

# NetMan Desktop Manager 4.5



H+H Software GmbH



# Table of Contents

Introduction	1
Contents of This Manual	3
NetMan Desktop Manager: The Basics	5
Performance Features	9
Desktop Sessions and Application Sessions	13
Sessions in the Windows Interface and in the Web Interface	15
Installation	17
System Requirements	19
System Requirements for Windows Server 2003 Terminal Server	21
System Requirements for Windows Server 2008 with Terminal Services Role	23
System Requirements for Windows Server 2008 R2 with Remote Desktop Services Role	29
Installation Principles	33
Overview	33
Installing NetMan Desktop Manager on a Terminal Server	34
NetMan Desktop Manager in a Multiple Terminal Server Environment	39
Installing NetMan Desktop Client	39
Distributing NetMan Desktop Client in the Network	41
The First Steps with NetMan Desktop Manager	45
The First Time an Administrator Runs NetMan Desktop Client	47
Allocation of NetMan Desktops	49
The First Time a User Runs NetMan Desktop Client	51
First Steps with the Web Interface	53
Advantages of the Web Interface	55
Logging in through the Web Interface	57
Installing the NetMan RDP Web Client	59
Calling Applications through the Web Interface	61
Examples of Integration in Terminal Server Environments	63
Overview	65
NetMan Desktop Client on a Workstation	67
NetMan Desktop Client as Terminal Server Interface	69
System Structure	71
Overview	73
Server Software	75
NetMan Databases	75
NetMan Service	75
NetMan Web Server	77
Certificates for NetMan Web Server	79

Client Installations .....	85
NetMan Desktop Client: The Basics .....	85
Technical Structure of the NetMan Desktop Client .....	86
Security Aspects Relating to NetMan Desktop Client .....	89
<b>NetMan Desktop Manager Programs</b> .....	<b>93</b>
<b>Management Console</b> .....	<b>95</b>
<b>Statistics</b> .....	<b>97</b>
<b>Monitors</b> .....	<b>99</b>
Trace Monitor .....	99
Trace Monitor for Console Messages .....	99
Environment Monitor .....	100
License Monitor .....	100
Database Browser .....	100
Server and Station Monitor .....	101
<b>Settings</b> .....	<b>103</b>
NetMan Settings .....	103
Internet Filter Settings .....	104
NetMan Web Services Settings .....	105
NetMan Access Control .....	105
<b>Wizards</b> .....	<b>107</b>
NetMan Desktop Client Distribution .....	107
Database Wizard .....	107
Registration Wizard .....	108
<b>Integrating Applications and Hyperlinks</b> .....	<b>109</b>
<b>NetMan Configurations</b> .....	<b>111</b>
<b>Working with the Management Console</b> .....	<b>115</b>
The Sample Desktop .....	115
A NetMan Configuration .....	116
Program Actions .....	121
Additional Program Properties .....	122
Creating and Deleting Desktop Entries .....	125
Your First Application .....	130
Access Privileges for Configurations and Actions .....	132
Creating New Desktops .....	137
<b>NetMan Actions</b> .....	<b>141</b>
Overview and General Rules .....	141
Using the Trace Monitor to Check Action Processing .....	142
Controlling an Action Sequence .....	144
Simple Examples of the Most Commonly Used Actions .....	148
Complex Actions .....	151
Windows Script Enhancements .....	154
<b>Special Configurations and Applications</b> .....	<b>159</b>
Startup and Shutdown Configurations .....	159
Integrating CD-ROM-based Applications .....	161

<b>NetMan Desktop Manager Resources</b>	<b>169</b>
Users, Stations, Groups and Profiles .....	171
NetMan Users .....	173
NetMan Stations .....	175
NetMan User Groups .....	177
NetMan Station Groups .....	179
NetMan User and Station Profiles .....	181
User Profiles .....	183
Station Profiles .....	185
<b>Web Interface</b>	<b>187</b>
Introduction to the Web Interface .....	189
2-Factor Authentication .....	191
Launch Methods for HTML View .....	193
Overview of Launch Methods .....	193
NetMan RDP Web Client .....	194
rdesktop using a Java Applet .....	199
Java RDP Web Client .....	199
Citrix Web Client .....	201
Citrix Java Client .....	204
Select ICA Automatically .....	205
Rules for Determining the Launch Method .....	205
Login Methods for HTML View .....	209
Overview of Login Methods .....	209
Login Data from HTML View .....	210
NetMan Anonymous Users .....	211
Anonymous Users .....	211
NetMan SSL Gateway .....	221
Introduction to the NetMan SSL Gateway .....	221
Installing NetMan SSL Gateway .....	222
Creating an SSL Certificate .....	223
Accessing Applications over the NetMan SSL Gateway .....	224
Configuring the NetMan SSL Gateway .....	226
NetMan SSL Gateway Connection Monitor .....	228
Web Interface Design .....	231
Introduction to Web Interface Design .....	231
Login Page .....	231
Example of Login Page Modification .....	232
HTML Page for Launching Applications .....	233
Simple Modifications to the Application Launch Page .....	236
<b>Opening Sessions from NetMan Desktop Client</b>	<b>241</b>
Launch Methods for NetMan Desktop Client .....	243
Overview of Launch Methods .....	243
NetMan RDP Web Client .....	244
Citrix Web Client .....	248
Rules for Determining the Launch Method .....	251

Login Methods on Terminal Servers.....	253
Overview of Login Methods.....	253
Use Local Login Data.....	254
One-time Login using NetMan Desktop Client.....	255
Interactive Login per Session.....	256
Use NetMan Anonymous Users.....	256
<b>Extensions for Terminal Servers</b> .....	<b>257</b>
Load Balancing in Application Sessions.....	259
Performance Report.....	263
Session Sharing.....	265
NetMan RDP Session Broker.....	267
Overview of the RDP Session Broker.....	267
Installing the RDP Session Broker.....	267
Configuring the RDP Session Broker.....	268
Accessing the NetMan RDP Session Broker.....	269
<b>Extensions for MetaFrame Servers</b> .....	<b>271</b>
Published Application.....	273
Login Methods on MetaFrame Servers.....	275
<b>Advanced Application Settings for a Session</b> .....	<b>277</b>
Separate Launch Method Settings for an Application Call.....	279
Separate Session Parameters for an Application Call.....	281
<b>Advanced Security Features</b> .....	<b>283</b>
Ticketing.....	285
User Tickets for the Web Interface.....	287
Access Privileges for Client Drives.....	289
Extended Access Privileges for Client Drives.....	289
Setting up Access Privileges for Client Drives.....	290
Using NetMan Actions to Modify Access in Client Drives.....	292
<b>Printing with NetMan Desktop Manager</b> .....	<b>293</b>
Overview.....	295
RDP Support for Local Printers.....	297
Modifying Printer Mapping.....	299
Universal Printer Driver in Windows Server 2003 SP1.....	301
Terminal Services Easy Print in Windows Server 2008.....	303
Universal PDF Printer Driver.....	305
Switching the PDF Print Preview On and Off.....	307
Showing or Hiding the Universal PDF Printer Driver.....	309
Bandwidth Management for the Universal PDF Printer Driver.....	311
<b>Additional Tips for Operation in Terminal Server Environments</b> .....	<b>313</b>
Defining the Maximum Number of Parallel Sessions.....	315
Station Names in the Terminal Server Environment.....	317

Granting Access Privileges in Client Drives .....	319
Problems Launching NetMan.....	321
Troubleshooting Application Problems.....	323
Citrix Anonymous Users in Domains.....	325
Monitored Processes for Application Sessions .....	327
<b>NetMan Internet Filter</b> .....	<b>329</b>
<hr/>	
Using the NetMan Internet Filter .....	331
Switching the NetMan Internet Filter On and Off .....	333
Editor for Internet Filter Files .....	335
Global Internet Filter .....	337
Creating Rules for Filtering URLs .....	339
Creating Rules for Filtering Processes .....	343
Testing an Internet Filter File.....	345
<b>Statistics</b> .....	<b>347</b>
<hr/>	
Statistical Analysis of Log Files.....	349
Statistical Analysis with the NetMan Statistics Program .....	351
Tables.....	353
Main Table .....	353
Table of Concurrent Use.....	355
Example .....	357
Analyzing Data with the NetMan Statistics Program .....	357
<b>Appendix</b> .....	<b>367</b>
<hr/>	
Glossary .....	369
Index .....	375





## Introduction





# Contents of This Manual

This chapter provides a general introduction to the operation and functioning of NetMan Desktop Manager and takes a brief look at the basic components, performance features and system requirements.

“**Installation**” describes the installation procedure step by step and illustrates the various installation options.

“**The First Steps with NetMan Desktop Manager**” shows you how the interface looks to users and administrators immediately following installation.

“**The First Steps with the Web Interface**” explains how to login on the web interface and use it to call applications.

“**Examples for Integrating Terminal Servers**” shows two ways to integrate NetMan Desktop Manager in combination with terminal servers: with fat clients (Windows PCs) and with thin clients.

“**System Structure**” takes a closer look at the components of NetMan Desktop Manager and how they interact. This provides a basis for understanding how NetMan Desktop Manager works.

“**NetMan Desktop Manager Programs**” describes all management and configuration programs available to the administrator through the NetMan Desktop Manager Toolbox.

“**Integrating Applications and Hyperlinks**” gives an introduction to the use of NetMan Desktop Manager’s Management Console.

“**Resources in NetMan Desktop Manager**” details the functions available for administration of users, user groups, user profiles, stations, station groups and station profiles in NetMan Desktop Manager. This chapter shows how you can use these resources as control elements in your NetMan Desktop Manager system.

“**Web Interface**” describes the components and functions of NetMan Desktop Manager’s web interface, from the basic configuration of launch methods to the **NetMan SSL Gateway** software.

“**Opening Sessions over NetMan Desktop Client**” provides detailed descriptions of the web services in NetMan Desktop Manager. These web services determine, for example, how users are authenticated on a terminal server, and which server is used when a session is opened.

“**Enhancements for Terminal Servers**” describes functional enhancements that have been added specifically for terminal servers.

“**Enhancements for MetaFrame Servers**” describes functional enhancements specifically for MetaFrame servers.

“**Special Features for Application Settings**” shows how you can modify settings for particular applications.

“**Advanced Security Features**” explains the functions that have been added for improved terminal server security.

**“Printers in NetMan Desktop Manager”** presents the options available for printing on local workstations. In addition to the options provided by Windows Server 2003 and Windows Server 2008, a universal PDF printer driver is described here in detail.

**“Notes on Working in Terminal Server Environments”** contains additional tips and comments on the operation of NetMan Desktop Manager in terminal server environments.

**“The NetMan Internet Filter”** describes how you can use NetMan’s filter mechanisms to control client access to HTML documents in intranets and the Internet.

**“Statistics”** acquaints you with NetMan’s statistical evaluation functions.

# NetMan Desktop Manager: The Basics

NetMan Desktop Manager is a highly efficient application management tool that makes it easy to serve applications to clients in Windows 2003 or Windows 2008 Terminal Server environments. The NetMan Desktop Manager system also facilitates operation for users and administrators alike and enables fast and easy application rollout. With its comprehensive statistics functions and integrated license management features, NetMan Desktop Manager helps you plan all your software investments carefully. Furthermore, it improves terminal server security, helps protect against system misuse and provides a universal PDF printer driver.

The advantages of terminal server technology, also called server based computing or SBC, are known worldwide today thanks to widespread practical use as well as a large number of specialized publications. One of the main advantages of terminal server technology is the reduction in total cost of ownership (TCO). This is made possible in part by the low administrative costs thanks to centralized application management, as well as relatively inexpensive terminals (thin clients) and reduced energy expenses.

When we designed NetMan, we implemented functionalities that will help to optimize your total costs of terminal server operation, eliminate many of the difficulties and flaws often encountered with terminal servers, and integrate new features.

NetMan Desktop Manager focuses on 5 main areas to transform Windows Server 2003 Terminal Server into a powerful application server:

- Individual and flexible application serving
- Simplified application rollout
- High degree of user comfort
- Comprehensive monitoring and reporting features
- Functional enhancements for better security

With all of these goals at the forefront NetMan Desktop Manager gives you a set of indispensable tools that lighten your administrative load while at the same time protecting your terminal server environment from attack. Moreover, a range of real-time monitors supports you in troubleshooting and enables optimum support for your users as well by providing comprehensive help-desk functions. Even technologically complex functions such as integrated 2-factor-authentication and the SSL gateway can be configured in NetMan Desktop Manager with just a few mouse clicks, making administration a breeze.

Benefits for your network users include NetMan Desktop Manager's invisible integration of terminal server applications in your local system. Seamless windows, single sign-on and content redirection all work together to ensure that users won't have to change their accustomed working procedures.

Thanks to individual application serving, users can access the applications they need (and for which they have access privileges) in their own Start menu, desktop, or web interface.

NetMan Desktop Manager takes all of these capabilities one step further: You can control many aspects of application execution or usage by adding parameters, in the form of "NetMan actions," that are applied based on application, user or access source. For

example, you can configure actions that block access to local drives, limit printer bandwidth, or any of a broad range of other mechanisms. These predefined actions can be added to applications at the click of a mouse, and then linked to conditions that determine whether or not they are executed. In the same manner, you can link scripts or batch files to application calls.

The administrative workload is further eased by the integrated PDF printer driver. This precludes the need to install drivers on the terminal server for locally connected printers.

In addition to all these advantages for reducing administrative costs and improving efficiency of hardware use, the integrated license management feature in NetMan Desktop Manager not only helps prevent software license violations, it also enables comprehensive analysis of the use of your applications. This makes it easy to stay within legal limits while achieving the most economical software licensing for your organization's requirements.

The statistics program can show you how often and how long your applications are used, when a given application is in use in multiple instances (parallel use), how often and how long users wait in a queue for a licensed application (because all licenses were already in use), and how often users cancel application calls rather than wait for a license to become available. This data can form the basis of your organizational and logistical decisions, by answering questions such as:

- Do you have more licenses than you need for a given application? Do you have too few licenses for another?
- Which stations and which users call which applications?
- Does the use of a given application justify the cost of its acquisition? How can you best distribute operating costs for the application within your budget?

You can configure licensing and statistical data acquisition features for each application separately if desired.

On the subject of lowered TCO, the use of anonymous published applications should not be overlooked. This is a mechanism that can serve applications to an unlimited number of users without additional administrative work. The drawback, however, is that you give up control over server access: anyone who can reach the terminal server over a network can also access it. Here, too, NetMan gives you additional control features. For example, you can permit or deny server access, or limit the client to certain applications, entirely on the basis of client IP address.

NetMan Desktop Manager eliminates another weak point in terminal servers with its RDP ticketing technique. Every RDP file is automatically provided with an encrypted time stamp and is only valid for the period of time defined by the NetMan administrator. If the file's validity has expired, it cannot launch a session. This prevents the use of manipulated RDP files for access to your terminal servers.

You can use NetMan Desktop Manager in a variety of environments:

- As an application management system for Microsoft Windows Server 2003 Terminal Server
- As an application management system for Microsoft Windows Server 2008 with Terminal Services role

- As an application management system for Microsoft Windows Server 2008 R2 with Remote Desktop Services role
- As an add-on for Citrix MetaFrame or Presentation Server
- In mixed environments, in combination with terminal servers and Citrix servers

In developing the NetMan Desktop Manager software suite, we have always insisted on ease of operation for administrators and users alike. NetMan's intuitive interface lets you configure even complex functions with just a few mouse clicks. Moreover, after a brief learning phase you will be able to create and manage extensive application portfolios and user structures with NetMan Desktop Manager.

---

**NOTE** Throughout this manual, "NetMan Desktop Manager" is often referred to simply as "NetMan," and its web interface as "HTML View."

**NOTE** Terminal servers have gone through various stages in the course of their development. One result has been that each edition has its own name for terminal services. In the context of Windows Server 2003, for example, terminal servers have "functionalities," while Windows 2008 servers have "a Terminal Services role." In Windows Server 2008 R2, the term is "Remote Desktop Services" (RDS). NetMan Desktop Manager supports all of these platforms, but for purposes of simplification, this manual often refers to each of these simply as terminal servers.

---



# Performance Features

NetMan Desktop Manager's powerful performance features are described in detail in the following:

- **Published applications:** In a pure terminal server environment, the administrator has to create shortcuts to individual applications manually on user desktops. With NetMan Desktop Manager, all the user needs to know is the name of the application in order to launch it; no indication is given of which terminal server the applications are actually installed on.
- **Seamless windows:** NetMan Desktop Manager's "Seamless Windows" mode ensures that all applications are displayed exactly the way users are accustomed to seeing locally installed applications. Applications running on the terminal server appear without an additional window frame in the terminal server session. The application window can be maximized, minimized, resized and moved in the usual way.
- **Application-based load balancing:** NetMan Desktop Manager lets you define the proportion of the load to be carried by each server individually. When an application is called, your load distribution settings determine which server it runs on. You can also define whether the load is distributed according to number of sessions or based on CPU load and memory utilization. This is one example of how NetMan Desktop Manager makes administration easy while optimizing the use of server resources.
- **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.
- **Universal Print Driver:** NetMan Desktop Manager supports a generic printer driver concept using the portable document format (PDF). Print jobs generated by the user in a terminal server session are converted to the PDF format and sent to the requesting station, where they can be printed using a PDF viewer such as Acrobat Reader or Foxit Reader. Thus all of the options offered by the local printer (print quality, paper format, etc.) are also available in the session. Alternatively, documents can be sent directly to the local default printer without a preview.
- **Web interface for starting applications:** With the new integrated web interface for starting applications, you can open applications and even terminal server desktops in a web browser. All common browsers and operating systems are supported, including Internet Explorer, Firefox, Opera, and others. The only prerequisite on Windows clients (Windows 98, NT, 2000, XP, XP Embedded, Server 2003, Server 2008, Server 2008 R2, or Windows 7) is the installation of a small client component. On other operating systems, such as Mac OS X or Linux, the terminal servers are accessed using a Java applet.
- **Content redirection:** With this mechanism, all it takes is a double-click on a file to open that file with the associated application. For example, if you run Microsoft Excel on a terminal server, double-clicking on an Excel spreadsheet will open that spreadsheet with Excel in a terminal server session.

- **NetMan SSL Gateway:** This software component of the NetMan Desktop Manager ensures that remote access of your terminal server is always secure. The gateway software is installed either in your network or on a separate server in the DMZ. It provides access to your applications through the web interface and encrypts RDP data traffic over SSL.

## Management and Usability

- **Pass-through authentication/single sign-on:** In a plain terminal server environment without NetMan Desktop Manager, even after users have logged on to the network additional authentication is required each time they open a terminal server session. With NetMan Desktop Manager, no second authentication is required: once a user logs on to the network, the same credentials are used for authentication on the terminal server. This applies for remote access as well: once the user logs on in the web interface, the same login data is used automatically for all sessions.
- **Processes independent of environment and users:** In the NetMan Desktop Manager system, calling an application can be much more than simply running an executable program (or starting a CD, or pointing a browser to a URL). You can configure any number of other processes, termed “NetMan actions,” to execute as well, before or after the program itself runs (or the CD starts, or the browser begins navigation). Here are just a few examples:
  - Check the environment properties and resources and provide anything required that is not found
  - Allocate network paths
  - Map drives
- **Uniform, centralized administration of all types of applications and hyperlinks:** NetMan Desktop Manager expands the term “application” to encompass all types of Windows-based and HTML-based resources. This provides for uniform management of the CD/DVD applications and web content frequently found in enterprises alongside application programs. Both the administration in NetMan Desktop Manager and the mechanisms for serving resources to client workstations are the same, regardless of the type of application.
- **Station-specific application roll-out:** With NetMan Desktop Manager, you can publish your applications not only for specific users and user groups, but also for stations and station groups. Station-specific application publishing is a major advantage for kiosk systems, for example, as well as for any other scenario in which stations may be shared but always enable the same set of tasks.

## Monitoring and Reporting

- **Server and Station monitor:** The server and station monitor shows all the workstations that are logged in, including computer name, active user, IP address, operating system and current activities. It also shows which users are logged in on which terminal servers, as well as the current usage of terminal server resources.
- **Log monitor:** The log monitor clearly lists all user activity, with time stamps, and makes this data available for analysis using NetMan’s extensive statistics functions.

- **Trace monitor:** All processes initiated by NetMan Desktop Manager's server components can be viewed by administrators in real time using the trace monitor, which can speed up the troubleshooting process. Furthermore, messages from NetMan Desktop clients can be analyzed for a complete overview of input and output on local workstations as well. The displayed events can be filtered by class or other criteria, to give you essential information at a glance and rapidly eliminate possible error sources.
- **License management:** NetMan Desktop Manager integrates a comprehensive license management tool for use with all of the common licensing schemes, including "node-locked" licenses (e.g., by user; by seat) and "floating" licenses (also called "concurrent use" licensing).
- **License queue:** If no license is available when a user attempts to launch a particular application (in concurrent-use licensing, for example), the user can wait in a license queue. In this case, NetMan Desktop Manager automatically opens the application for that user the moment a license becomes available. By automatically monitoring the status and use of application licenses in your network, NetMan Desktop Manager can make sure software licensing agreements are not violated.
- **Detailed usage statistics:** The data collected in the NetMan Desktop Manager's log files permits detailed analyses of all user activities, using a uniform format for all types of application data. As long as the application is managed by NetMan Desktop Manager, the application data can be logged and analyzed by NetMan programs regardless of where it is stored—whether on the terminal server, in a server farm, on the local workstation or on the Web. In addition to details such as start times and duration of usage, information on licenses used and time spent in license queues can be collected and analyzed as well. With these detailed evaluations, NetMan Desktop Manager can help make sure you don't purchase more software licenses than you need.

## Improved Security

- **RDP ticketing:** When a terminal server session is requested, the RDP file that is sent can be opened using any common editor. Unlike the Microsoft approach, with RDP files that are valid for an unlimited period of time, NetMan Desktop Manager limits the period of validity of its RDP files. If a user tries to send an RDP file that has expired, whether original or modified, access to the terminal server is blocked. This way, even expert users are prevented from manipulating RDP files for unauthorized logon.
- **Protecting login data:** SSL encryption protects the login data entered by your end-users in the web interface. For even better security, the data is not sent back to the client after the session has been opened. Ticketed user accounts that can log in on a terminal server only once are used for authentication to open the session. The session itself then uses same login data that the user entered in HTML View.
- **Client drive management:** Microsoft's Terminal Server technology provides access to local drives, but does not include an option for allocating access privileges to the drive's content (folders or applications). Here again NetMan implements its sophisticated security techniques to enhance terminal server functionality, this time by adding an option for allocating access privileges to local drives or USB ports. For example, you can effectively prevent the introduction of undesired applications into the network by permitting access only in folders authorized by the administrator, in locally connected drives or in USB ports.

- **SSL tunnel for RDP:** The NetMan SSL gateway is a web-based interface for calling applications. Following authentication, RDP sessions can be opened using NetMan's web interface. These sessions are encrypted over SSL to protect the RDP connections from spying, and no additional VPN infrastructure is needed. SSL-protected sessions can be operated over proxies.
- **2-factor authentication:** The 2-factor authentication feature provides additional protection from unauthorized access using the web interface. For example, your web interface users can access the Internet only if they enter a valid OTP token. All RADIUS-compatible token systems are supported.

# Desktop Sessions and Application Sessions

In the context of NetMan Desktop Manager, we frequently use the terms “desktop session” and “application session.” Detailed definitions of these terms are provided below; both refer to terminal server sessions or MetaFrame sessions:

- If the entire Windows interface is shown, including Start menu and task bar, we speak of a desktop session in this manual.
- If the session window contains only the window of one or more Windows applications, on the other hand, the session is referred to as an application session.



## Sessions in the Windows Interface and in the Web Interface

With the powerful performance features of NetMan Desktop Manager, terminal server sessions can be opened not only by a Windows client but also using a web interface. For the most part, the functions provided by NetMan in terminal server sessions are the same in both scenarios. There are a few differences in certain details, however. The table below shows which scenarios offers which functions.

Function	NetMan Desktop Client (or RDP client)	NetMan RDP web client	Java RDP web client	Rdesktop using Java applet
Sound support	Yes	Yes	Yes	Yes
Local drives	Yes	Yes	Yes	Yes
Content redirection	Yes	No	No	No
Seamless windows	Yes	Yes	Yes	No
Universal printer driver	Yes	Yes	Yes	No
Load balancing for applications	Yes	Yes	Yes	Yes
Published applications	Yes	Yes	Yes	Yes
SSL tunnel for client	No ("yes" for RDP sessions)	Yes	Yes	No
Single sign-on	Yes	Yes (one-time login on web interface)	Yes (one-time login on web interface)	Yes (one-time login on web interface)
Seamless application integration in Windows desktop	Yes	No (called from web interface)	No (called from web interface)	No (called from web interface)
Call a locally installed application	Yes	No	No	No
Session sharing	Yes	Yes	Yes	No
2-factor authentication	No	Yes	Yes	Yes
Supported operating systems	Windows 2000/Windows XP/Windows Vista/Windows Server 2003/R2/Windows Server 2008/R2	Windows 98/Windows NT 4.0/Windows 2000/Windows XP/Windows Vista/Windows Server 2003/R2/Windows Server 2008/R2	All operating systems with Java Runtime 1.5/1.6	All operating systems with Java Runtime + rdesktop 1.5.0/1.6.0 rdesktop is required
Installation required	Yes	Yes	No	





Installation





# System Requirements

NetMan Desktop Manager has two main components:

- NetMan Desktop Manager server
- NetMan Desktop client

A third component handles access to the NetMan Desktop Manager web interface:

- NetMan SSL Gateway

NetMan Desktop Manager 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 or**
- **Windows Server 2003 (32-bit or 64-bit) or**
- **Windows Server 2003 R2 (32-bit or 64-bit) or**
- **Windows Server 2008 (32-bit or 64-bit) or**
- **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.

---

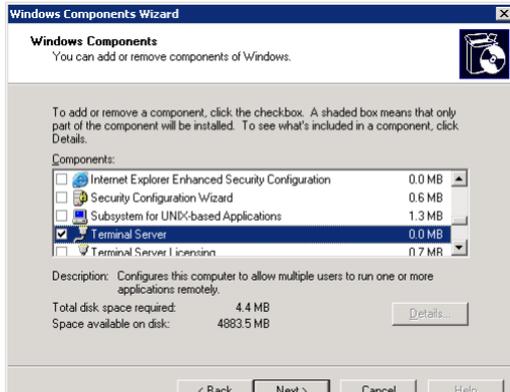
**NOTE** A license number must be entered during installation, whether a restricted (temporary) license code downloaded from the Internet for testing purposes, or the full license you received with your purchase of NetMan Desktop Manager.

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

---

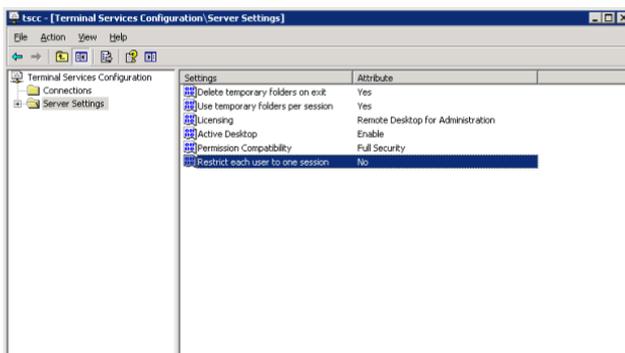
# System Requirements for Windows Server 2003 Terminal Server

Before you install NetMan Desktop Client on Windows Server 2003, terminal services have to be installed and configured on the server. To do this, select “Add/Remove Programs” from the **Control Panel** and click on **Add/Remove Windows Components**.



Select **Terminal Server** in the Windows Components Wizard dialog. We recommend deactivating the **Internet Explorer Enhanced Security Configuration** so that all users can run the Internet Explorer in same manner as on a workstation. The **Terminal Server Licensing** should be installed and activated on one server in your network, so that TS client access licenses (TS CALs) are available to all servers.

Change the default settings in the server configuration to permit users to open multiple server sessions. To do this, open **Start/Administrative Tools/Terminal Services** and select **Terminal Services Configuration**.



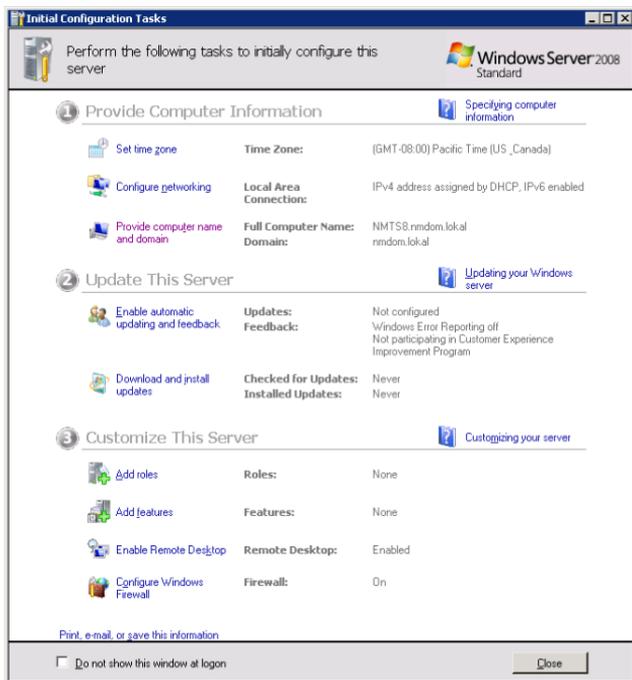
Set the **Restrict each user to one session** option to **No**. This completes the configuration required for operation of NetMan Desktop Manager.



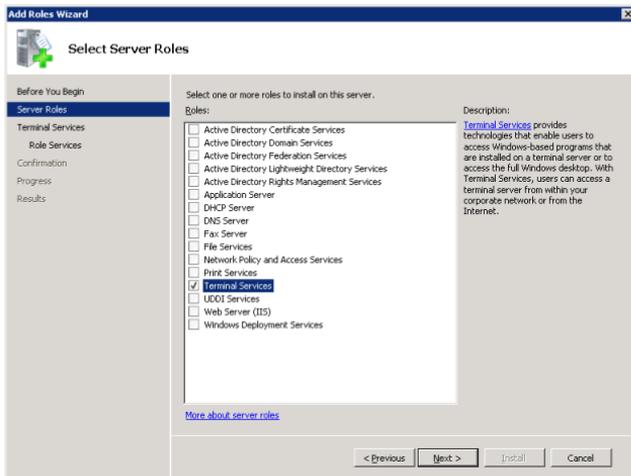
# System Requirements for Windows Server 2008 with Terminal Services Role

Before you install NetMan Desktop Client on a terminal server running Windows Server 2008, the “Terminal Services” role must be installed and configured on that server.

The **Initial Configuration Tasks** dialog opens automatically following installation of the server. Select **Add roles** in section 3.

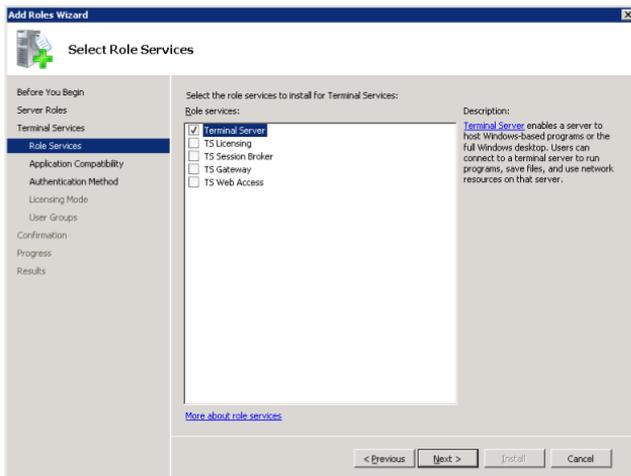


Select the “Terminal Services” role and click on **Next**.

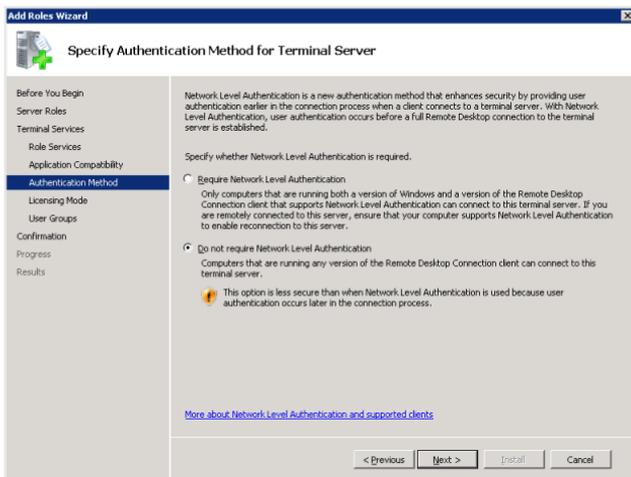


**Terminal Server** is the only role required.

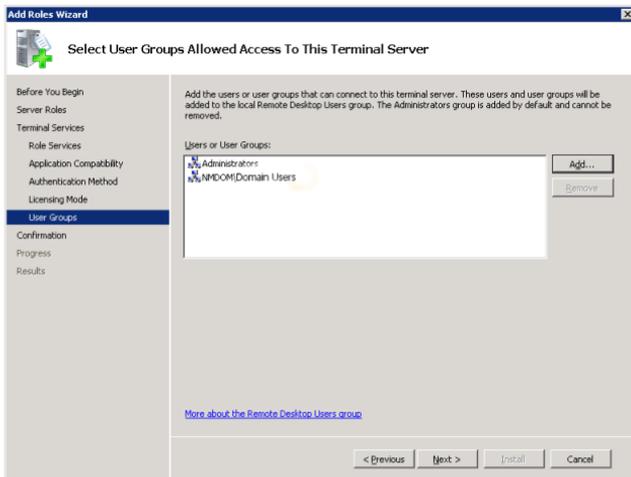
None of the other roles (**TS Session Broker**, **TS Gateway** and **TS Web Access**) are required for operating NetMan Desktop Manager. The **TS Licensing** role should be installed on one server in your network, so that TS client access licenses (TS CALs) are available to all servers.



In the “Add Roles” wizard, select **Authentication Method** and activate the **Do not require Network Level Authentication** setting. Otherwise, clients that support only RDP 5.x will be unable to access NetMan.

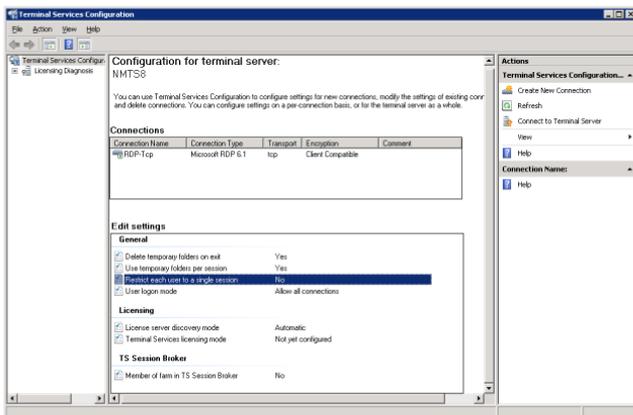


Then select “Licensing Mode” to configure licensing, and “User Groups” to specify which users can access terminal services. With the default settings, only **Administrators** have this access. You need to add a group that includes all users to whom you wish to permit terminal server access. For example, to grant access to all users in the domain, add **<domain>\Domains Users**.



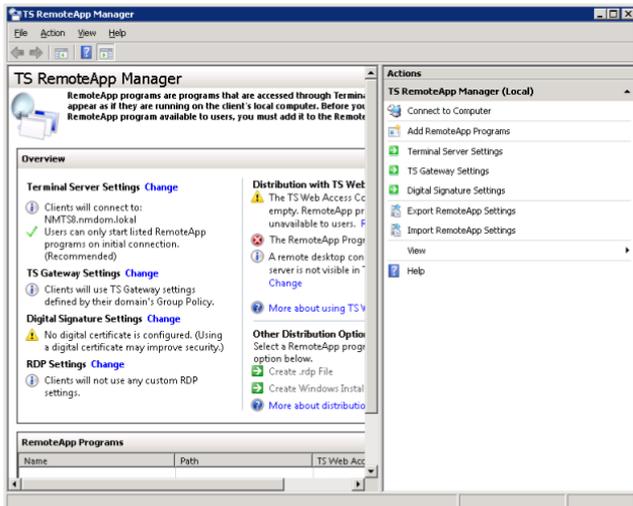
Following successful installation, configure the terminal services for operation in NetMan Desktop Manager as follows:

Change the default settings in the server configuration to permit users to open multiple server sessions. To do this, open **Start/Administrative Tools/Terminal Services** and select **Terminal Services Configuration**.

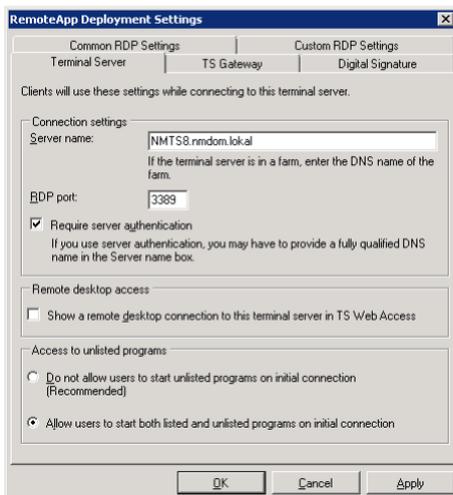


Set the Restrict each user to one session option to No.

The next step is to configure **Terminal Services RemoteApp Manager** to permit user access to unlisted programs. To do this, open **Start/Administrative Tools/Terminal Services** and select **TS RemoteApp Manager**.



In the RemoteApp Manager dialog, select **Terminal Server Settings**. Under **Access to unlisted programs**, activate the “Allow users to start both listed and unlisted programs on initial connection” option.



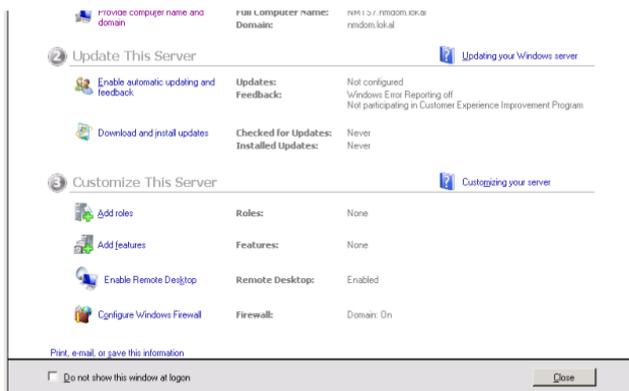
This completes the configuration required for operation of NetMan Desktop Manager.



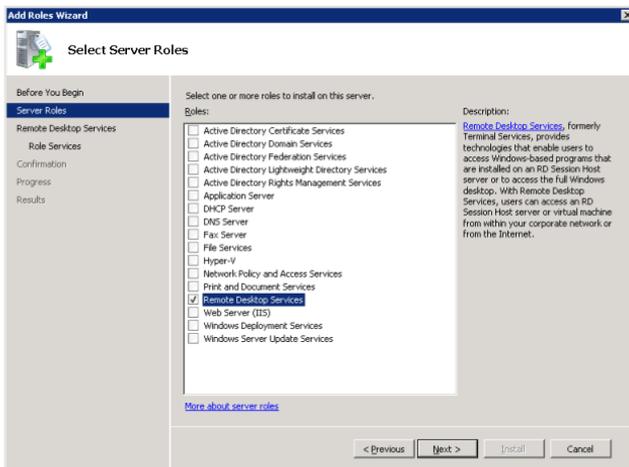
# System Requirements for Windows Server 2008 R2 with Remote Desktop Services Role

Before you install NetMan Desktop Client on a terminal server running Windows Server 2008 R2, the “Remote Desktop Services” role must be installed and configured on that server.

The **Initial Configuration Tasks** dialog opens automatically following installation of the server. Select **Add roles** in section 3.

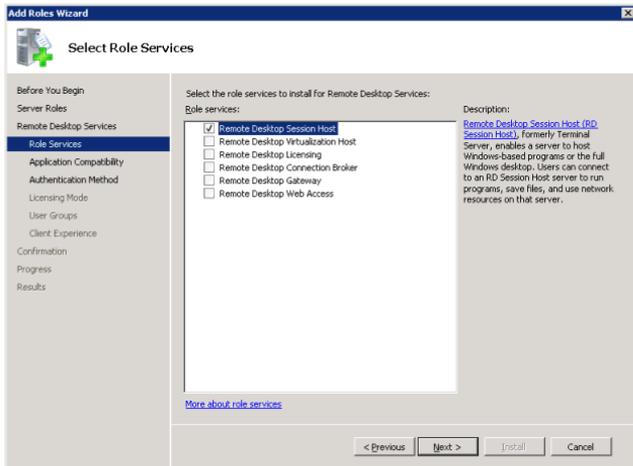


Select the “Terminal Services” role and click on **Next**.

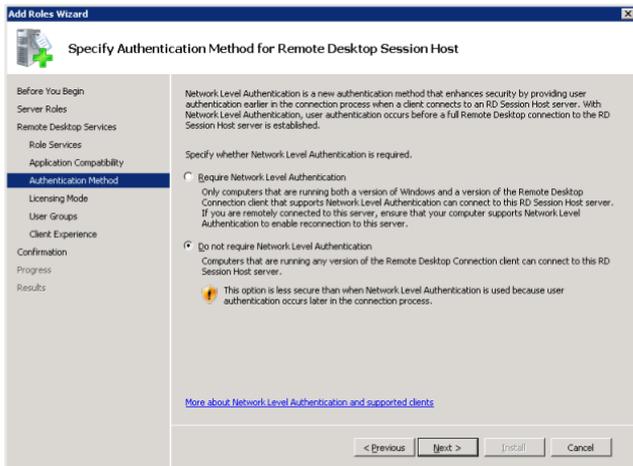


Remote Desktop Session Host is the only role required. None of the other roles (Remote Desktop Virtualization Host, Remote Desktop Connection Broker, Remote Desktop Gate-

way, Remote Desktop Web Access) are required for operating NetMan Desktop Manager. The Remote Desktop Licensing role should be installed on one server in your network, so that RDS client access licenses (RDS CALs) are available to the Remote Desktop servers.

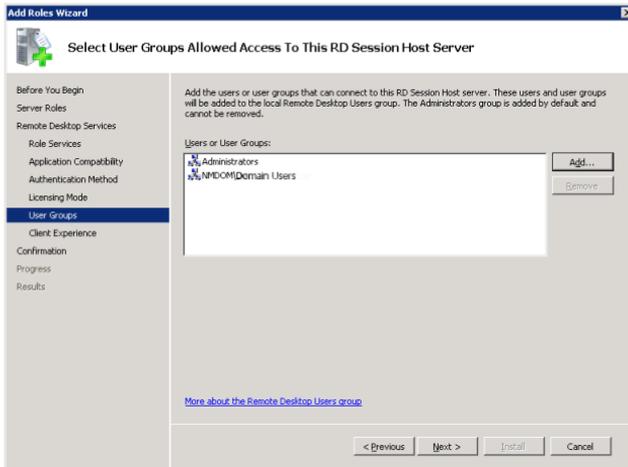


In the “Add Roles” wizard, select **Authentication Method** and activate the **Do not require Network Level Authentication** setting. Otherwise, clients that support only RDP 5.x will be unable to access NetMan.



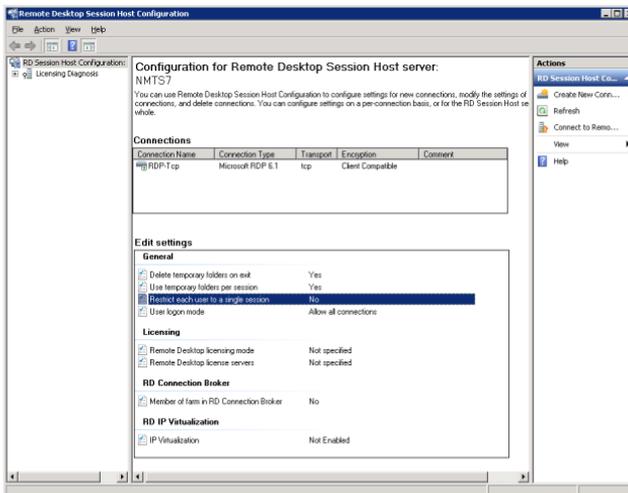
Then select “Licensing Mode” to configure licensing, and “User Groups” to specify which users can access terminal services. With the default settings, only **Administrators** have

this access. You need to add a group that includes all users to whom you wish to permit terminal server access. For example, to grant access to all users in the domain, add **<domain>\Domain Users**.



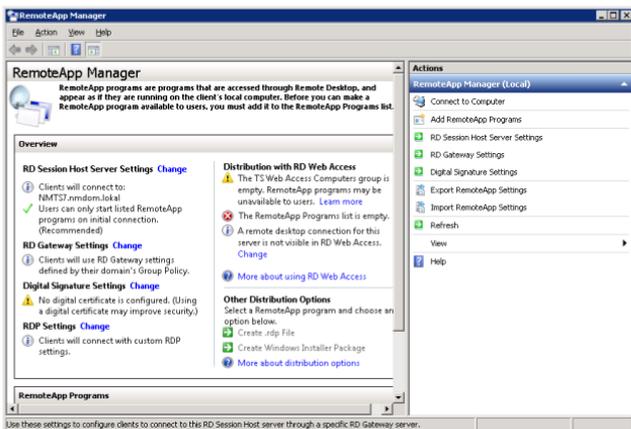
Following successful installation, configure the terminal services for operation in NetMan Desktop Manager as follows:

Change the default settings in the server configuration to permit users to open multiple server sessions. To do this, open **Start/Administrative Tools/Remote Desktop Services** and select **Remote Desktop Session Host Configuration**.

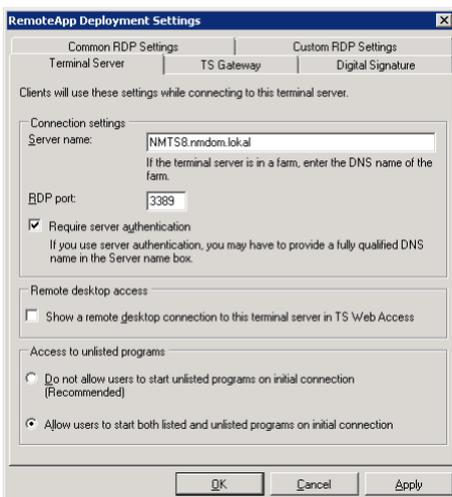


Set the Restrict each user to one session option to No.

The next step is to configure Remote Desktop Services to permit user access to unlisted programs. To do this, open **Start/Administrative Tools/Remote Desktop Services** and select **RemoteApp Manager**.



In the **RemoteApp Manager** dialog, select **RD Session Host Server Settings**. Under **Access to unlisted programs**, activate the "Allow users to start both listed and unlisted programs on initial connection" option:



This completes the configuration required for operation of NetMan Desktop Manager.

# Installation Principles

## Overview

There are two ways to install NetMan Desktop Manager:

- On a terminal server
- On a file server, for operation on multiple terminal servers

After installing the NetMan Desktop Manager server components, install NetMan Desktop Client on your workstations and on other terminal servers as needed:

- For operation with one terminal server, install NetMan Desktop Client on all workstations that will be using NetMan Desktop Manager.
- For operation with multiple terminal servers, install NetMan Desktop Client on all terminal servers as well.
- For operation with thin clients, install NetMan Desktop Client on the terminal server. Thin clients run NetMan Desktop Manager on the server in desktop sessions.

---

**NOTE** If you use MetaFrame in your system, install NetMan Desktop Client on your MetaFrame servers as well.

---

When you insert the NetMan CD, a dialog opens prompting you to select a language. Afterwards, you are presented with the following options:

- Install NetMan Desktop Manager
- Open the NetMan Desktop Manager manual (PDF)



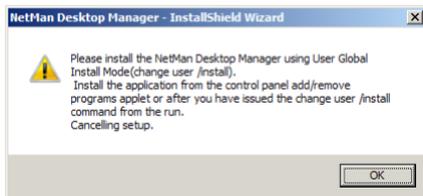
## Installing NetMan Desktop Manager on a Terminal Server

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

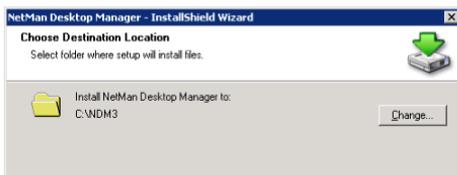
Run the setup program on the console of the terminal server on which you wish to operate NetMan Desktop Manager. You can execute the setup in a terminal server session if desired.

### NOTE

With Windows Server 2008 or Windows Server 2008 R2, setup is automatically canceled if the server is not in installation mode, and the InstallShield wizard shows the following message:



After you accept the licensing conditions, you are prompted to specify the destination path:



Both the NetMan Desktop Manager installation directory (the destination defined here) and the directories containing NetMan web services must be shared for administrative purposes. The names assigned to these shares by default are as follows:

- NetMan
- HHWebPath

With the default settings, user access in these shares is not restricted. Dialog for naming the NetMan share:



Dialog for naming the NetMan web services share:



Both dialogs contain the recommendation: ***“Please adapt the user privileges for this share to your requirements.”*** Since the reason for sharing these paths is simply to permit administrators to access NetMan databases from any workstation, access privileges are generally required only by administrators.

#### NOTE

During setup, a local group called **NDMAdmin-Local** is created automatically and given administrative rights in the NetMan Desktop Manager files. To give a user or user group NetMan administrative rights, just add it to the **NDMAdmin-Local** group.

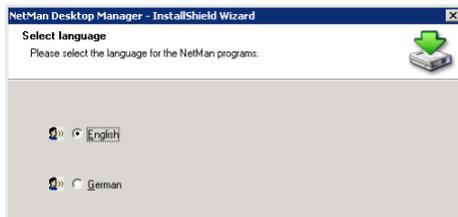
#### NOTE

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

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



Enter your name and the name of your organization. In the next dialog, you are prompted to specify the language in which the product will be installed and operated:



Station monitoring, license control, runtime recording, and serving documents that contain information on available resources for clients are all handled by NT services which are installed automatically. The dialog shown below prompts you to enter data for services and for communication between servers and clients.

The following input is required here:

- **IP address/host name:** IP address or DNS host name of the computer on which NetMan is installed. Clients require this data to establish contact with the NetMan Desktop Manager server.
- **NetMan service port:** Port used by NetMan Desktop Client and the NetMan service to exchange data on license and application usage.
- **NetMan loader port:** Port used for downloading desktop client configuration data from the server.

---

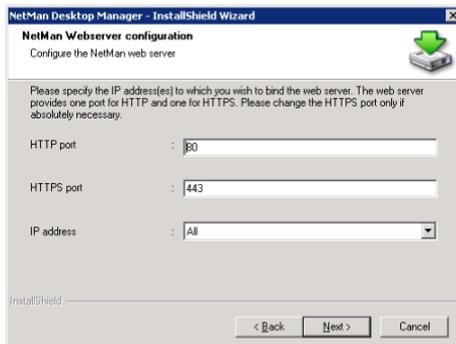
#### NOTE

As a rule, the default settings can be used. Make sure the ports specified here are available on any routers in the data path between NetMan Desktop clients and the NetMan server.

---

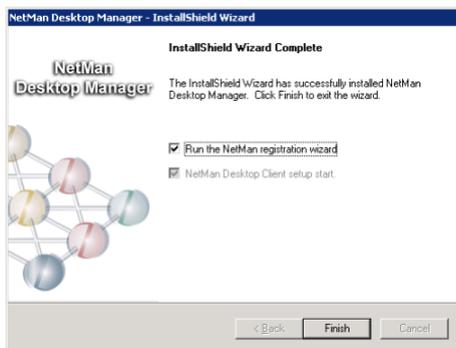
An independent web server is installed for NetMan Desktop Manager's web interface. In the next dialog, you can define the HTTP and HTTPS ports for this server.

If the server has multiple IP addresses, you can define which IP address the web server listens on. With the default settings, the web server listens on all IP addresses.

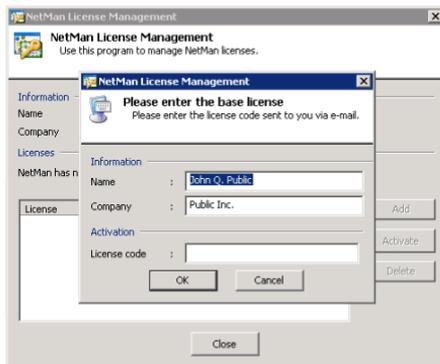


- **HTTP port:** This is the port over which NetMan Desktop Client retrieves its HTML pages, such as the Infoboard and information on applications.
- **HTTPS port:** NetMan Desktop Manager uses this port to serve the web interface for launching applications. This port is also used for output from *NetMan web services*.
- **IP address:** This setting lets you specify which IP address the web server is bound to. With the default settings, the web server listens on all of the server's IP addresses.

Following the installation of all files and the two services, **NetMan Service 3.0** and **NetMan Web Service**, the server installation setup program for NetMan Desktop Manager is closed.



Once you have completed installation of the server components, NetMan License Management starts automatically and prompts you to enter your license code.



If desired, you can change the data you had entered previously under **Name** and **Company**. Then enter your license code. If you obtained a restricted license code, for example, to test the program before purchasing, the license is valid for a limited period of time only. If you enter a code for the fully licensed version, you need to activate your program license after entering it here in order to register your NetMan software. To do this, select the license code and click on **Activate**. Restricted licenses are activated automatically.




---

**NOTE** NetMan Desktop Manager can only be operated if the license code has been activated. If the license code is not active, attempts to run NetMan Desktop Manager programs will fail and the error message depicted above will prompt you to obtain a valid license code.

---

**NetMan Desktop Client** is installed automatically following software registration, enabling operation of NetMan Desktop Manager on the server console, as well as remote operation in a terminal server session. For more detailed information on setting up your NetMan Desktop Client, see "Installing NetMan Desktop Client" in this manual.

---

**NOTE** We recommend installing the universal printer driver after you have installed NetMan Desktop Manager. This driver lets you print PDF files from terminal server sessions.

---

## NetMan Desktop Manager in a Multiple Terminal Server Environment

Running NetMan Desktop Manager in a multiple terminal server environment entails only a few differences in the installation procedure as compared to single-server installation. In this case, the server components are installed on a separate Windows server without terminal services. For example, you might use a file server or domain controller for this purpose. For very large installations with more than 20 terminal servers, we recommend using a separate Windows computer for your NetMan Desktop Manager server.

Installation of server components does not differ from the procedure described above, under "Installing NetMan Desktop Manager on a Terminal Server.." Additionally you need to install NetMan Desktop Client on all terminal servers in the system. This procedure is described in detail in the following two sections.

### Installing NetMan Desktop Client

NetMan Desktop Client installation runs automatically following installation of the server components. The setup program for the client begins by prompting you to enter certain server configuration data:

**NetMan 3 Desktop Client - InstallShield Wizard**

**Define your NetMan server configuration**

Please select the configuration data required for NetMan server components:

Enter the IP address or host name of the server on which your NetMan is installed, and specify the associated port. (In most cases, the defaults can be used.)

IP-address/Hostname : FILESERVER

NetMan service port : 3201

NetMan file loader port : 3200

NetMan Desktop Client service port : 3202

The following input is required here:

- **IP address/host name:** IP address or DNS host name of the computer on which NetMan is installed. Clients require this data to establish contact with the NetMan Desktop Manager server.
- **NetMan service port:** Port used by NetMan Desktop Client and the NetMan service to exchange data on license and application usage.
- **NetMan file loader port:** Port used for downloading desktop client configuration data from the server.
- **NetMan Desktop Client Service Port:** Port used for communication between Desktop Client and the client service.

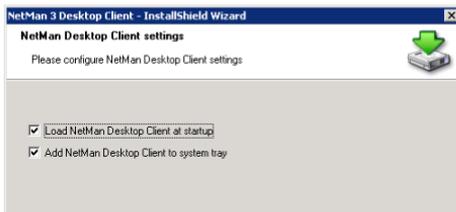
---

#### NOTE

These settings correspond to those entered during server setup. These ports should be changed only if the default ports are already in use on your server.

---

The next dialog lets you define whether NetMan Desktop Client starts automatically and whether an icon is shown on the task bar:

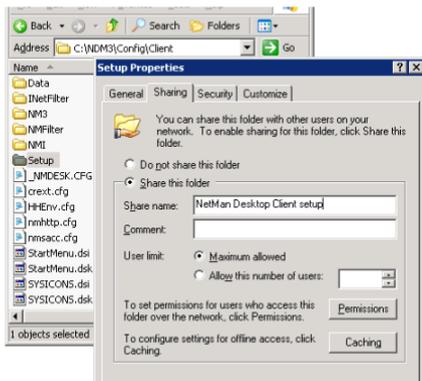


If the Client Setup program is running on a terminal server, the next dialog prompts you to specify whether the **universal printer support** should be installed.



The **universal printer support** provides a PDF printer driver for the terminal server. This is the last step in installing the client program on the server. The universal printer support mechanism lets you have data written to a PDF file rather than sent to a printer. NetMan Desktop Manager automatically passes the PDF files to the client, whether they can be opened for reading and printing with the Acrobat Reader.

The next step is to install the client on all workstations and, if applicable, on the remaining terminal servers. The NetMan setup program is stored in both the `%NMHome%\Config\Client\Setup\x64` and `%NMHome%\Config\Client\Setup\x86` directories. You can share the `%NMHome%\Config\Client\Setup` directory to distribute the client.



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:



An account with administrator rights must be used to install the Desktop Client.

Once the client has been installed, it will be updated automatically on all workstations any time a newer NetMan Desktop Client version is installed on the NetMan Desktop Manager server. Clients installed on terminal servers, however, are not updated automatically. These installations must be updated individually.

## Distributing NetMan Desktop Client in the Network

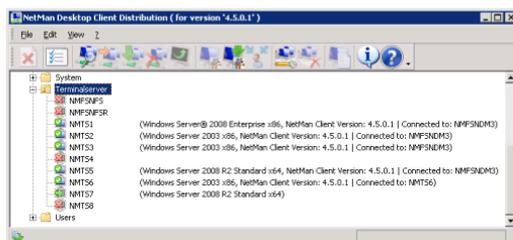
You can choose from a number of methods for distributing NetMan Desktop Client in network environments. The previous section described how the Client can be distributed by using a network share. This is a practical method, at least for small networks, but it does have some disadvantages:

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

The preferred option, particularly in large networks, is to use the **NetMan Desktop Client Distributor** to install the NetMan Desktop Client. To do this, open the **Wizards** folder in the Toolbox and select the distributor program.

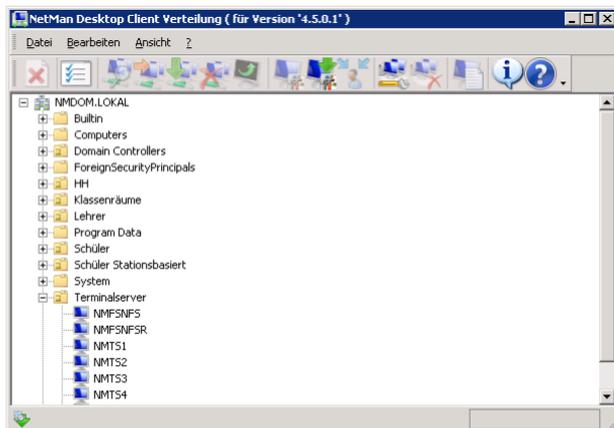


You can use this program to distribute the NetMan Desktop Client in your network.

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.

#### NOTE

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.

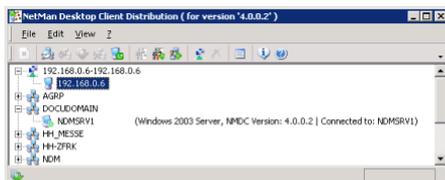
#### NOTE

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 operate in the same manner as for stations listed by name.

## NOTE

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.



## The First Steps with NetMan Desktop Manager





# The First Time an Administrator Runs NetMan Desktop Client

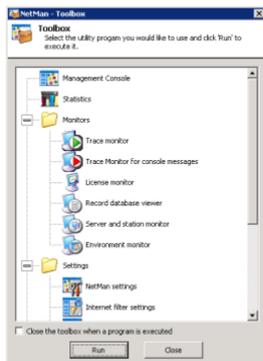
If NetMan Desktop Client does not start automatically following installation, use the shortcut in the Start menu, under **H+H NetMan/NetMan Desktop Client** to run it.



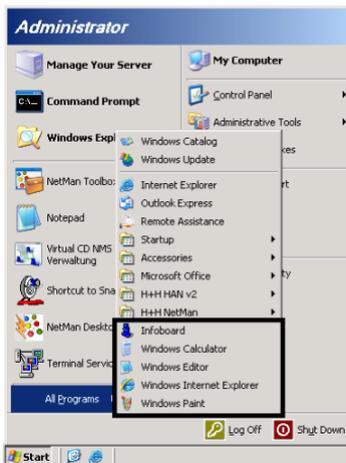
## NOTE

These are normal Start menu items created by the setup program on the console of the NetMan server. All these NetMan programs can be executed without **NetMan Desktop Client**. The **NetMan Desktop Client** link was added by the Desktop Client setup program.

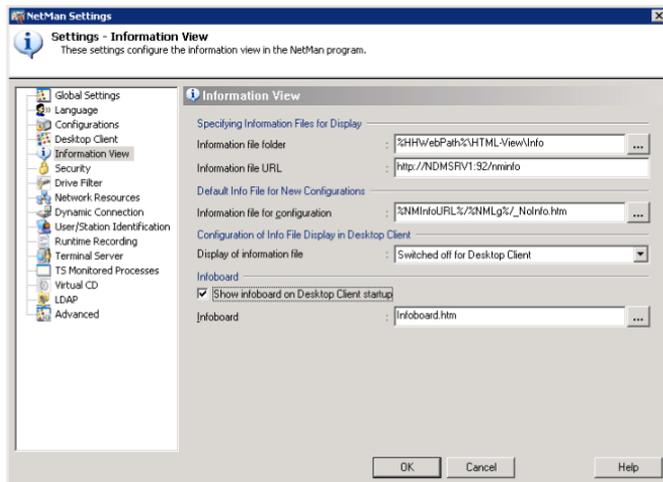
As soon as you run NetMan Desktop Client for the first time, a shortcut to the **NetMan Toolbox**, an interface to administrative utilities, appears on the desktop.



The NetMan Desktop Client installation also adds several examples of NetMan configurations to your Start menu, directly under **All Programs**:



**TIP** With the default settings, the Infoboard runs automatically every time NetMan is opened. The default Infoboard shows information about the NetMan Toolbox and the new items in the Start menu. In the **NetMan Settings** program, you can define whether the Infoboard is shown or not and, if it is, which file it shows:



# Allocation of NetMan Desktops

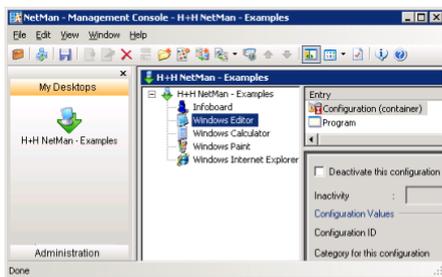
Expressed in NetMan terminology, the following took place when you ran the NetMan Desktop Client for the first time:

- A link to the “NetMan Administration” desktop was added to your desktop.
- The “H+H NetMan – Examples” item was added to your Windows Start menu.

Why this happened and what a NetMan Desktop consists of is described in the following.

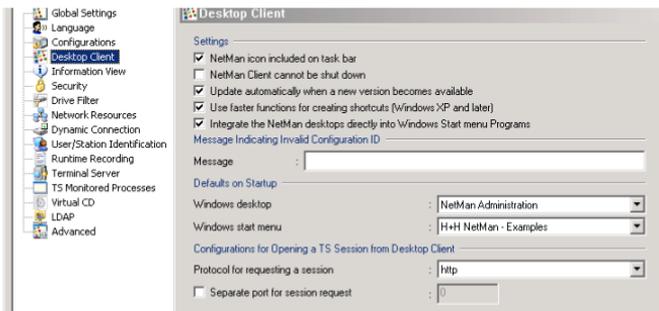
To follow along with the examples given below, run the **NetMan Toolbox** and select **Management Console**. This is the most important configuration program in NetMan administration.

You will find the “NetMan Administration” desktop in the sidebar under **Administration** and the “H+H NetMan – Examples” desktop under **My Desktops**. In the example below, the “Examples” desktop is open:



A NetMan Desktop can contain your choice of Windows applications as well as hyperlinks in a structured arrangement. You can define how your users access a NetMan desktop. By default, the “NetMan Administration” desktop is accessed through a shortcut on the Windows desktop, and the desktop containing examples (“H+H NetMan - Examples”) is accessed through the Start menu.

These features are configured in the **NetMan Settings** program. Expand the “Settings” node in the NetMan Toolbox, open **NetMan Settings**, and select the **Desktop Client** page:



On this dialog page you can specify default settings that determine which desktop is available in the Windows Start menu and which on the desktop when NetMan runs. These settings can be overwritten by settings for the following:

- User profiles
- User accounts
- Station profiles

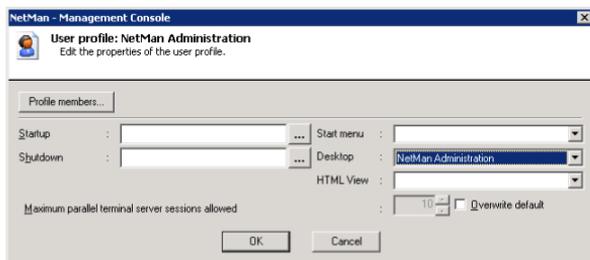
---

## NOTE

Global settings are overwritten by settings for user profiles, while profile settings are overwritten by settings for individual users. Settings for a station profile overwrite all of the above.

---

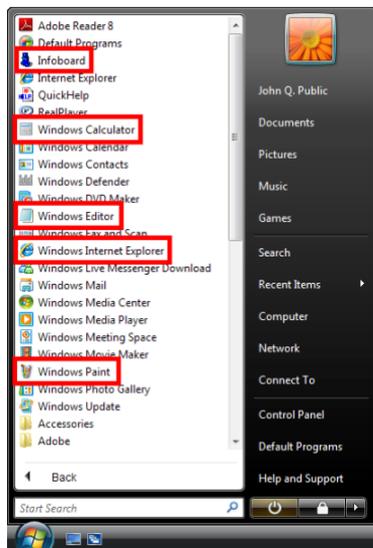
Thus for example you can have **no** desktop added to the Windows desktop by default, and then create a user profile for NetMan administrators that has the “NetMan Administration” desktop in the Start menu:



As seen in this example, only members of the **NetMan Administration** profile have access to the NetMan Administration desktop.

## The First Time a User Runs NetMan Desktop Client

Once you have installed NetMan Desktop Client on your client workstations, users can access the applications published by NetMan Desktop Manager. If you have not explicitly configured other settings for your users, the applications in **H+H NetMan - Examples** are found in the user's Start menu.



With the default settings, these are listed directly under “All Programs.” To move these shortcuts to a folder, open the **Desktop Client** page of the NetMan Settings program and deselect the option to have the desktops integrated directly in “All Programs.”

The user can call these applications like any other program in the Start menu. The **Windows Editor** and **Calculator** programs were chosen for use as examples because their program files are generally found on all Windows computers.

If a user calls the **Windows Editor** program, for example, an application session is opened and the **Editor** runs on a terminal server. Immediately following installation, user authentication is required before the session opens. You can adapt this feature to suit your requirements (see Login Methods on Terminal Servers for details).





## First Steps with the Web Interface





## Advantages of the Web Interface

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.



## 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:




---

**NOTE** This indicates the use of SSL encryption for a secure connection. Upon installation, NetMan Desktop Manager 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.

---

**NOTE** The automatic re-routing described above will function correctly only if you accepted the default port numbers when installing NetMan Desktop Manager. 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>
```

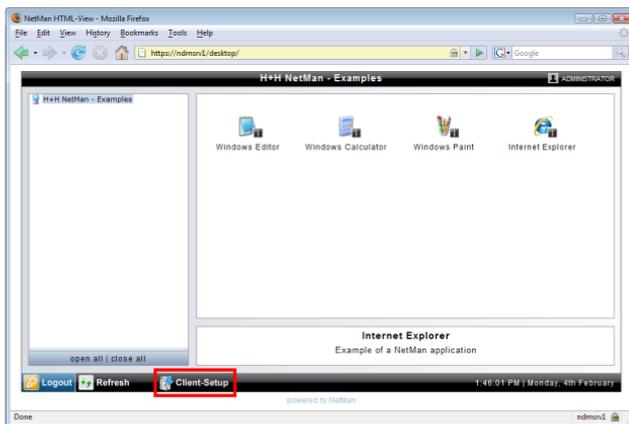
For "Port" enter the HTTPS port number for your NDM installation.

---



## 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.

---

**NOTE** Installation of the NetMan RDP web client requires administrator privileges.

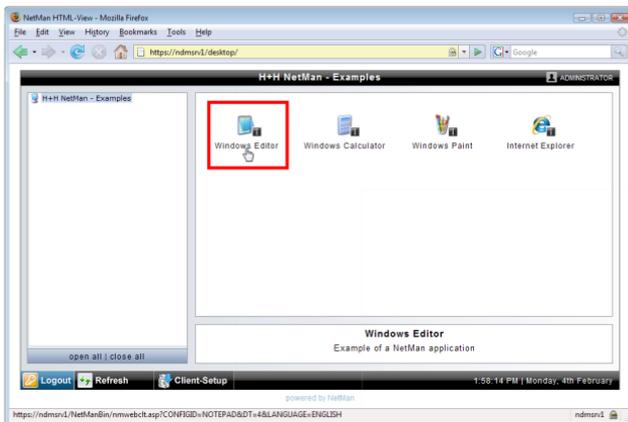
**NOTE** With the default settings, the NetMan RDP web client is used. To use a different client, such as the Java RDP client, configure the corresponding setting on the **Launch Methods for HTML View** page. For details, see Web Interface.

---



# Calling Applications through the Web Interface

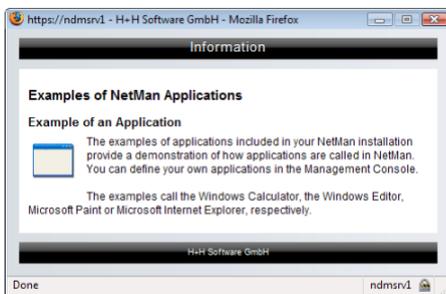
Once the NetMan RDP web client has been installed, you can run an application by clicking on the associated icon.



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

---

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







## Examples of Integration in Terminal Server Environments





## Overview

Up to this point, this manual has described NetMan Desktop Manager as used for application sessions, with or without the MetaFrame Server add-on. In such a scenario, a NetMan Desktop Client installation running on a workstation is used to launch application sessions. Another option is to use the NetMan Desktop Client, which is also installed on the terminal server, together with the Windows Explorer as the interface for desktop sessions. Both methods are described in detail in the following.

- NetMan Desktop Client on a Workstation
- NetMan Desktop Client as Terminal Server Interface



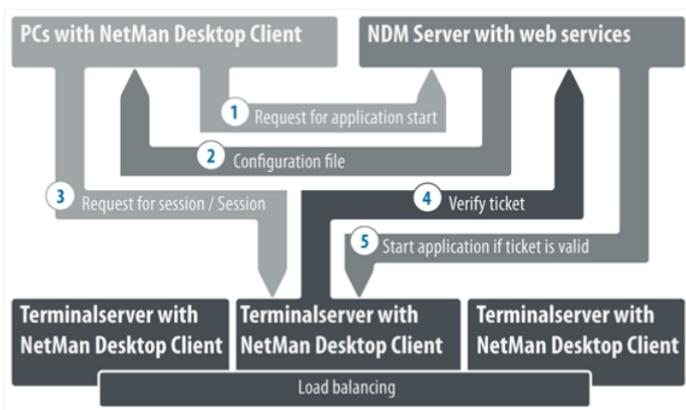
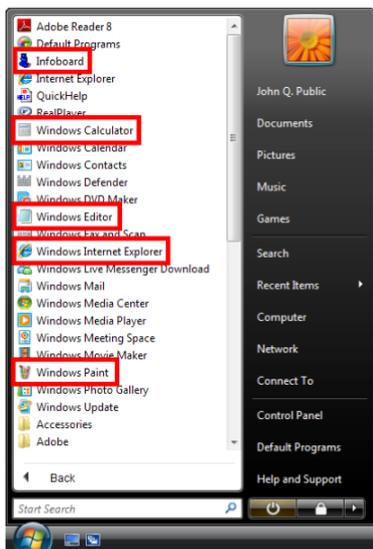
# NetMan Desktop Client on a Workstation

NetMan Desktop Client is seamlessly integrated to enhance the functions available in the Windows Explorer. NetMan Desktop Client can perform the following:

- Launch applications in application sessions on a terminal server or MetaFrame server
- Run applications locally
- Point a browser to a particular website or specified URL

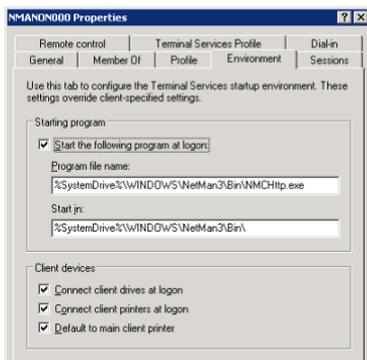
The user cannot see any difference between these forms of application call. If the NetMan configuration starts an application that runs locally, or points to a URL, the sequence is simple, and all process logic for calling the application or the URL runs on the local machine. When the application executes on the terminal server, on the other hand, the process is as follows:

- The workstation requests the application call from NetMan web services.
- The web services serve a configuration for calling a session using RDP or ICA. (An ICA client is required on the workstation for an ICA session.)
- NetMan Desktop Client initiates a session on the terminal server or MetaFrame server.
- Within the session, the ticketing mechanism determines which application is to be started.
- The application is opened in the user's session.

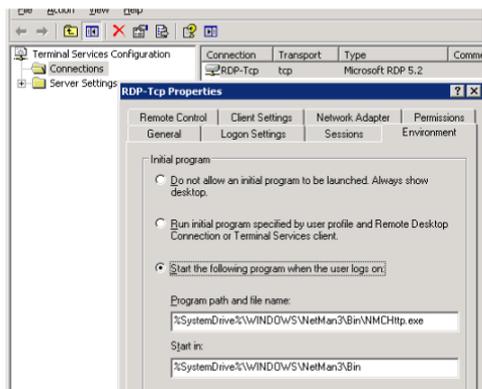


The `NMCHttp.exe` program has to be running on the terminal server to enable execution of application calls. This program can be called as follows:

- When RDP is used for access, the `NMCHttp.exe` program can be set in user properties as the startup program. For *anonymous users*, configure this setting in the *User Account Wizard* for the *NetMan web services*. We recommend setting `NMCHttp.exe` as the startup program for all users who access your system exclusively through NetMan.
- On a MetaFrame server or in a server farm, `NMCHttp.exe` is set up as a published application in the Citrix Management Console.

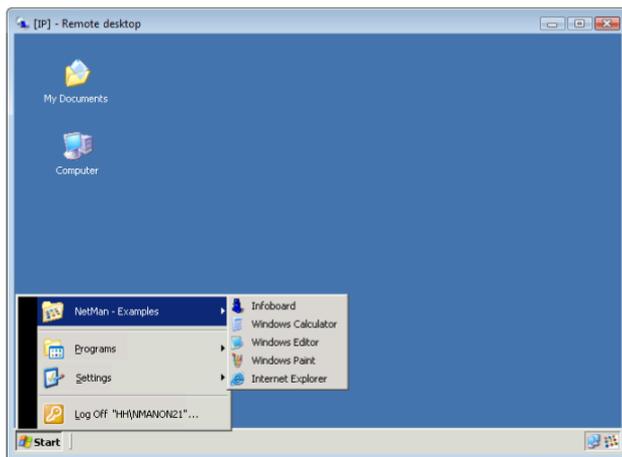


- For users who call other applications in addition to NetMan-controlled programs over RDP, specify the `NMCHttp.exe` program in the NetMan RDP web client or Microsoft RDP web client. For details, see “NetMan RDP Web Client” in this manual.
- The last variant consists in configuring the `NMCHttp.exe` program in the terminal server connection settings. In this case, the terminal server can be accessed only through NetMan Desktop Manager; not even administrators can log on to the terminal server using the Microsoft RDP client. One advantage of this method is that it is easy to configure—only one modification in one program is required.



## NetMan Desktop Client as Terminal Server Interface

The second of the two options mentioned above for integrating NetMan is to use NetMan together with Windows Explorer as the interface for terminal server sessions. In this case, the workstations or thin clients open desktop sessions that execute entirely on a terminal server or MetaFrame server. The NetMan Desktop Client is thus the user interface, and presents a customized Start menu and Windows desktop. The Windows interface on the terminal servers should be secured through the configuration of group policies and (binding) profiles so that users have only the privileges they require at the Windows Explorer end.




---

**TIP** This form of integration is ideal for use with thin-client terminals. The thin client connects to the terminal server automatically at startup, and those applications you have configured are available to the user.

---

For all users who explicitly log in on a terminal server, the startup of the NetMan Desktop Client is invisible. In other words, they do not see any indication that applications are provided through NetMan. With the default settings, an icon in the notification area of the task bar affords direct access to commands for refreshing the desktop and viewing information on NetMan Desktop Manager:



You can also choose not to have this icon shown:



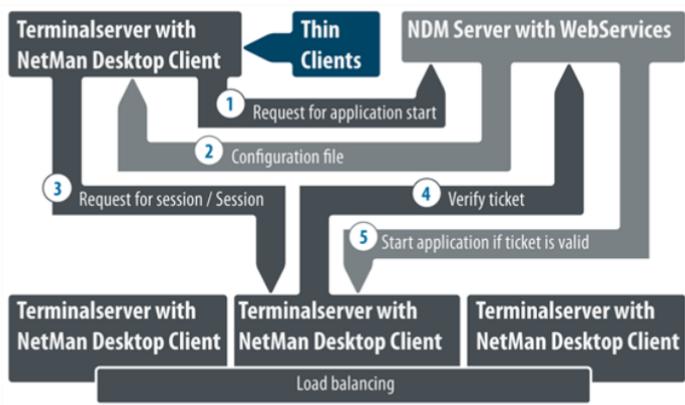
In the same dialog, you can switch automatic startup of NetMan Desktop Client on and off.

**NOTE** We recommend having NetMan Desktop Client run automatically for all users.

**NOTE** If you wish to use NetMan Desktop Manager on a terminal server only for particular users, you can switch off the automatic startup of NetMan Desktop Client and use the login script (`%Windir%/NetMan/bin/nmclnt32.exe` or `%Windir%/NetMan/bin/nmclnt64.exe`) to start the client for those users. If you wish to show the notification area icon for these users, run `Windir%/NetMan3/bin/nmctray32.exe` or `Windir%/NetMan3/bin/nmctray64.exe` after running the `nmclnt32` or `nmclnt64` program.

Calling an application session on a terminal server is analogous to calling an application on a workstation. In a desktop session, on the other hand, the terminal server takes on the function of the workstation:

- In the desktop session, NetMan Desktop Client sends a request to NetMan web services for an application call that executes on a terminal server
- The NetMan web services check whether the desired application is installed on the server that received the request. If the application is found, the application executes on that terminal server. If not, the process continues with the following steps:
- The web services provide a configuration that calls a session using the RDP or ICA protocol (an ICA client is required on the workstation for an ICA session)
- NetMan Desktop Client initiates a session on the terminal server or MetaFrame server
- Within the session, the ticketing mechanism determines which application is to be started.
- The application starts in the user's session.





## System Structure



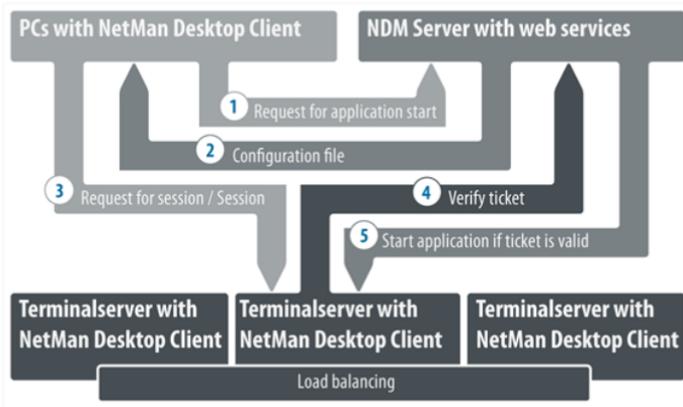


## Overview

As mentioned in the previous chapter, NetMan Desktop Manager 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 Desktop Manager 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

## NetMan Databases

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

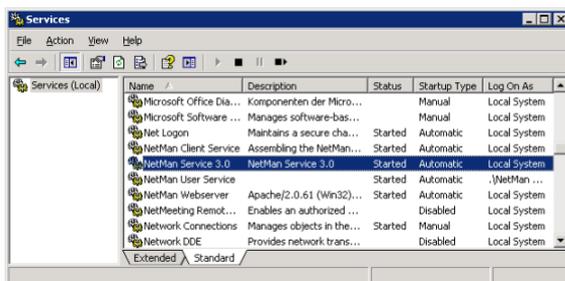
- Users, user groups and user profiles
- Stations, station groups and station profiles
- Installed applications and configurations
- Local and global variables
- Permissions and authentication services (directory services)
- NetMan internal action sequences and external scripts (Windows Script Host supported)

### NOTE

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.



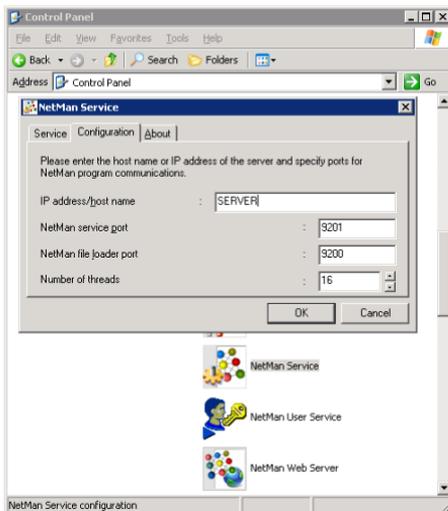
The NetMan Desktop client provides the following data:

- 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

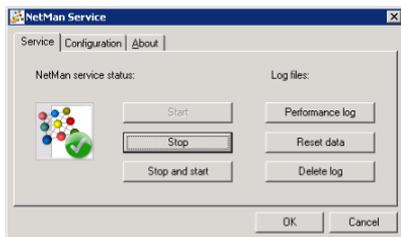
During communication between NetMan service and client, XML structures and configuration files are exchanged over TCP/IP using ports 9201 and 9200. The ports are specified during setup and can be changed on the server in the Control Panel.



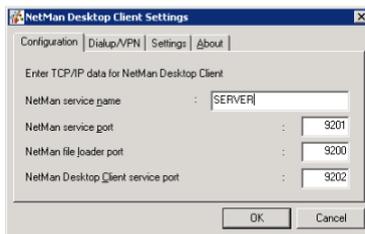
## NOTE

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.



**NOTE** 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 Desktop Manager. In addition to providing a web interface, this component also contains the NetMan web services. NetMan Desktop Manager 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:

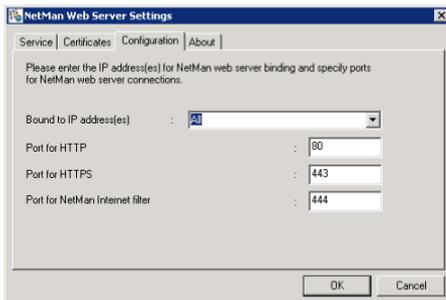
- Session color depth
- Session resolution
- Seamless Windows mode
- Sound settings
- Allocated client drives
- Allocated client printers

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”
- “Overview of Launch Methods”
- “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**.

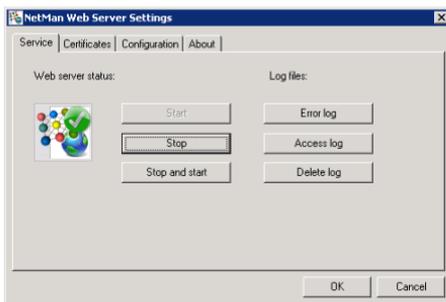
On the configuration page, you can define ports for HTTP and HTTPS as well as which IP addresses the server listens on.



## NOTE

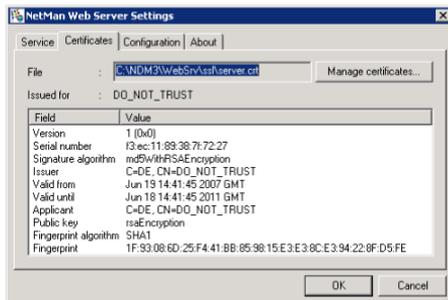
The port specified under **Port for NetMan Internet filter** is used by NetMan's Internet filter component to block access to certain pages. For more detailed information, please see the chapter entitled "NetMan Internet Filter."

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. You can use either of the following:

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

The next two sections describe the integration of certificates in more detail.

## Certificates for NetMan Web Server

### Creating a Self-Signed Certificate

Open the **Certificates** page of your NetMan Web Server settings and click on the **Manage certificates** button to open the wizard for managing certificates.



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:

- **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.

**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 umbuts or other special characters.

Specifications

Server FQDN (example: www.acmeco.com)	:	ndm.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.local

< Back   Next >   Cancel

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.

**NetMan Server Certificate**

**Create a new server certificate**  
You can create a self-signed certificate; for example, for a test installation, or a request for an official certificate authority (recommended).

Type of Certificate

Create a certificate request for an official certificate authority

Issue a self-signed certificate

Valid until : 25.01.2009 ... (366 days)

Password for the Private Key of the Certificate

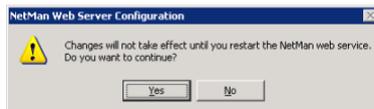
Please select a complex password to protect the private key for this certificate.

Password : [\*\*\*\*\*]

Repeat password : [\*\*\*\*\*]

< Back   Finish   Cancel

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

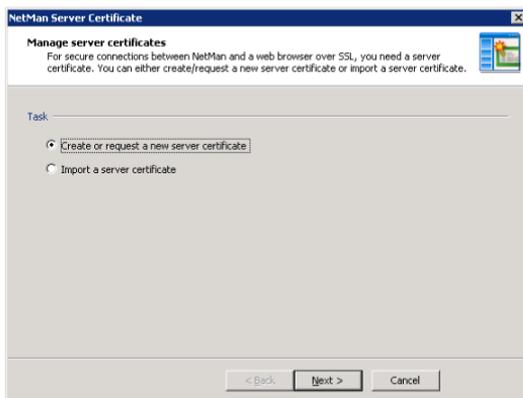
Using an official server certificate involves two main steps:

**STEP 1** 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.

**STEP 2** Importing the certificate: Once the certificate has been issued by the certificate authority, you need to import it to your server.

These two procedures are explained in detail in the following.

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



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:

- **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.

**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 unibits or other special characters.

Specifications

Server FQDN (example: www.acmeco.com)	:	ndm.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.local

< Back   Next >   Cancel

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.

**NetMan Server Certificate**

**Create a new server certificate**  
You can create a self-signed certificate; for example, for a test installation, or a request for an official certificate authority (recommended).

Type of Certificate

Create a certificate request for an official certificate authority

Issue a self-signed certificate

Valid until : [ ] [ ] (0 days)

Password for the Private Key of the Certificate

Please select a complex password to protect the private key for this certificate.

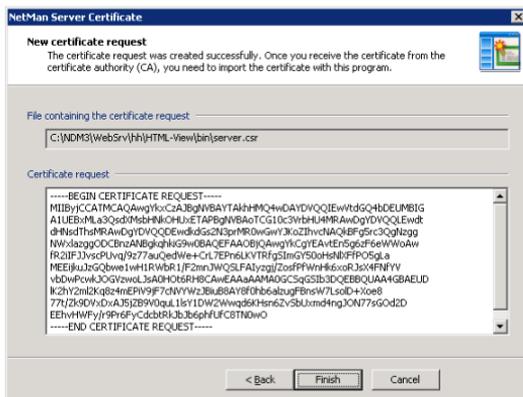
Password : [ ]

Repeat password : [ ]

< Back   Finish   Cancel

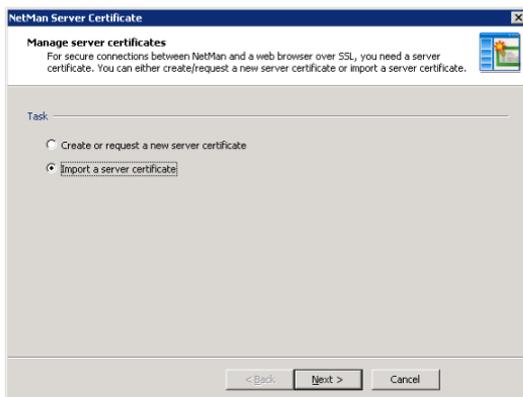
Click on **Finish** to create and view the certificate request.

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).



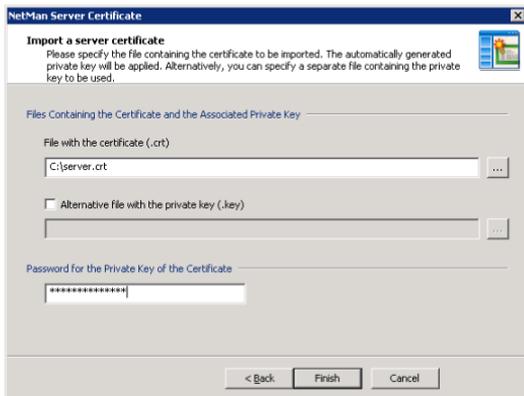
This concludes the first step. Once you have received the certificate from the certificate authority, you can proceed with Step 2 as follows.

**STEP 2** In the **NetMan Web Server Settings** dialog, click on **Manage certificates** to open the certificate management wizard.



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

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



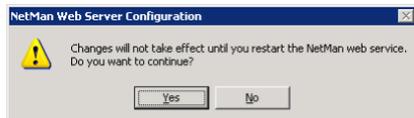
---

**NOTE** 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.

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

---

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.



# Client Installations

## NetMan Desktop Client: The Basics

The NetMan Desktop Client was mentioned in the previous chapter, “Installing NetMan.” 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.

## 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 "NetMan3" 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.

---

### NOTE

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.

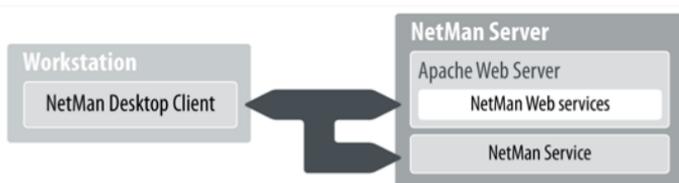
---

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 3 Desktop file -->
003 <NMDesktop>
004 <Desktop_english>H+H Applications and Links</Desktop_eng-
005 <Link>
006 <ConfigID>ENCARTA</ConfigID>
007 <Prompt_english>Encarta 2005</Prompt_english>
008 <Description_english>Microsoft Encyclopedia</Description_
  
```

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

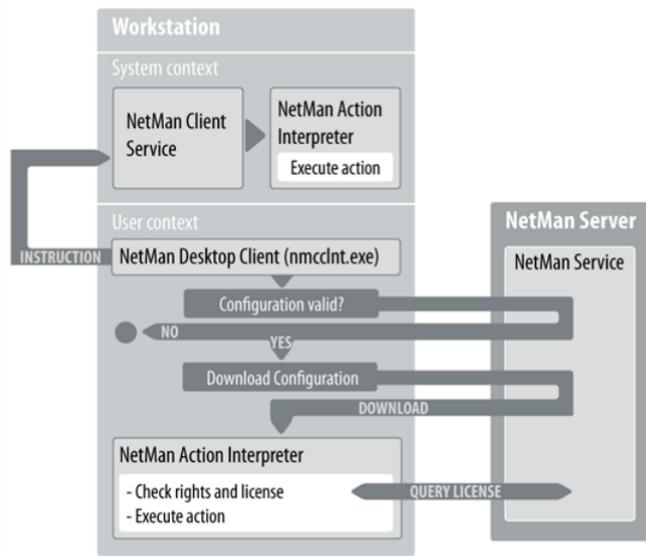
The desktop data is assembled and deleted by a service that is started automatically when the workstation is booted up. The Desktop Client itself and its tray program, on the other hand, run under the user account:

Image Name	User Name	CPU	Memory (K)	Description
nmcldnt.exe	SYSTEM	00	620 K	NetMan Desktop Client
nmcscr.exe	SYSTEM	00	72 K	NetMan3 Client Service
nmcstray.exe	00	492 K	492 K	NetMan Client Tray
OUTLOOK.EXE	00	7,944 K	7,944 K	Microsoft Office Outlook

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:

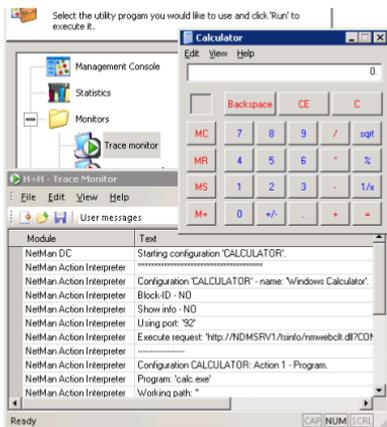
- A modification has been made on the server, through which the user no longer has permission to use the link
- The link was not generated by the NetMan Desktop Client, but was created or copied by the user.

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:

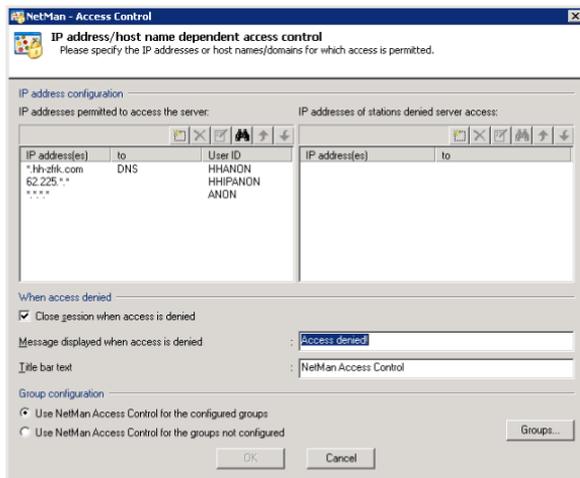
You can edit this default error message in the NetMan Settings. You can deactivate this security mechanism by deactivating the first option under **Security Settings** on this dialog page:



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:



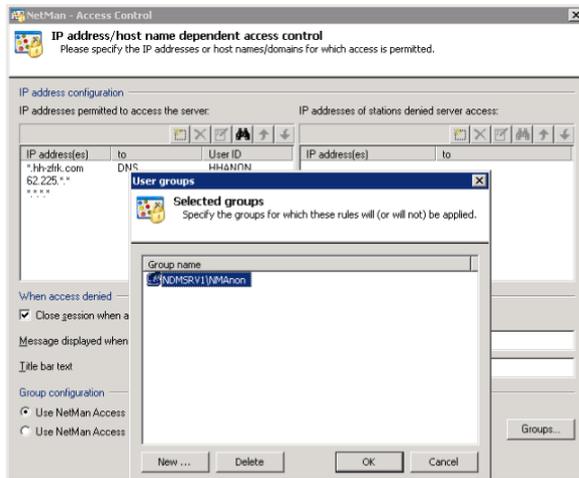
When you first run NetMan, access control is already active and three rules are configured as an example, but no user groups are configured to which the rules are applied.

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:



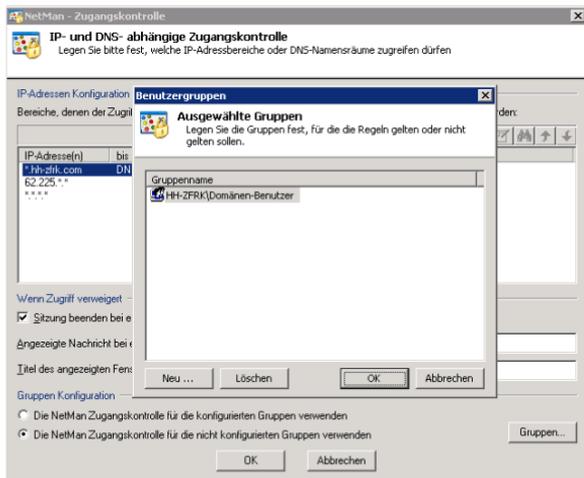
With the configurations shown above, the “anonymous” user name (NMANON001, NMANON002, etc.) is replaced by one of the user names shown under “User ID,” depending on the client IP address. These are more useful than strictly anonymous user names; for example, for recording application usage and for granting 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.



The title bar text and the body of the message can be edited, if desired.



# NetMan Desktop Manager Programs





# 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:

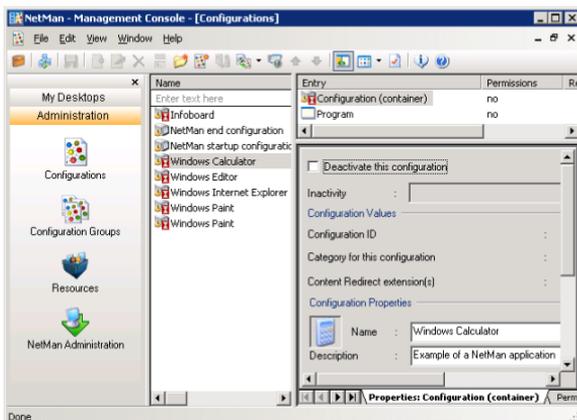
- My Desktops
- Administration

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.

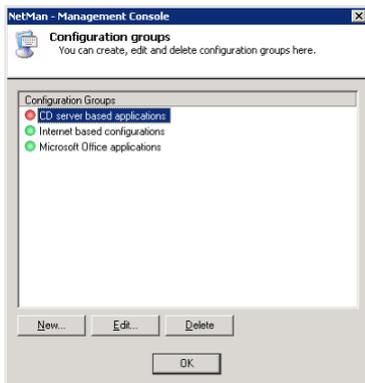


A  symbol shown with a configuration's icon indicates that this configuration is integrated in at least one desktop. A configuration that is linked to a desktop cannot be deleted.

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 for-

mer 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.

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.



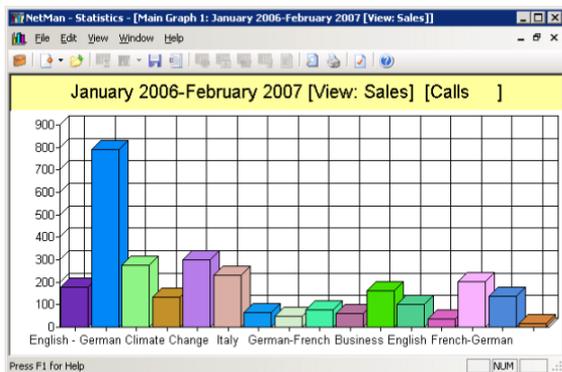
The **Resources** window lets you view and edit **users**, **stations**, **user groups**, **station groups**, **user profiles** and **station profiles**. These NetMan resources are described in detail in the chapter entitled “NetMan Desktop Manager Resources” in this manual.

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.

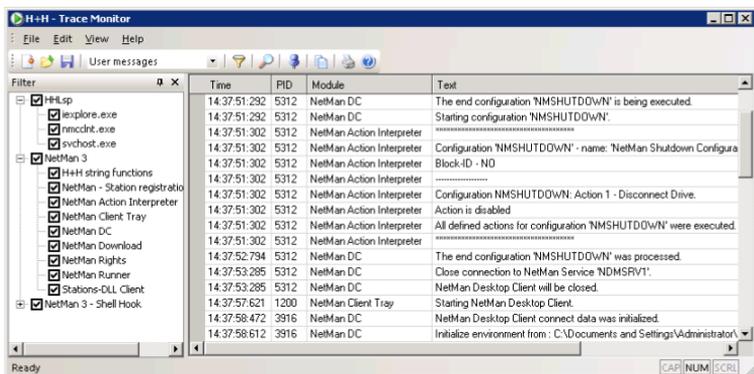




# Monitors

## 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 program shows messages indicating the status of internal processes.



You can configure settings to define the output. For example, you can assign different colors to each program module, and define the level of output. You can also determine whether the tree diagram on the left-hand side is shown or hidden.

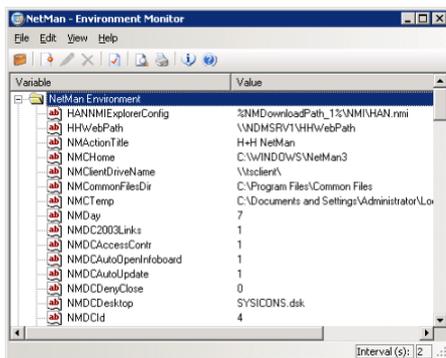
## Trace Monitor for Console Messages

In addition to the Trace Monitor, the Trace Monitor for Console Messages also shows process messages. Unlike the Trace Monitor, however, which only shows messages from processes active in the session in which the monitor is running, the Trace Monitor for Console Messages shows all messages generated by processes running on the terminal server. These include, for example, trace messages from NetMan Desktop Client to the console as well as messages from server components and the following services:

- NetMan service
- NetMan web services
- NetMan client service

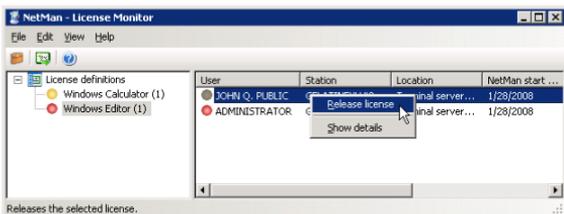
## Environment Monitor

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.



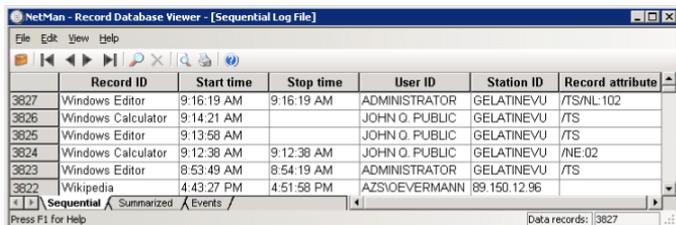
## License Monitor

The License Monitor shows the application licenses configured in NetMan with details on the licenses currently in use.



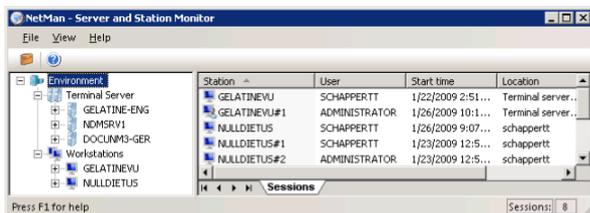
## Database Browser

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.



## 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.

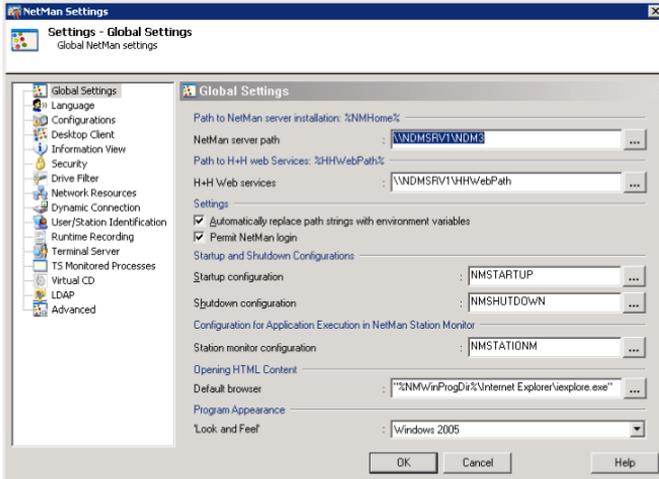




# Settings

## 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.

**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.

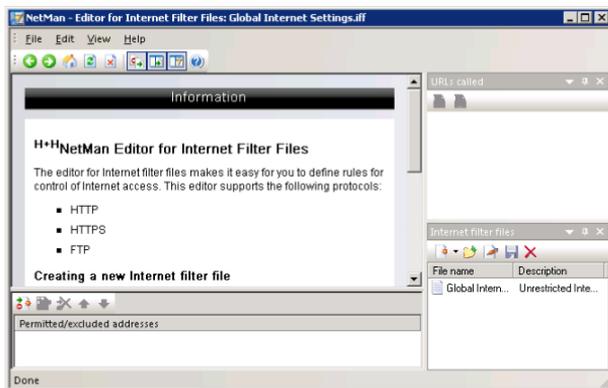
**Virtual CD:** Lets you configure settings that affect the way Virtual CD and NetMan work together.

**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

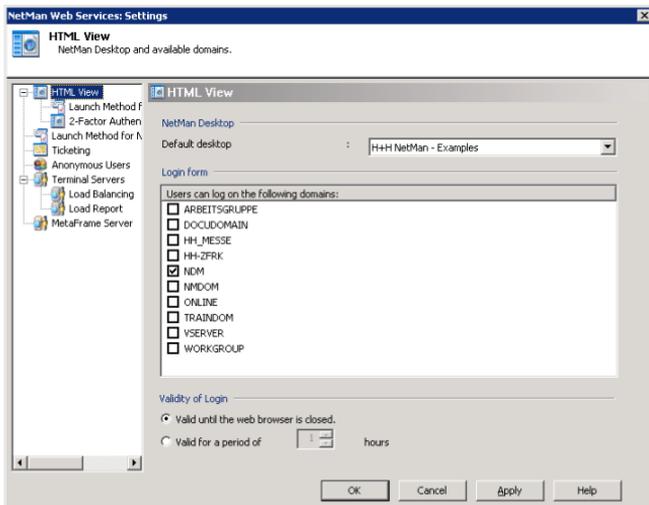
When you select “Internet Filter Settings” from the Toolbox, the editor for Internet filter files is opened. This is an interactive editor for creating rules that govern access over HTTP, HTTPS and FTP. You can define different sets of rules for different applications. These rules can limit access to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



For details on using this editor, see “NetMan 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 is defined in this settings program:

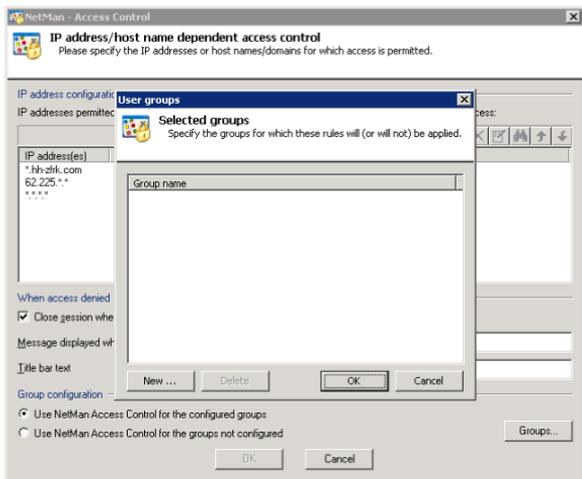
- Which domains can be logged in on through the web interface
- Settings for 2-factor authentication
- Which settings are configured for which stations by the selected launch method
- Settings for load balancing in application sessions
- Which login method is used at session start
- Properties of NetMan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

## 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.

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.




---

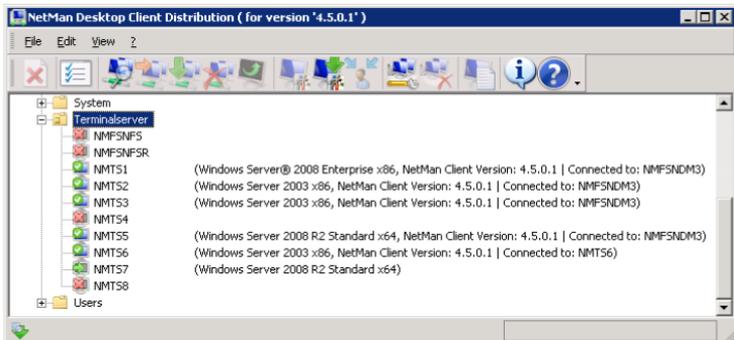
**NOTE** Exercise caution in defining groups and access privileges. Do not inadvertently prevent administrator accounts from running NetMan Desktop Client, as this would block access to all administrative functions.

---

# Wizards

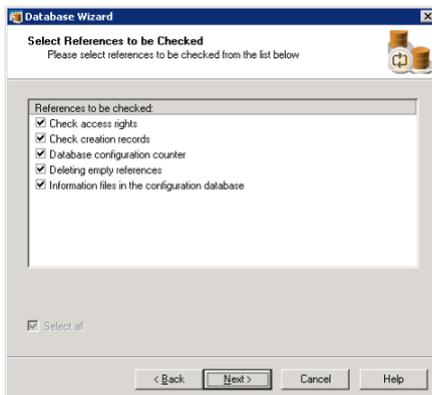
## NetMan Desktop Client Distribution

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.



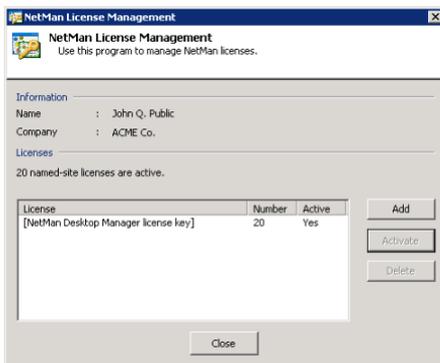
## Database Wizard

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 Desktop Manager program license. If your license is not registered, the NetMan software runs in demo mode. You can download a license that is valid for a limited period and lets you use NetMan's full functionality.





## Integrating Applications and Hyperlinks

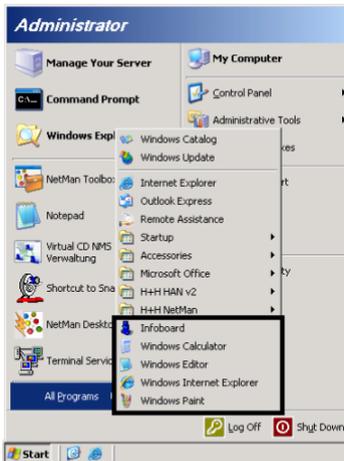




# NetMan Configurations

This section provides detailed definitions of the terms “configuration,” “application,” “program” and “hyperlink” as they are used in the context of NetMan, for a better understanding of both the manual and the way NetMan works.

NetMan Desktop Client automatically installs five NetMan configurations in the Start menu of the **H+H NetMan 3 Examples** desktop:




---

**NOTE** These configurations are automatically added to the Start menu under **All Programs**. To have the shortcuts displayed instead in a subfolder of the NetMan desktop folder, open the **Desktop Client** page of the **NetMan Settings** program and deactivate the **Add NetMan desktops to the top layer of the ‘All Programs’ folder in the Start menu** option.

---

All of the items that NetMan adds to a desktop are called (*NetMan*) *configurations*. There are basically two types of NetMan configuration:

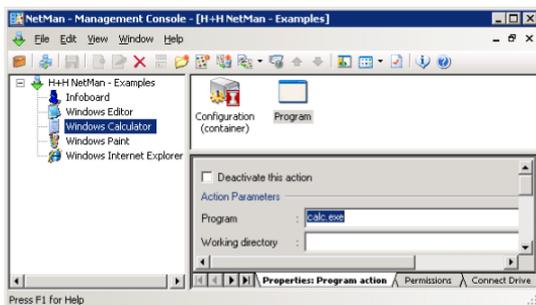
- Containers (also referred to as “application configurations” in this manual)
- Folders

*Folder* configurations are used to define structures within desktops.

The *type* of configuration is indicated both by its icon and by the designation (**container** or **folder**) shown in the NetMan Management Console:



**Container** configurations contain a sequence of actions. 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 a Linux or Macintosh system, a Windows terminal server is required for processing the actions. In general, NetMan container configurations are most frequently used to launch programs.



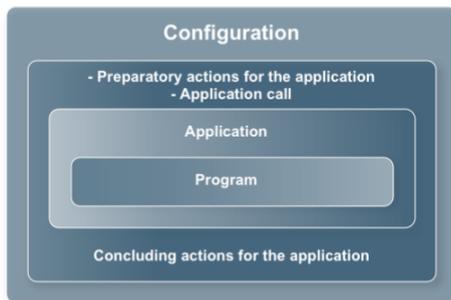
In the example shown above, the configuration called “Windows Calculator” runs the “Calc.exe” program. This program was chosen for use as an example because it is generally found on all computers that run Windows.

This brings us to the definitions of “program” and “application” in the NetMan context. Strictly speaking, the difference between the two is that a *program* can execute on its own, while an *application* consists of more than just a program call. For example, MS Word is referred to as a “Microsoft Office application” because the program itself, 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. Given these definitions, Notepad.exe is clearly a program—but with NetMan, you can make it into a customized application.

The term *configuration*, as used in the context of the NetMan software, is even broader; it refers to a completely user-definable 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 NetMan “Program action” that has been 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 to carry out a variety of functions. Here are just a few examples:

- Create a login dialog or map a network drive for access to the program, or for access to a resource the program requires, such as a CD-ROM.
- Write 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.
- Restore the working environment to its previous state when the program is closed.

The following diagram illustrates the relationships between a **program**, an **application** and a **container configuration**:



The most basic NetMan configurations do not contain any preparatory or concluding actions; the only action is the program call, as is the case in our “Notebook.exe” example.

In many cases, integrating an application 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 desired 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 conditions. Thanks to NetMan’s **Windows Script Host** interface, you can even create your own NetMan actions.

In summary: A container configuration is a logical unit that can be executed by a user; it may contain 999 actions, or none at all. A “Program” action runs an application that is integrated in a NetMan configuration.

---

#### NOTE

Whenever this manual mentions launching a NetMan application call, executing a NetMan configuration or calling a NetMan-controlled application, this means that the processing of a container configuration is initiated. The configuration in question can contain practically any number of other actions, which are processed either before or after the program action.

---

Today’s programs increasingly rely on access to data not only on the local workstation (whether in the “C:\Program Files” directory or on a CD-ROM), but also to data available only on the intranet or over the Internet. NetMan comes with an Internet filter that you can configure to control processes that are launched by NetMan actions and access the Internet.

With the increasing use of browser technology for accessing remote data, the NetMan *Hyperlink* action is gaining in importance. With this action, you can specify a browser and have it access the required HTML-based data, whether from the hard drive, from the CD-ROM drive, on the intranet or over the Internet.

A Hyperlink action loads an HTML document over HTTP. When a hyperlink configuration is activated, the NetMan Client runs the Microsoft Internet Explorer or, if you change the appropriate setting, a browser of your choosing. Hyperlink and Program actions have several properties in common:

- You can have execution of the action recorded in a log file.
- You can configure and assign a **NetMan Internet filter** for the action.

NetMan Desktop Client executes hyperlink actions by opening the browser specified in the NetMan settings and pointing it to the URL named in the action.

**Folder configurations** are for organizational purposes only and cannot contain any actions.

# Working with the Management Console

## The Sample Desktop

The following section describes the **H+H NetMan - Examples** item in the **My Desktops** view.

When you select this item, the **H+H NetMan – Examples** desktop is opened for editing. This is the default desktop, and is integrated in the Start menu for all NetMan users. Any changes you make here are implemented for all NetMan clients that use this desktop.

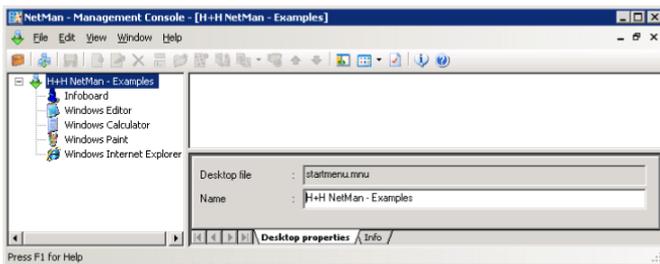
The screen capture below shows the fully expanded desktop structure, with the selection sidebar hidden. The active item in the folder view in this example is the root entry. Since the root entry is not a configuration and does not contain any entries or actions, the upper pane on the right, called the Entry pane, is empty.

---

### NOTE

With the default settings, the entries in a NetMan desktop are all listed under **All Programs** in the Start menu. To have only the desktop **name** shown under **All Programs** and the individual entries listed in a subfolder under the desktop name, open the **NetMan Settings** program and deactivate the **Add NetMan desktops to the top layer of the 'All Programs' folder in the Start menu** option on the **Desktop Client** page. When a NetMan desktop is opened on the Windows desktop, the desktop name is not visible.

---



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.

The Info page shows information on whatever entry is selected in the upper right-hand pane; if the desktop root is selected, as in this example, the information shown applies to the Desktop Editor itself.

---

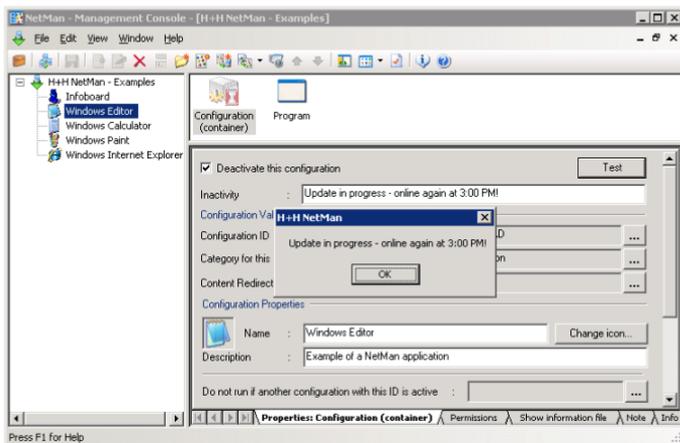
**TIP** When you first start working with NetMan, it can be helpful to read the Info pages on each of type of entry.

---

## A NetMan Configuration

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 Editor” 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 is still visible in the NetMan Client but if a user tries to activate it, a window opens with the message defined here under “Inactivity.” This lets you keep your network users informed, so they don’t need to seek you out with questions about why the application is not working. Here is an example:

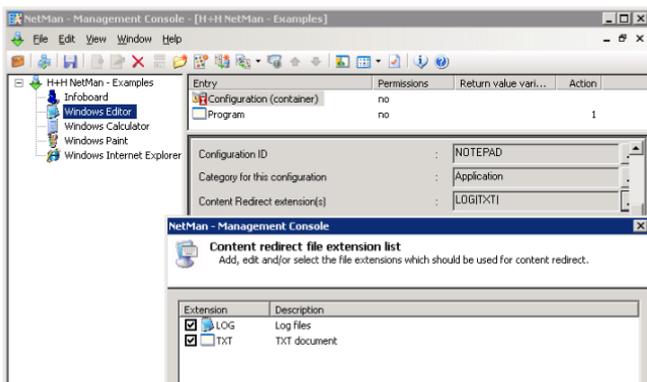


For a container configuration, you can enter an identifying string under **Do not run if another configuration with this ID is active**. This string is also referred to as a “lock ID,” and lets you prevent mutually incompatible applications from running simultaneously. This can be useful if particular applications (or separate instances of the same application) interfere with one another. For example, one application might try to access data that another application locks down during use, or an application might be internally designed to run in only a single instance on a given machine. You can configure any string you wish as an ID, and then enter the same string in this field for the other 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

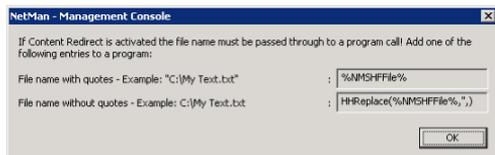
known as **content redirection**. To implement content redirection in a NetMan configuration, click on the button next to the “Content Redirect extension(s)” field and select or edit file name extensions as desired.



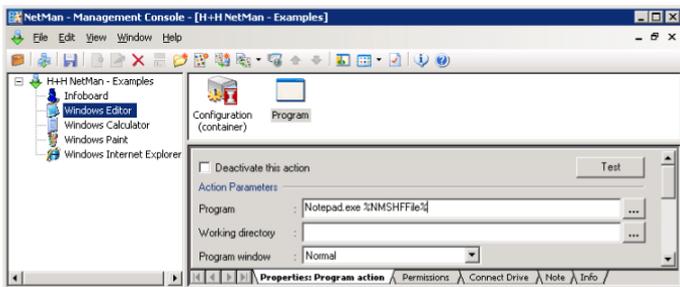
The following conditions must be met before content redirection can function properly.

**STEP 1** 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.

**STEP 2** 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.



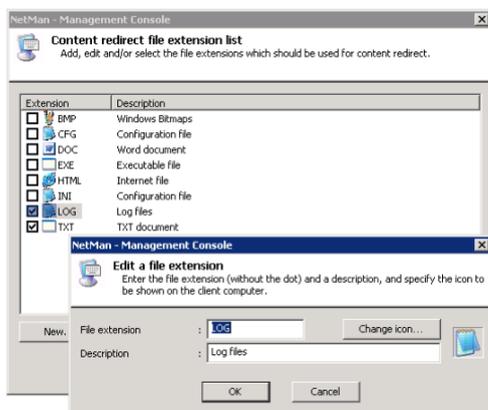
For example, the command line that calls Notepad.exe may take the following form:



**STEP 3** 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.

**NOTE** 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.

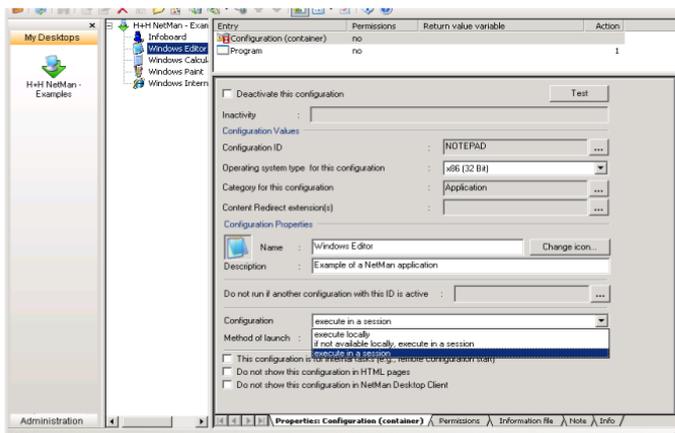
**NOTE** In the dialog for selecting file name extensions, you can specify an icon for each file name extension. Icon assignments are stored on the client machine by NetMan Desktop Client and registered for the specified file types. Thus even file types unknown to your operating system are shown in the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



The option **This configuration is for internal tasks** defines how the configuration is managed.

There are basically three ways to have a NetMan configuration processed:

- **Execute locally**
- **If not available locally, execute in a session**
- **Execute in a session**



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.

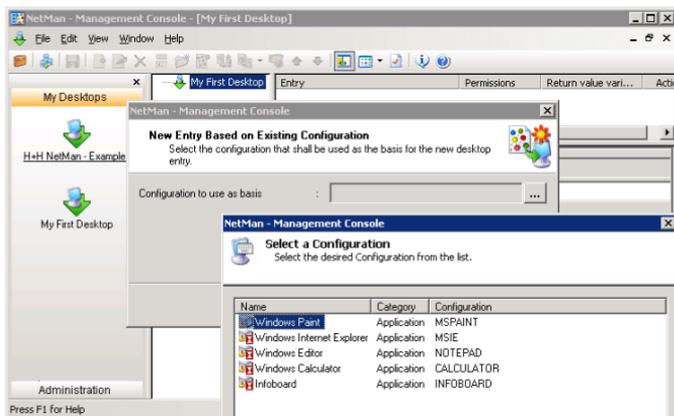
## NOTE

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.

**TIP** 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.



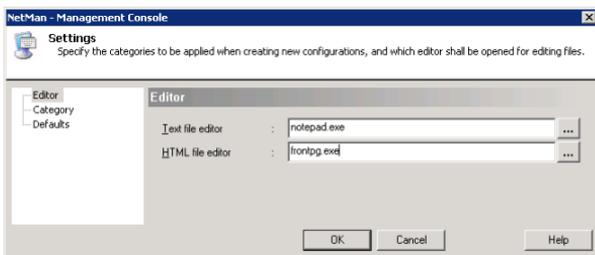
**NOTE** You can activate the **This configuration is for internal tasks** option for configurations that are not assigned to any desktop, and use those configurations for functions that are not desktop-specific.

Each configuration has the following dialog pages:

- **Properties: Configuration**
- **Permissions**
- **Information file**
- **Note**
- **Info page**

We will take a closer look at the “Permissions” page at a later point in this manual. 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** (or “Show information file”) tab to view the information page for this configuration. The default editor for opening this file is Notepad.exe. To use a different editor, select **Settings...** from the View menu and enter the command line call for the desired program:




---

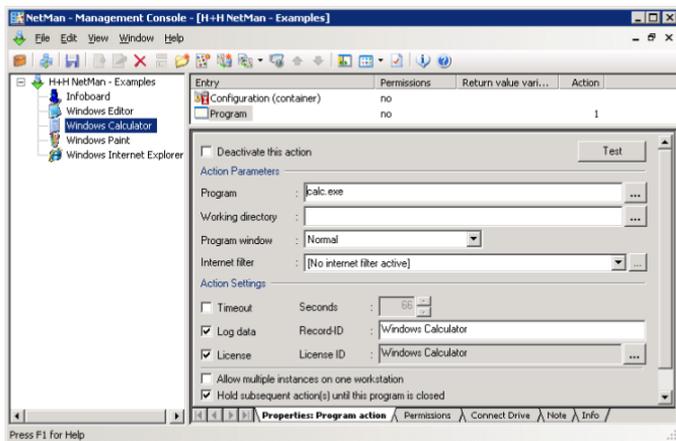
**TIP** Click on the **Info** tab to read the text about the “Configuration” entry.

---

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 (licensing codes or other special requirements).

## Program Actions

The next example shows the “Windows Calculator” configuration selected in the folder view and its “Program” action—the only action in this configuration—selected in the Entry pane. The information shown on the **Properties** page is explained below.



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 “NetMan 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** 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 string you enter in the “Record ID” field 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.

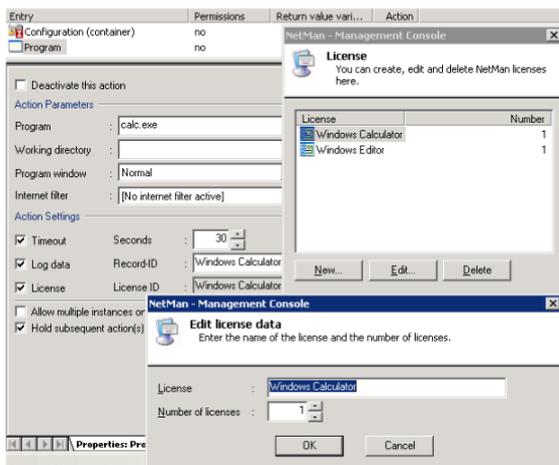
Unlike other actions, the Program action also has a **Connect Drive** dialog page, where you can map a drive designation to the network resource required by the program.

## 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 shown 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.



**NOTE** 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 use a single software license.

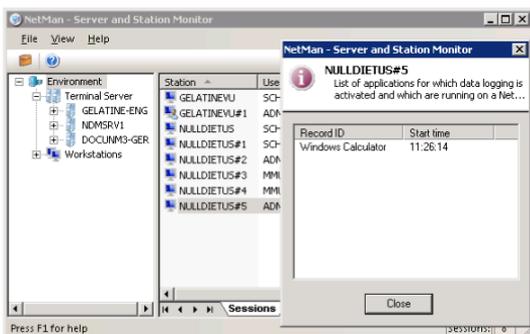
The settings configured here are effective in the NetMan Client as soon as they are saved. You can test your changes before saving the settings; the Test function is available in the toolbar, in the **Edit** menu and in the shortcut menu that opens when you right-click in the Entry pane. If an action 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.

**NOTE** Testing a licensed application 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:



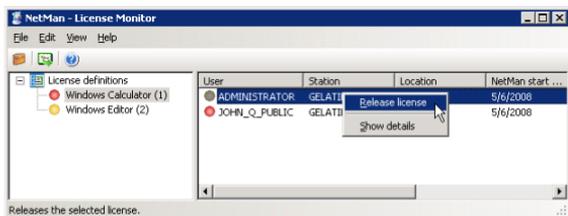
The message displayed on the third workstation indicates that the user is second in line. The next step is to call the **Station Monitor** from the NetMan Administration window and view the status of all connected clients: Select the workstation from which you called the program. Select "Recorded applications" from the View menu; the dialog shows that the "Windows Calculator" configuration is running on this workstation.



## NOTE

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 NetMan Help program.

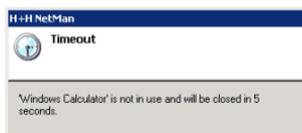
You can call the *License Monitor* to see which licensed applications are in use, and to release licenses if desired. In the example shown below, a license for the Windows Calculator program configuration is released, which causes the configuration to launch for the user who had been in the first position in the license queue:



## NOTE

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, the **database browser** (NetMan Record Database Viewer) shows the following:

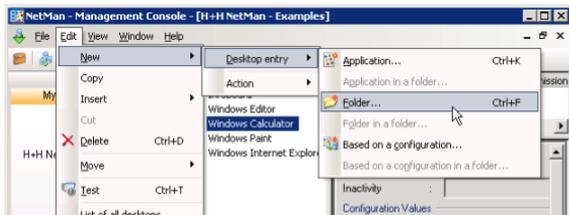
Record ID	Start time	Stop time	User ID	Station ID	Record attribute
3837	12:31:08 PM	12:31:41 PM	SCHAPPERTT	NULLDIETUS	/TSAWL:17
3836	12:28:17 PM	12:28:48 PM	ADMINISTRATOR	GELATINEVU	/TSAWL:11
3835	12:27:56 PM	12:28:27 PM	SCHAPPERTT	GELATINEVU	/TSAWL:21
3834	12:27:41 PM	12:28:16 PM	SCHAPPERTT	NULLDIETUS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

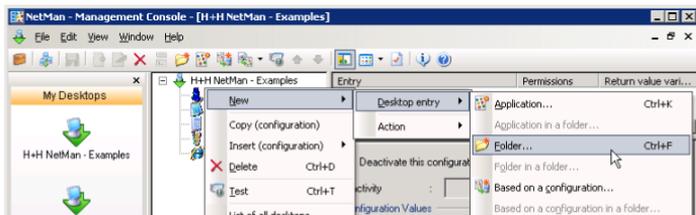
## Creating and Deleting Desktop Entries

In the examples above, we added new program properties to existing configurations. 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 item:



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.

## NOTE

If you select **Based on a configuration** or **Based on a configuration in a folder** a shortcut to an existing NetMan configuration is created. The other options create new configurations.

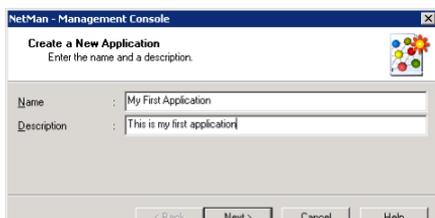
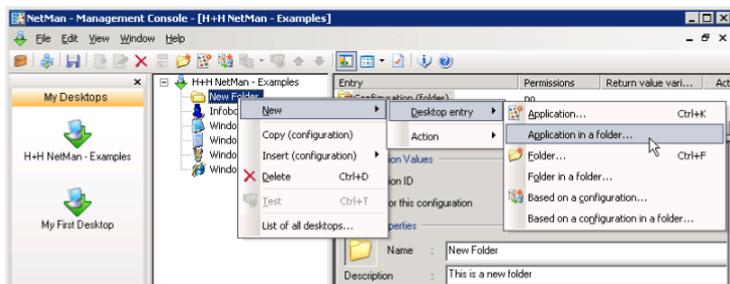
You can also use the following toolbar buttons to **Create a new folder [configuration]**, **Create a new application [configuration]** or **Create a new hyperlink [action]**.



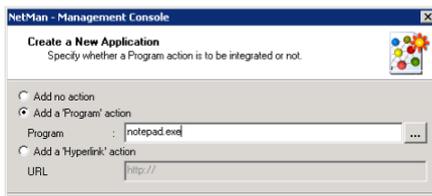
In the following example, we will create a folder called **New Folder**.



Here we enter a name and a brief description of the new folder and click "Finish." Next, we create an entry within this folder; this time it is an "application" item:

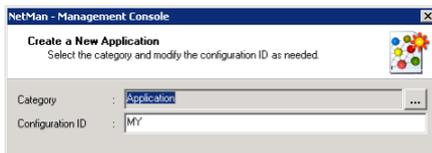


Again, we enter a name (“My First Application”) and a brief description; then we can go on to define a Program action for the new application configuration, because it was created as an application, not a folder:



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

- The ID of the new configuration (in this example, “MY”)
- 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 in the web interface.

---

**TIP** In many cases, it is important to modify the suggested configuration ID to make it more meaningful. 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.

---

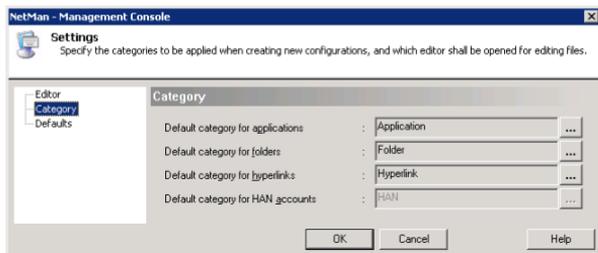
The **Category** of a configuration is basically a sorting criterion. As you can see in the list of all configurations (opened as described above), “Category” is one of the column headers:

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

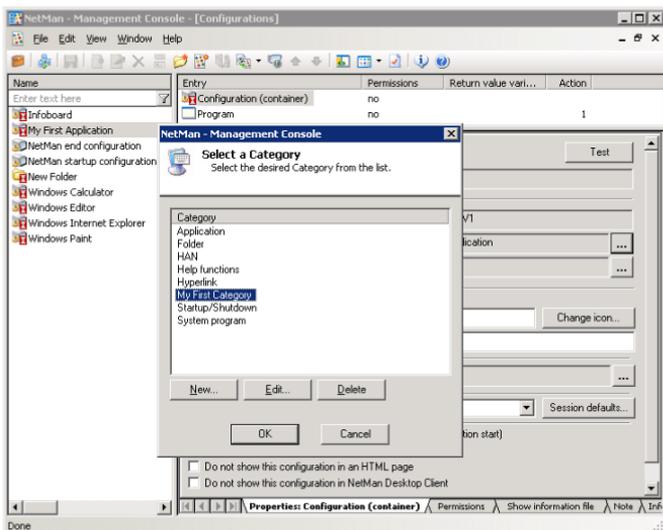
This table can be very long, depending on how many configurations you have. The use of categories can help you to keep track of your configurations, and to find a particular configuration more easily.

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

Let us return to our "My First Application" example. NetMan assigned the category "Application" automatically, based on a function that you can modify under **View/Settings**:

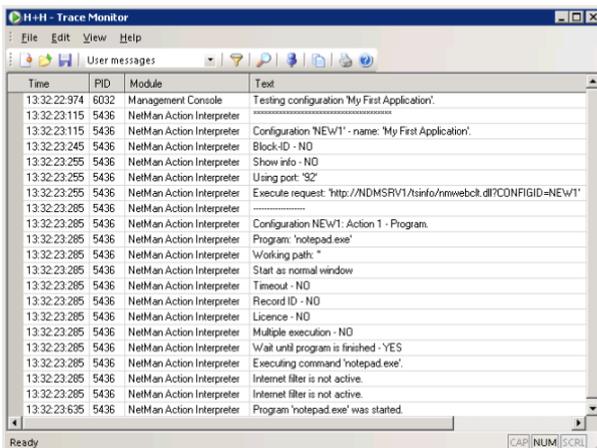


As you can see here, you can define your own categories and specify defaults. In our example, a new category called **My First Category** is assigned to the configuration called "My First Application:"

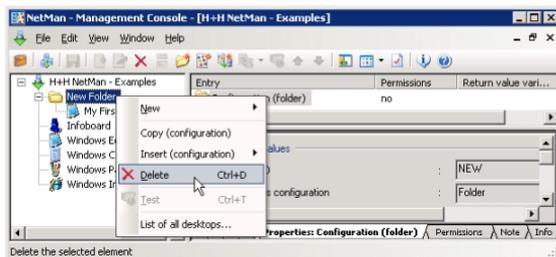


Now we test the new configuration with the Trace Monitor switched on.

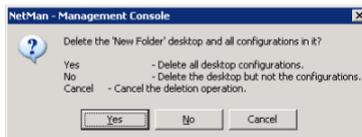
As the last entry below indicates, the Notepad.exe program was launched successfully.



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



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



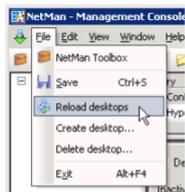
This question is always asked when you delete a configuration that is not assigned to any other desktop. If the entry is still linked in another desktop, it is simply removed from the active desktop when you select the “Delete” command, without prompting for confirmation, and is still available in the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

In the preceding steps, we made several changes in the desktop structure. If we save the changes now, or had done 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.

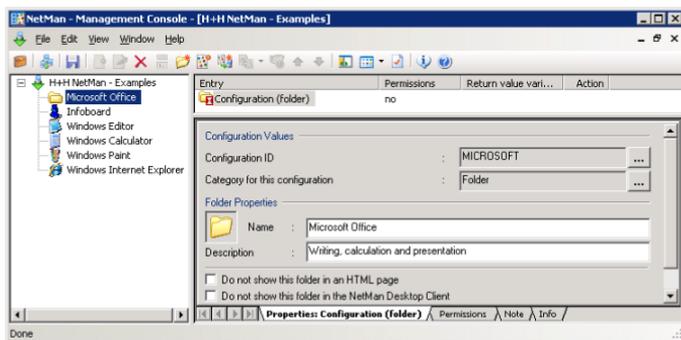
The NetMan Desktop Client registers the necessity to reload a desktop or configuration based on the date a desktop or configuration was created. If you have assigned rights to desktops and configurations, Desktop Client might not register changes made in external databases (e.g., in ADS). You can force a reload by selecting the “Reload desktops” command from the **File** menu in the Management Console.



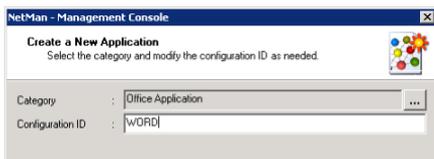
## Your First Application

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. This example shows you the options for integrating an application in your NetMan databases; it does not deal with the topic of MS Office installation.

We begin by creating a folder called Microsoft Office:



Then we create a new Application configuration as described in the previous section.

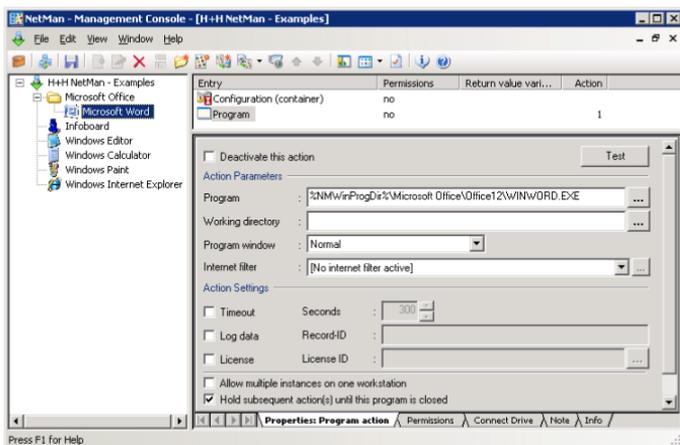


---

**NOTE** Make sure the **Execute configuration in a session** option is active so that the application is executed in a terminal server session. Otherwise, MS Word will execute on the local workstation.

---

NetMan automatically copies 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.




---

**NOTE** With the default global 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 ensures that the program is found on the terminal server(s), regardless of whether the drive letter is C: or D:, and no matter what the directory is called, as long as it is installed in the Windows directory.

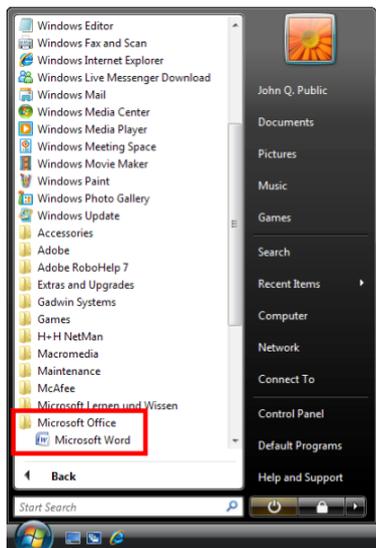
**NOTE** When you use the `%NMSHFFile%` variable to pass a file name to a program, it is important to know what the program requires. In the most simple case, only the file name is required. Some programs, on the other hand, require a switch to precede the file name on the command line.

---

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

On the **Information file** (or “Show information file”) page, you can create and assign a special HTML file for providing information to users if desired.

NetMan can now be put into operation with your first application. If you were to integrate all Microsoft Office applications in the same manner, the Start menu in NetMan Desktop Client might look something like this:



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, the information in this manual assumes that you know how to create, edit, delete and move desktop entries; details are provided only on other aspects of NetMan operating elements.

## Access Privileges 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 network groups. You can also grant or refuse access privileges based on any of a number of other conditions.

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

- **Global NT group**
- **Local NT group**
- **AD user group**
- **AD organizational unit (OU)**

- **LDAP group** (LDAP server required)
- **NetWare group**

This mechanism supports the groups used in the most common network operating systems. In other words, 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 privileges not only to **users' network login names**, but also to **workstation names**, as well as user and station groups and profiles.

With this feature, **NetMan bridges a gap in network operating systems** that generally 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 **conditional** 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**.

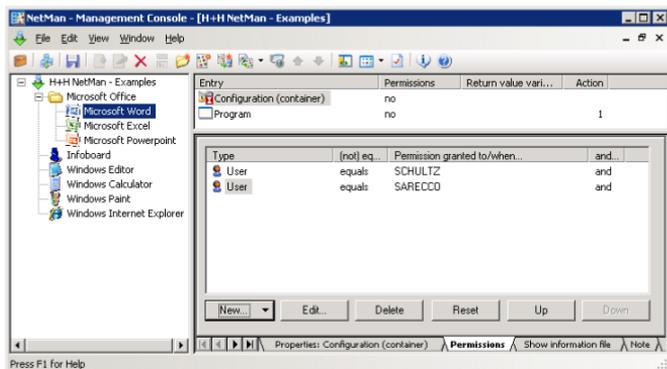
Furthermore, you can choose to show or hide configurations based on any of the following workstation factors:

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

These 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, 'execute' permission is granted 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." Enter 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**).

## NOTE

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

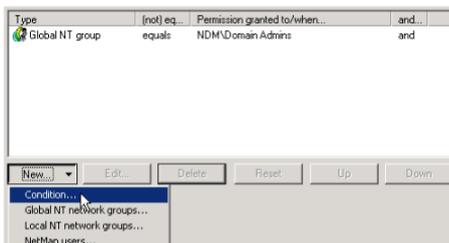
Type	(not) eq...	Permission granted to/when...	and...
Local NT group	equals	\\GELATINE-ENG\Administrators	and
Windows version check	equals	Windows TS-based	or
User	equals	ADMINISTRATOR	and
Windows version check	equals	Windows >XP	and

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

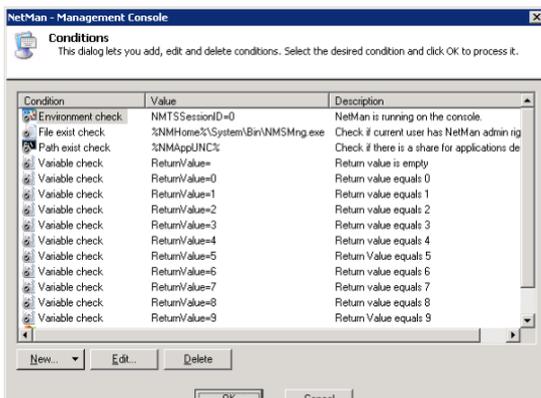
"Local NT Group" = ("GELATINE-ENG\Administrators" AND "Windows version" = "Windows Terminal Server") OR ("User" = "Administrator" AND "Windows version" = "Windows XP")

The next example illustrates a 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:



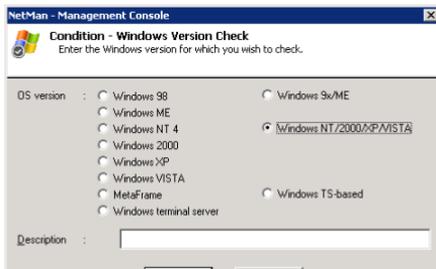
Click on **New...** and select "Condition;" this opens a list of conditions that you can choose from.



## NOTE

The conditions listed here immediately after installation are used by a number of NetMan's internal programs and 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 "Windows version check." In the next dialog box, select **Windows NT/2000/XP/VISTA**.



And that's it:

Type	(not) eq.	Permission granted to/when...	and...
Global NT group	equals	NDM\Domain Admins	and
Windows version check	equals	Windows NT/2000*/P/VISTA	and

Other conditions you can choose from include 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.

---

#### NOTE

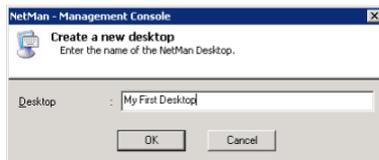
Please note that some of these conditions cannot be checked when configurations are accessed using the web interface. These include the following:

- 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**.

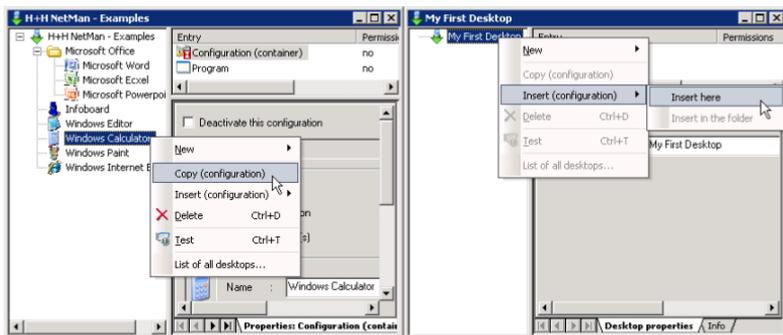
## Creating New Desktops

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



The new desktop is empty. You can choose from the following for your new desktop:

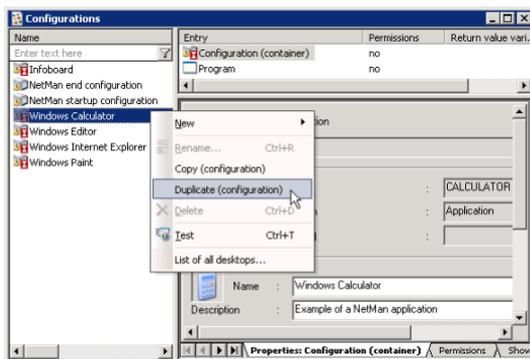
- Add folders and/or applications. This entails creating new NetMan configurations.
- Add desktop items from existing configurations. In this case, the desktop items link to existing configurations.
- Use the shortcut menu to copy existing items from other desktops or from the **Configurations** window. To do this, select the configuration you wish 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**.



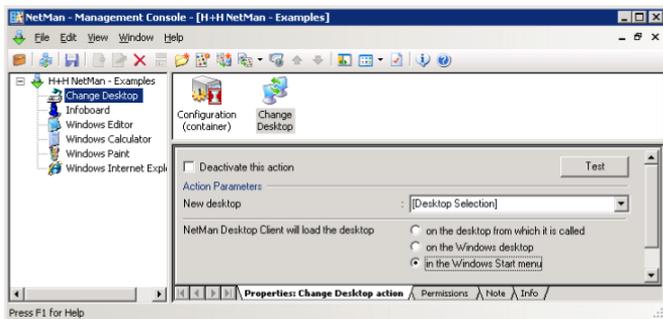
### NOTE

The **Insert (configuration)** command creates a link to an existing configuration. When you change configuration properties, the changes are effective in all desktops that have links to that configuration.

**TIP** 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 copies as desired. In other words, duplicate the configuration first in the **Configurations** window, then copy it using the **Copy (configuration)** command, and finally added to a desktop with the **Insert (configuration)** command.



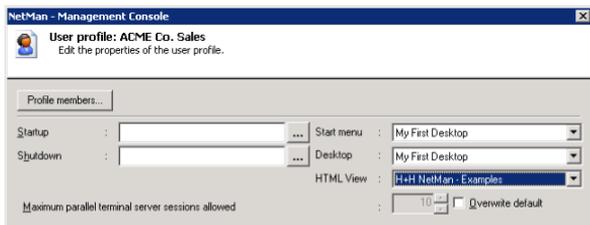
You can insert a Change Desktop action to load a desktop other than the default NetMan Client desktop. If you do not specify a desktop for the change, this action opens a list of all existing desktops for selection by the user. You can also specify whether the desktop is loaded as a shortcut in the Start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



**TIP** We strongly recommend creating a link to the desktop containing the Change Desktop action for testing purposes, so you can change back to your original desktop at any time. This helps you avoid "getting stuck" in the new desktop during testing. To prevent your users from changing to a particular desktop, you can assign 'execute' permissions within the Change Desktop action accordingly.

**NOTE** 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 starting desktop for a user, user profile or station profile:



**NOTE** 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' to this action only for 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.

**NOTE** 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.



---

Note 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")
  - User profile settings
  - User settings
  - Station profile settings
-

# NetMan Actions

## Overview and General Rules

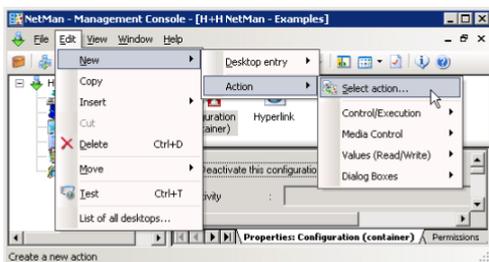
Throughout this manual we have repeatedly mentioned the broad range of possibilities afforded by the variety and number of actions you can add to your NetMan configurations. In this section, we present details on the different types of actions, and point out the convenience of adding other actions to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

NetMan actions are divided into the following categories:

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

As seen in the submenu opened under **File/New/Action**:

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 action, the Program 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 can be used in any combination.

### NOTE

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 a few practical examples involving some of the other actions which might help you to develop ideas for use in your own network.

Actions can generate **return values**; for example, resulting from user input. A return value can be stored in a variable and made available for processing by any or all of the subsequent actions in a given configuration, by defining a **Variable Check** condition to a subsequent action.

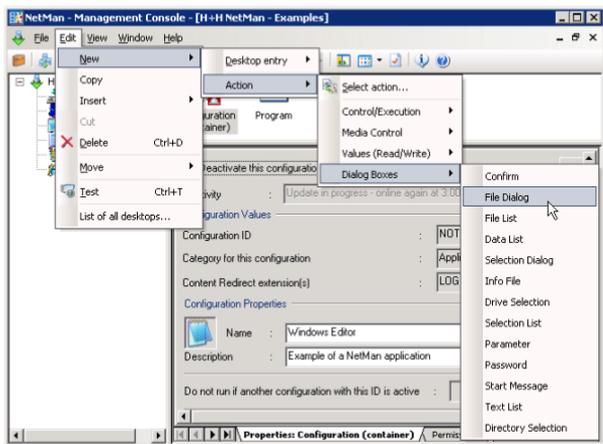
You can also use NetMan's Windows Script interface to integrate your own scripts in NetMan actions.

## Using the Trace Monitor to Check Action Processing

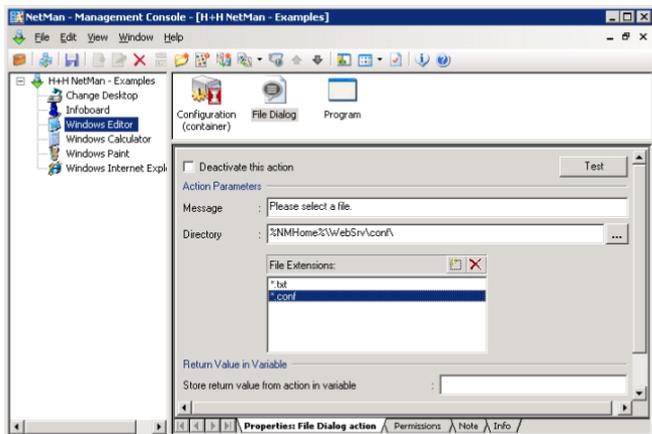
When you launch a NetMan container configuration, the processing of a sequence of actions is initiated. If anything goes wrong, you need a tool that helps you localize and diagnose the problem.

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

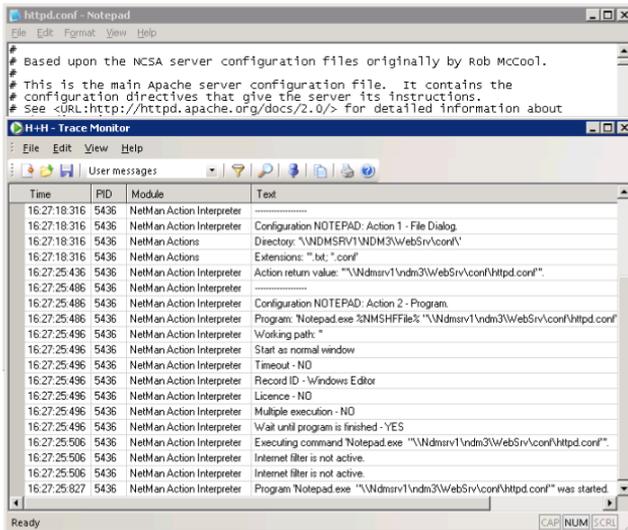
As an example, we shall add a File Dialog action to the **Windows Editor** (ID: NOTEPAD) so that the configuration not only launches the Windows Editor but also opens the “Open File” dialog.



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 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 something like the following output:



Note the text messages in the following:

```
001 Configuration 'NOTEPAD' - name: 'Windows Editor'.
002 Block-ID - Notepad
003 Show info - NO
004 nAppSessionID=1
005 Execute request: 'http://MAC-NDM35/tsinfo/nmwebclt.
    dll?CONFIGID=NOTEPAD'
006 bDualConfig=false
007 -----
008 Configuration NOTEPAD: Action 1 - File Dialog.
009 Directory: '\\MAC-NDM35\NDM3\WebSrv\conf\'
010 Extensions: '*.txt;*.conf'
011 Action return value: "\\Mac-ndm35\ndm3\WebSrv\conf\httpd.
    conf".
012 -----
013 Configuration NOTEPAD: Action 2 - Program.
```

```

014 Program: 'Notepad.exe %NMSHFFile% "\\Mac-ndm35\ndm3\Web-
Srv\conf\httpd.conf"' (->'Notepad.exe "\\Mac-ndm35\ndm3\
WebSrv\conf\httpd.conf"')
015 Working path: ''
016 Start as normal window
017 Timeout - NO
018 Record ID - Editor
019 Licence - Editor
020 Multiple execution - NO
021 Wait until program is finished - YES
022 Waiting for license.
023 Executing command 'Notepad.exe "\\Mac-ndm35\ndm3\WebSrv\
conf\httpd.conf"'

```

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

Check the Help program for details on the options available for the Trace Monitor. These include the following:

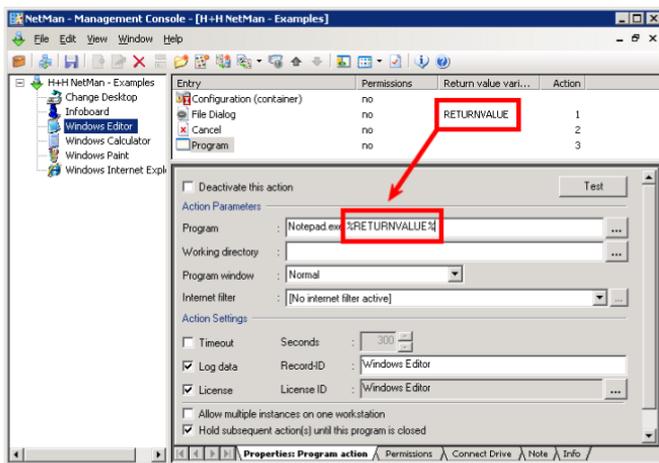
- Filtering output by program component
- Assigning font colors by component so you can identify certain processing steps at a glance
- Defining the level of output; for example, to obtain even more detailed output about certain internal sequences
- Saving output; for example, to append it to a support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

## Controlling an Action Sequence

In the example given in the previous chapter, the name of the selected file was passed to the subsequent Program action. Alternatively, this result can be stored 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 within the NetMan configuration that contains that action. Return value variables can be integrated in later action sequences. If the action is cancelled or fails, the configuration is not necessarily cancelled; the administrator configuring the action can define the response to such events.

Return value variables are both flexible and controllable, in that they can be used at any subsequent point in the action processing sequence and you can control the order in which return values are passed to Program actions. Returning to our Windows Editor 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:

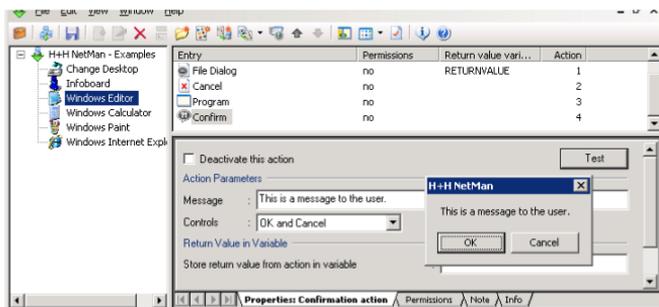


**TIP** We recommend having return values passed directly to subsequent Program actions only in the most basic NetMan configurations. In other cases, the use of return value variables is preferable.

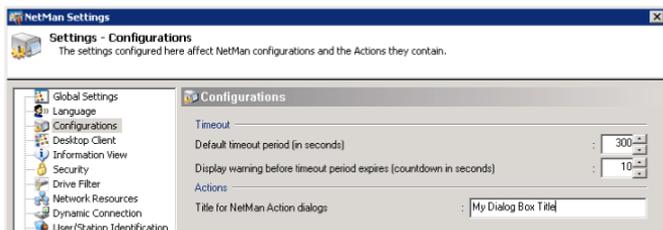
**TIP** You can store a return value in the NetMan environment, for use beyond the scope of the configuration in which it originated, by adding and configuring an **Environment** action.

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.



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 stored 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:**

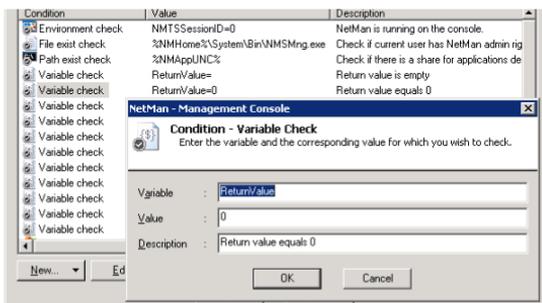
If you define a return value variable, the function of this action changes somewhat. the action returns one of two Boolean values and the sequence of actions in the NetMan configuration continues processing, even if the user selected “No” or “Cancel”.

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

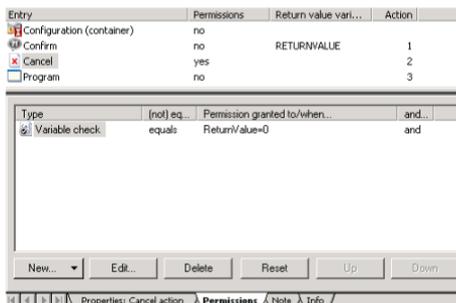
The value returned in the variable can be evaluated by subsequent actions. A **Cancel** or **No** from the user does not stop the NetMan configuration from processing.

Properties: Confirmation action | Permissions | Note | Info

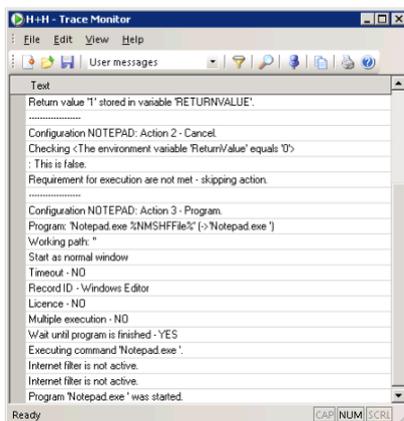
Read the **Info** page for details on available return values. For added control in our current example, we use a predefined Variable Check condition that requires the value “0”.



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



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



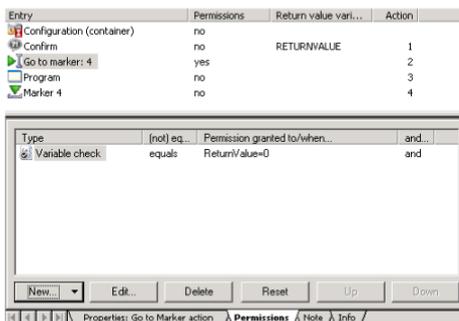
The ‘execute’ permission is evaluated logically: Because the return value is not “0”, permission to execute the **Cancel** action is denied—i.e., the configuration is not cancelled—and the next action is processed.

#### NOTE

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. If you configure a condition that denies ‘execute’ permission to the Password action for users operating under an administrator account, for example, administrators 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** 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, the processing jumps to the end of the configuration and the Program action is skipped entirely.

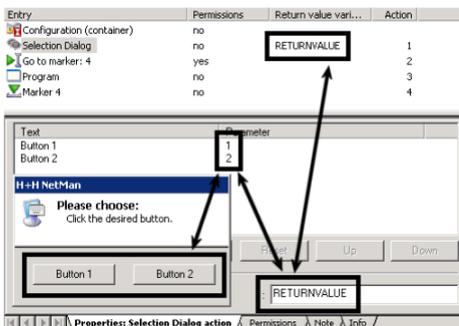


The **Go to Marker** action is very useful for skipping entire series of actions, where you would otherwise have to define ‘execute’ conditions for each action individually. You can also use it to jump back to an action located at an earlier position in the sequence. This lets you create logical loops;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

## Simple Examples of the Most Commonly Used Actions

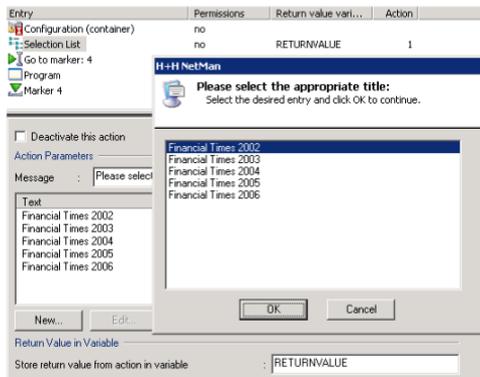
The **Selection Dialog** action is similar to the **Confirmation** action in that it lets you offer the user a choice of responses, in the form of buttons in a dialog.

Each response stores a particular value in the return variable resulting from this action. This value can in turn form the basis for other conditions defined in subsequent actions.

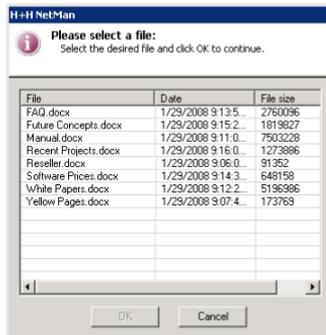


If you want to present the user with more than two options, you might insert a **Selection List** action instead of the **Selection Dialog**; the function is similar, but the choices are pre-

sented 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 sometimes cryptic character strings that are actually passed to the program.



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 user selection. You can define whether this selection window shows the file size, date and/or attributes, and specify the maximum number of files that can be selected:



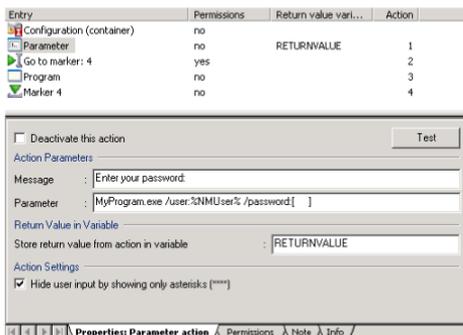
The **Parameter** action opens a dialog for user input which is then passed to the program as command line arguments.

- 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.

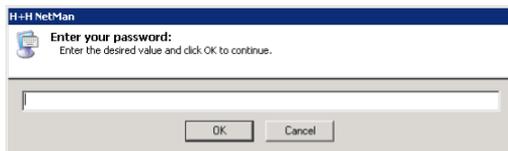
The following example illustrates one possible use of the Parameter action: Say you have a resource for which login is required, entailing input of a user name and a password. A **Password** action is not particularly well-suited for use here, as it serves in an action sequence to determine whether the 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>
```

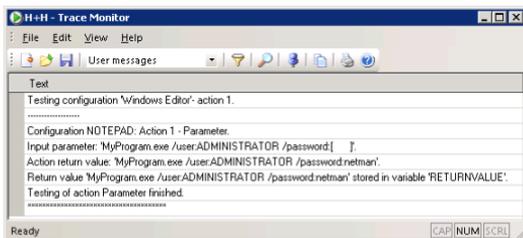
you can configure your Parameter action as follows:



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:

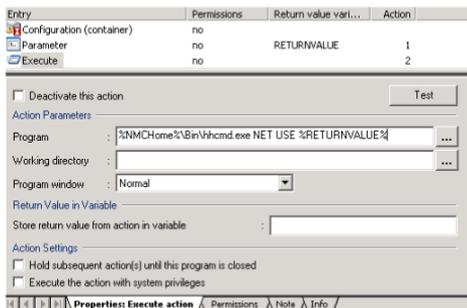


The syntax of the **NET USE** command is similar to that used in the example above:

```
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.

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



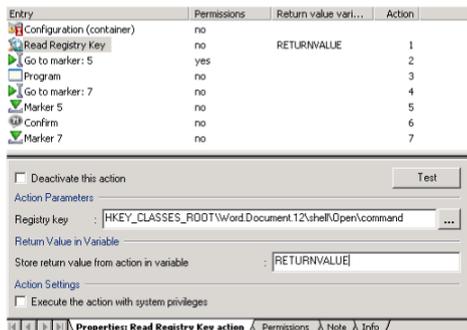
## Complex Actions

For the next example, we return to our MS Word configuration. Let us assume you want to find out where the Microsoft Office directory is located on a given workstation, and then launch MS Word from that directory.

You can configure this sequence as follows:

Entry	Permissions	Return value vari...	Action
Configuration (container)	no		
Read Registry Key	no	RETURNVALUE	1
Go to marker: 5	yes		2
Program	no		3
Go to marker: 7	no		4
Marker 5	no		5
confirm	no		6
Marker 7	no		7

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:

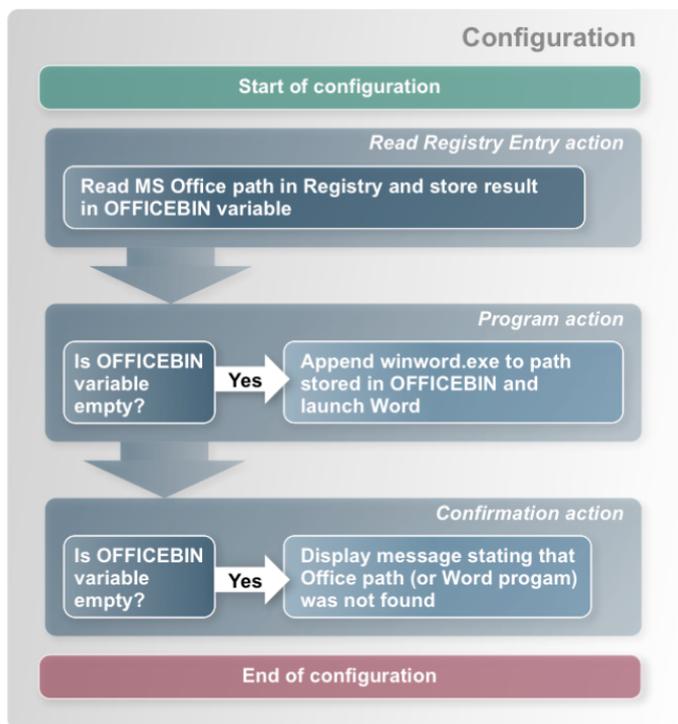


If the path is detected, it is stored in the variable which is used in the program call:

```
%ReturnValue%
```

If the MS 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:



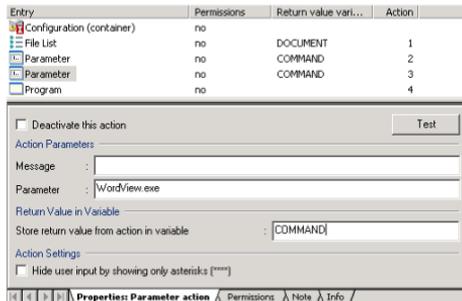
Our "MS Word" configuration clearly demonstrates the logical structure of NetMan container configurations. With one small addition, this can be used to address a particular problem that often comes up in the areas in which NetMan is used:

For this example, let us suppose NetMan is used by an information service in a large enterprise that provides MS Word documents on terminal servers as information sources.

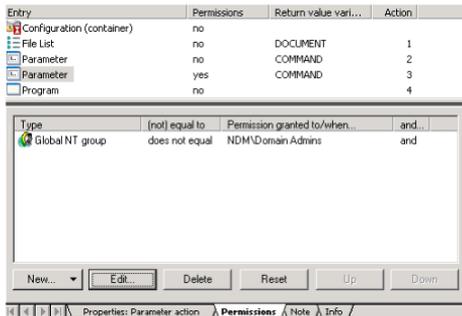
In this case, documents can be provided for selection using File Dialog, File List or other actions.

A Parameter action following file selection determines whether the chosen document is opened with Winword.exe and can be edited by the user, or is opened with WordView.exe in "read-only" mode.

The former variant is applied for members of staff in the Information Services department, and the latter for other users.



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:

- Opening different browsers for different user groups
- Opening the enterprise Web site either in a browser or in an HTML editor (e.g., Front Page)
- Open different programs for a given task, depending on the 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 extends the range of NetMan capabilities 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.

---

**NOTE**            The following information describes NetMan interfaces for Windows Script and is relevant only for 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. The `NMPParamExample.vbs` script provides an example of this. There are a number of sample scripts available on the Internet and in textbook appendices.

```

001  \ *****
002  \ *
003  \ * NetMan Desktop Manager Windows Script Host Interface
004  \ * (c) 2006 H+H Software GmbH
005  \ * VBScript NMPParamExample.vbs
006  \ *
007  \ * About: Sample script, to demonstrate how to pass pa-
008  \ *           rameters
009  \ *           from NetMan actions to a Windows script
010  \ *
011  \ *****
012  \ force explicit variable declaration ...
013  Option Explicit
014
015  \ declare variables ..
016  Dim oShell
017  Dim strParams, strMsgTitle
018  Dim nCounter
019
020  \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.", vbOKOn-
ly, strMsgTitle
034 End If
035
036 Set oShell = Nothing

```

---

Because this is such 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.

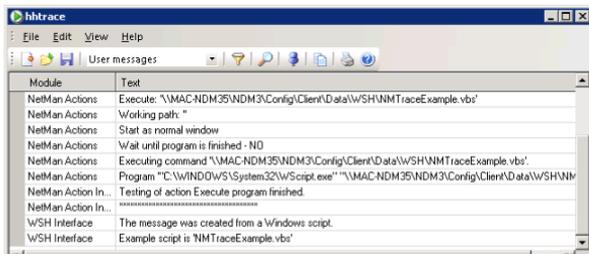
There are three options available for this output:

- 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)
```

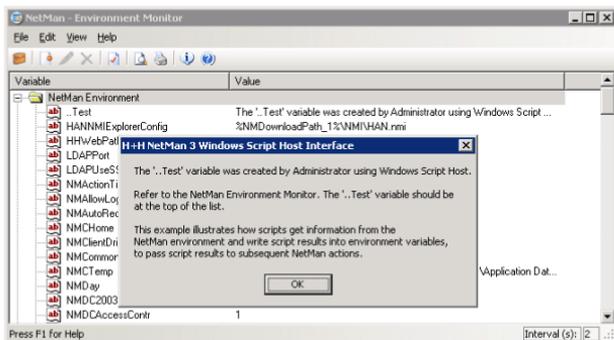
In our example, the **NMUser** and **NMHome** variables are read using **HHEnvGet** and a test variable set in the NetMan environment with **HHEnvSet**:

```
001  ` force explicit variable declaration ...
002  Option Explicit
003
004  `declare 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 oNMEnv = CreateObject("NMEnv.HHComEnv")
013  ` get value of variables NMHome and NMUser ...
014  strNMHome   = oNMEnv.HHEnvGet("NMHome")
015  strNMUser   = oNMEnv.HHEnvGet("NMUser")
016  strMsgTitle = "H+H NetMan 3 Windows Script Host Interface"
017  If strNMHome <> "" Then
018      ` create message ...
019      strMsg = "Your NetMan user name is: " + strNMUser +
020              Chr(10)_
021              + "NetMan home directory is: " + strNMHome +
022              Chr(10) + Chr(10)_
021              + "These variables were read from the NetMan
environment." + Chr(10)_
022              + "Now a new variable ('.test') will be set
in the NetMan environment."
```

```

023     MsgBox strMsg , vbOKOnly, strMsgTitle
024     ` set new variable in NetMan environment ...
025     strMsg = "The `Test..' variable was created by " &
strNMUser & " using Windows Script Host."
026     bRC = oNMEEnv.HHEnvSet("..Test", strMsg)
027     If bRC Then
028         MsgBox strMsg + Chr(10) _
029             + Chr(10) _
030             + "Check the NetMan environment monitor." +
Chr(10) _
031             + "This variable should be the first in the
list." + Chr(10) + Chr(10)_
032             + "This demonstrates how scripts retrieve in-
formation from the NetMan" + Chr(10)_
033             + "environment and store script results in
NetMan environment variables" + Chr(10)_
034             + "pass script results to subsequent NetMan
actions.", vbOKOnly, strMsgTitle
035     Else
036         MsgBox "Error: Unable to write test variable in the
NetMan environment.", vbOKOnly, strMsgTitle
037     End If
038 Else
039     ` strNMHome is empty ...
040     MsgBox "NetMan Desktop Client is either not installed
or not running.", vbOKOnly, strMsgTitle
041 End If

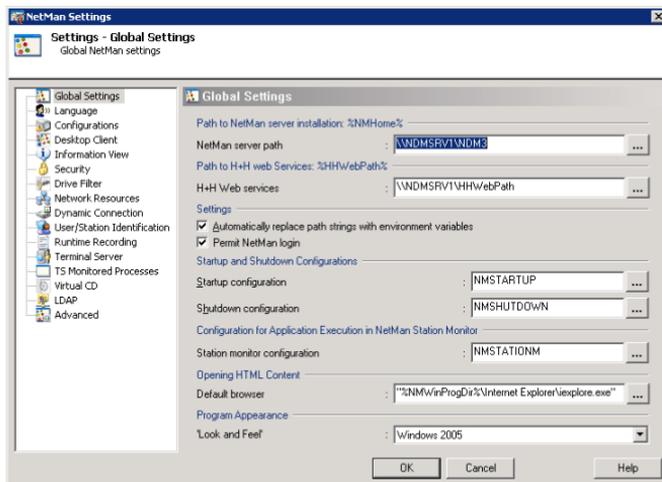
```



# Special Configurations and Applications

## Startup and Shutdown Configurations

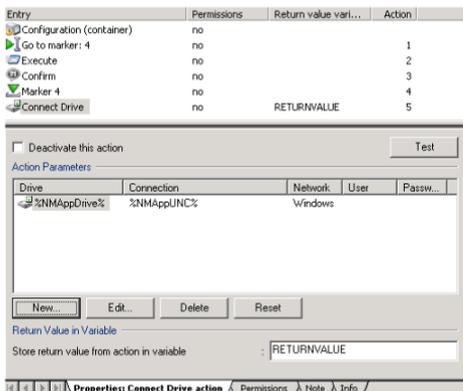
These configurations are not absolutely necessary, but can be quite useful. To create global Startup and Shutdown configurations, simply enter the IDs of the desired configurations in the corresponding fields on the Global Settings page of the NetMan Settings:



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, deactivate or delete this action.

### NOTE

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



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, and the Toolbox is not opened. 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 started every time)
- Set permissions for the Go To Marker action so that the Trace Monitor runs in 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 these 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. As system administrator, you might wish 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. These configurations are processed in that order after any global startup configurations have been processed.

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.

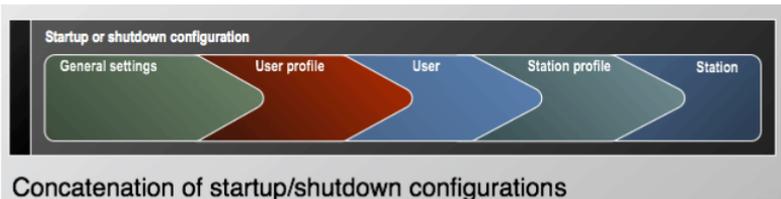
---

**TIP** 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.

---

**NOTE**

You can assign startup and shutdown configurations not only in the **NetMan settings** on the **Global Settings** page, but also in user and station accounts as well as user and station profiles. When more than one startup or shutdown configuration applies to a particular user or station, the order in which the configurations are processed determines which settings are effective on completion of startup or shutdown. The following diagram shows the order in which settings are processed:



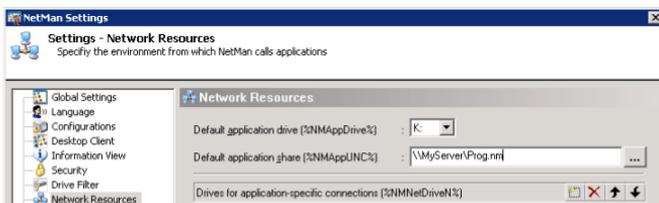
## Integrating CD-ROM-based Applications

A CD-ROM-based application (referred to in the following as a “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, since

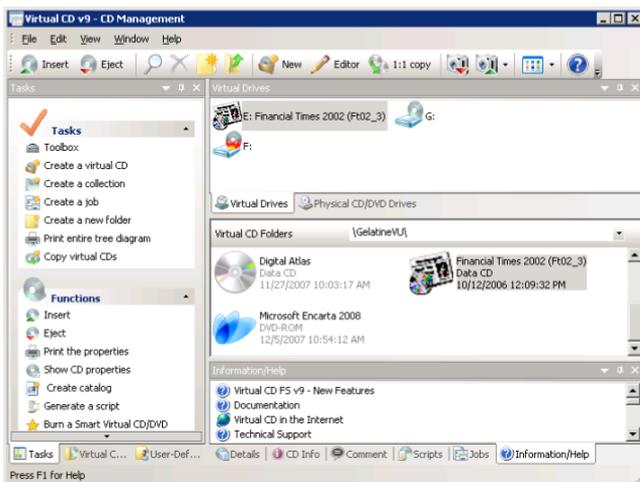
- CD applications often run only from the same drive in which they were installed.
- The drive entered during setup is often stored in the registry, in INI files or in non-editable files, which means it can be changed only by re-installing the program.
- The more CDs belong to a given application, the 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 next example, we demonstrate the installation of a CD application in NetMan. The following parameters apply for this example:

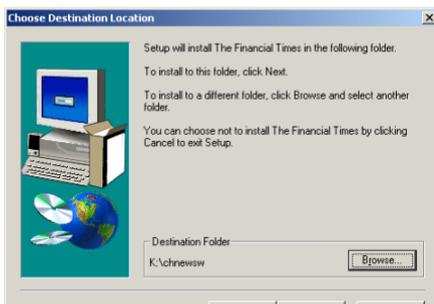
- The application will be installed on K:, the central application drive. Our application drive has already been defined in the NetMan Settings; with these settings, clients access the applications that are installed on the network at K: (**NMAppDrive**).



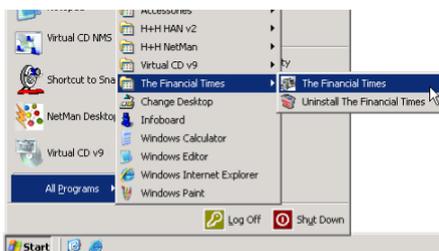
- The Virtual CD program is used to map the CD data. The (virtual) application CD is in the (virtual) F: drive using the Virtual CD Management program:



Now we begin the installation:



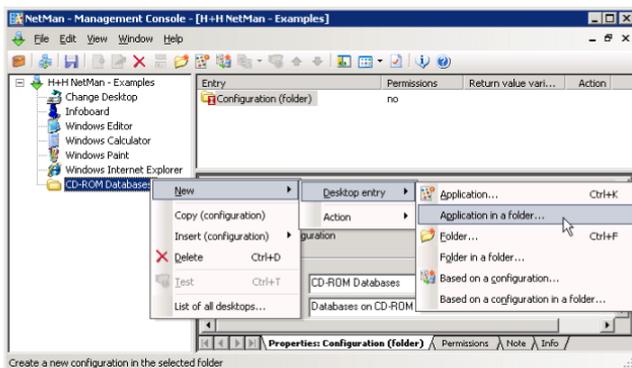
The Setup program offers us the option of specifying the CD drive or searching for the disk. We elect to search for the installation disk, and it is found in the F: drive. The program is then installed on the K: drive and a new entry is added to the Start menu:



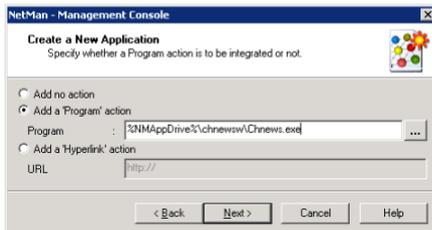
We start the application from here, and find it has no difficulty locating its CD data. Thus the new CD application is ready to use.

The next step is to distribute this application over the network.

We begin by creating an application in the “Databases on CD” folder:



We highly recommend copying the program call from the new link in the Start menu and pasting it into the Program action:

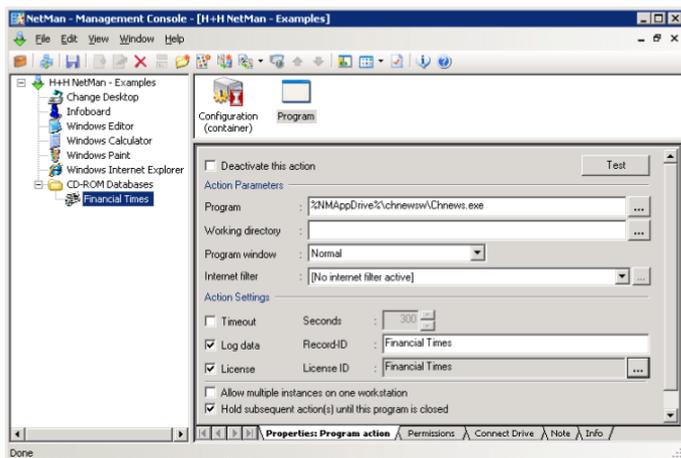



---

**TIP** Copying the program call ensures that the command and any arguments required are entered correctly. Use the same method to enter the working directory, if it differs from the program directory.

---

NetMan automatically converts **K:** to **%NMAppDrive%** in the command line. Our first test of the Program action is successful.

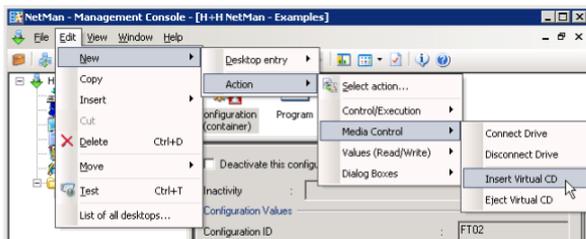


There are still two more functions to be configured:

- 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.

NetMan has two actions specifically designed to support Virtual CD:

- Insert virtual CD
- Eject virtual CD



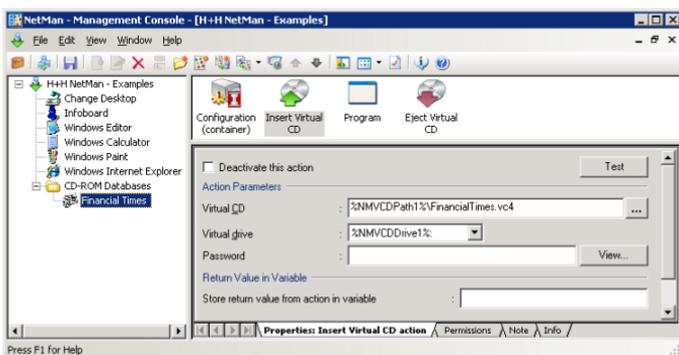
We add these two actions to the configuration, bracketing the Program action. NetMan automatically sets the **NMVCDDrive1** (or **NMVCDDrive2, 3, etc.**) variable(s) on the client workstation in accordance with the Virtual CD drive when the application is launched.

---

**TIP** 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 VCD Client Network setup—so that your (virtual) CDs can use the same drive letter on every station.

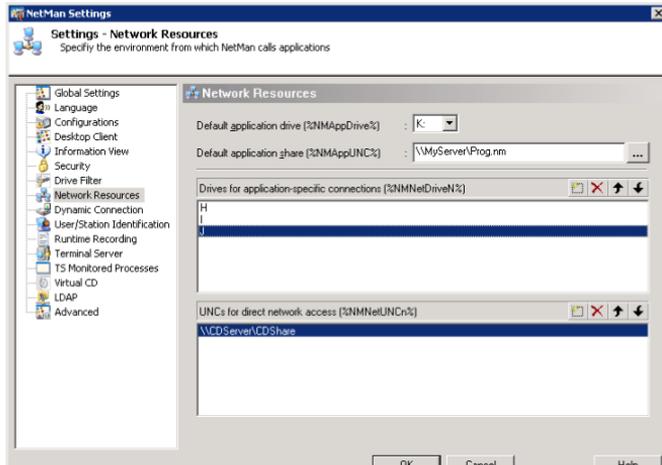
---

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:



**TIP** Remember, 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.

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.

**NOTE** 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.

---

**TIP** 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

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

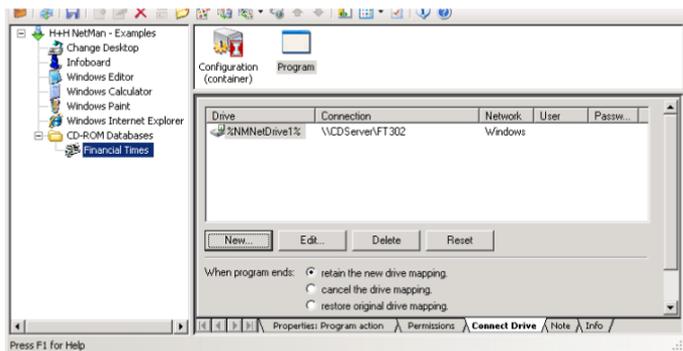
Then you can map a drive before the program starts, using the **NMNetDrive1** variable, to connect the CD to the reserved drive designation.




---

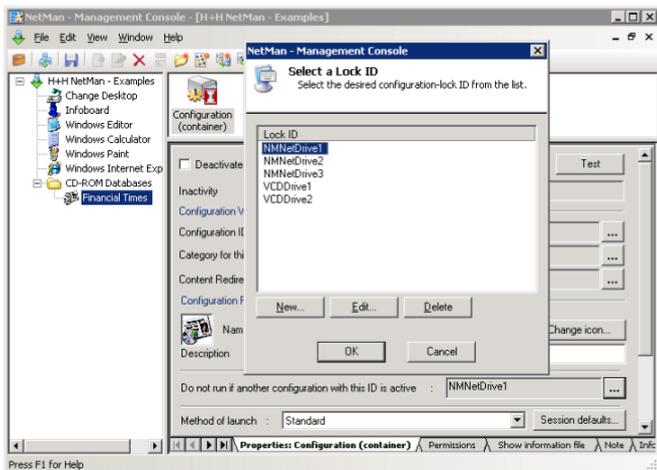
**TIP** Use the drive mapping mechanism integrated in the Program action, as this is much more powerful than the Connect Drive action. The latter is best used for other functions, such as startup and shutdown configurations for example, in which Program actions are not allowed.

---



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.

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



Configurations that have the same lock ID cannot run simultaneously on one machine. With our settings, 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:



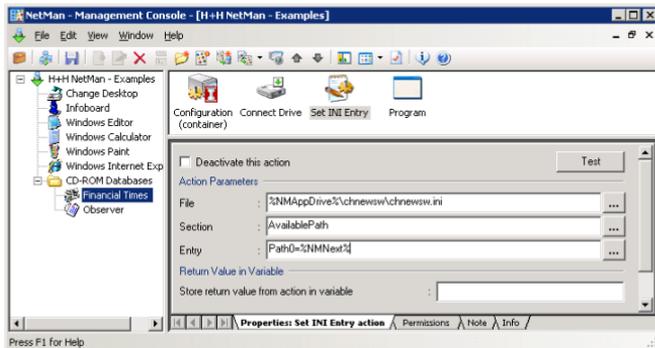
### Example: Mapping a Share to a Specific Drive

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 [DISLOCATION]
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** 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\CDShare\FT302
```

In this case, you require neither a special share for the CD (“CDShare” 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 cases. 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.



## NetMan Desktop Manager Resources

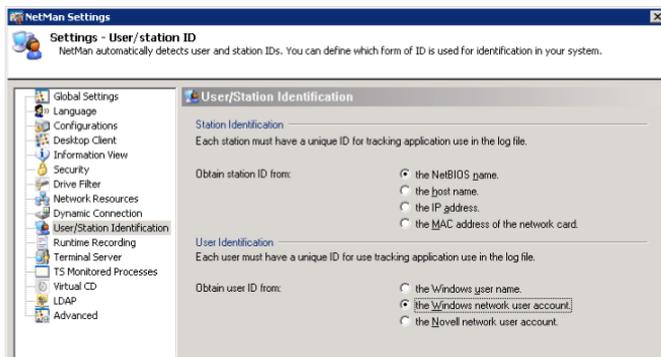




# Users, Stations, Groups and Profiles

The first time you launch NetMan, the users and workstations in your network are automatically added to the NetMan user and station databases. 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:



To view or edit these data records, select the Resources item in the Administration view of the Management Console sidebar:



## NOTE

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

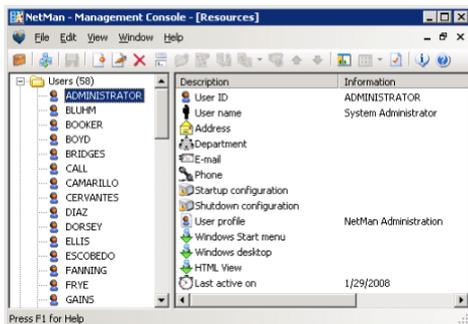
- NetBIOS name:** With this setting, the client name given in RDP or the ICA protocol is used. On Windows workstations, this client name is usually the station's NetBIOS name.
- Host name:** With this setting, the client's IP address is determined and reverse DNS lookup is used to determine the host 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.



## NetMan 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 **domainuser**. 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 screenshot shows the 'NetMan - Management Console' dialog box for editing the 'ADMINISTRATOR' user. The dialog has a title bar 'NetMan - Management Console' and a subtitle 'Users: ADMINISTRATOR' with 'Last active on 1/29/2008'. The form contains the following fields and controls:

- Name:** System Administrator (text field)
- Password:** (text field) with a 'View...' button
- Address:** (text field)
- Phone:** (text field)
- Startup:** (dropdown menu)
- Shutdown:** (dropdown menu)
- Profile:** NetMan Administration (dropdown menu)
- Start menu:** (dropdown menu)
- Desktop:** (dropdown menu)
- HTML View:** (dropdown menu)
- Department:** (text field)
- E-mail:** (text field)
- Maximum parallel terminal server sessions allowed:** 99 (spin box) with a checked 'Overwrite default' checkbox

At the bottom are 'OK' and 'Cancel' buttons.

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.

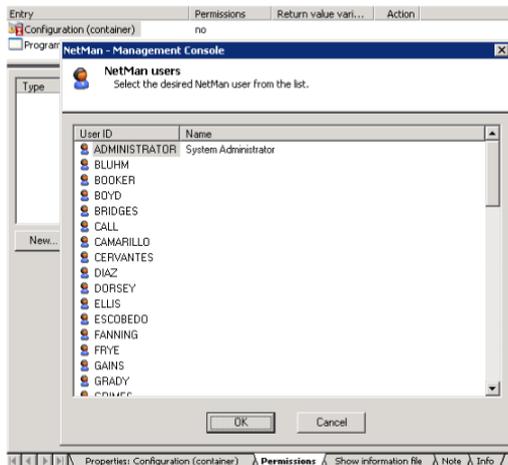
The **Name** you enter here is separate from the user ID; this name is recorded in user lists for statistical evaluation purposes.

---

**NOTE** 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.

---

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

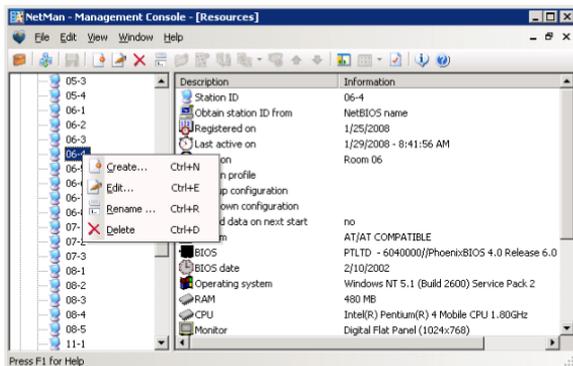
---

# NetMan Stations

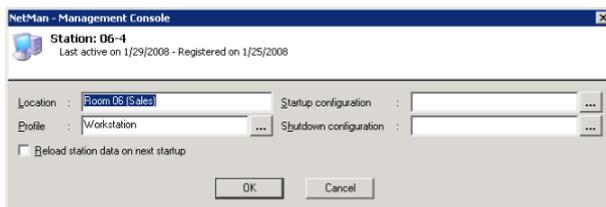
You can create, edit, re-name and delete station data records.

## NOTE

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.



A station data record contains the following fields:



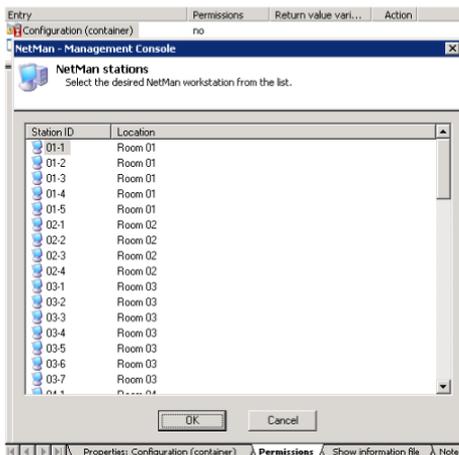
The “Last active on” field in the upper right-hand corner cannot be edited; it is updated every time NetMan runs on this station.

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.

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.

---

#### NOTE

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

---

# NetMan 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.

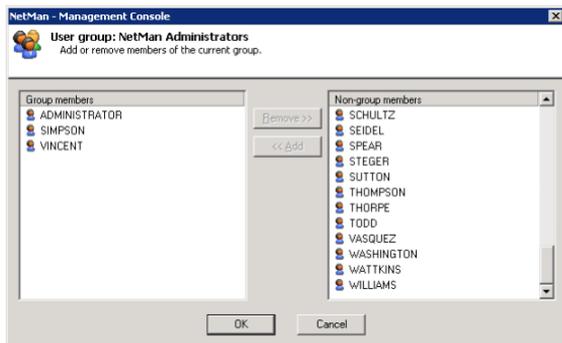
If you find that your existing network groups provide sufficient control over NetMan configurations, then you have no need of NetMan user groups.

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:

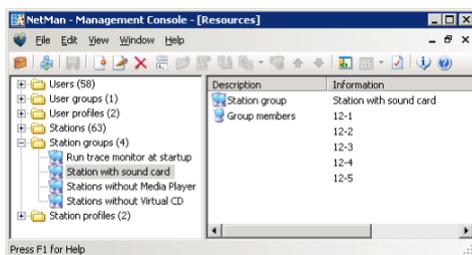




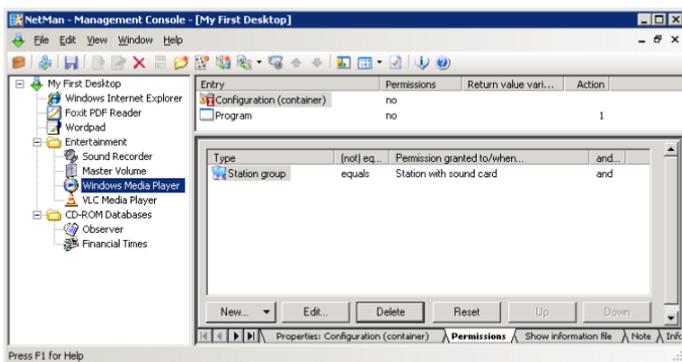
# NetMan Station Groups

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.



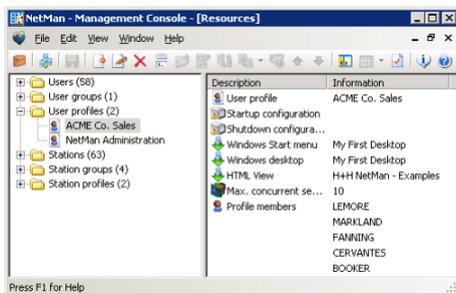
## NetMan User and Station Profiles

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. This is configured on the **Runtime Recording** page of the NetMan Settings.



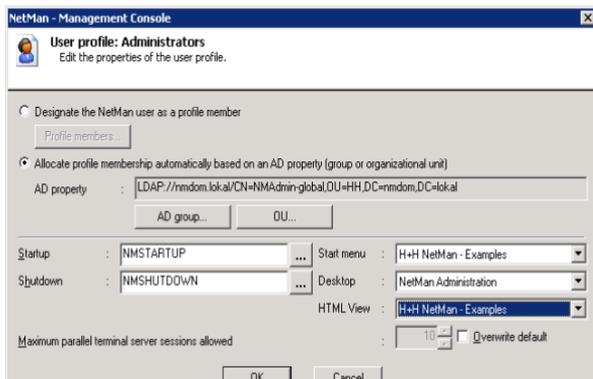
You can create, edit, re-name, and delete NetMan user and station profiles.



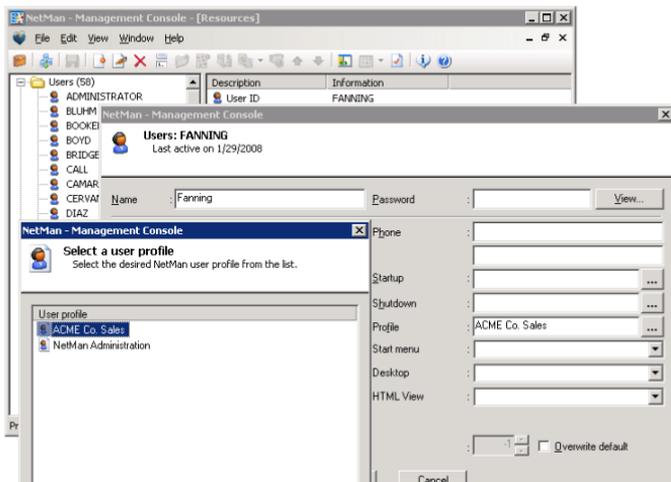
## User Profiles

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:



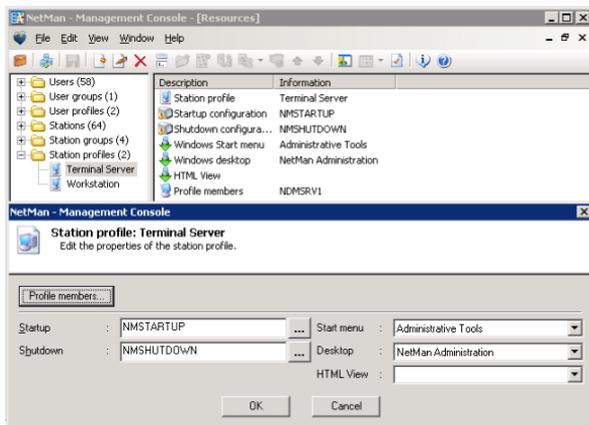
If you wish to add several users to a profile, however, it is easier to do this by editing the profile than by modifying each of the respective user data records. When you assign a user to a profile, any existing membership in another profile is automatically cancelled.

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".

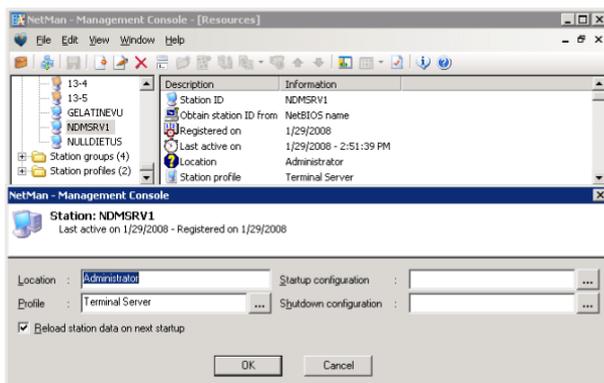


## Station Profiles

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".





Web Interface

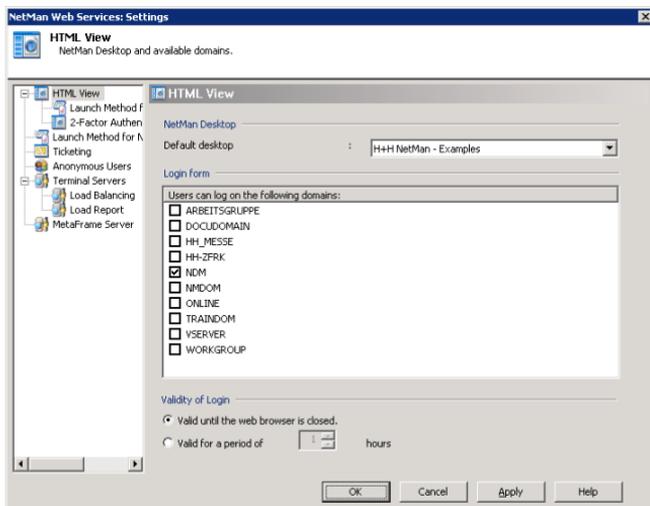




# Introduction to the Web Interface

The section entitled “First Steps with the Web Interface” presented an overview of the web interface and its features. In this section, we take an in-depth look at such topics as configuration and interface design.

The main configuration options are set in the **NetMan Web Services Settings** program. You can open this program from **NetMan Toolbox**.



In the **Default desktop** field, you can specify which NetMan Desktop is presented in the web interface. This setting can be overwritten by settings for users, user profiles and station profiles.

Below that field, in the **Login on the following domains possible** section, you can specify which domains are accessible.

---

**NOTE** If you have only one terminal server, that server is listed here and cannot be deactivated. If you operate more than one server in your installation, the terminal server login is not listed and users must log on to a domain. If you have used two or more servers in the past and now have only one, you need to delete the additional server(s) from this list before you can enable login on the server.

**NOTE** The login form is available only over HTTPS, to ensure secure authentication.

---

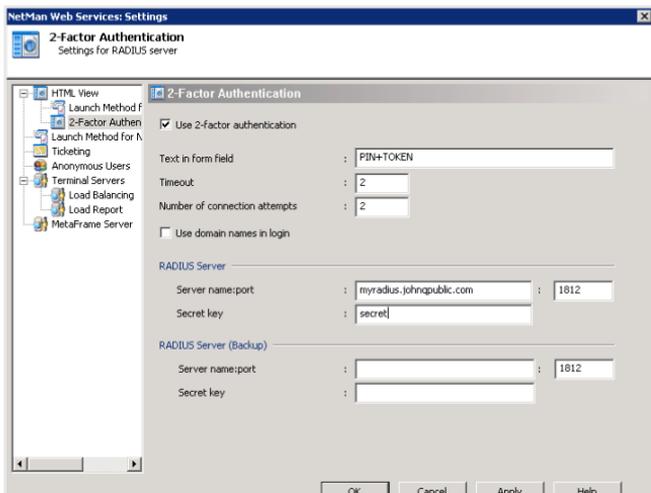


## 2-Factor Authentication

This is another technique for securing your web interface, in addition to mechanisms such as authentication based on user name and password. With 2-factor authentication, users must enter an additional factor for authentication.

NetMan Desktop Manager supports the most common one-time password systems that are RADIUS server-compatible:

- Aladdin
- Secure ID
- Safeword



Once you activate 2-factor authentication, you can define a label for the web interface with which your users are familiar from your OTP system, under “Text in form field.” All other settings apply to the way web services address the RADIUS server.

You can configure both a primary and a backup RADIUS server. The backup server is used any time the first server is inaccessible.

- **Timeout:** The period of time (in seconds) before the next request is sent.
- **Number of connection attempts:** The number of connection attempts per RADIUS server.
- **Use domain names in login:** Defines whether the user name is preceded by the domain name for authentication on the RADIUS server. In other words, this setting defines whether `user name` or `domain\user name` is used for authentication.

---

### NOTE

The PAP protocol is used for authentication on the RADIUS server.

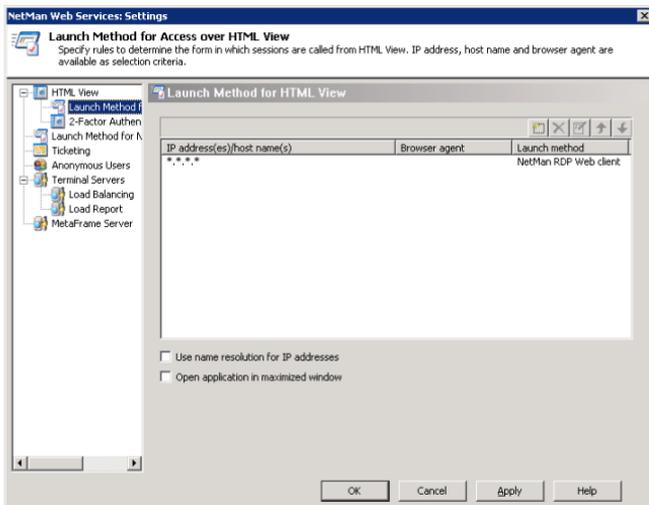
---



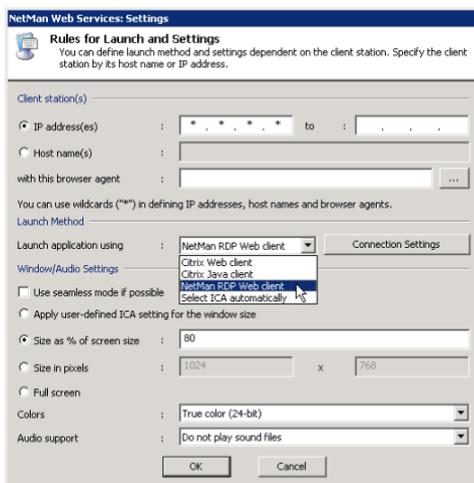
# Launch Methods for HTML View

## Overview of Launch Methods

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.

---

#### NOTE

If you select the Citrix client, both the *NetMan RDP Client* and an ICA client are required on the workstation. The ICA client can be either the *Program Neighborhood* or the *Citrix web client*.

---

The **Rules for Launch and Settings** dialog lets you define a number of properties for the session call. The following sections provide details on the options available here.

## NetMan RDP Web Client

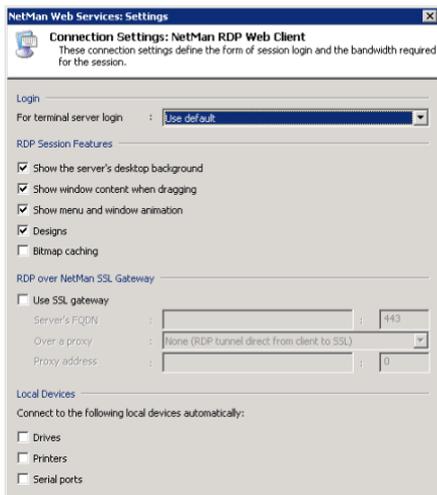
With the **NetMan RDP web client** launch method, the NetMan Web services generate a configuration file for the NetMan RDP Web client, which connects to a terminal server over RDP. This launch method can be called from NetMan Desktop Client and from the web interface, which is also referred to as “HTML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

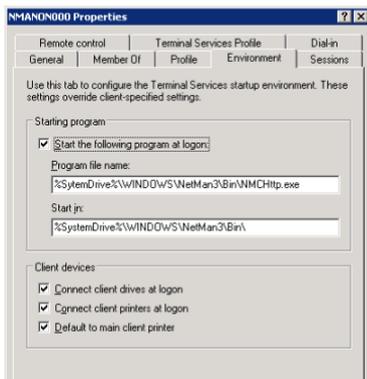
Activate **Use SSL gateway** to have the RDP connection made over a NetMan SSL gateway. In this case, the RDP connection between workstation and SSL gateway is embedded in an SSL tunnel. For a detailed description of the NetMan SSL gateway, please see "Introduction to the NetMan SSL Gateway." In the **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.

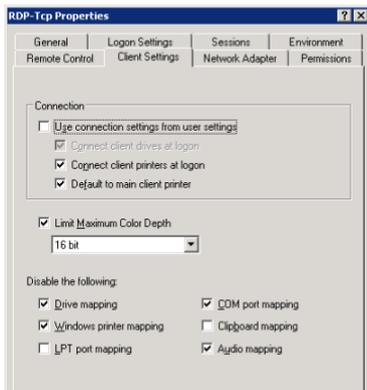
## NOTE

Your settings under **Local Devices** overwrite any analogous settings in the user properties.

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.



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: 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

---

**NOTE** 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.

---

`Standard.ndp`:

```
001 [Connection]
002 Server=@NM_RDP_SERVER
```

```

003 LogonType=@NM_LOGONTYPE
004 Domain=@NM_DOMAIN
005 User=@NM_USER
006 Password=@NM_PASSWD
007 RealUser=@NM_REAL_NAME
008 RealDomain=@NM_REAL_DOMAIN
009 RedirectDrives=@NM_REDIRECT_RDP_DRIVES
010 RedirectPorts=@NM_REDIRECT_RDP_COMPORTS
011 RedirectPrinters=@NM_REDIRECT_RDP_PRINTERS
012 PluginDLLs=TPClnRDP.dll
013 PerformanceFlags=@NM_RDPFLAGS
014 BitmapCache=@NM_RDPBMPCACHE
015 DomainList=@NM_LIST_DOMAIN
016 Ticket=@NM_TICKET
017 Serverlist=@NM_LIST_OF_SERVERS
018 SessionSharing=@NM_SESSION_SHARING
019 @NM_RDP_SSLGATEWAY
020
021 [Application]
022 ;StartApp=%windir%\netman3\bin\hhtrace.exe /L:6
    "/C:nmchttp.exe"
023 StartApp=%windir%\netman3\bin\nmchttp.exe
024 WorkDir=%windir%\netman3\bin\
025 Title=@NM_PROMPT
026
027 [Display]
028 @NM_RDP_DISPLAY

```

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`. In this example, the ThinPrint Engine from the ThinPrint company is integrated. The entry under `StartApp` specifies the program to be executed in the session.

---

**NOTE**

The starting program specified in `StartApp` is not launched if you have defined a program for users or in the RDP connection settings.

---

## rdesktop using a 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 Desktop Manager, 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.

## Java RDP Web Client

The Java RDP Web client launch method is an RDP client implemented as a Java applet. This applet contains the same functions as the NetMan RDP Web Client:

- Session window in full-size mode
- Session window with specified width and height (e.g.,: 1024 x 768 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
- Support for the universal NetMan PDF printer driver
- Support for the SSL gateway

---

### NOTE

This applet does not support direct access to client printers. This is not a serious disadvantage, however, as the universal PDF printer can be used to print to the local printer. This procedure is recommended in particular for use with Mac OS X and Linux clients.

---

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.

```

001  {"server": "@NM_RDP_SERVER",
002  "app_id": "@NM_ID",
003  "logontype": "@NM_LOGONTYPE",
004  "domain": "@NM_DOMAIN",
005  "user": "@NM_USER",
006  "password": "@NM_PASSWD",
007  "realuser": "@NM_REAL_NAME",
008  "realdomain": "@NM_REAL_DOMAIN",
009  "redirectdrives": "@NM_REDIRECT_RDP_DRIVES",
010  "win_screenpercent": "@NM_SCREENPERCENT",
011  "win_width" : "@NM_WIDTH",
012  "win_height" : "@NM_HEIGHT",
013  "Win_Type" : "@NM_WINDOWTYPE",
014  "seamless" : "@NM_SEAMLESS",
015  "bpp" : "@NM_DESIRED_COLORS",
016  "bmcache" : "@NM_RDPBMPCACHE",
017  "perfflag" : "@NM_RDPFLAGS",
018  "sound" : "@NM_SOUND_ICA_OPTIONS",
019  "sharesession" : "@NM_SESSION_SHARING",
020  "title" : "@NM_PROMPT",
021  "command" : "%windir%\netman\bin\nmchttp.exe",
022  "cdir" : "%windir%\netman\bin\",
023  "ticket" : "@NM_TICKET",
024  "use_ssl_gateway" : "@NM_USE_RDP_NM_RDP_SSLGATEWAY",
025  "ssl_gateway_server" : "@NM_RDP_GATEWAY_SERVER",
026  "proxy_type" : "@NM_RDP_PROXY_TYPE",
027  "proxy_server" : "@NM_RPP_PROXY_SERVER",
028  "serverlist" : "@NM_LIST_OF_SERVERS",
029  "archive" : "HHJavaRdp-1.2.21.jar,properJavaRDP-1.2.32.
jar,log4j-1.2.14.jar,java-getopt-1.0.13.jar",
030  "rdesktoparchive" : "HHAppRdesktop-1.0.5.jar"

```

{bmc hinweis\_72.bmp} 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

## Citrix Web Client

With the Citrix web client launch method, NetMan web services send a configuration file for the ICA client, which then connects 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 **Citrix web client** and click on the **Connection Settings** button. This opens the following dialog:

**CITRIX WEB CLIENT**  
These connection settings define the form of session login and the parameters required for contacting the MetaFrame server.

**Login**

For terminal server login : Use default

Published application :

**Server Location**

Network protocol: TCP/IP + HTTP

Address List	
MyMetaFrame:8080	

**Connection Settings**

Use data compression

Cache bitmaps on the hard disk

Buffer all mouse actions and keystrokes

Level of encryption : Basic

**Firewall and Proxy Settings**

Use alternate address for firewall connection

Proxy : None (direct connection)

Proxy address : : 0

**Local Devices**

Connect to the following local devices automatically:

Drives

Printers

Serial ports

### NOTE

This manual does not provide details 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 (with Citrix Secure Gateway in relay mode).

In addition to the native connection between server and client on TCP/IP port 1493, HTML View 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.

---

**TIP** 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 across the campus through a server farm in the media center.

---

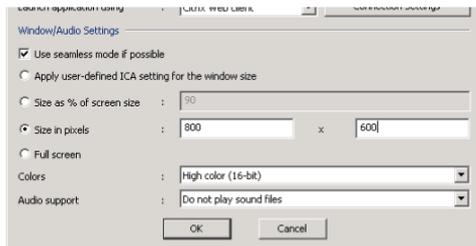


---

**NOTE** Citrix sessions are always called using the published applications mechanism. This technique enables NetMan to support load balancing over ICA. With the default settings, NetMan uses **one** Citrix published application (see "Published Application" under "Extensions for MetaFrame Servers"). Prerequisite for load balancing under Citrix is that all applications are installed on all servers. If this is not possible, you can call the published application in your NetMan configurations. For details, please refer to the section entitled "Separate Session Parameters for an Application Call" under "Special Features for Application Settings."

---

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
- 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

---

#### NOTE

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. In general, however, you will not need to modify the template file.

---

#### Standard.ica

---

```

001 [ApplicationServers]
002 @NM_PROMPT=
003
004 [WFClient]
005 Version=2
006 TcpBrowserAddress=@NM_TCPBROWSER
007 HTTPBrowserAddress=@NM_HTTPBROWSER
008 UseAlternateAddress=@NM_ALTERNATE_ADDRESS
009 CPMAllowed=@NM_REDIRECT_ICA_PRINTERS
010 CDMAllowed=@NM_REDIRECT_ICA_DRIVES
011 COMAllowed=@NM_REDIRECT_ICA_COMPORTS
012
013
014 [@NM_PROMPT]
015 TcpBrowserAddress=@NM_TCPBROWSER
016 HTTPBrowserAddress=@NM_HTTPBROWSER
017 @NM_ICA_DISPLAY

```

```

018 TransportDriver=TCP/IP
019 WinStationDriver=ICA 3.0
020 BrowserProtocol=@NM_BROWSER_PROTOCOL
021 SSLEnable=@NM_ICA_SSL_ENABLE
022 SSLProxyHost=@NM_SSL_PROXY_HOST
023 Compress=@NM_COMPRESS
024 Username=@NM_USER
025 Password=@NM_PASSWD
026 Domain=@NM_DOMAIN
027 UseLocalUserAndPassword=@NM_ICA_USE_LOCALUSERDATA
028 InitialProgram=#"@NM_PUBAPP" @NM_CMDPARAM
029 Address=@NM_PUBAPP
030 WorkDirectory=
031 @NM_SECTION_ENCRYPTION
032 @NM_SECTION_COMPRESS

```

Before the ICA file is sent, NetMan web services replace the @NM... placeholders with specific values.

---

#### NOTE

For details on the values available for these placeholders, please refer to the MetaFrame documentation.

---

## 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\HT-ML-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.

---

#### NOTE

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`.

---

**NOTE** 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.

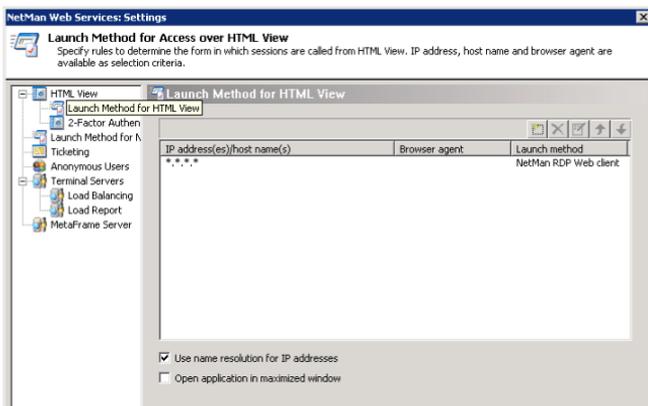
## Select ICA Automatically

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.

## 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:

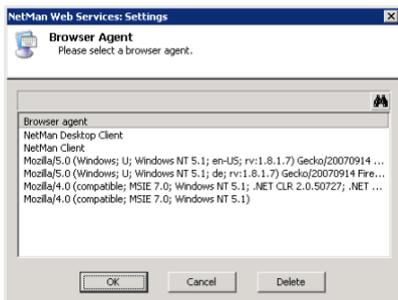


This opens the **Rules for Launch and Settings** dialog, where you can specify the

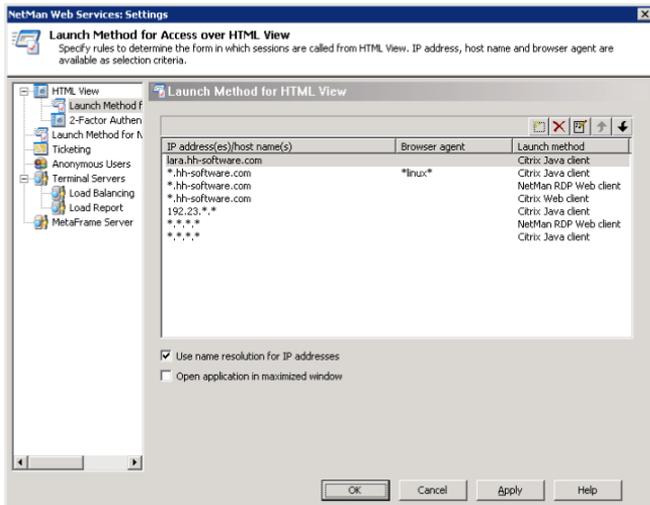
- IP address or host name, and/or
- browser agent of the client station

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.

**NOTE** To use host names in these rules, make sure the **Use name resolution for IP addresses** option is activated.



Here is an 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 “Special Features for Application Settings”) 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 Microsoft RDP web client or NetMan RDP web 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.

---

#### **NOTE**

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.

---



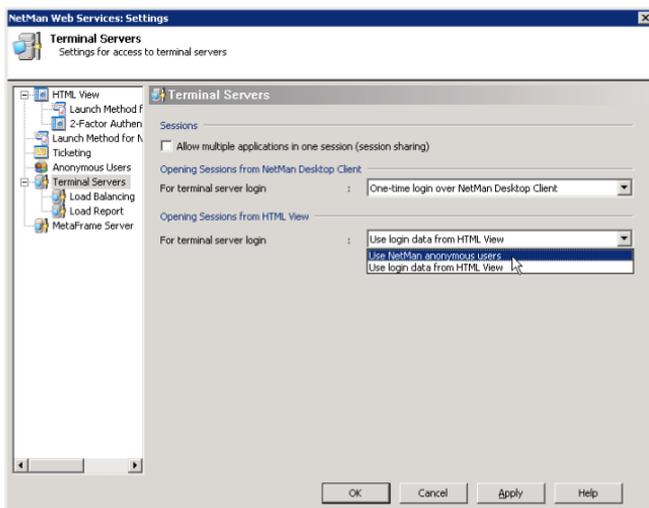
# Login Methods for HTML View

## Overview of Login Methods

Providing access to application sessions is one of the main tasks for NetMan Desktop Manager. 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 Desktop Manager provides a choice of options for authentication:

- Use login data from HTML View
- Use NetMan anonymous users

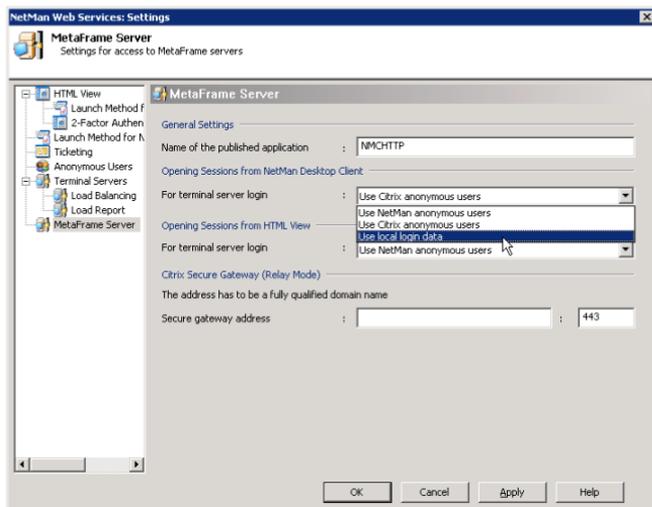
These settings are configured in NetMan web services. Run the NetMan Web Services Settings program from the Toolbox and open the **Terminal Servers** page. Select the desired login method in the **Opening Sessions from HTML View** section.



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 NetMan Desktop Client**:



The different methods are described in detail in the following sections.

## 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. In some cases the user will have to enter additional login data for 2-factor authentication as well. 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.

---

**NOTE** 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.

---

## 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 following sections of this manual.

## Anonymous Users

### Overview

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

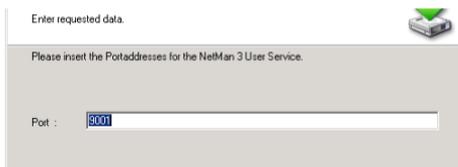
### Installing and Configuring the NetMan User Service

NetMan Desktop Manager offers you the option of working with **anonymous users**. The **NetMan User Service** sets the passwords for anonymous users.

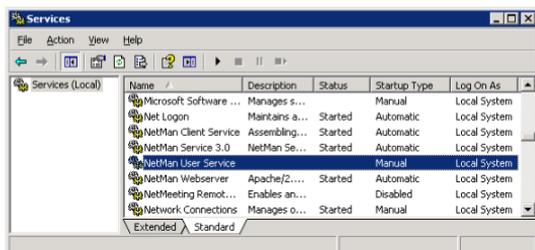
Following installation of NetMan, the `<%NMHOME%\WebSrv\HH\HTML-View\Setup.NetMan User Service` directory contains the setup program for the NetMan User Service.

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.

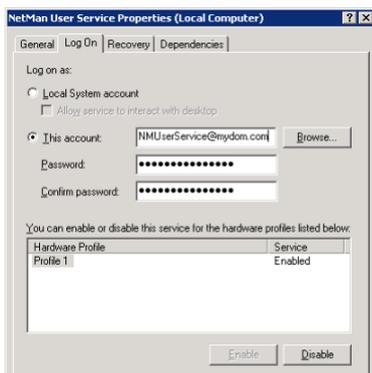
The default is port 9001; this port is usually available on Windows servers.



Once this installation is completed, the NetMan user service is listed under **Services** in your Computer Management program.



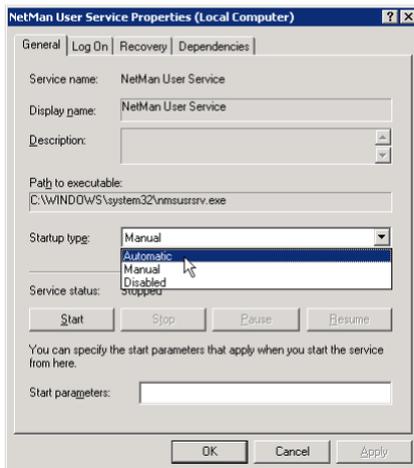
The service startup type is set to **Manual** and it has not been started because the service has not been configured. To ensure that this service has the right to set passwords for **anonymous users**, set up a separate account for this purpose and grant it Account Operator rights in the anonymous accounts. 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:



## NOTE

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.

Now you can change the **Startup Type** on the **General** page from **Manual** to **Automatic** and start the service:




---

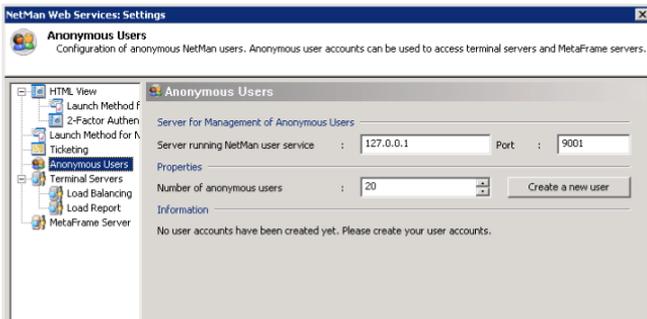
**NOTE** The NetMan User Service uses an NT4 domain interface to set passwords. If you use Active Directory (AD), make sure a PDC emulator is accessible.

---

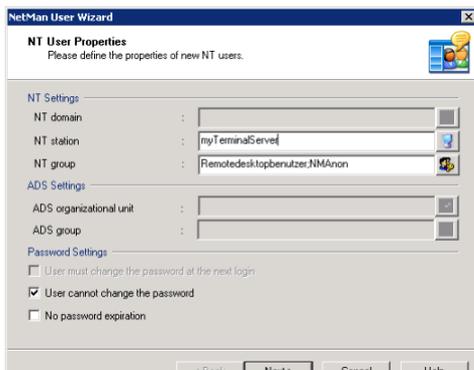
## Initial Setup of Anonymous User Accounts

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,” provides a detailed description of the configuration options for anonymous user accounts.

To set up anonymous user accounts, run the NetMan Web Service Settings program and open the **Anonymous Users** page.



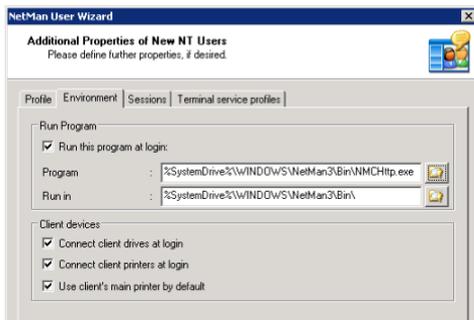
The **Information** section contains a message on the current status of your anonymous user accounts; in this example: “No user accounts have been created yet. Please create your user accounts.” Under **Number of anonymous users** enter the desired total number of anonymous users. The number entered here should not exceed the total number of parallel sessions permitted on the server. Click the **Create a new user** button to open the **User Account Wizard**.



Specify the properties for the users:

- The user accounts are created on the terminal server (in this example, “Terminalserver1”).
- 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.

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.



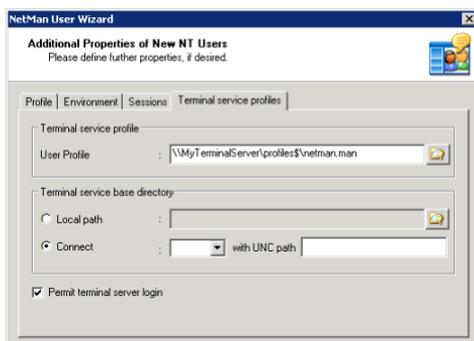
On the **Environment** page, enter `<SystemRoot>\NetMan3\Bin\nmchttp.exe` as the program to run when an anonymous user logs on. This ensures that anonymous

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.”

## Anonymous Users

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.

---

**NOTE**

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,

---

**NOTE**

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**.

The screenshot shows the 'NetMan User Wizard' dialog box. The title bar reads 'NetMan User Wizard'. The main title is 'NT User Properties' with the subtitle 'Please define the properties of new NT users.' Below this, there are three sections: 'NT Settings', 'ADS Settings', and 'Password Settings'. Under 'NT Settings', there are three fields: 'NT domain' (empty), 'NT station' (containing 'myTerminalServer'), and 'NT group' (containing 'Remotedesktopbenutzer:NMAnon'). Under 'ADS Settings', there are two fields: 'ADS organizational unit' (empty) and 'ADS group' (empty). Under 'Password Settings', there are three checkboxes: 'User must change the password at the next login' (unchecked), 'User cannot change the password' (checked), and 'No password expiration' (unchecked).

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:

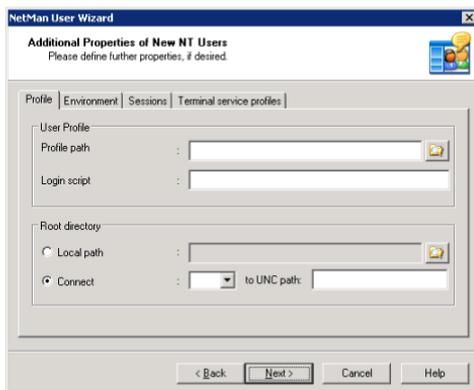
- **NT domain:** To create the user accounts in an NT4 domain, enter the domain here.
- **NT station:** If you use only one terminal server, you can create the anonymous user accounts in the server's local database. To do this, enter the name of the terminal server here.
- **NT group:** The anonymous 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 termi-

nal 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.

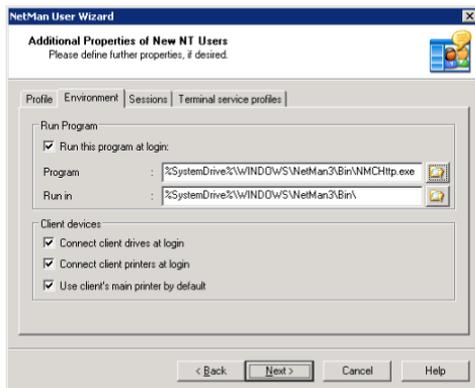
The password settings are made available here because passwords are set automatically by the NetMan User Service, and generally do not need to be—and should not be—changed by the user.

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\nmchtp.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:

---

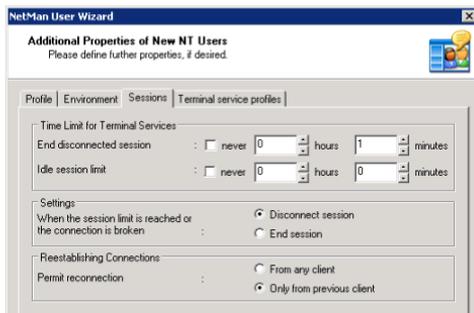
**NOTE**      **Connect client drives at logon:** This setting is applied only in sessions that use the ICA protocol. All local drives on the workstation are automatically connected within the session.

**NOTE**      **Connect client printers at logon:** All printers used by the workstation are automatically connected within the session.

**NOTE**      **Default to main client printer:** With this setting, the main printer as configured on the workstation is the default printer for the session.

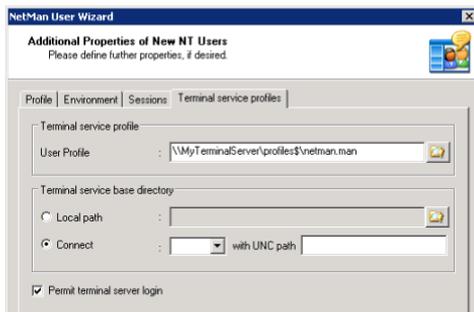
---

On the **Sessions** page, you can configure a number of session properties:



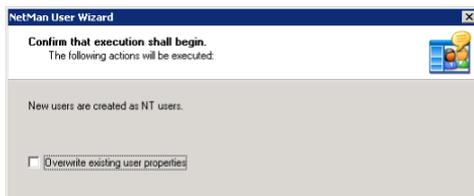
For example, you can define how long the session remains active when not in use. When the defined period has elapsed (“Idle session limit”) the session is disconnected or ended. You can also define what happens when a session is disconnected. Specifically, you can define whether the session can be re-connected 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.

---

**NOTE**

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.

---

# NetMan SSL Gateway

## Introduction to the NetMan SSL Gateway

The NetMan SSL gateway is an additional software component of NetMan Desktop Manager. NetMan SSL Gateway runs on Windows Server 2003 and acts as the connection point between the terminal server and remote clients.

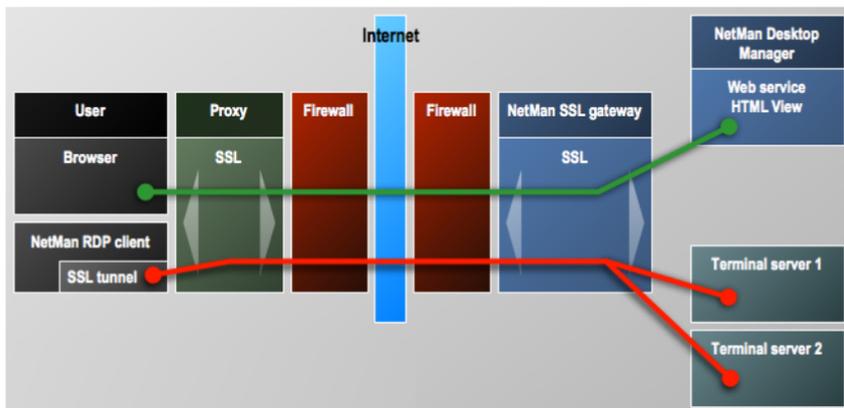
You can use any browser within your company to access the web interface directly and open RDP sessions. Generally, RDP traffic does not require additional encryption in this scenario.

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 as described under “First Steps with the Web Interface.”

The following diagram illustrates the function of the NetMan SSL gateway:



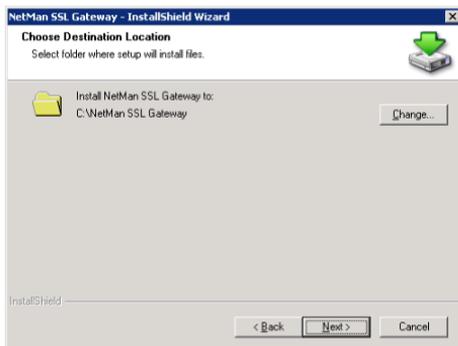
- When a user accesses the SSL gateway with a browser, the HTML View user interface is displayed. The NetMan SSL gateway is a proxy for HTML View and uses HTTPS for communication with client browsers and with HTML View.
- The gateway decrypts the RDP data traffic between itself and clients, and sends 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.

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.



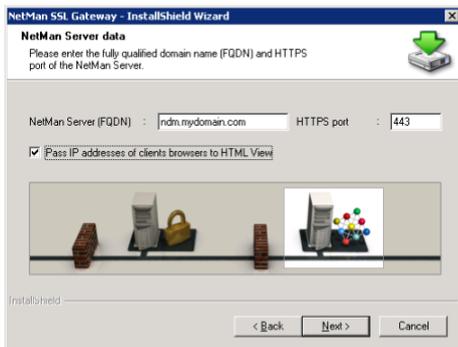
Next, you need to define the HTTPS port. The NetMan SSL gateway uses this port for external connections. We recommend using port 443, because firewalls usually permit remote HTTPS access over proxies only on this port.



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.

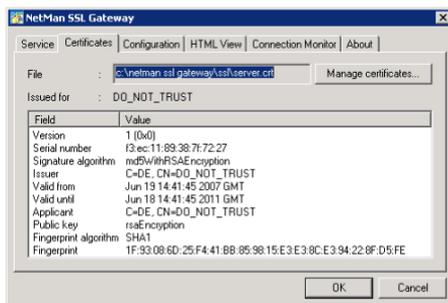


**NOTE** Make sure the server has the capacity to handle transmission of all RDP connections over the NetMan SSL gateway. If necessary, you can install NetMan SSL Gateway on other servers as well and use load balancing, for example, with round-robin DNS resolution. Alternatively, you could install hardware load balancers.

**NOTE** 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.

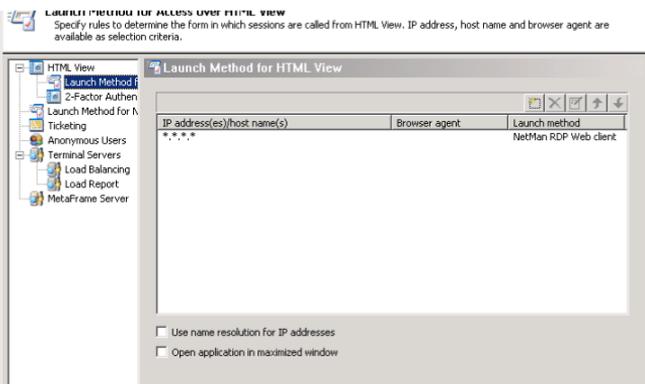
---

### NOTE

Please note that the NetMan SSL gateway must be entered on the client stations in the settings for remote connections as follows.

---

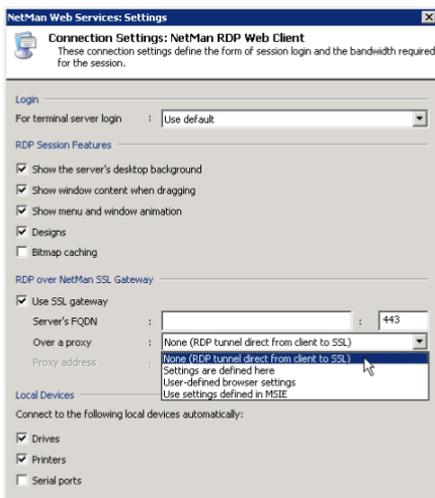
**STEP 1** Open the web service settings from the Toolbox and select the **Launch Method for HTML View** page. Since the following example assumes that all terminal server sessions are executed over the NetMan SSL gateway, open the default “\*.\*.\*.\*” rule for editing (double-click on the rule, or select it and click on the “Edit” button).



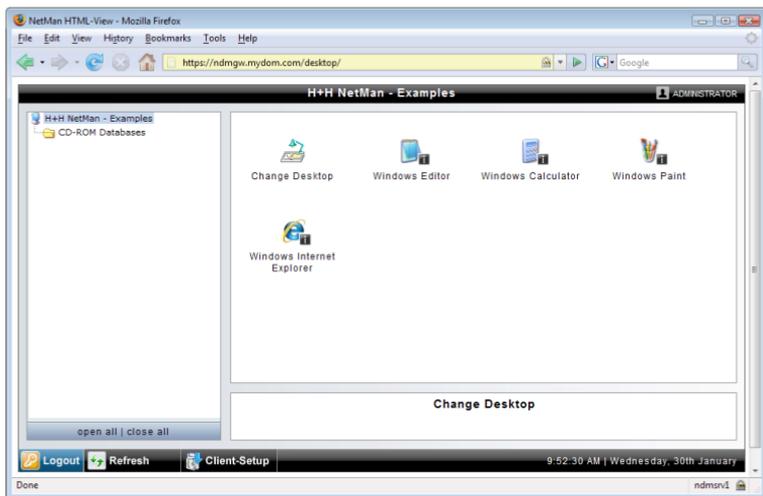
**STEP 2** Click on the **Connection Settings** button to open the dialog of the same name, and activate the **Use SSL gateway** option. In the **Server's FQDN** field, enter the fully qualified name of your NetMan SSL gateway. The port number is usually 443. In the **Over a proxy** field, you can define whether the RDP connection goes over a proxy and, if so, which settings are used. The following options are available:

- **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)**.



**STEP 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.



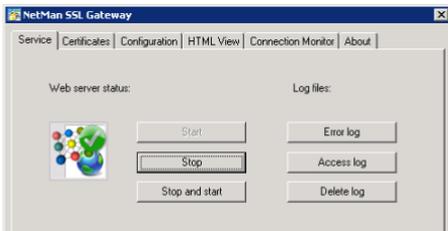
**NOTE** The **Settings** program is not shown in the web interface unless the client workstation configuration under **RDP over NetMan SSL Gateway** is set to **User-defined browser settings**.

**NOTE** 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.”

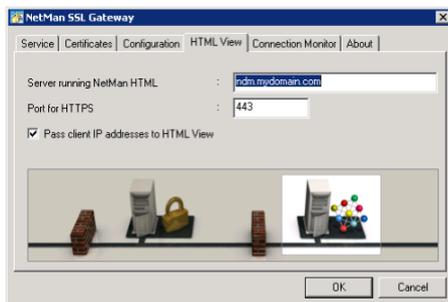


On the **Configuration** page, you can change the **port** on which NetMan SSL accepts external requests over HTTPS. We strongly recommend keeping the default setting, port 443, because a number of firewall products permit access over HTTPS only on this port. You can also specify an IP address for binding 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.



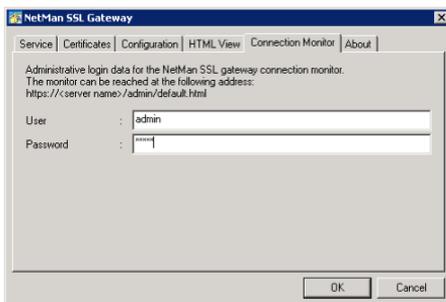

---

**NOTE** 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.

**NOTE** 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 the next section of this manual.

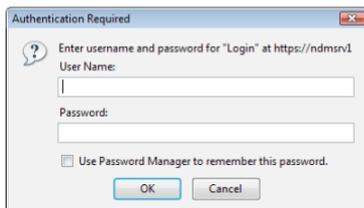
## NetMan SSL Gateway Connection Monitor

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**




---

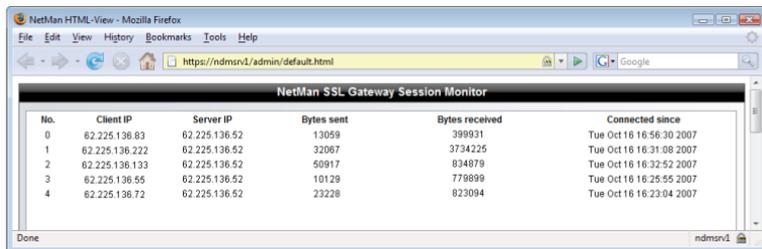
### NOTE

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	62.225.136.83	62.225.136.52	13059	399931	Tue Oct 16 16:56:30 2007
1	62.225.136.222	62.225.136.52	32067	3734225	Tue Oct 16 16:31:08 2007
2	62.225.136.133	62.225.136.52	50917	834879	Tue Oct 16 16:32:52 2007
3	62.225.136.55	62.225.136.52	10129	778989	Tue Oct 16 16:25:55 2007
4	62.225.136.72	62.225.136.52	23228	823094	Tue Oct 16 16:23:04 2007

## NOTE

In the "Refresh" field, you can define the intervals at which the monitor's display is updated.



# Web Interface Design

## Introduction to Web Interface Design

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.

## 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 following excerpt is from login.htm.en:

---

```

001 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transition-
002   al//EN">
003 <html>
004   <head>
005     <title>NetMan Login</title>
006     <meta http-equiv="Content-Type" content="text/html; ISO-
007       8859-1">
008     <link href="hh.css" rel="stylesheet" type="text/css">
009     <link href="hh-login.css" rel="stylesheet" type="text/
010       css">
011     <script language="javascript" src="hhlib.js"></script>
012   </head>
013   <body onLoad="show_clock()">
014     <div id="fenster">
015       <div id="header">
016         <p>Login</p>
017       </div>
018       <div id="image_box">
019         
020       </div>
021       <div id="content_box">

```

```

019     <p class="hello">Welcome</p>
020     <div id="form-zeile">
021         <H2>Login not possible.<br>Please make sure JavaScript
and cookies are enabled in your browser.</H2>
022     </div>
023 </div>
024 <script type="text/javascript">getSettings();</script>
025 <div id="footer">
026     <p><script language="javascript" src="liveclock.js"> </
script></p>
027 </div>
028 </div>
029 <p id="claim">powered by NetMan</p>
030 </body>
031 </html>

```

The `hh.css` and `hh-login.css` files are the cascading style sheets that determine the format of the login page.

The `hhlib.js` (or `hhlib.js.de`) 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.

## Example of Login Page Modification

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 `<img>` 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>
...

```

The result might look like this:



## 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`).

---

**NOTE** 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 `default.html.en` (or `default.html.de`) file provides a frameset that refers to three frames:

- `apps.html` contains the interface for starting the application
- `stopApplet.html` is an invisible frame that removes applets from the DOM structure once they have been closed.
- `listApplets.html` lists the applets that have been started.

When designing your interface, modify only the `apps.html`.

The `listApplets.html` and `stopApplet.html` files should remain unchanged.

The apps.html.en file contains the following:

```
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 <body onLoad="show_clock()">
012   <div id="window_box">
013     <div id="header">
014       <!--<p>Desktop title</p>-->
015     </div>
016     <div id="content_box">
017       <div id="content">
018         <!-- table of applications -->
019         <div id="netmanapps">
020           <h2>Please make sure JavaScript and cookies are en-
abled in your browser.</h2>
021         </div>
022         <!-- end of application table -->
023       </div>
024     </div>
025     <div id="info_box">
026       <div id="info">
027         <!-- detail information for each app -->
028         <h2>You can provide information about the application
here.</h2>
029         <!-- end of detail information -->
030       </div>
```

```

031 </div>
032 <div id="tree_box">
033   <div id="netmantree">
034 </div>
035 <div id="mainlink">
036   <p><a href="javascript: d.openAll();">open all</a> | <a
href="javascript: d.closeAll();">close all</a></p>
037 </div>
038 </div>
039 <div id="footer">
040   <div id="datetime">
041     <p><script language="javascript" src="liveclock.js"> </
script></p>
042 </div>
043 <div id="footermenu"></div>
044 </div>
045 </div>
046 <p id="claim">powered by NetMan</p>
047 <script type="text/javascript">
048   var d = new dTree(,d');
049   sendSearchReq();
050 </script>
051 </body>
052 </html>

```

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 next example shows how to adapt the HTML page for launching applications.

## Simple Modifications to the Application Launch Page

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 <body onLoad="show_clock()">
012 <p id="claim"></p>
013 <div id="window_box">
014 <div id="header">
015 <!--<p>Desktop title</p>-->
016 </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 as follows:

```
...
010 #content_box {
011     width: 654px;
012     height: 425px;
013     border: 1px solid #8c8c8c;
014     background-color: #ffffff;
015     position: absolute;
016     right: 10px;
017     top: 34px;
018 }
019 #content {
020     width: 652px;
021     height: 423px;
022     overflow: auto;
023     text-align: left;
024     position: absolute;
025     right: 0;
026     top: 0;
027 }
...
040 #info_box {
041     width: 654px;
042     height: 60px;
043     width: 0px;
044     height: 0px;
045     border: 1px solid #8c8c8c;
046     background-color: #ffffff;
047     position: absolute;
048     right: 10px;
049     bottom: 40px;
050 }
051 #info {
052     width: 652px;
```

```
053 height: 58px;
054 overflow: auto;
055 text-align: left;
056 position: absolute;
057 right: 0;
058 top: 0;
059 }
```

---

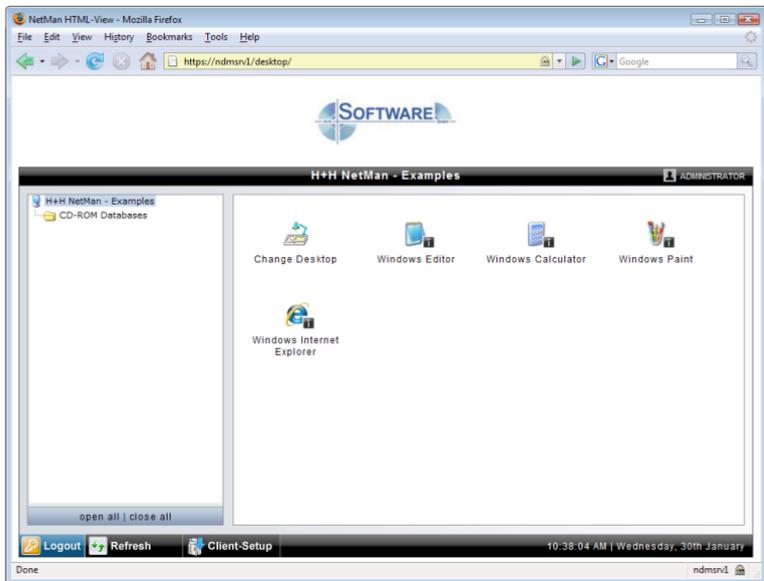
These lines are changed as shown below, with the result that the area showing application titles and descriptions is no longer shown and the area listing the applications is larger:

---

```
010 #content_box {
011     width: 654px;
012     height: 495px;
013     border: 1px solid #8c8c8c;
014     background-color: #ffffff;
015     position: absolute;
016     right: 10px;
017     top: 34px;
018 }
019 #content {
020     width: 652px;
021     height: 493px;
022     overflow: auto;
023     text-align: left;
024     position: absolute;
025     right: 0;
026     top: 0;
027 }
040 #info_box {
041     width: 0px;
042     height: 0px;
043     border: 0px solid #8c8c8c;
044     background-color: #ffffff;
045     position: absolute;
```

```
046     right: 10px;
047     bottom: 40px;
048 }
049 #info {
050     width: 1px;
051     height: 1px;
052     overflow: auto;
053     text-align: left;
054     position: absolute;
055     right: 0;
056     top: 0;
057 }
058 }
```

The result is shown in the following browser window:







## Opening Sessions from NetMan Desktop Client

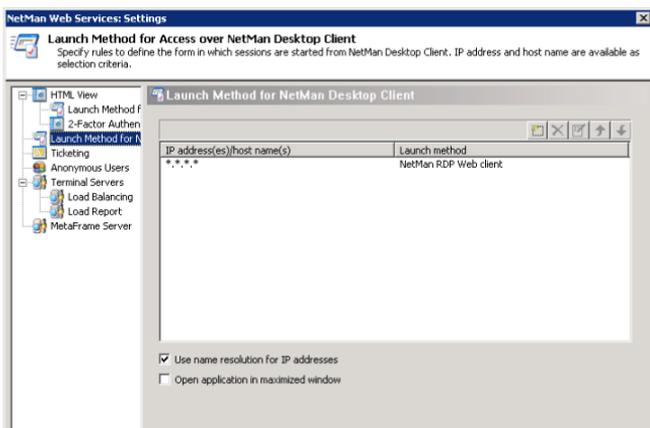




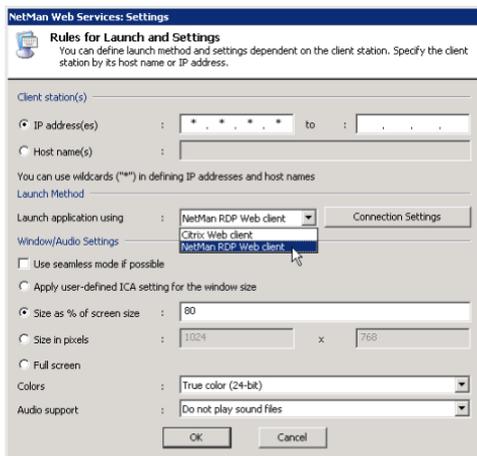
# Launch Methods for NetMan Desktop Client

## Overview of Launch Methods

The **NetMan web services** provided in your NetMan Desktop 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.

## NOTE

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*.

The Rules for Launch and Settings dialog lets you define a number of properties for the session call. The following sections provide details on the options available here.

## 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:

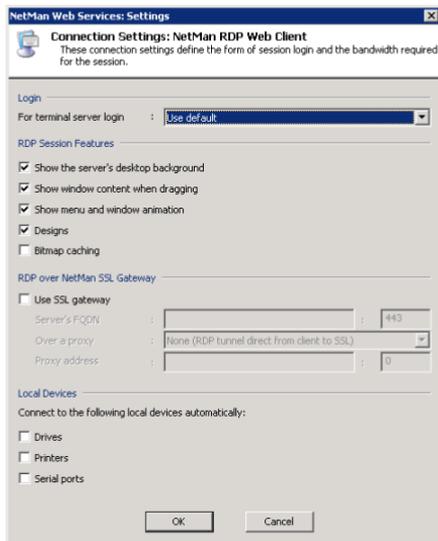
The settings options are divided into three categories:

- **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:

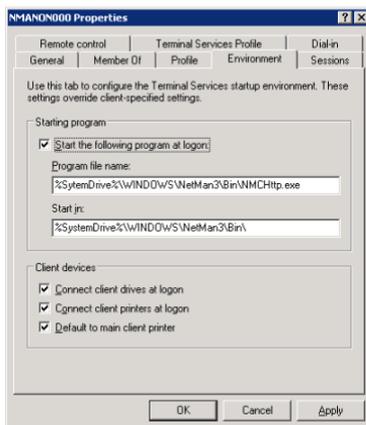
- **Drives:** Automatically connect local drives.
- **Printer:** Automatically connect local printers.
- **Serial ports:** Automatically connect local serial ports.

---

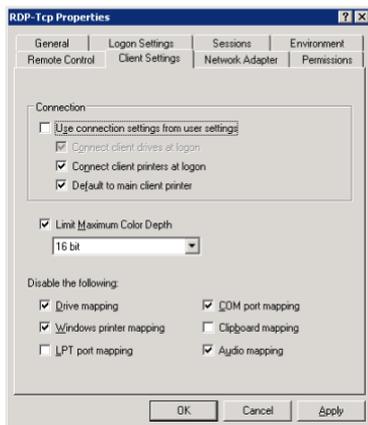
## NOTE

Your settings under **Local Devices** overwrite any settings for these features configured in the user properties.

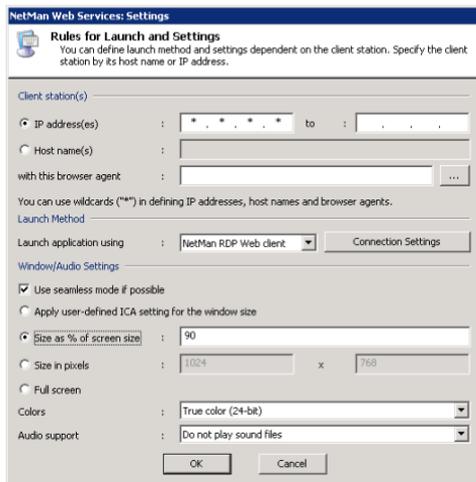
---



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

---

**NOTE** 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.

---

Standard.ndp:

```

001 [Connection]
002 Server=@NM_RDP_SERVER
003 LogonType=@NM_LOGONTYPE
004 Domain=@NM_DOMAIN
005 User=@NM_USER
006 Password=@NM_PASSWD
007 RealUser=@NM_REAL_NAME
008 RealDomain=@NM_REAL_DOMAIN
009 RedirectDrives=@NM_REDIRECT_RDP_DRIVES
010 RedirectPorts=@NM_REDIRECT_RDP_PORTS
011 RedirectPrinters=@NM_REDIRECT_RDP_PRINTERS
012 PluginDLLs=TPClnRDP.dll
013 PerformanceFlags=@NM_RDPFLAGS
014 BitmapCache=@NM_RDPBMPCACHE
015 DomainList=@NM_LIST_DOMAIN
016 Ticket=@NM_TICKET
017 Serverlist=@NM_LIST_OF_SERVERS
018 SessionSharing=@NM_SESSION_SHARING
019 @NM_RDP_SSLGATEWAY
020

```

```

021 [Application]
022 ;StartApp=%windir%\netman3\bin\hhtrace.exe /L:6
    "/C:nmchttp.exe"
023 StartApp=%windir%\netman3\bin\nmchttp.exe
024 WorkDir=%windir%\netman3\bin\
025 Title=@NM_PROMPT
026
027 [Display]
028 @NM_RDP_DISPLAY

```

For example, you can use the value of `DomainList` to determine which domains are displayed in the RDP web client login window. The `PluginDLLs` setting lets you integrate additional plug-ins in the RDP protocol. In this example, the ThinPrint Engine from the ThinPrint company is integrated. The entry under `StartApp` specifies the program to be executed in the session.

## 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.

---

**NOTE** 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**.

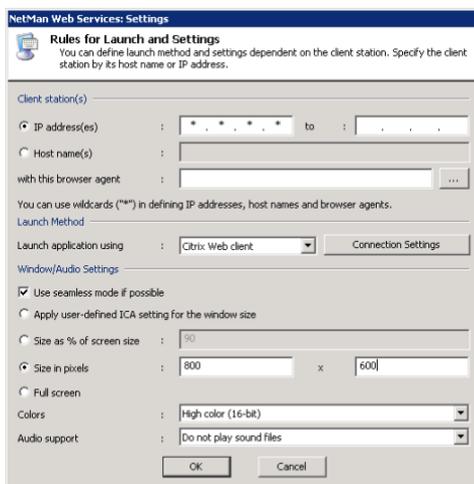
This opens the following dialog:

In the **Login** section, you can modify the default values for both the login and the published application. For detailed information on published applications, please refer to the Citrix documentation.

**NOTE** 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.

**NOTE** 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 “Special Features for Application Settings.”

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

---

**NOTE** 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.

---

`Standard.ica`:

```

001  [ApplicationServers]
002  @NM_PROMPT=
003
004  [WFClient]
005  Version=2
006  TcpBrowserAddress=@NM_TCPBROWSER
007  HTTPBrowserAddress=@NM_HTTPBROWSER
008  UseAlternateAddress=@NM_ALTERNATE_ADDRESS
009  CPMAssowed=@NM_REDIRECT_ICA_PRINTERS
010  CDMAssowed=@NM_REDIRECT_ICA_DRIVES
011  COMAssowed=@NM_REDIRECT_ICA_COMPORTS
012
013
014  [@NM_PROMPT]
015  TcpBrowserAddress=@NM_TCPBROWSER
016  HTTPBrowserAddress=@NM_HTTPBROWSER
017  @NM_ICA_DISPLAY
018  TransportDriver=TCP/IP
019  WinStationDriver=ICA 3.0
020  BrowserProtocol=@NM_BROWSER_PROTOCOL
021  SSLEnable=@NM_ICA_SSL_ENABLE
022  SSLProxyHost=@NM_SSL_PROXY_HOST
023  Compress=@NM_COMPRESS
024  Username=@NM_USER

```

```

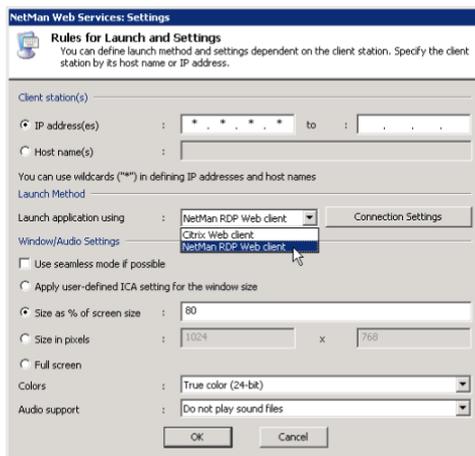
025 Password=@NM_PASSWD
026 Domain=@NM_DOMAIN
027 UseLocalUserAndPassword=@NM_ICA_USE_LOCALUSERDATA
028 InitialProgram=#"@NM_PUBAPP" @NM_CMDPARAM
029 Address=@NM_PUBAPP
030 WorkDirectory=
031 @NM_SECTION_ENCRYPTION
032 @NM_SECTION_COMPRESS

```

Before the ICA data is sent, NetMan web services replace the @NM placeholders with specific values.

## 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:

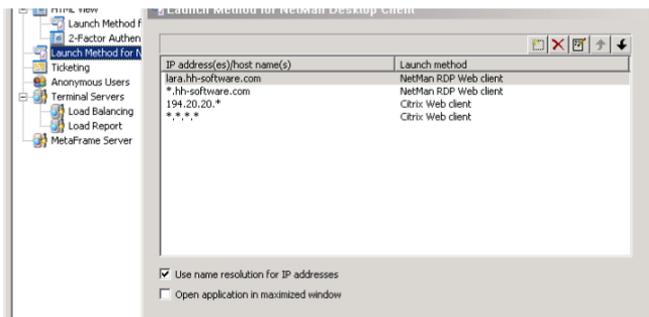


Set one of the following criteria in the NetMan web services for determination of the launch method:

- 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 Special Features for Application Settings) 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.

## NOTE

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.

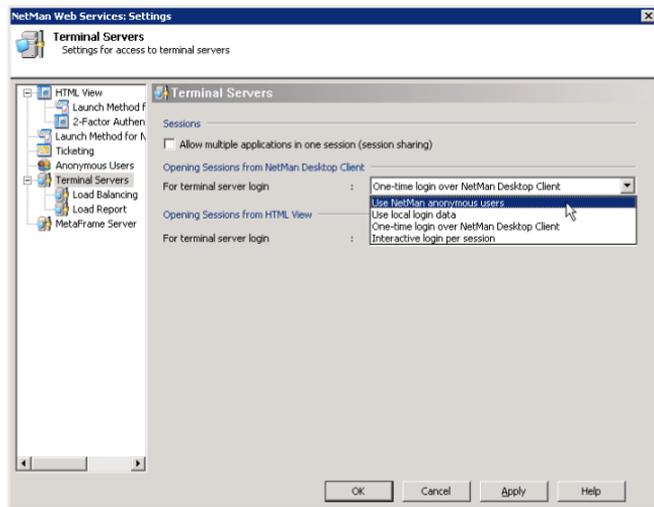
# Login Methods on Terminal Servers

## Overview of Login Methods

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

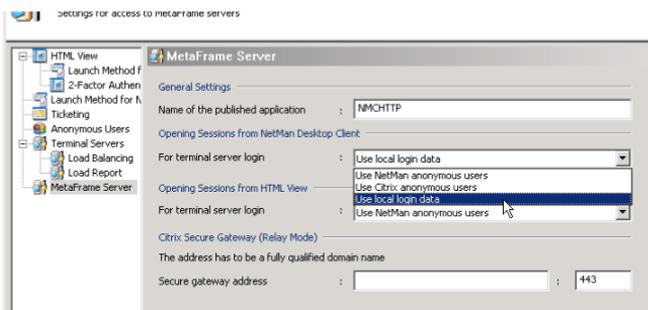
These settings are configured in NetMan web services. Run the **NetMan Web Services Settings** program from the Toolbox and open the **Terminal Servers** page. Select the desired login method in the **Opening Sessions from NetMan Desktop Client** section.



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)**

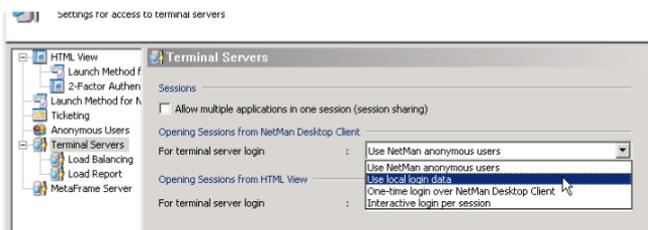
Select the desired option under **Opening Sessions from NetMan Desktop Client**:



The different methods are described in detail in the following sections.

## Use Local Login Data

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.

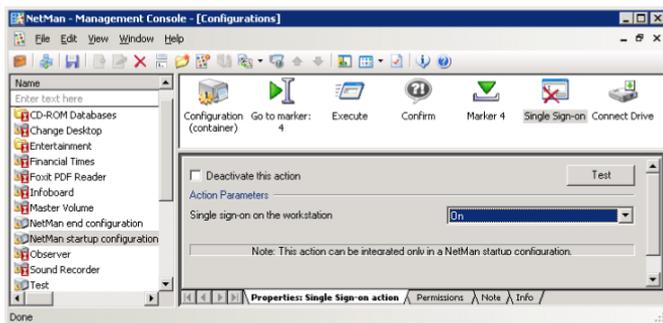


### NOTE

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.



**NOTE** 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 Client. After the 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.



**NOTE** 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`.

## NOTE

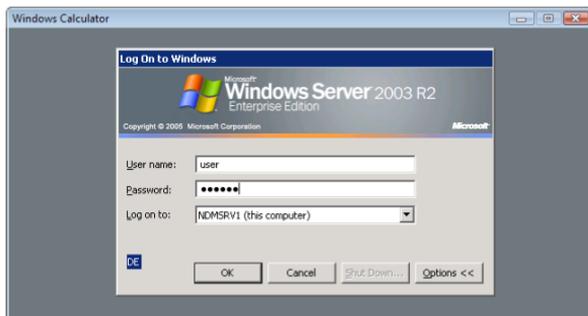
To use this login method, the single sign-on mechanism must be enabled for the NetMan Desktop Clients on all terminal servers on which application sessions run.

## 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 over 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

The context of an anonymous user can be used not only to execute sessions opened through the web interface, but also for sessions opened using NetMan Desktop Client. Prerequisite for such a scenario is that the **NetMan User Service** has already been installed and **NetMan anonymous users** have been set up. For a detailed description of these procedures, see “Anonymous Users” in the chapter entitled “Web Interface.”



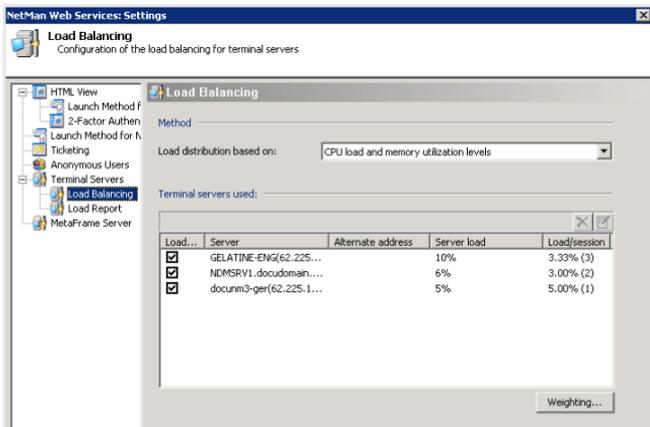
## Extensions for Terminal Servers





# Load Balancing in Application Sessions

NetMan Desktop Manager 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(62.225.1...		Automatic (33%)	3
<input checked="" type="checkbox"/>	NDMSRV1.docudomain...		Automatic (33%)	3
<input checked="" type="checkbox"/>	docunn3-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"/>	NDMSRV1.docudomain...		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.

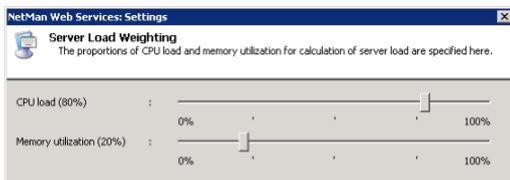
If a given terminal server does not respond for a certain period of time, it is no longer included in load balancing and the number of sessions is replaced with a dash (“—”). Servers can be removed from the load balancing cluster under certain circumstances, as detailed below:

- 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.



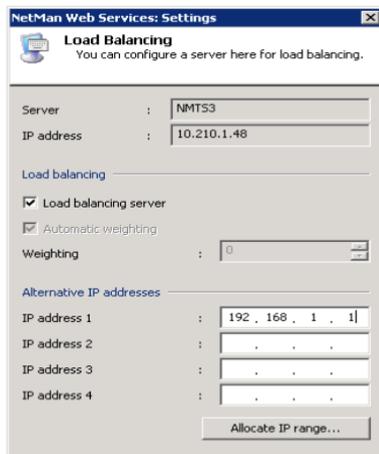
In the example shown here, the CPU load makes up 80% and memory utilization makes up 20% of the server load.

- 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.

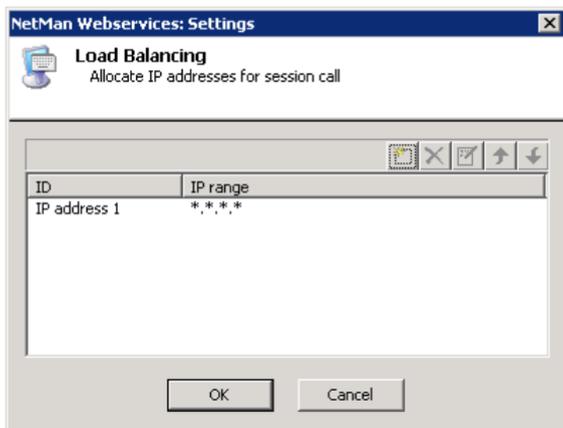
The server load calculated from these values is the basis for distribution of new sessions as they are opened. The server with the lowest load is used to open the next session requested, and is then allotted the current average load level so that subsequently, as a rule, a different server has the lowest 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.




---

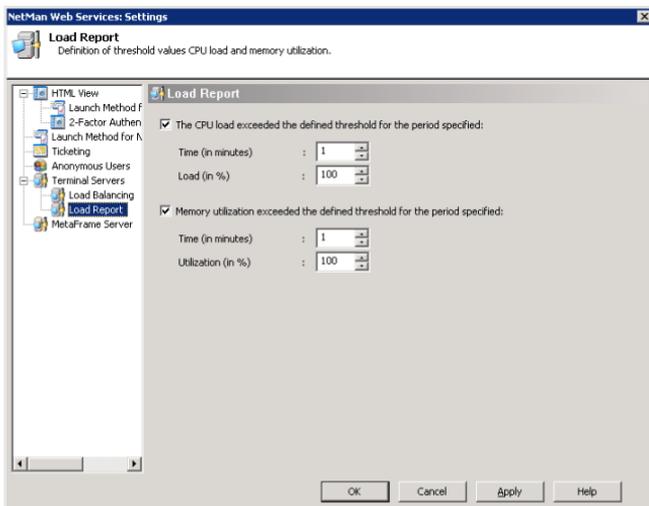
#### NOTE ON LOAD BALANCING

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.

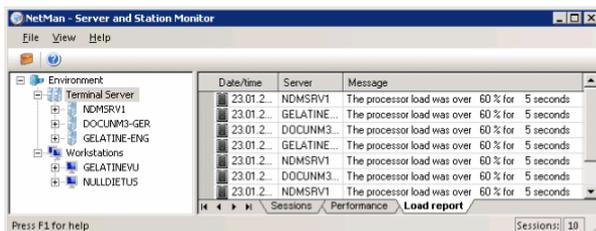
---

# Performance Report

In the **Performance Report** 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 Performance Report items in the **Server and Station Monitor**.



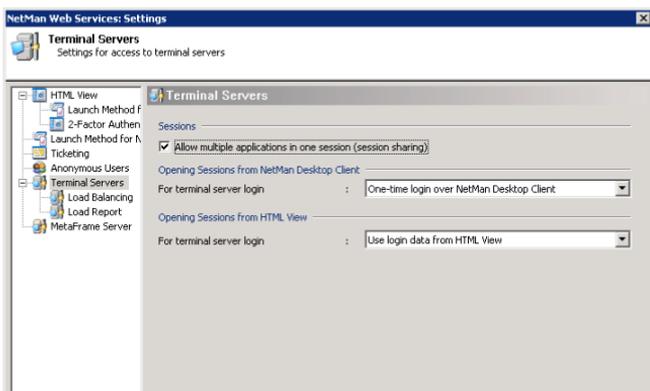


# Session Sharing

Without NetMan Desktop Manager'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:

---

**NOTE** 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.

**NOTE** 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.

**NOTE** 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

---

**NOTE**

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.

**NOTE**

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

## Overview of the RDP Session Broker

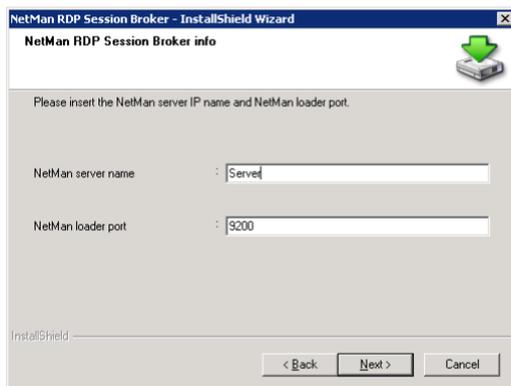
The RDP Session Broker lets you use NetMan Desktop Manager's load balancing features directly with thin clients.

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 Desktop Manager. 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.

## 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.

---

**NOTE** 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”.

---

You can deactivate the service at any time in the **NetMan RDP Session Broker** program in the Control Panel.

---

**NOTE** 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 Desktop Manager server in the clients' configuration.

With this configuration, thin clients show a different login screen:

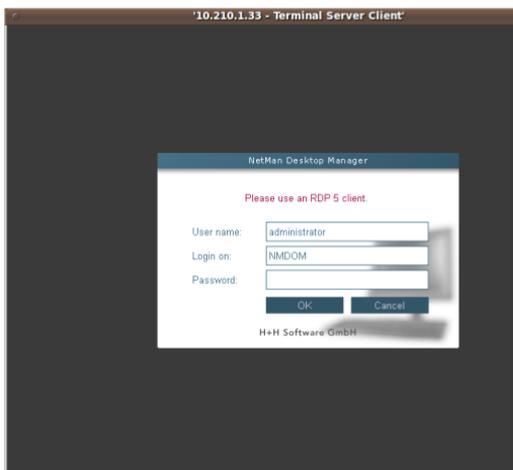
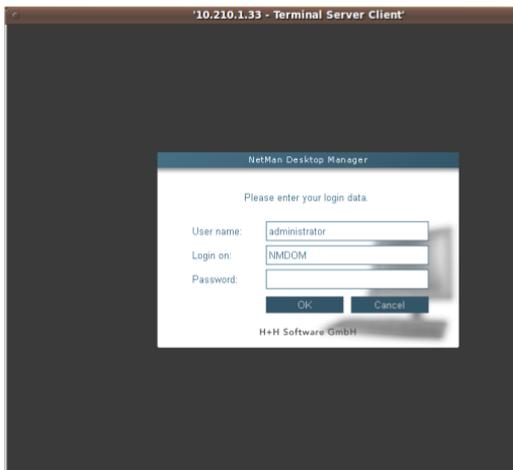
The login procedure is basically the same as before. Which domains are available to choose from is configured in the Web Services settings, on the "HTML View" page, under "Login form." The domains specified there for HTML View apply for the Session Broker as well.

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.







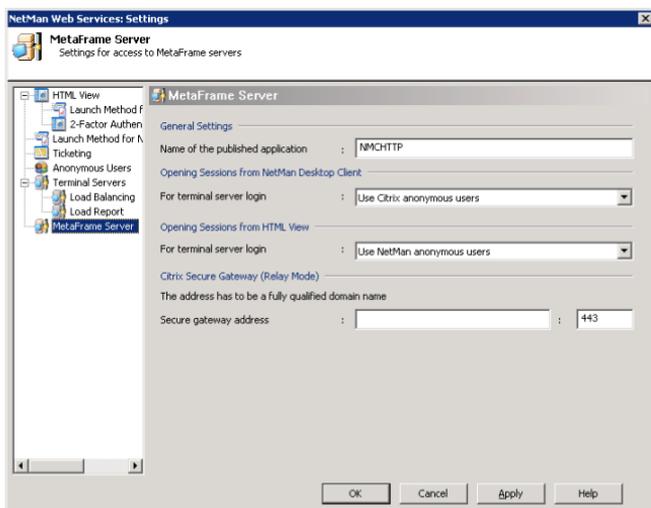
## Extensions for MetaFrame Servers





## 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.

---

### NOTE

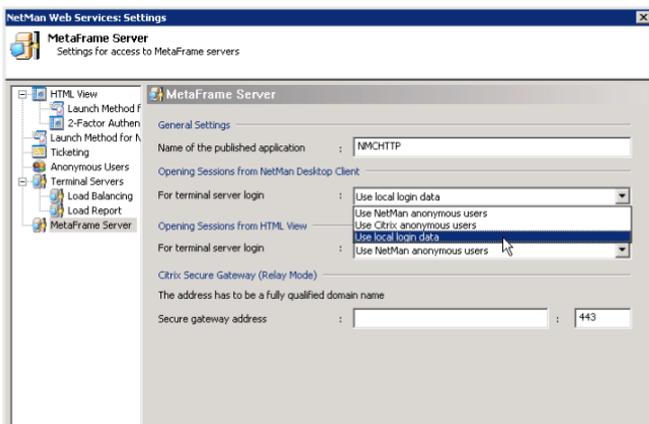
You can change program name (default: **NMCHTTP**) if desired, in the rules defined under **Launch Method for NetMan Desktop Client** and in the advanced settings for applications (see "Separate Launch Method Settings for an Application Call" for details).

---



## 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.

---

**NOTE** 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.

**NOTE** 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%\ICA-Client\APPSRV.INI` file. Program Neighborhood does not offer an interface for configuring this setting.





## Advanced Application Settings for a Session



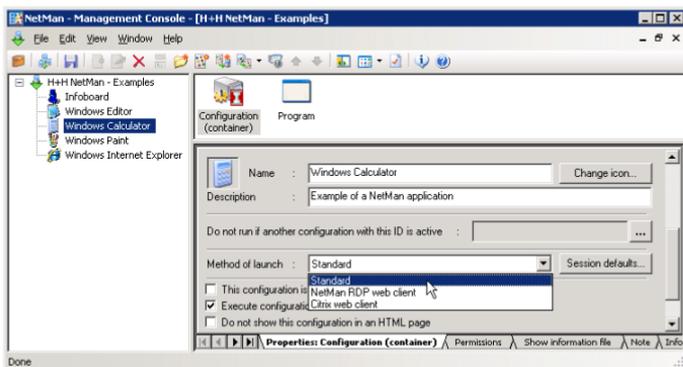


## Separate Launch Method Settings for an Application Call

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.

---

### NOTE

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:** With this setting, the application is launched using the ICA protocol.

---

### NOTE

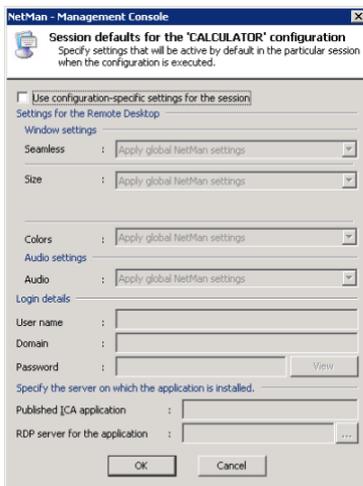
Make sure there is a rule defined in the *NetMan Web Services Settings* program that is applicable to the stations that call this NetMan configuration, and that uses the *Citrix web client* launch method. Otherwise, this application call will not find the connection settings for the ICA session.

---



# 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.



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**.

## NOTE

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

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**.

---

**NOTE**

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.

---

---

**TIP**

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.

---



Advanced Security Features

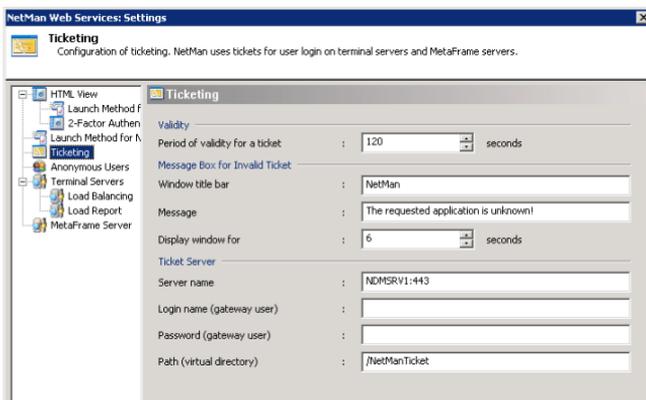




# Ticketing

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:

- **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 `NTicket` 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.



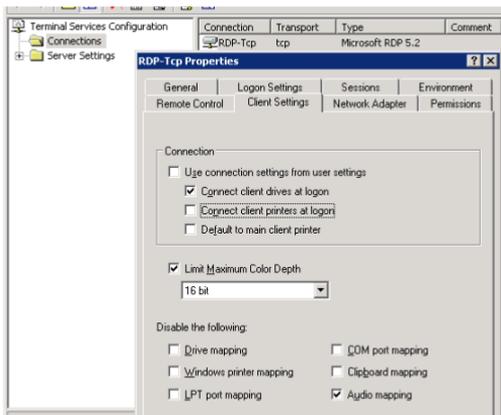
# Access Privileges for Client Drives

## Extended 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.

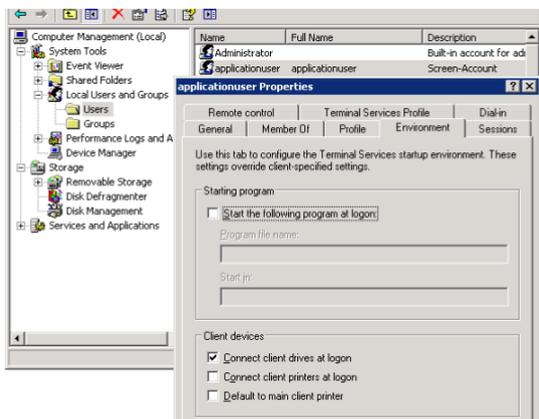
The following can be configured on a Windows Terminal Server:

- 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.



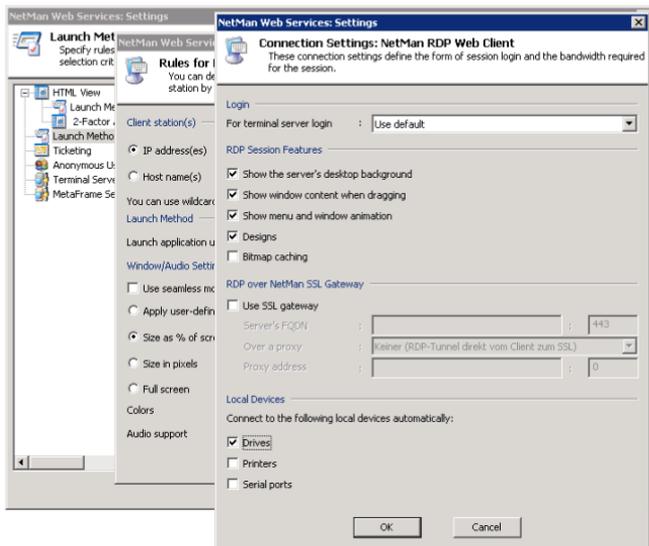
- You can configure user properties to define whether or not drives are accessible for a particular user.

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

To set up access privileges in client drives, begin by opening the NetMan Settings program from the NetMan Toolbox. 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.

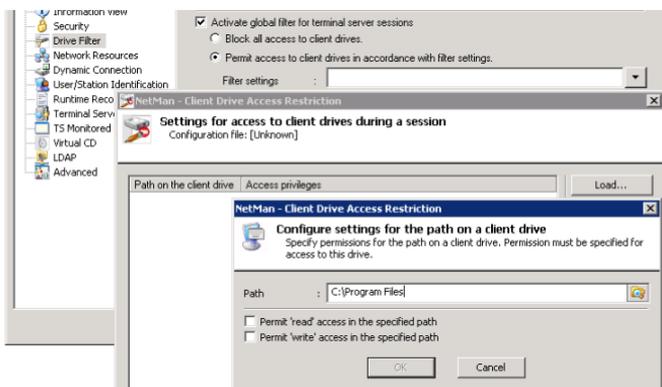


This filter must be switched on before the settings described below for access to the client drives can be applied. If the **Activate global filter for terminal server sessions** option is deactivated, all client drives can be accessed in the usual manner. Once you enable the **Activate global filter 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.

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.



Click on **New**, enter a path and select **Permit 'read' access in the specified path** or **Permit 'write' access in the specified path**.



## NOTE

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.

You can define additional rules if desired before clicking **Save** to store your settings in a configuration file.

---

**NOTE** 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.

**NOTE** 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**”)

---

**NOTE** 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.

---

**NOTE** 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.

**NOTE** 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 with NetMan Desktop Manager





## Overview

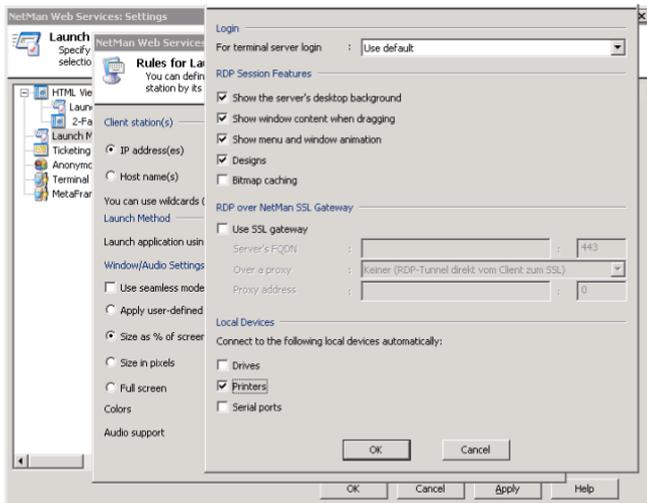
There are a number of methods for connecting and addressing printers in a terminal server environment. Aside from the technique generally implemented in the LAN, of granting user rights to a network printer for a company department or a building floor, for example, terminal server sessions in particular 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
- 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:

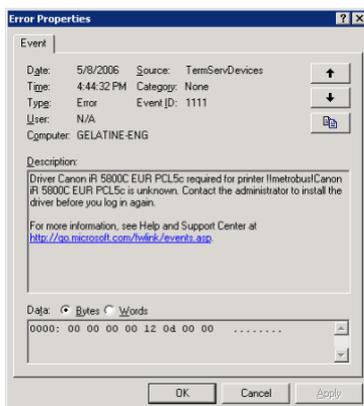
- If the printer driver on the server is an earlier version than that on the workstation, printouts might not show the expected results. If this is the case, you might need to install the latest driver version on the terminal server, which can be a problematic undertaking.
- If the driver for the printer 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 next section 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:

**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

**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 of the format for creating an INF file:

---

```
001 [Version]
002 Signature="$CHICAGO$"
003 [Printers]
004 "OEM printer driver name" = "Windows 2003 printer driver
    name"
```

---

**Example:**

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 Services 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.

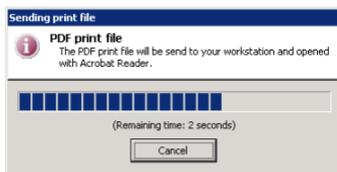
With Windows Vista + SP1 on the client machine, all required components are available and TS Easy Print is ready to use right out of the box. Windows XP + SP3 also supports TS Easy Print, but requires separate installation of .NET Framework 3.0 SP1. Remote Desktop Connection 6.1 is included in Windows 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 the NetMan Desktop Manager, and creates PDF files on the terminal server which are transferred to the client over RDP.



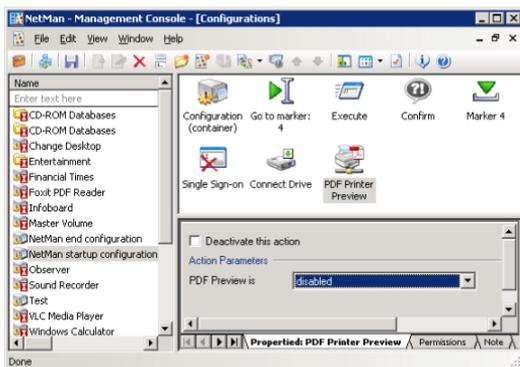
This file is automatically opened on the client by Acrobat Reader. Installation of Acrobat Reader from Adobe on the workstation is required for use of the PDF printer driver. Most workstations already have an Acrobat Reader installation. With Acrobat Reader you can print the file on any local or network 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.

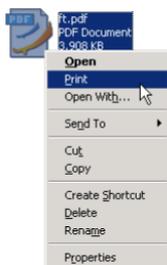
This action is often added to startup configurations. If the NetMan “PDF Print Preview” action is not used in a given terminal server session, then the preview function is available by default in that session.



If the PDF print preview function is switched off, all print jobs are automatically sent to the local workstation's default printer.

### NOTE

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.



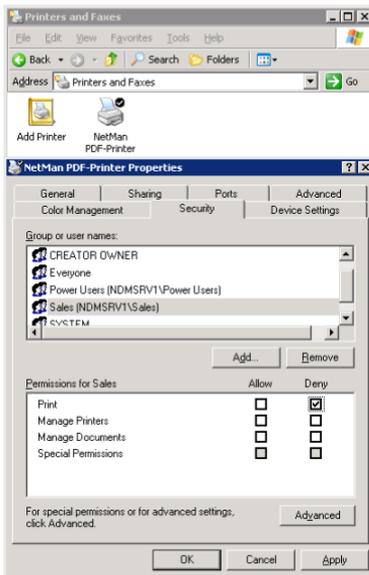


# Showing or Hiding the Universal PDF Printer Driver

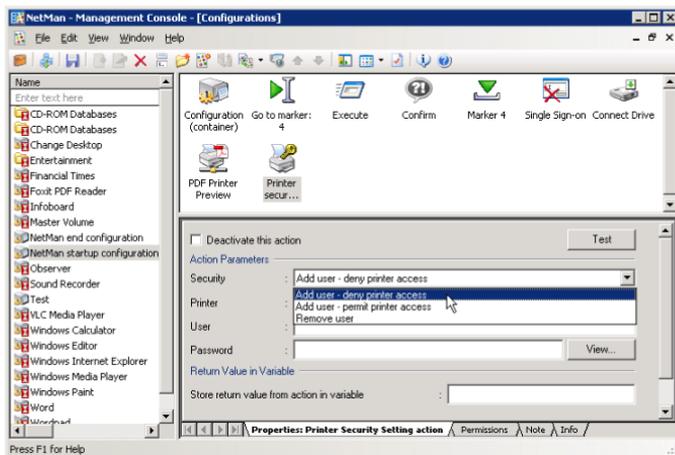
While the universal PDF printer driver can be a useful tool, there may be times when you want to block access to it for some or all users.

There are two ways to do this:

**STEP 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:



**STEP 2** 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:

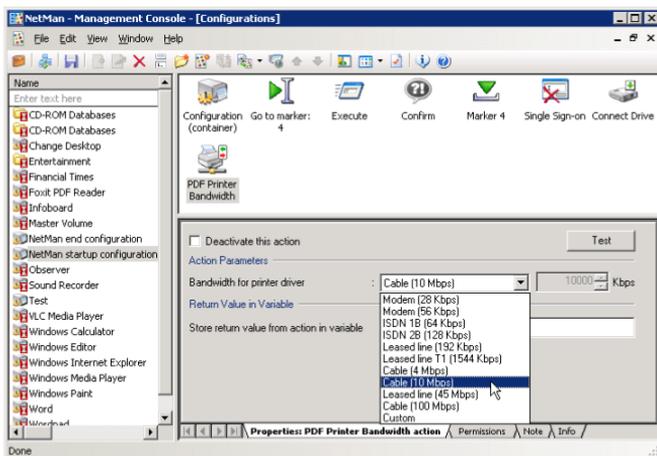
- **Add user – deny printer access:** The user can no longer access the printer.
- **Add user – permit printer access:** The user can access the printer.
- **Remove user:** The user is removed from the access list. In this case, the rights assigned statically to the printer object apply.

#### NOTE

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.



## NOTE

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)
- Leased line T1 (1544 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.





## Additional Tips for Operation in Terminal Server Environments





## Defining the Maximum Number of Parallel Sessions

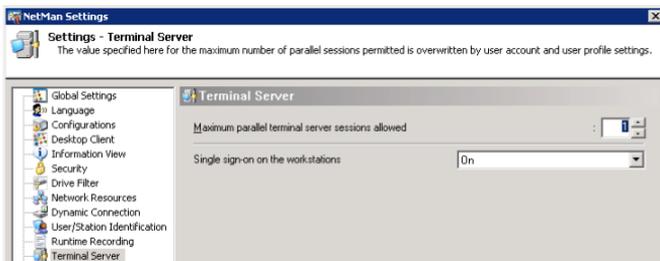
In many cases it can be useful to limit the number of parallel sessions that a single workstation can open. With NetMan, you can define not only whether parallel sessions are permitted, but also the maximum number of parallel instances allowed at any one time.

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.

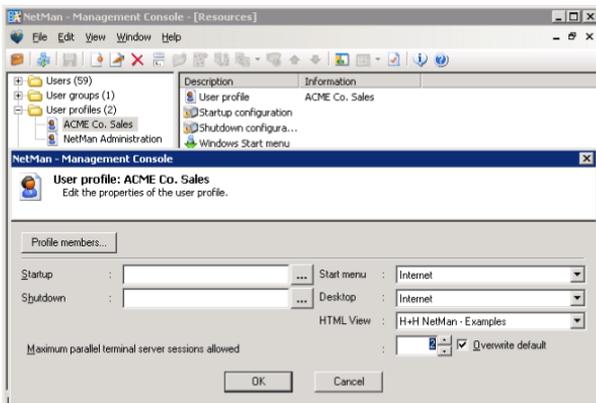
If the number of parallel sessions is set to different values at different levels, the global setting is overwritten by a user-profile setting, and a user setting overwrites both of these.

### 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. At the top, it displays "Users: ADMINISTRATOR" and "Last active on 2/1/2008". The main area contains a form for configuring a user account. The "Name" field is set to "System Administrator". The "Password" field is empty, with a "View..." button to its right. Below this are fields for "Address", "Phone", "Startup", "Shutdown", "Profile" (set to "NetMan Administration"), "Start menu", "Desktop", and "HTML View". At the bottom, there is a "Maximum parallel terminal server sessions allowed" field set to "99" and a checked checkbox for "Overwrite default". "OK" and "Cancel" buttons are at the bottom center.

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.

---

#### NOTE

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

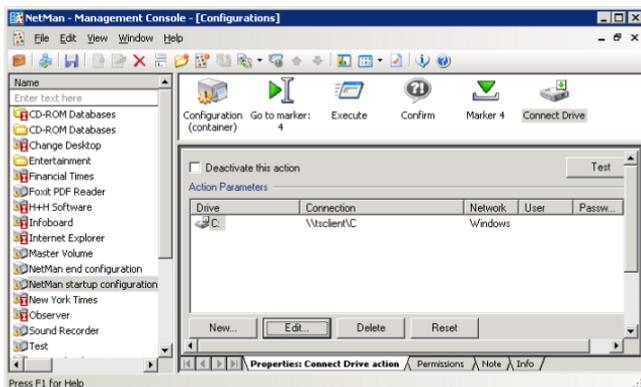
Since NetMan obtains the station ID from the network operating system, and the network requires a unique station designation, the uniqueness of the NetMan station ID is always assured by the network operating system in normal network operation. Only a single instance of NetMan can run on each workstation 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 “MyComputer#2”, and so on.

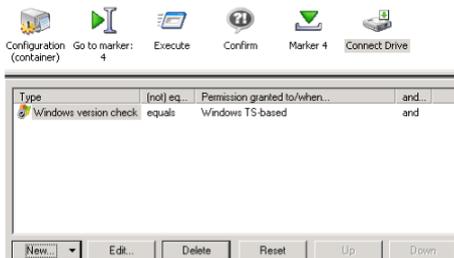


## Granting Access Privileges in Client Drives

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.

---

#### NOTE

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.

---



---

#### TIP

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**.

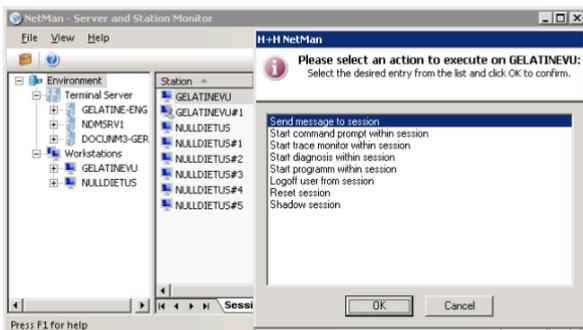


# Troubleshooting Application Problems

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.

---

**NOTE** 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.

**NOTE** 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.

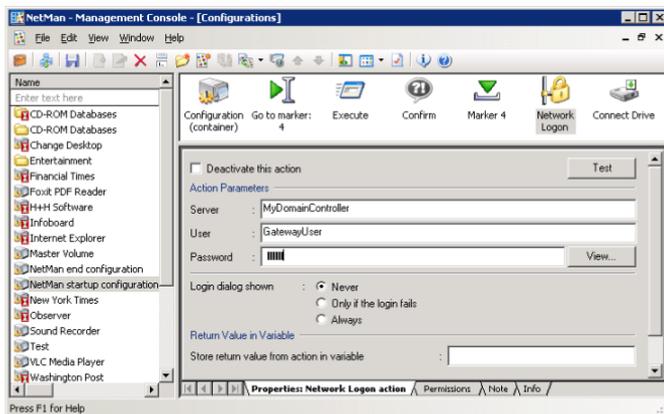
---

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 **Gateway user** on to a server. This gives anonymous users access to resources on **MyDomainController**.

---

**NOTE** 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.

**NOTE** Due to the potential complication described immediately above, it is better to implement anonymous users from NetMan than from Citrix.

---



# 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.

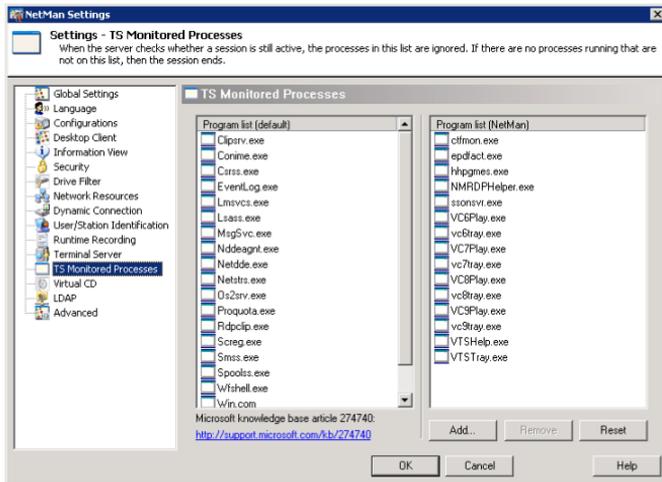
Generally, you want the sessions opened by your users to close again as soon as the user closes the application. To facilitate this function, Microsoft has implemented a process list, maintained by the operating system, which shows active processes that are not displayed in windows. Once there are no 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: `wisptis.exe`

The following H+H products also run background processes in terminal server sessions:

- Virtual CD
- NetMan 3.0

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.

---

**NOTE** The `NMRDPHelper.exe` program must be included on the list so it can close the session.

**NOTE** The mechanism for monitoring background processes in application sessions is automatically active on all terminal servers on which the NetMan Desktop Client is installed.

---



NetMan Internet Filter





# Using the NetMan 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

---

**NOTE**

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.



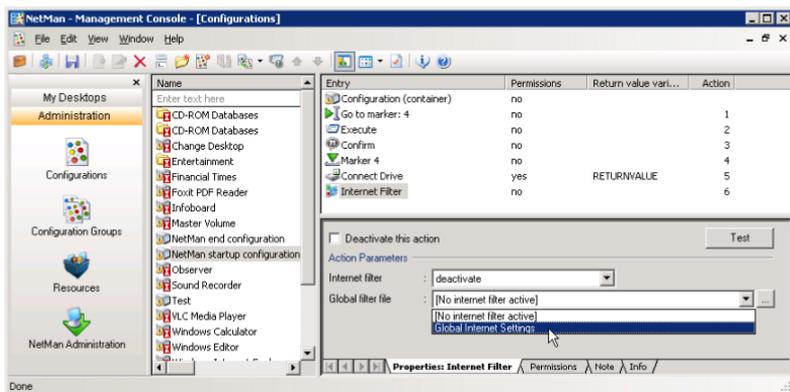
# Switching the NetMan Internet Filter On and Off

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.

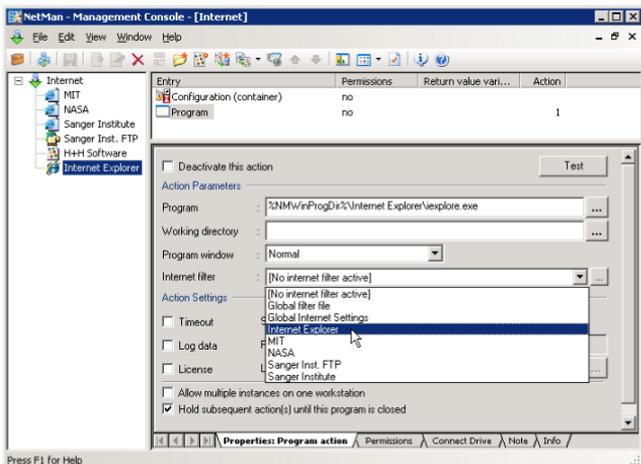
## Internet Access Filtering Mechanism in NetMan Actions

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."

**NOTE**

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.

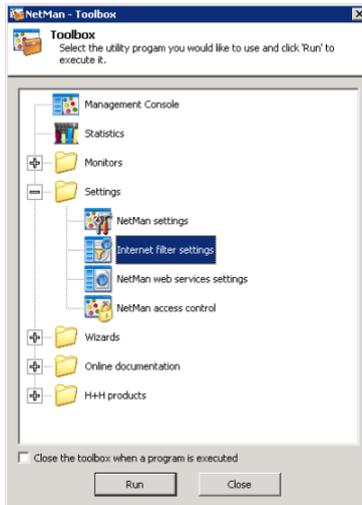
**NOTE**

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.

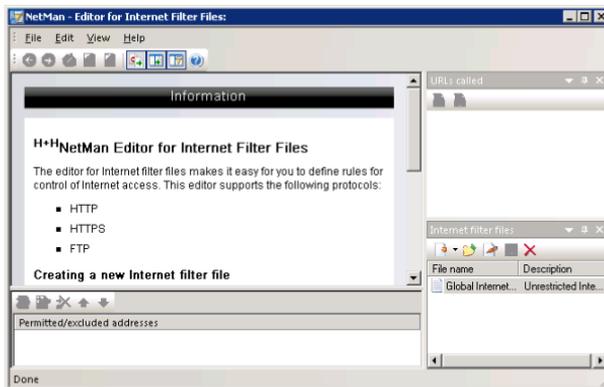
# Editor for Internet Filter Files

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 hyperlinks 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.

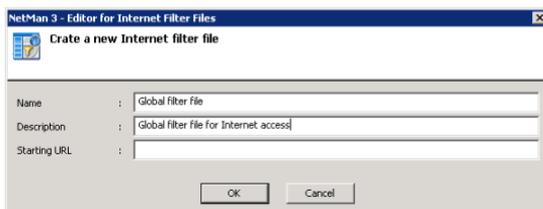
Each window page in which you can configure settings has its own toolbar. The name of the Internet filter file currently open for editing is shown in the title bar of the main window.

# 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.

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.

In the **Internet filter files** window, click on the “New” toolbar icon to create a new Internet filter file.

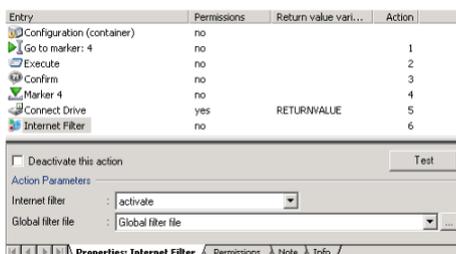


Enter a name and a description for the filter. No starting URL is entered in this case, because the purpose of this filter is to prevent all Internet access.

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.

Save the Internet filter file and close the editor.

In the Management Console, enter the name of your new Internet filter file and activate the Internet filter.



## NOTE

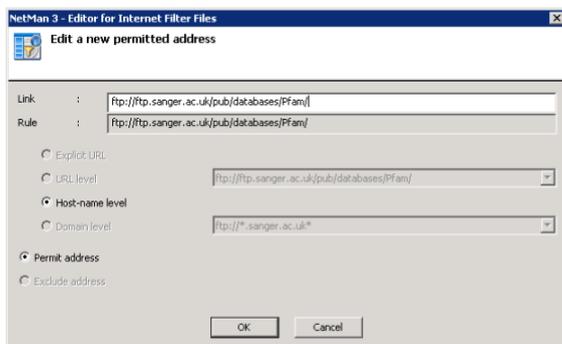
This filter also blocks access to HTTPS and FTP addresses. FTP folders in the Internet can still be seen, but the files cannot be opened or downloaded.



## 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.

### NOTE

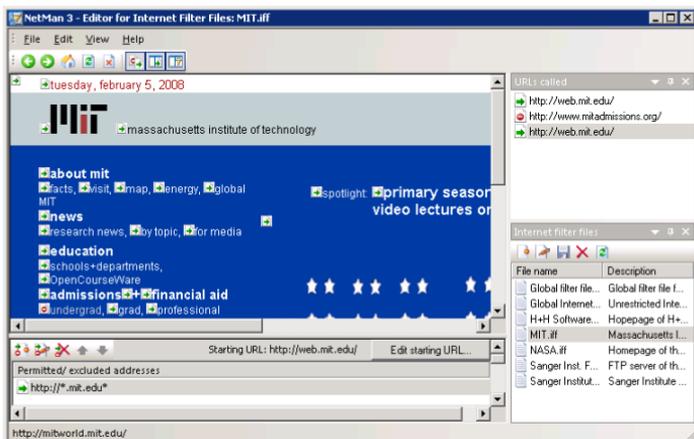
Keep in mind that blacklisting an FTP address does not prevent the user from pointing the browser to that address. The files at that site, however, cannot be downloaded or opened.

The NetMan Internet filter mechanism can filter HTTP addresses on different levels:

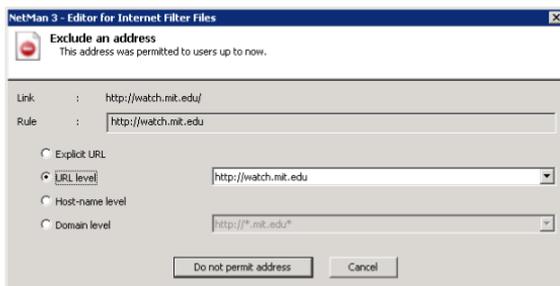
- Explicit URL
- URL level
- Host-name level
- Domain level

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.

---

**TIP** 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:

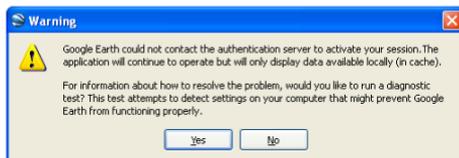
- You can designate certain applications to be monitored for Internet access attempts, or
- You can have all processes that run in your system monitored and any attempted Internet access blocked.

The first step is to create a new filter definition in the Internet Filter File Editor. To do this, select **New/Record from processes**. 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:



Save your new filter file and activate it either by specifying it in a Program 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.

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:



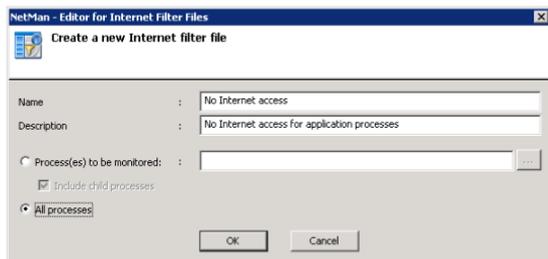
The application can still be used, but only with content that has been cached locally.

### NOTE

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.

---

**TIP** 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.

---

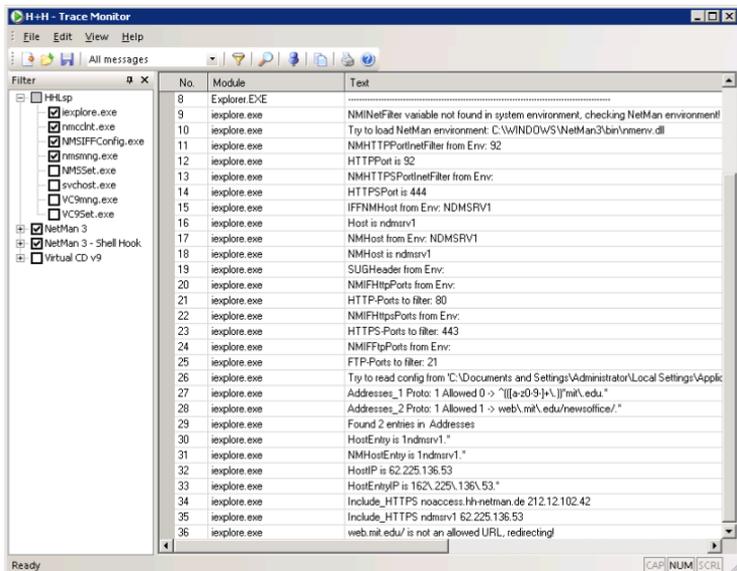
**NOTE** System services and similar system processes are not affected by the NetMan Internet filter file.

---

## 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





## Statistical Analysis of Log Files

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.

---

**TIP** Refer to the on-line Help for detailed information on the numerous settings available in the Statistics program.

---

**NOTE** 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**:

Record ID	Start time	Stop time	User ID	Station ID	Recce	
3825	Windows Calculator	4:30:02 PM	5:03:41 PM	JOHN_O_PUBLIC	GELATINEVU	/TSAWL_562
3824	Windows Calculator	4:18:39 PM	4:29:59 PM	ADMINISTRATOR	GELATINEVU	/TS
3823	Windows Calculator	4:18:35 PM	4:30:01 PM	ADMINISTRATOR	GELATINEVU	/TS
3822	Wikipedia	4:43:27 PM	4:51:58 PM	AZSVOEVERMAN	09.150.12.96	

Sequential  Summarized  Events

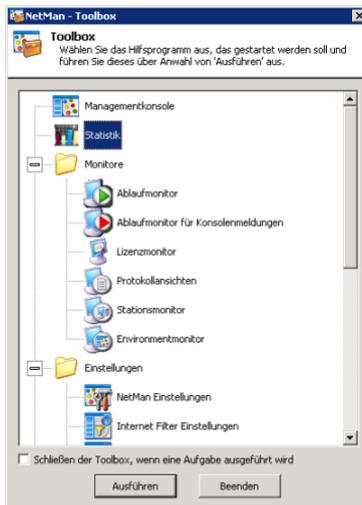
Data records: 3825

This data forms the basis for evaluations performed by the NetMan Statistics program.



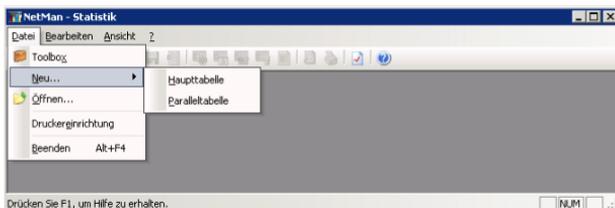
# Statistical Analysis with the NetMan Statistics Program

To run the Statistics program, click on **Statistics** in the NetMan Toolbox.



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

## 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.

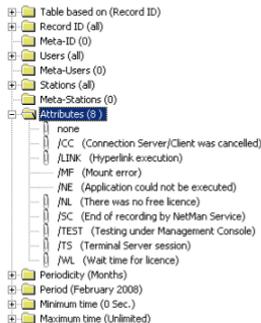
- **/CC**: Connection to client interrupted
- **/Link**: Execution of a Hyperlink action
- **/MF**: Mount error
- **/NE**: Program could not be executed
- **/NL**: No license available
- **/Test**: Test call from the Management Console
- **/TS**: Terminal server session
- **/WL**: Time in license queue

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.

### NOTE

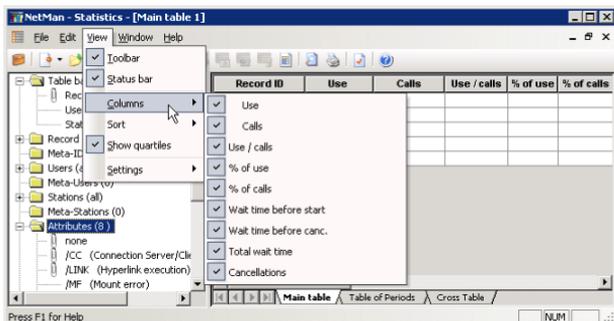
If no license is available and the user cancels the call rather than wait for a license, the call is recorded with a usage time of 0 seconds. If you wish to include such events in your statistical analysis, set the minimum time to "0 seconds."



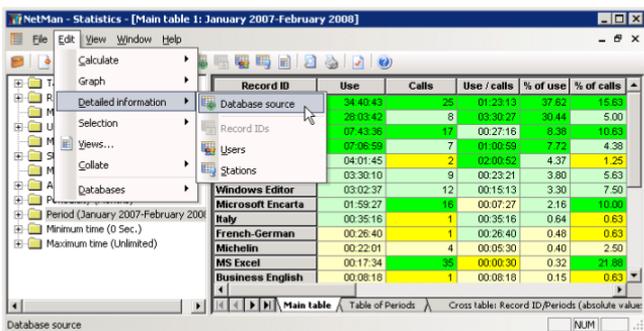
The main table shows the following values:

- 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.

## NOTE

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.

Protokoll-ID	Nutzung	Aufrufe	Nutzung / Aufruf	% der Nutzung	% der Aufrufe	Wartezeit
Microsoft Encarta	105					21,15
Tour d'Énergie	63					7,96
MapPoint	72					7,33
Deutsch - Italien	49					6,18
Französisch-Deut	19					5,46
Englisch - Deutsch	142					4,76
Wirtschaftsentg	78					4,39
Handbuch der Ete	15					3,89
MS Excel	09					3,64
Climate Change	7					3,53
Netzwerklast	05					3,35
Wetter Online	2					2,73
Editorial	01					2,06
Michelin	3					2,03
Windows Tasche	01					2,03
Netzwerklast	48					1,89
Online Telefonu	29					1,66
Astronomie	01					1,58
Informationen	00					1,37

## 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.

**TIP** 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.

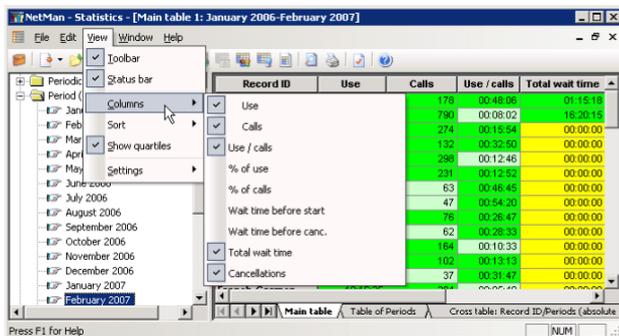
**TIP** If you have common licenses for multiple applications, you can group these applications in a **Meta-ID** to calculate the concurrent use of these licenses.



## Example

### Analyzing Data with the NetMan Statistics Program

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.



Then we run a calculation for this time span.

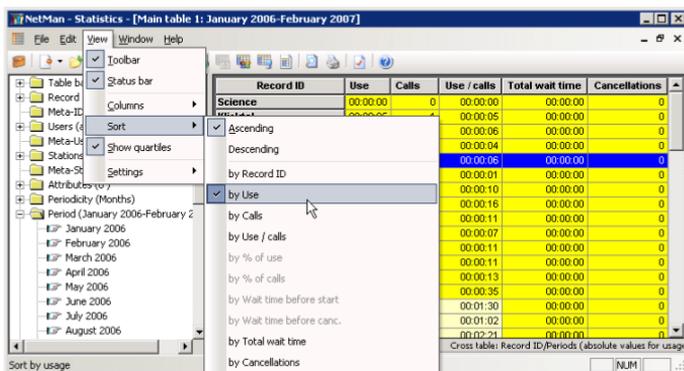
#### NOTE

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
Actebis	00:00:08	2	00:00:04	00:00:00	0
ADN	00:04:43	2	00:02:21	00:00:00	0
Adobe Photoshop	01:54:22	78	00:01:30	00:00:00	0
ALSO	00:00:45	4	00:00:11	00:00:00	0
American Heart Journal	00:00:45	6	00:00:07	00:00:00	0
Architecture	00:13:36	14	00:00:58	00:00:00	0
Astronomy	01:22:59	59	00:01:24	00:00:00	0
Business English	26:52:37	164	00:10:33	00:00:00	0
e't ROM	00:00:12	2	00:00:06	00:00:00	0
Climate Change	7:14:08	132	00:32:50	00:00:00	0
DCI Database	00:00:06	1	00:00:06	00:00:00	0
Dotnetpro	00:01:30	1	00:01:30	00:00:00	0
Editorial	01:52:56	78	00:01:28	00:00:00	0
Emeland	03:26:22	17	00:12:08	00:00:00	0
English - German	142:43:15	178	00:48:36	01:15:18	0
FAZ	00:00:46	4	00:00:11	00:00:00	0
Financial Times	12:03:45	16	00:45:14	00:00:00	0

The data shown is sorted by record IDs.

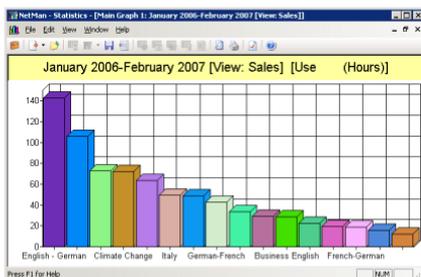
First of all, we want to know which accounts were used the longest and called most often, so we right-click with the mouse cursor on the spreadsheet to open a shortcut menu, and select **Descending/by Use**.



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 **Color settings**.



Now we choose a chart type for our data and generate the chart:



**NOTE**

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.

**NOTE**

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.

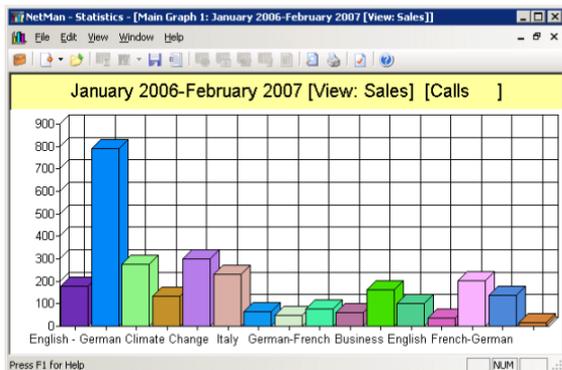
In the next step, the data is sorted by application call. With the default settings, the “Display Quartiles” option is active, so the highest and lowest values in the column can be recognized at a glance. The command for activating and deactivating this option is in the **View** menu. This option marks 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	Cancellation
English - German	142.43.1	176	00:48:06	01:15:18	2
Microsoft Encarta	105.51.1	790	00:08:02	16:20:15	8
MapPoint	72.36.55	274	00:15:54	00:00:00	1
Climate Change	72.14.08	132	00:32:50	00:00:00	0
Tour d'Énergie	63.28.55	298	00:12:46	00:00:00	0
Italy	49.33.42	231	00:12:57	00:00:00	0
The Economist	49.05.31	63	00:46:45	00:00:00	0
German-French	42.34.22	47	00:54:29	00:00:00	0
Michelin	33.89.06	78	00:29:41	00:00:00	0
Paint Shop Pro 9	29.30.07	62	00:28:33	00:00:00	0
Business English	28.52.37	164	00:10:33	00:00:00	0
Weather Online	22.29.26	102	00:31:13	00:00:00	0
Wikipedia	19.36.15	37	00:31:47	00:00:00	0
French-German	19.16.35	204	00:05:40	00:00:00	0
Statistics	15.44.59	136	00:06:50	00:13:08	13
Financial Times	12.03.45	16	00:45:14	00:00:00	0

Sorted by number of application calls, the chart looks like this:



Here we have sorted the table by time spent waiting for a license:

Record ID	Use	Calls	Use / calls	Wait time before start	Wait time before canc.	Total wait time	Cancellation
Microsoft Encarta	105:51:1	790	00:08:02	00:00:32	16:19:43	16:20:15	8
English - German	142:43:1	176	00:40:06	01:11:36	00:03:40	01:15:18	2
Statistics	15:44:59	136	00:06:50	00:00:00	00:13:06	00:13:06	13
Perinorm	07:45:12	19	00:24:29	00:09:03	00:03:45	00:12:48	3
Technology	00:16:49	16	00:01:03	00:00:00	00:09:31	00:09:31	1
Editorial	01:52:56	77	00:01:26	00:00:00	00:00:02	00:00:02	3
MapPoint	72:36:55	274	00:15:54	00:00:00	00:00:00	00:00:00	1

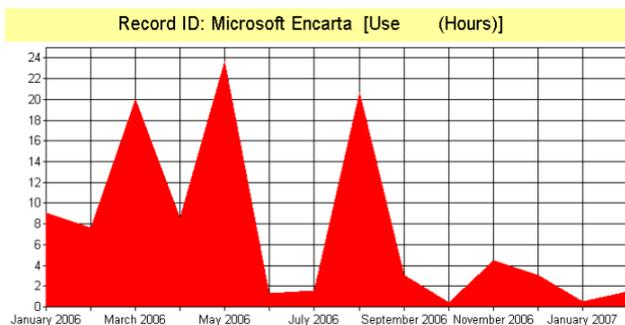
Table of Periods | Cross table: Record ID/Periods (absolute values for usage)

“Microsoft Encarta” is at the top of the list.

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:

Period	Use	Calls	Use / calls	Wait time before start	Wait time before canc.	Total wait time	Cancellation
January 2006	09:05:23	129	00:04:14				
February 2006	07:38:52	117	00:03:55				
March 2006	20:02:07	162	00:07:25				2
April 2006	08:39:10	147	00:03:31				1
May 2006	23:44:06	75	00:18:59	00:00:32	00:00:27	00:00:59	4
June 2006	01:18:32	8	00:09:49		16:19:16	16:19:16	1
July 2006	01:35:34	24	00:03:56				
August 2006	20:44:03	45	00:27:38				
September 2006	03:02:53	19	00:09:37				
October 2006	00:27:50	16	00:01:44				
November 2006	04:28:37	21	00:12:47				
December 2006	03:03:45	11	00:16:42				
January 2007	00:29:57	13	00:02:18				
February 2007	01:29:30	3	00:29:50				
Sum	105:51:1	790	00:08:02	00:00:32	16:19:43	16:20:15	8

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.



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):

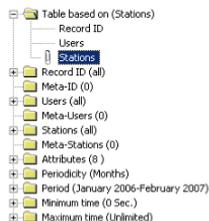
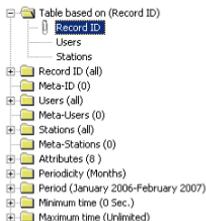
Record ID	January 2006	February 2006	March 2006	April 2006	May 2006	June 2006	July 2006	August 2006
Microsoft Encarta	129	117	162	147	75	8	24	45
English - German	44	27	9	15	20	5	10	6
Statistics								32
Perinorm								
Technology								
Editorial		9		7	16	45		
MapPoint	17	58	22	91	13	11	11	4
Climate Change	14	15	14	6	3	5	9	11
Tour d'Ernergie	55	88	118	31	5	1		
Italy	82	86	41	7	3		1	1
The Economist	23	10	3	3		1	4	3
German-French	10	7	4	9	4	2	5	
Michelin	1	4	12	11	3	4	4	14
Paint Shop Pro 9	3	11	13	4	3	2	5	7
Business English	133	18		2	1			4
Weather Online		19	64	15	4			
Wikipedia	7	3	2	1		3	1	8
French-German		23	23	30	9	20	7	49
Financial Times	3	5					1	2

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.

Record ID	January 2006	February 2006	March 2006	April 2006	May 2006	June 2006
Microsoft Encarta	129	117	162	147	75	8
English - German	44	27	9	15	20	5
Statistics						
Perinorm						
Technology						
Editorial				7	16	45
MapPoint	17	58	22	91	13	11
Climate Change	14	15	14	6	3	5
Tour d'Ernergie	55	88	118	31	5	1
Italy	82	86	41	7	3	1
The Economist	23	10	3	3		1
German-French	10	7	4	9	4	2
Michelin	1	4	12	11	3	4
Paint Shop Pro 9	3	11	13	4	3	2
Business English	133	18		2	1	
Weather Online		19	64	15	4	
Wikipedia	7	3	2	1		3
French-German		23	23	30	9	20
Financial Times	3	5				1

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	Wait time before start	Wait time before canc.
AZS:JOHNSON	326 16.5	717	00:27.26	01:12:00	16:22:56
HRIPANON	87:00:07	813	00:06:25	00:00:00	00:13:17
AZS:OEVERMANN	12:07:00	25	00:29:04	00:08:35	00:03:45
SIBBI	00:00:32	1	00:00:32	00:00:00	00:09:31
HRANON	60:13:59	344	00:10:30	00:00:26	00:00:00
AZS:HEUWILL	20:53:57	487	00:02:34	00:00:10	00:00:00
AZS:SARECCO	07:58:53	256	00:01:51	00:00:00	00:00:10
AZS:MMARON006	00:00:00	0	00:00:00	00:00:00	00:00:00
ANOW	01:52:32	52	00:02:09	00:00:00	00:00:00
ANOHYBUS	00:00:00	4	00:00:00	00:00:00	00:00:00
AZS2:SUPERVISOR	00:02:01	4	00:00:30	00:00:00	00:00:00

...and the 'Stations' table looks like this:

Stations	Use	Calls	Use / calls	Wait time before start	Wait time before canc.
15.38.120.22	319 43.2	780	00:24.35	01:12:00	16:22:56
89.150.12.13	07:36:17	11	00:41:28	00:00:00	00:13:08
89.150.12.27	00:03:15	6	00:00:32	00:00:00	00:09:31
15.38.120.17	05:41:03	10	00:34:06	00:03:22	00:03:44
89.150.12.96	07:44:20	19	00:25:47	00:05:41	00:00:00
89.150.12.50	23:38:55	63	00:02:39	00:00:10	00:00:08
15.38.120.115	119:37:0	489	00:14:43	00:00:00	00:00:13
89.150.12.44	10:01:35	331	00:01:49	00:00:00	00:00:10
15.38.120.100	02:21:41	30	00:03:37	00:00:00	00:00:00
15.38.120.105	00:02:03	3	00:00:41	00:00:00	00:00:00

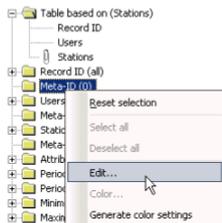
The calculations can be made not only according to *all* users, stations or applications, but also for *selected*

- applications,
- users,
- stations, or
- attributes.

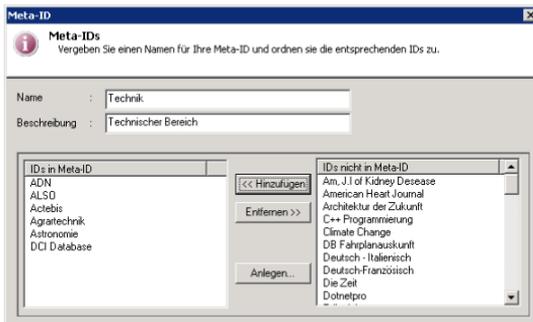
Furthermore, you can change the periodicity (quarterly, half-yearly, yearly or none), select different time spans, or set the minimum time to another value.

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:

Record ID	Use	Calls	Use / calls	Total wait time	Cancellation
Office Applications	188:31:0	1275	00:07:50	16:20:15	8
Dictionaries	233:26:4	593	00:23:37	01:15:18	2
IT	77:39:44	291	00:16:00	00:35:25	17
Magazines	81:56:23	625	00:09:21	00:00:02	7
Information	283:44:0	1052	00:15:10	00:00:00	5
<b>Sum</b>	<b>843:18:0</b>	<b>3736</b>	<b>[00:13:32]</b>	<b>18:11:00</b>	<b>39</b>

## NOTE

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.

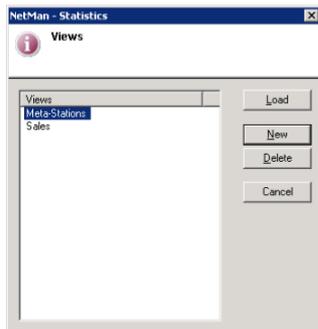
Next we group our stations:

Stations	Use	Calls	Use / calls	Total wait time	Cancellation
Local	580:45:5	1751	00:18:54	17:42:16	10
Network_89	262:03:5	1010	00:08:41	00:28:44	29
Network_90	00:01:57	154	00:00:00	00:00:00	0
<b>Sum</b>	<b>842:51:5</b>	<b>3715</b>	<b>[00:13:36]</b>	<b>18:11:00</b>	<b>39</b>

**TIP** 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.

**TIP** 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.

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.

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
Microsoft Encarta	9	9	1	00:00:27	5	1	00:03:51	3	2	00:00:53
MapPoint	5	3	1	00:00:10	2	11	00:11:49	1	70	05:58:08
Climate Change	2	2	7	01:53:50	1	68	14:59:51	0	0	00:00:00
MS Excel	5	2	4	00:23:57	1	24	01:11:38	0	0	00:00:00
English - German	1	2	3	03:19:06	1	95	11:22:16	0	0	00:00:00
Wikipedia	5	1	22	06:11:15	0	0	00:00:00	0	0	00:00:00
Virtuality	1	1	1	00:00:43	0	0	00:00:00	0	0	00:00:00

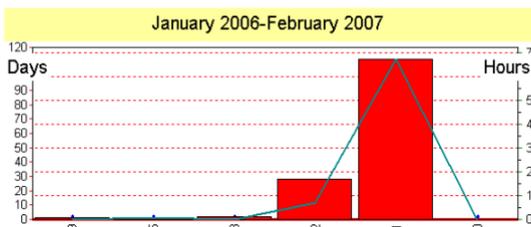
The **Licenses** column shows the number of licenses currently configured for the application. This generally defines the limit for parallel use.

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.

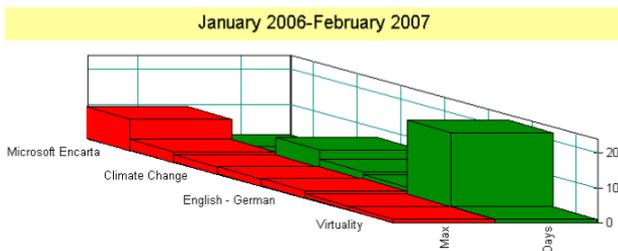
The subsequent columns show the same data for each of the next five lower simultaneous-use values.

As can be seen in the table above, the instances in which the "Wikipedia," "MapPoint" and "MS Excel" configurations were used simultaneously were always fewer than the number of licenses available. For the "Microsoft Encarta" application, however, all available licenses were in use at the same time on one particular day. Still, this maximum usage level was sustained for only a short period; if a tenth user had attempted to launch this application at that time, they would have had to wait only 27 seconds for a license to become available. The "Max-1" value shows that the second highest usage of "Encarta" licenses was 5 licenses, again only on one day. 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)**.





## Appendix





# Glossary

## A

---

<b>Account:</b>	Automatic access to an Internet resource through the optional -> HAN software component.
<b>Action:</b>	An element of a NetMan -> configuration (container type); an individual 'execute' job processed by the NetMan Action -> Interpreter.
<b>Active Directory:</b>	A directory service that Microsoft introduced with Windows 2000 for central storage of all properties, such as users, groups, workstations, etc.
<b>Almanac:</b>	An HTML document that provides an overview of NetMan directories, variables, log entry attributes and error messages.
<b>Anonymous users:</b>	User accounts on a terminal server or in a domain for anonymous access to terminal servers. Anonymous users generally have only strictly limited rights on a terminal server.
<b>Application:</b>	The term "application" as used in this manual is often interchangeable with the term "NetMan -> configuration."
<b>Application drive:</b>	Drive designation under which the applications integrated in NetMan are installed; stored in NetMan's %NMAAppDrive% variable.
<b>Application session:</b>	A terminal server session in which only a particular application is served, rather than an entire Windows desktop. In Citrix terminology, this is referred to as a "published application."

## B

---

<b>Blacklist:</b>	A list of IP addresses or host names of computers or sites to which access is denied. Also the verb for adding a computer or site to this list: "to blacklist."
-------------------	---

## C

---

<b>Category:</b>	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.
<b>Certificate authority:</b>	A certificate authority (CA) is a company that issues digital certificates. These certificates are comparable to a personal identification card. A digital certificate contains a "key," or decryption code, as well as additional information for authentication and for encryption and decryption of sensitive or confidential data distributed over the Internet and in other networks. This additional information can include, for example, the period of validity for the certificate, references to lists of blocked certificates, or similar information added to the certificate by the CA. The CA responsible for issuing and verifying such certificates.

<b>Citrix Web client:</b>	Enables access to MetaFrame server from the browser. Communication is over the ICA protocol.
<b>Configuration (container type):</b>	A user-definable logical unit containing a sequence of -> actions which are processed by the NetMan -> Interpreter: A user-definable logical unit containing a sequence of -> actions which are processed by the NetMan -> Interpreter.
<b>Configuration (folder type):</b>	For organizing NetMan desktop entries. Folder configurations can contain container and folder configurations.
<b>Console session:</b>	A special form of session in which the user is connected with the server using RDP, but sees the console window content. (Command to open the session: MSTSC.EXE /CONSOLE)
<b>Container:</b>	Type of a NetMan -> configuration

---

## D

<b>Desktop:</b>	The structured display of NetMan -> configurations in the NetMan Desktop Client or in an HTML page created by the NetMan HTML View or HTML Wizard.
<b>Desktop entry:</b>	An element of the NetMan desktop. A desktop entry is a container configuration, hyperlink configuration or folder configuration.
<b>Desktop session:</b>	A terminal server session that provides a Windows desktop, rather than only a single application.
<b>Digital certificate:</b>	Certificates are comparable to a personal identification card. A digital certificate contains a "key," or decryption code, as well as additional information for authentication and for encryption and decryption of sensitive or confidential data distributed over the Internet and in other networks. This additional information can include, for example, the period of validity for the certificate, references to lists of blocked certificates, or similar information added to the certificate by the -> CA.
<b>Dynamic connection:</b>	Mapping of a network share or volume to a specified drive. The dynamic connection mechanism can use any drive for mapping, or draw from a restricted set of drives that you define.

---

## E

<b>Environment:</b>	The NetMan environment contains the NetMan variables. Refer to the NetMan Almanac for descriptions of all available variables.
---------------------	--

---

## F

<b>Folder:</b>	Type of NetMan configuration; see also -> Configuration (folder)
----------------	--

---

## H

<b>H+H HAN:</b>	-> HAN
-----------------	--------

<b>HAN:</b>	Hidden Automatic Navigator (HAN; H+H HAN) is an optional NetMan module that lets you provide 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.
<b>HTML View:</b>	Name of NetMan software module implemented in earlier versions; still used to refer to the NetMan web interface or web services.
<b>Hyperlink:</b>	URL; on-line account; HTML pages in general; type of NetMan -> action in particular.

---

**I**


---

<b>ICA protocol:</b>	Communication protocol from the Citrix company. Used with MetaFrame products to transfer screen content and user actions between server and client.
<b>ICA session:</b>	A session on a MetaFrame server using the ICA protocol.
<b>IFF Editor:</b>	-> Internet filter file editor
<b>Internet filter file editor:</b>	Editor for writing and modifying files that filter Internet access.
<b>Interpreter:</b>	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.

---

**L**


---

<b>Launch method:</b>	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**


---

<b>MetaFrame:</b>	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 called -> Presentation Server.
<b>MetaFrame server:</b>	A product from the Citrix company that adds certain performance features to the Microsoft terminal services.
<b>Microsoft RDP Web client:</b>	Lets you access a Windows server with terminal services using RDP.

---

**N**


---

<b>Named licences:</b>	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. Also referred to as "per seat" licensing.
<b>NetMan access control:</b>	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 than Windows can for anonymous users, when using the NetMan User Service. An IP address 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.

<b>NetMan Client Service:</b>	A service that is required on stations on which the NetMan Desktop Client is installed.
<b>NetMan Desktop Client:</b>	An extension and enhancement of Windows Explorer.
<b>NetMan placeholders:</b>	Elements used by NetMan in HTML pages and templates. The HTML View module replaces placeholders with certain values or other contents.
<b>NetMan RDP Web Client:</b>	Lets you access a Windows server with terminal services using RDP. This client offers more functions than the Microsoft RDP Web client.
<b>NetMan service:</b>	Central NT service that manages data on users, stations, licenses and the usage of NetMan configurations.
<b>NetMan start file:</b>	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.
<b>NetMan tray program:</b>	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.
<b>NetMan user service:</b>	The NetMan user service sets passwords at run time for anonymous users created by the User Account Wizard of the NetMan Web Service.
<b>NetMan web services:</b>	Services that implement the main functions of NetMan's terminal server and web interface software.
<b>NT4 Domain:</b>	A central user database for Windows networks. Starting with Windows 2000, this has been replaced by --> Active Directory.
<b>NTFS:</b>	New Technology File System: developed by Microsoft for the Windows NT/2000/XP operating systems.

## P

---

<b>Per seat:</b>	-> Named licenses
<b>Presentation Server:</b>	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.
<b>Published application:</b>	An application on a MetaFrame server, specified in the Citrix Management Console, which is published for the execution of a MetaFrame server session.

## R

---

<b>RDP protocol:</b>	Remote desktop protocol for communication between workstation and terminal server, used to transfer screen content and user actions. Re-
----------------------	--

mote desktop protocol is based on the ITU standard T-120 and adapted by Microsoft for the special requirements of terminal servers.

<b>RDP session:</b>	A session on a terminal server using RDP.
<b>Record attribute:</b>	Item of information recorded in addition to standard items such as user name, station, date and time when data logging is active. Please see the NetMan Almanac for a complete list of available attributes.
<b>Remote administration:</b>	Technology that enables remote administration of servers and workstations. RDP is one of the protocols that Microsoft uses for remote administration.
<b>Remote desktop user:</b>	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

---

<b>Shutdown configuration:</b>	A configuration specified in the NetMan Settings; processed when the NetMan software is shut down.
<b>Startup configuration:</b>	A -> configuration specified in the NetMan Settings to be processed when NetMan is launched.
<b>Station database:</b>	NetMan database in which every station that starts NetMan is automatically registered under the specified NetMan -> station ID.
<b>Station ID:</b>	A unique designation that identifies a workstation; registered in the -> station database.
<b>Station profile:</b>	A set of defined preferences; you can assign the same profile to multiple stations, but each station can be assigned only one profile.

## T

---

<b>Terminal server:</b>	This term is used with the particular meaning defined by Microsoft Terminal Services. Microsoft Terminal Service expands the functionality of a Windows server so that remote users can access the server interface and run Windows applications on the server.
<b>Terminal services:</b>	Terminal services from Microsoft make it possible to open a session on a Windows server, during which screen content and user interactions are transferred over RDP.
<b>Ticketing:</b>	Technique for issuing a "ticket" (a form of authentication for server access). 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.
<b>Timeout:</b>	A program that monitors applications started by NetMan and ends them if no input is detected for a defined period of time.
<b>Toolbox:</b>	An interface to administrative utilities.

## U

---

- User database:** NetMan database in which every user that starts NetMan is automatically registered under the specified 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

---

- Whitelist:** A list of IP addresses or host names of computers or sites to which access is denied. Also the verb for adding a computer or site to this list: "to whitelist."
- Windows Script Host:** (WSH) Provided by Microsoft for enhancement of 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 9, 105, 191

## A

---

Access control 89, 290  
 Accessing applications over the NetMan SSL gateway 224  
 Accessing the NetMan RDP Session Broker 269  
 Access privileges on client drives 289  
 Actions 111, 141, 142, 144, 148, 159  
 Action sequences 75  
 Active desktop entry 125  
 Active Directory service 89  
 Active directory services 132  
 ADMIN\$ shares 41  
 Advanced settings 103  
 Advantages of the web interface 55  
 Allocated client drives 77  
 Analyzing data with the NetMan statistics program 357  
 a NetMan configuration 116  
 Anonymous users 211, 325  
 Anonymous Users 215  
 Application-based load balancing 9  
 Application session 13, 69  
 Applications in sessions 67  
 Applications run locally 67  
 application/x-ica 205  
 Associated client printers 77  
 Authentication 57

## B

---

Bandwidth 311  
 Bandwidth management 311  
 Bandwidth management for the universal PDF printer driver 311  
 Blocking access to particular URLs 339  
 Browser agent 205

## C

---

Calling applications through the web interface 61  
 Capturing trace messages from session 323  
 Cascading style sheets 231  
 Centralized administration of all types of applications and hyperlinks 9  
 Certificate 57, 77, 223  
 Certificate authority 81  
 Certificate file 81  
 Certificates 79  
 Change desktop 137  
 Citrix 5  
 Citrix Anonymous Users 275  
 Citrix anonymous users in domains 325  
 Citrix Java client 204  
 Citrixjava.htm Template file 204  
 Citrix MetaFrame server 5  
 Citrix web client 201, 243, 248  
 Citrix Web Client 279  
 Client drives 194, 201, 244, 248  
 Client drives with 'read only' privileges 289  
 Client drives with 'write only' privileges 289  
 Client printer 194, 201, 244, 248  
 Closing an application session 327  
 Codebase 204  
 COMAllowed 248  
 COM interface 154  
 Compress 201, 248  
 Computer name 317  
 Concurrent use table 355  
 Configuration 103  
 Configuration groups 95  
 Configurations 95  
 Configuring privileges to print objects 309  
 Configuring the NetMan gateway 226  
 Configuring the RDP Session Broker 268

- Connecting a printer 299
- Connection monitor 228
- Connection settings 194, 201, 244, 248
- Container 111
- Content redirect 116
- Contents 3
- CPMAllowed 248
- Creating anonymous users 211
- Creating a self-signed certificate 79
- Creating filter rules 339
- Creating SSL certificate 223
- CSS files 231

## D

---

- Database 97
- Database browser 100
- Databases 75, 100, 181
- Database wizard 107
- Data logging 103
- Default rule 205
- Default rules 251
- Defining the maximum number of parallel sessions 315
- Desktop client 103
- Desktop Client 47
- Desktop Client page of NetMan Settings 49
- Desktop entry active 125
- Desktop session 13, 69, 327
- Desktop sessions and application sessions 13
- Diagnostics in a session 323
- Distributing NetMan Desktop Client in the network 41
- DMZ 222
- Domain level 339
- Domain resources 325
- Dynamic connection 103

## E

---

- Editor for Internet filter files 104, 335
- Environment 154

- Environment check 132
- Environment monitor 100
- Environment-specific program sequences 9
- Environment variables 154
- Epdfact.exe 327
- Example of login page modification 232
- Examples 236
- Examples desktop 95
- Excluded addresses 104
- Extended access privileges for client drives 289

## F

---

- Filter definition for client drives 292
- Filtering URLs 331
- Firewall 201, 248
- Firewalls 226
- Folder 125
- FQDN 222
- FTP 104, 331, 339
- FTP addresses 339
- FTP resource 339

## G

---

- Gateway 222
- German 231
- Global Internet filter 337
- Global Internet filter file 333
- Global Internet Settings.iff 333
- GUID 287

## H

---

- Help programs 323
- HHTrace.exe 321
- Host name 175, 205, 251
- Host-name level 339
- HTML page for launching applications 233
- HTML pages 231
- HTML View 111, 221, 226
- HTTP 77, 104, 331
- HTTP addresses 339

HTTPBrowserAddress 201, 248  
 HTTPS 57, 77, 104, 226, 331  
 HTTPS addresses 339  
 HTTPS port 222  
 Hyperlinks 111, 339

## I

---

ICA 132  
 ICA client 201, 204, 248  
 ICA protocol 201, 204, 248  
 Improved security 9  
 INF file 299  
 Infoboard 47  
 Info page of the NetMan Settings 141  
 Information display 103  
 Information File page 130  
 Input prompt in a session 323  
 Installation 33, 34, 39, 211  
   *NetMan Desktop Manager in a multiple terminal server environment* 39  
   *NetMan Desktop Manager on a terminal server* 34  
 Installation of NetMan Desktop Client using a software deployment tool 41  
 Installation of NetMan Desktop Client using NDCDEPLOY 41  
 Installing NetMan Desktop Client 39  
 Installing NetMan SSL Gateway 222  
 Installing the NetMan RDP client 59  
 Installing the NetMan user service 211  
 Installing the RDP Session Broker 267  
 InstallShield 41  
 InstallShield package 41  
 Integrating CD-ROM-based applications 161  
 Interactive login per session 253, 256  
 Internet access 331  
 Internet filter action 333  
 Internet filter files 104  
 Internet filtering 331  
 Introduction to web interface design 231

IP address 205, 317  
 IP addresses 243, 251

## J

---

Java applet 204  
 Java scripts 231

## L

---

Language 103  
 Launch method 105, 251  
 Launch methods 243, 253  
 LDAP 103  
 License Monitor 100  
 Licenses 100  
 License waiting period 353  
 Licensing 108, 122  
 Linux workstation 205  
 List of terminal servers and load balancing 259  
 Load balancing 105, 201, 248, 259, 281  
 Load balancing in application sessions 259  
 Local application execution 67  
 Local printers 297  
 Local resources 319  
 Log files 349  
 Logging in through the web interface 57  
 Login 57, 189  
 Login data 254  
 Login Data from HTML View 210  
 Login method for sessions 105  
 Login Methods on MetaFrame Servers 275  
 Login page 231  
 Log users off of session 323

## M

---

Main table 351, 353  
 Management Console 95, 173  
 Manual startup 211  
 Mapping a printer 299  
 Mapping client drives 319  
 MetaFrame Presentation server 3.0 281

MetaFrame XP 281  
 Meta-IDs 353  
 Meta-users 353  
 Microsoftrdp.htm 194  
 Microsoft Terminal Server 5  
 Mirroring a session 323  
 Modified audio settings 281  
 Modified window settings 281  
 Modifying a login page 232  
 Modifying printer mapping 299  
 Modifying the launch method 243, 279  
 Monitored processes for application sessions 327

## N

---

Ncddeploy.exe 41  
 NetMan access control 105, 173  
 NetMan Access Control 89  
 NetMan Almanac 141  
 NetMan client service 99  
 NetMan configurations 111  
 NetMan databases 75, 107  
 NetMan Desktop Client 41, 73, 85, 86, 107, 111, 205, 251, 279  
 NetMan Desktop Client as Terminal Server Interface 69  
 NetMan Desktop Client Distribution 41, 107  
 NetMan Desktop Client on a workstation 67  
 NetMan Desktop Manager 95  
   *The Basics* 5  
 NDM server components 73  
 NetMan filter settings 104  
 NetMan interfaces 154  
 NetMan Internet filter 331  
 NetMan login 173  
 NetMan RDP web client 194, 205, 243, 244, 251  
 NetMan service 75  
 NetMan services 99  
 NetMan settings 103, 315  
 NetMan Settings program 49  
 NetMan Settings / Terminal Server 254  
 NetMan SSL gateway 9, 221, 223, 226  
 NetMan SSL Gateway 224  
 NetMan startup configuration 325  
 NetMan Statistics program 351  
 NetMan system administration 49  
 NetMan Toolbox 47, 49, 89  
 NetMan user database 173  
 NetMan user groups 177  
 NetMan users 173  
 NetMan User Service 211  
 NetMan web service 77  
 NetMan web services 99, 205, 243, 251, 259  
 NetMan web services settings 105  
 Network provider 254  
 Network resources 103  
 NM\_ALTERNATE\_ADDRESS 201, 248  
 NMAAppDrive 159  
 NMAAppUNC 159  
 NM\_BROWSER\_PROTOCOL 201, 248  
 NMCCInt.exe 69  
 Nmchttp.exe 273  
 NMCHttp.exe 67, 321  
 NMCHTTP.EXE 194, 244  
 NM\_CMDPARAM 194, 201, 244, 248  
 NM\_COMPRESS 201, 248  
 Nmcsetup.cfg 41  
 NMCTray.exe 69  
 NM\_DESCRIPTION 204  
 NM\_DOMAIN 194, 201, 244, 248  
 NM\_HEIGHT 204  
 NM\_HTTPBROWSER 201, 248  
 NM\_ICA\_DISPLAY 201, 248  
 NM\_ICA\_SSL\_ENABLE 201, 248  
 NM\_ICA\_USE\_LOCALUSERDATA 201, 248  
 NM\_LAUNCH 204  
 NM\_LIST\_DOMAIN 194, 244  
 NM\_LOGONTYPE 194, 244  
 NM\_PASSWD 194, 201, 244, 248

NM\_PROMPT 194, 201, 244, 248  
 NM\_PUBAPP 201, 248  
 NM\_RDPBMPDCACHE 194, 244  
 NM\_RDP\_DISPLAY 194, 244  
 NM\_RDPFLAGS 194, 244  
 NMRDPHelper.exe 327  
 NM\_RDP\_SERVER 194, 244  
 NM\_REDIRECT\_ICA\_COMPORTS 201, 248  
 NM\_REDIRECT\_ICA\_DRIVES 201, 204, 248  
 NM\_REDIRECT\_ICA\_PRINTERS 201, 204, 248  
 NM\_REDIRECT\_RDP\_COMPORTS 194, 244  
 NM\_REDIRECT\_RDP\_DRIVES 194, 244  
 NM\_REDIRECT\_RDP\_PRINTERS 194, 244  
 NM\_SCREENPERCENT 204  
 NM\_SEAMLESS 204  
 NM\_SECTION\_COMPRESS 201, 248  
 NM\_SECTION\_ENCRYPTION 201, 248  
 NMSHFile 116  
 NM\_SSL\_PROXY\_HOST 201, 248  
 NM\_TCPBROWSER 201, 248  
 NM\_USER 194, 201, 244, 248  
 NM\_WIDTH 204  
 NM\_WINDOWTYPE 204  
 NT group membership 105  
 Number of parallel sessions 315

---

## O

OEM printer driver name 299  
 Official certificate (from CA) 77  
 Official certificates 81  
 One-time login using NetMan Desktop Client 253, 255  
 Overview 211  
 Overview of launch methods 243  
 Overview of Launch Methods 193  
 Overview of login methods 253  
 Overview of Login Methods 209  
 Overview of system structure 73  
 Overview of the RDP Session Broker 267

---

## P

Pass-through authentication/SSO 9  
 Password 201, 248  
 PCL driver 301  
 PDC emulator 211  
 PDF preview 307  
 PDF printer driver 9  
 Performance features 9  
 Permissions 75  
 Permissions for client drives denied 290  
 Permissions for client drives granted 290  
 Permitted addresses 104  
 Placeholders 201, 248  
 Port 443 222  
 Port 1493 201  
 Port 3389 222  
 Postscript driver 301  
 Printer driver 297  
 Printer mapping 299  
 Printers in WAN environments 311  
 Print preview 307  
 Process list 327  
 Process list for application sessions 327  
 Profiles 132  
 Profile settings 315  
 Program actions 121  
 Protocol monitor 9  
 Proxy 201, 248  
 Published application 273  
 Published applications 5, 9

---

## R

RADIUS server 191  
 rdesktop using a Java Applet 199  
 RDP protocol 194, 244, 259  
 RDP session 194, 244  
 RDP sessions 244, 259  
 Record Database Viewer 100  
 Registration Wizard 108

Requesting and importing certificates 223  
 Requesting and importing official certificates 81  
 Resources window 95  
 Return values 144, 159  
 Rule 339  
 Rules for determining the launch method 205, 251  
 Running a program in a session 323  
 Running the trace monitor in a session 323

## S

---

Seamless mode 77, 201, 204, 248  
 Security 103  
 Security settings 89  
 Select ICA automatically 205  
 Self-signed certificate 77, 223  
 Sending a message to a session 323  
 Separate session parameters for an application call 281  
 Server certificate 57  
 Service 75, 77, 211  
 Session number 317  
 Session reset 323  
 Session resolution 77  
 Sessions 317  
 Session settings 105  
 Session Sharing 265  
 Sessions in the Windows interface and in the web interface 15  
 Set Client Drive Filter 292  
 Set Client Drive Filter action 292  
 Setting up access privileges for client drives 290  
 Setting up anonymous user accounts 213  
 Setup 107  
 Setup.exe 41  
 Show Information File page 130  
 Show or hide universal PDF printer driver 309  
 Shutdown configuration 159  
 Silent mode 107

Simple modifications to the application launch page 236  
 Single sign-on 103, 254, 255  
 Single Sign-on action 254  
 SOCKS-Proxy 201  
 Sound settings 77  
 SSL connection 221  
 SSLEnable 201  
 SSLProxyHost 201  
 SSL/TLS 201  
 SSL tunnel 9  
 Standard.ndp 255, 321  
 Startup configurations 159  
 Station-based seamless windows mode 9  
 Station database 175, 181  
 Station groups 75, 95, 179  
 Station ID 317  
 Station monitor 9, 101, 175  
 Station names in the terminal server environment 317  
 Station profile 49  
 Station profiles 75, 95, 181, 185  
 Stations 75, 95, 101, 175  
 Statistics 97  
 Statistics program 9, 351  
 Switching the NetMan Internet filter on and off 333  
 Switching the PDF preview on and off 307  
 System Requirements 19  
 System Requirements for Windows Server 2003 Terminal Server 21  
 System Requirements for Windows Server 2008 R2 with Remote Desktop Services Role 29  
 System Requirements for Windows Server 2008 with Terminal Services Role 23  
 System structure 75

## T

---

Table of concurrent use 351  
 TCO 5

TcpBrowserAddress 201  
 TCP/IP 75  
 Technical structure of the NetMan Desktop Client 86  
 Terminal server 132, 194, 244  
 Terminal servers 103, 243, 259, 315, 317  
 Testing an Internet filter file 345  
 The first time an administrator runs NetMan Desktop Client 47  
 The first time a user runs NetMan Desktop Client 51  
 The NetMan SSL Gateway connection monitor 228  
 The sample desktop 115  
 Thin client 5  
 ThinPrint Engine 244  
 Ticketing 285  
 Timeout 121, 122  
 Token systems 9, 191  
 Toolbox 95  
 Total cost of ownership 5  
 TPCInRDP.dll 244  
 Trace Monitor 9, 99, 321  
 Trace Monitor for console messages 99  
 TS monitored processes 103

## U

---

Uniform and centralized administration of all types of applications and hyperlinks 9  
 Universal PDF printer driver 5, 9, 295, 305, 309  
 Universal printer driver 5, 9  
 Universal printer driver in Windows Server 2003 SP1 301  
 URL level 339  
 Use local login data 253, 254, 275  
 Use NetMan anonymous users 253, 256, 275  
 User account 211  
 User groups 75, 95, 132  
 User ID/station ID 103  
 User profile 49, 95

User profiles 75, 183  
 Users 75, 95, 181  
 User-specific program sequences 9  
 User tickets for the web interface 287  
 Using a different published application 281  
 Using a different terminal server 281  
 Using NetMan actions to modify access in client drives 292  
 Using NetMan anonymous user data 211

## V

---

Variable check 132  
 Variables 100  
 Virtual CD 103  
 VPN infrastructure 9, 85

## W

---

Web interface 9, 55, 61, 105, 189  
 Weighting 259  
 Welcome 3  
 Window and audio settings 194, 201  
 Window/Audio settings 244, 248  
 Windows 98 9  
 Windows 2000 9  
 Windows 2003 9  
 Windows Embedded 9  
 Windows NT 9  
 Windows Server 2003 Terminal Server 5  
 Windows Vista 9  
 Windows XP 9

## X

---

XML structures 75







<http://www.hh-ndm.com>