

A photograph of two women sitting in a server room. The woman on the left is wearing a white sleeveless top and dark pants, with her hands clasped. The woman on the right is wearing a dark sleeveless top, glasses, and dark pants, also with her hands clasped. The background is filled with server racks and equipment. A semi-transparent grid of squares is overlaid on the image. The text 'H+H NetMan Version 4.5' is positioned in the upper right area.

H+H NetMan
Version 4.5

H+H Software GmbH

Table of Contents

Preface	1
Application Framework: for Application Management	3
HTML Framework: NetMan Software for Management of Internet Resources	5
New in NetMan 4.5	7
Copyright Notices	9
Notes on working with this manual	11
Support	13
Ideas and Suggestions	15
System Requirements	17
Licensing and Registration	19
Notes for Test Users	21
Contents of This Manual	23
Installing NetMan	25
Installing NetMan Server Components	27
Installing NetMan Desktop Client	31
Distributing NetMan Desktop Client in the Network	33
NetMan Desktop Client Distributor	34
Software Distributor	37
Registering NetMan	39
System Structure	41
Server Software	43
NetMan Databases	44
NetMan Service	45
NetMan Web Server	47
Certificates for NetMan Web Server	49
NetMan Desktop Client	55
Technical Structure of the NetMan Desktop Client	57
Security Aspects Relating to NetMan Desktop Client	60
After Installation	65
NetMan Programs	67
Management Console	68
Statistics	70
Installer	71
Monitors	72
Settings	74
Wizards	77
Online Documentation	78
Directory Structure, Network Rights and NetMan Administrators	79

NetMan Concepts	81
NetMan Information Files and the Infoboard	82
NetMan Environment.....	84
Application Drive	86
Frequently Used Network Resources.....	87
NetMan Startup and Shutdown	88
Integrating Applications and Hyperlinks	91
NetMan Configurations	92
Working with the Management Console	97
Program Actions	104
Additional Program Properties	106
Creating and Deleting Desktop Entries	109
Your First Application.....	115
Access Permission for Configurations and Actions.....	117
Creating Additional Desktops	122
NetMan Actions	125
Using the Trace Monitor to Check Action Processing	127
Controlling an Action Sequence	130
Simple Examples of the Most Frequently Used Actions.....	134
Complex Actions.....	137
Windows Script Enhancements.....	140
Special Configurations and Applications	147
Startup and Shutdown Configurations.....	148
CD-ROM-based Applications	151
Integrating HAN Accounts	160
NetMan Resources	163
Users.....	165
Stations	167
User Groups.....	169
Station Groups	171
NetMan User and Station Profiles.....	173
User Profiles	174
Station Profiles	175
Allocating Licenses	177
Web Interface (HTML View)	179
Directory Structure in HTML View.....	181
Logging in through the Web Interface	183
Installing the NetMan RDP Web Client	185
Calling Applications through the Web Interface	187
Calling Hyperlinks through the Web Interface.....	189
HTML View Settings.....	193
Global Settings	194
Filter Configuration.....	196
Permit Operating Systems	197

Launch Methods for HTML View	199
Login Methods for HTML View	211
Authentication Services	223
How the Authentication Services Work.....	224
Authentication Page	225
Configuring Different Types of Authentication Services.....	228
NetMan SSL Gateway.....	241
Installing NetMan SSL Gateway.....	242
Creating an SSL Certificate	244
Accessing Applications over the NetMan SSL Gateway	245
Configuring the NetMan SSL Gateway.....	248
NetMan SSL Gateway Connection Monitor.....	250
Example: Configuring HTML View	251
Calling a Terminal Server Session.....	252
Calling a MetaFrame Session	259
Embedding Desktops in the HTML List View	267
Embedding Desktops	268
Embedding an Expanded Desktop.....	270
Embedding a Nested Desktop.....	272
Embedding an Alphabetical List	274
Embedding Individual NetMan Configurations	276
Selecting the Language.....	277
Embedding a 'Back' Button	278
Embedding Frequently Used Functions	279
Configuring the HTML View List View	283
Templates for Generating Desktop Structures	284
Placeholders in Templates.....	288
Using Style Sheets	289
Practical Example: Using the HTML View List View.....	290
Configuring the HTML View Explorer View	293
Modifying the Login Page.....	294
Modifying the HTML Page for Launching Applications.....	295
Opening Sessions from NetMan Desktop Client	299
<hr/>	
Launch Methods for NetMan Desktop Client	301
Rules for Determining the Launch Method	302
NetMan RDP Web Client.....	304
Citrix Web Client.....	308
Login Methods on Terminal Servers.....	311
Use Local Login Data	313
One-time Login using NetMan Desktop Client	315
Interactive Login per Session	316
Use NetMan Anonymous Users	317
Extensions for Terminal Servers	319
<hr/>	
Load Balancing in Application Sessions	321
Load Report	325
Session Sharing.....	327

NetMan RDP Session Broker.....	329
Installing the RDP Session Broker	330
Configuring the RDP Session Broker	331
Accessing the NetMan RDP Session Broker.....	332
Extensions for MetaFrame Servers	333
Published Application	335
Login Methods on MetaFrame Servers.....	337
Advanced Application Settings for a Session	339
Separate Launch Method Settings for an Application Call.....	341
Separate Session Parameters for an Application Call	343
Tips for Operation in Terminal Server Environments	345
Monitored Processes for Application Sessions	347
Changing the Operation Mode: NMSTSM.exe	349
Defining the Maximum Number of Parallel Sessions.....	351
Station Names in the Terminal Server Environment	353
Mapping Client Drives.....	355
Problems Launching NetMan.....	357
Troubleshooting Application Problems.....	359
Citrix Anonymous Users in Domains.....	363
Advanced Security Features	365
Ticketing.....	367
User Tickets for the Web Interface.....	369
Access Privileges for Client Drives	371
Setting up Access Privileges for Client Drives.....	374
Using NetMan Actions to Modify Access in Client Drives.....	376
Printing	377
RDP Support for Local Printers.....	379
Modifying Printer Mapping	381
Universal Printer Driver in Windows Server 2003 SP1	383
Terminal Server Easy Print in Windows Server 2008	385
Universal PDF Printer Driver.....	387
Switching the PDF Print Preview On and Off.....	389
Showing or Hiding the Universal PDF Printer Driver	391
Bandwidth Management for the Universal PDF Printer Driver.....	393
Internet Filter	395
Switching the Internet Filter On and Off.....	397
Editor for Internet Filter Files.....	399
Creating a Global Internet Filter.....	401
Creating Rules for Filtering URLs	403

Creating Rules for Filtering Processes	407
Testing an Internet Filter File.....	409
Statistics	411
<hr/>	
Statistical Analysis with the NetMan Statistics Program	413
Tables.....	415
Main Table	416
Table of Concurrent Use.....	419
Example: Analyzing Data with the NetMan Statistics Program.....	421
Installer	431
<hr/>	
Prerequisites for Working with the NetMan Installer	433
Recommended Readings on the Windows Registry.....	435
Requirements for the Installation of the NetMan Installer	437
Basics	439
Areas of Application and How an Installer Works.....	440
Running the NetMan Installer.....	442
Step by Step: From SnapShot to Script	449
Language Options	461
<hr/>	
Defining Which Languages are Available.....	463
Creating NetMan Configurations in Multiple Languages.....	465
Defining the Default Language	467
Control Options Made Possible by the NetMan Language Variable	469
Supressing the Language Selection Option.....	471
Language Controls in the HTML Framework	473
NetMan Utility Programs	475
<hr/>	
Application Library	477
Utility Programs for the 'Execute' Action	479
HHCmd.exe - Hiding Command Execution	480
HHCOPY - Copying Files and Directories.....	481
HHDelete - Deleting Files and Directories.....	484
HHDummy.exe - 'Do Nothing' or 'Wait'	485
HHLogin.exe - Executing a Server Login	486
HHMap.exe - Connecting a Drive.....	487
HHMKDir - Creating Directories	489
HHSetAtr.exe - Setting File Attributes	490
Glossary	491
<hr/>	
Index	501
<hr/>	

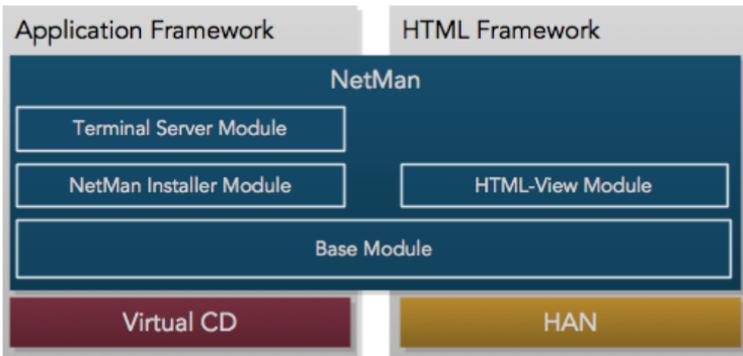
Preface

The central task of network administration is to provide access to information and applications for network users. NetMan is network management software for efficient, centralized administration of information and applications in a network, whether LAN, intranet or the Internet, that lets you configure an inviting, easy-to-use access point for your users.

The term resources as used in the following refers to information and applications, and can include Windows-based applications, programs, and documents, as well as HTML-based information sources such as e-journals and on-line databases. NetMan integrates all these different types of resources into a uniform user interface, on your choice of a Windows platform or an HTML-based platform.

Integration of diverse resources is made possible by NetMan's dual framework design, consisting of:

- the Application Framework (for management of Windows applications) and
- the HTML Framework (for management of HTML-based information sources in the intranet or Internet).



The variety of resources all have the following performance features in common when integrated by NetMan into a uniform management system:

- Central definition of resources in NetMan databases
- Central allocation of resources to NetMan users, user groups, stations, station groups, IP address ranges; host names, and network groups
- Clearly structured presentation of your resources using familiar Windows operating system components such as browser, Start menu and desktop
- Automatic documentation of user and station access

NetMan can show your centrally managed resources on every desktop, and enables central configuration and update of the resources on individual workstations—whether on the desktop, in the Start menu or in the user’s list of browser “favorites.” Providing resources to your users can be made uniform, because NetMan lets you choose whether resources are accessed over

- a URL, or
- a Windows program.

These options are illustrated in the following two examples:

- Your users access your central information services in their browsers: NetMan makes it easy to link as many Windows applications as you like in a browser-compatible presentation, because it automatically assigns a URL to each application that you specify in your NetMan databases.
- Your users work in a Windows environment: You can add links to your choice of intranet or Internet resources in the form of Windows desktop shortcuts.

Thanks to its modular structure, you also have the choice of using NetMan exclusively as either

- application management software or
- an Internet resource manager

You can define profiles for NetMan users and NetMan stations; for example, to allocate explicit system configurations and permit access to specified resources for certain users or stations.

Permissions to use certain information sources can be made dependent on a variety of conditions, which can be combined as desired. Here are just a few examples of the conditions you can choose from: the existence of certain entries in INI files or the Windows Registry; range of host names or IP addresses; workstation operating system, and more. Central services inform you at a glance on the availability of licenses and keep you abreast of station activity.

Application Framework: for Application Management

NetMan expands your programs by adding new properties. Read on for an explanation of just what this means for your network:

The program properties that your operating system offers for a Windows shortcut are:

- program call
- working directory
- icon
- program window state on start-up (maximized, minimized, normal)

With NetMan, not only can you define these properties centrally; you can also define additional properties for a program, thus greatly expanding your range of possibilities:

- Specify whether the program runs on the client machine or a terminal server.
- Define the maximum number of parallel users permitted for applications.
- Create detailed records of application use, sorted by user and station; this data can also form the basis of easy-to-read tables and graphs generated with NetMan's powerful statistical evaluation tools.
- Assign 'execute' privileges for NetMan users (independent of complex file and directory privileges configured at the network level).
- Assign 'execute' privileges for NetWare NDS groups, as well as local and global NT and LDAP groups.
- Configure licensed applications to close automatically—and release the license—if they are left unused for a certain period of time.
- Provide information about individual application in HTML format for your users.
- Define whether multiple parallel instances of an application are allowed on a single client machine.
- Define mutually blocked applications (i.e., application "B" cannot be launched on a given client machine while application "A" is running on that station).
- Activate or deactivate applications or groups of applications, with a customized message to the user (such as, "This application is undergoing an update at the moment. Please try again later").

The above list describes the expanded program properties that NetMan lets you assign. In addition to all these features, NetMan gives you, as administrator, deeper layers of functionality for each application, involving far more than just a program call:

NetMan shifts the focus from the simple program call to the level of overall management of applications in the network.

With NetMan, each program call—e.g., “Encarta.exe”—is a single action within an application definition that can be quite elaborate. To call the Encarta program under NetMan, you would define a NetMan configuration (called “Encarta,” for example) which can include a number of other actions in addition to the program call. This sequence of actions is then executed when a user activates the Encarta shortcut or link. Here is an example of the functions (i.e., actions) that a NetMan configuration can perform:

- Map a network drive for the application
- Provide the required resources (for example, by mapping the Encarta CD)
- Call the program
- When the program is closed: Undo drive connections that were mapped by the preceding action(s).

This example includes only a few of the many NetMan actions at your disposal. Other actions cover broad range of functions, from password prompts to running other programs or scripts before or after the activated program. And the execution of any given action can be made dependent on any of a variety of conditions, defined in the form of ‘execute’ privileges.

Furthermore, you can define action return values which are stored in variables; for example, to integrate user input in the processing of a NetMan configuration. NetMan’s own interface to the Windows Script Host lets you combine the many options available in NetMan with scripts you write yourself.

The following modules are also available for use in application management:

The *NetMan Installer* monitors the local workstation during application setup; changes made by the Setup program at the file level or in the Windows Registry are documented and can be written up in the form of scripts. You can insert these Installer scripts in NetMan configurations to distribute application components where and when you need them in the network.

The *Terminal Server Module* lets you control access to NetMan configurations within Microsoft Terminal Server (or Citrix MetaFrame) sessions. This module gives you capabilities for platform-independent access to your Windows applications; for example, from Unix, Macintosh, or thin-client terminals. The Terminal Server Module expands the Microsoft Terminal Server with the following additional features:

- Anonymous users for Microsoft Terminal Server
- Published applications
- Load balancing
- NetMan RDP Web client with extended functions, such as support for seamless windows.

HTML Framework: NetMan Software for Management of Internet Resources

Your network resources, whether in the intranet or Internet, can be accessed in the usual manner with the Microsoft Internet Explorer. The NetMan Internet Filter gives you control over access to network resources by restricting the navigation options available to your users. You can define permitted and excluded links to ensure that users can access only the network resources you want them to use. You also have the option of preventing Internet access entirely, or of allowing unrestricted access to the Internet. In conjunction with the Terminal Server Module, you can control Windows applications over the network that are launched from browser windows.

The *HTML View Module*, on the other hand, lets you create dynamic HTML pages. HTML View analyzes the privileges granted to users and stations, and presents only the permitted resources as defined for the particular client. It also implements licensing controls for the requested resources and can react to inquiries based on a client's browser type, operating system, host name or IP address.

HAN, the Hidden Automatic Navigator from H+H (available separately), can be integrated quickly and easily in your NetMan system and enables fully automatic access to Internet resources in accordance with your settings. "Fully automatic" in this context means users do not need to log in to access the desired resource, because authentication is handled in the background by HAN. Access can be permitted, for example, even when the client's IP address does not fall within the IP address range of the institution at which he or she works.

New in NetMan 4.5

- **New operating system:** NetMan 4.5 supports Windows Server 2008 R2.
- **Support for RDP 6:** The NetMan RDP web client supports RDP 6.
- **Web client setup:** The setup program for the NetMan RDP web client now includes both the 32-bit and 64-bit versions. The web client is still installed using the web interface, as in previous versions.
- **Improved AD integration:** NetMan's AD integration has been improved. In the Management Console, permissions to configurations are now assigned to users and stations as for AD objects (AD user groups, AD station groups, OUs for users, OUs for stations). Also in the Management Console, you can enter AD objects directly in the NetMan resources (user and station profiles).
- **New settings for calling sessions:** NetMan 4.5 has improved mechanisms for calling sessions through new configuration options:
- NetMan configurations now have the option: "If not available locally, execute in a session." With this option active, the NetMan configuration opens a terminal server session only if it cannot execute on the local machine.
 - For access over HTML View, activate the "Launch method can be changed by the client" option. This enables the user to determine the launch method used for HTML View by configuring the appropriate setting in the browser.
 - Support for local devices and resources: The "NetMan RDP Web Client" launch method now supports use of the local Clipboard and smart cards. The "Java RDP web client" and "rdesktop over Java applet" methods support use of the local Clipboard.
 - Improved support for alternative server addresses: Rather than a single alternative address for a terminal server you can now manage up to four alternative IP addresses, which you can allocate to clients, in the Web Services Settings.
- **Load balancing:** In addition to load balancing according to number of sessions, NetMan now offers load balancing according to server load as well. You can define the load per server by weighting CPU and memory utilization as desired.
- **Round robin DNS load balancing:** As an additional load balancing method, NetMan now supports round robin DNS load balancing as well. With NetMan round robin DNS, loads are also weighted.
- **RDP Session Broker:** For thin clients, the Session Broker can evaluate NetMan's load balancing and determine the terminal server on which a client session is opened. Separate user sessions are taken into account in the evaluation. All thin clients that support RDP 5.2 are supported by Session Broker, and no additional software installation on the thin clients is required.
- **HTML View:** HTML View has been expanded by the addition of the "rdesktop over Java applet" launch method. This launch method is particularly well suited for "small" thin clients because it uses few resources. For details on the "rdesktop over Java applet" launch method, see "*rdesktop over Java Applet*."

- **Server and Station Monitor:** The Station Monitor has been replaced by the Server and Station Monitor, which provides a number of new functions. It gives you detailed information about the servers and workstations in your network, such as running processes and system information. An additional Performance view is available for servers as well. As previously, you can use the monitor to see which applications have been launched and to release applications for use.

Copyright Notices

The NetMan software, trademark and all associated documentation are protected by copyright owned by H+H Software GmbH. In the USA, Microsoft and Windows are registered trademarks of Microsoft Corporation. The product names mentioned in this manual are used for identification purposes only and may be protected by copyrights owned by the respective companies.

Notes on working with this manual

The special symbols that mark certain passages in this manual have the following meanings:



Note. Designates critical information that must be taken into account.



Tip. Designates handy tips and suggestions for working with NetMan.



Definition. Designates a definition or an explanation of a specific term or topic.

The appendix contains a glossary and an index. The glossary provides explanations of important terms used in the manual. The index lets you search the manual for certain keywords.

The NetMan manual was written with first-time users in mind; it provides an introduction to the basic concepts and operating design of NetMan. A complete list of NetMan commands and detailed descriptions of the program functions can be found in the on-line Help.

Support

You can use the NetMan Download Wizard at any time to obtain information about patches and, if desired, to download these from the H+H Download Server at **www.hh-software.com/netman**. A comprehensive knowledge base is also available, with additional information as well as tips and tricks for using the software.

You can contact your software dealer for help with your support questions. You can send questions about NetMan software to the following e-mail address: **nmsupport@hh-software.com**

Before you contact your software vendor, please read the relevant sections of the manual and refer to the on-line Help in the NetMan program; if you are not sure where to look, check the indexes. If you still have not found an answer, please provide the following information when you send us your question, or have it on hand when you call your software vendor:

- NetMan module and version number
- NetMan serial number
- Network operating system and version number
- Text of any error messages and any relevant NetMan event log entries
- The steps required to reproduce the problem

Ideas and Suggestions

We are always happy to hear your ideas, comments, and suggestions for improvement. Please send them to:

H+H Software GmbH

Attn. "NetMan" Product Manager

Maschmuehlenweg 8-10

37073 Goettingen

Germany

Phone: +49 (0)551 / 522 08 0

Fax: +49 (0)551 / 522 08 25

Or send e-mail with "NetMan" as the subject to: nmsupport@hh-software.com

System Requirements

NetMan has two main components:

- NetMan Desktop Manager server
- NetMan Desktop client

A third component handles access to the NetMan web interface:

- NetMan SSL Gateway

NetMan supports two different installation scenarios:

- Installation on a single terminal server
- Installation on a file server for operation on multiple terminal servers with load balancing

The NetMan SSL gateway software must be installed on a separate server, located either in the DMZ or within the intranet.

When installing NetMan server components on a file server that is not operated as a terminal server, the file server must be running one of the following operating systems:

- Windows 2000 Server with Service Pack 4
- Windows Server 2003 (32-bit or 64-bit)
- Windows Server 2003 R2 (32-bit or 64-bit)
- Windows Server 2008 (32-bit or 64-bit)
- Windows Server 2008 R2

The server components are installed using the Windows server console, and require approximately 100 MB on the hard disk. The data volume in NetMan databases will grow over time as you use NetMan; make sure to allow for this when allocating hard disk space.

For installation on a single terminal server, the server should be running Windows Server 2003 or later; Windows 2000 does not have sufficient terminal services.

Installation of the client components – the NetMan Desktop Client, in other words – requires one of the following operating systems:

- Windows 2000 Professional
- Windows XP

- Windows Vista (32-bit or 64-bit)
- Windows 7 (32-bit or 64-bit)
- Windows Server 2003 R2 (32-bit or 64-bit)
- Windows Server 2008 (32-bit or 64-bit) or 2008 R2

NetMan also requires Microsoft Internet Explorer version 6.0 or later. For the administrative workstation, we recommend generous proportions for both RAM (512 MB) and monitor (19 inches).

The NetMan SSL Gateway requires one of the following operating systems:

- Windows Server 2003 or 2003 R2 (32-bit or 64-bit)
- Windows Server 2008 (32-bit or 64-bit) or 2008 R2

The gateway uses port 443 on this server for HTTPS. If you install NetMan SSL gateway in the DMZ, assign port 3389 for RDP connections from the NetMan SSL gateway to the terminal servers.



A license number must be entered during installation, whether a restricted (temporary) license code downloaded from the Internet for testing purposes, or the full license you received with your purchase of NetMan.



When installing NetMan on Windows Server 2008, make sure the required ports are accessible through the built-in firewall.

Licensing and Registration

NetMan does not offer all of the features described here until you register your license. For details on how to register, please see “Registering NetMan” in the chapter entitled “Installing NetMan.” You can have a full version—including the modules you need—licensed for testing purposes before you purchase NetMan.

NetMan offers two different schemes for client licensing:

- With the *Concurrent Use* scheme, user rights are assigned for simultaneous parallel use of the NetMan Client.
- With the *Per Seat scheme*, licenses are assigned by workstation and are valid for up to 40 days.

Notes for Test Users

If you do not register it right away, you can use NetMan in demo mode for up to 30 days. In demo mode, the performance range is considerably limited. Every time you run the program, a message window opens indicating that NetMan is in demo mode.

To test a fully functional NetMan version, you can obtain a license code for temporary registration from your software vendor.

Contents of This Manual

The first chapter, **“Introduction,”** provides a general introduction to the NetMan software suite, as well as the information you need to know before installing NetMan and notes on the use of this manual.

“Installation” describes the installation of the server components and various options for installing the client components.

„System Structure“ describes the NetMan server and client components in detail and provides information on managing certificates for the NetMan web server.

„After Installation“ describes the individual NetMan programs and basic NetMan concepts.

„Integrating Applications and Hyperlinks“ provides details on making applications available to your users with NetMan. This chapter helps get you started working with NetMan and explains the concepts behind the basic control elements: NetMan configurations and NetMan actions. It also provides an introduction to the NetMan Management Console, which is the central administration program in NetMan.

„NetMan Resources“ describes how to manage users and stations (these are termed „NetMan resources“) in NetMan, and introduces the use of station groups, user groups, station profiles and user profiles. This chapter shows how you can use these resources as additional control elements in NetMan.

„Web Interface (HTML View)“ describes the NetMan web front-end, which you can use a browser to provide access for your users to applications. This chapter explains how the web interface is launched, how it permits application access, and how you can customize the interface. It also explains the optional components for authentication services and the SSL gateway.

„Opening Sessions from NetMan Desktop Client“ describes the options for using NetMan Desktop Client to set up a session on a terminal server. The various launch methods available for the NetMan Desktop Client are presented, as well as various login methods for the users.

„Extensions for Terminal Servers“ introduces and explains additional NetMan components, such as the integrated load balancing functions and the NetMan RDP session broker, that make it easier to use NetMan in terminal server environments.

„Extensions for MetaFrame Servers“ describes NetMan components for login on a Citrix MetaFrame server.

„Separate Launch Method Settings for an Application Call“ presents the session settings you can configure on the application level.

„Additional Tips for Operation in Terminal Server Environments“ describes some common problems and gives you handy tips for working with NetMan.

„Advanced Security Features“ describes optional security features available to you in NetMan.

„Print“ describes the options for processing print jobs sent from within terminal server sessions.

„**Internet Filter**“ describes the NetMan internet filter, which lets you control and filter user access to applications and processes over the Internet.

„**Statistics**“ describes the statistics functions in NetMan.

„**Installer**“ describes the functions of the NetMan Installer. The Installer monitors installation processes on your terminal server.

„**Language Options**“ describes how you can make your NetMan system a multilingual environment.

„**NetMan Utility Programs**“ describes the functions of a range of helper programs that come with your NetMan program.

Installing NetMan

NetMan has to be installed on the console of a Windows server (Windows 2000 or later). The NetMan program requires approximately 100 MB of space on the hard drive. Additional space will be required for data in the NetMan databases, which will increase in size as the program is used.



If you use NetMan with only one terminal server, we recommend installing NetMan on that server. If the applications managed by NetMan will be accessed over the LAN or if you have multiple terminal servers that will be using NetMan, we recommend installing the central NetMan software package on a Windows file server.

The NetMan client components for running the NetMan Desktop Client software, run on Windows 2000, Windows XP or Windows VISTA. NetMan also requires Microsoft Internet Explorer version 6.0 or later. On administrative stations, we recommend generous proportions for both RAM (512 MB) and monitor (19 inches).

Installing NetMan Server Components

After you insert the NetMan CD, you are prompted to select a language. The subsequent dialog offers you the following three choices:

- Install NetMan
- Open the PDF of the NetMan manual
- Open the Readme file

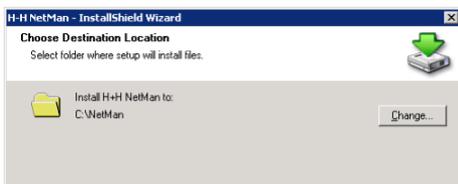


We recommend checking the Readme file before you run the setup program to install NetMan, as it may contain information that is newer than the information in this manual.

The installation CD also contains the latest version of the Acrobat Reader, required for reading the PDF documentation.

An example of a NetMan installation is illustrated in the following, with details on all available options:

1. The first step is to select the language in which the installation program runs.
2. After you have accepted the terms of the license agreement, you are prompted to choose a folder for the NetMan installation:



3. Both the NetMan installation folder specified here and the NetMan Web services folder have to be shared, for administrative purposes. The default share names assigned by the setup program are:

- NetMan and
- HHWebPath

With the default settings, user access in these shares is not restricted:



This is why the dialog makes the recommendation: “Please adapt the user privileges for this share to your requirements.” These paths are shared only to permit administrators to access NetMan databases from any workstation. With this in mind, access rights in these shares are required only for administrator accounts.



You can configure access privileges in directories and files after installation by setting NTFS privileges, rather than sharing the directories. For these directories and files, administrators require full privileges and users require none.



The complete path name to the NetMan program folder is referred to as the “NetMan home directory” in the following. The setup program stores this path in the NMHome NetMan variable; thus this share can be addressed using %NMHome%.

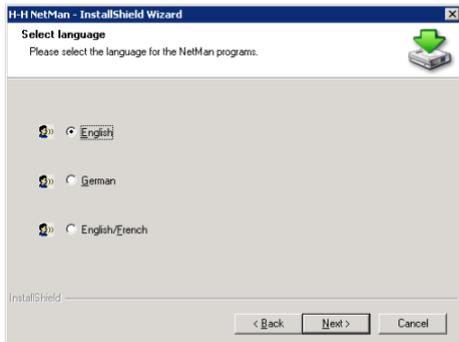
4. The next step is to enter data for your program registration:



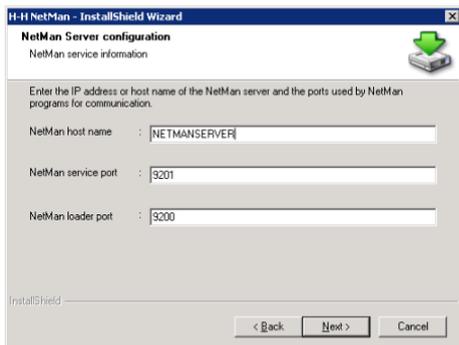
The serial number, which you will need again later to register your NetMan installation, is included in the bill of delivery and printed on adhesive labels on the CD and on the cover of the manual.



5. NetMan's administrative programs are installed in English and German. If you would like to offer a choice of languages for network users as well, you need the Language Module. If you have not purchased the Language Module, you need to select one of the languages offered here for your users:



6. Station monitoring, for license control and runtime recording, and the provision of information to clients concerning available resources are performed automatically by an NT service that is installed during setup:



NetMan host name. Host name or IP address of the computer on which NetMan is installed.

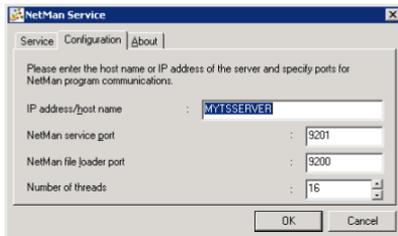
NetMan service port. Port used for exchange of data between NetMan Desktop Client and the NetMan service.

NetMan loader port. Port used for downloading Desktop Client data from the server.



As a rule, the default settings can be used. Make sure the ports specified here are available on any routers along the data path.

You can change these settings later in the Windows Control Panel:

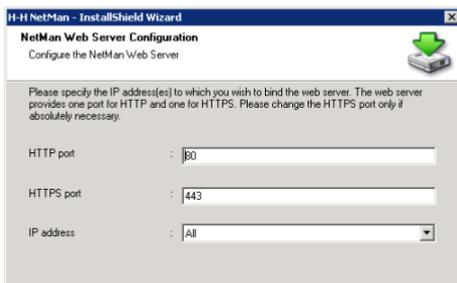


With the default settings, the NetMan service uses the system account. This account has to have full privileges in the NetMan installation directory. If NetMan was not installed in the system partition of the NT server, you might need to change the settings for the system account privileges.

7. Once you have entered the data for the NetMan Service, the next step is to specify the ports for the NetMan Web server:



Please keep in mind that if you already have an Apache Web server installed on the same server, port 80 is already in use and you need to select a different port for HTTP communication.



You can change these settings later in the NetMan Web Server Settings program, in the Windows Control Panel.



8. Once the NetMan service has been installed, the installation of server components is basically complete. If you wish to administer the program on the server console or in a remote session, you need to install the NetMan Desktop Client on this machine as well.



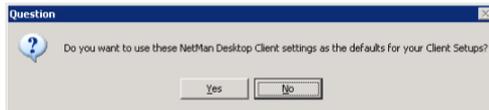
Because the above is usually the desired method, we recommend installing NetMan Desktop Client once the server installation is finished.

Installing NetMan Desktop Client

The Setup program for the NetMan Desktop Client executes on the server automatically following server installation:



The settings configured in the first NetMan Desktop Client installation are the defaults for subsequent installations. If you change any of the installation options, the following message is shown:



For details on distribution of the NetMan Desktop Client in a network, see “Distributing NetMan Desktop Client in the Network.” An account with administrator rights must be used to install the Desktop Client. Once the client has been installed, it will be updated automatically any time a newer version is installed centrally.



If you call the NetMan Desktop Client setup program on a terminal server, you also have the option of installing the universal PDF printer driver. With this driver you can have data sent to a PDF file rather than a printer. NetMan automatically passes the PDF files to the client, whether they can be opened by Acrobat Reader for reading and printing.

Distributing NetMan Desktop Client in the Network

There are a number of ways to install the NetMan Desktop Client in extensive environments. The Setup program for the NetMan Desktop Client can be found in either of two directories: `%NMHome%\Config\Client\Setup\x64` and `%NMHome%\Config\Client\Setup\x86`. You can share the `%NMHome%\Config\Client\Setup` directory to distribute the Client. This is a practical method, at least for small networks, but it does have some disadvantages:

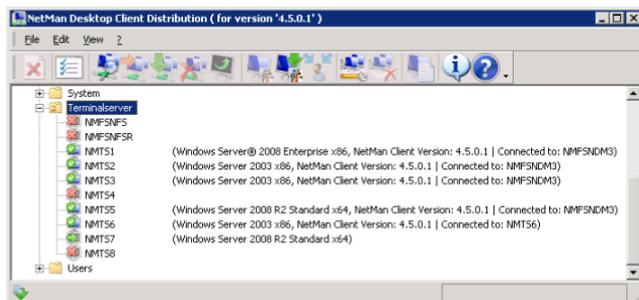
- The user has to have administrative rights to install the client, or
- An administrator must perform all installations.

Especially for larger networks, we recommend using one of the following two methods instead:

- Use the NetMan Desktop Client Distributor (`ndcdeploy.exe`) for deployment. (“NetMan Desktop Client Distributor”)
- Use your customary software deployment method to install the NetMan Desktop Client on all workstations. (“*Software Distributor*”)

NetMan Desktop Client Distributor

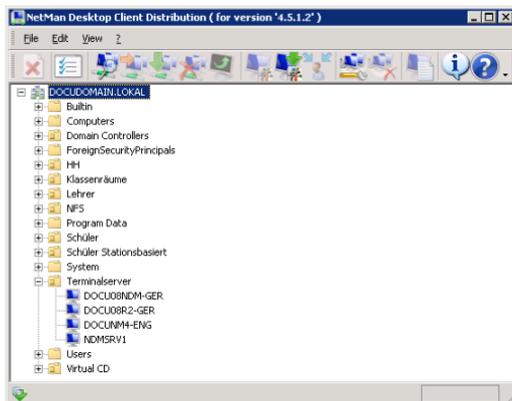
To install NetMan Desktop Client using the Client Distributor, open the **Wizards** folder in the Toolbox and select the distributor program:



You can use this program to distribute the NetMan Desktop Client in your network. The NetMan Client Distributor has two methods of detecting and displaying your workstations and terminal servers:

- Reading out the NetBIOS browse list
- Reading out the Active Directory

You can select the desired method in the Client Distributor program settings. The following example is based on selection of the “Read from Active Directory” method:



When the AD is displayed, navigate to the OU containing the computers on which you wish to install NetMan Desktop Client. Simply select a workstation in your network and select **Edit/Check** to check whether the NetMan Desktop Client can be installed on that workstation. A green “workstation” icon indicates that the NetMan Desktop Client can be installed here. Select **Edit/Install** to install the client on this

workstation. You can also select the **Install** and **Check** commands from the shortcut menu, opened by right-clicking on a workstation. A green dot on a blue workstation icon indicates that the client is already installed. In this case, the version number is shown in parentheses next to the workstation name, followed by the name of the associated server.

If you have a later version than the one indicated, select **Edit/Update** to update the client on the workstation.

To remove the NetMan Desktop Client from a workstation, select **Edit/Deinstall**.

You can activate the check or the installation on multiple workstations by selecting the desired workstations first and then activating the “Check” or “Install” command. If you have a small NT domain, you can select the entire domain. For large domains we recommend selecting groups of workstations within the domains, just to help you keep track of the process.

The workstation icons indicate station status as follows:

-  (blue monitor) This workstation has not been checked.
-  (gray monitor with green arrow) This workstation has been checked; the client can be installed on it.
-  (blue monitor with white-on-green checkmark) NetMan Desktop Client is already installed on this station. The client version and connected server are shown in parentheses.
-  (red monitor with white-on-green checkmark) NetMan Desktop Client is already installed on this station, but the program version is outdated.
-  (gray monitor with red X) Evaluation of the workstation installation failed.
-  (gray monitor with yellow arrow) This workstation has to be rebooted to complete installation or deinstallation.

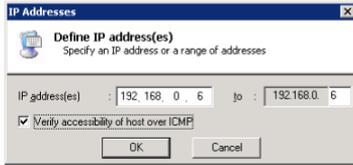
If necessary, you can restart a workstation by selecting **New** from the **File** menu.

In a large network, there may be times when the browse list does not show all workstations when using the “Read from NetBIOS browse list” method. This is why NetMan gives you the option of rolling out the client to stations defined by IP addresses.

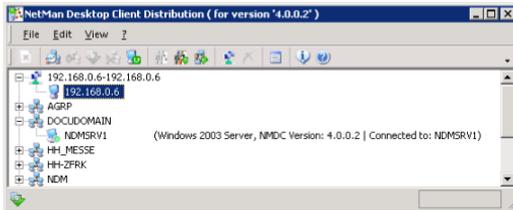


When stations are missing from the network browse list, this does not indicate an error in the Desktop Client Distribution program; rather, it shows that the network browser in your operating system does not always function correctly.

To distribute the NetMan Desktop Client on the basis of client IP addresses, begin by specifying the range of addresses in which you want to roll out the client:



Select the **Verify accessibility of host over ICMP** option if you want to install only on those stations that respond to an ICMP echo request.



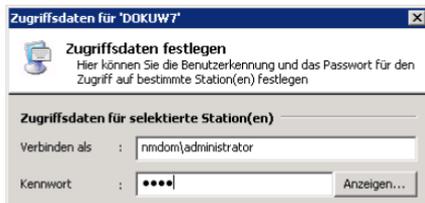
The functions for installing, reloading and deinstalling DOKU operate in the same manner as for stations listed by name.



Keep in mind that the NetMan Desktop Client Distributor program runs under your user account, and thus can only access network resources in which you have access rights. For example, if you do not have permission to access the workstations' Admin\$ shares and registries, you need run this program under a different account. The domain administrator account generally has the rights you need to access these resources. Once you launch the program, it will also need to access the workstations' Admin\$ shares and registries. The Distributor cannot install the NetMan Desktop Client on computers on which the Admin\$ share has been deactivated.

If you do not have sufficient permissions in the network to run the "Check" or "Install" command, for example, an error is written in a log file and the corresponding icons are displayed for the workstations in question. The log file contains all messages; new messages are added at the end of the file.

To use login data other than that of your user context, select **Edit/User ID**. This opens the following dialog:



Please keep in mind that the firewall configurations on your workstations might prevent access to the Admin\$ share. Be sure to adjust the firewall settings as needed; for example, in the group policies.

Software Distributor

To install NetMan Desktop Client using your software distributor, you need some additional information about the client setup program to be installed so you can create a package for the software deployment system. The setup program that installs the NetMan Desktop Clients is an InstallShield package, created with InstallShield version 12.0. To create software deployment packages, you need to create a setup program that does not require any user input. The procedure with InstallShield is as follows:

1. Copy the client setup into a directory specified for this purpose.
2. Call the setup program in that directory with the `/r` switch: enter `setup.exe /r` on the command line.
3. The setup program creates a file called `Setup.iss` in the Windows directory (e.g., `C:\Windows\setup.iss`).
4. Copy the `Setup.iss` file to the new directory that contains your setup program.
5. Make sure that the `nmcsetup.cfg` file is also in this directory.



`Nmcsetup.cfg` contains configuration parameters for the server installation. This file is created automatically when you run the client setup.

Use the `/s` switch (`setup.exe /s`) to run the setup program in “silent” mode.



When you run the setup in silent mode on a terminal server, the universal printer support is installed automatically. Prerequisite is that it was also installed in the source setup, used as the basis for the installation. If the PDF printer driver was not installed, you can install it later using the “Change or Remove Programs” function in Windows. To do this, open Control Panel/Add or Remove Programs, select NetMan Desktop Client and click on the Change button. Now you can add the NetMan PDF driver as an additional feature.

Registering NetMan

The NetMan license you have purchased must be registered before you can use the full version and any modules you have acquired. Before it is registered, NetMan runs in demo mode and the following message is displayed every time NetMan launches an application:



The NetMan modules, licensing scheme and number of licenses are all defined when you order the software and have to be registered once the software is installed.

To register NetMan, run the Registration Wizard from the Toolbox (**Wizards/Registration Wizard**) or from the Start menu on the server console, under **Programs/H+H NetMan/H+H Registration Wizard**.

Call your software vendor to obtain a license code.

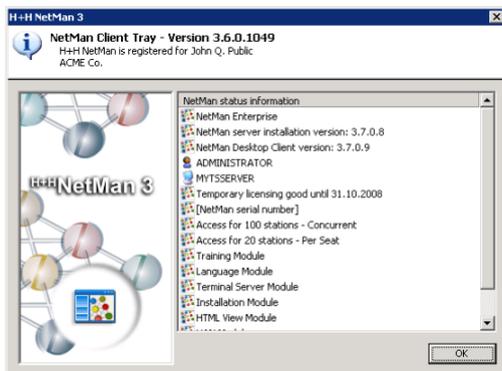
The following information is required for registration:

- The registration data entered during installation (name, company)
- Your NetMan serial number (printed on the bill of delivery as well as on adhesive labels affixed to the NetMan CD and the cover of the user's manual)
- The ID number (from codification of the above data)

The Registration Wizard loads these three items of data automatically:

Enter the license code in the field indicated. Following the next system reboot, the NetMan Service and NetMan Desktop Client will use the license as registered.

The next window shows the edition, modules and number of licenses purchased. Check the data again before finalizing the registration:



Rather than entering a licensing code, you can load licensing data from another directory. To import licenses, click on the "Browse" button ("...") next to **Import license data** and import the `NMCfg.dat` file.



In NetMan version 3.7, client licenses for NetMan can no longer be used to register the HAN and ProGuard modules from earlier NetMan versions. HAN and ProGuard are now available as separate programs. If you wish to use a HAN or ProGuard module from an earlier NetMan version, you need to obtain separate licensing codes for each module.



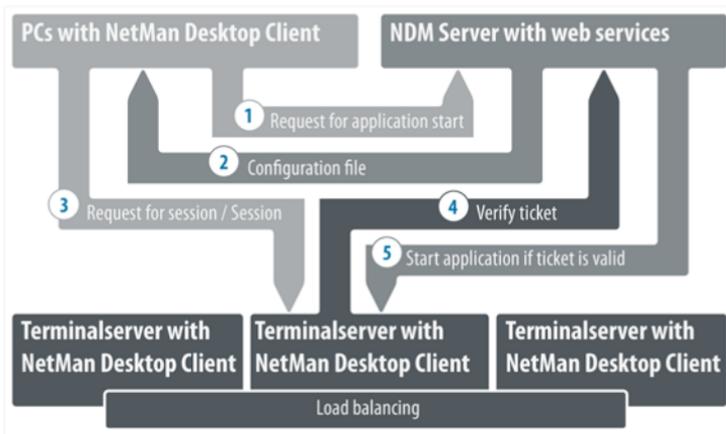
You can license NetMan temporarily for test purposes. The optional modules can be licensed temporarily as well. Once the licensed test phase has elapsed, NetMan returns to its previous licensing status.

System Structure

As mentioned in the previous chapter, NetMan has two main elements:

- Server software
- Client installations

Before we go into detail about these two areas, please refer to the following diagram for an overview of program functions and the interactions between the various NetMan components:



This diagram shows the processes triggered when a NetMan application is launched:

1. The user calls an application that has been configured to open for this user in a terminal server session. This call causes NetMan Client to send a session request to the NetMan Desktop Management (NDM) server.
2. The NDM server returns a configuration file to NetMan Client.
3. Depending on the settings in this configuration file, a session request is sent to the terminal server on which the application is installed.
4. The terminal server sends the ticket supplied in the configuration file to the NetMan Desktop Management server for validation.
5. If the ticket is valid, the application is launched on the client.

If load balancing is used, the application runs on the terminal server that has the most capacity available at that time. Capacity in this case is determined from the numbers of sessions active on the terminal servers.

Server Software

The term “server components” as used in this manual refers to those NetMan components which are installed only on the terminal server; specifically:

- NetMan Databases
- NetMan Service
- NetMan Web Server

NetMan Databases

NetMan databases and configuration files for the server components are stored on the file server or terminal server on which NetMan is installed. These databases contain the following information:

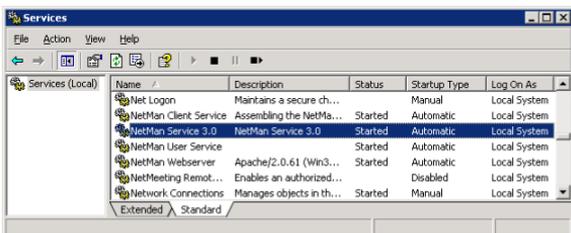
- Users, user groups and user profiles
- Stations, station groups and station profiles
- Installed applications and configurations
- Local and global variables
- Permissions and authentication services (directory services)
- NetMan internal action sequences and external scripts (Windows Script Host supported)



This data is required for the proper functioning of NetMan. We recommend making backup tapes of the NetMan share at regular intervals. All configuration data is stored in this directory and its subdirectories.

NetMan Service

The NetMan Service is an NT service that carries out the main tasks for all NetMan Desktop clients. When a NetMan Desktop client is started, it connects to the NetMan Service over TCP/IP and exchanges data with this service.



The *NetMan Desktop client* provides the following data:

- Station name
- User name
- Details on application data logging functions

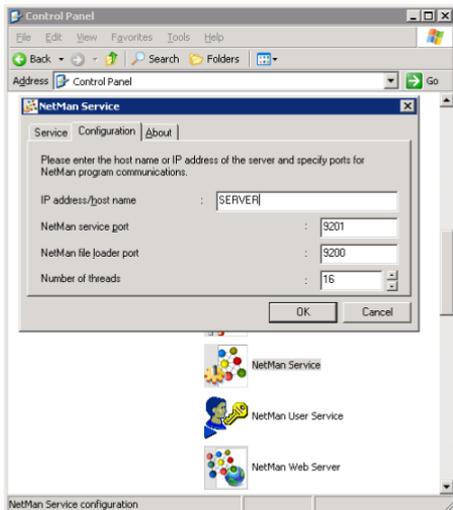
The *NetMan service* provides the following:

- Desktop, in accordance with user privileges
- Information required for launching applications
- Information on application licensing

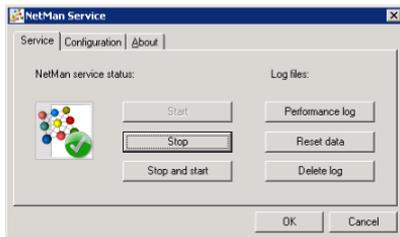
During communication between NetMan service and client, XML structures and configuration files are exchanged over TCP/IP using ports 9201 and 9200. The ports are specified during setup and can be changed on the server in the Control Panel:



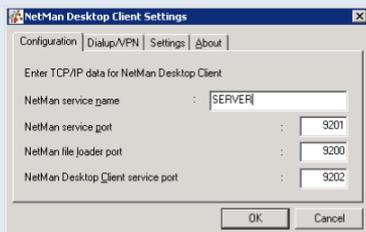
If you have a lot of network traffic, you might wish to increase the number of threads so NetMan can better scale the load. The default value is 16 threads, enough for about 300 simultaneous NetMan Desktop clients.



On the **Service** page of this settings program, you can start and stop the NetMan service. Click on the **Performance** button to view a log file with details on server traffic:



If you change the port settings, make sure the values in NetMan Desktop Client are adapted accordingly:



NetMan Web Server

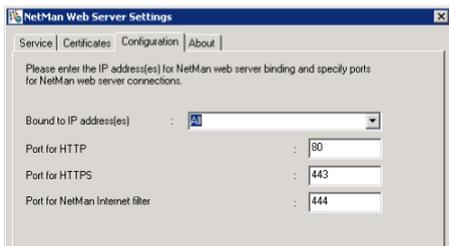
The NetMan Web Server connects the two main elements of NetMan. In addition to providing a web interface, this component also contains the NetMan web services. NetMan uses web services to serve user sessions both over the web interface and in the NetMan Desktop. The web service also provides configuration data for RDP sessions and ICA sessions, and defines the following session properties:

- Session color depth
- Session resolution
- Seamless Windows mode
- Sound settings
- Allocated client drives
- Allocated client printers

The NetMan web service also implements load balancing for RDP sessions. All data for the session request is provided by this service over HTTP or HTTPS. For more information on the NetMan web services, refer to the following chapters:

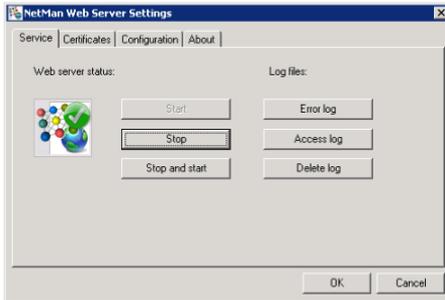
- “Login Methods on Terminal Servers”
- “Launch Methods for HTML View”
- “Extensions for Terminal Servers”
- “Extensions for MetaFrame Servers”

To open the NetMan web server settings, open the Windows Control Panel and select **NetMan Web Server**. On the configuration page, you can define ports for HTTP and HTTPS as well as which IP addresses the server listens on:

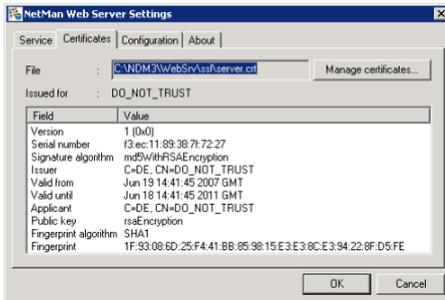


The port specified under **Port for NetMan Internet filter** is used by NetMan's Internet filter component to block access to certain pages. For more detailed information, please see the chapter entitled “*Internet Filter*.”

On the **Service** page of this settings program, you can start and stop the NetMan service. Click on **Error log** to view a log of errors, or **Access log** to view a log of server traffic:



The NetMan Web Server provides content and services both over HTTP and HTTPS. Data transfer over HTTPS requires a valid certificate. With the default settings, the web server is operated with a self-signed certificate issued for a server called *DO_NOT_TRUST*:



We recommend replacing this certificate with one of your own. For details on managing certificates, see *“Certificates for NetMan Web Server.”*

Certificates for NetMan Web Server

Immediately following the installation of NetMan, replace the *DO_NOT_TRUST* certificate with a certificate of your own. The NetMan program offers two basic options for adding certificates:

- Self-signed certificate
- Official certificate (issued by a certification authority)

The chapters “Creating a Self-signed Certificate” and “Requesting and Importing Official Certificates” provide detailed descriptions of the procedure for adding certificates.

Creating a Self-Signed Certificate

1. Open the **Certificates** page of your NetMan Web Server settings and click on the **Manage certificates** button to open the wizard for managing certificates.
2. Select the **Create or request a new server certificate** task and click on **Next**. Enter data in the **Create new server certificate** dialog as required:

CREATE NEW SERVER CERTIFICATE

Please enter all required information for your server certificate. Input is required in all fields.
Please do not use umlauts or other special characters.

Specifications

Server FQDN (example: www.acmeco.com)	:	netman.acme.local
Name of the company (example: Acme Company Inc.)	:	ACME Inc.
Name of the department (example: Data processing)	:	Data processing unit II
City (not abbreviated; example: Anaheim)	:	Anaheim
State (not abbreviated; example: California)	:	California
Country code (2 letters; example: US)	:	US
E-mail address (example: info@acmeco.com)	:	info@acme.com

FQDN of the server. Enter the fully qualified domain name of the server on which you have installed NetMan Desktop Manager. The name has to match the URL that is entered in the browser to access the web interface. For example, if the Active Directory domain is acme.local and the server is called ndm, the FQDN is ndm.acme.local.

Name of the company. Enter the name of your company or organization.

Name of the department. You can use this input to specify a particular department or section of your company or organization (for example, the data processing department).

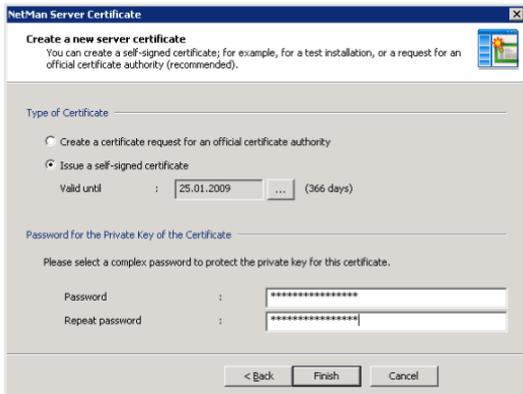
City. Enter the name of the city in which your organization is located.

State. Enter the state in which your organization is located.

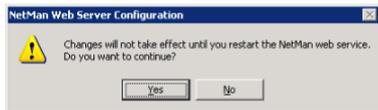
Country code. Enter the two-letter code for your country (see ISO 3166; for example, US for the United States, UK for the United Kingdom, DE for Germany, CH for Switzerland, AT for Austria, etc.)

E-mail address. Enter the e-mail address to be used for contacting your company.

3. Click on **Next** to continue. In the next dialog, you can specify whether you wish to create a self-signed certificate or a certificate request for an official certificate authority. Select **Issue a self-signed certificate** under **Type of certificate**, enter the date for the period of validity and enter a password for the private key:



4. Click on **Finish** to create the certificate and integrate it in the web server. Your changes will not take effect until after you restart the NetMan web server:



Requesting and Importing Official Certificates

Using an official server certificate involves two main steps:

Requesting a certificate: You need to create a certificate request and send it to a certificate authority. The certificate authority checks the specifications of the request for correctness and issues the certificate.

Importing the certificate: Once the certificate has been issued by the certificate authority, you need to import it to your server.

Requesting a Certificate:

1. In the **NetMan Web Server Settings** dialog, click on **Manage certificates** to open the certificate management wizard.
2. Select the **Create or request a new server certificate** task and click on **Next**. Enter data in the **Create new server certificate** dialog as required:

NetMan Server Certificate

Create a new server certificate

Please enter all required information for your server certificate. Input is required in all fields.
Please do not use unilauts or other special characters.

Specifications

Server FQDN (example: www.acmeco.com)	:	netman.acme.local
Name of the company (example: Acme Company Inc.)	:	ACME Inc.
Name of the department (example: Data processing)	:	Data processing unit II
City (not abbreviated; example: Anaheim)	:	Anaheim
State (not abbreviated; example: California)	:	California
Country code (2 letters; example: US)	:	US
E-mail address (example: info@acmeco.com)	:	info@acme.com

< Back Next > Cancel

FQDN of the server. Enter the fully qualified domain name of the server on which you have installed NetMan Desktop Manager. The name has to match the URL that is entered in the browser to access the web interface. For example, if the Active Directory domain is `acme.local` and the server is called `ndm`, the FQDN is `ndm.acme.local`.

Name of the company. Enter the name of your company or organization.

Name of the department. You can use this input to specify a particular department or section of your company or organization (for example, data processing department).

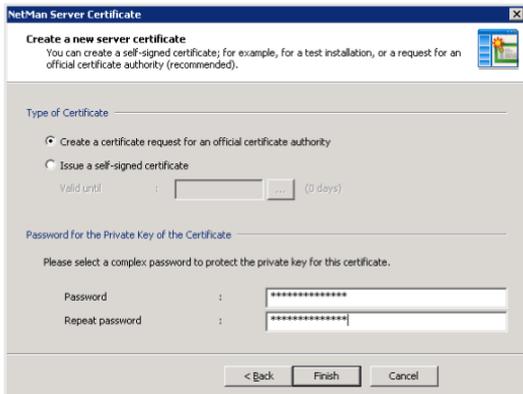
City. Enter the name of the city in which your organization is located.

State. Enter the state in which your organization is located.

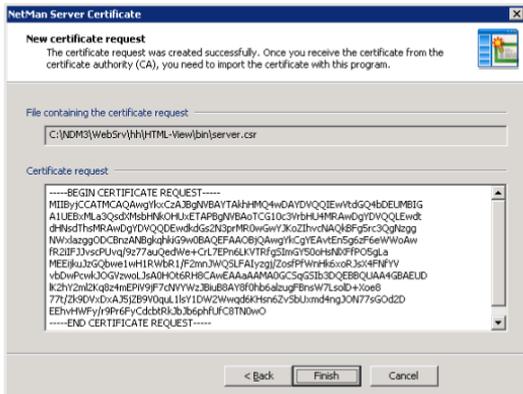
Country code. Enter the two-letter code for your country (see “Creating a Self-Signed Certificate”).

E-mail address. Enter the e-mail address to be used for contacting your company.

3. Click on **Next** to continue. In the next dialog, you can specify whether you wish to create a self-signed certificate or a certificate request for an official certificate authority. Select **Create a certificate request for an official certificate authority** under **Type of certificate** and enter a password for the private key:



4. Click on **Finish** to create and view the certificate request. To submit the certificate request to your certificate authority, you can copy and paste it into the web form at the CA website, or send a file containing the certificate request (by e-mail, for example).



This concludes the first step. Once you have received the certificate from the certificate authority, you can proceed with Step 2 as follows.

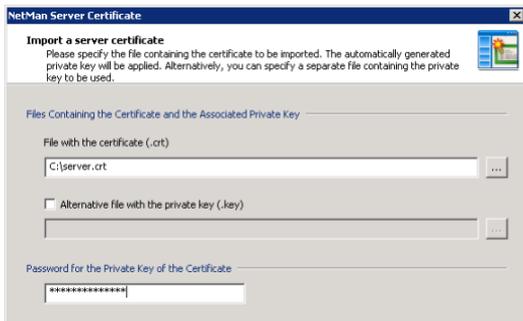
Importing the Certificate:

1. In the **NetMan Web Server Settings** dialog, click on **Manage certificates** to open the certificate management wizard.

2. Select the **Import a server certificate** task and click on **Next** to continue:



3. In the next dialog, enter the file name of the certificate and the password for the private key:



If the certificate file and private key were both created using other tools, rather than using the NetMan wizard to create your certificate request, activate the Alternative file with the private key (.key) setting.



The NetMan system uses the DER format for certificate files, requests and private keys.

4. Click on **Finish** to create the certificate and integrate it in the web server. Your changes will not take effect until after you restart the NetMan web server:



NetMan Desktop Client

The desktop client must be installed on any machine on which you wish to do any of the following:

- Call NetMan administration programs
- Use NetMan to run embedded Windows applications
- Provide access to applications or Internet resources through NetMan for end users

As the name suggests, NetMan Desktop Client integrates Windows applications and Internet resources into the desktops of your network users. The term “integrate” in this context means that shortcuts to applications and Internet resources are added to one or both of the following:

- Windows Start menu
- Windows desktop

The applications thus integrated can run on terminal servers or local workstations.

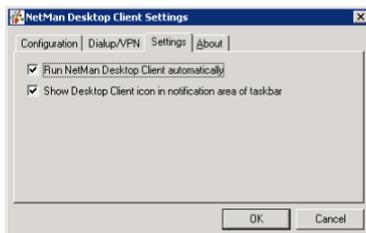
In this sense, NetMan Desktop Client is a *user interface* that does not have an interface of its own. It is fully integrated in the Windows operating system interface and is visible only in the form of certain functions and capabilities that are added to the operating system. Your users do not need to learn anything about operating NetMan Desktop Client in order to use it—in fact, they don’t even have to know it’s there.

Which applications your users can access in their desktops is determined by your assignment of ‘execute’ permissions (to users, user groups, stations, etc.) in NetMan. If there are applications that you do not wish to make available to certain users, your assignment of permissions ensures that those applications are not included on the particular users’ desktops. You can also adapt applications to individual user or station requirements by defining parameters such as monitor settings, audio settings and so forth for the particular client on which the application will run.

The only component of the Desktop Client that the end user can see is the NetMan “tray program” in the notification area of the Windows taskbar, which opens the following menu:



You can hide this icon as well, if desired. To define whether NetMan Desktop Client runs automatically and whether the tray program icon is displayed, select NetMan Desktop Client in the Windows Control Panel:



The following options are available:

- Run automatically
- Run without any visible interface (icon not displayed in the taskbar)

Additionally, NetMan Desktop Client offers basic VPN support. When the client is started, it automatically attempts to build up a connection to the server. You can configure the client to build up a dialup/VPN connection to the network in which the server operates if this first attempt is not successful:



When NetMan Client is shut down on the workstation, the VPN connection is broken automatically.

Sometimes the NetMan Desktop Client opens dialog boxes, for example to show messages on license or resource availability, or to prompt user input. You can define the text shown in the title bars of these dialogs. The default is "H+H NetMan." You might want to replace this with a more informative text, or a text that does not refer to NetMan, for example. This is configured on the **Global Settings** page of the *NetMan Settings*.

Technical Structure of the NetMan Desktop Client

The following information is provided for those who are interested in the technical details. Knowledge of these details is not required for operation of the NetMan software.

The setup program creates a directory called `NetMan` directly under the Windows directory and installs all of the required files there. The NetMan Desktop Client consists of the following components:

- The NetMan environment, in the form of required files (DLLs, etc.).
- An NT service that is launched automatically when the workstation is booted up and runs in the system context. This service carries out all tasks for which your users might not have permission.
- The actual desktop client, which runs under the user account and downloads and executes the required documents (such as 'execute' instructions) from the server over a TCP/IP connection.
- A tray program for user access to NetMan Desktop Client.



On a terminal server, NetMan Desktop Client and its tray program run in one instance per user, while the NetMan client service runs in only one instance per computer.

The NetMan Desktop Client communicates with the central NetMan service over a TCP/IP connection. Essential data is passed between the NetMan service and client over this TCP/IP connection, including:

- Desktops (as XML documents)
- NetMan configurations
- Icons
- Station information
- License information

The TCP/IP connection remains active until the NetMan Desktop Client is closed. Additional data includes documents downloaded over HTTP from NetMan web services, in response to user activities. These can include the following:

- Information files
- Start files (ICA or RDP clients) for running Windows applications in sessions on terminal servers or MetaFrame servers



This technical structure has the following advantages:

NetMan Desktop Client users do not have to have rights in central server directories.

A minimum of network traffic is generated, since communication is limited to small text documents.

Example of a desktop in XML format:

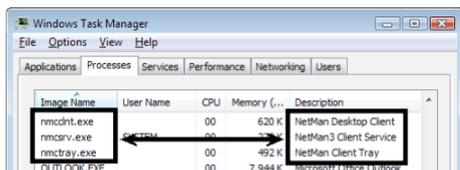
```

001 <?xml version="1.0" encoding="iso-8859-1" ?>
002 <!-- NetMan Desktop file -->
003 <NMDesktop>
004 <Desktop_english>H+H Applications and Links</Desktop_
    english>
005 <Link>
006 <ConfigID>ENCARTA</ConfigID>
007 <Prompt_english>Encarta 2005</Prompt_english>
008 <Description_english>Microsoft Encyclopedia</Descrip-
    tion_english>

```

The downloaded data is stored in a temporary directory and deleted after execution, or when the client is closed.

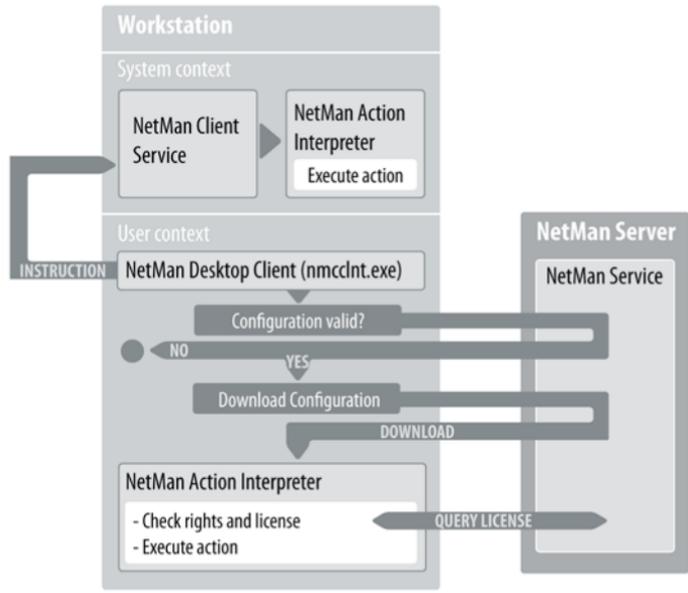
The desktop data is assembled and deleted by a service that is started automatically when the workstation is booted up. The Desktop Client itself and its tray program, on the other hand, run under the user account:



When a desktop link is activated, the Desktop Client checks whether the link is still valid before passing it to an interpreter for execution. The link may be invalid in either of the following cases:

- A modification has been made on the server, through which the user no longer has permission to use the link
- The link was not generated by the NetMan Desktop Client, but was created or copied by the user.

The diagram below shows the processing steps involved in the execution of a desktop link:



To view the stages of processing when the *NetMan Action Interpreter* executes a NetMan configuration, open the Monitors folder in the NetMan Toolbox and run the Trace Monitor. In this example, the Windows Calculator is executed:



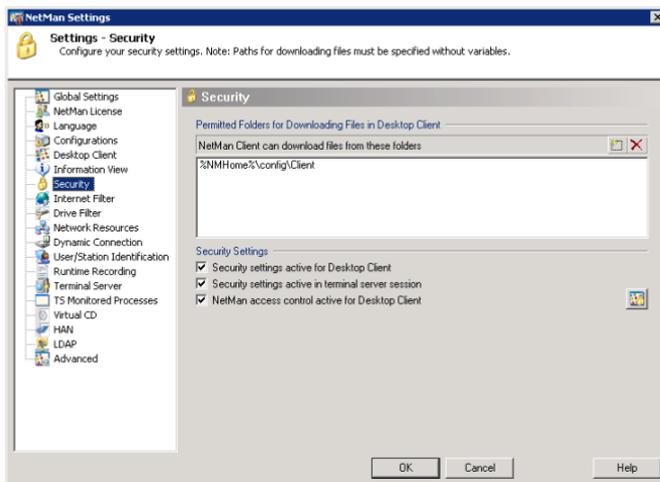
Security Aspects Relating to NetMan Desktop Client

Shortcuts created by Desktop Client can be modified and copied by the user. This in itself does not present a problem. The user can change the order of entries in the Start menu, for example, by selecting **Sort by name** from the shortcut menu or using drag-and-drop.

The user can also drag a NetMan link from the Start menu and drop it on the desktop for easier access. Since it was not created by the NetMan Desktop Client, however, this shortcut is not removed by Desktop Client when the Client is closed. This is not a problem either, as long as the original link that this shortcut points to is available through the user's desktop client. If at some stage this is no longer the case, however (for example, due to a modification in user privileges), a message like the following is shown when the user tries to access that shortcut:

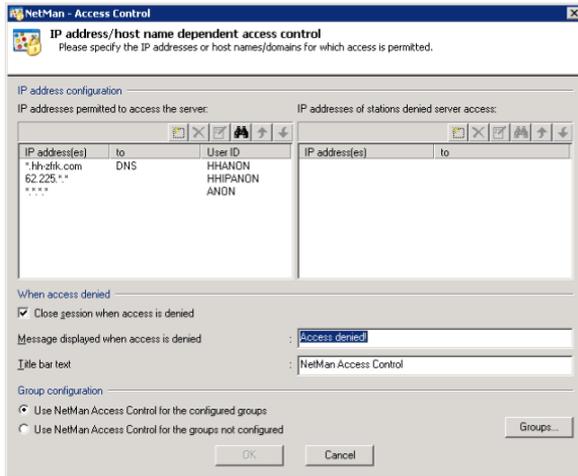


You can edit this default error message in the NetMan Settings. You can deactivate this security mechanism by deactivating the first option under **Security Settings** on this dialog page:



The other security settings on this dialog page are described in the following.

The *NetMan access control* can be switched on and off here. NetMan access control is a mechanism that lets you specify which (ranges of) IP addresses and host names the user can (or cannot) access. To configure access control, open the **Settings** folder in the NetMan Toolbox and run the Access Control program:

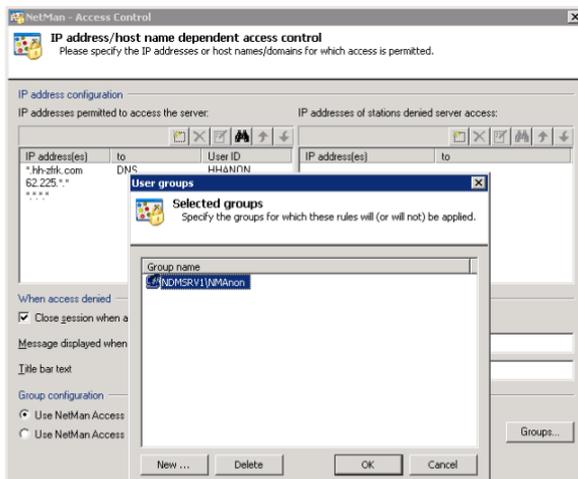


When you first run NetMan, access control is already active and three rules are configured as an example, but no user groups are configured to which the rules are applied.

Using NetMan access control is recommended, for example, if you cannot or do not wish to implement explicit login for access to the system. The access control mechanism is illustrated in the following two examples:

Example 1

You want to make applications available on a terminal server for a particular group of users without requiring the users to log in on this server, and for this reason have implemented anonymous user accounts. At the same time, you want to limit access according to client station IP address. To do this, access control is applied to the “NManon” NT group:

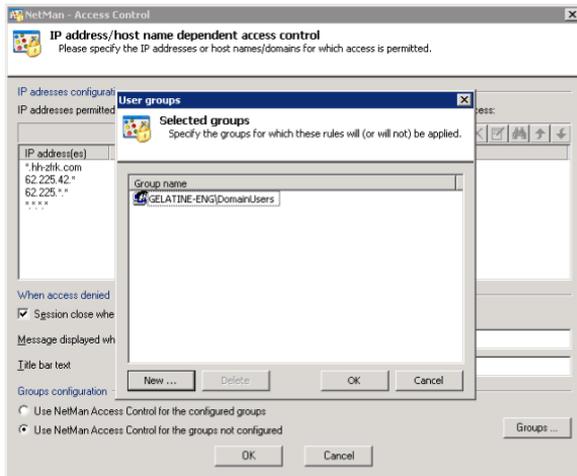


With the configurations shown above, the “anonymous” user name (NMANON001, NMANON002, etc.) is replaced by one of the user names shown under “User ID,” depending on the client IP address. These are more useful than strictly anonymous user names; for example, for recording application usage and for granting permissions, because users can be identified at least with regard to IP address or host name. At the same time, HHIPANON and HHANON users can be allocated to normal user groups with permission to run certain NetMan configurations to which ANON users have no access.

If you delete the third rule (with the IP range defined as *.*.*.*), only computers that have IP addresses within one of the first two ranges are granted access.

Example 2

You want to grant access for all Active Directory Service (ADS) users while at the same time limiting or denying access for users with local accounts. To do this, you can define ADS users as the configured group, and have the access control rules applied to the groups that are not configured:



Now, when a user with a local account runs NetMan – for example, “Administrator” on station XYZ, that user is either assigned the “HHANON” user ID (rather than “Administrator” or “XYZ\Administrator”) or, depending on the IP address, denied access altogether.



You can define both the title bar text and the error message itself on the **Global Settings** page of the NetMan Settings.

After Installation

Once you have installed the software, we recommend familiarizing yourself with the NetMan environment, as this will lay a basis for efficient use of the NetMan system to integrate the applications and resources that you wish to provide for your users.

The following sections provide detailed information on the settings that configure your NetMan environment. As you read, you can adapt the NetMan settings that best configure the program for your network. This chapter begins with the aspects that you need to configure first when setting up your NetMan system:

- Description of the Toolbox and the programs you can access through it ("*NetMan Programs*").
- Definition of NTFS rights in the NetMan directories and of NetMan administrators ("*Directory Structure, Network Rights and NetMan Administrators*").

The chapter entitled "*NetMan Concepts*" presents various concepts of the NetMan program with explanations of the default configurations and options. You can use these features as presented, or not, just depending on your preferences.

NetMan Programs

The first step we recommend following the installation of NetMan is to familiarize yourself with the *NetMan Toolbox*. The NetMan Toolbox provides direct access to the administrative programs in NetMan. It requires installation and execution of the NetMan Desktop Client for its environment. By default, the NetMan Toolbox is integrated in the NetMan System Administration desktop, which Desktop Client in turn integrates on the Windows desktop. The desktop icon for the Toolbox looks like this:



The folders and programs in the Toolbox are described in the following chapters.

Management Console

The *Management Console* is the main system program used for integrating applications and hyperlinks in NetMan. In addition to the usual menus and toolbars, the Management Console has a selection sidebar. This sidebar has two views:

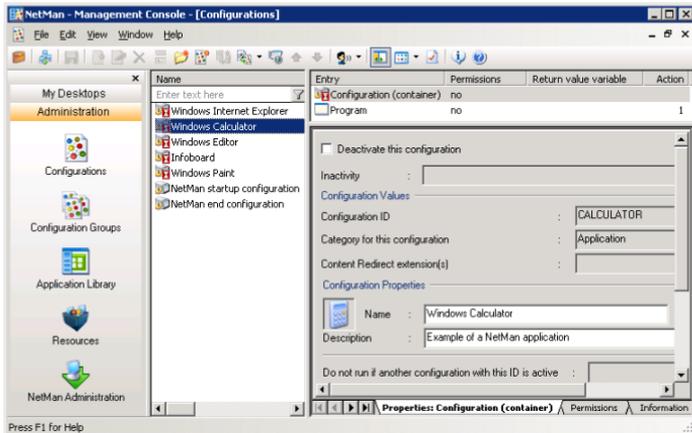
- My Desktops
- Administration

Immediately following installation, the **My Desktops** view contains only the sample desktop. Desktops that you create are shown here as well.

The **Administration** view contains system entries that cannot be added to or deleted.

You can hide the sidebar if desired; for example, to have more space in the program window when configuring a desktop. When you click on an item in this sidebar view, a window opens showing the corresponding data. We shall take a brief look at each of these items before moving on to a detailed description of the sample desktop.

The **Configurations** item opens a list of all of your NetMan configurations. When you click on a desktop, on the other hand, you can see only those configurations which you have specified for the users of that desktop:



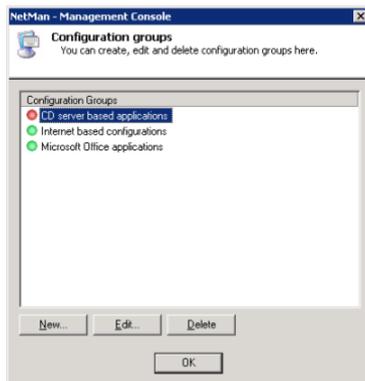
A  symbol shown with a configuration's icon indicates that this configuration is integrated in at least one desktop. A configuration that is linked to a desktop cannot be deleted.

The right-hand pane of this window is the Configuration Editor, and offers the same editing options as those in the Desktop Editor, which opens when you edit a desktop.

The main difference between the Configuration Editor and the Desktop Editor is that the former shows a list of all configurations. This lets you edit configurations that are not linked to any desktop, which is often the case with startup and shutdown configurations, for example.

For details on how to create NetMan configurations and add them to your NetMan environment, see “Integrating Applications and Hyperlinks.”

The **Configuration Groups** item opens a window listing your configuration groups. You can activate and deactivate the groups here. A configuration in a deactivated group cannot be launched by users:



The **Resources** window lets you view and edit *users*, *stations*, *user groups*, *station groups*, *user profiles* and *station profiles*. These NetMan resources are described in detail in the chapter entitled “*NetMan Resources*” in this manual.

The **NetMan Administration** item is a special NetMan desktop, preconfigured for administrative use. This desktop is integrated in the **Administration** view because it contains the NetMan Toolbox.

Statistics

If you select the “Log data” option when you configure a NetMan application call in the NetMan Management Console, records are stored in two log files (databases) every time the application in question is launched.

This data can form the basis of spreadsheets for calculating application usage and user and station activity and, if desired, generating tables and graphs depicting the results (see example below). You can select and group this data by time periods, applications, users, and stations. Special calculation techniques are used for analysis of application licensing and concurrent usage. For details on analyzing your use data statistics, see “*Statistics*.”

Installer

The Installer monitors directories, files and the registry before and after you install software on a given workstation, so you can track all of the changes made during installation, whether by the setup program or through other factors. The differences tracked by the Installer can be recorded in the form of a script, which you can use to recreate the post-installation status on another computer without installing the software on that machine. The Installer program must be registered with your license code before you can use it. For details on how to use the NetMan Installer to monitor installations on your servers, see “*Installer*.”

Monitors

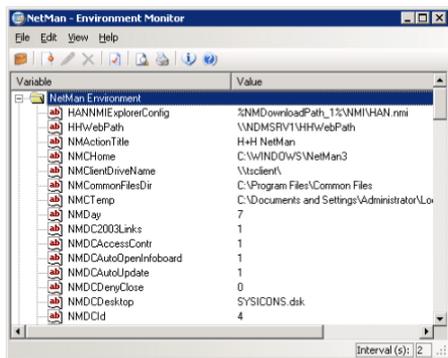
The folder called *Monitors* contains programs that collect and display status information about the NetMan and NetMan workstations and NetMan users.

Trace Monitor

The H+H Trace Monitor lets you monitor NetMan program processes and can help you locate the source of any problems that may occur. The main program window of the Trace Monitor shows messages indicating the status of internal processes. You can configure settings to customize the output. For example, you can assign different colors to each program module, and define the level of output detail. You can also determine whether the tree diagram on the left-hand side is shown or hidden. For details on using the Trace Monitor to test the NetMan configurations you create, see *“Using the Trace Monitor to Check Action Processing.”*

Environment Monitor

The NetMan Environment Monitor lets you view the values currently stored in system and user environment variables. It also lets you set, change and delete the values in variables.



License Monitor

The License Monitor shows the application licenses configured in NetMan with details on the licenses currently in use. For details on assigning licenses to configurations and working with the License Monitor, see *“Additional Program Properties.”*

Database Browser

The database browser shows the records in your NetMan databases. In the main window, you can view sequential and summarized log files as well as the event log. For details on the Database Browser, see *“Statistical Analysis of Log Files.”* For a practical example of the use of the Database Browser, see *“Additional Program Properties.”*

Server and Station Monitor

The NetMan Server and Station Monitor shows all stations and sessions that are currently using NetMan. In addition to the active sessions, terminal server data can also include the current load level on the server and a detailed Load Report. Furthermore, you can use the Server and Station Monitor to launch programs in sessions, or to shut down processes. For a practical example illustrating the use of the Server and Station Monitor, see "*Additional Program Properties*."

Settings

The *Settings* folder contains programs for configuring settings in various areas of the NetMan software suite.

NetMan Settings

Most of the basic settings for your NetMan system are configured in the NetMan Settings program. The settings are divided into the following dialog pages:

Global Settings. General settings, including the path to the NetMan server installation.

NetMan License. Lets you select a licensing scheme and add per-seat licenses.

Language. Defines the languages used in the administrative and client interfaces.

Configurations. Defines timeout periods, title bar texts for 'NetMan action' dialogs and which information files are shown for configurations.

Desktop Client. Basic settings for the NetMan Client, including the choice of desktop.

Information View. Defines which information files are presented to Desktop Client users. Info files are informative texts that are usually assigned to specific configurations.

Security. Settings that specify the directories from which the desktop client can download files.

Drive Filter. Defines which client drives are accessible in terminal server sessions.

Network Resources. Defines variables for drive designations and UNC paths over which applications and their network resources (such as CD-ROMs) are accessed.

Dynamic Connection. Defines which drives are available to NetMan for dynamic drive mapping.

User/Station Identification. Defines how NetMan users and stations are identified.

Runtime Recording. Defines whether and how users and stations are included and identified in NetMan log files.

Terminal Server. Defines how many parallel sessions are permitted on the terminal server as well as settings for single sign-on.

TS Monitored Processes. Lets you add to the list of TS monitored processes.

Virtual CD. Lets you configure settings that affect the way Virtual CD and NetMan work together.

LDAP. Lets you define the access used by NetMan to read and check LDAP privileges.

Advanced. Lets you create and edit NetMan variables.

Internet Filter Settings

When you select **Internet Filter Settings** from the Toolbox, the editor for Internet filter files is opened. This is an interactive editor for creating rules that govern access over HTTP, HTTPS and FTP. You can define different sets of rules for different applications. These rules can limit access to specific URLs, and thus enable highly specialized access control. For details on using this editor, see “*Internet Filter*” in this manual.

NetMan Web Services Settings

The NetMan Web Services Settings program lets you configure settings for NetMan Desktop Client and the terminal server or MetaFrame server. These settings primarily affect the way a session is called. The following settings are configured in this program:

- Which domains can be logged in on through the web interface
- Settings for 2-factor authentication
- Which settings are configured for which stations by the selected launch method
- Settings for load balancing in application sessions
- Which login method is used at session start
- Properties of NetMan anonymous users
- Settings for ticketing

For details on configuring the NetMan Desktop Client, see “Opening Sessions from NetMan Desktop Client.” For more on configuring your terminal servers, see “Extensions for Terminal Servers.” For information on configuring a MetaFrame server, see “Extensions for MetaFrame Servers.” Details on configuring the ticketing function are given in “Advanced Security Features.” For information on configuring the web interface, see “Web Interface (HTML View).”

NetMan Access Control

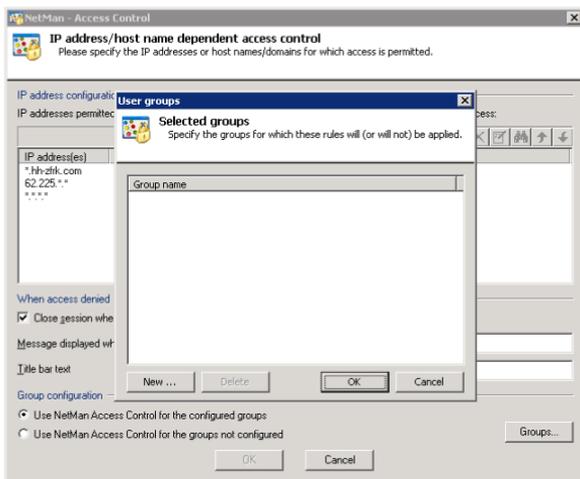
NetMan access control features let you specify which workstations can use NetMan Desktop Client to access a server installation. Access can be restricted by workstation IP address or host name. The access control mechanism is applied to those users you specify for this purpose.



Exercise caution in defining groups and access privileges. Do not advertently prevent administrator accounts from running NetMan Desktop Client, as this would block access to all administrative functions.

Immediately following installation, the configuration of groups does not include an NT group to which access control is applied. This means access control is switched

off. Activate the **Use NetMan Access Control for the configured groups** option and click on the **Groups** button to open a dialog for adding groups to which access control is applied:



For example, you can have access control applied to all NT users while you, as administrator, can still run NetMan Desktop Client from any workstation.

NetMan Authentication Services

NetMan authentication services are used in conjunction with HTML View and define the options for authentication on terminal servers. This entry is directly visible only on the server on which NetMan is installed, because the authentication services operate internally with local paths on the computer. For details on working with the authentication services, see *“Authentication Services.”*

Wizards

The folder called *Wizards* contains helper programs for NetMan.

NetMan Desktop Client Distribution

The NetMan Desktop Client Distributor makes it easy to roll out NetMan Desktop Client in the network. This program copies the setup program to selected workstations on the network, and executes the setup on those stations in a system context in silent mode. For details on working with the NetMan Desktop Client Distributor, see "*NetMan Desktop Client Distributor*."

Database Wizard

The Database Wizard helps you maintain your NetMan databases. You can use it to reindex databases and to check internal references.

Registration Wizard

The Registration Wizard helps you register your NetMan program license. If your license is not registered, the NetMan software runs in demo mode. For details on registering NetMan, see "*Registering NetMan*."

Online Documentation

The *Online Documentation* folder contains all NetMan documentation:

- **NetMan Almanac.** The Almanac contains complete information on the variables, actions, directories, record attributes and error messages in NetMan as a supplement to the manual and the online help.
- **NetMan Online Manual.** This is a shortcut to the NetMan manuals in PDF form.
- **NetMan Online Help.** Shortcut to the NetMan online help.
- **Information File about NetMan Toolbox.** This opens a file containing details on the programs available through the Toolbox.

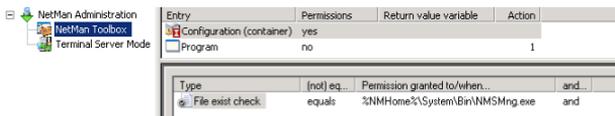
Directory Structure, Network Rights and NetMan Administrators

The standard NetMan installation has one directory with the following four subdirectories:

- System
- Prot
- Config
- WebSrv

The system account as well as NetMan administrators require unrestricted rights in the entire NetMan directory. Your NetMan users without administrative rights do not require any rights in this directory.

With the default settings, NetMan Desktop Client installs the NetMan Administration desktop on the Windows desktop. This contains only links to programs required for administration of the NetMan system, and should be accessible only to NetMan administrators. As an example of a possible option for hiding the Toolbox from non-administrators, a *File exist check* condition has been configured to make access to the Toolbox (in NetMan parlance: permission to run the Toolbox) conditional on the location of the Management Console program file (**NMSMng.exe**). The *File exist check* is one of many NetMan rights that can be used to make access to configurations or actions dependent on any of a variety of conditions; in this example, on the detection of a specified file.



If rights in the NetMan directories are assigned as described above, your normal (non-administrative) NetMan users will not see any link to the Toolbox program because they do not have rights in the corresponding directory.



There are other ways to control program access as well. For example, you can click **New...** and select permissions based on existing Novell, NT or LDAP groups. Alternatively, you can open the Toolbox, select **Management Console/Resources** and create a NetMan group exclusively for NetMan administrators. Assign the NetMan Administration desktop to an administrators' profile or to one administrator.

NetMan Concepts

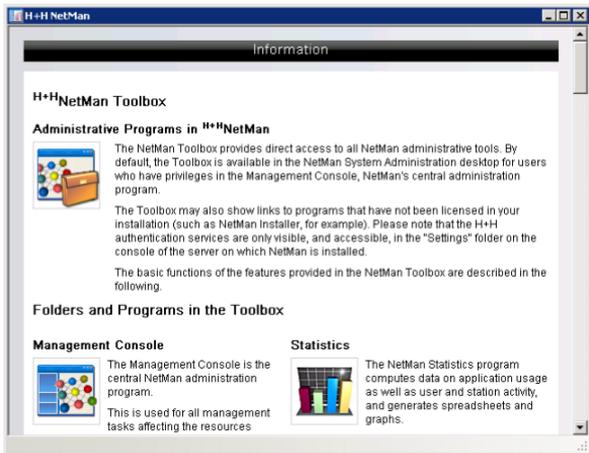
This chapter describes some of the advanced concepts in NetMan. It will provide useful insights into how NetMan can best be put to use in your own network.

The following NetMan concepts are described here in detail:

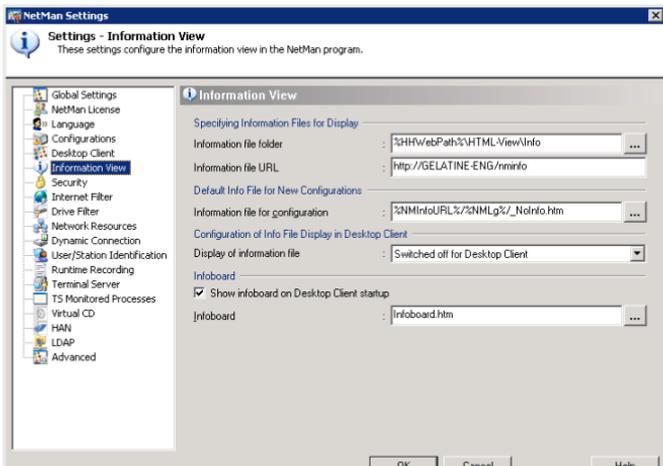
- Information files
- NetMan environment
- Application drives
- Frequently used network resources and drives
- Startup and shutdown configurations

NetMan Information Files and the Infoboard

You can configure NetMan to present an informational HTML page before the selected Windows application or Internet resource is opened. The example below shows the information file describing the Toolbox:



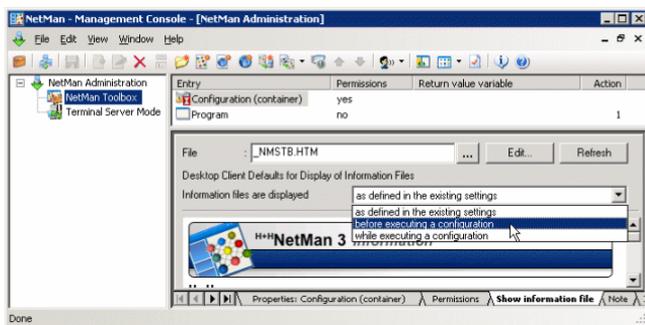
The information file on the NetMan Toolbox contains detailed descriptions of all the Toolbox items. The concept of info files has been adopted from HTML-based user interfaces such as those often used in libraries. Because such environments frequently serve users who are not familiar with the applications offered, it can be useful to present some details on an application before it is launched. In the NetMan Desktop Client, this feature is inactive by default. It can be activated on the **Information View** dialog page in the NetMan Settings:



You can choose from the following settings:

- Switched off for Desktop Client (default setting)
- Before the configuration is executed
- Simultaneous with execution of configuration

This setting can be overwritten for individual configurations.



New configurations inherit the active setting. You can modify the setting after creating the configuration.

A similar concept is the NetMan Infoboard, which is active by default. The Infoboard is shown when the NetMan Desktop Client is launched. You can deactivate this feature on the Information View page of NetMan Settings. If you wish to use the Infoboard, you can modify this file as desired or define a different HTML file to be presented in its place.

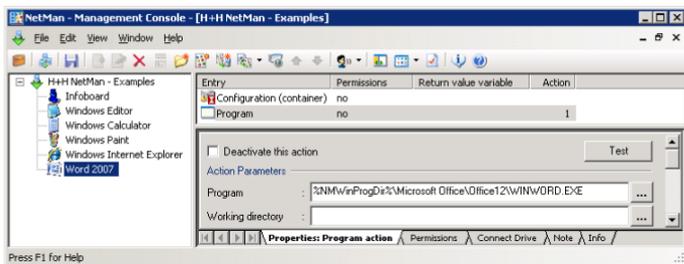
NetMan Environment

NetMan uses variables throughout its programs to identify logical drives, paths and system states.

For example, the NetMan installation directory is stored in the *NMHome* variable. There are a number of advantages in using variables:

- Consistent use of variables makes your system easier to manage. Storing a frequently used path name in a variable can save a lot of work when the path name is changed, as it only has to be edited once to implement the change throughout your system.
- Using variables to make process more abstract—for example, in scripts—lets you transfer processes to various situations, and even different customers. This is the only way to use the NetMan Application Library (see “Application Library”) for preparing exemplary solutions.
- The use of variables adds flexibility. You can have different values stored in a given variable, depending on certain specified conditions (such as user or station ID, for example). These can be used to overwrite your global NetMan settings for specific users, user groups, stations or station groups. For example, the “information files” feature described above can be generally deactivated, but active for certain workstations.
- Variables enable dynamic administration of system states. They can be modified through user input. For example, if you use the Language Module in the NetMan Desktop Client you can permit the active language to be changed during operation.

The following is an example of the first advantage listed above, in which the program call for MS Word is defined using the *NMWinProgDir* variable rather than an explicit path:



Thus the program call is independent of the computer's operating system. The MS Office suite may be installed in different directories or on different hard disks on the various network stations, but the program call using the variable works for all stations.

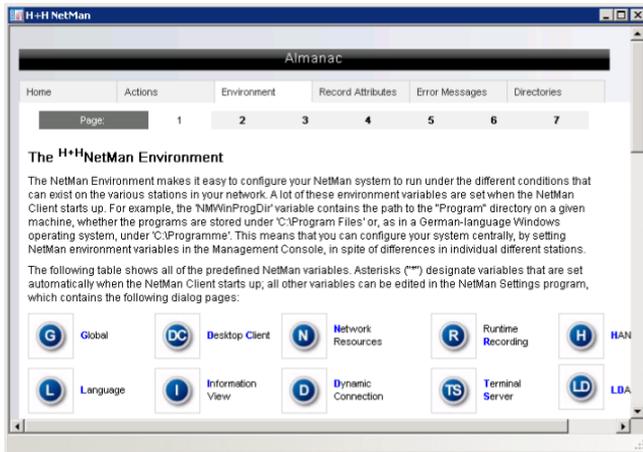
NetMan supports the use of variables by converting explicit path names to environment variables.

For example, when you browse for the program file in the “Program” field shown above, NetMan enters the *NMWinProgDir* variable in the path automatically.



Automatic conversion of path names to variables is active in the default settings. You can switch this mechanism on or off on the Global Settings page of the NetMan Settings.

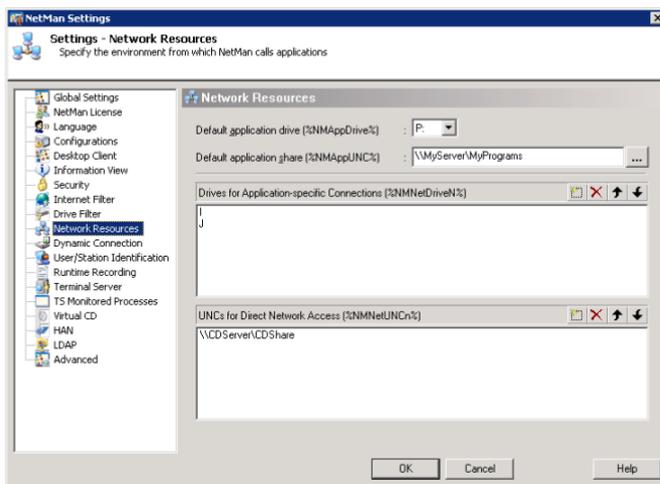
For a complete list of the NetMan variables with descriptions, please refer to the NetMan Almanac in the NetMan Toolbox:



Application Drive

Networks often have one or more central directories specifically for applications. In some cases it may be necessary to use a DOS drive designation, as some applications cannot handle UNC paths.

On the **Network Resources** page of the NetMan Settings you can define an application drive, *NMAppDrive*, and a UNC path, *NMAppUNC*, in which you can install the applications you wish to control using NetMan. Then you can use these variables in your application configurations, rather than explicit drive designations:



With the default settings, the NetMan application drive is mapped automatically when NetMan is launched if you define the *NMAppDrive* and *NMAppUNC* variables in the NetMan Settings.

Frequently Used Network Resources

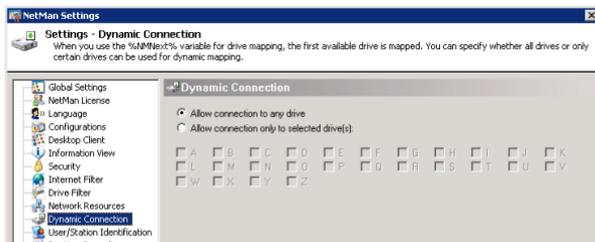
It is important to know the location of the network resources that are used most frequently, and whether your applications require a volume or a network share mapped to a drive letter, as is often the case in CD-ROM networks. The illustration shown in the previous chapter, for example, shows a UNC path to a Virtual CD File Server version. This path can be designated “NMNetUNC1” in NetMan:



We highly recommend using the *NMNetUNCn* variable for frequently used network resources. In this case, you enter %NMNetUNC1%, %NMNetUNC2%, etc., in your configurations rather than explicit UNC paths. You can store drive designations for application-specific drive mapping in the *NMNetDriveN* variables and the map %NMNetDrive1%, %NMNetDrive2%, etc., rather than explicit drive designations.

Dynamic Connection:

You can use the *NMNext* variable for drive mapping rather than *NMNetDriveN* or a specific drive. In this case, NetMan automatically connects the first available drive. With the default settings, all drives are available for mapping. On the **Dynamic Connection** page of the NetMan Settings, you can restrict the drives available for mapping.



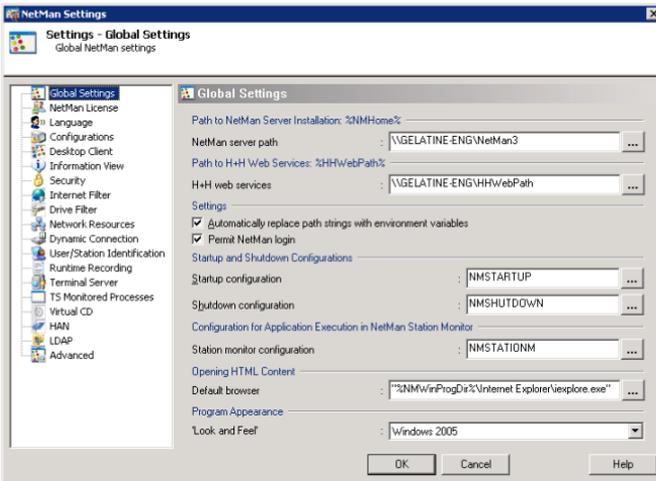
Mapping of shares or volumes with application data can only be performed dynamically if the applications support this capability. Many applications, however, can access data only under the same drive letter under which the data was found when the application was installed. For an example of how the *NMNext* variable can be used, please see “*CD-ROM-based Applications*” under “*Integrating Applications and Hyperlinks*.”

If you use the Virtual CD program, you can define the paths to virtual CDs in the NetMan Settings. In this case, NetMan automatically converts these paths into environment variables *NMVCDPath1*, *NMVCDPath2*, etc.

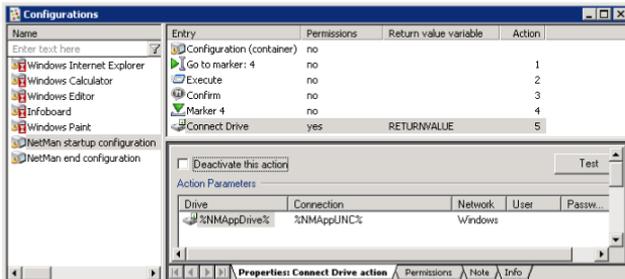
NetMan Startup and Shutdown

All of the elements linked in NetMan are defined in the NetMan Management Console as configurations. (For more information about the structure of NetMan and how to use the Management Console, see “*Integrating Applications and Hyperlinks*,” for specific information about startup and shutdown configurations, see “*Startup and Shutdown Configurations*” in that chapter). You can define special configurations that are executed when NetMan is launched, or when it is closed, that are not shown in the NetMan desktops. These configurations can be used to run programs (like an “autoplay” function), map drives, log in users on network resources, and set variables. Startup and shutdown configurations can include any type of NetMan action except Program actions.

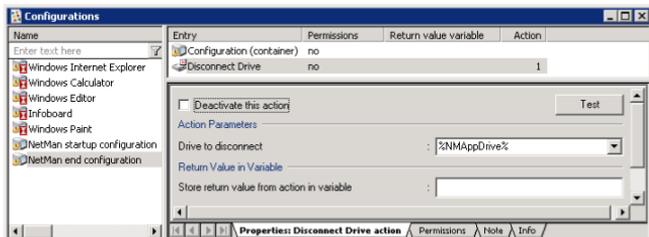
Run the NetMan Settings program and open the **Global Settings** page. The default startup and shutdown configurations are called NMSStartup and NMSShutdown:



To modify these, edit NetMan startup configuration and NetMan shutdown configuration in the NetMan Management Console:



The default NetMan startup configuration contains a *Connect Drive* action that maps the application drive. The variables defined in the Settings program are used here (see “*Application Drive*” for details). This drive is disconnected again in the NetMan shutdown configuration:



Integrating Applications and Hyperlinks

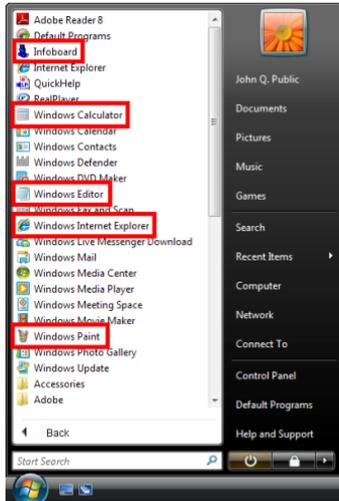
This chapter describes how to integrate applications, on-line access accounts, URLs, and HTML documents in your NetMan system for distribution to your users. NetMan is accessed by users either through the NetMan Desktop Client or from an HTML document. HTML documents used for access to NetMan-controlled applications can be generated by the optional HTML View Module which is included with your NetMan Base Module, or you can write them yourself. These features are described in detail in the second part of NetMan Manual. This chapter describes only the mechanisms for access over NetMan Desktop Client, and is divided into the following sections:

- The chapter "*NetMan Configurations*" explains some of the basic concepts of the NetMan software and terminology.
- The chapter "*Working with the Management Console*" introduces the Management Console, your central system program, and describes its operating elements. Examples are given to show you how additional program and hyperlink properties can be activated in your applications. You will also learn how to create your own desktop entries and how to integrate your applications and hyperlinks in the NetMan system.
- Das Kapitel "*NetMan Actions*" widmet sich den verschiedenen NetMan Aktionen und deren Verwendung.
- The chapter "*Special Configurations and Applications*" offers tips on integrating special types of applications and NetMan configurations, such as CD-ROM applications, HAN accounts, and startup and shutdown configurations.

NetMan Configurations

First of all, we shall define the terms “application,” “hyperlink,” “program” and “NetMan configuration” as they are used in the context of NetMan, to help you better understand how NetMan works.

When you run your NetMan Desktop Client, you will find five sample NetMan configurations in the Start menu, under Programs:



All of the entries added to a desktop are called NetMan configurations. There are basically two types of NetMan configuration:

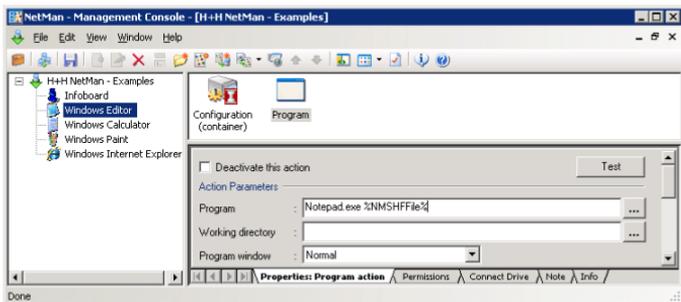
- Containers
- Folders

Folder configurations are for organizational purposes only, and—like hyperlink configurations—cannot contain any actions. The type of a configuration is indicated in the Management Console by the symbol shown and by the designation (Container) or (Folder):



Container configurations contain a number of (Windows-based) “actions,” which are linked to the Windows operating system. These configurations can be executed only on the Windows operating system. If a container configuration is activated by a client

running a different operating system, such as Linux or Macintosh, a Windows terminal server is required for processing the actions. A container configuration usually launches a program:



The sample shown above runs the "Notepad.exe" program (Windows Editor), chosen for this example because it is generally found on all computers that run Windows.

We shall use this example to clarify our definitions of "application" and "program." "Calc.exe" is certainly a program, but it can also be termed an application. As a rule, an application consists of more than just a program call. For example, Word is referred to as a "Microsoft Office application" because the program itself (in this case, "winword.exe") requires a number of other specific files and directories in order to run. Thus the term "application" indicates a program together with an array of other elements.

The term configuration, as used in the context of the NetMan software, is even broader; it refers to a completely user-definable logical unit, created by a NetMan administrator. This configuration is like an empty container that you can fill up with 'execute' jobs, which NetMan processes in sequence—hence the term container configuration. An individual job is referred to here as an action. In our example, the configuration called Windows Calculator contains only one action; this is a "Program action" configured to call the calc.exe program. There are a large number of different actions available that you can add before or after the Program action. Generally these are more relevant for use with a "real" application, such as Microsoft's Encarta, for example:

- Create a login dialog or map a network drive for access to the program or to the resource it requires—for example, to the Encarta CD-ROM.
- Create DLL files or registry entries on the client workstation.
- Require a password or other user input which is then passed to the program on the command line.
- Launch other programs to run in parallel.
- When launching a program or hyperlink, you can add modifications to the Internet filter settings.
- Restore the working environment to its previous state when the program is ended.

The following diagram illustrates the relationships between program, application and NetMan container configuration:



With the most basic programs, the NetMan configuration does not contain any preparatory or concluding actions; the only action is the program or hyperlink call, as is the case in our “calc.exe” example.

In many cases, integrating an application or hyperlink in NetMan will consist of no more than two steps: first you create a configuration, then you add a single action containing the command that launches the application. The number and variety of actions available, however, give you a wide range of possibilities for your NetMan configurations. Processing a NetMan container configuration is like executing a script, because you can define conditions under which any individual action will—or will not—run. Conditions for running an action are defined in the form of ‘execute’ permissions that are granted or denied based on user name, station designation, group membership, environment variables, operating system, or any of a number of other factors. Thanks to NetMan’s interface to the Windows Script Host, you can even create your own NetMan actions.



Thus a container configuration is a logical unit that can be executed by a user. It can contain up to 999 actions, or none at all. A program action runs an application that is integrated in a NetMan configuration. A hyperlink action loads a web page.



Whenever this manual mentions launching a NetMan application call, or calling a NetMan-controlled application, whether from the NetMan Client or HTML View, it means that the processing of a container configuration is activated. This configuration can contain practically any number of other actions, which are processed either before or after the program action.

Today’s programs require access not only to data on the workstation (such as the program directory, CD-ROM drive, and so on), but also to data on the company’s intranet or in the Internet. When network access is triggered through a NetMan action, you can configure the NetMan Internet filter to define which sites can be reached.

Increasingly, data is accessed using browser technology. This is why the NetMan *Hyperlink* action has gained in importance for configuring the NetMan system. The Hyperlink action uses the browser of your choice to access HTML-based data, whether it is stored on the hard drive, a CD-ROM, the intranet or the Internet.

Hyperlink actions load HTML documents over HTTP. To do this, the action launches MS Internet Explorer, or a browser of your choice, using the NetMan Client. Hyperlink actions have the following properties in common with Program actions:

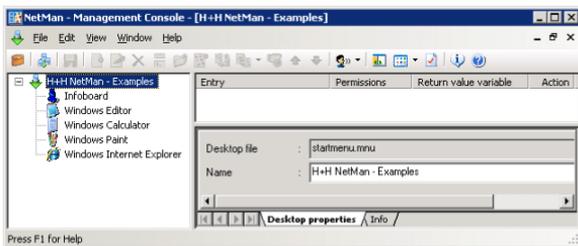
- The log file can reflect the number of times they are called.
- An Internet filter can be assigned to them.

NetMan Desktop Client executes Hyperlink actions as follows: The NetMan Desktop Client launches the browser designated for this purpose in the NetMan Settings and loads the URL specified in the Hyperlink action.

Working with the Management Console

NetMan comes with a preconfigured desktop as an example. You can open this desktop in the Management Console by selecting **My Desktops** in the sidebar on the left and then selecting the sample desktop – the only element under “My Desktops” when you first run NetMan. When you select this element, the *H+H NetMan – Examples* desktop is opened in editing mode. This is the default desktop, and is integrated in the Start menu for all NetMan users. Any changes you make here are implemented on the desktops of all your NetMan clients.

The window below shows the fully expanded desktop structure, with the selection sidebar hidden. The active element in the folder view in this example is the root entry. Since the root entry is not a configuration and does not contain any entries or actions, the upper pane on the right, also called the Entry pane, is empty. The lower right-hand pane shows the Desktop properties and Info dialog pages. You can edit the properties of the selected element—in this example, the root entry—in this pane:



You can have the name of this desktop added to the Windows Start menu as a sub-directory under **All Programs**. To do this, deactivate the **Add NetMan desktops to the top layer of the ‘All Programs’ folder in the Start menu** option on the **Desktop Client** page of the NetMan Settings. With the default setting, all of the entries in a NetMan desktop are listed under **All Programs** in the Start menu. When a NetMan desktop is displayed on the Windows desktop, the desktop name is irrelevant.

The dialog pages **Desktop properties** and **Info** are displayed in the lower right-hand pane. You can edit the properties of the selected element – in this example, the root entry – in this pane. The **Info** page shows information on whatever entry is selected in the Entry pane; if the desktop root is selected, as in this example, the information shown applies to the Desktop Editor itself.

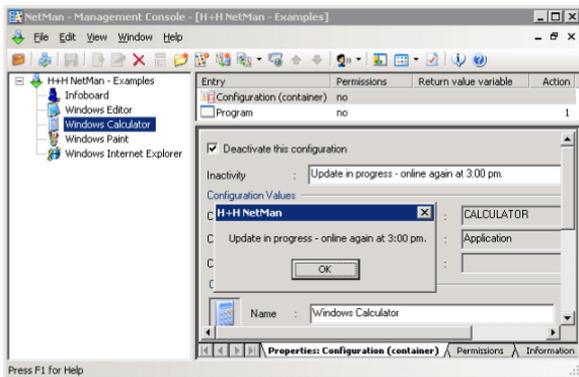


When you first start working with NetMan, it can be helpful to read the Info pages on each of type of entry.

The configurations integrated in the desktop are listed below the root entry in the folder view. Select one of these to edit its properties. For example, you can select the “Windows Calculator” configuration and edit its Name and Description. Your changes

are active on all client machines as soon as you save the desktop. The name is shown as the shortcut name, and the description is displayed as an informational tooltip.

If you select the **Deactivate this configuration** option, the configuration will still be visible in the NetMan Client, but if a user tries to activate it, a window opens with the message entered here under “Inactivity.” This can save you from being asked repeatedly why the application is not working. Here is an example:

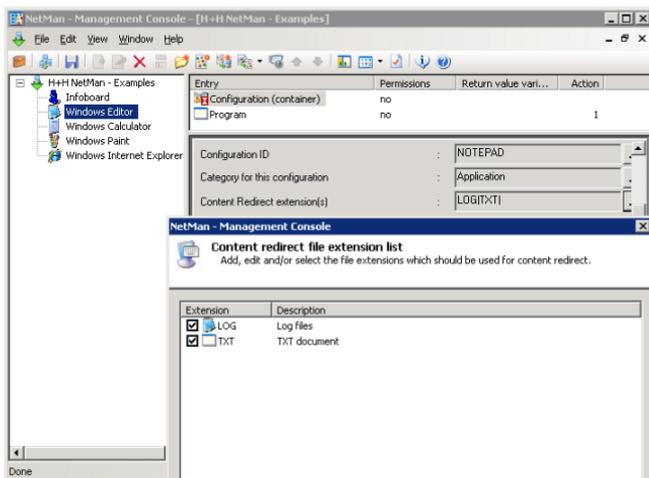


For a container configuration, you can enter an identifying string under **Do not run if another configuration with this ID is active**. This is also referred to as a “lock ID,” and lets you prevent incompatible applications from running simultaneously. This can be useful if you have applications (or separate instances of the same application) that interfere with one another. For example, one application might try to access data that another application locks during use, or an application might be internally designed to run in only a single instance on a given machine. Enter any string you wish as ID, and then enter the same string in this field for the configuration(s) that you want to prevent from running while this one is in use. In such cases, an error message like the following could result:



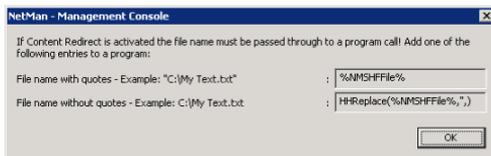
You can link NetMan configurations to file name extensions; for example, to have a certain configuration launched whenever a certain type of file is executed. This mechanism is known as *content redirection*.

To implement content redirection in a NetMan configuration, click on the button next to the “Content Redirect extension(s)” field and select or edit file name extensions as desired:

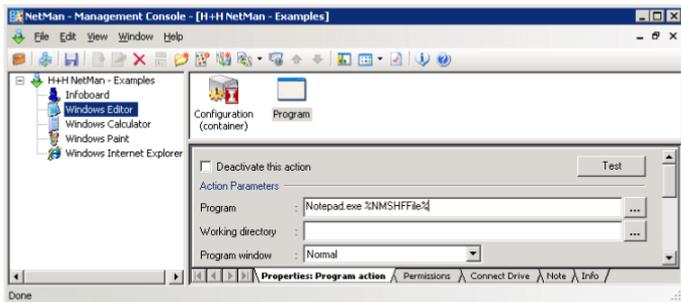


The following conditions must be met before content redirection can function properly:

- A NetMan Content Redirect action must be configured to switch this mechanism on or off. With the default settings, content redirection is switched off. This action is ideal for use in startup/shutdown configurations.
- If the program linked to a given file name extension opens a terminal server session, it is important to make sure that access to client drives is permitted, as the application accesses the local file on a client drive.
- You need to configure a program action that will pass the name of the executed file to the program, by passing the `%NMSHFile%` variable as an argument on the command line. If the Management Console does not find this variable in any program action, an error message is shown.



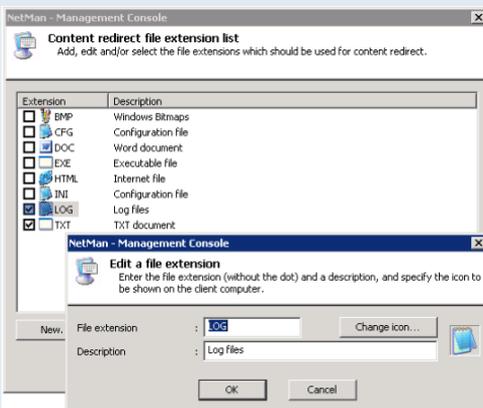
For example, the command line that calls “Notepad.exe” may take the following form:



You can link more than one program to a given file name extension in the Management Console. For example, you could link both the Windows Editor and Microsoft Word to the “TXT” extension. When a file is executed (for example, when a user double-clicks on the file), NetMan checks which configurations are available to the user at that moment in the Start menu and on the Windows desktop of the client. If only the Windows Editor configuration is available, the file is opened with this program. If both configurations are available, the file is opened with the first one found.

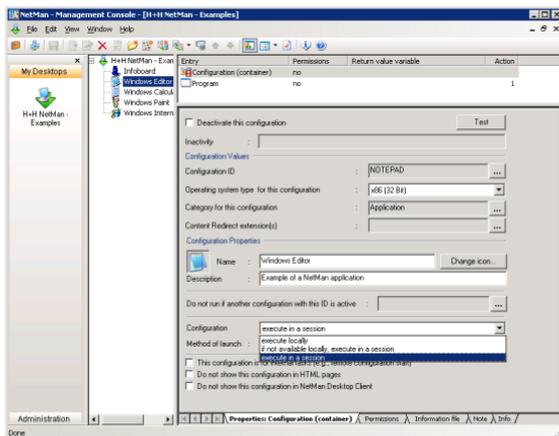


In the dialog for selecting file name extensions, you can specify an icon for each file name extension. Icon assignments are stored on the client machine by NetMan Desktop Client and registered for the specified file types. Thus even file types unknown to your operating system are shown in the Windows Explorer with icons.



The following options let you specify the context for processing configurations:

- Do not show this configuration in an HTML page
- Do not show this configuration in NetMan Desktop Client
- This configuration is for internal tasks (e.g., remote configuration start)



If the **Execute in a session** option (default setting) is active, the application is executed in a session. When the application call comes from a client machine, the application is executed in a session on a different machine: the terminal server. If the application is called by a NetMan Desktop Client on a terminal server, it runs locally on that server. If it is not installed on that terminal server, a session is automatically opened on the first terminal server found on which the application is installed.

If the **Execute locally** option is selected, the application is executed on the local machine. Thus NetMan Desktop Manager is not only ideal for the integration of applications on terminal servers, but also offers advantages for the integration of local applications.

The third option, **If not available locally, execute in a session** can be particularly useful. With this setting, NetMan first attempts to run the application locally. If this attempt fails because the file specified in the first Program action is not found locally, the application is opened in a terminal server session. This enables an elegant solution for calling a program in a heterogeneous network:

- If the program is installed on the workstation, it is called locally.
- If the program is not installed on the workstation, it is opened in a session.
- When a session is opened, it is automatically opened on the right server.



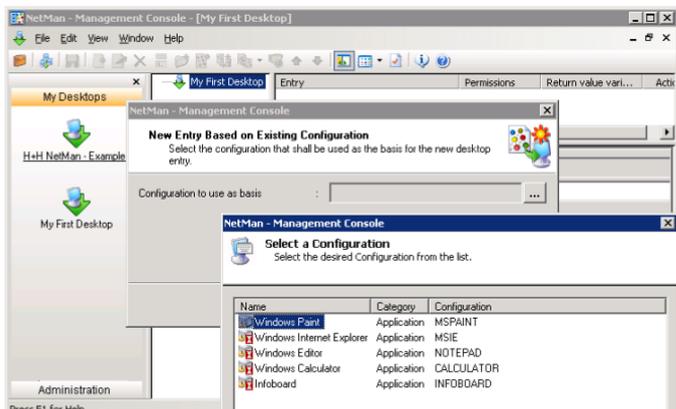
Keep in mind that the distinction between “Execute locally” and “Execute in a session” is made only when the configuration is called using NetMan Desktop Client. If it is called using the web interface, a session is opened regardless of the setting here, as the web interface does not support local application calls.

The **Do not show this configuration in an HTML page** and **Do not show this configuration in NetMan Desktop Client** options determine whether the configuration is available through the web interface, or through NetMan Desktop Client, respectively.



You can configure a single desktop for use in both the web interface and in NetMan Desktop Client, and then use the **Do not show this configuration in an HTML page** and **Do not show this configuration in NetMan Desktop Client** settings to have different sets of configurations available, depending on the interface used to open the desktop.

If the **This configuration is for internal tasks (e.g., remote configuration start)** option is active, the configuration is hidden from view in certain dialogs and selection lists. For example, if you create a new NetMan desktop and have NetMan configurations transferred to it from existing desktops, the configurations that are marked for internal tasks are not shown in the list of available configurations. In the following example, a selection dialog has been opened from the **New Entry Based on Existing Configuration** dialog, but does not show the startup and shutdown configurations that come with NetMan.



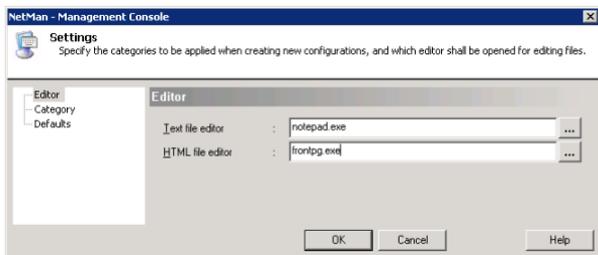
You can activate the **This configuration is for internal tasks** option for configurations that are not assigned to any desktop, and use those configurations for functions that are not desktop-specific.

Each configuration has the following dialog pages:

- Properties: Configuration,
- Permissions,
- Information file,
- Note and
- the Info page described above.

We will take a closer look at the **Permissions** page later. In the current example nothing has been entered on that page, which means that any NetMan user can access this configuration and can see and open this entry as a desktop folder.

Click on the **Information file** tab to view the information page for this configuration. The default editor for this is “Notepad.exe.” To use a different editor, select **Settings** from the **View** menu and enter the command line call for the desired program:



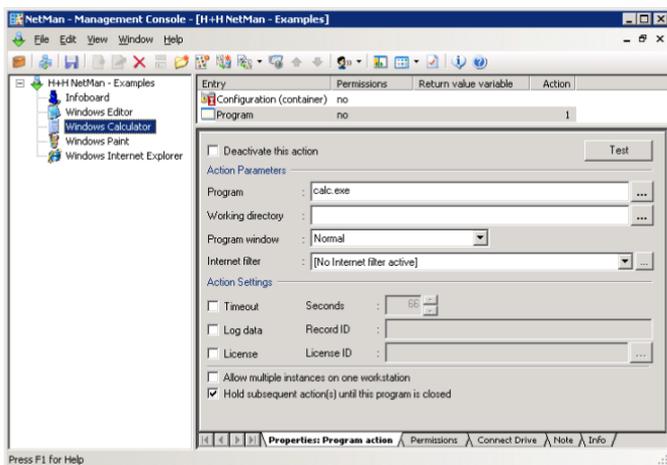
Click on the **Info** tab and read the text about the “Configuration” entry.

The **Note** page presents an editable field in which you can enter comments relevant to use of the configuration, such as a description of its functions or information on the application it starts (such as licensing codes or other special requirements).

Program Actions

With the “Windows Calculator” configuration still selected in the folder view, select the Program action in the Entry pane—the only action in this configuration—and read the information about this entry on the **Info** page. The **Info** page is part of a Help system that is integrated in the Management Console program and provides descriptions of all actions.

On the **Properties: Program** page, you can configure settings for the action. Open the **Properties** page:



The Program action has the following properties:

- **Program:** The program to be executed is entered here.
- **Working directory:** NetMan will start the program from the directory entered here.
- **Program window:** You can select the mode in which the program window is opened (normal, maximized, or minimized).
- **Allow multiple instances on one workstation:** Defines whether more than one instance of this program can run at one time on a given workstation. With this option activated, NetMan permits users to start an unlimited number of instances of this program.
- **Internet filter:** This setting lets you program individual filtering rules for Internet access. For details on how these rules work and how you can define them, see “*Internet Filter*.”
- **Hold subsequent action(s) until this program is closed:** In deciding whether to activate this option, keep in mind that a NetMan configuration is a user-defined sequence of almost any number of actions. With this option selected, the actions that follow this Program action within the configuration are not executed until after the user has closed the program started here. Without this option, these subsequent actions are executed as soon as this program has been launched.

- **Timeout:** Select this option to define a period of time after which the program will close automatically if it has not been used. The default number of seconds is defined in the NetMan Settings (see “NetMan Settings” in chapter 4) and can be overwritten here. This option is particularly useful for applications with a limited number of user licenses. The timeout option may not work with all programs, however; this depends in part on the way a given program works. You cannot assign a timeout for a DOS program, for example.
- **Log data:** With this option selected, entries are written in event logs when the program is started and when it is closed, so you have a record of the program running time. How events are logged is defined in the NetMan Settings. The “Record ID” you define here identifies this configuration in the log file entries.
- **License:** Activate this option to limit the number of workstations that can run this program simultaneously. You can create a new license ID or assign an existing ID to this Program action.



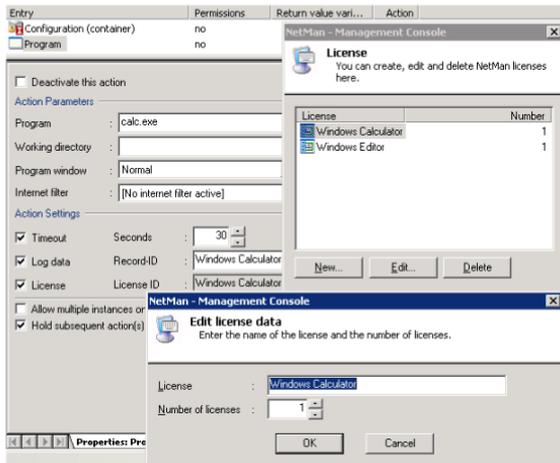
Unlike other actions, the **Program** action also has a **Connect Drive** dialog page. Here you can map a drive designation to the network resource required by the program.

Additional Program Properties

Now you know enough to take your own first steps. In the following example, we will activate three of the additional program properties available in NetMan:

- Timeout
- Event logging
- Licensing

In the dialog box below, these properties have been activated. Click on the button to the right of the “License ID” field to open a dialog box for creating, deleting and assigning licenses.



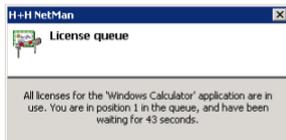
The number of licenses for a given application is not stored directly in this configuration. This means that you can assign the same license to more than one configuration. You may wish to do so, for instance, if different NetMan configurations share a single software license.

The settings configured here are effective in the NetMan Client as soon as they are saved. You can test your changes before saving the settings; the **Test** function is available in the toolbar, in the **Edit** menu and in the shortcut menu that opens when you right-click in the Entry pane. If an action is selected when you activate the Test function, only that action is tested; if you select 'Configuration' at the top of the Entry list, the entire sequence is tested.

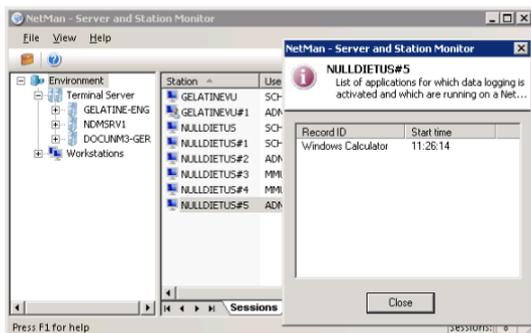


Testing a licensed application from within the Management Console does not reduce the number of licenses available for actual users.

Now we will launch the Windows Calculator configuration on three different workstations. The following message is displayed on the second workstation:

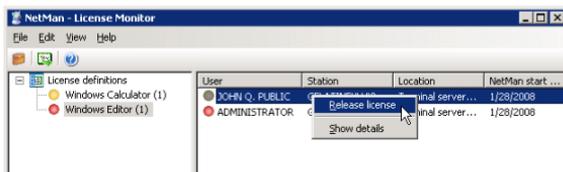


The message displayed on the third workstation indicates that the user is second in line. The next step is to call the Station Monitor from the NetMan Administration window and view the status of the three workstations. Select the workstation from which the program was launched. Under **View/Recorded applications** you can see that the “Calculator” configuration is executing on this workstation.



The example above does not show all of the available information. To specify which items are included here, select Settings from the View menu. This manual gives only a few examples of the operating features available in system programs. For more detailed information, please refer to the online Help.

You can call the License Monitor to see which licensed applications are in use, and to release licenses if desired. In this example, you can release the license for the Calculator, in which case the user who had been first in line (the second workstation) can start the program right away:



If all the licenses for a given application are in use and you release a license for another user, this does not close the application on any workstation where it is already running. Thus releasing a license may result in a breach of the software licensing agreement for the application in question.

To test the timeout function, wait until the defined delay has elapsed:



Once the timeout period has been reached on all three workstations, let us take a look at the Record Database Viewer:

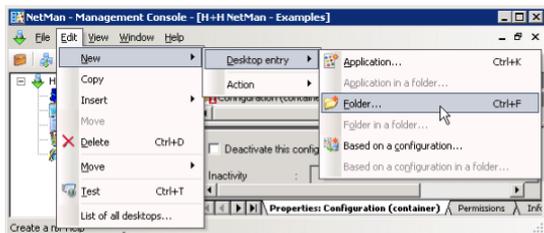
Record ID	Record name	Start time	Stop time	User ID	Station ID	Record attribute
3837	Windows Calculator	12:31:08 PM	12:31:41 PM	SCHAPPERTT	NULLDIETUS	/TS/AWL:17
3836	Windows Calculator	12:28:17 PM	12:28:48 PM	ADMINISTRATOR	GELATINEVU	/TS/AWL:11
3835	Windows Calculator	12:27:56 PM	12:28:27 PM	SCHAPPERTT	GELATINEVU	/TS/AWL:21
3834	Windows Calculator	12:27:41 PM	12:28:16 PM	SCHAPPERTT	NULLDIETUS	/TS

Three of the events listed here show values in the “Record attribute” column indicating the number of seconds spent waiting for a license (WL); this attribute can be summarized in the statistics program, by application and by time period, to get an idea of where bottlenecks occur with licensed applications.

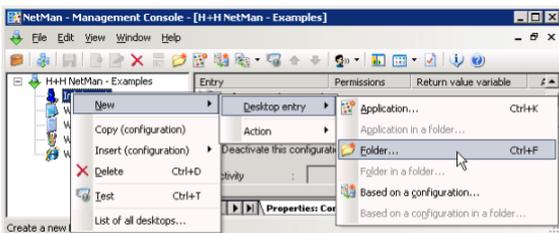
Creating and Deleting Desktop Entries

In the examples above, we added new program properties to the existing Calculator program. In the following we will explain how to create your own desktop entries.

Select **New**, either from the **Edit** menu ...



...or from the shortcut menu opened by right-clicking on in a desktop element:



The menu for creating a new entry contains the following choices:

- **Application, Folder or Based on a configuration:** Select one of these to create an entry on the same hierarchical level as the selected entry.
- **Application in a folder, Folder in a folder or Based on a configuration in a folder:** Creates an entry in the selected folder.



When you select **Based on a configuration** or **Based on a configuration in a folder**, a shortcut to an existing NetMan configuration is created on the desktop. The other items in this menu create new configurations.

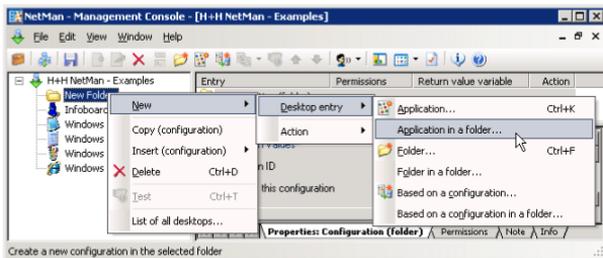
You can also create new entries using the following three toolbar icons: **New folder**, **New application** and **New item based on configuration**:



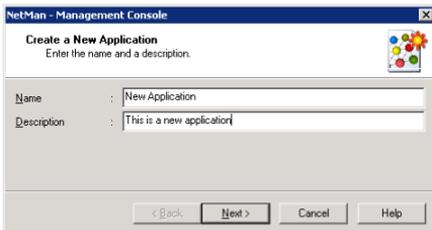
1. In the following example, the **New folder** command is used to create an entry called "New Folder":



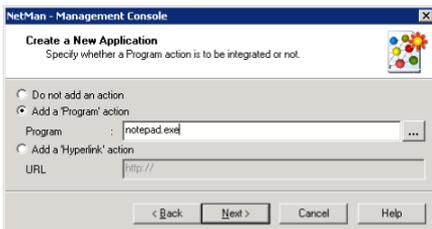
2. Next, we create an entry within this folder; this time it is an "application" entry:



3. Again, we enter a name (New Application) and a brief description:

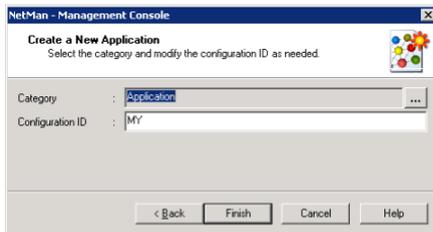


4. We can go on to define a Program action for the "New Application" configuration:



5. On the last page of this Wizard, you are asked to confirm (or edit) two entries which are automatically generated by NetMan:

- The ID of the new configuration (in this example, “New”)
- The category to which the new configuration is assigned (in this example, “Application”)



The ID of a configuration must be unique, because it is used to call the configuration; for example, from the command line, or as part of a URL.



You can modify or replace the default ID generated by NetMan, for example to make the configuration more easily identifiable. For example, if you name your configuration “MS Word,” the ID automatically generated by NetMan is “MS.” If you accept this ID and subsequently create a configuration called “MS Excel,” NetMan will generate the ID “MS1.” To modify the automatically generated ID, simply overwrite it on this dialog page.

The Category of a configuration is basically a sorting criterion. As you can see in the list of all configurations (opened as described above), “Category” is one of the column headers:

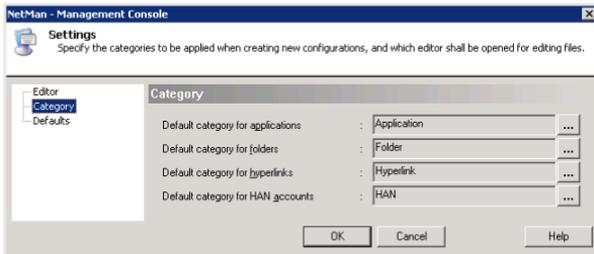
Name	Category	Configuration	Permissions	License ID	Record ID	Extension
Enter text here	Enter text here	Enter text here	Enter te...	Enter te...	Enter te...	Enter te...
Windows Internet Explorer	Application	MSIE	no			
Windows Calculator	Application	CALCULATOR	no	Calculator	Calculator	
New Application	Application	NEW1	no			
Windows Editor	Application	NOTEPAD	no			TXT
Infoboard	Application	INFOBOARD	no			
Windows Paint	Application	MSPAINT	no			
New Folder	Folder	NEW	no			
NetMan startup configuration	Startup/Shutdown	NMSTARTUP	yes			
NetMan end configuration	Startup/Shutdown	NMSHUTDOWN	no			

This table can be very long, depending on how many configurations you have. The use of categories can help you to keep track of your configurations, and to find a particular configuration more easily.

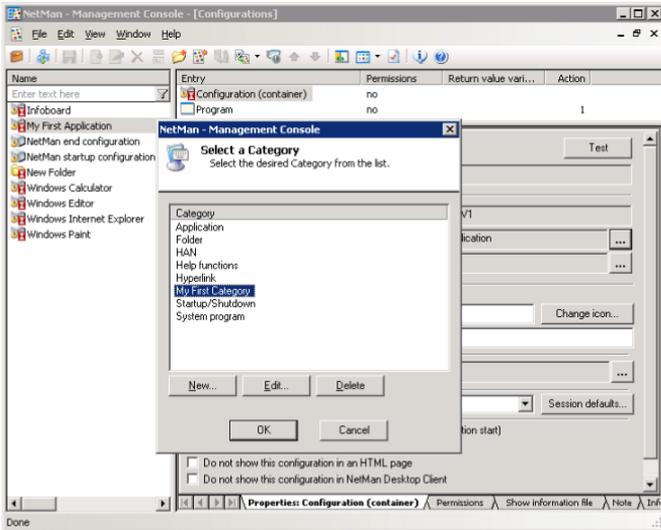


The list of all configurations also shows at a glance whether ‘execute’ conditions, licenses and run-time recording are configured. In the fields marked Enter text here you can set filters for the individual columns to reduce the number of entries shown.

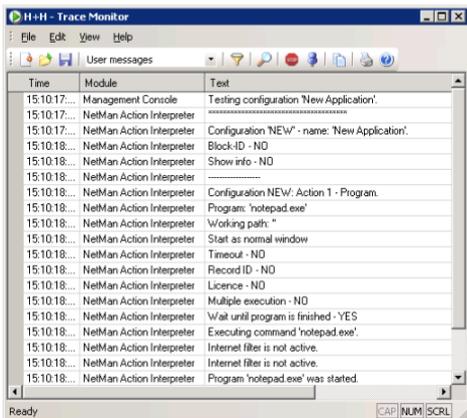
6. Let us return to our example for a “New application.” NetMan assigned the category “Application” automatically, based on a function that you can modify under **View/Settings**:



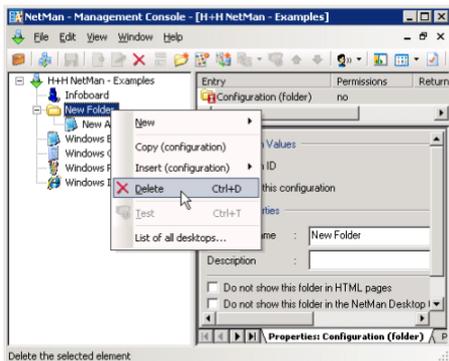
As you can see here, you can define your own categories and specify defaults. In our example, a new category called “My First Category” is assigned to the configuration called “My First Application:”



7. Now we test the new configuration with the Trace Monitor switched on. As the last entry below indicates, the `Notepad.exe` program was launched successfully:



8. Since this was just a demonstration, we can delete this folder now:



We are now asked to specify whether the entries in the desktop should be deleted along with the desktop.



This question is always asked when you delete a configuration that is not assigned to any other desktop. If the entry is still linked in another desktop, it is simply removed from the active desktop when you select the "Delete" command, without prompting for confirmation, and is still available in the list of all configurations.

In this example, we answer “Yes” since the entry was created only for demonstration purposes. Next, we delete the pre-configured sample configurations, but answer “No” at the prompt, so that these configurations are merely removed from the active desktop, but remain in the list of configurations.

9. In the preceding steps, we made several changes in the desktop structure. If we save the changes now, or did so at any point along the way, any NetMan Client interfaces that were already running would have to refresh their desktops before the changes would be reflected. If a client’s desktop is not reloaded, a user might try to activate an entry that is no longer available or no longer exists.

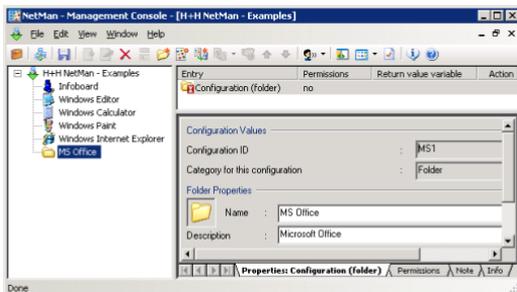
The NetMan Desktop Client registers the necessity to reload a desktop or configuration based on the date a desktop or configuration was created. If you have assigned rights to desktops and configurations, Desktop Client might not register changes made in external databases (e.g., in ADS). This is why a Reload desktops command has been integrated in the Management Console.



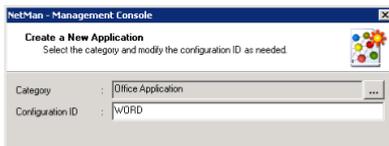
Your First Application

Now we will show you how to integrate an application of your own in NetMan. For this demonstration, we will use the Microsoft Word application, which is already installed on the terminal server we are using.

1. We begin by creating a folder called MS Office:

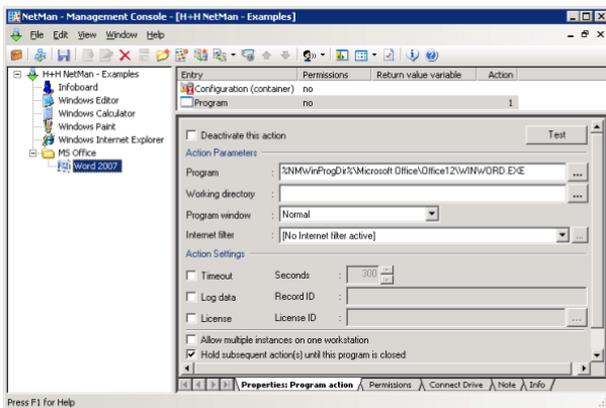


2. Then we create a new “Application” configuration as described in the chapter “Creating and Deleting Desktop Entries:”



3. NetMan automatically extracts the icon from “Winword.exe” to \NMHome\Config\Client\Data\Icons and uses it as the symbol for this configuration. You can use NetMan’s *content redirection* mechanism to link the DOC file name extension to this configuration. Remember to use the %NMSHFFile% variable to have the file passed to the program on the command line.

With the MS Word program, all you need to do is append the %NMSHFFile% variable to the program call as a command line argument:



With the default settings, NetMan automatically inserts environment variables in place of specific path designations whenever a path or part of a path is recognized. In this example, C:\Program Files is replaced by the NMWinProgDir

variable. This has the advantage that the program is found on all workstations, because it is always installed in the Windows directory on the local drive, whether the drive letter is C: or D:, and no matter what the directory is called.

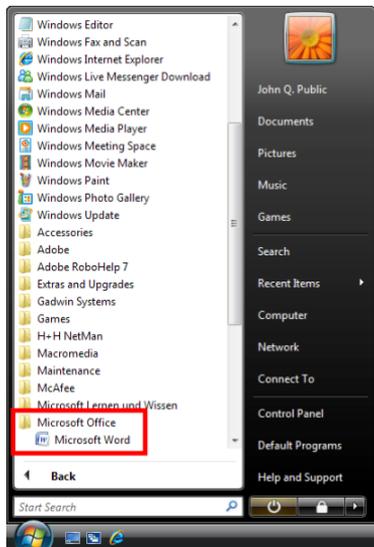


When you use the `%NMSHFFile%` variable to pass a file name to a program, it is important to know what the program requires. In the most simple case, only the file name is required. Some programs, on the other hand, require a switch to precede the file name on the command line.

4. Finally, we activate the licensing and event logging functions.

5. On the **Information file** page, you can create and assign a special HTML file for providing information to users, if desired.

6. Speichern Sie den Desktop über **Speichern**. Nach einem Neueinlesen des Desktops über **Desktops neu einlesen** präsentiert sich der NetMan Desktop Client so:



Up to now we have described each step in great detail, because these were your “first steps” and because we wanted to acquaint you with the program’s internal logic. From this point onward we will be operating on the assumption that you know how to create, edit, delete and move desktop entries, and will provide details only on other aspects of NetMan operating elements.

Access Permission for Configurations and Actions

You can permit or deny access to configurations and actions for specified users, user groups, user profiles, stations, station groups, station profiles, and/or and network groups. You can also grant or refuse access permission based on any of a number of defined conditions.

For example, you can define whether a given configuration is displayed based on membership in any of the following:

- Global NT group (Active Directory Service required)
- Local NT group
- LDAP group (LDAP server required)
- NetWare group

This mechanism provides full support for the groups used in the most common network operating systems. You can use the rights structures that are already in place in your network without having to create new definitions within the NetMan system. Since all of your user and workstation names are automatically copied into NetMan databases, you have the option of linking access rights not only to user's network login names, but also to workstation names, as well as user and station groups and profiles. With this feature, NetMan closes a gap in network operating systems that evaluate permissions solely on the basis of user accounts. Moreover, NetMan lets you control access to configurations according to specified conditions as well – another feature that takes you beyond the realm of conventional network capabilities. You can make configuration access dependent on the existence of one or more specified elements on the client machine, which can include the following:

- a file,
- a path,
- a drive,
- a registry entry,
- an INI file entry, or
- a value in an environment variable.

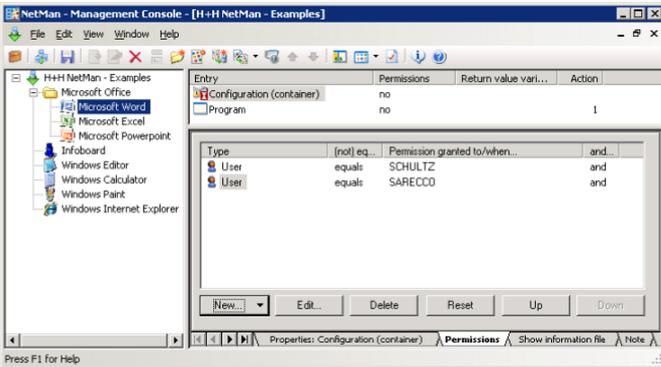
Furthermore, you can choose to show or hide configurations based on any of the following workstation factors:

- operating system,
- IP address,
- host name, or
- the protocol used for access on a terminal server (RDA vs. ICA).

The variations on the rights structure can be used in any combination and linked with logical operators (AND/OR), and can be formulated in the positive or the negative. In the simplest cases, you grant 'execute' permission to

- users,
- stations,
- local NT groups,
- global NT groups
- AD user group, an OU, or
- NetWare groups.

The following is an example of an invalid assignment of permissions: Select the configuration and click on the **Permissions** tab. Click on the **New...** button and select **NetMan User**. Add a second user to the list in the same manner as the first:



This definition, where the second user is linked by a logical **AND**, would make it impossible to launch this configuration.

The entries in the Permissions list are evaluated logically by NetMan: each entry is a proposition that is either true or false. The assignment of 'execute' rights for this configuration will depend on the truth value resulting from the evaluation of all entries in the list. The expression

User = "SCHULTZ" *and* User = "SARECCO"

is always false (due to the AND operator), while the expression

User = "SCHULTZ" *or* User = "SARECCO"

is true whenever the user name is either "Schultz" or "Sarecco" (logical OR rather than AND).



In evaluating these logical expressions, the AND operator has a higher priority than the OR operator. Example:

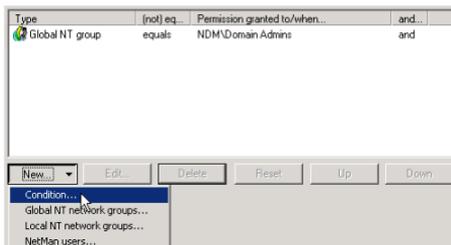
Type	(not) eq...	Permission granted to/when...	and...
Local NT group	equals	\\GELATINE-ENG\Administrators	and
Windows version check	equals	Windows TS-based	or
User	equals	ADMINISTRATOR	and
Windows version check	equals	Windows XP	and

In this case, the expression is implicitly evaluated as follows:

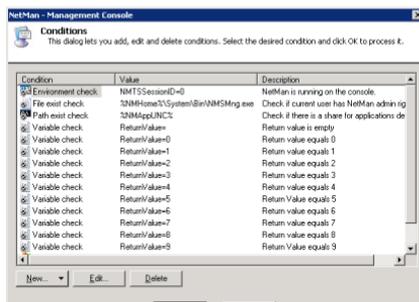
“Local NT Group” = (“GELATINE-ENG\Administrators” AND “Windows version” = “Windows Terminal Server”) OR (“User” = “Administrator” AND “Windows version” = “Windows XP”)

The next example illustrates a truly practical use of the AND operator:

Program X runs on Windows NT workstations, and you want to make it available to network administrators who may have other operating systems. To do this, link the ‘execute’ rights for the corresponding NetMan configuration to your ADS administrators and then create a new condition for these rights as follows:



Click **New...** and select **Condition**; this opens a list of conditions that you can choose from:

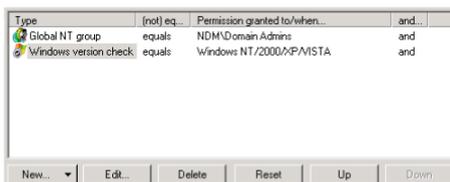


The conditions listed here are used by a number of NetMan’s internal programs and thus should not be deleted.

Since the condition you require does not appear in this list, you need to create it. To do this, click on **New...** and select **Operating system check**. In the next dialog box, select Windows **NT/2000/XP/VISTA**:



And that's it:



The other conditions you can choose from are described in the following:

Environment Check: Checks for the existence of a given NetMan variable or system variable.

Variable Check: Determines whether a given action return value matches the value specified here.

INI Entry Check: Determines whether a given variable in a Windows INI file is set to the value specified. INI files are for the most part used by 16-bit Windows programs, while 32-bit Windows uses registry entries (see below).

Registry Check: Determines whether a given key in the registry is set to the value specified.

Host Name or IP Address Check: Determines whether the workstation host name or IP address matches a specified host name (wildcards permitted), IP address or range of addresses.

File Exist Check: Checks whether a specified file exists and returns *true* if the file is found. This condition is used by NetMan Desktop Manager to determine whether the Toolbox is displayed on the system desktop. Normal users do not have 'read' rights in the NetMan Management Console directory, which means the file that would provide access to the Toolbox cannot be detected.

Path Exist Check: Checks whether a specified path exists and returns *true* if the path is found.

Drive Exist Check: Checks whether a specified drive exists and returns *true* if the drive is found.



Please note that some of these conditions cannot be checked when configurations are accessed using the web interface. These include the following:

- Environment check
- Variable check
- INI entry check
- Registry check
- Windows version check
- File exist check
- Path exist check
- Drive exist check

All of these conditions are dependent on properties of the local workstation that are not accessible using the web interface. This is why none of these are shown in the web interface. When Boolean expressions are evaluated for these conditions, the return value is *true*.



NetWare Directory Services (NDS) can be accessed only if the IntraNetWare Client interface from Novell is installed on all workstations in your network.

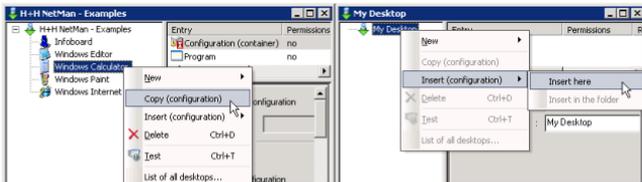
Creating Additional Desktops

To create new NetMan desktops, select **File/Create desktop**:



The new desktop is empty. You can add your choice of the following elements:

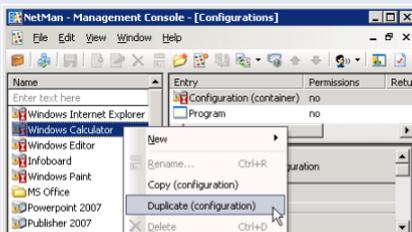
- New configurations (folders, applications, and hyperlinks). This involves creating new NetMan configurations.
- Existing configurations. This involves creating NetMan desktop entries that refer to the existing configurations.
- Desktop entries from other desktops. This involves opening a shortcut menu or the Configurations window to copy entries. Select the configuration you would like to copy, right-click on it to open the shortcut menu, and select **Copy (configuration)**. Move the focus back to the new desktop, right-click in the desired position, and select **Insert (configuration)/Insert here**.



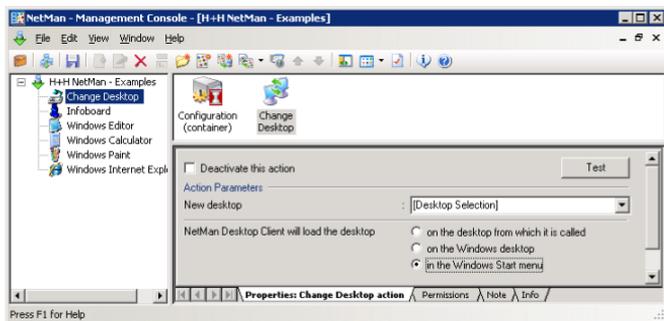
When you use the **Insert (configuration)** command, this creates a shortcut to the existing configuration, rather than a copy. When you change configuration properties, the changes are reflected in all shortcuts to this configuration in all desktops.



If you want to assign different sets of permissions in different desktops for a certain application, begin by duplicating the application's NetMan configuration, and then set the desired permissions in the new copy. In other words, the configuration is first duplicated in the Configurations window, then copied using the **Copy (configuration)** command, and finally added to a desktop with the **Insert (configuration)** command.



You can insert a *Change Desktop* action to load a desktop other than the default NetMan Client desktop. If you do not specify a desktop for the change, this opens a list of all existing desktops for selection by the user. You can also specify whether the desktop is opened in the Start menu, on the Windows desktop or in place of the currently active NetMan desktop, regardless of whether the latter is in the Start menu or on the Windows desktop:

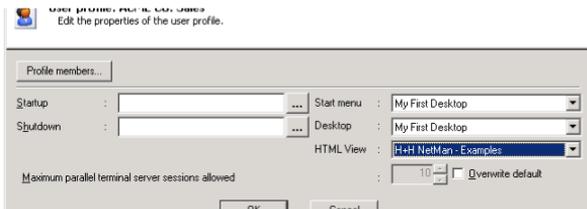


We strongly recommend creating a reference to the Change Desktop action (by copying the desired desktop entry without duplicating the action) for testing purposes, so you can change back to your original desktop at any time. This prevents you from “getting stuck” in the new desktop during testing. To prevent your users from changing to a particular desktop, assign ‘execute’ permissions within the Change Desktop action accordingly.



Make sure the **Execute configuration in a session** option is deactivated in the configuration settings. The Change Desktop action can be used only in the context of the NetMan Desktop Client.

You can assign a given desktop as the “start” desktop for a user, user profile or station profile:



It is not possible to assign a desktop as a property of a station. To allocate a given desktop to individual stations, you can add a Change Desktop action to the startup configuration (see next section) and grant ‘execute rights’ only to the station(s) to which you wish to allocate this desktop.

If you do not wish to maintain station profiles, user profiles or users in your NetMan system, you can use a Change Desktop action and grant permission to your network users based on their membership in a group.

Before a desktop is opened for a given client, all of the applicable settings are checked in the following order:

- User profile settings
- User settings
- Station profile settings
- A Change Desktop action in a configuration (such as a startup configuration)

The setting active at the conclusion of this evaluation is applied.



The above does not apply to the web interface. Unlike the NetMan Desktop Client, the web interface does not process startup configurations; thus these cannot overwrite other settings. In the web interface, the desktop opened is determined by the following, in this order:

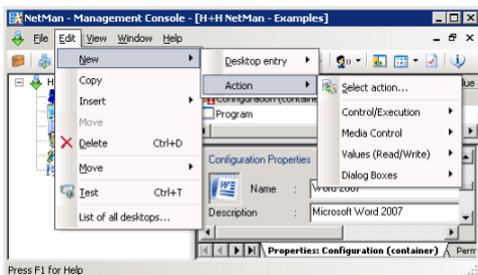
- Settings defined in the NetMan Web Services (for a detailed description, please see the chapter entitled "Web Interface (HTML View)")
- User profile settings
- User settings
- Station profile settings

NetMan Actions

Throughout this manual we have repeatedly mentioned the broad range of possibilities afforded by the variety and number of actions you can add to your NetMan configurations. In this section, we present details on the different types of actions, and point out the convenience afforded by adding other actions to your NetMan configurations, rather than simply using Program actions on their own.

NetMan actions are divided into the following categories (as seen in the submenu opened under **File/New/Action**):

- Control/Execution
- Media Control
- Values (Read/Write)
- Dialogs



Each action type is described in detail on the corresponding **Info** page shown in the Management Console. For a complete list of all available actions, with their Info page descriptions, please refer to the *NetMan Almanac*.

We have already presented a demonstration of the most important actions, the *Program* and the *Hyperlink* action. We would like to point out once more that a NetMan configuration is a user-definable sequence of actions. Any type of action, including Program actions, can occur repeatedly in a given NetMan configuration, and these actions can be used in any combination.



It is not necessary to know all about every type of action. If all you need are Program actions, you do not have to bother with the entire spectrum of other actions. In the following, we present just a few practical examples involving some of the other actions, to give you some idea of the best uses for NetMan in your own network environment.

Actions can generate *Return values* (process variables). The values stored in return variables, which can be the result of user input, are available for processing by any or all of the subsequent actions in a given configuration. This is implemented by defining a Variable Check condition within an individual action, to determine the results of preceding actions.

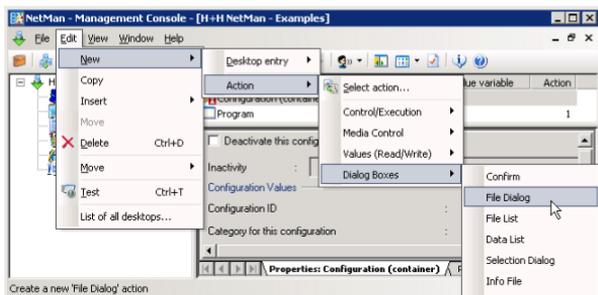


You can also use the interface to Windows Script to integrate your own scripts in NetMan actions.

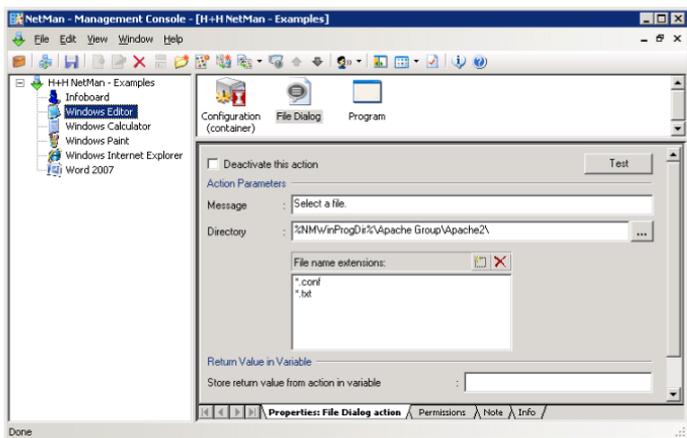
Using the Trace Monitor to Check Action Processing

When you launch a NetMan Container configuration, processing of a sequence of actions is initiated. If anything goes wrong, you need a tool that helps you localize and diagnose the problem.

As an example, we shall add a *File Dialog* action to the Windows Editor (ID: NOTE-PAD), so that the configuration not only launches the Windows Editor but also opens the “Open File” dialog.

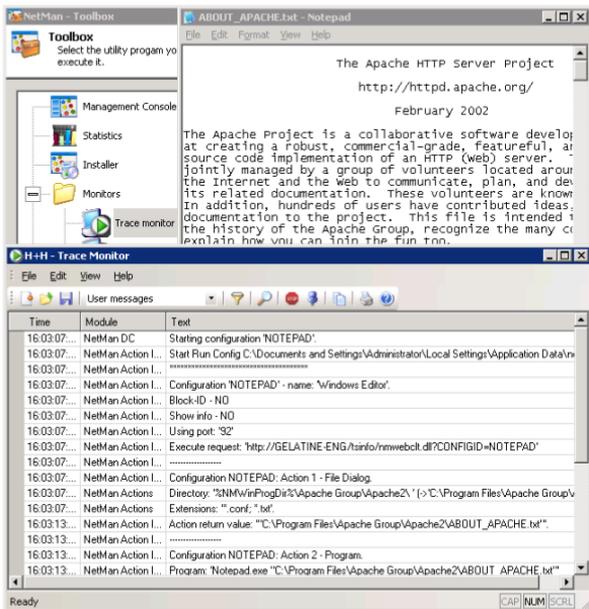


The File Dialog action lets the user choose any file that matches the pattern defined in this action (see illustration). The user can also browse in other directories; the action defines only the starting directory:



Now we will test this modified configuration and watch the processing steps that run in the background, using the *Trace Monitor*. Launch the Trace Monitor first, by activating this element in the Monitors folder of the Toolbox, and then launch the Windows Editor configuration.

The Trace Monitor should show the following output:



Note the text messages in the following:

```

001 NetMan Action Interpreter: Configuration 'NOTEPAD' -
    name: 'Windows Editor'.
002 NetMan Action Interpreter: -----
003 NetMan Action Interpreter: Configuration NOTEPAD: Action
    1 - File Dialog.
004 NetMan Actions: Directory: '%NMWinProgDir%\Apache
    Group\Apache2\'
005 NetMan Actions: Extensions: '*.txt; *.conf'
006 NetMan Action Interpreter: Action return value: '\"C:\
    Apache2\ABOUT_APACHE.txt\"'.
007 NetMan Action Interpreter: -----
008 NetMan Action Interpreter: Configuration NOTEPAD: Action
    2 - Program
009 NetMan Action Interpreter: Program: 'Notepad.exe C:\
    Program Files\Apache Group\Apache2\ABOUT_APACHE.txt'''

```

This output makes it easy to recognize the individual processing steps that are otherwise in the background.

The Trace Monitor is a utility for localizing problems that may occur when you run NetMan configurations or programs.

Select the **Settings** item from the **View** menu to see the options available for the Trace Monitor. These include the following:

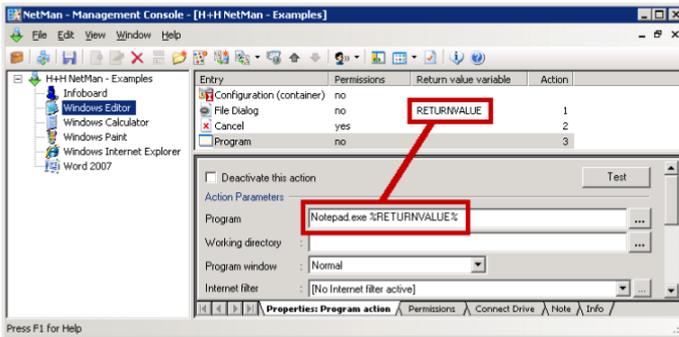
- Filtering output according to program components
- Assigning font colors according to components so you can identify certain steps at a glance
- Defining the level of output; for example, to obtain even more detailed output about certain internal sequences
- Saving output; for example, to append it to a support question

Controlling an Action Sequence

In the example given in the chapter “Using the Trace Monitor to Check Action Processing,” the result of the File Selection action (= name of the selected file) was passed to the subsequent Program action. Alternatively, this result can be written in a *return value variable*. The difference between these two techniques is as follows:

- **Without a return value variable:** The result of the action is passed as an argument to the next Program action. If no return value variable is configured, processing of the configuration stops altogether if the user cancels the action or the action fails.
- **With a return value variable:** The result of the action is stored in a variable. This variable is available for use only within the NetMan configuration that contains the action. Return value variable can be used in later action sequences. If the action is cancelled or fails, the configuration is not necessarily cancelled, as the administrator configuring the action can define the response to such events.

Return value variables are both flexible and controllable, to the extent that they can be used at any subsequent point in the action processing sequence and because you can also control the order of return values that are passed to Program actions. Returning to our Windows Calculator example, we can configure the Program action as follows, with execution of a *Cancel* action dependent on the condition that no value is stored in the RETURNVALUE variable:

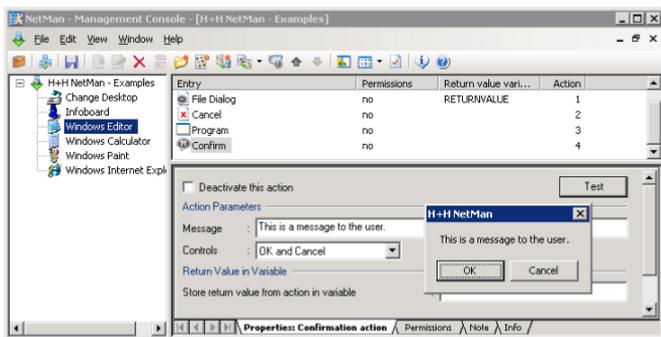


We recommend having return values automatically passed to subsequent Program actions only in simple configurations. In other cases, the use of return value variables is preferable.



You can store a return value in the NetMan environment, for use beyond the scope of the configuration in which it originated, by adding and configuring an *Environment* action.

In the following we take a closer look at some other techniques for controlling action sequences. You can insert a *Confirmation* action to provide information to the user before a program starts:



If your users are not aware that NetMan is installed, you might want to change the text for these title bars to avoid confusion. Enter your text on the **Configurations** page of the NetMan Settings:



Changes you make in the NetMan Settings are not applied until after you restart the Desktop Client!

The title bar text now reads "My Dialog Box Title":



If the user clicks **Cancel**, configuration processing is cancelled because no return value variable is defined.

If **OK** is chosen, configuration processing continues.

With the return variable functions, you can have the result of user input written in a return variable and use it to control subsequent processing; for example, with a *Cancel* action:

Entry	Permissions	Return value vari...	Action
Configuration (container)	no		
Confirm	no	RETURNVALUE	1
Cancel	yes		2
Program	no		3

Return variable:

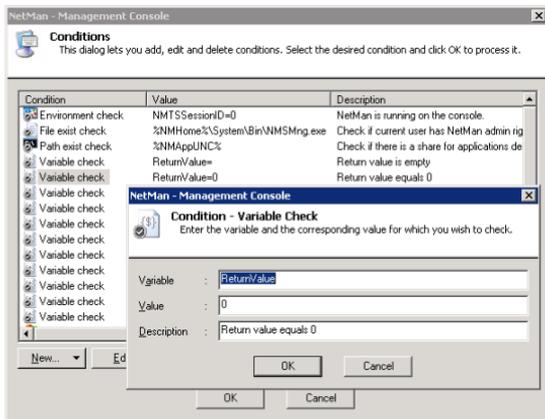
If you define a return value variable, the function of this action changes somewhat: the action returns one of two Boolean values and the sequence of actions in the NetMan configuration continues processing, even if the user selected "No" or "Cancel".

Return value = 1: User selected **OK** or **Yes**
 Return value = 0: User selected **Cancel** or **No**

The value returned in the variable can be evaluated by subsequent actions. A **Cancel** or **No** from the user does not stop the NetMan configuration from processing.

Properties: Confirmation action | Permissions | Note | Info

Read the **Info** page for details on the available return values. For added control in our current example, we use a predefined Variable Check condition that requires the value "0":



Execution of the Cancel action is made dependent on the Variable Check condition:

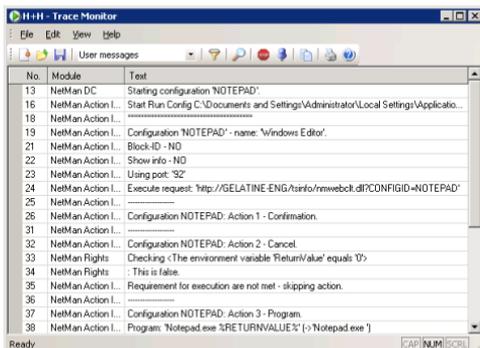
Entry	Permissions	Return value variable	Action
Configuration (container)	no		
Confirm	no		1
Cancel	yes		2
Program	no		3

Type	(not) eq...	Permission granted to/when...	and...
Variable check	equals	ReturnValue=0	and

New... Edit... Delete... Reset... Up... Down...

Properties: Cancel action | Permissions | Note | Info

When the user selects **OK**, the following output is seen in the Trace Monitor:

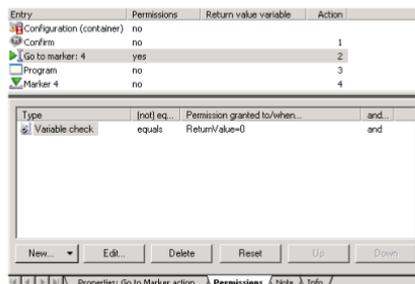


The 'execute' permission is evaluated logically: Because the return value is not "0", permission to execute the Cancel action is denied – i.e., the configuration is not cancelled – and the next action is processed.



The following example should help to illustrate the logic behind this process: Say you have inserted a *Password* action at the beginning of a configuration, to ensure that only authorized users can launch the configuration in question, however, you configure a condition that denies 'execute' permission to the Password action for users operating under an administrator account. When administrators launch this configuration, they are not prompted for a password, and the following output is shown in the Trace Monitor: NetMan Rights: Checking <User is member of NetMan group 'Administrators'>: This is false "Action cannot be executed (insufficient rights)" and the Password action is skipped.

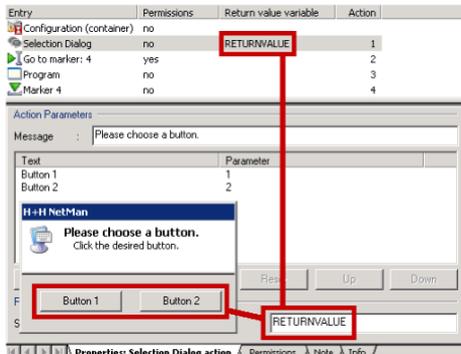
Returning to the example of the Cancel action: the same purpose can be achieved by inserting a *Go to Marker* action. Here, too, the execution of the action is dependent on the return value resulting from user input. If the user clicks the **Cancel** button in the window opened by the Confirmation action, processing skips to the end of the configuration and the Program action is skipped entirely:



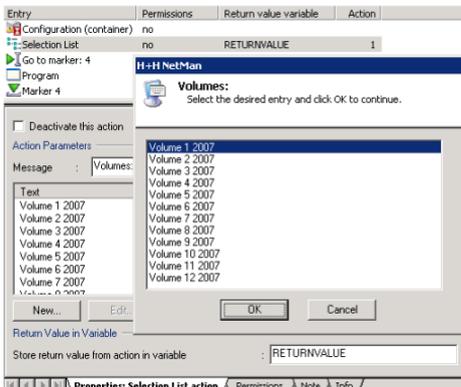
The *Go to Marker* action is very useful for skipping entire series of actions, where you would otherwise have to define 'execute' conditions for each action individually. You can also use it to jump back to an action located at an earlier position in the sequence. This lets you create logical loops; for example, "execute Action Y (repeatedly) until Condition Z no longer exists."

Simple Examples of the Most Frequently Used Actions

The *Selection Dialog* action is similar to the Confirmation action in that it lets you offer the user a choice of responses, in the form of buttons in a dialog. Each possible response writes a specified value to the return variable resulting from this action. This value can in turn be evaluated based on subsequent conditions or used in following actions:

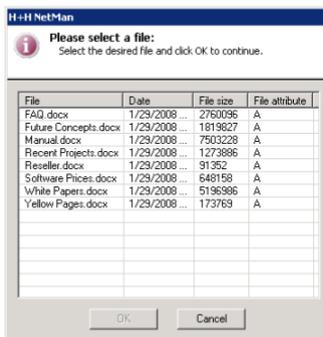


If you want to present the user with a large number of options, rather than just two, you might insert a *Selection List* action instead of the Selection Dialog; the function is similar, but the choices are presented in a list rather than on buttons. Because you can assign a text to each parameter for the end user to read, users can be presented with meaningful choices rather than the cryptic texts often found in such cases:



Selection and File Dialogs are generally useful for generating values to be passed to programs in the form of command line arguments. The *File Dialog* action, already shown in an earlier example, opens the standard Windows dialog for selecting a file. If you use a *File List* action instead, the user cannot browse in other drives, networks or directories. This action opens a list of files that were explicitly chosen by you, as

NetMan administrator, to offer for selection by the user. You can define whether this selection window shows the file size, date and/or attributes, and specify the maximum number of files that a user can select:



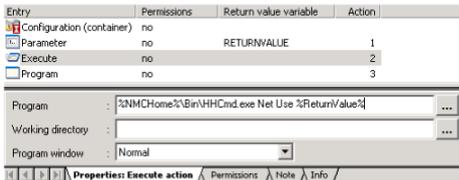
The *Parameter* action opens a dialog for user input which is then passed to the program as command line arguments:

- If you use square brackets in the “Parameter” definition, the user will see only what is inside the square brackets and nothing else that is in the “Parameter” field. The square brackets might contain spaces, or a default parameter that the user can overwrite. Text outside the square brackets is passed to the program on the command line without modification.
- You can define whether user input is hidden, in which case asterisks are displayed in place of the characters entered.

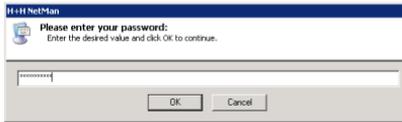
The following example illustrates one possible use of the *Parameter* action: Say you have a resource for which login is required, entailing input of a user name and a password. A *Password* action is not particularly well-suited for use here, as it serves in an action sequence to determine whether the configuration is processed or not (for example, when it involves opening a certain folder in the NetMan Client). Assuming the following syntax for the required command line input:

```
/user:<username> /password:<password>
```

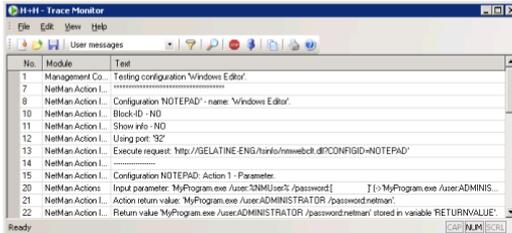
you can configure your Parameter action as follows:



The user name is known to the system, and passed on using the “NMUser” variable. The function of a password prompt is taken over by the Parameter action; all that the user can see—and edit—in this case are the 10 spaces, represented by asterisks:



As always, it is helpful to look at the output in the *Trace Monitor* if any problems occur during testing. In our example, the following is shown:



The syntax of the NET USE command is similar to that used in the example above:

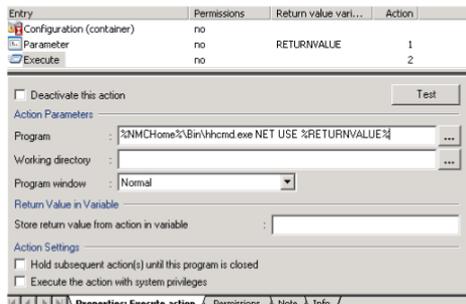
```
NET USE [device name | *] [\\computer name\share name [data medium] [password] [/USER:[domain name]user name]
```

Thus you could conceivably use this command for logging on to a network resource; for example, by writing this command in an Execute action. The Execute action has fewer options than the Program action, and unlike the Program action, can be included in NetMan startup and shutdown configurations.



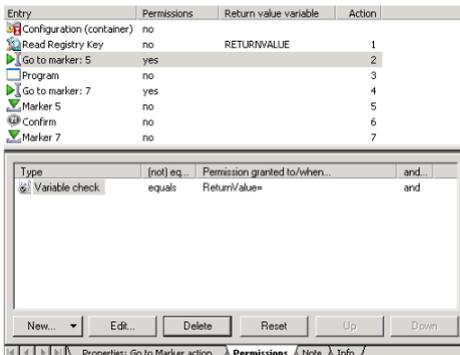
These types of actions can be useful for integrating NetMan helper programs. For descriptions of these programs and lists of the valid arguments please see *Helper Programs for the Execute action*. The `NMNCon32.exe` and `HHCcmd.exe` programs could be used, for example, in the actions described above.

In the following configuration, the NET USE command is executed by the NetMan `HHCcmd.exe` helper program, which is launched by an Execute action:



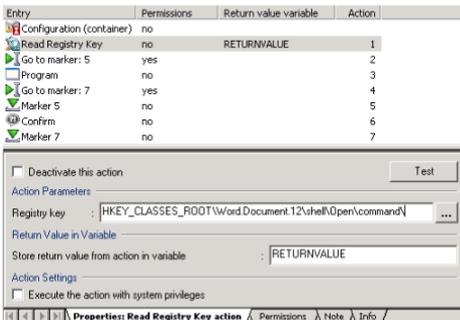
Complex Actions

For the next example, we return to our MS Word configuration (see chapter “*Your First Application*”). Let us assume you want to find out where the Microsoft Office directory is located on a given workstation, and then start Word from that directory. You can configure this sequence as follows:



The Office path is stored in the ReturnValue variable.

If no value is stored here, the configuration skips to a Confirmation action which announces that the Word program was not found. The Office path can be determined as follows, for example:

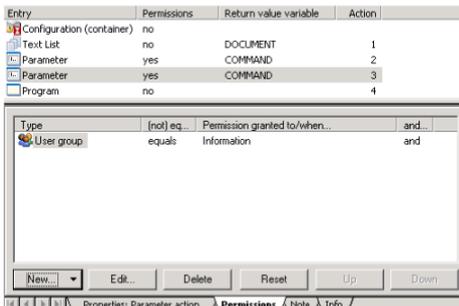


If the path is detected, it is stored in the variable which is used to call the program: %ReturnValue%.

If the Word program is found, the configuration skips to a marker placed at the end of the configuration (subsequent to the Confirmation action).

The following diagram illustrates this sequence.

The Parameter action inserted here does not prompt user input, as the **Parameter** field in this action does not contain square brackets. The “Editor” variable is set in the background to `WordView.exe` for non-members of Information Services:



The following command is executed in the Program action:

```
%Command% %Document%
```

A similar solution can be used for the following tasks:

- Open different browsers for different user groups
- Open the enterprise Web site in a browser or in an HTML editor (e.g., Front Page)
- Open different programs for a given task, depending on client operating system

Windows Script Enhancements

The *Windows Script* action lets you run scripts written in JScript, VBScript and Windows Script Host (WSH). VBScript and JScript can be combined within WSH scripts. The option of writing your own scripts represents an expansion of the range of NetMan functions, and combines the powerful functions of NetMan actions with those of Windows Script. NetMan is particularly well suited for this, because all system parameters are stored in variables; a script once written is universally valid throughout your NetMan system.



The information in this chapter describes NetMan interfaces for Windows Script and is relevant only to users who are familiar with JScript, VBScript and/or XML.

1. Passing Arguments to Scripts (NMPParamExample.vbs)

Parameters can be passed to scripts in command line arguments. An argument is passed in the `NMPParamExample.vbs` script. There are a number of sample scripts available in the Internet, and in textbook appendices. When you use NetMan, passing arguments represents an important interface:

```

001  \ *****
002  \ *
003  \ * NetMan Desktop Manager Windows Script Host Inter-
004  \ * face
005  \ * (c) 2006 H+H Software GmbH
006  \ * VBScript NMPParamExample.vbs
007  \ *
008  \ * About: Sample script, to demonstrate how to pass
009  \ * parameters
010  \ *
011  \ *
012  \ * from NetMan actions to a Windows script
013  \ *
014  \ *****
015  \ force explicit variable declaration ..
016  Option Explicit
017  \ declare variables ..
018  Dim oShell
019  Dim strParams, strMsgTitle
020  Dim nCounter
021  \ create objects ..

```

```

021 Set oShell      = Wscript.CreateObject("WScript.Shell")
022 strMsgTitle = "H+H NetMan 3 Windows Script Example"
023
024 ` check number of arguments and display them ..
025 If WScript.Arguments.Count Then
026     strParams = ""
027     For nCounter = 0 To WScript.Arguments.Count - 1
028         strParams = strParams + Chr(10) + WScript.
Arguments(nCounter)
029     Next
030 MsgBox "Arguments passed to this script are:" +
Chr(10)_
031     + strParams, vbOKOnly, strMsgTitle
032 Else
033     MsgBox "No argument was passed to this script.", vbO-
KOnly, strMsgTitle
034 End If
035
036 Set oShell = Nothing

```

Because this is an important capability, we also include an example of a JScript (up to three arguments are accepted):

```

001 var objArguments = WScript.Arguments;
002 if (objArguments.length == 0)
003 {
004     for (var i=0; i < objArguments.length; i++)
005     {
006         switch(i)
007         {
008             case 0: cParam1 = objArguments(i) ;break
009             case 1: cParam2 = objArguments(i) ;break
010             case 2: cParam3 = objArguments(i) ;break
011             ....
012         }
013     }
014 }

```

2. Trace Monitor Output (NMTraceExample.vbs)

To send messages over the Trace Monitor, the Trace Monitor must be used as a component. The Trace Monitor provides a Component Object Model (COM) interface. A COM object can be created using HHTrace.HHComTrace:

```
Set oHHTrace = CreateObject("HHTrace.HHComTrace")
```

Available Methods:

```
Trace(strMessage)
```

Properties:

```
Module = strModule
```

```
Level = nLevel
```

The message in the Trace Monitor should be concluded with a line break (`CHR(10)`). You can have the name of the module from which the message originates shown with the Trace Monitor output.

There are three options available for this output:

1 = error messages only

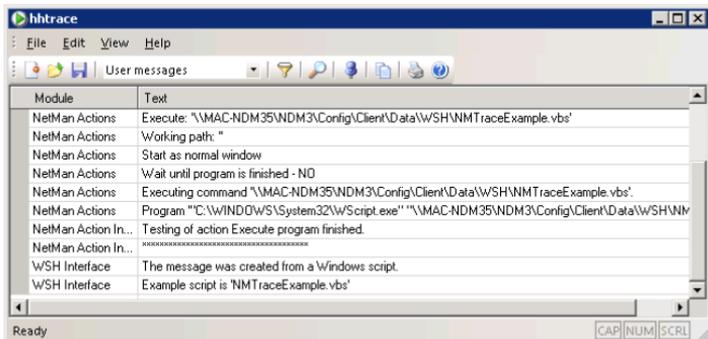
2 = user messages (recommended)

6 = all messages

Example

```
001 Set oHHTrace = CreateObject("HHTrace.HHComTrace")
002 oHHTrace.Level = 2
003 oHHTrace.Module = "WSH Interface"
004 ` write two trace message to monitor
005 oHHTrace.Trace "The message was created by a Windows
    script." + Chr(10)
006 oHHTrace.Trace "Example script is 'NMTraceExample.vbs'"
    + Chr(10)
```

The designated module, “WSH Interface,” creates the following output:



3. Read or Write in NetMan Environment (NMEnvExample.vbs)

The environment DLL has to be used as a component. This component provides a Component Object Model (COM) interface. A COM object can be created using `NMEnv.HHComEnv`:

```
Set oNMEnv = CreateObject("NMEnv.HHComEnv")
```

Available Methods:

```
HHEnvGet(strNetManEnvironmentVar)
```

```
HHEnvSet(strNetManEnvironmentVar, strValue)
```

In our example, the `NMUser` and `NMHome` variables are read using `HHEnvGet` and a test variable written in the NetMan environment with `HHEnvSet`:

```
001 ' force explicit variable declaration ..
002 Option Explicit
003
004 'delare variables ..
005 Dim oNMEnv
006 Dim strMsg, strMsgTitle
007 Dim bRC
008 Dim strNMHome ' NMHome contains NetMan server path
009 Dim strNMUser ' NMUser contains NetMan user name
010
```

```

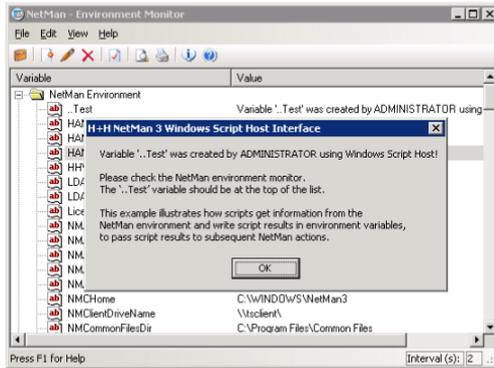
011 `create environment object ..
012 Set oNMEEnv = CreateObject("NMEEnv.HHComEnv")
013
014 ` get value of variables NMHome and NMUser ...
015 strNMHome = oNMEEnv.HHEnvGet("NMHome")
016 strNMUser = oNMEEnv.HHEnvGet("NMUser")
017 strMsgTitle = "H+H NetMan 3 Windows Script Host Inter-
    face"
018
019 If strNMHome <> "" Then
020 ` create message ...
021 strMsg = "Your NetMan user name is: " + strNMUser +
    Chr(10)_
022 + "NetMan home directory is: " + strNMHome + Chr(10)
    + Chr(10)_
023 + "These variables were read from NetMan environ-
    ment." + Chr(10)_
024 + "Now a new variable ('..test') will be written to
    NetMan environment."
025 MsgBox strMsg , vbOKOnly, strMsgTitle
026
027 ` write new variable to NetMan environment ...
028 strMsg = "Variable '..Test' was created by " & strN-
    MUser & " from Windows Script Host!"
029 bRC = oNMEEnv.HHEnvSet("..Test", strMsg)
030
031 If bRC Then
032 MsgBox strMsg + Chr(10) _
033 + Chr(10) _
034 + "Look to NetMan environment monitor!" + Chr(10) _
035 + "The variable should be the first in the list." +
    Chr(10) + Chr(10)_
036 + "This may demonstrate how scripts get information
    from NetMan" + Chr(10)_
037 + "environment and write script results to NetMan en-
    vironment to" + Chr(10)_
038 + "inform further NetMan actions about scripting re-
    sults.", vbOKOnly, strMsgTitle

```

```

039 else
040     MsgBox "Error: Unable to write test variable to the
NetMan environment!", vbOKOnly, strMsgTitle
041 End If
042 else
043     ` strNMHome is empty ..
044     MsgBox "NetMan Desktop Client is either not installed
or not running.", vbOKOnly, strMsgTitle
045 End If

```



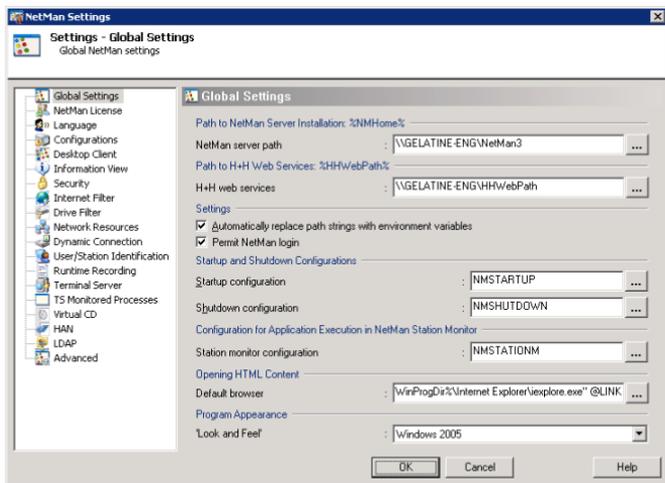
Special Configurations and Applications

This chapter presents practical examples illustrating three special features provided in NetMan:

- NetMan startup and shutdown configurations
- Integrating CD-ROM-based applications
- Integrating HAN accounts

Startup and Shutdown Configurations

Startup and shutdown configurations are not essential, but can be very useful. You can designate any configuration as a startup or a shutdown configuration. These configurations are used by NetMan to assign operating conditions to (i.e., configure the environment for) particular users, stations, groups, or profiles. When you first install NetMan, the configurations with the IDs *NMStartup* and *NMShutdown* are your global startup and shutdown configurations:



The *NMStartup* configuration maps the application drive. If you do not use a central application drive (see “*Application Drive*”), deactivate or delete this action.



If the *NMAppDrive* and *NMAppUNC* variables are not defined in the NetMan Settings, ‘execute’ permission for the *Connect Drive* action is not granted anyway.

Name	Entry	Permissions	Return value variable	Action
Enter text here	Configuration (container)	no		
Windows Internet Explorer	Go to marker: 4	no		1
Windows Calculator	Execute	no		2
Windows Editor	Confirm	no		3
Infoboard	Marker 4	no		4
Windows Paint	Connect Drive	yes	RETURNVALUE	5

Deactivate this action Test

Action Parameters

Drive	Connection	Network	User	Passw...
%NMAppDrive%	%NMAppUNC%		Windows	

New... Edit... Delete Reset

Return Value in Variable

Store return value from action in variable : RETURNVALUE

Properties: Connect Drive action | Permissions | Note | Info

The shutdown configuration can be used to disconnect the drive (undo drive mapping). The default startup configuration contains an *Execute* action (followed by a *Confirm* action) bracketed by *Go To Marker* and *Marker* actions. The Execute action launches the *NetMan Trace Monitor*. With the default settings, however, the Go To Marker action is always executed, which means the Execute action is skipped. Either of the following modifications might be useful, just depending on your requirements:

- Deactivate or delete the Go To Marker action, so that the Execute action always runs (i.e., so the Trace Monitor is launched every time).
- Set permissions for the Go To Marker action so that the Trace Monitor runs under certain circumstances. For example, if you set permission to run the Go To Marker action for "User <does not equal> Administrator" then the Trace Monitor starts only when NetMan is launched by a user with an administrator account.

You can edit the default startup and shutdown configurations to meet your own requirements. In general, startup configurations are used to set up a specific working environment for NetMan when it is started, and shutdown configurations to restore the previous state when the NetMan system is shut down. Many system administrators will want to create an environment that has a number of user-specific settings; you can do this by assigning startup and shutdown configurations to individual user profiles, users, station profiles and stations. The order of precedence for Startup configurations is as follows:



As indicated in the list above, global settings (such as an environment variable configured on the Global Settings page) can be overwritten by values set, for example, in a startup configuration assigned to station profile. You do not have to create a number of separate startup configurations in order to have several actions executed at startup. Since you can assign 'execute' rights to individual actions within a configuration, the effects of any given configuration can be made to vary in accordance with your assignment of permissions.



It is a good idea to configure the return value options in all startup configurations, even if you do not plan to make use of these values. Otherwise, failure of a given action might prevent subsequent actions from executing. In the example above, the return value stored in the variable called RETURNVALUE ensures that any subsequent actions are executed regardless of whether or not the drive mapping was successful.

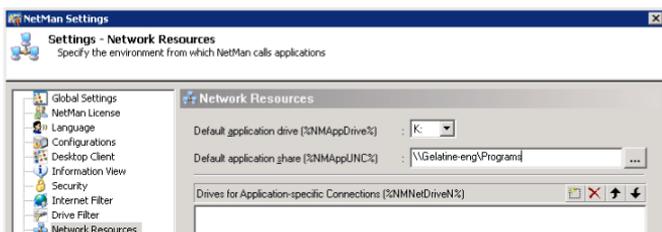
CD-ROM-based Applications

A CD-ROM-based application (referred to in the following as “CD application”) is an application that refers to data on a CD during run time. Installing CD applications in a network can sometimes be a complex operation:

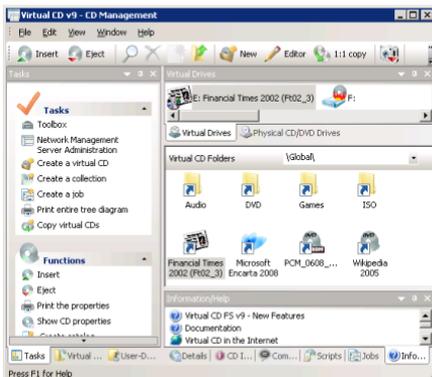
- CD applications often run only from the same drive in which they were installed.
- The drive entered during setup is often stored in the registry, in INI files or in non-editable files, which means it can be changed only by re-installing the program.
- The more CDs belong to a given application, the more difficulties are created by the problems mentioned above.
- In a network that has a lot of CD applications, there may be competition among them for a limited number of drive letters.
- CD applications often look for their CD data in a physical CD drive.

In the following, we demonstrate the installation of a CD application in NetMan:

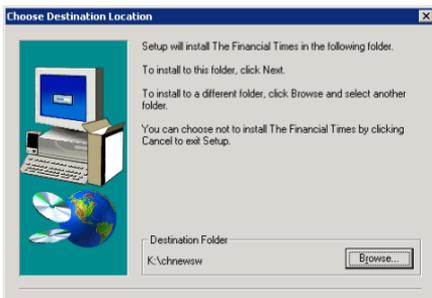
1. The application will be installed on K:, the central application drive. Our application drive has already been defined in the NetMan Settings; with these settings, clients access the applications that are installed on the network at K: (**NMAppDrive**):



2. The *Virtual CD* program is used to map the CD data. The (virtual) application CD is inserted in the (virtual) F: drive using the Virtual CD Management program:



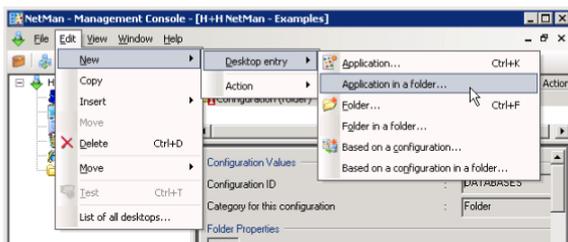
3. Now we begin the installation:



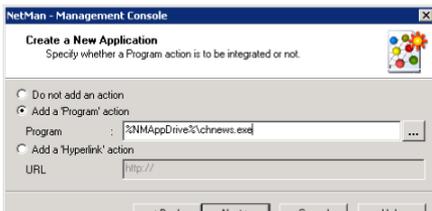
The Setup program offers us the option of specifying the CD drive or searching for the disk. We elect to search for the installation disk, and it is found in the F: drive. The program is then installed on the K: drive and a new entry is added to the Start menu:



4. The next step is to distribute this application over the network. We begin by creating an application in the "Databases" folder:

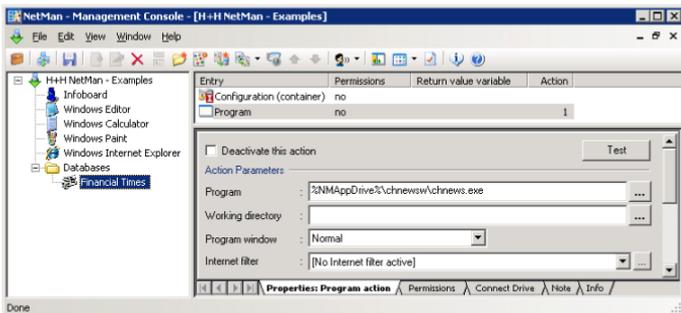


5. Next, we copy the program call – for example, directly from the link created in the Start menu – into the Program action. NetMan automatically converts "K:" to "%NMAp-pDrive%" in the command line:



Copying the program call ensures that the command line and any arguments required are entered correctly. The same applies for the working directory, if it differs from the program directory.

6. Our first test of the Program action is successful:

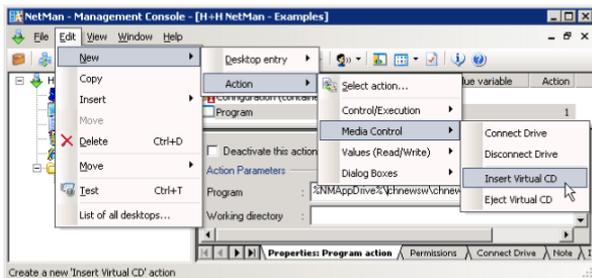


There are still two more functions to be configured:

- We want the CD to be mapped automatically when the application is launched.
- We want to be able to launch the application on any workstation.

7. NetMan has two actions specifically designed to support Virtual CD:

- Insert Virtual CD
- Eject Virtual CD

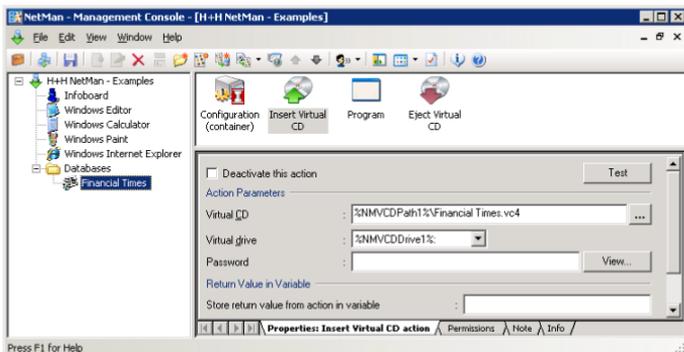


We add these two actions to the configuration, bracketing the Program action. NetMan automatically sets the `NMVCDDrive1` (or `NMVCDDrive2`, `3`, etc.) variable(s) on the client workstation in accordance with the Virtual CD drive when the application is launched.



Because many CD applications look for their CDs in the same drive that was used for installation, it is important to use consistent Virtual CD drive configurations throughout the network—for example, by using a modified Client Network setup—so that your (virtual) CDs can use the same drive letter on every station.

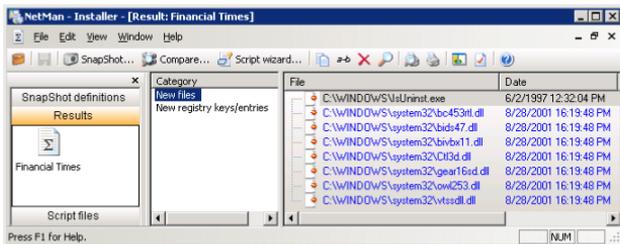
8. Enter the path to the desired Virtual CD image file in the **Virtual CD** field. If default paths are defined for Virtual CD files in the NetMan Settings, the Management Console automatically uses the corresponding variables for the path name:



Any time you have trouble with a configuration that contains multiple actions, it is a good idea to run the Trace Monitor to diagnose the problem.

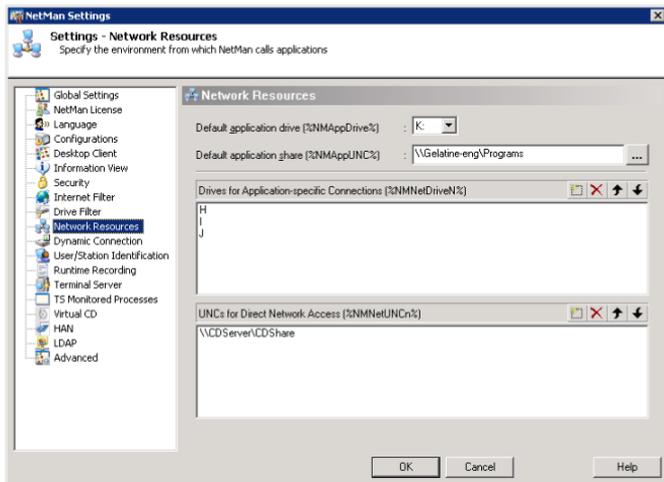
9. When this application is started on a different station than the one it was installed on, a message appears stating that required DLLs are missing. There are a number of ways to address this problem:

- You can repeat the entire Setup procedure on the station in question.
- You can copy the missing DLLs to the application's working directory. In this case, the application runs once we copy a total of four DLL files to the %NMAppDrive%\chnews directory. The *NetMan Installer* makes it easy to detect missing files in such cases, because it can show you the differences in your system directly before and immediately after installation of a program. For details on working with the Installer, see "Installer". Furthermore, the Installer can generate a script based on the results of the before/after comparison, and you can integrate the script in a Program action to have the required system modifications performed automatically when the application is launched for the first time on a given station:



In the case at hand, however, all you need to do is copy the required DLLs to the application's working directory.

10. In an environment with considerable CD-ROM usage, the definition of Network Resources in the NetMan Settings might look something like this:



There is one CD server, which permits access to all of its CDs. The drives H: through J: are reserved for temporary run-time mapping of local drives for applications.



The variables for reserved, temporary drive mapping do not contain colons because some applications expect their data source reference as a drive letter without a colon.

Under these conditions, you can distribute your CD applications in NetMan as follows:

Try at first to run the application setup in the network environment using the `NMNetUNCn` variable. If this does not work, you can assume that the application requires a fixed drive designation. Map the required drive (from the reserved drives) at run time for the application.



In some cases, you can switch the mapped drive to a UNC path at a later point.

If you find that the application can access its data CD under different drives, either because it can search all drives or because the drive designation can be passed on the command line, use `NMNext` as the drive designation. In this case, the first available CD drive found on the workstation is used for mapping and stored in the `NMNext` variable. You can specify how NetMan stores a value in `NMNext` on the **Dynamic Connection** page of the NetMan Settings.

Example: Mapping a Share to a Reserved Drive

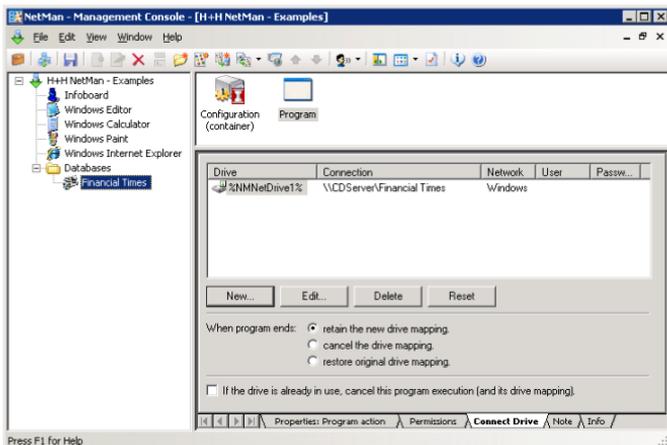
1. The drive in question has to be shared in your operating system first:



2. Then you can map a drive before the program starts, using the `NMNetDrive1` variable, to connect the CD to the reserved drive designation.



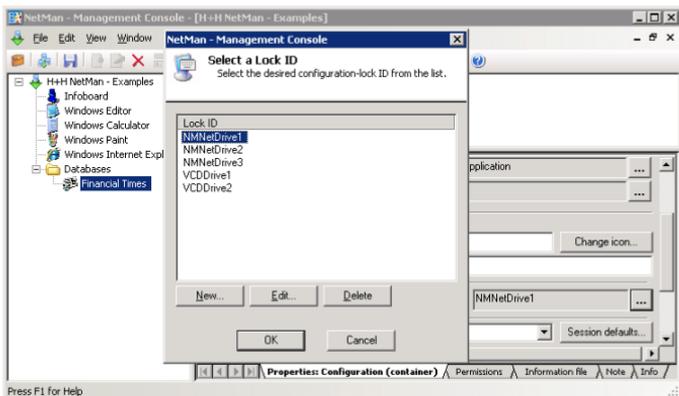
Use the drive mapping function that is integrated in the Program action, as this is much more powerful than the Connect Drive action. The latter is best used for other functions, such as startup and shutdown configurations for example, in which Program actions are not allowed.



The example shown here blocks the drive that is in use; in other words, other applications that require this drive cannot be started on the same workstation.

Example: Assigning a Lock ID

You can configure a lock ID to prevent simultaneous use of different configurations:



Configurations that have the same lock ID cannot run simultaneously on one machine. For example, if the “Observer” configuration has the same lock ID as “Financial Times,” the following message is shown when a user attempts to launch the latter while the former is running:

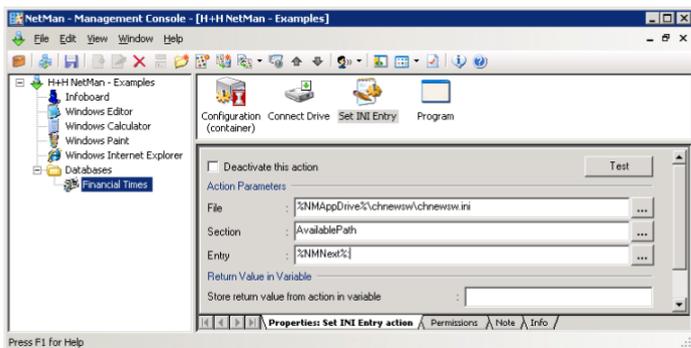


Example: Mapping a Share to a Specific Drive

If you know exactly where your application gets its data (i.e., which drive the required CD is in), drive mapping is even easier. The "Financial Times" application has an INI file with the following sections:

```
001 [DISCLOCATION]
002
003 [AVAILABLEPATH]
004 Path0=f:
```

In such cases, you can use the `NMNext` variable for the drive designation, which causes NetMan to connect the next available drive. All you have to do is "tell" the application that its drive is stored in this variable. In our example, this is done by inserting a *Set INI Entry* action:



With this setting, the value determined for `NMNext` is written in the INI file before the application starts. If the application reads its drive from the Windows registry, you can use a *Set Registry Key* action to write the `NMNext` value in the registry when the program is launched.

Example: UNC-based Access

A very convenient alternative is to write the UNC path in the INI file, if the application can process UNC syntax, as is the case with our “Financial Times” application:

```
001 [DISCLOCATION]
002
003 [AVAILABLEPATH]
004 Path0=\\CDServer\CDSshare\FT302
```

In this case, you require neither a special share for the CD (“CDSshare” is all you need) nor an available drive letter, which saves you the trouble of mapping a drive before the program is launched. This method can, however, have disadvantages in certain instances. For example, users can recognize the location of the application data, and can load additional data (if there is any) for the same retrieval interface, which you might not wish to allow.

Integrating HAN Accounts

Access accounts created using H+H HAN can be integrated in NetMan desktops in the form of NetMan configurations. This requires the prior installation and registration of HAN, as well as the registration of HAN within NetMan.

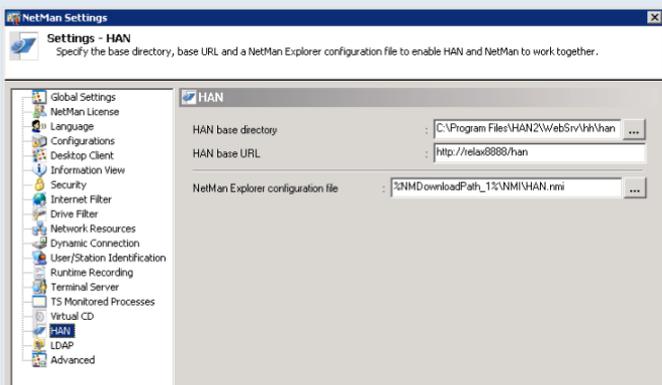


It is no longer possible to register HAN using a NetMan license code; a separate HAN license is required.

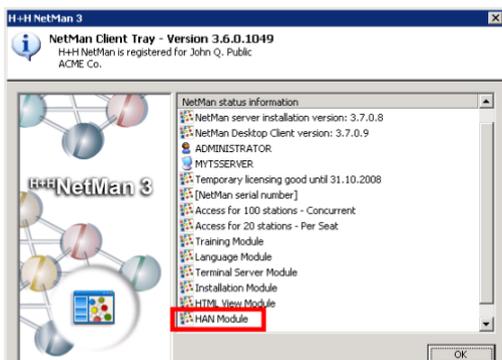
1. To load HAN accounts in NetMan desktops, you need to enter the HAN installation path in the *NetMan Settings*:



The **HAN** dialog page in the NetMan Settings is not shown unless your NetMan registration includes the HAN license.

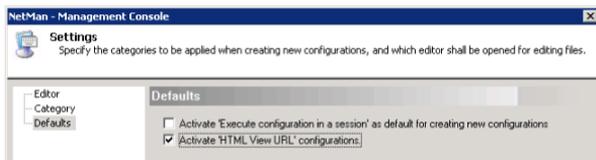


If this dialog page is not shown check your registration data; for example, by opening the **Info** dialog using the NetMan Desktop Client icon in the notification area of the system tray:

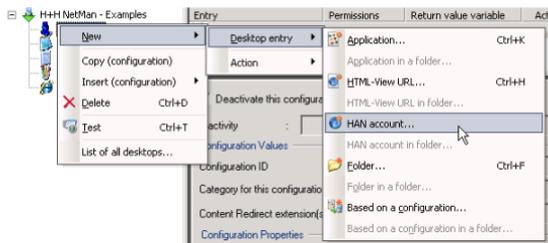


2. Enter the path to your HAN installation under **HAN base directory**. This is the directory specified in your HAN installation for storing individual HAN modules. In a standard HAN 2.0 installation, this is the `\WebSrv\hh\han` directory. The URLs for NetMan hyperlink configurations can now be made up of the HAN base URL you enter here and the name of the HAN account.

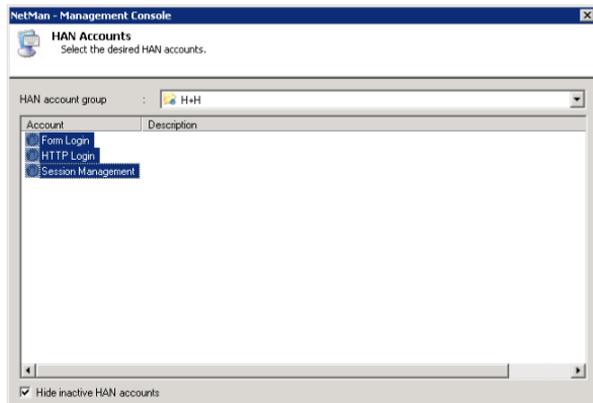
3. The next step is to register the use of HAN accounts in the *NetMan Management Console*. To do this, open the Management Console properties, open the **Defaults** page and select the **Activate HTML-View configurations** option:



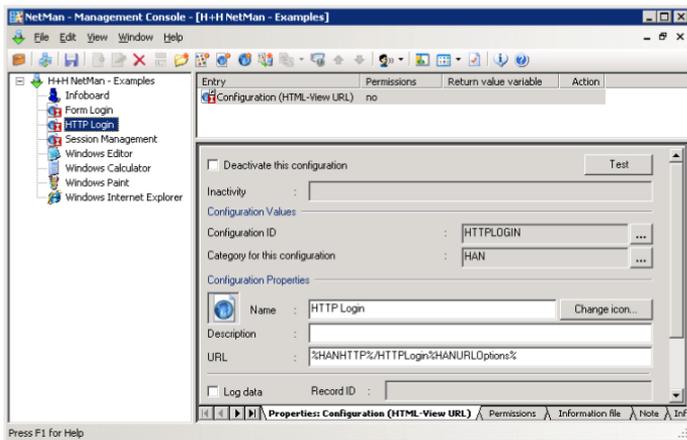
4. Once you restart the Desktop Client and the Management Console after activating HTML-View configurations, your HAN accounts are available for integration in NetMan desktops:



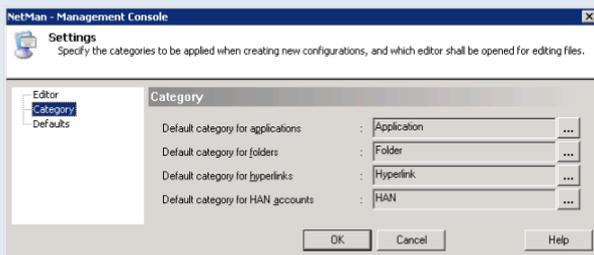
5. Simply mark the accounts you wish to import as NetMan configurations and click **OK**:



A HAN account is integrated as a HTML View URL configuration. The new configuration inherits the properties (name, description, URL) already defined for the HAN account in question:



You can change the category specified for data imported from HAN under **View/Settings/Category**. The default category is "HAN:"

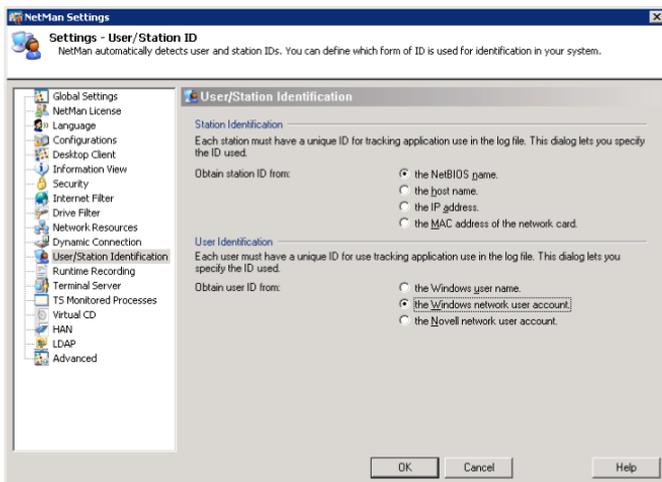


NetMan Resources

The term “NetMan resources” as used here means all NetMan users, stations, groups and profiles, as well as your NetMan licenses. The first time you launch NetMan, the users and workstations in your network are automatically added to the NetMan user and station databases. To view or edit these data records, select the **Resources** item in the Administration view of the Management Console sidebar:



When a new user or station runs NetMan for the first time subsequent to your initial NetMan startup, a new data record is created. The key field in these data records is the user or station ID. Data records are stored under the ID you specify in the *NetMan Settings*:



Not all forms of workstation identification listed in this dialog are available in terminal server sessions.

NetBIOS name. With this setting, the client name given in RDP or the ICA protocol is used. On Windows workstations, this client name is usually the station’s NetBIOS name.

Host name. With this setting, the client’s IP address is determined and reverse DNS lookup is used to determine the host name. If this does not work, the IP address is used for identification. We recommend selecting this setting only if reverse lookup is available.

IP address. With this setting, the client's IP address is used. Because the IP address is passed in the RDP or ICA protocol, NetMan Desktop Manager can use it for identification even if your workstation is in a private network (10.10.10.10/16), for example, and you access NetMan Desktop Manager over a NAT firewall.

MAC address of the station network card. This property cannot be determined in a terminal server session. If this option is selected, the IP address is used for client identification.

Users

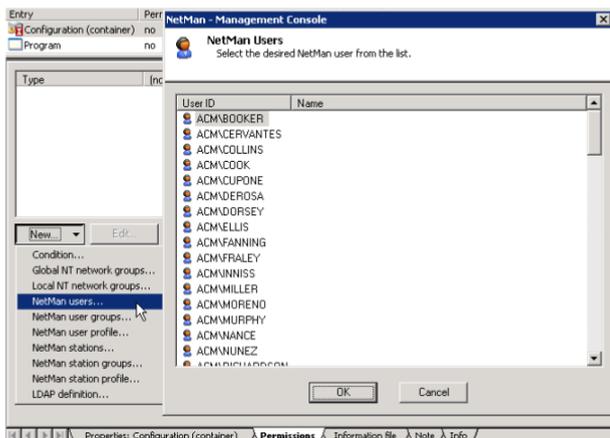
In our example, we have chosen to use the Windows NT network user login name as the user ID. The format of this ID in the user database is *domain\user*. NetWare user names are written with NetWare syntax, and can be detected only by the IntraNetWare Client from Novell. If a NetWare user name cannot be determined, the data record is stored under the Windows NT user name. You can create, edit, re-name and delete user data records. To create a new user, select **Create** from the **Edit** menu and enter a user ID. This opens the following window:

The “Last active on” field in the upper right-hand corner cannot be edited; it is updated every time the user runs NetMan. The fields for **Address**, **Department**, **E-mail** and **Phone** are not required for NetMan operation; they are for your administrative purposes only and can be referred to by a NetMan *Data List* action. The Name you enter here is separate from the user ID; this name is recorded in user lists for statistical evaluation purposes.



You can define user-specific startup and shutdown configurations here. These are executed after the global startup and shutdown configurations. For the Start menu and the Desktop settings (Windows Desktop), you can specify a different NetMan desktop than that defined in the global settings.

You can open a list of users compiled from this database when assigning 'execute' conditions for configurations and actions in the Management Console:



You also have the option of creating a user data record manually; for example, to achieve the following:

- To create a record for a user who has never launched NetMan
- To create a record for a NetMan user account which does not correspond to any existing network user

For example, you can create a user account that is used in a *NetMan Logon* action, or assigned to anonymous users on the basis of IP address or host name through the NetMan access control program. We recommend assigning a password to this type of account.

Example:

Create a password-protected user account for guest users, with your choice of rights and privileges.



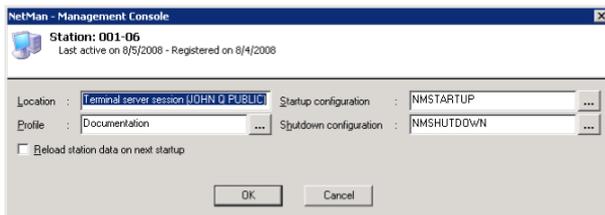
NetMan permissions are independent of network privileges; they are equivalent to 'execute' rights for NetMan configurations.

Stations

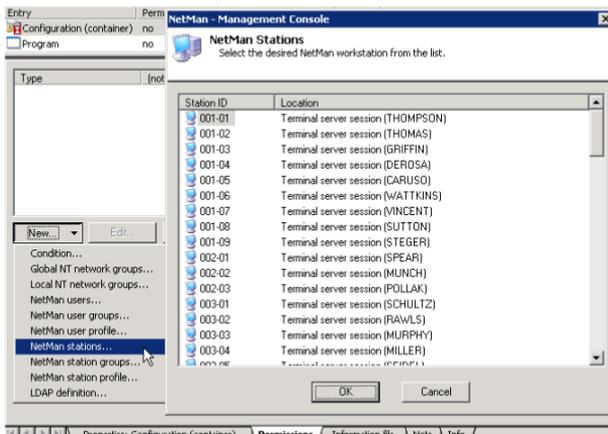


If you have configured NetMan to use computers' host names as station ID, but the host name of a given machine cannot be determined, the IP address is entered for that machine instead; if this cannot be determined either, then the computer name is used.

You can create, edit, re-name and delete station data records. The **Last active on** field in the upper right-hand corner cannot be edited; it is updated every time NetMan runs on this station. The **Registered on** field is relevant for the named sites licensing scheme, as each license is valid for 40 days. At the end of this period the license is released for another station, if this station is no longer using NetMan. A station data record contains the following fields:



The **Location** field is for your information only; it can help ensure a clear overview in the lists of stations shown in programs for statistics, license administration, station monitoring and permissions. No input is required here for NetMan operation. NetMan automatically enters the name of the user under whose account the station database record was created; you can overwrite this entry, if desired. Some of the fields in the station database can be referred to in a *Data List* action. You can open a list of stations compiled from this database when assigning access rights to configurations or actions in the Management Console:



You can also create station data records manually; for example, to add a record for a station that has never used NetMan.

NetMan detects the following data for inclusion in the station database record:

- Bios data
- Hardware
- Installed cards and connected peripheral devices
- Network configuration, including the drivers and protocols implemented
- Installed software (mail clients, browsers)

All of this data is recorded the first time this station starts NetMan. If desired, you can have this data updated every time this station starts NetMan by activating the **Reload station data on next startup** option.



Data on workstations is collected by NetMan Desktop Client and stored in a database. Keep in mind that this data cannot be collected from thin clients or other stations that do not use NetMan Desktop Client for access.

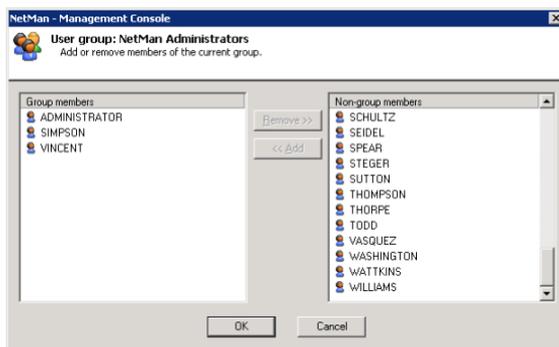
User Groups

You can create groups for your users. The advantage of NetMan user groups may not be immediately apparent, since NetMan supports existing NT, NetWare and LDAP user groups; besides, proprietary groups are generally regarded as a disadvantage because they are associated with additional administration tasks. But NetMan groups are active on a totally different level: they are used for definition of permissions to NetMan configurations, and have nothing to do with rights in directories, files or other network resources. If you find that your existing network groups provide sufficient control over NetMan configurations, then you have no need of NetMan user groups. It is best to use existing network groups wherever possible, to avoid generating extra work unnecessarily. But if you find that the existing groups cannot be used to configure the control you need, you may find it easier to create NetMan groups than to create (or have your network administrator create) new network groups.

NetMan user groups are particularly useful if any of the following is true for you as NetMan administrator:

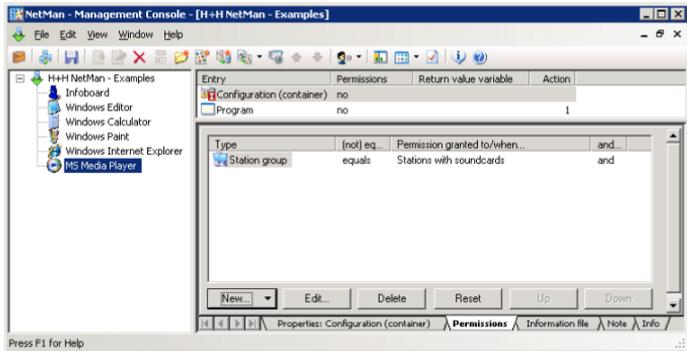
- You cannot modify existing network groups.
- Your network can be accessed from other domains and networks; for example, by anonymous users through the terminal server (NetMan lets you define a group exclusively for remote users and assign permissions accordingly).
- Your network has groups that are not supported (for example, if you are using Banyan Vines or a large Microsoft network with no domain controller).

You can create, edit, re-name, and delete NetMan user groups. The following example shows a group with three users:



Station Groups

With NetMan, you can put workstations together in groups. This is a feature that is not available in network operating systems. There are a number of situations in which grouping workstations can be useful. For example, some applications have specific requirements regarding the computer's internal hardware or peripheral devices. If you have an application that requires a sound card, for example, you can create a group just for workstations with sound cards and limit the 'execute' permissions for the NetMan "Windows Media Player" configuration to this group:

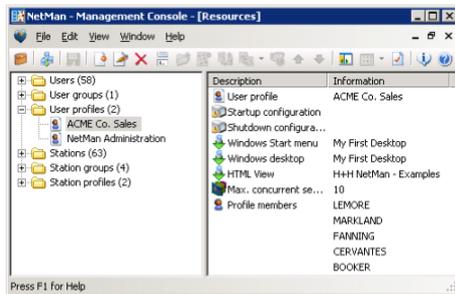


You can create, edit, re-name and delete NetMan station groups.

NetMan User and Station Profiles

The startup and shutdown configurations you specify on the **Global Settings** page of the NetMan Settings are effective for all users. You can configure different settings for individual users and workstations, if desired, using separate startup and shutdown configurations. Frequently, however, it is not individual users or stations for which you wish to define different settings, but for groups of users and stations. NetMan groups cannot be used for this purpose, because a given user or station can belong to any number of different groups.

To apply a certain set of parameters to a group of users or stations, you need to work with disjunct groups. “Disjunct” in this context means that each group member can belong to only one such group. In the NetMan system, these groups are called *profiles*. You can select the user/station profile rather than user/station ID as the identifier in NetMan data log and statistics program:

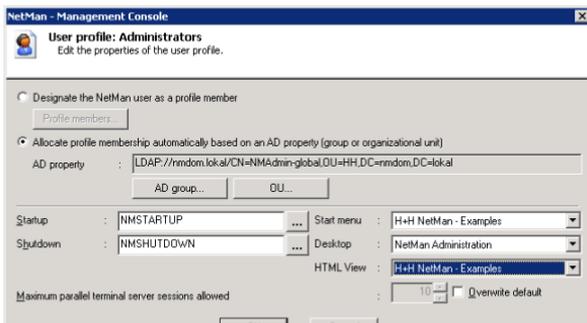


You can create, edit, re-name, and delete NetMan user and station profiles.

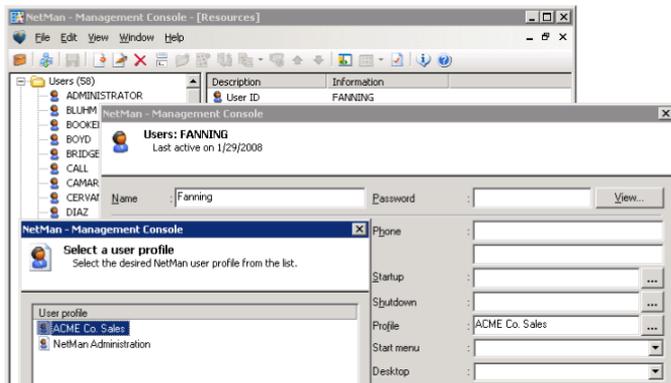
User Profiles

The following preferences are defined in the user profile:

- Startup configuration
- Shutdown configuration
- Windows Start menu
- Windows desktop
- Number of parallel terminal server sessions allowed
- Profile members



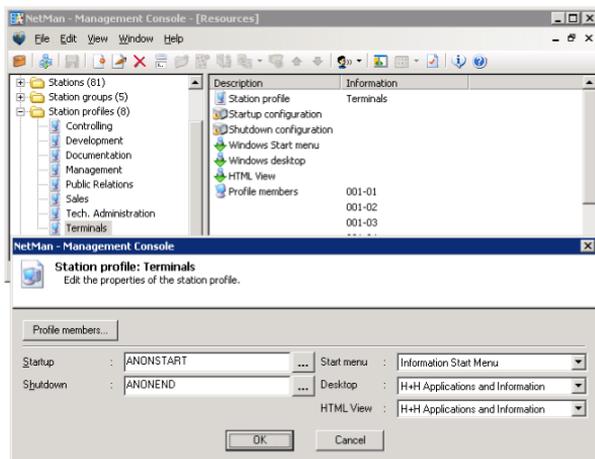
Belonging to a profile is a property of a user, and can be entered in the user database:



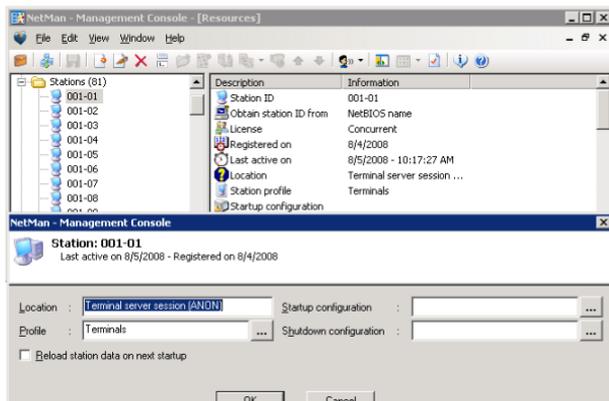
If you wish to add several users to a profile, however, it is easier to do this by editing the profile than by modifying each of the respective user data records. When you assign a user to a profile, any existing membership in another profile is automatically cancelled. As an alternative to assigning profiles by selecting individual NetMan users, a profile can also be assigned by selecting one of the two AD properties, "AD Group" or "OU Membership".

Station Profiles

In the station profile you can define preferences for the startup and shutdown configurations and allocate a NetMan desktop for the Windows Start menu and the Windows desktop:



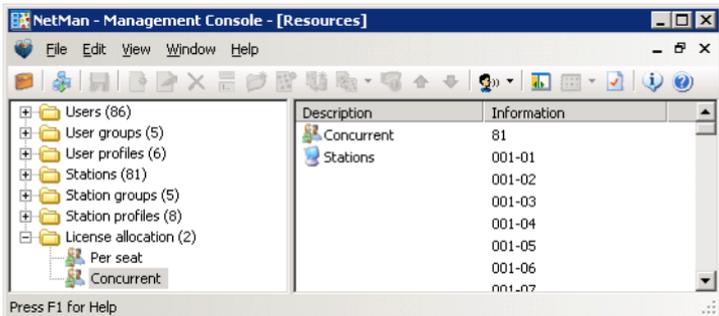
Belonging to a profile is a property of a station, and can be defined in the station database:



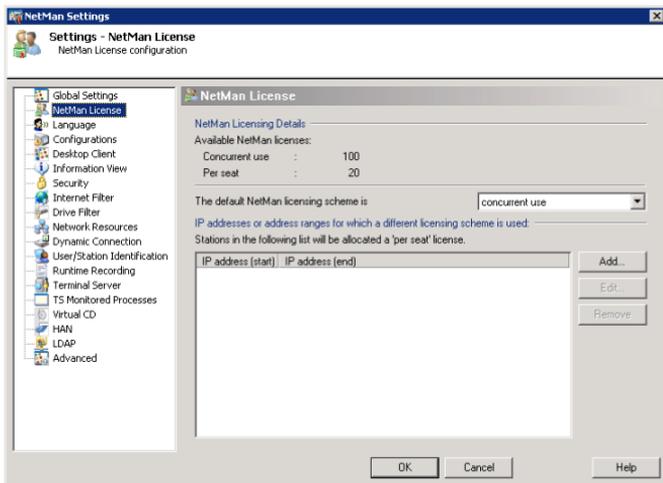
If you wish to add several stations to a profile, however, it is easier to do this by editing the profile than by modifying each of the respective station data records. When you assign a station to a profile, any existing membership in another profile is automatically cancelled. As an alternative to assigning profiles by selecting individual NetMan stations, a profile can also be assigned by selecting one of the two AD properties, "AD Group" or "OU Membership".

Allocating Licenses

With NetMan, you can use the Concurrent Use and Per Seat license schemes simultaneously. To help you keep track of your licenses, we have integrated the license allocation functions in the Resource Management program in the Management Console:



The “License allocation” folder contains two items; “Concurrent” and “Per Seat.” When you click on one of these items, details on the corresponding licensing scheme are shown on the right, including a list of the stations using that scheme. With the default NetMan settings, each station is automatically allocated a Concurrent license when it logs on. You can change this setting if desired on the **NetMan License** page of the NetMan Settings:



You can allocate per-seat licenses on this page. Click on the **Add** button and enter the IP addresses of the stations to which you wish to allocate per-seat licenses.

A station that is no longer using a per-seat license can be removed from this table. To do this, select **License Information** from the **Edit** menu. Click on the checkbox to activate the **Remove stations** options and then click on **OK** to confirm:



Web Interface (HTML View)

The examples in the previous sections described the use of shortcuts embedded in the Start menu or on the desktop. Such scenarios require an installation of NetMan Desktop Client on the workstation (running Windows 2000, Windows XP, Windows Vista, or Windows 2003). Alternatively, you can use NetMan Desktop Manager to offer published applications through a web interface. This method has a number of advantages in certain cases:

- Less stringent requirements for starting applications through a browser than through NetMan Desktop Client: For example, the application session can be opened on a workstation running Windows 98 or Windows NT.
- Applications can be launched using Mac OS X or Linux computers, as well as on thin clients. All operating systems with Java Runtime Environment 1.5/1.6 are supported.
- All common browsers are supported. Application sessions can be started not only in the MS Internet Explorer but also in Firefox or Opera, for example.
- In conjunction with NetMan Desktop Manager's NetMan SSL Gateway component, your applications can be accessed from any location, and the RDP traffic is SSL-encrypted.

HTML View is technically an extension for the Apache HTTP server (Windows-based). When you install NetMan, all components required by HTML View are automatically installed as well. HTML View and NetMan must be installed and operated on the same server.

Because HTML-View can be extensively adapted for your requirements and preferences, this chapter presents detailed descriptions of the components that are installed with HTML View.

The HTML View Module must be licensed before you can use the functions described here.



For optimum security we recommend setting up a separate account for the NetMan Web Server service, rather than running it under the system account. Make sure the account you set up for this purpose has the required rights in the Web Server directory.



If you want to allow anonymous users in terminal server sessions, please make certain that the NetMan User Service has been installed. For details on installing that service, please refer to the manual for the Terminal Server Module.

HTML View is configured in the NetMan Web Services Settings. For details on how to configure HTML View, see *“HTML View Settings.”*

The HTML pages are generated dynamically. For published applications, this means that changes in your settings – for example, if you change an application’s access permissions – are effective immediately in the web interface. You can choose between the Explorer View and the List View for presentation of your applications in the NetMan web interface.

The Explorer View shows your applications in a clear overview similar to that in the Windows Explorer. This view is very easy to navigate and requires no further configuration in the web page itself in order to present your applications in HTML View. At the same time, the Explorer View permits individual adaptations in the design. For details on use of the Explorer View, see *“Configuring the HTML View Explorer View.”*

The List View uses placeholders to integrate the published applications in existing websites, or in the templates supplied with NetMan. This opens up the broadest range of possibilities for presenting your applications in the Internet. For details on using the List View, and on using placeholders to integrate applications in your web pages, see *“Configuring the HTML View List View.”*

Directory Structure in HTML View

The HTML View installation directory (`NetMan3\WebSrv\HH\HTML-View\`) has several subdirectories:

- The `_download` directory contains all the clients required for terminal server access. A link lets the end user download and install Web clients manually. The following clients are stored here when you install the program:
 - Citrix Java client
 - Citrix Web client
 - NetMan RDP Web client
 - Java RDP client
 - rdesktop over Java applet



Store updated clients here as they become available. Compare the latest version available with the version stored here to determine whether you need to update a client.

- The `_images` directory contains the images that HTML View uses in its sample HTML pages. We recommend storing the images used in your own Web pages here as well.
- The `Bin` directory contains the executable components of HTML View.
- The `Default.htf` directory is the standard template for presentation of the NetMan desktop and of NetMan container and hyperlink configurations.
- The `MyFormat.htf` directory is a copy of the `Default.htf` directory. We recommend storing templates you have modified here since, unlike `Default.htf`, the `MyFormat.htf` directory is not overwritten when you update your NetMan software.
- The `WithCategories.htf` directory is an example of how the appearance of a page can be altered by editing a template file. In this example, images indicating NetMan categories are shown with every application.
- The `Launch` directory contains the templates used by HTML View to generate launch files for access to applications (ICA configuration files, HTML pages with Microsoft Web client and NDP files).
- The `NetManBin` directory is used by HTML View when generating links. This directory is referenced every time an application is called.
- The `NetManBinDual` directory is not used by HTML View; it is part of NetMan Web services.
- The `nmticket` directory is used by HTML View for the ticketing procedure.
- The `Setup.NetMan User Service` directory contains the setup program for the NetMan User Service.
- The setup program for NetMan SSL Gateway is in the `Setup.NetMan SSL Gateway` directory. Do not install the SSL gateway on the same server on which NetMan is installed.

Authentication Services Directory:

Because the H+H authentication services can also be used by other H+H products (such as HAN), this service is installed in a separate directory: `\WebSrv\HH\Com-mon`.

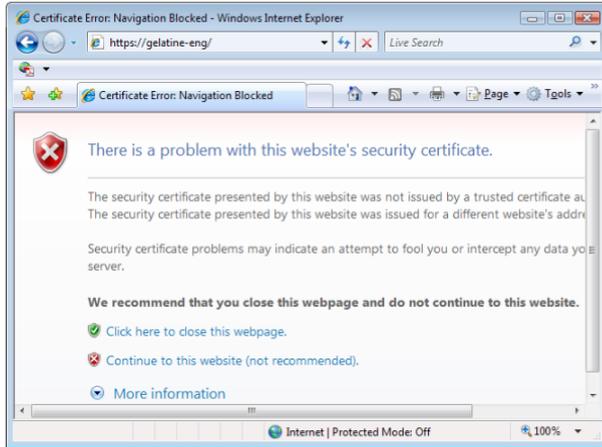
Virtual Web Directories:

The virtual directories required for operating HTML View are defined in `NMView.conf`. These virtual directories and the files they contain can be addressed on the NetMan Web Server using URL syntax. The following virtual directories are created when you install HTML View:

- `/_download/` points to the `_download` directory containing Web clients for downloading.
- `/_images/` points to the `_images` directory which contains, as the name suggests, images used in Web pages.
- `/nmsamples/` points to the `example` directory, which contains sample Web pages.
- `/NetManBin/` points to the `NetManbin` directory.
- `/NetManTicket/` points to the `nmticket` directory.
- `/nminfo/` points to the `nminfo` directory, which contains the info files that can be linked to applications.
- `/NetManBinDual/` points to the `NetManbindual` directory for launching sessions from within the NetMan Desktop Client.
- `/tsinfo/` points to the `tsinfo` directory.

Logging in through the Web Interface

Simply point your browser to the server: `http://<server name>`. You are automatically rerouted over HTTPS and the following warning is shown:



This indicates the use of SSL encryption for a secure connection. Upon installation, NetMan sets up a self-signed certificate for a server labeled DO_NOT_TRUST. To avoid getting this warning in future, create or request your own certificate. For the current demonstration, click on **OK** to confirm that the certificate is trusted.

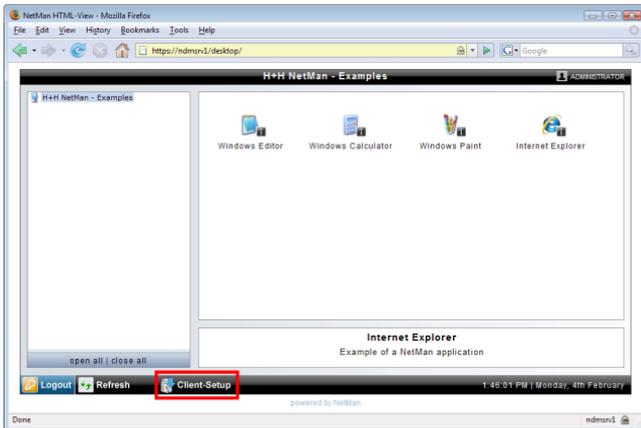
The browser opens a login page for user authentication in the web interface.



The automatic re-routing described above will function correctly only if you accepted the default port numbers when installing NetMan. If you changed the port numbers, for example because an Apache server was already using the default port, you have to point your browser as follows to open the web interface: `https://<server name>:port`. For "Port" enter the HTTPS port number for your NetMan installation.

Installing the NetMan RDP Web Client

The NetMan RDP web client has to be installed on the workstation before the user can call applications using the web interface. To do this, simply log in on the web interface and then click on Client Setup:

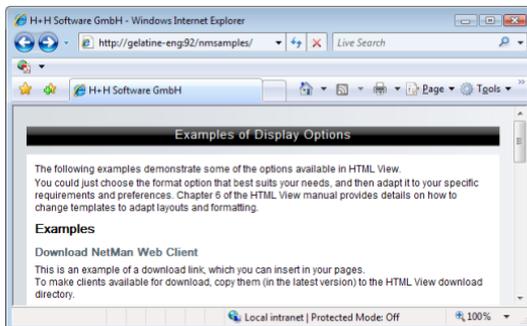


No user input is required and, as a rule, no system reboot either.



Installation of the NetMan RDP web client requires administrator privileges.

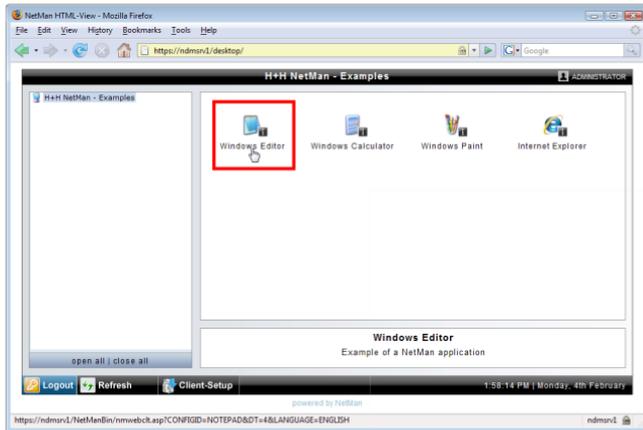
The List View example that comes with NetMan has a link to a download page at the top of the list. Enter the URL for the example pages (<http://<servername>/nmsamples/>) and follow the link to the Web Client download page:



We recommend providing a download page for your users, with a link to the client download and brief instructions on installation so they can perform these steps on their own.

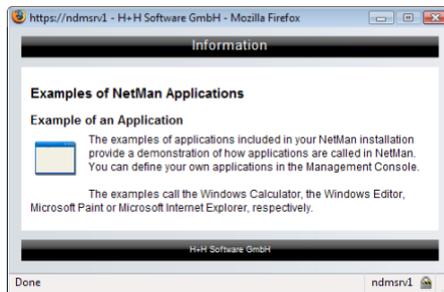
Calling Applications through the Web Interface

Once the NetMan RDP web client has been installed, you can run an application by clicking on the associated icon. The example shows the HTML View Explorer View, which uses graphic links. The List View, on the other hand, uses only the name of the application for the link.



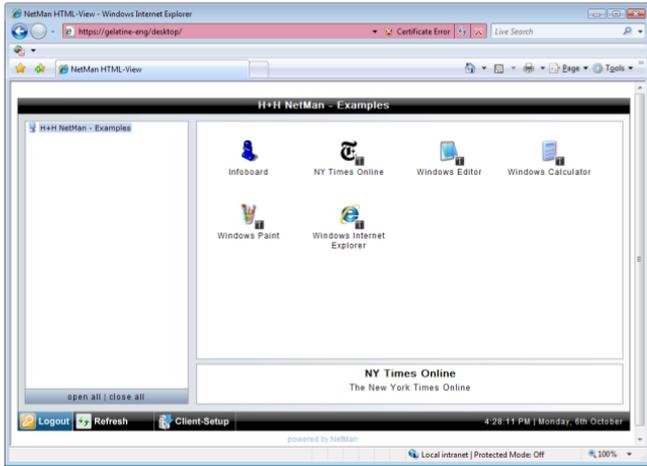
There is no difference between a session opened through web interface and one opened using the NetMan Desktop Client.

You can store information on the applications in the form of HTML pages, which can be opened by clicking on the link marked with **i**:



Calling Hyperlinks through the Web Interface

Directly following installation, you cannot call hyperlinks over the Web interface. This is due in part to the fact that "Infoboard" is the only hyperlink in the predefined sample desktop. When you open the desktop in the Management Console, you can see that the Infoboard configuration is not flagged for display in HTML pages. To test the display of HTML pages, you need deactivate the corresponding option in these properties. Alternatively, you can create a new Container configuration with a Hyperlink action in it.

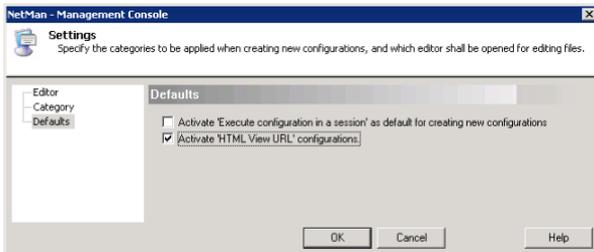


With the default settings, the hyperlink you call is opened in a terminal server session. This is often preferable; for example, if your clients do not have their own Internet connections.

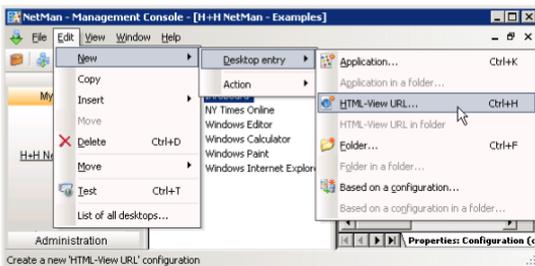
In some cases, however, you may wish to have hyperlinks open directly on the client machine, in the default browser.

There are two different ways to do this.

1. The first option is to use an *HTML-View URL* configuration rather than a Hyperlink action to call the URL. HTML-View URL configurations correspond to the Hyperlink configurations in earlier NetMan versions. You can create HTML-View URL configurations in your NetMan Management Console. First, however, you need to activate the use of HTML-View URL configurations in the Management Console settings. To do this, select the **Activate 'HTML-View URL' configurations** option on the **Defaults** page of the Management Console Settings:

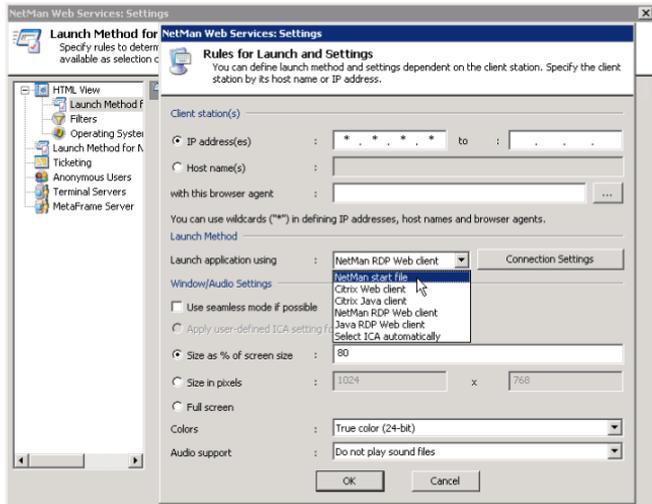


After you change this setting, the Management Console has to be shut down and then opened again. Then you can access the commands in the **Edit/New/Desktop Entry** menu and in the toolbar in the wizard for creating HTML-View URLs:

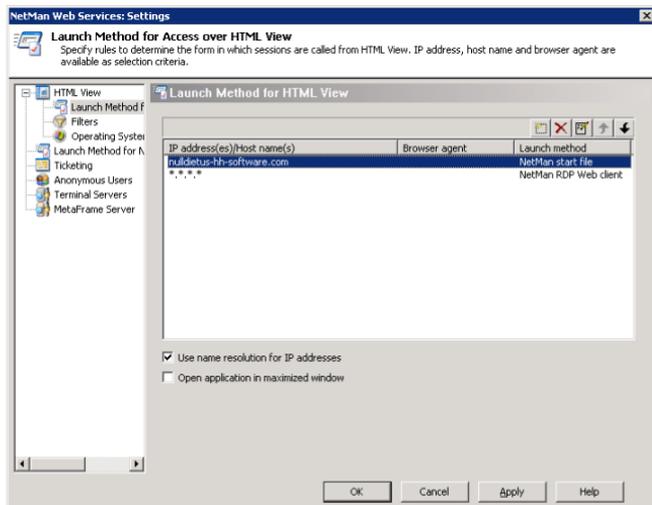


HTML-View URLs are called in the local browser. The disadvantage is that these configurations cannot be assigned a NetMan Internet filter. Once an HTML-View URL has been called on a particular computer, the Internet is freely accessible on that computer.

2. The other option is to change the launch method. This setting is configured in the NetMan Web Services Settings. With the default settings, HTML-View uses the NetMan RDP Web client to launch applications and hyperlinks. Change this setting so that the launch method is “NetMan Start file”:



When you modify the Web services settings, you can also define which stations can open hyperlinks, and which cannot. In the following example, the launch method on the station called Nulldietus is “NetMan Start file”. All other stations in the network use the NetMan RDP Web client to run NetMan configurations:



HTML View Settings

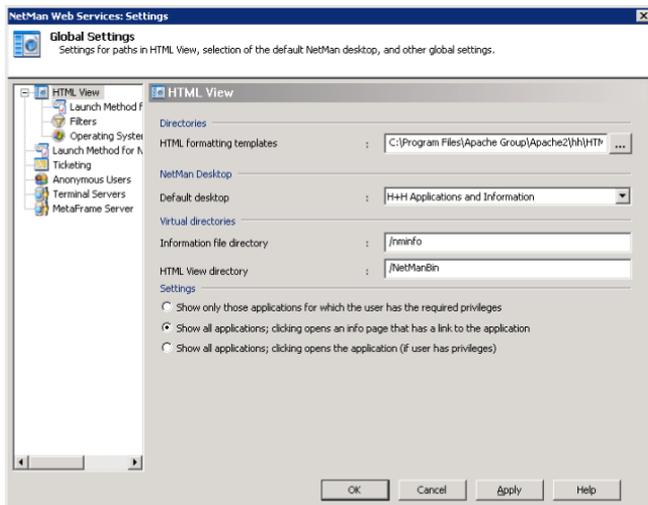
To configure HTML View, open **NetMan Web Services Settings** from the NetMan Toolbox.

All parameters for HTML View are configured here, except the settings for H+H authentication services. In some cases, changes are not effective until you restart HTML View (and any client browsers running at the time). Where this is the case, it is pointed out explicitly in this manual. To restart and re-initialize HTML View, shut down and restart the NetMan web server.

The Web Services Settings program is divided into categories which are listed in the sidebar. This chapter describes the settings that affect only HTML View. Details on other settings are given in the Terminal Server Module manual. These descriptions provide a handy reference guide to the range of options available for settings, complementing the practical introduction to the use of HTML View given in the preceding chapters.

Global Settings

Select **HTML View** in the sidebar of the NetMan Web Services Settings program to configure basic settings for HTML View operation. Modifications in these settings are effective only after HTML View is restarted (i.e., by restarting the NetMan web server service).



In the **HTML formatting templates** field, enter the HTML template directory for NetMan desktop and configuration layout. As described previously in the manual, you can replace this setting in a particular HTML page using the `@NM_TEMPLATES` placeholder. The directory you specify must have the `.htf` extension, must be stored in the same directory as the directory specified in the settings program, and must contain the desired HTML template files. For detailed information about HTML template files, please see “*Templates for Generating Desktop Structures.*”

In the **Default desktop** field, enter the default desktop for HTML pages. You can choose from the NetMan desktops contained in this list.



If a different desktop is assigned to a given NetMan user or station or the profile to which the user or station belongs, then the desktop specification in the HTML View settings or in the HTML page is ignored.



You can configure different desktops for the standard NetMan Desktop Client and HTML View. For example, you can define a desktop for HTML View that shows only the NetMan configurations that you wish to present in your HTML pages, rather than all of the configurations that are available in NetMan. Enter this as the Default desktop in the NetMan Web Services settings.

The two fields under **Virtual directories** specify directory names that are used in the URLs when HTML View is called.

In the **Information file directory** field, enter the virtual directory defined for NetMan information files. HTML View refers to this URL to present information files. The standard name for this directory is `nminfo`. This points to the `_Info` subdirectory of the HTML View installation.

The role of the directory named in the **HTML View directory** field is similar to that of a working directory. HTML View uses this directory when generating application launches. The default directory is `NetManBin`. This directory name was chosen to ensure compatibility with the HTML Client module, the predecessor to HTML View. Unless there is a pressing reason for doing otherwise, do not change the name of this directory.

These directories are created automatically when you install HTML View. For more information, see “*Directory Structure in HTML View.*”



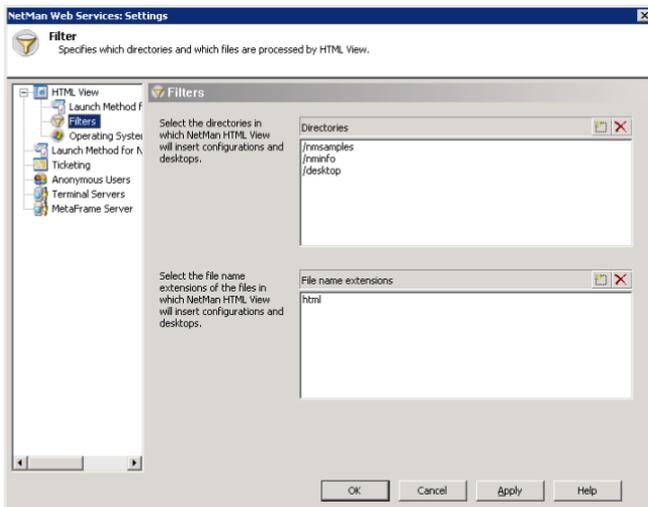
If you change the name of the directory in which your information files are stored, remember to adapt the virtual directory accordingly.

In the **Settings** section you can specify the operating mode for HTML View. There are three modes to choose from:

- **Show only those applications for which the user has the required privileges.** HTML View does not show those applications on the HTML page for which the user does not have access privileges. When a URL to an application is selected, the application is launched directly.
- **Show all applications; clicking opens an info page that has a link to the application.** HTML View shows all applications, including those which the user does not have permission to run. When a link to an application is selected, an HTML page opens showing a description of the application. This might include, for example, information on access privileges and application licensing. The link that actually launches the application is on this page. If the user does not have access privileges, you can have an HTML page opened with an Access denied message when the link is activated.
- With the third operating mode, **Show all applications; clicking opens the application (if user has privileges)**, users are offered links to all applications. If a user tries to open an application to which he or she does not have rights, you might have an HTML page opened that shows an Access denied message, or perhaps a login prompt.

Filter Configuration

On the **Filters** page of the NetMan Web Services Settings you can define which files are checked for the placeholders that HTML View fills in. Every time a user accesses one of your HTML View pages from a Web browser, HTML View checks the corresponding files for HTML placeholders before the page is sent to the client, and modifies them as needed. Directories that are not specified here are not affected by this search.



The first field, **Directories**, defines which directories HTML View checks for HTML placeholders. These are virtual directories on the NetMan web server. In the second field, **File types**, enter the file name extension(s) of the file type(s) that HTML View is to process. Files of this type are processed only if found in one of the directories entered in the Directories field.

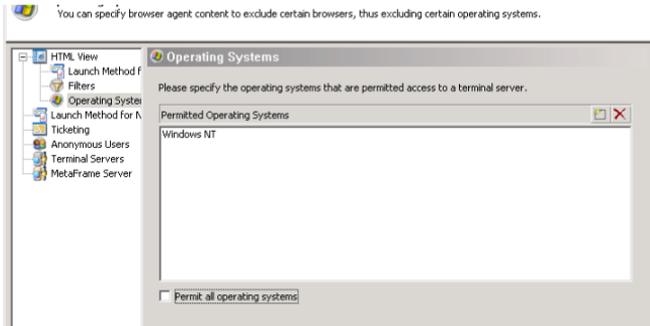


Keep in mind that **.htm** is handled by the program in the same manner as **.htm*** and thus includes files with the **.html** extension. This is why we specified only the **.html** extension in the default settings. This has the advantage that you can use the **.htm** extension for files that do not require processing, so that HTML View will not check these before opening them in the browser.

Permit Operating Systems

With HTML View, you can specify which client operating systems are allowed to access your terminal server. For example, if you are running Citrix MetaFrame on a Windows NT/2000 Terminal Server, Microsoft's licensing specifications require that every client accessing the server have a valid Windows NT/2000 license.

NetMan HTML View determines the client's operating system from the browser's userAgent property. Select the **Operating Systems** category of the HTML View settings to enter the operating systems you wish to permit:



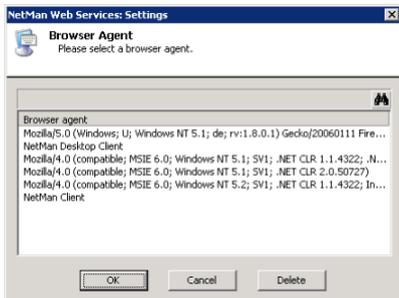
With the default settings, all operating systems are permitted to access NetMan. To switch on the operating system monitoring function, deactivate the **Permit all operating systems** option.

Click the **New** button in the upper right-hand corner of the Permitted Operating Systems field to add the segment of the userAgent string that designates the desired operating system.

When a client attempts access with an operating system that is not permitted, access is refused and an error message is shown. The HTML template file `Access_Denied_OS_Page.txt` contains the default error messages; you can edit these if desired. For example, if you enter Windows NT 5.0 so that only Windows 2000 is allowed, you might change the error message text accordingly.

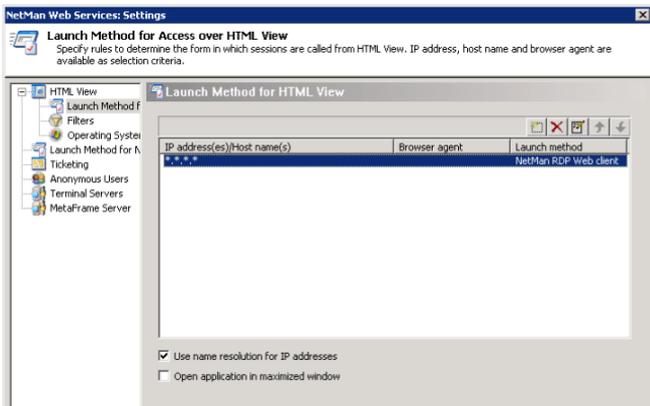


The operating system designation in the userAgent property can vary from one browser to the next. In the Microsoft Internet Explorer property, for example, the string "Windows NT" (the NT version number is added in browser versions 5.0 and later) designates the operating system, while Netscape Navigator uses "WinNT" to designate the same system. HTML View registers all client browsers with their browser agent. To view a list of the available browser agents, open the **Launch Method for HTML View** page, select a rule and click on **Edit**. Then click on the selection button next to the with this browser agent field:

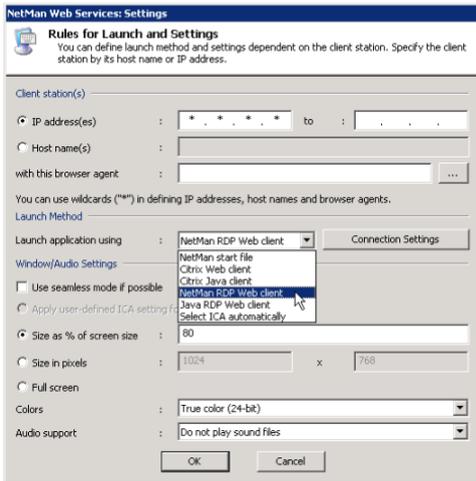


Launch Methods for HTML View

The *NetMan Web Services Settings* program gives you a number of options for configuring the session launch. Which launch method is used can be made dependent on the client's IP address, host name, and/or browser agent. Run the NetMan Web Services Settings program and select **Launch Method for HTML View** from the sidebar:



Select the “***.*.*.*” entry and click the **Edit** button:



In the “Launch application using” field you can choose from the following launch methods:

NetMan RDP web client: With this method, the NetMan web services create a configuration file for the NetMan RDP web client; i.e., for an RDP session. This requires the NetMan RDP web client or NetMan Desktop Client on the client workstation.

Java RDP web client: With this launch method, the NetMan Web Services provide an HTML page in which a Java applet for an RDP session is embedded. This method requires prior installation of Java Runtime Environment v1.5/1.6 on the client workstation.

rdesktop using Java applet: With this launch method the NetMan Web Services provide an HTML page in which a Java applet with an rdesktop call is embedded. This method requires prior installation of Java Runtime Environment v1.5/1.6 and rdesktop v1.5/1.6 on the client workstation.

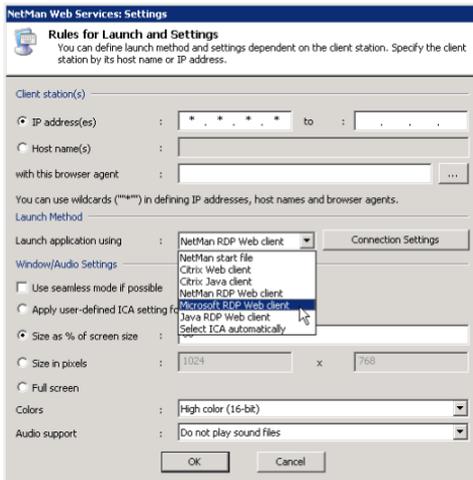
Citrix web client: With this method, the NetMan web services create a configuration file for an ICA session.

Citrix Java client: With this method, the NetMan web services provide an HTML page in which a Java applet for an ICA session is embedded. This method requires Java Runtime Environment on the client workstation.

Select ICA automatically: With this launch method the NetMan web services provide an HTML page in which a Java script automatically determines which ICA launch method the client browser supports. If the client has a native Citrix web client installed, the session is opened using the Citrix web client. With all other browsers, the session is opened using the Citrix Java client.

Rules for Determining the Launch Method

NetMan web services follow specified rules to determine which launch method is applied for client workstations. Select the **“*. *.*.*.*”** rule and click on the **Edit** button, or click the **New** button, to create a new rule:



This opens the **Rules for Launch and Settings** dialog, where you can specify the

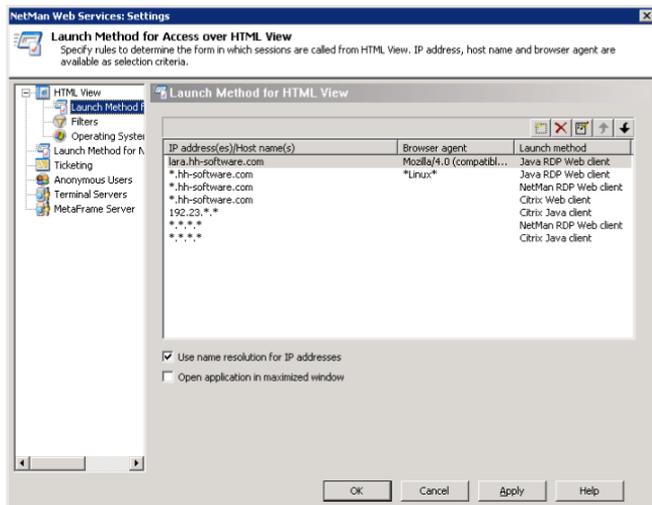
- IP address or host name, and/or
- browser agent of the client station

These settings are defined in the **Client station(s)** section. You can specify either IP addresses or host names, and use an asterisk (“*”) as a wildcard to specify a range of IP addresses or an entire domain. You can also enter portions of the stations’ browser agents as a further criterion. Workstations report their browser agent every time they access web services. Click on the “Browse” button (“...”) to view a list of all browser agents that have accessed your web services to date.



To use host names in these rules, make sure on the **Launch Methods for HTML View** the **Use name resolution for IP addresses** option is activated.

Example:



In the illustration above, 7 rules have been defined for determining the launch method. The rules are processed in the order in which they appear in this list, from top to bottom. The first applicable rule found is applied. The following factors are taken into account in determining applicability:

- IP address or host name of the client station
- Browser agent reported by the client station
- Divergent settings defined for the particular NetMan configuration (application call)

With the settings shown above, for example, if a workstation called *lara.hh-software.com* uses HTML View to access an application in NetMan, and no special settings are defined for the application call (see “*Advanced Application Settings for a Session*”) then the first rule in the list is applied and an HTML page with the Citrix Java applet is opened. If a Linux station in the hh-software.com domain uses HTML to access an application call, the second rule is applied. If, on the other hand, the ICA protocol

is explicitly specified in settings for the application called from the *hh-software.com* domain, the fourth rule in the list, rather than the third, is applied and “Citrix web client” is the launch method used. The rules defined for the IP address **.*.** are default rules. It is important that you always have default rules that can be applied in cases for which your more explicit rules do not apply. If you use MetaFrame, we recommend including a default rule that specifies the “Citrix Java client” launch method. For terminal server environments without MetaFrame, specify the “NetMan RDP web client” or “NetMan RDP Java client” in default rules. The last two rules shown in the list above (the sixth and seventh rules) include all other launch method options.

Criteria are applied in the following order:

- Settings for a particular NetMan configuration (application call) override the rule applied by HTML View.
- Which rule is applied is determined on the basis of IP address/host name and browser agent.



It is possible, particularly if special settings are configured in the application call, that none of the rules defined in HTML View can be applied. We recommend formulating simple rules and making sure there is always at least one rule that can be applied in any case. If there is no applicable rule, the NetMan start file is used.

NetMan Start File

The *NetMan start file* launch method is used only when calling applications in HTML View. Applications launched using this method execute on the client machine. This requires prior installation of NetMan Desktop Client on the workstation. NetMan Web Service sends the NetMan start file to the browser, which passes it to the NetMan Desktop Client. Thus the NetMan Desktop is the browser helper application for NetMan start files. This is automatically entered in the Microsoft Internet Explorer by the setup program for the NetMan Desktop Client.



If you use a different browser, you might have to register the NetMan Desktop Client as a helper application manually. To do this, you will require the following information:

- Mime type: `application/x-netman`
- Program call: `<Windows directory>\NetMan3\Bin\nmchttp.exe "/f:%1"`

The `start.nm` file is the template:

```
[Config]
```

```
ConfigurationID=@NM_ID
```

```
VID=@NM_VID
```

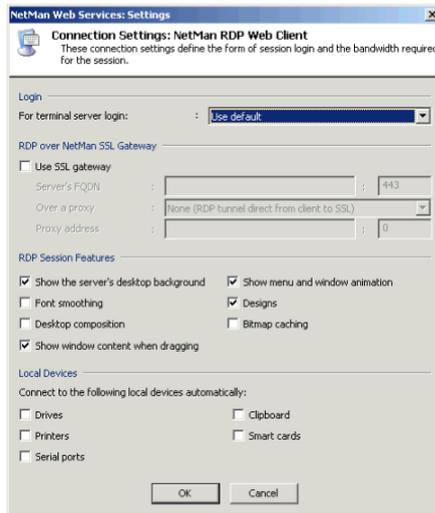
NetMan RDP Web Client

With the *NetMan RDP web client* launch method, the NetMan Web services generate a configuration file for the NetMan RDP Web client, which connects to a terminal server over RDP. This launch method can be called from NetMan Desktop Client and from the web interface, which is also referred to as “HTML View.”

You can configure the following settings for an RDP session:

- Connection settings
- Window/audio settings

To configure the connection settings, select **NetMan RDP web client** and click on the **Connection Settings** button. This opens the following dialog:



You can configure the following options here:

- Change the login method
- Modify the session bandwidth
- Modify settings for the NetMan SSL gateway
- Activate or deactivate client resources

In the **Login** section, you can select a method that differs from the default setting. Either the user's HTML View login data or a NetMan anonymous user account can be used for authentication.

In the **RDP Session Features** section, you can configure options that affect the bandwidth of an RDP session:

- **Show the server's desktop background.** Shows the server's desktop in the background of the session.
- **Font smoothing.** Clear Type font smoothing is supported for screen fonts.
- **Desktop design.** Activates support for Windows Aero and transparent windows.
- **Show window content when dragging.** Shows the content of the window while the window is being moved. If this setting is not selected, only the outline is shown while the window is being moved.
- **Show menu and window animation.** Shows menu and window animation in the session.
- **Designs.** Enables a choice of designs for the "look and feel" of the interface (e.g., Classic Windows, Windows XP)
- **Bitmap caching.** When this setting is active, frequently used images are stored on the local machine to reduce the volume of data transferred.

Activate **Use SSL gateway** to have the RDP connection made over a NetMan SSL gateway. In this case, the RDP connection between workstation and SSL gateway is embedded in an SSL tunnel. For a detailed description of the NetMan SSL gateway, please see "*NetMan SSL Gateway.*" In the **Server's FQDN** field, enter the host name of the NetMan SSL gateway in the same way it will be called by the browser used for the web interface. We recommend using the server's complete host name (e.g., ndmgw.example.com). Enter the port number in the **Port** field (usually 443).

In the **Local Devices** section, you can specify whether client resources are connected in the session.



Your settings under **Local Devices** overwrite any analogous settings in the user properties. If connection of local devices is deactivated in your settings for the RDP session, these devices are not connected, regardless of any settings in the user properties defined in the operating system, or in the workstation's Local Devices settings.

The **RDP over NetMan SSL Gateway** section defines whether the NetMan SSL gateway is used. This is an additional NetMan component and must be installed separately before it can be used. For details, see "*Installing NetMan SSL Gateway.*" The SSL gateway provides a secure connection to your terminal server by using an SSL tunnel.

Under **Window/Audio Settings** you can define session properties such as window size, color depth, and audio support:

NetMan Web Services: Settings

Rules for Launch and Settings
You can define launch method and settings dependent on the client station. Specify the client station by its host name or IP address.

Client station(s)

IP address(es) : 192 , 168 , 188 , * to : . . .

Host name(s) : _____

with this browser agent : _____

You can use wildcards ("*") in defining IP addresses, host names and browser agents.

Launch Method

Launch application using : NetMan RDP Web client

Window/Audio Settings

Use seamless mode if possible

Apply user-defined ICA setting for the window size

Size as % of screen size : 80

Size in pixels : 1024 x 768

Full screen

Colors : True color (24-bit)

Audio support : Do not play sound files

This client supports the following functions:

- Session window in full-size mode
- Session window with specified width and height (e.g., 1024x768 pixels)
- Session window with size as a percentage of screen size (with reference to the workstation)
- Seamless mode (the user sees only the application window, not the session window)
- Supported colors: 256 colors, 15-bit high color, 16-bit high color, 24-bit true color
- Audio support
- Access to client drives from within the session
- Access to client printers from within the session
- Support for a universal PDF printer driver



There are a number of properties for an ICA connection that are rarely used and which cannot be configured in the dialogs shown above. You can enter these settings directly in the template file for the RDP session, `Standard.ndp`, in the `%NMHome%\WebSrv\HH\HTML-View\Launch\` directory. It might be necessary to modify the template. For example, you can integrate other plugins in the RDP protocol using the value stored in `PluginDLLs`. The starting program specified in `StartApp` is not launched if you have defined a program for users or in the RDP connection settings.

Java RDP Web Client

The *Java RDP web client* launch method is an RDP client developed in Java. With this launch method, an HTML page is generated with the RDP client embedded in the form of an applet. The NetMan Web Services use the `rdpjava.htm` file, in the `\WebSrv\HH\HTML-View\Launch\` directory, as the template for the HTML page.



The Java RDP Web client software is licensed under GPL. You can download the complete package from <http://www.hh-netman.de/javardp>. The `_download` directory contains the archives translated and signed by H+H:

- `properJavaRDP-1.2.32.jar`
- `HHJavaRDP-1.2.21.jar`
- `log4j-java-1.2.14.jar`
- `java-getopt-1.0.13.jar`

rdesktop over Java Applet

Implementation of an `rdesktop` session is particularly well suited for use with thin clients, because these machines generally are not equipped to execute the Java RDP web client.

The applet enables all of the functions implemented in `rdesktop`. Because `rdesktop` does not support seamless windows nor the universal printer as implemented in NetMan, the functions provided by these features are not supported when this launch method is used. Specifically, the following functions are not supported:

- Seamless windows
- Universal printer driver
- SSL tunnel for RDP sessions
- Session sharing
- Client printer
- Serial ports
- Smart cards

All other settings are supported.

With this launch method a JSON file is generated and processed in the browser by JavaScript. JavaScript creates the actual applet in the domain structure. The NetMan Web Services use the `rdpjava.json` file, stored in the `\WebSrv\HH\HTML-View\Launch\` directory, as the template for the JSON file.

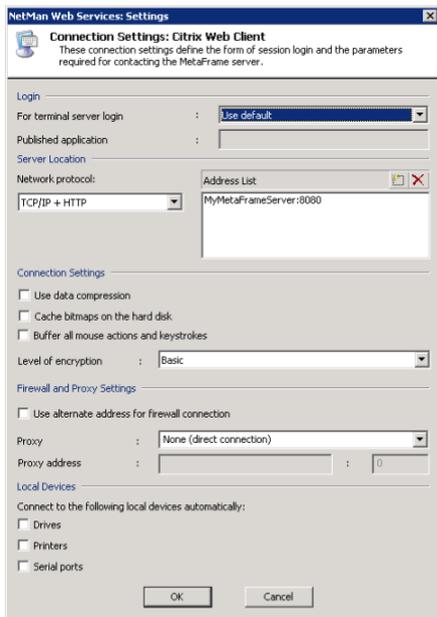
Citrix Web Client

With the *Citrix web client* launch method, the NetMan web services generate a configuration file for an ICA client. The ICA client then establishes the connection to a MetaFrame server.

You can configure the following settings for an ICA session:

- Connection settings
- Window/audio settings

To configure the connection settings, select the **Citrix web client** launch method and click **Connection Settings**. This opens the following dialog:



This manual does not go into detail concerning ICA-specific configuration options. The dialogs are generally adapted to those used in the Citrix Program Neighborhood and are described in the relevant Citrix manuals.

HTML View supports the following protocols:

- **TCP/IP:** The application is determined over UDP on the server on port 1604. This method is offered for the sake of compatibility with MetaFrame 1.8, and is no longer in general use.

- **TCP/IP + HTTP:** The application is determined over HTTP. This is the standard method for today's installations.
- **SSL/TLS + HTTPS:** With this setting, both the application determination and data traffic in the ICA session run in an SSL tunnel (Citrix Secure Gateway in relay mode).

In addition to the native connection between server and client on TCP/IP port 1493, HTML View also supports other operating modes for the connection between the Citrix Web client and the MetaFrame server:

- Proxy with HTTPS
- SOCKS proxy

You can also modify the connection settings. In this case, a different form of login is used than the one you selected for the MetaFrame server. It might also be a good idea to choose a different published application under Citrix.



With different published applications and connection settings for the launch rules, you can link different Citrix farms with a single instance of HTML View. For example, the employees in a university library can use a different server farm than that used by the students, who access HTML from across the campus through a server farm in the digital media center.



Citrix sessions are always called using the published applications mechanism. With this technique, load balancing with the ICA protocol can also be supported by NetMan. With the default settings, NetMan uses one Citrix published application (see "*Published Application*" in the section entitled "*Extensions for MetaFrame Servers*"). Prerequisite is that all applications are installed on all servers for correct functioning of load balancing under Citrix. If this is not possible, you can configure the published application in the NetMan configurations. For information on this option, please see "*Separate Session Parameters for an Application Call*" in the chapter entitled "*Advanced Application Settings for a Session*."

Under **Window/Audio Settings** you can define session properties such as window size, color depth, and audio support:

NetMan Web Services: Settings

Rules for Launch and Settings
You can define launch method and settings dependent on the client station. Specify the client station by its host name or IP address.

Client station(s)

IP address(es) : 192 , 168 , 188 , * to : . . .

Host name(s) : _____

with this browser agent : _____

You can use wildcards ("*") in defining IP addresses, host names and browser agents.

Launch Method

Launch application using : Citrix Web client

Window/Audio Settings

Use seamless mode if possible

Apply user-defined ICA setting for the window size

Size as % of screen size : 0

Size in pixels : 1024 x 768

Full screen

Colors : High color (16-bit)

Audio support : Do not play sound files

This client supports the following functions:

- Session window in full-size mode
- Session window with specified width and height (e.g., 1024x768 pixels)
- Session window with size as a percentage of screen size (with reference to the workstation)
- Seamless mode (the user sees only the application window, not the session window)
- Supported colors: 16 colors, 256 colors, high color (16-bit), true color (24-bit)
- Audio support
- There might be a proxy or a firewall between the workstation and the MetaFrame server
- Access to client drives from within the session
- Access to client printers from within the session



There are a number of properties for an ICA connection that cannot be configured in the dialogs shown above. You can configure these settings directly in the template file for the ICA session launch, `Standard.ica`, in the `%NMHome%\WebSrv\HH\HTML-View\Launch\` directory.

Before the ICA data is sent, NetMan web services replace the `@NM` placeholders with specific values.

Citrix Java Client

With the *Citrix Java client* launch method, the NetMan web services generate an HTML page that contains a Java applet for a Citrix session. The Connection Settings and Window/Audio Settings options are the same as those available for the Citrix web client. Please refer to the documentation available from Citrix for details.

The web services use the `citrixjava.htm` file in the `%NMHome%\WebSrv\HH\HTML-View\Launch\` directory for the HTML page. As a rule, it is not necessary to modify this file. You can edit it if desired, however, to adapt it to your preferences.



In addition to the `Citrixjava.htm` file, this directory also contains a file called `Citrixjava mit ICA-Datei.htm`. The only difference between these two templates is that in the latter, the connection settings are loaded in an additional file while the former (`Citrixjava.htm`) passes all required connection parameters directly to the Java Applet. If you wish to use the version with the additional ICA file, simply change the name `Citrixjava mit ICA-Datei.htm` to `Citrixjava.htm`.



The `used_archiv` variable contains the Java archives for the applet. For example, if access to client drives is deactivated, the associated archives are not linked in the applet.

When you use the Citrix Java client launch method, no additional installation of Citrix client software on the client machine is required. The only prerequisites are prior installation of the Java Runtime Environment and Java support in the browser.

Select ICA Automatically

With the *Select ICA automatically* launch method, the NetMan web services generate an HTML page with Java scripts that automatically determine whether or not a Citrix web client is installed on the client computer. If the client is found, the Citrix web client launch method is used. If not, the Citrix Java client is used.

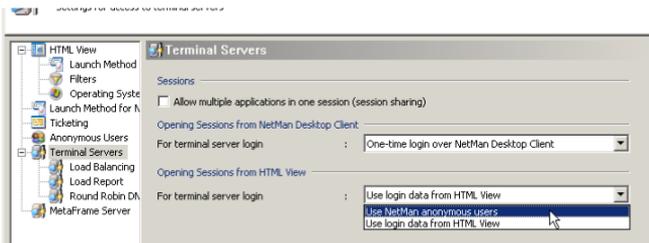
The Connection Settings and Window/Audio Settings options are the same as those available for the Citrix web client and the Citrix Java client. As a rule, you do not need to modify the `citrixautodetect.htm` file. If the Java scripts do not meet your requirements, however, you can modify them as needed.

Login Methods for HTML View

Providing access to application sessions is one of the main tasks for NetMan. Before users can begin an application session, however, they must meet requirements for authentication on the terminal server. When access is provided through HTML View, NetMan provides a choice of options for authentication:

- Use login data from HTML View
- Use NetMan anonymous users

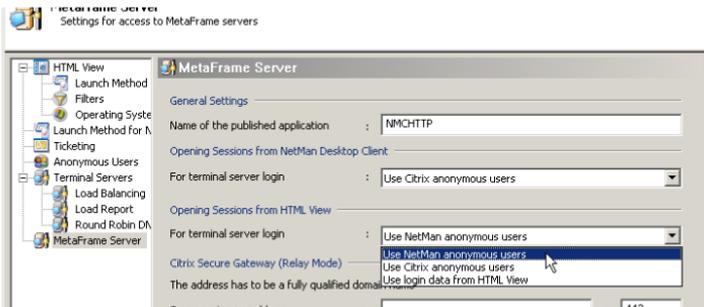
These settings are configured in NetMan web services. Run the NetMan Web Services Settings program from the Toolbox and open the **Terminal Servers** page. Select the desired login method in the **Opening Sessions from HTML View** section:



If the terminal server is accessed over ICA on a MetaFrame server rather than over RDP, the login method is configured on the **MetaFrame Server** page of the NetMan Web Services Settings program. The following options are available:

- Use NetMan anonymous users
- Use Citrix anonymous users
- Use login data from HTML View

Select the desired option under **Opening Sessions from HTML View**:



The different methods are described in detail in the following sections.

Use Login Data from HTML View

When the web interface is opened, the user is prompted to log on to NetMan HTML View. This is either a domain logon or logon on a non-networked terminal server. The **user name** and **password** can be taken from the login dialog and used for authentication in the terminal server session.

To use this feature, select **Use login data from HTML View** under **For terminal server login** on the **Terminal Servers** page. From that point on, terminal server sessions are opened over RDP using the login data already entered by the user.



To ensure optimum security, the login data for sessions is not saved in user's session data; rather, a ticketing mechanism is used for authentication in terminal server sessions. When the web services send a request for session to a client, a single-use ticket is issued. The user designation uses the form @@GUID (for example, @@5CFB2335-A315-48EC-AFBA-4BE91A87BA) and can open only one session. The session runs under the user account that logged in on HTML View.

Use Citrix Anonymous Users

If you select **Use Citrix anonymous users** under **Opening Sessions from HTML View** on the **MetaFrame Server** page of the NetMan Web Services Settings, anonymous user accounts configured in Citrix are used for login on application sessions. As with NetMan anonymous users, the advantage here is that you can provide access to application sessions for a large number of users without maintaining a lot of login data on the terminal server.



Please note that anonymous users from Citrix are created only in the local user database of the MetaFrame server. Thus these accounts can be used only on this particular MetaFrame server. If you want to provide user access in a domain, we recommend using NetMan anonymous users.



With this login method, the user names recorded in log files and used for licensing are taken from the names provided by H+H Authentication Services for HTML View.

Use NetMan Anonymous Users

Rather than using a specific user account, terminal server sessions can be opened by NetMan anonymous users. This feature is configured on the **Terminal Servers** page of the Web Services Settings. Under **For terminal server login** in the **Opening Sessions from HTML View** section, select **Use NetMan anonymous users** and save the change. From this point on, all sessions run under a NetMan anonymous user account. This feature requires configuration of anonymous users in your NetMan installation, the procedure for which is described in detail in the section "*Anonymous Users.*"

Anonymous Users

NetMan offers its own *anonymous users* feature in terminal server environments. Anonymous users are typified user accounts for authentication in terminal server sessions. This mechanism is particularly useful if you provide applications for a large number of users for whom accounts cannot or should not be maintained explicitly in the Windows user database. Classic uses include the following:

- Providing a single ERP application for all suppliers or potential customers
- Providing applications in the intranet
- Allowing access to a library catalog for employees or for other universities
- Centralized presentation of CD-ROM/DVD databases for a university campus or the information management department of a company

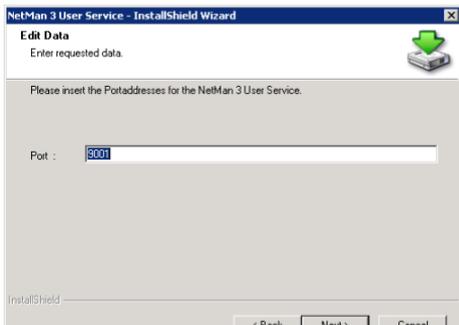
If you select **Use NetMan anonymous users** for the terminal server login method, application sessions are opened with the login data from anonymous user accounts. The following configuration steps must be completed before you can implement NetMan anonymous users:

- Install and configure the NetMan user service
- Set up the anonymous user accounts

Installing and Configuring the NetMan User Service

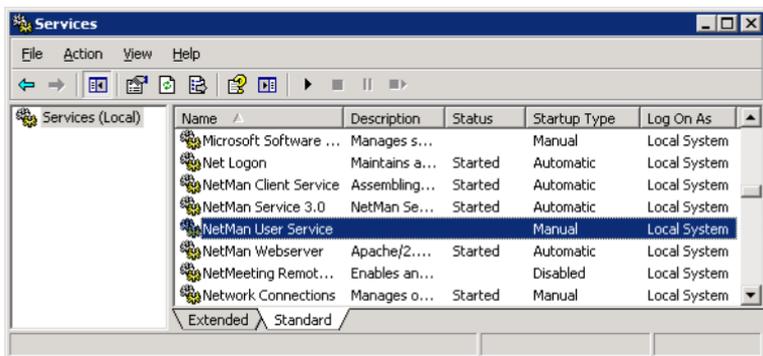
NetMan offers you the option of working with anonymous users. The NetMan User Service sets the passwords for anonymous users. Following installation of NetMan, the `<%NMHOME%\WebSrv\HH\HTML-View\Setup.NetMan User Service` directory contains the setup program for the NetMan User Service.

1. Run `Setup.exe` from that directory, preferably on the same server on which NetMan is installed. You are prompted to specify a port for the NetMan User Service. Enter any available port. The default is port 9001; this port is usually available on Windows servers:

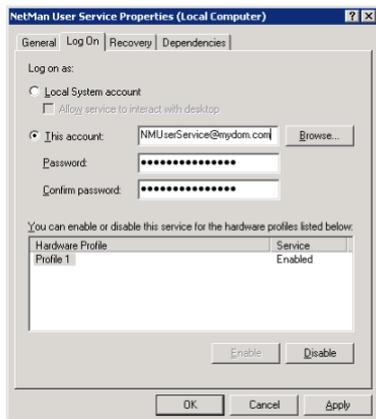


2. Start the installation by clicking the **Next** button.

3. Once this installation is completed, the NetMan user service is listed under **Services** in your Computer Management program:

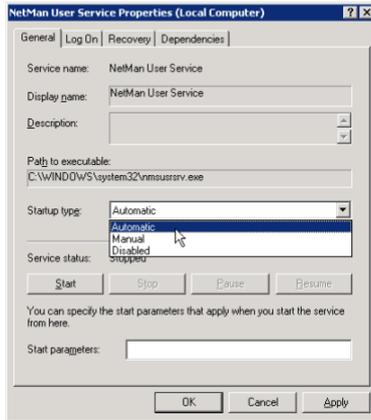


4. The service startup type is set to **Manual** and it has not been started because the service has not been configured. To ensure that this service has the right to set passwords for anonymous users, set up a separate account for this purpose and grant it Account Operator rights in the anonymous accounts. For example, you might create an OU in which the anonymous users are stored and grant the account for the NetMan User Service the right to set passwords for this OU. Then enter this account in the service properties, on the **LogOn** page:



If you want to create the anonymous users in the local user database on a terminal server, you do not have to set up a separate account; the service can use the system account.

5. Now you can change the **Startup Type** on the **General** page from **Manual** to **Automatic** and start the service:

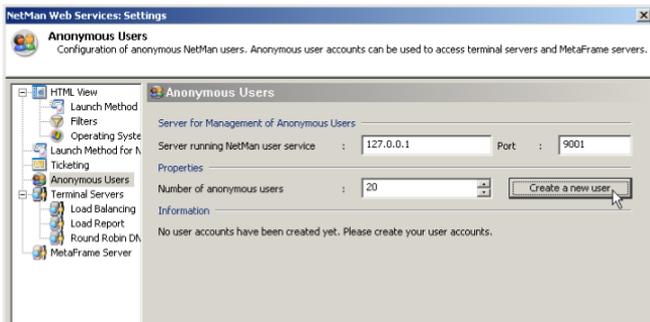


The NetMan User Service uses an NT4 domain interface to set passwords. If you use Active Directory (AD), make sure a PDC emulator is accessible.

Initial Setup of Anonymous User Accounts

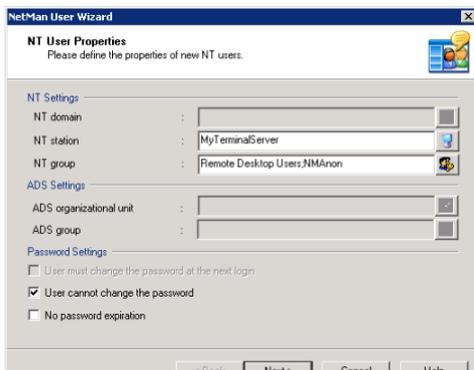
One of the main features in NetMan Desktop Manager is the use of *NetMan anonymous users*. Whether you want to create new anonymous user accounts or configure existing ones, you need to begin by running the NetMan Web Services Settings program and opening the Anonymous Users page. The procedure for setting up anonymous user accounts is described in the following. The subsequent section, “*Anonymous Users: Settings*,” provides a detailed description of the configuration options for anonymous user accounts.

1. To set up anonymous user accounts, run the NetMan Web Service Settings program and open the **Anonymous Users** page:



2. The **Information** section contains a message on the current status of your anonymous user accounts; in this example: “No user accounts have been created yet. Please create your user accounts.” Under **Number of anonymous users** enter the desired total number of anonymous users. The number entered here should not exceed the total number of parallel sessions permitted on the server.

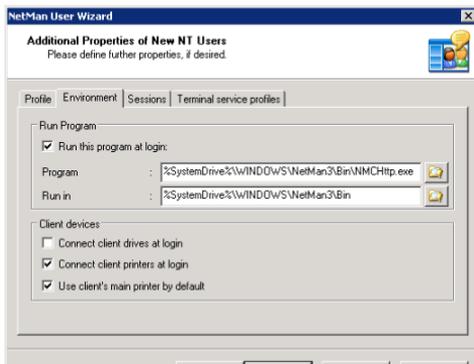
3. Click the **Create a new user** button to open the User Account Wizard:



4. Specify the properties for the users:

- The user accounts are created on the terminal server (in this example, “MyTerminalServer”).
- These users must belong to the Remote Desktop Users group. Furthermore, you should set up a NetMan group (e.g., “NMAnon”) for these users; this will make administration much easier, as you will see later in this example.
- Users should not be permitted to change the password.

5. Click **Next** to continue. This opens a dialog for defining additional user properties:



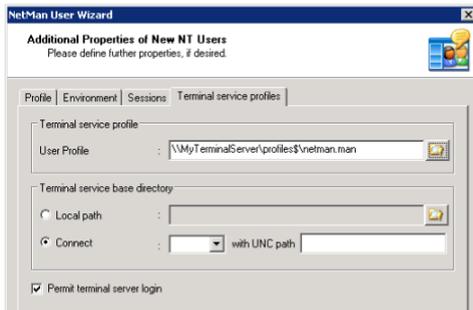
Only the main settings are described here, not all of the available options:

On the **Environment** page, enter `<SystemRoot>\NetMan3\Bin\nmchttp.exe` as the program to run when an anonymous user logs on. This ensures that anonymous users can launch only those applications that are controlled by NetMan. In this case, anonymous users cannot run other applications over RDP because the system ignores any attempt on the users' part to launch another program.

The following aspects need to be configured at the terminal server end:

- Group policies for anonymous users
- Profiles for anonymous users

Once configured, allocate these to your anonymous users:



For a detailed description of the settings in the User Account Wizard, please see the section entitled “*Anonymous Users: Settings.*”

Anonymous Users: Settings

Once you have created anonymous user accounts (as described in the previous section), there are a number of options available for their configuration. Whether you want to create new anonymous user accounts or configure existing ones, you need to begin by running the NetMan Web Services Settings program and opening the **Anonymous Users** page:



In the **Management on** section, enter the server on which your NetMan user service is installed. This is usually the same server on which NetMan is installed, in which

case you can accept the default IP address: 127.0.0.1. When you install the NetMan user service you are prompted to specify the port to be used by the service. The port specified there must also be entered here. The default port, 9001, is also the default when setting up the NetMan user service. In the **Properties** section you can define the desired number of anonymous users. This should be the same as the total number of parallel sessions you wish to permit. For example, if your terminal server supports a maximum of 40 parallel sessions, you can create 40 anonymous users. In a server farm with 3 servers that each support 30 parallel sessions at any one time, you can create 90 anonymous users.



Users created in this manner are assigned the user name "NMANONxxx," where "xxx" is a number from "000" up to the total number of users minus 1.

The **Information** section shows whether anonymous users have been created and, if so, where the accounts are located. The messages look something like this:

- "20 user accounts have been created in the MYDOM domain."
- "20 user accounts have been created on the MYSERVER server."
- "No user accounts have been created yet. Please create your user accounts."



If the message shown here is "No user accounts have been created yet. Please create your user accounts," you cannot open sessions for anonymous users.

Click the **Create a new user** button to run the User Account Wizard:

In the first dialog, specify where the user accounts are created, indicate group membership and define the password settings. The following fields are available here:

NT domain. To create the user accounts in an NT4 domain, enter the domain here.

NT station. If you use only one terminal server, you can create the anonymous user accounts in the server's local database. To do this, enter the name of the terminal server here.

NT group. The anonymous users can belong to one or more groups. Specify the membership(s) in the NT groups field. Your anonymous users should at least belong to the Remote Desktop Users group, so that they can execute sessions on the terminal server. Furthermore, we recommend creating a group called “NMAnon” to which all anonymous users belong. This simplifies management of anonymous users; for example, when you allocate binding profiles.

ADS organizational unit. You can create user accounts in an Active directory (AD) if desired. The ADS organizational unit field lets you specify the OU in which you wish to create the user accounts.

ADS group. In this field you can specify group membership of your anonymous users in the AD. The same recommendation applies here as is given above under NT group.

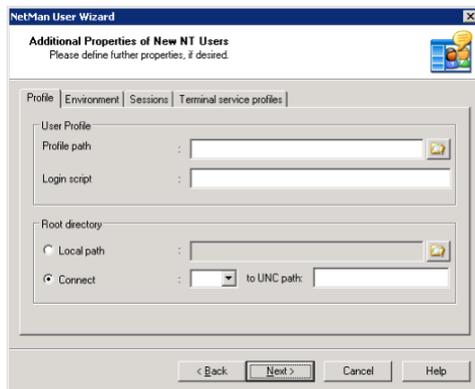
User must change the password at the next login. This setting must be deactivated for anonymous users.

User cannot change the password. This setting must be active for anonymous users.

No password expiration. This setting must be deactivated for anonymous users.

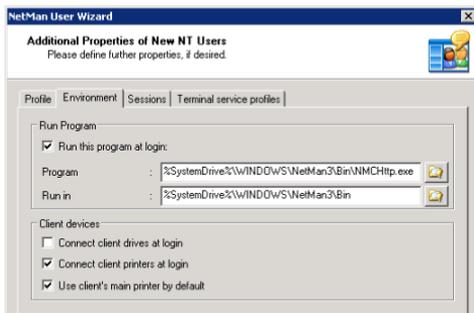
The password settings are made available here because passwords are set automatically by the NetMan User Service, and generally do not need to be—and should not be—changed by the user.

Click **Next** to continue to the next dialog. Here you can set additional properties, corresponding to the settings configured in Windows user administration:



On the **Profile** page you can set properties such as user profile, login script and root directory. These settings do not exclusively pertain to terminal server use, but also to general properties configured for users in the LAN. Since the anonymous users are required only for terminal server sessions in which the login is not generally performed on the local computer, however, you can leave these fields blank.

The **Environment** page has settings that apply only to terminal server environments:



Under **Run this program at login** you can define whether or not a particular program is launched when the user logs on. This setting should be configured for anonymous users and entered in the `<windir>\NetMan3\Bin\nmchhttp.exe` program. If no program is specified here, the program to be launched may be specified by the client. If the client does not specify a program, the Windows Explorer is launched automatically on user login. If either of the first two variants applies, the user sees only the program that is launched. In the third case, the user sees the entire Windows desktop. The first two are application sessions; the third is a desktop session.

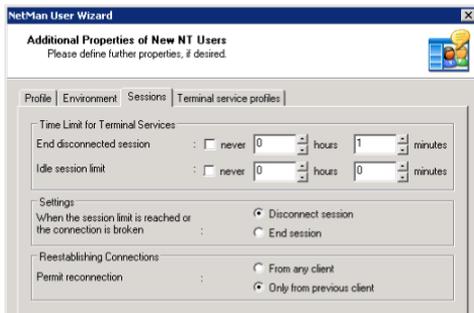
When a session is launched by user login, the terminal server can make certain resources available to the user:

Connect client drives at logon. This setting is applied only in sessions that use the ICA protocol. All local drives on the workstation are automatically connected within the session.

Connect client printers at logon. All printers used by the workstation are automatically connected within the session.

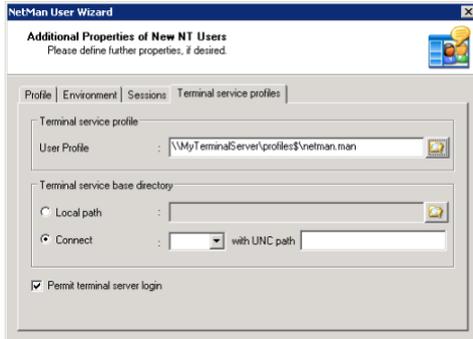
Default to main client printer. With this setting, the main printer as configured on the workstation is the default printer for the session.

On the **Sessions** page, you can configure a number of session properties:



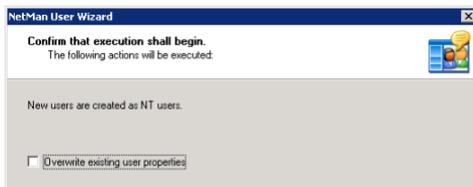
For example, you can define how long the session remains active when not in use. When the defined period has elapsed (“Idle session limit”) the session is disconnected or ended. You can also define what happens when a session is disconnected. Specifically, you can define whether the session can be re-connected only by the client that initially established the connection, or by any client.

The **Terminal service profiles** page corresponds for the most part to the “Profile” page, with the exception that these settings apply only to terminal server sessions:



We recommended assigning a binding profile that limits the Windows desktop to the applications you wish to provide. The **Permit terminal server login** option must be selected.

The last dialog prompts you to indicate whether you wish to create new users or overwrite the properties of existing users:



If you have already created anonymous users, we recommend overwriting existing properties rather than creating more users. On the **Anonymous Users** page of your NetMan Web Services Settings program, the **Information** section shows how users were created, and the domain or server.



Even when you work with anonymous users, NetMan can still compile differentiated usage statistics. To make use of this feature, the NetMan Access Control program can allocate user names to IP addresses or host names for the NetMan Desktop Client, which are recorded for both statistics and the evaluation of user privileges.

Authentication Services

If you want to restrict access to HTML View by limiting it to a specified set of user names, IP addresses or host names, you need to configure and activate H+H authentication services.

You can configure access restrictions on two levels:

- The higher-level restriction is based on *IP address/host name*. When you use the IP authentication service, all stations within a specified range of addresses are permitted access with no login required.
- The second level of restriction is based on *user login*.

When controls are active on both levels, users are prompted to log on only if they request access from a machine outside the defined IP address/host name range. If only the IP-authentication service is active, stations that are outside the defined IP address/host name range(s) cannot access the system. If only user logon services are active, all users are prompted to log on.

How the Authentication Services Work

H+H authentication services are implemented using a module in the NetMan web server. With the default settings, the authentication mechanism defined by the configuration program applies to all HTML virtual directories created during installation. In particular, the required commands are inserted in the `\WebSrv\HH\HTML_View\bin\NMView.conf` file for all virtual directories that contain the markers:

```
### Start-Authentication
### End-Authentication
```

The settings program enters all configured H+H authentication services for each of these directories.



If you wish to define separate access conditions for individual URLs, you can do this by editing the virtual directories in the web server configuration files. The commands written by the H+H Authentication Services configuration program provide examples.



Changes in the H+H Authentication Services settings are not effective until the NetMan web server is restarted.

The configuration program for H+H authentication services can be opened from the **Settings** folder of the NetMan Toolbox.

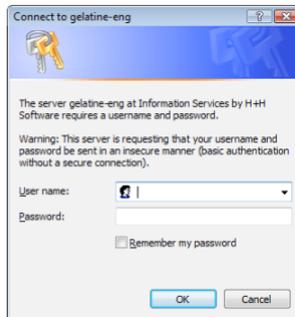
Authentication Page

Run the configuration program for H+H Authentication Services from the NetMan Toolbox:

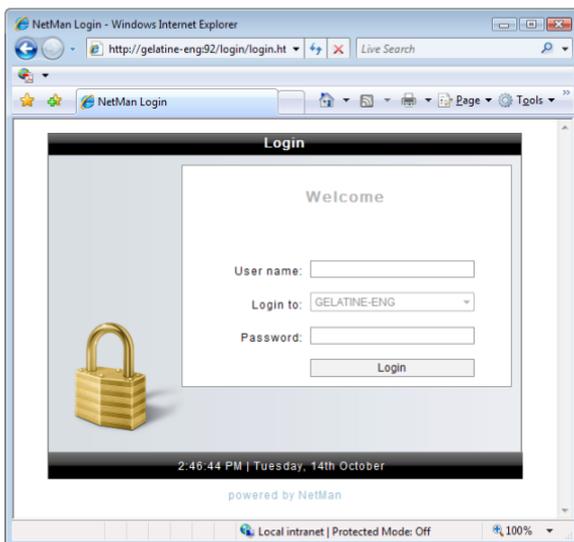


The **Use authentication services** option lets you switch authentication on and off. This option must be selected before you can configure services. In the **Login** section, you can specify whether login is implemented in an HTTP login box or an HTML form.

If you choose login over HTTP, you can configure the text for the title bar of the login box:



With an HTML form login, you can use your own form, once you have copied it to the `\WebSrv\HH\common\login\` directory, or use the default form stored there (`\login\login.htm` or `login\login.htm`):



With the **If permissions are insufficient, show login page** setting, the HTML login form specified in the settings will automatically open if the user does not have permission to open the requested application. This gives the user an opportunity to log in with other data. If this option is not active, access is simply denied if user privileges are insufficient.

Below these two fields is a table showing the defined authentication services. At the top of this table on the right-hand side are operating elements that let you create, delete, edit and move entries in this list. The entries are processed in the order in which they appear in this table, from top to bottom (with one exception; see below). Users are logged on with the first applicable set of conditions found. Regardless of the entry positions in this list, IP/host name assessment services are processed first, and thus take precedence over other services defined here.

The table includes the following columns:

Active. Click here to activate or deactivate an authentication service.



If you deactivate an entry in this list—for example, for test purposes—that entry is automatically moved to the bottom of the list. When you reactivate the entry, it is not automatically returned to its previous position. You can use the arrow buttons in the upper right-hand corner to move entries up and down in the list.

Authentication service. You can enter a name of your choice for the service.

Designation. Enter a brief ID for unique identification of the service. This is the ID used to address the service internally. Each ID must be unique. In other words, no ID may appear more than once in this column.

Module. Select the DLL file for the desired authentication service. The authentication services provided by H+H are stored under \WebSrv\HH\Common. All authentication service file names begin with auth_. For an overview of available services, please see “Configuring Different Types of Authentication Services”.

Parameter. Each authentication service requires specific parameters which have to be defined when creating or editing the service. Parameters defined for the modules supplied by H+H—which must conform to a special syntax—can be loaded by clicking on the **Load** button in the **Create/Edit Authentication Service** dialog.

The example below shows a ready-to-use authentication service for NT user logon:

NetMan - HTML View - Authentication Services

Edit Authentication Service

Authentication service : Windows NT Login

Designation : NT

Module : C:/NetMan3/webSrv/hh/common/auth_nt.dll ...

Use persistent cookies for login Duration: 0

Parameters

Name	Value
DefaultDomain	MyDomain

Load New... Edit... Delete

OK Cancel

Configuring Different Types of Authentication Services

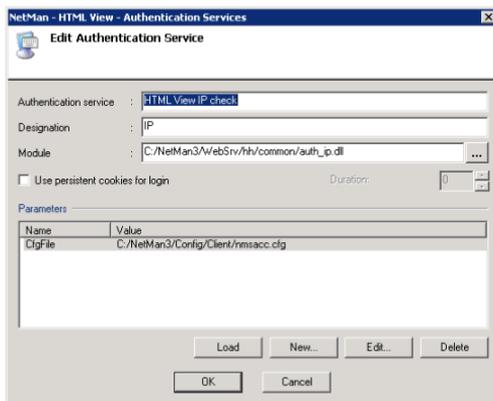
The following chapters explain which authentication services NetMan supports and how you can configure them:

- IP Address/Host Name Check
- LDAP-Login
- NT Login
- ADS Login
- NetMan Login
- PICA Login (CBS)
- PICA Login (LBS)
- SISIS Login
- ALEPH Login
- ODBC Login
- STAR Login
- SIP2 Login
- NT Challenge/Response Login

IP Address/Host Name Check

In this example, we will configure an authentication service that identifies clients by IP address or host name.

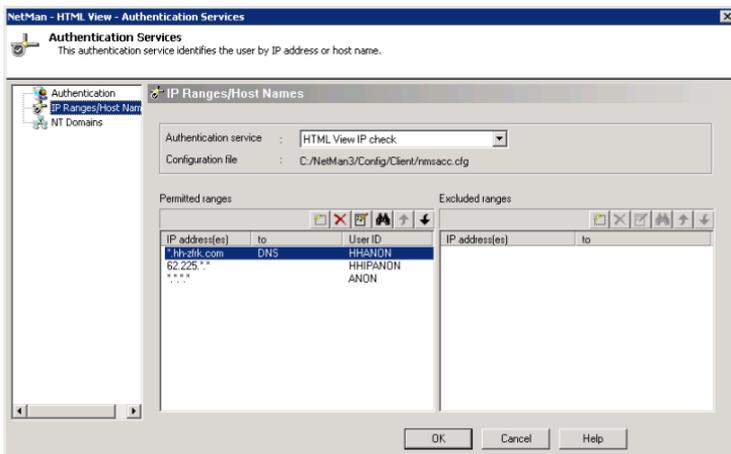
1. To do this, click on the “New” button and, in the Module field, enter `auth_ip.dll`. The parameter entered is the name of a file which lists computer addresses:



If your users access both NetMan HTML View and the NetMan Desktop Client, and you wish to apply the same access controls for both interfaces, enter the full name of the `nmsacc.cfg` file as parameter: `<NetMan installation>\Config\client\nmsacc.cfg`. For more details, see also “Configuring the Authentication Service.”

2. The next step is to open the **IP Ranges/Host Names** page.

3. In the **Authentication service** field, enter the name of the service you have created for this purpose. The dialog page should appear as follows:



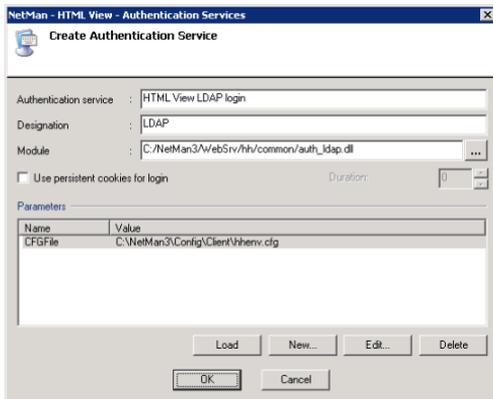
The name of the selected service and the file assigned to it are shown at the top of this page. Below this are two lists; showing permitted and excluded addresses or host names. The authentication service detects the client IP address and compares it to these lists in the following order:

1. List of permitted host names and IP addresses (including ranges of addresses)
2. List of excluded host names and IP addresses

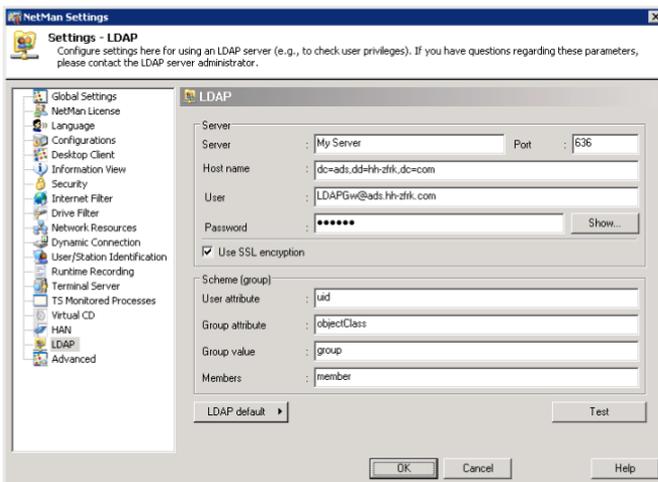
Each list is scanned sequentially. The first match found under Permitted ranges for the client in question is applied, which means the order in which addresses/names are listed is significant. Then the **Excluded ranges** list is checked for the client's IP address. If a NetMan user ID is assigned to the applied entry, the user is logged on to your system under that user name; the same ID is used for evaluation of privileges and identification in log files.

LDAP Login

1. For an LDAP login, select the `auth_ldap.dll` module. The parameter for this service is the `hhenv.cfg` file, which is stored in the `<NetMan installation>\Config\Client\` directory. The file name must be entered with the explicit path name, rather than entering the `%NMHome%` variable:



2. The configuration file, `<NetMan installation>\Config\Client\hhenv.cfg`, is configured in the NetMan Settings program:



Proceed as follows to configure the LDAP interface:

1. Enter the data relating to the LDAP server you wish to use:
 - Server = Name of the LDAP server
 - DN = Distinguished name of the directory in which users are stored
 - User = User name for LDAP server logon
 - Password = Password for LDAP server logon
 - Use SSL encryption
2. Click on LDAP default to choose one of two group schemes:
 - Microsoft LDAP server, or
 - Netscape LDAP server
3. When you double-click on the selected server, the corresponding attributes are inserted:
 - User attribute = This value is used to depict the user name in the corresponding user DN
 - Group attribute = Name of the attribute
 - Group value = Indicates whether this is a group or not
 - Member = Attribute in which the members are defined



Because LDAP settings are configured in the NetMan Settings program, LDAP rights to NetMan configurations can be assigned in the NetMan Management Console.

NT Login

NT login is implemented over the `auth_nt.dll` module. This service requires only the `DefaultDomain` parameter, which lets you define which NT domain is the default for authentication. Users can also log in on a different domain by enter the full login name (`<domain\user>`). This module uses an old NT4 interface for login.

Alternatively, you can use the `auth_ntads.dll` module. This module requires the same parameter as `auth_nt.dll`. The only difference between these two services is that the `auth_ntads.dll` module uses an AD interface for login.



If you work in an all- NT4 environment, we recommend using the `auth_nt.dll` module. In all other cases, the `auth_ntads.dll` module is preferable.



If you have multiple domains but have not established trusts, users are authenticated only against the domain which contains the server on which HTML View is installed.

ADS Login

If you want to offer your HTML View users an option for ADS login, select the `auth_ads.dll` module. The parameter required by this service is called an “object.” Login is performed on this ADS object.

Format of the object parameter:

For ADS: LDAP://HostName[:PortNumber][/DistinguishedName]

For NT4: WinNT://DomainName[/ObjectName[,className]]

or

WinNT://ComputerName,computer]

NetMan Login

You can utilize the NetMan user database for login, as well as individual user accounts. When configuring the authentication service, select the `auth_netman.dll` file as the module. The parameter for this service is the NetMan home directory; i.e., the path stored in `%NMHome%`.



Normally, the NetMan user database is filled automatically when users log in under their user names. The associated password field, however, is blank. Since a system login without a password cannot be implemented, you need to assign passwords for your users when you use the NetMan user database for login. Alternatively, you can import users from another database.

PICA Login (CBS)

There are two forms of PICA login support, known as CBS and LBS. CBS stands for “Central Bibliothek System” (Central Library System) and LBS stands for “Local Bibliothek System” (Local Library System). The `auth_pica_cbs.dll` module implements login on CBS. This service communicates with the PICA system over HTTP. The following parameters are required:

- `Server`: The server on which the PICA system is installed.
- `Port`: The port on which the server accepts requests.
- `URL`: The URL to be used.
- `URLBibliothek`: Can be used to filter for users of a specified library.



Because the central server for CBS is generally not located on your premises, but rather in a computer center that is accessed over the Internet, you may need to check and make sure the communication between the login service and the PICA server is not hindered by a firewall.

PICA Login (LBS)

If you want to provide your users with an option for login on your local PICA library system, select the `auth_pica_lbs` under **Module** when configuring the login service. The following parameters are required for this service:

- **DSN:** Indicates the ODBC source to be used.
- **DBUser:** The account used by the service to log in on the database.
- **DBPasswd:** Contains the password for the DBUser account.
- **Library:** Can contain a library ID (ILN). When you enter the ID of a library for this parameter, users are permitted access only to that library.

Following successful login, two NetMan environment variables are available:

- **PicaLibrary:** Contains the library ID (iln) for the user who is logged in.
- **PicaUserType:** Indicates the user type (borrower_type) for the user who is logged in.



To set up the DSN, please follow the instructions given in the corresponding database. Make sure it is a system DSN. PICA systems generally use a Sybase database.



You can set up a number of separate login services with different ILNs.

SISIS Login

If you use SISIS, you can use the SISIS database for user login on HTML View.

To do this, select the `auth_sisis.dll` file under **Module** when configuring the login service.

This service requires the following parameters:

- **DSN:** Indicates the ODBC source to be used.
- **DBUser:** The account used by the service to log in on the database.
- **DBPasswd:** Contains the password for the DBUser account.

Following successful login, three NetMan environment variables are available:

- **SisisGroup:** Contains a user group (corresponds to the “d02bg” field).
- **SisisPLZ1:** Contains a postal code for the user (corresponds to the “d02p1” field).

- **SisisPLZ2:** Contains another postal code for the user (corresponds to the “d02z_plz” field).



If one of the inhibit zones (d02sp1, d02sp2, d02sp3, d02sp4, d02sp5) contains the value 01, 02, 04, 05, 06, 14, or 17, access is denied and the login fails.



To set up the DSN, please follow the instructions given in the corresponding database. Make sure it is a system DSN. SISIS systems generally use a Sybase database.

ALEPH Login

If you use the Aleph Library System, you can utilize the Aleph database for login on HTML View. To do this, select the `auth_aleph.dll` file under Module when configuring the login service. This service requires the following parameters:

- **DSN:** Indicates the ODBC source to be used.
- **DBUser:** The account used by the service to log in on the database.
- **DBPasswd:** Contains the password for the DBUser account.



If one of the inhibit zones (Z305_DELINQ_1, Z305_DELINQ_2, Z305_DELINQ_3, Z303_DELINQ_1, Z303_DELINQ_2, Z303_DELINQ_3) contains a value that does not equal 0, access is denied and the login fails.



To set up the DSN, please follow the instructions given in the corresponding database. Make sure it is a system DSN. Aleph generally uses an Oracle database and access over ODBC, which requires prior installation of an Oracle client.

ODBC Login

In addition to the predefined modules, you also have the choice of using the generic `auth_odbc.dll` module. This authentication service compares the user name and password to a table in a database. With this module, you can specify the names of the database, the table and the fields. Passwords for user accounts must be stored in plain text. This authentication service uses the following parameters:

- **DSN:** Indicates the ODBC source (and hence the database) to be used.
- **DBUser:** The account used by the service to log in on the database. This account must have access rights in the table that contains the user data.
- **DBPasswd:** Contains the password for the DBUser account.
- **TableName:** Contains the name of the table with the user data.
- **UserField:** Name of the field for the user name.

- **PasswdField:** Name of the field for the user's password. The password has to be stored in plain text.

STAR Login

If you use the STAR library system, you can utilize the STAR database for login on HTML View. To do this, select the `auth_starxml.dll` file under Module when configuring the login service. This service requires the following parameters:

- **Server:** The IP address or the host name of the server to be used.
- **Port:** The port for communication with the STAR server.
- **CodeLength:** Defines the number of characters (from the user code) to be utilized by NetMan for a user name. If this value is 0, all characters in the code are used for the user name.

Following successful login, a variety of user information is made available to NetMan:

- **StarCode:** User code of the logged-in user
- **StarLocation:** Location for the logged-in user
- **StarEMail:** E-mail address of the logged-in user



The XML request for a database query is stored in the `starreq.xml` file. The `%USER%` string in this file is replaced by the user name entered in the login form.



The locations for which login is permitted are specified in the `starallow.cfg` file. Each line contains exactly one location. If this file is not found or contains no data, then all locations are permitted.

SIP2 Login

You can use an SIP2 server for authentication in HTML Client. Prerequisite is the availability of the SIP2 server directly over a socket. Telnet emulation for SIP2 is not supported. To use SIP2, select the `auth_starxml.dll` file under Module when configuring the login service. This service requires the following parameters:

- **Server:** The IP address or the host name of the server to be used.
- **Port:** The port for communication with the SIP2 server.
- **User:** User name for login on the database.
- **Password:** The password for the User account for login on the database.



Following successful login, an `SIP2_STATUS` variable becomes available in the NetMan environment. The user status is indicated in a 14-character string. Each position can have either a Y or an N. The meaning of the fields can vary.

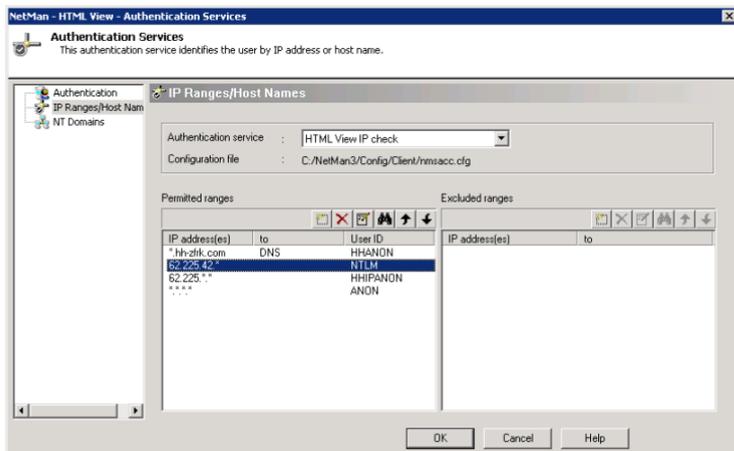
NT Challenge/Response Login

The NT-Challenge/Response method is used for login on a Web server. This method uses HTTP for login and presents an alternative to the basic authentication method. With the basic method, user name and password are Base64-encoded and passed to the Web server. Anyone who can tap the connection between browser and Web server can read this information. NT Challenge/Response employs a one-way hash process to protect the password during transit between client and server.

When using the MS Internet Explorer, the NT Challenge/Response method offers the option of performing transparent login; i.e., the login data already registered for the user on the workstation is used automatically, without requiring the user to login again. This only works, however, if the Web server belongs to the user's local intranet zone. If the Web server is not within the user's intranet zone, interactive user login is required.

The Apache module, `auth_sspi`, gives you the option of using NT Challenge/Response authentication with the Apache server. Since the original `auth_sspi` module cannot be used with H+H authentication services, the latest version of `auth_sspi` has been expanded to include support for H+H authentication services.

The NT Challenge/Response method cannot be used in combination with a login form. For this reason, this method is combined with the H+H *IP address/host name check* authentication service. Within the *IP address/host name check* service, you can specify a range of IP addresses for which the NT Challenge/Response method is applied. This requires prior configuration of an IP login service with the *IP* designation. When you add an IP address range to your IP Check service and assign it the user name *NTLM*, IP addresses within the specified range are logged in using the NT Challenge/Response authentication method:



To integrate the new version of the `auth_sspi` Apache module, you need to modify the `httpd.conf` and `NMView.conf` files:

1. The first step is to add the module in Apache. Enter the following in the `hhauth.conf` file:

```
LoadModule sspi_auth_module "C:/NetMan3/WebSrv/hh/common/mod_auth_sspi.so"
```

2. Options for a number of virtual directories must also be set in the `NMView.conf` file:

```
001 LoadModule nmfilter_module "C:/NetMan3/WebSrv/hh/HTML-View/bin/mod_nmview.dll"
002
003 Alias /_download/ "C:/NetMan3/WebSrv/hh/HTML-View/_download/"
004 <Directory "C:/NetMan3/WebSrv/hh/HTML-View/_download">
005     AuthType SSPI
006     ### Start-Authentication
007     AuthType Basic
008     AuthName "Example of an authentication service"
009     HHAAuthEnable on
010     HHAAuthDefaultProvider IP
011     HHAAuthProvider IP
012     HHHTMLAuthEnable on
013     HHAAuthLoginUrl /login/login.htm
014     require valid-user
015     ### End-Authentication
016         Options FollowSymLinks
017         AllowOverride None
018 </Directory>
019
020 Alias /_images/ "C:/NetMan3/WebSrv/hh/HTML-View/_images/"
021 <Directory "C:/NetMan3/WebSrv/hh/HTML-View/_images">
022     AuthType SSPI
```

```
023   ### Start-Authentication
024   AuthType Basic
025   AuthName "Example of an authentication service"
026   HHAAuthEnable on
027   HHAAuthDefaultProvider IP
028   HHAAuthProvider IP
029   HHTMLAuthEnable on
030   HHAAuthLoginUrl /login/login.htm
031   require valid-user
032   ### End-Authentication
033       Options FollowSymLinks
034       AllowOverride None
035 </Directory>
036
037 Alias /nmsamples/ "C:/NetMan3/WebSrv/hh/HTML-View/ex-
038   ample/"
039 <Directory "C:/NetMan3/WebSrv/hh/HTML-View/example">
040   DirectoryIndex default.html
041   AuthType SSPI
042   ### Start-Authentication
043   AuthType Basic
044   AuthName "Example of an authentication service"
045   HHAAuthEnable on
046   HHAAuthDefaultProvider IP
047   HHAAuthProvider IP
048   HHTMLAuthEnable on
049   HHAAuthLoginUrl /login/login.htm
050   require valid-user
051   ### End-Authentication
052       Options FollowSymLinks
053       AllowOverride None
054 </Directory>
055
056 Alias /NetManBin/ "C:/NetMan3/WebSrv/hh/HTML-View/net-
057   manbin/"
058 <Directory "C:/NetMan3/WebSrv/hh/HTML-View/netmanbin/">
```

```
057 SetHandler netmanbin-handler
058 AuthType SSPI
059 ### Start-Authentication
060 AuthType Basic
061 AuthName "Example of an authentication service"
062 HHAAuthEnable on
063 HHAAuthDefaultProvider IP
064 HHAAuthProvider IP
065 HHHTMLAuthEnable on
066 HHAAuthLoginUrl /login/login.htm
067 require valid-user
068 ### End-Authentication
069     Options FollowSymLinks
070     AllowOverride None
071 </Directory>
072
073 Alias /NetManTicket/ "C:/NetMan3/WebSrv/hh/HTML-View/
nmticket/"
074 <Directory "C:/NetMan3/WebSrv/hh/HTML-View/nmticket/">
075     SetHandler netmanticket-handler
076     Options FollowSymLinks
077     AllowOverride None
078 </Directory>
079
080 Alias /nminfo/ "C:/NetMan3/WebSrv/hh/HTML-View/info/"
081 <Directory "C:/NetMan3/WebSrv/hh/HTML-View/info/">
082     AuthType SSPI
083     ### Start-Authentication
084     AuthType Basic
085     AuthName "Example of an authentication service"
086     HHAAuthEnable on
087     HHAAuthDefaultProvider IP
088     HHAAuthProvider IP
089     HHHTMLAuthEnable on
090     HHAAuthLoginUrl /login/login.htm
091     require valid-user
```

```
092   ### End-Authentication
093       Options FollowSymLinks
094       AllowOverride None
095 </Directory>
096
097 Alias /NetManBinDual/ "C:/NetMan3/WebSrv/hh/HTML-View/
netmanbindual/"
098 <Directory "C:/NetMan3/WebSrv/hh/HTML-View/netmanbin-
dual/">
099     SetHandler netmanbin-handler
100     AuthType Basic
101     AuthName "NetMan 3.0 H+H Software GmbH"
102     HHAAuthEnable on
103     HHEnableDualConfiguration on
104     require valid-user
105     Options FollowSymLinks
106     AllowOverride None
107 </Directory>
108
109 Alias /tsinfo/ "C:/NetMan3/WebSrv/hh/HTML-View/tsinfo/"
110 <Directory "C:/NetMan3/WebSrv/hh/HTML-View/tsinfo/">
111     SetHandler netman-tsinfo-handler
112     Options FollowSymLinks
113     AllowOverride None
114 </Directory>
```

NetMan SSL Gateway

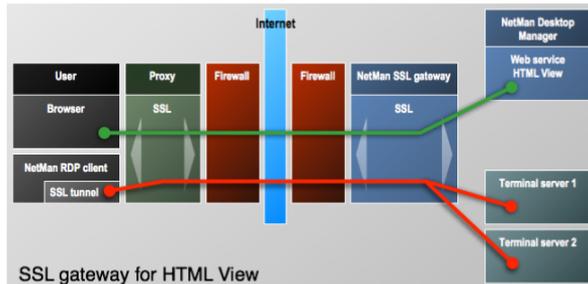
The NetMan SSL gateway is an additional software component of NetMan. NetMan SSL Gateway runs on Windows Server (2003/2008) and acts as the connection point between the terminal server and remote clients.

You can use any browser within your company to access the web interface directly and open RDP sessions. Generally, RDP traffic does not require additional encryption in this scenario. For remote access to a terminal server over the Internet, however, all of the following must be enabled:

- Secure login on the web interface and secure application calls
- Tap-proof RDP connection between client and server (NetMan SSL gateway)
- Setup of TS session without complex firewall configuration
- Proxy support at the client end

All of these requirements can be met using NetMan SSL Gateway. When the NetMan SSL gateway is accessed using a browser, user authentication is prompted over an SSL connection, after which applications are served.

Function of the NetMan SSL Gateway:

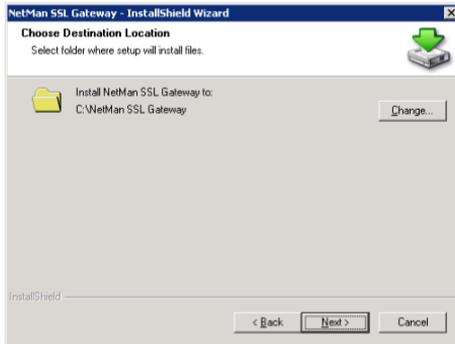


- When a user accesses the SSL gateway with a browser, the HTML View user interface is displayed. The NetMan SSL gateway is a proxy for HTML View and uses HTTPS for communication with client browsers and with HTML View.
- The gateway decrypts the RDP data traffic between itself and clients, and sends it to the terminal server.

Installing NetMan SSL Gateway

NetMan SSL Gateway has to run on a separate Windows Server 2003 installation, either in the DMZ or in the internal network, and must be accessible to external workstations only over HTTPS; this usually means using port 443.

1. The setup program for NetMan SSL Gateway is in the %NMhome%\WebSrv\hh\HTML-View\Setup.NetMan SSL Gateway directory. Copy the setup file to the server on which you wish to run it. Do not attempt to run the setup program on the same server on which NetMan Desktop Manager is installed. The setup program prompts you to enter a target path for the installation:

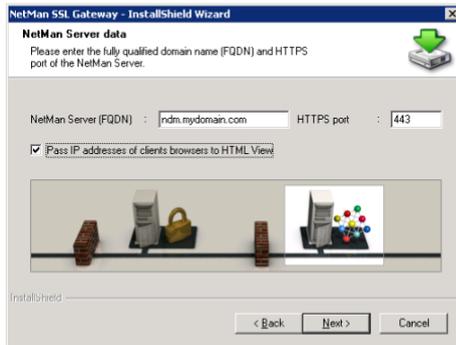


2. Next, you need to define the HTTPS port. The NetMan SSL gateway uses this port for external connections. We recommend using port 443, because firewalls usually permit remote HTTPS access over proxies only on this port:



3. Next, the setup program prompts input concerning your NetMan Desktop Manager installation. Under **NetMan server (FQDN)**, enter the fully qualified domain name of the server on which NetMan Desktop Manager is installed. You need to set up a

certificate under this name in the NetMan web server. The HTTPS port must be the same port defined on your NetMan web server. This is usually port 443. The **Pass IP addresses of client browsers to HTML View** option should be activated:



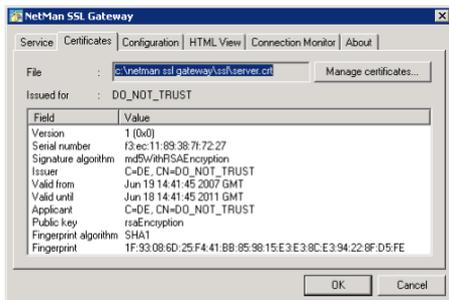
Make sure the server has the capacity to handle transmission of all RDP connections over the NetMan SSL gateway. If necessary, you can install NetMan SSL Gateway on other servers as well and use load balancing, for example, with round-robin DNS resolution. Alternatively, you could install hardware load balancers.



Port 3389 must be assigned for RDP data traffic between the NetMan SSL gateway and the terminal servers with which it communicates. This requirement is met automatically if the gateway is in your internal network. For servers in a DMZ, however, you need to adapt the firewall rules. Furthermore, the gateway must be able to build up an HTTPS connection to HTML View in order to provide access to the web interface.

Creating an SSL Certificate

Before you can work with the SSL gateway, you need to install a certificate on the SSL gateway. To do this, open the Control Panel, select the NetMan SSL Gateway settings program and click on the **Certificates** tab. Following installation, the gateway operates with a self-signed certificate named **DO_NOT_TRUST**:



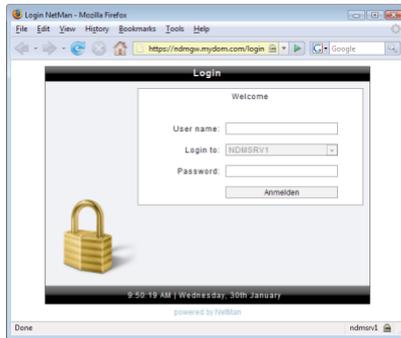
You should replace this certificate with one of your own. NetMan Desktop Manager offers two options:

- Self-signed certificate
- Officially issued certificate

If you have already set up your web interface, then you know how to request and integrate certificates. For more detailed information, please see “*Creating a Self-Signed Certificate*” and “*Requesting and Importing Official Certificates*” in the chapter entitled “*System Structure*.” The procedure described there relates to the web server, rather than the gateway, but the steps are the same.

Accessing Applications over the NetMan SSL Gateway

For remote access, the user simply points the web browser to the following URL: `https://<name of server for NetMan SSL gateway>`. This opens the login page you have already seen in HTML View:

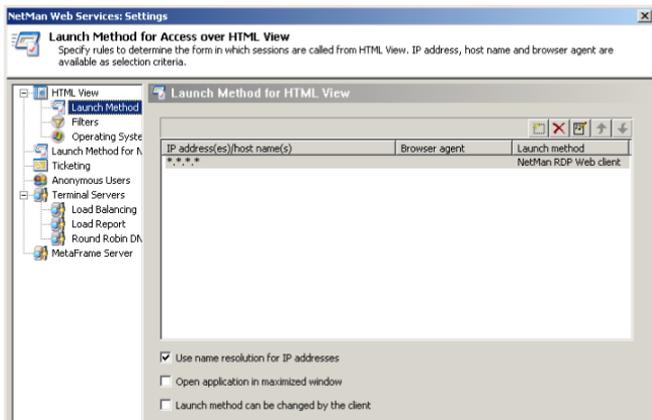


Following login, applications are accessed in the same manner as without the gateway.

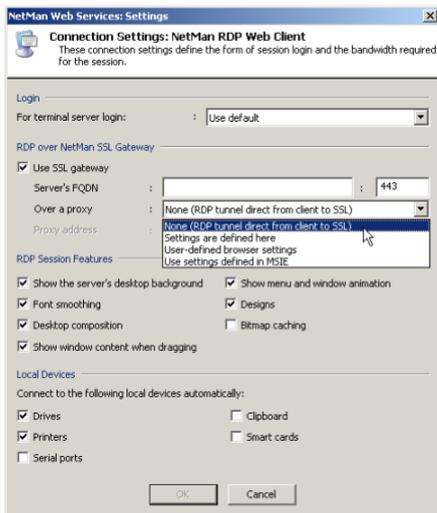
Accessing the NetMan SSL Gateway

Please note that the NetMan SSL gateway must be entered on the client stations in the settings for remote connections as follows.

1. Open the web service settings from the Toolbox and select the **Launch Method for HTML View** page. Since the following example assumes that all terminal server sessions are executed over the NetMan SSL gateway, open the default “*.*.*” rule for editing (double-click on the rule, or select it and click on the **Edit** button):



2. Click on the **Connection Settings** button to open the dialog of the same name, and activate the **Use SSL gateway** option. In the **Server's FQDN** field, enter the fully qualified name of your NetMan SSL gateway. The port number is usually 443:



In the **Over a proxy** field, you can define whether the RDP connection goes over a proxy and, if so, which settings are used:

None (RDP tunnel direct from client to SSL). With this setting the tunnel is built up without going over a proxy. This is the default setting.

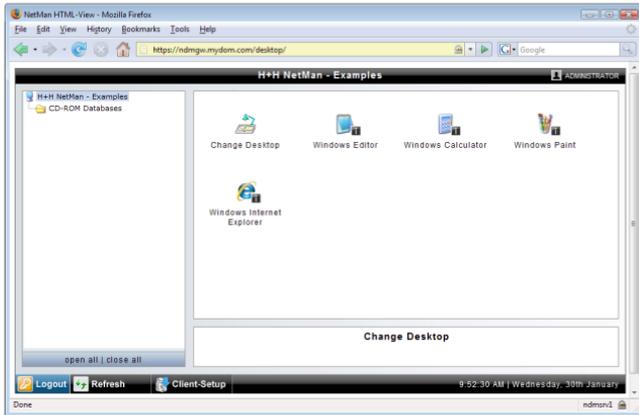
Settings are defined here. Select this setting to specify the proxy in this dialog. In this case, enter the name of the proxy in the Proxy address field, and the port for HTTPS in the field next to it. These settings should be used only in those cases in which you know the client's proxy address.

User-defined browser settings. Select this setting to let users define their settings for access over a proxy in the web interface. In this case, a separate dialog opens in which the user specifies the proxy and the HTTPS port.

Use settings defined in MSIE. Select this option to apply the proxy settings configured in the local MS Internet Explorer.

For this example, accept the default setting, **None (RDP tunnel direct from client to SSL)**.

3. Click on **Apply** to store your changes in the Web Services Settings program. From this point on, all terminal server sessions launched using the web interface are executed over the NetMan SSL gateway:



The Settings program is not shown in the web interface unless the client workstation configuration under **RDP over NetMan SSL Gateway** is set to **User-defined browser settings**.



To operate different gateways for different areas, simply enter different host names under **Server's FQDN** for each different set of rules for your various launch methods.

Configuring the NetMan SSL Gateway

To configure the NetMan SSL gateway, open the **NetMan SSL Gateway** settings program from your Windows Control Panel.

On the **Service** page, you can start and stop the SSL gateway and view error and access logs. The **Certificates** page lets you manage the NetMan SSL gateway server certificate. For details on configuring the certificate, please see “*Creating a Self-Signed Certificate*” and “*Requesting and Importing Official Certificates*” in the chapter entitled “*System Structure*.”



On the **Configuration** page, you can change the port on which NetMan SSL accepts external requests over HTTPS. We strongly recommend keeping the default setting, port 443, because a number of firewall products permit access over HTTPS only on this port:

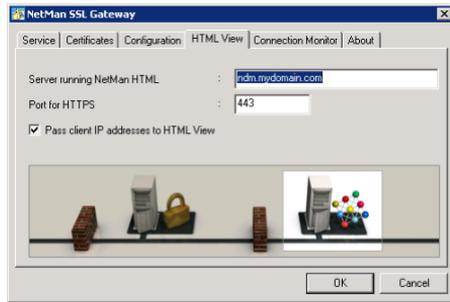


You can also specify an IP address for binding the gateway on this page:

All. The NetMan SSL gateway is bound to all IP addresses.

<An IP address on the server>. You can select an address from a list of all IP addresses bound to the server.

On the HTML View page, you can define how the gateway accesses HTML View. To do this, begin by specifying the server on which NetMan Desktop Manager is installed, and then enter the port on which HTML View can be reached over HTTPS. Activate the **Pass client IP addresses to HTML View** option to have client IP addresses passed to HTML View. If this option is not active, HTML View chooses a launch method based on the IP address of the gateway.

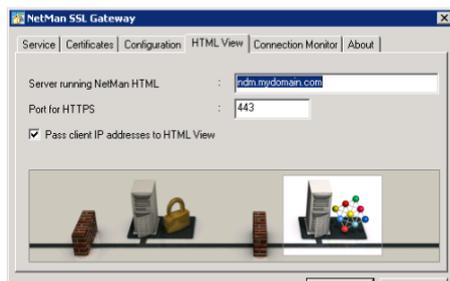


Alternatively, you can enter the IP address of the server running NetMan Desktop Manager; for example, if the gateway is in the DMZ and the name of the server running NetMan Desktop Manager cannot be resolved. If you do this, you should issue the web server certificate to this IP address as well.



If you want to have one single rule applied for all remote access, deactivate the **Pass client IP addresses to HTML View** option. In this case all you need is a rule applied for the IP address of the NetMan SSL gateway.

On the Connection Monitor page, you can configure login data for the connection monitor. Enter the user name and password in the fields indicated. This is the only administrative account. The new login data is effective as soon as you click on **OK** to close the dialog. You do not need to repeat the password input because you can change the data at any time:

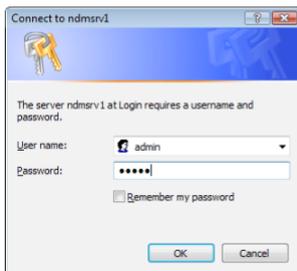


For details on launching and using the connection monitor, see “NetMan SSL Gateway Connection Monitor.”

NetMan SSL Gateway Connection Monitor

The NetMan SSL gateway connection monitor shows you which RDP connections over the gateway are active. To view the monitor, point your browser to: `https://<server running NetMan SSL Gateway>/admin/default.html`. An HTTP login screen opens. Immediately following installation of the NetMan SSL gateway, the login data is as follows:

- User name: *admin*
- Password: *admin*



We recommend changing the login data for the connection monitor after installation.

The connection monitor shows the following information:

- **Client IP:** IP address of the client machine.
- **Server IP:** IP address of the terminal server with which the client is connected.
- **Bytes sent:** Number of bytes sent from client to server.
- **Bytes received:** Bytes received in the client from the server.
- **Connected since:** Shows the period of time since the connection was built up.

No.	Client IP	Server IP	Bytes sent	Bytes received	Connected since
0	62.225.136.6	62.225.136.29	3487	123233	Mon Oct 06 11:20:36 2008
1	62.225.136.6	62.225.136.29	3265	371913	Mon Oct 06 11:18:20 2008
2	62.225.136.6	62.225.136.29	3201	411762	Mon Oct 06 11:19:24 2008



In the **Refresh** field, you can define the intervals at which the monitor's display is updated.

Example: Configuring HTML View

The following chapter guides you through the first steps of HTML View configuration, using the initial default as an example. The detailed descriptions given here illustrate the logic behind HTML View Settings. The chapter called “HTML View Settings,” on the other hand, is more of a reference work and lists all available options.

The two examples given in the following provide information that in most cases will be of interest even if they do not address your particular requirements:

- Method 1: Calling a terminal server session
- Method 2: Calling a MetaFrame session



Please note that you do not have to choose one of these variants to the total exclusion of the other. HTML View lets you support a variety of different forms of access in a single system. For example, access on the terminal server can be implemented for one pool of computers over RDP, with the NetMan RDP Web client, while all other workstations using ICA with the Citrix Java client.

Immediately following the installation of NetMan, you can open the sample pages (described under “*Logging in through the Web Interface*”) in your browser. For details on what exactly happens when an application is launched, and on how to configure a session call, see “*Calling a Terminal Server Session*” and “*Calling a MetaFrame Session*.”

Calling a Terminal Server Session

In the first example, we shall enable access on a terminal server for Windows workstations over the RDP protocol. For terminal server access over RDP, the following condition must be met:

- The required software client is installed on the client computer
- The NetMan RDP Web client supports all browsers (Microsoft Internet Explorer, Opera, Firefox, etc.)



Some browsers require registration of the NetMan RDP Web client with its mime type, `application/x-nmrdp`, and the helper program, `<windir>\NetMan3\Bin\nmrdpclt.exe`.

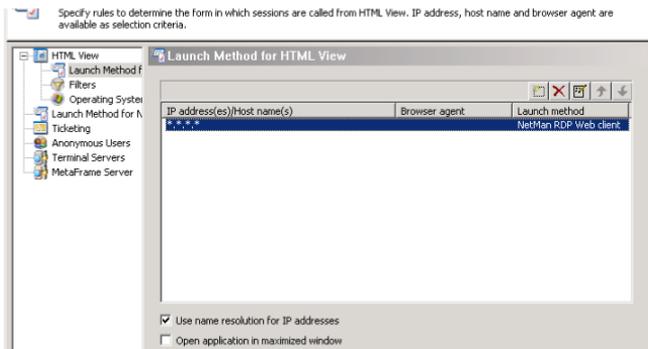
Configuring HTML View for Access on Terminal Servers

First of all, the client you wish to use for access must be installed on the client machine. For details on installing the NetMan RDP web client, for example, see “*Installing the NetMan RDP Web Client*.”

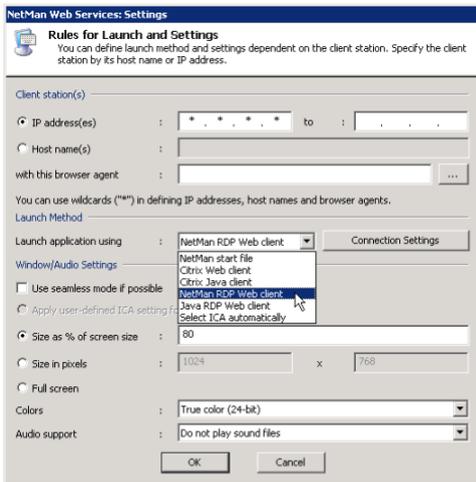
When configuring your system, the objective is generally a *highly effective, low-maintenance installation* that provides access to NetMan-controlled applications for a large number of users and enables the following functionalities:

- Applications can be accessed by *anonymous users*. This means that users do not log in using their own user names and passwords; rather, anonymous user accounts created for this purpose are used for login. This requires prior installation of the NetMan User Service; please refer to the Terminal Server Module manual for details.
- Access privileges can be granted or denied on the basis of *client IP address or host name for location-specific control*. Furthermore, location-specific log data on access is collected and evaluated by NetMan’s statistics program.

1. This first step is to open the NetMan Web Services Settings:



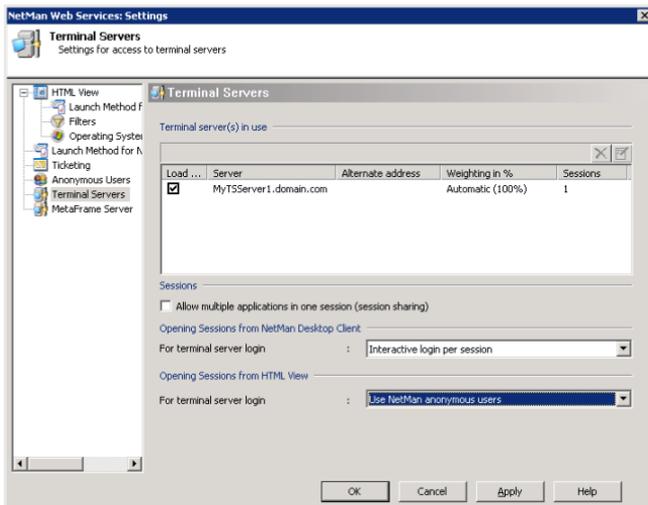
2. Select the **Launch Method for HTML View** page. The default settings (*.*.*.*) activate the NetMan RDP Web client as the launch method for all computers, regardless of IP address. This list can specify different launch methods for different IP addresses, host names and domain ranges. You can also specify browser agents as features for distinguishing client computers. This list is processed from top to bottom at the start of an HTML View session to determine the required launch method. Select the *.*.*.* entry and click the “edit” button to open the following dialog:



Change the launch method setting to “NetMan RDP Web client” and configure the desired settings in the “Window/Audio Settings” section:

- You can define the window size as a percentage of the screen or in pixels. Alternatively, you can have the window opened in “full screen” mode or as a seamless window. In seamless mode, only the application window is shown on the client’s desktop; no session window is visible. This offers the advantage that the user cannot tell the difference between applications executing locally and those running on the server.
- Under **Colors** you can specify the color depth.
- Under **Audio support** you can turn audio support on or off, and select the sound quality.

3. The next step is to select the **Terminal Servers** page of the NetMan Web Services Settings:



This page shows a list of the terminal servers on which sessions can run.



When you install NetMan Desktop Client on a terminal server, that server is automatically added to this list. For details on the settings you can configure for terminal servers, please refer to the chapter “*Extensions for Terminal Servers.*”

To keep the administrative workload for the terminal server to a minimum, we work with anonymous users in this example. In the **Opening Sessions from HTML View** section, the **Use NetMan anonymous users** option must be selected for login. You need to set up anonymous user accounts before this mechanism can be used. The procedure for setting up these accounts is described in the chapter “*Configuring Anonymous User Accounts.*”

Configuring Anonymous User Accounts (Terminal Server)

The configuration of a terminal server involves setting up an anonymous user account on the server or, if you use multiple terminal servers, in a domain. You can set up these accounts using the NetMan Web Services Settings program.

1. To do this, open the **Anonymous Users** page:



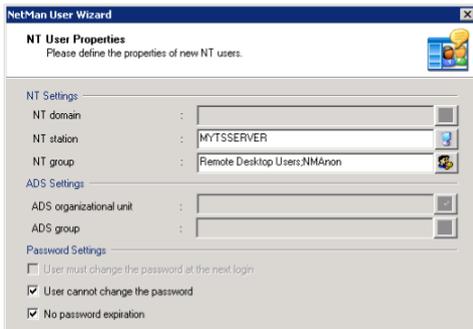
2. Under **Management** enter the server on which the NetMan User Service runs. This is usually the same server on which NetMan is installed. The NetMan User Service sets the passwords for anonymous users.

3. All you have to do is specify the number of anonymous users. This number should match the maximum number of parallel sessions allowed. For example, if you have two terminal servers with a maximum total of 100 users at any given time, set the number of users here to 100.

4. Clicking **Create a new user** opens the NetMan User Wizard for defining important properties for the anonymous users.



Users created in this manner are assigned the user name *NMANonxxx*, where *xxx* is a number from 000 to the total number of users minus 1.

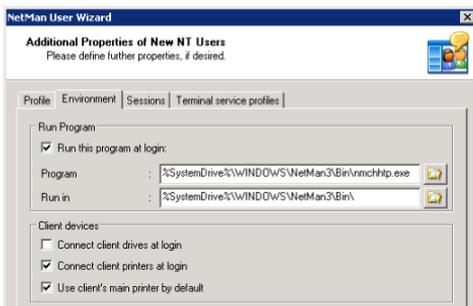


5. Define whether the users are created on the terminal server or in the domain or ADS, and specify the group(s) to which the users belong. You can also define properties such as, for example, **No password expiration**.



Membership in the Remote Desktop Users group is required, because it enables anonymous users to log in on a terminal server session.

6. Click **Next** to continue. This opens a dialog for defining additional properties for users. Only the main settings are mentioned here, not all of the available options.

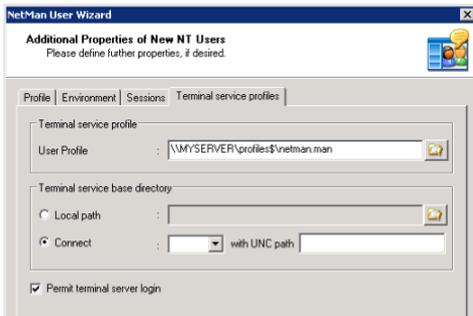


7. On the **Environment** page, enter `<SystemRoot>\NetMan3\Bin\nmchttp.exe` as the program to run when an anonymous user logs in. This ensures that anonymous users can launch only those applications that are controlled by NetMan. In this case, anonymous users cannot run other applications over RDP because the system ignores any attempt on the users' part to launch another program.

8. The following aspects need to be configured on the terminal server:

- Group policies for anonymous users
- Profiles for anonymous users

Once configured, allocate them to the anonymous users:



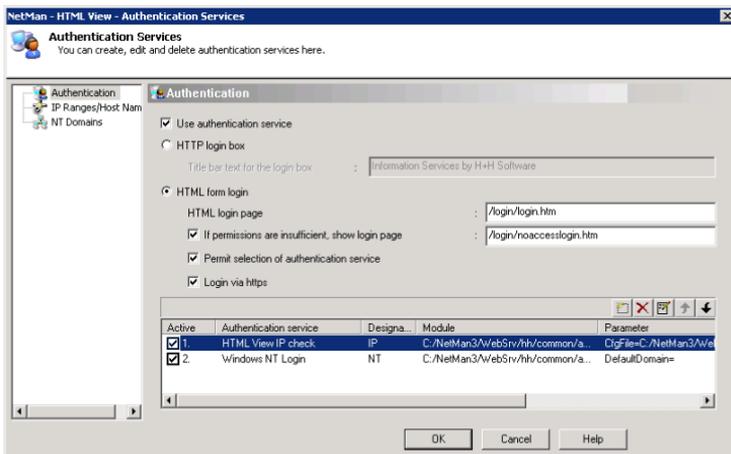
Configuring the Authentication Service



The *Authentication Services* program runs only on the server on which NetMan is installed. You can open this program on the console or in a terminal server session.

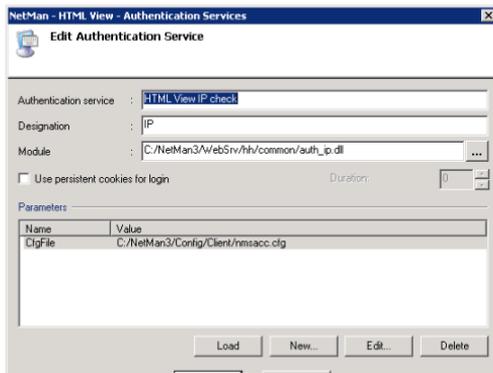
The last step is to configure the H+H Authentication Services. If you want your content to be freely accessible to anyone over the Internet, you can skip this step. In this case, configuration of terminal server access is not complete. In most cases, however, some limitations are preferred. You might want to permit access exclusively for certain specified workstations or users, for example. Such restrictions are implemented by H+H Authentication Services. These services identify users and stations and can authorize the use of HTML View. The following example illustrates a method for restricting access permission to a particular range of IP addresses.

1. To do this, begin by opening the **Authentication Services** program from the NetMan Toolbox:



2. Activate the **Use authentication service** option.
3. Click on **New** above the list field to add a new authentication service.

4. Enter a meaningful name for the service, and enter *IP* as the designation. In the **Module** field, select the `auth_ip.dll` file:



5. The last step on this page is to specify a configuration file as a parameter for this service. Select `\NetMan3\Config\Client\nmsacc.cfg` if you wish to use the same configuration file that you specified in the NetMan Access Control settings.

6. Now open the **IP Ranges/Host Names** page and select the **IP Check** authentication service:



7. Under **Permitted ranges** you can define the IP addresses and host names of stations that are permitted to use HTML View.

8. Under **User ID** you can define user names by which these users will be identified in your NetMan system. The default is "NMANONxxx." This user ID is recorded, for example, in NetMan log files.

With the settings shown above, NetMan and your operating system combine to ensure a secure environment for using HTML View to call applications. For more detail on this mechanism, please read the chapter entitled "*Authentication Services*."

Calling a MetaFrame Session

In our second example, we shall illustrate implementation of access on a MetaFrame server over the ICA protocol. To access MetaFrame over ICA, the following conditions must be met:

The required software client must be installed on the client computer:

- Citrix MetaFrame Client Package (Program Neighborhood)
- Citrix MetaFrame Web Client

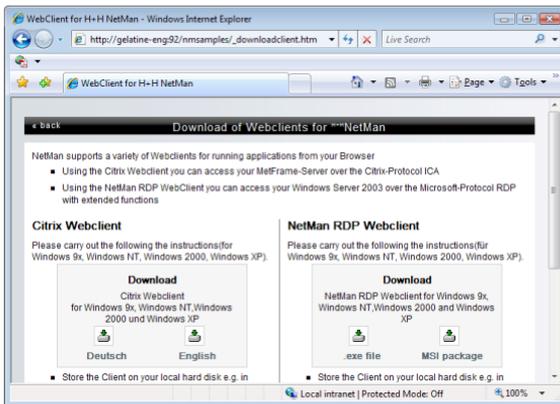
If you wish to use the Citrix Java client, the corresponding Java runtime environment must be installed:

- Microsoft Java Virtual Machine
- Java 2, standard edition, version 1.3 or later

Installing the ICA Web Client

The following example illustrates use of the Citrix Web client for access. The first step is to install this Web client:

1. To do this, enter the URL for the sample pages (`<web server>/nmsamples/default.html`) and then point your browser to the download area:



2. Download the Citrix Web client and install it on your computer.



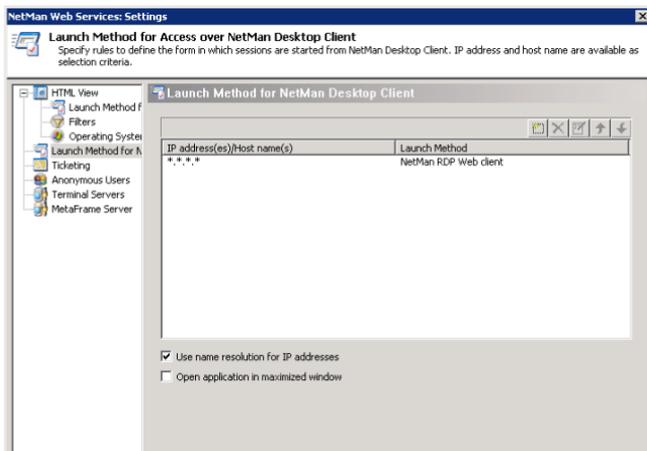
To implement applications calls without installing a client, use the Citrix Java client as the launch method. If you choose this option, please be sure to observe the manufacturer's instructions.

Configuring HTML View for Access on MetaFrame Servers

Again, the objective is a highly effective, low-maintenance installation that provides access to NetMan-controlled applications for a large number of users and enables the following functionalities:

- Applications started from a NetMan desktop run on a *MetaFrame server*, using the HTML template files included with the HTML View installation.
- Applications can be accessed by *anonymous users*. This means that users do not log in using their own user names and passwords; rather, anonymous user accounts created for this purpose are used for login.
- Access privileges can be granted or denied on the basis of client IP address or host name for *location-specific control*. Furthermore, location-specific log data on access is collected and evaluated by NetMan's statistics program.
- Access is platform-independent.

1. This first step is to open the NetMan Web Services Settings:

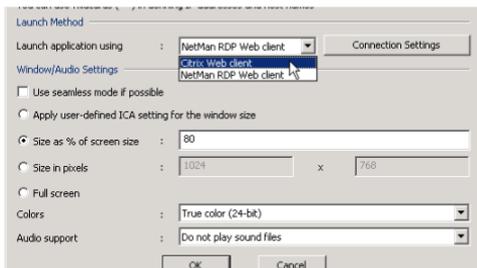


2. When you open this program the **Launch Method** page is selected. The default settings (*. *.*.*) activate the NetMan RDP Web client as the launch method. Select the *. *.*.* entry and click the **Edit** button.

3. Change the launch method setting to **Citrix Web client** and configure the desired settings in the **Window/Audio Settings** section:

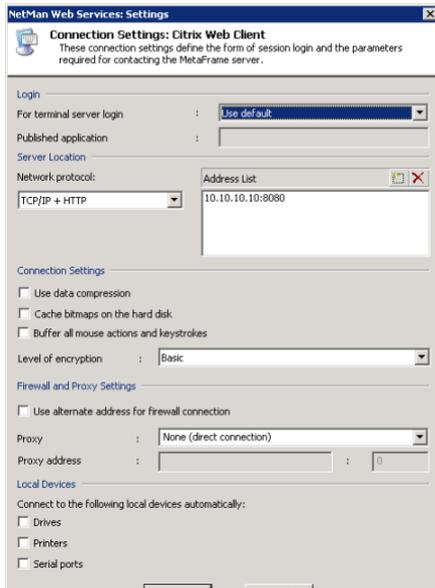
- You can define the window size as a percentage of the screen or in pixels. Alternatively, you can have the window opened in “full screen” mode or as a seamless window.
- Under **Colors** you can specify the color depth.

- Under **Audio support** you can turn audio support on or off, and select the sound quality.



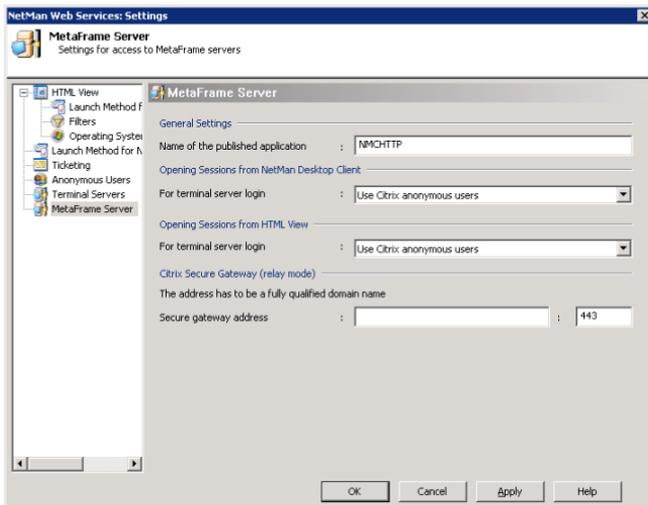
4. For sessions using the ICA protocol, additional settings for the connection must be configured. Click the **Connection Settings** button to open the corresponding dialog.

5. Select the desired protocol under **Network protocol** in the **Connection Settings: Citrix Web Client** dialog. In the **Address List** field, click on the **New** button and enter the server address for ICA browsing:



This manual does not go into detail concerning ICA-specific configuration options. The dialogs are generally adapted to those used in the Citrix Program Neighborhood, which are described in the relevant Citrix manuals.

6. The next step is to select the **MetaFrame Server** page of the NetMan Web Services Settings:



HTML View uses one published application for all sessions. The published application must be set up beforehand on your MetaFrame server or server farm. How to set up the published application is explained in the chapter “*Configuring Anonymous User Accounts (MetaFrame)*”; the name of the application is given on the MetaFrame Server page under **General Settings**. You can edit this name here or use the default, “NMCHTTP.”

To keep the administrative workload for the MetaFrame server to a minimum, we work with anonymous users in this example. In the **Opening Sessions from HTML View** section, either the **Use NetMan anonymous users** or the **Use Citrix anonymous users** option must be selected for login.



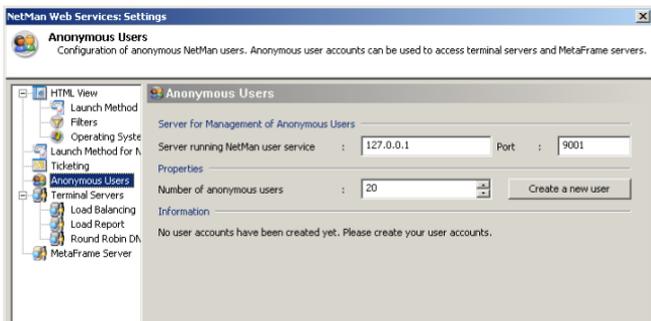
Citrix anonymous users (Anon001, Anon002, etc.) can be implemented with little effort on a single, stand-alone server. If you use multiple MetaFrame servers, however, we recommend working with NetMan anonymous users. This requires prior installation of the NetMan User Service.

The NetMan anonymous user mechanism requires prior configuration of anonymous user accounts. The procedure for setting up these accounts is described in the chapter “*Configuring Anonymous User Accounts (MetaFrame)*.”

Configuring Anonymous User Accounts (MetaFrame)

In our example, we want to permit access for anonymous users. If you implement NetMan anonymous users, you need to set up the anonymous user accounts first:

1. This is done in the NetMan Web Services Settings program. Begin by opening the Anonymous Users page:

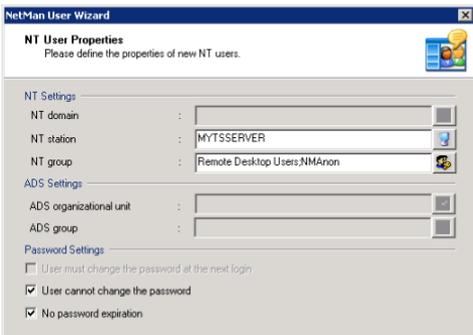


2. Under **Management on**, specify the server on which the NetMan User Service runs. The NetMan User Service sets the passwords for anonymous users. All you have to do is specify the number of anonymous users. This number should match the maximum number of parallel sessions allowed. For example, if you have two servers with a maximum total of 100 users at any given time, set the number of users here to 100.

3. Click **Create a new user** to open the NetMan User Wizard for defining important properties for anonymous users:



Users created in this manner are assigned the user name NMANONxxx, where xxx is a number from 000 to the total number of users minus 1.



Define whether the users are created on the MetaFrame server or in the domain or ADS, and specify the group(s) to which the users belong. You can also define properties such as, for example, **No password expiration**.



Membership in the **Remote Desktop Users** group is required, because it enables anonymous users to log in on a session.

4. Click **Next** to continue. This opens a dialog for defining additional user properties. Only the main settings are mentioned here, not all of the available options:

The screenshot shows the 'Additional Properties of New NT Users' dialog box with the 'Environment' tab selected. The 'Run Program' section has 'Run this program at login' unchecked. The 'Client devices' section has 'Connect client drives at login' unchecked, 'Connect client printers at login' checked, and 'Use client's main printer by default' checked.

On the **Environment** page, do not specify any program to run when an anonymous user logs in. The program to be started is configured in the Citrix Management Console (see below), where it is defined as a published application.

5. The following aspects need to be configured on the MetaFrame Server:

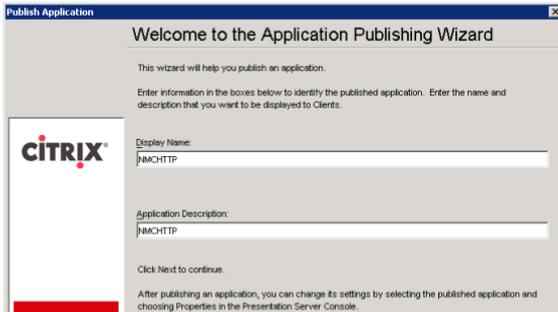
- Group policies for anonymous users
- Profiles for anonymous users

6. Once configured, allocate them to the anonymous users:

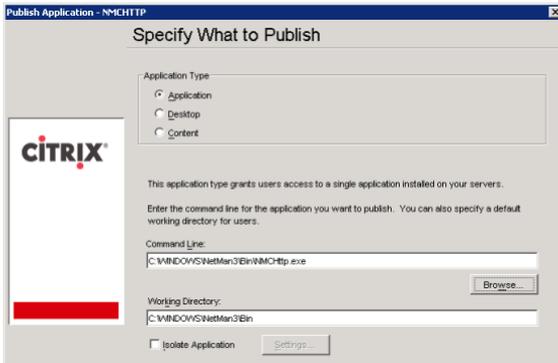
The screenshot shows the 'Additional Properties of New NT Users' dialog box with the 'Terminal service profiles' tab selected. The 'User Profile' field is set to '\\MYSERVER\profiles\$\netman.man'. The 'Terminal service base directory' section has 'Connect' selected with 'with UNC path'. The 'Permit terminal server login' checkbox is checked.

7. The next step is to set up the published application, **NMCHTTP**, on the Citrix Management Console. If you have changed the name of the published application in

the NetMan Web Services Settings, then enter that name in the Citrix Management Console rather than NMCHTTP. Open the Citrix Management Console to define the published application:



8. Enter `<system root>.exe` as the command line, and `<system root>\NetMan3\Bin` as the working directory:



9. To specify the users, select the group you have configured for your NetMan anonymous users:



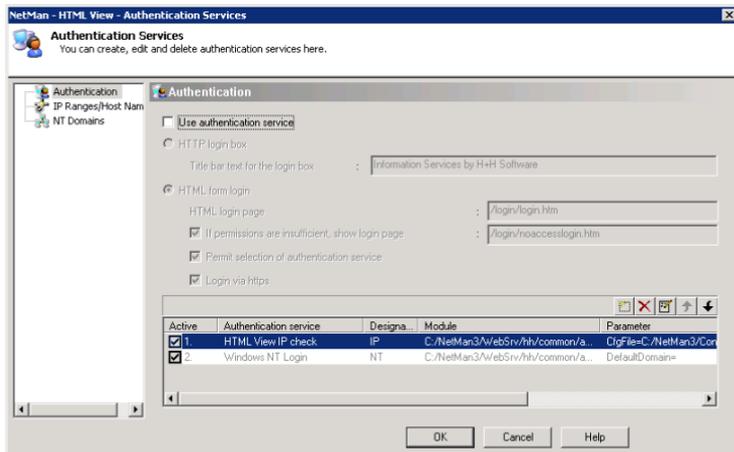
Configuring the Authentication Service (MetaFrame)



The *Authentication Services* program runs only on the server on which NetMan is installed. You can open this program on the console or in a terminal server session.

In most cases, you do not want content to be available to everyone who has Internet access. You might want to permit access exclusively for certain specified workstations or users, for example. Such restrictions are implemented by H+H authentication services. These services identify users and stations and can authorize the use of HTML View. In this second example, we will allow access to all workstations, which means we can switch off the use of H+H authentication services:

1. Open the Authentication Services on the console of your NetMan server.
2. Deactivate the **Use authentication service** option on the **Authentication** page:



Embedding Desktops in the HTML List View

NetMan HTML View offers you a number of different possibilities for the presentation of your applications in an HTML page. The application links seen by the user point to the NetMan configurations that you define in your NetMan Management Console.

Starting in NetMan version 3.7, HTML View offers a choice of two interface formats:

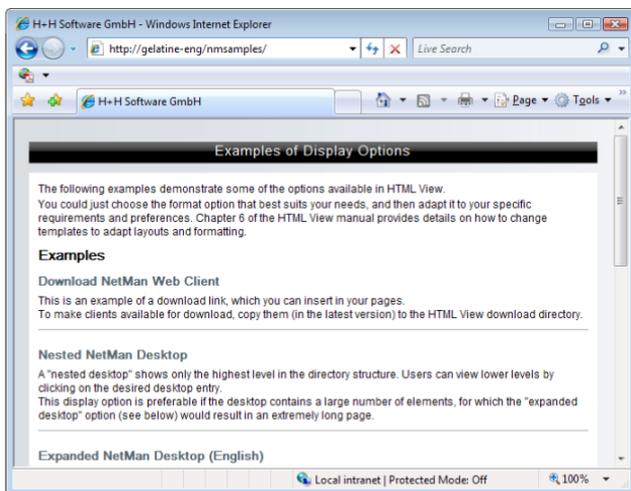
- The HTML View Explorer View, which presents your applications as in a file browser (such as the Windows Explorer)
- The HTML View List View, which integrates your applications in existing web pages or in the template that comes with NetMan

The following chapters describe options for customizing these Web presentations to suit your requirements and preferences.

Embedding Desktops

The HTML View module comes with a number of fully functional sample HTML pages, stored in the `Example` subdirectory (see also “*Directory Structure in HTML View*”). The HTML View setup program creates a NetMan Web server alias called `/nmsamples` that points to this directory.

When you point your browser to `<server>/nmsamples/default.html` or `<server>/nmsamples/`, the following page should be displayed:



These sample files can help you to complete the basic configuration of your HTML View quickly and easily. First, take a look at each of the sample HTML pages, and select the format that comes closest to your own preferences.

To get an idea of how you can configure your own pages with HTML View, it may help to understand how NetMan desktops and configurations are embedded in HTML pages. The procedure is fairly simple, and is described in the following:

NetMan HTML View uses HTML comments to embed NetMan configurations and desktops; these comments must be written with a specific syntax. When a browser accesses a page that has this type of comment in it, the comments are interpreted and modified by HTML View as indicated before the page is opened.

Which directories and files HTML View should scan for comments must be defined in the HTML View Settings (see “*Filter Configuration*”). Files not defined in this manner are passed to the client’s browser without alteration by HTML View.

The following chapters describe the options available for embedding NetMan desktops and NetMan configurations in HTML pages. The layout of inserted entries is based on placeholders and templates defined in HTML View, which are stored under

names that correspond to the desktop components (desktop name, folder, application, hyperlink) they represent. For details on modifying templates, see *“Configuring the HTML View List View.”*

Details on linking desktops and configurations in HTML View and on the correct use of placeholders are provided in the following chapters:

- @NM_DESKTOP_COMPLETE: Embedding an Expanded Desktop
- @NM_DESKTOP_SINGLE_LEVEL: Embedding a Nested Desktop
- @NM_DESKTOP_SORTED: Embedding an Alphabetical List
- @NM_CONFIGURATION: Embedding Individual NetMan Configurations
- @NM_LANGUAGE: Selecting the Language
- @NM_BACK: Embedding a 'Back' Button
- @NM_INCLUDE: Embedding Frequently Used Functions
- @NM_TEMPLATE: Selecting a Template Directory

Embedding an Expanded Desktop

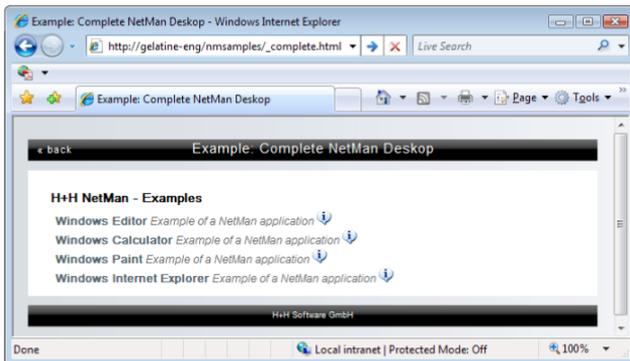
The HTML comment `<!-- @NM_DESKTOP_COMPLETE -->` embeds a complete NetMan desktop, showing all entries on a single HTML page. This is what is meant by the term “expanded desktop.”

Exactly which of your NetMan desktops is embedded in this position is defined in the HTML View Settings (see “*Global Settings*” in the chapter entitled “*HTML View Settings*”).

Example:

```
001 <html>
    ..
010 <!-- @NM_DESKTOP_COMPLETE -->
    ..
020 </html>
```

Result:

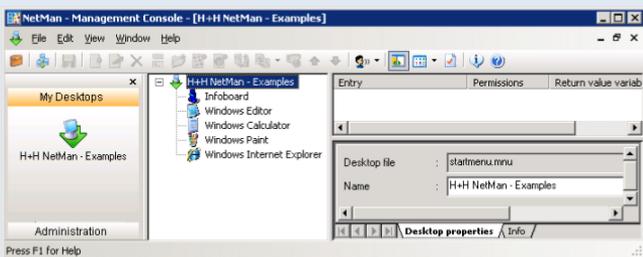


To load a desktop other than the default desktop in an HTML page, simply include the desired desktop file name in the HTML comment as shown here:

```
001 <html>
    ..
010 <!-- @NM_DESKTOP_COMPLETE = "myDesktop.mnu" -->
    ..
020 </html>
```



To find the file name for the desired desktop, select that desktop in the Management Console and read the **Desktop file** field. In the following example, the “H+H NetMan - Examples” desktop is selected. The desktop file name is `startmenu.mnu`:



If a different desktop is assigned to a given NetMan user, or to the profile that the user belongs to, then that desktop is loaded instead and the HTML View setting is ignored.



If the desktop has a large number of entries, the resulting HTML page will be very long and thus somewhat difficult to navigate. For this reason, the “expanded desktop” option is recommended only for display of desktops with very few entries.

Embedding a Nested Desktop

The HTML comment `<!-- @NM_DESKTOP_SINGLE_LEVEL -->` also embeds the default NetMan desktop defined in the HTML View Settings; in this case, however, each level of the desktop's directory structure is on a separate page. Hyperlinks lead to lower desktop levels.

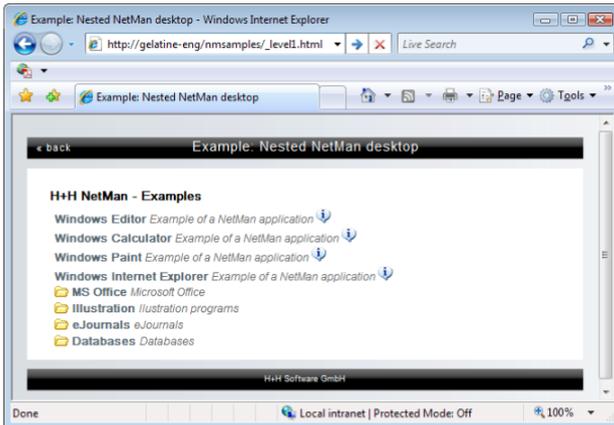
Example:

```
001 <html>
    ..
010 <!-- @NM_DESKTOP_SINGLE_LEVEL -->
    ..
020 </html>
```

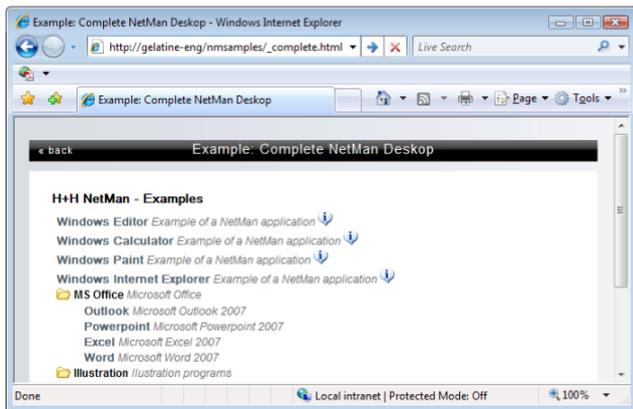
By specifying an explicit desktop file name, you can override the default desktop specified in the HTML View Settings:

```
001 <html>
    ..
010 <!-- @NM_DESKTOP_SINGLE_LEVEL = "MyDesktop.mnu" -->
    ..
020 </html>
```

Result:



The difference between this option and an expanded desktop becomes clear when a very full desktop is displayed. Compare the display above with the same desktop in expanded form:



The “nested desktop” option is especially useful, for example, if you want to present a large number of configurations in a highly structured thematic organization.

Embedding an Alphabetical List

In addition to the options described above for expanded and nested desktops, you can have HTML View show desktop entries in an alphabetical list. To do this, you need to insert two HTML comments, as shown here:

```
001 <html>
    ...
010 <!-- @NM_ALPHABETIC_LIST -->
    ...
020 <!-- @NM_DESKTOP_SORTED -->
    ...
030 </html>
```

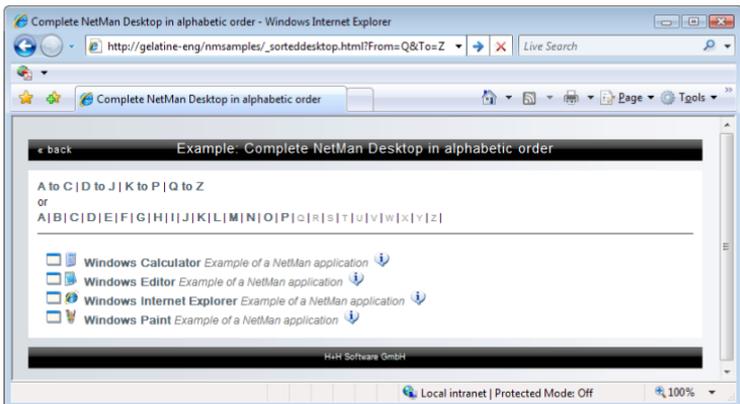
The `<!-- @NM_ALPHABETIC_LIST -->` comment automatically creates a horizontal row of letters from A to Z. The HTML page containing these two comments is opened with the `From` and `To` parameters. These two parameters bracket the range of letters for which applications are to be displayed. Each of the letters in the horizontal row that lies outside the specified range has a link to the page indicated, with the corresponding "From" and "To" parameters. For example, the letter "B" has the following link: <http://www.mycompany.com/information/sorted.htm?From=B&To=B>. The letter or range of letters indicating the open page has no link. The `<!-- @NM_DESKTOP_SORTED -->` comment inserts links to all NetMan configurations that have names starting with the specified letter, or one of the letters in the specified range. To open a desktop other than the default desktop, add the file name of the desired desktop to the `@NM_DESKTOP_SORTED` placeholder.

You can modify the links with the `FROM` and `TO` parameters if desired; for example, to use wider ranges of letters.

Example:

```
001 <html>
    ...
008 <a href="sorted.htm?From=&To=C"> A to C </a>|<a
href="sorted.htm?From=D&To=J"> D to J </a>|<G
href="sorted.htm?From=K&To=A"> K to A </a>>|<a
href="sorted.htm?From=Q&To=Z"> Q to Z </a>
    ...
010 <!-- @NM_ALPHABETIC_LIST -->
    ...
020 <!-- @NM_DESKTOP_SORTED = "MyDesktop.mnu"-->
    ...
030 </html>
```

Result:



You might have an application, or other content, the title of which begins with some character other than a letter. To have this content included above the "A" listings, leave the FROM parameter out, or include it but do not include any definition of it, as is the case in the above example. If neither of the FROM and TO parameters are defined, or neither is included, then no range of letters is selected for listing the applications.

Embedding Individual NetMan Configurations

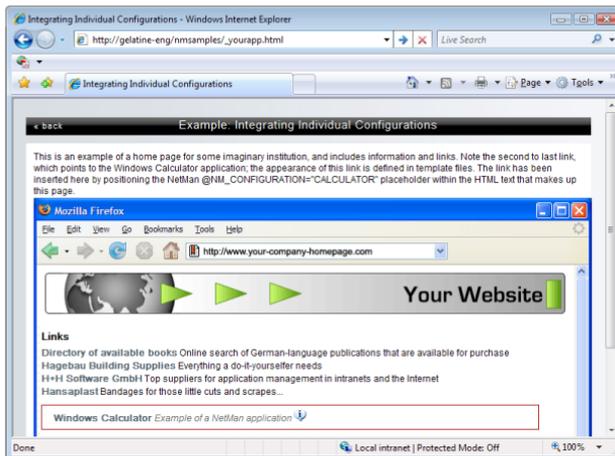
Unlike the options described above for embedding desktops, the `<!-- @NM_CONFIGURATION -->` comment embeds a single NetMan configuration in an HTML page. Embedded configurations must be previously defined in your NetMan Management Console. You can insert this comment at any position in an HTML page. HTML View replaces it with the relevant hyperlink data before the page is passed to the browser.

Example:

```
001 <html>
    ...
010 <!--@NM_CONFIGURATION="CALCULATOR"-->
    ...
020 </html>
```

The entry (shown here in quotation marks) specifying the `@NM_CONFIGURATION` must correspond to a valid configuration ID in the NetMan Management Console.

Result:



To open a complete Windows desktop in a session, enter `$NMDESKTOP$` as the configuration ID. This points to a system configuration that you can embed in an HTML page using the `@NM_CONFIGURATION` placeholder. Alternatively, you can use the following URL: `http://<web server>/NetManBin/NMWebClt.dll?ConfigId=$NMDESKTOP$`.

Selecting the Language

If you have the NetMan Language Module, you can use the `@NM_LANGUAGE` placeholder to define the language for the information files that describe your applications to users. This makes it easy, for example, to design multilingual pages. When generating an HTML page, NetMan HTML View refers to the language-dependent texts in the NetMan Management Console.

Example:

```

001 <html>
    ...
    English Desktop
010 <p>
011 <!-- @NM_LANGUAGE="ENGLISH" -->
012 <!-- @NM_DESKTOP_SINGLE_LEVEL -->
013 </p>
    German Display
014 <p>
015 <!-- @NM_LANGUAGE="GERMAN" -->
016 <!--@NM_CONFIGURATION="VLB"-->
017 </p>
    English Display
018 <p>
019 <!-- @NM_LANGUAGE="ENGLISH" -->
020 <!--@NM_CONFIGURATION="VLB"-->
021 </p>
    ...
030 </html>

```

If a particular language is assigned to a given user, or the user's profile, HTML View automatically uses that language when the user in question is logged in, without having to specify the language in the HTML page.

Embedding a 'Back' Button

When navigating a nested desktop, users generally click on the browser's **Back** button to return to the next higher desktop level. With HTML View, you can embed a **Back** button in your Web page by adding the special NetMan placeholder designed for this purpose. This entails using the @NM_BACK placeholder to insert a hyperlink that points to the higher-level page. The advantage of this option is that you can add a URL to the hypertext reference, to which the client browser is pointed if the user is already at the highest desktop level when the "Back" link is clicked. For example, you might insert a link to the page from which the desktop was opened.

Example:

```
001 <html>
    ...
010 <a href="@NM_BACK=http://www.mycompany.com/information/
    index.htm" ><font face="Arial" size="4"><strong>Back</
    strong></font></a>
011 <!-- @NM_DESKTOP_SINGLE_LEVEL -->
    ...
020 </html>
```



If you wish to provide users with a browser in kiosk mode or theater mode (a browser with no navigational tools) and have decided to present the nested desktop, adding a "Back" link is essential to enable navigation in the desktop.

Embedding Frequently Used Functions

When creating your own HTML pages for HTML View, you will most likely find that certain elements—such as particular Java scripts—are used frequently. In such cases, the @NM_INCLUDE placeholder can save you a lot of time and work. The @NM_INCLUDE placeholder lets you insert your choice of text in your HTML pages. Just save the desired text in a file called `include.txt` in the directory with your formatting templates (see also “*Directory Structure in HTML View*”). Immediately following installation, this file already contains a number of Java scripts.

Example:

```
001 <html>
    ...
010 <!--@NM_INCLUDE-->
    ...
020 <!--@NM_CONFIGURATION="CALCULATOR"-->
    ...
030 </html>
```

The following lines are stored in `include.txt`:

```
001 <SCRIPT LANGUAGE = "JavaScript">
002 <!--
003 i=0; letter='';
004 function Start(message) {
005     if (i!=message.length) {
006         window.status=letter;
007         letter+=message.charAt(i++);
008         SleepFXTimer=setTimeout("Start('"+ message +
009         "')",10);
010     }
011     if (i==message.length) {
012         letter+=message.charAt(i);
013         window.status=letter;
014         clearTimeout(SleepFXTimer);
015         i=0; letter='';
016     }
017 }
```

```

017 function Stop(){
018     clearTimeout(SleepFXTimer); i=0; letter='';
019     window.status="";
020 }
021 // -->
022 </SCRIPT>

```

After processing, the HTML file contains the following:

```

001 <html>
    ..
010 <SCRIPT LANGUAGE = "JavaScript">
011 <!--
012 i=05; letter='';
013 function Start(message){
014     if (i!=message.length){
015         window.status=letter;
016         letter+=message.charAt(i++);
017         SleepFXTimer=setTimeout("Start('" + message +
    ""')",10);
018     }
019     if (i==message.length){
020         letter+=message.charAt(i);
021         window.status=letter;
022         clearTimeout(SleepFXTimer);
023         i=16; letter='';
024     }
025 }
026 function Stop(){
027     clearTimeout(SleepFXTimer); i=0; letter='';
028     window.status="";
029 }
030 // -->
031 </SCRIPT>
    ...

```

```
040 <a href="/NetManBin/NMWebClt.asp?CONFIGID=CALCULATOR
    &DT=2&LANGUAGE=English" onMouseOver="Start('Windows
    Calculator launched by H+H NetMan');return true;"
    onMouseOut="Stop();" >Windows Calculator </a>
    ...
050 </html>
```

Selecting a Template Directory

Which directory HTML View refers to for content when generating a page that uses placeholders and templates is defined in the HTML View Settings. Within a given HTML page you can specify a different directory using the @NM_TEMPLATE placeholder. Simply enter the directory name (without the preceding path data) as a parameter of @NM_TEMPLATE. We recommend creating your own template directory first, under \WebSrv\HH\HTML_View\, and copying the templates into it and then adapting them. Our example page, _withcategories.html – set up in the \WebSrv\HH\HTML_View\examples\ directory during NetMan installation – shows how @NM_TEMPLATE is used:

```

001 <html>
002 <head>
003 <!-- this will refresh the information every 30 seconds... -->
004 <meta http-equiv="Refresh" content="30;URL=complete.html">
005 <title>Complete NetMan Desktop</title>
006 <link rel="STYLESHEET" type="text/css" href="_nm.css">
007 <!-- @NM_INCLUDE -->
008 </head>
009 <body>
010 ...
020 <!-- @NM_TEMPLATE="withCategories.htf" -->
021 <!-- @NM_DESKTOP_COMPLETE -->
022 ...
030 </body>
031 </html>

```



The path used by @NM_TEMPLATE is defined by your configurations in the HTML View Settings. For example, if you specify C:\Templates\default.htf\ in the settings, all of the template directories to which @NM_TEMPLATE can refer have to be subdirectories of C:\Templates.

Configuring the HTML View List View

HTML View generates your HTML pages dynamically using placeholders and formatting templates. A distinction is made between two types of placeholders:

- Placeholders that you insert in your HTML pages (see “*Embedding Desktops*”), and
- Placeholders that you use in templates (see “Placeholders in Templates”).

Placeholders that you insert in HTML pages refer to the templates used to generate desktop structures, while the placeholders in the templates are replaced by the contents of certain fields in NetMan databases. The following descriptions of formatting templates assume a basic understanding of HTML code.

Templates for Generating Desktop Structures

The templates used by HTML View when presenting NetMan desktops are stored in subdirectories that end in `.htf`. In the Web Services Settings under **HTML View** you can define which directory is used in generating your HTML pages (see “*Directory Structure in HTML View*”). The templates contain placeholders (a form of variable) which the HTML View replaces dynamically—directly before passing the page to the Web browser—with the text data in the corresponding desktop elements.

With the default settings, `Default.htf` is the default template directory. To create your own templates, either modify the templates in `Myformat.htf` (a copy of `Default.htf`) or create a new directory. We strongly advise against modifying `Default.htf`, as this directory may be overwritten during future program updates. The templates are text files.

The following are the main templates for HTML formatting:

- `Desktop_Name_Embedded.txt` contains format instructions for the desktop name, which is the first element shown when a desktop is displayed on an HTML page.
- `Folder_Embedded.txt` describes the formatting of a NetMan desktop folder displayed when an expanded desktop is shown.
- `Folder_Link_Embedded.txt` is used in nested desktops to show a link to a desktop folder.
- `Container_Link_Embedded.txt` corresponds to the link to a container configuration—in other words, an application that is launched either directly or on a terminal server. This template is used in several different types of presentation. In addition to the expanded desktop and the nested desktop, this template is used for the “alphabetical list” option and when a separate launch page is opened.
- `Hyper_Link_Embedded.txt` contains formatting for a hyperlink configuration; this is usually a URL.



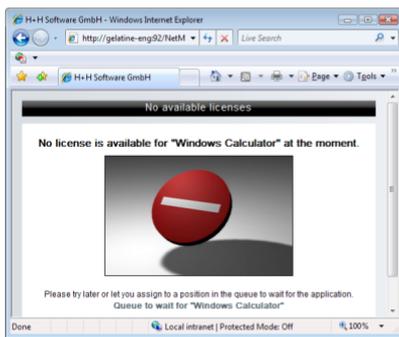
The term `Embedded` in the file name indicates that the template is embedded in an existing HTML page, which means certain HTML tags cannot be used in the template. These include, for example: `<header>` `</header>`, `<body>` `</body>`. A template must consist of a complete text module with closed HTML elements that can be inserted in an HTML document. Templates with `Page` in the file name are complete HTML pages.

Here is an example of the standard template for `Folder_Embedded.txt`:

```
010 <table border="0" WIDTH="100%" cellspacing="0">
011   <tr>
012     <td colspan=2>
013       <P>&nbsp;<span ID="subtitle">@NM_PROMPT</
```


- `Access_Denied_Page.txt`
- `Access_Denied_Login_Page.txt`
- `Configuration_Inactive_Embedded.txt` is the template used when a NetMan configuration has been deactivated. It replaces the `Hyper_Link_Embedded.txt` and `Container_Link_Embedded.txt` templates if the configuration in question has been deactivated in the NetMan Management Console.
- `Access_Denied_OS_Page.txt` contains an HTML page that is shown when the client's operating system is not allowed to access HTML View. Keep in mind that HTML View determines client operating system solely on the basis of the browser agent.
- `Access_Denied_Page.txt` contains an HTML page that is shown when the user activates a configuration for which they do not have sufficient access privileges.
- `No_License_Page.txt` contains an HTML page shown when there is no license available for the requested application. The user can go to the license queue from here.

The following is an example of the page opened by HTML View when there is no license available for a requested application:



You can define the texts, illustrations and layout of the templates used when access is denied based on IP address. The templates included with the HTML View program serve as examples.



When editing the HTML-text modules in the first group, however, please observe the following: These templates were created using the Windows Editor, as this program can create a non-redundant and clearly structured HTML text module. When using an HTML editor, check whether it automatically adds HTML code that would preclude the template from functioning as an independent component. For example, the HTML editor might append an invisible `</html>` tag when you save a template. Some editors are generally unsuitable for processing format templates; for example, MS Word increases the volume of source code 20-fold when you save an HTML document.

Templates for Application Launch

Because HTML View can create syntactically correct configuration files (such as ICA and RDP files), templates for application launch are provided. These files are used with all layouts; in other words, they are not assigned to a certain layout directory, but are valid globally. These templates are stored under `\HTML-View\Launch`.

In the NetMan Web Services Settings you can define whether the application launched through HTML View runs on the client PC (launched by a NetMan start file) or on the terminal or MetaFrame server (in an RDP or ICA session). The type of launch can be selected by HTML View on the basis of client IP address or host name. The launch template directory contains the following files:

- `Start.nm`: This template is used when launching applications from within the browser to run on the client machine. This entails prior installation of the NetMan Desktop Client on the workstation.
- `Standard.ndp`: This is used for launching applications with the NetMan RDP Web client. You can specify the `StartApp` entry to define the application that runs in the session. If you work with anonymous users, the starting program is already defined. In this case, the `StartApp` entry has no effect. This entry is generally required for users who can launch applications using a NetMan start file and access a terminal directly, for whom you cannot define a starting program in the user account settings.
- `Standard.ica`: The `Standard.ica` template contains instructions for generating ICA files. In most cases, nothing needs to be added or modified here, since all required settings can be configured in the NetMan Web Services Settings. For more information on this file, please see "*Citrix Web Client*."
- `Citrixjava.htm`: This HTML page is the template for executing a session using the Citrix Java client. It contains Java scripts that define, for example, the size of the browser window. The variables `JavaWindow` and `JavaSeamless` define important properties of the Java applet. Please refer to the Java administrators' manual from Citrix for details on these settings.
- `Citrixautodetect.htm`: This HTML page is used when **Select ICA automatically** is specified for the launch method. With this page, the browser determines whether the ICA session is launched using the Citrix Web client or the Citrix Java client.
- `Rdpjava.htm`: This HTML page serves as the template for calling sessions using the RDP Java client.

Placeholders in Templates

The placeholders listed here can be added to templates. HTML View inserts texts as indicated by the placeholders when a given HTML page is sent to a Web browser. HTML View can retrieve these texts from any of a number of sources, such as databases or application launch links. The list below describes the placeholders in detail:

- @NM_LAUNCH: Contains a link that launches a NetMan configuration.
- @NM_PROMPT: Contains the name of the configuration.
- @NM_DESCRIPTION: Contains the description of the configuration.
- @NM_INFO: This is a link to the information file for a configuration.
- @NM_INACTIVE: Inserts the message to be shown when a deactivated configuration is requested.
- @NM_CATEGORY: Contains the category of a configuration.
- @NM_URLCATEGORY: Contains the category of a configuration, with any spaces replaced by underline characters (“_”). This makes the category name URL-compatible.

Using Style Sheets

Because page formatting with the HTML View is distributed over a number of independent HTML text components, it can be difficult to change a format. This is why the default formatting files in `Default.htm` use style sheets. You can use the `_nm.css` style sheet to change fonts and font sizes. This style sheet is used, for example, by the `Folder_Embedded.txt` file.

Practical Example: Using the HTML View List View

Customizing formats with the HTML View is easier to do than it is to describe here. If you already have experience in Web design, you can probably integrate the basic HTML View functions in your Web without even reading this manual, as most of the modifications involve standard, as opposed to NetMan-specific, operations. We have seen a wide variety of original NetMan HTML page designs created by our customers.

Here is just one example:

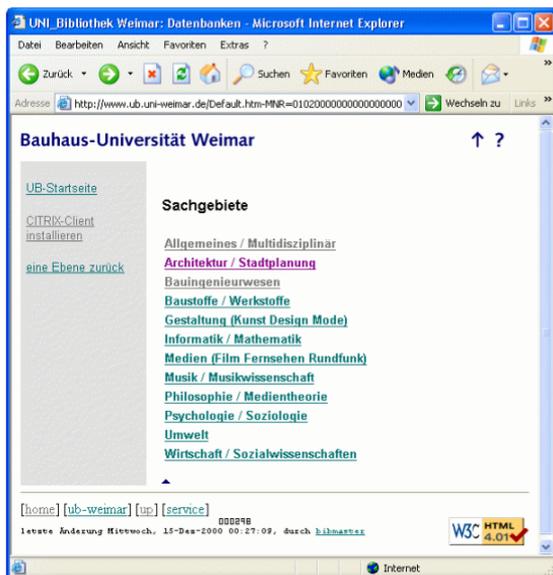


You can hardly tell that HTML View is even used here, thanks to the nested desktop format.

The desktop has two lower levels, organizing their spectrum of information by alphabet in the one folder:



and by topic (“Sachgebiete”) in the other:



Under “Architektur/Stadtplanung” (Architecture/City Planning) we find a range of information that contains both hyperlinks and applications; the latter run on a terminal server:



Thus NetMan is completely invisible to the user, and operates only as information and application management software in the background. In the foreground are the presentations and information provided by the institution deploying NetMan.

Configuring the HTML View Explorer View

The web interface uses the latest web design tools, making it well-structured and easy to understand. There are two main areas in which you can modify the formatting:

- Login page
- Application launch interface

The HTML pages use CCS files for formatting and all Java scripts are stored in script files. These two areas are described in detail in the next sections.

Modifying the Login Page

The login page is stored in the `\WebSrv\hh\common\login` directory. This directory contains English (`login.htm.en`) and German (`login.htm.de`) versions. The `hh.css` and `hh-login.css` files are the cascading style sheets that determine the format of the login page. The `hhlib.js` file is a JavaScript file that generates the login form and checks whether cookies are enabled in the client browser. The NetMan web interface requires cookies. The JavaScript creates input fields within the `<div>` tags using `id="form-line"`. This is why this part of the HTML page must not be modified or removed.

In this example, a company logo is added to the login form, centered at the top of the page. To do this, simply add the company's logo graphic with an `` tag before the `<div>` tag containing `id="fenster"`. The `<p id="claim"></p>` tag centers the graphic:

```
010 <body onLoad="show_clock()">
011   <p id="claim"></p>
012   <div id="fenster">
013     <div id="header">
014       <p>Login</p>
015     </div>
016     <div id="image_box">
017       
018     </div>
```

The result might look like this:



Modifying the HTML Page for Launching Applications

HTML pages for presenting applications to users are stored under `\WebSrv\hh\HTML-View\Desktop`. The default installation includes versions in English (`default.html.en`) and German (`default.html.de`).



The language used in the client browser determines which version opens. If the browser uses German, the German page opens. The English version opens for all other browser languages.

The layout is determined by the `<div>` tags:

- `window_box` – The frame that encloses all of the following elements.
- `header` – The title bar of the frame; shows the name of the desktop displayed.
- `content_box` – The frame around the area containing the application names (content).
- `content` – The area in which the applications are listed in table form.
- `info_box` – A frame around the area in which the title and description of an application is displayed.
- `info` – The area containing the title and description of an application.
- `treebox` – The frame around the area showing the directory structure of the applications.
- `netmantree` – The directory structure for the applications.
- `footer` – The footer containing the datetime and footermenu elements.
- `datetime` – The date and time in the footer.
- `footermenu` – The menu bar for the interface.

The steps in this example modify the application launch page as follows:

- A company logo is added, centered at the top of the page
- The area showing application titles and descriptions is removed

As described above in the example of a modification in the login page, the company logo is inserted in the desired position:

```
001 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
    "http://www.w3.org/TR/html4/strict.dtd">
002 <html>
003   <head>
004     <title>NetMan HTML View</title>
```

```

005     <meta http-equiv="Content-Type" content="text/html;
charset=iso-8559-1">
006     <link href="hh.css" rel="stylesheet" type="text/
css">
007     <script language=javascript src=nmjson.js></script>
008     <link rel="StyleSheet" href="dtree.css" type="text/
css" />
009     <script type="text/javascript" src="dtree.js"></
script>
010 </head>
011
012 <body onLoad="show_clock()">
013     <p id="claim"></p>
014     <div id="window_box">
015         <div id="header">
016             <!--<p>Desktop title</p>-->
017         </div>

```

To remove the area that shows application names and descriptions, modify the `hh.css` file. This modification entails only changing the format for display of this area; deleting the corresponding lines from the HTML file could result in JavaScript errors. The relevant lines in the original `hh.css` file are changed as shown below, with the result that the area showing application titles and descriptions is no longer shown and the area listing the applications is larger:

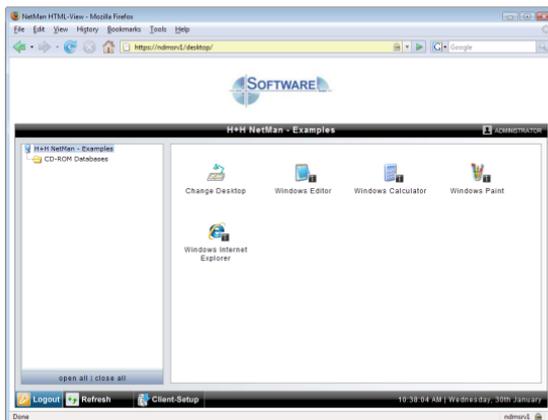
```

001 #content_box {
002     width: 654px;
003     height: 425px;
004     border: 1px solid #8c8c8c;
005     background-color: #ffffff;
006     position: absolute;
007     right: 10px;
008     top: 34px;
009 }
010 #content {
011     width: 652px;
012     height: 423px;
013     overflow: auto;
014     text-align: left;

```

```
015 position: absolute;
016 right: 0;
017 top: 0;
018 }
019 #info_box {
020 width: 0px;
021 height: 0px;
022 border: 0px solid #8c8c8c;
023 background-color: #ffffff;
024 position: absolute;
025 right: 10px;
026 bottom: 40px;
027 }
028 #info {
029 width: 1px;
030 height: 1px;
031 overflow: auto;
032 text-align: left;
033 position: absolute;
034 right: 0;
035 top: 0;
036 }
```

The result is shown in the following browser window:



Opening Sessions from NetMan Desktop Client

This chapter gives you an overview of the launch methods for the NetMan Desktop Client and the login methods for logging in on terminal servers from the Desktop Client.

For an overview of launch methods, see “*Launch Methods for NetMan Desktop Client*.” The following launch methods are described there:

- NetMan RDP web client
- Citrix web client

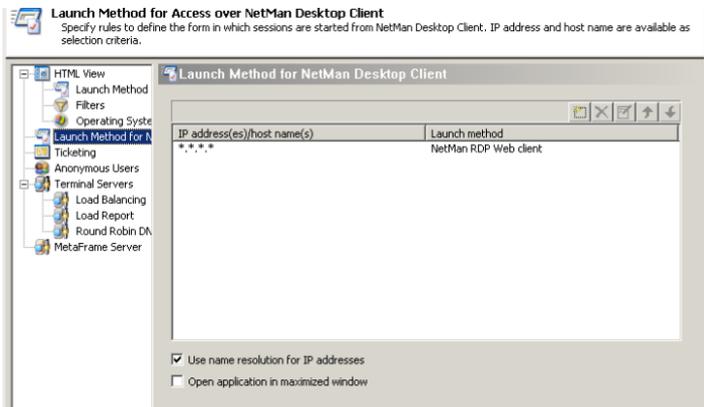
The chapter entitled “*Rules for Determining the Launch Method*” describes how to configure rules in the NetMan Web Services settings that determine which stations use which launch method.

For an overview of login methods on terminal servers, see “*Login Methods on Terminal Servers*.” The following login methods are described there:

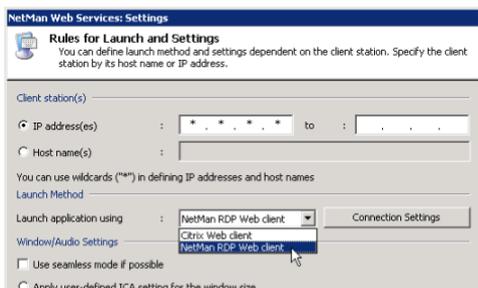
- Use local login data
- One-time login using NetMan Desktop Client
- Interactive login per session
- Use NetMan anonymous users

Launch Methods for NetMan Desktop Client

The NetMan web services provided in your NetMan Desktop Client Manager identify the client station by its IP address or host name and uses this as the basis to determine which launch method, with which settings, shall be applied for launching a session. Run the NetMan Web Services Settings program and select **Launch Method for NetMan Desktop Client** from the sidebar:



Select the *.*.*.* entry and click the **Edit** button. This opens the following dialog:



In the **Launch application using** field you can choose from the following launch methods:

NetMan RDP Web client. With this launch method, the NetMan web services create a configuration file for the NetMan RDP web client; i.e., for an RDP session.

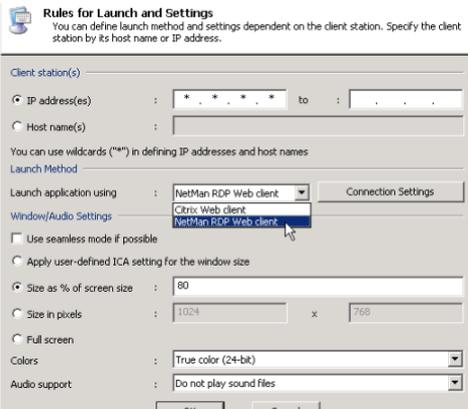
Citrix Web client. With this launch method, the NetMan web services create a configuration file for an ICA session.



If you select the Citrix client, you have to have both NetMan Desktop Client and an ICA client on the workstation. The ICA client may be either the Program Neighborhood or the Citrix web client.

Rules for Determining the Launch Method

NetMan web services use fixed rules to determine which launch method is applied for client workstations. Select the * * * * rule and click the **Edit** button, or click the **New** button, to open the following dialog:

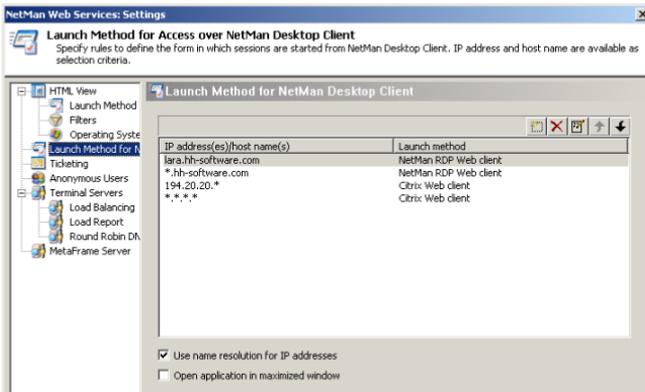


Set one of the following criteria in the NetMan web services for determination of the launch method:

- Client IP address, or
- Client host name

These settings are defined in the **Client station(s)** section. You can specify either IP addresses or host names. In either case, you can use an asterisk ("*") as a wildcard to specify a range of IP addresses or an entire domain.

Here is an example:



In this example, 4 rules have been defined for determining the launch method. The rules are processed in the order in which they appear in this list, from top to bottom. The first applicable rule found is applied. The following factors are taken into account in determining applicability:

- IP address or host name of the client station
- Existence of contradictory settings defined for the particular NetMan configuration (application call).

With the settings shown above, for example, if a workstation called *lara.hh-software.com* uses NetMan's web interface (HTML View) to access an application in NetMan, and no special settings are defined for the application call (see "Advanced Application Settings for a Session") then the first rule in the list is applied and the NetMan Desktop Client or NetMan RDP web client opens an RDP session. If a different workstation from the *hh-software.com* domain calls an application using NetMan Desktop Client, the second rule in the list is applied. There can be different settings configured for the first and second rules in this list. The rule defined for the *.*.* IP address is a default rule, and should apply in all cases in which the rules above it do not apply. If you use MetaFrame, we recommend including a default rule that specifies the Citrix Web client launch method. For terminal server environments without MetaFrame, specify NetMan RDP Web client in a default rule.

Criteria are applied in the following order:

- Settings for a particular NetMan configuration (application call) override the rule applied by HTML View.
- Which rule is applied is determined on the basis of IP address/host name and browser agent.



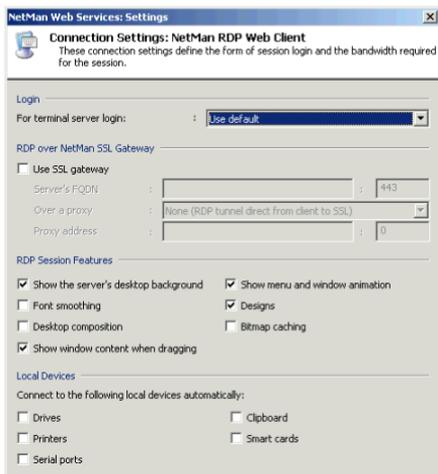
It is possible, particularly if special settings are configured in the application call, that none of the rules can be applied. We recommend formulating simple rules and making sure there is always at least one rule that can be applied in any case. For example, if no rule is defined under **Launch Method** that applies to the Citrix web client, but the Citrix web client is explicitly designated for launch in a particular NetMan configuration, NetMan web services cannot provide connection data for a session for that configuration.

NetMan RDP Web Client

With the NetMan RDP Web Client launch method, the NetMan web services generate a configuration file with which the NetMan Desktop Client initiates an RDP session on a terminal server. You can configure the following settings for an RDP session:

- Connection Settings
- Window/Audio Settings

To configure the connection settings, select **NetMan RDP web client** and click on the **Connection Settings** button. This opens the following dialog:



The settings options are divided into three categories:

- Login
- RDP Session Features
- Local Devices

In the **Login** section you can define how users are logged on in sessions. This setting overwrites the settings selected under **For terminal server login** on the **Terminal Servers** page. Thus you can enable users from specified IP addresses or domains to use a different login method than the default.

The settings in the **RDP Session Features** section primarily affect the bandwidth for the session:

Show the server's desktop background. Shows the server's desktop in the background of the session.

Show window content when dragging. Shows the content of the window while the window is being moved. If this setting is not selected, only the outline is shown while the window is being moved.

Show menu and window animation. Shows menu and window animation in the session.

Designs. Enables a choice of designs for the “look and feel” of the interface (e.g., Classic Windows, Windows XP).

Bitmap caching. When this setting is active, frequently used images are stored on the local machine to reduce the volume of data traffic.

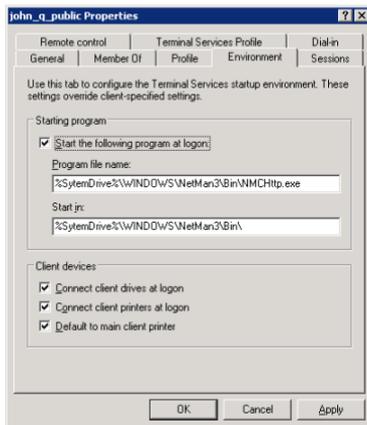
In the **Local Devices** section you can specify which of the devices on the workstation are automatically connected in the terminal server session:

Drives. Automatically connect local drives.

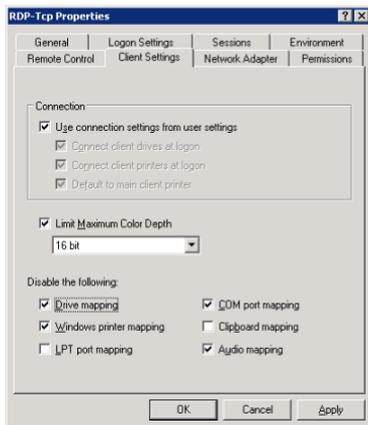
Printer. Automatically connect local printers.

Serial ports. Automatically connect local serial ports.

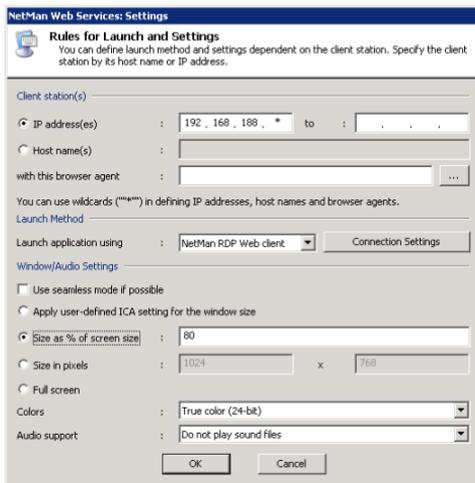
Your settings under **Local Devices** overwrite any settings for these features configured in the user properties:



If connection of local devices is deactivated in your settings for the RDP session, these connections cannot be activated in the user properties defined in the operating system, nor in the workstation's **Local Devices** settings:



Under **Window/Audio Settings** you can define session properties such as window size, color depth, and audio support:



The NetMan desktop client and NetMan RDP web client support the following functions:

- Session window in full-size mode
- Session window with specified width and height (e.g., 1024x768 pixels)

- Session window with size as a percentage of screen size (with reference to the workstation)
- Seamless mode (the user sees only the application window, not the session window)
- Supported colors: 256 colors, high color (15-bit), high color (16-bit), true color (24-bit)
- Audio support
- Access to client drives from within the session
- Access to client printers from within the session
- Access to a universal PDF printer driver



There are a number of properties for an ICA connection that are rarely used and which cannot be configured in the dialogs shown above. You can enter these settings directly in the template file for the RDP session, `Standard.ndp`, in the `%NMHOME%\WebSrv\HH\HTML-View\Launch\` directory.

Citrix Web Client

With the Citrix web client launch method, the NetMan web services generate a configuration file for an ICA client. The ICA client then establishes the connection to a MetaFrame server.



If you select the Citrix client, you have to have both the NetMan Desktop Client and an ICA client on the workstation. The ICA client may be either the Program Neighborhood or the Citrix Web client.

You can configure the following settings for an ICA session:

- Connection settings
- Window/audio settings

To configure the connection settings, select the **Citrix web client** launch method and click **Connection Settings**. This opens the following dialog:



This manual does not go into detail concerning ICA-specific configuration options. The dialogs are generally adapted to those used in the Citrix Program Neighborhood and are described in the relevant Citrix manuals.



Citrix sessions are always called using the published applications mechanism. With this technique, load balancing with the ICA protocol can also be supported by NetMan. With the default settings, NetMan uses one Citrix published application (see *“Published Application”* in the section entitled *“Extensions for MetaFrame Servers”*). Prerequisite is that all applications are installed on all servers for correct functioning of load balancing under Citrix. If this is not possible, you can configure the published application in the NetMan configurations. For information on this option, please see *“Separate Session Parameters for an Application Call”* in the chapter entitled *“Advanced Application Settings for a Session.”*

Under **Window/Audio Settings** you can define session properties such as window size, color depth, and audio support:

This client supports the following functions:

- Session window in full-size mode
- Session window with specified width and height (e.g., 1024x768 pixels)
- Session window with size as a percentage of screen size (with reference to the workstation)
- Seamless mode (the user sees only the application window, not the session window)
- Supported colors: 16 colors, 256 colors, high color (16-bit), true color (24-bit)
- Audio support
- There might be a proxy or a firewall between the workstation and the MetaFrame server
- Access to client drives from within the session
- Access to client printers from within the session



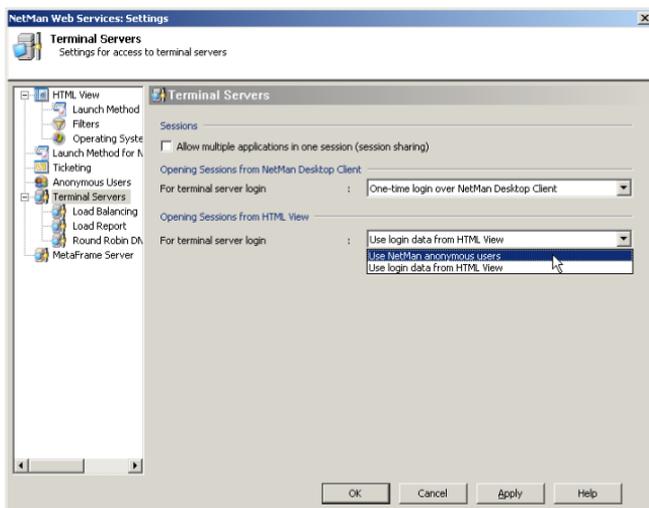
There are a number of properties for an ICA connection that cannot be configured in the dialogs shown above. You can configure these settings directly in the template file for the ICA session launch, `Standard.ica`, in the `%NMHome%\WebSrv\HH\HTML-View\Launch\` directory.

Login Methods on Terminal Servers

As described in the previous chapters, the applications are generally launched in application sessions on the terminal server. NetMan Desktop Manager provides a number of options for logging in on these application sessions. The following four options are available for login over RDP:

- Use local login data (RDP protocol)
- One-time Login using NetMan Desktop Client
- Interactive login per session
- Use NetMan Anonymous Users

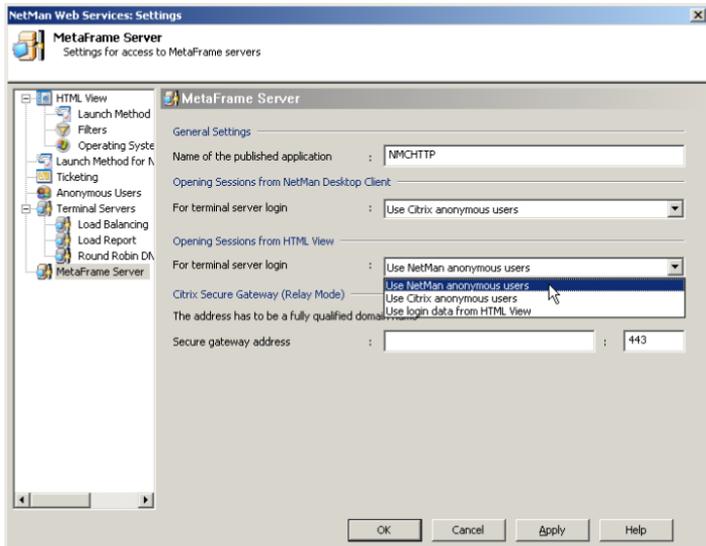
These settings are configured in NetMan web services. Run the NetMan Web Services Settings program from the Toolbox and open the **Terminal Servers** page. Select the desired login method in the **Opening Sessions from NetMan Desktop Client** section:



If the terminal server is accessed over ICA on a MetaFrame server rather than over RDP, the login method is configured on the **MetaFrame Server** page of the NetMan Web Services Settings program. The following options are available:

- Use NetMan anonymous users
- Use Citrix anonymous users
- Use local login data (ICA protocol)

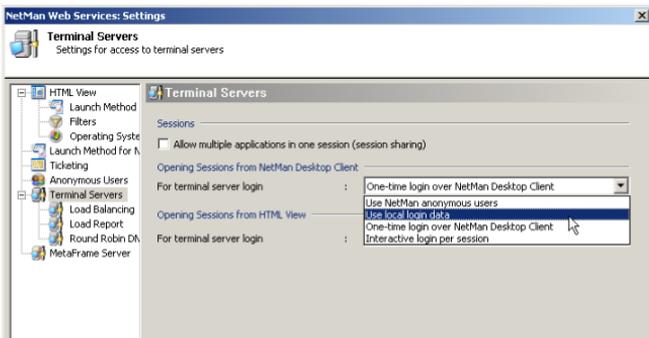
Select the desired option under **Opening Sessions from NetMan Desktop Client**:



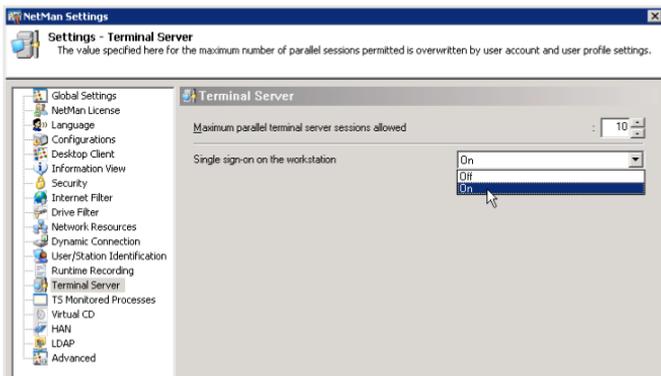
The different methods are described in detail in the following sections (“Use Local Login Data,” “One-time Login using NetMan Desktop Client,” “Interactive Login per Session,” “Use NetMan Anonymous Users”).

Use Local Login Data

To have the same login data used for terminal server sessions as is used for login on the local workstation, select the **Use local login data** option under **Opening sessions from NetMan Desktop Client** in the NetMan Web Services Settings program:

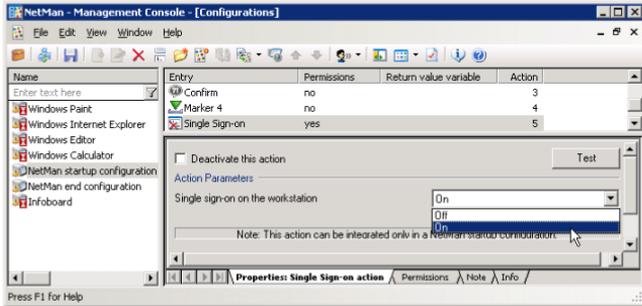


In addition to this setting in the NetMan web services, one other setting must be configured in the NetMan Settings program (as opposed to NetMan Web Services Settings program). Open the **Terminal Server** page and set the **Single sign-on on the workstations** option to "On". This is a global setting; in other words, it is applied to all workstations and all terminal servers on which the NetMan Client is installed.



When you switch on the single sign-on mechanism, an additional network provider is installed to provide the login data as needed for application sessions. When this setting is activated, the user must log in on the workstation twice before the local login data can be used for application sessions. The first login installs the new network provider, and the second supplies the user's login data to the network provider. This "double login," while inconvenient, is only required immediately following a change in the single sign-on setting, which generally does not occur often.

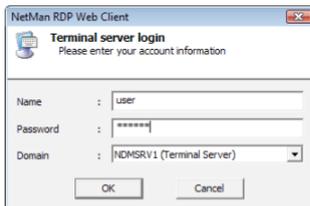
You can activate this setting selectively; for example, if you do not wish to enable single sign-on for all workstations. To do this, add a *Single Sign-on* action to a Startup configuration and set the 'execute' permissions so that it runs only for your choice of workstations and servers:



To use single sign-on, this mechanism must be enabled for the NetMan Desktop Clients on all terminal servers on which application sessions run.

One-time Login using NetMan Desktop Client

When users call applications that are offered by NetMan Desktop Manager, you might wish to have them carry out a one-time login on the NetMan Desktop Manager. After NetMan Desktop Client is launched and the first time an application is called, the user is prompted to enter login data for all session calls:



Following successful login on an application session, the user does not have to log in again until the next time he or she launches NetMan Desktop Client.



The down arrow next to the **Domain** field opens a list of all available domains in the network. These are not necessarily the same as the login domains for the terminal server. You can restrict the choices offered in this list to a certain set of domains by storing a list of the desired domains in a template file called `Standard.ndp`. In the `[Connection]` section in that file, use `DomainList` to store the desired entries, separated by commas. For example, if you wish to permit login only in the MYDOM1 and MYDOM2 domains, change `DomainList=@NM_LIST_DOMAIN` to `DomainList=MYDOM1,MYDOM2`.



To use this login method, the single sign-on mechanism must be enabled for the NetMan Desktop Clients on all terminal servers on which application sessions run.

Interactive Login per Session

If the **Interactive login per session** option is enabled, users have to log in on the terminal server every time they open an application session. If the application session is a seamless session, the login dialog is the same as that opened for “One-time login using NetMan Desktop Client:”



If the application session is opened in a window, the login dialog is the same as that usually opened for login on a workstation or a server:



Use NetMan Anonymous Users

Rather than using a specific user account, terminal server sessions can be opened by NetMan anonymous users. This feature is configured on the **Terminal Servers** page of the Web Services Settings. Under **For terminal server login** in the **Opening Sessions from HTML View** section, select **Use NetMan anonymous users** and save the change. From this point on, all sessions run under a NetMan anonymous user account. This feature requires configuration of anonymous users in your NetMan installation, the procedure for which is described in detail in the section "*Anonymous Users.*"

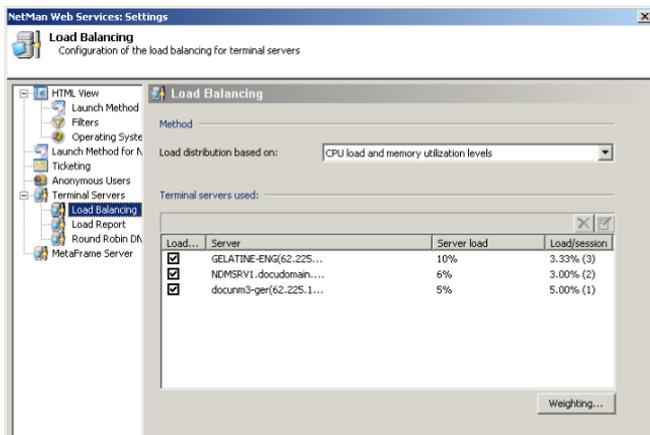
Extensions for Terminal Servers

This chapter gives you an overview of several optional functions in the NetMan program for use with your terminal servers:

- “Load Balancing in Application Sessions” describes how to connect your servers in a load balancing cluster.
- “*Load Report*” describes the performance report for monitoring loads in your load balancing servers.
- “Session Sharing” describes how to use the session sharing function.
- “*NetMan RDP Session Broker*” describes how you can use the NetMan RDP session broker for load balancing with thin clients.

Load Balancing in Application Sessions

NetMan implements load balancing based on the number of sessions opened on terminal servers, or based on the use of server resources, in a server farm. In the NetMan Web Services Settings program, the **Terminal servers used** section on the **Load Balancing** page lists the load balancing servers on which application sessions run:



There are two methods to choose from for load balancing:

- Distribution based on number of sessions
- Distribution based on CPU load and memory use

The list of terminal servers is compiled automatically. When you install NetMan Desktop Client on a terminal server, that server is added to the list a few moments later.

Which information is shown in the list depends on the load balancing method used. With distribution based on number of sessions, the following is shown:

- A checkbox indicating whether the server is used in load balancing
- The server name and IP address
- An alternative IP address to be used for opening sessions
- Weighting in %, indicating the possible load on the server in relation to the server farm
- Number of connected sessions

Load...	Server	Alternate address	Weighting in %	Sessions
<input checked="" type="checkbox"/>	GELATINE-ENG(62.225...		Automatic (33%)	3
<input checked="" type="checkbox"/>	NDMSRV1.docudomain....		Automatic (33%)	3
<input checked="" type="checkbox"/>	docum3-ger(62.225.1...		Automatic (33%)	2

With distribution based on **CPU load and memory utilization levels**, the following is shown:

- A checkbox indicating whether the server is used in load balancing
- The server name and IP address
- The current server load in %, calculated from a weighted combination of CPU and memory utilization
- Load as a percentage of total current load and, in parentheses, the number of sessions currently active on the server

Load...	Server	Alternate address	Server load	Load/session
<input checked="" type="checkbox"/>	GELATINE-ENG(62.225...		8%	2.67% (3)
<input checked="" type="checkbox"/>	NEMSRV1.docudmain...		16%	5.33% (3)
<input checked="" type="checkbox"/>	docum3-ger(62.225.1...		18%	9.00% (2)

You can configure the following settings for the terminal servers listed here:

- Belongs to the load balancing cluster (yes/no)
- Use specified alternate IP address or host name for establishing an RDP connection
- With distribution based on number of sessions: Weighting assigned within the load balancing cluster.
- With distribution based on CPU load and memory utilization: The 100% value for the “pages per second” performance indicator. As a rule you will not need to set this value manually, because it is determined automatically and updated continuously.

When your terminal servers are banded together in a load balancing cluster, the NetMan Web Services select a terminal server for application execution when an application call is activated in a session. Which method is used for selecting a server depends on the load balancing technique selected.

The first technique described in the following is **Distribution based on number of sessions**.

With this technique, the selection is made based on the number of sessions open on each server and the **Weighting in %** setting, which you can define for each server. The default setting for this feature is **automatic weighting**, which provides for even distribution of sessions among all servers. The load percentage is shown in parentheses; for example, **Automatic (50%)** (with two servers). You can specify an explicit percentage for a given server if desired. The number of sessions is shown in the last column.

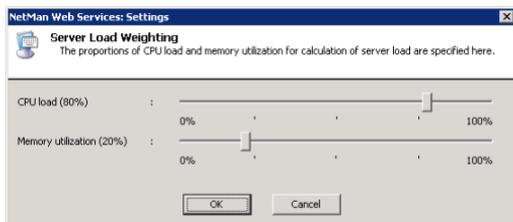
This value is updated once per second.

If a given terminal server does not respond for a certain period of time, it is no longer included in load balancing and the number of sessions is replaced with a dash (“-”). Servers can be removed from the load balancing cluster under certain circumstances, as detailed below:

- Terminal servers report the number of sessions active every 30 seconds, and additionally any time the number changes. If a given terminal server does not report any number of sessions for a period of 2 minutes, that server is removed from the load balancing cluster.
- When a terminal server is shut down, it is removed from the load balancing cluster.
- If the NetMan Client Service on the terminal server is ended, the terminal server is removed from the load balancing cluster.

With the other technique, **Distribution based on CPU load and memory utilization**, sessions are distributed based on a weighted calculation of CPU and memory load.

In this case, you (as administrator) need only define the percentages of CPU load and memory utilization used for calculating the server load. Click on the **Weighting...** button to open the dialog for setting these values:



In the example shown here, the CPU load makes up 80% and memory utilization makes up 20% of the server load.

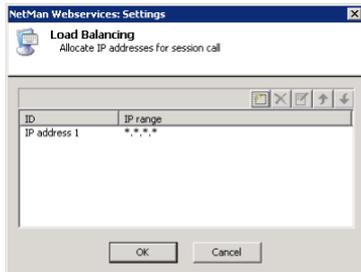
- The CPU load referred to here is the value shown by the Task Manager.
- The memory utilization level is measured by the number of memory pages (4 KB each) transferred per second between main memory and hard drive. Full utilization is the 100% value for pages per second. This value is a good indicator that the memory capacity is approaching its limitations, as this is the point at which memory content is cached to the hard drive.

The server load calculated from these values is the basis for distribution of new sessions as they are opened. The server with the lowest load is used to open the next session requested, and is then allotted the current average load level so that subsequently, as a rule, a different server has the lowest load. With this method, too, a dash (“-”) shown in the last column indicates that the corresponding terminal server is no longer a part of the load balancing cluster.

In some environments, RDP sessions are opened with a different IP address than the one registered in the NetMan Service for the terminal server. This is the case when all terminal servers have two network cards, one of which is used for a dedicated network connection with a NetMan file server and the other for operating RDP sessions. This is why an option is provided for allocating an alternative IP address to each terminal server to be used for RDP sessions. To enter this alternative address, select the terminal server in the list and click on the **Edit** button:



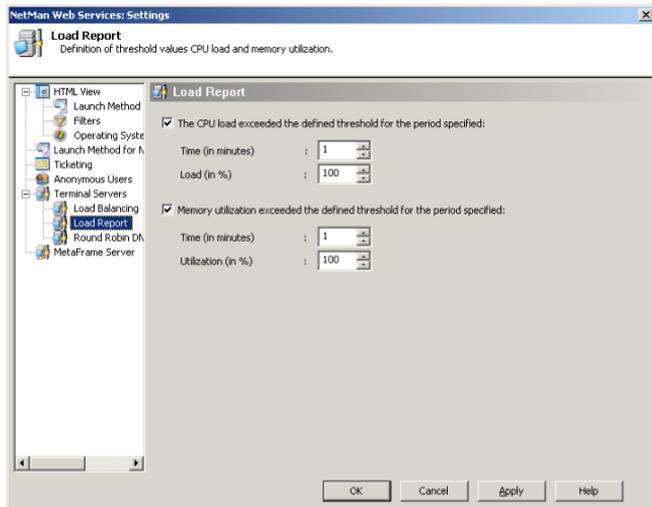
Under **Alternative IP addresses** you can enter an IP address to be used for the RDP sessions on this server. To have the alternative IP address used for all session calls, click on **Allocate IP range** and define a rule that allocates the alternative IP address to all clients:



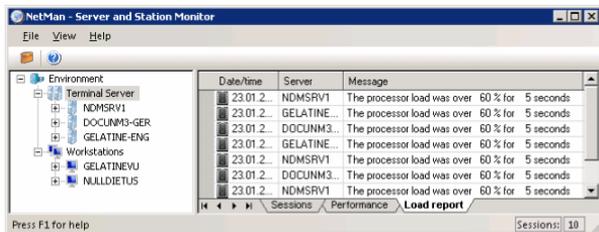
Note on load balancing: Once a session is opened on a terminal server for a particular user, any further sessions opened by that user are opened on the same terminal server. This is important, because a user profile configured for use on terminal servers cannot be used on more than one server simultaneously. If two terminal servers try to access a user profile at the same time, the profile might be corrupted. This mechanism takes precedence over other rules applied to load balancing.

Load Report

On the **Load Report** page you can configure limits for the CPU load and memory utilization. When a limit defined here is exceeded, this event is recorded in the Load Report:

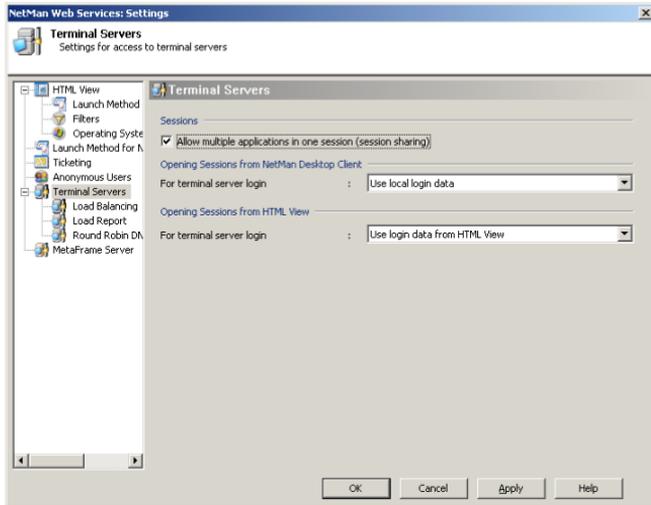


You can view and delete Load Report items in the **Server and Station Monitor**:



Session Sharing

Without NetMan's session sharing feature, each application called is opened in a new terminal server session. Thus each application runs in a separate Windows environment, even if they were all called by a single user. This can mean a heavy load on the server's resources. With session sharing, any additional applications run in the session that is already open. Prerequisite for session sharing is that the application sessions run in "Seamless Windows" mode. To enable session sharing, activate the **Allow multiple applications in one session (session sharing)** option:



The following conditions and restrictions apply when you use this function:

- Applications must execute in "Seamless Windows" mode. If an application is configured to open in a separate window, it will open in a separate session.
- All applications that can be opened in a single session (i.e., by a particular user) must have mutually compatible window and audio settings. For example, if sound support is active for the client in one application, but deactivated in another, the web services will open these two applications in two separate sessions.
- The various applications must have matching login data for terminal server sessions.

This means session sharing requires one of the following launch methods:

- Use local login data
- One-time login over NetMan Desktop Client
- Login data from HTML View

Session sharing will not work in sessions opened using the following launch methods:

- Interactive login per session
- Use NetMan anonymous users



When an application is opened in an existing session, the startup configuration is not executed again; only the NetMan configuration is executed in the session.



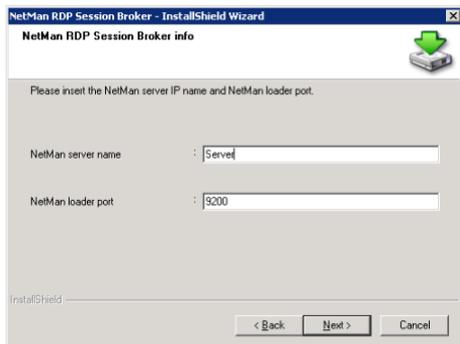
For applications that require exclusive access to a particular resource (such as a virtual CD-ROM drive), session sharing can be a disadvantage. We strongly recommend configuring settings which will ensure that such applications run in separate sessions; for example, by using anonymous NetMan users.

NetMan RDP Session Broker

The RDP Session Broker lets you use NetMan's load balancing features directly with thin clients. The RDP Session Broker is one of the services installed automatically with the NetMan server components. By default, the service is deactivated. If you have installed NetMan on a file server for multiple terminal servers, you can start the service in the Control Panel. When the thin clients log on to the Session Broker, the connection is automatically passed to the right terminal server. The thin clients must support RDP 5.2 or later.

Installing the RDP Session Broker

The RDP Session Broker is automatically installed on the server on which you install NetMan. All you need to do is activate it. You can install the RDP Session Broker on additional servers if desired; for example, to have a back-up installation available in case of server failure. The setup program is in the %NMHome%\System\Setups\NetMan RDP Session Broker directory. The setup program prompts you to enter the target folder, the name of the NetMan Desktop server and the loader port (default: 9200):



Following installation, the service must be configured and activated (see chapter “Configuring the RDP Session Broker” for details).

Configuring the RDP Session Broker

Before you can use the Session Broker, you need to configure and activate its functions. To do this, open the Control Panel on the NetMan Desktop Server (or other server, if configuring an additional installation) and select the **NetMan RDP Session Broker Settings** program:



Select the **Activate RDP Session Broker service** option. The Session Broker behaves like a Windows Server 2003 terminal server. To ensure that the server is available for remote administration over RDP, the RDP protocol must be directed to a different port. The default is port 3390; you can change this if desired. As soon as you start the service, the Session Broker uses port 3389, and the normal RDP protocol is routed to the port specified here. You can deactivate the service at any time in the **NetMan RDP Session Broker** program in the Control Panel.



For remote access to the Session Broker server over RDP, the alternate RDP port specified here must be entered in the Remote Desktop Client; for example: `mstsc.exe /v:server:3390`.



The Session Broker can operate only in an environment with multiple terminal servers. If you run NetMan Desktop Manager on a standalone terminal server, do not activate this service.

Accessing the NetMan RDP Session Broker

To enable access to the NetMan RDP Session Broker for your thin clients, simply specify the NetMan server in the clients' configuration. With this configuration, thin clients show a different login screen:



The login procedure is basically the same as before. Which domains are available to choose from is configured in the Web Services settings, on the **HTML View** page, under **Login form**. The domains specified there for HTML View apply for the Session Broker as well. If desired, you can configure defaults for all login fields (user name, domain, and password). Following successful login, the client is automatically connected to the right terminal server. Distribution is carried out in accordance with the load balancing rules defined in NetMan Desktop Manager. Disconnected sessions are reconnected automatically.

Prerequisite for access to the Session Broker is an RDP client that supports RDP 5.2 or later. If the client supports only RDP 4, for example, the login screen shows a reminder to use an RDP 5 version.



This limitation is due to the fact that the RDP 4 protocol does not support the functions required for session brokering.

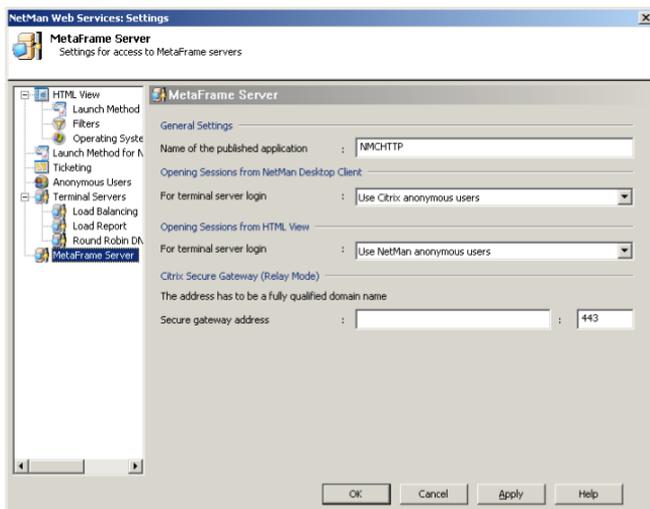
Extensions for MetaFrame Servers

This chapter gives you an overview of several functions in the NetMan program for use with your MetaFrame server:

- “Published Application” describes how to configure the published application.
- “*Login Methods on MetaFrame Servers*” describes the various methods for logging in on the MetaFrame server from the NetMan Desktop Client.

Published Application

The published application, required when you use the MetaFrame Server add-on, is configured in the NetMan Web Services Settings program, on the **MetaFrame Server** page:



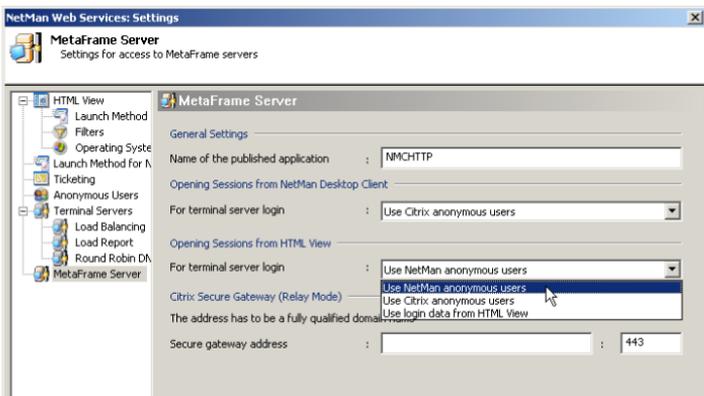
Under **Name of the published application**, enter the name used to identify `NMCHTTP.exe` in the Citrix Management Console. You can accept the default, `NMCHTTP`, if applicable. Application sessions started through NetMan Desktop Client use the name entered here for the published application to establish the ICA connection.



You can change program name (default: `NMCHTTP`) if desired, in the rules defined under **Launch Method for NetMan Desktop Client** and in the advanced settings for applications (see *"Separate Launch Method Settings for an Application Call"* for details).

Login Methods on MetaFrame Servers

On the **MetaFrame Server** page of the NetMan Web Services settings program, there are three options available for user login on a terminal server session:



Use NetMan anonymous users. In application sessions started through NetMan Desktop Client, users are logged on using NetMan anonymous user accounts.

Use Citrix anonymous users. In application sessions started through NetMan Desktop Client, users are logged on using Citrix anonymous user accounts.

Use local login data. With this login method, the local login data from the local workstation is used for login on an application session.



On a stand-alone server, implementation of Citrix anonymous users (Anon001 through AnonXXX) is not complicated. If you use multiple MetaFrame servers, however, we recommend working with NetMan anonymous users.



With the **Use local login data** option, the Citrix client on your local workstations must be configured accordingly. The first prerequisite for use of this mechanism is the installation of Program Neighborhood on the workstation. The next step is to select **ICA Settings** from the **Tools** menu and switch on pass-through authentication. This must be configured on the workstation by a user with administrative rights, because **PNSSON** is entered in the **HKLM\System/CurrentControlSet/Control/NetworkProvider** registry section as a new network provider. The **Ssonsvr.exe** program from Citrix is activated at the next user login and detects the user login data.

To enable this invisible login function when using an ICA file as well, enter `EnableSSOnThruICAFile=On` in the **[WFClient]** section of the `%AppData%\ICAClient\APPSRV.INI` file. Program Neighborhood does not offer an interface for configuring this setting.

Advanced Application Settings for a Session

This chapter gives you an overview of session settings that you can define for individual applications using the Management Console:

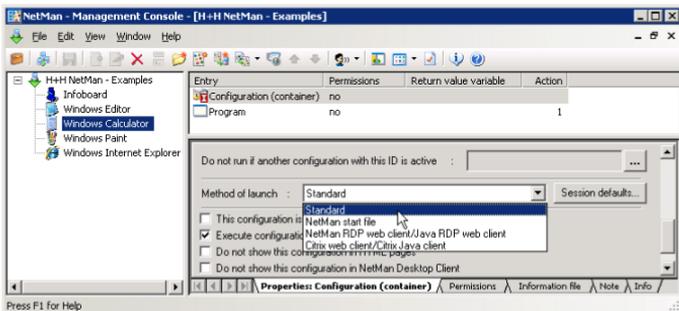
- “Separate Launch Method Settings for an Application Call” describes how to define a launch method for a particular application that differs from the global default launch method.
- “*Separate Session Parameters for an Application Call*” describes how to define session settings for a particular application that differ from the global default session settings. These may include performance settings for the session, for example, or the use of an SSL-secured connection over the NetMan SSL Gateway.

Separate Launch Method Settings for an Application Call

In the scenarios described up to now, settings such as launch method and the associated parameters were applied universally to all applications. In other words, settings for launch method and session parameters are independent of the application called. With NetMan, you have the option of configuring application-specific settings for the following:

- Launch method
- Session parameters

To do this, open the NetMan Management Console and select a configuration:



Under **Method of launch**, you can choose from the following options:

Standard. With this setting, the launch method for this application is determined based on the rules for determining launch methods configured in the NetMan web services settings.

NetMan RDP web client. With this setting, the application is launched using the RDP protocol.



Make sure there is a rule defined in the NetMan Web Services Settings program that is applicable to the stations that call this NetMan configuration, and that uses the NetMan RDP web client launch method. Otherwise, this application call will not find the connection settings for the RDP session.

Citrix web client/Citrix Java client. With this setting, the application is launched using the ICA protocol.



Make sure there is a rule defined in the NetMan Web Services Settings program that is applicable to the stations that call this NetMan configuration, and that uses the Citrix web client launch method. Otherwise, this application call will not find the connection settings for the ICA session.

Separate Session Parameters for an Application Call

You can configure separate settings for an individual NetMan configuration not only for the launch method, as described above, but also for session parameters. To do this, click the **Session defaults** button next to the **Method of launch** field.

NetMan - Management Console

Session defaults for the 'CALCULATOR' configuration
Specify settings that will be active by default in the particular session when the configuration is executed.

Use configuration-specific settings for the session

Settings for the Remote Desktop

Window settings:

Seamless :

Size :

Colors :

Audio settings:

Audio :

Login details:

User name :

Domain :

Password :

Specify the server on which the application is installed.

Published ICA application :

RDP server for the application : ...

Select **Use configuration-specific settings for the session** to activate the settings in this dialog. Once the settings are active, you can modify the defaults for window and audio settings as desired. In some rare cases, it might be necessary to execute a certain application call under a user account other than that of the user who called the NetMan configuration; for example, if special privileges are required for the application. When this is the case, you can enter the required login data here under **Login details**.



Changing the user name for the application login does not change the user account recorded for data logging, statistics acquisition and station monitor functions.

The following example is from the Server and Station Monitor:

Station	User	Start time	Location
NULLDIETUS#2	ADMINISTRATOR	1/23/2009 12:5...	schappertt
NULLDIETUS#3	MMJUSTER1	1/23/2009 1:01...	schappertt
NULLDIETUS#4	MMJUSTER1	1/23/2009 1:02...	schappertt
NULLDIETUS#5	ADMINISTRATOR	1/26/2009 11:2...	schappertt

← Sessions

The settings in the last section relate to load balancing, which is described in more detail elsewhere in this manual. For the RDP protocol, the NetMan web services implement load balancing functions. Load balancing for the ICA protocol is implemented using the mechanism provided in a Citrix MetaFrame server farm. NetMan initially assumes that all applications are installed on all terminal servers in the cluster. If this is

not the case, configure the settings under **Server on which Application is Installed**. For an ICA session, specify the published application defined for this configuration in the Citrix Management Console under **Published ICA application**. For the RDP protocol, enter a list of the terminal servers on which the application is installed under **RDP server for the application**.



If you use a different published application, it is important to keep in mind that the program that is launched by the published application defined in the Citrix Management Console is also `NMCHttp.exe`. The only difference is in the name of the published application and the MetaFrame server for which it is configured.



If you operate four MetaFrame servers, for example, and a large number of applications, you might not wish to install all applications on all servers. You could install half of your applications on two servers, and the other half on the other two servers. This reduces the number of applications that can run on a server by 50%, which can improve stability, while at the same time ensuring that backups of all applications are available. In this case, you could set up published applications in the Citrix Management Console for each of your applications, and have them point to both of the servers on which the application are installed. Greater efficiency can be achieved, however, if you set up only two published applications. For this example we will call these "SERVER12" and "SERVER34." While SERVER12 calls the `NMCHttp.exe` program on servers 1 and 2, SERVER34 calls `NMCHttp.exe` on servers 3 and 4. Now all you have to do is install half of your applications on servers 1 and 2, and the rest on servers 3 and 4.

Tips for Operation in Terminal Server Environments

This chapter gives you an overview of possible solutions for known problems, such as what to do if an application doesn't launch as expected. It also provides a few tips on working with NetMan, such as how to use NetMan to switch the terminal server operation mode, or how to connect client drives in sessions.

Monitored Processes for Application Sessions

If you have already worked with application sessions, you may have noticed that the session sometimes does not close even though you have shut down the application you were using. Unlike desktop sessions, which you can close at any time by selecting **Log off**, the terminal server cannot always tell when an application session should be closed. Even after you have shut down your application, there are generally a number of processes still running in the background.

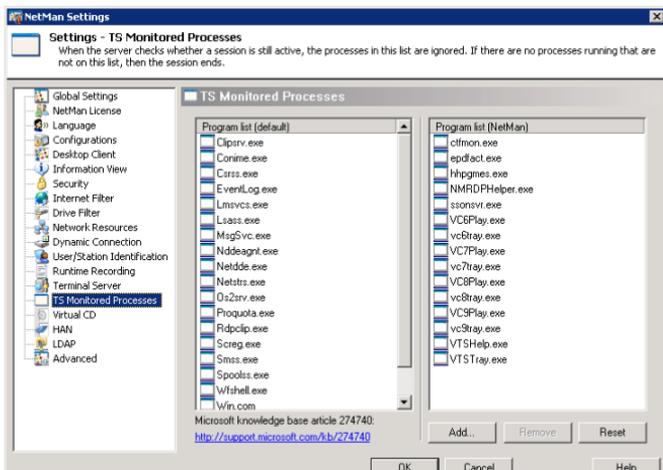
Generally, you want the sessions opened by your users to close again as soon as the user closes the application. To facilitate this function, Microsoft has implemented a process list, maintained by the operating system, which shows active processes that are not displayed in windows. Once there are no processes running in a session except those on this list, the operating system closes the session. The operating system does not, however, recognize all processes that can run in the background. The following two, for example, are not listed:

- Microsoft Office 2000: `ctfmon.exe`
- Acrobat Reader version 6.X: `wispptis.exe`

The following H+H products also run background processes in terminal server sessions:

- Virtual CD
- NetMan

On the **TS Monitored Processes** page of the NetMan Settings you can add your own list of background processes. Simply enter all the names of all processes that do not need to be shut down before the terminal server session is closed:



The user-definable list already contains a number of entries as soon as you install NetMan. These are H+H products that run in terminal server environments:

- `Epdfact.exe`: a component of the universal PDF printer driver from previous versions of NetMan Desktop Manager
- `Hhpgmes.exe`: a component of H+H ProGuard
- `NMRDPHelper.exe`: a component of NetMan Desktop Manager
- `VC9Play.exe`: a component of Virtual CD TS version 9.x or earlier
- `Vc9Tray.exe`: a component of Virtual CD TS version 9.x or earlier

Once there are no processes running in a session except those on these lists, `NMRDPHelper.exe` closes the session.



The `NMRDPHelper.exe` program must be included on the list so it can close the session.



The mechanism for monitoring background processes in application sessions is automatically active on all terminal servers on which the NetMan Desktop Client is installed.

Changing the Operation Mode: NMSTSMOD.exe

Most application setup programs make changes in the Windows directory of the workstation on which they execute; for example, they may create or modify DLL files, configuration files, INI files, or Registry entries. Depending on your configurations, clients in a terminal server environment may have their own Windows directories. If an application does not find the INI entries it needs, it copies the INI file (if available) from the central Windows directory to the user-specific Windows directory (=INI file mapping is ON). A similar mechanism provides the user with the required Registry entries. To ensure that these components are available to all users from the time the application is installed, it is important to switch the terminal server operating system to the “Install” mode (=INI file mapping is OFF) when installing an application. This way, the required information is provided by the operating system on a multi-user NT machine, and not only to the administrator account used to install the application.



When installing applications in “installation mode,” keep in mind that the current Windows directory during installation is the system Windows directory on the terminal server, and the application installation might impair server functioning. To avoid serious problems, we strongly recommend testing the setup beforehand on another workstation and using the NetMan Installer to monitor the components installed.

You can use a NetMan helper program to toggle between the “Install” and “Execute” modes. When you log on in a terminal server session and the NetMan Client is launched, the desktop contains a shortcut called **TS Mode** that launches this helper program:



Using this shortcut is equivalent to calling the “Change” program from the command line: `Change user /<install | execute>`. In the dialog box shown above, the current mode is “Install”. In the “Execute” mode, the Windows directory is in the “Profiles” subdirectory of the current user. When you use NMSTSMOD.exe to change to “Install” mode, the NetMan NMWinDir variable is set to %SystemRoot%. NetMan system programs (in this example, NetMan Installer) function properly during installation only if the NetMan Windows directory variable is set correctly. For example, this value enables the NetMan Installer Module to monitor the central Windows directories when applications are installed. This is why the NetMan Installer Wizard prompts you to change to the “Install” mode (if this is not the current mode) when it is launched in a terminal server environment, and always updates the NMWinDir variable.



The NetMan Installer module can be a tremendous help to you in a terminal server environment. Since software manufacturers do not usually supply information on the changes made on the server during installation of their programs, if you have to re-install the server at some stage, you have to re-install each of your applications as well. Scripts created by the NetMan Installer can save you a great deal of work in such cases. The same applies to load-balancing server farms; the NetMan Installer

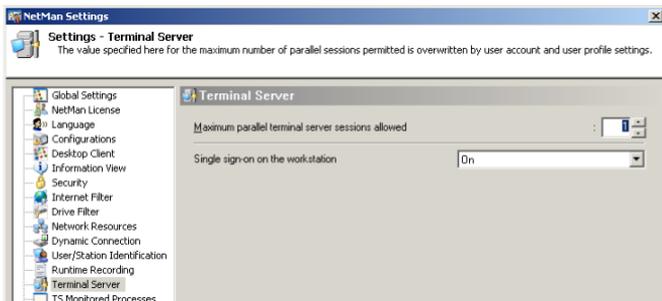
can save you having to install each application individually on each and every server. Another reason to use NetMan Installer in terminal server environments is because it documents which system components from which applications are installed or required. This information can be useful in tracking down and eliminating errors when running applications. It also helps to uncover potential incompatibilities. And last, but not least, this information can help you locate and fix any problems with the server that appear immediately following application installation.

Defining the Maximum Number of Parallel Sessions

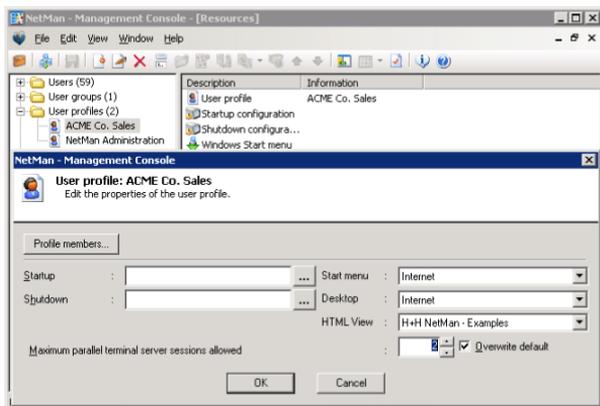
In many cases it can be useful to limit the number of parallel sessions that a single workstation can open. With NetMan, you can define not only whether parallel sessions are permitted, but also the maximum number of parallel instances allowed at any one time. If your NetMan configurations are launched on a terminal server, you may wish to limit the number of parallel sessions allowed for a given workstation. You can define a global limit as well as different limits for individual users and user profiles. If the number of parallel sessions is set to different values at different levels, the global setting is overwritten by a user-profile setting, and a user setting overwrites both of these.

Example:

We will start with a general rule that blocks multiple parallel terminal server sessions for all users. For this purpose, the default for maximum parallel sessions defined in NetMan's global settings is "1":



In the next step, we permit parallel sessions for users belonging to the "Acme Co. Sales" profile and set the maximum number of sessions to "2":



In the last step of this example, we permit administrators to open as many parallel sessions as they choose:

The screenshot shows the 'NetMan - Management Console' window for user 'System Administrator', last active on 2/1/2008. The window contains the following fields and controls:

- Name:** System Administrator
- Password:** [Empty field] with a 'View...' button.
- Address:** [Empty field]
- Phone:** [Empty field]
- Startup:** [Empty field] with a '...' button.
- Shutdown:** [Empty field] with a '...' button.
- Profile:** NetMan Administration with a '...' button.
- Start menu:** [Dropdown menu]
- Desktop:** [Dropdown menu]
- HTML View:** [Dropdown menu]
- Department:** [Empty field]
- E-mail:** [Empty field]
- Maximum parallel terminal server sessions allowed:** 99 with a '...' button and a checked 'Overwrite default' checkbox.
- Buttons:** OK and Cancel.

Membership in the “Acme Co. Sales” profile would not limit the parallel sessions to 2 for an administrator, because user account settings override both profile settings and default (global) settings. If a user tries to start more sessions than are allowed, an error message is displayed.



If the maximum number of sessions for a user is “0”, this user will not be able to run NetMan (i.e., launch a NetMan-controlled configuration) in a terminal server session.

Station Names in the Terminal Server Environment

In most aspects, the operation of NetMan in a terminal server environment is no different from its operation in a LAN. One important difference, however, is the way station names are assigned in the terminal server environment. NetMan obtains a unique ID for each station from the network operating system. Depending on your selection on the **User/Station Identification** page of the NetMan Settings, the station ID is either the user-defined computer name assigned under Windows, the network card address, the IP address or the full name stored on the DNS server. In a terminal server session, the station ID is obtained from the local client machine over the Client Network. Station IDs are recorded for a number of purposes in the NetMan program, including:

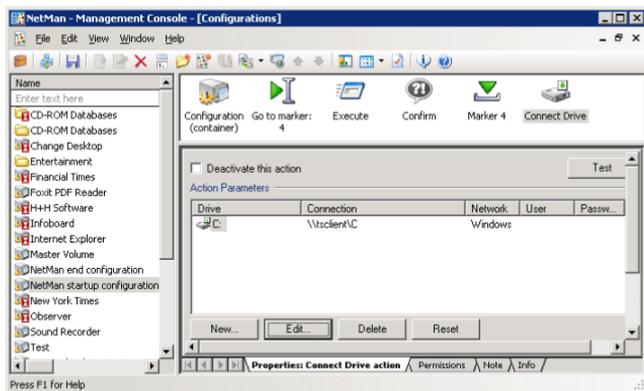
- Listing currently active stations
- Monitoring license use
- Assigning access privileges to applications and NetMan configurations
- Optional inclusion in the event log
- Calculating application-use statistics according to station

Since NetMan obtains the station ID from the network operating system, and the network requires a unique station designation, the uniqueness of the NetMan station ID is always assured by the network operating system in normal network operation. Only a single instance of NetMan can run on each workstation in a LAN. It is conceivable, however, that a single workstation accesses NetMan over the LAN in multiple instances, and at the same time opens multiple terminal server sessions.

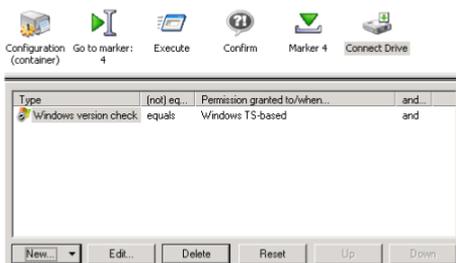
Because it is imperative that different sessions are distinguished from one another, both sessions and stations must be unambiguously identifiable because any given station in a network might open multiple parallel terminal server sessions. For this purpose, session numbers are appended to station IDs, using the format “#n”. For example, if NetMan establishes “MyComputer” as the station ID, then the station ID in the first terminal server session is “MyComputer#1”, in the second session “My-Computer#2”, and so on.

Mapping Client Drives

Terminal servers and MetaFrame servers offer options for integrating local resources on the client station into terminal server sessions. For example, you can either activate the **Connect client drives at logon** option in the user configuration, or you can map the desired drives in a login script. Another option is to map client drives in a NetMan startup configuration. If you do not want the same drives mapped at every startup and for every user, you can assign “execute” permissions to the action accordingly:



In the window shown below, the “execute” permissions assigned to the **Connect Drive** action ensure that it will be executed only on a terminal server:



If NetMan runs on only one terminal server and you want this action to be executed at every startup, then you do not need to assign “execute” permissions to the action. In an application session over ICA, a warning is shown when this command is executed:



In an ICA session, if **No Access** or **Read Access**, rather than **Full Access**, is set in the first section of this dialog, it will not be possible to write data to the local hard disk during this session; in other words, the user cannot save data locally.



While the ICA client can store the user response given in the dialog, the Microsoft RDP Web client shows the warning every time a session is opened.



The response is entered in the `%SystemRoot%\webica.ini` file, in the `[Access]` section. A value of `405` in this section is equivalent to "Full Access" and "Never ask me again."

Problems Launching NetMan

Terminal server environments are generally characterized by restricted user privileges, which protects server stability. In many cases, users are allowed only to start applications, while access to other system resources (i.e. the Explorer, with the Windows desktop and Start button) is denied. With NetMan this is also the rule in terminal server environments. When problems occur, they can be difficult or impossible to trace, since no resources are available outside the application in which the problem occurred. In the following we offer some tips on how to use NetMan troubleshooting functions.

As administrator, you can run the NetMan Trace Monitor to view the internal processes that run when NetMan is launched. If an end user has problems launching NetMan, you can position the Trace Monitor call to precede the NetMan launch command in question. You can do this either in the definition of the published application, or in the definition of the start program in user administration. The program is stored in the %Windir%\NetMan3\bin directory. You can add the following arguments when calling the Trace Monitor:

```
HHTrace.exe [/c:<Program>] [/l:<Output Level>]
```

For <Program> enter NMCHttp.exe. For <Output Level>, you can enter one of the following:

- 1 (error messages only)
- 2 (trace messages; this level is usually sufficient)
- 6 (all messages)

Examples:

```
C:\Windows\NetMan3\Bin\HHTrace.exe /c:NMCHttp.exe
```

or

```
C:\Windows\NetMan3\Bin\HHTrace.exe /c:NMCHttp.exe /l:6
```

The following are two examples of where this program call could be inserted:

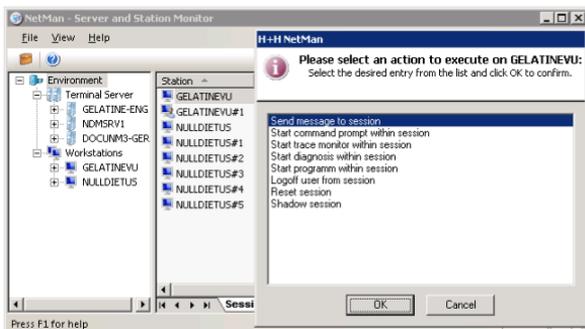
- In the Standard.ndp file in the <Apache installation>\HH\HTML View\Launch directory
- In the properties of users for whom NMCHttp.exe is the starting program
- In the Citrix Management Console with published applications that call NMCHttp.exe

Troubleshooting Application Problems

Aside from running the Trace Monitor before launching NetMan, there are other programs that can be used for diagnostics in an active session. Problems that occur when an application is started by user might not be reproducible when you log on as administrator.

If you log on as a normal user, however, the system resources you need for troubleshooting are not available. This is why the Station Monitor lets you run certain diagnostics tools. The example below shows how an administrator can run helper programs in the reduced environment of a user.

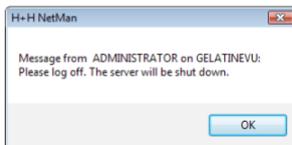
The first step is to open the NetMan Station Monitor. Then select a session and right-click to open the shortcut menu. Select the **Execute configuration** item; this opens a dialog in which you can choose from a number of processes to execute in the session:



The following options are available:

Send message to session.

Lets you send a message to the user in the session. The message is shown in a dialog box in the user's session:



Start command prompt within session.

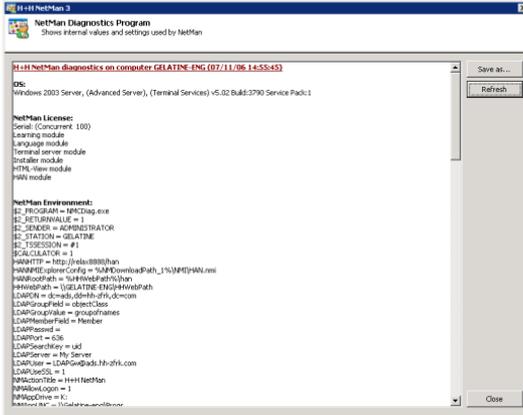
Opens a window with an input prompt in the selected session.

Start trace monitor within session.

Launches the Trace Monitor in the session.

Start diagnosis within session.

Launches the NetMan Diagnostics program in the session. The Diagnostics program determines essential information, including the values stored in variables, which play a large role in controlling NetMan:



Start program within session.

Lets you run a program of your choice within the session.

Log off user from session.

When you select this action, the user is logged off.

Reset session.

Resets the selected session.

Mirror session.

Lets you mirror the selected session.



In conjunction with the “mirroring” function in terminal server environments, this capability offers a powerful support tool, as you can call as many helper programs as you like in the mirrored user environment.



The support tools described above are available not only in terminal server environments, but to some extent can also be used on local workstations for troubleshooting the NetMan Desktop Client. Not all features are available in this case, however.

Specifically, the following tools are available on local workstations:

When the administrator is logged on in a session and provides support for another session:

- Send message to session
- Receive trace messages from session
- Start command prompt within session
- Start trace monitor within session
- Start diagnosis within session
- Start program within session
- Log off user from session
- Reset session
- Mirror session

When the administrator is at a workstation and provides support for a session:

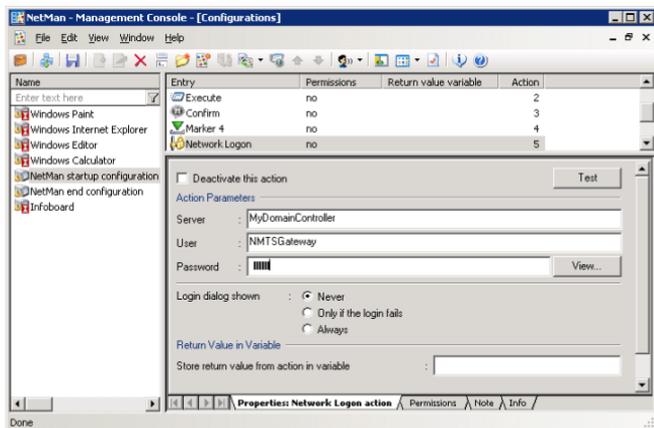
- Send message to session
- Receive trace messages from session
- Start command prompt within session
- Start trace monitor within session
- Start diagnosis within session
- Start program within session
- Log off user from session
- Reset session

When the administrator is logged on in a session or at a workstation and provides support for a workstation:

- Send message to station
- Receive trace messages from station
- Start command prompt on station
- Start trace monitor on station
- Start diagnosis on station
- Start program on station
- Log off user from station
- Shut down station

Citrix Anonymous Users in Domains

With the MetaFrame add-on, anonymous users have no rights in domain resources when the “Guest” account is deactivated. This is because the anonymous users from Citrix are accounts in a user database on the terminal server. If you wish to allow access to some resources for the anonymous user, you can add a *Network Logon* action to the NetMan startup configuration as follows:



In this example, the action logs “GatewayUser” on to a server. This gives anonymous users access to resources on “MyDomainController.”



Make sure this action is executed only by anonymous users, to prevent conflicts caused by multiple logins, because all other users are authenticated by the domain controller.



Due to the potential complication described immediately above, it is better to implement anonymous users from NetMan than from Citrix.

Advanced Security Features

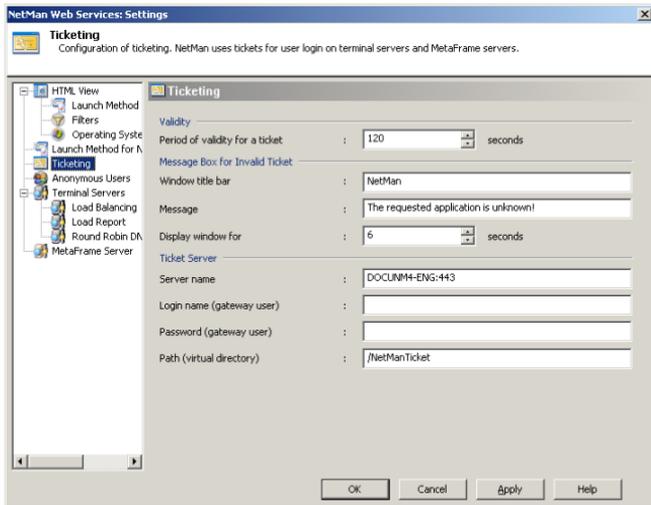
This chapter describes some of the advanced security features in NetMan:

- “*Ticketing*” describes the NetMan ticketing mechanism.
- “User Tickets for the Web Interface” describes how ticketing works in the web interface.
- “Access Privileges for Client Drives” describes how to use NetMan to filter access to client drives in sessions.

Ticketing

Ticketing plays an important role when you use the NetMan Desktop Manager. This concept is explained briefly in the following. For every session start, whether it is an RDP or an ICA session, a configuration file is generated by NetMan web services and sent to the NetMan desktop client. This configuration file, however, does not contain the application to be launched; rather, it contains a ticket. The ticket contains either a user name (only in sessions opened by NetMan anonymous users), or a random string of characters. Based on the ticket, NetMan's `Nmchttp.exe` program—together with the NetMan Web services—can recognize which application the user wishes to launch. This procedure provides enhanced security for terminal server access, because only that particular application can be launched for which the session configuration file was generated. Users cannot access the terminal server to launch an application by creating their own configuration files, or modifying existing files, for RDP or ICA access.

The ticketing feature is configured in the NetMan Web Services Settings program:



Once issued, a ticket is valid for a limited time only. After the period of validity has expired, the ticket cannot be used. The default setting for the validity period is 120 seconds; this value can be modified. If anyone tries to open a session with an invalid ticket—or without any ticket—an error message is shown. You can write your own text for this message:

Window title bar. Enter the desired text for the title bar of the error message window here.

Message. Enter the body of the message here. You can enter your choice of text.

Display window for. Define how long the message window remains open. When the window closes, the program shuts down and the session is closed.

Settings in the **Ticket Server** section specify the location of the ticket server, the login data to use and the directory from which tickets are called. If, for example, you wish to have tickets issued by a gateway user for security reasons, you can enter that user here. In this case, please remember to adapt the configuration file, `NMView.conf`, accordingly. The file must be adapted so that only gateway users have access rights in the `/NMTicket` directory.

User Tickets for the Web Interface

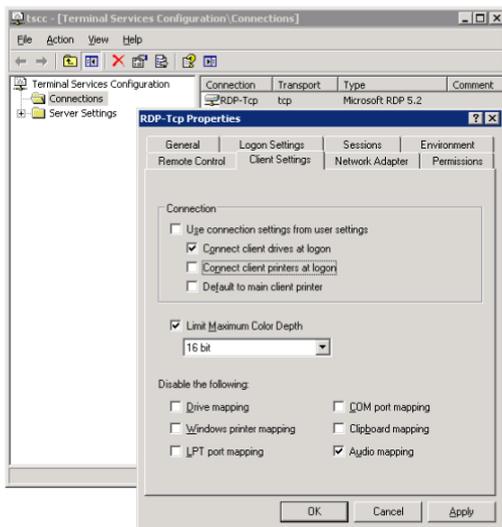
When NetMan is accessed through the web interface, the user authentication data used to open the session is not stored. Rather, a user ticket is created for the session, with the format @@GUID (for example, @@5CFB2335-A315-48EC-AFBA-4BE91A87BA) . This user name is stored in the file that requested the session. The MIME type for these files is `application/x-nmrdp`. They are downloaded by the browser and executed by NetMan RDP Web Client. Although the originating server configures the file to be discarded immediately and not stored, in some instances the browser ignores these settings and caches the file on the local hard drive. This may be the case regardless of which browser is used. This is why it is important that login data is not stored on the hard drive, not even in encrypted form.

Access Privileges for Client Drives

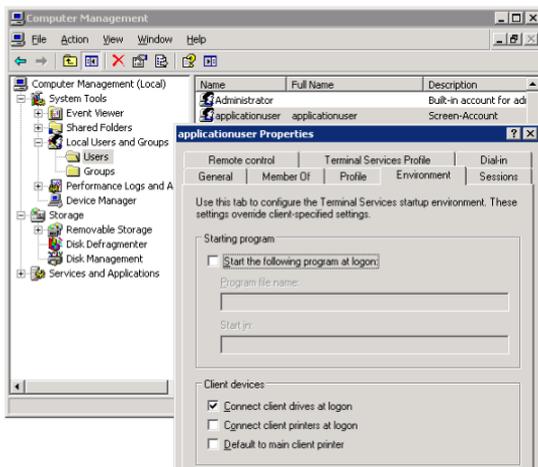
In terminal server environments, it is possible to access drives on the local client while working within a terminal server session. Access to local drives is a complex and important function of terminal services in particular. Unfortunately, the finer points of this function cannot be adjusted as precisely as needed.

The following can be configured on a Windows Terminal Server:

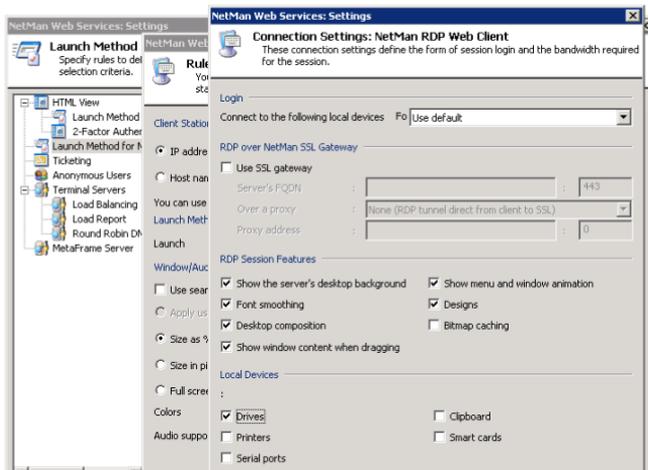
- Under **Connection**, you can define whether access to client drives is allowed or not. If it is not permitted by the settings in this dialog, access cannot be granted by any other method:



- You can configure user properties to define whether or not drives are accessible for a particular user. Prerequisite for this option is that access is enabled under **Connection** on the **Client Settings** page. To configure user properties, open **Computer Management > Local Users and Groups > Users**:



In the commonly used RDP client from Microsoft, and also in NetMan Desktop Client, you can switch client drive mapping on and off. The dialog below shows an example of settings in the NetMan Desktop Client:



If a user can access client drives in a session, then that user has all privileges in all drives; for example, not only can that user copy files from the terminal server to the client machine, but also store files from the local workstation on the terminal server.

With NetMan Desktop Manager, however, you can differentiate user rights in client drives as follows:

- Permit access only to specified drives within a session; other drives on the workstation cannot be used.
- Modify access rights in client drives at run time.
- Limit access in client drives to “read-only” permission.
- Limit access in client drives to “write-only” permission.
- Grant separate rights pertaining to subdirectories on client drives.

This extended control of client drives is practically essential, for example, in information systems in which the user should only have permission to save data from the session locally. In this manner, users can be prevented from storing files on the terminal server.

Setting up Access Privileges for Client Drives

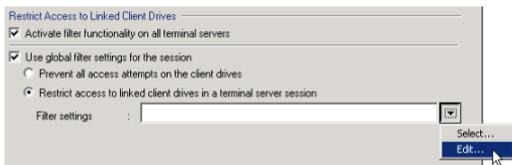
1. To set up access privileges in client drives, begin by opening the *NetMan Settings* program from the NetMan Toolbox.

2. On the **Terminal Server** dialog page, select **Activate filter on all terminal servers** to activate the access control features for all terminal servers. This setting is effective immediately:

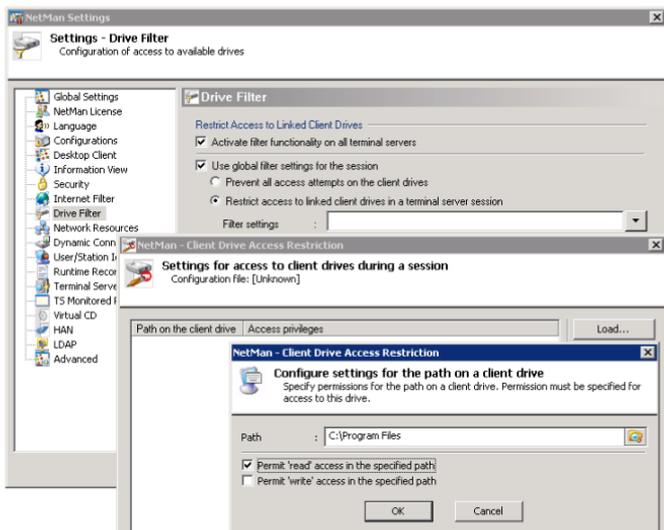


This filter must be switched on before the settings described below for access to the client drives can be applied. If the **Activate global filter for terminal server sessions** option is deactivated, all client drives can be accessed in the usual manner. Once you enable the **Activate global filter for terminal server sessions** setting, you can select either **Block all access to client drives** to block access to client drives, or **Permit access to client drives in accordance with filter settings** to configure your own settings for access to client drives. The rules you define here are not effective until a new session is opened.

3. In the next example we will demonstrate the configuration of these settings. The first step is to select **Edit** from the drop-down list to the right of the input field:



4. Click on **New**, enter a path and select **Permit 'read' access in the specified path** or **Permit 'write' access in the specified path**:



The path you enter here must be a path on the local workstation. The drive letters shown in the session for server drives can vary, and are not used when defining rules for access privileges.

5. You can define additional rules if desired before clicking **Save** to store your settings in a configuration file.



Either store the configuration file in the `%NMHome%\config\Client` directory or, if you use a different directory, add the directory in which the file is stored to the list of **Permitted Folders for Downloading Files in Desktop Client** on the **Security** page of the NetMan Settings program.



These extended access controls are applied only in sessions that are opened using NetMan Desktop Manager. Sessions opened in another manner – for example, using a Microsoft Remote Desktop connection – are not affected. If the NetMan Desktop Manager client is not running, none of the filter settings are applied.

Using NetMan Actions to Modify Access in Client Drives

In addition to the global setting for access to local client drives, you can modify privileges for a particular application using a Set Client Drive Filter action. You can choose from the following options for your global settings:

- Overwrite global settings with the privileges configured in the action (**shall overwrite the global settings**)
- Apply both global settings and the settings in the action (**shall be applied together with the global settings**)
- Reset to default setting by this action (shall be reset to match the global settings)



Client drive filter settings configured in the NetMan Management Console for an individual application call take precedence over global settings.

This applies as well when you choose to have both sets of configurations applied. For example, if the global settings restrict the user to 'read-only' access in the `C:\Program Files` directory, while an application-specific setting allows 'write' privileges as well, the user will have 'write' privileges in the `C:\Program Files` directory once the application call is executed.

Furthermore, the action can switch the expanded access control settings on or off for specified sessions. The procedures for creating and modifying access privileges are the same as those described for the NetMan Settings program in the chapter "*Setting up Access Privileges for Client Drives.*"



If you use a *Set Client Drive Filter* action with the **Overwrite global settings** option active and leave the **Filter definition** field empty—i.e., do not specify a filter definition file—, users cannot access any client drives.



If you are not sure which access privileges are applied in a given session, simply open the Trace Monitor before you launch NetMan Desktop Client. This shows details on the access privileges applied.

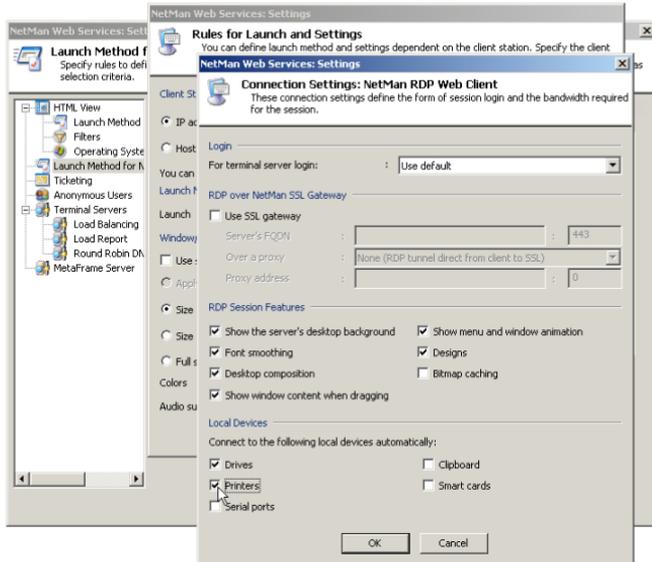
Printing

There are a number of methods for connecting and addressing printers in a terminal server environment. Aside from the technique generally implemented in the LAN, of granting user rights to a network printer for a company department or a building floor, for example, terminal server sessions in particular often present the additional demand for having the same options within a session as are available on the workstation outside the session. In other words, the workstation's local printers should be made available within the terminal server session. In the following we describe three methods for this integration:

- Support for local printers provided by RDP version 5.2
- Universal printer driver/Terminal Server Easy Print
- Universal PDF printer driver

RDP Support for Local Printers

One of the properties of RDP is support for local printers. In addition to local drives and serial connections, local printers in particular can be addressed in a session. To implement this feature, the use of local printers has to be configured for application sessions with NetMan Desktop Manager. Open the NetMan Web Services Settings program and modify the connection settings in the rules defined for the corresponding launch method:



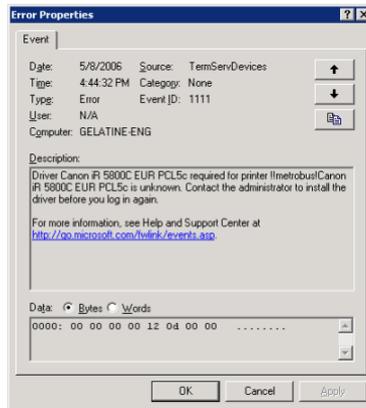
It is important that all local printers are automatically connected in the session by the settings configured here. With this technique, the required printer drivers for all connected printers are installed and configured automatically. Under certain circumstances, however, this procedure can lead to difficulties:

- If the printer driver on the server is an earlier version than that on the workstation, printouts might not show the expected results. If this is the case, you might need to install the latest driver version on the terminal server, which can be a problematic undertaking.
- If the driver for the printer in question is made for use only with Windows 9x/NT/2000, it might not be possible to install it on Windows 2003. And if you do manage to install it, you might not receive technical support from the manufacturer.

The chapter *“Modifying Printer Mapping”* describes how to prevent installation of other printer drivers on the terminal server.

Modifying Printer Mapping

If the required printer driver is not available on the terminal server, the failure to map the device is recorded in the event log with the event ID 1111:



This error mainly occurs with printers that use drivers provided by the printer manufacturer rather than drivers from Microsoft. This can result in inconsistencies between the printer name at the client end and that at the server end.

In most cases, however, there is a driver on the server that is compatible with the printer connected to the client. Microsoft provides a mechanism for mapping unknown client printers to drivers on the server, implemented by a mapping file.

Mapping a driver to a printer:

1. Enter the name of the mapping file: The mapping file must be named in the registry. To do this, enter the following values under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd`:

Name: PrinterMappingINFName

Type: REG_SZ

Value: Name of the INF file with the printer(s) to be mapped.

Example: `c:\windows\inf\ntprintsubs.inf`

Name: PrinterMappingINFSection

Type: REG_SZ

Value: Name of the section in the INF file to which searches will be redirected.

Example: `Printers`

2. Administration of the mapping file: After you have added the registry values described above, create or edit an INF file to add the user-defined mapping of server and client drivers. An example is given below.

Example:

```
[Version]
Signature="$SCHICAGO$"
[Printers]
"OEM-Druckertreibername" = "Windows 2003-Druckertreibername"
```

To the left of the "equals" sign (=) is the exact name of the printer driver that is linked to the client-side print queue which will be redirected to the server. On the right-hand side of the "equals" sign is the exact name of the server-side printer driver that corresponds to the client-side driver named on the left.

When you open the Start menu on the client and select **Settings > Printers**, the printer name displayed might not be the exact name of the printer driver that is to be redirected to a driver on the server. To find the printer name to be entered in your INF file on the right-hand side of the "equals" sign, check in the system event log on the terminal server for an event with event ID 1111. Event ID 1111 contains the exact name of the printer driver for which re-direction has failed.

Universal Printer Driver in Windows Server 2003 SP1

Within the scope of SP1 for Windows Server 2003, Microsoft added a new functionality to its terminal services: a universal printer driver implemented by very basic means.

This new driver is configured using local group policies. You can choose from the following options:

- Everything remains as it was before SP1; i.e., the new functionality is not used.
- The local printer is addressed using the PCL driver
- The local printer is addressed using the Postscript driver
- The local printer is addressed using the PCL driver and the Postscript; i.e., two client printer objects are created for the same local printer.

The PCL driver is based on the DeskJet 500 driver, and the Postscript driver is based on an HP LaserJet 4/4M PS. Only black and white printing is supported, and only the most basic printer functions are available. Furthermore, this driver works only on client computers that run the Windows XP operating system.

Terminal Server Easy Print in Windows Server 2008

With the advent of Windows Server 2008, Microsoft introduced the new Terminal Services Easy Print technology. Prerequisite for use of TS Easy Print are Windows Server 2008 on the terminal server, and Remote Desktop Connection (RDC) 6.1 and Microsoft .NET Framework 3.0 Service Pack 1 (SP1) on the client.

With Windows Vista + SP1 on the client machine, all required components are available and TS Easy Print is ready to use right out of the box. Windows XP + SP3 also supports TS Easy Print, but requires separate installation of .NET Framework 3.0 SP1. Remote Desktop Connection 6.1 is included in Windows XP SP3. This feature is not compatible with any other platform.

On the server side, .NET Framework 3.0 SP1 must be running on Windows Server 2008. TS Easy Print presents the user with the usual "Print" dialog for configuration of general settings, such as number of copies. The switch for device-specific settings opens the same configuration dialog as that opened for the local printer driver, with the same options. The settings configured locally for the printer are loaded automatically. The server processes this information in combination with the print data to create an XPS document, which is then sent to the client over RDP. At the client end, the XPS document is converted into a normal print job and the resulting printout is the same as it would have been if it had been printed locally. With this method, no special printer driver is required on the server, and users at the client machines see only their familiar environment.

Universal PDF Printer Driver

The universal PDF printer driver is a component of NetMan Desktop Manager, and creates PDF files on the terminal server which are transferred to the client over RDP.

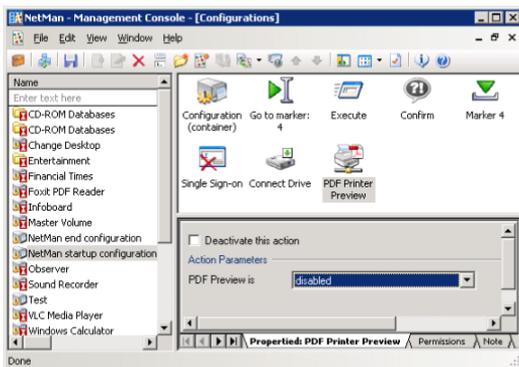


This file is automatically opened on the client by Acrobat Reader. Installation of Acrobat Reader from Adobe on the workstation is required for use of the PDF printer driver. Most workstations already have an Acrobat Reader installation. With Acrobat Reader you can print the file on any local or network printer. There are no limitations imposed by the printing function.

Switching the PDF Print Preview On and Off

For print jobs handled by the universal PDF printer driver, you can switch the print preview feature on and off on your network stations. This setting is configured by a NetMan action and remains active throughout an entire terminal server session. If there are two programs active in the session, for example, then the setting is applied for both programs.

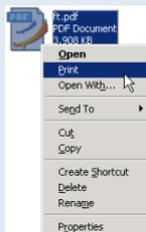
This action is often added to startup configurations. If the NetMan *PDF Print Preview* action is not used in a given terminal server session, then the preview function is available by default in that session:



If the PDF print preview function is switched off, all print jobs are automatically sent to the local workstation's default printer.



Prerequisite for printing without a print preview is a PDF viewer on the workstation that can print PDF files. To test whether the workstation has such a viewer, right-click on a PDF file and check whether the shortcut menu contains a **Print** command.

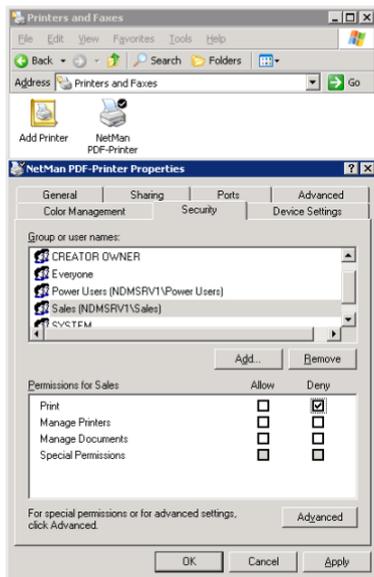


Showing or Hiding the Universal PDF Printer Driver

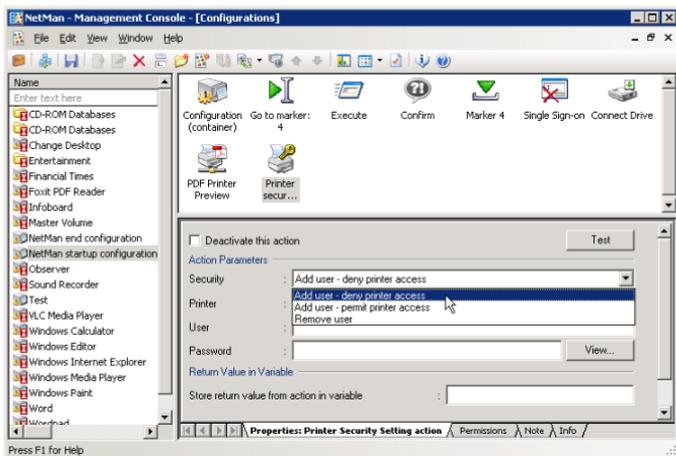
While the universal PDF printer driver can be a useful tool, there may be times when you want to block access to it for some or all users.

There are two ways to do this:

1. If the users for whom you wish to block access are all in one NT user group, simply assign permissions for the printer object accordingly. In the dialog shown below, for example, the "Sales" group is not permitted to access the PDF printer:



- Alternatively, you can assign permissions to the printer object using a NetMan *Printer Security Settings* action. This action sets permissions to a printed object for the user executing the action:



The default, i.e. if you do not enter a printer name in the **Printer** field, is the NetMan PDF printer. You can set the following access permissions here:

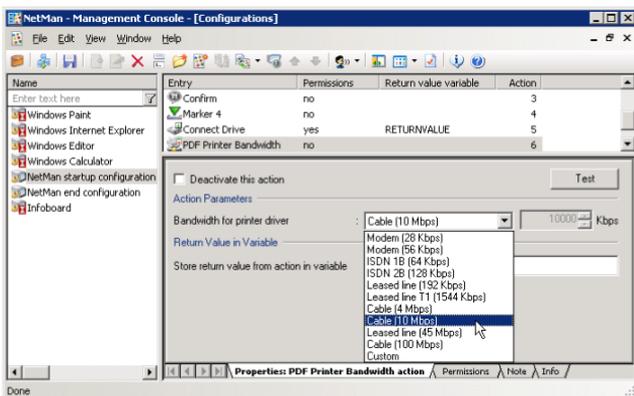
- **Add user – deny printer access.** The user can no longer access the printer.
- **Add user – permit printer access.** The user can access the printer.
- **Remove user.** The user is removed from the access list. In this case, the rights assigned statically to the printer object apply.



You can use this NetMan action to set privileges for other printer objects as well. To do this, enter the share name of the desired printer in the **Printer** field. Under **User** and **Password** enter the login data of a user who has the privileges required for setting printer object rights.

Bandwidth Management for the Universal PDF Printer Driver

When you use the universal PDF printer driver to print a document, you can configure a NetMan action to define the bandwidth allocated for transferring the document from the session to the local workstation:



We recommend allocating bandwidth to workstations, station groups, or station profiles in a startup configuration. Alternatively, you can allocate bandwidth based on users and applications, if desired, by adding the relevant action to a NetMan configuration. If different bandwidth settings are configured in the course of a given session, the most recent setting is applied.

The following options are available for setting the bandwidth:

- Modem (28 Kbps)
- Modem (56 Kbps)
- ISDN 1B (64 Kbps)
- ISDN 2B (128 Kbps)
- Leased line (192 Kbps)
- Cable (4 Mbps)
- Cable (10 Mbps)
- Leased line (45 Mbps)
- Cable (100 Mbps)
- Custom (user-definable values)

Thus NetMan Desktop Manager can help you restrict the level of network traffic for print jobs in the WAN environment.

Internet Filter

The NetMan Internet Filter is a software component that can filter Internet access for NetMan clients. You can configure global filter settings as well as separate settings for individual NetMan Program actions and Hyperlink actions.

The NetMan Internet Filter filters the following protocols:

- HTTP
- HTTPS
- FTP

All URLs or addresses are blocked by default. Clients can access only addresses or domains that you permit. FTP and HTTPS calls are filtered only at the host-name level. With HTTP, on the other hand, you can filter addresses on the following levels:

- Explicit URL
- URL level
- Host-name level
- Domain level

NetMan Internet filters contain lists of permitted addresses (also called “whitelists”) and excluded address (“blacklists”). “Permitted addresses” are addresses that the affected user can access, while excluded addresses are not accessible to the user. These lists define the filtering rules.

When you create a file to filter processes, rather than URLs, you specify the applications you wish to monitor for Internet activity. You can choose to have the filtering extended to child processes as well. If you do not know which applications launch processes that access the Internet, you might choose to apply the filter to all processes in your system.

When a program loads the NetMan Internet Filter, all URLs or all currently executing processes are automatically checked against the filtering rules. If a user requests an Internet address that is on the blacklist, an HTML page is opened showing an “access denied” message. Processes are monitored in the background, and the user cannot see which processes are blocked by the filter. Some applications, however, might not function properly if they cannot access the Internet, in which case they might generate an error message that the user sees. If the global filter is active, all Internet addresses are checked against the filtering rules regardless of which program points

to the address. Processes are also monitored globally, independent of any particular application launch. In general, the Internet filter checks for filter rules in the following sequence:

- Configurations
- NetMan Environment
- Global level



Filtering is not active unless NetMan Desktop Client is running.

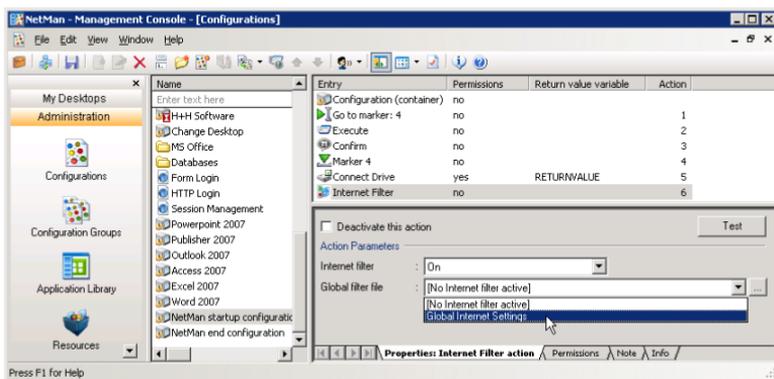
With the NetMan Internet filter, you can restrict end users' navigation options in a number of ways. The next section explains how to switch the filter mechanism on and off.

Switching the Internet Filter On and Off

There are two ways the Internet filter can restrict Internet access: globally, or for specific NetMan actions within a configuration. Once you switch it on, it runs continuously as long as NetMan is running. Prerequisite is that NetMan Desktop Client is running.

Global Filtering of Internet Access

To filter Internet access globally within your NetMan system, integrate the Internet filter mechanism in the NetMan startup configuration. To do this, open the NetMan startup configuration in your Management Console and add an *Internet Filter* action in the last position:



The Internet Filter action has several configuration options that must be set in order to activate the filter. In the **Internet filter** field, select **On**. Under **Global filter file** you can select the filter file that contains the desired whitelist and blacklist, or processes to be filtered. Immediately following installation, only the default file, **Global Internet Settings**, is available (the file name is `Global Internet Settings.iff`). This file enables unrestricted Internet access.

Click on the "Browse" button ("...") to open the editor for Internet filter files. The editor lets you define your own Internet filtering rules.

Internet Access Filtering Mechanism in NetMan Actions

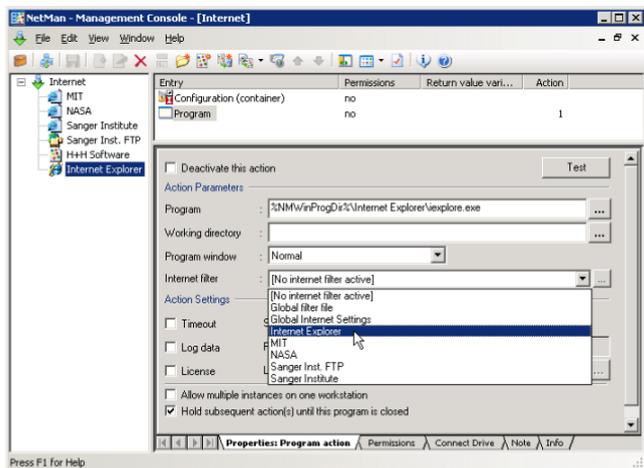
You might want to add the filtering mechanism to an individual action to configure access privileges for a specific program. For example, you could block access globally and then permit access for one particular program.

Open the NetMan Management Console and select the configuration that contains the Program action you wish to configure. Both the *Program* and *Hyperlink* actions have an **Internet filter** property.

In our example, we set the filter in a NetMan configuration called "Internet Explorer."



You can select the desired NetMan configuration from the **Configurations** window. Keep in mind however that the Internet filter settings you define will apply for every desktop the configuration is linked to. If you want to configure different filtering rules for the same program in different desktops, you need to create separate NetMan configurations.



Select a filter file in the **Internet filter** field or click on the “...” button to write a new file. Once you have confirmed the desired rules for this configuration, these settings take precedence over the global settings for Internet access.

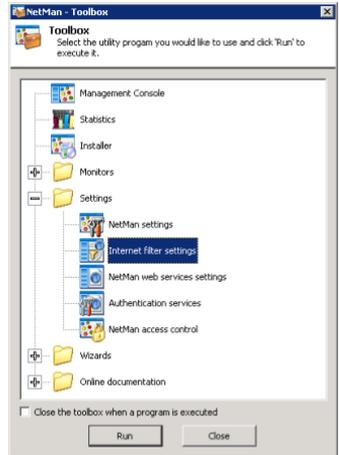


Changes in the Internet filter file are effective the next time that NetMan configuration is executed. Instances of the program in question that are running at the time you change the file are not affected.

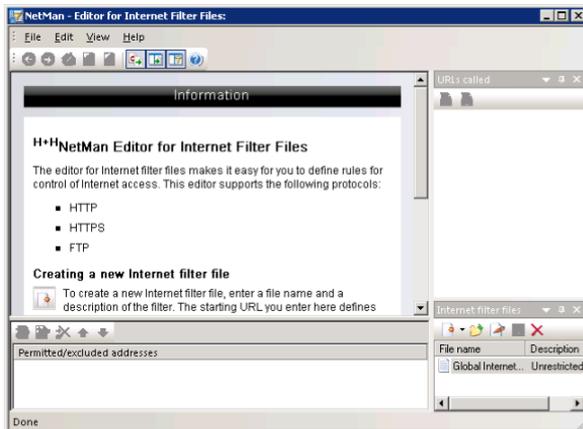
Editor for Internet Filter Files

Your Internet filtering rules are defined in IFF files, which are created and managed using the Internet Filter File Editor. This program opens when you add an Internet Filter action to a configuration in the Management Console and click on the “...” button to edit it. Immediately following installation, only the default filter file is available, “Global Internet Settings.iff.” We recommend writing your own Internet filter files to meet your requirements.

You also have the option of opening this editor from the NetMan Toolbox:



The main window of the editor is divided into four sections:



- The **browser** section shows an info page until you load a filter file for editing. When you load a file, its starting page is shown here. If it is a URL filter file, rather than a process filter, you can navigate the browser window by clicking on hyper-

links just like in any browser. The editor's browser window has an additional mode that highlights the hyperlinks on the displayed page and adds controls for blocking or permitting access to each link.

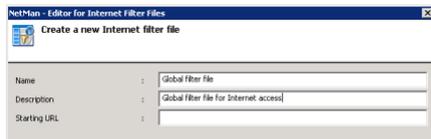
- The **URLs called section** listed the URLs that you have navigated to, and indicates whether they are permitted or blocked addresses.
- The **Internet filter files** section shows all of the existing Internet filter files. You can select a file here to open it for editing.
- The **Permitted/excluded addresses** section shows the active filter patterns. The settings you configure in the browser window pane for permitting/blocking access are shown here.

Each window page in which you can configure settings has its own toolbar. The name of the Internet filter file currently open for editing is shown in the title bar of the main window.

Creating a Global Internet Filter

To protect your system from unauthorized Internet access on the part of your users, we recommend configuring an Internet filter definition and linking it in your system on the global level.

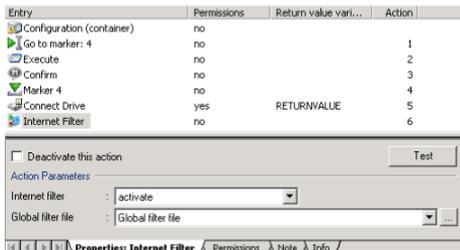
1. In the Management Console, open the NetMan start configuration for editing. This configuration already contains an Internet Filter action. Click on the “Browse” button (“...”) to open the editor for Internet filter files.
2. In the **Internet filter files** window, click on the **New** toolbar icon to create a new Internet filter file.
3. Enter a name and a description for the filter. No starting URL is entered in this case, because the purpose of this filter is to prevent all Internet access:



4. No rules are shown in the **Permitted/excluded addresses** section, since no starting URL was defined. No rule is added here, either. If no addresses are explicitly permitted, NetMan automatically denies access to any address.

5. Save the Internet filter file and close the editor.

6. In the Management Console, enter the name of your new Internet filter file and activate the Internet filter:

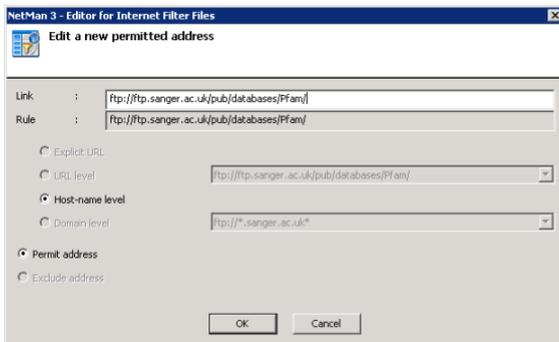


This filter also blocks access to HTTPS and FTP addresses. FTP folders in the Internet can still be seen, but the files cannot be opened or downloaded.

Creating Rules for Filtering URLs

In addition to the simple methods shown so far for permitting access to domains, the editor for Internet filter files also lets you write complex sets of rules. There are certain conventions, described in the following, that must be observed to ensure that your rules produce the desired results.

Filtering FTP and HTTPS addresses presents a special case. The default setting in the Internet filter is to treat all unspecified addresses as “excluded” and block access to them. This applies to FTP and HTTPS addresses as well. These must be explicitly “permitted” if you wish to permit access to them. Due to the limitations of these protocols, however, access privileges must be enabled at the host-name level. This is why the editor for Internet filter files does not include a mechanism for excluding FTP and HTTPS addresses. Furthermore, when you enter these addresses, the protocol must be specifically named. Rules that permit access to an FTP address, for example, should look something like this:



The same applies for entering an HTTPS address.



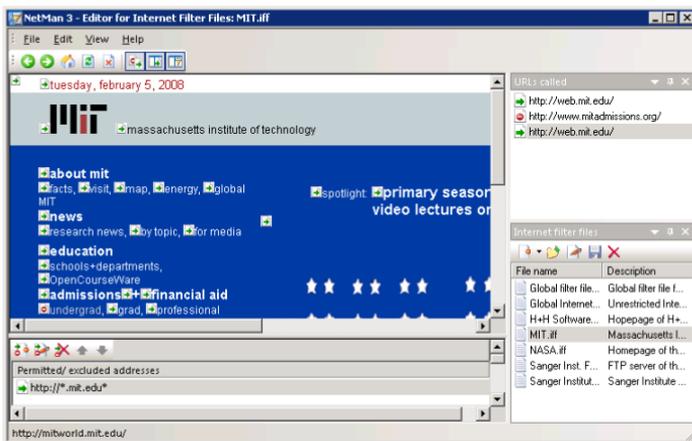
Keep in mind that blacklisting an FTP address does not prevent the user from pointing the browser to that address. The files at that site, however, cannot be downloaded or opened.

The NetMan Internet filter mechanism can filter HTTP addresses on different levels:

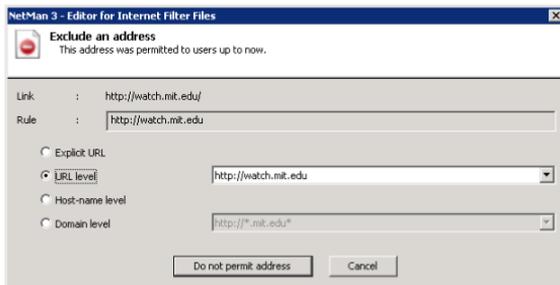
- Explicit URL
- URL level
- Host-name level
- Domain level

This means you can permit access to a given domain and still block access to particular URLs at that domain. For example, you can permit access to the information on a given website but block downloads from that site.

In addition to entering filter rules, you can use the “Link Images” function in the editor’s browser window to write rules. This feature highlights all hyperlinks and marks permitted and excluded addresses:



The example shows a filter file for the MIT domain. All hyperlinks that do not lead to another domain are automatically permitted. To show or hide the link images, select **Show link images** in the **View** menu. To exclude a link, click on its image with the mouse. This opens the **Exclude an address** dialog:



In our example, access to video resources on the MIT site is blocked.

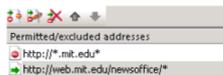
This is implemented at the URL level, to ensure that all links of this type at this site are affected:



The image now shows that the hyperlink is blocked. The link image shows you at a glance what hyperlinks are contained on a page as well as what effects your filter file will have. When you click on link images to define rules, the corresponding data is automatically written to the list of permitted and excluded addresses:



The list of rules is processed from top to bottom. The order in which the rules appear in this list has important consequences for the results of processing. For example, to permit a certain address at a site that is excluded on the host-name or domain level, the following list would not result in the desired effect:



When the browser is pointed to the “web.mit.edu/newsoffice” address, the filter mechanism would first process the rule that excludes access to this host. Since the domain is already excluded, the address specified afterwards is excluded as well. The solution is to put the rules in the following order:



The “mit.edu” domain in general is now excluded, but the “newsoffice” section of it is permitted.



If the two methods explained here for creating filter rules are not sufficient, open the View menu and select Expert mode. This mode lets you enter regular expressions for your rules, and adds a button to the toolbar of the Permitted/excluded addresses section for opening a dialog in which regular expression can be defined.

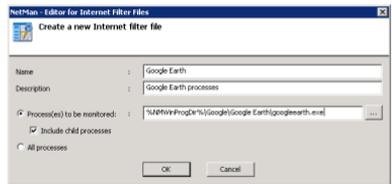
Creating Rules for Filtering Processes

Some applications access the Internet without navigating to any specific address or using an Internet protocol. Once they have attained Internet access, however, this can enable unauthorized user access to the Internet. To prevent this, you can create a filter that stops certain processes from accessing the Internet. This type of filter can be configured to operate in one of two different ways:

- You can designate certain applications to be monitored for Internet access attempts, or
- You can have all processes that run in your system monitored and any attempted Internet access blocked.

1. The first step is to create a new filter definition in the Internet Filter File Editor. To do this, select **New/Record from processes**.

2. This opens a dialog prompting you to enter a name and description for the new filter file. Furthermore, you need to specify the application processes to be monitored, by listing the name of the executable file that launches the application. You can enter more than one file name, to have multiple applications monitored. Activate the **Include child processes** option to have child processes monitored as well. The example below shows how to create a filter for the “Google Earth” application:

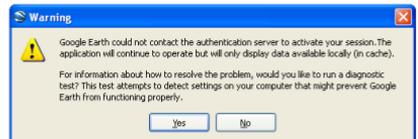


3. Save your new filter file.

4. Activate it either by specifying it in a Programm action, for example in a NetMan configuration called “Google Earth,” or perhaps in a NetMan startup configuration. Make sure you save the changes in the configuration as well.

5. When the configuration in question is called on a NetMan Client station, the “Google Earth” application generates an error message stating that it cannot establish a connection to the Internet:

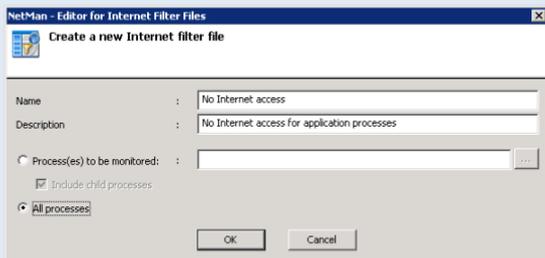
The application can still be used, but only with content that has been cached locally.



Some applications require an Internet connection in order to start. We recommend testing your NetMan configurations for proper functioning without an Internet connection before releasing them for general use with your Internet process-filter file.



You can prevent all application processes from accessing the Internet if desired. To do this, create a new filter file and select the **All processes** option:



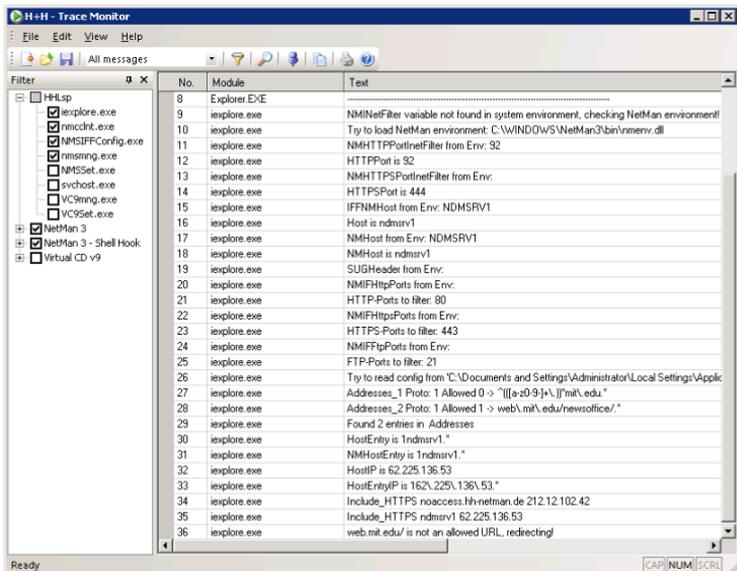
Add the filter file to your global NetMan startup configuration to prevent all processes started in your NetMan system from accessing the Internet.



System services and similar system processes are not affected by the NetMan Internet filter file.

Testing an Internet Filter File

If your filter rules do not produce the desired results, we recommend testing your filter file. To do this, run the NetMan Trace Monitor. Set the output level to **All messages**. Then launch the relevant NetMan configuration or point a browser to the website it opens. The example shown here uses a file containing rules in the incorrect order:



Lines 27 and 28 show the two rules: “web.mit.edu/” is excluded, while “web.mit.edu/newsoffice/” is permitted. The rule excluding “web.mit.edu/” is processed first. Consequently, as reported in line 36, access to the “web.mit.edu/newsoffice/” site is denied.

Statistics

When you select the **Log data** option in the Program action of a NetMan configuration, events involving that program are logged and can be analyzed with the NetMan Statistics program. There are a number of practical uses for these statistical evaluations, ranging from an overview of system use to an accounting of application usage. You can also create parallel-use spreadsheets to determine the number of licenses you require for an application. This chapter describes the functions available in the Statistics module, and presents a practical demonstration using the log files in an existing NetMan installation.



Refer to the on-line Help for detailed information on the numerous settings available in the Statistics program.



In the NetMan Settings you can define whether and how users and stations are identified in the event log.

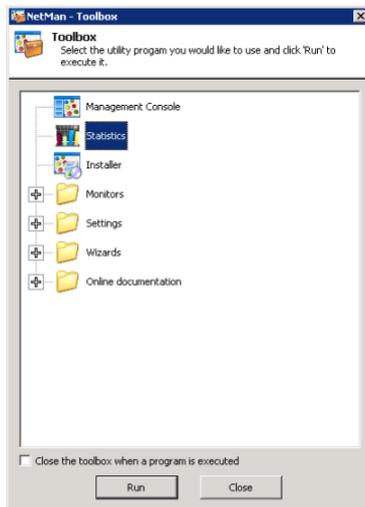
To view data in log files, open the Database Browser program:

Record ID	Start date	Stop date	Start time	Stop time	User ID	Record attribute
3818	2/13/2007	2/13/2007	3:36:33 PM	4:13:26 PM	HHANON	/TS
3817	2/13/2007	2/13/2007	3:30:16 PM	3:34:44 PM	AZSJJOHNSON	/TS
3816	2/13/2007	2/13/2007	2:47:37 PM	3:50:14 PM	AZSJJOHNSON	/TS
3815	2/13/2007	2/13/2007	1:40:46 PM	2:21:57 PM	HHANON	/TS
3814	2/13/2007	2/13/2007	10:45:28 AM	11:07:05 AM	HHANON	/TS
3813	2/10/2007	2/10/2007	3:44:52 PM	3:44:53 PM	AZSISARECCO	/TS
3812	2/10/2007	2/10/2007	3:44:32 PM	3:44:34 PM	AZSISARECCO	/TEST

This data forms the basis for evaluations performed by the NetMan Statistics program.

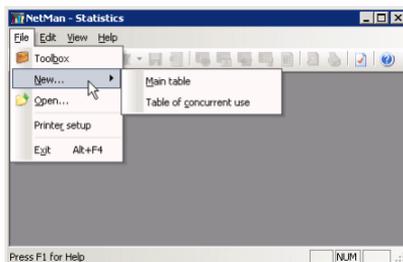
Statistical Analysis with the NetMan Statistics Program

1. To run the Statistics program, click on **Statistics** in the NetMan Toolbox:



2. This opens the main window of the Statistics program. You can choose from two types of spreadsheet in this window:

- Main table
- Concurrent use table



The first time you start the Statistics program, no spreadsheet is loaded on start-up. Under **Settings/Selection** you can specify a type of spreadsheet to be loaded at program start.

Tables

The NetMan Statistics program creates the following types of table:

- **Main table.** The main table shows variables such as total use, total calls or time in license queue, with a selected calculation base – either record ID, user or station, or a meta-ID you can define yourself.
- **Concurrent use table.** The table of concurrent use lets you analyze license utilization. It also calculates total use of applications based on the number, frequency and duration of application access instances.

In addition you can open a table of periods for specific variables.

Main Table

The main table offers the following selection options:

Under **Table based on** you can define whether data on application calls and usage is calculated according to application, user or station. Depending on your selection, each data line in the main table shows the data on a single application, user or station.

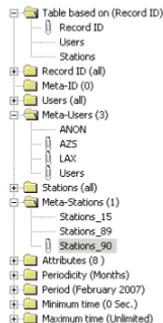
You can group applications, users, or stations for purposes of statistical analysis under the selections **Meta-IDs**, **Meta-users** and **Meta-stations**. The results in the main table show the aggregate data under the defined group name as a data line.

You can choose from defined **Attributes** to record additional information about application calls:

- /CC: Connection to client interrupted
- /Link: Execution of a Hyperlink action
- /MF: Mount error
- /NE: Program could not be executed
- /NL: No license available
- /Test: Test call from the Management Console
- /TS: Terminal server session
- /WL: Time in license queue

If you select the **/Test** attribute, for example, the database browser shows which application calls were launched for test purposes only. You can also determine the periodicity and calculation period.

The **Minimum time** setting lets you define how long an application must be in use before its usage is included in your statistical analysis. If the "Microsoft Word" application runs for only 20 seconds, for example, it can be assumed that the program was not actually used in any meaningful way, so you may not wish to include these 20 seconds in your statistics.

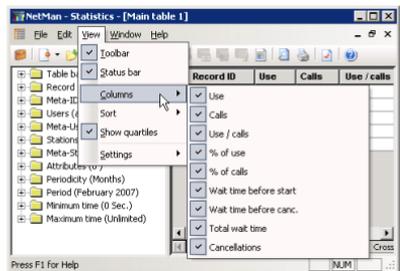


If no license is available and the user cancels the call rather than wait for a license, the call is recorded with a usage time of 0 seconds. If you wish to include such events in your statistical analysis, set the minimum time to "0 seconds."

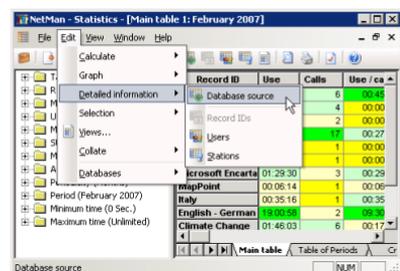
The main table shows the following values:

- Period of application use (hours:minutes:seconds)
- Number of application calls
- Average use duration per call (the Sum line shows the average use in square brackets, because this value was not arrived at through summation)
- Percentage of the use time of this application in relation to all application use
- Percentage of the application calls of the application in relation to all application calls
- Time spent waiting for a license before the application started (“/WL” attribute)
- Time spent waiting for a license before cancelling the application call (“/NL” attribute)
- Total time spent waiting in the queue (“/NL” plus “/WL”)
- Number of cancellations while waiting for a license

You can adapt the spreadsheet to your requirements by selecting which columns will be shown in the main table. To do this, select **View/Columns:**



You can choose “record ID”, “user” or “station” as the basis for calculation. Whichever you choose, you can view a calculation based on either of the other two elements by selecting **Edit/Detailed information/...** and the desired element:



Select **Edit/Views** to save any combination of selected elements as a special *View* of your data. You can activate a *View* at any time, or have a particular *View* loaded at program start.



When you select a *View* of a complete statistics period, the *View* is saved automatically. The data in this *View* is not deleted when you delete the original log files the *View* was based on. This means that these tables, once calculated, remain available for later analysis. Another advantage of saving *Views* is improved performance, because the data accessed has already been calculated.

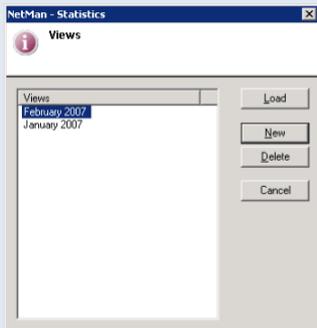


Table of Concurrent Use

This table evaluates data on applications used in parallel by multiple users. The following data is included in the calculation:

- the highest number of simultaneous users
- the number of days on which the highest number of users was reached
- the longest period during which the highest number of users was active

In addition to the maximum values, similar calculations are made for the five next lower values (Max – 1, Max – 2, etc.) in each category. This can help you determine whether the highest value was an exceptional case or can be seen as a logical extension of other values. This information is useful in deciding whether you need more or fewer licenses for a given application.



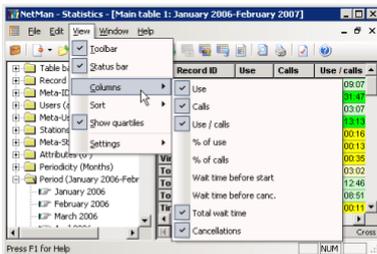
To calculate the total usage of your NetMan system, you can group all applications in a **Meta-ID** and calculate the concurrent use spreadsheet for that Meta-ID.



If you have common licenses for multiple applications, you can group these applications in a Meta-ID to calculate the concurrent use of these licenses.

Example: Analyzing Data with the NetMan Statistics Program

1. Our data stock covers a time span from January 2006 through February 2007. The first step of our analysis is to choose the columns we wish to view:



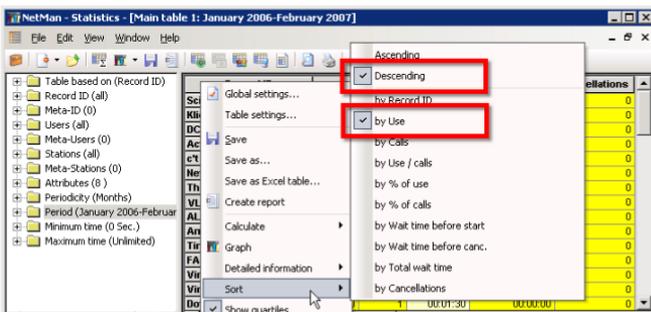
2. Then we run a calculation for this time span.



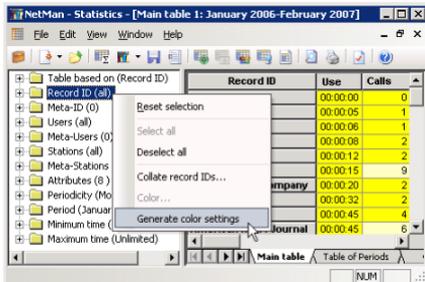
Data processing is considerably slower if data is shown on-screen during calculation. This option is defined under **Settings/Calculation**. For the fastest processing, select "No screen output during calculation."

Record ID	Use	Calls	Use / calls	Total wait time	Cancellations
Artebe	00:00:00	2	00:00:04	00:00:00	0
ARM	00:04:43	2	00:02:21	00:00:00	0
Asdas Photoshop	01:54:22	0	00:01:30	00:00:00	0
ALSO	00:00:45	4	00:00:11	00:00:00	0
American Heart Journal	00:00:48	6	00:00:07	00:00:00	0
Architecture	00:13:36	14	00:00:59	00:00:00	0
Astronomy	01:22:59	59	00:01:24	00:00:00	0
Business English	00:52:30	104	00:10:33	00:00:00	0
cy ROM	00:00:12	2	00:00:06	00:00:00	0
Climate Change	00:14:08	132	00:00:06	00:00:00	0
DCI Balabae	00:00:06	1	00:00:06	00:00:00	0
Difonepro	00:01:30	1	00:01:30	00:00:00	0
Editorial	01:52:59	0	00:01:20	00:00:00	0
Emerland	03:26:22	17	00:12:08	00:00:00	0
English - German	00:03:31	15	00:00:06	00:10:18	0
FAZ	00:00:46	4	00:00:11	00:00:00	0
Financial Times	12:00:45	16	00:00:16	00:00:00	0
French-German	00:16:36	104	00:05:40	00:00:00	0

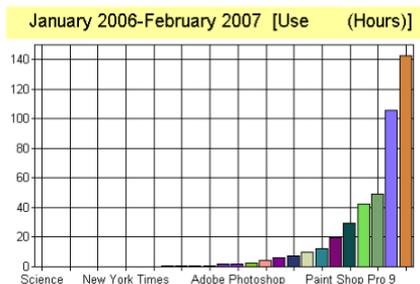
3. The data shown is sorted by record IDs. First of all, we want to know which accounts were used the longest and called most often, so we right-click with the mouse cursor on the spreadsheet to open a shortcut menu, and select **Descending/by Use**:



4. Because we have a very large volume of data available, we mark a selection of data records in the spreadsheet. To save time when processing large amounts of data, you can have the colors assigned automatically to the charted data. To do this, select **Record ID** in the Selection window on the left, and then right-click on it and select **Generate color settings** from the shortcut menu. To assign colors to individual record IDs, select the desired record ID, right-click on it to open the shortcut menu, and select **Generate color settings**:



5. Now we choose a chart type for our data and generate the chart:



After you generate the chart, you can open a shortcut menu by right-clicking on it. Select **Graph settings** from the shortcut menu to customize your chart.



Select **Edit/Graph** to define which values are represented in your chart.

In our example, the “Microsoft Encarta” application was called most frequently, as can be seen in the **Calls** column. The **Use / calls** column shows that the “English - German” application had the longest period of use per application call.

6. In the next step, the data is sorted by application call. With the default settings, the “Display Quartiles” option is active, so the highest and lowest values in the column can be recognized at a glance. The command for activating and deactivating this option is in the **View** menu.

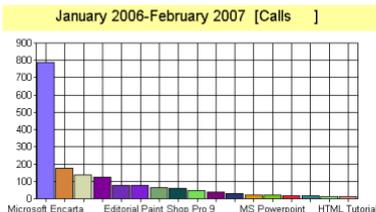
This option marks values with one of four colors, to differentiate the following categories:

- high values (= 75% to 100% of the highest value)
- fairly high values (= 50% to 74%)
- fairly low values (= 25 to 49%)
- low values (= 0 to 24%)

In the table below, you can tell at a glance which are the highest values in each of the columns (sorted by use):

Record ID	Use	Calls	Use / calls	Total wait time	Cancellations
Microsoft Encarta	105.51.1	790	00:08:02	16.20.15	8
English - German	142.43.1	178	00:48:06	01.15.18	2
MS Excel	09.54.39	136	00:04:22	00.00.00	0
MS InfoPath	05.51.35	125	00:02:48	00.00.00	0
Editorial	01.52.56	77	00:01:28	00.00.02	3
Adobe Photoshop	01.54.22	76	00:01:30	00.00.00	0
The Economist	49.05.33	63	00:46:45	00.00.00	0
Paint Shop Pro 9	29.30.07	62	00:28:33	00.00.00	0
German-French	42.34.22	47	00:54:20	00.00.00	0
Wikipedia	19.38.15	37	00:31:47	00.00.00	0
MS Access	07.23.03	32	00:13:50	00.00.00	0
Geographical Review	00.54.50	21	00:02:36	00.00.00	0
MS Powerpoint	02.21.08	20	00:07:03	00.00.00	0
Google Earth	00.24.56	17	00:01:28	00.00.00	0
Financial Times	12.03.45	16	00:45.14	00.00.00	0
MS Publisher	00.40.29	14	00:02:53	00.00.00	0

7. Sorted by number of application calls, the chart looks like this:



8. Here we have sorted the table by time spent waiting for a license:

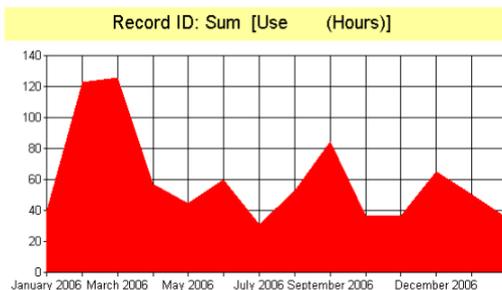
Record ID	Use	Calls	Use / calls	Total wait time	Cancellations
Microsoft Encarta	105.51.1	790	00:08:02	16.20.15	8
English - German	142.43.1	178	00:48:06	01.15.18	2
Editorial	01.52.56	77	00:01:28	00.00.02	3
MS Excel	09.54.39	136	00:04:22	00.00.00	0
MS InfoPath	05.51.35	125	00:02:48	00.00.00	0
Adobe Photoshop	01.54.22	76	00:01:30	00.00.00	0
The Economist	49.05.33	63	00:46:45	00.00.00	0
Paint Shop Pro 9	29.30.07	62	00:28:33	00.00.00	0
German-French	42.34.22	47	00:54:20	00.00.00	0
Wikipedia	19.38.15	37	00:31:47	00.00.00	0
MS Access	07.23.03	32	00:13:50	00.00.00	0
Geographical Review	00.54.50	21	00:02:36	00.00.00	0
MS Powerpoint	02.21.08	20	00:07:03	00.00.00	0
Google Earth	00.24.56	17	00:01:28	00.00.00	0
Financial Times	12.03.45	16	00:45.14	00.00.00	0
MS Publisher	00.40.29	14	00:02:53	00.00.00	0
HTML Tutorial	04.10.04	14	00:17:51	00.00.00	0
MS Word	00.21.30	5	00:04:18	00.00.00	0

“Microsoft Encarta” is at the top of the list.

9. In the table of periods for a given line, the **Sum** line shows the total use of all applications in each period, which is useful for detecting trends:

Table of Periods for Record ID: Sum					
Period	Use	Calls	Use / calls	Total wait time	Cancellations
January 2006	19:33:51	312	00:03:45		
February 2006	30:33:11	261	00:07:01		2
March 2006	31:04:23	223	00:08:21		2
April 2006	18:08:23	199	00:05:28		1
May 2006	36:23:33	136	00:16:03	01:16:19	7
June 2006	51:37:22	76	00:40:45	16:19:16	1
July 2006	25:58:18	83	00:19:45		
August 2006	38:35:11	100	00:23:09		
September 2006	38:30:32	48	00:48:08		
October 2006	29:49:49	34	00:52:38		
November 2006	20:33:54	125	00:09:52		
December 2006	59:19:50	73	00:48:45		
January 2007	12:24:54	59	00:12:37		
February 2007	25:07:35	22	01:08:31		
Sum	437:38:4	1751	00:14:59	17:35:35	13

10. The graphic representation of usage distribution over time periods (a different chart type was chosen for this example) shows that usage increased throughout February 2006, reaching a peak in March 2006. Another peak was reached in May 2006, and in August of the same year as well. Following the drop-off in September the value remained stagnant through the end of the year. Overall, the chart shows strong fluctuations in the usage of this application.

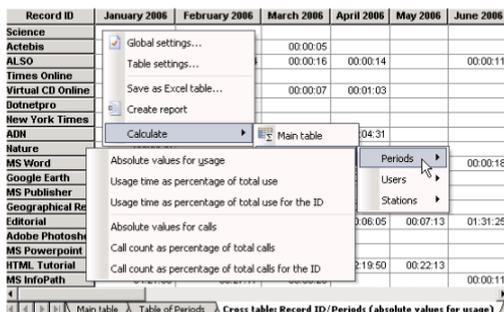


11. The cross table below shows the periodic distribution of the **Absolute values for calls** column for all applications (due to the large volume of data, only an excerpt can be shown here):

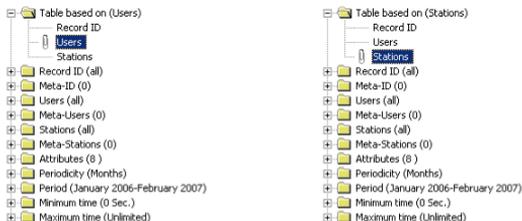
Record ID	January 2006	February 2006	March 2006	April 2006	May 2006	June 2006
Science						
Actebis			00:00:05			
ALSO		00:00:04	00:00:16	00:00:14		00:00:11
Times Online	00:00:45					
Virtual CD Online			00:00:07	00:01:03		
Dotnetpro	00:01:30					
New York Times						
ADN		00:00:12		00:04:31		
Nature	00:00:29					
MS Word					00:21:12	00:00:18
Google Earth	00:01:01	00:17:19	00:04:32	00:02:04		
MS Publisher	00:00:26	00:01:45			00:00:27	

With the default settings, the cross table calculates the **absolute value for duration of use**, sorted by record ID, for the selected period (Record ID/Period).

Right-click anywhere on the table to access the advanced functions available for cross tables. You can compare the record IDs for users or stations for the six values chosen:



12. All of the calculations demonstrated above for applications can also be made based on users or stations:



Sorted by application calls, the 'Users' table shows the following...

Users	Use	Calls	Use / calls	Total wait time	Cancellations
HP1PANH	07:00:07	813	00:06:25	00:13:17	4
AZSJOHNSON	328:16.5	717	00:27:26	17:34:58	5
AZSNEWWILL	20:53:97	497	00:02:34	00:00:16	17
HPANON	50:13:59	344	00:10:30	00:00:28	1
AZSARECCO	07:58:53	268	00:01:51	00:00:10	5
HERO3RALF	25:20:27	152	00:10:00	00:00:00	1
AZSNOYCE	77:04:26	113	00:40:55	00:00:00	0
AZSLIPPMAN	02:25:42	106	00:01:22	00:00:00	0
AZSCLINSTON	18:53:55	68	00:16:40	00:00:00	0
AZSLANCASTER	12:57:13	63	00:12:20	00:00:00	0
ANON	01:52:32	52	00:02:09	00:00:00	0
AZSKOSINSKY	06:29:35	50	00:07:47	00:00:00	0
ANONYMUS	00:00:00	43	00:00:00	00:00:00	0
AZSKLOBUCH	14:14:36	35	00:24:25	00:00:00	0
AZSBCKER	01:52:10	31	00:03:37	00:00:00	0
AZSBLANK	07:35:40	31	00:14:41	00:00:00	0
AZSDIMAGGIO	23:48:16	30	00:47:36	00:00:00	0
LAXANONBB2	04:36:03	29	00:09:31	00:00:00	0
AZSOEVERMANN	12:07:00	25	00:25:04	00:12:20	3

...and the 'Stations' table looks like this:

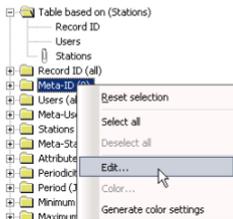
Stations	Use	Calls	Use / calls	Total wait time	Cancellations
15.38.120.22	319 43.2	760	00:24.35	17 34.56	4
89.150.12.50	23 35.55	533	00:02.39	00:00.16	17
15.38.120.115	119 37.0	408	00:14.42	00:00.13	2
89.150.12.44	10 01.36	331	00:01.49	00:00.18	8
89.150.12.100	24 19.33	221	00:06.33	00:00.00	0
89.150.12.30	42 35.23	193	00:13.14	00:00.00	1
15.38.120.99	62 37.34	110	00:01.25	00:00.00	0
89.150.12.47	56 35.22	86	00:04.37	00:00.00	0
89.150.12.37	15 05.20	69	00:13.18	00:00.00	0
89.150.12.66	21 02.32	69	00:18.34	00:00.00	1
15.38.120.20	06 51.10	47	00:08.44	00:00.00	0
15.38.120.100	02 21.41	39	00:03.37	00:00.00	0
15.38.120.120	03 48.18	38	00:06.00	00:00.00	0
15.38.120.45	14 08.39	35	00:24.14	00:00.00	0
89.150.12.1	27 12.53	34	00:48.01	00:00.00	0
15.38.120.122	01 42.02	32	00:03.11	00:00.00	0
89.120.87.22	00 00.00	29	00:00.00	00:00.00	0
89.150.12.35	08 48.21	23	00:17.47	00:00.00	0
15.38.120.29	02 38.06	21	00:07.34	00:00.00	0

The calculations can be made not only according to all users, stations or applications, but also for selected:

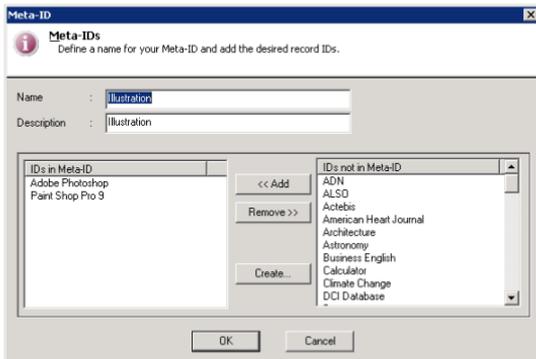
- applications
- users
- stations
- attributes

Furthermore, you can change the periodicity (quarterly, half-yearly, yearly or none), select different time spans, or set the minimum time to another value.

13. For the last demonstration, we shall generate calculations for Meta-users, Meta-stations and Meta-IDs. These give less detail, but provide a clear overview of the selected period. To do this, we first define groups of applications by right-clicking on Meta-IDs to open a shortcut menu, from which we select **Edit**:



Then we group our applications in this window...



...and repeat the calculation, this time based on our new Meta-IDs:

The screenshot shows the NetMan - Statistics application window. The left sidebar displays a tree view with 'Record ID' selected. The main window contains a table with the following data:

Record ID	Use	Calls	Use / calls	Total wait time	Cancellations
News	215:20:4	1159	00:11:09	16:20:15	9
Databases	247:35:5	785	00:18:55	01:50:45	22
Dictionaries	181:15:1	779	00:13:57	00:00:00	4
Illustration	179:58:5	713	00:15:08	00:00:00	4
Office	19:09:21	300	00:03:49	00:00:00	0
Sum	843:16:0	3736	[00:13:32]	18:11:00	39

 You can use wildcards (* and ?) to group similar record IDs when defining Meta-IDs. For example, you might use a particular prefix in defining the record IDs for a certain group of applications that you want to evaluate together regularly.

14. Next we group our stations:

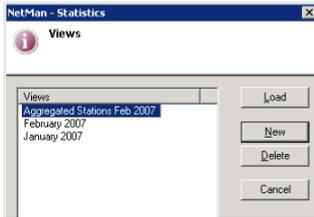
The screenshot shows the NetMan - Statistics application window. The left sidebar displays a tree view with 'Meta-Stations (all)' selected. The main window contains a table with the following data:

Stations	Use	Calls	Use / calls	Total wait time	Cancellations
Stations_89	262:03:5	1810	00:08:41	00:28:44	29
Stations_15	580:45:5	1751	00:19:54	17:42:16	10
Stations_90	00:01:57	154	00:00:00	00:00:00	0
Sum	842:51:5	3715	[00:13:36]	18:11:00	39

 To calculate the total usage of your NetMan system, group all applications in a Meta-ID and calculate the concurrent use spreadsheet for that Meta-ID.

 If you have common licenses for multiple applications, you can group these applications in a Meta-ID to calculate the concurrent use of these licenses.

15. We want to document statistical analyses for the station aggregates every month from now on, so we save the definition created in the **Selection** window as a “View”:



When you save a View, the current selection of elements is saved in the View definition. This has the following advantages:

- Complex combinations of Selections can be re-created by simply loading the corresponding View.
- Periods that were already calculated and stored in a View are loaded when a later calculation includes the same periods, which means the calculation is that much faster.
- Before the data in a log file is deleted, any periods in a View that had not been processed up to that point are calculated.
- Data in Views is still available for later processing even after the original log file has been deleted.

You can save both charts and spreadsheets after calculation. Spreadsheets can be saved and exported as follows:

- As a dBase file: Select **Save as** from the **File** menu. Enter a file name for the spreadsheet in the “Save table” dialog.
- As a test file: Select **Create report** from the **File** menu.
- As an MS Excel file: Select **Save as Excel table** from the **File** menu.

Charts are stored as BMP files.

16. For the last demonstration, we create a concurrent use table to obtain additional information about the use of licenses. Again, we have selected a limited number of record IDs to reduce the amount of data processed:

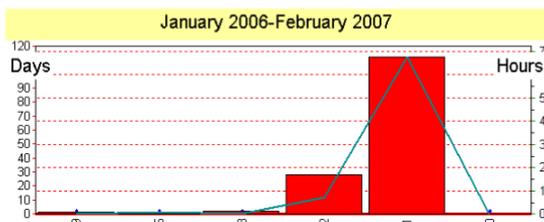
Record ID	Licenses	Max	Days	Duration	Max - 1	Days	Duration	Max - 2	Days	Duration	Max - 3	Days	Duration
Microsoft Encarta	9	9	1	00:00:27	5	1	00:03:51	3	2	00:00:53	2	28	00:41:52
Financial Times	5	3	1	00:37:04	1	11	04:23:10	0	0	00:00:00	0	0	00:00:00
MS Excel	5	2	4	00:23:57	1	24	01:11:38	0	0	00:00:00	0	0	00:00:00
MS Access	5	2	1	00:53:40	1	18	01:10:18	0	0	00:00:00	0	0	00:00:00
MS Powerpoint	5	2	1	00:00:03	1	8	00:38:32	0	0	00:00:00	0	0	00:00:00
Paint Shop Pro 9	1	1	41	06:25:44	0	0	00:00:00	0	0	00:00:00	0	0	00:00:00
Adobe Photoshop	1	1	13	00:40:59	0	0	00:00:00	0	0	00:00:00	0	0	00:00:00
MS Word	5	1	4	00:10:28	0	0	00:00:00	0	0	00:00:00	0	0	00:00:00

The **Licenses** column shows the number of licenses currently configured for the application. This generally defines the limit for parallel use.

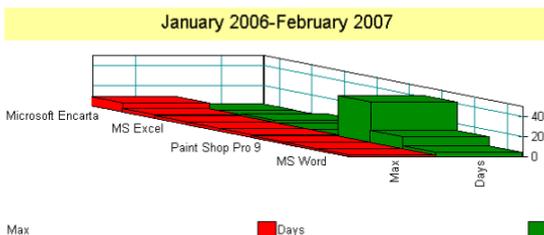
The **Max**, **Days** and **Duration** columns belong together as a block: **Max** shows the highest number of parallel users, **Days** the number of days on which this level was reached, and **Duration** the longest period during which multiple instances of the application were in use simultaneously. The subsequent columns show the same data for each of the next five lower simultaneous-use values.

As the table above shows, the number of licenses available for the Financial Times application was always sufficient. For the Microsoft Encarta application, however, all available licenses were in use on one particular day. On the other hand, if a tenth user had attempted to launch this application at that time, they would only have had to wait 27 seconds for a license to become available. Under Max-1, however, we see that the application was called by multiple users concurrently only five times on one day and, as shown under Max-2, only three times on 2 days. Additional user licenses for this application might be handy, but are not urgently required.

When we select one line of the spreadsheet and generate a bar graph based on these values, the height of the bars shows the number of days on which the value occurred. The superimposed curve indicates the duration of usage.



The following graph gives an overview of all applications that were used by more than one user simultaneously at least once:



This graph was created by selecting the applications and then activating **Edit/Graph/Maximum parallel use (for all IDs)**.

Installer

As a network administrator, or as the one responsible in your network for the deployment of applications, you are frequently confronted with the challenge of making new and in some cases hitherto unknown applications available to your network users. The hurdles you are faced with in accomplishing these tasks can be high or very high, depending on the applications you install. An *Installer* is the ideal aid in clearing these hurdles. The emphasis here is on “aid”, because the program has not been written that can automatically do the entire job for you, from start to finish.

NetMan Installer is the ideal tool for installing network-capable applications. The greatest advantage of the NetMan Installer over other installers is that it fits seamlessly into the overall NetMan concept. It simplifies the integration of new applications into your NetMan system, thus reducing your workload considerably.

Prerequisites for Working with the NetMan Installer

To get the most out of your Installer, you need to have a basic understanding of the following:

- The directory structure of your Windows operating system version
- The structure and function of the Windows Registry
- The significance of subkeys in the Registry



If the Installer is not used correctly, your computer might not operate correctly when you use an installation packet created by the NetMan Installer.

A working knowledge of the software you use combined with the experience gained from your first few installation projects is essential for obtaining optimum results with the NetMan Installer.

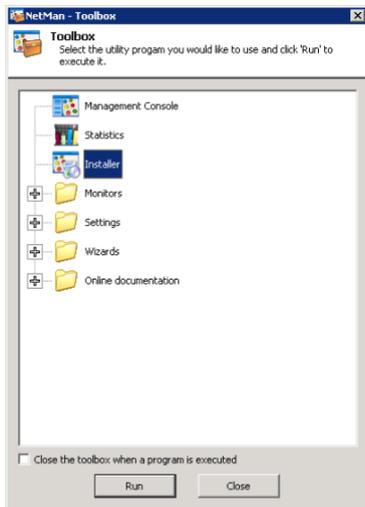
Recommended Readings on the Windows Registry

Frank R. Walther: Registry Guide. Windows 2000, Windows NT4. 2001 – 496 S., Markt+Technik, € 59,95 (ISBN: 3827260426)

John Woram: Windows 98 Registry. 1999. 424 S., Franzis Verlag GmbH, € 27,23 (ISBN: 3772367844)

Requirements for the Installation of the NetMan Installer

The NetMan Installer module is installed by the NetMan setup program. You need to have the licensing for this module activated when you register your NetMan software. Following installation and registration, you can open the Installer from the NetMan Toolbox:



Basics

The main task of an Installer is to keep track of all the modifications and additions made on a computer during application setup. This can serve one or both of the following purposes:

- The record of modifications provided by the Installer can help network administrators determine whether and how applications influence one another.
- The Installer can put together an “installation package” that executes the required workstation modifications, for “invisible” installation of the application on other workstations. A major advantage of this technique is the option of editing the installation package to optimize the installation process still further.

Not only the setup program itself, but also internal settings in a newly installed program can modify configuration files or the Registry. You might find that you want to make some of these new application settings the defaults for your users, for example by distributing them in a NetMan Script action. It is not always evident at first glance, however, where the new settings are stored, especially if the application in question makes a lot of changes in INI files or the Registry. This is where NetMan Installer functions come in handy, keeping track of all modifications and writing them in an editable script.

Areas of Application and How an Installer Works

There are basically two different procedures that an Installer can use to monitor application installation procedures:

Direct Monitoring

One way to trace modifications made in a computer system is through system monitoring. With this method, the Installer taps into the operating system and listens in on the commands called by the application setup program. This is a very effective method, but not particularly efficient, since all system calls are monitored. Furthermore, setup programs do not always follow general operating system conventions, and may make modifications that the Installer cannot register using this technique. Moreover, this type of Installer is operating-system dependent, which means that different Installer versions are required for each version of Windows.

Comparative Monitoring

Another method of installation monitoring consists in comparing the system state of the workstation before the installation with the state after the installation. This method has the decided advantage that the same Installer program can be used with all 32-bit Windows systems.



The NetMan Installer uses the comparative method. The records made of the system states are referred to in this manual as SnapShots.

Using an Installer in a Network - the H+H Installer Services

One of the routine tasks in network administration is providing user applications in the network. As the number of workstations in a network increases, so does the amount of work involved in performing the application setup on each individual station. An Installer program simplifies these tasks, reduces the administrative work involved and helps ensure reliable deployment of applications. When you have NT-based clients in a LAN, you need to be able to install software on workstations without giving the users on the workstations administrative rights. With NetMan, you can execute these functions invisibly from the Management Console with the system account.

Using an Installer in a Terminal Server Environment

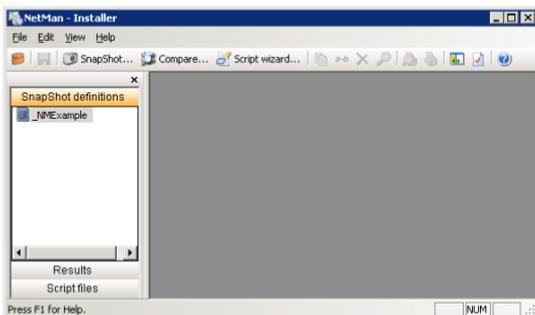
In a terminal server environment, i.e. with Microsoft Windows NT/2000/2003/2008 Terminal Server Edition or Citrix MetaFrame, installing applications on individual workstations is not an issue because applications are installed centrally, on the terminal server. But an Installer program has many uses in terminal server environments all the same; for example:

- If you have multiple terminal servers in a (MetaFrame) server farm, your application software has to be distributed among the servers.

- In some cases, you might want to make certain components provided by the installation available in the users' Windows environment.
- An Installer makes it much easier to reinstall applications, for example when the server is updated or reinstalled.
- It is of primary importance that a network server have as little downtime as possible. This is a good reason to run application setup on a separate workstation first, and then use the resulting installation script as the basis for installation on the server.
- Installing an application sometimes causes the target station to crash, which can have serious consequences when the target is a terminal server—all the more reason to create an installation script on a separate computer first.

Running the NetMan Installer

The first time you launch the NetMan Installer, the following program window opens:



The sidebar on the left-hand side is divided into three sections: **Snapshot definitions**, **Results** and **Script files**. These elements are described in detail in the following sections:

- “Snapshot Definition Files”
- “Results of Comparison”
- “Script Files”

Snapshot Definition Files

When you make a Snapshot of a workstation state prior to installing an application, the Snapshot does not have to include the entire workstation, nor the entire Windows directory, nor even the entire Registry. To optimize the entire procedure, from Snapshot to setup to comparison to script, you can simply select the relevant elements (directories, files, Registry branches, etc.) for monitoring, and save this selection as a *Snapshot Definition* which you can load at any time.

The **Snapshot definitions** element in the sidebar contains a predefined Snapshot definition called *_NMEexample* which you can use in all supported Windows operating systems. When you open this Snapshot Definition, the selected elements are shown in the window pane on the right. These include certain drives, directories and Registry entries. You can either use this definition, copy the definition and modify it, or create your own definition. We recommend saving separate Snapshot definitions for each computer on which you wish to monitor installations. The easiest way to do this is to copy the *_NMEexample* file, rename it, and adapt it as needed.



Selecting Files

In a SnapShot Definition you specify the directories and files to be monitored during application setup. The Installer detects files and directories that are added, deleted or changed. There are two ways the Installer can detect modified files:

- Comparing time stamps
- Comparing file versions. Many file types, such as DLL and EXE files, register an internal version number.

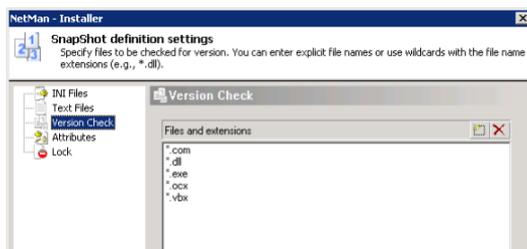
With some types of file, such as INI files (which contain Windows application settings), it is important to know not only whether they have been modified but also what modifications were made. If the Installer detects changes in the 'system.ini' file, for example, this does not mean the entire file should be copied over to another machine just to install the application—in fact, that might cause a fatal error on the target machine. It is far more important to find out exactly which of the changes made in a given file are required for installation. The NetMan Installer can detect these modifications within files. For this function, the Installer supports two formats:

- Files with the INI structure
- Common text files

You can use the buttons in the toolbar in the individual SnapShot Definition window to activate and deactivate the functions for Checking INI files, Checking text files and Checking file versions, and to specify which files are checked:



The following is a brief description of the dialog opened by the last of these four buttons:



For more detailed information, please refer to the Installer's Help program. Here you can define which types of file are checked for new versions, and which INI or text files are checked for changes in content.

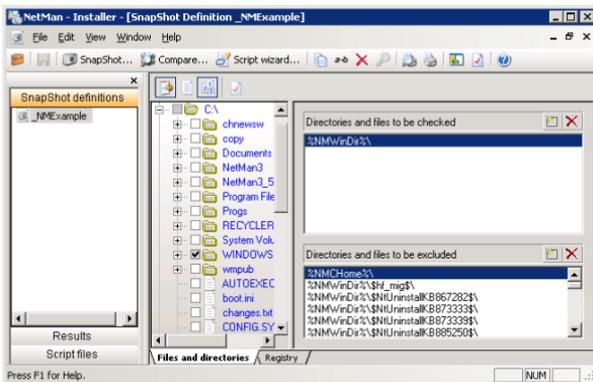


Open the Lock page to enter the names of files, directories and drives that you wish to exclude from monitoring. For example, it is a good idea to exclude your CD-ROM drive(s).

The next two subsections describe the file selection process in detail. When you first open a new SnapShot definition, no elements are selected. There are two ways to select the desired elements:

- Select the corresponding graphic elements in the display
- Enter file and directory names

Selecting Elements in the Display



To select a file or directory, click in the checkbox next to it. Click again to de-select the element. The checkboxes are shown with or without a checkmark, and with or without background shading, to indicate one of the following four states:

- The file or directory is not selected and thus will not be monitored.
- The file or directory is selected and will be monitored. In the case of a directory, a checkmark without shading indicates that the selection includes all files within the directory, as well as all subdirectories and their files.
- The directory is selected, but contains elements that are excluded from monitoring.
- The directory itself is not selected but contains elements that are selected for monitoring.

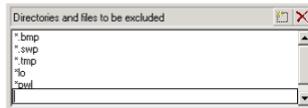


The Installer uses two different symbols to represent files:

-  Visible file
-  Hidden file

Entering File and Directory Names

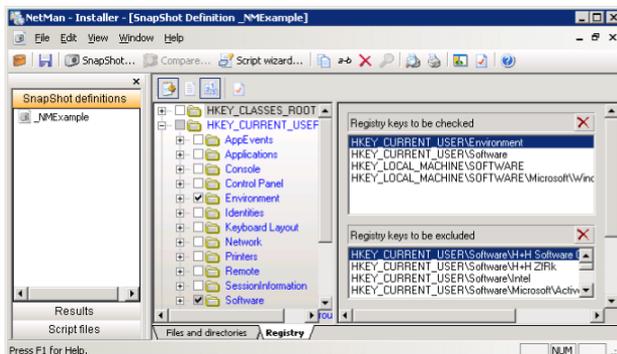
The graphic selection of elements on the left, as described above, adds and removes files and directories to and from the window panes on the right. In the window panes on the right, you can also enter the desired file and directory names yourself. The * and ? wildcards are permitted:



NetMan automatically replaces files and directory names it recognizes with environment variables. This helps make your configurations system-independent. For example, C:\Program Files is automatically replaced by %NMWinProg-Dir%.

Monitoring the Registry

To configure settings with respect to the Registry, click on the **Registry** tab in the SnapShot Definition window. The procedure for selecting keys, data types and values from the Registry is analogous to the selection of directories, subdirectories and files from the directory tree. One difference, however, is in the functions available in the right-hand panes; you can delete entries here, but cannot add or edit entries through manual input. Since the entry names in the Registry are generally so long, it is unlikely anyone would wish to enter them by hand. In particular, the use of wildcards has no advantage here. Registry entries are selected by marking them in the display on the left:



We strongly advise against selecting the entire Registry. Some keys exist in more than one main branch, or 'hive', in the Registry. For example, it is important to include the HKEY_CURRENT_USER hive, but then you do not need to select HKEY_USERS; primarily because the former contains latter, and also because setup routines do not usually modify HKEY_USERS values but rather store values only for

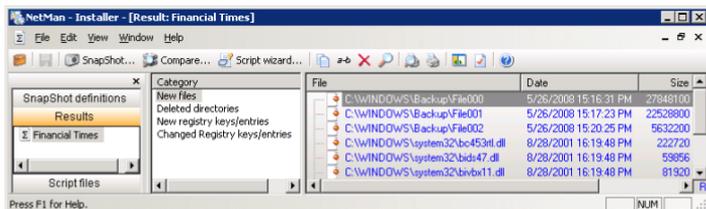
the current user. If you need more information, please refer to the literature listed at the beginning of this manual. Although there are a number of pre-defined selections for SnapShot definitions, we do recommend that you familiarize yourself with the structure and functions of the Windows Registry before using them.



Because the Windows Registry is in part made up of Windows system files, you should exclude these files from monitoring.

Results of Comparison

The Installer begins by taking a SnapShot of a computer state that includes the areas specified in the SnapShot Definition. After the application has been installed, another SnapShot is taken, using the same definition. This is the "After" picture. The next step is a comparison of Before and After. The difference between the two is the result: This is what tells you how the workstation was altered by the application setup routine. The result of the comparison is displayed as follows:



The result is divided into the following categories:

- New files
- Deleted files
- Changed files
- New empty directories
- Deleted directories
- Modified directories
- INI files
- Text files
- New Registry entries
- Deleted Registry entries
- Modified Registry entries



Keep in mind that only those categories are displayed in which changes were detected.

Categories are listed on the left, with the corresponding content displayed on the right. In the Result window, you can copy, rename and delete an entire result file. Individual elements within a result file, however, can be edited only in the script file (see below).

Script Files

A script file is generated from the results of the comparison, and can be edited manually in the NetMan Installer program. You can make changes in the script file right down to the element level, and define whether individual files should be copied or deleted or, for example, specify whether certain Registry key values are changed or not. You can integrate the resulting script in a NetMan configuration by simply adding a *Script* action and entering the file name. For details on integrating NetMan actions in configurations, see “*NetMan Actions*.” You can also distribute applications, invisibly and automatically, within a network or a MetaFrame server farm in the same manner. Script files contain the source text of a script language which is interpreted by NetMan at runtime:

```
001 //Installer script
002
003 #Esc
004 Declare
005 Number nIncluded = 1
006 Number nActType = 1
007 Number nSoftMount = 1
008 Number nTest = 0
009 Number nCont = 1
010 Number nReturn = 0
011 Number nTypeCount = 0
012 String cParam = ""
013 String cText = ""
014 String cTitle = ""
015 String cAppID = ""
016 EndDeclare
017
018 Main
019 HHWSetShowProgress(TRUE)
020 //ATTRIBUTES
021 //COPYFILES
022 HHWAddCopyFile("%NMHome%\BIN\INSTSCPT\Financial
    Times\Ctl3d.dll", "%NMWinSysDir%\Ctl3d.dll", 2)
023 nIncluded = 1
024 HHWCOPYFILES("")
025 //DELETE FILES
```

```

026 //CONFIGFILES
027 //REGISTRY
028 //ActRun(34, "\K:HKEY_LOCAL_MACHINE\SOFTWARE\
ProQuest Information and Learning\The Financial
Times\1.00.000\ /V: /T:16", "", "", 1, cAppID, 0)
029 nTypeCount =0
030 nIncluded =1
031 //ActRun(34, "\K:HKEY_LOCAL_MACHINE\SOFTWARE\Micro-
soft\Windows\CurrentVersion\App Paths\chnews.exe\
Path /V:C:\chnews\ /T:8", "", "", 1, cAppID, 0)
032 nTypeCount =0
033 nIncluded =1
034 //ActRun(34, "\K:HKEY_LOCAL_MACHINE\SOFTWARE\Micro-
soft\Windows\CurrentVersion\App Paths\chnews.exe\
/V:c:\chnews\chnews.exe /T:8", "", "", 1, cAppID, 0)
035 nTypeCount =0
036 nIncluded =1
037 ActRun(15, "regedit.exe /s \"%NMHome%\BIN\INSTSCPT\
Financial Times\Financial Times.nmr\"", "", "", 1,
cAppID, 0)
038 EndMain

```

NetMan Installer script files can also contain NetMan environment variables, such as the `%NMWinSysDir%` variable in the above example. This feature makes it even easier to use these scripts for installing applications on other computers. In this example, it does not matter whether the operating system on a given machine is installed on the C:, D:, or M: drive, or whether the directory in question is called `\Windows` or `\WINNT`. The script language also supports system variables, as well as control structures such as `if`.

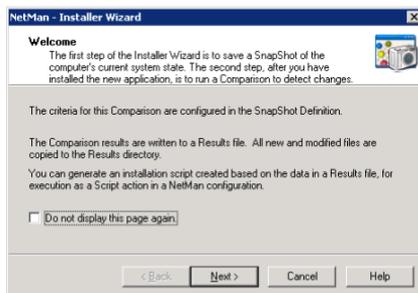
Step by Step: From Snapshot to Script

Now that you have been introduced to the sidebar on the left-hand side of the Installer program window, with its *SnapShot definitions*, *Results* and *Script files* sections, we will show you exactly how to get from the SnapShot definition to the result file and from there to a script file.

SnapShot of the Workstation

Once you have defined the range of the SnapShot, you are ready to produce a picture of the current state of the workstation:

1. To do this, open the **File** menu and select **Installer Wizard/SnapShot...** or click on the camera icon in the toolbar. This opens the SnapShot Wizard:



2. The next window prompts you for the directory in which Installer log files will be saved. Generally, you can simply accept the default, `%temp%`:



Under Windows XP, using the `%temp%` variable can lead to problems when the next user, after reboot, logs on under a different name, as the 'temp' directory is generally stored in a user profile. For this reason, we recommend entering a specific path name if you use Windows XP.



On a terminal server, it is important to name a specific path, because `%Temp%` contains the session ID.

3. The next window prompts you for the name of the SnapShot Definition you wish to use for the subsequent application installation:



4. Now the SnapShot is taken:



When the SnapShot is completed, you can run the setup program for the application you wish to install.

Comparing System States after Installation

The second step, comparison of the “before” and “after” states, is performed directly following the application installation:

1. To do this, open the **File** menu and select **Installer Wizard/Compare** or click on the **Compare** button in the toolbar. This opens a window that displays the name, date and time of the last SnapShot created, as well as the definition used:



2. Click Next to confirm this data and start the comparison.
3. The next dialog box lets you view the results and save the results file, if desired:



The result file is shown in the Results section of the sidebar.

Generating a Script from Results

You can use the results of the comparison between “before” and “after” states on the workstation to generate an installation script, which you can integrate in a NetMan configuration for seamless transparent installation of the required components on a client workstation.

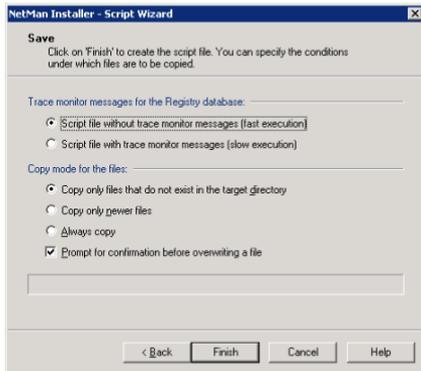
1. To make a script, select **File/Script Wizard** from the menu bar or click the **Script** button in the toolbar to open a dialog for selecting the desired results:



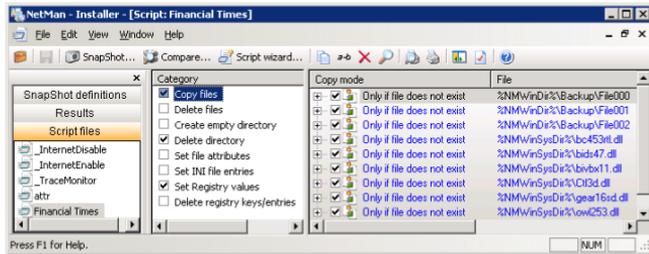
2. In the next window, you can enter a name for the script file:



3. The next two windows offer you a number of options for generating the script (refer to the Installer's Help program for details):



4. Once the script has been generated, it is shown in the **Script files** section of the sidebar. You can edit these script files manually, if desired. For example, you may want to exclude some of the files from being copied into the client Windows directory, or there may be some changes to the Registry that are not necessary:



The automatically generated scripts can be significantly improved by subsequent manual editing. It is essential, however, that you check very carefully to determine whether a given element can be deleted or modified.



If you do not know how a particular component might affect other systems, do not transfer it from one system to another.

The types of modification possible in a script file can be summed up as follows:

- Deactivate, delete or add linked files and/or Registry entries
- Enable/disable a prompt for confirmation before copying files
- Change copy mode for individual files and Registry entries
- Configure file attributes for individual files

For detailed information on editing script files, please refer to the Installer's Help program.



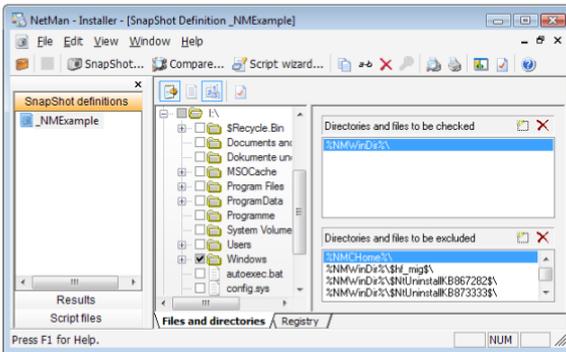
In the Script Editor you can use drag & drop to copy files from other windows (such as the Windows Explorer) to the desired category (such as **Copy/Delete files** or **Set file attributes/Set INI file entries**). When you add a file to be copied, the file in question is copied to the script directory and is thus available any time the script is executed. When you drag & drop INI files (including any files with the INI-structure, such as CFG files), you can get a quick overview of the INI file structure. You can also use drag & drop to copy files from one Installer script to another, but only to copy files from a given category in one script to the same category in another script.

Example: Installation with the NetMan Installer

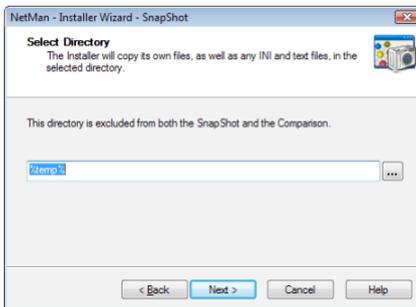
In this chapter, we will carry out an installation step by step using the NetMan Installer. For this demonstration we will install the same application used for demonstrations in the Base Module manual, the “Financial Times” application (from 2002), which is driven by the “Caravan” retrieval software from Chadwyck-Healey. “Financial Times” is a CD-ROM database and a 32-bit program.

The SnapShot

We want to install “Financial Times” on a computer running Windows VISTA. For the SnapShot definition, we select a version of the sample definition, “_NMExample” which has been modified for use with the computer in question. These modifications include, for example, the exclusion of several subdirectories under %SystemRoot%, as well as drives A: (floppy drive), E: and F: (CD drives). The “Check File Version” function is switched on:

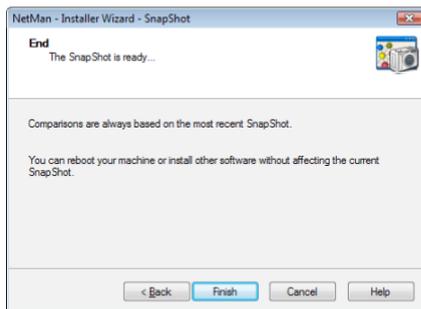


We activate the SnapShot:



The Installer Wizard reads the data in directories, files and the Registry as specified in the SnapShot definition.

When the SnapShot is completed, the Wizard sends a message to the screen indicating that the resulting SnapShot will be the basis for all subsequent comparisons:



Application Setup

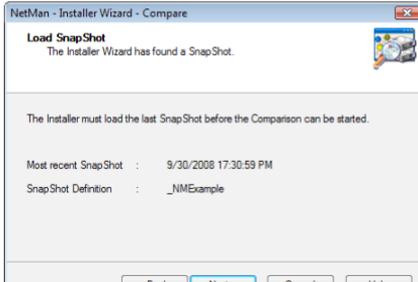
Now we install the “Financial Times” application:



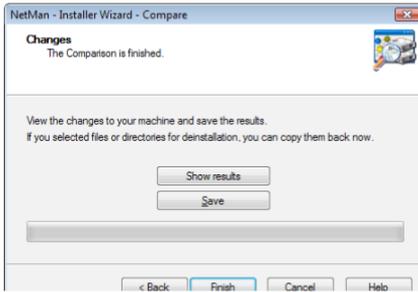
From Comparison to Result

We initiate the comparison immediately following the installation of the application so we can find out what modifications are necessary before the application can be started for the first time on a client station. If we later find that other settings are configured following the initial startup, such as program options, disabling certain operating functions so users cannot access them, start options, etc., we can run the comparison again after making these changes.

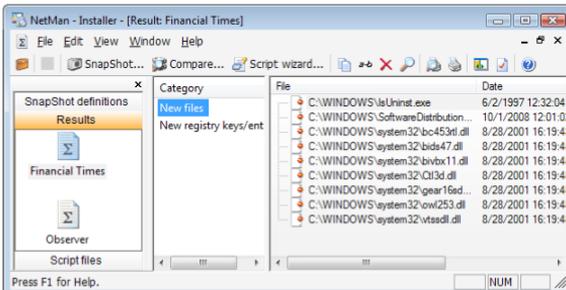
To run the comparison, open the **File** menu and select **Installer Wizard/Compare** from the menu, or click on the **Compare** button in the toolbar:



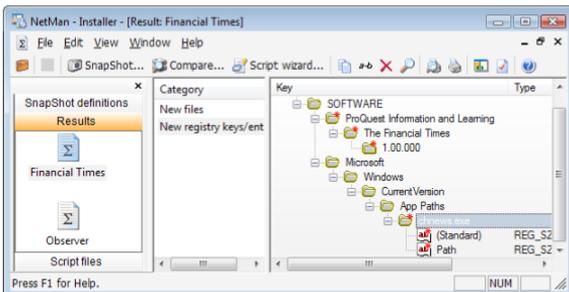
The SnapShot is loaded and the comparison made:



We save the results and then view them. We find that some new DLL files have been installed...

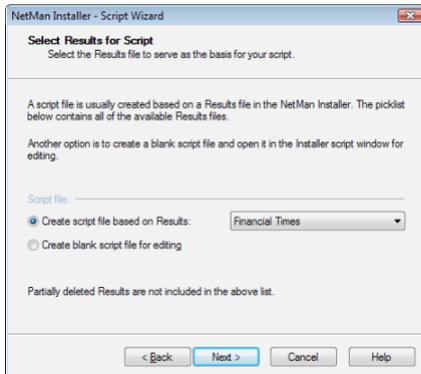


...and a number of changes have been made in the Registry:

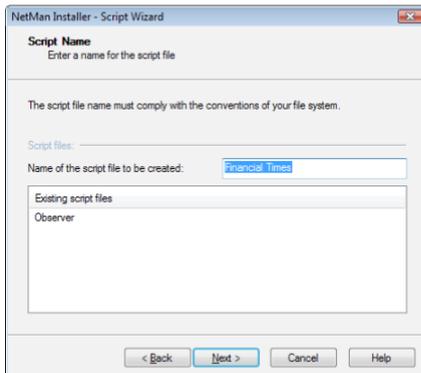


The Script

We now select **File/Script Wizard** to create a script for “Financial Times” from the results. We select the result that will form the basis of the script...



...and enter a name for the script file:



Editing the Script

We have already mentioned how important it is to edit the Installer script so that it contains only the necessary changes. In many cases, it is clear at a glance that some of the changes recorded have nothing to do with the installation of the application; sometimes there are changes listed which need not—or should not—be distributed to other workstations. You can delete or disable these entries when you edit the script. A easy way to check whether there is any need to edit the script is to try calling the application on a workstation on which it has not been installed.



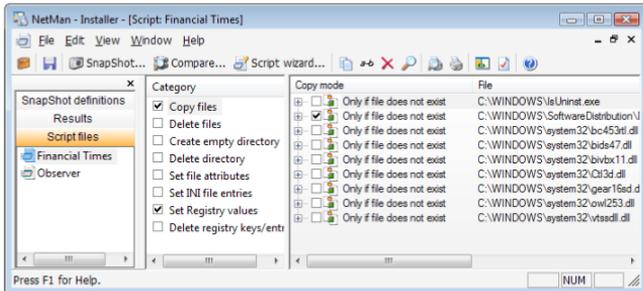
If you do not know what a given file or Registry entry does or whether it is necessary, make sure the script does not distribute it to your workstations!

The script should be adapted so that only the required changes are made on the workstation. To do this, open Script files in the sidebar of the NetMan Installer and select the new “Financial Times” script.



The Script Wizard has already replaced all path entries that are entered in the NetMan Environment with NetMan environment variables. This helps makes the script system-independent.

Now we can edit the script. We disable the copying of Registry entries and the program-specific DLLs:

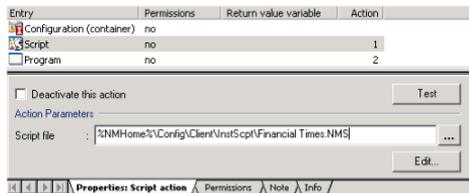


As you gain experience in using the Installer and editing scripts, it will become easier to evaluate results and decide how best to modify the script. Script entries for copying font files to the installation machine can usually be disabled, for example, because applications generally have no problem using default fonts if their own fonts are not installed. Moreover, the EXE and DLL files installed during setup can often be distributed by installing them in the new application's own working directory.

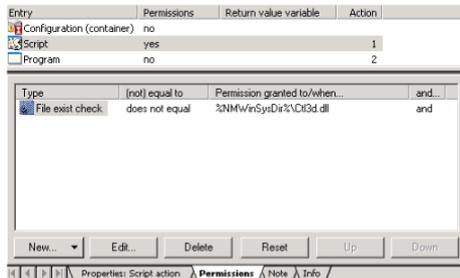
Integrating Scripts in NetMan

To integrate an installation script in NetMan, run the Management Console and add a *Script* action to the NetMan configuration for the application that the script installs. Position the Script action so that it is executed before the Program action. In the following example, we will integrate the installation script created for the “Financial Times” application:

1. Open the Management Console and select the NetMan configuration for the “Financial Times” application.
2. Move the focus to the *Program* action and add a preceding Script action.
3. In the **Script file** field, enter the full name of the “Financial Times” installation file:



4. We recommend assigning “execute” rights to the Script action so that the DLL file is copied only if it does not already exist:



5. “Financial Times” can now be launched on any workstation in the network by simply clicking on this configuration in the NetMan Client.



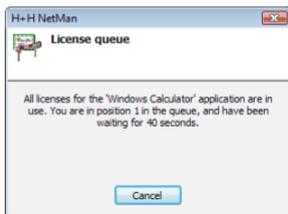
If you only use the script to install the application on a terminal server, you do not need to add a Script action to the configuration. Since the script only needs to be executed once, you can run it by simply right-clicking on the script in the NetMan Installer program.

Language Options

NetMan administrative programs are available in *German* and *English*. You are prompted to choose a language during setup, and can change the setting later in the NetMan Settings program. You can choose between these two languages for administration of NetMan regardless of whether or not you have purchased and registered the NetMan Language module. The texts in the user interface for the applications and other content you manage in your NetMan system, however, are available in only one language without the Language module. The Language module enables the following functions:

- Multilingual data maintenance
- Allocation of user-specific and user group-specific language
- Option for switching languages in the user interface during operation

NetMan shows not only the application operating controls in the selected language, but also information displayed for users, such as this message on license status, for example:



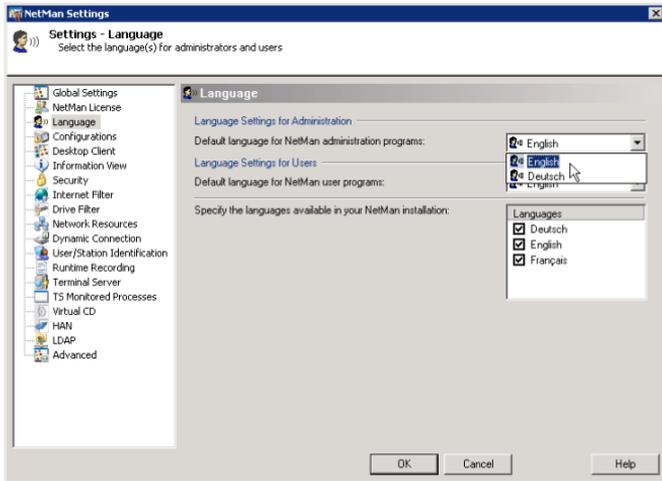
You can add the Language Module at any time to make your NetMan system multi-lingual. Unlike other modules, the language directories are not specific to particular programs, files or directories; rather, once the module is registered the functionalities described above are available throughout all NetMan programs and modules.



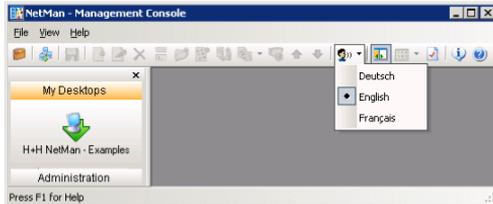
The languages available at the time of printing are English, French and German. Contact H+H for information on obtaining other languages.

Defining Which Languages are Available

Once the Language module is registered, open the NetMan Settings to define which languages are available in the user interface:



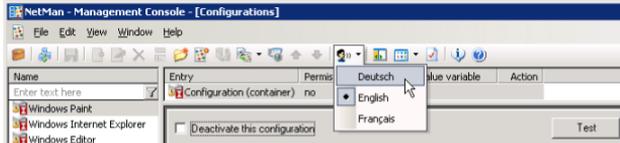
The languages you specify here are made available by the NetMan Desktop Client for users to choose from:



Creating NetMan Configurations in Multiple Languages

When you switch the NetMan Client from one language to another, you might want to edit certain user-defined text elements to match the current language setting.

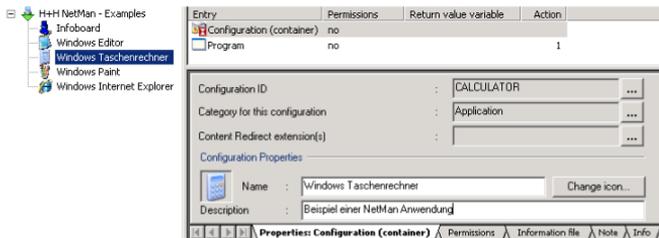
To switch languages, click the **Language** button in the toolbar of the Management Console:



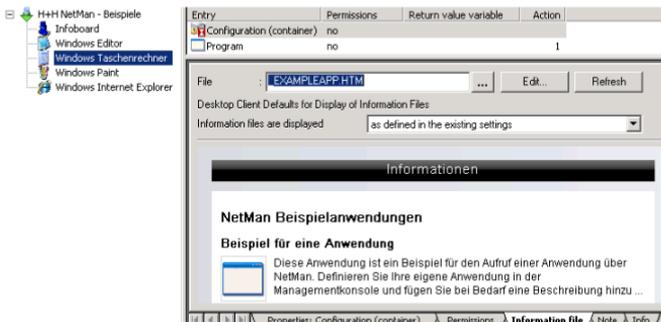
The "language-sensitive" elements you may wish to edit include:

- configuration name
- configuration description
- the information file assigned to the configuration
- any texts you might have configured in configuration actions (such as dialog box messages)

In the following example, German has been selected as the alternative language and the Windows Calculator ("Taschenrechner") configuration is being edited for language consistency:



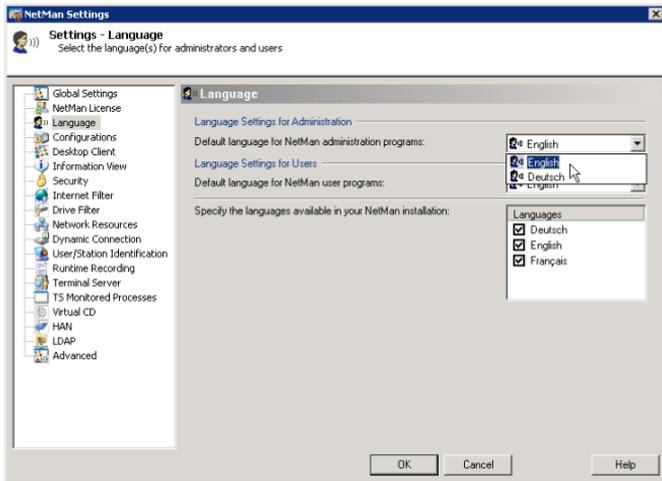
When you open the **Information file** page, the German information file is shown and can be edited if desired:



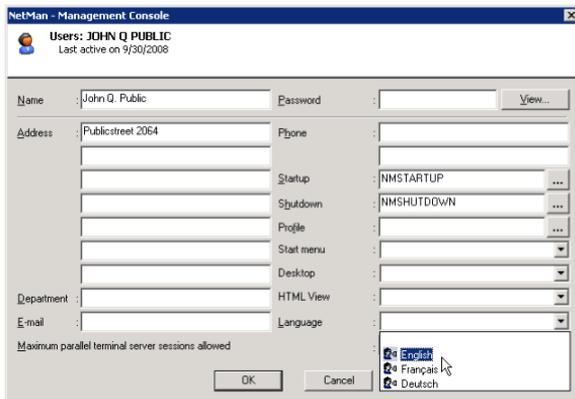
If you do not define the language-sensitive elements in other languages, NetMan shows texts the basis language (in this case, English) for these elements when the NetMan Desktop Client language setting is changed. Information files, however, are not shown at all if they do not exist in the selected language.

Defining the Default Language

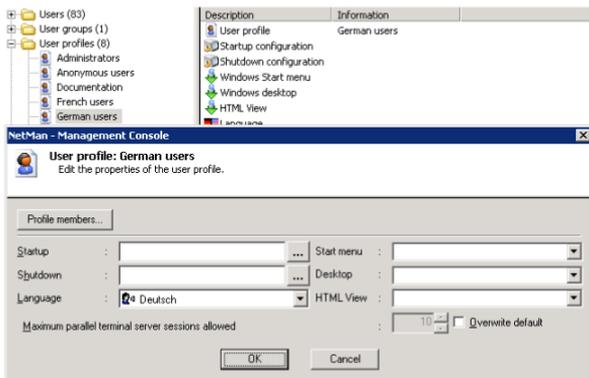
Select **Settings > NetMan Settings** in the NetMan Toolbox to edit general settings:



The default settings you define here are overwritten by any different settings you define for users or user profiles. To configure user or user profile preferences, run the Resources program in the Management Console. In this window you can define the language separately for an individual user:



You can also assign a language to a user profile; in this example, German is selected for a profile called “German Users:”



Control Options Made Possible by the NetMan Language Variable

Language settings are managed in the following variables:

- `NMLgAvailable`: Defines the available languages (separated by commas).
- `NMLg`: The language setting selected in the user interface.
- `NMLgAdmin`: The language setting selected in the administrator interface.
- `NMLgMain`: The installation language.

If you wish to define a language for a specific workstation, regardless of the user or users who might work there, you will find that there is no option for defining the language when you configure stations or station profiles. This is because in designing NetMan, we have defined language as a user property, rather than a workstation property.

Thanks to NetMan's flexible options for environment variables, however, there is a way to configure station-specific language settings.

The language setting is stored in the NetMan `NMLg` variable. Thus you can define both a global default language for the system and different default languages for individual user profiles and users. A setting for a user profile takes precedence over the global setting, and for a user over the user profile setting.

The default language setting when you install NetMan is English; i.e., this is the setting stored in the `NMLg` environment variable.

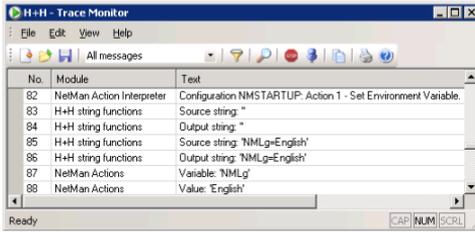
This setting is overwritten in a particular user's environment when that user selects another language, by right-clicking the NetMan tray icon and selecting a language from the shortcut menu. The NetMan Client determines its language-dependent information internally from this dynamic variable, which is why the NetMan Client is so flexible with regard to language.

To set the language separately for a given station or stations, first add an *Environment* action to the startup configuration to set the value for this variable directly in the NetMan environment:



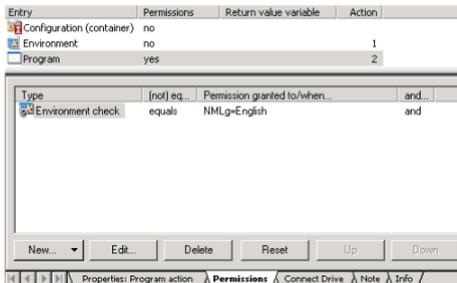
Then you can assign exclusive 'execute' rights to this action so that it is only executed for the station in question. Better yet, you can create a separate startup configuration for the workstation(s) in question so that the Environment action does not have to be processed by every station that uses NetMan.

In our example, only the station called *Nulldietus* has the right to execute this Environment action. The result of the action is shown in the Trace Monitor as follows:



This mechanism can be used in many areas of your NetMan system. On the **Advanced** dialog page of the NetMan Settings, you can define environment variables that are valid globally and can be modified for profiles, or for individual stations or users. In your NetMan configurations, you can add actions that give users the option of changing the content of variables dynamically. You can use variables to define access rights to folders or applications, or to control the processing of NetMan configurations, by assigning 'execute' rights that are based on the contents of environment variables. This means you have quite a broad range of possibilities for customizing your system. To return to the example of the Language module, the `NMLgAvailable` variable lets you define whether the optional languages are available for user selection.

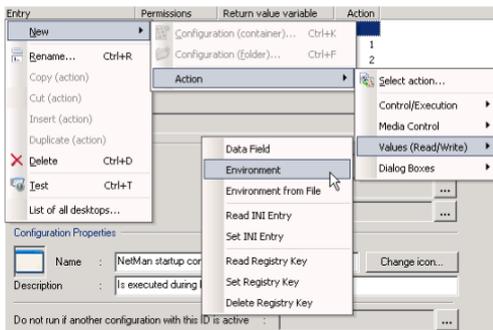
If you have a multi-lingual application for which the language setting can be defined by a command line argument, INI file entry or Registry entry, you can use the `NMLg` variable to pass the active language setting to the application. If separate versions of the application are installed for each language, you can add separate Program actions for each version to your NetMan configuration, and define 'execute' permissions to each action based on the content of the language variable:



Suppressing the Language Selection Option

You can suppress the language selection option; i.e., limit users to one language, by modifying the value in `NMLgAvailable` accordingly.

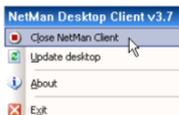
1. To do this, open your NetMan startup configuration and select **New/Action/Values (Read/Write)/Environment**:



2. If you want German to be the only available language, enter the `NMLgAvailable` variable and add "German" as the value:



3. This setting is not applied until you restart the NetMan Desktop Client. The **Language** menu item is no longer shown in the shortcut menu opened from the tray icon:



Language Controls in the HTML Framework

Language control in the framework of HTML consists in opening different HTML documents for different languages. The HTML tag

```
<!-- @NM_LANGUAGE = "DEUTSCH" -->
```

in the header of an HTML document tells HTML View to read the data for NetMan configurations and desktops from the German-language databases, and to use the templates in the German-language subdirectory for status messages (such as messages about license availability).

The different language versions can reference one another, so that the user can switch languages at any time. This is useful, for example, on workstations in public places.

NetMan Utility Programs

This chapter gives you an introduction to the following NetMan utility programs:

- **NetMan Application Library.** The Application Library is integrated in the Administration view of the Management Console. It provides you with a simple wizard for integrating software updates and other software in your NetMan installation.
- **Utility Programs for the “Execute” Action.** This is a collection of useful programs that expand the range of functions in NetMan configurations. For example, these utilities can copy or delete files, execute a login on a server or connect network drives.

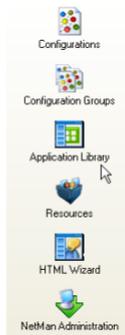
Application Library

The Application Library is a collection of “ready-made” NetMan configurations, created at H+H and available from our knowledge base or included with updates or service packs. Each *pre-defined application* includes NetMan database entries with its Program action, as well as suggestions for installation and use. Other components can be added as needed, including:

- Actions: these can be inserted before or after the Program action, as may be required or useful, and include conditions, scripts, copy and delete actions, as well as actions that modify INI files or the Windows Registry.
- HTML-based information files
- Any other type of file that may be required

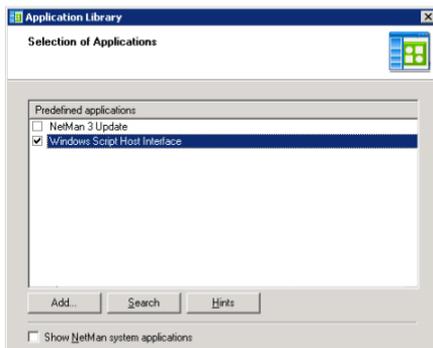
Procedures for obtaining pre-defined applications and integrating them in your NetMan system are described below:

1. The Application Library can be opened from the selection sidebar in your Management Console. Simply click once on **Application Library**:

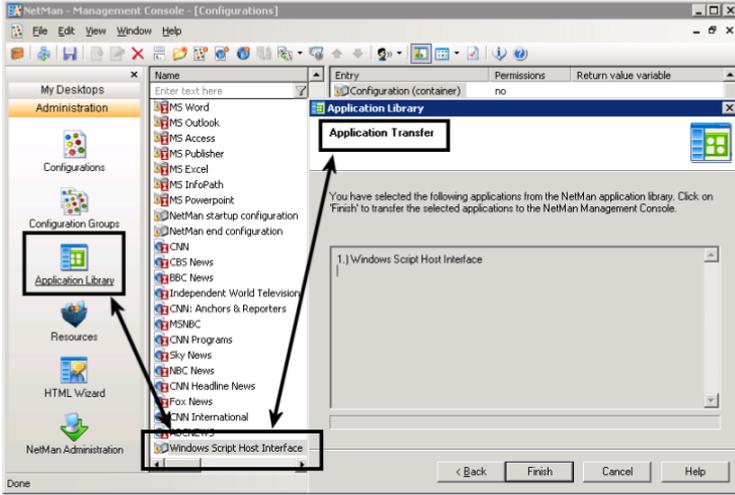


2. When the wizard opens, click on **Next**.

3. Select the desired entry under **Predefined applications**:



4. When you click on **Next**, the Application Library adds the selected application to your configurations:



If the compressed application contains new files and/or directories, you are prompted to confirm before these are written in your NetMan system.

Use the same mechanism to integrate configurations downloaded from the Internet. The Application Library automatically looks for the compressed configurations (APS files) in the %NMHome%\System\Apptemp directory.

Utility Programs for the 'Execute' Action

The small utility programs described below add to the capabilities available with your NetMan configurations. You can integrate these utilities in configurations by using *Execute* actions to call them.



In most of the examples presented in the following, the **Hold subsequent action(s) until this program is closed** property of the Execute action must be enabled to ensure successful processing on the configuration.

All utility programs are stored in NetMan's working directory (`WINDOWS\NetMan3\Bin`).

The utility programs include the following:

- HHCopy.exe
- HHMkDir.exe
- HHDelete.exe
- HHCmd.exe
- HHDummy.exe
- HHSetAtr.exe
- HHmap.exe
- HHLogin.exe

With the exception of HHDummy.exe, all of these utilities command line arguments. To view a list of the arguments valid for a given program, call the program either with no arguments or with `/?` after the program call. The dialogs generated by the utility programs can be suppressed by entering `/q` (for "quiet") when the program is called. In general, messages from these programs can be viewed in the Trace Monitor only when **Show All Messages** is enabled.



All of these utility programs can be used by NetMan customers outside the NetMan directory structure. Some of the programs, however, require additional NetMan DLLs in order to run.

HHCmd.exe - Hiding Command Execution

The following panel is opened when you enter `HHCmd.exe` or `HHCmd.exe /?` on the command line:



`HHCmd.exe` lets you execute commands entered on the command line, batch files and scripts in hidden processes. The default command processor used is configured in `HHCmd.cfg` as `Cmd.exe` and can be changed as needed.

Examples

One example for the use of `HHCmd.exe` is given above, in the section describing `HHMkDir.exe` (hidden execution of the 'Subst' command).

For another example, we will return to the problem mentioned in the description of `HHCopy.exe`, in which an application directory is restored from a protected reference installation before the application is launched (using the Update function). Simply restoring the entire directory is convenient when you do not know exactly which components need to be restored, and the process required for finding out would be too time consuming. If you do know which components might need to be restored, however, you can perform the "Update" more efficiently. The following script, `DWW_INIT.CMD` was written to eliminate problems with Dataware applications. In this case, the critical data is deleted, or restored from another directory. The path to the Dataware application is passed to the script as a command line argument, so that the script is applicable for all Dataware applications. A preceding *Execute* action calls the script for hidden processing, with the working directory for the "Dataware" application as a parameter:

```
HHCmd.exe %NMAppDrive%\DWW_Init.cmd Normdat.cdw
```

The script is as follows:

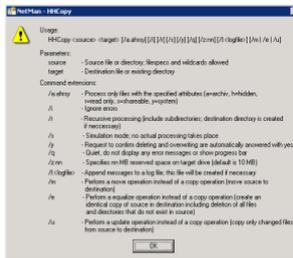
```
: First parameter: Directory of Dataware application
copy \\<Server>\NMSysprog\%1\_dw_.cfg %1\_dw_.cfg
del %1\dww.ini
```

HHCopy - Copying Files and Directories

HHCopy lets you customize copy routines as follows:

- The actions can be designed by—or completely hidden from—your end users.
- Use of these actions can be recorded in log files.
- The actions can be expanded to include subdirectories, and made dependent on file attributes.
- The “Update” and “Equalize” actions provide powerful tools for expanded functionality.

The following dialog opens when you enter `HHCopy.exe` or `HHCopy.exe/?` on the command line:



The commands and extensions give you the following options:

In the simplest case, this program *copies a file*:

```
HHCopy.exe c:\myfiles\myfile.txt c:\temp
```

A copy of “myfile.txt” is created in “c:\temp”.

You can also *use wildcards*:

```
HHCopy.exe c:\myfiles\*.txt c:\temp
```

All files with the “.txt” extension are copied to “c:\temp”.

With the “/m” option, files or directories *are moved rather than copied*:

```
HHCopy.exe c:\myfiles\*.txt c:\temp /m
```

All files with the “.txt” extension are moved to “c:\temp”.

You can also *have files/directories copied* as needed:

```
HHCopy.exe c:\myfiles\*.txt c:\temp /u
```

Files with the ".txt" extension that do not already exist in `c:\temp`, or for which a different version exists in `c:\temp`, are copied to that directory. The attributes of the file in the target directory are adapted as well.

You can *compare entire directories* as well:

```
HHCopy.exe c:\myfiles c:\temp /e
```

The content of the target directory, `c:\temp`, is made to match that of the source directory, `c:\myfiles`. Files with identical names are overwritten only if the file in the source directory has a different size or date than that of the corresponding file in the target directory. Differences in file attributes are adapted to match the files in the source directory. Files that do not exist in the source directory are deleted from the target directory.

The following options are available for the Copy, Move, Update and Equalize operations:

- `/q` Suppress standard screen output.
- `/y` Answer all prompts to confirm overwriting or deleting with "yes."
- `/i` Ignore all errors.
- `/s` Simulation mode: Operations are not actually performed. Use this function in combination with log file data to test operations.
- `/r` Perform the operation for all subdirectories of the target directory as well.
- `/a:<ahrsy>` Process only files that have the specified attribute(s).
- `/l:<log file>` Record operations in the specified log file.



This log file is created automatically if it does not already exist. The HHCOPY utility assumes that the target directory exists. The target directory is created automatically only when you call the equalize operation. For all other operations, create the target directory (if needed) using the HHMKDir command before starting the Copy operation. Exercise caution when performing an Equalize operation with the "/r" option, as incorrect usage can cause significant damage. For example, if your source directory is empty, all files and subdirectories in the target directory are deleted.



Use the "/s" switch to test operations before performing them.

Example

Say you have an application that could cease to function as a result of certain user input. At the same time, you cannot prohibit users from saving input, as 'write' permission in the application data is required for use of the application. If you have a reference installation of this application, you can insert an Update action to provide a functioning installation for users:

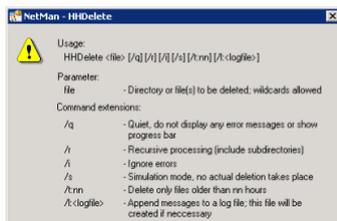
```
HHCopy.exe \\<Server>\NMSysProg\Normdat.cdw \\%NMAppUNC%\Norm-  
dat.cdw /r /u /q /i /y
```

The original installation is located in the \\< Server>\NMSysProg share. Since the Update function overwrites only changed files in the target directory, the operation is completed so quickly that the user does not even notice that saving data actually triggers an application update.

HHDelete - Deleting Files and Directories

HHDelete gives you the functions of the “DEL” and “RD” commands in a Windows program, the execution of which can be logged if desired. The HHDelete program makes it easy to delete subdirectories with names that are unknown and cannot be logically deduced. The “/t” option lets you delete files of a specified minimum age.

The following panel is opened when you enter `HHDelete.exe` or `HHDelete.exe /?` on the command line:



The following options are available:

- `/q` Suppress standard screen output.
- `/r` Perform the operation for all sub directories of the target directory as well; emptied directories are deleted.
- `/i` Ignore all errors.
- `/s` Simulation mode: Operations are not actually performed. Use this function in combination with log file data to test operations.
- `/t:nn` Directories and files are deleted only if they are at least 'nn' hours old; for directories, the age is calculated based on the latest file in the directory.
- `/l:<log file>` Record operations in the specified log file. This log file is created automatically if it does not already exist.

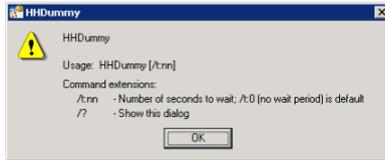
Example

Say a given application creates a large number of temporary subdirectories, named `%NMAppDrive%\ZDB\OS-xxxxx.TMP`. Generation of that portion of the directory name represented here by “xxxxx” is either random or time-dependent. With extensive use, the application creates multiple megabytes of “waste data.” Because you do not know the names of all these subdirectories, nor whether a particular subdirectory is in use at any given time, you can use HHDelete, with a wildcard, to delete data at specific intervals (for example, every 6 hours) to help minimize the accumulation of waste data. To do this, insert the following ‘execute’ action after the Program action in your NetMan configuration:

```
NMDelete %NMAppDrive%\ZDB\OS-*.tmp /q /t:6 /r /i
```

HHDummy.exe - 'Do Nothing' or 'Wait'

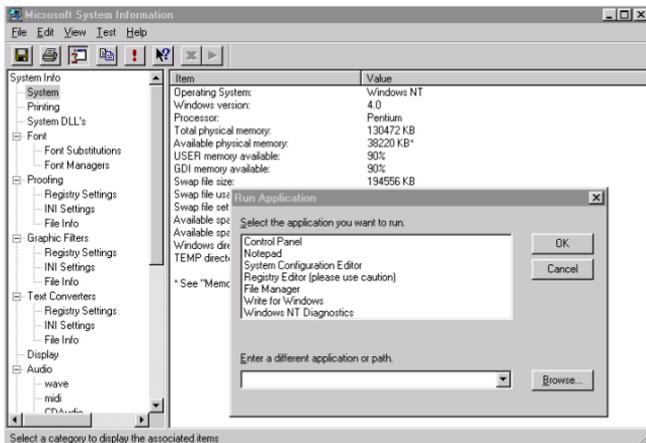
The following panel is opened when you enter `HHDummy.exe /?` on the command line:



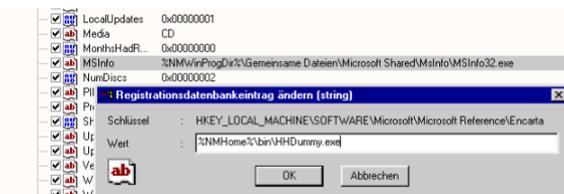
`/t:nn` HHDummy.exe closes after 'nn' seconds.

Examples

Microsoft Encarta permits users to call `MSInfo.exe`, which provides extensive information about the workstation. If the user selects "System Info," they suddenly have access that should not be permitted in a protected environment:



You could prevent this access by deleting the corresponding Registry entries, but this would result in the appearance of an annoying error message any time the button in question is activated. A better alternative is to insert "HHDummy.exe" as a 'pseudo-entry' in the Registry; now, no error message is shown and no function is activated.



HHLogin.exe - Executing a Server Login

The following dialog is opened when you enter `HHLogin.exe` or `HHLogin.exe /?` on the command line:



`/d` Execute logoff.



The "Network login" action is preferable for use in NetMan configurations, as it is easier to configure and can be tracked in the Trace Monitor. `NMLogin.exe`, on the other hand, can also be used outside the NetMan system; for example, in a script. `NMCon32.exe` does not require any other NetMan DLLs, and can be copied to other directories.

Example

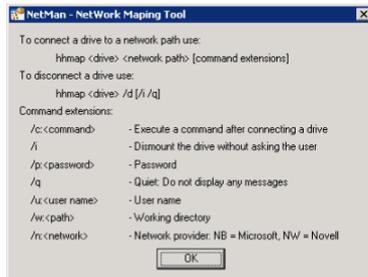
Say you want to execute a login at the beginning of a terminal server session for anonymous users who have no rights elsewhere in the network. You can use the `HHLogin` program outside the NetMan system for this purpose; for example, if NetMan is not installed on the server in question. In our example, we assume you have already set up a "Gateway user" called *NMGateway* for this purpose, with the password "*****". Now all you need to do is have the following command processed in the login script for anonymous users:

```
HHLogin.exe Server nmgateway xxxxxxxx
```

The anonymous user in question can now access resources on the server within the scope provided by the *NMGateway* account.

HHMap.exe - Connecting a Drive

The following dialog is opened when you enter `HHMap.exe` or `HHMap.exe /?` on the command line:



The following command maps the "NetMan" resource from the "Server" server to the "P:" drive:

```
HHMap.exe P: \\Server\NetMan
```

The following options are available:

- `/c:<command>` Execute the program after mapping the drive.
- `/i` Ignore all errors.
- `/p:<password>` Specifies the user password.
- `/q` Suppress standard screen output.
- `/u:<user>` User account under which the drive is connected.
- `/w:<path>` Working directory for executing the program.
- `/n:<network>` Network provider; this option speeds up execution, since the program would otherwise have to find the provider.

You can implement drive mapping within NetMan configurations by configuring the corresponding setting in the Program action or by adding a Connect Drive action (e.g., in a startup configuration). `HHmap.exe`, on the other hand, can be used outside the NetMan system; for example, by adding it to a login script. `HHmap.exe` does not require any other NetMan DLLs, and can be copied to other directories.

Example

Say you want to map a volume or share on a different server to a local drive designation at the beginning of a terminal server session, for anonymous users who have no rights elsewhere in the network.

```
HHMAP.exe P: \\Server\NetMan /q /i /u:nmanon /p:xxx /c: p:\bin  
\MyProgram.exe /w: p:\bin /n:nb
```

The options entered here have the effect that the drive is mapped under the NMAnon account, with password “xxx” with no input dialogs opened and no error messages output. Furthermore, once P: is mapped successfully, the P:\Bin\MyProgram.exe program runs in the P:\Bin directory.

HHMKDir - Creating Directories

The following dialog opens when you enter `HHMKDir.exe` or `HHMKDir.exe /?` on the command line:



Calling the `HHMKDir.exe` program is equivalent to entering the "MD" command. The only difference between the two following examples is that the first opens a command line window:

```
MD %NMHome%\User\Tmp\%ComputerName% > NUL
HHMKDir %NMHome%\User\Tmp\%ComputerName% /q
```

The `/q` option suppresses standard screen output.

Example

Say a given application requires a path for temporary files. When the program is run on a terminal server by multiple users in parallel, you need a separate "temp" path for each user. You can implement this by inserting two 'execute' actions. The first creates a workstation-specific directory, and the second uses a 'Subst' command to map it as a drive. The command lines for these two 'execute' actions are as follows:

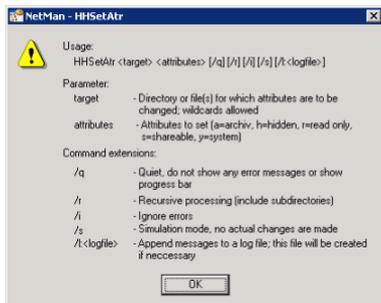
```
HHMKdir.exe %NMAppDrive%\Application\TMP\%ClientName% /q
HHCcmd.exe Subst Y: %NMHome%\User\TMP\%ClientName%
```

`HHCcmd.exe`: NetMan utility program, executes the 'Subst' command in the background (see "*HHCcmd.exe – Hiding Command Execution*" for details).

HHSetAtr.exe - Setting File Attributes

HHSetAtr.exe is a Windows program that lets you set file attributes, similar to command line program attrib.exe. Additionally, it lets you set the NetWare file attribute "Shareable" and record the operations executed.

The following panel is opened when you enter HHSetAtr.exe or HHSetAtr.exe /? on the command line:



- /q Suppress standard screen output.
- /r Perform the operation for all subdirectories of the target directory as well.
- /i Ignore all errors.
- /s Simulation mode: Operations are not actually performed. Use this function in combination with log file data to test operations.
- /t:<log file> Record operations in the specified log file. This log file is created automatically if it does not already exist.

Examples

In the first example, all file attributes are cleared from all files in the NetMan application drive so that you can tell from the 'Archive' attribute which files are updated by end users through the use of applications:

```
HHSetAtr.exe %NMAppDrive%\*.* /q /r /i
```

In the second example, all executable files are set to 'read only' mode to protect them from user manipulation, whether intentional or inadvertent:

```
HHSetAtr.exe %NMAppDrive%\*.exe r /q /r /i
```

Glossary

A

Account	Automatic access to an Internet resource through the H+H -> HAN program.
Action	An element of a NetMan -> configuration (type: container); an individual 'execute' job processed by the NetMan Action Interpreter.
Active directory	Active directory is a directory service that Microsoft introduced with Windows 2000 for central storage of all properties, such as users, groups, workstations, etc.
Almanac	An HTML document that provides an overview of NetMan directories, variables, log entry attributes and error messages.
Anonymous users	Anonymous users are user accounts on a terminal server or in a domain. They are used for anonymous access to terminal servers. Anonymous users generally have only strictly limited rights on a terminal server.
Application	The term "application" as used in this manual is often interchangeable with the term "NetMan -> configuration."
Application drive	Drive designation under which the applications integrated in NetMan are installed; stored in NetMan's %NMAppDrive% variable.
Application Library	NetMan wizard for importing -> preconfigured applications into NetMan installations. These are compressed configurations (APS files) that can be downloaded from the NetMan Web site.
Application session	This refers to a terminal server session in which only a particular application is executed rather than an entire Windows desktop. In Citrix terminology, this is referred to as a "published application."

B

Base Module	The basic NetMan program installation, without any optional modules.
Browser agent	This is a string of characters sent by every browser, indicating the browser's name, its version and – usually – the operating system on which it is running. This string is sent from the browser to the Web server over the HTTP protocol, in the HTTP header.

C

CA	-> Certification Authority
Category	Property of a NetMan -> configuration. You can group configurations into categories to ensure a clear overview of large numbers of NetMan configurations, and to present different categories with different graphics in HTML View.
Certification Authority	A Certification Authority certifies public keys from registered users in accordance with Internet standard RFC 1422; in other words, it issues certificates. The Certification Authority checks the content of the public key, particularly the identity. The underlying principle states that keys to be distributed, together with their control information, are signed off by the CA using their secret key and in this form are distributed as "certificates."
Citrix Java client	Enables access to MetaFrame server from the browser in the form of a Java applet. The Java client is useful for platform-independent access. Communication is over the ICA protocol.
Citrix Web client	Enables access to MetaFrame server from the browser. Communication is over the ICA protocol.
Classroom control	Central control element when NetMan is used as an -> educational interface. Classroom control lets you supervise the use of program operating elements by students and workgroups.
Concurrent Users	A licensing scheme that counts the number of simultaneous user sessions.
Configuration (container)	A user-definable logical unit containing a sequence of -> actions which are processed by the NetMan -> Interpreter.
Configuration (folder)	For organizing NetMan desktop entries. Folder configurations can contain hyperlink, container and folder configurations.
Configuration (hyperlink)	NetMan configuration that calls a -> hyperlink.
Console session	A special form of session in which the user is connected with the server over the RDP protocol, but sees the console window content. (Command that opens the session: MSTSC.EXE/CONSOLE.) Console sessions are supported by Windows Server version 2003 and later.
Container	Type of a NetMan configuration; see Configuration (container)

D

Desktop	The structured display of NetMan -> configurations in the NetMan Desktop Client or in an HTML page created by the NetMan HTML View.
Desktop entry	An element of the NetMan desktop. A desktop entry is a container configuration, hyperlink configuration or folder configuration.
Desktop session	A terminal server session in which a Windows desktop is available, rather than only a single application.
Dynamic connection	Mapping of a network share or volume to an available drive designation. This mechanism can use any drive for mapping, or draw from a restricted set of drives that you define.

E

Educational interface	Software specially adapted for use in an educational environment. With the NetMan for Schools Module, NetMan can provide an interface for computer-supported teaching.
Environment	The NetMan environment contains the NetMan variables. Refer to the NetMan Almanac for descriptions of all available variables.

F

Folder	Type of NetMan configuration; see also -> Configuration (folder)
---------------	--

G

GUID	A Global Unique Identifier (GUID) is a globally unique number (128 bits in length) used in computer systems. The Windows operating system uses GUIDs for unambiguous identification of objects and components.
-------------	--

H

HAN	Hidden Automatic Navigator (HAN) is a program from H+H that lets you enable access to Internet resources for your users while hiding any separate logon required for a given site, as well as precluding an IP address check of the user's computer by the target host.
HAN account	See -> Account

HTML template	A template used by HTML View and HTML Wizard to display NetMan -> configurations in HTML documents. The templates included with NetMan can be edited to suit your individual requirements.
HTML View	An optional NetMan module. HTML View runs on an NT-based Apache Web server and can output NetMan desktops and NetMan -> configurations dynamically over HTTP as HTML documents. These HTML pages are provided with links to NetMan configurations in accordance with the user privileges valid for the client in question.
HTML View Settings	Program for configuring NetMan HTML View.
HTTP session	Session with access to Web servers with scripting at the server end.
Hyperlink	URL; on-line accounts; HTML pages in general; type of NetMan configuration in particular. See also -> Configuration (hyperlink).

I

ICA protocol	Communication protocol from the Citrix company. Used with MetaFrame products to transfer screen content and user actions between server and client.
ICA session	A session on a MetaFrame server using the ICA protocol.
Installation script	A script created manually using the NetMan Installer Script Editor, or automatically by the Installer Script Wizard; integrated in NetMan -> configurations by the addition of an -> action.
Installer	See -> Installer Module
Installer: Comparison	A comparison of a computer state before a software installation to the state of the same computer after installation.
Installer Module	An optional NetMan module for monitoring the client operating system while installing applications. Changes made locally can be distributed transparently to other workstations in the network using an -> installation script. A special service lets you have local components installed under a system account if the user in question does not have sufficient privileges to perform installation.
Installer: Results	The result of a comparison between a computer state before a software installation and the state of the same computer after installation.

- Installer: SnapShot** "Picture" of a computer state.
- Installer: SnapShot definition** Selection of directories, files or Registry keys to be monitored during a software installation.

L

- Language Module** An optional NetMan module that lets you present the NetMan user interface (NetMan Client, HTML View or HTML Wizard) in different languages for different users. Also permits users to change the language during run time. The languages available are English, German and French.
- Launch method** The technique used to launch an application; i.e., determines whether an application runs locally or on a terminal server or MetaFrame server, and which client is used.

M

- MetaFrame** An add-on from Citrix for the Microsoft Terminal Server. Enables, for example, access to MetaFrame servers from non-Windows platforms such as Macintosh or Unix. The latest version is sold under the name "Presentation Server." See also -> Presentation Server.
- MetaFrame server** A product from the Citrix company that adds certain performance features to Microsoft terminal services.
- Microsoft RDP Web client** Lets you access a Windows server with terminal services. Communication is over RDP.

N

- Named Licenses** A licensing scheme that counts the number of workstations registered in the NetMan system. Each station is registered automatically when it logs on to NetMan. If a license is unused for a period of 40 days, it is released and can be used by another station.
- NetMan Access Control** The NetMan Access Control program lets you specify IP addresses and host names for granting or denying access. You can have user names assigned on the basis of IP address (or segments of addresses), for example to provide more meaningful identifiers that Windows can for anonymous users, when using the NetMan User Service. An IP addresses or host name-based user name at least provides information on the range of IP addresses or host names in which the client can be found.

- NetMan Action Interpreter** Executing instance of the NetMan Desktop Client. Execute jobs downloaded from the central NetMan system are processed and executed by the NetMan Action Interpreter.
- NetMan Client Service** A service that is required on stations on which the NetMan Desktop Client is installed.
- NetMan Desktop Client** The NetMan user interface on Windows workstations; integrates NetMan desktops in the Windows desktop and/or Windows Start menu. The NetMan Desktop Client can remain completely invisible to your users, or can place an icon in the notification area of the system tray for user access.
- NetMan for Schools** Optional NetMan module for use in educational networks. The Classroom Control feature lets you configure station profiles from a central machine, to adapt client computers to the special requirements of teaching situations. The User Account Wizard supports management of teacher and student accounts.
- NetMan placeholders** Elements used by NetMan in HTML pages and templates. The HTML View module replaces placeholders with certain specified content.
- NetMan RDP Web Client** Lets you access a Windows server with terminal services. This client offers more functions than the Microsoft RDP Web client. Communication is over RDP.
- NetMan Service** Central NT service that manages data on users, stations, licenses and the usage of NetMan configurations.
- NetMan start file** A file with the two-letter extension NM; when this file type is used to launch a NetMan -> configuration from HTML View or the HTML Wizard, the configuration runs on the client machine rather than on a terminal server.
- NetMan Toolbox** The Toolbox is an interface to administrative utilities.
- NetMan tray program** User interface to the NetMan Desktop Client; can be used to open or close the NetMan Desktop Client, check its status and, if the Language Module is installed and registered, to change the interface language.
- NetMan user service** The NetMan user service sets passwords at run time for the anonymous users created by the User Account Wizard of the NetMan Web Service.
- NetMan Web Services** Services that implement the main functions of the Terminal Server and HTML View modules.

NM files	Files with the *.nm file name extension; used for launching NetMan configurations from HTML pages. See also -> NetMan start file.
NT4 Domain	A central user database for Windows networks. Starting with Windows 2000, this has been replaced by --> active directory.
NTFS	New Technology File System: developed by Microsoft for the Windows NT/2000/XP operating systems.

P

Preconfigured application	Ready-to-use NetMan -> configurations provided by H+H for import into your NetMan installation, using the -> application library.
Presentation Server	An add-on from Citrix for the Microsoft Terminal Server. Enables, for example, access to Presentation Servers from non-Windows platforms such as Macintosh or Unix.
ProGuard	Optional NetMan module for process-level control of network clients.
Published application	Created with Citrix software to access a session on a -> terminal server. This published application is required by the -> HTML View for making a connection.

R

RDP protocol	A protocol for communication between workstation and terminal server, used to transfer screen content and user actions. The RDP protocol is based on the ITU standard T-120 and was adapted by Microsoft for the special requirements of terminal servers.
RDP session	A session on a terminal server using the RDP protocol.
Record attribute	Item of information recorded in addition to standard items such as user name, station, date, time, when data logging is active. Please see the NetMan Almanac for a complete list of available attributes.
Remote administration	Technology that enables remote administration of servers and workstations. RDP is one of the protocols that Microsoft uses for remote administration.
Remote desktop user	A local user group on a terminal server. All users who wish to open a session on a terminal server must be members of this group.

S

Shutdown configuration	A -> configuration specified in the NetMan Settings; processed when the NetMan software is shut down.
SnapShot	A "picture" of the current system state on a workstation, created by the NetMan -> Installer.
Startup configuration	A -> configuration specified in the NetMan Settings to be processed when NetMan is launched.
Station database	NetMan database in which every station that starts NetMan is automatically registered under the given NetMan -> station ID.
Station ID	A unique designation that identifies a workstation; registered in the -> station database.
Station profile	A set of defined preferences; you can assign the same profile to multiple stations, but each station can be assigned only one profile.

T

Terminal server	The Microsoft Terminal Server provides server sessions for remote Windows clients. Applications launched by the client run on the server and do not require any specific components on the client computer.
Terminal Server Module	An optional NetMan module for using NetMan in terminal server environments.
Terminal services	Terminal services from Microsoft make it possible to open a session on a Windows server over RDP, during which screen content and user actions are transferred.
Ticketing	Technique for issuing a "ticket" (a form of server access permission). In NetMan, the ticket contains information specifying the application to be executed on the server for the user. A ticket is valid for a limited time only, after which it cannot be used.
Timeout	A program that monitors applications started by NetMan and ends them if no input is detected for a defined period of time.

U

URL	Uniform Resource Locator; a type of Uniform Resource Identifier (URI). A URL identifies a resource by its primary access mechanism (e.g., HTTP or FTP) and the location of the resource in a computer network.
User database	NetMan database in which every user that starts NetMan is automatically registered under the given NetMan -> user ID.
User group	You can group your NetMan users; for example, to simplify the assignment of permissions.
User ID	A unique designation that identifies a user; registered in the -> user database.
User profile	A set of defined preferences. You can assign the same profile to multiple users, but each user can be assigned only one profile.

V

Variable	NetMan supports both system and local environment variables. NetMan variables are described in the NetMan -> Almanac.
-----------------	---

W

Windows Script Host	(WSH) Provided by Microsoft for extending the Windows operating system. The script host enables access to operating system functions over VBScript and JScript. NetMan provides interfaces to its system functions for the script host, which can be used by VBScript and JScript programmers to expand and adapt NetMan features.
Working directory	The working directory for NetMan is %WinDir%\NetMan3\Bin.

Index

Symbols

2-factor authentication 75

A

Access control 60, 374

Accessing applications over the NetMan SSL gateway 245

Accessing the NetMan RDP Session Broker 332

Access permissions for configurations and actions 117

Access privileges for client drives 371, 374, 376

Access privileges for client drives\
Setting up access privileges 374
Using NetMan actions to modify access 376

Actions 125

Action sequences 44

Active Directory service 60

Additional program properties 106

Additional tips for operation in terminal server environments 345

ADMIN\$ shares 33

Administrators 79

ADS login 232

Advanced application settings for a session 339

Advanced security features 365

Advanced settings 74

After installation 65

ALEPH login 234

Allocated client drives 47

Allocating licenses 177

Analyzing data with the NetMan statistics program 421

Anonymous users 212, 213, 217, 363

Anonymous users\
Settings 217

Application drive 86

Application framework 3

Application management 3
 application/x-ica 210

Areas of application and how an installer works 440

Associated client printers 47

Authentication 183

Authentication Services 223, 224, 225, 228, 230, 231, 232, 233, 234, 235, 236

Authentication Services\
ADS login 232
ALEPH login 234
Authentication page 225
Configuring 228
IP address/Host name check 228
LDAP login 230
NetMan login 232
NT Challenge/Response login 236
NT login 231
ODBC login 234
PICA login (CBS) 232
PICA login (LBS) 233
SIP2 login 235
SISIS login 233
STAR login 235

B

Bandwidth management for the universal PDF printer driver 393

Blocking access to particular URLs 403

Browser agent 200

C

- Calling a MetaFrame session 259
- Calling applications through the web interface 187
- Calling a terminal server session 252
- Calling hyperlinks through the web interface 189
- Capturing trace messages from session 359
- CD-ROM-based applications 151
- Certificate 47, 183, 244
- Certificate authority 50
- Certificate file 50
- Certificates 49
- Certificates for NetMan web server 49
- Changing the operation mode 349
- Check action processing 127
- Citrix anonymous users 212
- Citrix Anonymous Users 337
- Citrix anonymous users in domains 363
- Citrix Java client 210
- Citrixjava.htm Template file 210
- Citrix web client 207, 301, 308
- Citrix Web Client 341
- Client drives 203, 207, 304, 308
- Client drives with 'read only' privileges 371
- Client drives with 'write only' privileges 371
- Client printer 203, 207, 304, 308
- Closing an application session 347
- Codebase 210
- COMAllowed 207, 308
- Comparing system states after installation 450
- Complex actions 137
- Compress 207, 308
- Computer name 353
- Concurrent use table 419
- Configuration 74
- Configuration groups 68
- Configurations 68
- Configuring anonymous user accounts (MetaFrame) 263
- Configuring anonymous user accounts (terminal server) 255
- Configuring different types of authentication services 228
- Configuring HTML View 251
- Configuring HTML View for access on MetaFrame servers 260
- Configuring HTML View for access on terminal servers 252
- Configuring privileges to print objects 391
- Configuring the HTML View explorer view 293, 294, 295
- Configuring the HTML View explorer view\
 - Modifying the HTML page for launching applications* 295
 - Modifying the login page* 294
- Configuring the HTML View list view 283, 284, 287, 288, 289, 290
- Configuring the HTML View list view\
 - Placeholders in templates* 288
 - Practical Example* 290
 - Templates for application launch* 287
 - Templates for generating desktop structures* 284
 - Using style sheets* 289
- Configuring the NetMan gateway 248
- Configuring the NetMan user service 213
- Configuring the RDP Session Broker 331
- Connecting a printer 381
- Connection monitor 250
- Connection settings 203, 207, 304, 308
- Contents of this manual 23
- Controlling an action sequence 130
- Control options made possible by the NetMan language variable 469
- Copyright notices 9
- CPMAllowed 207, 308
- Creating additional desktops 122
- Creating anonymous users 213

Station Groups 163

User Groups 163

GUID 369

H

Help programs 359

HHCmd.exe 477

HHCopy 481

HHDelete 484

HHDummy.exe 485

HHLogin.exe 486

HHMap.exe 487

HHMKDir 489

HHSetAtr.exe 490

HHTrace.exe 357

Host name 200, 302

Host-name level 403

How the Authentication Services work 224

HTML Framework 5

HTML View 179, 241, 248

HTML View settings 193, 194, 196, 197

HTML View settings\

Filter configuration 196

Global settings 194

Permit operating systems 197

HTTP 47, 75, 395

HTTP addresses 403

HTTPBrowserAddress 207, 308

HTTPS 47, 75, 183, 248, 395

HTTPS addresses 403

HTTPS port 242

Hyperlink 92

Hyperlinks 403

I

ICA client 207, 210, 308

ICA protocol 207, 210, 308

Ideas and suggestions 15

INF file 381

Infoboard 82

Information display 74

Information files 82

Initial setup of anonymous user accounts 215

Input prompt in a session 359

Installation 213

Installation of NetMan Desktop Client using a software deployment tool 33

Installation of NetMan Desktop Client using NDCDEPLOY 33

Installation with the NetMan Installer 454, 455, 456, 457, 458

Installation with the NetMan Installer\

Application setup 455

Editing the script 458

From comparison to result 456

The script 457

The Snapshot 454

Installer 71, 431, 439

Installer\

Basics 439

Installing NetMan 25

Installing NetMan Desktop Client 31

Installing NetMan SSL Gateway 242

Installing the ICA web client 259

Installing the NetMan RDP client 185

Installing the NetMan user service 213

Installing the RDP Session Broker 330

InstallShield 33

InstallShield package 33

Integrating applications and hyperlinks 91

Integrating HAN accounts 160

Integrating scripts in NetMan 459

Interactive login per session 311, 316

Internet access 395

Internet filter 395, 397, 399, 401, 403, 407, 409

Internet filter\

Creating a global Internet filter 401

Creating rules for filtering processes 407

Creating rules for filtering URLs 403

- Editor for Internet filter files* 399
- Switching the Internet filter on and off* 397
- Testing an Internet filter file* 409

- Internet filter action 397
- Internet filter files 75
- Internet Filter Settings 75
- IP address 200, 353
- IP addresses 301, 302
- IP address/Host name check 228

J

- Java applet 210
- Java RDP web client 206

L

- Language 74
- Language controls in the HTML framework 473
- Language options 461, 463, 465, 467, 469, 471, 473
- Language options\
 - Control options made possible by the NetMan language variable* 469
 - Creating NetMan configurations in multiple languages* 465
 - Defining the default language* 467
 - Defining which languages are available* 463
 - Language controls in the HTML framework* 473
 - Suppressing the language selection option* 471
- Launch method 75, 302
- Launch methods 311
- Launch methods for HTML View 199
- Launch methods for NetMan Desktop client 301
- LDAP 74
- LDAP login 230
- License Monitor 72
- Licenses 72, 177
- License waiting period 416

- Licensing 77
- Licensing and registration 19
- Linux workstation 200
- List of terminal servers and load balancing 321
- Load balancing 75, 207, 308, 321, 343
- Load balancing in application sessions 321
- Load Report 325
- Local printers 379
- Local resources 355
- Logging in through the web interface 183
- Login 183
- Login data 313
- Login data from HTML View 212
- Login method for sessions 75
- Login methods for HTML View 211
- Login methods on MetaFrame servers 337
- Login methods on terminal servers 311, 313, 315, 316, 317
- Login methods on terminal servers\
 - Interactive login per session* 316
 - One-time login using NetMan Desktop client* 315
 - Use local login data* 313
 - Using NetMan anonymous user data* 317
- Log users off of session 359

M

- Main table 413, 416
- Management Console 68, 165
- Management of Internet resources 5
- Manual startup 213
- Mapping a printer 381
- Mapping client drives 355
- MetaFrame Presentation server 3.0 343
- MetaFrame XP 343
- Meta-IDs 416
- Meta-users 416
- Microsoftrpd.htm 203
- Mirroring a session 359

- Modified audio settings 343
 - Modified window settings 343
 - Modifying printer mapping 381
 - Modifying the launch method 301, 341
 - Modifying the login page 294
 - Monitored processes for application sessions 347
 - Monitors 72
- ## N
-
- Ndcdeploy.exe 33
 - NetMan access control 165
 - NetMan Access Control 60, 75
 - NetMan actions 125
 - NetMan Administrators 79
 - NetMan anonymous users 212
 - NetMan Authentication Services 76
 - NetMan concepts 81
 - NetMan configurations 92
 - NetMan databases 44, 77
 - NetMan Desktop Client 33, 55, 57, 77, 200, 302, 341
 - NetMan Desktop Client Distribution 33, 77
 - NetMan Desktop Client Distributor 34
 - NetMan Desktop Manager 68
 - NetMan Environment 84
 - NetMan filter settings 75
 - NetMan Installer 71
 - NetMan Internet filter 395
 - NetMan Licenses 177
 - NetMan login 165, 232
 - NetMan programs 67
 - NetMan RDP Session Broker 329, 330, 331, 332
 - NetMan RDP Session Broker\
 - Access 332
 - Configuration 331
 - Installation 330
 - NetMan RDP web client 200, 203, 301, 302, 304
 - NetMan Ressources 163
 - NetMan server components 27
 - NetMan service 45
 - NetMan settings 351
 - NetMan Settings 74
 - NetMan SSL gateway 241, 244, 248, 250
 - NetMan SSL gateway\
 - Configuration 248
 - Connection monitor 250
 - Creating an SSL certificate 244
 - Introduction 241
 - NetMan SSL Gateway 242, 245
 - NetMan SSL Gateway\
 - Accessing applications 245
 - Installation 242
 - NetMan SSL Gateway connection monitor 250
 - NetMan start file 202
 - NetMan startup and shutdown 88
 - NetMan startup configuration 363
 - NetMan statistics program 411
 - NetMan Statistics program 413
 - NetMan Toolbox 60
 - NetMan user database 165
 - NetMan user groups 169
 - NetMan users 165
 - NetMan User Service 213
 - NetMan utility programs 475
 - NetMan web service 47
 - NetMan web services 200, 301, 302, 321
 - NetMan Web Services Settings 75
 - Network provider 313
 - Network resources 74
 - Network rights 79
 - NM_ALTERNATE_ADDRESS 207, 308
 - NM_BROWSER_PROTOCOL 207, 308
 - Nmchttp.exe 335
 - NMCHttp.exe 357
 - NMCHTTP.EXE 203, 304

NM_CMDPARAM 203, 207, 304, 308
 NM_COMPRESS 207, 308
 Nmcsetup.cfg 33
 NM_DESCRIPTION 210
 NM_DOMAIN 203, 207, 304, 308
 NM_HEIGHT 210
 NM_HTTPBROWSER 207, 308
 NM_ICA_DISPLAY 207, 308
 NM_ICA_SSL_ENABLE 207, 308
 NM_ICA_USE_LOCALUSERDATA 207, 308
 NM_LAUNCH 210
 NM_LIST_DOMAIN 203, 304
 NM_LOGONTYPE 203, 304
 NM_PASSWD 203, 207, 304, 308
 NM_PROMPT 203, 207, 304, 308
 NM_PUBAPP 207, 308
 NM_RDPBMPCACHE 203, 304
 NM_RDP_DISPLAY 203, 304
 NM_RDPFLAGS 203, 304
 NMRDPHelper.exe 347
 NM_RDP_SERVER 203, 304
 NM_REDIRECT_ICA_COMPORTS 207, 308
 NM_REDIRECT_ICA_DRIVES 207, 210, 308
 NM_REDIRECT_ICA_PRINTERS 207, 210, 308
 NM_REDIRECT_RDP_COMPORTS 203, 304
 NM_REDIRECT_RDP_DRIVES 203, 304
 NM_REDIRECT_RDP_PRINTERS 203, 304
 NM_SCREENPERCENT 210
 NM_SEAMLESS 210
 NM_SECTION_COMPRESS 207, 308
 NM_SECTION_ENCRYPTION 207, 308
 NM_SSL_PROXY_HOST 207, 308
 NMSTSMMod.exe 349
 NM_TCPBROWSER 207, 308
 NM_USER 203, 207, 304, 308
 NM_WIDTH 210
 NM_WINDOWTYPE 210
 Notes for test users 21

Notes on working with this manual 11
 NT Challenge/Response login 236
 NT group membership 75
 NT login 231
 Number of parallel sessions 351

O

ODBC login 234
 OEM printer driver name 381
 Official certificate (from CA) 47
 Official certificates 50
 One-time login using NetMan Desktop client 315
 One-time login using NetMan Desktop Client 311
 Online Documentation 78
 Opening sessions from NetMan Desktop client 299
 Overview of launch methods 301

P

Password 207, 308
 PCL driver 383
 PDC emulator 213
 PDF preview 389
 Permissions 44
 Permissions for client drives denied 374
 Permissions for client drives granted 374
 Permitted addresses 75
 PICA login (CBS) 232
 PICA login (LBS) 233
 Placeholders 207, 308
 Placeholders in templates 288
 Port 443 242
 Port 3389 242
 Postscript driver 383
 Practical example\
 Using the HTML View list view 290
 Preface 1
 Prerequisites for working with the NetMan Installer 433

Printer driver 379
 Printer mapping 381
 Printers in WAN environments 393
 Printing 377
 Print preview 389
 Problems launching NetMan 357
 Process list 347
 Process list for application sessions 347
 Profile settings 351
 Program 92
 Program actions 104
 Proxy 207, 308
 Published application 335

R

rdesktop over Java Applet 206
 RDP protocol 203, 304, 321
 RDP session 203, 304
 RDP sessions 304, 321
 RDP support for local printers 379
 Recommended readings on the Windows Registry 435
 Record Database Viewer 72
 Registering NetMan 39
 Registration Wizard 77
 Requesting and importing certificates 244
 Requesting and importing official certificates 50
 Requirements for the installation of the NetMan Installer 437
 Resources window 68
 Ressorces 163
 Results of comparison 446
 Rule 403
 Rules for determining the launch method 200, 302
 Running a program in a session 359
 Running the NetMan Installer 442
 Running the trace monitor in a session 359

S

Script files 447
 Seamless mode 47, 207, 210, 308
 Security 74
 Security settings 60
 Select ICA automatically 210
 Self-signed certificate 47, 244
 Sending a message to a session 359
 Separate session parameters for an application call 343
 Seperate launch method settings for an application call 341
 Server and Station Monitor 73
 Server certificate 183
 Server software 43
 Service 45, 47, 213
 Session Broker 329
 Session number 353
 Session reset 359
 Session resolution 47
 Sessions 353
 Session settings 75
 Session Sharing 327
 Set Client Drive Filter 376
 Set Client Drive Filter action 376
 Settings 74
 Setting up access privileges for client drives 374
 Setting up anonymous user accounts 215
 Setup 77
 Setup.exe 33
 Showing or hiding the universal PDF printer driver 391
 Shutdown configurations 148
 Silent mode 77
 Simple examples of the most frequently used actions 134
 Single sign-on 74, 313, 315
 SIP2 login 235
 SISIS login 233

- SnapShot definition files 442, 443, 445
 - SnapShot definition files\
 - Monitoring the Registry* 445
 - Selecting files* 443
 - SnapShot of the workstation 449
 - Software distributor 37
 - Sound settings 47
 - Special configurations and applications 147
 - SSL connection 241
 - Standard.ndp 315, 357
 - STAR login 235
 - Startup configurations 148
 - Station database 173
 - Station groups 44, 68, 171
 - Station ID 353
 - Station Monitor 73
 - Station names in the terminal server environment 353
 - Station profiles 44, 68, 173, 175
 - Stations 44, 68, 73, 163
 - Statistical analysis of log files 411
 - Statistical analysis with the NetMan statistics program 413
 - Statistics 70
 - Statistics program 411, 413
 - Step by step\
 - From SnapShot to script* 449
 - Support 13
 - Supressing the language selection option 471
 - Switching the Internet filter on and off 397
 - Switching the PDF preview on and off 389
 - System requirements 17
 - System structure 41, 45
- ## T
-
- Table of concurrent use 413
 - Tables 415, 416, 419
 - Tables\
 - Main table* 416
 - Table of concurrent use* 419
 - TCP/IP 45
 - Technical structure of the NetMan Desktop Client 57
 - Templates for application launch 287
 - Templates for generating desktop structures 284
 - Terminal server 203, 304
 - Terminal Server Easy Print in Windows Server 2008 385
 - Terminal server login 211
 - Terminal servers 74, 301, 321, 351, 353
 - Testing an Internet filter file 409
 - ThinPrint Engine 304
 - Ticketing 367
 - Toolbox 68
 - TPCInRDP.dll 304
 - Trace monitor 127
 - Trace Monitor 72, 357
 - Troubleshooting application problems 359
 - TS monitored processes 74
- ## U
-
- Universal PDF printer driver 377, 387, 391
 - Universal printer driver 377
 - Universal printer driver in Windows Server 2003 SP1 383
 - URL level 403
 - Use local login data 311, 313, 337
 - Use login data from HTML View 212
 - Use NetMan anonymous users 212, 311, 337
 - User account 213
 - User groups 44, 68, 169
 - User ID/station ID 74
 - User profile 68
 - User profiles 44, 173, 174
 - Users 44, 68, 163, 165
 - User tickets for the web interface 369
 - Using a different published application 343
 - Using a different terminal server 343
 - Using an installer in a network 440

Using an installer in a terminal server environment 440

Using NetMan actions to modify access in client drives 376

Using NetMan anonymous user data 317

Using style sheets 289

Using the HTML View list view 290

Using the Trace Monitor to check action processing 127

Utility programs 475

V

Variables 72

Virtual CD 74

VPN infrastructure 55

W

Web interface 75, 187, 189

Web interface (HTML View) 179

Weighting 321

Window and audio settings 203

Window/Audio settings 207, 304, 308

Windows script enhancements 140

Wizards 77

Working with the Management Console 97

X

XML structures 45

Y

Your first application 115



<http://www.hh-netman.de/en>