JDisc

360° Network Inventory | Topology | Relations

# JDisc Discovery 5.0

# Security Whitepaper

## Legal Notice

## Copyright

JDisc GmbH
Kuppinger Weg 25
D-71116 Gärtringen
Germany

# JDisc Discovery Security Guide

This guide provides the most important information needed to run JDisc Discovery in secure Windows, Linux and Unix IT environments. Please do not hesitate to contact us if you require additional information.

All descriptions are given most carefully as possible. Please follow this and any additional info of other used software carefully. We disclaim liability for security problems you might have.

# Contents

# 1 Introduction

JDisc Discovery is a high-end network inventory solution that does not need to deploy agents on 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 security guide explains general security related aspects of network discovery products and JDisc Discovery aspects in more detail.

Security has many aspects. The second chapter explains how JDisc Discovery secures its data and the third chapter provides security information that is important when discovering devices.

## 1.1 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.
Agent deployment can also be time consuming and might create security and performance risks unless thoroughly tested and well designed.

## 1.2 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.

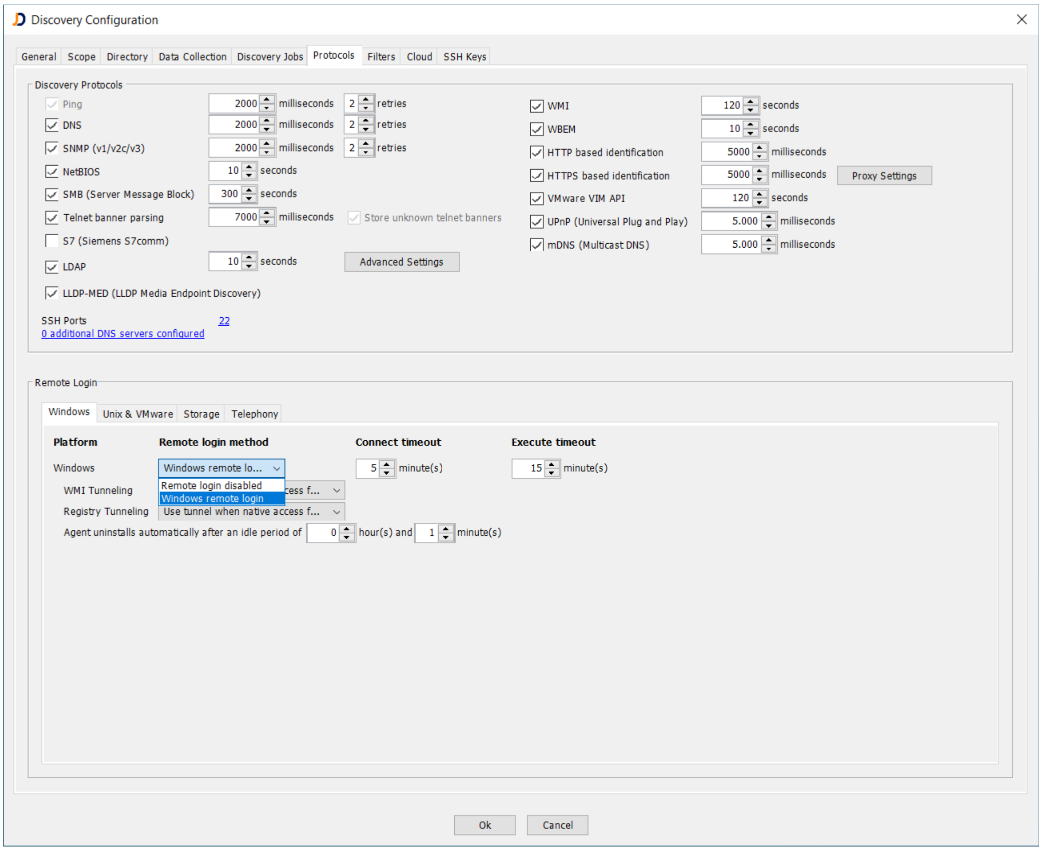
Agent-less products can be easily deployed because they do not need to install proprietary agents on target computers. With a wide variety of protocols, they can get very detailed information.

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 collect  detailed information from devices.

## 1.3 JDisc Discovery

By default JDisc Discovery uses a zero-footprint approach for Windows computers. Zero footprint means that an agent can be temporarily deployed to target computers. The agent will automatically uninstall itself when the computer is detected (typically after 1 minute). This approach minimizes the agent's impact on target computers.

Agent usage can be disabled in the JDisc Discovery's settings by changing the Windows Remote Logon settings from enabled to disabled.



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) 300 seconds
☑ Telnet banner parsing 7000 milliseconds ☑ Store unknown telnet banners
□ S7 (Siemens S7comm)
☑ LDAP 10 seconds
☑ LLDP-MED (LLDP Media Endpoint Discovery)

SSH Ports 22
0 additional DNS servers configured

☑ WMI 120 seconds
☑ WBEM 10 seconds
☑ HTTP based identification 5000 milliseconds
☑ HTTPS based identification 5000 milliseconds
☑ VMware VIM API 120 seconds
☑ UPnP (Universal Plug and Play) 5.000 milliseconds
☑ mDNS (Multicast DNS) 5.000 milliseconds

Remote Login

| Platform | Remote login method | Connect timeout | Execute timeout |
|---|---|---|---|
| Windows | Windows remote lo... | 5 minute(s) | 15 minute(s) |
| WMI Tunneling | Remote login disabled<br>Windows remote login | | |
| Registry Tunneling | Use tunnel when native access f... | | |

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

Whether you use agent-less or agent-based technologies, thorough testing of network discovery applications is important to establish a relationship of trust between you and the discovery product vendor. You must trust the detection application as it often has full access to many devices on your network.

# 2 Application Security

This chapter describes application-aware security, including its architecture, its underlying database, and client-server communications.

## 2.1 Application Architecture

JDisc Discovery uses zero footprint and agentless technologies. It follows the client-server architecture. The User Interface Client communicates with the Discovery Server via RMI. The Discovery Server runs as a Windows service in the background. The User Interface Client and the Discovery  server can also be installed on different computers.

The following figure illustrates the architecture of JDisc Discovery.

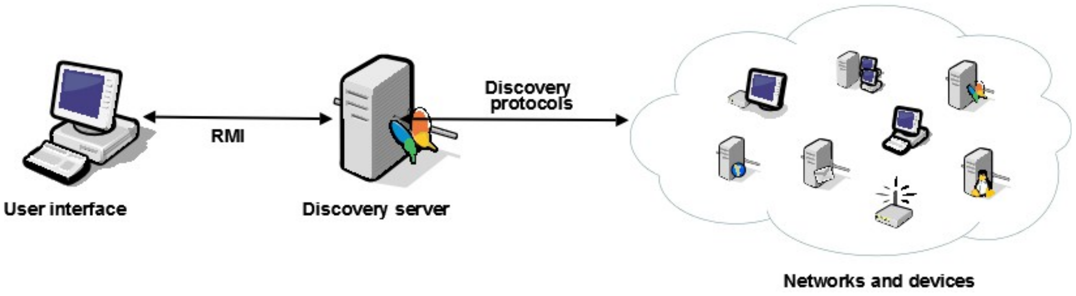


Figure: JDisc Discovery architecture

The discovery server

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

The user interface client

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

## 2.2 Database Security

JDisc Discovery uses a standard SQL database for discovered devices, network information, and configuration information such as credentials. We know that most companies keep IT information confidential, and that's why we protect your information.

JDisc uses an embedded PostgreSQL database and updates it with each major product release. The JDisc Discovery program automatically configures the database and creates two database users. A database user is granted access and used by JDisc Discovery tread and write data to the database.The second database user is a read-only user that can be used to extract information from the JDisc Discovery database to other applications (e.g. CMDB solutions).

When installing JDisc Discovery, you will be prompted for passwords for both users. Database users' passwords can also be changed through the JDisc Discovery user interface.

To increase database security for stand-alone installations (when data export to other tools is not required), the JDisc Discovery administrator can disable remote database access.

Access to the JDisc Discovery database is password protected! Access can be limited to the local system only.

## 2.3 Access Credential Data Security

Like any other agent-less network discovery product, JDisc Discovery stores access credentials in its database to access devices. Without credentials, network discovery products collect very limited or no information.  JDisc is aware that access data is strictly confidential and must be protected from unauthorized access.

The JDisc Discovery setup program creates a unique encryption key - called the machine key for each installation. JDisc Discovery uuses the machine key for encrypting

- the database user (postgres and postgresro) passwords.
- the database's unique AES-128 encryption key (also created during setup) used to encrypt sensitive information such as passwords, SSH keys, and SNMP communities.

This prevents passwords and unauthorized access even when all database tables are backed up and imported into another database installation or when performing SQL queries against the database.

All passwords are stored with an encryption key unique to each JDisc Discovery installation.

## 2.4 User Interface Security

JDisc Discovery does not display passwords in clear text in the user interface.

However, there is one exception. SNMP read communities are displayed in clear text. However, SNMPv1 and v2c are inherently insecure because all communications, including transmission from SNMP communities, are not encrypted. Because of this, administrators often apply access lists to their switches and routers.

JDisc Discovery encrypts all requests whenever the client communicates with the server to protect user-entered passwords.

Only a definable set of users has access to the product. The JDisc Discovery administrator can grant or revoke users' access to the product. Each user can have different access rights (e.g. view data, configure product, start scans, ...). Users authenticate with their normal Windows account.

# 3 Scanning Devices

This chapter deals with security aspects when scanning computers in the network.

Device scanning requires some form of access credentials. It depends on the operating system and protocol whether a regular user account is sufficient or whether you need an administrator account.

Without providing access data there is no (or only little) inventory information. Similar to your credit card: no PIN, no money!

## 3.1 Ports And Protocols

JDisc Discovery uses a variety of different protocols to collect information from network devices. The actual protocols used depend on the device configuration, device type and operating system version. The following table shows all protocols and their associated ports.

| **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)<br>138 (UDP)<br>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 |

Table: Protocols and Ports

## 3.2 Scanning Windows Computers

As described in chapter 1, JDisc Discovery can either use its zero-footprint agent or run in a fully agent-less mode. The zero-footprint agent is enabled by default.

### 3.2.1 Using The Zero-Footprint Agent On Windows

JDisc Discovery uses its zero-footprint agent to gather hardware, software, and configuration information.

#### 3.2.1.1 Automatic Installation / Uninstallation

The automatic install / uninstall zero footprint agent technology works as follows:

- JDisc Discovery creates a secured install share (only for administrators) on the target computer to install the agent.
- JDisc Discovery copies the agent executable to the install share on the target computer.
- JDisc Discovery deletes the install share, registers and starts the agent service and finally connects to it.
- After the scan is complete, the agent will stop and uninstall itself, deleting the session directory and files on the target computer.

To automatically deploy the agent to the target computer, JDisc Discovery needs administrative access on the target computer (either a local administrator or a domain administrator account).

The JDisc Discovery zero footprint agent is enabled by default but can be disabled.

Administrative rights are required to install the JDisc Discovery zero-footprint agent on Windows computers.

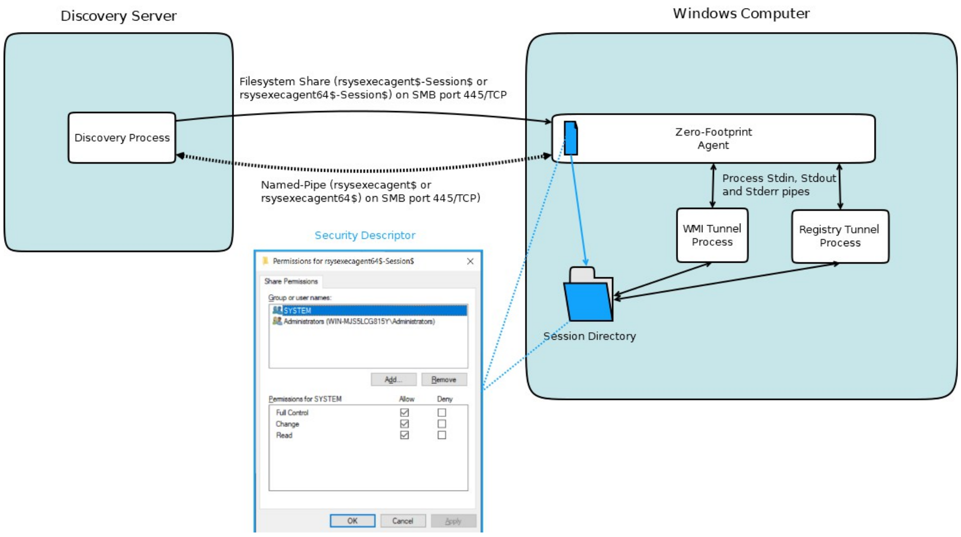
JDisc Discovery's zero-footprint agent is firewall friendly as it uses only a single TCP/IP port (SMB protocol on port 445/TCP) and tunnels all information through that port.

### 3.2.1.2 Communication And Security

The JDisc Discovery zero footprint agent communicates with the discovery server via a named pipe. Depending on the target Windows operating system (32-bit or 64-bit) the pipe is named rsysexecagent$ or  rsysexecagent64$.

The named pipe's security descriptor permits access only to members of the local Administrators group, the SYSTEM account and depending on your agent security settings, one or multiple user groups / users for privilege elevation. All communication between the discovery server and the agent is compressed and encrypted.

Files are transferred from the discovery server to the agent and vice versa via the rsysexeagent$-Session$ or rsysexeagent64$-Session$ share. This share uses the same security descriptor settings as the named pipe. The session share is mapped to a dedicated session directory that is automatically removed when the agent is stopped or uninstalled. Again,  the session directory uses the same security descriptor settings as the named pipe and the session share.


Discovery Server
Windows Computer
Discovery Process
Filesystem Share (rsysexecagent$-Session$ or rsysexecagent64$-Session$) on SMB port 445/TCP
Named-Pipe (rsysexecagent$ or rsysexecagent64$) on SMB port 445/TCP)
Zero-Footprint Agent
Process Stdin, Stdout and Stderr pipes
WMI Tunnel Process
Registry Tunnel Process
Session Directory
Security Descriptor
Permissions for rsysexecagent64$-Session$
Share Permissions
Add...
Remove
OK
Cancel
Apply

Group or user names:
- SYSTEM
- Administrators (WIN-MJS5LOG815Y\Administrators)

| Permissions for SYSTEM | Allow | Deny |
|---|---|---|
| Full Control | ☑ | □ |
| Change | ☑ | □ |
| Read | ☑ | □ |

Figure: Discovery Server – Agent Communication

### 3.2.1.3 Permanent Installation / Uninstallation

The agent can be permanently installed on Windows computers. This allows to configure the agent for non-admin users to run processes with elevated privileges. This feature provides a Linux/Unix SU or SUDO like functionality on Windows.

For a permanent installation, distribute the respective agent executable from the *<JDisc Discovery installation>\bin* directory

- rsysexeagent64.exe (x64 64-bit Windows)
- rsysexeagent32.exe (x86 32-bit Windows)

to the desired Windows computers using your software distribution tooling. You can run the agent executable also from the NETLOGON share used for logon scripts on domain controllers.

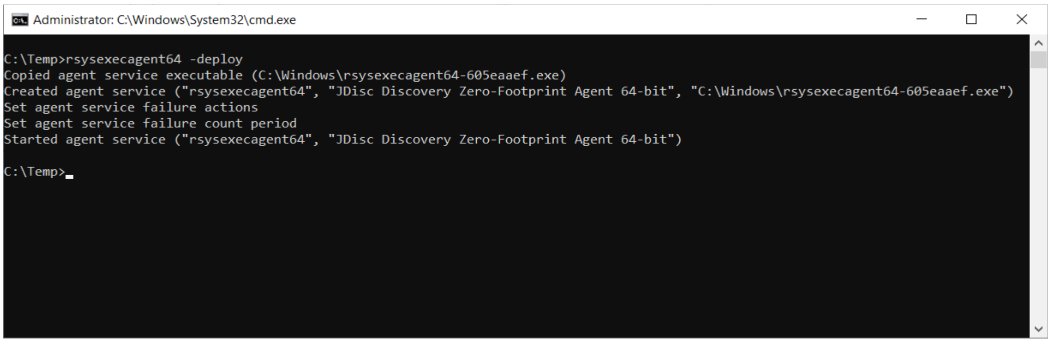
#### Agent Executable Command Line Options

The 32-bit and 64-bit agent executables can be run using any of these command line options:

- `-deploy [-PrivilegeElevationUserGroup <User or Group Name>]`
- `-undeploy`

#### Agent Installation

The JDisc Discovery Zero Footprint Agent service installs from the current directory (for example, c:\temp) into the Windows directory.



```
C:\Temp>rsysexecagent64 -deploy
Copied agent service executable (C:\Windows\rsysexecagent64-605eaaef.exe)
Created agent service ("rsysexecagent64", "JDisc Discovery Zero-Footprint Agent 64-bit", "C:\Windows\rsysexecagent64-605eaaef.exe")
Set agent service failure actions
Set agent service failure count period
Started agent service ("rsysexecagent64", "JDisc Discovery Zero-Footprint Agent 64-bit")

C:\Temp>
```

Figure: Permanent Agent Install

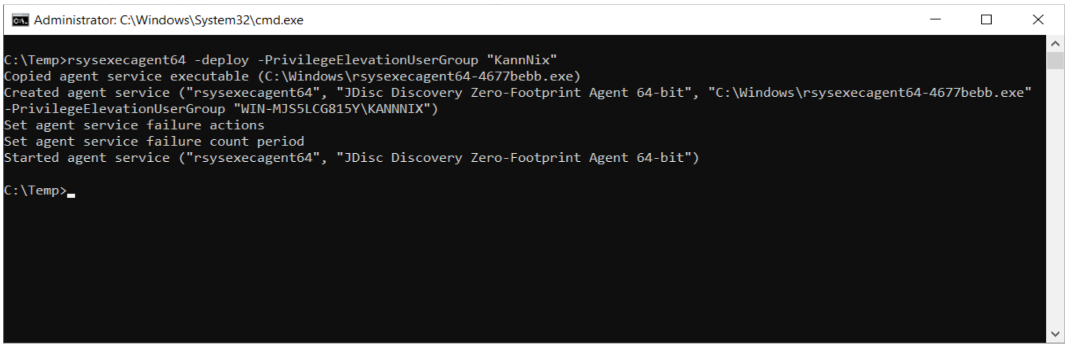
The `-deploy` option copies the `rsysexecagent64.exe` executable into the Windows directory, registers the service startup to automatic and start the agent service.

If the agent service is already installed the `-deploy` option will update the agent service executable if needed.

When JDisc Discovery connects to the agent service it will also update the agent as needed.

### Agent Installation With User and User Group Elevation

The `-PrivilegeElevationUserGroup` option allows specifying user groups or user names to run processes with elevated privileges.



```
C:\Temp>rsysexecagent64 -deploy -PrivilegeElevationUserGroup "KannNix"
Copied agent service executable (C:\Windows\rsysexecagent64-4677bebb.exe)
Created agent service ("rsysexecagent64", "JDisc Discovery Zero-Footprint Agent 64-bit", "C:\Windows\rsysexecagent64-4677bebb.exe"
-PrivilegeElevationUserGroup "WIN-MJS5LCG815Y\KANNNIX")
Set agent service failure actions
Set agent service failure count period
Started agent service ("rsysexecagent64", "JDisc Discovery Zero-Footprint Agent 64-bit")

C:\Temp>
```

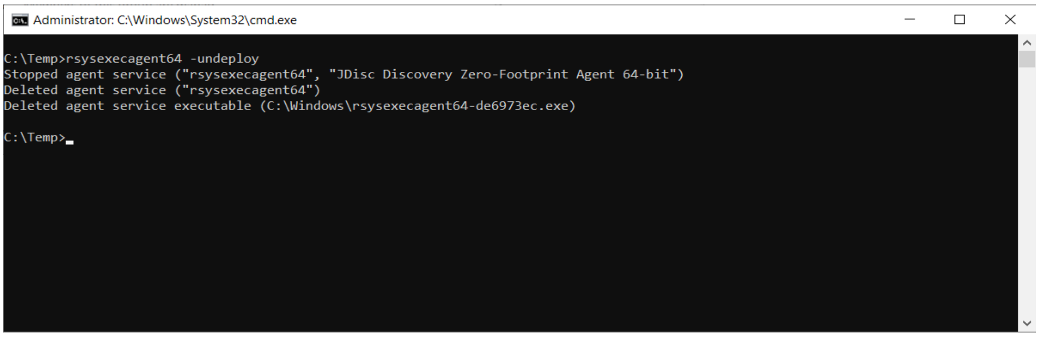
Figure: Permanent Agent Install With Privilege Elevation

In the example above, the local user `"KannNix"` is permitted to connect to the agent and run processes with elevated privileges.

If the agent service is already installed the specified user group or user names will be reconfigured.

### Agent Uninstallation

If you no longer need the JDisc Discovery Zero Footprint Agent service, you can uninstall it using the `-undeploy` command line option.



```
C:\Temp>rsysexecagent64 -undeploy
Stopped agent service ("rsysexecagent64", "JDisc Discovery Zero-Footprint Agent 64-bit")
Deleted agent service ("rsysexecagent64")
Deleted agent service executable (C:\Windows\rsysexecagent64-de6973ec.exe)

C:\Temp>
```

Figure: Agent Uninstallation

This first stops the agent service and then deletes the service executable from the Windows directory.

#### 3.2.1.4 WMI And Registry Tunnelling

JDisc Discovery's zero footprint agent can tunnel WMI and registry access to remote Windows computers. Tunneling is faster and uses less network bandwidth than native protocol implementations.

The tunnelling operation is implemented by these processes:

- WmiQuery.exe or WmiQuery64.exe
- RegQuery.exe or RegQuery64.exe

that communicate with the agent via the stdin, stdout, and stderr console pipes.

The console pipes stdin, stdout, and stderr are extended from the agent to the discovery server and allow execution of WMI and registry queries, respectively.

### 3.2.2 Using Agent-Less Technologies On Windows

The JDisc Discovery zero-footprint agent can be disabled in the Discovery configuration dialog. JDisc Discovery then uses standard protocols available on Windows computers.

NetBIOS and SMB (anonymous) are used for initial classification (OS and patch levels), LDAP for Microsoft Active Directory lookup and mapping of computers to directory objects. SMB is also used to access the Windows remote registry. The most well-known protocol for collecting hardware and software information is the WMI protocol.

---

You may encounter more firewall problems when using agentless technologies, since you need more protocols and TCP/IP ports than with JDisc Discovery's zero-footprint agent.

---

It is possible to run WMI with a non-administrative user account, but this requires additional configuration for WMI to work (see chapter Fehler: Referenz nicht gefunden for more details on configuring WMI with non-administrative access).

---

**TCP/IP Ports required for this discovery method:**

- Server Message Block (SMB): 445 (TCP)
- NetBIOS: 137 (UDP), 138 (UDP), 139 (TCP)
- WMI: 135 (TCP) and a negotiated port between 1024 and 65535.

## 3.3 Scanning Unix Computers

JDisc Discovery connects to the Unix console to obtain hardware- and software information by logging on via telnet or SSH and executing system commands. Some system commands require root access. In this case, JDisc Discovery can either use the “su” command to switch to the root account or use “sudo” on Linux or “.do” on HP-UX. When the privileged access is no longer required, JDisc Discovery reverts to the ordinary account that was used to log on.

JDisc Discovery executes the following commands with root privileges to collect hard- and software details on Linux computers:

| | |
|---|---|
| Hardware | /usr/sbin/dmidecode |
| Network Interface Speed | /sbin/ethtool<br>/usr/sbin/ethtool<br>/sbin/ethtool/mii-tool<br>/usr/sbin/mii-tool |
| XenServer Virtual Machines | /opt/xensource/bin/xe vif-list params=vm-uuid,MAC,device<br>/opt/xensource/bin/xe vm-list params=name-label,networks,power-state,is-control-domain,uuid |
| Cluster Configuration | /usr/bin/clustat -x |
| IBM DB2 Database: | <DB2-Installdir>/adm/db2licm -l |

Instead of configuring a privileged (root) user, you can grant an ordinary user the right to execute the above commands using “sudo”.

JDisc Discovery always attempts to collect information with the least possible access privilege. However, depending on the operating system, a root account might be required.

JDisc Discovery can use SSH login/password or the SSH username/SSH keys to authenticate.

If you don't specify a root/administrative access, JDisc Discovery will not collect all available information. For instance on Linux, JDisc Discovery requires root access to collect model, manufacturer and serial number information from the system BIOS. Accessing the system BIOS requires root access. Without root access this information will not be collected.

## 3.4 Scanning Network Infrastructure Devices

SNMP is the primary protocol for scanning network infrastructure devices such as routers, switches, hubs or networked printers.

While most customers are using SNMPv1 and v2c versions, JDisc Discovery also supports the secure version of SNMP: SNMPv3. Hardware and software information is collected from standard and private manufacturer SNMP MIB tables and variables.