

**AMI Education
Solutions Ltd**

Ranger for Networks
Product Information Guide

May 2009

Table of Contents

RANGER FOR NETWORKS PRODUCT OVERVIEW	3
YOUR RETURN ON INVESTMENT	4
THE CHALLENGES FACING ICT MANAGEMENT	5
<i>Local Control</i>	5
<i>Management</i>	5
<i>Visibility</i>	6
THE RANGER FOR NETWORKS SOLUTION.....	7
<i>Local Control</i>	7
<i>Management</i>	7
<i>Visibility</i>	7
RANGER FOR NETWORKS PRODUCT DESCRIPTION	8
LAN RANGER	8
RANGERREACT.....	8
RANGER ADMINISTRATOR	9
RANGER ACCOUNT MANAGER	11
SPACE ANALYSER	12
RANGER PACKAGE BUILDER	12
RANGER WEB TRACKING.....	13
RANGER REPORT MANAGER	13
RANGER UTILITIES.....	14
<i>Disk Quota Management</i>	14
<i>Directory Monitor</i>	14
<i>User Control Panel</i>	14
HOW RANGER FOR NETWORKS WORKS.....	15
RANGER FOR NETWORKS SAMPLE CUSTOMERS.....	16
RANGER FOR NETWORKS FEATURES SUMMARY	17
SYSTEM REQUIREMENTS	18

Ranger for Networks Product Overview

Ranger for Networks is an affordable suite of tools which sits alongside your current operating system, simplifying and enhancing your network and enabling technical staff of all abilities to use their time more effectively

Ranger has been designed specifically for networks where machines are subject to accidental or deliberate configuration changes and tampering. Typically, these are networks where the movement of users is high or the user cannot be forced to take responsibility for any machine that is used. In addition, Ranger is used on networks where statistics and control of machine usage are important.

About Sentinel	Ranger for Networks Key Features
<ul style="list-style-type: none"> • Established in 1999 • 2500 School customers • Used in 25% of Secondary Schools and Academies • Continued rapid growth in Primary schools • Over 50 accredited partners nationwide • Full range of professional services: installation, project management, training, customer support and consultancy. 	<ul style="list-style-type: none"> • Designed specifically for education • Simple to install and easy to operate • Works alongside all Microsoft operating systems including Vista • Requires no new hardware • Scalable for all types of network • Can be installed on one or more servers in a single- or multiple-domain network
Sentinel Support Services and Performance	Sample Sentinel Customers
<ul style="list-style-type: none"> • Web support facility for FAQs, upgrade downloads, etc. • Dedicated team of Helpdesk Engineers and Trainers • Choice of self installation or by accredited partner • Project Management team for larger installations • 82% customer help desk approval* • 92% installation satisfaction* • Sentinel User Group and forum <p>*Performance stats based on 2007 customer survey</p>	<ul style="list-style-type: none"> • Perins Community College • Newcastle College • Falmer High School • Gateacre Community Comprehensive School • Samuel Lucas JMI School • St Thomas More Catholic Comprehensive • Churston Grammar • Ferryhill Business & Enterprise College • Swanmore Middle School • St Joseph's College • Oldway Primary School • The Bridge Academy (PRU) • Mill Chase Community Technology College

Your Return on Investment

How Ranger for Networks efficiency savings can help you reduce costs

By streamlining and automating routine ICT tasks and administration, Ranger for Networks will save a typical school ICT department time and costs equivalent to two technicians a year.

So, as well as freeing technical staff to focus on other activities, you can benefit from annual cost-savings of approximately £20–30k

How? Ranger for Networks works independently, or in harmony with, Microsoft Policies to:

- Simplify PC and network lock-down and security.
- Simplify package roll-out.
- Simplify user and group set-up, configuration and passwords etc.
- Control application usage rights and access privileges.
- Identify any actions which could threaten network integrity or disrupt learning.
- Report on PC, application and licence usage, to facilitate budgeting and asset deployment.

Ranger for Network's 'React' function is frequently used to shut down PCs automatically at the end of the day. Experts' estimate that a single PC left on overnight can cost in excess of £50 pa, in unnecessary electricity. For a school with 200 PCs, using this feature alone, Ranger for Networks could pay for itself in less than 60 days.

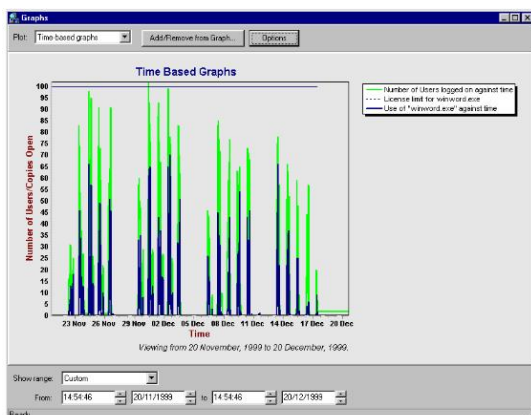


Figure 1 - Sample License Utilisation Graph

The sample graph indicates that for 94% of the time, less than 25% of licences were in use.

The Challenges facing ICT Management

Local Control

Microsoft operating systems such as Windows XP and Vista are now extremely advanced and are thus fully configurable to suit users' exact preferences. Unfortunately, left alone, many of these customisation settings are machine based and will remain in place to affect subsequent users. Similarly, if a user installs software on a machine, then not only may the institution be in breach of copyright and licensing laws, but the software may affect other legitimate programs.

This problem is compounded in establishments where users are naturally inquisitive and whilst maybe not being malicious, do not realise the full impact of configuration changes to other users and network administrators.

To combat this Microsoft provides Group Policy for the centralized management and configuration of computers and remote users in an Active Directory environment. In other words, it controls what users can and can't do on a computer network to restrict certain actions that may pose potential security risks.

Management

From a management perspective, maintaining a PC-based network can be an extremely time consuming task, especially in environments such as schools and offices where users are very keen to customise, modify and personalise their computing environment. A great deal of technician and support time can be expended, even more so if your ICT management personnel change.

The new Multiple Local GPO facility, which is based on layers, can get a bit complicated with three potential local GPOs that can affect any particular user who sits down at the machine. Of course, if the system has been joined into an Active Directory domain, the Active Directory Group Policy Objects take precedence over local policies but it's still not a straightforward business. Then consider the sheer number of GPOs; Windows Vista brings about 800 new policy settings to the table, bringing the total to approximately 3000 possible settings in GPO.

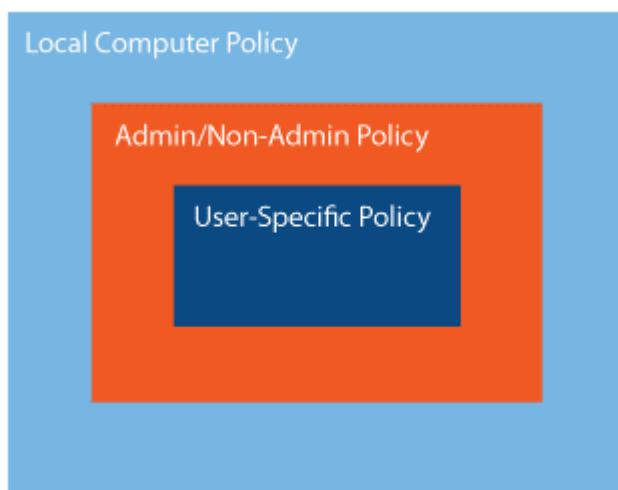


Figure 2 - Users' Total Local Group Policy

Working happily alongside Microsoft GPO, Ranger provides a simple tick box interface for common settings that allow network managers to be confident that machines are protected and letting technicians concentrate on the occasional ubiquitous Windows software or hardware error. Management of Ranger policy settings is straightforward, maintaining the transparency of the

configuration of your network and even offering the opportunity for users unfamiliar with GPO to manage settings.

Visibility

Sometimes the hardest part of network management can be proving that a user was using a particular application at a given time. Traditionally, this logging has only been provided in a static file format involving manual searching to identify the relevant information. In addition, there is typically no central console to show an instant 'real time' view of machine usage.

The Ranger tools return this control to the network manager by providing both 'real time' network control and a comprehensive log of network events. Machines can be controlled to an extent where they can be shut down remotely or 'taken over' for troubleshooting or teaching purposes.

This emphasis on a 'secure and controlled' network where machines are protected with software and the almost 'Big Brother' ethos that all activities are logged can be deterrent enough for even the most determined hackers.

The Ranger for Networks Solution

In response to these challenges the main functions of Ranger can be summarised as below:

	Function	
Local Control		
Changes	Ensure workstations are as secure as possible from accidental or deliberate configuration changes	✓
	Ensure workstations on the network remain consistently configured	✓
Desktop	Ensure users have access to as much of the Windows functionality as possible within the network environment	✓
	Retain the full “look and feel” of Windows without changing the user interface	✓
Management		
Disk Quotas	Provide network administrators with a configurable and comprehensive set of disk quota and space management utilities.	✓
User Accounts	Provide a simple system for adding and maintaining user accounts and associated directory and security permissions on a network server – either individually or as bulk imports	✓
	Enable administrators to take control of the degree to which different users can customise their Windows environment	✓
Drives	Make “illegal” and remove the ability of users to view the local “C” drive, USB drives and selected network drives.	✓
	Remove the ability of users to run system or other “illegal” applications such as Policy Editor, System Editor, DOS sessions, games etc...	✓
Management tools	Provide network based management tools for time restricting applications, licence control, remote management and user activity tracking	✓
Installs	Provide a facility to assist with installation of software across selected machines on a network without the need to visit each one and install manually	✓
Visibility		
Real time view	Provide a network administration system that shows in real time and logs all machine, system, user and application usage across the network	✓
Reports	Produce network-wide reports and graphs detailing application and machine usage over time, licence utilisation, user activity and attempted security violations.	✓

Ranger for Networks Product Description

Ranger consists of a number of different modules that work together to create the controlled network environment. Together this suite of applications form a coherent solution to help you manage your network

- Saves time and effort.
- Simplifies and speeds up repetitive and time-consuming tasks for easier and more effective network management.
- Helps you to tailor your network to your school or college's specific requirements.
- Enables technical staff of all abilities to use their time more effectively.
- Central management of PC configuration prevents unauthorised changes.
- Displays a real-time view of what is happening across the network, so that you remain firmly in control, at all times.
- Enables you to tailor appropriate interfaces for different users, helping to protect your network and your students.
- Provides advanced functionality, so that you can maximise your ICT investments.



LAN Ranger

LAN Ranger is the main network management and control module. This module provides both a 'real time' view of network usage as well as audit and log facilities. Some of the features of LAN Ranger include the ability to remotely shut down or log off machines and display machine usage statistics in graphical or raw data format.

LAN Ranger is used to schedule installation of software 'packages' created with the Ranger RollOut Package Builder module. It is also used to create and manage RangerREACT tasks.

LAN Ranger can be run from a client machine with a more limited range of operations.

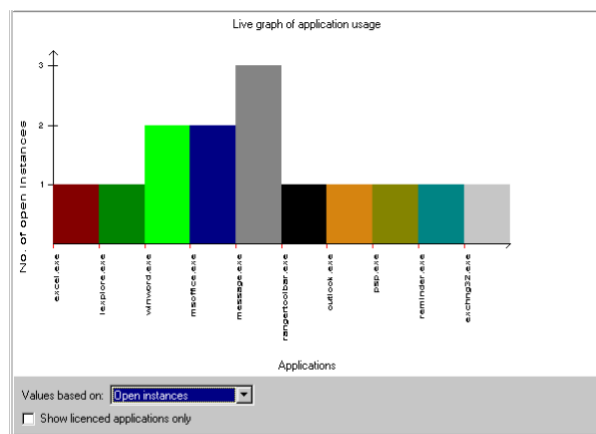


Figure 3 - Application Usage

RangerREACT

This module is responsible for automating responses to network activity and events. It contains pre-built and custom definable templates for automating tasks such as logging off banned users, take screenshots of security violations and shutdown all machines at the end of the day.

In addition, this module allows administrators to build new custom defined responses based on controls, triggers and actions. For instance you may wish to build a customer RangerREACT task such as turning all of the library computers off after a certain period of time.



Ranger Administrator

Ranger Administrator is the single point of management for Ranger. Local Security is configured from Ranger Administrator and is a key Ranger for Networks module designed to work with Windows XP and Vista operating systems. It starts protecting a machine as soon as the operating system starts and remains in operation continuously until it is shut down.

- Close illegal applications by 'Window signature'
- Close illegal applications and dialogs by title
- Remove illegal drives from Explorer and "My Computer"
- Ensure users cannot change to illegal drives by constantly monitoring all dialog entry fields and checking text typed
- Ensure all file dialog boxes default to a pre-configured drive/path
- Customise user environment including desktop shortcuts and start menu
- Remove the ability to edit the path of shortcuts by disabling file fields in shortcut property sheets
- Shut down machine if an attempt is made to terminate Ranger security
- Default open/save path
- Emit a default system sound upon detection of an attempted security violation (optional)
- Send messages to LAN Ranger detailing any attempted security violations
- Securely (i.e. without users being able to bypass the startup folder) start applications either on logon or periodically
- Report details of all applications starting and closing, security violations, log on or off events to the LAN Ranger module
- Interface with LAN Ranger to allow remote control and monitoring of the machine.

Key Benefits

- The user is presented with the standard operating system interface.
- Special Windows keys (DEL, Ctrl-Alt-Del, Escape etc) are not disabled.
- Users have full (but safe) access to Explorer.
- Users can create their own shortcuts (if allowed).

- Users can create folders, copy, drag files and use normal Windows functions.
- Users can use and maintain their home data area.
- Users are not permitted to change any options that would affect the way the machine works for subsequent users.

Key Features

Policy-based security - Ranger deploys policy-based settings as the user logs in to change the user's environment. Policy settings include restrictions to the desktop, to stop a user selecting wallpaper, or changes to the start menu, such as removing the 'run' and 'settings' commands. These settings are defined for each group within Ranger Administrator. Ranger can also co-exist with other policy-based settings (Active Directory) which may be present in the operating system or set up before Ranger was installed.

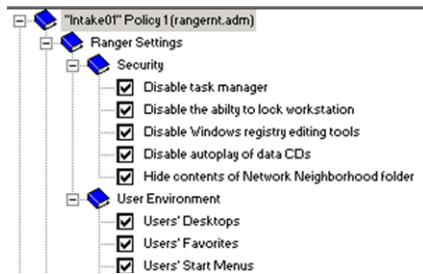


Figure 4 - Ranger Policies Example

File System security - Ranger has been written to restrict the user's ability to browse, change to or view the contents of illegal drives **without** restricting applications on those drives, or physically restricting drive access. This is achieved by monitoring screen dialogs, automatically removing all references to illegal drives from dialogs, and making it impossible for users to change to or browse these drives.

Default open/save path - Windows file dialogs are a set of common controls that applications use to select and name files to be opened or saved. Some applications allow a default path to be defined that will initially be displayed on opening/saving files while many do not. To the user that is not aware of folder structures, drive letters or paths, user data can end up in many different areas. This can cause frustration and lost files. Ranger overcomes this by providing a simple but extremely useful function of detecting when a open/save/browse/close file dialog is opened in any application and instantly changing the drive/folder path to a pre-defined location. All applications will open and save to the same location, including simple applications such as Notepad and Paint. In practice this means that users will always find their data in the same place, never again losing data or accidentally saving it to a local hard disk.

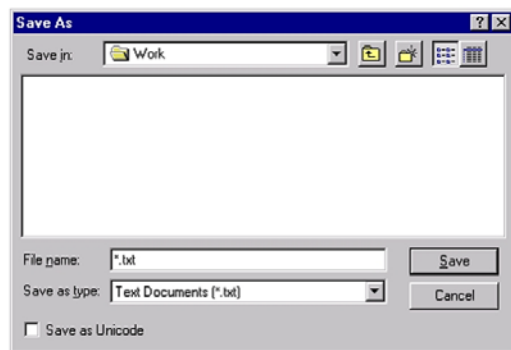


Figure 5 - Save Example

Application security - Ranger has the ability to detect illegal applications from a configurable list and close them as soon as it detects them starting. This avoids the need to remove the executable from the local machine as the only method of security. Ranger does not simply look for the application executable name as this is too simple to bypass. Instead, two methods of defining illegal applications are used: "window signature" and "title checks".

Window signature - Every Windows application contains a unique internal signature that cannot be changed. Ranger detects this as each application starts, and immediately closes the application if it is defined as illegal. The signatures for illegal applications are stored and managed by Ranger Administrator.

Title checks - Some applications use shared components (particularly dialogs), which cannot be made illegal without affecting other applications. Ranger allows the use of the window title text to identify the Illegal window or application. 'Title checking' can be as specific as necessary and can be set to check for exact text matches, text appearing anywhere in a title and text at the start of a title. Title checks are very powerful and provide an extremely flexible method of banning both applications and individual windows. Control panel applets are banned this way, as could any dialog displayed by an application.

Path limitation security - Ranger has the ability to stop a user from launching executable programs (such as .exe or .com) files from designated 'drives'. This allows 'data only' areas for the user and helps to stop the possibility of unauthorised software installation



Ranger Account Manager

Ranger Account Manager is a module designed to assist with the process of creating user accounts on Microsoft Windows networks.

Ranger Account Manager provides 'wizard' based options to create and manage single user accounts as well as facilities for the creation and deletion of multiple user accounts.

User accounts can be generated from any popular file format. The wizard includes sections to determine all aspects of user account creation including account name design, password details and group membership.

Ranger Account Manager is comprised of server and client software. The server component can run on any Windows 2000/3 Server or Windows Server 2008.

It is possible to run Ranger Account Manager Client from any Windows 2000, XP or Vista PC, and can be rolled out to non network administrators to change passwords, providing additional flexibility.

Ranger Account Manager also includes the 'Ranger Migrate' program to assist with moving large amounts of user accounts and data between networks.

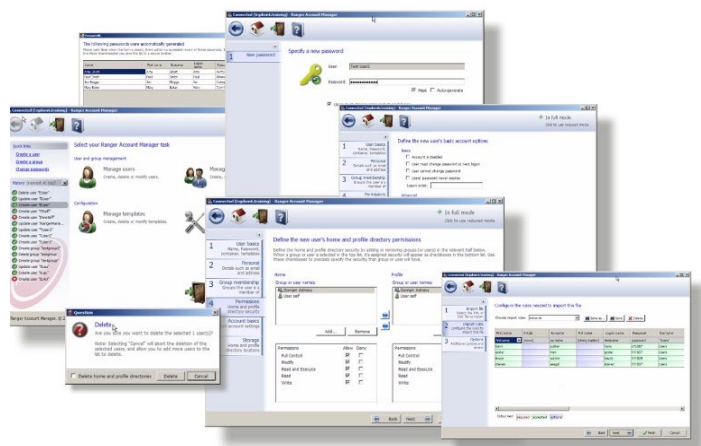


Figure 6 - Ranger Account Manager



Space Analyser

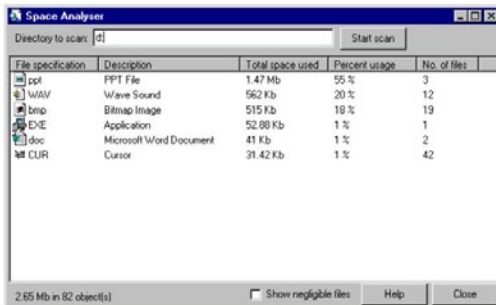


Figure 7 - Space Analyser

Space Analyser is a simple utility that provides an in-depth analysis of disk usage by file type.

The application gives a summary of how many files of each type exist, how much disk space they take up and what percentage of the disk is used up by them. It can also be used to identify file extensions that are being renamed deliberately to avoid detection by Directory Monitor

Like Directory Monitor, Space Analyser is most commonly run from a server, as this is where the source data will reside although it can be run from a client machine if required.



Ranger Package Builder

Using Ranger Package Builder involves two programs. Package Builder is used to create, edit and delete packages. *LAN Ranger* is used to schedule and manage package rollouts.

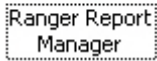
Package Builder is used to create a self-contained software installation package for scheduled 'roll out' to Ranger clients. The package contains all files, shortcuts and registry modifications that were performed by the manual software installation process.



Figure 8 - Package Builder



Ranger Web Tracking



Ranger Web Tracking is a module designed to assist Network Managers in monitoring internet usage on a per group basis, without the need for any new hardware.

Ranger Web Tracking is essentially invisible to the Administrator as well as to the end users. There is no visible indication that a user's web usage is being monitored.

You are able to turn Ranger Web Tracking on or off for the entire site, as well as on or off on a per group basis. The default option is 'on' for all groups and the site.

Ranger Web Tracking Reports are generated with the Ranger Report Manager. Please refer to the section titled Ranger Report Manager for more information regarding the reporting functions.



Ranger Report Manager

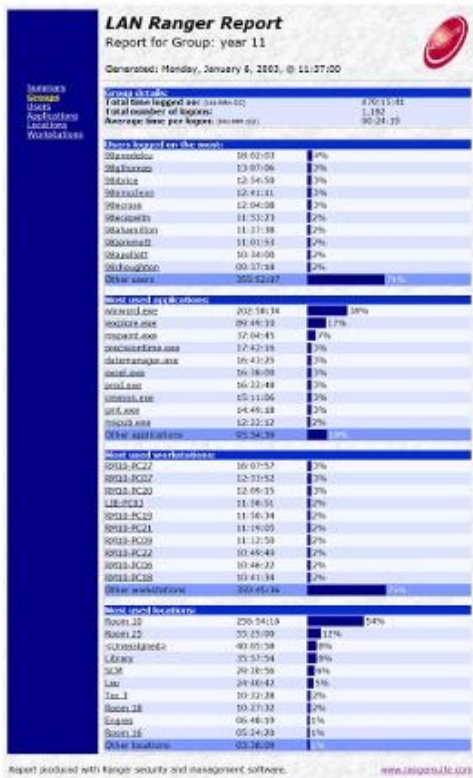
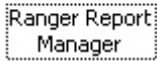


Figure 9 - Group usage report

Ranger Report Manager is an application which will enable Network Managers to generate reports based on the relevant Report Packs* installed.

Reports generated through the Ranger Report Manager can be custom defined, which means that you need to request specific data to report on, or run as summary pre-built templates that you can then analyze and drill down through.

Generated reports are saved in an HTML format and are viewed through the Ranger Report Manager application. Reports can also be saved in XML format which will allow them to be imported into many 3rd party reporting engines.

The Ranger Report Manager application can be installed onto any workstation on the network. It is installed by default onto the Network Ranger server during an upgrade or new installation.

*Report Packs will be released as they become available...

Ranger Utilities



Disk Quota Management

This module consists of three programs. Quota Enforcer checks the user 'home' area regularly to see if the user is over their group quota of disk space. If so, a constant dialog appears warning the user to resolve this.

Quota Explorer is a secure 'Windows Explorer' interface that allows management of the user home area. All files and folders are displayed along with statistics such as file size, data and overall percentage of disk space used. The user can also use My Computer and Windows Explorer to manage their space if these programs are available to them.

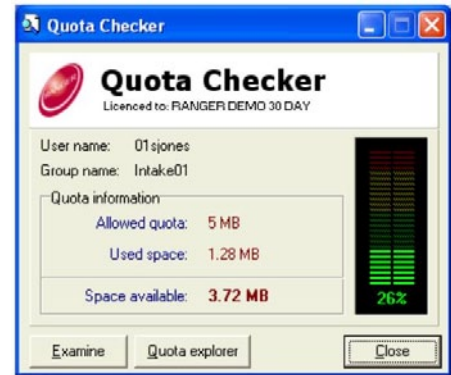


Figure 10 - Disk usage

Quota Checker is a program for users to be pro-active about their disk space usage. It gives details on the current disk space used compared to the total allowed as well as providing access to Quota Explorer.



Directory Monitor

Directory Monitor is a tool to 'police' the user storage areas. In a large network, there can be as many as 2000 of these areas full of data and Directory Monitor is used to 'scan' these for illegal data types.

Areas can be searched for illegal file types, date and time specific files or files larger than a certain size. Once these files have been identified, they can be moved, copied, deleted or just logged as proof that a user was in possession of them.

Directory Monitor can be run regularly for housekeeping purposes, deleting temporary files, work files or data from disused home directories.



User Control Panel

User Control Panel is a simple interface to allow users some control over their personal settings. Specifically, it has a section to allow the user to change their password. This stops the need to grant access to the system 'Control Panel' section. Other features include changing mouse configuration, setting a custom background or colour scheme from an 'allowed' list and a simple personal scheduler.

How Ranger for Networks Works

Installing Ranger for Networks onto a new or existing network is easy. In less than 10 minutes your computers can have the additional security and benefits of Ranger software. Ranger Server software is installed on your own domain controller, while client software is installed remotely to each pupil and teacher workstation.

Ranger is designed to install either into an existing network structure or as part of a new installation. The installation of Ranger on the server will have no affect on the users or computers until the client software is installed onto the workstations.

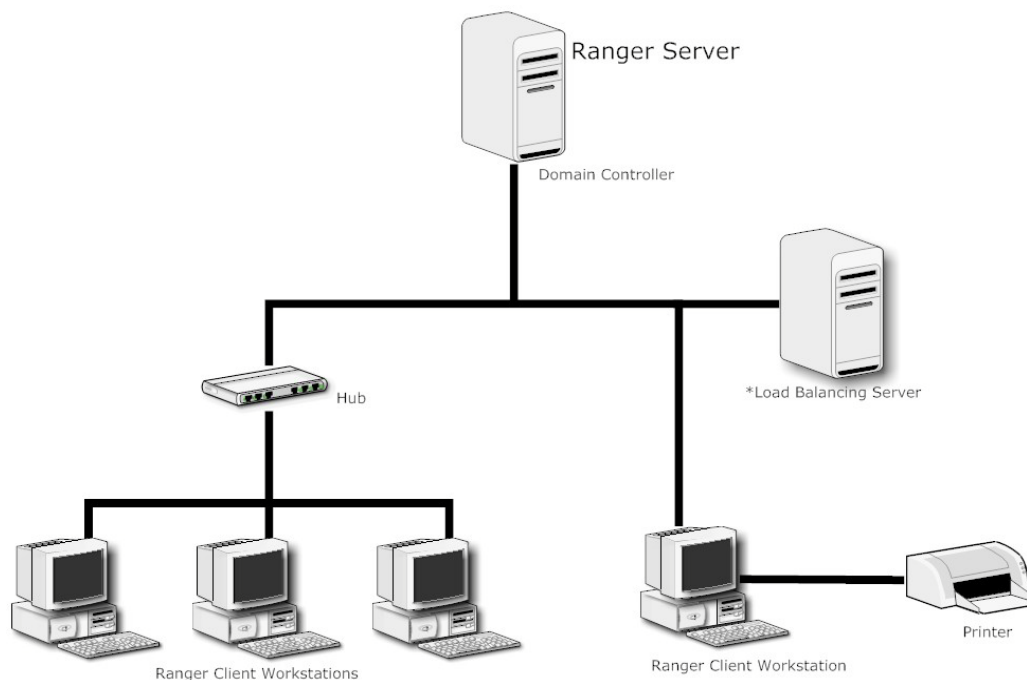


Figure 11 - Simple Ranger for Networks example

A Ranger installation consists of three main phases:

- Phase 1** Core Ranger system files are copied to a central location on the server. Start menu folders and shortcuts are created and the product licence information is entered.
- Phase 2** Ranger is configured utilising the group structure in place. Default options such as security and disk quota are decided.
- Phase 3** The Ranger client software is 'rolled out' to machines attached to the network. Ranger security and other facilities are then active and available for use.
- Phase 4*** Ranger is 'extended' on to another server for load balancing and fault tolerance. Core Ranger files are copied to this server and then it is 'linked' to other Ranger servers to share information.

** This phase is optional*

Ranger for Networks Sample Customers

“Ranger is used in 25% of all UK Secondary Schools and Academies”

Sample Large Installations

Customer	Number of PCs	School Type
University of East London	3500	University
People’s College	2000	College
Middlesbrough College	1550	College
Newcastle College	1850	College
Oxclose Community	800	Secondary
Gateacre Community Comprehensive School	750	Secondary
Sacred Heart RC Primary	250	Primary

Sample customers

Primary Schools	Secondary Schools	Academies
Ash Grange Primary School	Ashburton Community School	Ashcroft Technology Academy
Batling Brook School	Bedford Modern School	Bradford Academy
Canberra Primary School	Cambridge School	Bridge Academy, Hackney
Epson Primary School	Coulsdon High School	City Academy Bristol
Gorse Hill Primary School	Dartford Grammar School for Boys	Charleston Academy
Grange Primary School	Gartree high School	Harris Academy
Langley First School	Guildford County School	Lambeth Academy
Montpelier Junior School	Hayesfield School	London Academy Barnet
Meadows Primary School	Hodge Hill Girls School	Marlow Academy
Petts Hill Primary	Inverness High School	North Sefton City Learning Centre
Sandwich Junior School	John Bramston School	St Josephs Academy
Seaview Primary School	Lady Manners School	Wallasey School
Springfield Primary	Manchester High School for Girls	Walsall Academy
Sun Hill Infants School	Newcastle high School	Westminster Academy
Tyne View Primary	Perins School	
Underhill Primary	Reigate School	
Waverley Primary	Sutton Community High School	
Wingove Primary	Tonbridge Grammar School	
Yardley Primary School	West Bridgford School	
Yorkemead Junior School	Wye Valley School	

Ranger for Networks Features Summary

Ranger for Networks provides a layer of additional security, simplifies complex processes, automates repetitive tasks and provides a real-time view of your network and user activities.

Key Features	
Centralised Workstation Management (Accounts, User, Security, Shell)	✓
Bulk User Import – saves time when administering large volume of users	✓
Scheduled deployment – Minimise impact to users	✓
Web Tracking – Report on internet usage	✓
Policy & Security – Default policy and security templates	✓
Reporting – Visibility of network usage	✓
Live View – Real time view over the network, PC and users	✓
Alerts/Alarms - Inform users that their actions are being monitored	✓
Automated Tasks – Create automated responses to network events	✓
User Defined Reporting	✓
Vista and XP simultaneously	✓
Tools to assist Password maintenance	✓
Bulk change password	✓
Change password only (Staff Mode)	✓
Mask or clear password - Suitable for non-technical users	✓
Random password generation – simplifies complex password policy	✓
Automatically Turn Off PCs – Save Energy and Costs	✓
Remotely Start and Stop Applications – Control Software Usage	✓
Stop programs running from removable devices – Protect your network	✓
Stop configuration changes	✓
Limit access to CDs, Floppies, USB Drives, etc	✓
Stop Logon by location – stop unsupervised access	✓

System Requirements

Software	Ranger for Networks or Ranger Primary
Server	Minimum CPU Requirements for OS
Server Operating system	Windows 2000/2003 Server Windows Server 2008
Server RAM	Minimum 16MB
Other	250MB hard disc free space
Client PC	Minimum CPU Requirements for OS
Client OS	Windows 2000 Professional Windows XP Professional WINDOWS VISTA Business, Enterprise, Ultimate 32-BIT EDITIONS
Client RAM	Minimum RAM Requirements for OS

If you have any queries regarding system pre-requisites, please contact your Ranger reseller or visit the Ranger web site: www.rangersuite.com