

- General:** A text box explains that JDisc Discovery discovers devices in parallel. Below it are three spinners: 'Discover not more than 10 devices in parallel', 'Ping networks and IP ranges with 4 threads in parallel', and 'Abort device discovery when inactive for more than 60 minutes'.
- Find New Devices:** Three checkboxes: 'Discover DNS domain controllers', 'Discover DNS servers', and 'Discover devices found in ARP caches of routers and switches'.
- Device Naming:** A dropdown menu labeled 'Set device name' with the value 'Normal (no changes)'.
- Aging Out:** Three checkboxes: 'Age out devices after 40 day(s)', 'Age out JDisc Discovery application events after 60 day(s)' (checked), and 'Track device deletion' (checked). Below the last checkbox is a spinner for 'Delete device deletion audit log entries after 180 day(s)'.
- Jumphost for improved Device and Manufacturer Identification:** A text box explains that JDisc Discovery runs the ARP command on servers and clients in remote networks. Below it is an unchecked checkbox 'Enable remote ARP Jumphost' and a spinner for 'Max. Jumphost worker threads for each remote network' set to 5.

At the bottom of the window are 'Ok' and 'Cancel' buttons.

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.

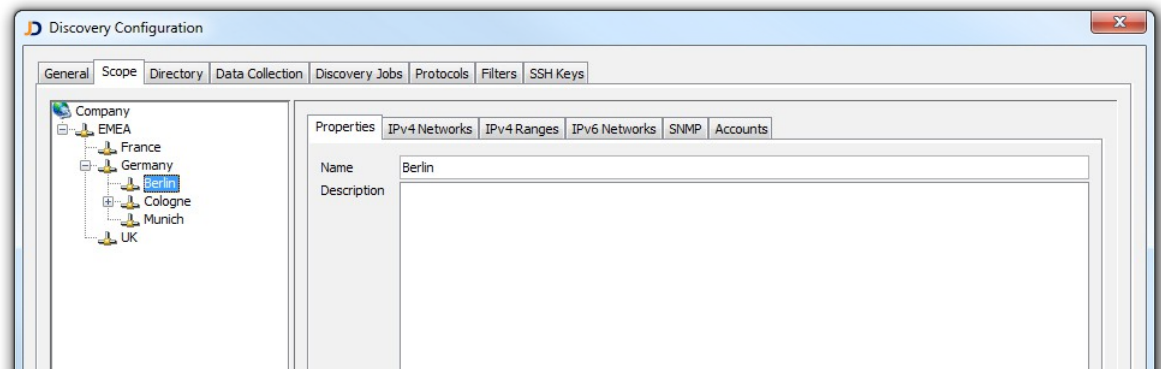


Figure: Properties Tab

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.

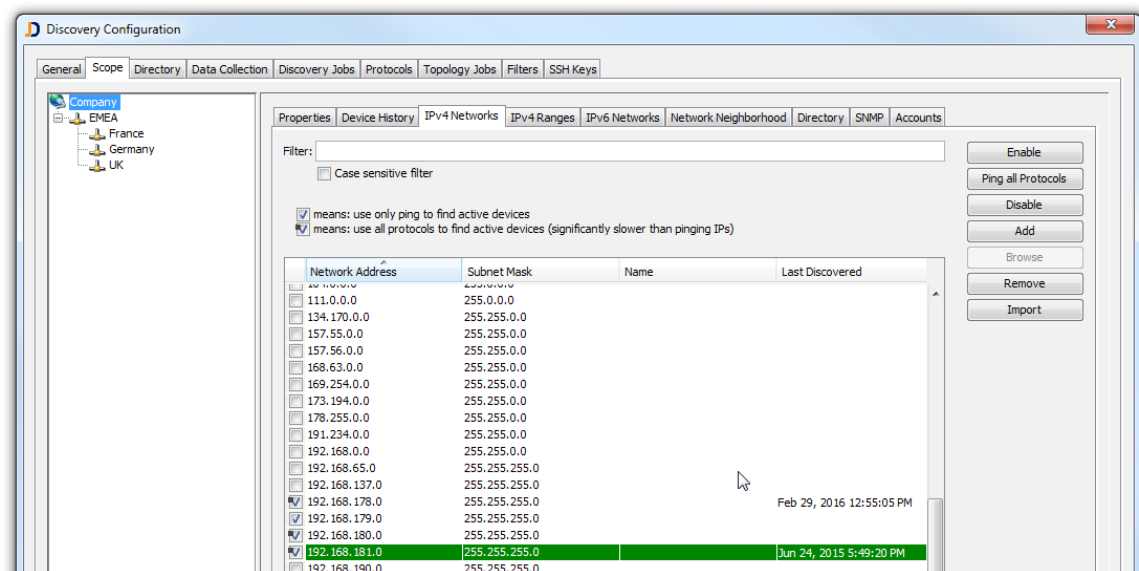


Figure: IPv4 Networks Tab

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.

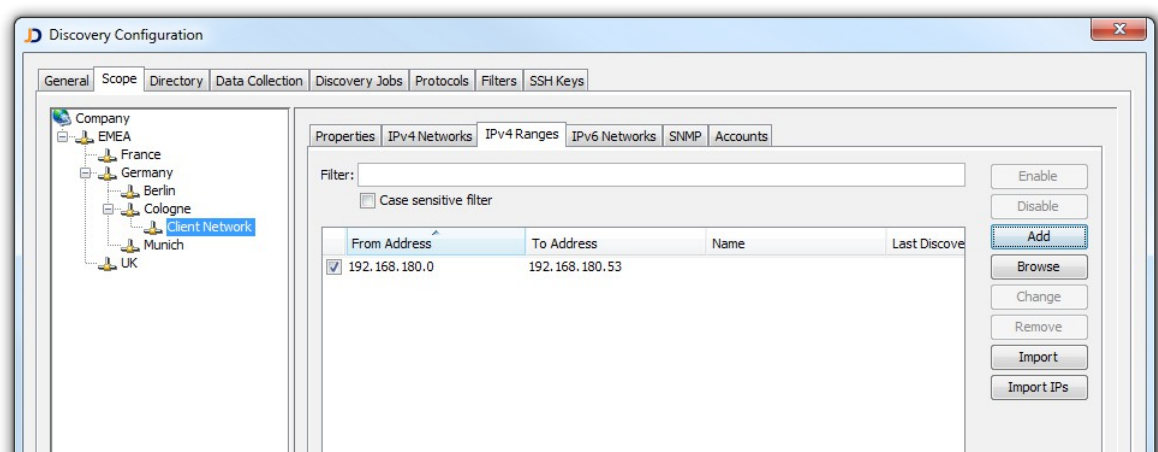


Figure: IPv4 Address Ranges

Enter a name in the IP range table's name column.

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.

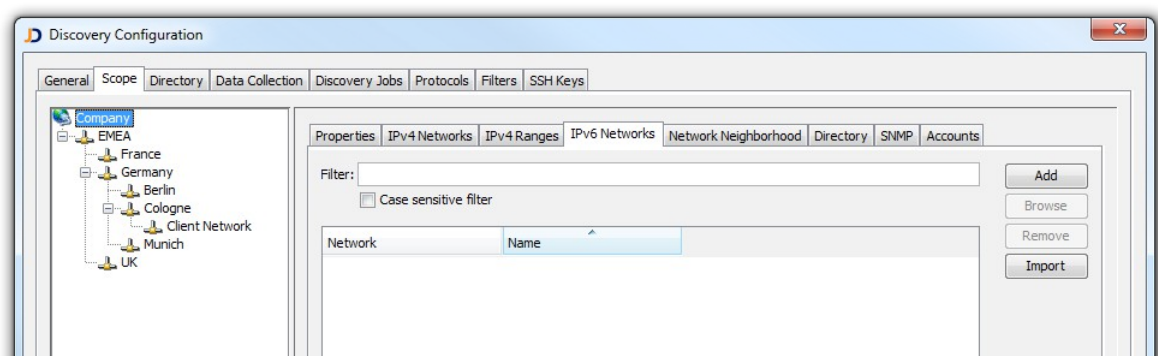


Figure: IPv6 Networks Tab

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.

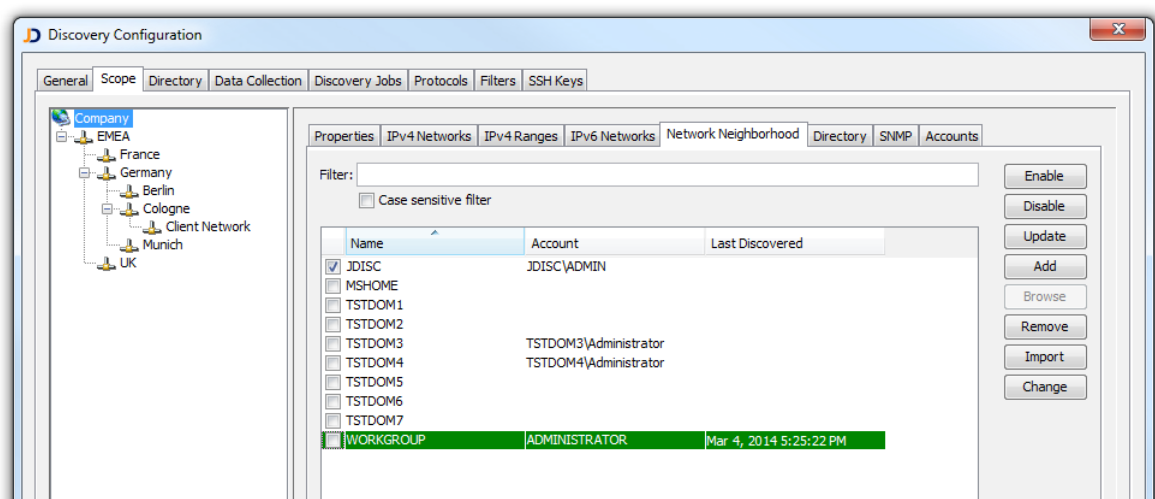


Figure: Network Neighborhood Tab

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 following 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.

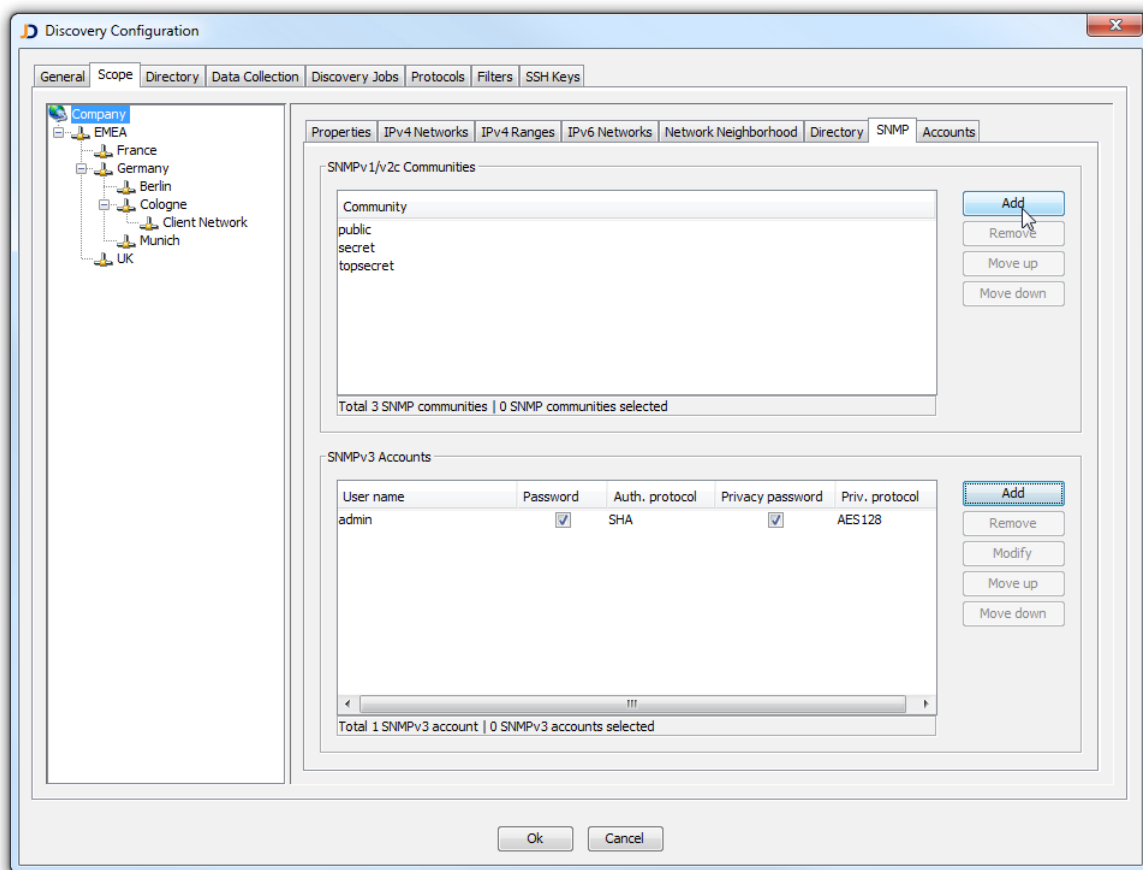


Figure: Default SNMPv1/v2c Communities and SNMPv3 Accounts

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.

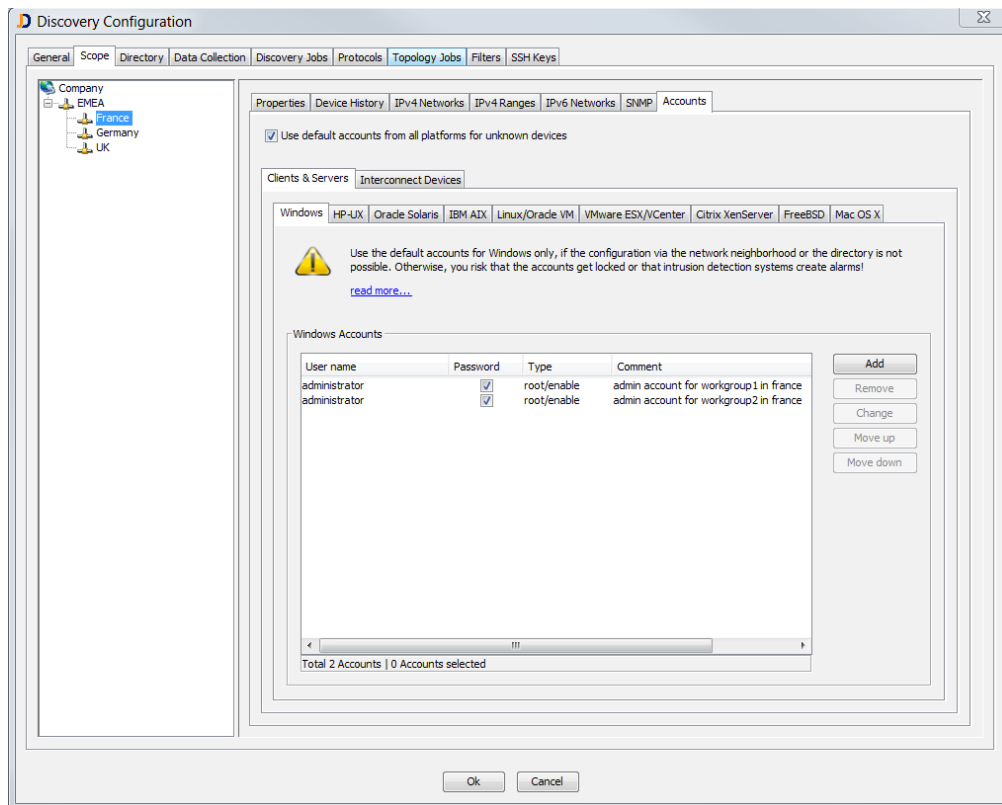


Figure: Default Accounts

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.

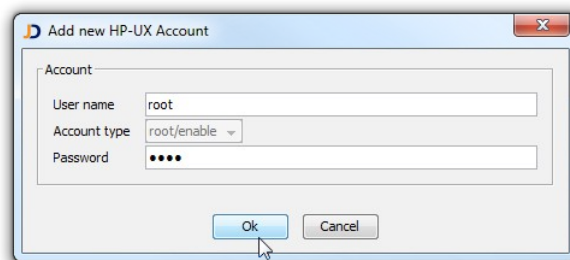


Figure: Add new Default Account

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.

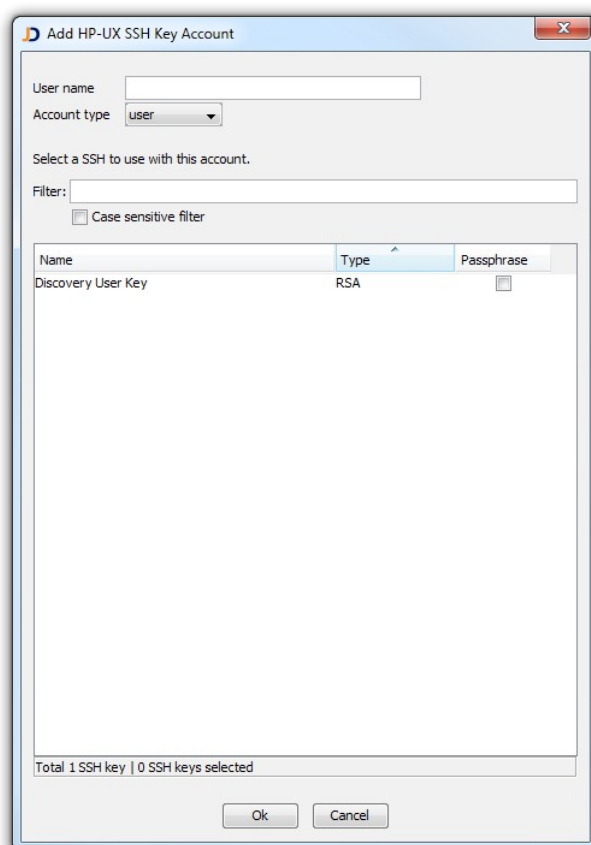


Figure: Add new public/private Key Account

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 subgroup 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.

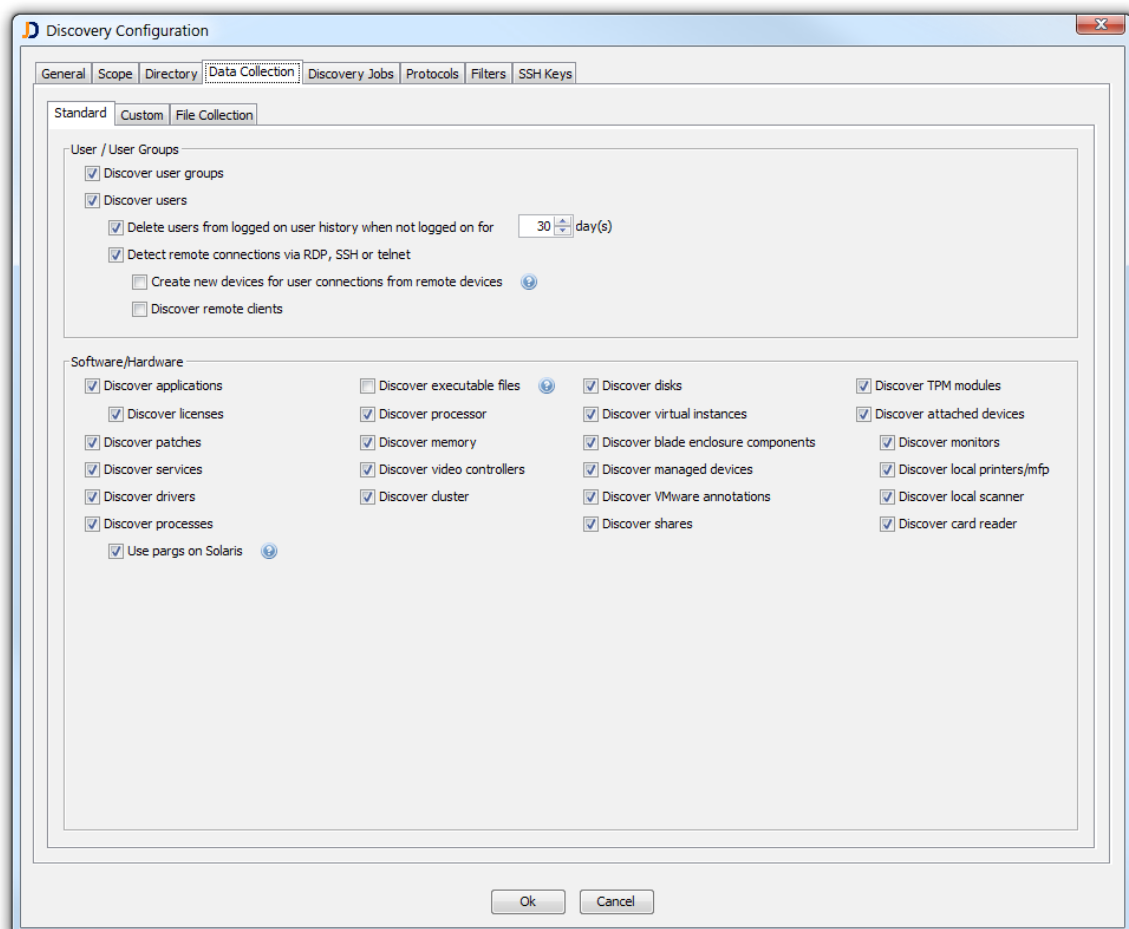
- If the *DNS Domain Controller* panel contains at least one host name, click *Change* to open the *Directory Service Account* dialog and enter login credentials for the directory's DNS Domain Controllers.
- Finally click *Test* to test the connection to all configured DNS Domain Controllers for the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



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
- Services⁷
- Drivers
- Processors
- Memory modules
- Video controller⁸

⁷ For Windows and Solaris

⁸ 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 computer⁹)
- 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.

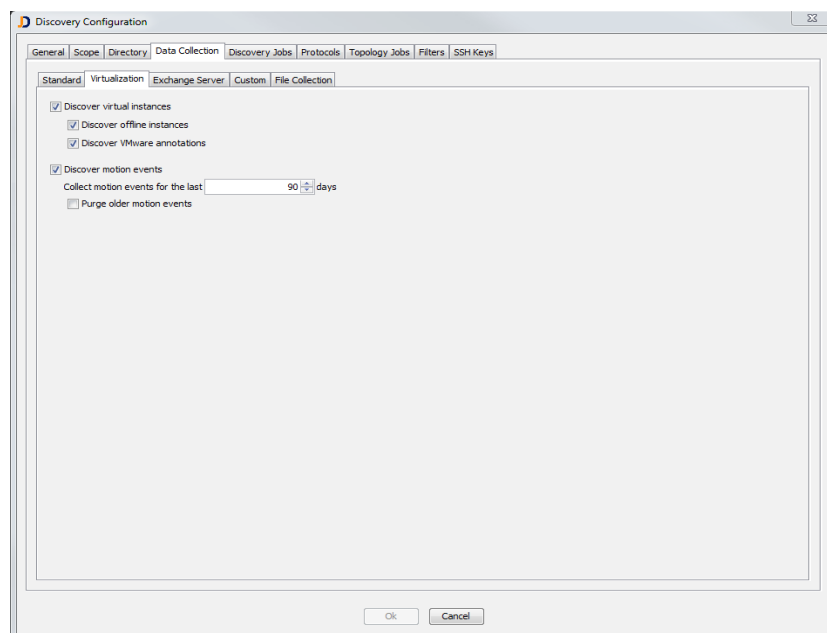


Figure: Virtualization Data Collection

⁹ 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.

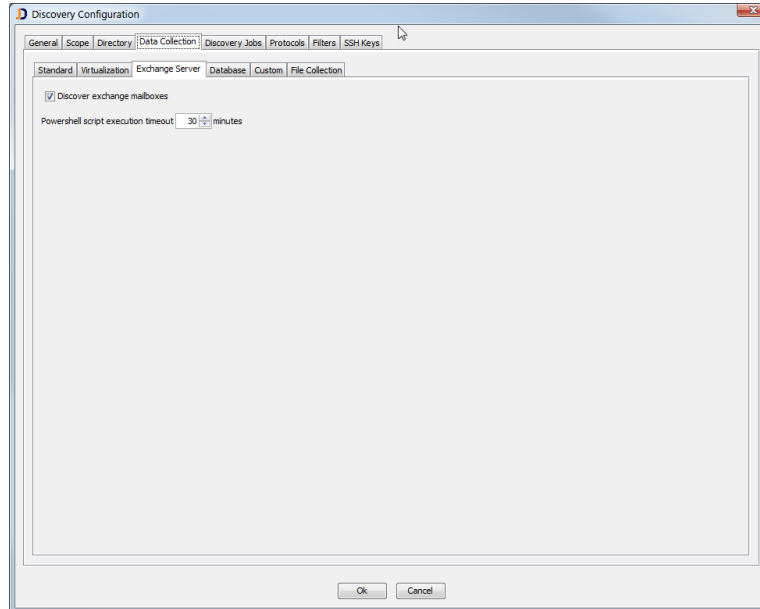


Figure: Exchange Server Discovery Configuration

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.

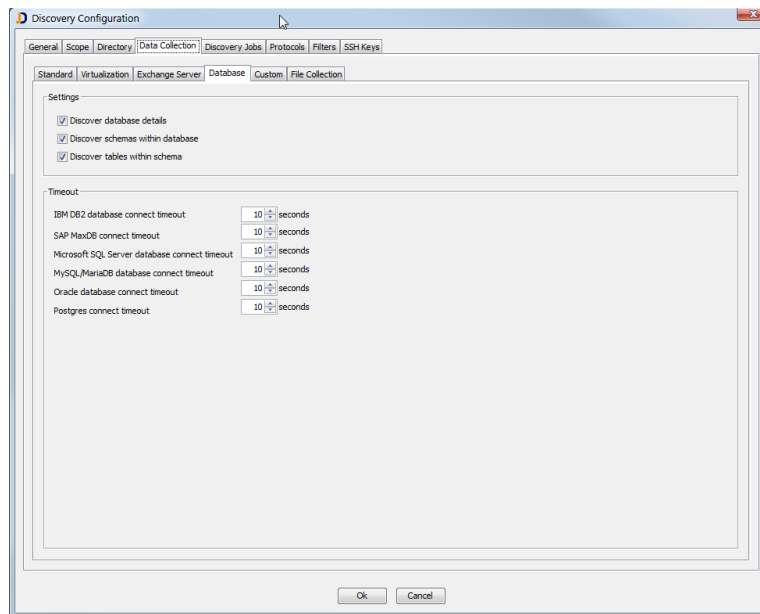


Figure: Database Discovery Settings

5.4.5 Custom Data Collection

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

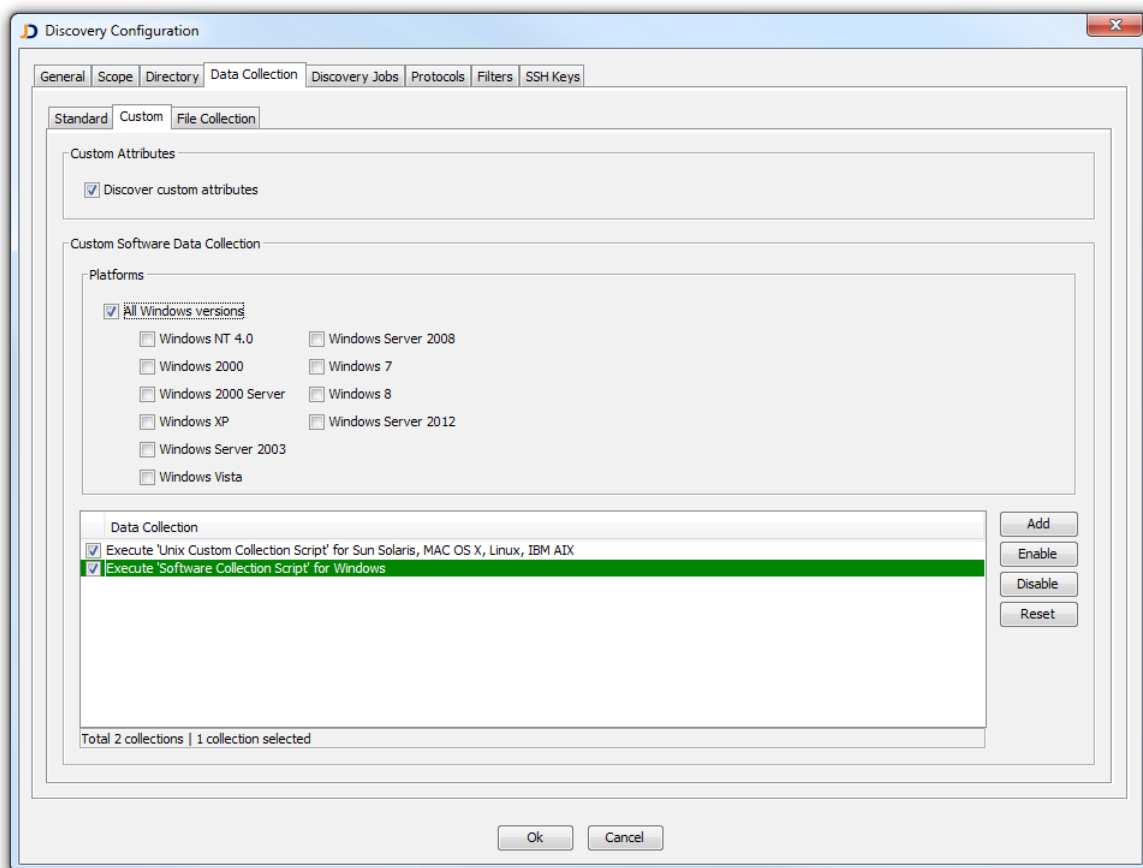


Figure: Custom Data Collection Configuration

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.

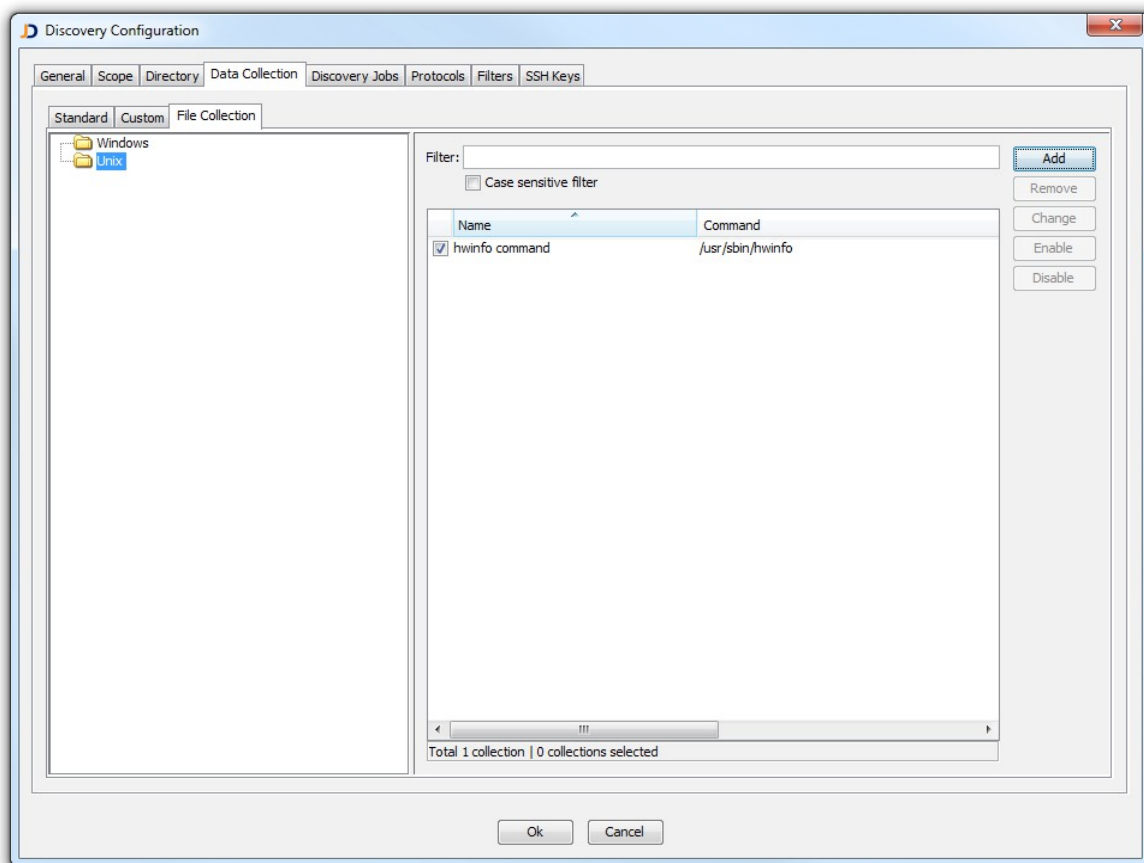


Figure: File Collections

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.

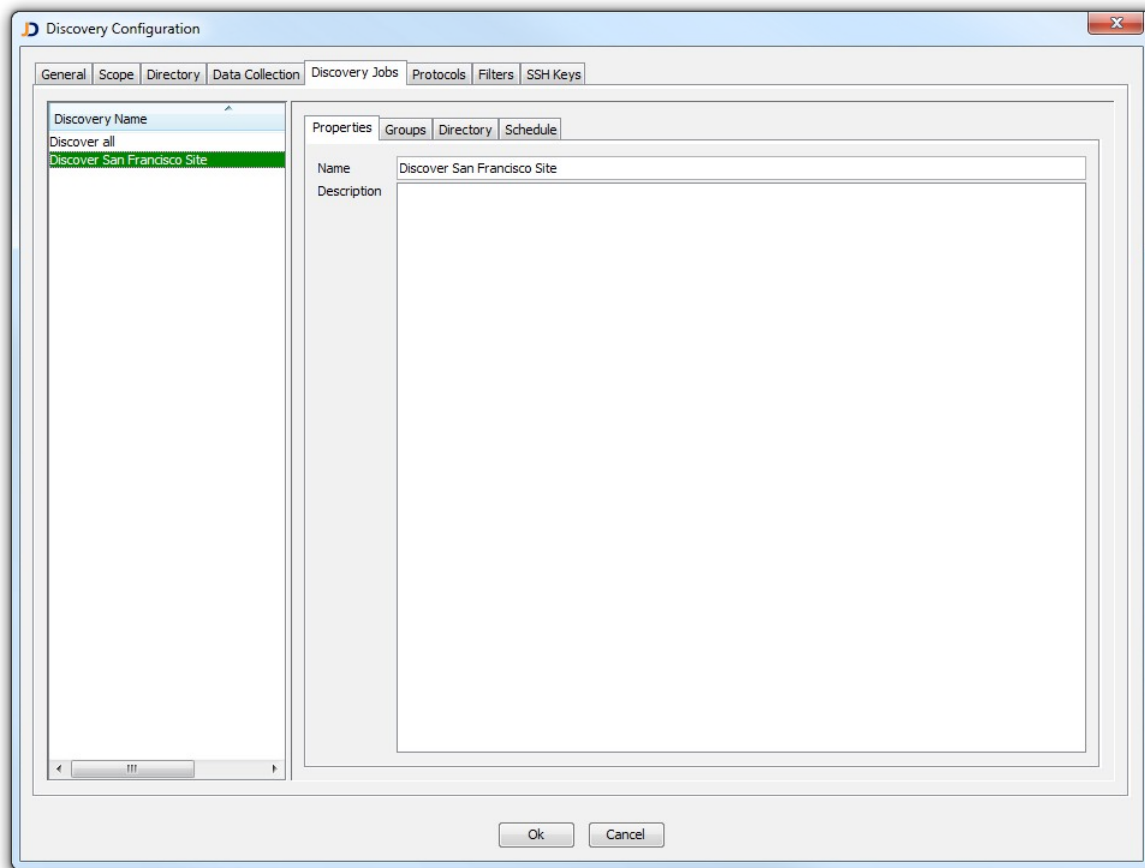


Figure: Discovery Jobs Tab

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.

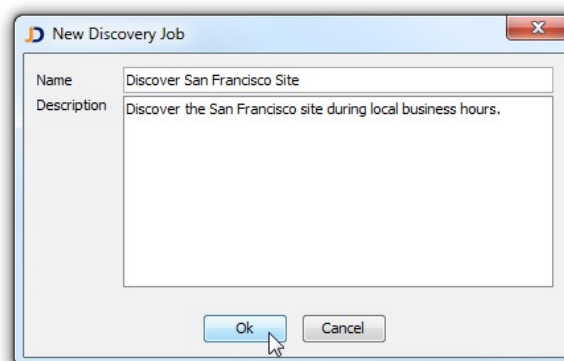


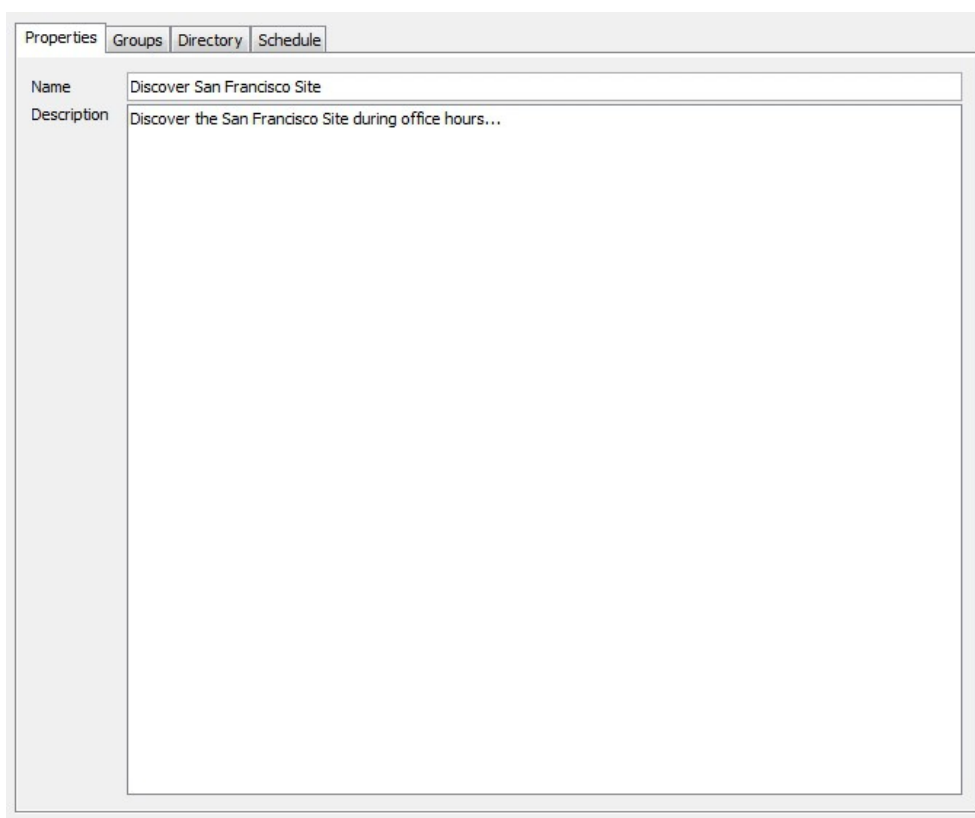
Figure: Create new Discovery Job

Change a discovery job's settings in any of these 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.



The screenshot shows a window with four tabs: Properties, Groups, Directory, and Schedule. The Properties tab is active. It contains two text input fields. The first field is labeled 'Name' and contains the text 'Discover San Francisco Site'. The second field is labeled 'Description' and contains the text 'Discover the San Francisco Site during office hours...'. The rest of the window is empty.

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.

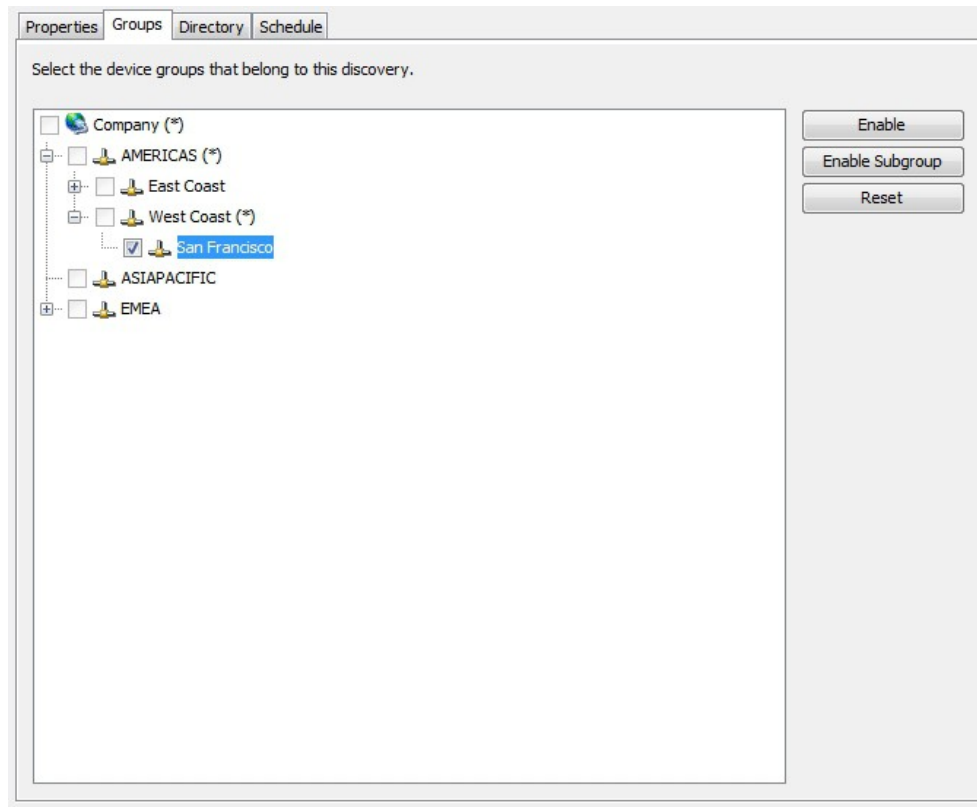


Figure: The Groups Tab

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.

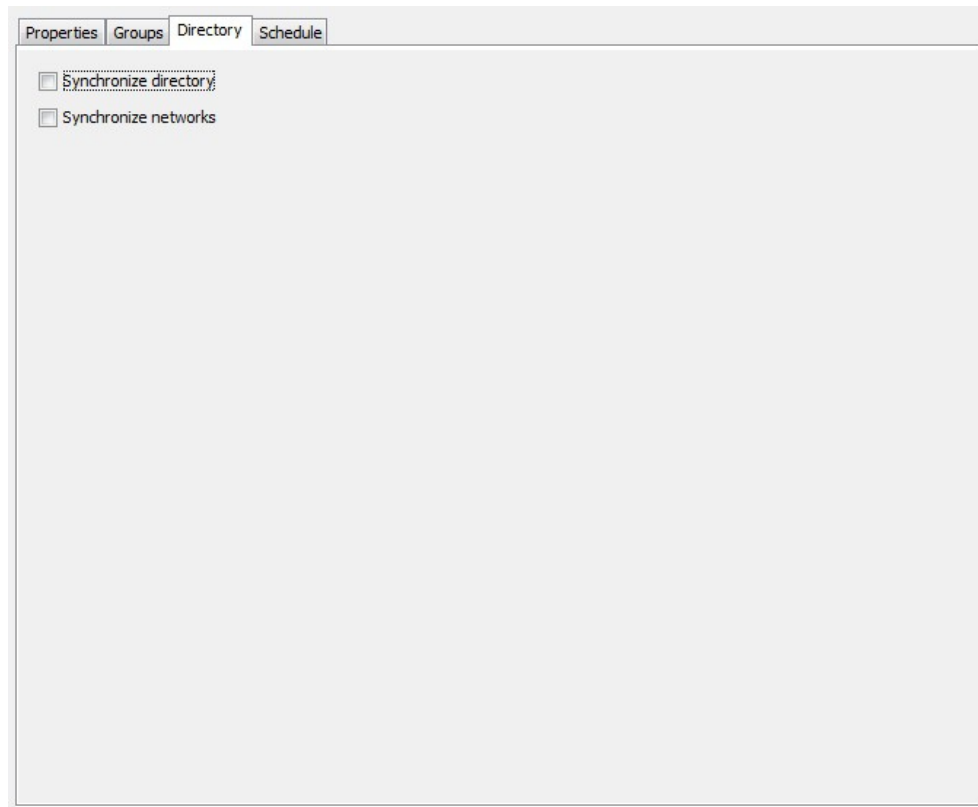


Figure: Directory Synchronization Options

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.

The screenshot shows a software window with four tabs: 'Properties', 'Groups', 'Directory', and 'Schedule'. The 'Schedule' tab is active. It contains a 'Schedule type' dropdown menu set to 'Run once'. Below this, there are two input fields: 'Date' set to '3/5/10' and 'Time' set to '7:00 PM'. Both fields have small calendar and clock icons respectively for date and time selection.

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.

The screenshot shows the same software window with the 'Schedule' tab active. The 'Schedule type' dropdown menu is now set to 'Daily'. Below it, there is a single input field labeled 'Run every day at' set to '12:00 PM', with a small clock icon for time selection.

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.

The screenshot shows the same software window with the 'Schedule' tab active. The 'Schedule type' dropdown menu is now set to 'Weekly'. Below it, there are two input fields: 'Run every' set to 'Sunday' and 'At' set to '6:57 PM'. The 'Run every' field has a dropdown arrow, and the 'At' field has a small clock icon for time selection.

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.

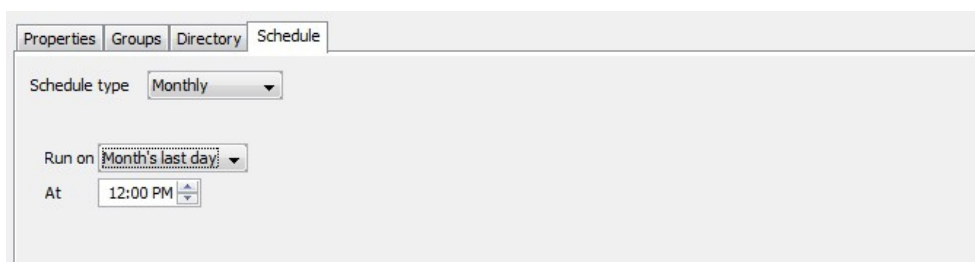
The screenshot shows the 'Schedule' tab of a configuration window. It has four tabs: 'Properties', 'Groups', 'Directory', and 'Schedule'. The 'Schedule' tab is active. Under 'Schedule type', a dropdown menu shows 'Monthly'. Below this, 'Run on' is set to 'Month's last day' and 'At' is set to '12:00 PM'.

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.

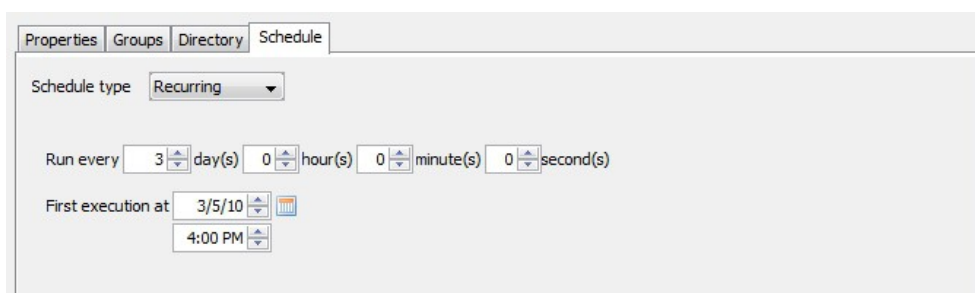
The screenshot shows the 'Schedule' tab of a configuration window. It has four tabs: 'Properties', 'Groups', 'Directory', and 'Schedule'. The 'Schedule' tab is active. Under 'Schedule type', a dropdown menu shows 'Recurring'. Below this, 'Run every' is set to '3 day(s)', '0 hour(s)', '0 minute(s)', and '0 second(s)'. 'First execution at' is set to '3/5/10' and '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.

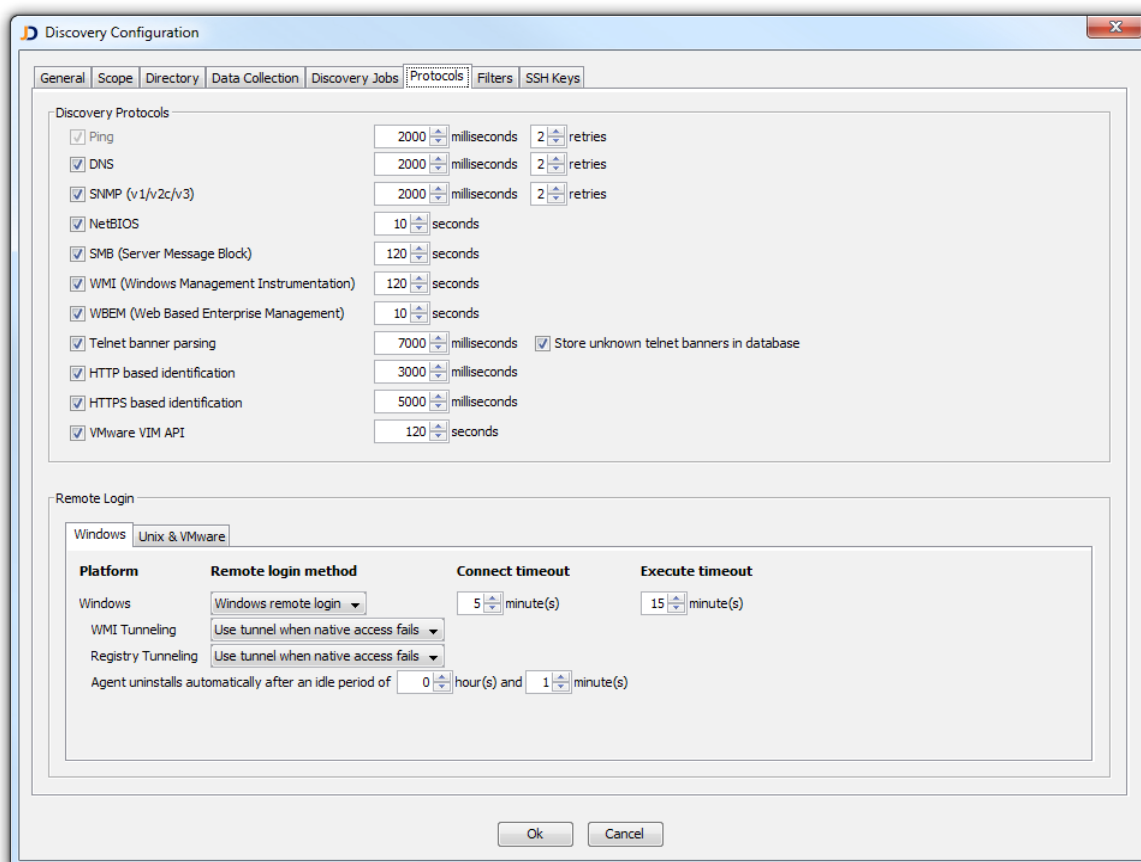


Figure: Protocols Tab

This dialog might vary depending on the licensed edition.

JDisc Discovery's installation program configures default 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 functionality, 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 separately.

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, or 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.

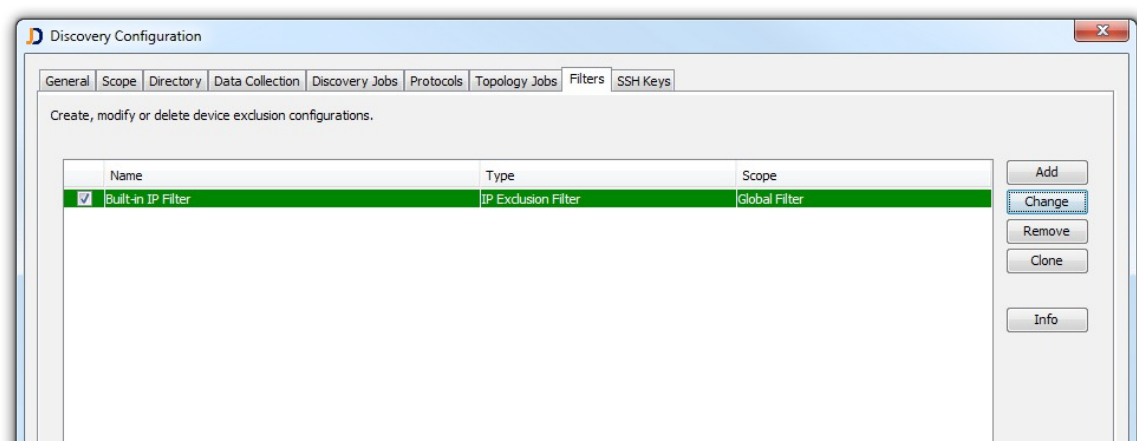


Figure: Filter Tab

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 individually.

5.7.1 IP Exclusion Filter

Create a new IP exclusion filter by clicking the *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.

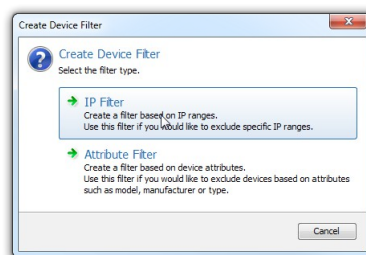


Figure: Choose the Filter Type

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

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.

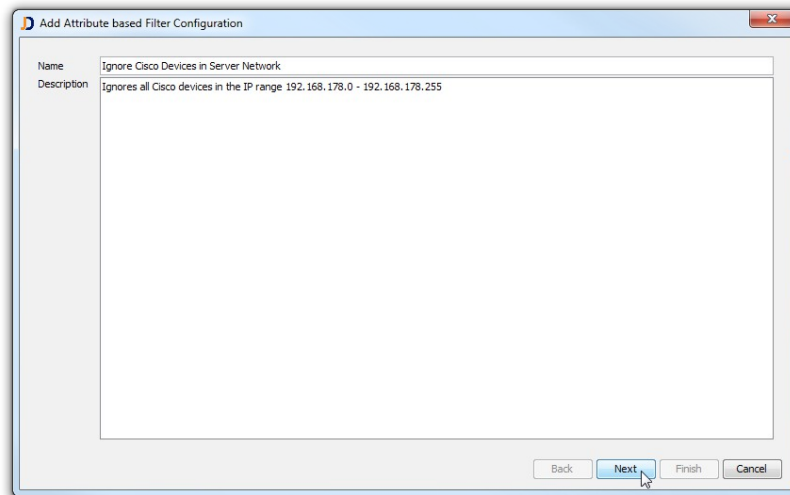


Figure: Define filter name and description

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)

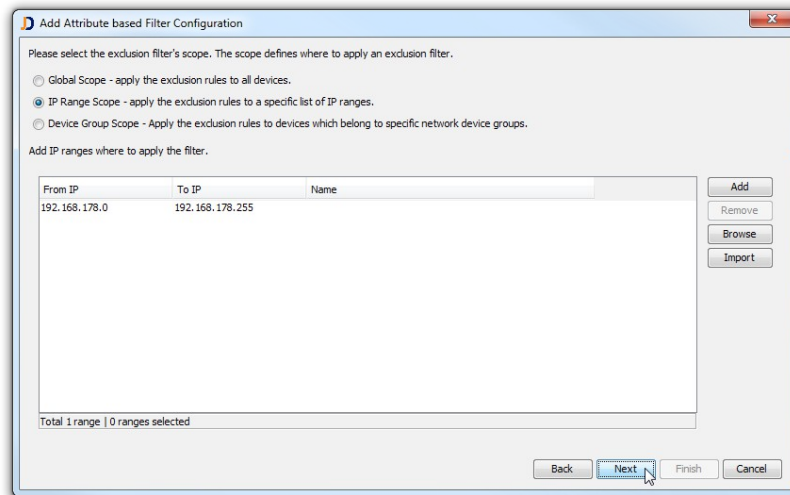


Figure: Define the Filter Scope

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.

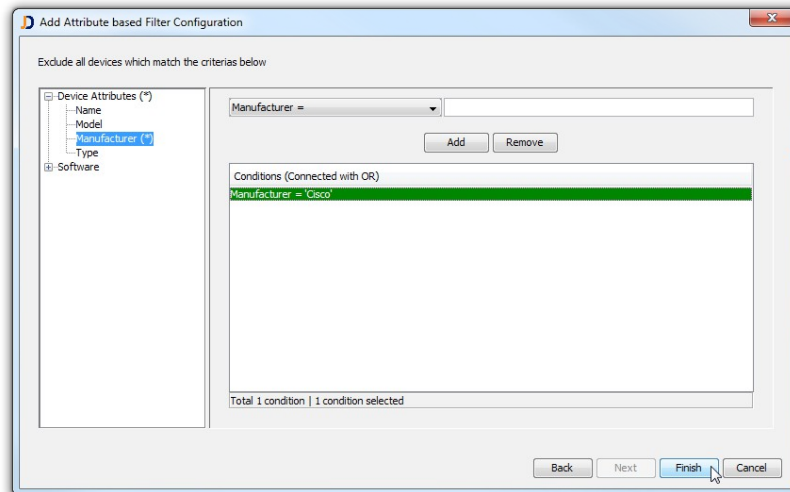


Figure: Define Filter Criteria

Click *Finish* to complete the filter definition.

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.

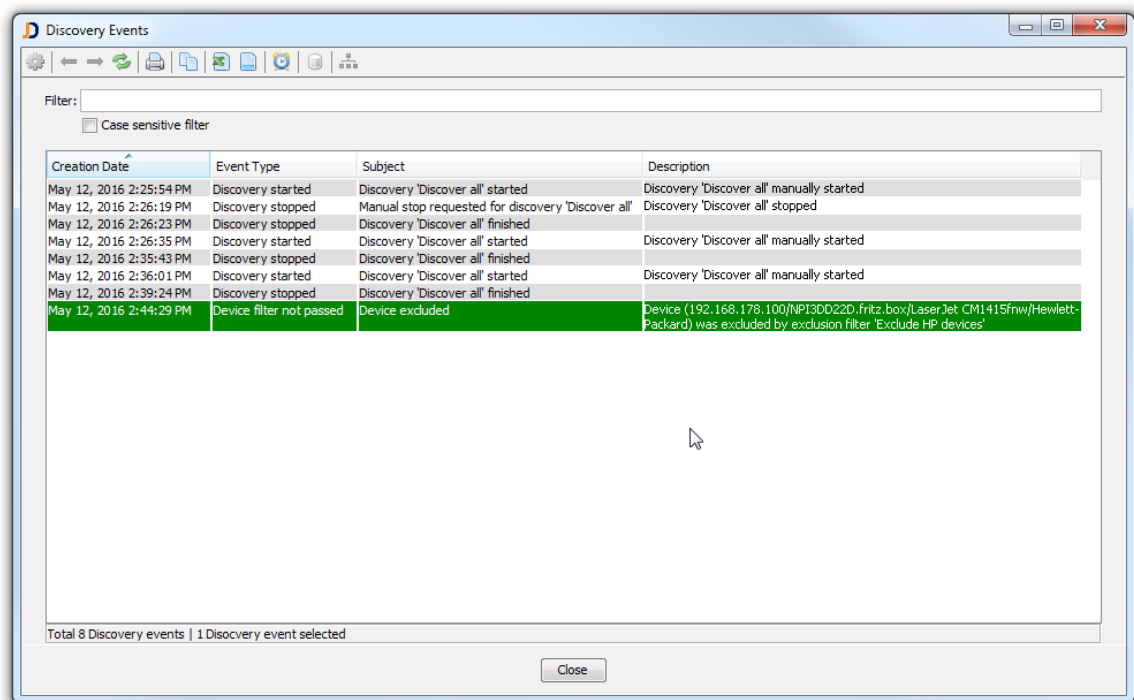


Figure: Attribute Filter Events

5.7.3 Filter Information

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

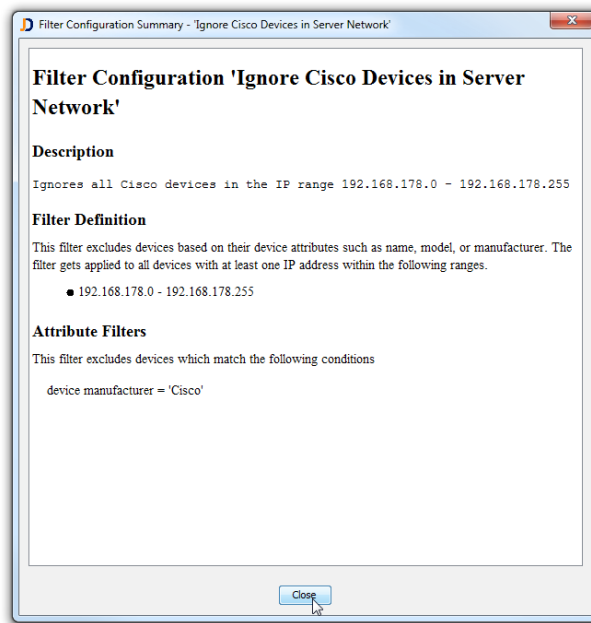


Figure: Filter Configuration Summary

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.

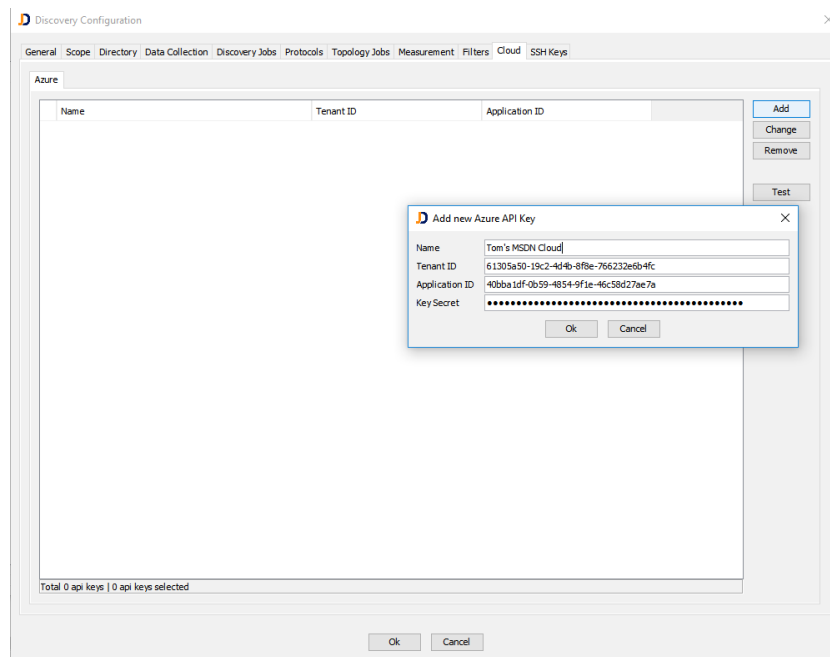


Figure: Add access credentials for an Azure cloud directory

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.

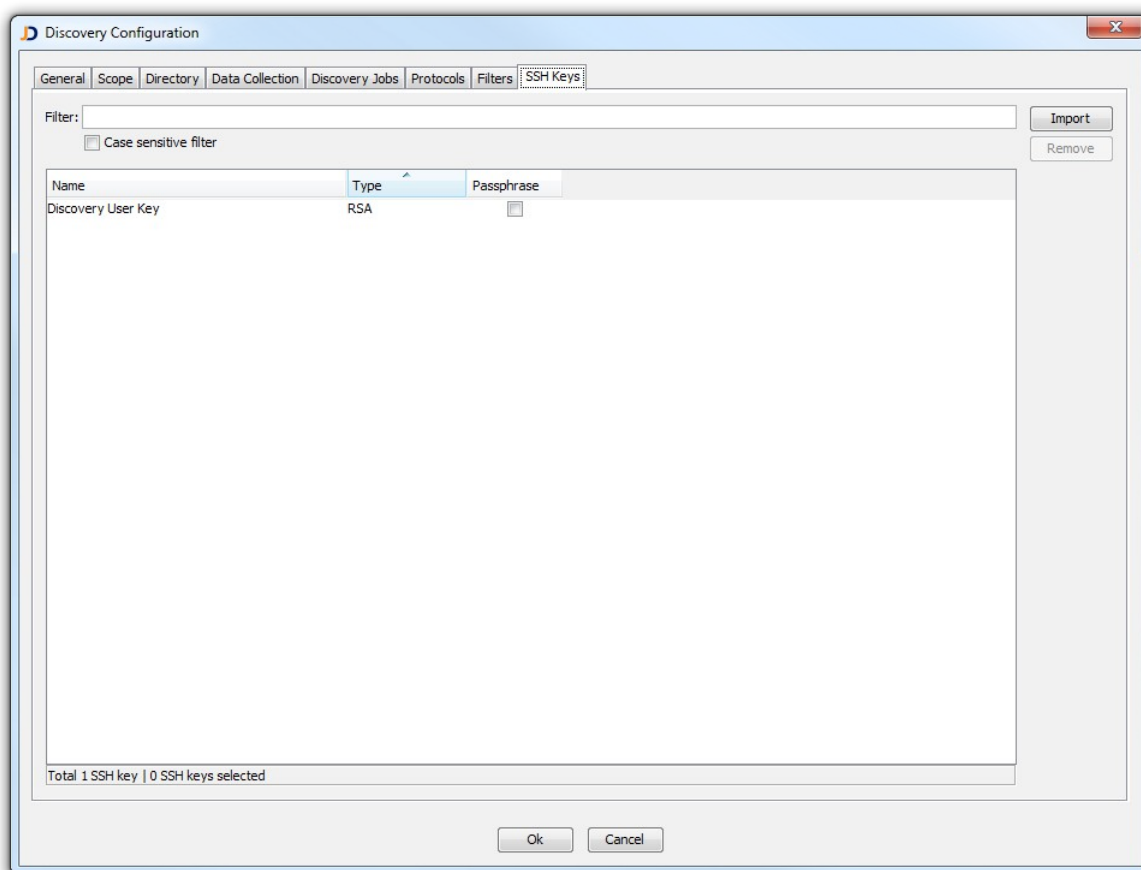


Figure: Private Keys

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!

6 Reporting

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

Name	IP Address	Manufacturer	Model	Type	OS Version
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	S558V20	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 5308xd	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

Figure: A typical JDisc Discovery Device Report

Use the filter field 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
- 📄 Open 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
- 📄 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.

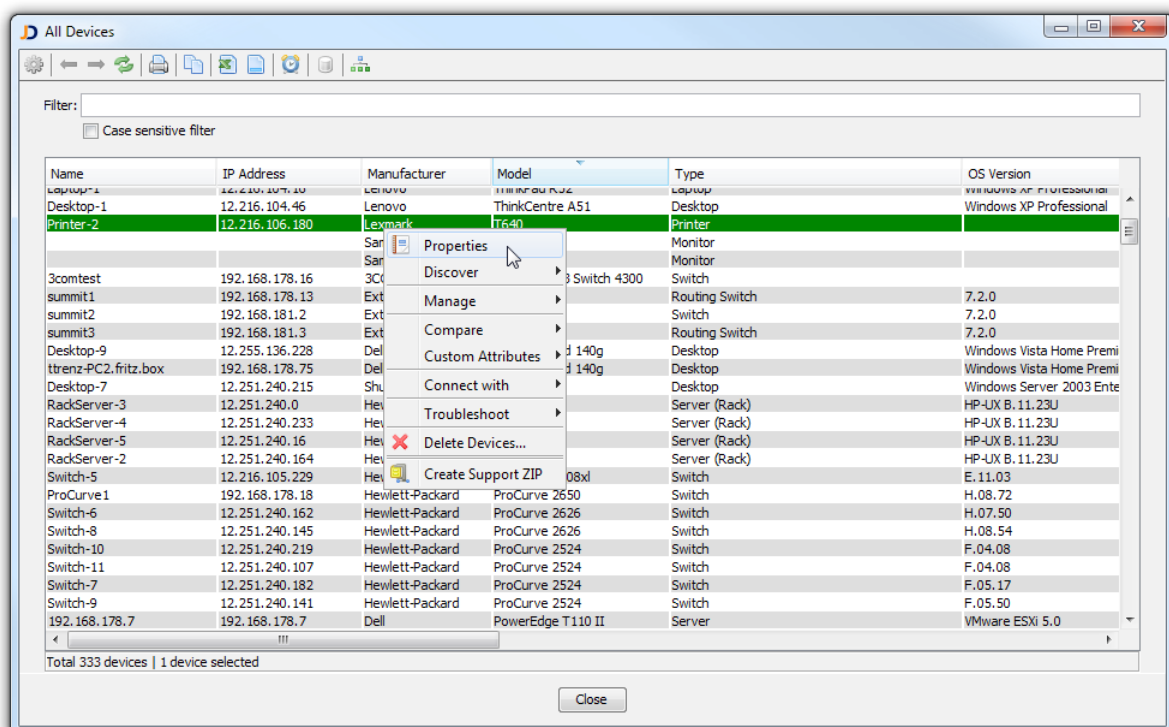


Figure: Report Context Menu

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
- Type
- 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 discovery process uses the Directory Object *Login* to connect to the directory's member computers.
-

- 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 all occurrences of the login's Old password with the New password in the database. Enter the Old password to replace 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.

Delete Logins

Delete Logins
Delete logins from the database.

☒ All
Delete all logins named 'JDISC-INTERNAL\ADMINISTRATOR' from the database.

☐ By Password
Delete logins named 'JDISC-INTERNAL\ADMINISTRATOR' having a specific password.

Cancel

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.

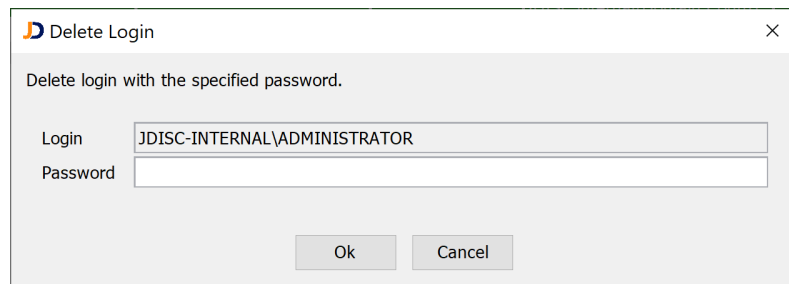


Figure: Delete Login

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	<p>Click <i>Discover » 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.</p> <p>Click <i>Discover » Selected IP Addresses</i> to discover selected devices via their IP addresses. This is not</p>

	recommended for devices and networks using DHCP, because the IP address might have changed.
IPv4 network report	Click <i>Discover » Selected Network(s)</i> to discover selected IPv4 networks.
IPv4 address range report	Click <i>Discover » 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.

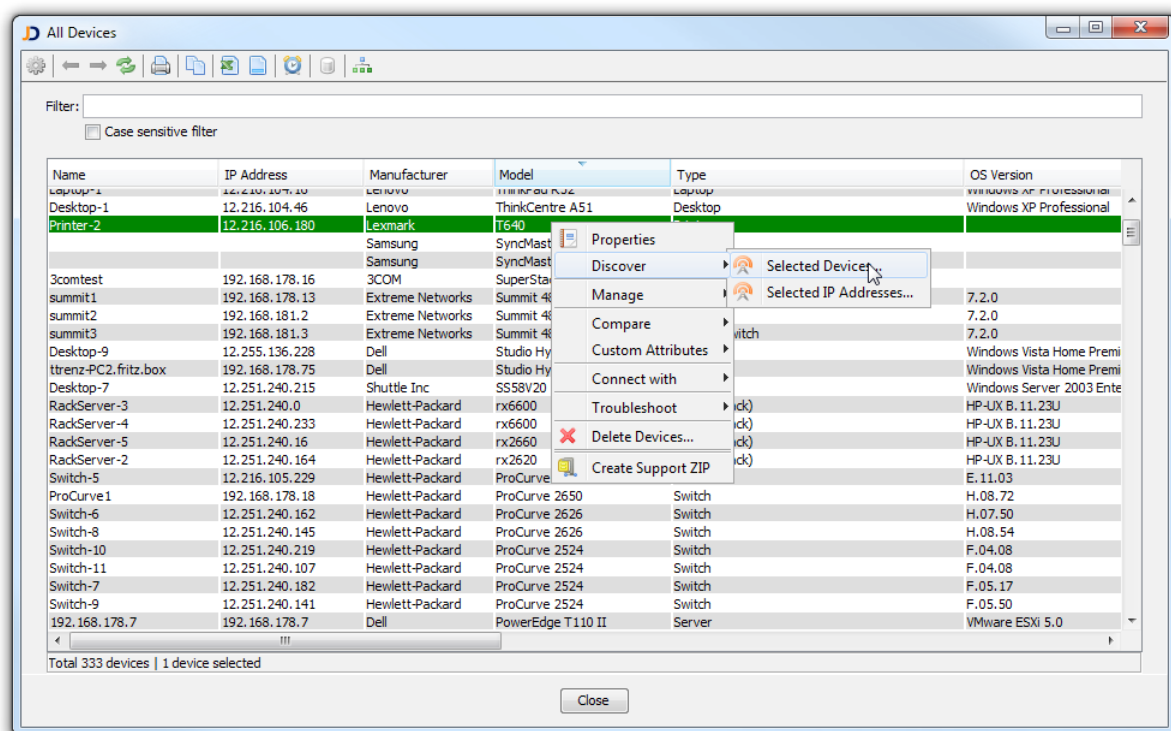


Figure: Discover selected Devices

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.

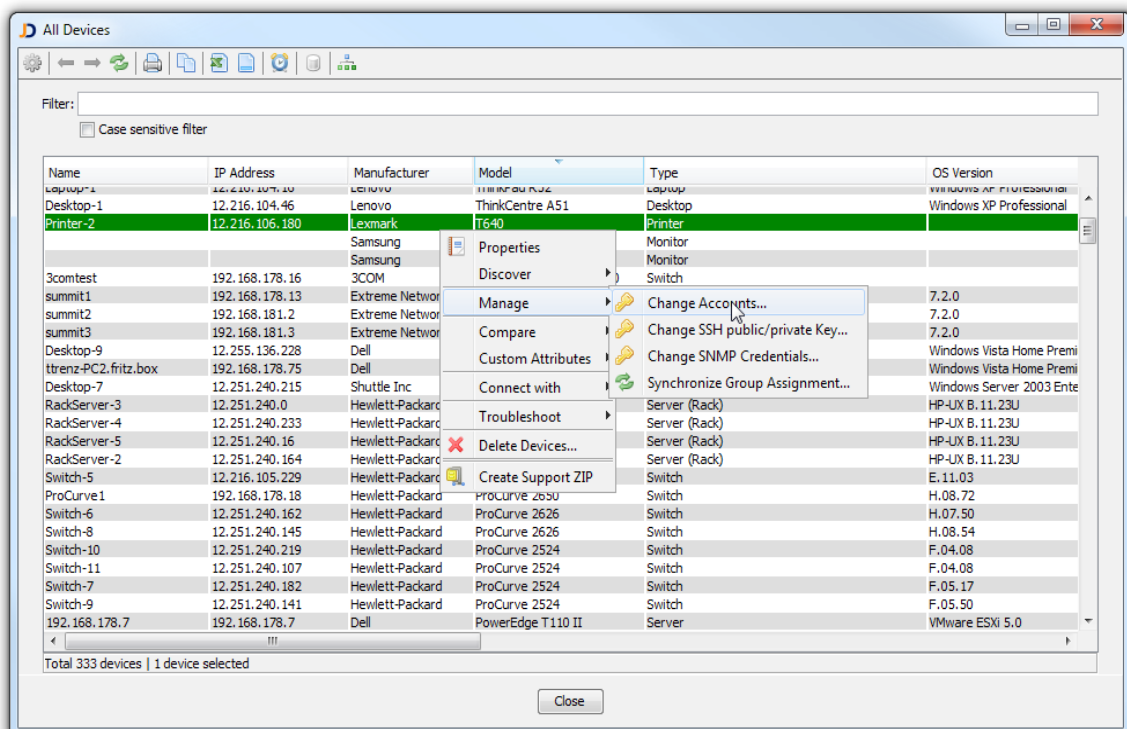


Figure: Manage Devices

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.

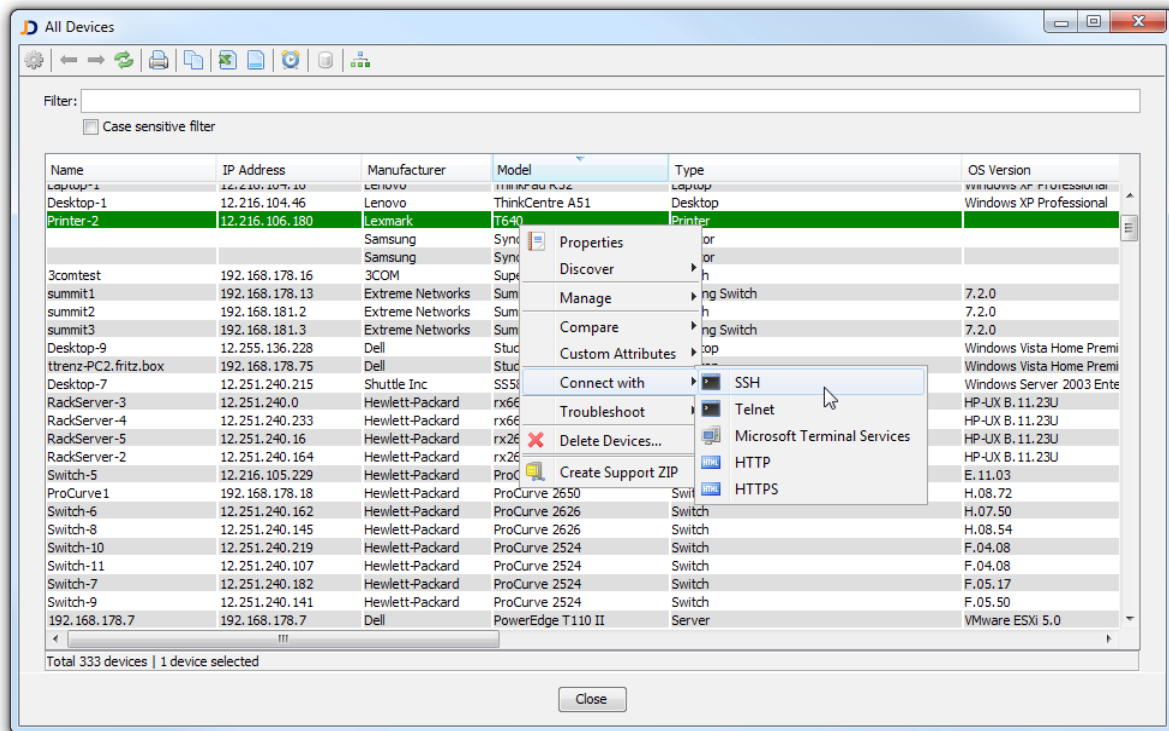


Figure: Connect to a Device

6.2.5 Troubleshooting

Click *Perform SNMP Walk* from the *Troubleshooting* menu to dump all SNMP variables of a SNMP enabled device.

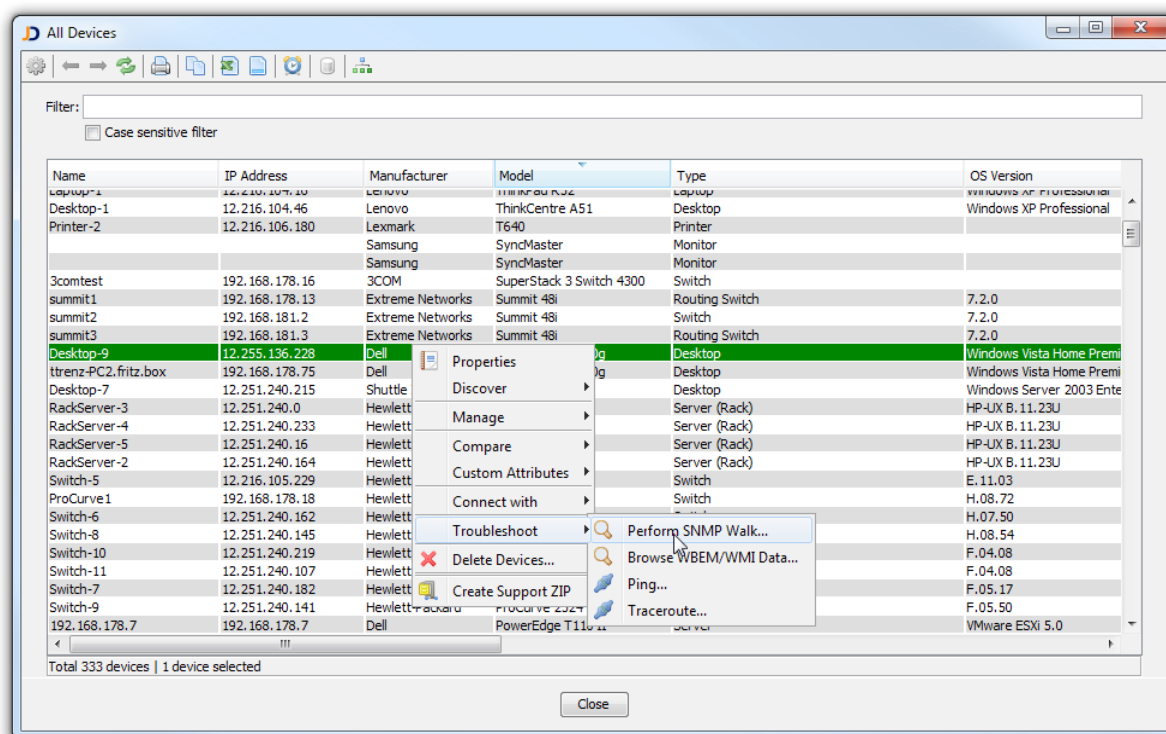


Figure: SNMP Walk

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
- Type
- 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.

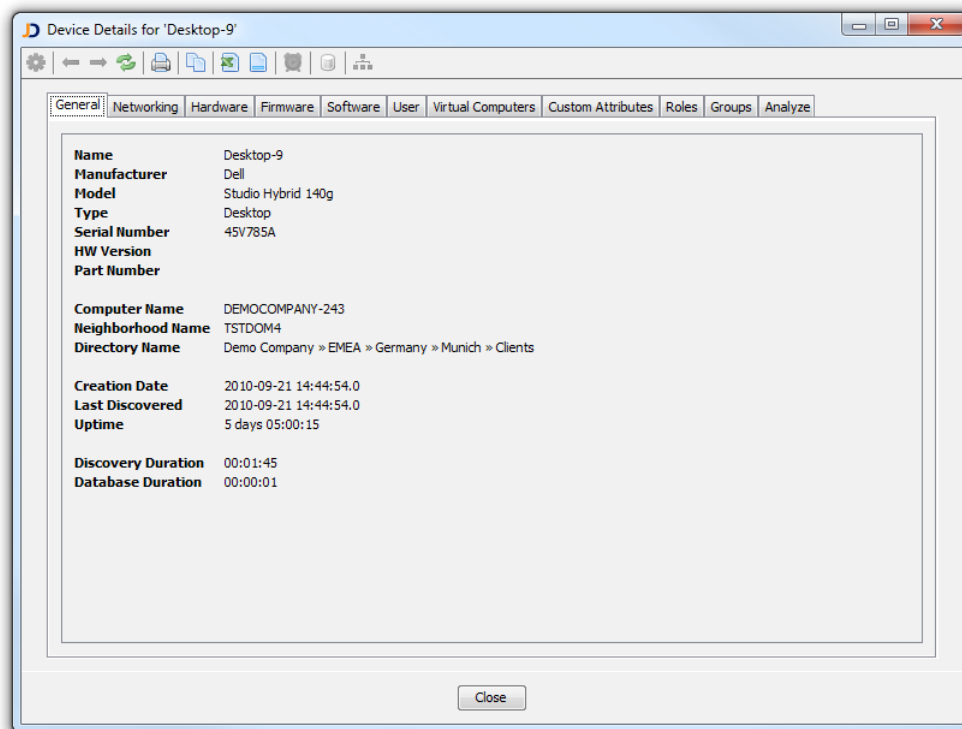


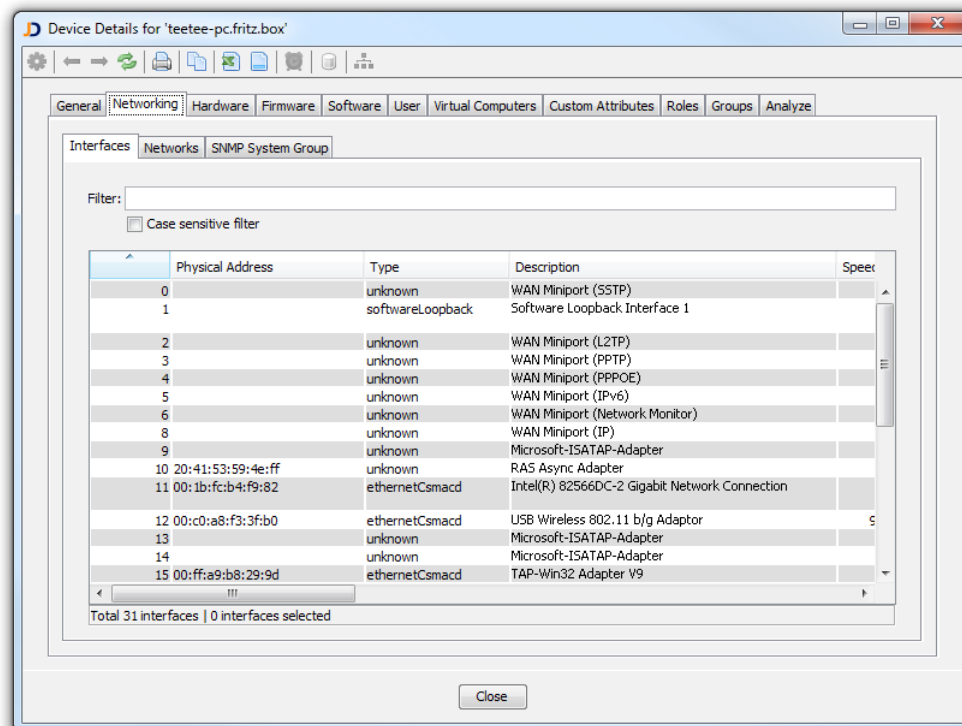
Figure: Device Details » General Tab

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.



	Physical Address	Type	Description	Speed
0		unknown	WAN Miniport (SSTP)	
1		softwareLoopback	Software Loopback Interface 1	
2		unknown	WAN Miniport (L2TP)	
3		unknown	WAN Miniport (PPTP)	
4		unknown	WAN Miniport (PPPOE)	
5		unknown	WAN Miniport (IPv6)	
6		unknown	WAN Miniport (Network Monitor)	
8		unknown	WAN Miniport (IP)	
9		unknown	Microsoft-ISA-TAP-Adapter	
10	20:41:53:59:4e:ff	unknown	RAS Async Adapter	
11	00:1b:fc:b4:f9:82	ethernetCsmacd	Intel(R) 82566DC-2 Gigabit Network Connection	
12	00:c0:a8:f3:3f:b0	ethernetCsmacd	USB Wireless 802.11 b/g Adaptor	5
13		unknown	Microsoft-ISA-TAP-Adapter	
14		unknown	Microsoft-ISA-TAP-Adapter	
15	00:ffa9:b8:29:9d	ethernetCsmacd	TAP-Win32 Adapter V9	

Total 31 interfaces | 0 interfaces selected

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.

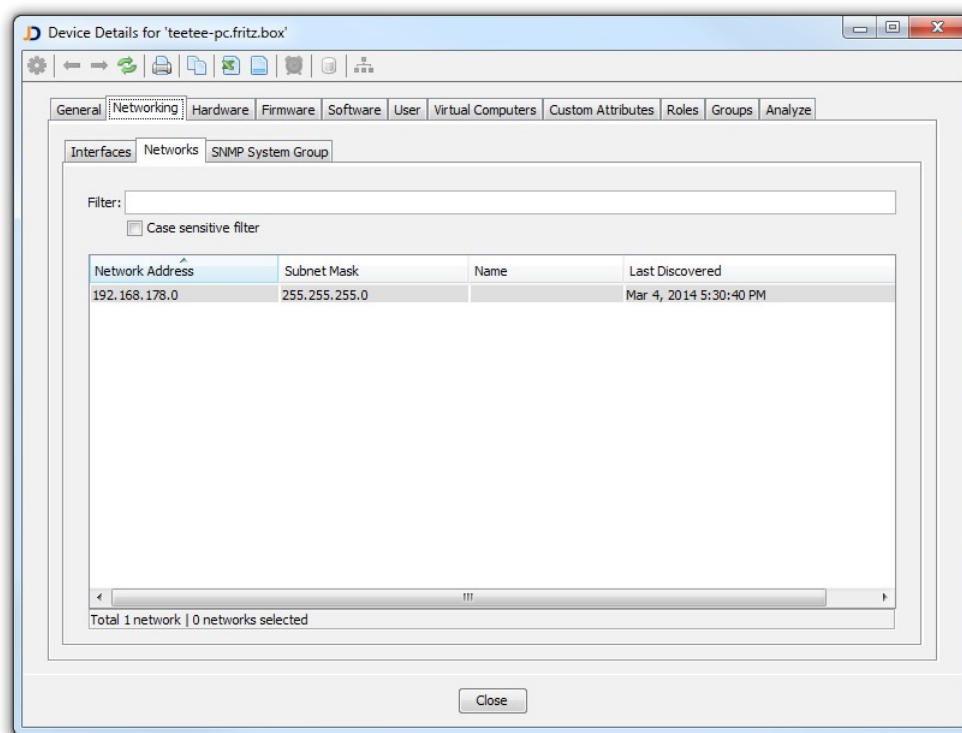


Figure: Networks Table

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.

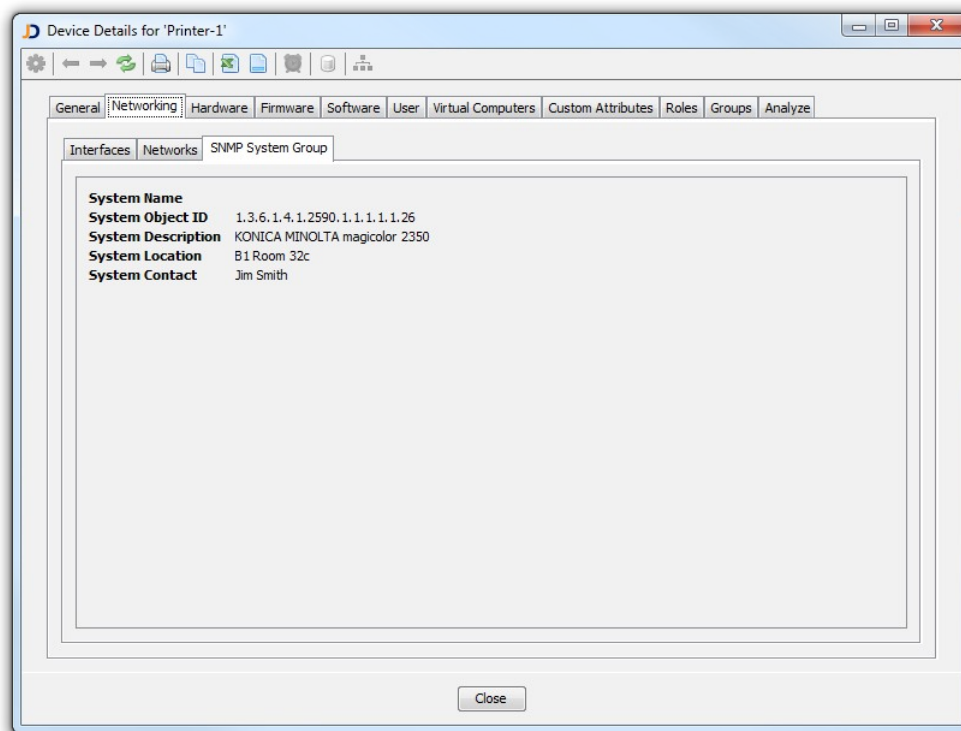


Figure: SNMP System Group Tab

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.

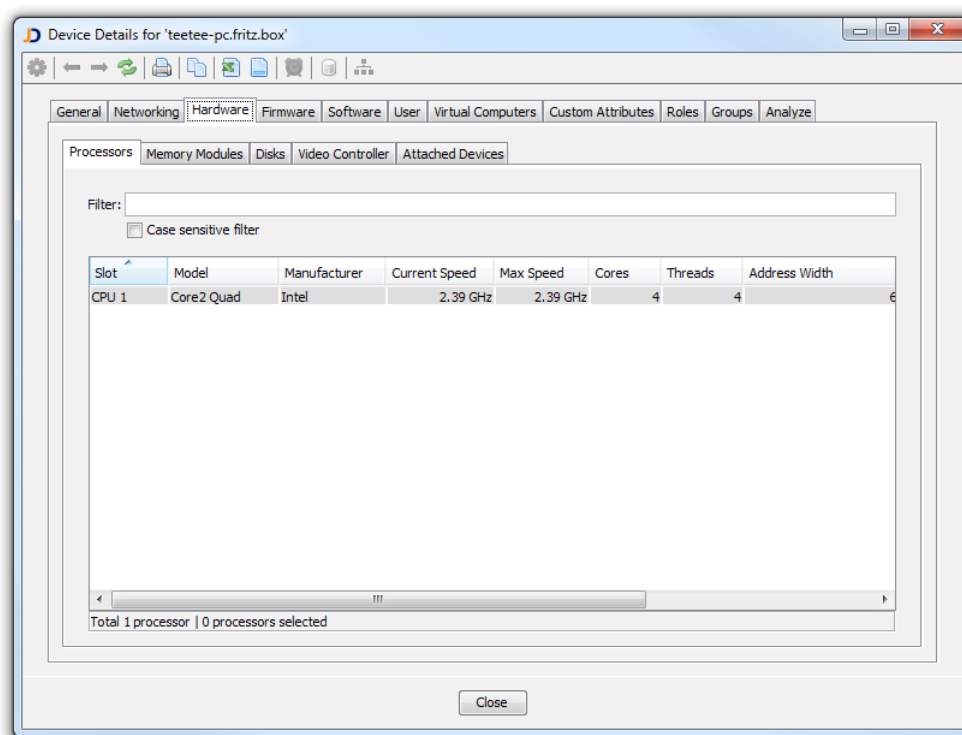


Figure: Processors Tab

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'.

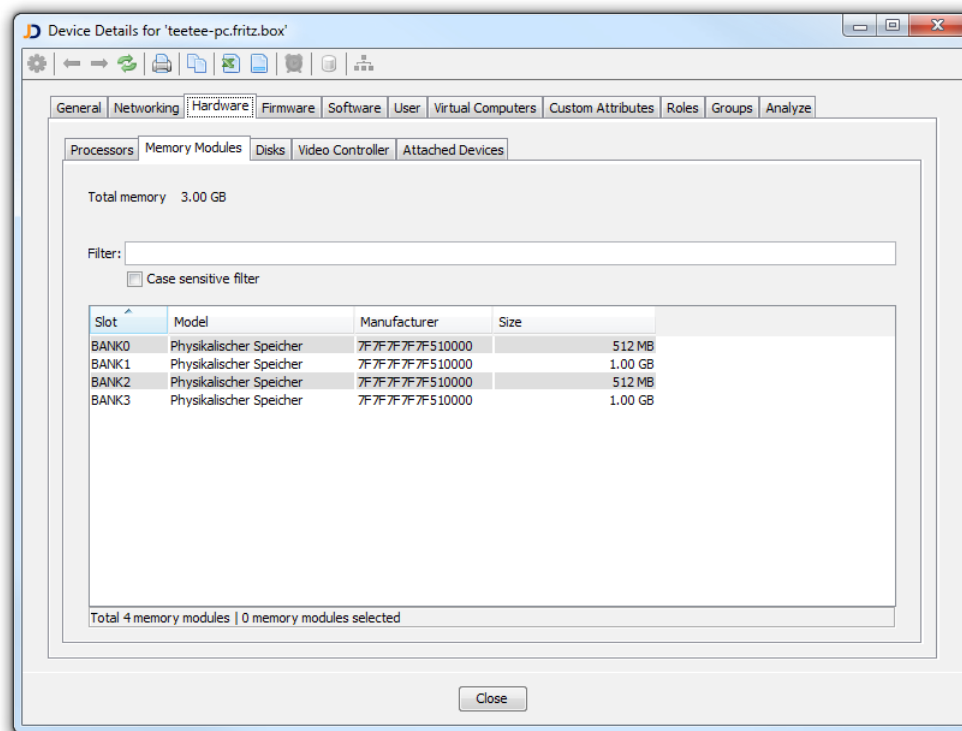


Figure: Memory Modules Tab

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.

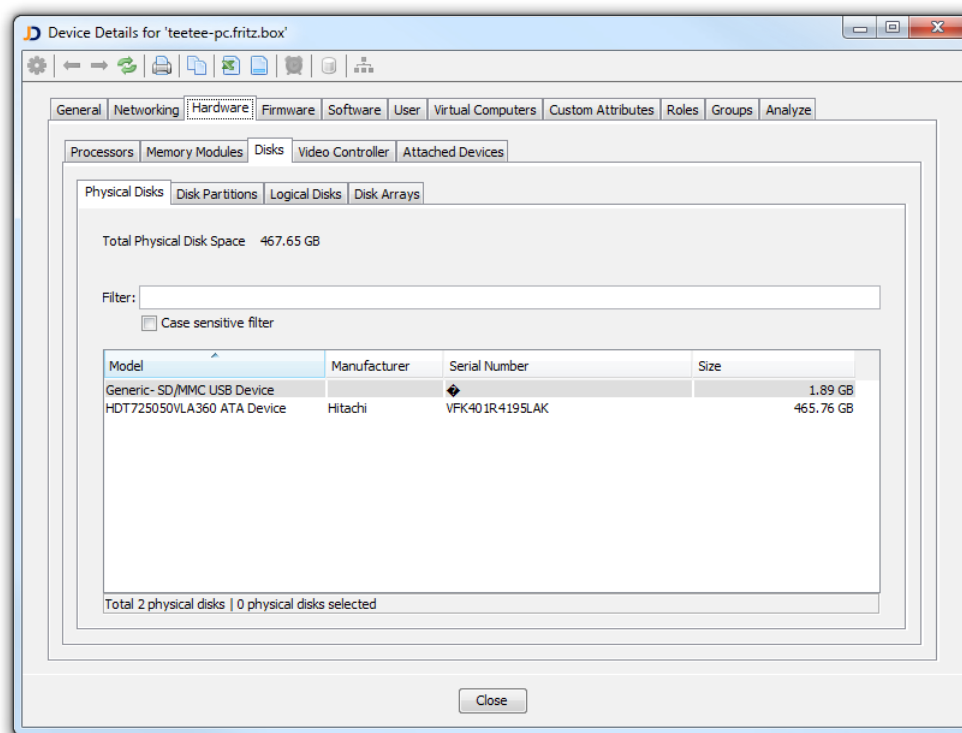


Figure: Physical Disks Tab

The *Total Physical Disk Space* displays the sum of all physical disks.

Disk Partitions

The *Disk Partitions* tab displays all partitions on the computer.

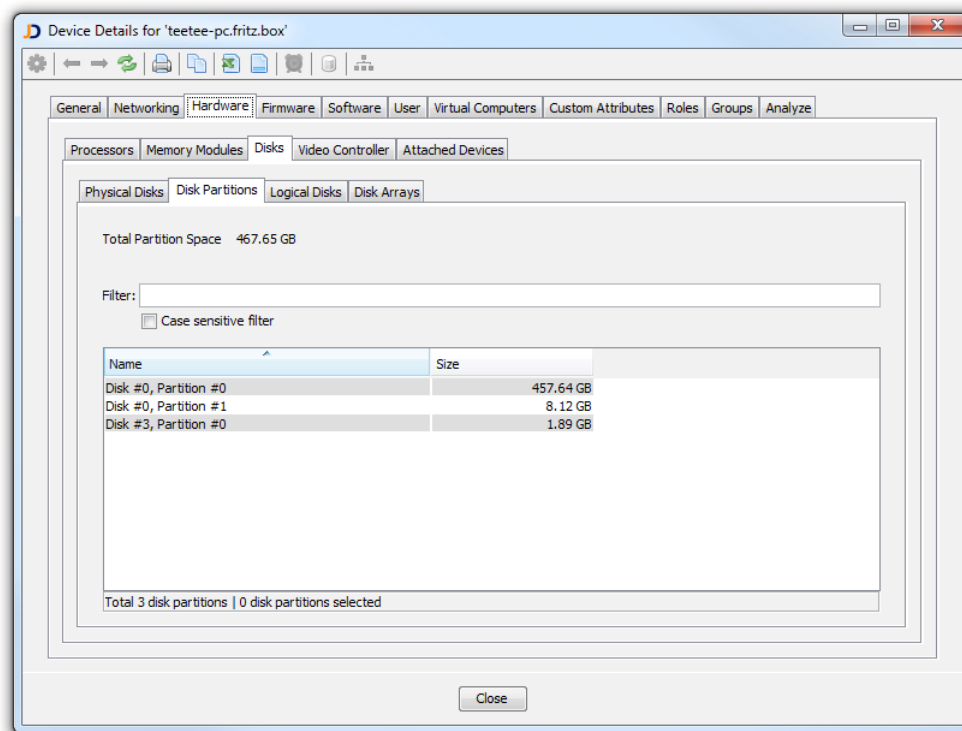


Figure: Disk Partitions Tab

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

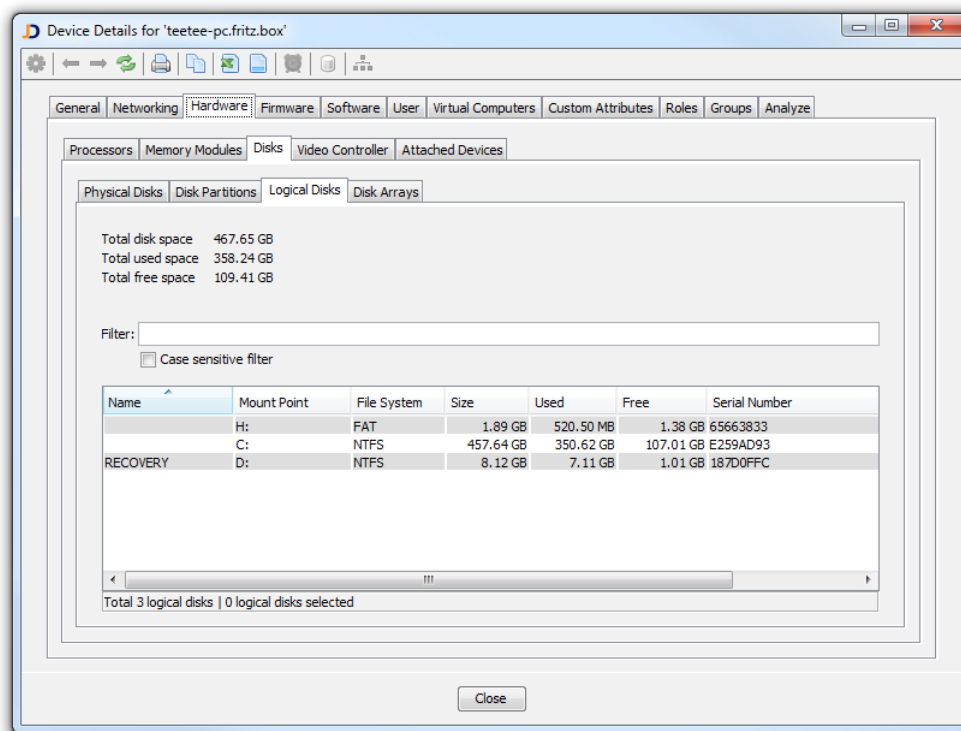


Figure: Logical Disks Tab

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.

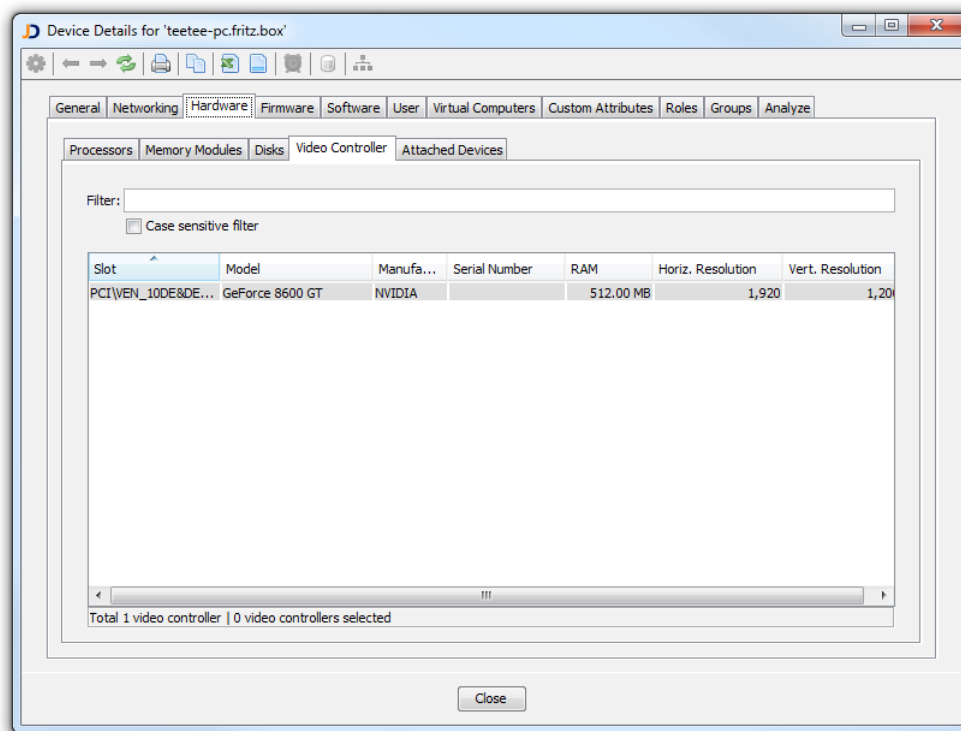


Figure: Video Controllers

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

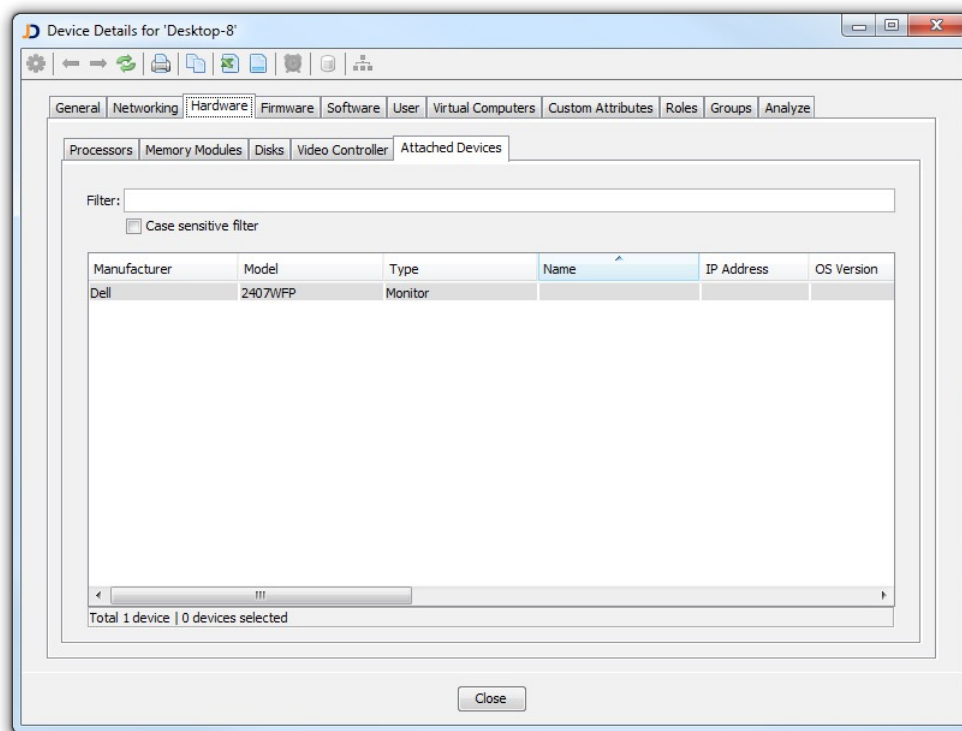


Fig: Attached monitor

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

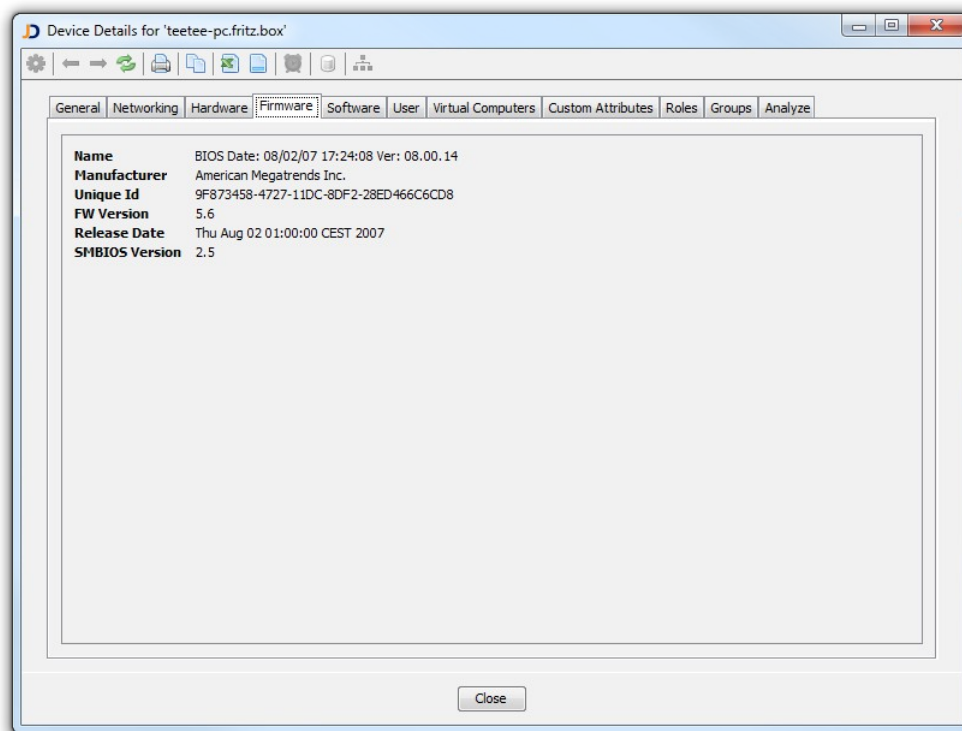


Figure: Firmware Tab

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

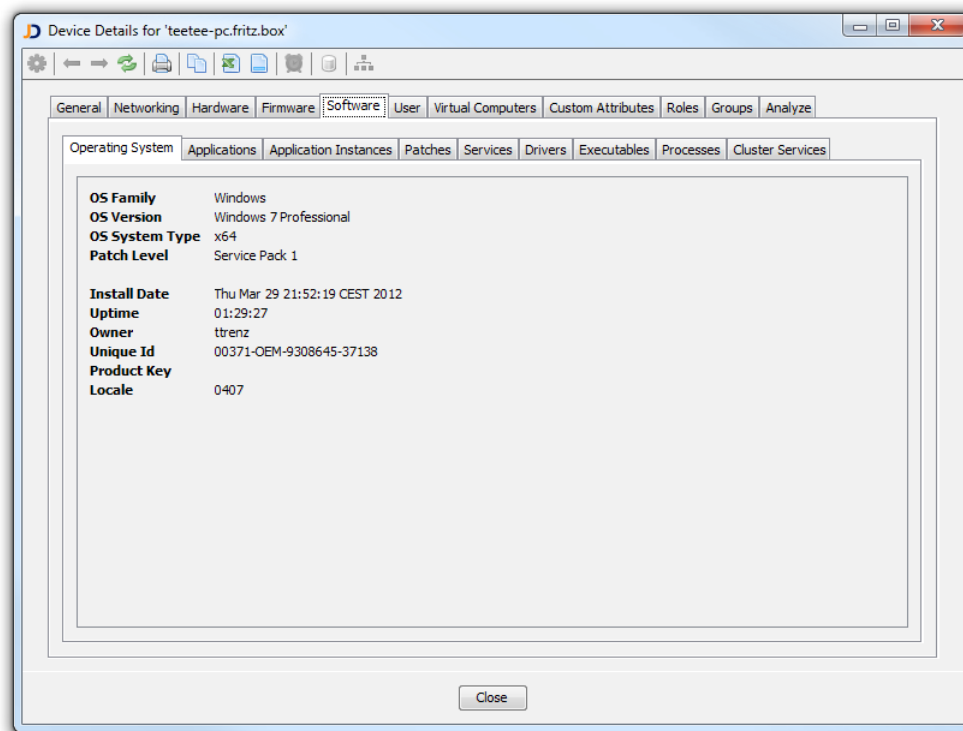


Figure: Operating System Information

6.3.5.2 Applications

The *Applications* tab displays installed applications.

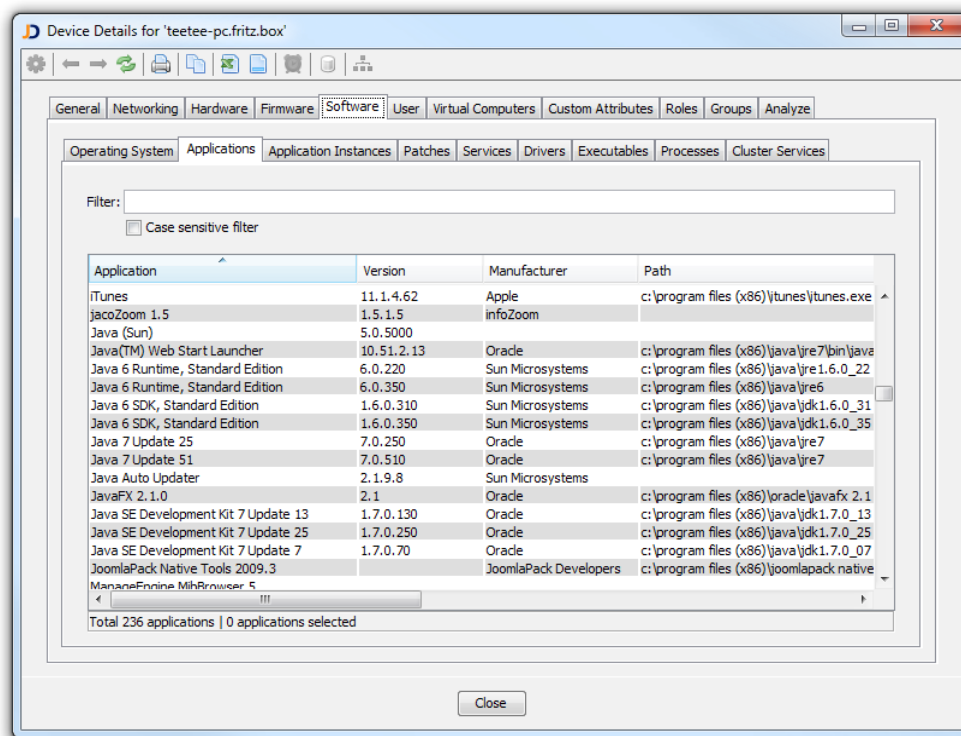


Figure: Applications Tab

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.

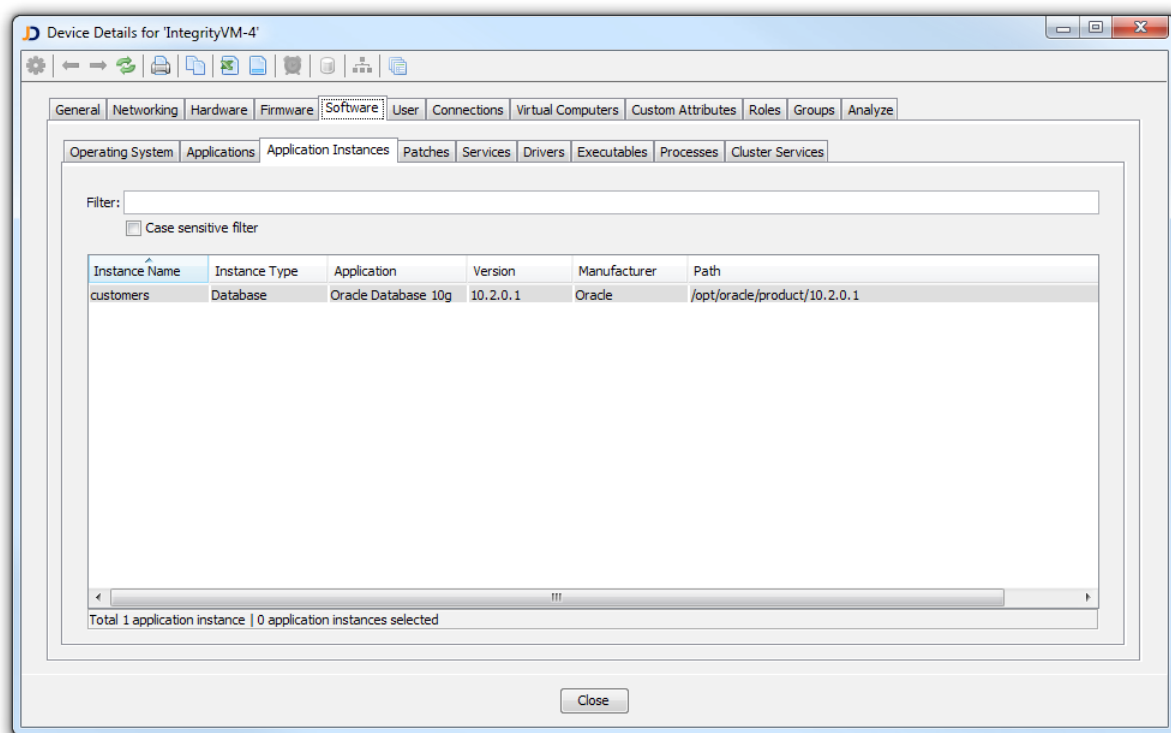


Figure: Application Instances

6.3.5.4 Patches

The *Patches* tab displays installed patches.

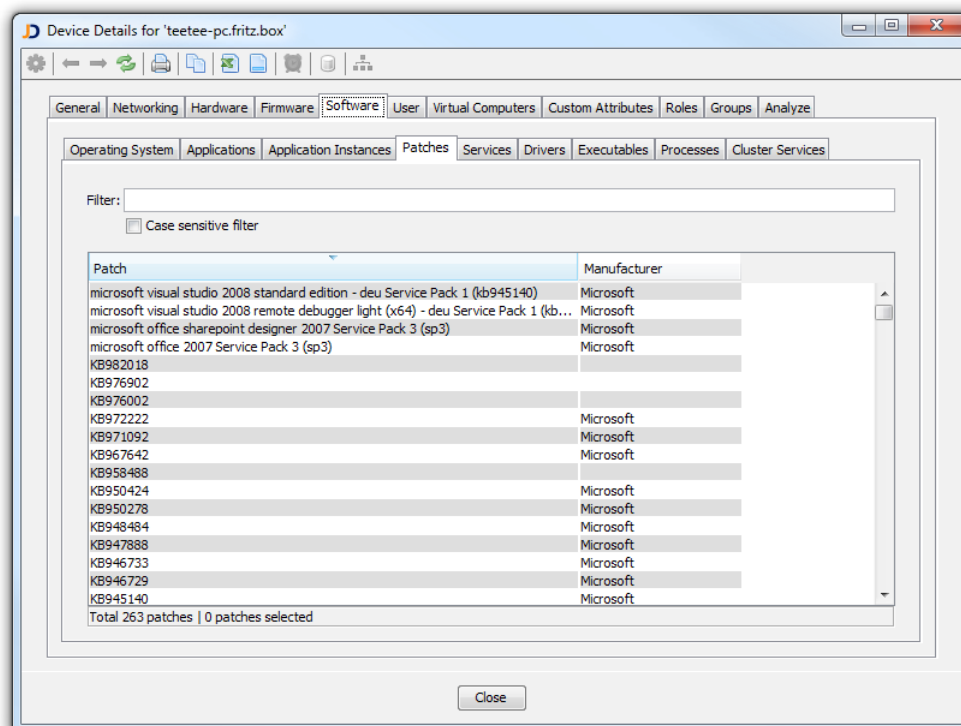


Figure: Patches Tab

6.3.5.5 Services

The *Services* tab displays installed services including important service attributes.

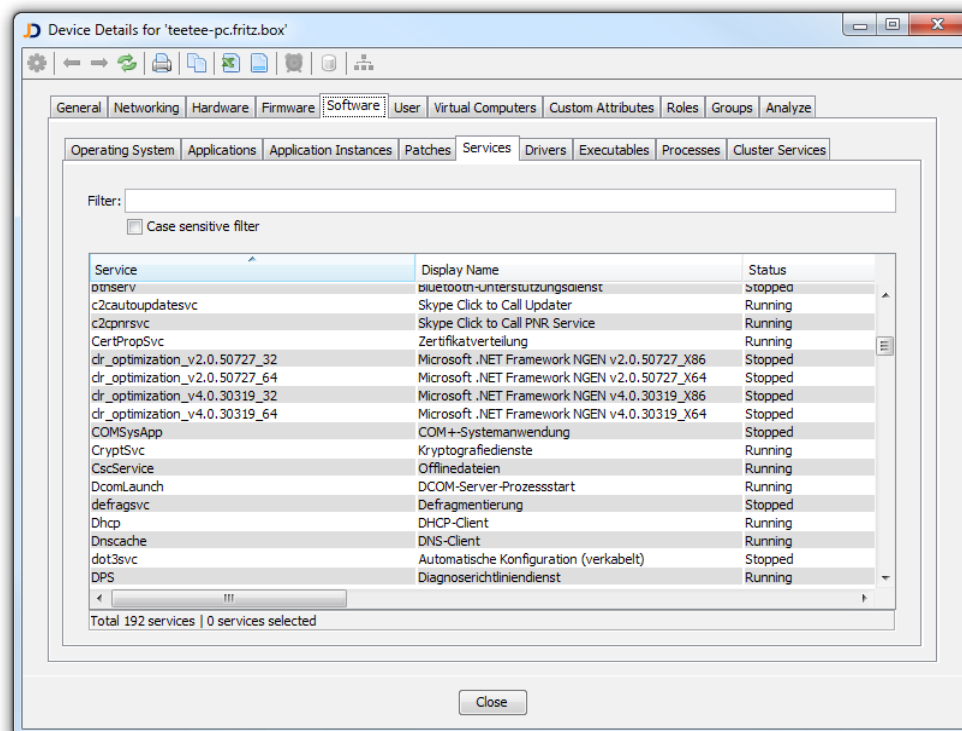


Figure: Installed Services

6.3.5.6 Drivers

The *Drivers* tab displays installed drivers including important driver attributes.

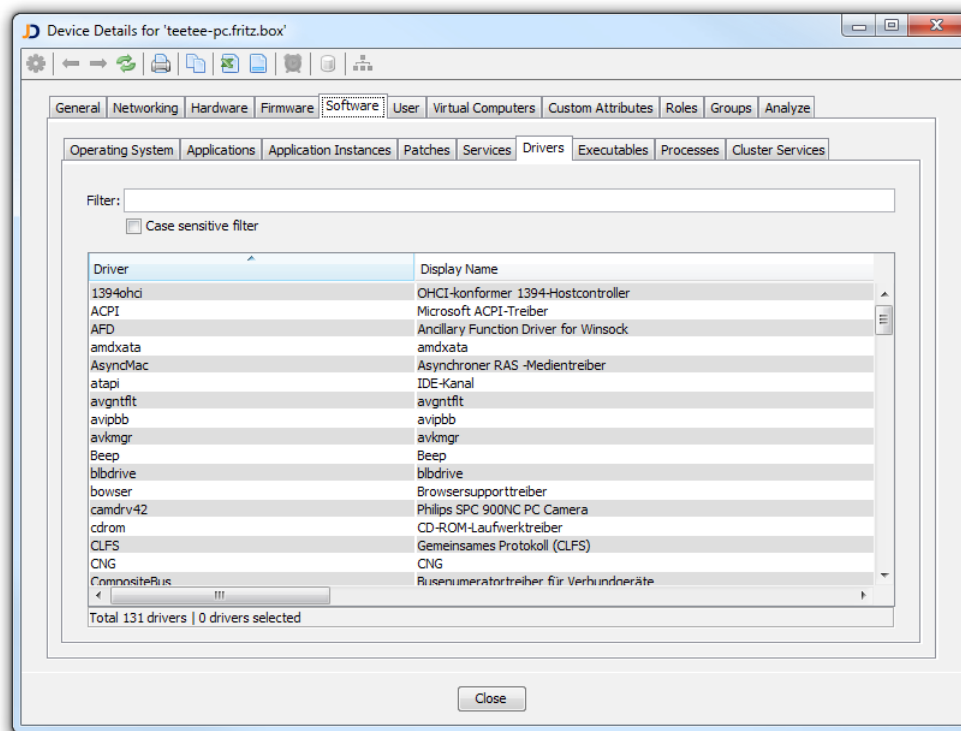


Figure: Installed Drivers

6.3.5.7 Executables

The *Executables* tab displays the list of all executables found on local harddrives.

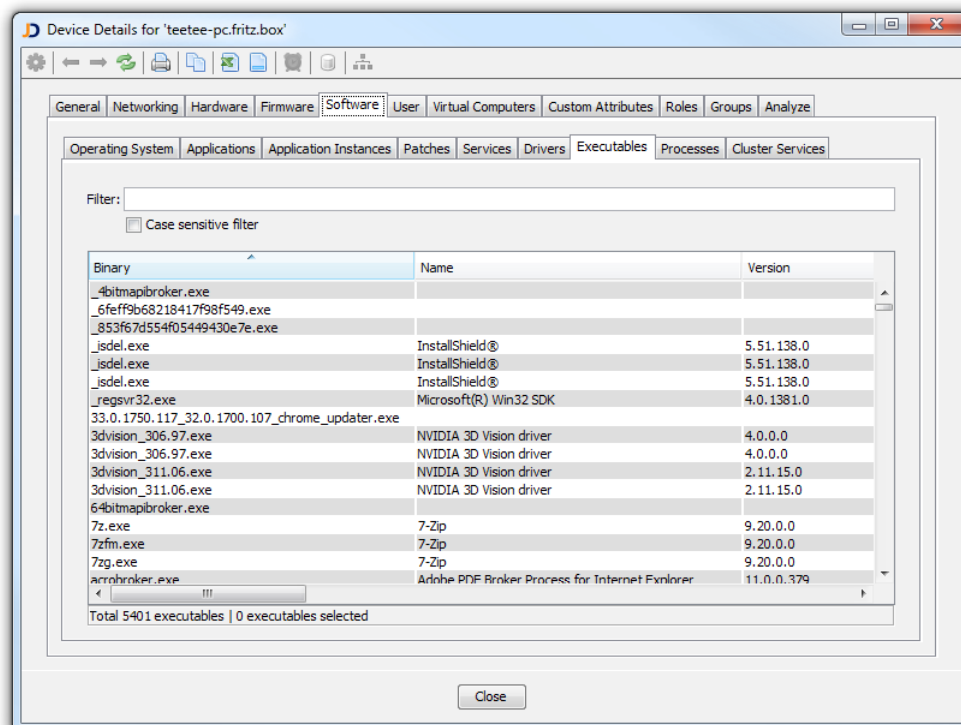


Figure: The list of all local executables

6.3.5.8 Processes

The *Processes* tab displays running processes including important process attributes.

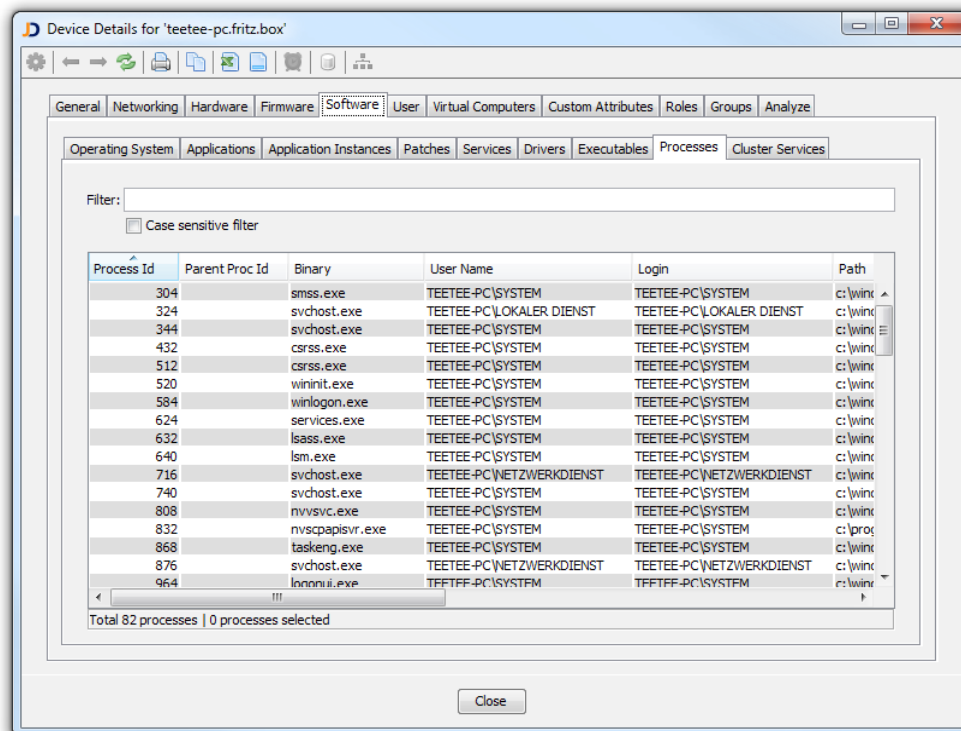


Figure: Running Processes

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.

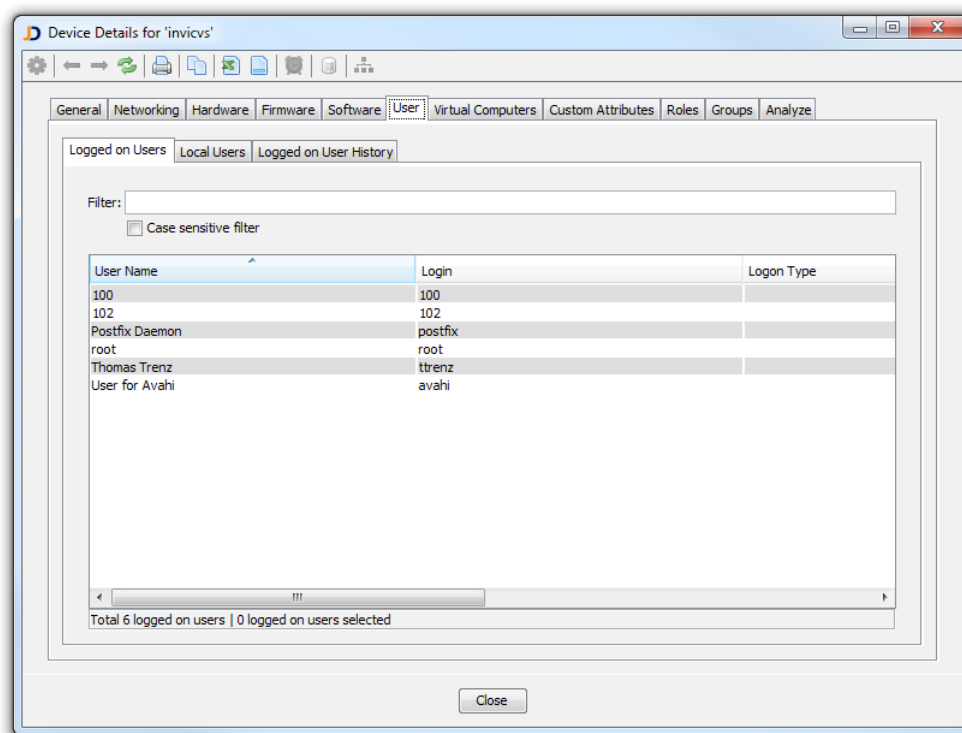


Figure: Logged on Users

6.3.6.2 Local Users

Displays local users.

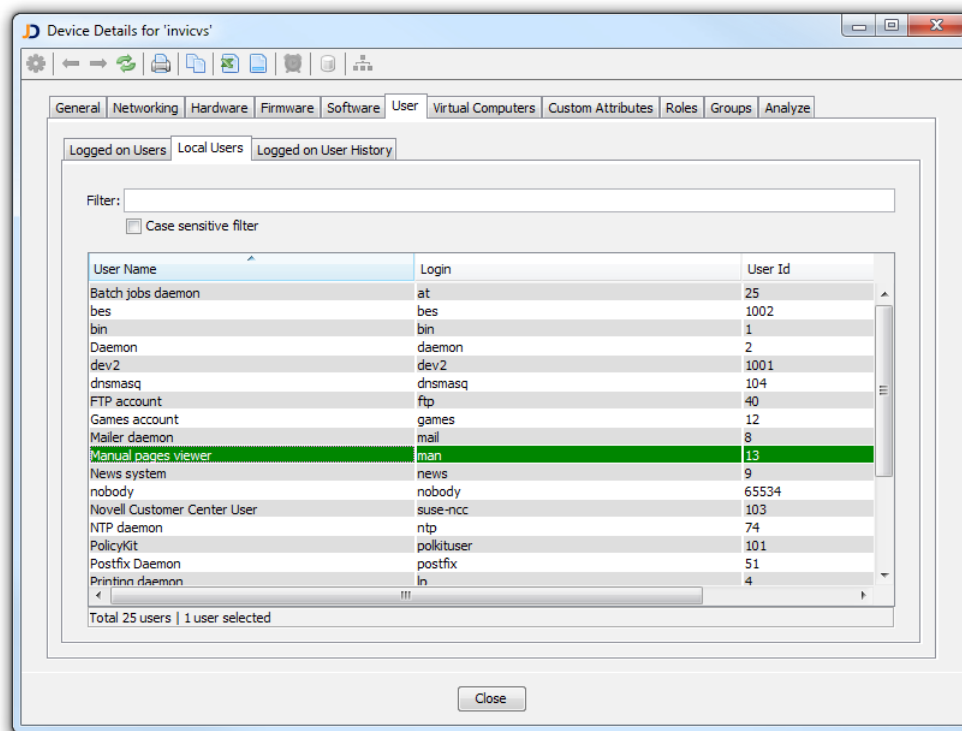


Figure: Local Users

6.3.6.3 Logged On User History

Displays users that have been logged within a configurable number of days.

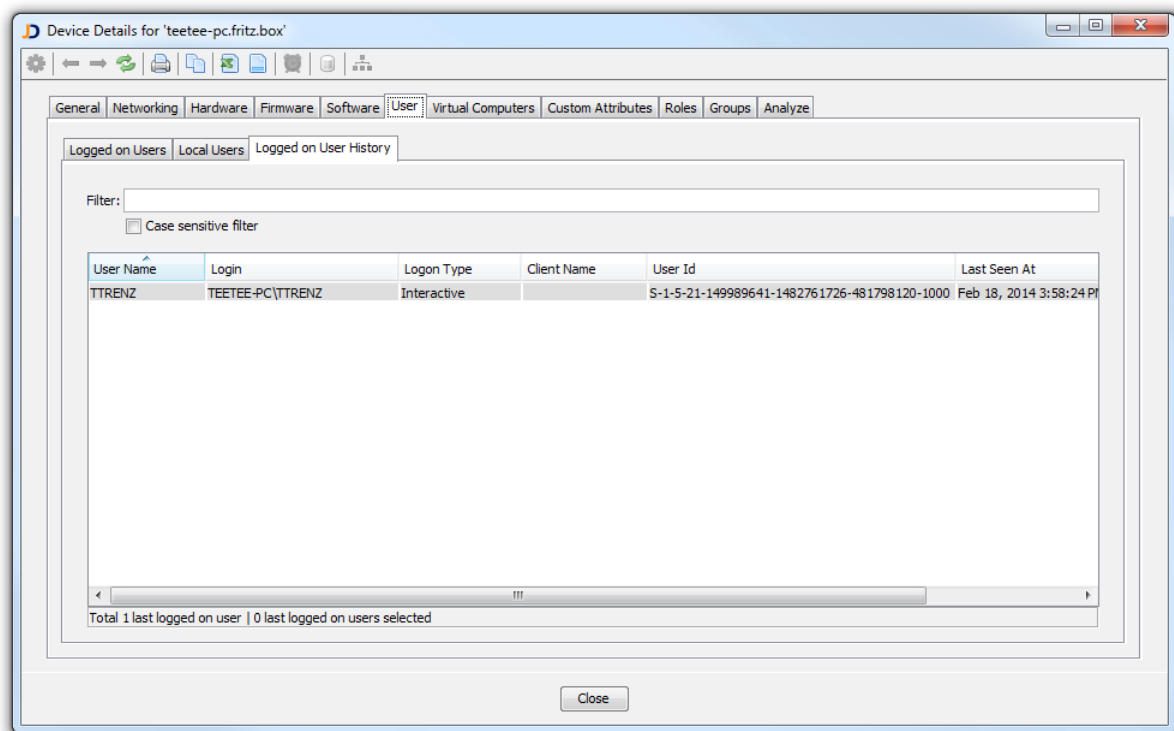


Figure: Logged on User History

6.3.7 Virtual Computers

The *Virtual Computers* tab displays virtual computers (for example VMware) running on a host server.

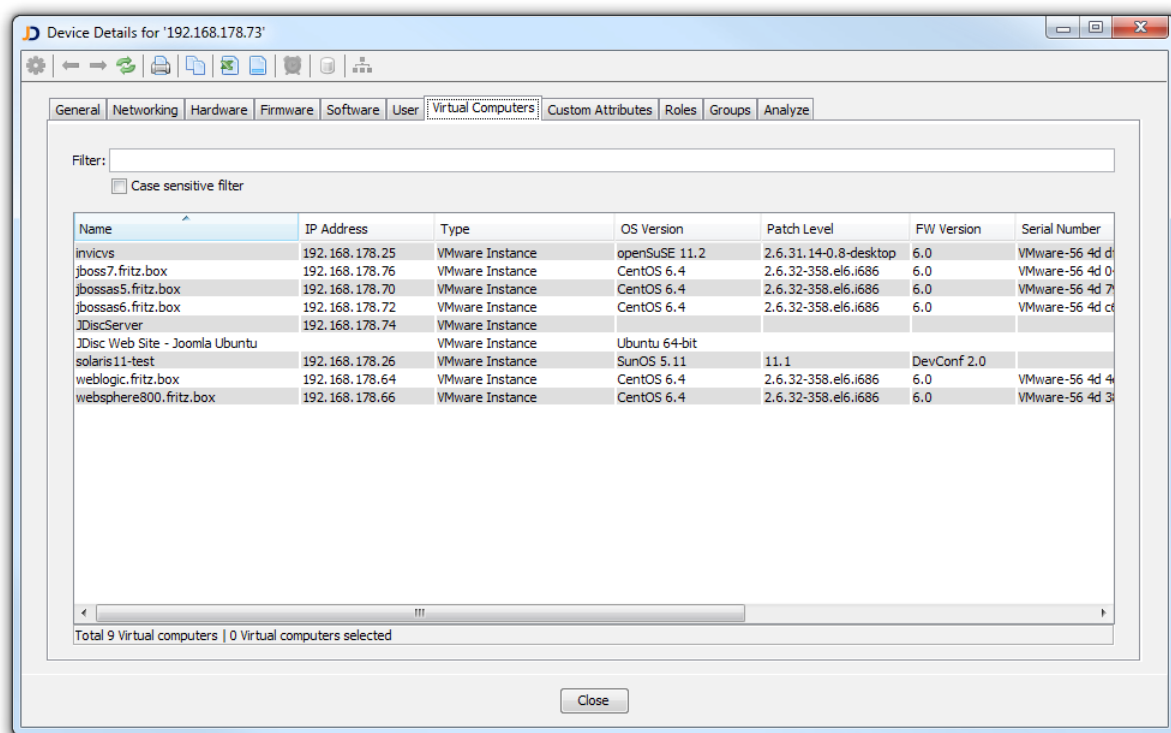


Fig: Virtual Computers tab

6.3.8 Custom Attributes

The *Custom Attributes* tab displays the custom attribute hierarchy including the attributes for the selected folder.

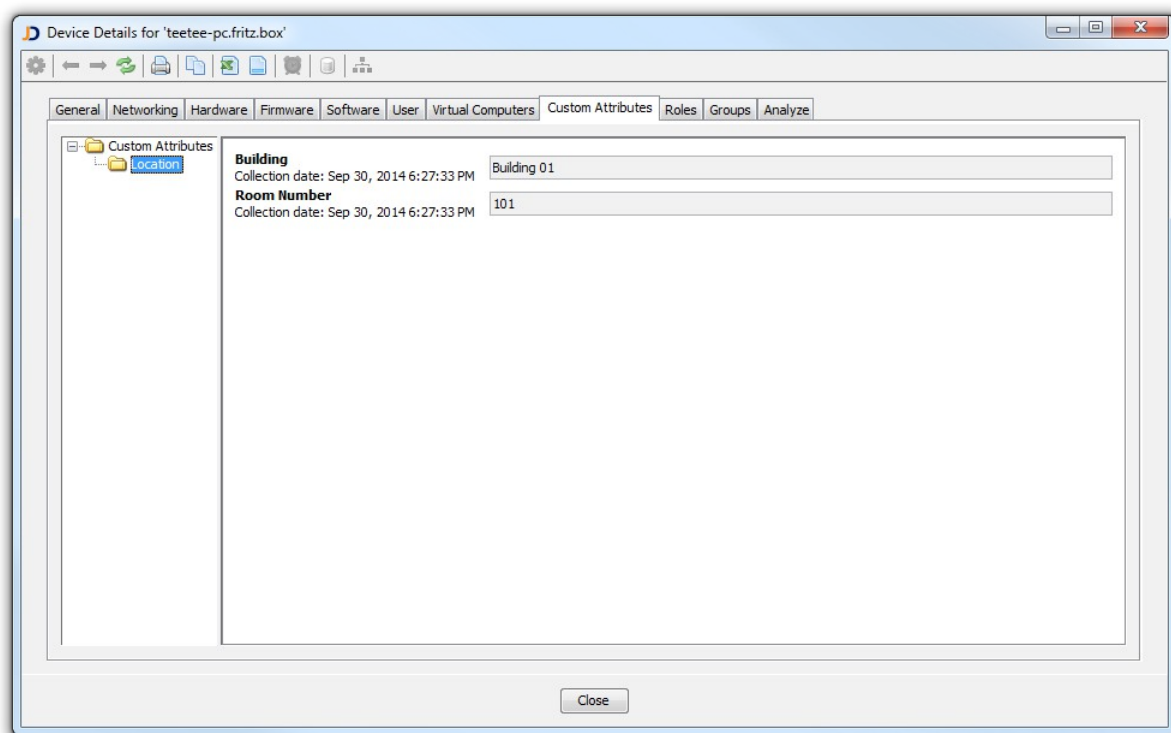


Figure: Custom Attributes Tab

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.

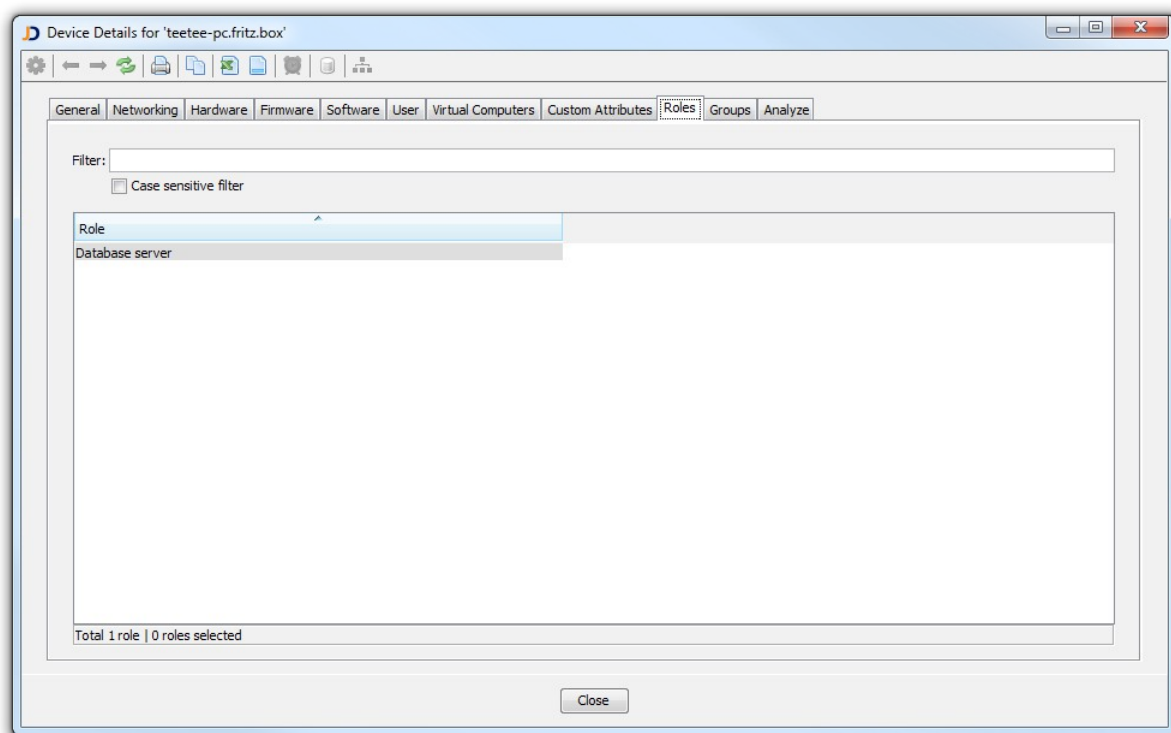


Fig: Roles tab

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.

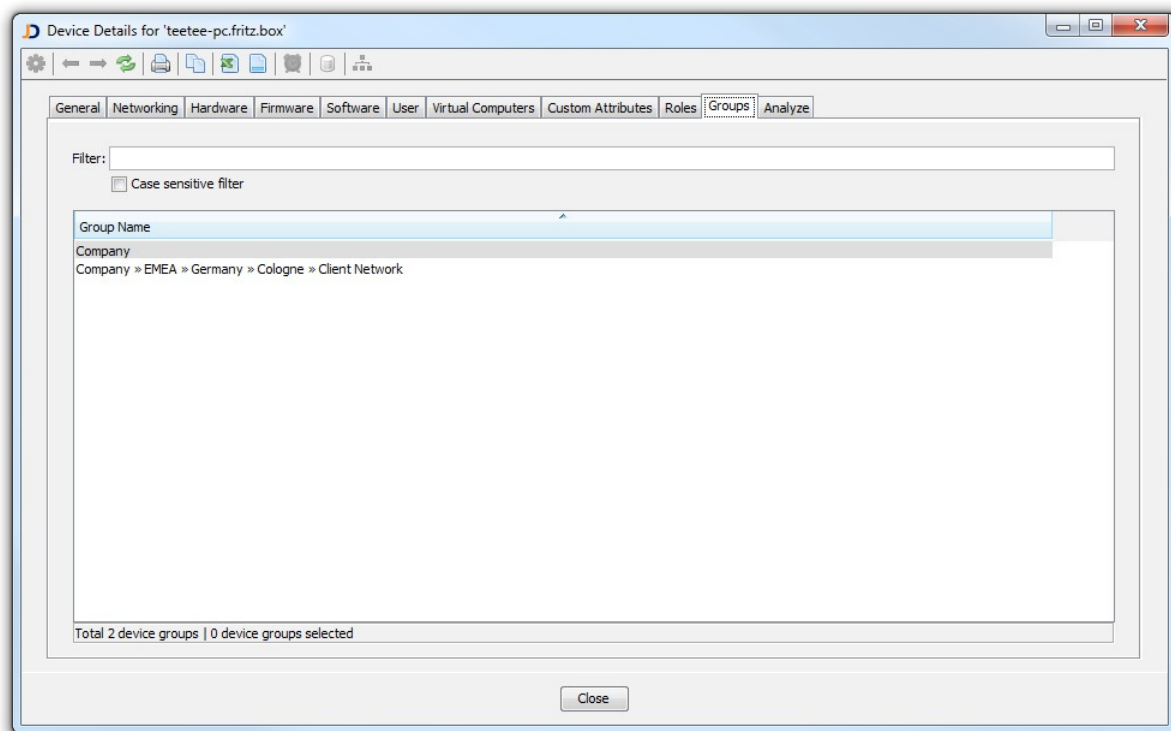


Figure: Groups Tab

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.

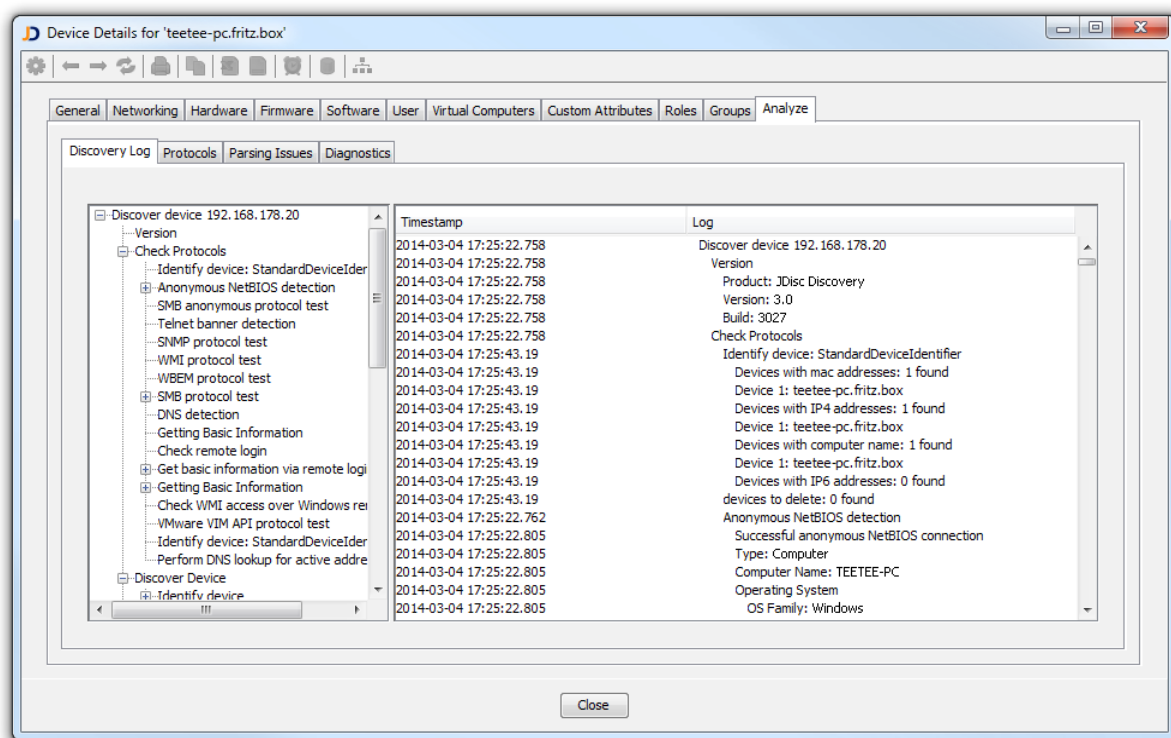


Figure: Discovery Log Tab

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.

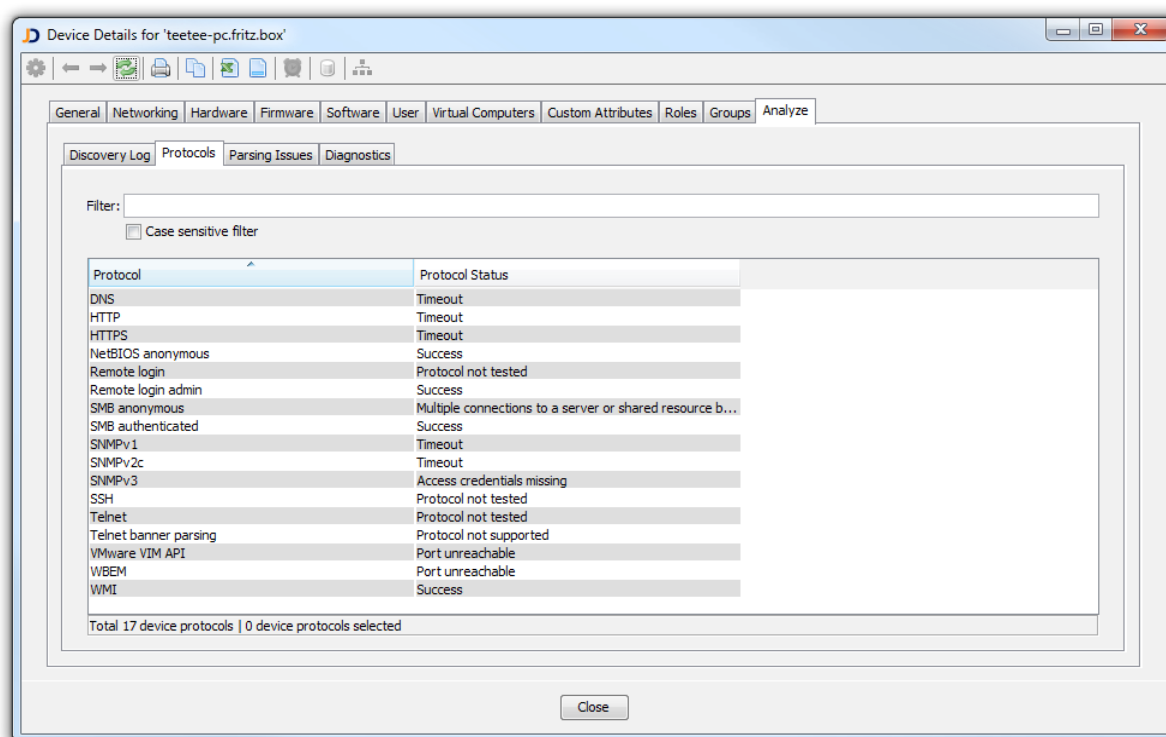


Figure: Protocols Tab

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.

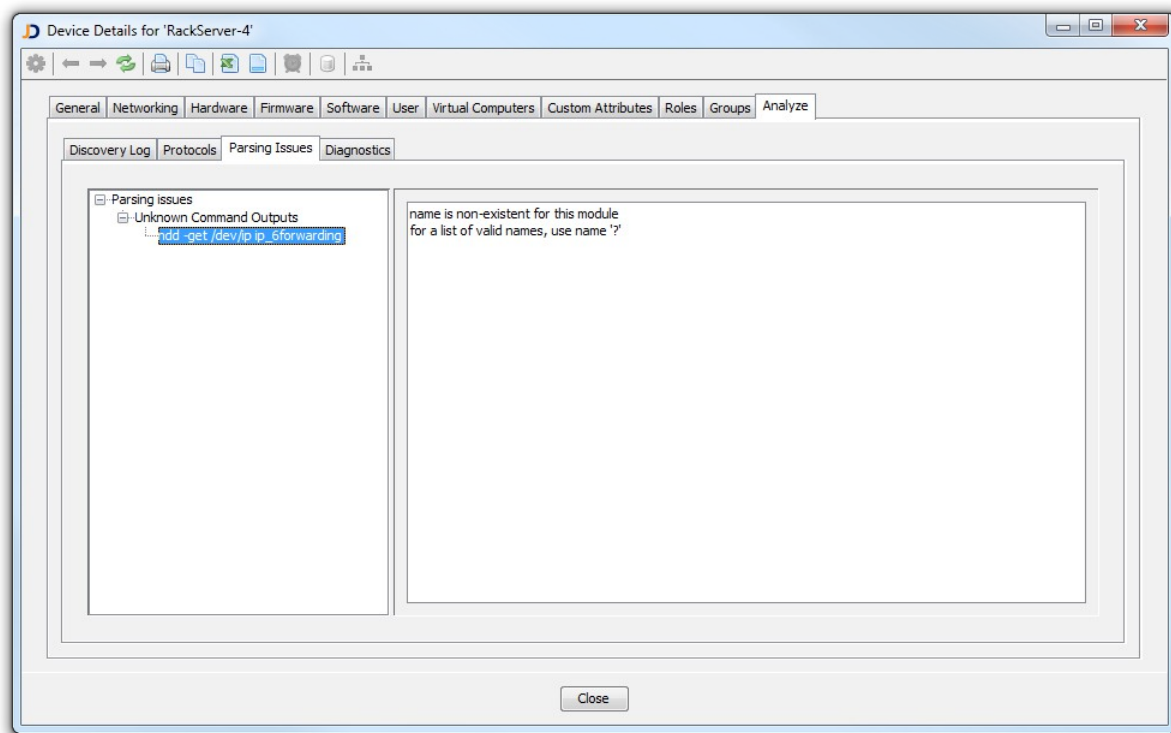


Figure: Parsing Issues Tab

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.

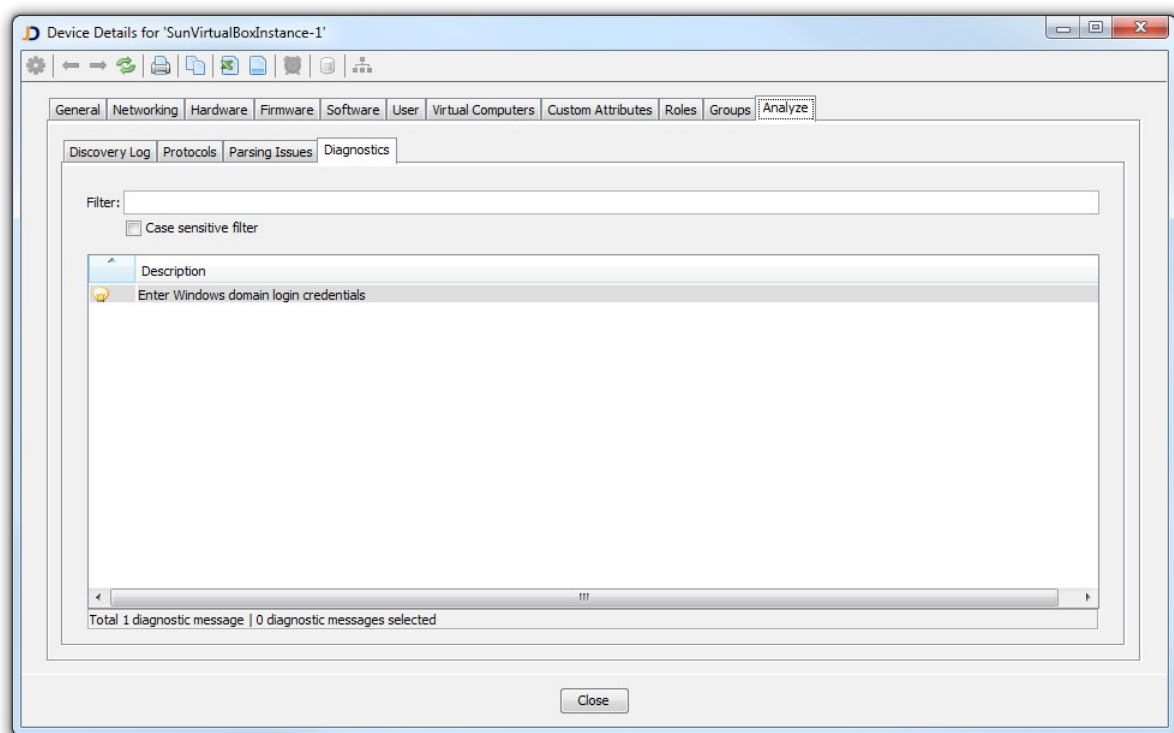







Figure: Diagnostics Tab

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:

- : Management servers for a virtualization technology (for instance vCenter installations)
- : Virtual datacenters
- : Cluster
- : Physical server hosting virtual machines
- : VM running as on a physical host

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.

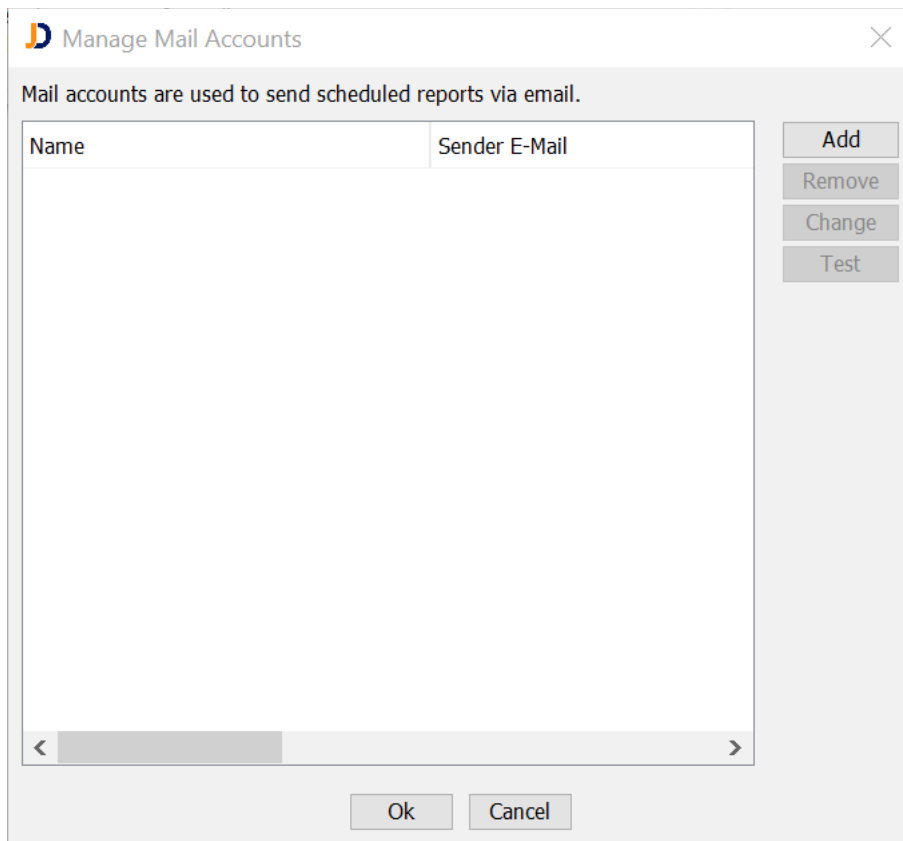


Fig: Manage your mail servers and accounts

Clicking on *Add* buttons takes you to the dialog where you can setup the reports sender email address.

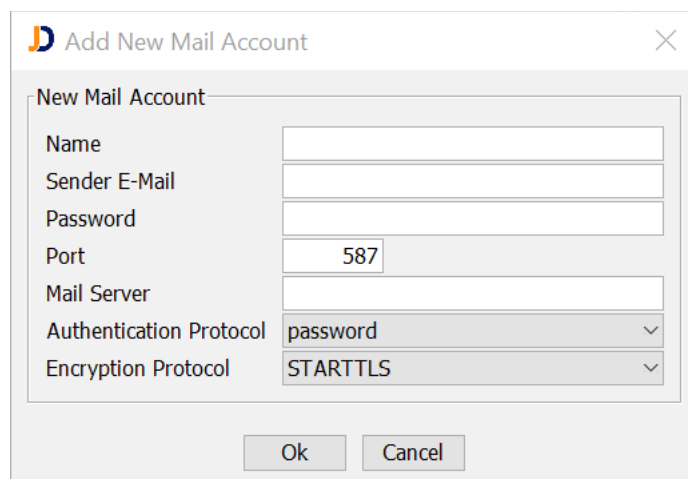


Fig: Add a new mail server and account

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:

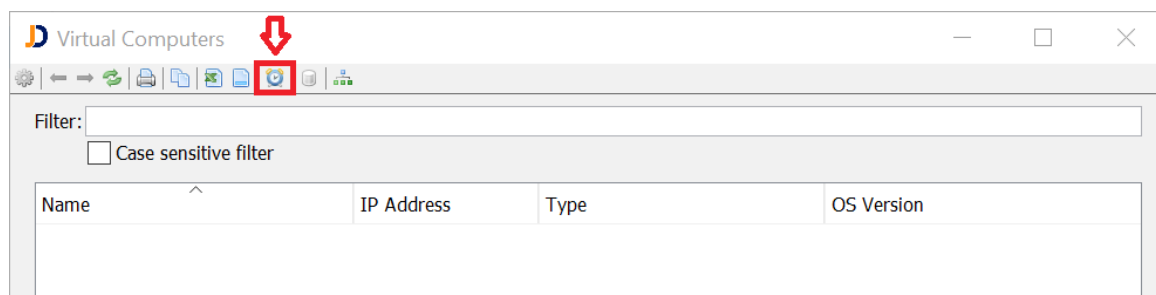


Fig: Schedule a Report Export or Mail Message

From the appeared dialog, select *Send report via email* option.

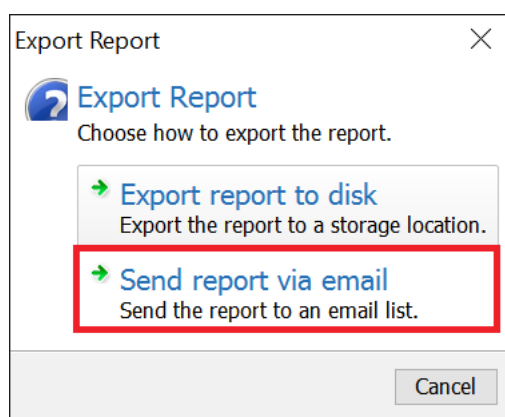


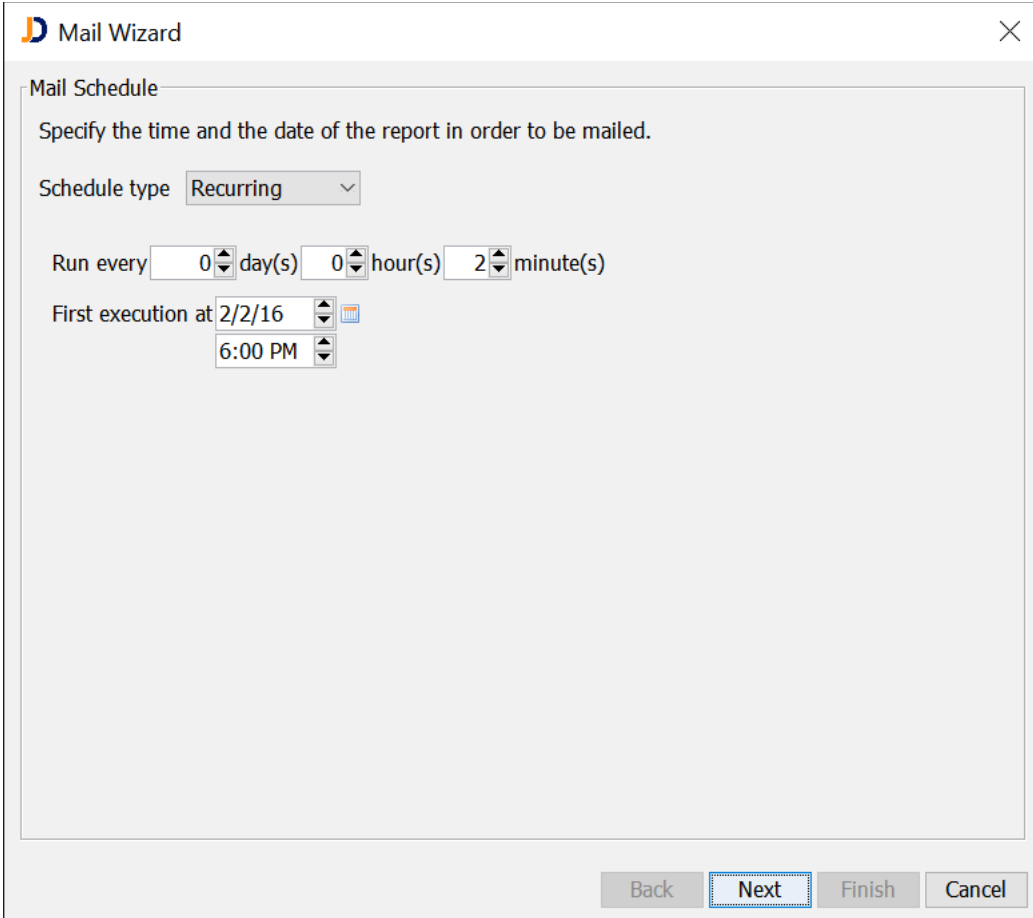
Fig: Send Report via EMail

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.



The image shows a 'Mail Wizard' dialog box with a 'Mail Schedule' tab. The instruction 'Specify the time and the date of the report in order to be mailed.' is displayed. The 'Schedule type' is set to 'Recurring'. The frequency is configured as 'Run every 0 day(s) 0 hour(s) 2 minute(s)'. The 'First execution at' is set to '2/2/16' at '6:00 PM'. At the bottom, there are four buttons: 'Back', 'Next' (which is highlighted with a blue border), 'Finish', and 'Cancel'.

Mail Wizard

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)

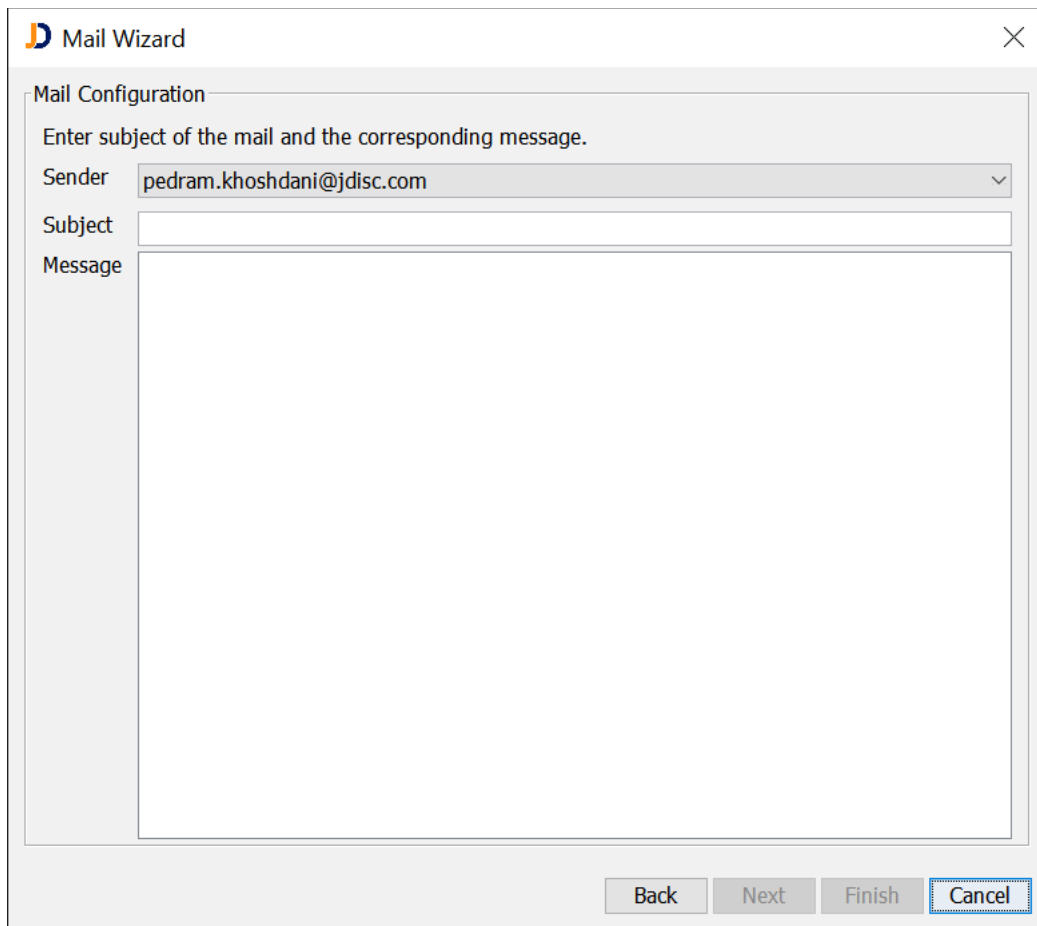
First execution at 2/2/16 6:00 PM

Back Next Finish Cancel

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.

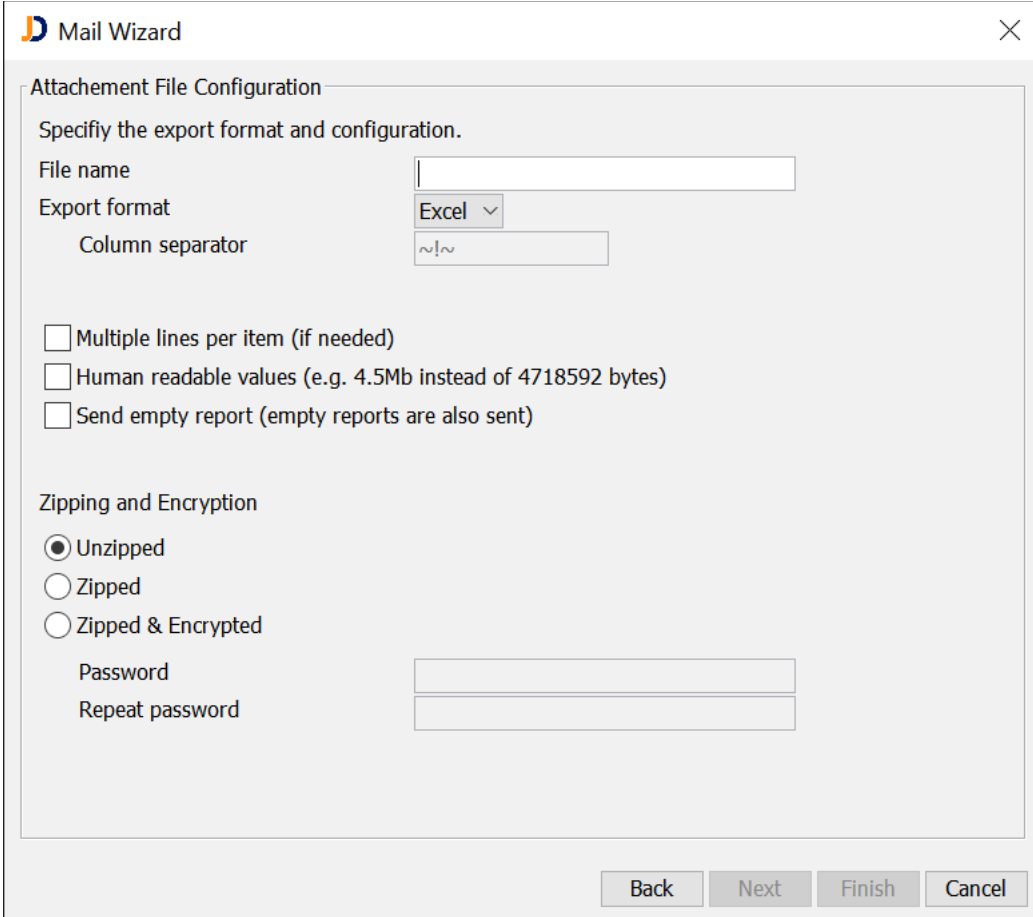


The image shows a 'Mail Wizard' dialog box with a title bar containing a logo and the text 'Mail Wizard'. The main area is titled 'Mail Configuration' and contains the instruction 'Enter subject of the mail and the corresponding message.' Below this, there are three input fields: 'Sender' (a dropdown menu showing 'pedram.khoshdani@jdisc.com'), 'Subject' (a text box), and 'Message' (a large text area). At the bottom right, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel' (which is highlighted with a blue border).

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 [X]

Attachement File Configuration

Specify the export format and configuration.

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)

Zippping and Encryption

☒ Unzipped

☐ Zipped

☐ Zipped & Encrypted

Password:

Repeat password:

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.

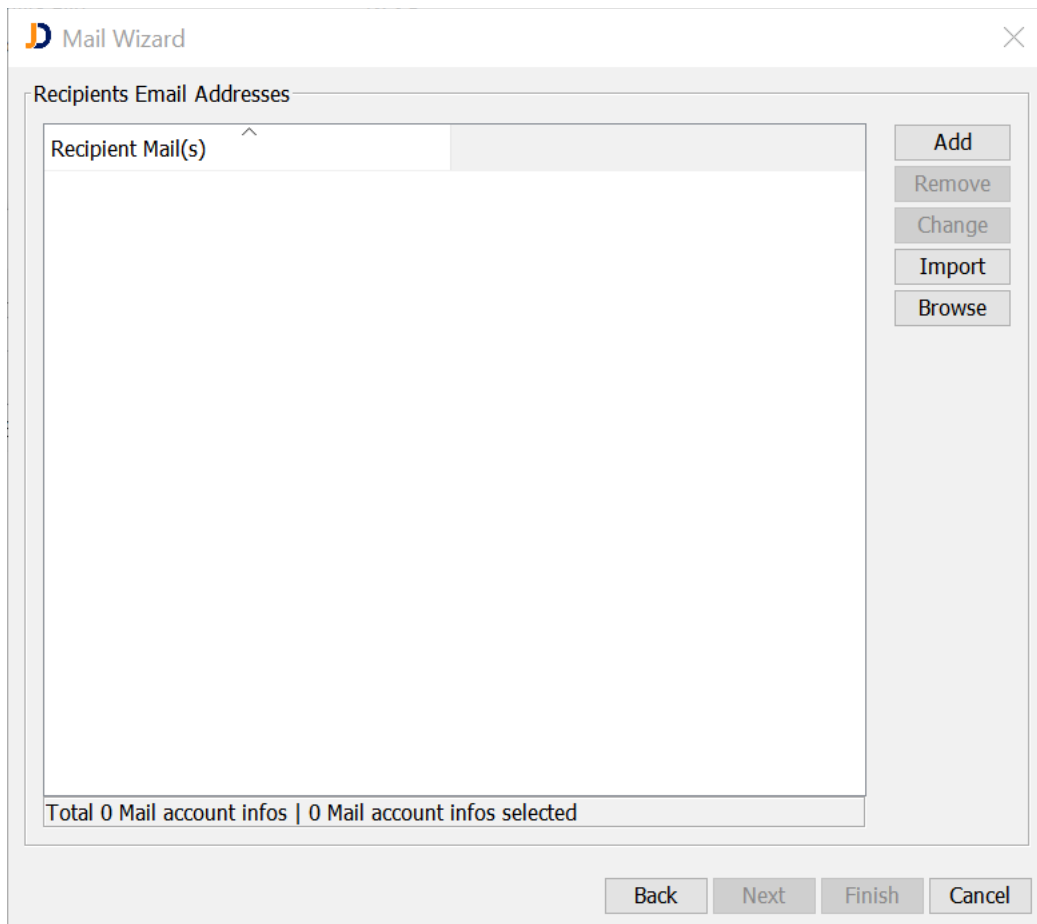


Fig: Add the Mail Recipients

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.

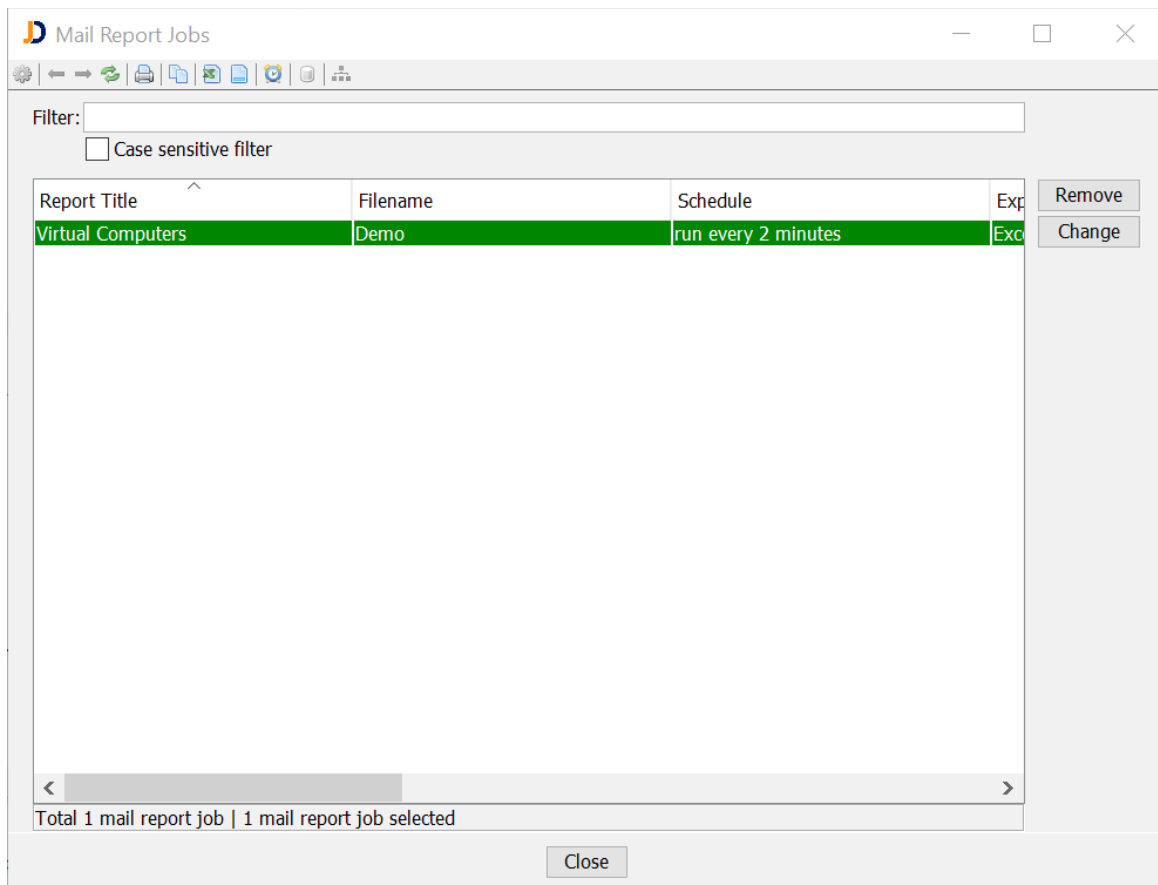


Fig: Manager your scheduled Mail Jobs

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.

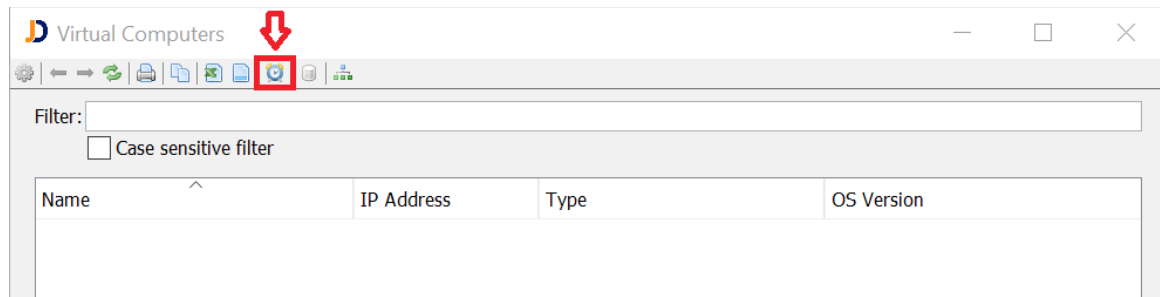


Fig: Schedule report export

And then from the opened menu select the *Export report to disk* option.

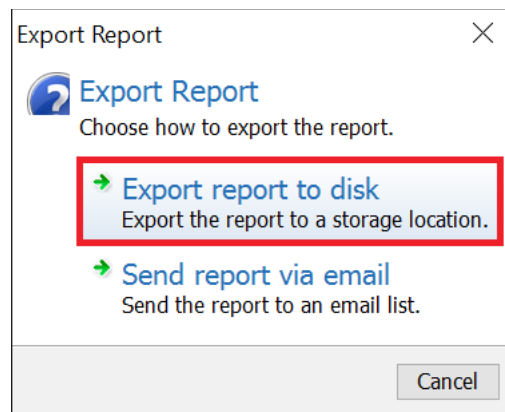


Fig: Export report options menu

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.

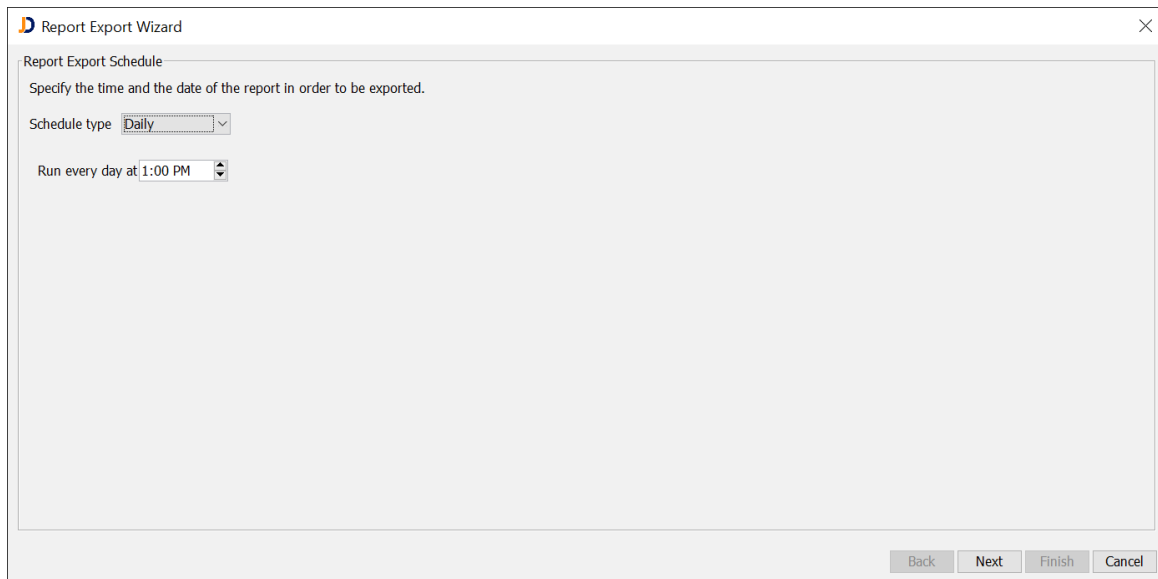
The screenshot shows a window titled "Report Export Wizard" with a close button (X) in the top right corner. The main area is labeled "Report Export Schedule" and contains the instruction "Specify the time and the date of the report in order to be exported." Below this, there is a "Schedule type" dropdown menu currently set to "Daily". Underneath, it says "Run every day at:" followed by a time selection field set to "1:00 PM". At the bottom right of the window, there are four buttons: "Back", "Next", "Finish", and "Cancel".

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)

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.

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 Dialog This 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.

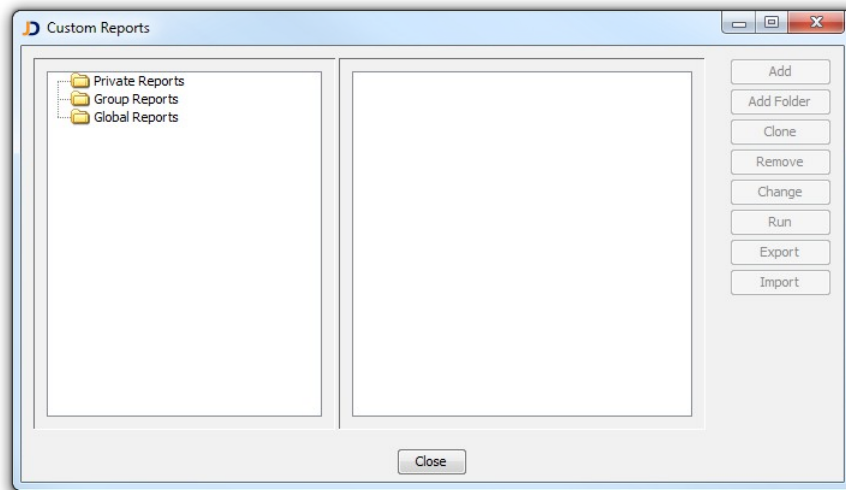


Figure: Custom Reports Dialog

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*.

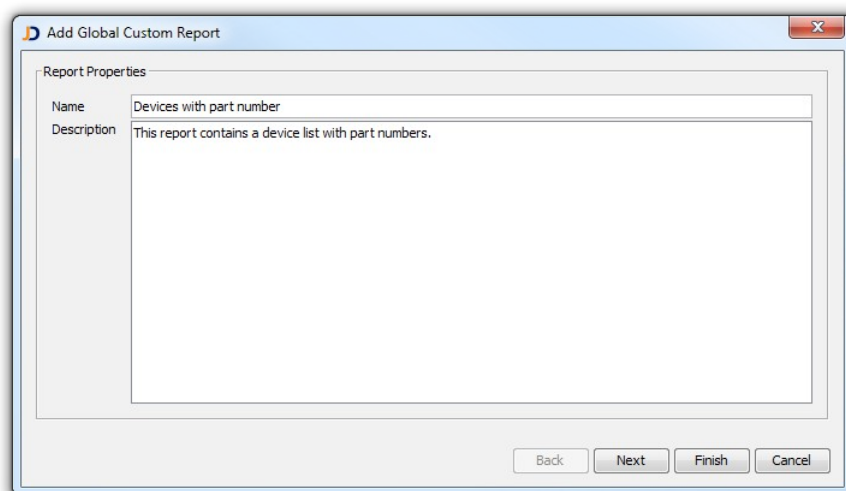


Figure: Custom Report Name and Description

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.

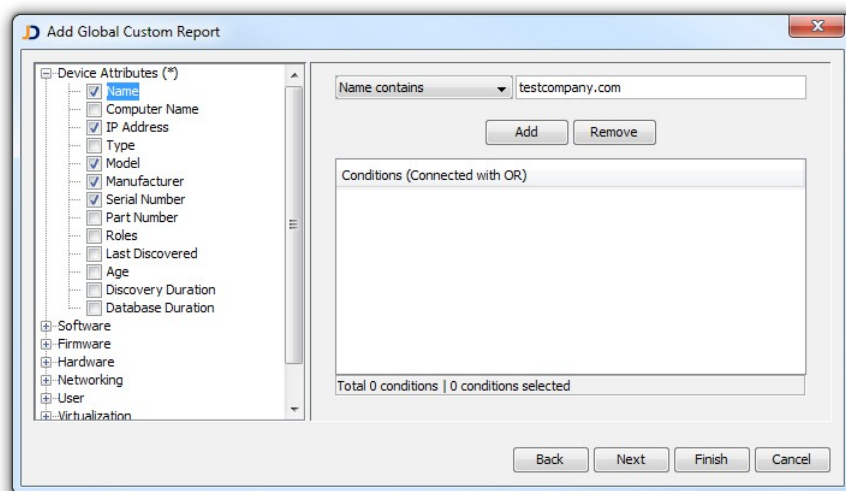


Figure: Custom Report Attributes

Click *Next* to change the attribute order, if desired. Use *Move up* and *Move down* to change the attribute order as desired.

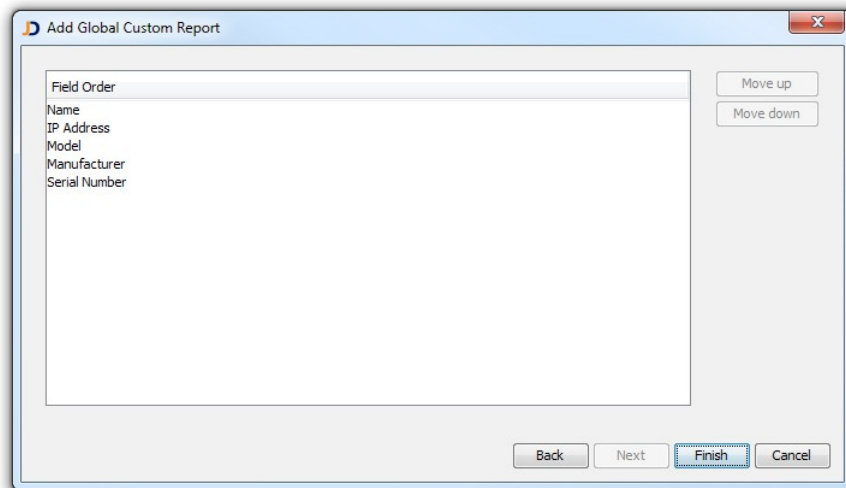


Figure: Attribute Order

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.

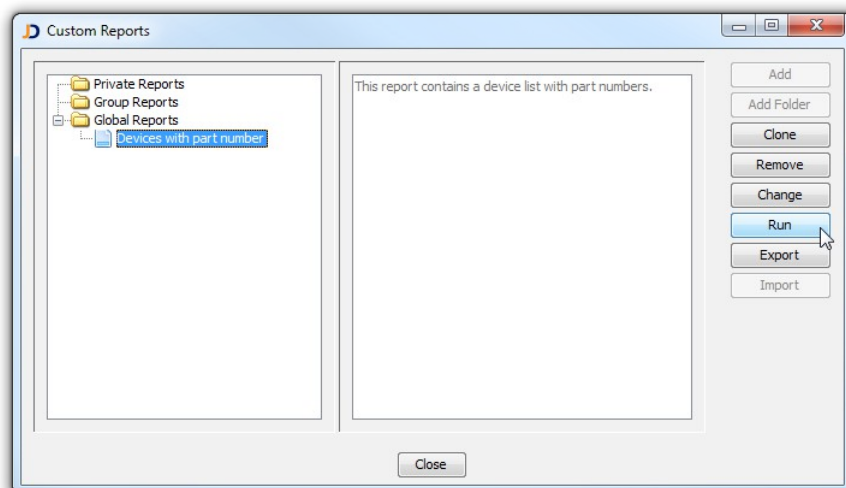


Figure: Run a Custom Report

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.

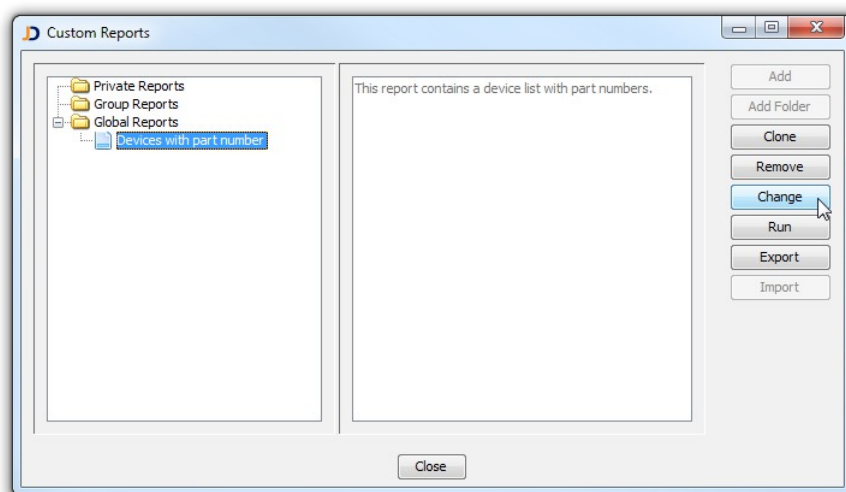


Figure: Change existing Reports

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.

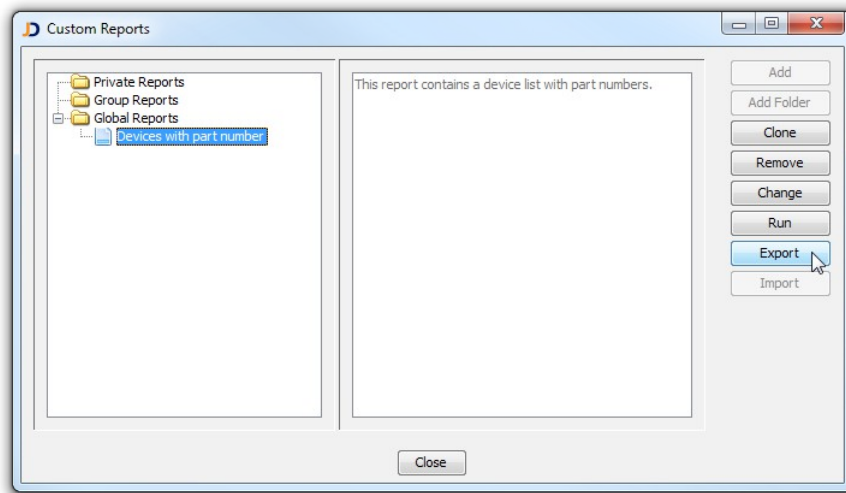


Figure: Export a Custom Report

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.

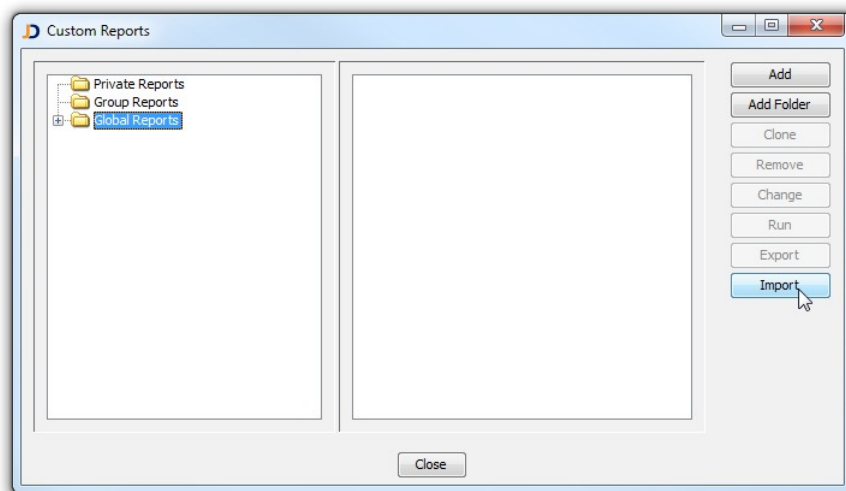


Figure: Import a Custom Report

7 WMI/WBEM Browser

7.1 Background

The WBEM (**W**eb **B**ased **E**nterprise **M**anagement) 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 (**W**indows **M**anagement **I**nstrumentation) 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.

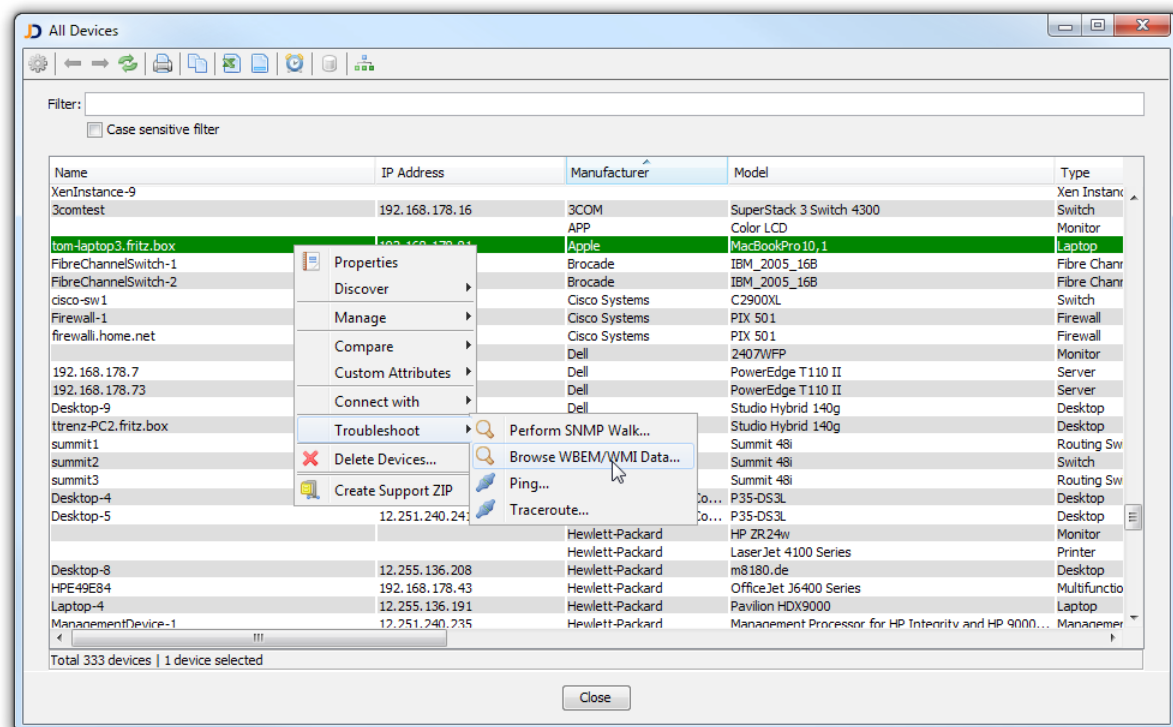


Figure: Open WMI/WBEM Browser from the device report's context menu

This menu item opens the browser window.

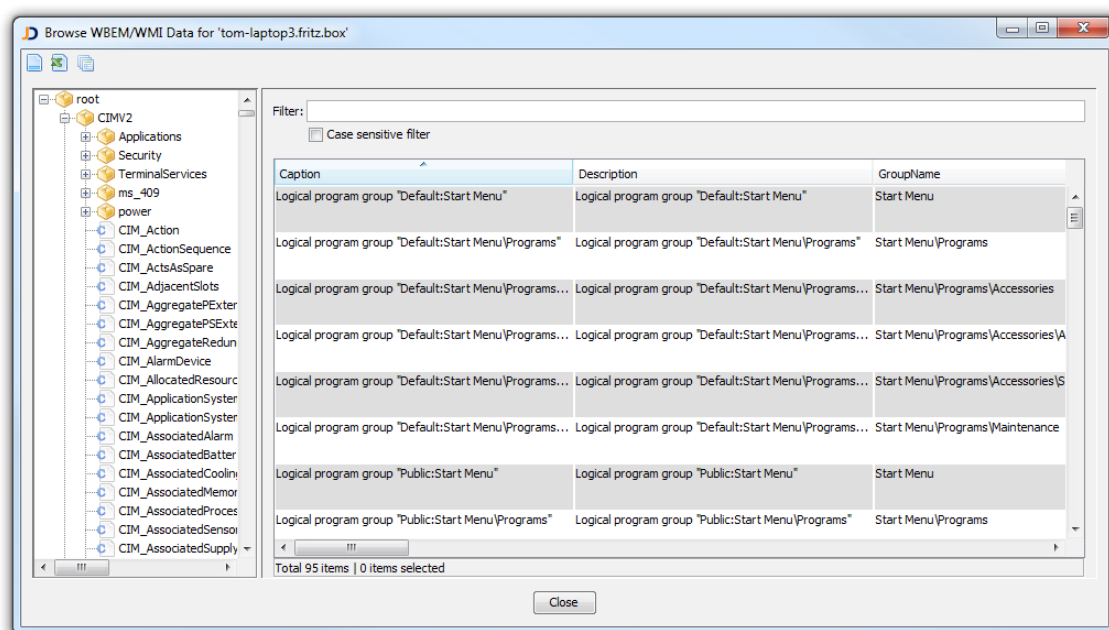


Figure: WMI/WBEM browser window

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.

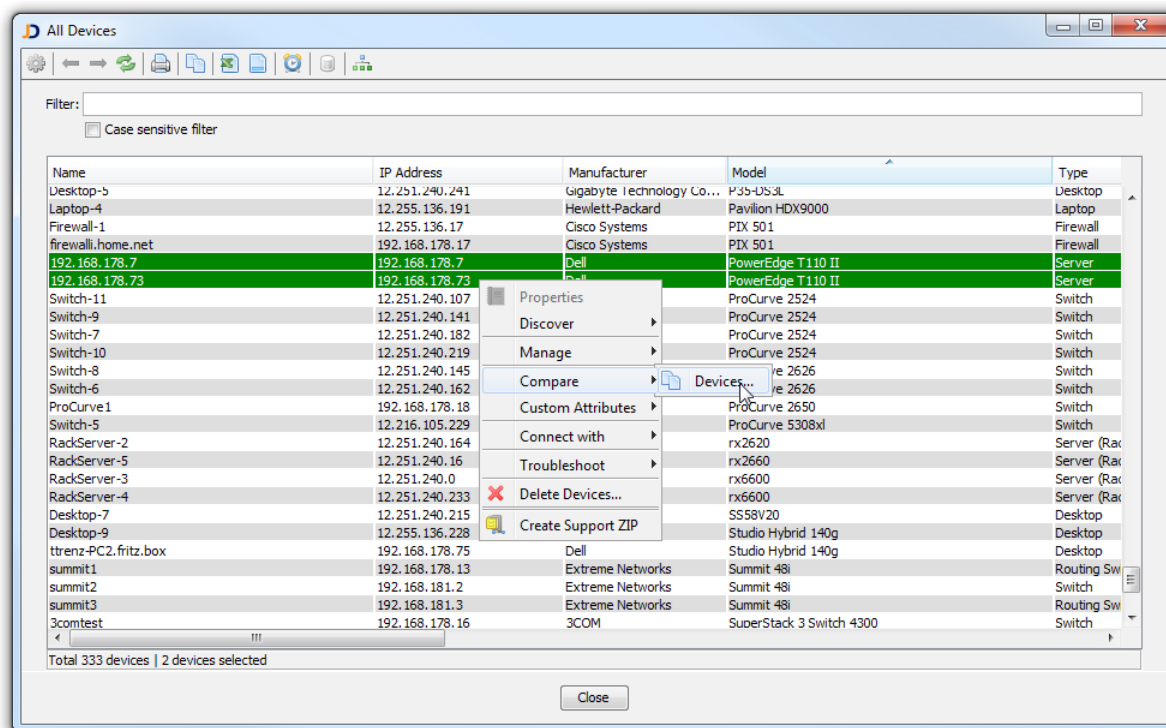


Fig: Open the device compare dialog

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.

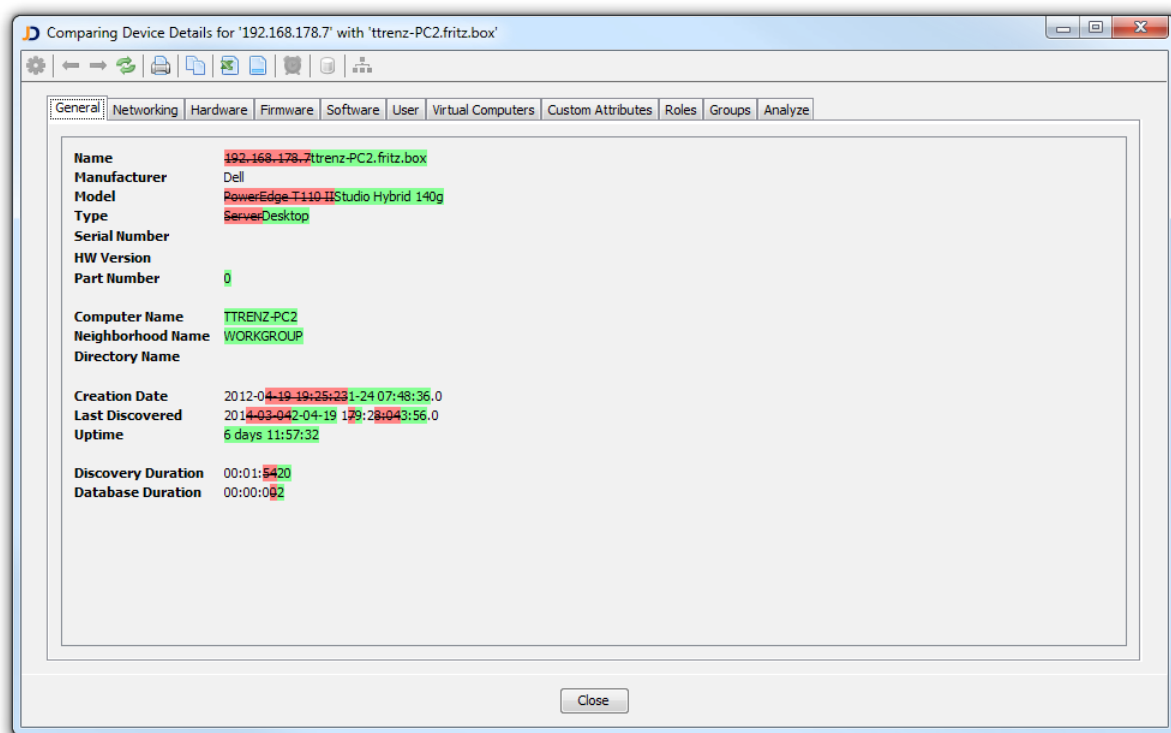


Fig: Compare report of the operating system tab

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.

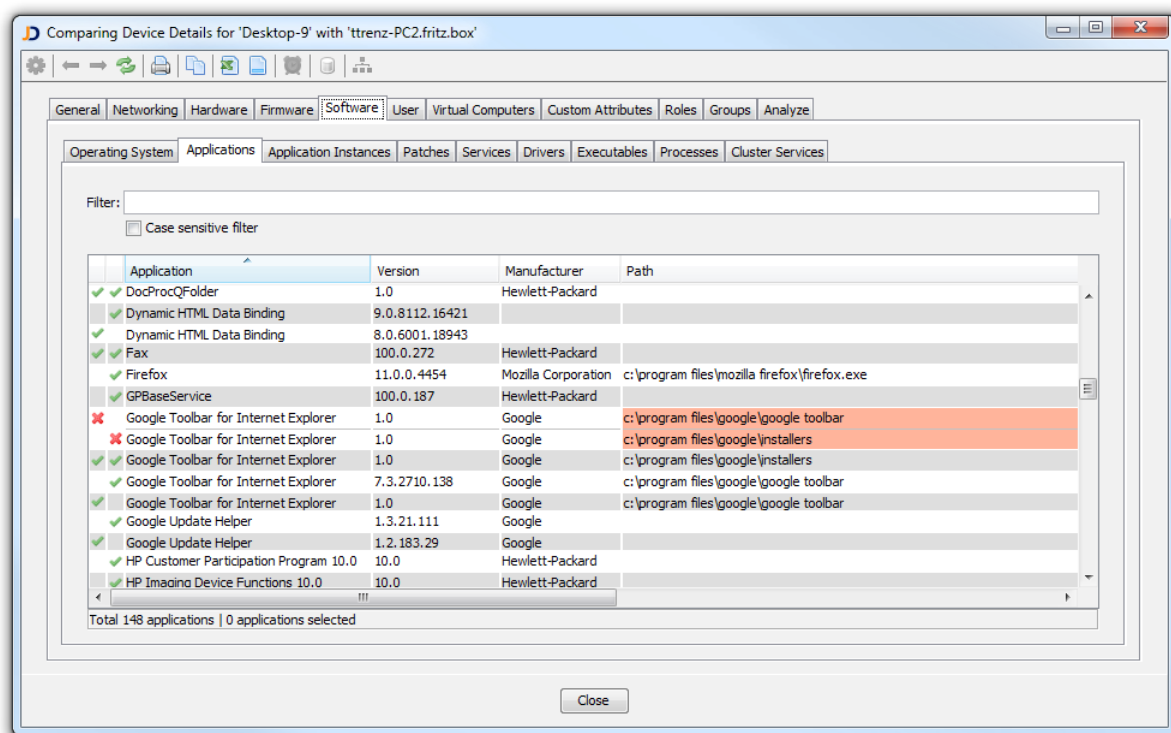


Fig: Differences in a table based report

9 Custom Attributes

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.

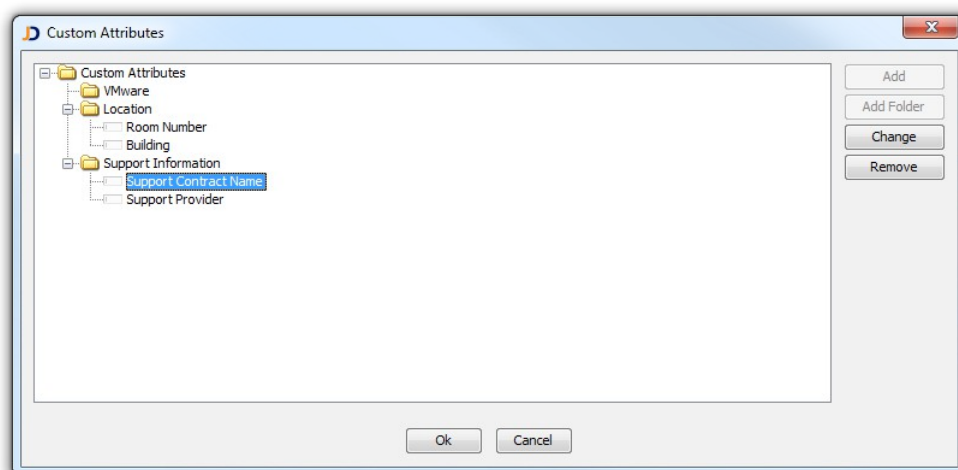


Figure: Custom Attributes Configuration Dialog

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:



Figure: Edit Custom Attributes

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 keep 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.

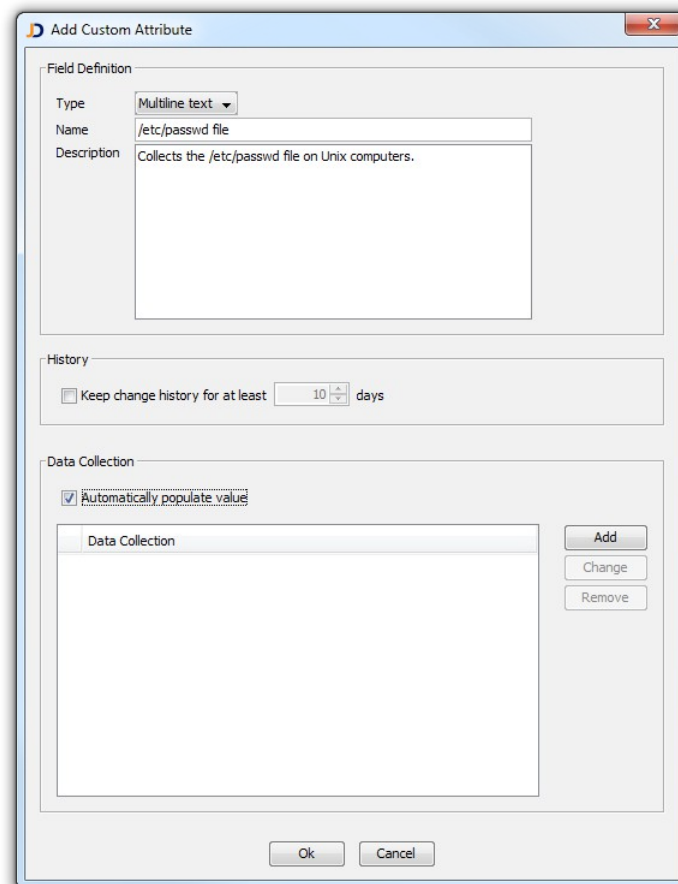


Figure: Enable automatic Data Collection

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.

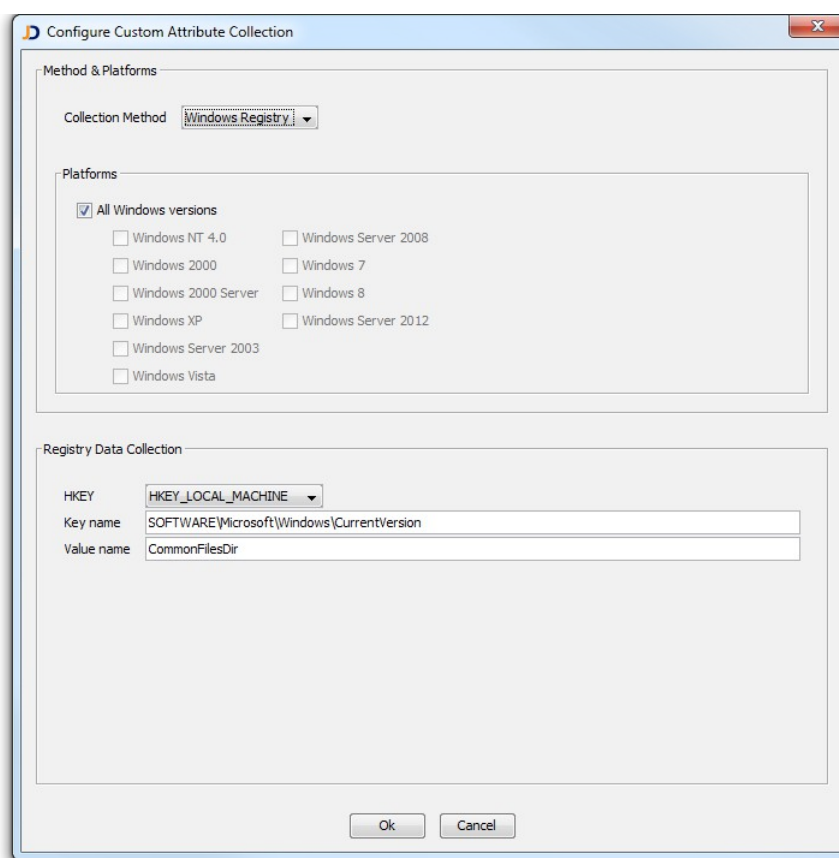


Figure: Windows Registry Custom Attribute Data Collection

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 ls 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.

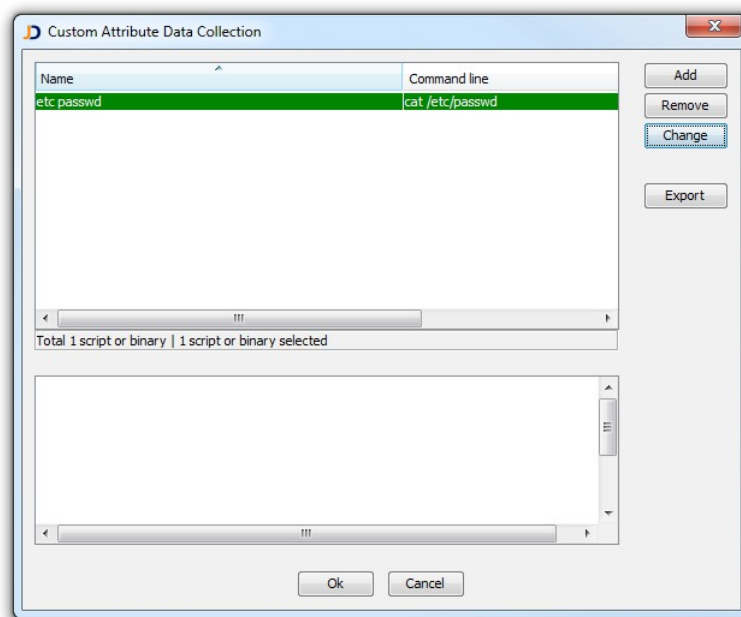


Figure: Configure Custom Attribute Data Collections

!!!! BE CAREFUL !!!!

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

execution).

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.

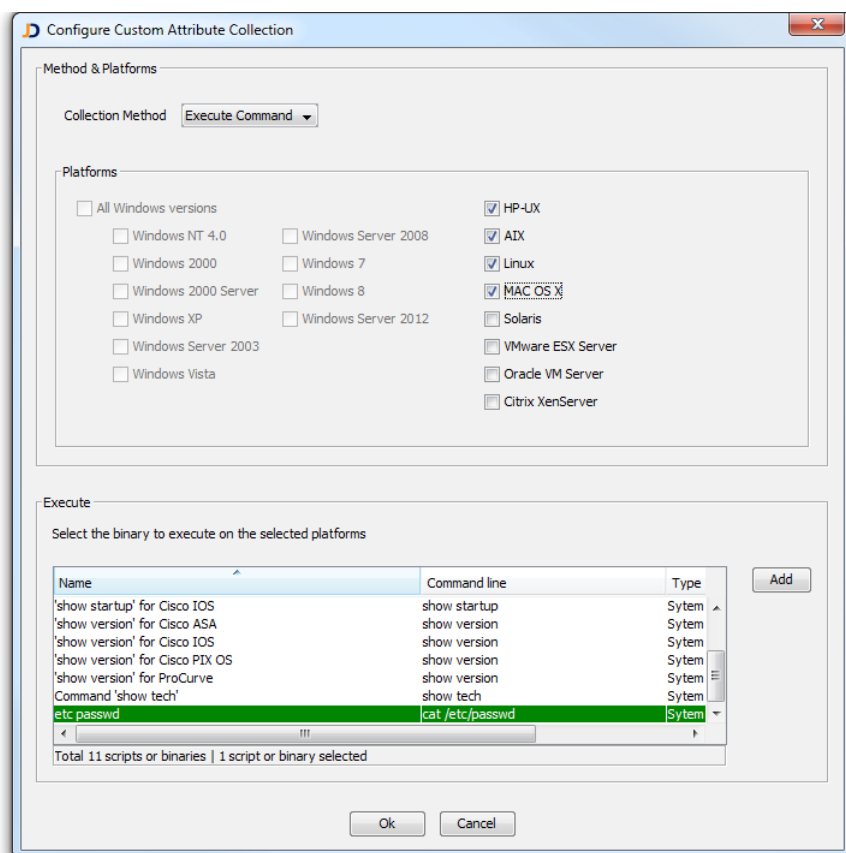


Figure: Configure Custom Attribute Data Collection

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.

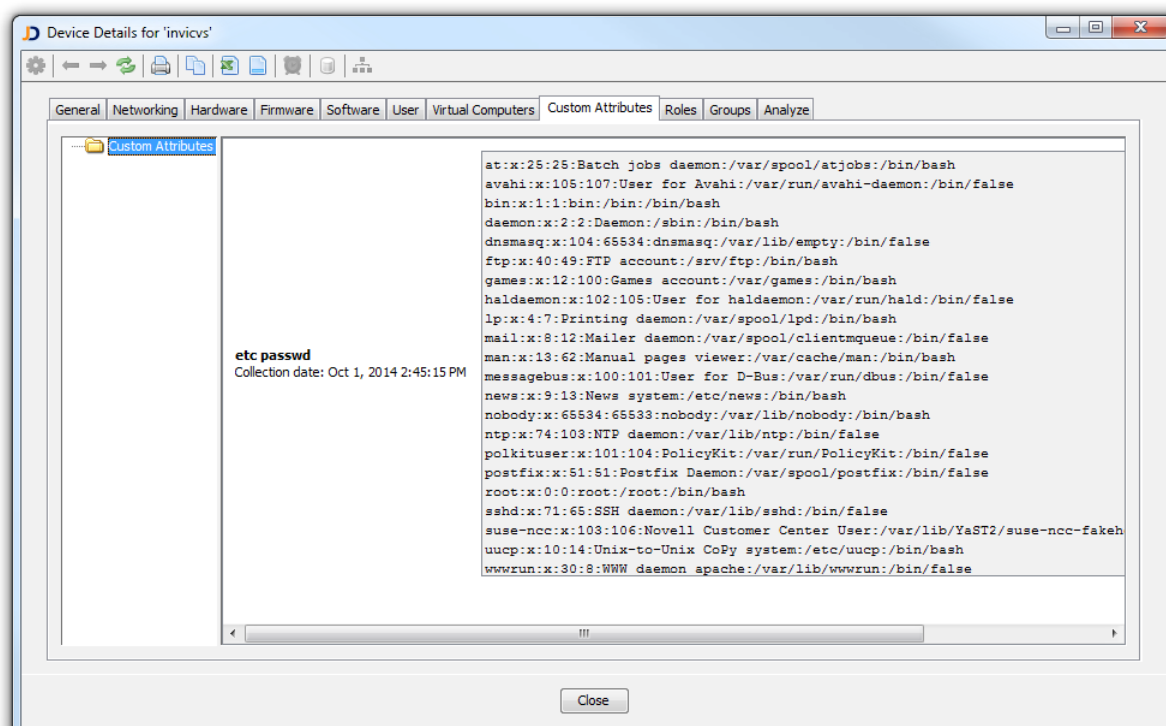


Figure: Data Collection with 3 Revisions

Click the revisions link to open a new dialog displaying all collected revisions including their values. Select a date to review the custom attribute value from that time.

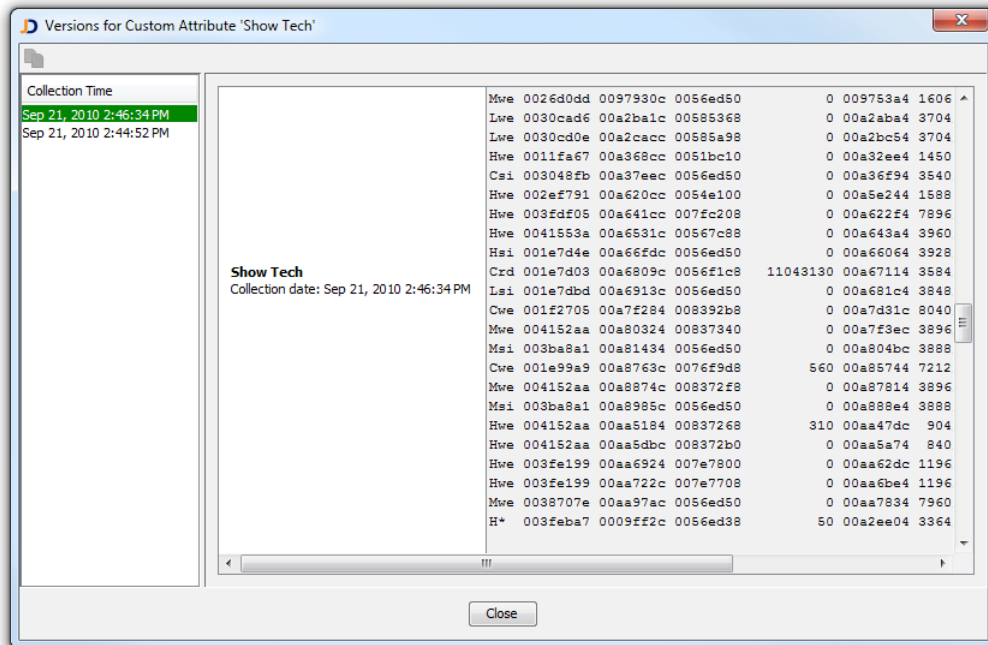



Figure: Versions with Collection Data for Attribute 'Show Tech'

Select two revisions and click the Compare button  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.

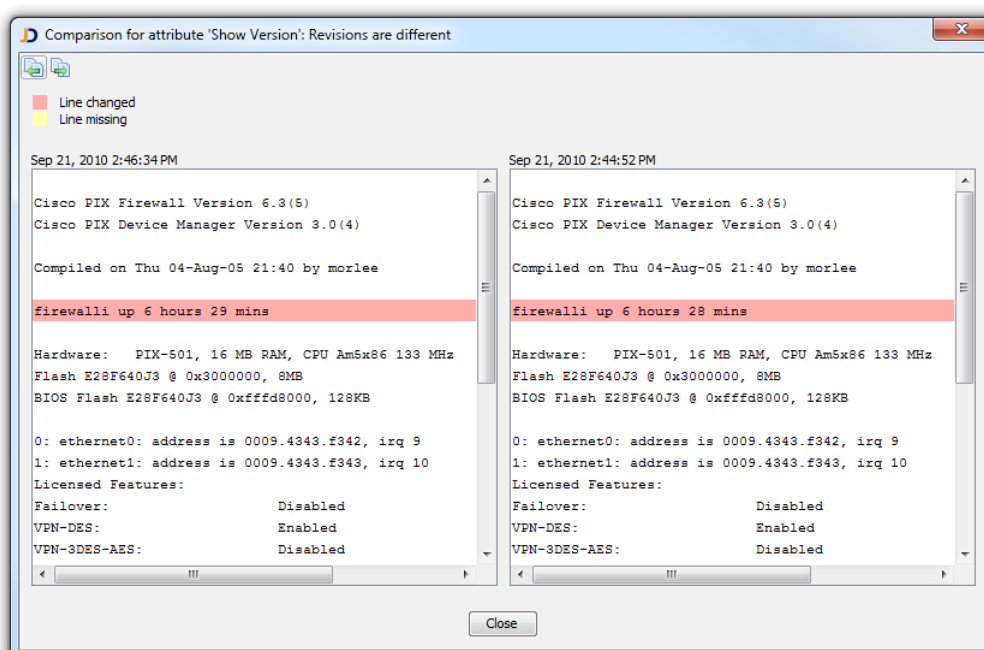


Figure: Comparison Report

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.

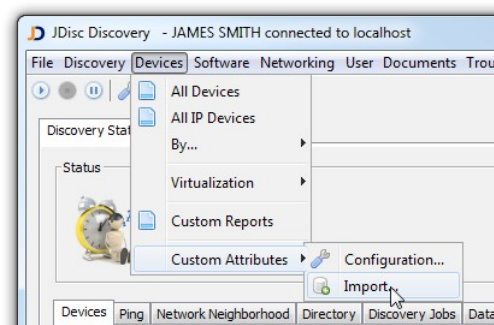


Figure: Import Custom Attribute values

Select the custom attribute that you would like to import.

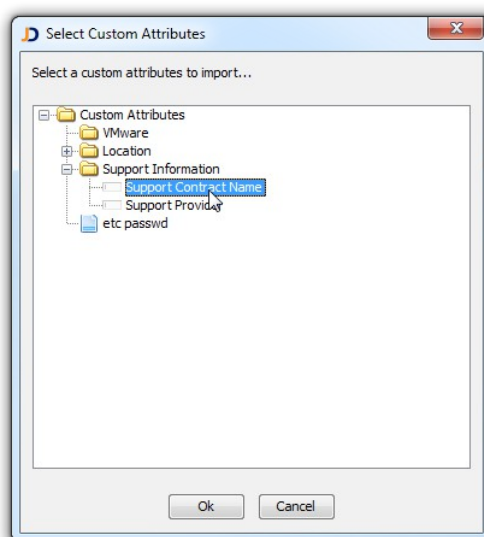


Figure: Select a Custom Attribute to import

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.

Device	Status	Line	Result
192.168.178.4	✓	1	Successfully identified 'cisco-sw1
192.168.178.17	✓	2	Successfully identified 'firewall1.home.net
192.168.178.18	✓	3	Successfully identified 'ProCurve1
trenz-pc2	✓	4	Successfully identified 'trenz-PC2.fritz.box
trenz-pc	✓	5	Successfully identified 'trenz-PC2.fritz.box
Diddel Daddel	✗	6	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 starts with 'Diddel Daddel'.
<no identifier>	✗	7	No device value pair found!
<no identifier>	✗	8	No device value pair found!
192.168.178.4	✓	9	Successfully identified 'cisco-sw1
192.168.178.17	✓	10	Successfully identified 'firewall1.home.net
192.168.178.18	✓	11	Successfully identified 'ProCurve1
trenz-pc2	✓	12	Successfully identified 'trenz-PC2.fritz.box
trenz-pc	✓	13	Successfully identified 'trenz-PC2.fritz.box
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 where hostname starts with 'Diddel Daddel'.
<no identifier>	✗	15	No device value pair found!
<no identifier>	✗	16	No device value pair found!
192.168.178.4	✓	17	Successfully identified 'cisco-sw1
192.168.178.17	✓	18	Successfully identified 'firewall1.home.net
192.168.178.18	✓	19	Successfully identified 'ProCurve1
trenz-pc2	✓	20	Successfully identified 'trenz-PC2.fritz.box

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.

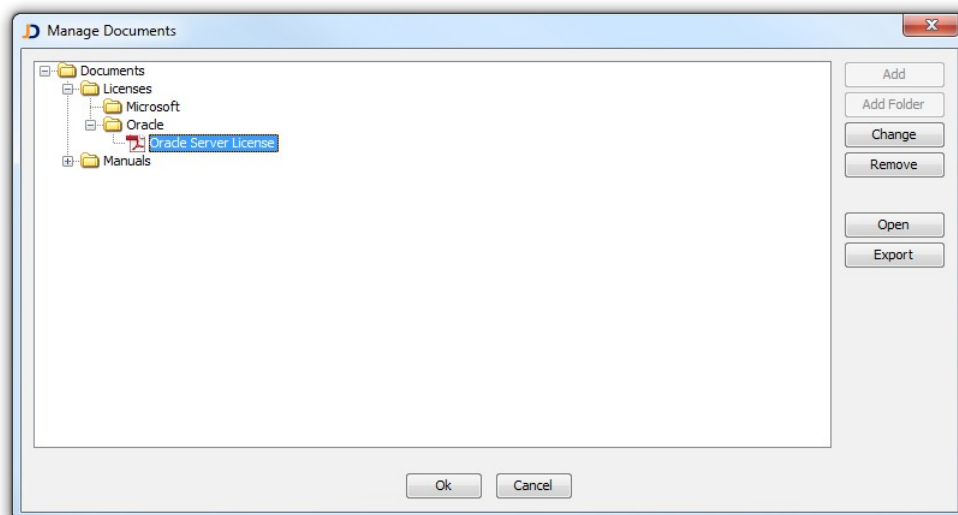


Figure: Manage Documents Dialog

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.

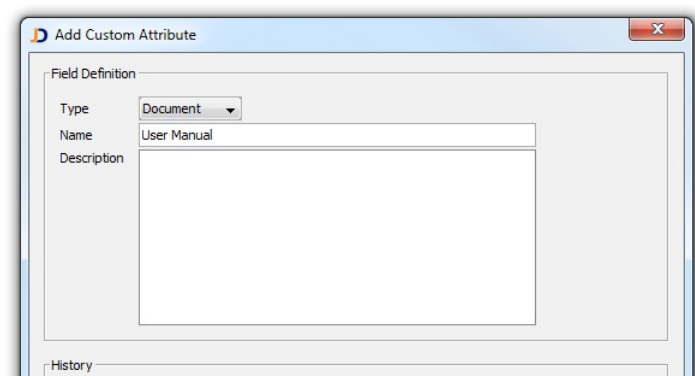


Figure: Add a new Custom Attribute of Type *Document*

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.

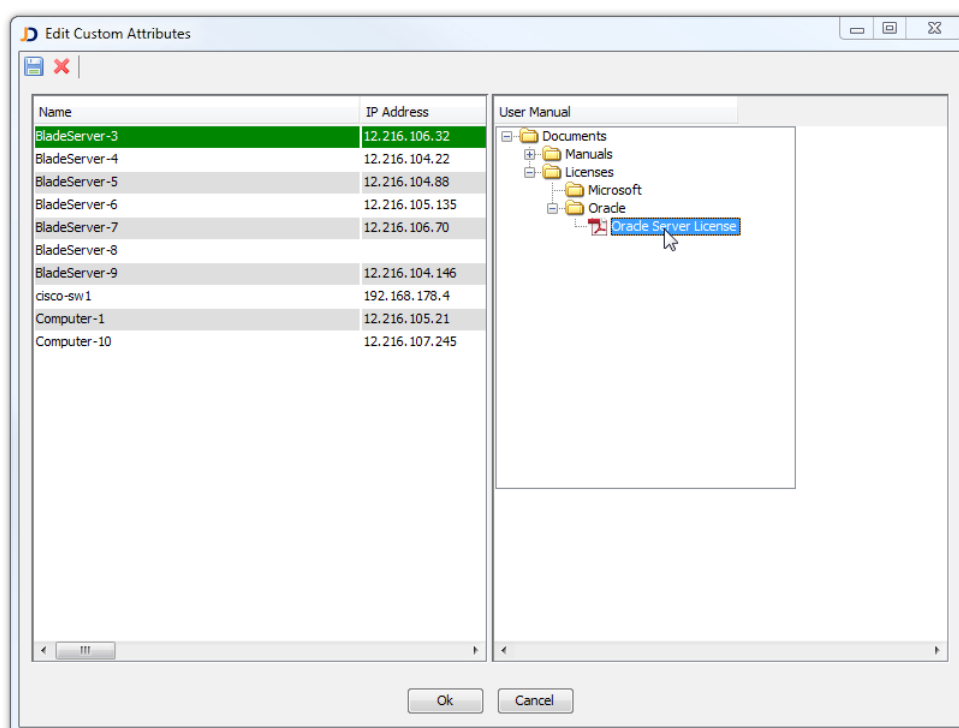


Figure: Edit Document Custom Attributes

JDisc Discovery opens the document hierarchy 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

the device.

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.

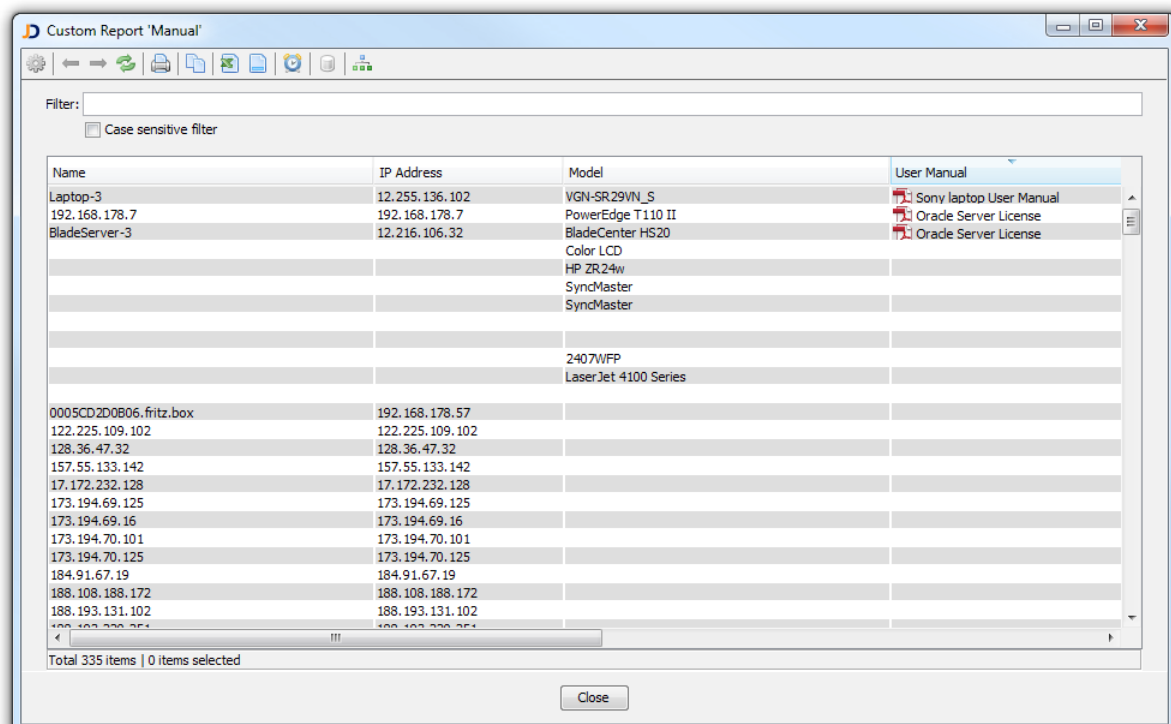


Figure: Custom Report with a Document

Double-click the document icon cell to open the document. Documents appear as any other custom attribute in the *Custom Attributes* tab.

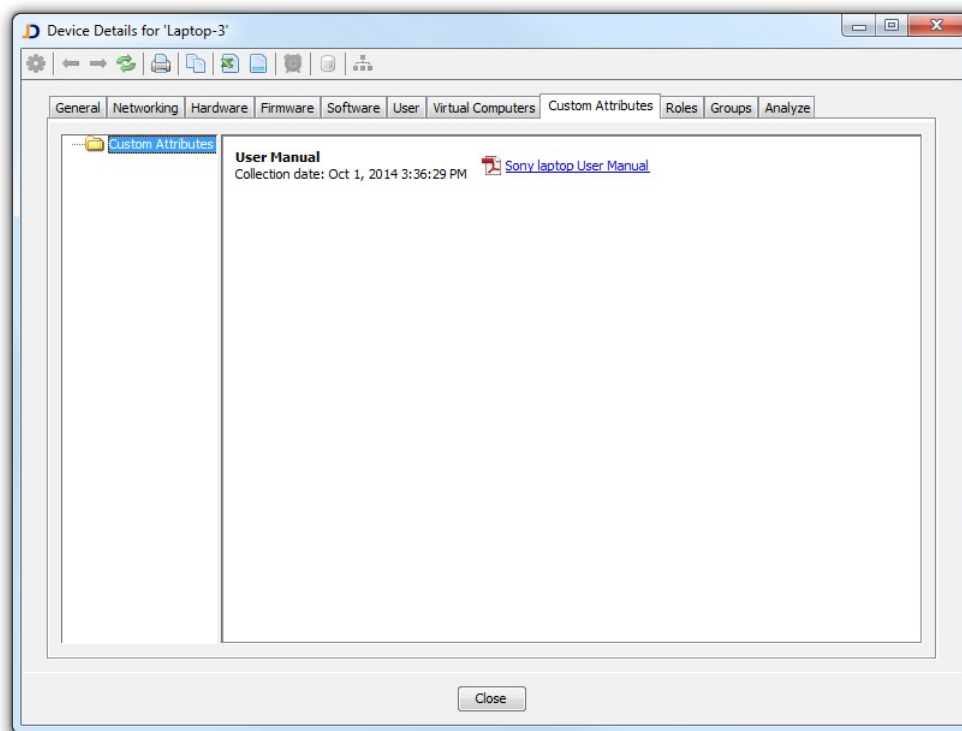


Figure: Document Custom Attribute within the Device Details Dialog

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

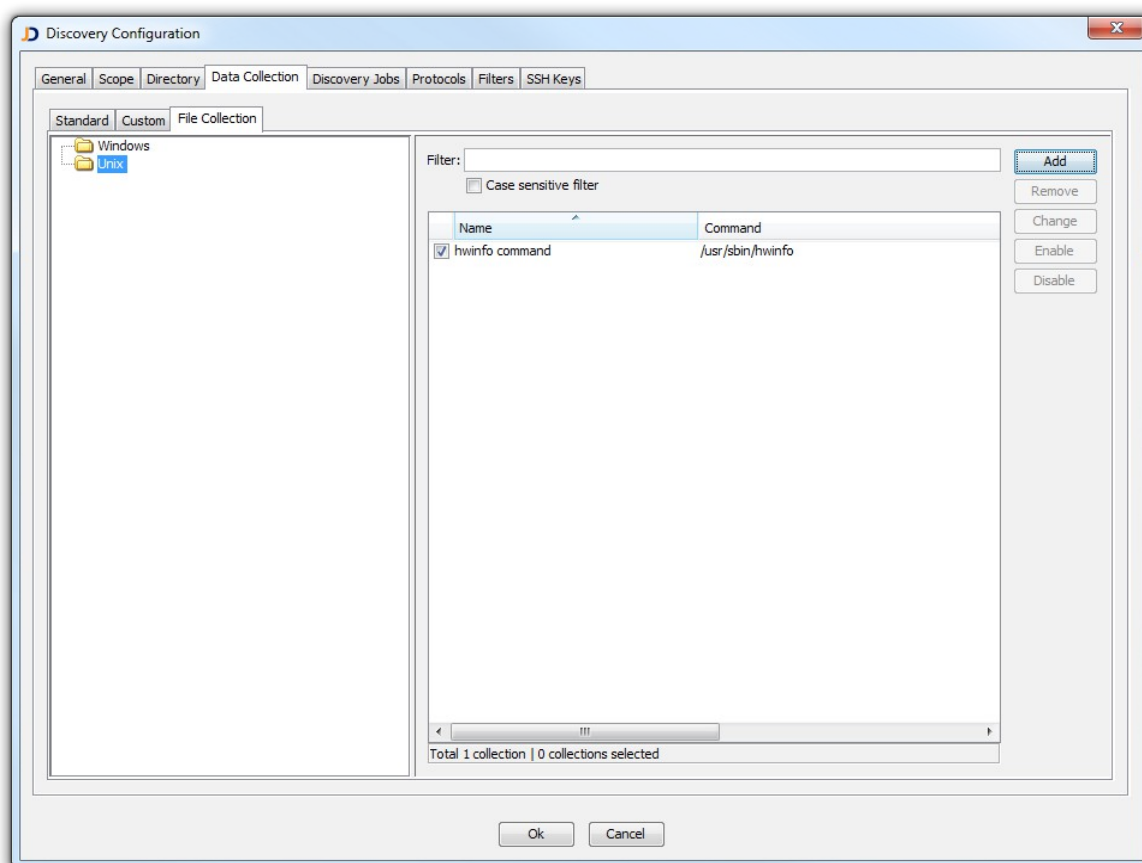


Figure: File Collections

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.

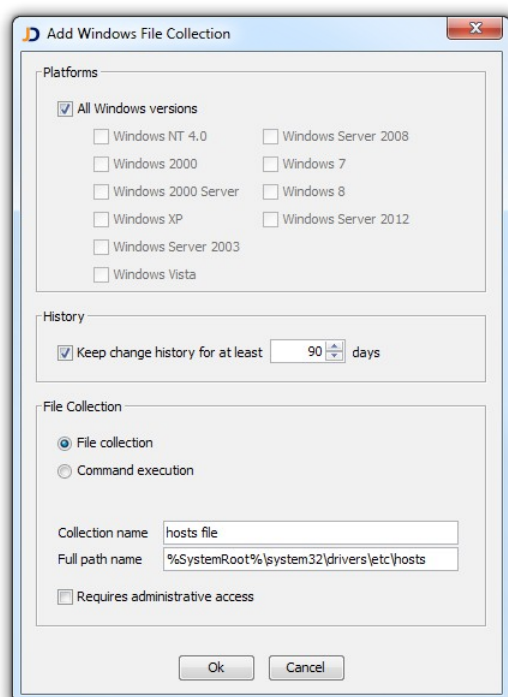


Figure: Add Windows File Collection

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>
</software>
```

```

<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 .

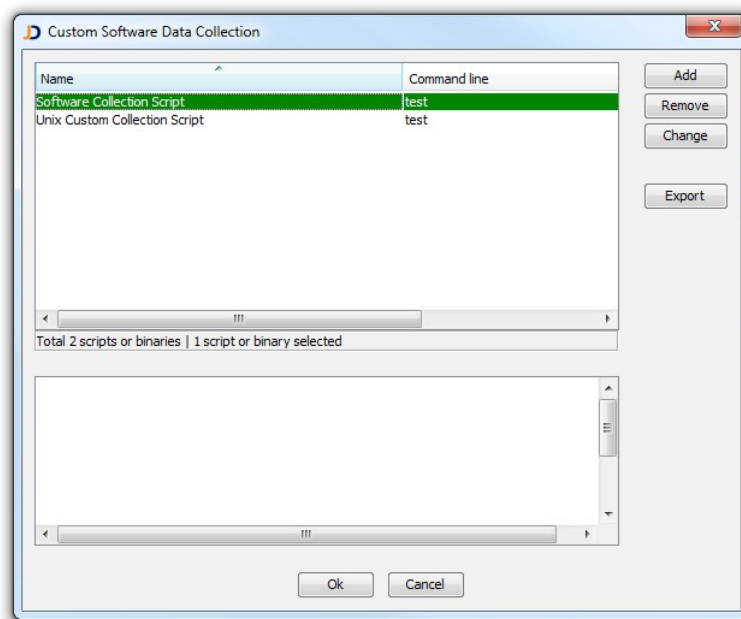


Figure: Configure Custom Software Data Collection

!!!! 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.

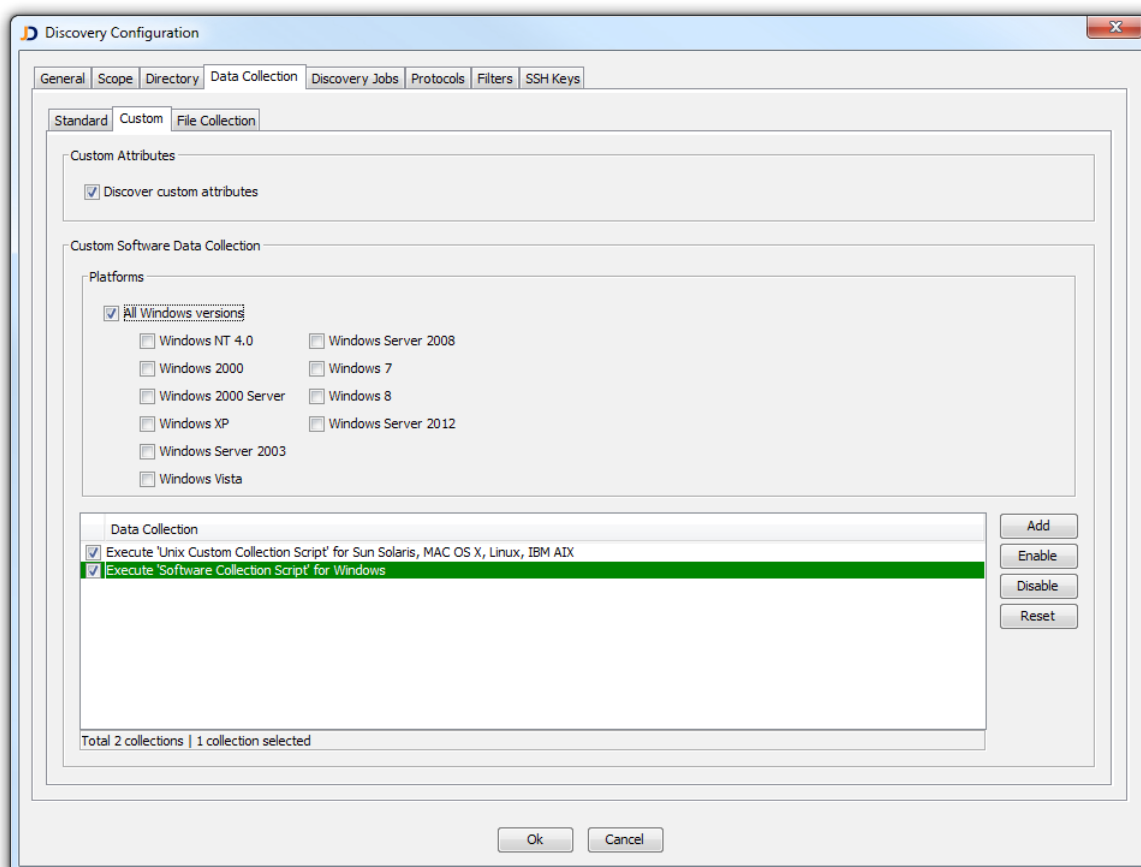


Figure: Configure Custom Software Data Collection

You can run multiple custom software data collection scripts for a operating system platform.

13 Troubleshooting

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.

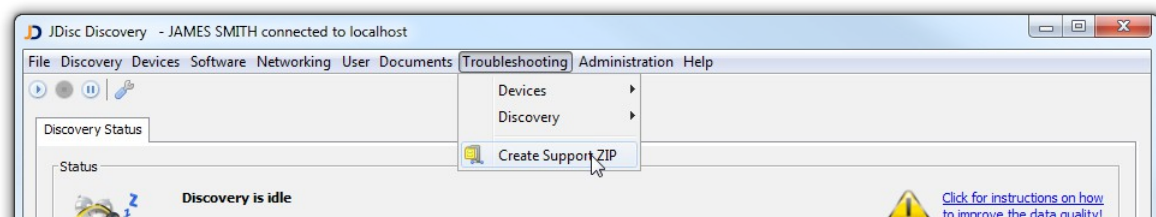


Figure: Create a product support ZIP file

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.

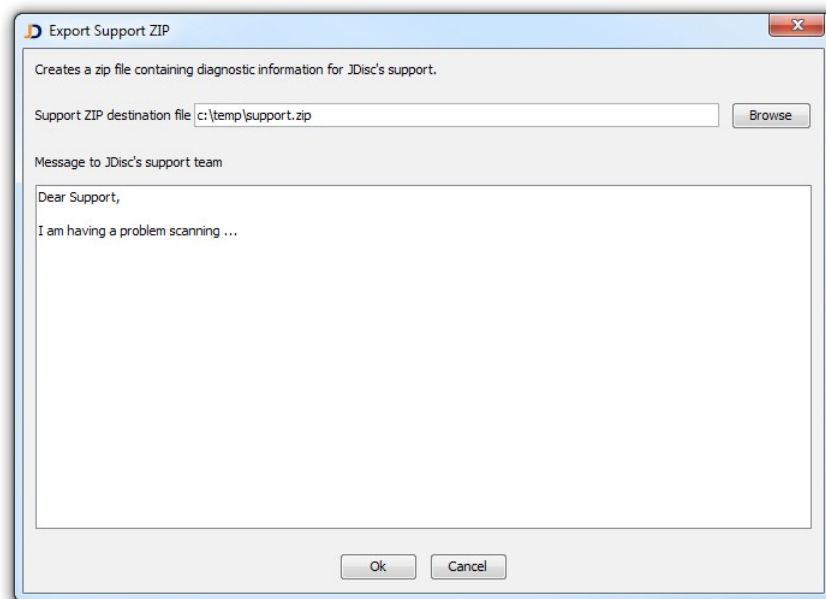


Figure: Export a Support ZIP file

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.

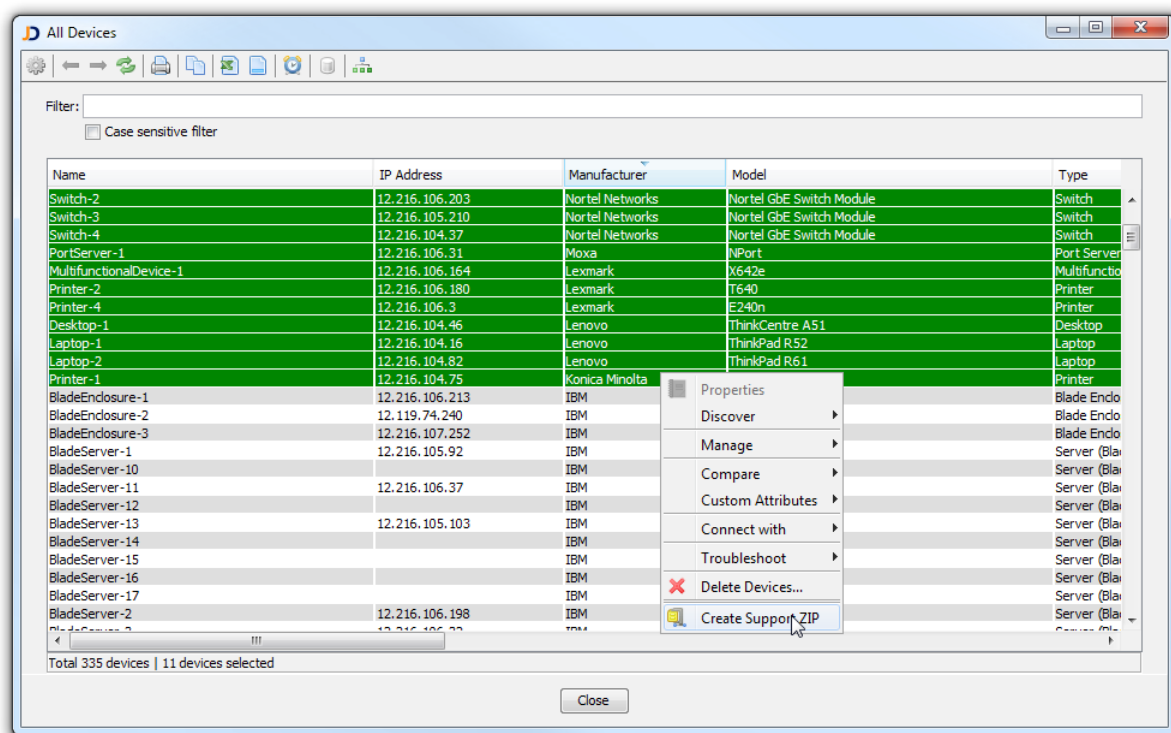


Figure: Create a device support ZIP file

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.

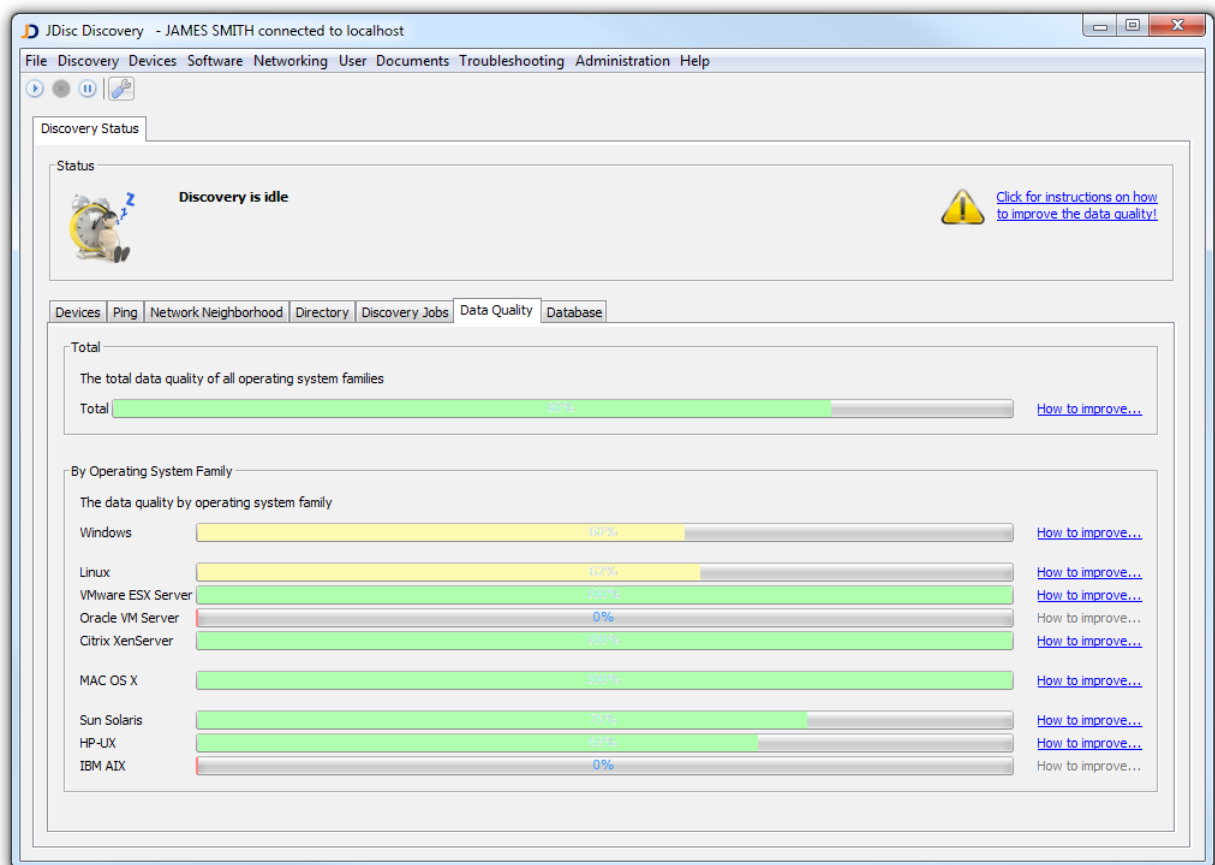


Figure: Data Quality Tab

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.

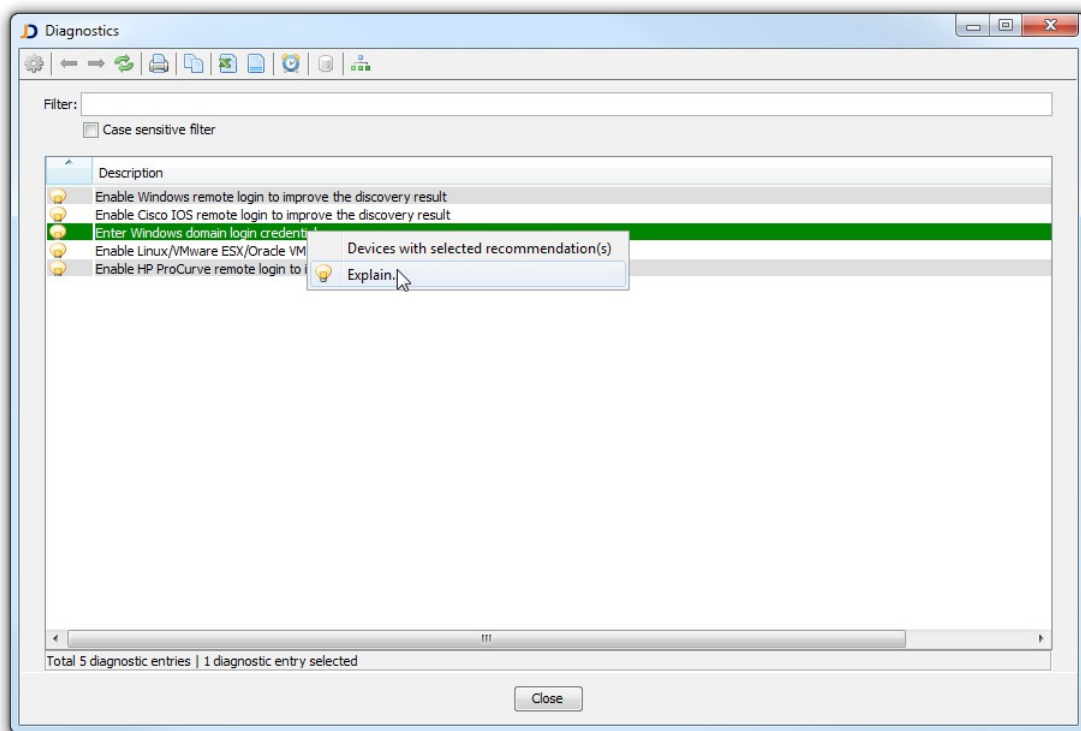


Figure: Diagnostics Report

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.

The screenshot shows a window titled "Discovery Protocol Status". It contains a table with four columns: "Protocol", "Success", "Warning", and "Error". The table lists 17 protocols and their corresponding counts. At the bottom, it states "Total 17 protocols | 0 protocols selected" and has a "Close" button.

Protocol	Success	Warning	Error
DNS	7	212	33
HTTP	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.

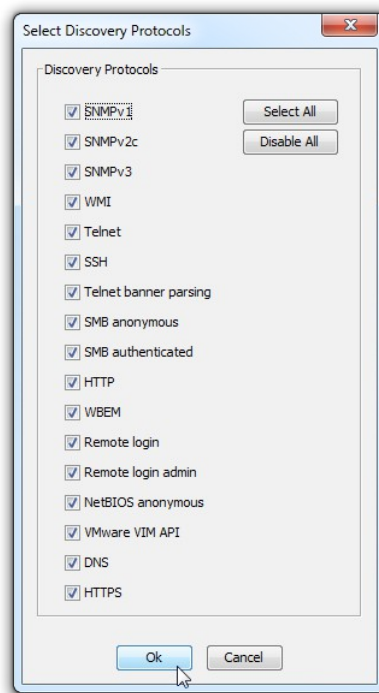


Figure: Discovery Protocols Selection Dialog

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.

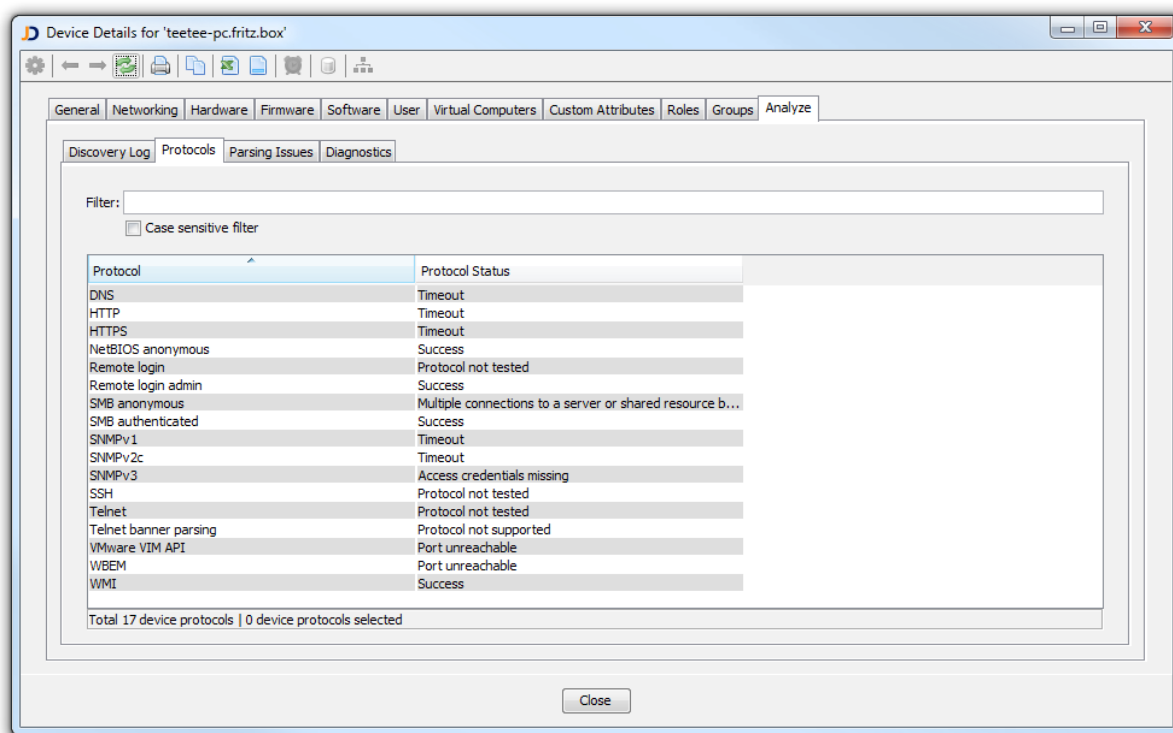


Figure: Protocols Tab displaying the Protocol Status for a single Device

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 email-address. 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.

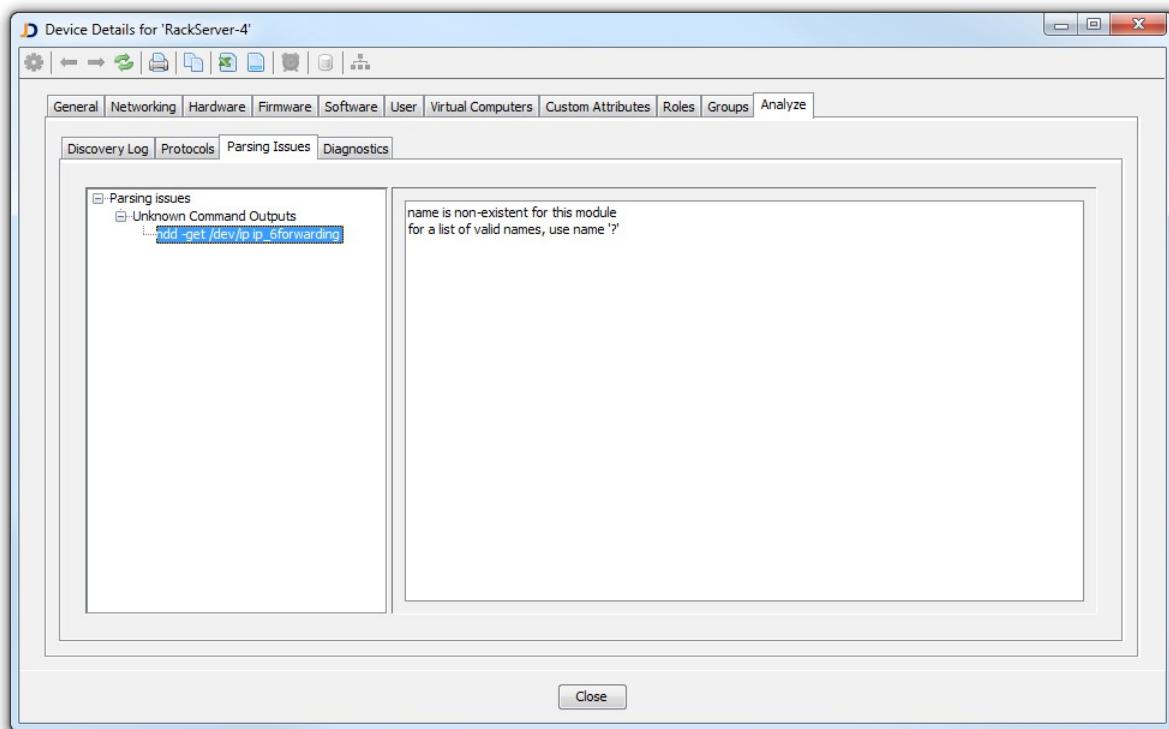


Figure: Unknown Telnet Banner Report

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.

14 Open Source

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 (<http://www.apache.org>). 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' (<http://www.famfamfam.com/lab/icons/silk>).
- This product includes Kai Toedter's 'Jcalendar' (<http://www.toedter.com/en/jcalendar/index.html>).
- This product includes the JUNG layout library (<http://jung.sourceforge.net>).
- This product includes the COLT numeric library (<http://acs.lbl.gov/~hoschek/colt>).
- This product uses the Postgres database (<http://www.postgresql.org>).
- This product uses SNMP4J (<http://www.snmp4j.org>).
- This product uses the Ganymed SSH library (<http://www.ganymed.ethz.ch/ssh2>).
- This product uses the drools rule engine (<http://jboss.org/drools>).
- This product uses the janino compiler (<http://www.janino.net>).
- This product uses Jython (<http://www.jython.org/Project>).
- The product calls the dmidecode binary (<http://www.nongnu.org/dmidecode>).
Find the source code in the 'sources' directory.
- This product uses icons from 'Crystal Clear' (http://commons.wikimedia.org/wiki/Crystal_Clear).
- This product uses the 'PUTTY' ssh client.
- This product uses the dom4j library (<http://dom4j.sourceforge.net/dom4j-1.6.1>).
- This product uses the Jaxen library (<http://jaxen.org/>)

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