



JDisc Discovery 5.0

Administration Guide

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 out of the use of this information remains with recipient. In no event JDisc GmbH 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 GmbH 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 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 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 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 belong to their respective companies.

© Copyright JDisc GmbH, 2025.

Contents

1 Administration.....	6
1.1 Starter Edition.....	6
1.2 Start/Stop Application.....	6
1.3 Database.....	7
1.3.1 Create A Database Archive.....	7
1.3.2 Scheduled Archives.....	9
1.3.3 Scheduled Database Compact.....	10
1.3.4 Restore A Database Archive.....	10
1.3.5 Clear The Database.....	11
1.3.6 Change The Database Password.....	13
1.3.7 Change The Database Location.....	14
1.4 User Management.....	14
1.4.1 User Authorization.....	15
1.4.1.1 Adding users and groups.....	16
1.4.1.2 users logging in as members of groups.....	17
1.4.2 Permissions Groups.....	17
1.4.2.1 Adding a permissions group.....	17
1.4.2.2 Managing permissions group members.....	18
1.5 Configuring Communication Ports.....	20
1.6 Configuring Invalid MAC addresses.....	20
1.7 Configuring Java Runtime Environment.....	21
1.7.1 Error Recovery.....	21
1.7.2 Configuring Custom Settings.....	22
1.7.2.1 Configuring Maximum Memory Size.....	22
1.7.2.2 Configuring the Discovery Server IP Address on Multi-Homed Servers	23
2 Database Access.....	24
3 Command Line Tools.....	25
3.1 Database Export (XML).....	25
3.2 Database Backup and Restore via batch file.....	25
3.2.1 Credential file.....	25
3.2.2 Database Backup (SQL).....	26
3.2.3 Database Restore (SQL).....	26
4 Security.....	28
4.1 Client Server Communication.....	28
4.1.1 TLS Protocol and Ciphers	28
4.2 Password encryption.....	30
4.3 Database access.....	30
5 Open Source	32

1 Administration

This document explains how to administer JDisc Discovery. Typical administration tasks include starting and stopping of the application, archiving and restoring the database as well as creating user groups and adding users to user groups.

1.1 Starter Edition

Note that the feature-set is limited when using JDisc Discovery 's Starter Edition! The Starter edition does not contain all dialogs or reports described in this manual!

1.2 Start/Stop Application

The Database archive, restore and clear tasks can only be performed when the application has been stopped. Stopping the application will also stop the discovery and most of the reporting and configuration functionality. When JDisc Discovery is stopped only a limited set of administrative tasks can be performed.

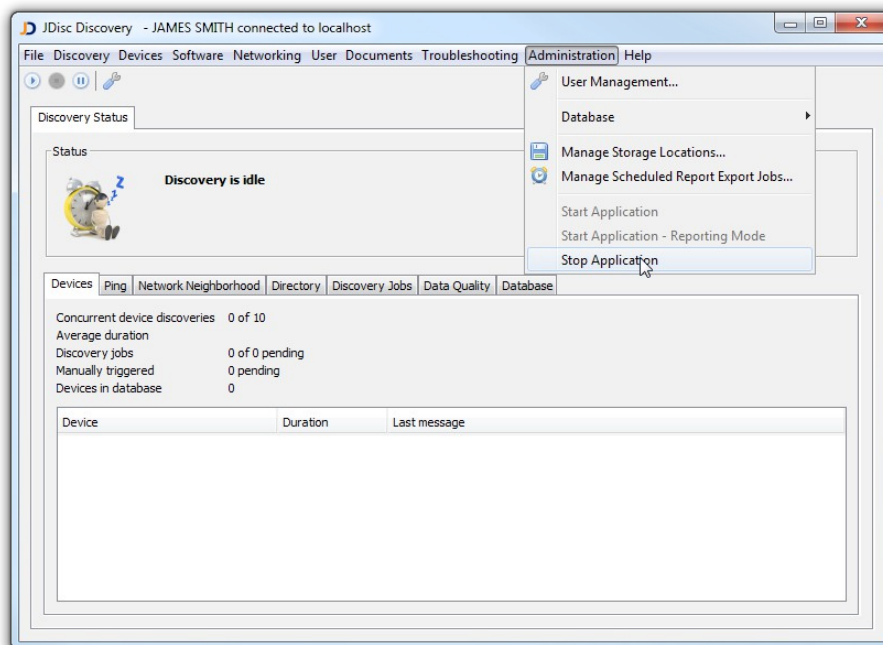


Fig: Stop JDisc Discovery

Stopping JDisc Discovery can take a while when the discovery is running because it

will wait until all pending devices have been discovered.

When starting the application, you can choose among these options:

- *Start Application* to start the application with full functionality.
- *Start Application – Reporting Mode* to view archived data. All discovery and topology jobs are stopped, scheduled compact and archive database activities are suspended and the discovery settings cannot be changed.¹

1.3 Database

Database administration offers archiving, clearing, and restoring of JDisc Discovery's database in addition to changing the database password.

1.3.1 Create A Database Archive

JDisc Discovery allows creating a database archive from its database that can be imported into another installation or for later review. Select *Administration » Database » Archive* to create a database archive. It is recommended, but not required to stop the application first.

Archiving creates a ZIP-file containing a dump of all database table. The ZIP file can be encrypted by providing an encryption password. You may choose to also include login credentials in the database archive. Disable the “Include passwords in the archive” option if you plan taking the database archive outside your company.

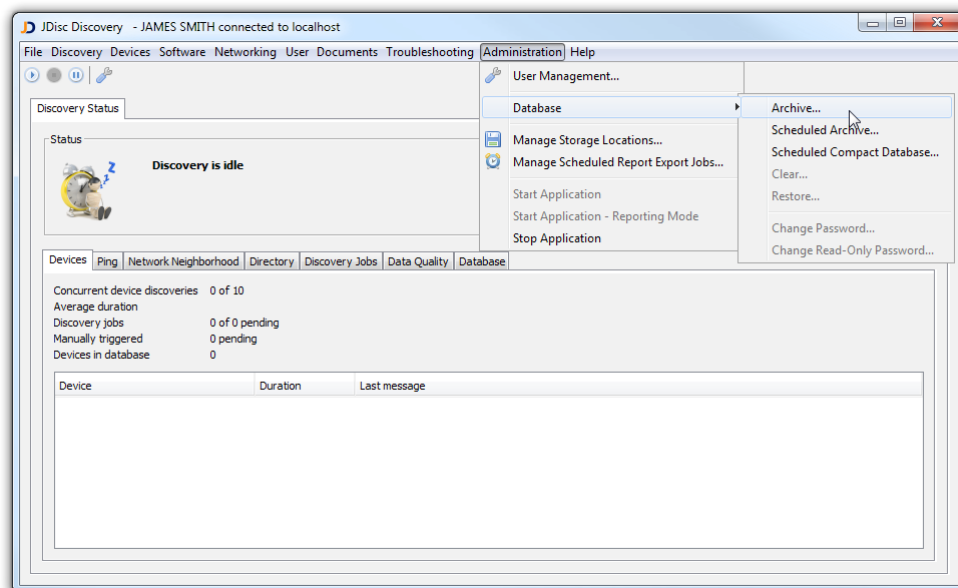


Fig: Create a database archive

¹ This mode is useful to analyze results from IT network assessments.

Including passwords is important for creating database backups. In this case an encryption password is required to create the database archive. The encryption password is converted into an encryption key that is used to crypt all login credentials in the database table dumps. The encryption password is needed to restore a database archive. The database archive cannot be restored without the correct encryption password.

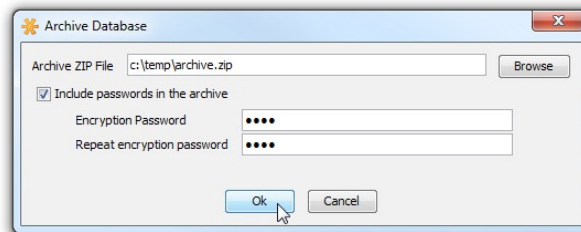


Fig: Database archive options



Use the encryption password to encrypt login credentials in the database archive and to encrypt the resulting ZIP archive.

Depending on the database size archiving can take several minutes.

1.3.2 Scheduled Archives

JDisc Discovery can backup its database on a regular basis to a local directory on the discovery server or to a network share.

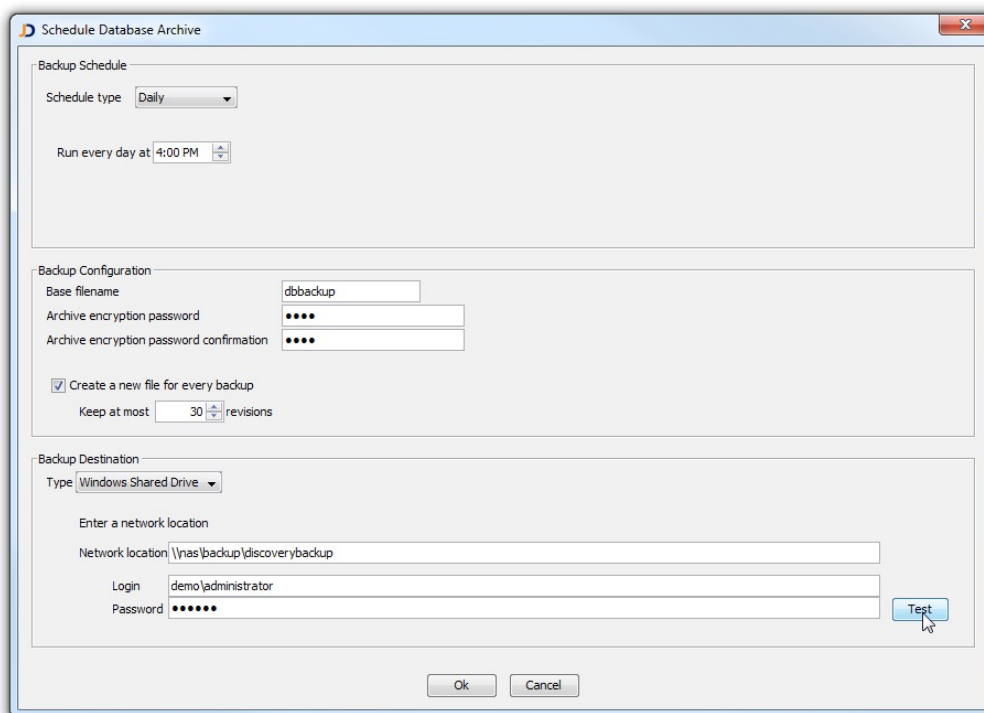


Fig: Scheduled Archive Dialog



It is best practice to schedule the automatic backup at times when the application is idle - when no discovery or device history jobs are running.

Select *Administration » Database » Scheduled Archive* to configure a scheduled database archive job:

- **Schedule**
Configure the database backup schedule in the *Backup Schedule* group.
- **Base filename**
When the *Create a new file for every backup* is turned on, JDisc Discovery appends the time of the database backup to the base filename. Archive files are always .zip files.
- **Archive encryption password**
Access credentials and passwords are encrypted using the archive encryption password. This password is needed to restore the database archive later on.
- **Create a new file for every backup**
When turned on, JDisc Discovery will create new database archive files and does not overwrite an existing database archive file.
- **Backup destination**
Choose a destination directory for the database backup. The destination can be either a local directory on the discovery server or a directory on a network share.

JDisc Discovery creates an event in its event log whenever the database is archived.

1.3.3 Scheduled Database Compact

Most databases need some kind of maintenance to reduce the database size on the disk and to maintain high performance speed. Frequent discoveries and high traffic can cause fragmentation within the database that reduces the overall performance. Schedule a database compact to keep the performance at an optimal level.

Recommended is a database compact every two weeks on large databases (> 3000 devices) and frequent discoveries. On smaller databases with fewer discoveries, a compact once a month is recommended.

Select *Administration » Database » Scheduled Database Compact* to schedule the database maintenance.

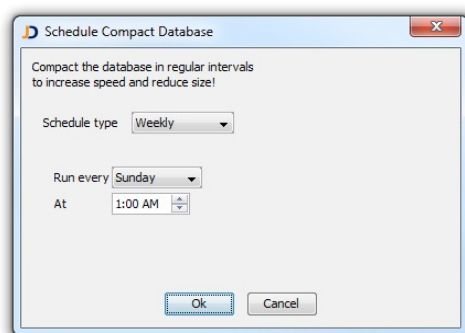


Fig: Schedule Compact Database

1.3.4 Restore A Database Archive

Stop JDisc Discovery and select the *Administration » Database » Restore* to restore a database archive.

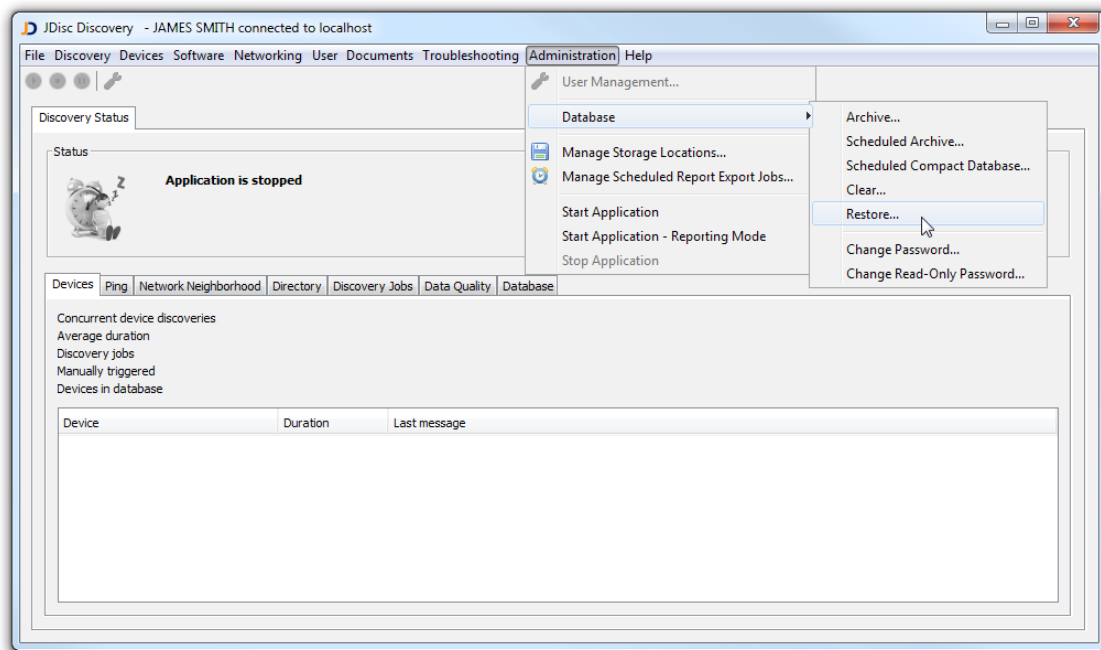


Fig: Restore a database archive

Select the database archive ZIP-file and enter the encryption password when the database archive contains login credentials.



Restoring the database deletes JDisc Discovery's current database content!

Depending on the database size restoring a database archive can take several minutes.

1.3.5 Clear The Database

Stop JDisc Discovery and click *Administration » Database » Clear* to clear the database.

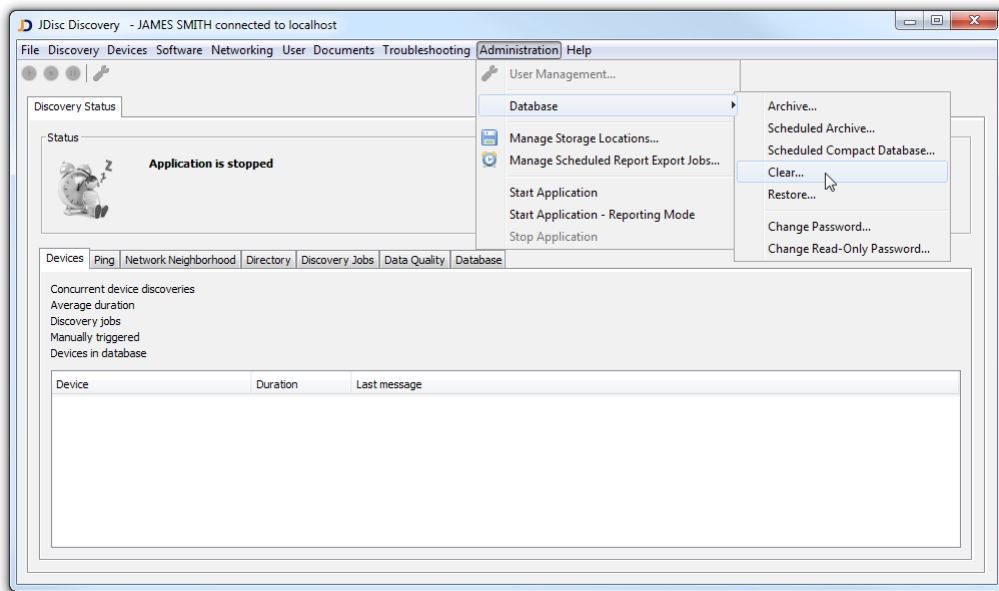


Fig: Clear the database

Clearing the database offers the options below:

- *Discovered data* will delete only discovered device information. It will not delete configured users or the discovery configuration.
- *Discovered data and users* deletes all discovered device information and the users that have access to the product. The user which deletes the database becomes the main administrator for the product.
- *Discovered data and discovery configuration* deletes all discovered device information and the discovery configuration. It will not change the users that have access to the product.
- *All* deletes all information and creates an empty database.

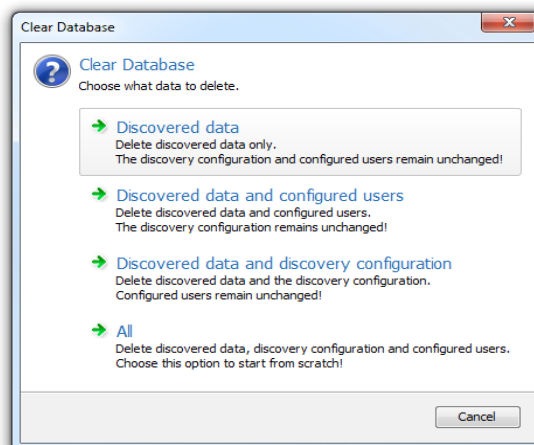


Fig: Clear database options

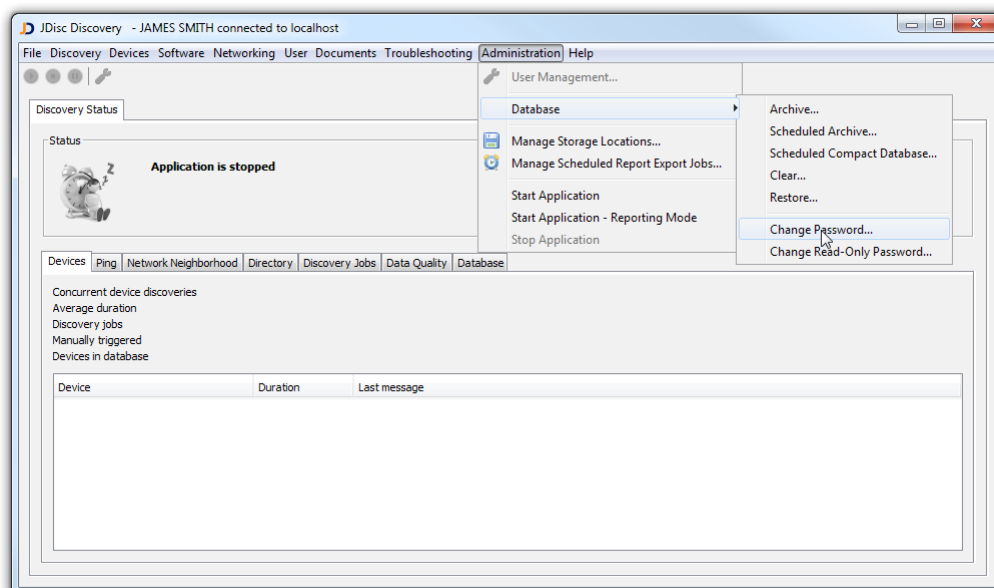
Clearing the database can take several minutes depending on the database size.

1.3.6 Change The Database Password

Stop JDisc Discovery and select the *Administration » Database » Change Password* menu item to change the administrative database password. Select *Administration » Database » Change Read-Only Password* to change the read-only password.

Fig: Change the database password

Set a new database password and repeat the new password to change the current



database password.

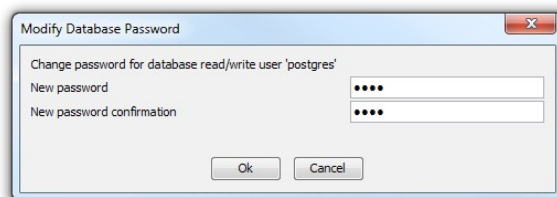


Fig: Set a new database password

1.3.7 Change The Database Location

By default, JDisc Discovery uses the Windows *ProgramData* directory for storing its database. However, the ProgramData directory is by default on the C: drive which is often used for the operating system only.



Always create an archive of your existing database first before you modify any database files!

Follow the steps below in order to move the database to another location or drive.

- IMPORTANT: Create an archive of your database first!
- Stop all JDisc Discovery services (including the database service) from the services control panel
- Enable *Show hidden files* in the Windows file explorer
- Navigate to [c:\ProgramData](#) and copy the *JDisc* folder to the desired location.
- Finally, we need to configure the database service to use the new location. Open regedit and navigate to *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\JDisc Discovery5.0Database*. Edit the entry *ImagePath* and adjust the path behind the -D option. This is the path to the actual database files. It must end with *\ldb* with possibly trailing backslashes.
- Reboot your server in order to use the new service settings
- Finally, we test whether everything is working fine by renaming the old directory. So just rename *c:\ProgramData\JDisc* to *c:\ProgramData\JDisc.old*.
- Restart the JDisc Discovery services again from the service control panel.
- Try to log-on. If you can logon, then everything works fine and you can finally delete the old database folder *c:\ProgramData\JDisc.old*.

1.4 User Management

Access to JDisc Discovery is managed through native Windows user authentication supporting both local and domain users. Domain users can log in to the JDisc Discovery Client and Web User Interface by providing their credentials in any of these formats:

- down-level format (DOMAIN\USERNAME) or
- user principal name format ([username@domain](#))

Local users log in to the JDisc Discovery Client and Web User Interface with their respective (username) only.

1.4.1 User Authorization

User authorization is managed through JDisc Discovery's permissions groups. Permissions groups can be assigned one or more permissions from a predefined set of JDisc Discovery-specific permissions. Windows users and groups (either local or domain) can be assigned to permissions groups to grant them the appropriate permissions.

JDisc Discovery includes two built-in permissions groups that cannot be modified or deleted:

- **Administrators**, who are granted complete access rights
- **Guests**, who have restricted access to viewing reports only



After a fresh installation of JDisc Discovery, the first user to log in through the Product Client or the Web User Interface is automatically granted membership in the Administrators permissions group.

Click *Administration » User Management* to access the *User Management* dialog.

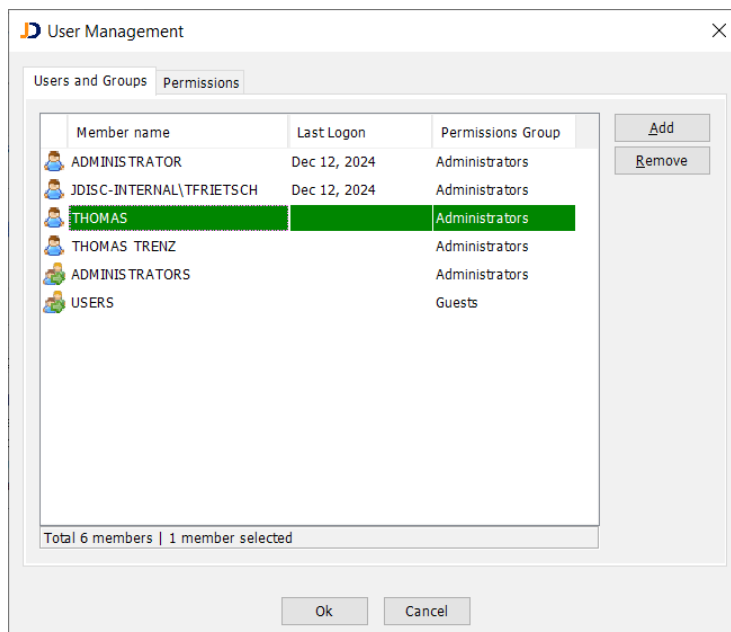


Fig: User Management dialog

The *Users and Groups* tab lists all Windows users and groups that are permitted access to JDisc Discovery. The **Permissions Groups** column shows the membership of each Windows user or group in the respective permissions groups. A more detailed description of the permissions groups is provided in chapter Permissions Groups.

1.4.1.1 Adding Users And Groups

Click the *Add* button to add a Windows user or group and assign it to the selected Permissions Group.

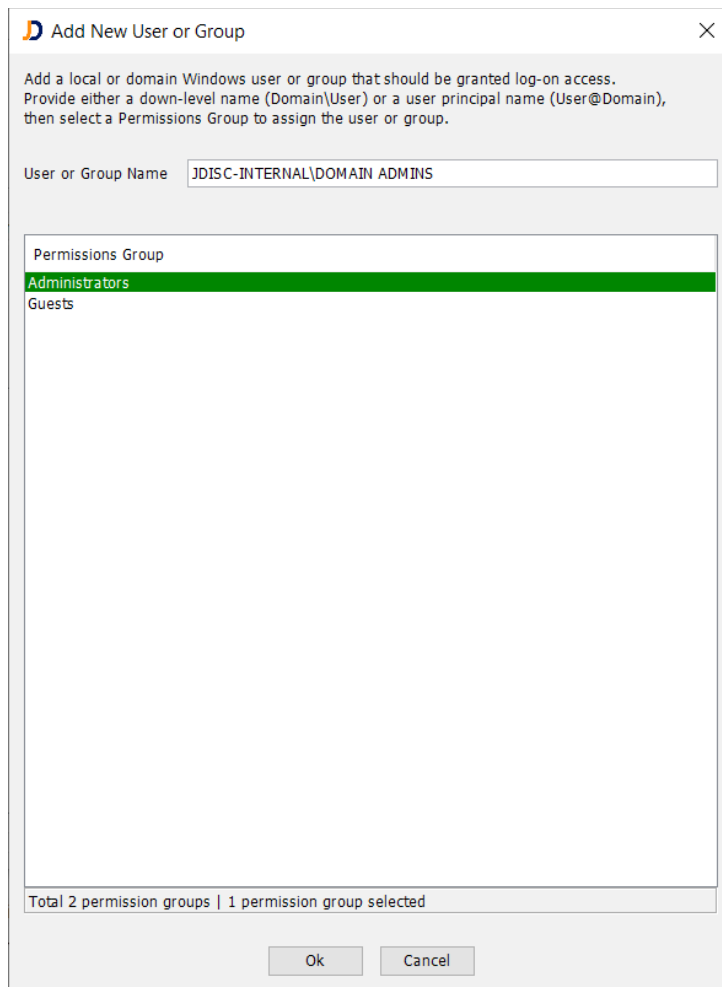


Fig. Add New User or Group



JDisc Discovery verifies whether the user or group name exists in the specified domain or on the local computer.

1.4.1.2 Users Logging In As Members Of Groups

Windows users that are members of configured Windows user groups in JDisc Discovery's **User Management**, can log in without being individually added. When such users log in, JDisc Discovery automatically adds them to **User Management** implicitly.

This is done for the following reasons:

- Each user logged into JDisc Discovery needs a user profile that stores their individual settings, preferences, custom reports, etc.
- Record the date of the last logon for management and transparency purposes.



Implicitly created users are also displayed in the **User Management** dialog-box underneath the **Users and Groups** tab.

1.4.2 Permissions Groups

Permissions groups can be assigned a set of JDisc Discovery-specific permissions. In essence, a permissions group defines the rights that can be granted to native Windows users and groups (either local or domain).

JDisc Discovery includes two built-in permissions groups that cannot be modified or deleted:

- **Administrators**, who are granted all permissions
- **Guests**, who have restricted permissions to viewing reports only

You can create your own permissions groups, configure the necessary permissions, and link them to native Windows users and groups through the **Permissions** tab in the **User Management** dialog.

1.4.2.1 Adding A Permissions Group

From the **Permissions** tab in the **User Management** dialog, click the *Add* button to add a new permissions group.

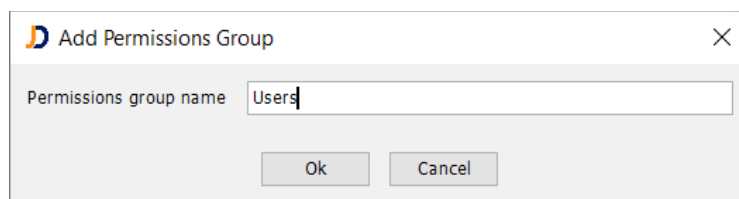


Fig. Add Permissions Group

Provide a name for the new permissions group (e.g., "Users" in this example).

Next, you can update the *Description* field to include a description about the newly created permissions group.

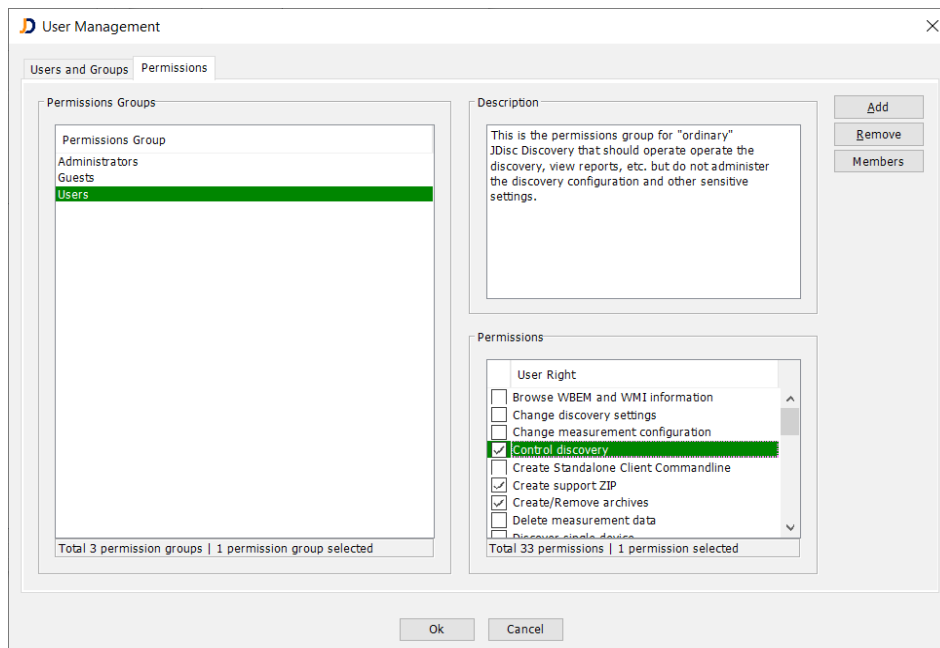


Fig.: User Management Permissions Groups

Finally, you should configure the needed permissions for the newly created permissions group using the *Permissions* panel located in the lower-right area.

Of course, you can modify permission groups just as you would when creating a new one. Additionally, you have the option to delete permission groups if needed.



Built-in permissions groups cannot be deleted or altered.

1.4.2.2 Managing Permissions Group Members

When adding new Windows users and groups, you must associate them with one of the existing permission groups. However, you can also update these associations later on.

In the **User Management** dialog, navigate to the **Permissions** tab, select the permission group whose members (Windows users and groups) you want to modify, and click the *Members* button.

The **Members of Permissions Group** dialog shows the Windows users and groups associated with the selected permissions group.

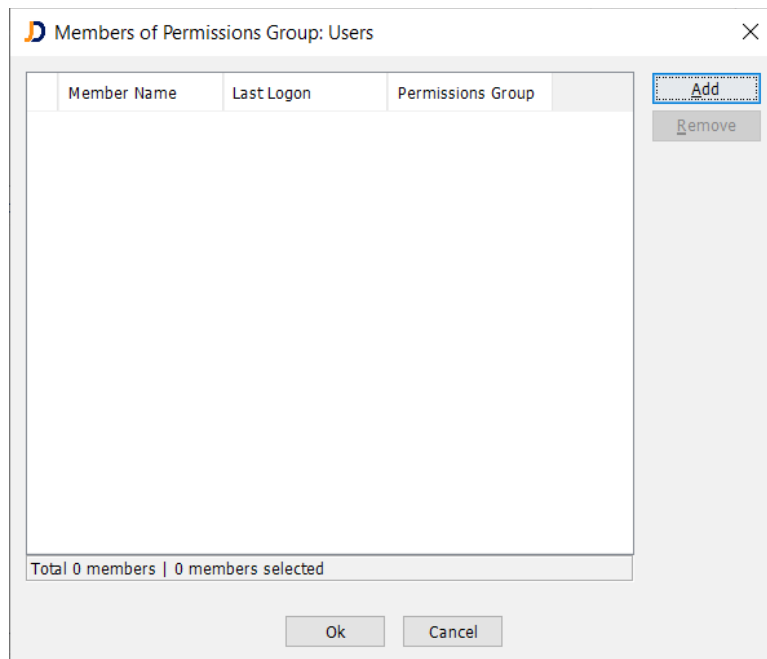


Fig. Manage Members of Permissions Group

To add a new member to the permissions group, click the *Add* button and select the member (Windows user or group).

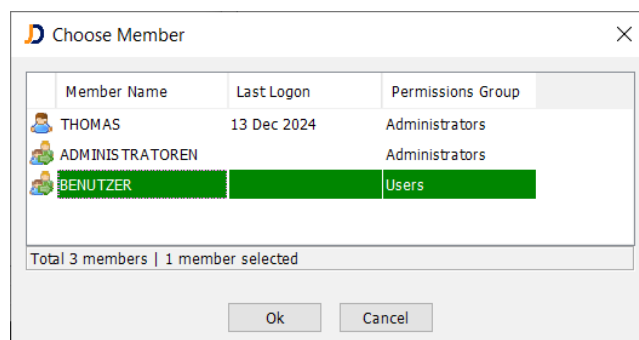


Fig. Add Permissions Group Members

You can also remove members from a permissions group. Just select the member and click the *Remove* button.



If a user or group member belongs to multiple permissions groups, their effective permissions are determined by combining the permissions from all those groups.

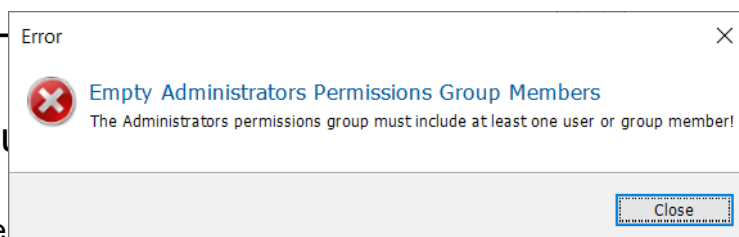


The Administrators permissions group must have at least one user or group member. If all members are removed, the error message

shown below will appear, and you will be unable to save your changes.

1.5 Config

JDisc Discover



vable in its

configuration file. The configuration file is located in the 'config' subdirectory underneath the installation directory and is called 'Config.xml'.

If the default port numbers should conflict with other applications on the computer or firewall rules, change the port numbers for the database and RMI communication. The database port number is defined in the *Database* section.



When you have changed the database port number in the configuration file, also modify the port number in the Postgres configuration file 'postgresql.conf'. The configuration file is located in the 'c:/ProgramData/JDisc/JDiscDiscovery/db' directory. Note that the ProgramData directory is hidden by default! Change the line containing

port = 5432

(change requires restart)

and configure the new port number.

JDisc Discovery uses the Java RMI protocol for client - server communication. Both, the server and the client expose Java objects using the RMI protocol. The *RmiRegistry* section defines two ports. *RegistryPort* defines the server port number and *ClientPort* defines the client's port number.



Do not modify any other settings than the ports.

1.6 Configuring Invalid MAC Addresses

The *MACAddresses.xml* file contains a set of MAC addresses and MAC address patterns that should not be used by JDisc Discovery's discovery for device identification purposes.

JDisc Discovery's discovery assumes a MAC address belong to exactly one device. Although MAC addresses ought be unique, new technologies, such as server-virtualization or hot stand-by protocols override this rule often times and create duplicated MAC addresses. When two or more devices share the same MAC address

and this shared/duplicated MAC address has not been configured as an invalid MAC address, JDisc Discovery's discovery will merge these devices.

1.7 Configuring Java Runtime Environment

JDisc Discovery can use a Java run-time environment (JRE) which is installed by JDisc Discovery's setup program.

JDisc Discovery's stores its JRE runtime configuration parameters in the registry key below:

Windows platform	Registry Key
-------------------------	---------------------

64-bit	HKLM\SOFTWARE\JDisc\JDisc Discovery 5.0\InventoryService64
--------	---

1.7.1 Error Recovery

The registry values in the table below determine how to recover from an unexpected termination of the JVM process.

Parameter	Default Value	Description
JVMAutoRestart	1	Set this value to 1 to automatically restart the JVM process in the event of an unexpected process termination. If the value is set to 0, the JVM process is not automatically restarted in the event of an unexpected process termination.
JVMRestartDelay	10000	The delay in milliseconds to wait before the JVM process restarts.
JVMRestartAttempts	5	The maximum number of restarts when the JVM process ends unexpectedly.
JVMRestartDuration	300000	The restart duration in milliseconds. If the JVM process is restarted

more than "JVMRestartAttempts" times during the restart duration, the 'JDisc Discovery Server' service is stopped and a Windows application event log record is created to indicate an unrecoverable problem.

1.7.2 Configuring Custom Settings

You can add custom JRE parameters using the 'CustomJVMParameters' registry value. Changes to the 'CustomJVMParameters' registry value will be preserved when you upgrade JDisc Discovery.

1.7.2.1 Configuring Maximum Memory Size

When you run JDisc Discovery on a server with plenty of RAM (>4GB) or when you have noticed diagnostic memory messages in the Windows Application Event Log or in the JDisc Discovery standard error log files, you should set the maximum memory size.



The 64 bit JRE uses by default up to 25% of the maximum available physical memory.

Depending on your needs, you can add the Java max. memory size option `-Xmx` to the 'CustomJVMParameters' registry value. The `-Xmx` option needs an integer value as argument that specifies the max. memory size in MB. For example `-Xmx1300M` means a max. memory size of 1300 MB. The option `-Xmx4G` means a max. memory size of 4GB.



When you have changed the JRE configuration by editing the 'CustomJVMParameters' registry value, restart the 'JDisc Discovery Server' service to make your changes effective.

1.7.2.2 Configuring The Discovery Server IP Address On Multi-Homed Servers

When you run JDisc Discovery on a multi-homed server, you might need to bind the IP address of the network interface (NIC) to the discovery process, which is most publicly available. This is important for :

- Establishing the communication between the JDisc Discovery User Interface Client and the JDisc Discovery Server.
- Some protocols to get information from devices on the network.

To configure the most publicly available IP address of your JDisc Discovery Server,

add the following parameters (separated with a blank) to the 'CustomJVMParameters' value:

- `-Djava.rmi.server.hostname=<IP address>`
- `-Dcom.jdisc.discovery.ip=<IP address>`

and restart the JDisc Discovery Server service.

2 Database Access

JDisk Discovery stores its data in a Postgres database instance that is installed and configured by JDisk Discovery's installation program. The installation program creates two users:

1. The administrative user 'postgres'. JDisk Discovery connects to the database using this user to write discovery results to the database and to run queries for the user interface.
2. The read-only user 'postgresro'. JDisk Discovery does not use this user. However this user can be used to integrate JDisk Discovery's data with other products.

JDisk Discovery currently uses postgres version 9.2.4. You find all kind of drivers for the postgres database on its homepage <http://www.postgresql.org>.

3 Command Line Tools

3.1 Database Export (XML)

In cases, a direct database access is not suitable or desired, JDisc Discovery can export its data as an XML file. The XML file includes (except some product internal information) all discovered data.

To protect sensitive information, all passwords are encrypted with a encryption password.

Start the export from a console window. Change to the JDisc Discovery bin-directory and call

```
XmlExport <encryptionPwd> <DestinationFile>
```

The export might take some time depending on the number of devices in JDisc Discovery's database.

You find the schema definition for the XML file in the 'schemas' directory within JDisc Discovery's home directory.

3.2 Database Backup And Restore Via Batch File

3.2.1 Credential File

Optional you can create a credential file for later use with the Database Backup and Restore. Both scripts have a -credentials option for this generated file.

```
CreateCredentialFile [-output credential file] [-user user] [-password password] [-encryptionPassword encryption password]
```

- output credential file name of the credential file to write or stdout if it is missing

- user user JDisc (Windows) username

- password password JDisc (Windows) password

- encryptionPassword encryption password Password for encrypting the passwords in the database

The credential file contains the user and the encrypted passwords. If no user or passwords are given on the commandline they are asked on the console.

3.2.2 Database Backup (SQL)

It is possible to make a database backup for a later database restore. The database backup is stored in a ZIP file as a bunch of SQL files. The passwords in the database are encrypted.

Start the backup from a console window. Change to the JDisc Discovery bin-directory and call

```
DatabaseBackup [-host host] [-port port] [-clientPort clientPort] [-  
credentials credential file] -output outputfile.zip [-overwrite]
```

where

-host JDisc server host (default localhost)

-port port for the JDisc server host

-clientPort port for sending the output file to the client. This is only necessary if special ports are blocked by a firewall (default a random port)

-output name of the output zip-file

-overwrite overwrite outputfile if exists otherwise fails

-credentials credentials name of a file containing credentials. First line is the username, second line the password, third line the encryption password for the passwords in the database. The credential file must be generated with the CreateCredentialFile.bat before because the passwords have to be encrypted. If the parameter is missed, they are prompted at console.

The backup might take some time depending on the number of devices in JDisc Discovery's database.

3.2.3 Database Restore (SQL)

To restore the database from an earlier backup, change to the JDisc Discovery bin-directory and call

```
DatabaseRestore [-host host] [-port port] [-clientPort clientPort] [-  
credentials credential file] -input inputfile.zip
```

where

-host JDisc server host (default localhost)

-port Port for the JDisc server host

-clientPort port for sending the output file to the client. This is only necessary if special ports are blocked by a firewall (default a random port)

-input inputfile.zip name of the input file

-credentials credentials name of a file containing credentials. First line is the username, second line the password, third line the encryption password for the passwords in the database. The credential file must be generated with the CreateCredentialFile.bat before because the passwords have to be encrypted. If the parameter is missed, they are prompted at console.

The backup might take some time depending on the number of devices in the backup file.

4 Security

Discovery products including JDisc Discovery require security sensitive information, such as administrative/root accounts or domain administrator accounts to collect detailed device information. Therefore it is critical to store and transmit this type of data securely.

4.1 Client Server Communication

JDisc Discovery uses Java RMI for client – server communication. RMI calls that transmit login credentials are encrypted using TLS and are not visible for network packet sniffing and capturing tools, such as Wireshark.



RMI over TLS protects JDisc Discovery's communication from network sniffing tools such as Wireshark.

4.1.1 TLS Protocol And Ciphers

The table lists all available protocols and ciphers to protect the Java RMI client – server communication. The protocol and cipher marked in bold is configured by default.

Protocols	Ciphers
TLSv1.3	TLS_AES_256_GCM_SHA384
TLSv1.2	TLS_AES_128_GCM_SHA256
TLSv1.1	TLS_CHACHA20_POLY1305_SHA256
TLSv1	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
SSLv3	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
SSLv2Hello	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256

	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
	TLS_DHE_DSS_WITH_AES_256_CBC_SHA
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA
	TLS_DHE_DSS_WITH_AES_128_CBC_SHA
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
	TLS_RSA_WITH_AES_256_GCM_SHA384
	TLS_RSA_WITH_AES_128_GCM_SHA256
	TLS_RSA_WITH_AES_256_CBC_SHA256
	TLS_RSA_WITH_AES_128_CBC_SHA256
	TLS_RSA_WITH_AES_256_CBC_SHA
	TLS_RSA_WITH_AES_128_CBC_SHA,TLS_EMPTY_RENEGOTIATION_INFO_SCSV

You can change the protocol and cipher configuration by editing the 'JVMPParameters' value that is located below the 'InventoryService64' registry key as outlined in the table below.

Windows platform	Registry Key
64-bit	HKLM\SOFTWARE\JDisc\JDisc Discovery 5.0\InventoryService64

To set the protocol, edit the value in quotes following the equal-sign of

`-Djavax.rmi.ssl.SslRMIServerSocketFactory.cipherSuites`

To set the cipher, edit the value in quotes following the equal-sign of

`-Djavax.rmi.ssl.SslRMIServerSocketFactory.protocols`



When you have changed the protocols/cipher configuration by editing the 'JVMPParameters' registry value, restart the 'JDisc Discovery Server' service to make your changes effective.

4.2 Password Encryption

Login credentials are stored encrypted in JDisc Discovery's database using a 128-bit AES encryption algorithm.

JDisc Discovery's installation program creates a 128-bit unique AES encryption key that is being used to encrypt login credentials in the database. This unique 128-bit AES encryption key is stored in JDisc Discovery's configuration file encrypted using a 128-bit computer specific encryption key. The 128-bit computer specific encryption key is based on hardware and operating system specific attributes .

Login credentials are protected even if an “attacker” could copy the binary database files and configuration files to another computer. The “attacker” could not decrypt the 128-bit unique AES encryption key because the unique 128-bit computer specific encryption key would be different.

The database archive and restore feature provide the only means to transfer a database between computers running JDisc Discovery's. Refer to the Administration section for more details.



Passwords are stored encrypted as cipher-text in the database.

4.3 Database Access

JDisc Discovery uses the Postgres database system (<http://www.postgresql.org>) to store it's data. Access to the database is protected by the database password entered when installing JDisc Discovery. The database password can be changed using JDisc

Discovery's administration menu. Refer to the Administration section for more details.

The database password is stored encrypted in JDisc Discovery's configuration file using the 128-bit computer specific encryption described in chapter 4.2 Password encryption.

Even if an “attacker” could copy JDisc Discovery's configuration file to another computer, the unique 128-bit computer specific encryption keys are different and prevent decoding the database password to remotely access the Postgres database server.



The database password is stored encrypted as cipher-text in JDisc Discovery's configuration file.

5 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'.
- This product includes the 'SBLIM' WBEM implementation.
- 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 trilead SSH library (http://www.trilead.com/Products/Trilead_SSH_for_Java).
- 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.