

Sentinel Products Ltd | **Ranger for Networks**

Release Notes

December 2007

Table of Contents

1.	RELEASE SUMMARY	3
2.	RELEASE VERSION.....	3
	2.1 Supported Servers and Versions	3
	2.2 Supported Clients and Versions	3
3.	NEW FEATURES IN THIS RELEASE	3
4.	ERROR CORRECTIONS	4
5.	KNOWN ISSUES.....	4
6.	NOTES	4
7.	FEATURE LIST	7

1. RELEASE SUMMARY

Note: All updates since the last release can be found in [blue](#)

Upgrades are only supported from 3.x onwards

[Microsoft Windows Vista 32-Bit compatibility](#)

[Separate handling of policies for Windows Vista](#)

[Redirection of local content from local computer to network under Vista policies](#)

[Title Scanner to help with title check rules](#)

[Lan Ranger defaults to a plain background](#)

[Ranger Administrator defaults to a plain background](#)

2. RELEASE VERSION

Ranger for Networks [5.9](#)

Ranger Primary [5.9](#)

2.1 Supported Servers and Versions

Windows NT Server v4.0 (service pack 6a or later recommended)

Windows 2000/2003 Server

2.2 Supported Clients and Versions

Windows NT Workstation (SP6a)*

Windows 98 (1st or 2nd edition)*

Windows Millennium Edition (Me)*

Windows 2000 Professional

Windows XP Professional

[WINDOWS VISTA Business, Enterprise, Ultimate 32-BIT Editions](#)

3. NEW FEATURES IN THIS RELEASE

- [New Environment branch in Ranger Admin to handle Vista profile & policies.](#)
- [Introduced Vista branch profile redirection policies to control security permissions](#)
- [Redirection will move content from local computer to network](#)
- [Branches of the Environment in Ranger Admin can be hidden. There is a prompt on first start-up to determine which branches \(9x/Me versus NT4/2000/XP versus Vista\) are relevant. Users can change which branches are hidden in Edit/Settings/Environment at any time.](#)
- [Ranger Admin expects RangerVista.adm file with Vista policy definitions](#)
- [Additional ADM policy files **cannot** be imported for Vista.](#)
- [Ranger Admin will inform users of what's new. The displayed text is fetched from 'WhatsNew.rtf'. This is a new file.](#)
- [Ranger Admin 5.9 cannot upgrade sites using Ranger 1.](#)
- [Ranger Admin will generate additional .rrg files suffixed 'Vista.rrg' in the 'Control' directory.](#)
- [Ranger Admin will generate 'VistaGroup.rpl' and 'VistaComputer.rpl' files to store policy settings.](#)
- [Ranger Admin will store Vista profiles under the 'Profiles\Vista' directory.](#)
- [TitleScan.exe allows the user to capture the window title in hidden windows. Initially intended for Vista where some windows \(e.g. Explorer and Internet Explorer\) show no title. The title can be copied to the clipboard.](#)

- TitleScan runs on Windows 98 and later (it will not run on Windows 95).
- TitleScan can be launched from Ranger Admin Title Checks page.
- The new Paste button on the Ranger Admin Title Checks page will initiate creation of an illegal text rule using the text in the clipboard.
- The Ranger icon is displayed in the Notification Area (shell tray) on Vista computers. When clicked, the Ranger splash dialog is displayed showing details such as User Group, User Name, Audit Server, etc. The splash dialog is the same as in Ranger 5.7.
- No splash dialog is displayed during logon on Vista computers
- SecMon will merge a PreShellVista.rrg file from the root of the server's Ranger directory into every Vista users' registry.
- Ranger Manager (Client installation program) now prevents install on 64-bit operating systems
- Fail-safe mode allows members of local administrators to logon to workstation. Only local administrator user used to have fail safe mode but this account is disabled by default in Vista.
- New application called StartRgrMan.exe which is used to launch the existing rgrman.exe. StartRgrMan.exe exists so it can request the appropriate elevated security that rgrman needs when running under Windows Vista.
- With the addition of a separate workstation module (RgrUsrDaemon), Active Security is supported under Vista.
Note: installonvista.txt must be present in the server's ranger directory for rgrman to allow an install on a Vista workstation
- Changed Ranger Administrator Environment Policy Description pane background colour to white

4. ERROR CORRECTIONS

- Resolved a multi-core processor issue which would sometimes cause Application Banning to match applications which are not banned

5. KNOWN ISSUES

- Bug introduced to the web tracking component which stops log files being created. This disables the ability to report on web traffic
- Uninstalling Ranger for Networks Corrupts Ranger Reporter
If Ranger for Networks is removed and Ranger Reporter is retained, then the Ranger Reporter Engine fails because it cannot open the web tracking package file 'WT Pack.ini'
- Double Right Click Needed in Ranger Admin
To obtain the context menu in Ranger Admin Profile Desktop you have to double right-click

6. NOTES

Based on the analysis performed below, it is decided that Ranger 5 only needs the following Active Security features to work under Windows Vista:

- Application Banning
- Title checking

What is active security?

Application Banning

What is it?

Should be more accurately referred to as application window banning as it does not ban an entire application; it “bans” windows by window class identifier.

Do we need it under Vista?

There are no technologies available under Vista that render Application Banning obsolete. Therefore to support the existing Ranger 5 feature set under Vista, Application Banning must be available.

Title checking

What is it?

Effectively “bans” windows by matching the text present in its title bar to a list of banned titles.

Do we need it under Vista?

There are no technologies available under Vista that renders Title Checks obsolete. Therefore to support the existing Ranger 5 feature set under Vista, Title Checks must be available.

HTML frame analysis

What is it?

A technology which analyses any locally-loaded html document for inline frames <iframe> which point to a disk resource banned by drive security. Any browsers displaying such a document are closed.

Currently only protects Windows 9x workstations running Internet Explorer; relies on policies to stop unauthorised disk resource access in other environments.

Do we need it under Vista?

No, for the same reasons that we don't need it under Windows XP.

Integrity Constraints

What is it?

Integrity constraints lock down miscellaneous parts of the Windows operating system. These parts are:

- Registry Editor
- Outlook Find
- Windows 3.1 File Manager
- Shortcut properties sheet
- Explorer options
- Disk resource banning through title bar parsing for:
 - Explorer
 - Internet Explorer
 - Explorer “open” (Cabinet) window
- Find: All Files
- Find: Computer
- Go To Folder
- Map Network Drive
- Disconnect Network Drive
- Run Application

Do we need it under Vista?

Almost without exception, integrity constraints only bring a security benefit to Windows 9x systems. NTFS permissions and Windows Policies lock down most of the above list adequately on modern operating systems.

Open/save path defaulting

What is it?

When an open or save common dialog is first displayed, it’s initial path is reset to the default open/save path set in Ranger’s configuration. This is done by disabling all controls on the dialog and automatically “typing” the absolute path into the dialog and “pressing” enter.

Do we need it under Vista?

Most modern applications, including Vista, honour the “User Shell Folders” registry value for My Documents and therefore already default themselves to the correct place. Even for applications which don’t honour this registry value, NTFS permissions should stop users opening or saving where they shouldn’t.

Therefore it is concluded that this feature is not needed for Vista.

7. FEATURE LIST

- 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