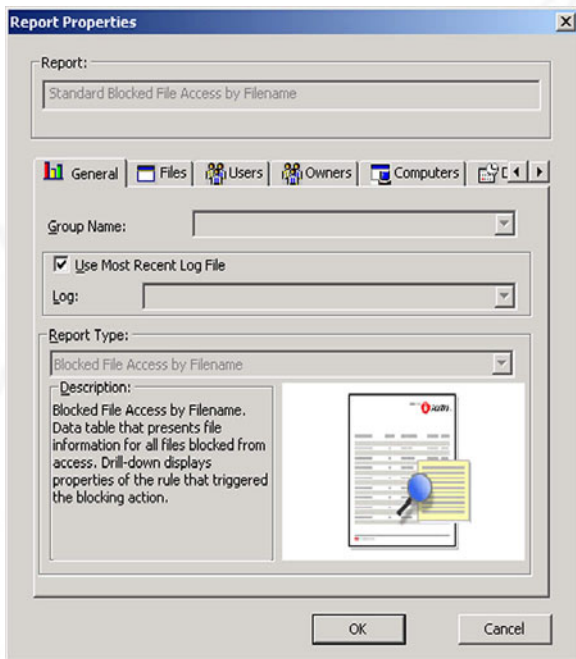


Anti-spyware and Real-time Protection



Scan and manage your entire network from one simple and powerful management console. Deploy Real-Time Monitors, run reports and manage categories with ease.



Customizable reporting provides you with the information you need.

DynaComm i:scan® provides enterprises with the most powerful, flexible and easy to manage anti-spyware solution available.

Built from the ground up for the enterprise market, DynaComm i:scan gives you the power to find and eliminate a broad range of threats, including spyware, adware, P2P clients, intellectual property theft, unauthorized removable storage devices, copyright infringement and any user-definable files or content.

Enterprise management

One centrally deployed console will manage all content security functions from one place, making deployment and management easy. Control distributed scans, manage Real-time monitor rules, even schedule and deliver reports all from one simple interface.

Anti-spyware power

DynaComm i:scan comes with a complete set of content and threat categories containing thousands of keywords and file signatures, including spyware, adware, hacking tools, Trojans, keyloggers and other dangerous infections.

Build long-term protection through DynaComm i:scan's unique Real-time Monitor and file filter, lock hosts files, prevent unauthorized registry changes and ensure that once spyware is removed from your network, it stays gone.

Broad protection, granular management

Control individual processes and users, or implement enterprise-wide policies rapidly and easily. Manage individual users or an entire organization through the same combination of distributed scans and Real-time Monitors, securely and effectively.

Take the guesswork out of Content Security

DynaComm i:scan's ability to locate, categorize and report on your enterprise is unmatched. Create overview, detailed, or drill-down reports on the fly or as part of scheduled tasks. DynaComm i:scan gives you the knowledge to manage and control content security threats before they become business-damaging incidents.

DynaComm i:scan Features

Easily manage a range of security threats

Use DynaComm i:scan to track, manage or eliminate P2P or instant messaging clients, adware, spyware or hacking tools.

Real-Time file monitor

The DynaComm i:scan Real-Time Monitor enables system-by-system management, including tracking and blocking of files and applications.

Powerful anti-spyware capabilities

Predefined and constantly updated signatures and categories keep spyware off your network.

Lock-down USB and removable media

Manage and monitor potential security threats from removable media.

Protect systems across your enterprise

Enterprise-wide management from just one console.

Hands-free administration

Automate maintenance and administration tasks to enable hands-free management of content security tasks. Schedule updates, scans, reports and ensure your content is secured with the minimum of management time.

Comprehensive reporting capabilities

Flexible and comprehensive reporting enables you to review the results of scans or track activity on systems with the Real-Time Monitor. Build a comprehensive picture of file and application content throughout your organization.

Extensive, and customizable content categories

Build new content categories or add to existing ones to enhance your content control capabilities.

System Requirements

Installation of DynaComm i:scan components require Windows NT or more recent operating systems. However, file scans can be run on files stored on Windows 95 and 98 systems.

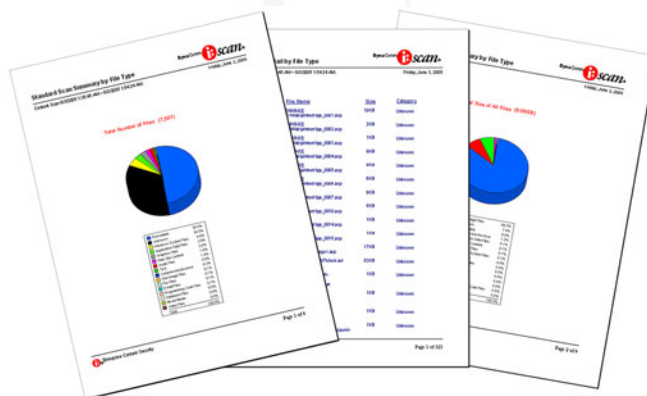
In general, system requirements increase as the number of resources to scan/monitor increase, the number of saved log files increase and the number of saved reports increase.

In a Server component installation, the console component, Admin and Scans databases are installed File Scan log files are created when file scan logs are retrieved and merged to the File Scans folder. RTM log files are created when real-time monitor session logs are retrieved and merged to the RTM folder.

- Windows 2000 with SP2 (or higher), Windows XP with SP1 or Windows Server 2003
- 1.0 GHz or faster processor, 512 MB RAM, 10 GB disk space

The client service is deployed when either a file scan or real-time monitor configuration is run, or when the Client Management topic is used to install the client on selected systems.

- Windows NT 4.0 with SP6 (or higher), Windows 2000 with SP2 (or higher), Windows XP with SP1 or Windows Server 2003
- 500 MHz or faster processor, 128 MB RAM, 100 MB disk space



Flexible and powerful reporting shows the results of network scans and Real-Time Monitor activity.