JDisc

360° Network Inventory | Topology | Relations

JDisc Discovery 4.0

Evaluation Guide

Legal Notice

JDisc UG (haftungsbeschränkt) 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 out of the use of this information remains with recipient. In no event JDisc UG (haftungsbeschränkt) shall 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 UG (haftungsbeschränkt) has been advised of the possibility of such damages. The foregoing shall apply regardless of the negligence or other fault 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 UG (haftungsbeschränkt) 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 UG (haftungsbeschränkt) may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

JDisc UG (haftungsbeschränkt)
Kuppinger Weg 25
D-71116 Gärtringen
Germany

Document and Printing History

New editions are complete revisions of the manual. The printing dates for each edition are listed below.

Version	Date
1.1	January 2010
1.2	July 2010
2.0	October 2010
2.5	December 2011
2.6	April 2012
2.7	June 2012
2.8	October 2012
2.9	February 2013
3.0	September 2013
3.1	March 2014
3.2	November 2014
3.3	December 2015

Contents

1 Introduction

JDisc Discovery is a high-end network inventory solution that does not need to deploy agents on the target computers. Most, but unfortunately not all environments, are a good fit for JDisc Discovery. Because of that, it is important to test the software upfront in your environment.

The evaluation guide explains what is important during the evaluation and how to test specific features of the product.

The evaluation is divided into three sections. The first section explains how to get an extended evaluation license. The second part covers how to evaluate the discovery of different operating system platforms such as Windows, Unix, MAC OS X, or virtual servers such as VMware ESX servers. Finally, the last section explains how to test remote sites if there are any.

2 Evaluation

JDisc Discovery comes with a demo license for a maximum of 25 devices. The demo license is not time restricted. Although this is not required for initial tests, we recommend to request an enhanced demo license.

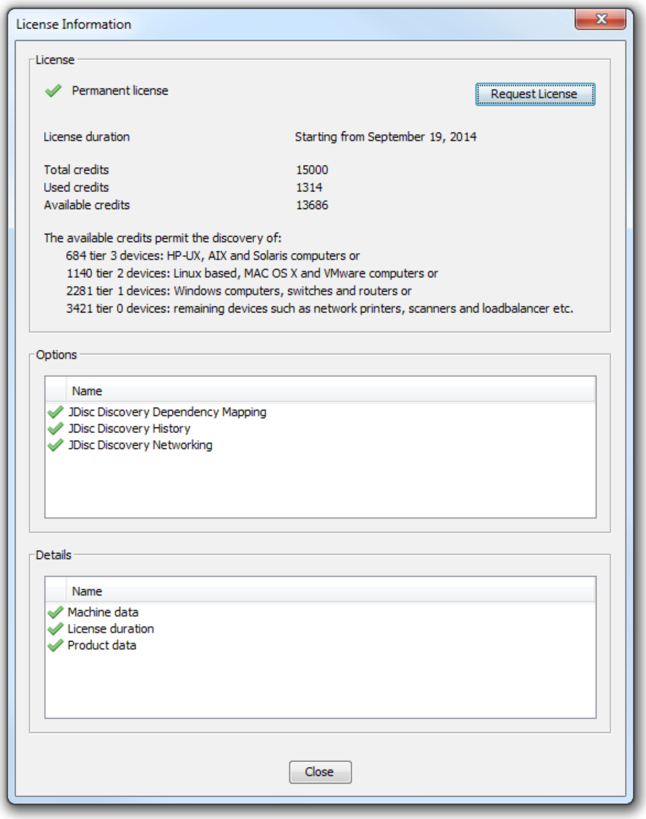
2.1 Free Support During The Evaluation Phase

JDisc offers free support during the evaluation phase. So don't hesitate to send your questions to support@jdisc.com.

2.2 Request An Enhanced Demo License

JDisc Discovery licenses are node locked to the computer on which the software runs. Therefore, you need to create a “license request file” that contains hardware and configuration information including the serial number and mac addresses.

To create a license request file, install JDisc Discovery. Once the software is installed, start the user interface and choose *Help » License Info*.



✓ Permanent license

License duration   Starting from September 19, 2014

Total credits   15000
Used credits   1314
Available credits   13686

The available credits permit the discovery of:
684 tier 3 devices: HP-UX, AIX and Solaris computers or
1140 tier 2 devices: Linux based, MAC OS X and VMware computers or
2281 tier 1 devices: Windows computers, switches and routers or
3421 tier 0 devices: remaining devices such as network printers, scanners and loadbalancer etc.

Name
✓ JDisc Discovery Dependency Mapping
✓ JDisc Discovery History
✓ JDisc Discovery Networking

Name
✓ Machine data
✓ License duration
✓ Product data

Figure: License Dialog

Click *Request License* to create a license request file. Send this file to support@jdisc.com along with the desired **number of devices** and we'll create an enhanced demo license that is valid for 2 weeks.

2.3 Run Your First Discovery

The installation procedure enables the local network for discovery. So let's start the first discovery by clicking the start button from JDisc Discovery's toolbar. Alternatively, you can start your first discovery from the *Discovery » Control » Start Discovery* menu item.

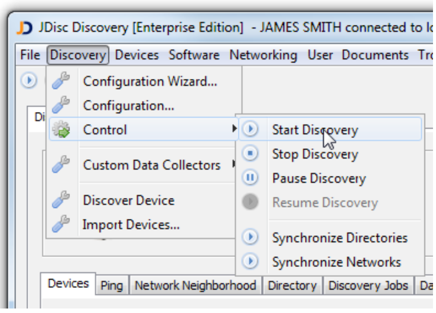
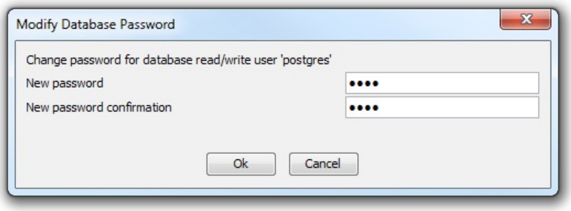


Figure: Start first Discovery Cycle

When the discovery is started for the first time, a dialog appears that prompts for the Windows domain or workgroup administrative account and password.



Modify Database Password

Change password for database read/write user 'postgres'

New password ••••

New password confirmation ••••

Figure: Enter the administrative account for your workgroup/domain

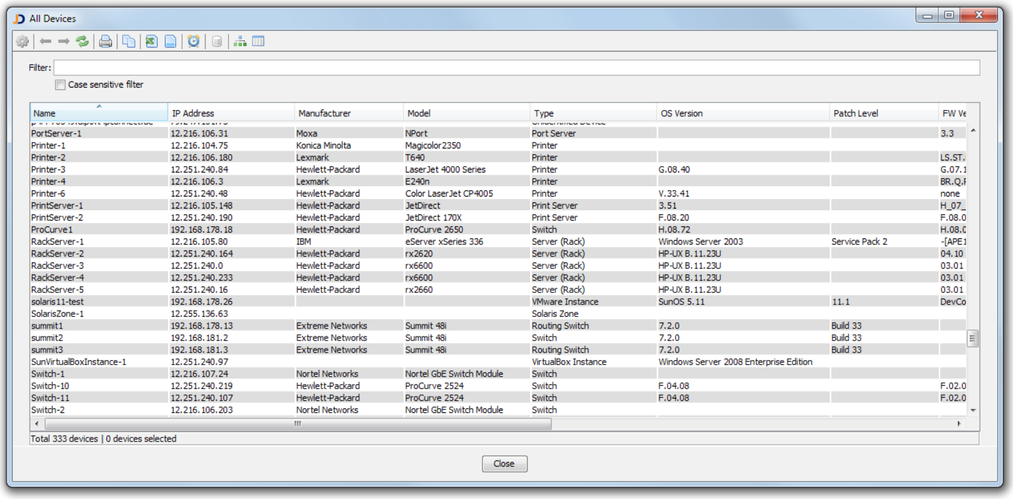
Whenever JDisc Discovery discovers a Windows computer that belongs to this workgroup or domain, it will use the specified administrative account to discover this computer.

Don't enter the workgroup prefix when the neighborhood name belongs to a Windows workgroup and not to a Windows domain.

The most important leason is that JDisc Discovery requires access credentials to discover detailed device information. Without access credentials, JDisc Discovery gets only little or no information at all.

Always enter fully qualified access credentials including the domain!

When the first discovery is finished, all Windows computers that belong to the specified workgroup or domain should be successfully discovered. Open the “All Devices” report from the *Devices » All Devices* menu item.



Name	IP Address	Manufacturer	Model	Type	OS Version	Patch Level	FW Ve
PortServer-1	12.216.106.31	Moxa	NPort	Port Server			3.3
Printer-1	12.216.104.75	Konica Minolta	Magicolor2350	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
RackServer-1	12.216.105.80	IBM	eServer xSeries 336	Server (Rack)	Windows Server 2003	Service Pack 2	-[APE1
RackServer-2	12.251.240.164	Hewlett-Packard	rx2620	Server (Rack)	HP-UX B.11.23U		04.10
RackServer-3	12.251.240.0	Hewlett-Packard	rx6600	Server (Rack)	HP-UX B.11.23U		03.01
RackServer-4	12.251.240.233	Hewlett-Packard	rx6600	Server (Rack)	HP-UX B.11.23U		03.01
RackServer-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: A typical all devices report.

Successfully discovered Windows computers usually have the model, manufacturer and serial number fields populated.

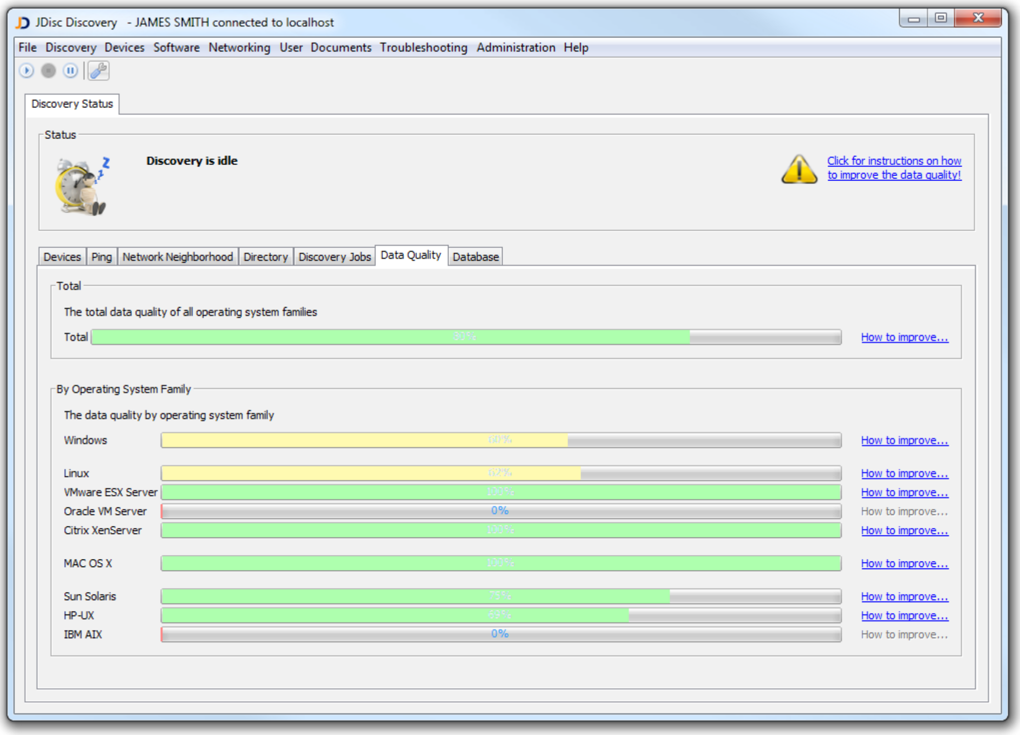
The two main reasons for an unsuccessful discovery of Windows computers are personal firewalls (blocking all discovery protocols) or incorrect/missing access credentials. Refer to the troubleshooting section in this document to learn how to troubleshoot discovery issues.

2.4 General Tips

This section explains general hints and tips when using JDisc Discovery.

2.4.1 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.



JDisc Discovery - JAMES SMITH connected to localhost

File Discovery Devices Software Networking User Documents Troubleshooting Administration Help

Discovery Status

Status

Discovery is idle

Click for instructions on how to improve the data quality!

Devices | Ping | Network Neighborhood | Directory | Discovery Jobs | Data Quality | Database

Total

The total data quality of all operating system families

Total 80% How to improve...

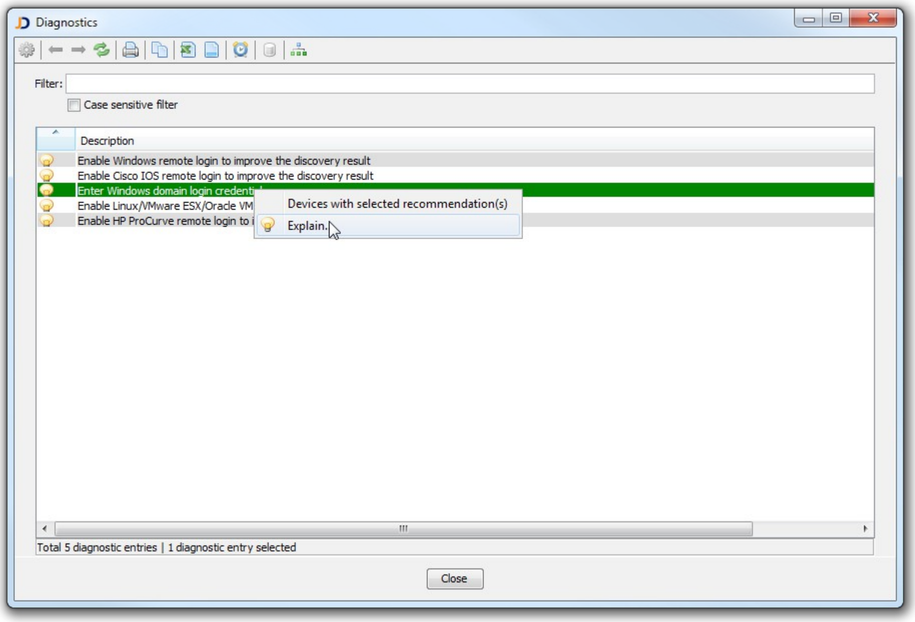
By Operating System Family

The data quality by operating system family

Windows	60%	How to improve...
Linux	62%	How to improve...
VMware ESX Server	100%	How to improve...
Oracle VM Server	0%	How to improve...
Citrix XenServer	100%	How to improve...
MAC OS X	100%	How to improve...
Sun Solaris	75%	How to improve...
HP-UX	69%	How to improve...
IBM AIX	0%	How to improve...

Figure: Data Quality Tab

Follow the *How to improve...* link in the right area in order to open a new diagnostics report. This report displays a list of tasks on how to improve the data quality.



Diagnostics

Filter:

□ Case sensitive filter

	Description
	Enable Windows remote login to improve the discovery result
	Enable Cisco IOS remote login to improve the discovery result
	Enter Windows domain login credenti
	Enable Linux/VMware ESX/Oracle VM
	Enable HP ProCurve remote login to i

Total 5 diagnostic entries | 1 diagnostic entry selected

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.

2.4.2 Firewalls

For the initial tests, disable any personal firewall on the computer running JDisc Discovery. Depending on the configuration, personal firewalls can negatively influence the result.

> Personal firewalls can either block connections to the embedded database or have a negative impact on the discovery process.

2.4.3 Discover Individual Devices

When testing the discovery, you will often need to discover a single device or a list of devices. For instance, when you have changed the access credentials of devices and you would like to re-discover those devices.

To discover individual devices, select them in any device report (for instance from *Devices » All Devices*). Open the context menu (click on right mouse button) and select *Discovery » Selected Devices* or *Discovery » Selected IP Addresses*. *Selected Devices* first performs a DNS lookup on the device name to determine its current IP address. This is useful in DHCP environments when the IP address might have changed.

2.4.4 Basic Troubleshooting

When your discovery result are to not as good as expected you can troubleshooting for common problems such as:

- Misconfigured or wrong access credentials.
- Personal or network based firewalls blocking the discovery traffic.
- Disabled remote login for Unix platforms.

JDisc Discovery provides several reports to support the troubleshooting process. Open the *Device Details* dialog (either double click on a device or use the context menu) to inspect a single device. The *Analyze* tab is the key for troubleshooting. It consists of four tabs:

- *Discovery Log* displays a detailed discovery log.
- *Protocols* displays all protocols and protocols status.
- *Parsing Issues* displays all system command outputs, that JDisc Discovery failed to parse. Parsing issues often occur when software vendor change the output format of their system commands in newer operating system versions.
- *Diagnostics* uses a rule based system to determine suggestions on how to improve the discovery of Windows computers.

For Windows computers, the WMI protocol is important. An error message like “The RPC Server is unavailable” is a strong indication for the presence of a personal firewall blocking the discovery traffic.

2.5 Discover Windows Computers

Administrative access credentials are the key for a successful discovery of Windows computers. Without access credentials, JDisc Discovery will discover only basic information, such as operating system version. For security reasons, it is impossible to remotely discover detailed device information, such as installed applications without administrative access credentials.

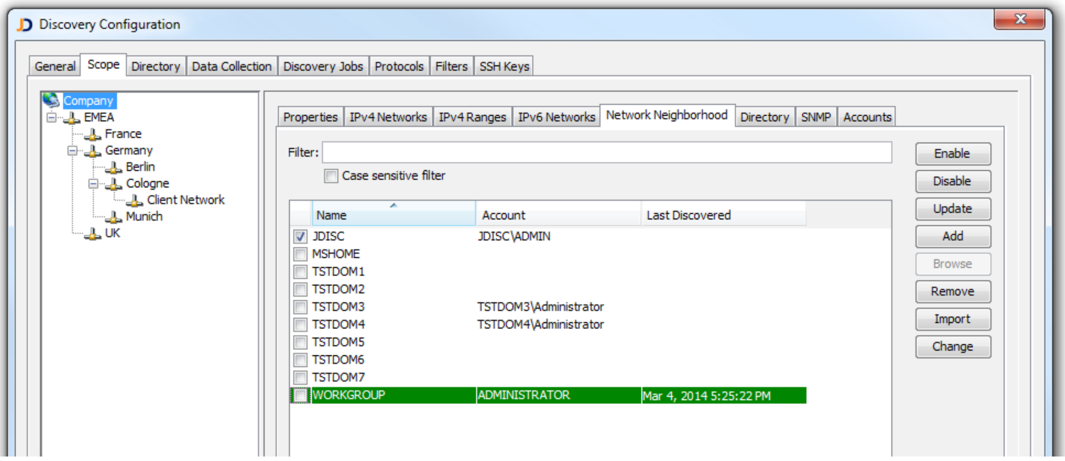
Furthermore, configuring access credentials on a per Windows computer basis is impractical. Therefore JDisc Discovery provides several options to configure administrative access credentials per Windows domain or Active Directory object. Choose the option which suits your network environment.

Consider using remote login to improve your discovery result and speed up the discovery for computers at remote sites. Refer to chapter 2.5.4 for more information on remote login.

2.5.1 Enter Windows Domain Accounts

When your Windows network is based on Windows NT domains, you should enter administrative access credentials for each domain in JDisc Discovery's configuration dialog.

Open the *Discovery Configuration* dialog and select the *Network Neighborhood* tab within the *Scope* top level tab.



Name	Account	Last Discovered
☑ JDISC	JDISC\ADMIN	
□ MSHOME		
□ TSTDOM1		
□ TSTDOM2		
□ TSTDOM3	TSTDOM3\Administrator	
□ TSTDOM4	TSTDOM4\Administrator	
□ TSTDOM5		
□ TSTDOM6		
□ TSTDOM7		
□ WORKGROUP	ADMINISTRATOR	Mar 4, 2014 5:25:22 PM

Figure: Windows domain configuration

Click *Add* to add Windows domains and *Change* to modify administrative access credentials for a domain. You might use multiple select to enter administrative access credentials for multiple domains.

2.5.2 Accounts For Microsoft Active Directory Objects

If your Windows network runs Microsoft Active Directory, JDisc Discovery can synchronize its directory structure and discover computers that are a member of the directory.

First of all, you need to configure one or more DNS domain controllers serving your Active Directory and provide access credentials for the directory. Open the *Discovery Configuration* dialog from *Discovery » Configuration* and select the *Directory* top-level tab. If the *DNS Domain Controller* panel already contains one or more host name, click *Change* to open the *Directory Service Account* dialog and enter login credentials for the DNS domain controllers. Otherwise click *Add* to add a new DNS domain controller. Enter a directory user account having at least read access rights to the directory. JDisc Discovery will only use this user account to query the directory.

Click *Discovery » Control » Synchronize Directory* to synchronize directory objects with JDisc Discovery's database.

Once again open the *Discovery Configuration* dialog from *Discovery » Configuration,* select the *Scope* tab and then select the *Directory* tab on the right panel. The *Directory* tab displays the directory hierarchy including directory objects such as DNS domains or organizational units.

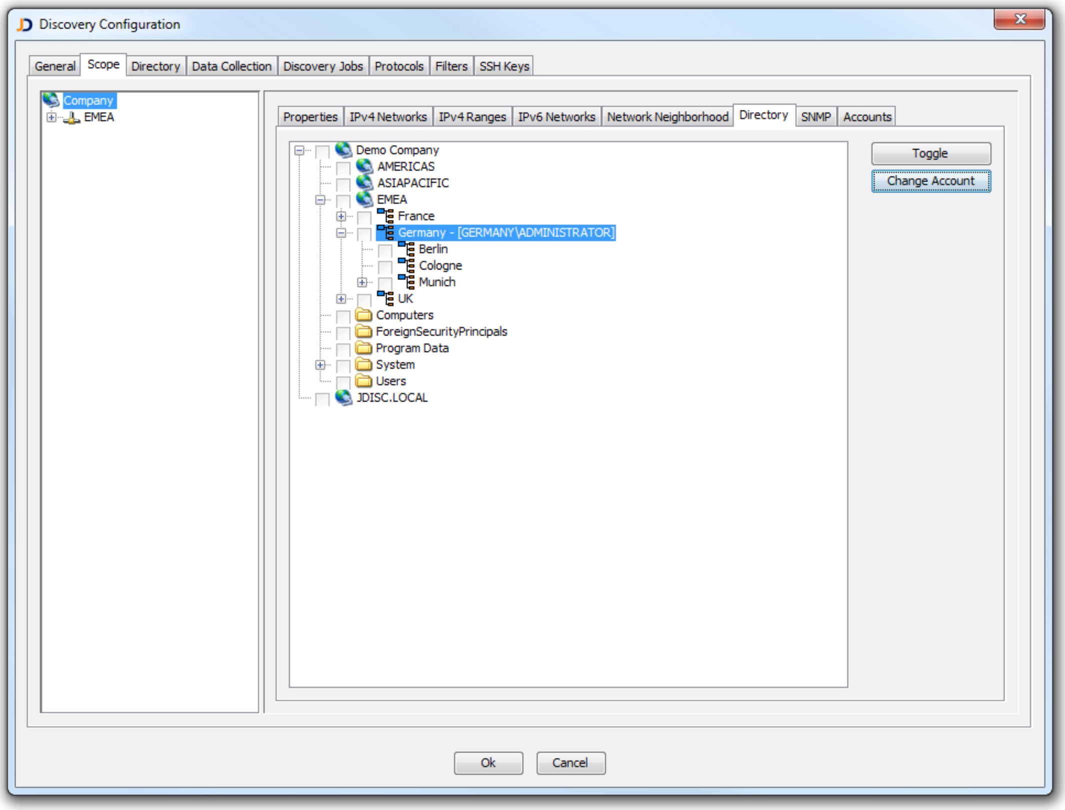


Figure: Configure Accounts for Organizational Units

The directory hierarchy serves two purposes:

- Associate directory objects to a group
- Configure access credentials for selected directory objects. JDisc Discovery uses these access credentials to logon to Windows computers that are member of this directory. Make sure to use the full login name (domain/username) or the user principal name (username@domain).

To enable directory discovery:

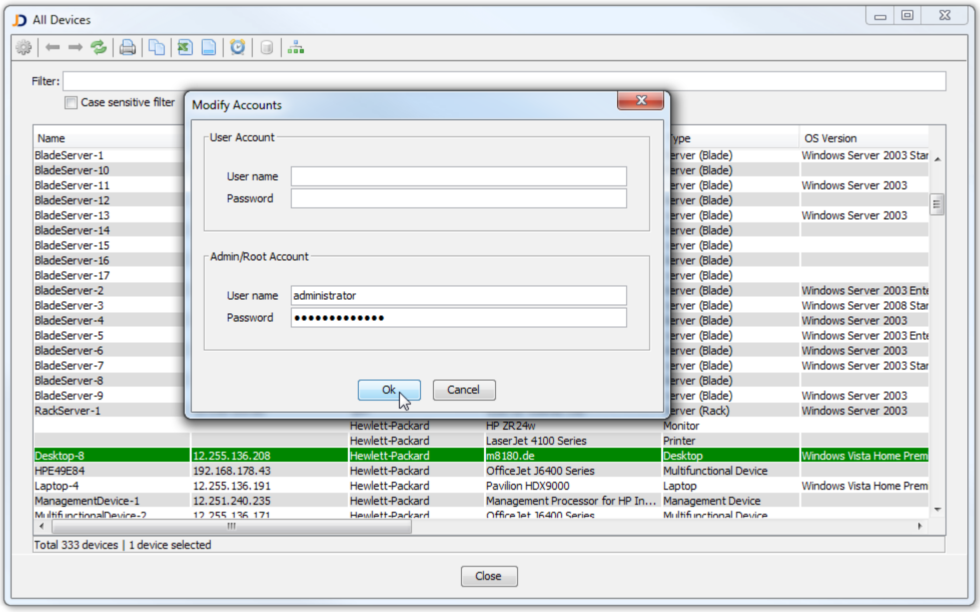
- Select a group
- Select directory objects, open the context menu and choose:
    - *Enable* to only discover and include computers belonging to selected directory objects. Directly enabled directory objects are indicated with a black check mark symbol.
    - *Enable subtree* to discover and include computers belonging to selected directory objects and all subordinate directory objects. Indirectly enabled directory objects (part of a subtree) are indicated with a grayed check mark symbol.

Use *Toggle* or the *Space* key to toggle between *Disable*, *Enable* and *Enable subtree*.

2.5.3 Per Device Access Credentials

If none of the options above apply, you can configure access credentials for each device individually. JDisc Discovery always uses individually configured accounts to discover a device.

Select one or more devices, open the context menu (right mouse button) and select *Manage » Change Accounts*. Enter the administrative access credentials in the *Admin/Root Account* fields for selected devices.



User Account
User name
Password

Admin/Root Account
User name administrator
Password •••••••••••••

Name				Type	OS Version
BladeServer-1				erver (Blade)	Windows Server 2003 Star
BladeServer-10				erver (Blade)	
BladeServer-11				erver (Blade)	Windows Server 2003
BladeServer-12				erver (Blade)	
BladeServer-13				erver (Blade)	Windows Server 2003
BladeServer-14				erver (Blade)	
BladeServer-15				erver (Blade)	
BladeServer-16				erver (Blade)	
BladeServer-17				erver (Blade)	
BladeServer-2				erver (Blade)	Windows Server 2003 Ente
BladeServer-3				erver (Blade)	Windows Server 2008 Star
BladeServer-4				erver (Blade)	Windows Server 2003
BladeServer-5				erver (Blade)	Windows Server 2003 Ente
BladeServer-6				erver (Blade)	Windows Server 2003
BladeServer-7				erver (Blade)	Windows Server 2003 Star
BladeServer-8				erver (Blade)	
BladeServer-9				erver (Blade)	Windows Server 2003
RackServer-1				erver (Rack)	Windows Server 2003
		Hewlett-Packard	HP ZR24w	Monitor	
		Hewlett-Packard	LaserJet 4100 Series	Printer	
Desktop-8	12.255.136.208	Hewlett-Packard	m8180.de	Desktop	Windows Vista Home Prem
HPE49E84	192.168.178.43	Hewlett-Packard	OfficeJet J6400 Series	Multifunctional Device	
Laptop-4	12.255.136.191	Hewlett-Packard	Pavilion HDX9000	Laptop	Windows Vista Home Prem
ManagementDevice-1	12.251.240.235	Hewlett-Packard	Management Processor for HP In...	Management Device	
MultifunctionalDevice-2	12.255.136.171	Hewlett-Packard	OfficeJet J6400 Series	Multifunctional Device	

Total 333 devices | 1 device selected

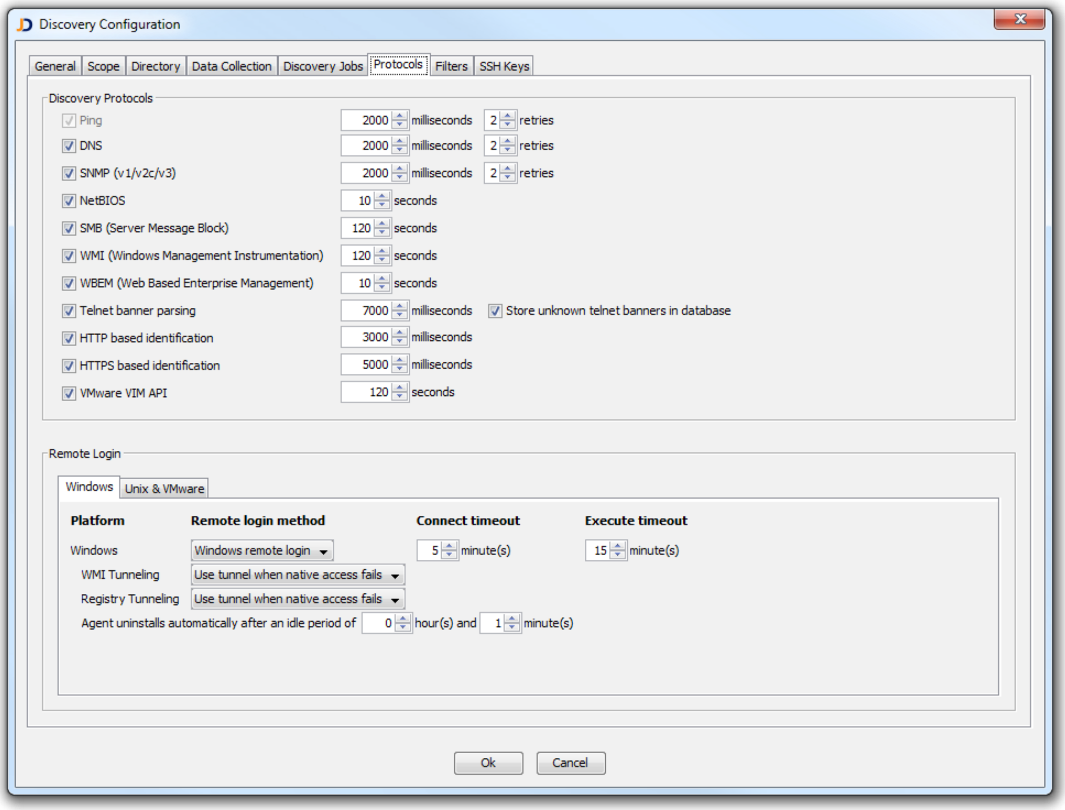
Figure: Change Device Accounts

2.5.4 Remote Login For Windows

JDisc Discovery offers a unique feature called *Remote Login*. When remote login is enabled, then JDisc Discovery copies a small temporary agent to the target computer. The agent runs only for the duration of the scan and deletes itself and all temporary files from the target computer. There are several advantages of using remote login:

1. Remote login can tunnel WMI and registry requests through the temporary agent. WMI and registry is access through the tunnel is for remote sites with comparably slow lines up to 6 times faster than native WMI or registry queries.
2. Remote login requires only port 445. With Remote login, JDisc Discovery can discover highly secured clients (which would block WMI traffic) or servers within the DMZ.
3. With remote login, JDisc Discovery can discover information that is not available through WMI or other protocols.

Enable remote login for Windows from within the discovery settings dialog within the protocols tab.



Discovery Protocols

☑ Ping 2000 milliseconds 2 retries
☑ DNS 2000 milliseconds 2 retries
☑ SNMP (v1/v2c/v3) 2000 milliseconds 2 retries
☑ NetBIOS 10 seconds
☑ SMB (Server Message Block) 120 seconds
☑ WMI (Windows Management Instrumentation) 120 seconds
☑ WBEM (Web Based Enterprise Management) 10 seconds
☑ Telnet banner parsing 7000 milliseconds ☑ Store unknown telnet banners in database
☑ HTTP based identification 3000 milliseconds
☑ HTTPS based identification 5000 milliseconds
☑ VMware VIM API 120 seconds

Remote Login

Windows | Unix & VMware

Platform	Remote login method	Connect timeout	Execute timeout
Windows	Windows remote login	5 minute(s)	15 minute(s)
WMI Tunneling	Use tunnel when native access fails		
Registry Tunneling	Use tunnel when native access fails		

Agent uninstalls automatically after an idle period of 0 hour(s) and 1 minute(s)

Figure: Enable remote login for Windows

2.6 Discover Unix Computers

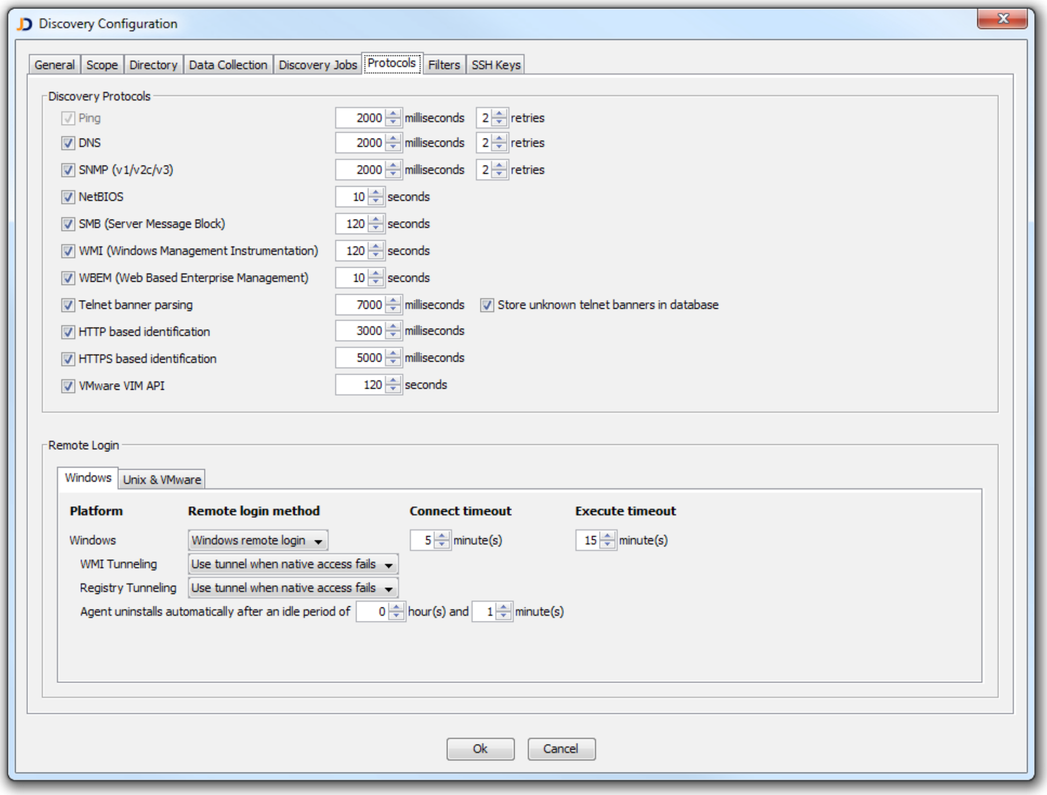
Typically, Unix computers rarely have standard management protocols, such as SNMP or WBEM installed out-of-the-box or if installed, often do not provide detailed hardware, software and configuration information.

JDisc Discovery compensates the lack of standard management protocols by logging on using telnet or SSH, executing selected system commands, and parsing the command output to retrieve hardware, software and configuration information. In most cases ordinary user privileges are sufficient, 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 the desired operating system platforms. Remote login is disabled for all operating system platforms by default. To enable remote login, open the *Discovery Configuration* dialog.
- Enable remote login for *unknown devices*. This option is important for hardened systems. JDisc Discovery then first logs on the computer, executes the uname command to determine the device's platform. If the device's platform has been determined successfully, the discovery process the device according to the device's platform configuration.
- Configure default credentials for desired operating system platforms. If using default credentials is not an option, configure per-device credentials.

When you have SSH keys deployed on your devices, you can import your SSH keys from the top level *SSH Keys* tab. Once imported, the SSH keys can be used to configure default access credentials or access credentials for individual computers.



Discovery Protocols

☑ Ping 2000 milliseconds 2 retries
☑ DNS 2000 milliseconds 2 retries
☑ SNMP (v1/v2c/v3) 2000 milliseconds 2 retries
☑ NetBIOS 10 seconds
☑ SMB (Server Message Block) 120 seconds
☑ WMI (Windows Management Instrumentation) 120 seconds
☑ WBEM (Web Based Enterprise Management) 10 seconds
☑ Telnet banner parsing 7000 milliseconds ☑ Store unknown telnet banners in database
☑ HTTP based identification 3000 milliseconds
☑ HTTPS based identification 5000 milliseconds
☑ VMware VIM API 120 seconds

Remote Login

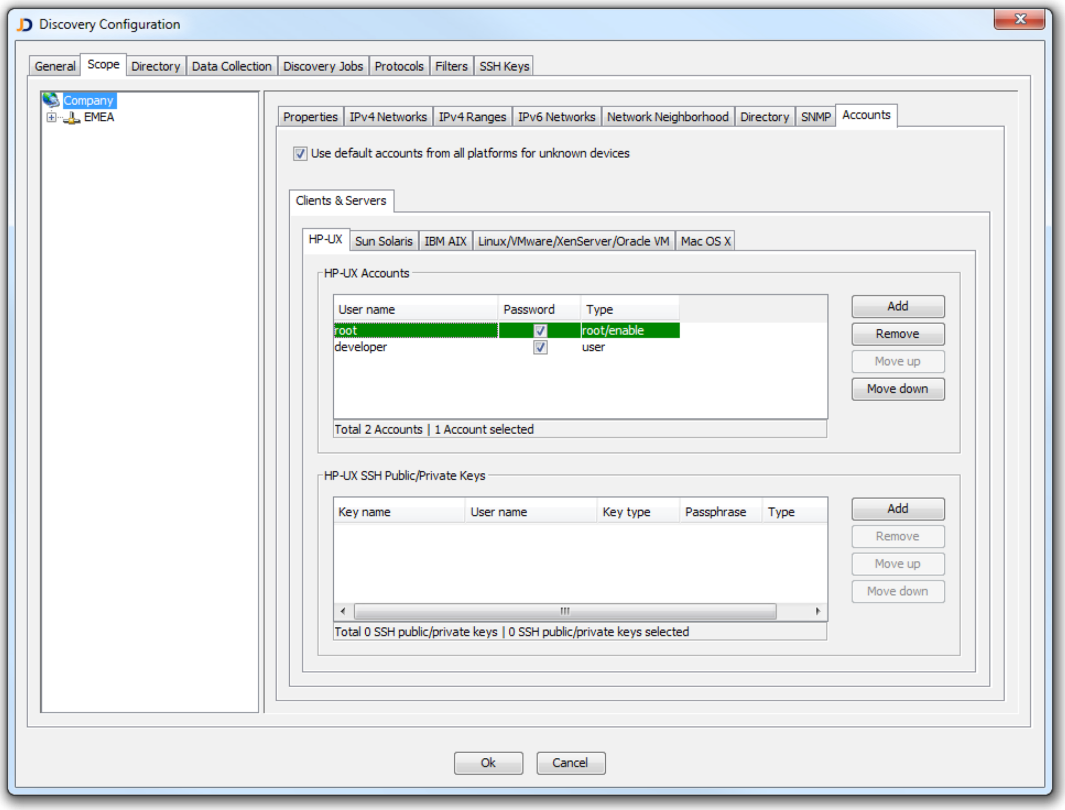
Windows | Unix & VMware

Platform	Remote login method	Connect timeout	Execute timeout
Windows	Windows remote login	5 minute(s)	15 minute(s)
WMI Tunneling	Use tunnel when native access fails		
Registry Tunneling	Use tunnel when native access fails		

Agent uninstalls automatically after an idle period of 0 hour(s) and 1 minute(s)

Figure: Protocol configuration

When you have enabled all protocols, switch to the *Scope* tab and select the *Accounts* sub-tab. Select the desired platform and add new default accounts or SSH access credentials as needed.



☑ Use default accounts from all platforms for unknown devices

HP-UX Accounts

User name	Password	Type
root	☑	root/enable
developer	☑	user

Total 2 Accounts | 1 Account selected

HP-UX SSH Public/Private Keys

Key name	User name	Key type	Passphrase	Type

Total 0 SSH public/private keys | 0 SSH public/private keys selected

Figure: Define Default Accounts for HP-UX

Once all default accounts have been configured, either run a new discovery job or discover your Unix computers individually.