

visionapp Remote Desktop 2010 (vRD 2010)

Convenient System Management



visionapp
Remote Desktop

Product Information

www.vRD2010.com

Inhalt

1	Introduction.....	1
2	Overview of Administration Tools	1
2.1	RDP Administration Tools.....	1
2.2	Access via ICA.....	2
2.3	VNC Management Tools	3
2.4	Telnet and SSH Management Tools	4
2.5	Administration via HTTP/S	5
3	Added Value Through visionapp Remote Desktop 2010	7
3.1	News and Update Page.....	8
3.2	Bulk Import of Servers	8
3.3	Database Access for Increased Flexibility	8
3.4	Display Options	9
3.5	Connection Settings	10
3.6	Configuration Settings.....	10
3.7	Security.....	10
3.8	Reporting.....	11
3.9	Backup and Restore	11
4	External Applications	12
5	Disclaimer.....	16

1 Introduction

Every day, administrators are facing the challenge of having to administrate a large number of remote computers.

This document provides an overview of the fundamental possibilities for the administration of remote computers based on different protocols (RDP, ICA, VNC, Telnet, SSH, HTTP/S). It also looks at how administration tools can contribute to a significantly higher efficiency and effectiveness of IT operations (as exemplified by the visionapp Remote Desktop admin tool).

2 Overview of Administration Tools

This section presents the most common tools used for the administration of remote systems.

A major drawback of most applications is that they have to be started and used in parallel. Normally, it will not be possible to start different tools from a console, manage login credentials centrally or use them automatically for connection purposes.

One exception to this is visionapp Remote Desktop: The administrator is able to use different protocols, store login credentials centrally and assign them to different connection objects. In addition, various useful functionalities provide assistance in daily administration work.

2.1 RDP Administration Tools

Remote Desktop Protocol (RDP) is a network protocol from Microsoft used to display and control desktops on remote computers. It sets the rules for addressing and using Microsoft Terminal Services.

Whoever wants to use Microsoft's Remote Desktop Connection tool has to manually enter the name of the remote computer and the login information. This method is rather cumbersome, in particular if different settings are to be used according to the target system.

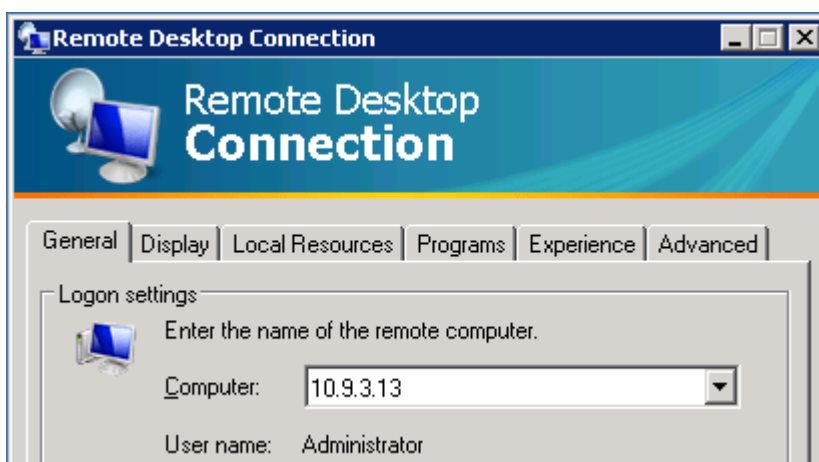


Abb. 1 Remote Desktop Connection from Microsoft

Alternatively, the RDP connections can be saved in separate files, which in turn can be saved in different folders. When handling a large number of systems, there is a risk that the file and folder structure rapidly becomes confusing and difficult to maintain.

These tasks can be organized somewhat more efficiently with the Remote Desktop Management Console – included in the Windows Server 2003 Administration Tools Pack or as snap-in directly under Windows Server 2008.

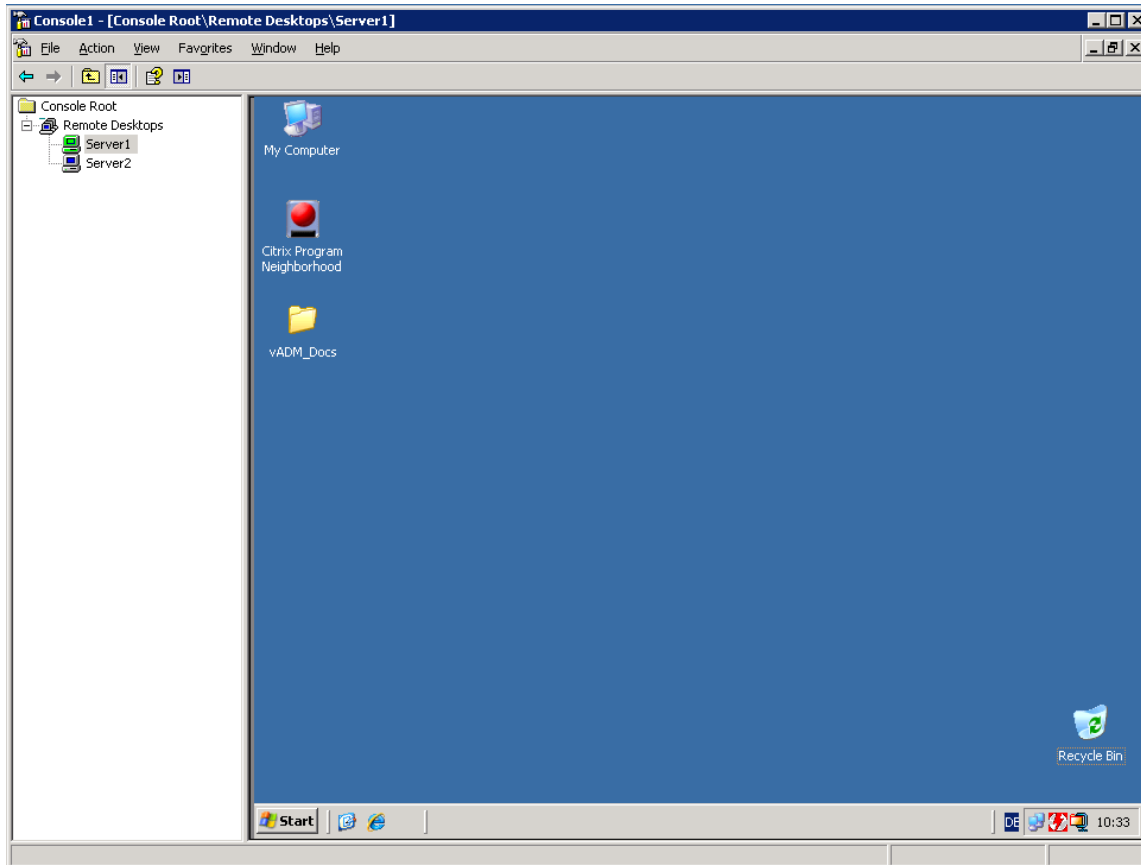


Abb. 2 Microsoft Management Console Remote Desktops – Managing login credentials and folder structures is not possible

However, it is not possible to reasonably organize the connection objects in additional hierarchical structures. Moreover, login credentials have to be assigned to all objects separately – all in all a very cumbersome and inflexible way to work.

2.2 Access via ICA

Independent Computing Architecture (ICA) is a protocol for a terminal server / application service providing system developed by Citrix Systems. The protocol sets a specification for the transmission of data between the server and clients, but it is not bound to any specific platform.

ICA-compliant application products include Citrix WinFrame, MetaFrame and Citrix Presentation Server products. These products allow to run common Windows applications on an appropriate Windows server (or Unix derivate application on an appropriate Unix derivate server), with any supported client able to access these applications. The client platform does not necessarily require Windows, clients for e.g. Macintosh and Unix are supported as well.

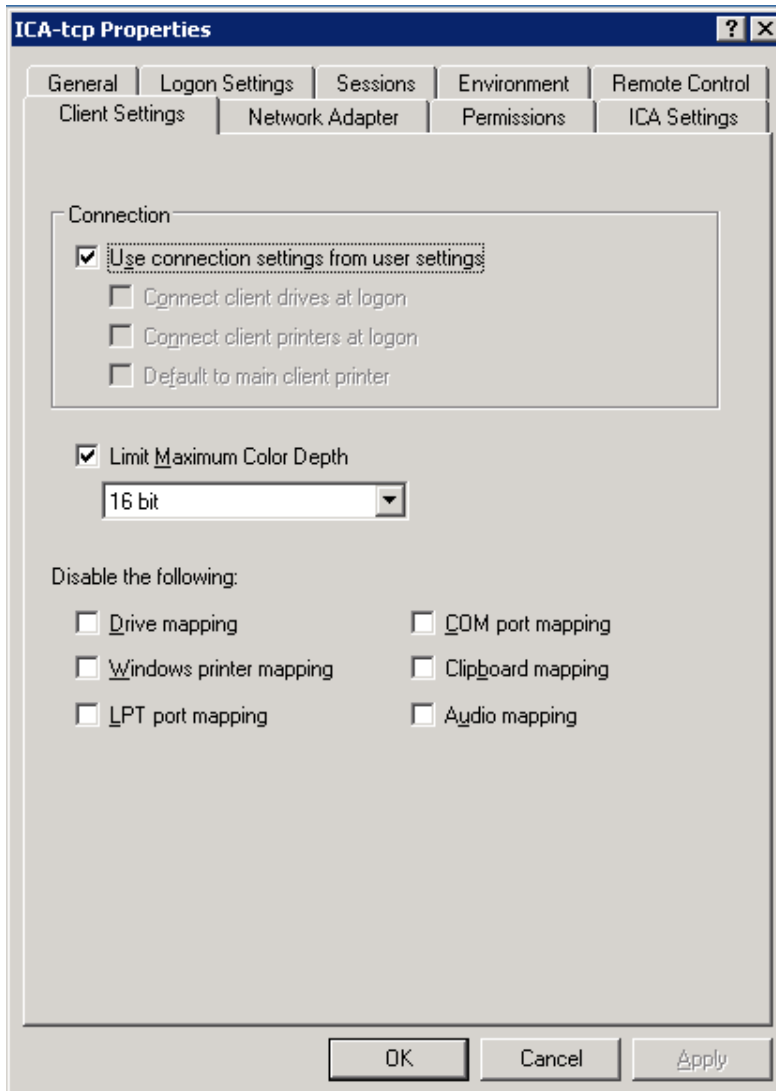


Abb. 3 ICA Client Properties

2.3 VNC Management Tools

Virtual Network Computing (VNC) is a software that displays the screen of a remote computer on a local machine and, in return, sends the local keyboard inputs and mouse movements to the remote computer. This lets you work on the remote computer as if you were sitting at it. Unlike other remote maintenance software, VNC is independent of the platform used. All it requires is running the server component on the remote system and the client component on the local computer.

Known VNC programs that can be used both as server and as client include, for instance, RealVNC, TightVNC or UltraVNC.

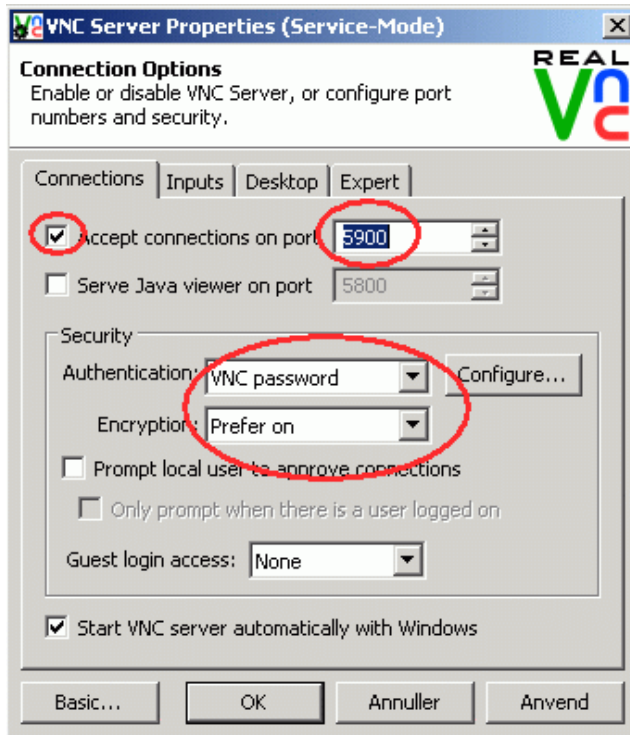


Abb. 4 RealVNC Configuration

2.4 Telnet and SSH Management Tools

Telnet (Telecommunication Network) is the name of a network protocol widely used in the Internet. It is based on a character-oriented data exchange between the client and the server through a TCP connection. Due to the missing encryption it is gradually being replaced by the Secure Shell protocol.

Typically, Telnet is used to establish connections between text terminals and remote computers via a network. Either the establishment of the connection and the tasks of the terminal are performed by a terminal emulator or a terminal is connected to a terminal server that takes care of establishing the connection.

Secure Shell or **SSH** refers to both a network protocol and the corresponding programs that allows to establish a secure connection to a remote computer. This method is often used to transmit a remote command line to the local machine, i.e. the remote console outputs are redirected to the local machine. In other words, the local console is used to output remote inputs while the local keyboard inputs are sent to the remote computer.

SSH allows for a secure, authenticated and encrypted connection between two computers via an insecure network. Thus, it serves as replacement for the earlier rlogin, telnet and rsh protocols, which transmit the entire network traffic without encryption, including passwords. The original purpose was to log on to remote computers via a network (usually the Internet), but in particular SSH-2 is not limited to terminal functions.

Both Telnet and SSH can be used through the free PuTTY tool, a popular SSH and Telnet client.

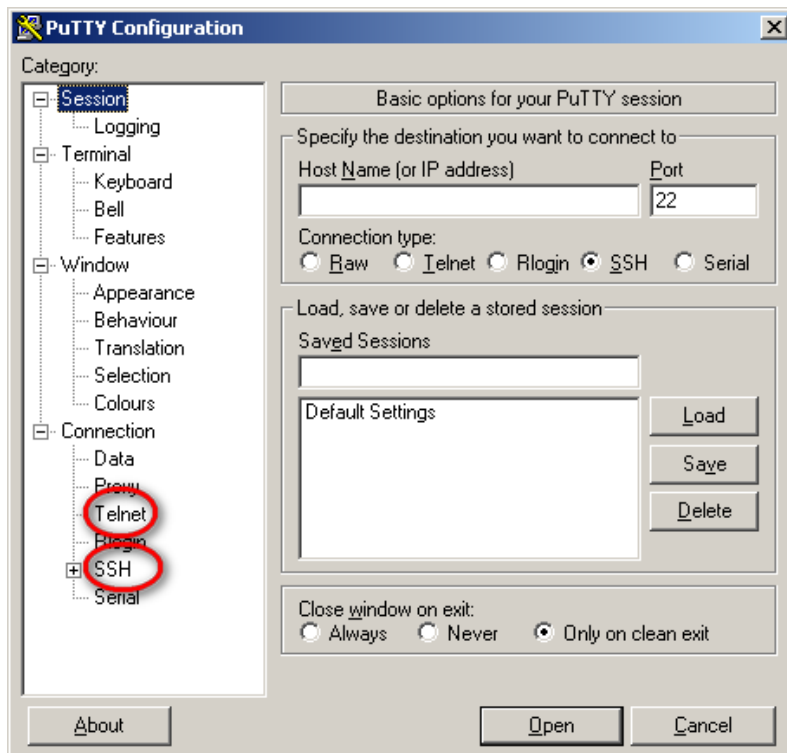


Abb. 5 PuTTY Configuration

2.5 Administration via HTTP/S

In a server-based network, the server components in particular have to be available around the clock. For instance, the domain controller in a global corporation must be able to handle user logins at all times. For the remote maintenance of servers, desktop control, monitoring and file access services alone are not necessarily sufficient to ensure quick response to server errors or perform server management efficiently. When a server crashes, when SCSI, RAID or system BIOS settings need to be reconfigured, or when the server is infected with a virus, traditional remote maintenance services are of no real help – as they all depend on the server to be running.

Using a **Server Management Board** however, the server can be accessed and remotely maintained or administrated at any time, even when the operating system is down. To do so, a connection is established via HTTP or HTTPS following authentication with a username and password.

Moreover, in today's offices many of the existing **end devices** such as copiers or printers are equipped with a browser-based interface. Using that the status and additional information may be retrieved via HTTP.

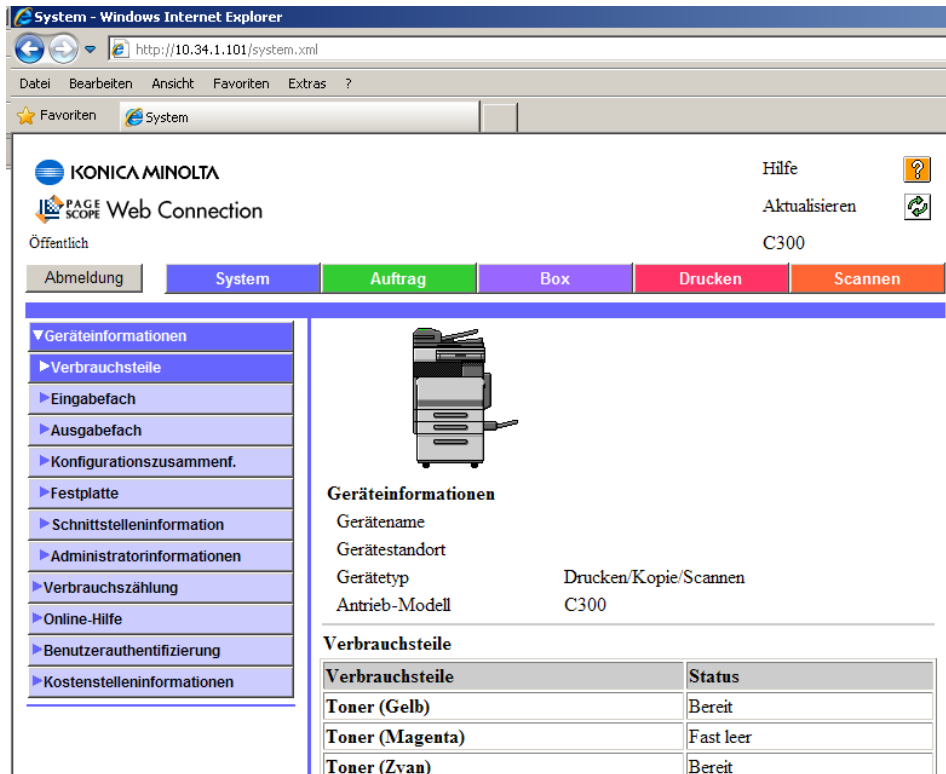


Abb. 6 Remote Management of a Copier

3 Added Value Through visionapp Remote Desktop 2010

With visionapp Remote Desktop 2010 (vRD 2010) the administrator is able to simplify and automate many of his activities – thus saving time every day.

For instance, it is possible to manage all connections in a hierarchical structure of folders and subfolders. This makes locating individual connections much easier and also greatly simplifies management. It is also possible to assign login credentials to these connection objects or entire folders. In addition, the objects can be freely rearranged at any time, for instance to respond to changing business requirements. Also, any new connection object can automatically inherit the settings of the folder where it is located.

A further advantage of vRD 2010 is that it allows to quickly switch between simultaneously open connections. Each active connection is displayed in a tab, in a separate window or in full-screen mode. In the tree view administrators have a complete overview of all connections and their status.

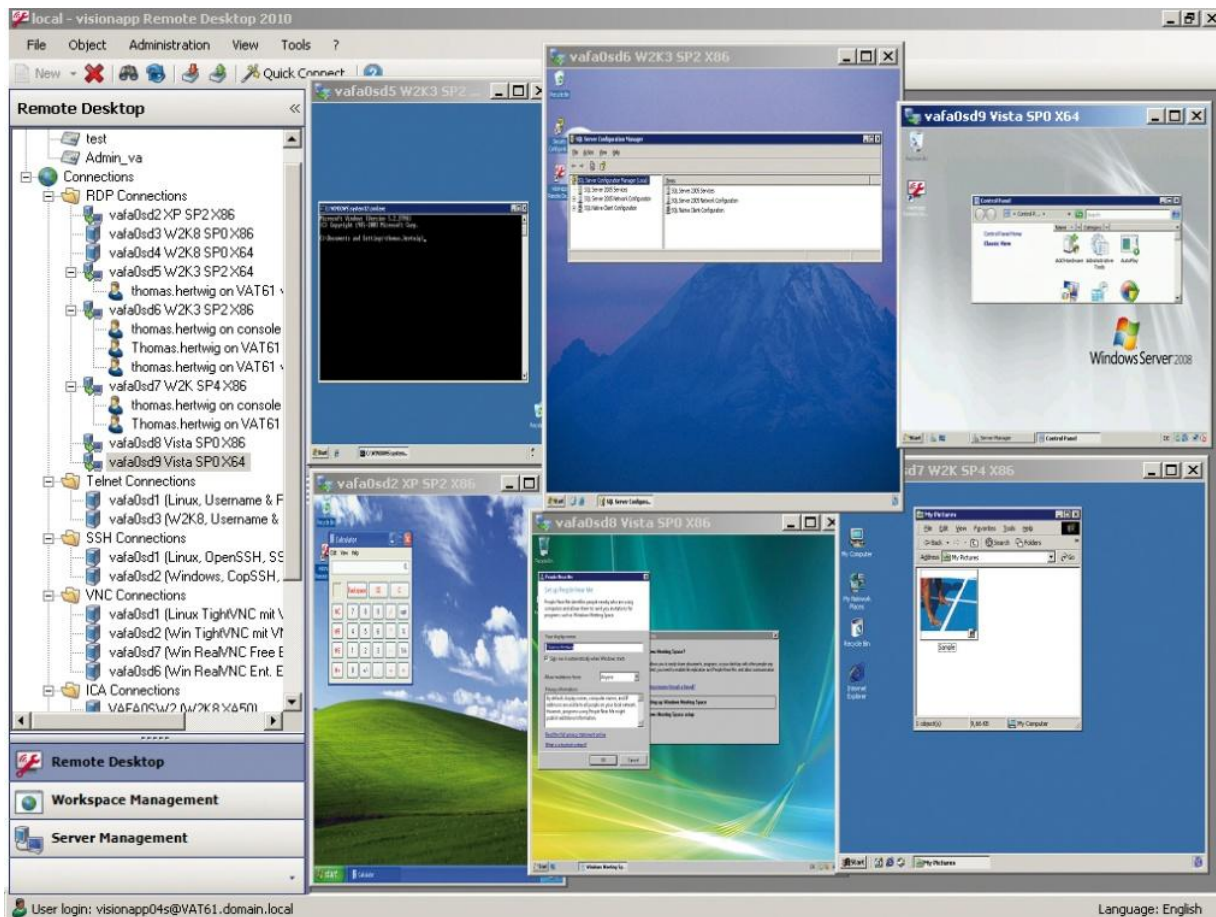


Abb. 7 Overview of the vRD 2010 User Interface

3.1 News and Update Page

Using the News and Update page available directly in vRD 2010, the administrator is provided with current information on updates and the latest tools in real-time. It also provides useful tips and tricks on how to use this remote admin tool.

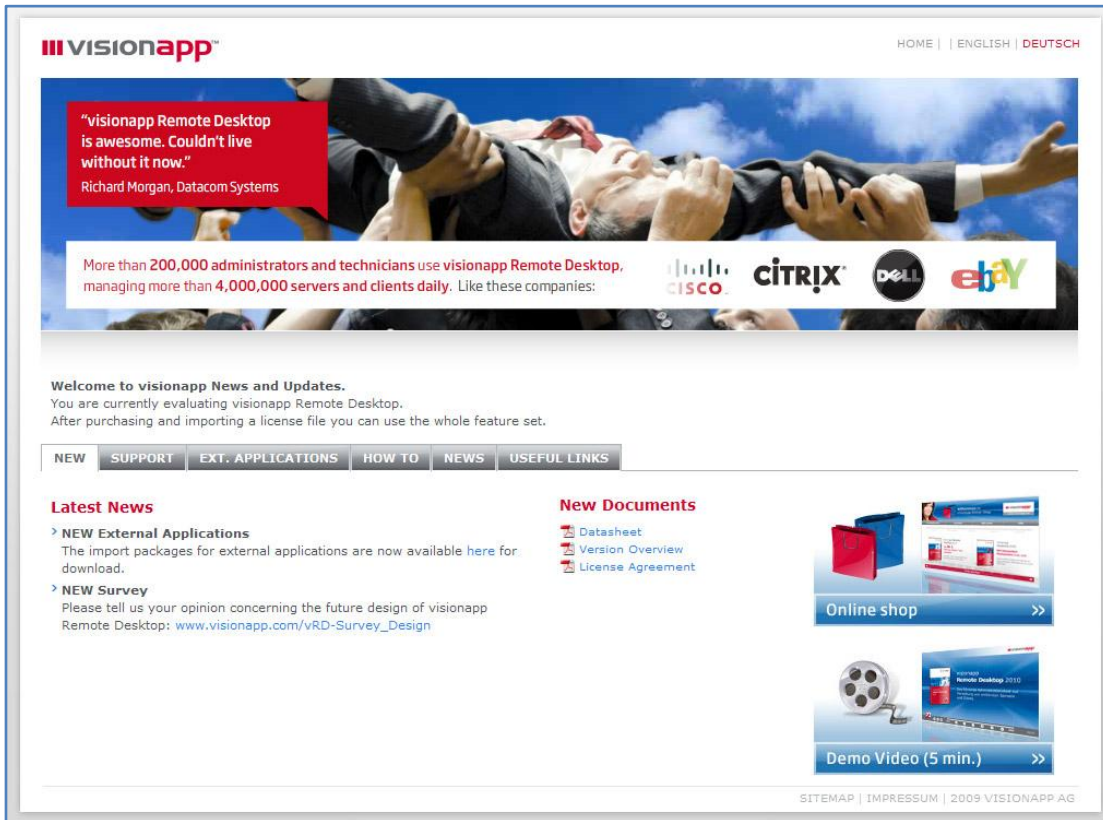


Abb. 8 News and Update Page

3.2 Bulk Import of Servers

A real challenge for any administrator is importing huge numbers of servers. As the standard Microsoft tools require a manual creation of every single connection object, any form of assistance in this area is likely to be at the top of the administrator's wish list. A particularly user-friendly solution is a direct import from the company's Active Directory using a CSV file, as made possible by vRD 2010. When imported, the connection settings for the imported objects can be set separately – irrespective of the settings previously made in vRD 2010.

3.3 Database Access for Increased Flexibility

Depending on the size of the IT infrastructure to be managed, several administrators may have to be able to access the same connections at the same time. This requires saving all settings (login credentials and connection objects) in a central database, password-protected for security reasons.

To prevent unauthorized use of vRD 2010, users or user groups can be provided with specific administrative permissions that limit access to the objects only they actually need for their work.

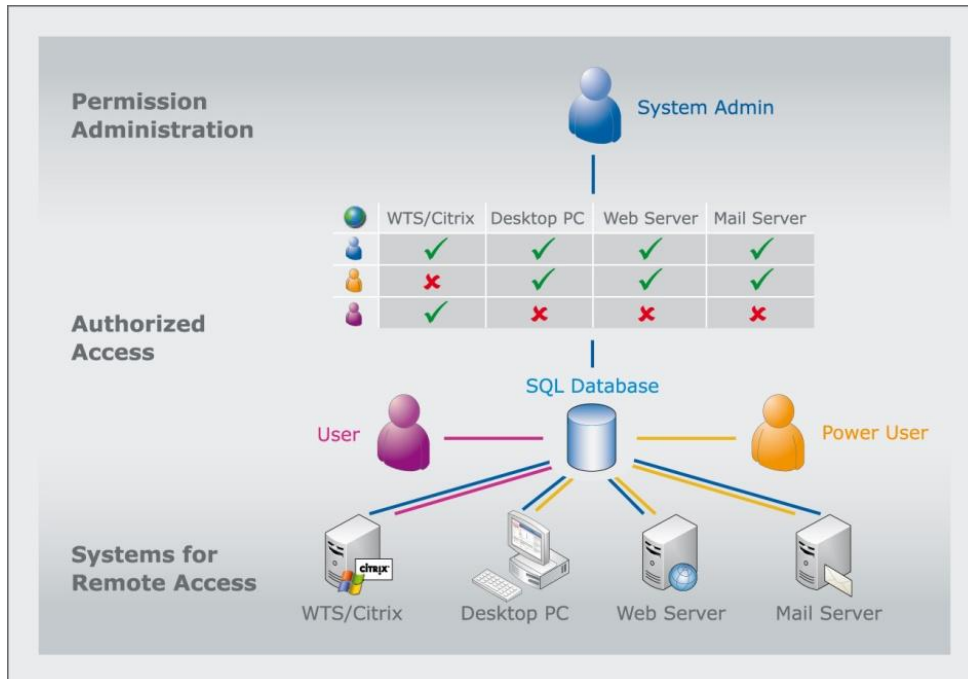


Abb. 9 Administrative Permissions in vRD 2010

In addition, database mode offers further benefits: Logging events, changes and activities ensures the traceability of all operations at all times. Together with the connection history, this provides the administrator with a perfect overview, which greatly facilitates troubleshooting in the event of an error.

3.4 Display Options

The more complex the IT infrastructure, the more difficult it is for administrators to keep track of operations. The overall view of all connected servers, as offered by vRD 2010, is of great help. A wide range of display options allow to rearrange all active connections in different ways. And switching between the different display options is just a few clicks away.

In addition, the administrator can arrange connections individually, for instance to get an overall view of all computers. It is also possible to use colored tabs for more clarity and have the tab title display both the protocol and the login credentials used.

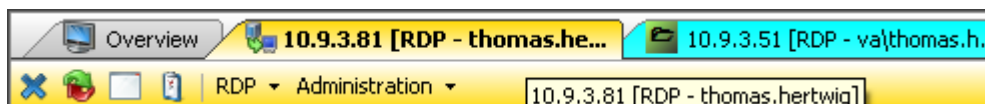


Abb. 10 Custom Display in vRD 2010

3.5 Connection Settings

A major improvement for administrators is the possibility to carry out administrative tasks simultaneously. For instance, using vRD 2010 you have the possibility to simultaneously connect or disconnect all servers within a folder with a simple double-click. Also, the Quick Connect feature allows to start an individual connection without having to create a server object previously.

When a server has to be restarted, vRD 2010 automatically reconnects to this system, i.e. a manual reconnection is no longer required. And for a better overview, the restart of the server is identified in the tree structure by an appropriate icon.

Regardless of the specific settings stored for a connection, vRD 2010 allows to freely select the display mode, the login credentials or the connection protocol from the context menu. The configured settings do not have to be changed to do so.

3.6 Configuration Settings

For administration purposes it is often necessary to have direct access to a server's console, e.g. to terminate an open local connection. Furthermore with vRD 2010, it is possible to automatically start remote servers through Wake-On-LAN (Magic Package) and their MAC address. Moreover, vRD 2010 allows to manage running servers through an existing Management Board (via HTTP or HTTPS).

Default settings such as the color depth, the availability of local drives in the remote session or display options (full screen, separate window, tabbed view) are very easy to set and are automatically applied to all new connections. With the display options set accordingly, the view of a remote desktop is automatically adjusted to the tab size in vRD 2010.

3.7 Security

A major issue in the administration of large infrastructures are so-called orphaned connections. To provide a solution to this issue, vRD 2010 displays all currently active connected users right underneath the server object.

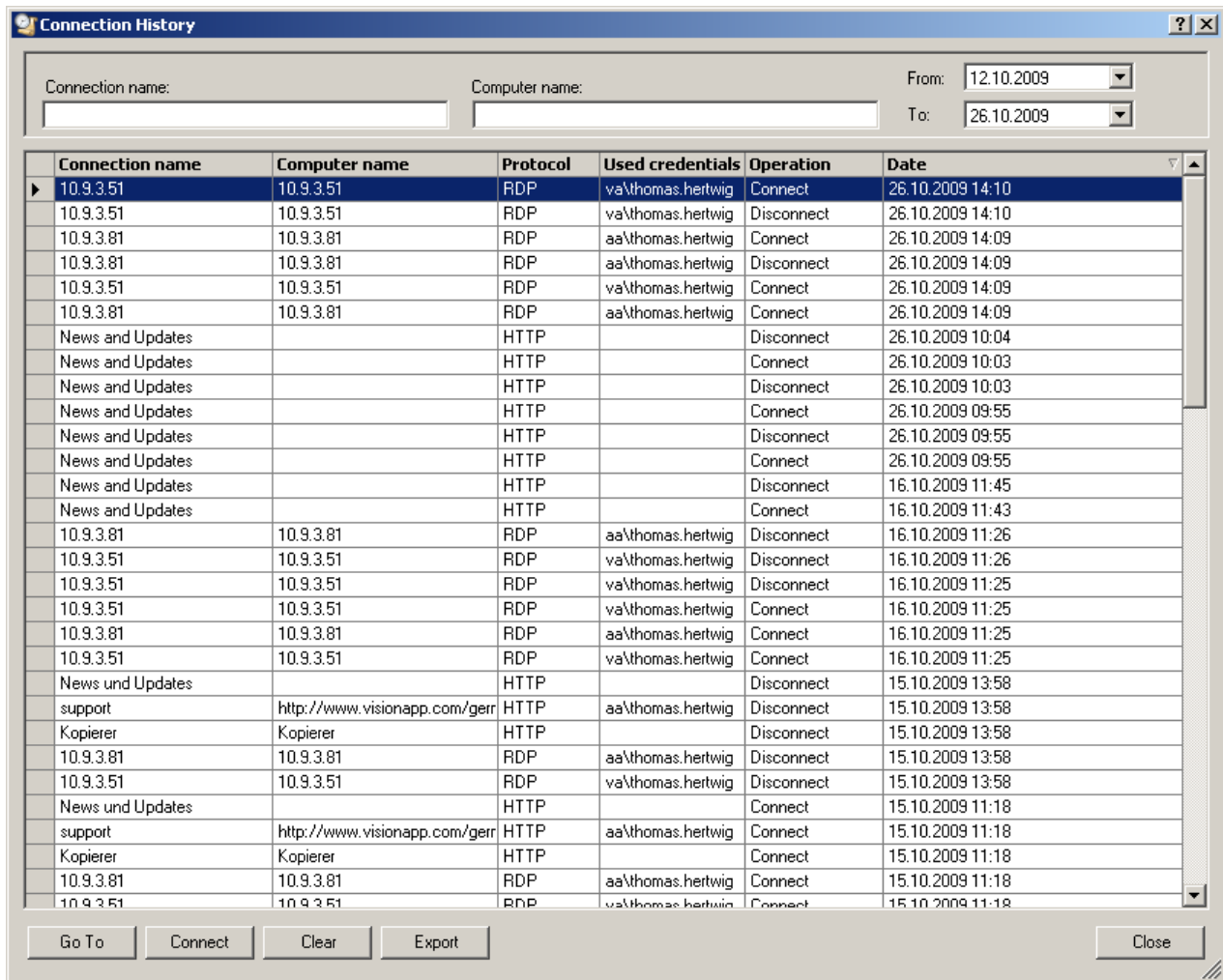
If no active connection to the remote computer is available to the administrator, the still active user sessions are nonetheless displayed underneath the corresponding connection object. From here the administrator can send messages to these users or log off their sessions in order to be able to perform specific tasks in the proper way.

In addition, when accessing remote computers via RDP, the administrator can use a secure server authentication or the Network Level Authentication (NLA) feature. If the RDP port is not to be accessible from outside through the company's firewall, the administrator can use a Microsoft Terminal Services Gateway to access in-house terminal servers.

Moreover, when using VNC or ICA as connection protocol, the administrator is still able to send data encrypted.

3.8 Reporting

In particular environments with a very large number of servers require a comprehensive reporting function. With vRD 2010, the last connections used are displayed in the connection history, including the user and the login credentials used. This allows to locate them very quickly and reconnect them from there if required.



Connection name	Computer name	Protocol	Used credentials	Operation	Date
10.9.3.51	10.9.3.51	RDP	va\thomas.hertwig	Connect	26.10.2009 14:10
10.9.3.51	10.9.3.51	RDP	va\thomas.hertwig	Disconnect	26.10.2009 14:10
10.9.3.81	10.9.3.81	RDP	aa\thomas.hertwig	Connect	26.10.2009 14:09
10.9.3.81	10.9.3.81	RDP	aa\thomas.hertwig	Disconnect	26.10.2009 14:09
10.9.3.51	10.9.3.51	RDP	va\thomas.hertwig	Connect	26.10.2009 14:09
10.9.3.81	10.9.3.81	RDP	aa\thomas.hertwig	Connect	26.10.2009 14:09
News and Updates		HTTP		Disconnect	26.10.2009 10:04
News and Updates		HTTP		Connect	26.10.2009 10:03
News and Updates		HTTP		Disconnect	26.10.2009 10:03
News and Updates		HTTP		Connect	26.10.2009 09:55
News and Updates		HTTP		Disconnect	26.10.2009 09:55
News and Updates		HTTP		Connect	26.10.2009 09:55
News and Updates		HTTP		Disconnect	16.10.2009 11:45
News and Updates		HTTP		Connect	16.10.2009 11:43
10.9.3.81	10.9.3.81	RDP	aa\thomas.hertwig	Disconnect	16.10.2009 11:26
10.9.3.51	10.9.3.51	RDP	va\thomas.hertwig	Disconnect	16.10.2009 11:26
10.9.3.51	10.9.3.51	RDP	va\thomas.hertwig	Disconnect	16.10.2009 11:25
10.9.3.51	10.9.3.51	RDP	va\thomas.hertwig	Connect	16.10.2009 11:25
10.9.3.81	10.9.3.81	RDP	aa\thomas.hertwig	Connect	16.10.2009 11:25
10.9.3.51	10.9.3.51	RDP	va\thomas.hertwig	Connect	16.10.2009 11:25
News und Updates		HTTP		Disconnect	15.10.2009 13:58
support	http://www.visionapp.com/gerr	HTTP	aa\thomas.hertwig	Disconnect	15.10.2009 13:58
Kopierer	Kopierer	HTTP		Disconnect	15.10.2009 13:58
10.9.3.81	10.9.3.81	RDP	aa\thomas.hertwig	Disconnect	15.10.2009 13:58
10.9.3.51	10.9.3.51	RDP	va\thomas.hertwig	Disconnect	15.10.2009 13:58
News und Updates		HTTP		Connect	15.10.2009 11:18
support	http://www.visionapp.com/gerr	HTTP	aa\thomas.hertwig	Connect	15.10.2009 11:18
Kopierer	Kopierer	HTTP		Connect	15.10.2009 11:18
10.9.3.81	10.9.3.81	RDP	aa\thomas.hertwig	Connect	15.10.2009 11:18
10.9.3.51	10.9.3.51	RDP	va\thomas.hertwig	Connect	15.10.2009 11:18

Abb. 11 Connection History in vRD 2010

3.9 Backup and Restore

It is possible to export connection objects to a file and, for instance, re-import them on another PC. Furthermore, a complete backup also allows to store the login credentials. To prevent unauthorized access to such sensitive company information, the data is encrypted (256-bit AES) and password-protected.

The data can be used in both local and database mode. If the latter, login credentials can only be viewed by other administrators if they have been defined as public.

4 External Applications

To administrate computers running different operating systems such as Windows, Mac OS, Unix, Linux, etc., today's administrators need to deal with a wide range of protocols and tools.

To cope with increasing requirements related to security and globalization, the administrators has to take over an increasing number of responsibilities and tasks. In order not to lose track, he has to rely on a variety of administration tools run independently of each other. And he has to keep a permanent eye on these tools to stay informed of the state of the network and the different systems.

To do so, he may use administration tools such as the Computer Management tool as a Microsoft Management Console snap-in. In this case however, he will first have to manually specify the name for the remote computer to be administrated before he is able to access it.

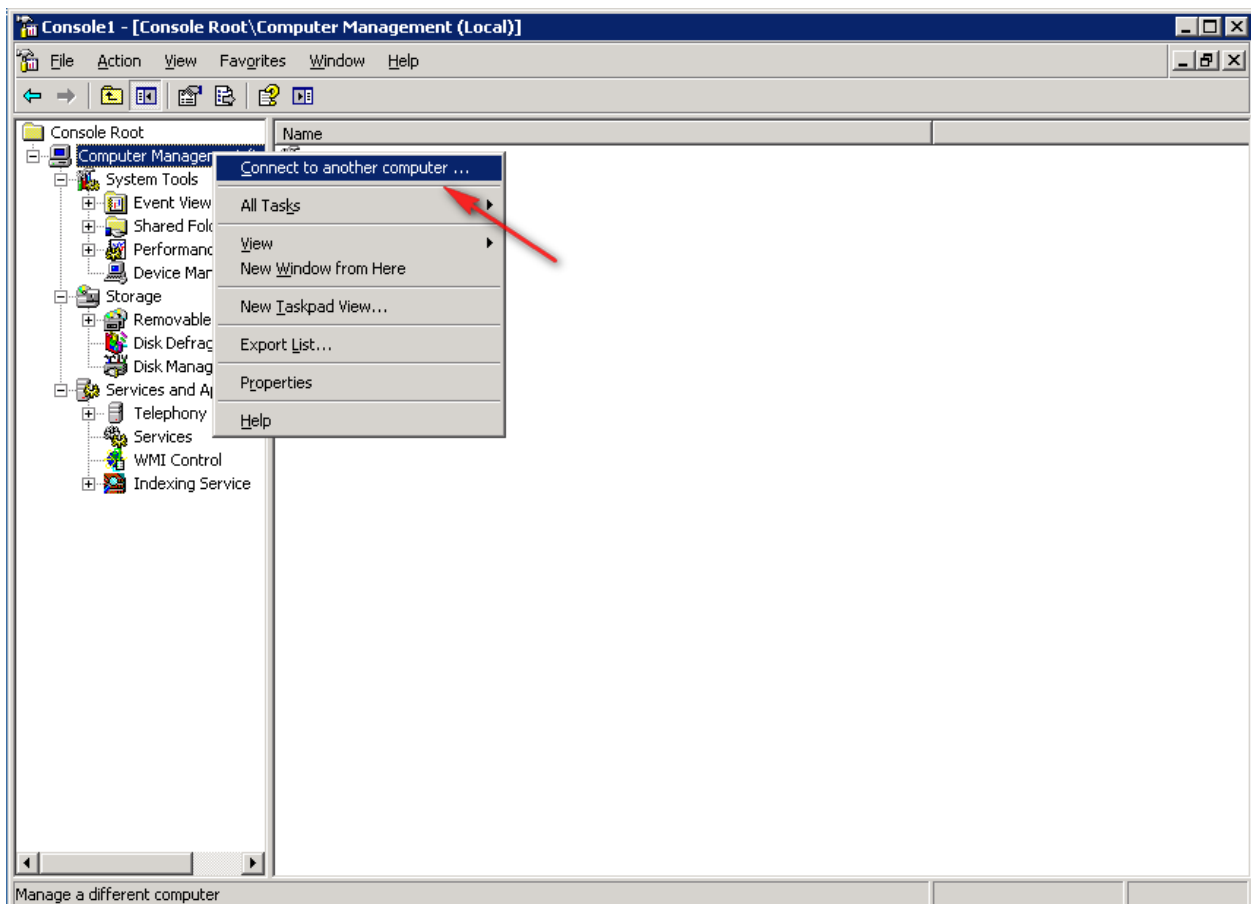


Abb. 12 Computer Management as example for an additional administration tool. The computer to be administrated has to be selected manually.

As opposed to this, vRD 2010 allows to open an external application such as the Computer Management tool together with a connection – thus automatically adding the name of the computer to be administrated. All this requires is storing the appropriate variable (here %computername%) in vRD.

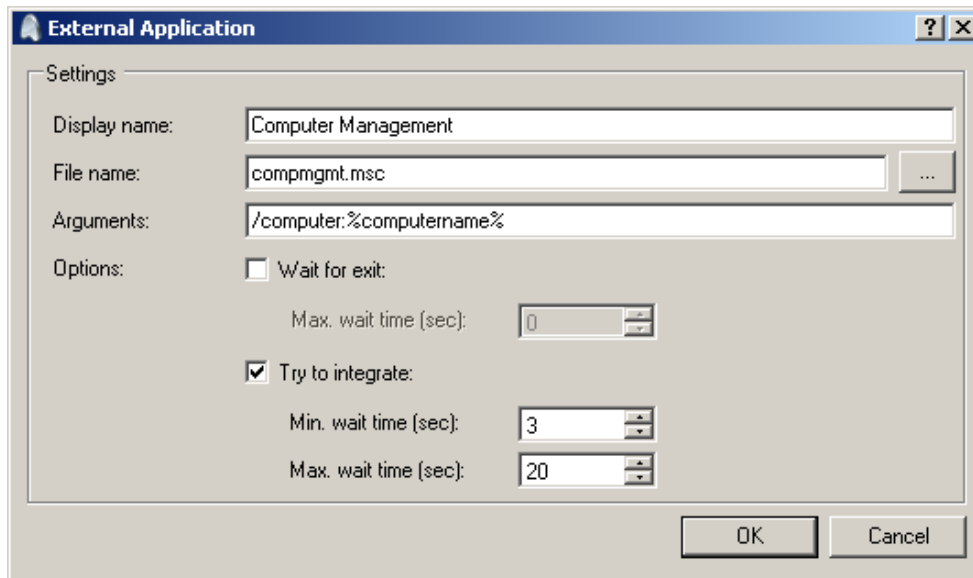


Abb. 13 Settings for the External Computer Management Application

Another scenario is alternate access to various sites, e.g. as service provider. To this end, you first need to set up a secure connection through a VPN tunnel and then establish the connection to the remote systems. Without vRD 2010, this requires a number of manual steps:

Steps prior to access to the system

- > Starting the VPN client
- > Establishing the VPN tunnel
- > Starting the RDP connection to the remote computer
- > Entering the login credentials
- > Accessing the remote computer

Steps after completion of work

- > Logging off from the remote computer
- > Disconnecting the RDP session
- > Launching the VPN client
- > Disconnecting the VPN tunnel

With vRD 2010, all of these steps can be automated. Thus, in the example below, two external applications are assigned to the connection object. The first one (VPN Start) is automatically started before the actual connection to the remote server is established, the other one (VPN Stop) is called when the connection is to be disconnected:

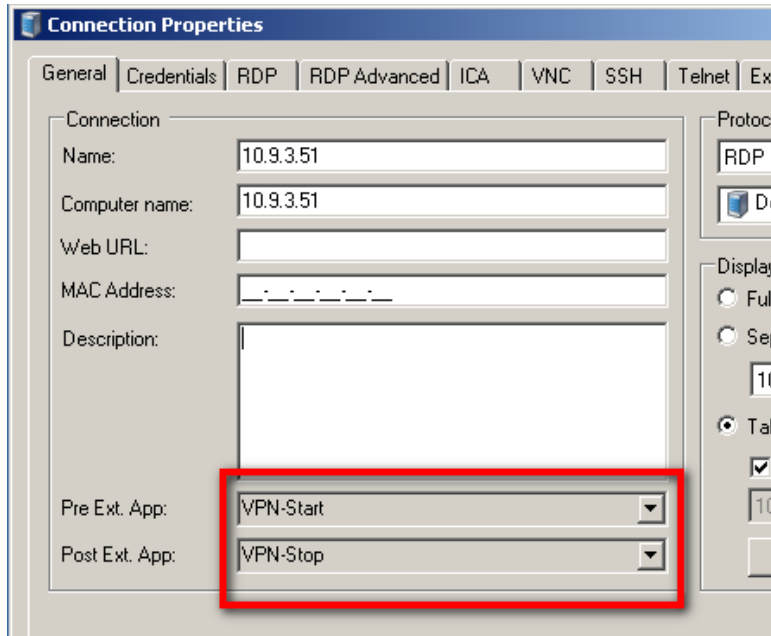


Abb. 14 Assigning External Applications to an Existing Connection

In addition, by assigning the appropriate login credentials it is possible to have the system automatically log on the corresponding user when the connection is activated.

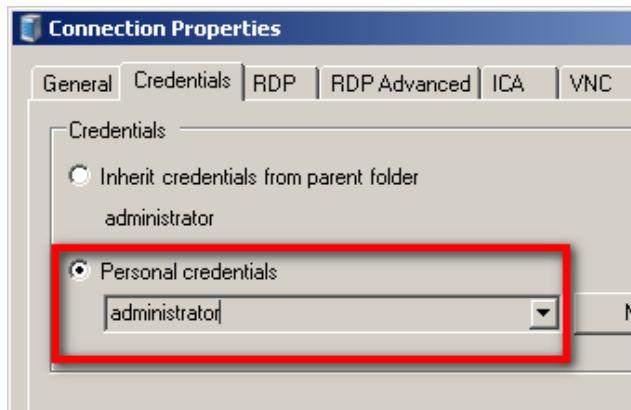


Abb. 15 Assigning Login Credentials to an Existing Connection for Automatic Login

Besides these examples, there is a multitude of other applications that can be used in vRD 2010.

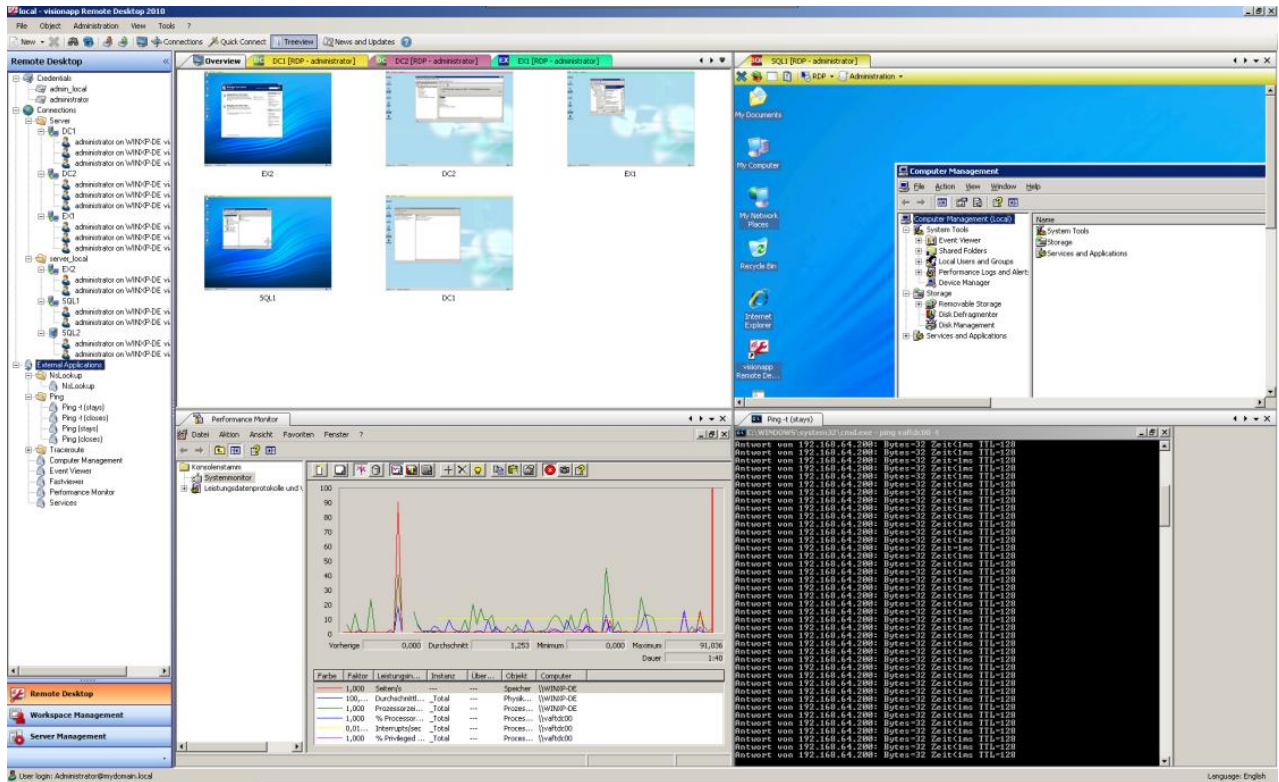


Abb. 16 Integrating External Applications in vRD 2010 (e.g. Ping, System Monitor, FTP Client)

5 Disclaimer

Disclosure and Warranty

The information, concepts, and ideas contained in this document are the property of visionapp AG. No part of this document may be disclosed or reproduced in any form without written permission of visionapp AG. Any violation thereof will be pursued.

All brand names and product names used in this document are trademarks of their respective holders and are recognized as such.

Any product descriptions or representations in this document are for identification purposes only and are not to be construed as a warranty of specific properties or guarantee or warranty of any other type. visionapp shall assume no liability, either explicit or implied, for the documentation.

All rights reserved ©visionapp AG, October 2009

About visionapp

visionapp specializes in the design, implementation and operation of server-based infrastructure and portal solutions based on Microsoft and Citrix technologies. The company provides unique products and services for optimization and cost-effective administration of Windows Terminal Server infrastructures. visionapp Application Delivery Management Suite including visionapp Server Management and visionapp Workspace Management as well as consulting and ASP services form the core business.

The visionapp products and solutions will be provided through a worldwide certified partner network. Only in Germany visionapp delivers products and solutions directly to large enterprises. The SME market is also being supplied through certified partners.

Further Information

visionapp AG
Head Office Frankfurt am Main
Helfmann-Park 2
65760 Eschborn
Germany
web: <http://www.visionapp.com>