



Integard Professional

User Guide

Version 2.0

Legal Notices

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the copyright owner.

Copyright © 2008 Race River Corporation Pty Ltd.

All rights reserved.

Table of contents

1	Introduction.....	3
1.1	Welcome to Integard Professional	3
1.2	System Requirements.....	3
1.3	Integard Installation.....	3
2	Integard Professional – Key Features	4
3	Administration.....	5
3.1	Status Screen	6
3.2	User Settings	6
3.3	System Settings.....	11
3.4	Program Limits.....	14
3.5	Keywords.....	16
3.6	Personal Information.....	17
3.7	Allowed Sites	18
3.8	Blocked Sites	18
3.9	Reporting	19
4	Integard Professional features.....	20
4.1	HTTP and Email Proxy Server	20
4.2	Port Forwarding	20
4.3	Authentication via Active Directory	21
4.4	IP User mapping	21
4.5	User Profiles	21
4.6	Internet Usage Policy.....	22
4.7	Customisation	22
4.8	Windows Server with Terminal Services	23
5	Central Administration	24
5.1	Central Administration Configuration.....	24
5.2	Integard Client Installations.....	25
5.3	Daily Usage reports	25
6	Additional Information.....	26
6.1	Automatic Data Updates	26
6.2	Using Integard with Firewall and Anti-Virus Software.....	26
6.3	Email notifications	26
6.4	Bypassing Integard	27
6.5	General Precautions	27
	Troubleshooting	28
6.6	Integard is blocking too much.	28
6.7	Integard is not blocking pages that it should	28
6.8	Anti-Virus Software and Personal Firewalls	29
7	Un-Installing Integard	30

1 Introduction

1.1 Welcome to Integard Professional

Integard Professional is an internet filter designed for use in the workplace, schools and libraries.

It has all the features of the Integard Home edition with additional functionality to support running on a server or a large number of users.

Once installed Integard can Block, Filter and Log internet activity giving you the power to prevent control, limit and monitor access to the internet.

The Integard Administration interface lets you customise the level of access and filtering for each user individually or as a group.

1.2 System Requirements

Operating System	Microsoft Windows 2008 Server, 2003 Server, Vista, XP and 2000
Internet Browser	Internet Explorer 5, 6 and 7, Opera 8, 9 or Firefox
Memory	64 Mb RAM minimum
Disk space	10 Mb minimum hard-disk space
CPU	Pentium III or later

1.3 Integard Installation

Integard is quick and easy to install and begins filtering without any additional configuration.

The Integard 'Default' user is automatically created and will be set to the filtering level specified during the installation.

Please refer to the Integard Quick Start guide for detailed instructions on Installation.

2 Integard Professional – Key Features



The following table is a summary of the features of Integard Professional.

Feature	Description
HTTP Proxy Server	Integard can run on a server as a proxy server for all web and email traffic.
Support for Windows Server Terminal Services	With Windows terminal services Integard can monitor and filter each user session independently.
Central Administration	If Integard is deployed across several PC's the administration can be centralised and automatically distributed.
Internet Usage Policy	As an option an internet policy can be specified and shown to users to which they must agree before they can access the internet.
Content Filtering	Integard can block web pages according to 30 categories. Integard comes with a comprehensive database of websites and keywords that is continuously updated.
Dynamic analysis	Web page content is analysed in real-time and categorised on the fly.
Set Time and Data Limits	Limit users to a particular amount of time or data per day.
Chat / IM Monitoring	Monitor and record chat conversations. Generate alert emails if suspicious or inappropriate language is used.
White List only surfing	Limit access to only websites specified by the administrator. Everything else can be blocked automatically.
Web Based Administration	Configure Integard and monitor usage using a browser from the same PC or remotely over the network.
User defined keywords and site lists.	Set your own custom rules for blocking based on keywords, phrases and web site addresses.
Instant Override	Override page blocks or time limits quickly and easily with the admin password.
Safe searching	Forces popular search engines into their safe search mode, which restricts search results. This is in addition to Integard's automatic filtering and blocking, creating a powerful combination of protection and usability.

3 Administration

Integard configuration is performed using the Integard Administrator.

You can access it in one of the following ways.

1. Start Menu -> Programs -> Integard – Administrator.
2. Right click on the Integard icon  in the system tray and select Administrator.
3. Double left click on the Integard icon  in the system tray.
4. Open a browser and type <http://integard> or <http://127.0.0.2> on the machine Integard is installed.
5. From another computer on the same LAN with the IP address of the PC Integard is installed onto. Example: <http://192.168.0.3:18881>

When the Integard login page is displayed use the password entered during the installation.

Once logged in you will have access to several configuration pages as shown below.

Menu Item	Description
Integard Status	Quick overview of the status of Integard.
User Settings	Customise each user's access to the internet and create new users.
System Settings	Integard system configuration such as password and email address.
Program Limits	Allow or restrict particular applications access to the internet or to run.
Keywords	Specify keywords or phrases that will cause a page to be blocked.
Personal Info	Specify personal information details that should be prevented from being sent out to other people or websites on the internet.
Allowed Sites	Set a list of sites that are allowed on a system level.
Blocked Sites	Set a list of sites that are blocked on a system level.
Reporting	Detailed and Summary reports of Internet usage per user.
Logout	Logout of the Integard Administrator.

The following sections guide you through the above menu options in detail.

3.1 Status Screen

The Integard Status screen gives a one page summary of the version of Integard, its current state, subscription details, the user that is logged in and Integard and system time.

3.1.1 Version

This section displays the version of Integard and website filtering database currently running and in-use.

3.1.2 Status

The Status section indicates if Integard is currently enabled or disabled. When Integard is enabled it is monitoring, filtering and logging connections to the internet.

When Integard is disabled it allows all internet data to pass without interruption. When Integard is disabled logging is prevented also.

This also shows both the Integard time and system time and displays which time that Integard is using for calculating any time limits that have been set.

3.1.3 Integard Users

This displays the name of the Windows user and Integard user currently logged in to Integard and their usage for the current session. For a more detailed and complete account of internet usage refer to the reporting section.

3.1.4 Subscription Status

This will indicate if you are in a 30-day trial or your subscription is active.

The Integard subscription refers to the automatic downloading of filter and website data as well as software updates as they become available.

When the 30-day trial expires the maximum number of users is limited to 3 but all other functionality remains.

You can subscribe to Integard online at <http://www.raceriver.com>.

Alternatively you can disable or uninstall Integard using the administration password.

3.2 User Settings

This screen shows a table of the Integard users that have been created and gives you the option to create a new user. When creating a new user the options are as follows.

3.2.1 General Settings

Username

The username is used to allow different users to login to Integard. If multiple users are configured each user has to login with a password to access the internet.

Full Name

The full name is used in various screens and reports as a more readable name.

Password

The password is required to use the internet unless the user is configured as the 'default' user in the System Settings.

3.2.2 Filter Mode

Filter Mode	Description
Dynamic analysis and allowed sites	All websites will be displayed provided that they are not in the website category that is blocked in the Web Site Categories section below. This may result in a large percentage of pages being blocked and is usually used in conjunction with a user defined white or Safe list.
Allowed sites only mode	All websites will be blocked unless they specifically belong to an allowed category below or listed in the user defined 'Allowed List'
Block all access to the internet	The user is blocked from accessing the internet.
No filtering	The user is not restricted by the Category list or the Blocked list. All websites will be displayed.

3.2.3 Filter Sensitivity

Each website visited is checked against a database of known sites and if the category is blocked then the page is blocked. When the site is not in the database, Integard examines the page and determines the category automatically by scanning the page. The sensitivity of the scanning engine can be controlled through this setting.

Sensitivity Level	Description
Level 1	Maximum blocking
Level 2	Very High
Level 3	High
Level 4	Medium
Level 5	Low
Level 6	Very low
Level 7	Minimum blocking

3.2.4 Image Search

The Integard 'Image Search' feature forces popular search engines into their safe search mode, which restricts search results. This provides another layer of protection beyond the filtering performed by Integard.

3.2.5 HTTPS Filter

The 'HTTPS' filter blocks all HTTPS/SSL connections. This provides an increased protection against proxy sites that may allow Integard to be bypassed. It will block access to most sites that require a login including banks and web mail. If this is too restrictive you can disable it.

3.2.6 Web Site Categories

Select here which categories of web sites can be accessed by the user.

3.2.7 Chat/IM options

Chat/IM Applications: Allow or block all chat applications.

If set to 'Allow', the following chat applications are allowed: MSN Messenger, Yahoo Messenger, ICQ, AOL Instant Messenger, Myspace Messenger and IRC.

If set to 'Block' all chat programs including some not listed above should be blocked.

3.2.8 Other applications

In this section access to Email, FTP and News groups can be allowed or blocked and logging can be enabled. Email can also be set to monitor so that any inappropriate language, keywords or personal information that is sent will generate an alert to the contact email address showing who the email was to, who it was from, time it was sent and the subject of the email. This can only be done for email clients using POP3 and SMTP servers. Logs can be viewed in the reporting section of the Integard administrator.

Note: Newsgroup filtering refers specifically to NNTP based newsgroup readers such as Microsoft Outlook Express. It does not provide any control of web based newsgroups.

3.2.9 Allowed Web Sites

This allows you to allow sites for the specific user in question. Any sites here will only be allowed for this user.

3.2.10 Blocked Sites

This allows you to block sites for the specific user. Any sites added here will only be blocked for this user.

3.2.11 Custom Block Page

This feature allows you to choose between the standard block page,

Copyright © 2008 Race River Corporation Pty Ltd. All rights reserved.

customised message on the standard block page and using a web page designed by you.

3.2.12 Set time and data limits

Daily Time Limit: The daily time limit allows you to give each user a maximum number of minutes of internet access per day.

Daily Data Limit: The daily data limit allows you to give each user a data quota. Both uploads and downloads are counted.

When the data or time limits are reached the user will not be able to access websites, send/receive email or chat online. But they will be able to continue using the computer offline.

3.2.13 Set daily access times

In this section you can configure the hours of the day the user can access the internet.

3.3 System Settings

3.3.1 General Settings

Email Address

Integard can send daily reports and alerts of blocked web pages or inappropriate chat conversations to this email address. It is also used to recover a forgotten password. Because of the information contained in these emails it is important to ensure that mail sent to the specified email address can not be accessed by the restricted users.

Stealth Mode

When stealth mode is enabled Integard tries to hide from the user. The tray icon is removed and blocked pages are displayed as an error that would be seen if the website is down. The user should simply assume the web site they are trying to visit is not available instead of being blocked.

Disable Firewall

Integard has an inbuilt firewall that prevents software from accessing the internet. You can choose to add a particular program or port to the allowed list but you also have the option to disable the firewall completely. With the firewall disabled Integard will only filter and monitor chat, web and email ports.

Count Uploads

Integard is able to limit internet usage by the amount of data consumed by the user in megabytes. Some internet plans base usage on downloads only. Other internet plans base usage on combined uploads and downloads. If usage is based on downloads only then leave this box un-checked. If it is based on uploads and downloads then this box should be checked.

Windows Username

When this box is checked Integard will try to select the user profile that has a username which matches the currently logged in Windows user. If it is unable to match the username it will instead default to the username selected in the 'Default User' field below.

Auto Create Users

With this feature on a Windows user that logs on and does not correspond with an Integard username will automatically be given an Integard profile based upon the default settings within Integard.

Default User

The default user is the user that is automatically logged in when the computer starts if Windows username is not selected or there are no corresponding Windows and Integard usernames. To change to a different user simply select 'Logout User' from the Integard tray icon right-click menu and Log in as a different user.

Admin Password

The Admin password is required to login to the Integard Admin pages. It is also used to override blocks and to disable or Un-Install Integard.

Re-Enter Password

The password must be entered twice to detect accidental typing mistakes when changing the admin password.

3.3.2 Automatic reports and alerts**SMTP Server**

The SMTP server must be specified to receive automatic alerts and daily reports. Check with your ISP or look at your email client settings for the correct value to enter.

From Address for notifications

The 'From' Email address for alerts and automated daily reports can be configured here. By default it will use the Administrators Email address configured above as the 'From' address if this field is not configured.

SMTP Username and Password

Some SMTP servers require a username and password to use their services. If so you can enter the details here to use SMTP server authentication. If you are unsure please check with your service provider.

Send Daily Reports

Click to enable a daily report email to the address entered above. The report lists the internet usage for each user for the last 7 days. (Requires SMTP Server setting.)

Send Email on Web page content blocks

Click to enable an immediate email alert whenever a web page is blocked to content filtering. It does not send an email for cases where an action was blocked due to time or data limits. (Requires SMTP Server setting.)

Send Email on Personal Information detection

Click to enable an immediate email alert whenever personal information is blocked from being sent from the computer. (Requires SMTP Server setting.)

3.3.3 Proxy Server

Use Proxy Server

If your connection to the internet requires the use of a proxy server then check this box and enter the details of the proxy server below.

This is different to enabling Integard as a proxy server. If Integard Professional is enabled as a proxy server, by setting the proxy setting here you will be enable proxy chaining. This is where Integard is a proxy server and it passes all web traffic to another proxy server.

Note: Only enable and set the proxy server settings if you are sure of the configuration as the wrong settings can cause all web access to fail.

Proxy Server

Proxy server hostname or IP Address.

Proxy Port

Proxy server port number (1 to 65535)

3.3.4 External Whitelist

This feature can be used to load a whitelist from an external source such as www.openwhitelist.com. This can be useful if you only want to allow access to a particular whitelist of pre-approved sites.

3.3.5 Time Settings

This allows you to synchronise the Windows and Integard time zones and also gives you the option for Integard to bypass the local Windows time and use the Integard servers by selecting the Internet time box. This prevents any time tampering that may be used to bypass any time limits set within Integard. It also displays both the system and Internet times to show any discrepancies between the two.

3.4 Program Limits

3.4.1 Program Rules

On this Program Limits page you can permit or deny internet access to any program. You can also prevent a program from running at all.

Execution Rights.

Restriction	Description
Normal Restrictions	Normal restrictions are the same as not being in the list at all in terms of filtering. But allows a program to stay in the list to be easily altered at another time without having to add it again.
No Network Access	All access to the internet for the specified application is blocked.
Not allowed to run	The specified program is not permitted to run and will be automatically closed if started
No Restrictions	The specified program is given full unfiltered and unmonitored access to the network. Applications with this level of privilege are excluded from the data limits that may be set for a user.
Delete from list	Select this value and apply changes to remove the application from the list.

When specifying an application you can use the Browse button and select the executable program (ie. Files with a .EXE file extension) or just enter the executable name such as Notepad.exe. The full path is not required.

Most applications won't need to be specified in this list. Examples of ones that may need to be added are FTP clients, VOIP phones and Web Servers due to their unique networking requirements.

Note: Network activity by applications listed here with 'No Restrictions' will not be counted towards a users Data limit and will not be monitored or filtered in any way.

3.4.2 Ports

The ports list can be found at the bottom of the Program Limits page.

Here you can list TCP and UDP ports that Integard should not block.

For example if you have a remote administration tool that requires TCP port 4899 to work you can enter it here in the TCP field.

Note: Network activity on ports listed here might not be counted towards a user's Data limit.

3.4.3 Recently Blocked Programs

This table displays a list of recently blocked programs and the port at which they were blocked on. The table also gives you the option to allow the program or port by clicking on the blue link within the table. This will automatically add to the lists above.

Please note that you should never add a browser as it will bypass Integard's web filtering ability for that browser.

3.5 Keywords

On the Keywords page you can list words and phrases that should cause web pages to be blocked if they appear anywhere in the page being displayed.

This could be useful if there are certain topics that should not be shown to the user.

Keywords and phrases must be separated onto separate lines.

Example :

computer cats and dogs

In this example if the keyword "computer" appears anywhere on a web page the page will be blocked.

In addition if the phrase "cats and dogs" appears in a page it will be blocked. The phrase "dogs and cats" would not be blocked. It must be an exact match.

Keywords and phrases are not case-sensitive. That means "Computer" and "COMPUTER" would also be blocked.

3.6 Personal Information

List words and phrases here that you want to prevent being sent out to the internet. Examples of private details you might want to block are of your address, phone numbers or even credit card numbers.

Unlike the keywords list which blocks based on content coming to your computer from the internet, this list blocks words going away from your computer to the internet.

If these words are detected being sent out in a web form or chat session they will be blocked and an alert email will be sent to the email address specified on the system settings page.

You can specify word or phrases on a separate line.

Example:

34872312 riverside place

In this example if the keyword "34872312" or the phrase "riverside place" appears anywhere in a web form or chat conversation leaving your computer it is blocked.

Keywords and phrases are not case-sensitive. That means "Riverside Place" and "RIVERSIDE PLACE" would also be blocked.

3.7 Allowed Sites

List domain names and URL's of websites here that you want to be allowed regardless of what category it is or any words or phrases that may be present on the page.

Each entry must be placed on a separate line. Entering http:// at the front of each line is not required.

If you enter a domain name the entire site will be allowed.

If you enter a path to a specific page then only that page will be allowed. Every other page will be allowed or blocked based on content and category determined by Integard.

Example :

www.cybersmartkids.com.au kidsites.org en.wikipedia.org/wiki/Cat
--

The "www." is also not required and is often best to leave off as some websites occasionally use a different prefix to "www."

3.8 Blocked Sites

List domain names and URL's of websites here that you want to be blocked.

These are websites selected by you to be blocked that may not be blocked by Integard automatically.

Entries must be listed on separate lines. Entering http:// at the front of each line is not required.

Example:

www.badsite1.com badsite2.net www.oksite.com/BadPage.htm
--

The "www." is also not required and is often best to leave off as some websites occasionally use a different prefix to "www."

3.9 Reporting

Integard provides two types of reports. Summary reports and detailed reports.

3.9.1 Summary Report

The summary report displays a summary of all activities for the last 7, 14 or 30 days.

It shows how much Web, Chat and Email were used, how many minutes were spent online, Megabytes used and pages blocked.

Example:

Date	Weekday	Web	Chat	Email	Data	Minutes	Blocked
25-2-2007	Sun	169	22	17	1.96 Mb	10	3
24-2-2007	Sat	510	33	107	22.94 Mb	43	1
23-2-2007	Fri	137	12	55	1.02 Mb	19	0
22-2-2007	Thu	1018	53	50	6.97 Mb	59	1
21-2-2007	Wed	121	3	57	0.77 Mb	11	1
20-2-2007	Tue	1047	43	21	10.03 Mb	52	3
19-2-2007	Mon	259	12	19	1.36 Mb	11	6

The weekly report can be emailed automatically to the email address configured in the system settings.

3.9.2 Detailed Report

The detailed report shows a complete list of all activity by the user.

3.9.3 System Event Report

The system event report provides a log of various system or administrator level actions such as block overrides, disabling Integard and password failures.

4 Integard Professional features

This section details the features of Integard Professional that are not found in Integard Home. This additional functionality is centred on services that would be useful in the workplace, schools or libraries.

4.1 HTTP and Email Proxy Server

Integard can be configured to as a proxy server.

4.1.1 HTTP Proxy configuration options:

TCP Port: The port that the proxy server listens on. By default it is set to 8080 but can be set to any value.

Chaining: Integard can chain HTTP proxy requests

HTTP Proxy configuration options:

4.1.2 SMTP Proxy configuration options:

Local Port: The TCP port that the proxy listens on. By default the value is set to 25.

Destination Server: The IP Address or hostname of the SMTP server that Integard relays

Destination Port: The port number of the destination server.

4.2 Port Forwarding

Port forwarding allows specific ports to be relayed to another server but with Integard reporting and controls.

An example might be for restricted access to a telnet, FTP, news or VPN server.

Integard treats these connections a simple data streams, as such the protocol used is not relevant and can be used for any type of traffic.

4.3 Authentication via Active Directory

When Integard is used as a proxy server it can be configured to authenticate remote users using Active Directory.

To enable Active Directory authentication select the 'Authentication' menu open in the Integard Administrator and click the check box.

Integard uses LDAP to communicate with the Active Directory server.

You will need to set the following options:

Directory Server: IP address or hostname of the Active Directory server.

AD/LDAP port: The port to connect to on the server. Default: 389

Integard User: The Integard user to select when logging in via Active Directory.

4.4 IP User mapping

Integard allows proxy users to be automatically logged in when the connection originates from a specific IP address or range of IP addresses.

This would be a useful feature for organisations such as libraries to designate a group of machines to be automatically assigned a user profile configured for Public access.

4.5 User Profiles

User profiles are a collection of settings that can be applied to a user or a group of users.

For example a profile might be set up for Students, Staff or the Public with varying degrees of filtering.

User accounts can be linked to a particular User Profile. If multiple users are linked to the same profile, any changes to the profile are reflected immediately for all linked users.

4.6 Internet Usage Policy

As an option each user can be required to agree to an Internet Usage policy before being able to access any websites.

A sample policy is provided which can be customised to suit each organisation's specific requirements.

4.7 Customisation

All windows seen by the users can be customised to varying degrees. These include the login, blocked and usage policy pages.

Most customisation requires adding or changing files located in the 'Custom' subdirectory located in the directory Integard is installed into.

Tip: By default Integard is installed into C:\Program Files\Integard.

4.7.1 Company logo

The Integard logo which appears in the login, blocked and sample usage policy pages can be easily replaced. Simply place a file called logo.jpg into the custom directory mentioned above.

4.7.2 Internet usage policy

4.7.3 Blocked Page

4.8 Windows Server with Terminal Services

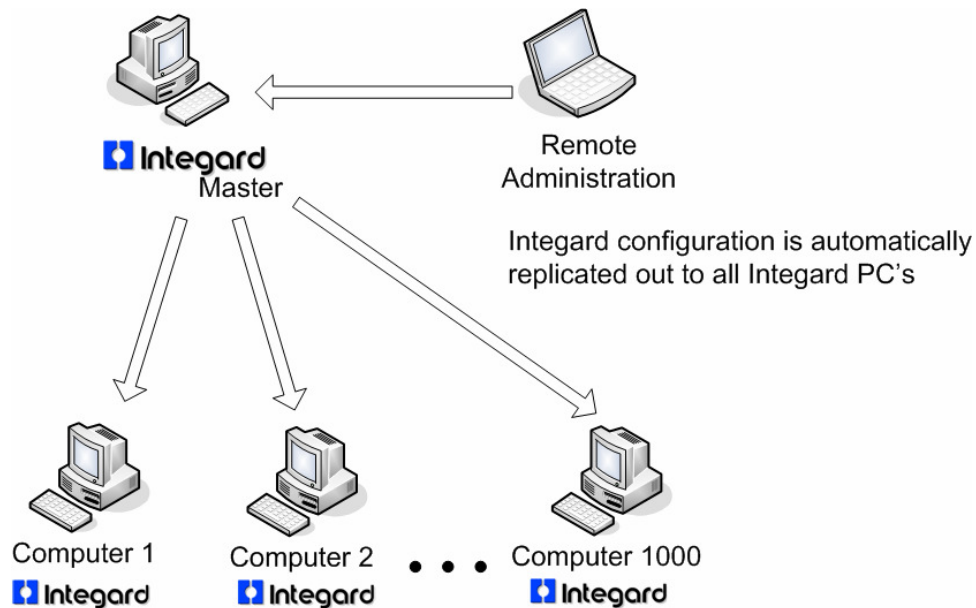
When deploying Integard on Windows Server with Terminal Services, each terminal services user is treated as a different Integard user.

Terminal services support works best when:

- Integard is configured to use a profile based the windows username
- Auto create users is enabled under System Settings
- Each terminal services user has a different Windows username

5 Central Administration

Integard can be installed on multiple PC's with one PC designated as the master. The configuration of the master Integard PC is automatically replicated out to all of the client Integard installations.



5.1 Central Administration Configuration

A small amount of configuration is required to set up central administration.

5.1.1 Client Configuration

Either during installation or from within the Integard Administrator the client must specify that it gets its configuration from another Integard installation. The IP address or hostname of the Master Integard must be provided.

5.1.2 Master Configuration

The Master Integard installation maintains a list of client Integard installations that it notifies when there are any changes to the configuration. The list of client Integard computers can be found under 'Client Installs' in the Integard Administrator.

5.2 Integard Client Installations

The master installation of Integard maintains a list of the IP addresses of all client installations. The list is automatically appended when it receives a configuration update request from a new client but may need to be managed manually in some cases.

5.3 Daily Usage reports

5.3.1 Daily Usage by IP Address

This report is a snapshot of the current day's internet usage broken down by IP address. It is sorted by total data usage with the highest usage at the top.

This report is most useful when users are using Integard as a proxy server. If users are local or using terminal services they will all appear under the same IP address.

5.3.2 Daily usage by user

This report is a snapshot of the current day's internet usage broken down by user account. It is sorted by total data usage with the highest usage at the top.

This report is most useful when users are logging in to Integard using different accounts.

6 Additional Information

6.1 Automatic Data Updates

If you are on the 30-Day trial or have an active Integard subscription you can receive updates to the Integard database automatically.

Integard checks for updates and downloads them automatically when the computer starts up or daily if it is left running continuously.

Automatic updates can be disabled by logging into the Integard Administration interface, selecting 'System Settings' from the menu, opening the Automatic Updates section, and un-checking the box labelled 'Auto Updates'.

6.2 Using Integard with Firewall and Anti-Virus Software

Integard can be installed along side most popular Anti-Virus and Firewall products. In some cases the firewall may need to be configured to allow Integard to access the internet.

When the firewall asks if Integard should be allowed to access the internet you should let it or you won't be able to access the web at all.

This is because Integard sits between your Web Browser, Email program and chat programs and the internet so that it can monitor the content. Because of this it will appear to the firewall that Integard is accessing the internet instead of those applications.

6.3 Email notifications

Integard can send emails notifications on the following events.

- Web page is blocked
- Personal information detected in a web form
- Personal information sent in a chat program
- Chat messages blocked for containing bad language
- Suspicious chat messages that may be an adult trying to groom a child.

To enable email notifications you must do the following;

- Enter the email address under System Settings
- Set SMTP server under System Settings | Automatic reports

- Check the boxes to enable email notifications

Then for each user under Chat/IM options enable notifications as required.

6.4 *Bypassing Integard*

Because Integard is designed to limit access to the internet, the restricted user may try to bypass it.

Integard has a multitude of mechanisms in place to resist tampering and attempts to disable or un-install it without the Integard administrator password.

There are precautions that can be taken as the administrator of the computer to increase the difficulty of bypassing Integard that are detailed in the next section.

6.5 *General Precautions*

To maximise the effectiveness of Integard it is best to make it as difficult as possible to bypass Integard and access restricted content.

We recommend taking the following steps;

Create a separate Operating System user for the users that do not require Administrator privileges. (Requires Windows NT, 2000, XP or Vista)

Change the system BIOS settings to prevent boot from CD so that they can't boot to an alternate operating system that has no restrictions or use boot CD's to circumvent the administrator accounts. You may also want to add a password to the BIOS to prevent changing of the boot sequence.

Ensure that the email address configured in Integard is not accessible by children or other restricted users.

Choose a password for administration that is not known or easily guessed.

Troubleshooting

6.6 Integard is blocking too much.

If Integard is blocking too much you can reduce the filtering sensitivity by reducing the users filtering level. To do that log in to the Integard Administrator with a web browser, select User settings, click on the username, and adjust the sensitivity under 'Filter Settings'.

If there are specific pages or sites that should be allowed you can enter them in the 'Allowed Sites' list.

6.7 Integard is not blocking pages that it should

If Integard is not blocking pages it should be you can:

- Increase the filtering sensitivity by increasing the users filtering level.
- Add your own keywords and phrases to be blocked.
- List pages or websites to the blocked list.

All of these can be configured using the Integard Administrator. For details on logging in and using it refer to the Administration section of this guide.

Another possibility is that the page you are viewing has been cached by Internet Explorer. When a page is cached your browser will get the page from a copy on the hard disk and not from the actual website. When that happens Integard is not able to block it. To be sure it would be best to delete your temporary internet files. With Internet Explorer v6.0 you can do this by selecting 'Internet Options' from the Internet Explorer Tools menu and then clicking 'Delete Files' in the 'Temporary Internet Files' section.

6.8 Anti-Virus Software and Personal Firewalls

Integard has been tested with various Anti-Virus and Firewall products. As both Integard and these applications have an interest in gaining access to the networking aspects of the operating system there is a tendency for them to interfere with the correct operation of each other.

Anti-Virus

The most common side effect of using Integard in conjunction with an Anti-Virus product is that the Anti-Virus product will try to scan emails in the same way Integard does but for different reasons. With both applications trying to do the same thing there is a chance of interference. If Integard detects a problem it may stop scanning and logging emails in order to prevent a problem with emails being sent or received at all. If sending and receiving Email does stop working after installing Integard you could try either disabling the email scanning in your Anti-Virus program or allowing TCP ports 25 and 110 on the Integard Program Limits configuration page.

Firewalls

The most common side effect of using Integard in conjunction with a firewall product is that the firewall product will need to be told that Integard is 'Allowed' to access the Internet. This is essential because Integard accesses the Internet on behalf of your web, email and chat applications and therefore must be given permission. This may happen automatically or it may require your input depending on the firewall product you are using.

7 Un-Installing Integard

To Un-Install Integard you will need to have 'Administrator' rights to Windows if you are using Windows 2000, Windows XP or Windows Vista.

You will also need the Integard Administrator password. If you do not know what this is it will be difficult to remove Integard from the computer.

To run the Integard Un-Install program select it from either:

- Start Menu -> Program Files -> Integard -> Un-Install
- or
- Control Panel -> Add Remove Programs

When prompted enter the Integard Administration password to authorise the removal of Integard.



