H+H Software GmbH

Administration Manual
Data protection

NetMan 5

Modern application and information management

Version 5.8

H+H Software GmbH

Maschmühlenweg 8-10
37073 Göttingen
Telefon: +49 551 52208-0
Telefax: +49 551 52208-25

hh@hh-software.com
www.hh-software.com

Contents

Introduction

This manual explains the data privacy features of the software NetMan. It will help you to comply with your legal obligations regarding data protection.

Help Conventions

In this manual, we use specific notation to highlight facts for you:

Note, identifies issues that you should be aware of**.**

Tip, identifies important tips and hints for working with NetMan. Shows how you can simplify things or avoid problems in advance.

Definition, denotes the definition or explanation of a particular term or subject, or introduces a subject**.**

In some parts of this manual, we explain examples step by step to make various procedures understandable. The individual steps are marked as follows:

Step 1

<Description to step 1>

Step 2

<Description to step 2>

In addition to these specially marked information or work steps, there are also the following presentation formats that are particularly highlighted in the text:

- Controls or buttons
- **Titles/names**
- **`User Inputs / PC Outputs / Code Examples / Software Terms`**
- *References*

Data Protection in NetMan

Any form of data protection begins in the structuring of the data-processing software. NetMan offers the following technical and organizational measures for data protection:

- NetMan is installed on your server. The hosting and thus the data processing is in the hands of your institution.
- Any data transmission over the Internet is encrypted (HTTPS).
- Authentication/authorization mechanisms and ticketing procedures secure working with NetMan.
- NetMan follows the principle of reduction and economy in the processing of personal data (data reduction/data economy): Only such data is collected and stored as is necessary for the execution of NetMan or the statistical evaluation.
- Access to the administrative and data processing functions of NetMan requires authentication (username and password).
- The central NetMan Database is password protected.
- NetMan offers an anonymization function for personal log data. This is configurable and protected according to the 4-eyes principle.
- Log data (except for the usage log, which can be anonymized) is automatically deleted.
- System processes can be closely monitored and analyzed using monitoring tools.
- User accounts are password protected.
    - 2-factor authentication (optional)
- NetMan is operated on one or more dedicated servers. An evaluation of the collected data with third-party software does not take place.
- Entries and changes to personal data in NetMan are logged.
- The use of data carriers on data processing systems is restricted (client-drive filter).
- With Program Control, only approved processes can be started. This prevents malware from being installed or executed.
- NetMan is designed for continuous operation (24 hours/7 days).
- High availability can be achieved using the NetMan Replication Mechanism. The NetMan Replication Mechanism is a chargeable additional service.

As part of the installation, we document your specific settings. You will find an overview of the contents of the installation report in the *Appendix*.

Initial Startup

After the installation of NetMan it is necessary to protect your system and especially your data from unauthorized access.

- **NetMan Database:** The database is the heart of your NetMan Installation. All data is stored in the database. After installation, the database is protected by an automatically generated password. On how to set the password for the database, read the chapter *Password Protection of the Database*. The replication mechanism protects your system against failure. You can read about the basics of the failover mechanism in the *Failover by Replication* chapter.
- **Anonymous logging:** NetMan anonymizes user and computer data in the call log by default. This simplifies your data processing in that you can freely evaluate anonymized log data statistically. You then do not have to worry about the personal reference. The settings of the anonymization function are protected by password protection according to the 4-eyes principle. This means that you can assign 2 passwords to 2 employees and the setting can only be changed if both employees each enter their password. You can read how to configure this password protection in the chapter *Protect Anonymous Logging*.

Data protection practice

- **Correct, block, delete data:** When processing personal data, you are obliged to keep the data up to date. This results in the obligation to correct outdated or incorrect data immediately. You are also obliged to immediately delete data of persons who no longer participate in the process NetMan without delay. In the event of a dispute or pending legal proceedings, it may be necessary to block the data. For information on how to correct, block or delete data, see the chapter *Correct, Lock, Delete*.
- **Create data disclosure:** According to the Data Protection Act, you are obligated to provide data information upon request, if a person affected by data processing by your office demands it. For information on how to create a data disclosure in the software, please refer to the chapter *Data Subject Rights and Creating Data Disclosure*.
- An overview of all types of in NetMan processed personal data can be found in the *Appendix*.

Password Protection of the Database

The central database of NetMan contains all data used by NetMan. Therefore, it is important to protect access to the database with a strong password. After installation, the database is protected with a randomly generated default password. You change the database password in the NetMan system settings.

1 Open Windows Control Panel

Open the Windows Control Panel.

2 Open System and Safety/H+H NetMan

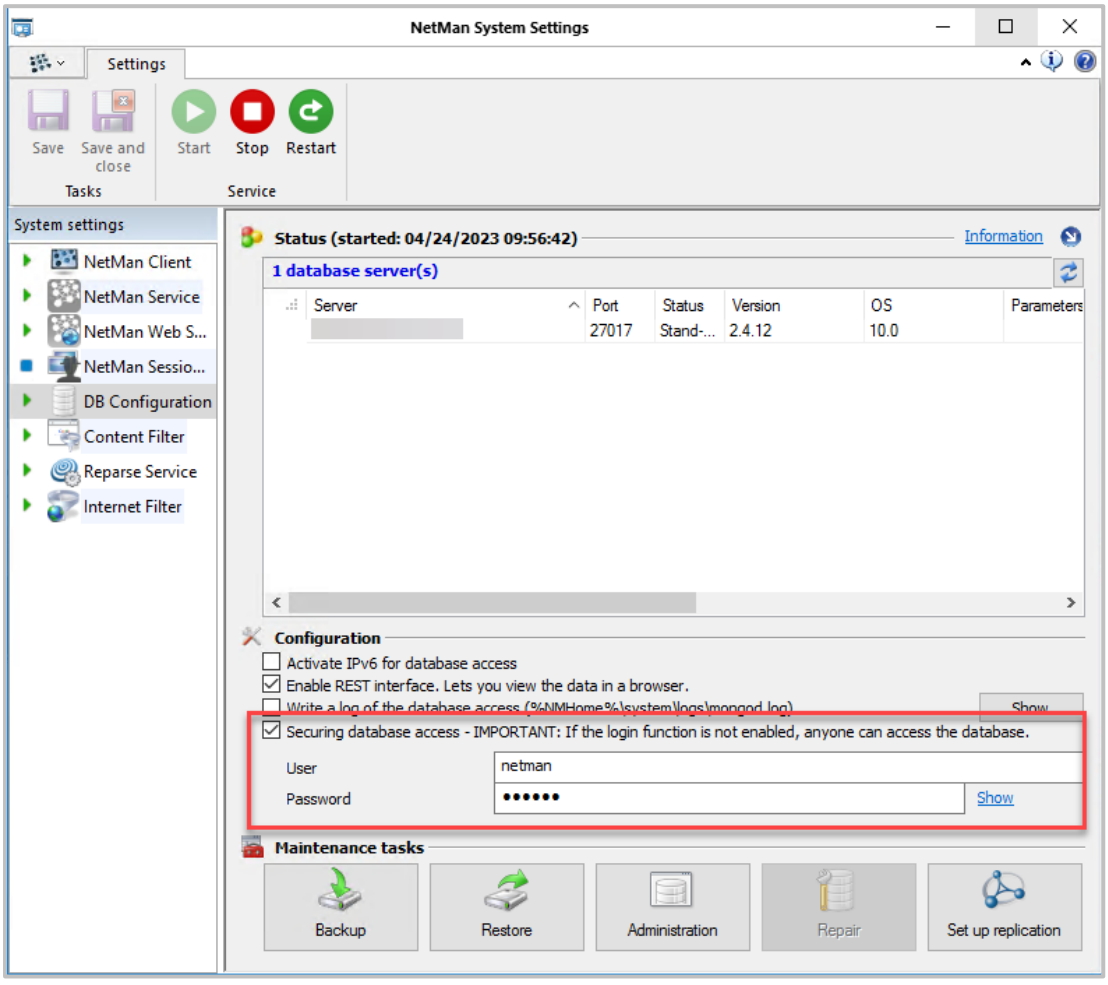
In the Control Panel, select **System and Security/H+H NetMan**.

3 Open DB configuration

In the NetMan System Settings open the **DB configuration** page.

4 Secure database access

On the **DB Configuration** page, the option **Securing database access** has to be active.



5 Enter username and password

Next to **User**, enter the username of the authorized user, and next to **Password**, enter the password that secures database access.

A strong password is one for which the effort to crack it exceeds the real benefit. The BSI gives the following tips for creating strong passwords: at least eight characters long, upper and lower case letters, special characters and digits, no names of family

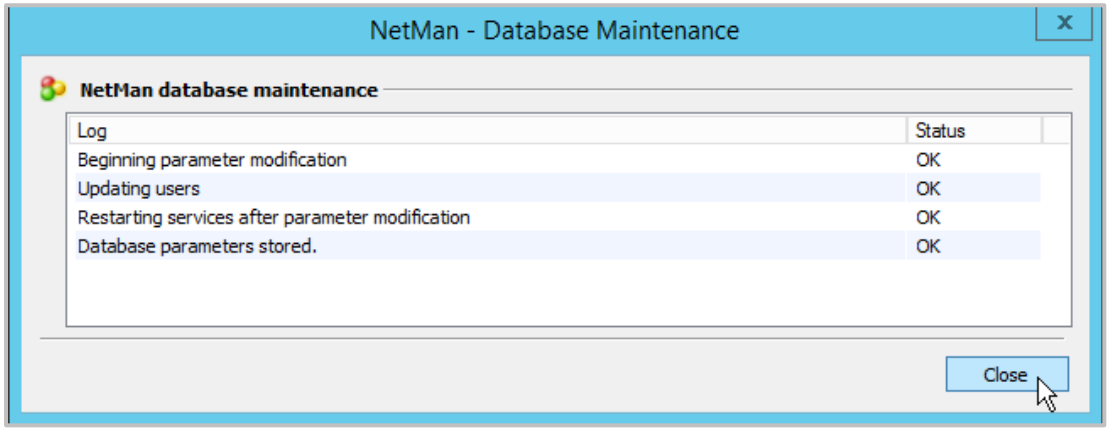
members, pets or birthdays of these, no words from dictionaries, no sequences of numbers or digits (123, abc), no keyboard patterns (qwerty), no simply appending digits or special characters to words (love1). Also, avoid umlauts, as they cannot be easily entered on foreign keyboard layouts. Detailed information on password security can be found on the *BSI Creating Secure Passwords website*.

6 Save changes

Click the Save button in the ribbon. The changes are written to the database and the Database Service is restarted automatically.

7 Close dialog

Click Close to close the maintenance dialog. The login data has been changed.



Failover by Replication

This chapter gives you an overview of how the NetMan Replication Mechanism works.

The NetMan Replication Mechanism realizes fail-safety for your NetMan system. Failover ultimately enables the availability and integrity of your data.

If you decide to use replication in your NetMan system, the system will be set up accordingly by the H+H installation team.

Basics

The basis of the Replication Mechanism is the NetMan Database that supports asynchronous replication of data between database servers. Only one database server writes data, the primary database server. All database servers are merged into one replica set. A replica set consists of

at least three servers: one primary and two secondary database servers. Additional secondary database servers can be added, but the total number of database servers (primary plus secondary) has always to be odd (i.e. 3, 5, 7, etc.)! In a system with three servers, a total of one server can fail, in a system with five servers, two, and so on. On the primary database server NetMan is fully installed as the primary installation. A secondary NetMan Installation is performed on the two secondary database servers.

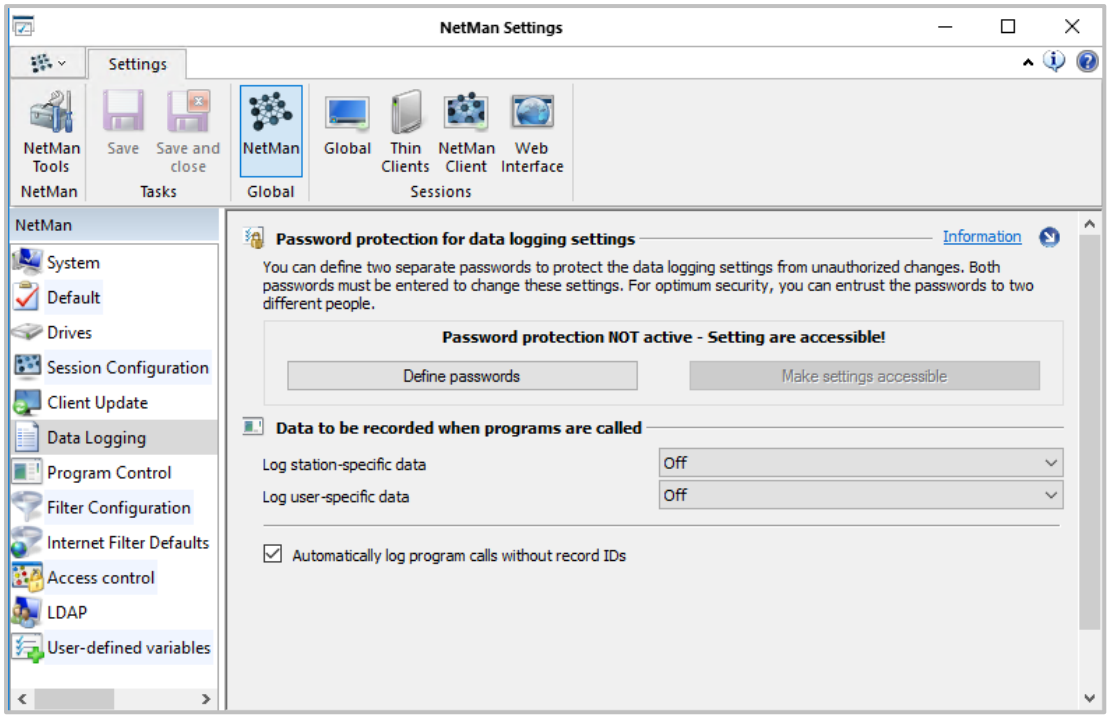
Functionality

The NetMan Database maps the failure safety. Decisive for the question when a server is down is the NetMan Service. If the NetMan Service on the primary database server is no longer accessible, the database is also no longer accessible. The server is considered to be down and the failover mechanisms kick in. The secondary servers elect a new primary database server to take over the tasks of the failed server.

The replication of the NetMan Data refers only to the content of the NetMan Database! In order to map the failover as desired, you have to ensure that a new primary NetMan Server also has access to all resources that were available to the failed server. The NetMan Replication includes only the NetMan system components, no third-party programs. So, to implement replication, ideally you should systematically separate your NetMan server and your remote desktop session hosts. Failure of applications deployed through your session hosts is not taken into account by the NetMan Replication Mechanism. Data required by scripts to perform their function should be stored in the database.

Protect Anonymous Logging

A core function of NetMan is the logging of program calls and related data. Knowing who worked with an application, when and for how long, and whether they had to wait for the application to start (queue) provides important information, e.g. about the utilization of your product licenses. However, logging personal data for statistics is not without risk. If a data subject subsequently objected to the use of his or her personal data, you would theoretically have to delete your entire statistical database, since the data could not be separated from the rest of the data restrospectively. Therefore NetMan logs usage data by default without specifying the user or computer. You configure this anonymization mechanism in the NetMan Settings, in the section **NetMan** on the **Logging** page.



The screenshot above shows the state after installation: Station and username logging **(log station-specific data** and **log user-specific data**) is disabled. This setting protects you from unauthorized access by restricting access. NetMan offers password protection according to the 4-eyes principle. You define 2 passwords and assign them to 2 different people. This increases security enormously, because it is now no longer enough to be in possession of 1 password.

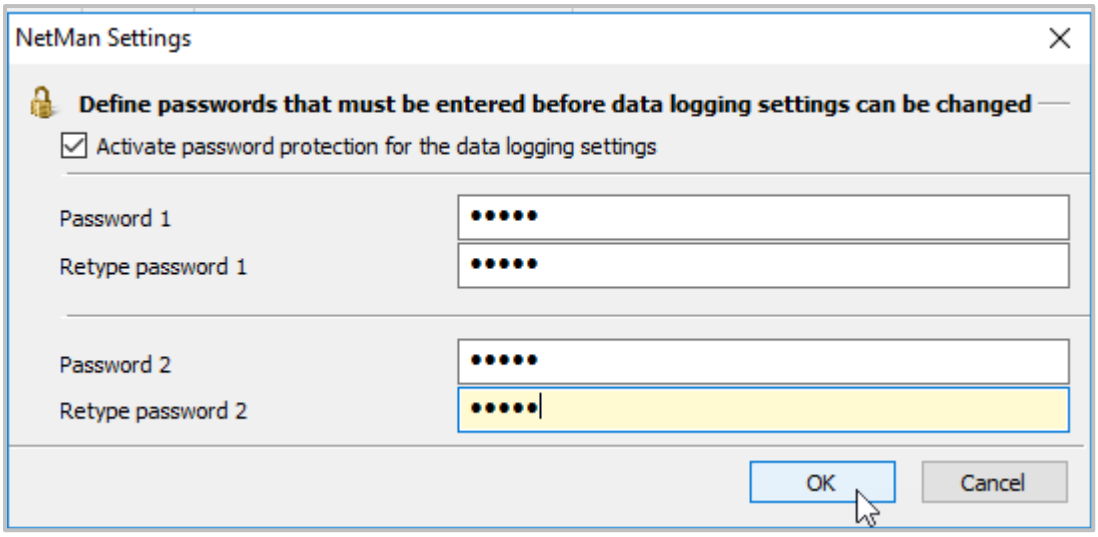
Set passwords

1 Set passwords

Click the Define passwords button.

2 Enter and confirm passwords

In the **Define passwords that must be entered before data logging settings can be changed** dialog, enter two passwords and confirm by clicking OK.

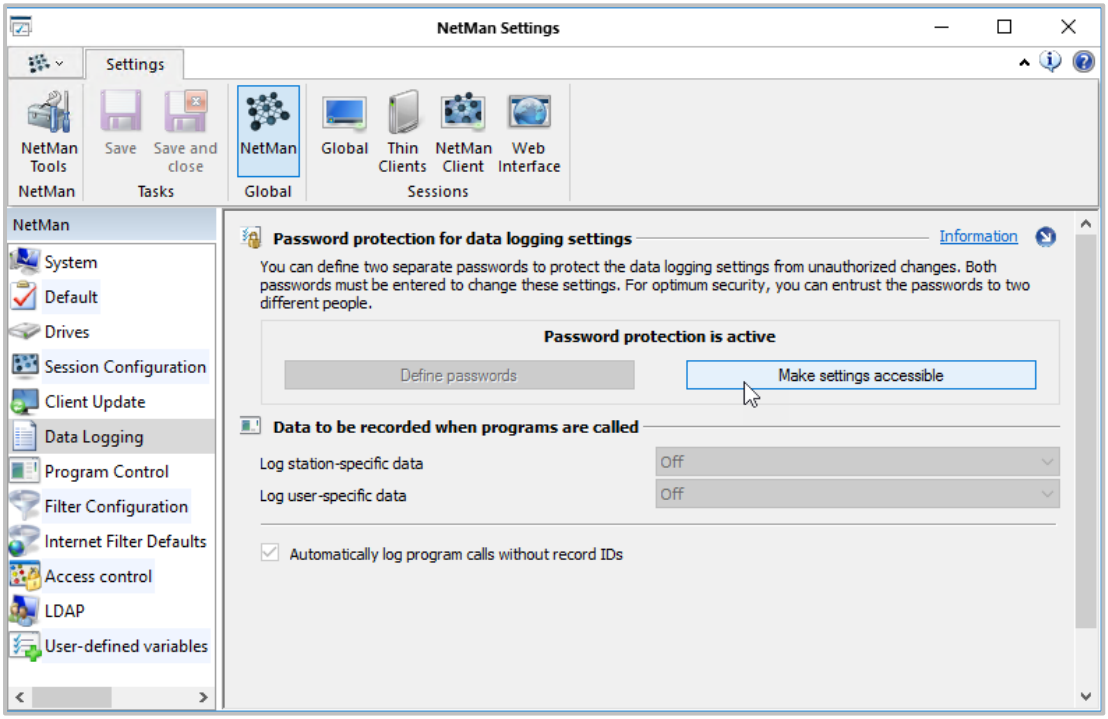


3 Save

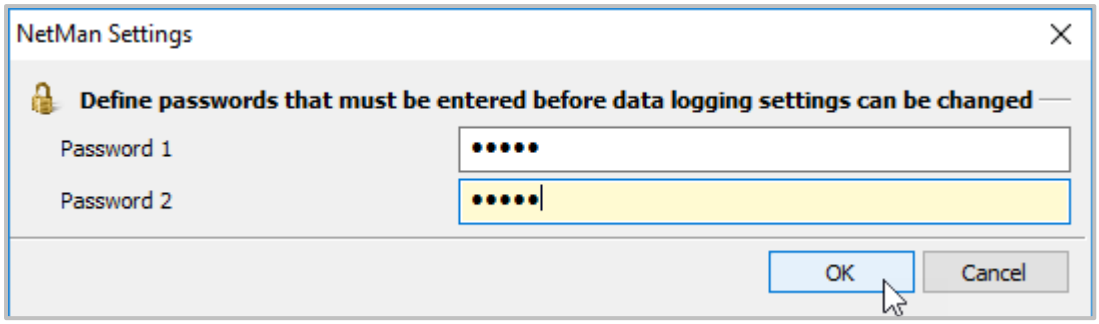
Click Save in the ribbon. The log settings are locked.

4 Unlocking the log settings

To unlock and change the log settings, select **Make settings accessible**.



In the following dialog you have to enter both passwords.



Correct, Lock, Delete

This chapter shows you how to correct, block and delete personal data in NetMan.

Correct data

If you learn of an error in personal data, you are obligated to correct this error immediately. This is best done via the NetMan Programs. You need either appropriate access rights yourself or the help of a person with administrative rights in the process NetMan.

For more information, read the following chapters:

- *Data Storage Locations* shows where in NetMan personal data can be stored.
- To learn how to lock personal data, see the *Restrict Data Processing/Block Data* chapter.
- For information on how to delete personal data and when personal data in NetMan are automatically deleted, read the chapter *Deletion Periods/Deleting Data*.

Data Storage Locations

To correct, block or delete personal data in NetMan, you first need to know where to find which personal data in the software.

All data is stored in the central NetMan Database. The database is password protected. However, instead of direct access to the database, access via the NetMan Programs is recommended, as this puts the data in the corresponding context.

Data storage locations in NetMan

System:

- Windows User Group - the Windows User Group is a property of the AD user object on the domain controller.
- Windows Active Directory Organizational Unit (AD-OU) - The AD-OU is a property of the AD user object on the domain controller.

- Windows User Profile - In the Windows User Profile all data of the working environment of the respective user are stored. User profiles are stored on the NetMan server for each user.
- Windows Logon Script - NetMan supports the use of Windows Logon Scripts, but does not use them by itself. A logon script is a property of the AD user object on the domain controller.
- Web Service access log: **`\\NetMan Server\NM5\Bin\WebSrv\logs`**
- Database: **`NetManServer\HH\NMS5\db`**; therein:
  - **`logs`**: Log files
  - **`data`**: Database records.

NetMan Center:

- NetMan User Group
- NetMan User Profile
- Time of last login
- NetMan User Settings; therein:
  - NetMan Startup Setting (optional)
  - Language (optional)
  - Start script (optional)
  - End script (optional)
  - Windows Start Menu (optional)
  - Windows Desktop (optional)
  - Web Interface (optional)
  - Maximum allowed parallel sessions (optional)

  These settings are mostly set via the user profile and are then not person-related, but only have a reference to the user profile.

- Contact details; therein:
  - Username
  - Address (optional)
  - Department (optional)
  - E-mail addresses (2) (optional)
  - Phone numbers (2) (optional)
  - NetMan autostart script (optional)
  - Fully qualified domain name
  - User SID
  - Description (optional)
- Object properties (see *Special case: Object properties* section for details).

The aforementioned data is consistently personal data that is defined directly in the NetMan Center and entered by NetMan administrators. The corresponding administrators have full access to the data. Not all of this data has to be set!

NetMan Protocols:

- Call log: script calls including log ID, timestamp (start and stop), user (only if set), computer, log attributes
- Internet Filter log: log, timestamp, user, computer, application, URL, Internet Filter status, Content Filter status.
- Internet Filter error log: Timestamp, user, computer, application
- Content Filter: performance log
- Program Control: program, timestamp, path, user, computer
- NetMan Web Service: access log
- NetMan Web Service: error log

In the NetMan Monitor you can see the currently logged in sessions and license usage. No export function is integrated here, the current actual state is shown.

All logs are shown in the NetMan Log Viewer, which is available via the NetMan Report Center, to which NetMan administrators have access.

Special case: object properties

Each object in NetMan can be assigned object properties. Object properties consist of an identifier and a value. They can be edited with the actions **Read object property** and **Set object property**. They are freely defined, therefore personal data can theoretically also be defined here for user objects. Check your NetMan configuration concept to see if you use object properties to store personal information. Object properties can be found in the **properties** dialog on the P**roperties** page. Double-click the user object to open the properties. The properties also show the data from the Contact page, except for the address.

Restrict Data Processing/Block Data

The new concept of **restriction of processing (restriction)** introduced in the GDPR corresponds to that of blocking as used in data protection law prior to 2016.

If there are ambiguities regarding data processing, errors have been discovered or objections are raised, it may be necessary to restrict data of a user for processing, specifically, to block this data set so that no further data processing can take place.

In advance: Not all data of a user within NetMan can be locked. It is not possible to block log data if its time of creation is in the past. This would distort the statistical evaluation of usage data to such an extent that a meaningful evaluation of the usage of NetMan would no longer be possible. Therefore, blocking a user in this context only has the effect that no further log data of this user is collected. However, most log data, with the exception of pure usage data, is deleted/overwritten at a certain time interval or can be deleted manually. How log data of the user is deleted can be read in the chapter *Deletion periods/Deleting data*.

To lock user data, it is **frozen** at the last state and the user is then removed from the NetMan system.

The NetMan Center has a **restrict function** for user objects. This automatically exports user objects for you.

To learn how to export user data, see the *Exporting User Data* section. To learn how to delete users, see the *Deleting Users* section. All user data is saved on an external storage medium, e.g. a USB stick, and can thus be fed back into the system if required.

You have to first lock the user in your AD to prevent the user from logging into the system again. Re-logging in would create a new user object in NetMan and generate new data eventually.

Exporting user data

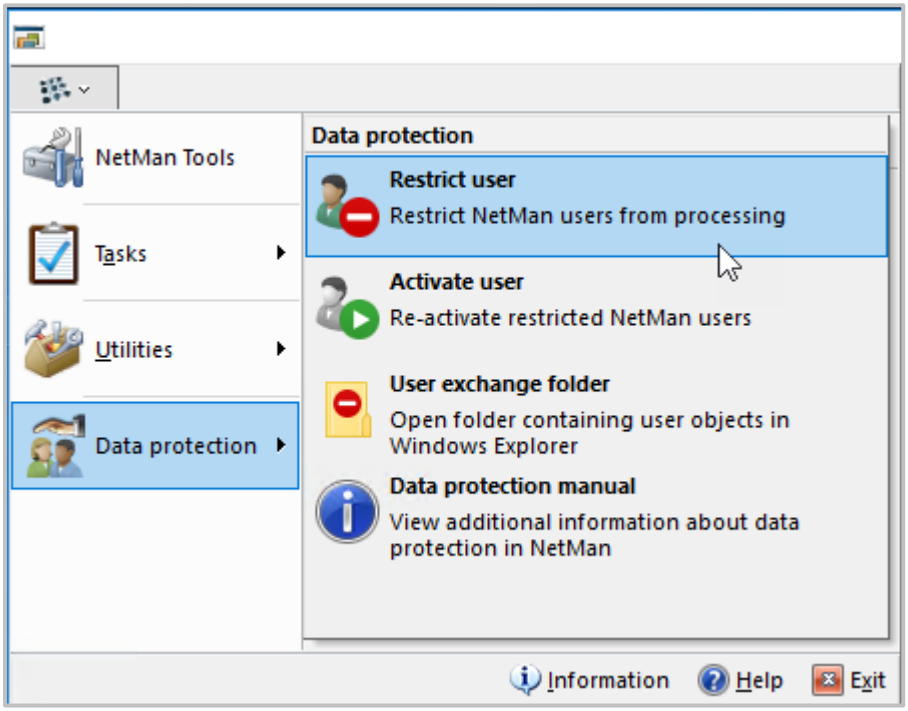
You can export user data from NetMan Center.

NetMan Center

In the NetMan Center you restrict and lock the user objects. You open the NetMan Center via the desktop shortcut **NetMan Tools**.

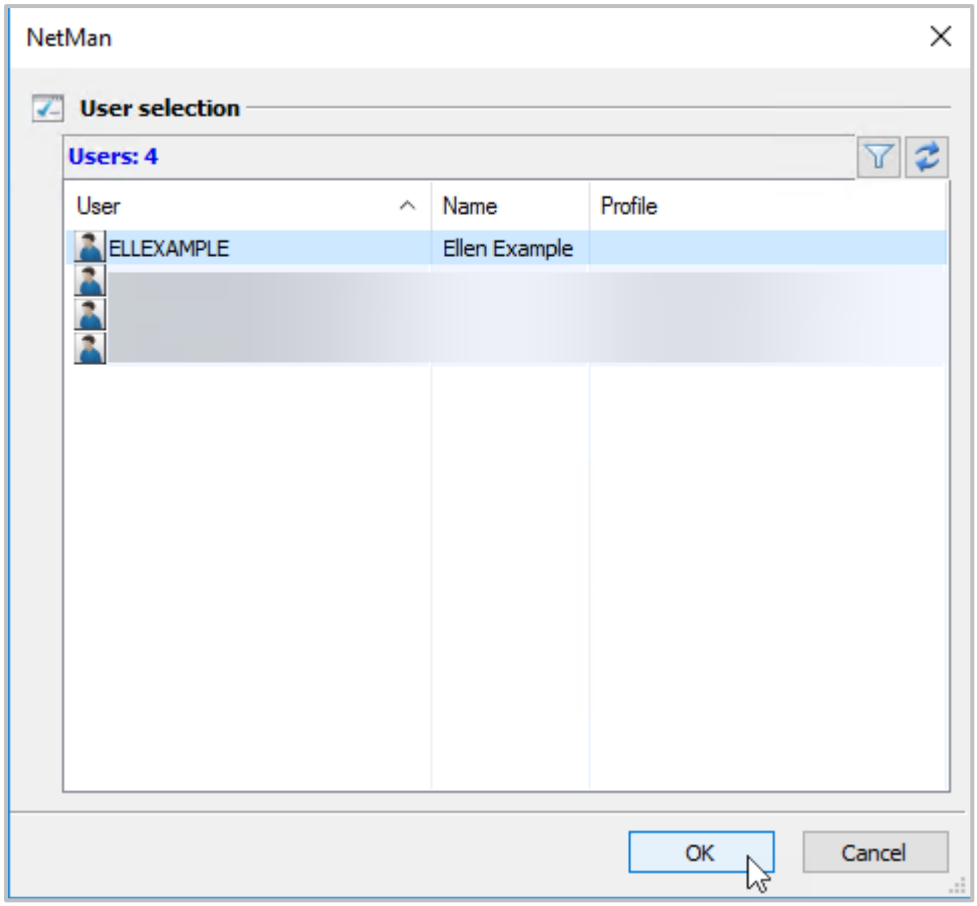
1 Data protection/Restrict user

In the NetMan Center, select in the program menu Data protection / Restrict user.

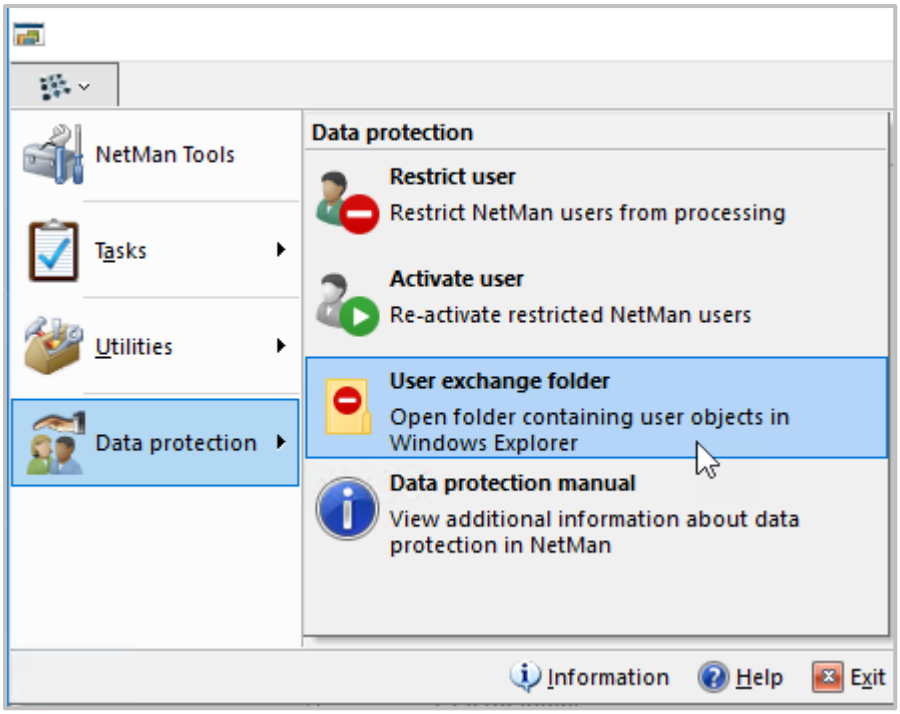


2 Select user

In the **User selection** dialog, select the user and confirm with OK.

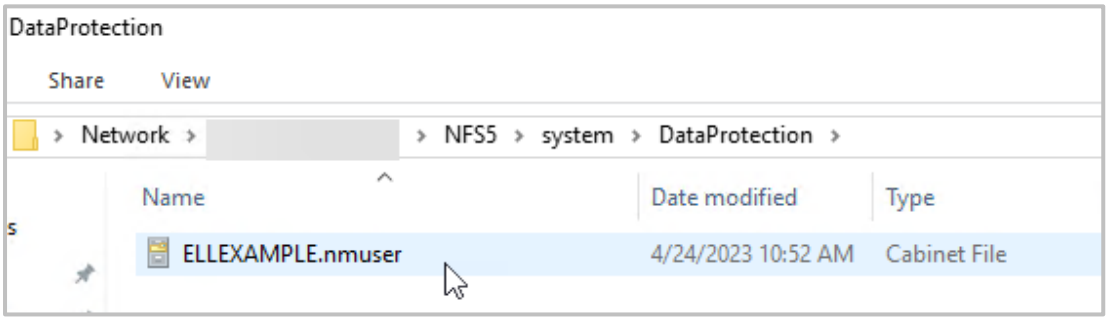


The user object is exported as a CAB file and deleted from the NetMan Center. You open the exchange folder by selecting Data protection / User exchange folder from the program menu. From here you can transfer the CAB file to an external storage medium.



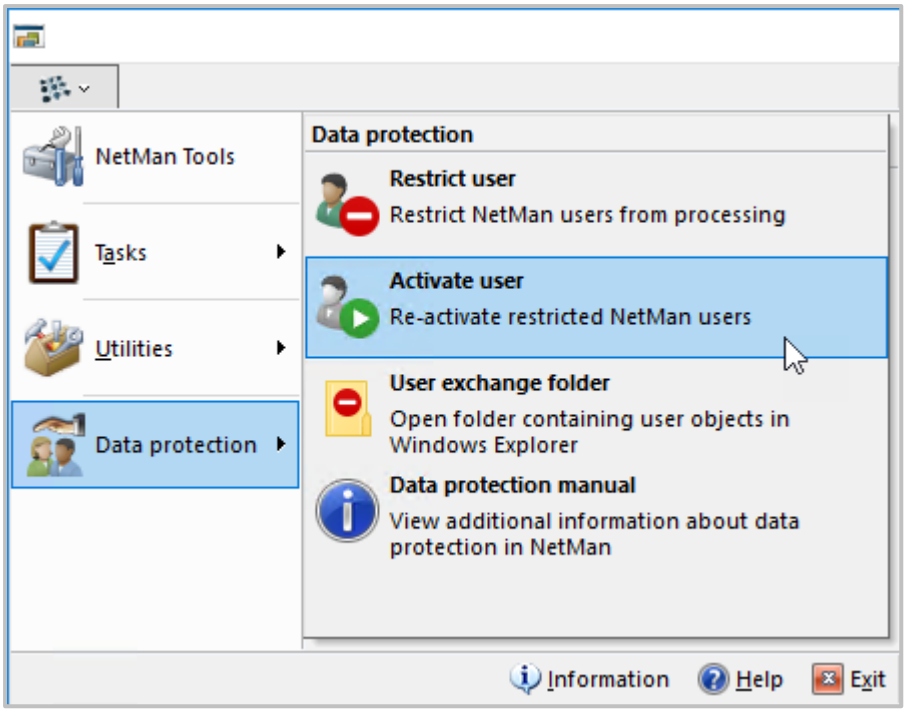
Re-Import

To re-import user objects, open the user exchange folder – either via the NetMan Center or manually (**\\<NetMan Server>\NM5\system\DataProtection**). Copy the object into it. After that import.



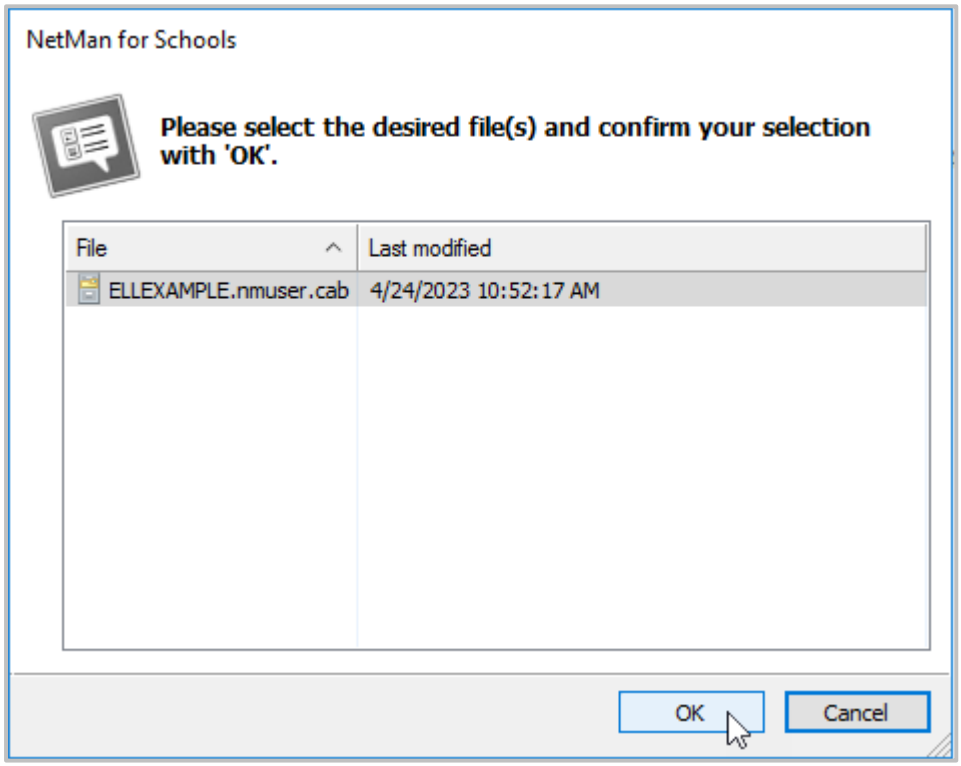
1 Open Data protection/Activate user

In NetMan Center open the program menu and select Data protection/Activate user.



2 Select and import user object

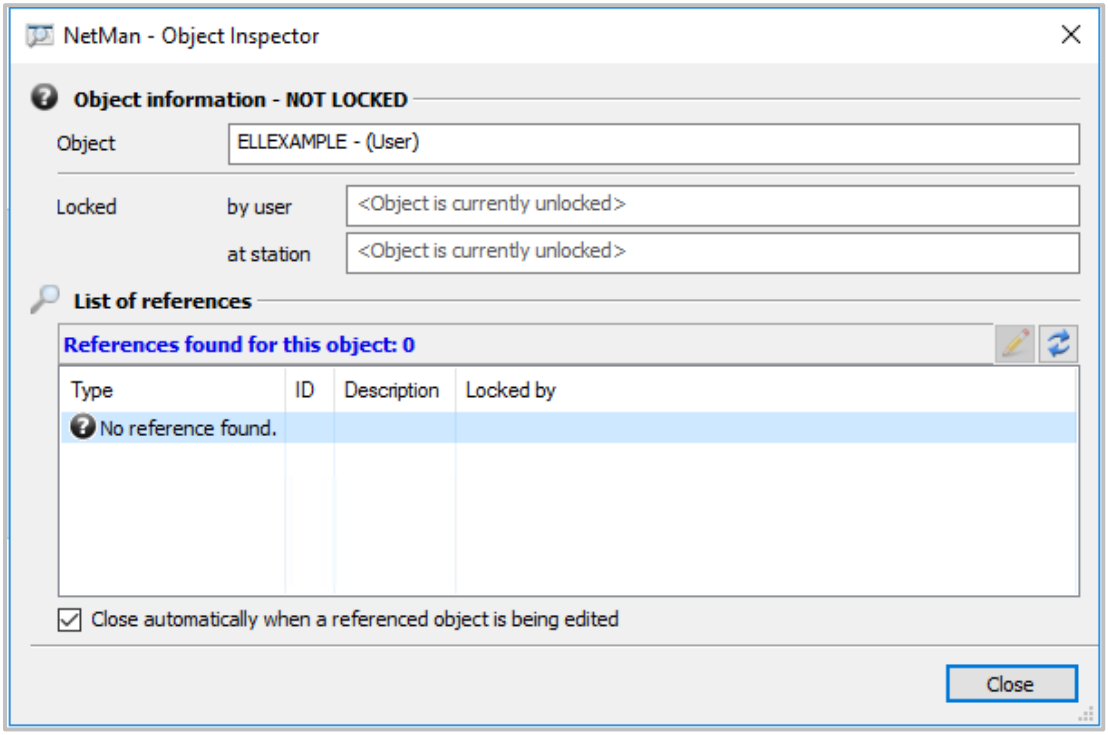
In the Import dialog, select the user object and click OK to import the object.



Deleting users

In the NetMan Center, delete users by selecting the corresponding user object and clicking the Delete button in the ribbon. When restricting users, the user object is automatically deleted after export via the **restrict function**.

The user object can only be deleted in the NetMan Center if it is no longer referenced by other objects, e.g. groups. Before deleting, you have to resolve all references. You show the references by selecting the user object and clicking the Used by button in the ribbon.



Deletion Periods/Delete Data

In NetMan the data of the call log, which is indispensable for the statistical evaluation of the use of the system, is collected anonymously if desired. This makes a later statistical evaluation possible. However, the event and error logs also collect and store information about the station and user. Without this data, no analysis would be possible in the event of an error.

Either an automatic deletion mechanism or a manual deletion function has been implemented for this data. Read below to find out in which logs personal data is collected and stored and how it is deleted:

NetMan Web Service: The NetMan Web Service has an access log and an error log. It is possible that the log shows data that has a personal reference.

You delete the log manually in the NetMan System Settings, on the **NetMan Web Service** page.

Event Viewer: You can see the Event Viewer in the NetMan Log Viewer. Events related to users or stations are logged in plain text for the error case.

Event Viewer data is automatically deleted after 70 days.

Internet Filter log: You can see the Internet Filter log in the NetMan Log Viewer. It shows all accesses via the Internet Filter. This information is security-relevant and therefore includes details of the station and user.

Data in the Internet Filter log is automatically deleted after 42 days.

Internet Filter error log: You can see the Internet Filter error log in the NetMan Log Viewer. It shows all error cases of the Internet Filter. This information is security-relevant and the username and station ID must be recognizable for error analysis.

Data in the Internet Filter error log is automatically overwritten after 42 days.

Performance log: You can see the performance log in the NetMan Log Viewer. The performance log analyzes performance and utilization of all stations in your network. This requires logging of the station ID.

Data in the performance log is automatically deleted after 14 days.

Program Control: You can see the log of the Program Control in the NetMan Log Viewer. The Program Control prevents that programs can be started past NetMan. The Program Control log lists all cases where Program Control was triggered. Username and station are logged. This information is relevant to security.

Data in the Program Control log is automatically deleted after 42 days.

Privacy log: You can see the privacy log in the NetMan Log Viewer. In the privacy log, actions on user objects are logged. For this purpose, the names of the user objects are listed. The privacy log is not deleted.

WebDAV log: You can see the WebDAV log in the NetMan Log Viewer. The WebDAV log records access to the NetMan system via WebDAV. For the purpose of traceability, the username and the accessing IP address are logged.

Data in the WebDAV log is automatically deleted after 42 days.

WebDAV Lock Log: You can see the WebDAV lock log in the NetMan Log Viewer. In the WebDAV lock log, you can see all current WebDAV locks (resources locked due to usage). For the purpose of traceability, the owner (user) is logged.

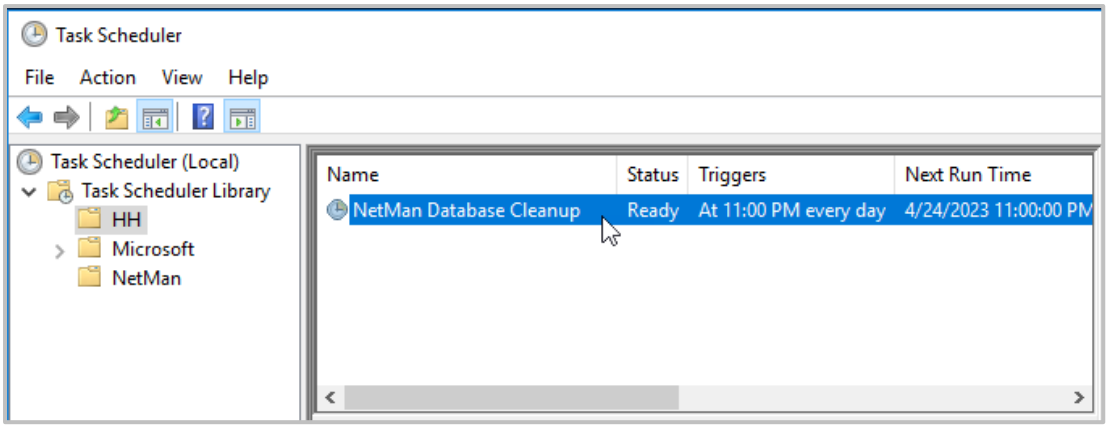
Data in the WebDAV lock log is deleted 1 second after the respective resource is released (no caching).

Configure Deletion Period Internet Filter Protocol

Most deletion periods are set directly in the database and can be configured there if necessary. You configure the deletion period for the Internet Filter protocol via Windows task scheduling.

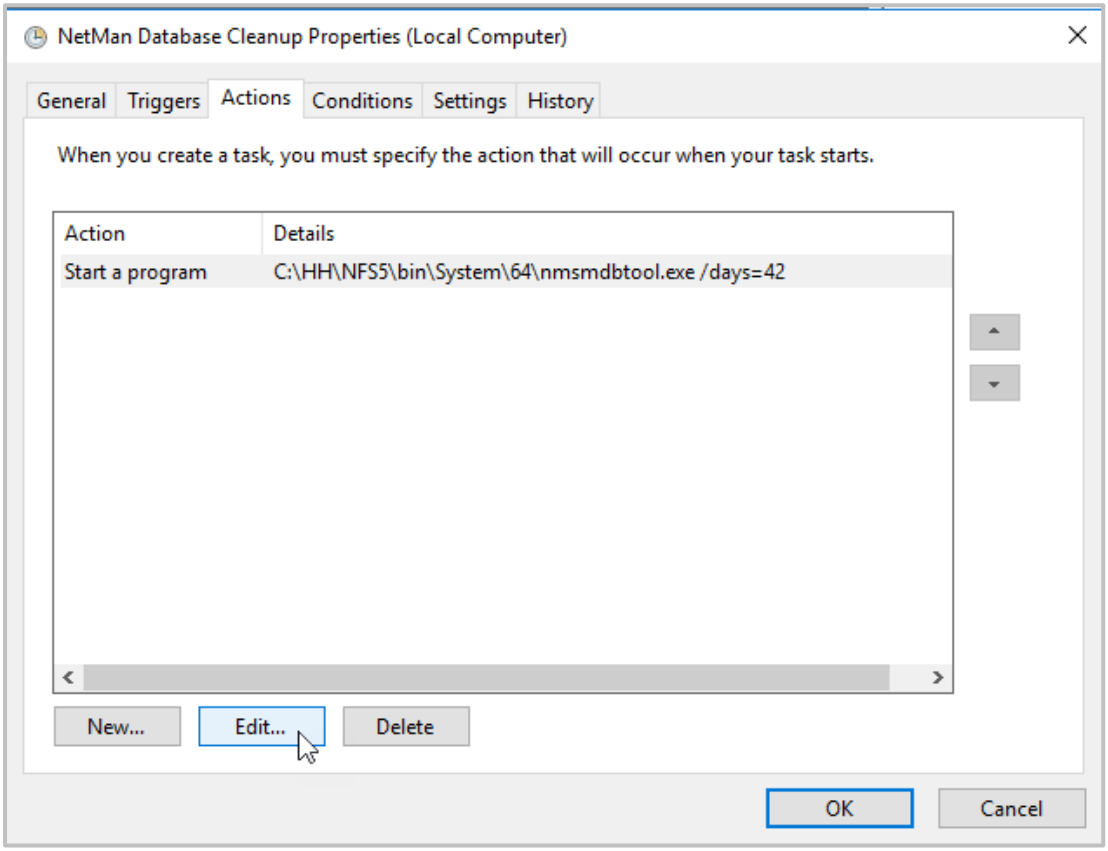
1 Task Scheduler/HH NetMan Database Cleanup

Open the Windows **Task Scheduler** on your NetMan Server. In the task scheduling library, select the HH folder. In it you will find the task **NetMan Database Cleanup**. Double-click the task NetMan Database Cleanup to open the task properties.



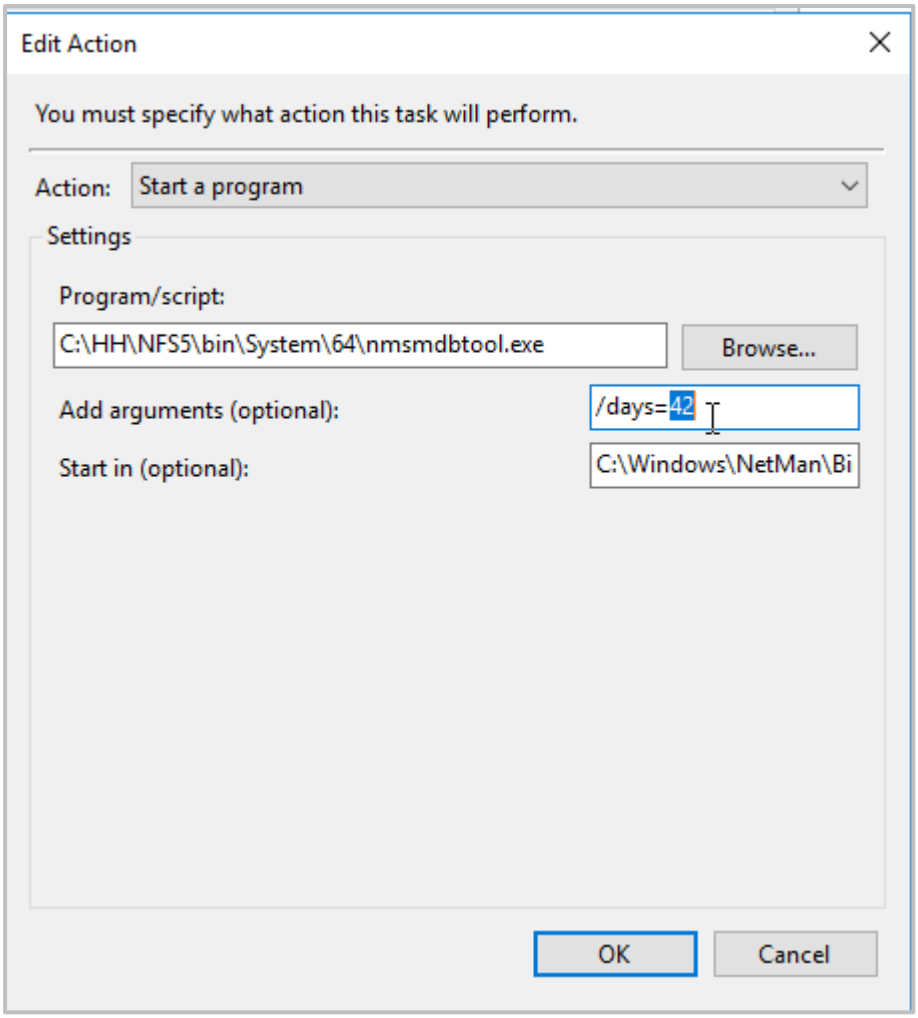
2 Properties NetMan Database Cleanup

In the **Properties** dialog of **NetMan Database Cleanup** select the **Actions** tab. There click Edit.



3 Edit Action

In the **Edit Action** dialog, change the deletion interval by changing the number after **/days=** next to **Add arguments (optional)**. The preset default value is **42**.



Confirm your change with OK.

Logging of Data Protection Operations

NetMan logs data protection operations (create, delete, lock, reactivate users) so that you can meet your legal documentation obligations. You can find the Data Protection log in the Log Viewer.

1 Open NetMan Tools

Open the NetMan Tools via the desktop shortcut of the same name.

2 Select Report Center

Select NetMan Report Center and click OK.

3 Log in

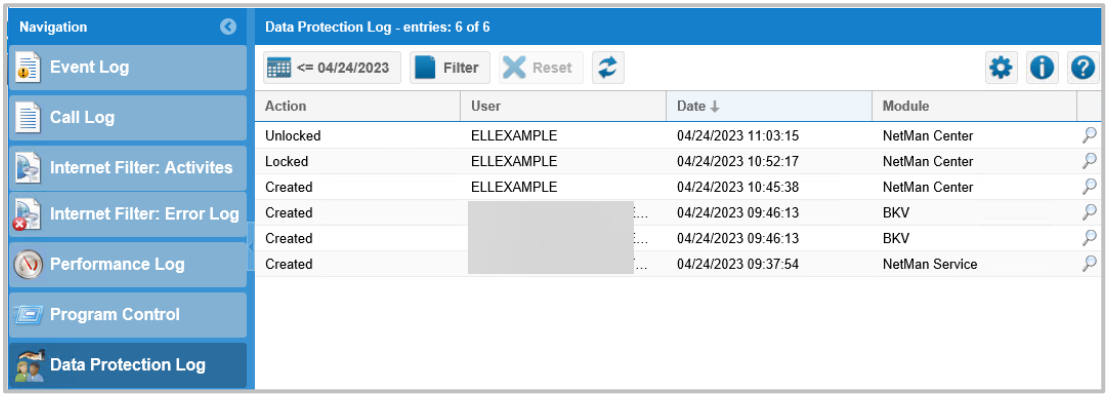
Log in. To log in, you need administrative rights or access rights to the statistical analysis of NetMan.

4 Open Log Viewer

In the Report Center, select **Log Viewer**.

5 Open Data Protection log

In the Log Viewer, switch to the **Data Protection Log** page.



Here you can see all data protection operations concerning user objects in the NetMan system logged.

Data Subject Rights and Creating Data Disclosure

Persons affected by data processing have a right to information as to which of their personal data is being collected, stored and processed in specialized procedures. You determine internally in your institution which person(s) are authorized to provide data information. In order to collect all data, the assistance of additional employees with administrative rights is required.

A data disclosure does not automatically list all data that is stored and processed for a specific person. In the request for data disclosure, the data subject needs to state which data he or she wishes to be informed about.

No information must be provided about personal data that serves data security or data protection control purposes. This applies, for example, to system logs that ensure error-free operation of the NetMan process and thus serve to ensure the integrity of the data collected. Basically, the following type of data is defined for NetMan about which information is provided:

- **Personal data/contact data:** This type of data can be found in NetMan Center, each assigned to the corresponding user object.

The prerequisite for data disclosure is the request of the person concerned. Ensure the identity of the claimant. The request can be made informally. The time of the request must be recorded. The request can only ask for the type of data or request a copy of the raw data. The form in which the information is provided must correspond to the request. It can be made orally, in writing or electronically.

The following chapters explain the procedure for creating a data report:

Export Personal Data/Contact Data shows how to export personal data and contact data from the NetMan Center.

Statistics: create a view, print shows how to create and print a user-specific view, if you log usage data in plain text.

Export Personal/Contact Data

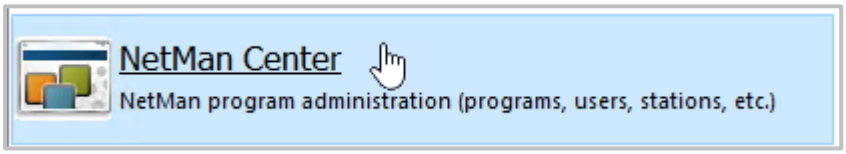
This chapter shows how to export personal and contact data from the NetMan Center.

NetMan Center

1 Open NetMan Center

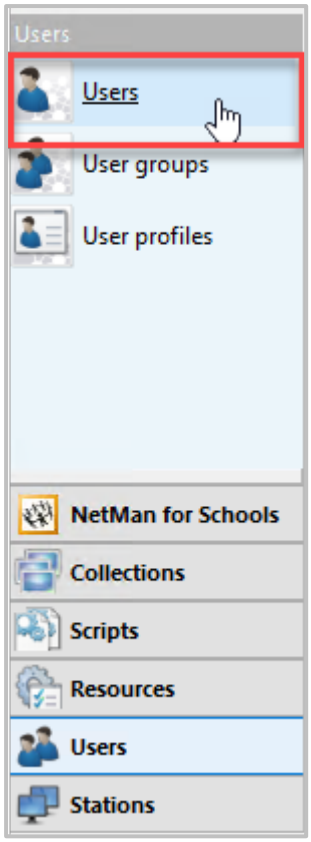
You open the NetMan Center via the desktop shortcut **NetMan Tools**.

You need administrative rights to open the NetMan Center and display user objects. Have an administrator assist you.



2 Open properties of the user object

In NetMan Center open the properties of the corresponding user object: click the Users selection button.

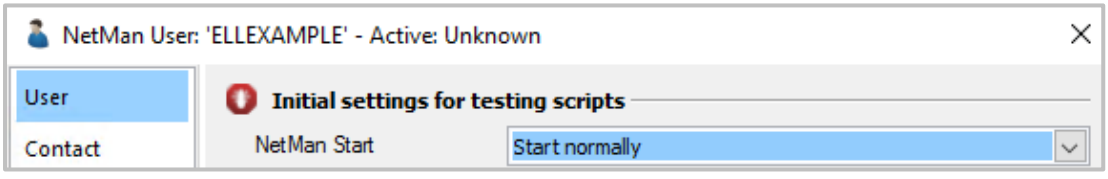


3 Open user object

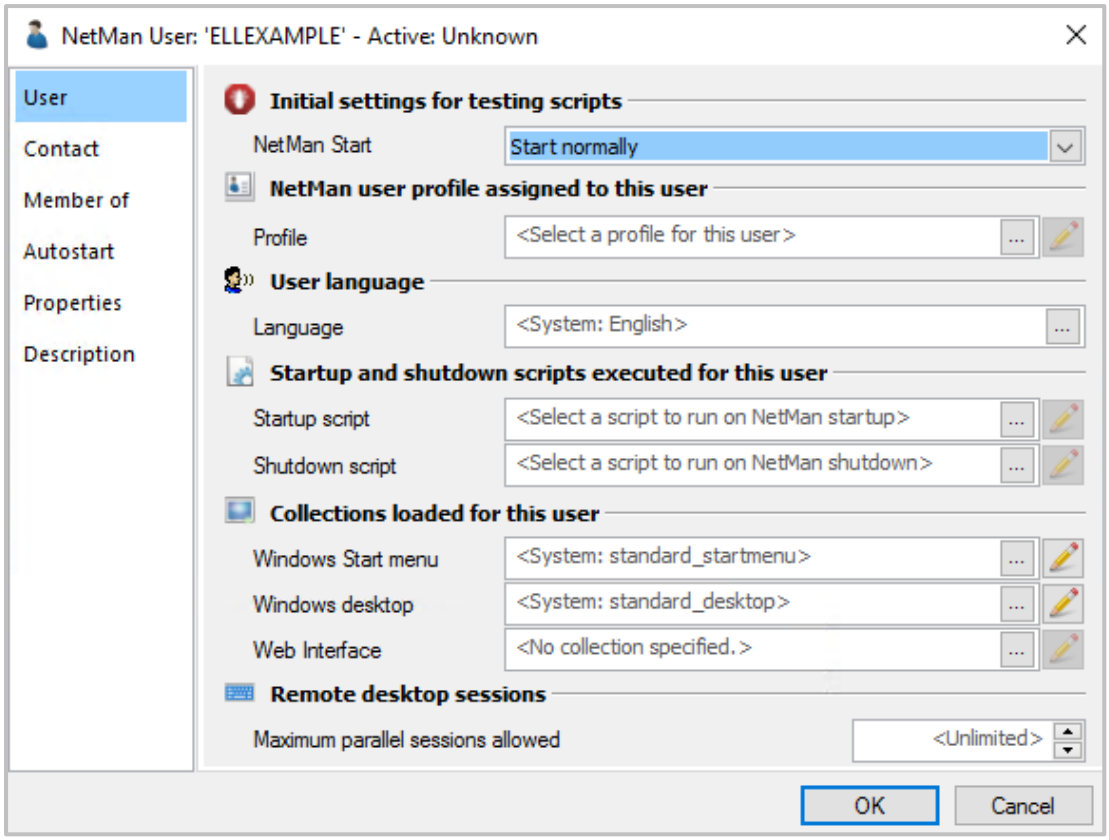
Double-click the corresponding user object.

4 Show username and time of last login

In the properties dialog, the NetMan username and the time of the last login are shown in the header.



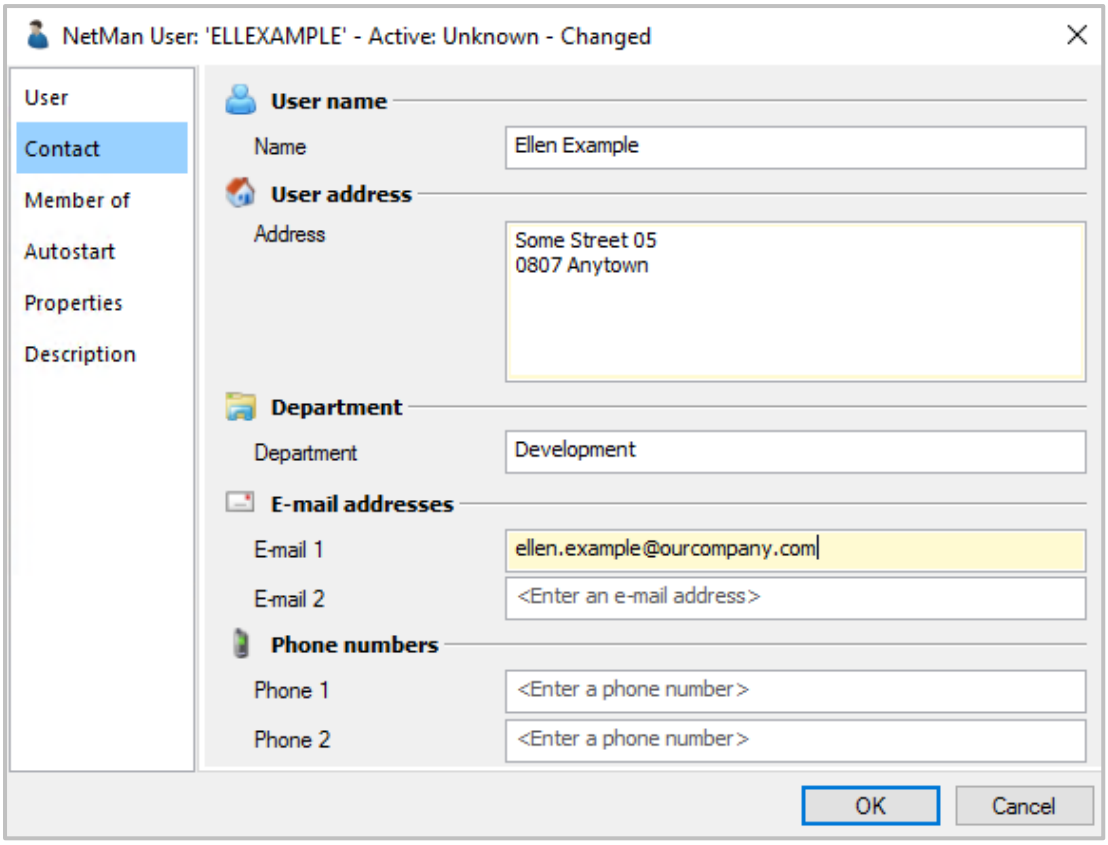
If next to **Active** is written only **Unknown** instead of a time, the user has never logged on to NetMan.



5 Show contact details

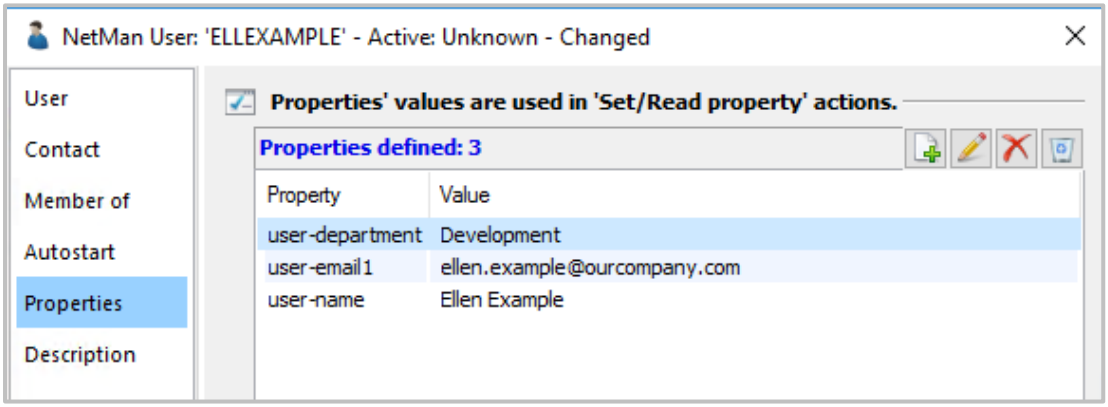
Switch to the **Contact** page. There you can see all contact data entered for this user.

All values on this page need to be added manually. The entry of these values is optional and according to your NetMan concept. So it may well be that no data is entered here for any user.



6 Show properties

Switch to the **Properties** page. Check whether object properties are entered and whether they contain personal data. Add personal data to the data disclosure. The properties show the contact data, except for the address. If you have already added the contact data to your data report, there should be no additional relevant information in the properties. The **user-name** is security-relevant data and therefore not part of a data disclosure.



7 Description

Switch to the **Description** page. If a description is entered, transfer it to the data disclosure.

Statistics: create a view, print

If you do not log NetMan usage data anonymously, you have to provide information about the usage data of the data subject in the event of a corresponding request. To export only the data of the person concerned, create a calculation for this one user using the NetMan Statistics and print using the statistics print function or export as a CSV file. Attache the printout or export to the data report.

You check the anonymization setting in the NetMan Settings, in the section NetMan, on the **Data Logging** page. For information on how to log data anonymously, see the chapter *Protect Anonymous Logging* and the NetMan documentation.

In this chapter you will read how to create a user-specific calculation using the statistics and how to print this calculation.

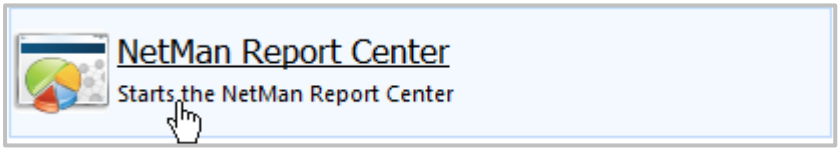
Create user-specific calculation

You create a user-specific calculation within the NetMan Statistics.

To work with the NetMan Statistics, you need appropriate access to the program. If in doubt, have an administrator assist you.

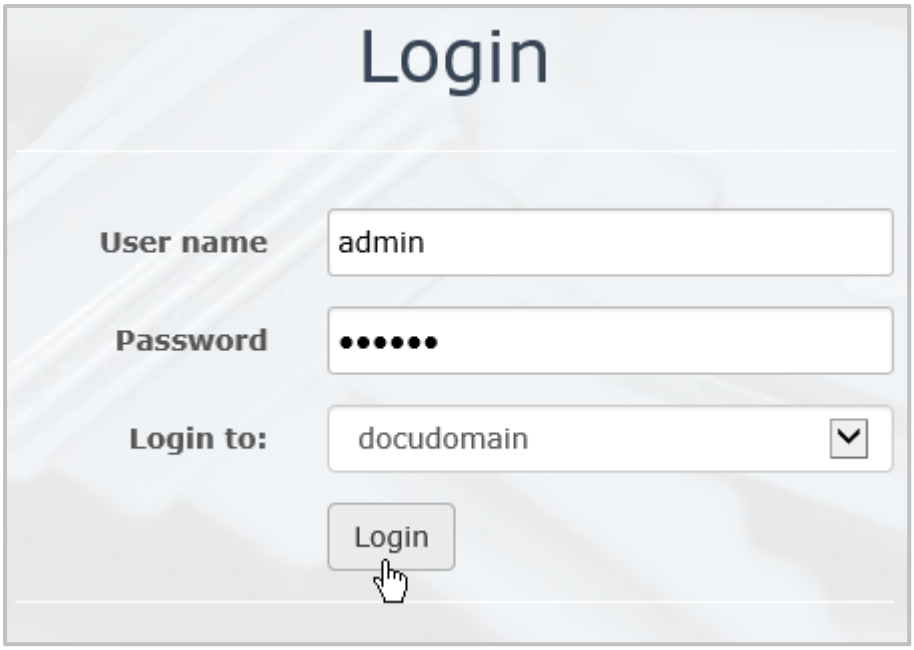
1 Open NetMan Report Center

You start the NetMan Statistics via the Report Center. To open the Report Center, double-click the desktop shortcut **NetMan Tools** and select **NetMan Report Center**.



2 Log in

Authenticate yourself at the Report Center.

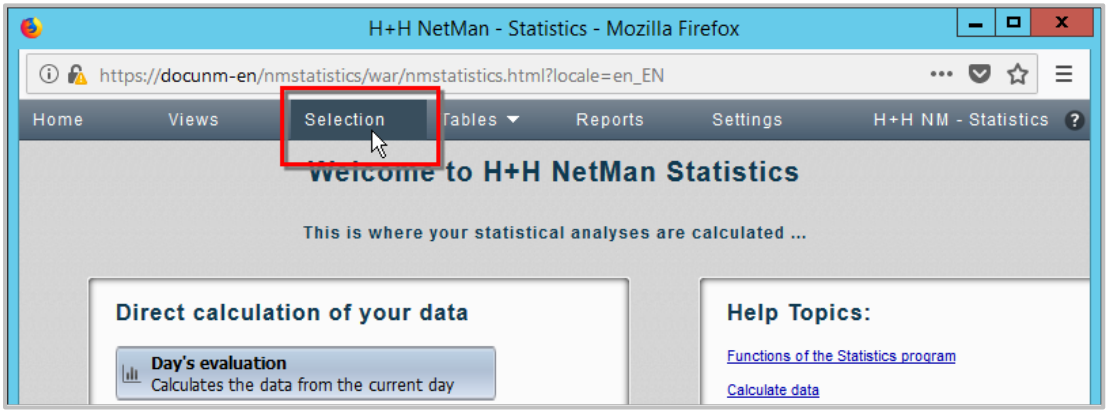


3 Open NetMan Statistics

In the Report Center, open the statistics by selecting **Statistics**.

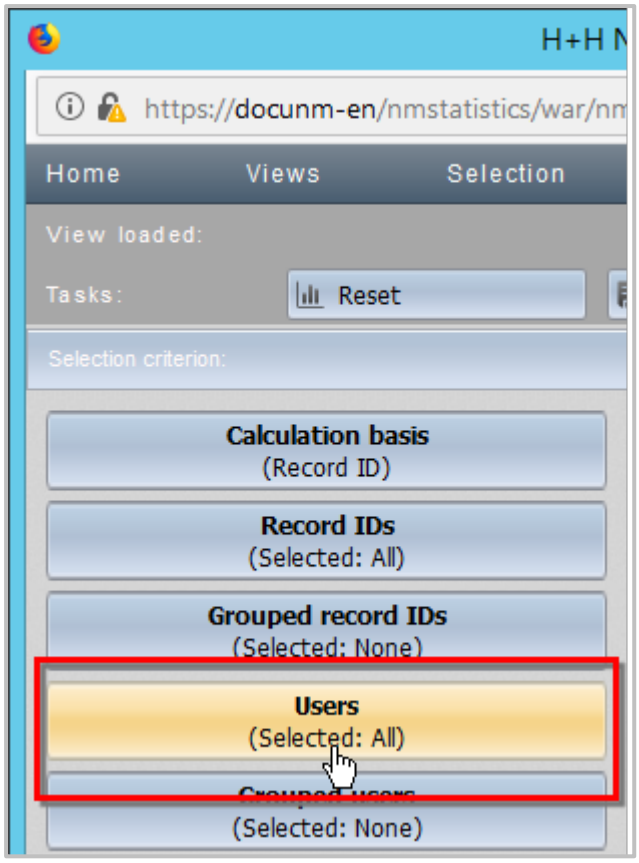
4 Click selection

In the main statistics window, click Selection in the menu bar.



5 Select Selection Criterion user

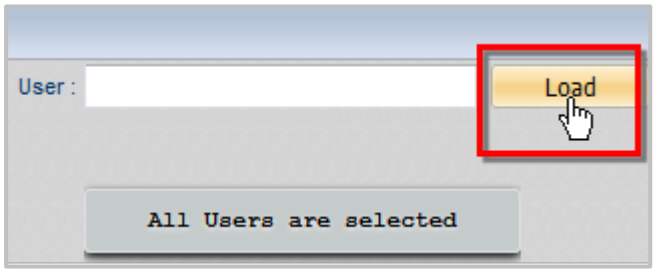
To calculate the data of a specific user, click the Users selection button.



6 Load user list

Initially, all users are loaded in the calculation. To display the users, click the Load button above the user list.

If you have a lot of users, you can use the input field above the list to filter the list. For example, type **`MyDomain\B*`** to display all users of the **MyDomain** domain that begin with the letter **B**.

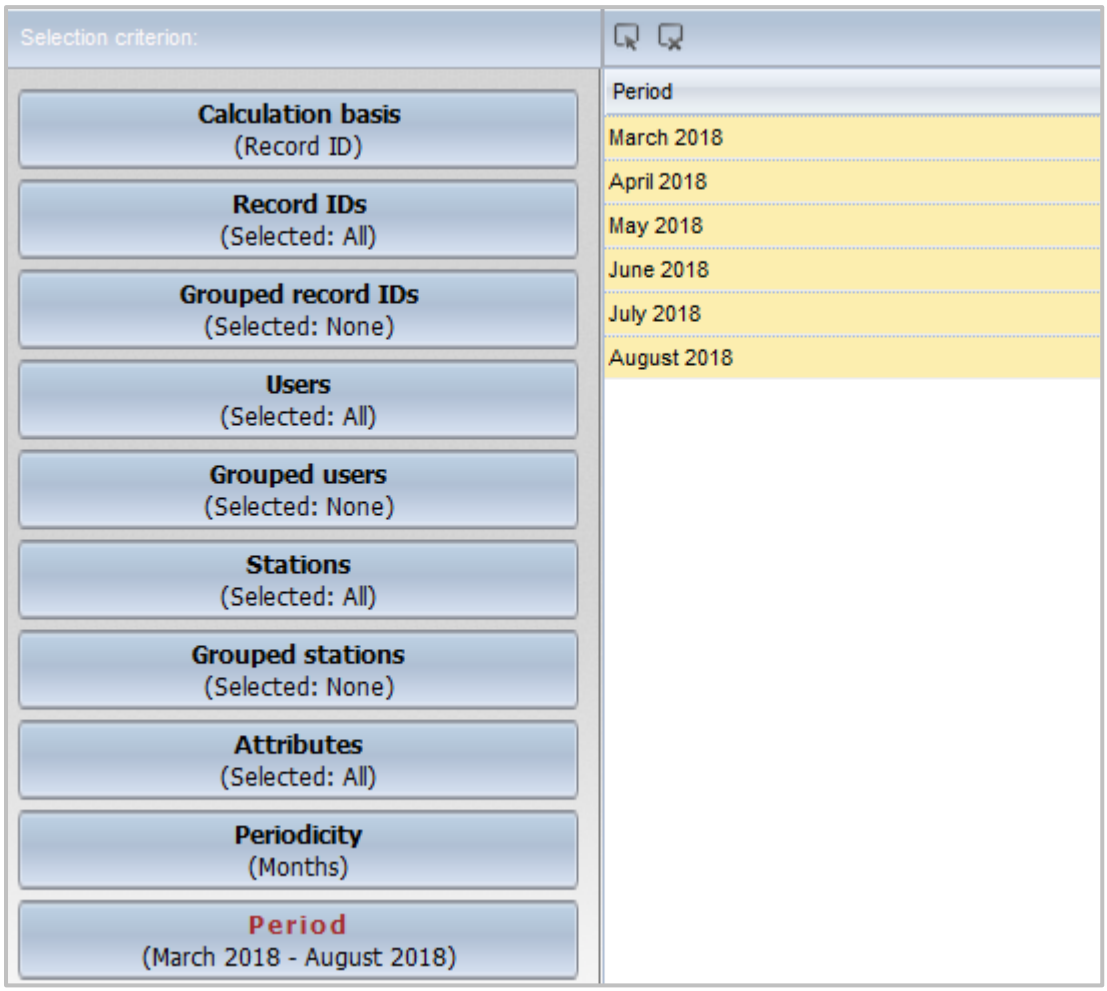


7 Select user

Select the appropriate user from the list.

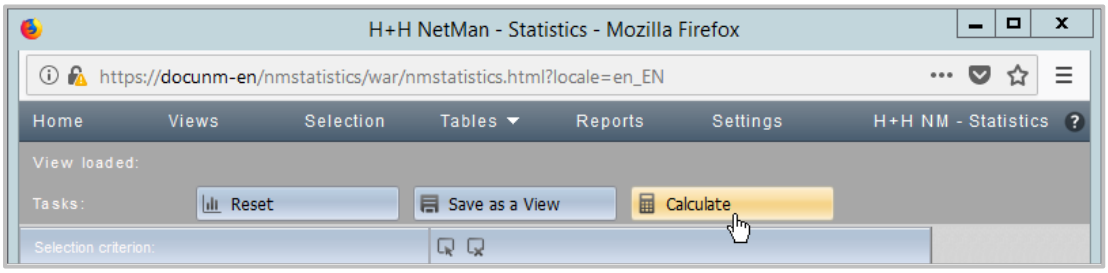
8 Select period

Click the Period button in the selection bar and select the period, for which data is requested.



9 Calculate data

In the Task Bar click the Calculate button.



10 Choose table form

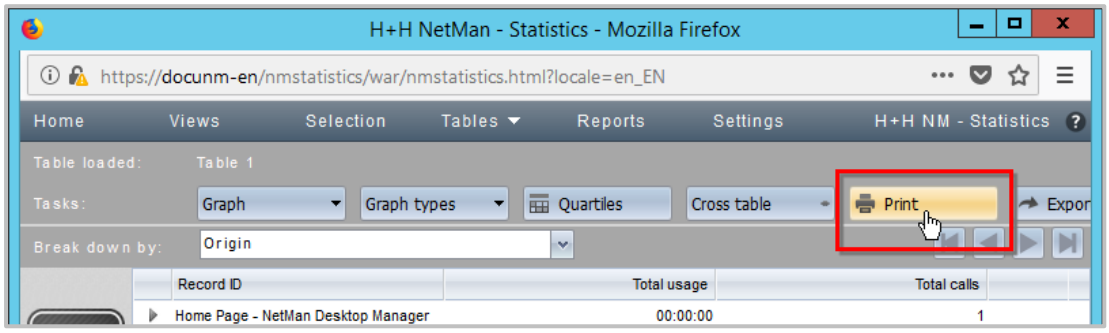
Select Main table as the table form. The table will be calculated and shown.

Print calculation

To attach the calculated data to the data report, print it from NetMan Statistics.

1 Open print preview

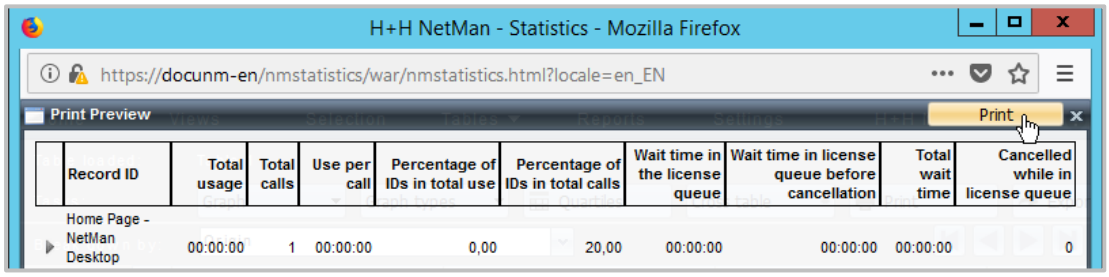
In the task bar click Print.



This opens the print preview.

2 Print click

In the print preview click the Print button.



3 Select printer and print

In the print dialog, select an available printer and print the document. In case of a digital data disclosure, create a PDF instead of the printout.

4 Add printout as attachment

Attach the printout or PDF to the data report.

Appendix

In the appendix you will find references to further documents that contain security and data protection relevant information on NetMan. Here you will also find an overview of all data stored in NetMan.

Data in NetMan

In NetMan you will find the following records in the specified locations:

System component	Stored data	Data storage location	Reason for storage	Deletion period
System	Windows User Group	The Windows User Group is a property of the AD user object on the DC.	functionally necessary	is deleted with the user object
System	Windows Active Directory Organizational Unit (AD-OU)	The AD-OU is a property of the AD user object on the DC.	functionally necessary	is deleted with the user object
System	Windows User Profile	In the Windows User Profile all data of the working environment of the respective user are stored. User profiles are stored for each user on the NetMan server.	functionally necessary	
System	Windows Login Script	NetMan supports the use of Windows Login Scripts, but does not use them by itself. A login script is a property of the AD user object on the DC.	optional	
Web Service	Access log	**\\NetMan Server\NM5\Bin**	safety relevant	42 days

System component	Stored data	Data storage location	Reason for storage	Deletion period
		\WebSrv\logs		
Web Service	Error log	**\\NetManServer\NM5\Bin\WebSrv\logs**	Error analysis	42 days
Web Service	blocked users/IP addresses	NetMan Settings/ locked accounts/IPs	safety relevant	
Database	Log files	**NetManServer\HH\NM5\db\logs**	safety relevant	
Database	Records of the database.	**NetManServer\HH\NM5\db\data**	functionally necessary	
NetMan Center	NetMan User group	NetMan Center	functionally necessary	
NetMan Center	NetMan User Profile	NetMan Center	functionally necessary	
NetMan Center	Time of the last registration	NetMan Center	safety relevant	will be overwritten at the next login
NetMan Center	NetMan User settings; therein: • NetMan Startup setting (optional) • Language (optional) • Start script (optional) • End script (optional) • Windows start menu (optional) • Windows desktop (optional) • Web Interface (optional) • Maximum allowed parallel sessions (optional)	NetMan Center	These settings are mostly set via the user profile and are then not person-related, but only have a reference to the user profile.	

System component	Stored data	Data storage location	Reason for storage	Deletion period
NetMan Center	Contact details; therein: • Username • Address (optional) • Department (optional) • E-mail addresses (2) (optional) • Phone numbers (2) (optional) • NetMan Autostart script (optional) • Fully qualified domain name • User SID • Description (optional)	NetMan Center	Defined in the NetMan Center and entered by NetMan administrators; The corresponding administrators have full access to the data. Not all of this data must be set!	
NetMan Center	Object properties	optional	Defined in the NetMan Center and entered by NetMan administrators; the corresponding administrators have full access to the data.	
NetMan Protocols	Call log: script calls with log ID, timestamp (start and stop), user, computer, log attributes	Logs are shown in the NetMan Log Viewer. This is available via the NetMan Report Center, to which NetMan administrators have access.	Statistics, anonymizable	
NetMan Protocols	Internet Filter log: log, timestamp, user, computer, application, URL, Internet Filter status, Content Filter status.	NetMan Log viewer	safety relevant	42 days

System component	Stored data	Data storage location	Reason for storage	Deletion period
NetMan Protocols	Internet Filter error log: Timestamp, User, Computer, Application	NetMan Log viewer	Error analysis	will be overwritten after 42 days
NetMan Protocols	Content Filter: Performance protocol	NetMan Log viewer	safety relevant	
NetMan Protocols	Program Control: program, timestamp, path, user, computer	NetMan Log viewer	safety relevant	42 days
NetMan Protocols	NetMan Web service: access log	NetMan Log viewer	safety relevant	
NetMan Protokolle	NetMan Web service: error log	NetMan Log viewer	Error analysis	
NetMan Protocols	Privacy log: Privacy operations (create, delete, lock, reactivate users)	NetMan Log viewer	Documentation requirement	never
NetMan Protocols	Event display: Events related to users or stations are logged in plain text in the event of an error.	NetMan Log viewer	Security/Error analysis	70 days
NetMan Protocols	Performance log: analyzes performance and utilization of all stations in your network. This requires logging of the station ID.	NetMan Log viewer	safety relevant	14 days
NetMan Protocols	WebDAV protocol: Accesses to the NetMan system via WebDAV are logged. For the purpose of traceability, the username and the accessing IP address are logged.	NetMan Log viewer	safety relevant	42 days
NetMan Protocols	WebDAV lock log: all current WebDAV locks (resources locked	NetMan Log viewer	functionally necessary	Data in the WebDAV lock log is deleted 1 second after

System component	Stored data	Data storage location	Reason for storage	Deletion period
	due to usage). For traceability purposes, the owner (user) is logged.			the respective resource is released (no caching)
NetMan Monitor	currently logged in users, stations IP address, timestamp	NetMan Monitor	safety relevant	Only visible at runtime

Installation Report

The installation report contains the specific settings at the time of the NetMan Installation. Some of these settings are security and privacy relevant.

Infrastructure Installation Report

The Infrastructure installation report contains the settings within your infrastructure at the time of the NetMan installation. Depending on your specific requirements and settings, you will find the following information there:

Domain Controller:

- Name of the DC
- Windows update status of the DC
- Network settings:
  - IP configuration (hostname, primary DNS suffix, node type, IP routing, WINS proxy, DNS.suffix lookup list)
  - Ethernet configuration (description, physical address, DHCP enabled yes/no, auto connfiguration enabled yes/no, link local IPv6 address, IPv4c address, subnet mask, default gateway, DHCPv6 IAID)
  - DHCPv6 client DUIS, DNS server, Netbios over TCP/IP.
- System: basic information about the computer: Windows edition, processor, working memory, system type, computer name, domain, Windows activation).
- Licensing
- ASBDC - Domain Controller Settings:
  - Network connection
  - IP address
  - Default gateway
  - DNS server

  - AD domain name
  - NetBIOS domain name
- DNSLint Report
- Installed software
- Drives
- Remote Desktop Licensing Host configuration

NetMan File server:

- Windows update status
- Network settings:
  - IP configuration
  - Ethernet configuration
- System: Basic information
- Licensing
- Installed software
- Drives
- Shadow copies: Setup of shadow copies for the NetMan drive of the file server. Backup interval, max. memory used by the backups.

Terminal Server:

- Windows update status, restart time for necessary updates
- Network settings:
  - IP configuration
  - Ethernet configuration
- System: Basic information
- ASBTS: AD settings: OU of the terminal server
- Licensing
- Installed software
- Drives
- If any, information about other terminal servers

SSL Gateway:

- Windows update status
- Since the SSL gateway is not in the domain, no group policies apply there. Therefore, the SSL gateway has to be regularly checked for updates manually and restarted if necessary.
- Network settings:
  - IP configuration
  - Ethernet configuration
- System: Basic information

Azure AD Connection:

- Information on Global Administrator

- Powershell modules
- Adjustments to the AD
- UPN suffix
- OU for M365
- User **adconnectsync**: User **adconnectsync** is required for synchronization from AD accounts into Azure AD.
  - Installation AzureAD Connect
  - User synchronization

Infrastructure:

- IP address list
  - Server network (VLAN)
  - Gateway server VLAN
  - Gateway client VLAN
  - Server list with functional description of each server
  - Printer
  - IP address range of the clients
- AD overview: Overview of the OUs that are used in the context of NetMan including their descriptions.
- HH users: enabled accounts for support
- administrative accounts
- user administration accounts
- group policy objects
- group policy customizations
- extensions
- software rollout via GPO
- DNS
- reverse lookup zones

Relution:

- accesses
- passwords

Microsoft 365:

- accesses (Azure AD, AAD-Connect)
- passwords

Hypervisors (Hyper-V, VMware):

- accesses
- passwords
- information about VMs

Domain:

- administrative access to
  - DNS
  - AD
  - GPOs
  - server
  - clients
  - etc.
- domain passwords (in separate list if necessary)
- service accounts

Further notes:

- Special settings for the specific installation.
- Problems encountered during the installation.

NetMan Installation Report

As part of the installation, settings are made in program NetMan in your NetMan environment, specifically according to your requirements. These settings can be found in the NetMan part of the installation report. Specifically, this may include the following:

- setup of NetMan and configuration of services
- NetMan Server XXX; installation directory **XXX:\HH\NM5**
- directories within the directory structure HH
- NetMan Version and license data
- license account: Person / email address and possibly password, of the license account
- installed services on the NetMan Server
  - NetMan Service (communicates with the NCs)
  - NetMan Database Service (controls access to the NetMan Database)
  - HH Webservices (provides NDP and ICA files, among others)
  - H+H Reparse Service (assigns directories to students)
  - H+H Contentfilter (filters internet access)
  - NetMan Client Service (belongs to NetMan Client and communicates with NetMan Service)
- listing of services on the NetMan Server with activity status and assigned ports
- services settings
- NetMan Database Service
- stored tasks (e.g. regular DB backup)
- settings of the NetMan Web Services
- settings of the NetMan Content Filter
- NTFS permissions and used shares

- basic configuration NetMan
- configuration of NetMan administrators
- configuration of the system host farm
- configuration of the application drive
- Program Control
- NetMan Web Interface
- installed applications
  - applications on the RDH
  - central application drive for applications that can be run without setup
  - applications on Windows clients
- advanced customized NetMan scripts
- file redirection configuration: certain files (file extensions) are linked to the corresponding programs
- context menu used
- terminal device control
- room profiles with printer assignments (functional rooms)
- short introductions on site (participants/topics)

Index

A

C

D

E

F

H

I

J

L

O

P

R

S

T

V