



Version 5.2

SurfControl RiskFilter - E-mail *Starter Guide*

Enterprise Threat Protection™

NOTICES

Updates to the SurfControl documentation and software, as well as Support information are available at www.SurfControl.com/support.

Copyright ©1998-2006 SurfControl plc. All rights reserved.

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.

SurfControl is a registered trademark and SurfControl and the SurfControl logo are trademarks of SurfControl plc. All other trademarks are property of their respective owners.

Version 5.2 printed November 2006.

CONTENTS

- NOTICES I**
- CONTENTS II**
- ABOUT THIS GUIDE 1**
 - Glossary of terms 1
- OVERVIEW 2**
 - RISKFILTER COMPONENTS 2
 - RISKFILTER ARCHITECTURE 3
- BEFORE YOU START 6**
- WHERE TO DEPLOY THE APPLIANCE 8**
 - INBOUND AND OUTBOUND FILTERING 8
 - Deployment scenarios 9
- CONFIGURATION 12**
 - Stage 1: Hardware Setup 12
 - Stage 2: Configuring the appliance 13
 - Stage 3: Updating the Software 17
 - Stage 4: Running the Configuration Wizard 18
 - Stage 5: AVA and ASA Updates 20
 - Setup Complete 20
- INTERFACE OVERVIEW 21**
 - RiskFilter Console 21
 - RiskFilter System Management Console 25
- FURTHER READING 30**
- TECHNICAL SUPPORT 31**

ABOUT THIS GUIDE

This Starter Guide will give you all the information you need to help you to install RiskFilter – E-mail with the default settings, so that you can begin filtering e-mail as quickly as possible. It also gives you a quick summary of the interface to help get you started with administering the appliance. The **RiskFilter – E-mail Filter Hardware Setup Guide** and the **RiskFilter – E-mail Administrator’s Guide** contain more detailed information. To access the SurfControl Knowledge Base, visit <http://kb.surfcontrol.com/>.

When you update the RiskFilter – E-mail appliance software you will receive the latest RiskFilter – E-mail appliance documentation. You can download updated documentation from www.surfcontrol.com. Select **Downloads > User Guides** from the main menu, then select the documents you want to download.

GLOSSARY OF TERMS

The following terms are used in this guide:

Table 1 Terms used

Term	Description
administrator	The account that sets up RiskFilter.
appliance	The RiskFilter appliance.
workstation	The computer used to configure the appliance.
configuration wizard	Enables you to set up licensing, test system connectivity, configure protected domains and DNS MX Records.
firstboot.pl	Configures the RiskFilter hardware from the command line interface.
firstboot wizard	Enables you to set up the appliance on your network using a wizard interface.
rfmng	The account that configures the RiskFilter software and environment.

OVERVIEW

RiskFilter is an enterprise e-mail security appliance. It combines the advantages of secure and scalable hardware with the effectiveness and accuracy of the best filtering software.

RISKFILTER COMPONENTS

The RiskFilter components consist of:

- RiskFilter System Management console - this is for the maintenance of the RiskFilter hardware, and enables you to configure issues such as disk usage, network cards etc. See “RiskFilter System Management Console” on page 25..
- RiskFilter Management console - this is where policies and message routes are configured, to enable you to manage the e-mail that passes through RiskFilter. You can also update licenses here. See “RiskFilter Console” on page 21..
- SurfControl OS
- RiskFilter MTA, AVA, ASA
- Linux kernel

This is all included in a ‘ready-to-install’ hardware appliance.

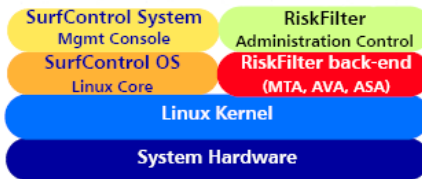


Figure 1 RiskFilter Components

SurfControl OS

The SurfControl OS is a Linux-based operating system that has been developed with security in mind. SurfControl has created this operating system to run its RiskFilter e-mail filtering software. The SurfControl OS includes enhanced features such as an easy-to-use CGI-based Linux management console and a tuned Linux kernel.

RISKFILTER ARCHITECTURE

Understanding how RiskFilter processes e-mail will help you to best configure it for your network. RiskFilter writes messages directly to raw disk, completely by-passing the OS file system. RiskFilter uses the database to manage message storage. It also uses it to allocate and manage free space.

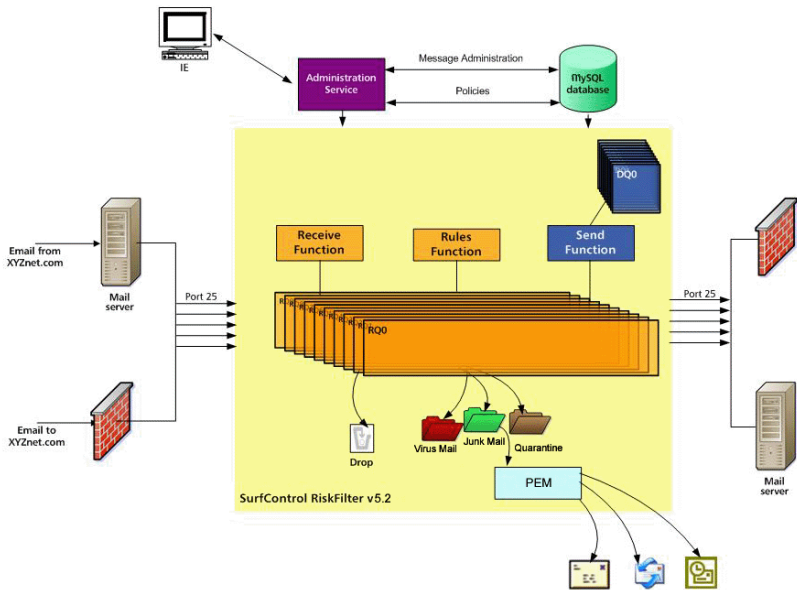


Figure 2 RiskFilter architecture

Receive Function

The Receive function is responsible for managing SMTP connections to the RiskFilter appliance and pre-screening e-mail for processing. Once an e-mail passes the pre-screening the following steps are carried out:

- 1 The Receive function queries the database for a free file location.
- 2 It then writes the e-mail to that location.
- 3 It notifies the Rules function that an e-mail is ready for processing, giving the location within the RQ.

Receive Queues

RiskFilter places all e-mail that passes the pre-screening criteria into the Receive Queues. These are a set of ten files: RQ0-RQ9.

Rules Function

The Rules function is responsible for analyzing e-mail against the configured filtering policies. If an e-mail triggers a policy, the Rules function takes one of the following actions:

- **Deliver** - This also occurs if no policy is triggered. The Rules function notifies the Send function that an e-mail is ready for delivery, and provides the location within the RQ.
- **Drop** - The Rules function notifies the database and the pointer record is removed.
- **Isolate** - The Rules function notifies the database and the pointer record to the RQ is removed from the database. The Rules function then queries the database for a location in the appropriate isolation file, and writes the e-mail to that location. There are three isolation files:
 - Junk Mail - for any e-mail caught by the Anti-Spam Agent.
 - Virus Mail - for any e-mail caught by the Anti-Virus Agent.
 - Quarantine - for any e-mail caught by custom policies.

You can also create your own custom queues and assign them to the desired filters.

Send Function

The Send function attempts to deliver e-mail to the next hop (as identified by the Mail Routing configuration). If the Send function cannot deliver the e-mail at the first attempt, it carries out the following steps:

- 1 It queries the database for free space in the Deferred Queue (DQ).
- 2 The pointer record to the RQ is removed from the database.
- 3 The DQ location is written to the database.
- 4 The e-mail is written to that location in the DQ. This re-queues the e-mail for attempted re-delivery.

The Send function uses the re-queueing scheme when attempting to re-deliver the e-mail.

Deferred Queues

RiskFilter places deferred (re-queued) e-mail into the Deferred Queues.

Administration Service

The Administration service provides a conduit for web-based administration.

Personal E-mail Manager (PEM)

PEM enables end-users to view e-mail isolated by the ASA policy. PEM validates user access against entries on an existing LDAP server. End-User Control can enable end-users to create custom white lists and black lists within PEM.

MySQL Database

The MySQL database holds configuration data, policies, message IDs, and off-set locations for the RQ/DQ and isolation queues. This database does not store the message itself.

LDAP

LDAP is an open, standard protocol for accessing information services that use Internet transport protocols, such as TCP. LDAP uses a hierarchical data structure where entries are in a tree-like structure called a DIT. RiskFilter requests data from an LDAP server to validate domain users. It also uses LDAP to validate e-mail addresses and to authenticate end-users for PEM.



Note: Certain types of LDAP server connections may require some knowledge of LDAP query construction.

BEFORE YOU START

Before you begin, check that your shipment contains the following items:

Table 1 Shipment Contents

Hardware	Support Materials
SurfControl RiskFilter appliance	End User License Agreement
Appliance rack mounting hardware	Hardware Setup Guide
RS232 Serial Direct port cable	Starter Guide
Power Cord (country specific)	Declaration of Conformity
	Recovery CD-ROM – use only with guidance from SurfControl Support.

This guide contains detailed information on how to configure the software of the RiskFilter appliance but there are a couple of things that must be checked before you start to configure the appliance:

- **Knowledge Base Article 1534** - contains important information about the latest version of the RiskFilter – E-mail software. Always having the most up-to-date software ensures that the appliance is always filtering at its most efficient.

Visit <http://kb.surfcontrol.com> and search for ID Number 1534.

- **RiskFilter – E-mail Hardware Setup Guide** - supplied with the appliance. You will need this to learn how to install the RiskFilter appliance onto the rack and integrate it into your network.

You will also need to collect the following information:

Table 2 Useful Information

Information	Explanation	Make a note here
Host Name	Host name for the appliance	
Domain Name	The domain name of your network, e.g. mycompany.com	
IP Address	The IP Address used for the appliance eth0 port, e.g. 192.168.5.23	
Subnet Mask	e.g. 255.255.255.0	
Default Gateway	The default Internet Gateway for the appliance	
IP Address of DNS Server(s)	The IP address of any DNS Servers to be used by the appliance.	
Time zone setting	The time zone where the appliance resides e.g.Europe\London	
License Key	SurfControl supply a license key via e-mail when the appliance is shipped to you. If this is not the case, contact SurfControl Customer Services.	

WHERE TO DEPLOY THE APPLIANCE

SurfControl recommends deploying RiskFilter in the DMZ.

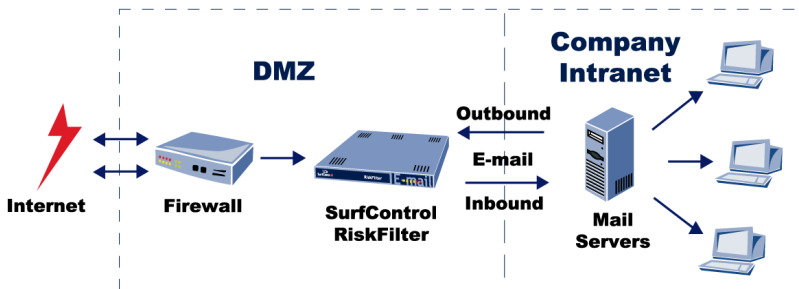


Figure 3 Deploy RiskFilter in the DMZ

This enhances security by ensuring that the appliance cannot be used to see the rest of your internal network.

INBOUND AND OUTBOUND FILTERING

RiskFilter is extremely effective at stopping spam and viruses at the gateway, and in this way frees up network resources. Spam and viruses are typically an inbound problem.

A quick and easy way to stop spam and viruses from entering your network is to simply enable the global Anti-Virus Agent and Anti-Spam Agent policies. You can then configure RiskFilter for inbound filtering only.

However, RiskFilter can provide additional benefits if you configure it to perform outbound filtering. This enables it to scan messages for confidential or potentially liable information before routing the e-mail to the intended recipient. RiskFilter can also add custom disclaimers to a message before it leaves your network. In addition, many policies can apply to both inbound and outbound traffic. For example, with a single policy, you can stop inbound and outbound viruses.

See the Administrator's Guide for more information on configuring RiskFilter to scan inbound and outbound messages.

DEPLOYMENT SCENARIOS

You can deploy RiskFilter in any of the following scenarios:

- Stand - Alone
- Clustering
- Hot Standby

Stand - Alone

This is the default, 'out of the box' configuration. The stand-alone deployment processes incoming e-mail, maintains logs, messages and configuration data on a single appliance. It can be converted at any time to a Master or Slave configuration.

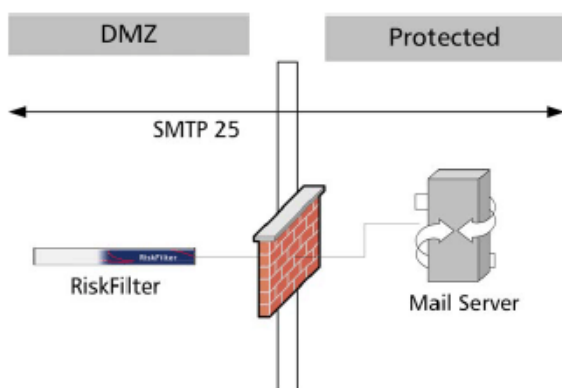


Figure 4 Stand-alone deployment

In this deployment, RiskFilter filters all inbound and outbound SMTP traffic. Inbound e-mail travels from the Internet to RiskFilter for filtering. RiskFilter then routes the e-mail to the next host, which is typically the internal mail server.

Outbound e-mail flows from the internal mail server to RiskFilter for filtering. RiskFilter uses available DNS to resolve MX records and route the SMTP traffic.

Clustering

You can configure two or more clients in a cluster. In this deployment, one appliance acts as the Master appliance and the remaining appliances are deployed as Slaves.

The Master appliance:

- Maintains the cluster configuration.
- Pushes policy changes to the slaves.
- Manages Slave configuration.
- Maintains all isolation queues and archived e-mail for the cluster.

The Slave appliance:

- Belongs to the master.
- Processes SMTP connections.
- Sends logs, isolated e-mail and archived e-mail to the Master.
- Can be promoted to Master.

With the clustering model, the Slave performs the majority of the filtering duties and RQ/DQ management. The Slave passes log data and isolated/archived e-mail back to the Master for data storage. This improves each Slave's processing capability.

The Master manages the mySQL database, which holds the configuration data, and the traffic/rules logs from each Slave. All administration is done on the Master (the administration function is disabled on each Slave), then pushed out to the Slaves.

Figure 5 shows an example of a RiskFilter cluster, there is a single Master and two Slaves. In this scenario, load-balance incoming traffic using DNS MX records with the same preference.

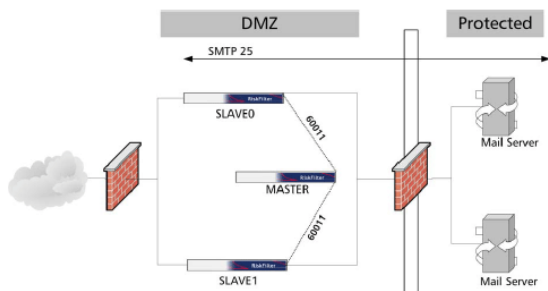


Figure 5 RiskFilter cluster

The Master communicates with the Slaves in the cluster over port 60011. You create and manage all policies on the Master. The Slaves receive SMTP connections over port 25 and sends all log data to the Master over port 60011. Load-balancing is managed by DNS round-robin.

Hot - Standby

RiskFilter can also be configured in a hot-standby configuration. This means that a spare appliance can be configured in an identical manner to the primary appliance and can take over filtering if the primary appliance fails.

Set up hot-standby by using two RiskFilter appliances with the same configuration and policies. Configure one appliance with the relay configuration and policies, then transfer this information to the standby appliance. Assign a separate IP address to each appliance, but use the same MX record. Give the active appliance a lower MX preference than the back-up (by default, e-mail is sent to the appliance with the lowest MX preference). If the active appliance fails, e-mail is automatically routed to the standby.

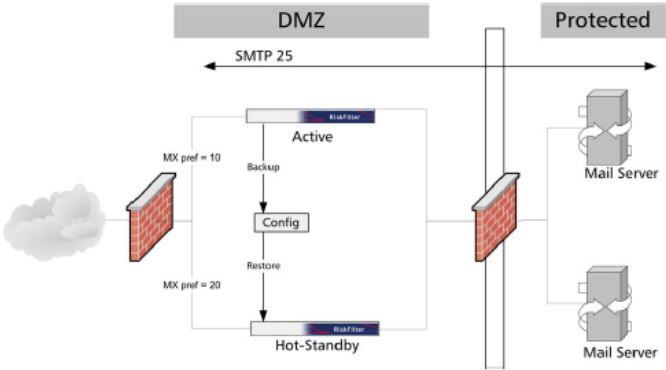


Figure 6 Hot-standby

CONFIGURATION

Configuring RiskFilter is a five stage process. Once you've completed these stages, RiskFilter is ready to begin filtering e-mail.

Table 1 Configuration stages

Stage	Page
Stage 1: Hardware Setup	12
Stage 2: Configuring the appliance	13
Stage 3: Updating the Software	17
Stage 4: Running the Configuration Wizard	18
Stage 5: AVA and ASA Updates	20

STAGE 1: HARDWARE SETUP

Before you power up the RiskFilter – E-mail appliance, follow the steps in the Hardware Setup Guide to mount the appliance on its rack.

Don't plug it into the network yet.

Now proceed to Stage 2: Configuring the appliance.

STAGE 2: CONFIGURING THE APPLIANCE

You must now create a means of interacting with the appliance in order to configure it. You can do this in one of three ways:

- **Option 1** - This is the easiest, and preferred, option. Connect a workstation to the appliance using a CAT-5 crossover cable, and log in using the appliance's default IP address. You can then use the wizards available in RiskFilter.
- **Option 2** - By setting up a serial connection to the RiskFilter appliance using the supplied RS232 Serial Direct port cable, and logging in via a terminal emulator such as 'Hyper Terminal'.
- **Option 3** - By connecting a monitor and keyboard to the appliance to log in using the console.



Note: To use the wizards in RiskFilter, you will need to disable any pop-up blockers in your web browser. Pop-up blockers will stop the wizards from launching.

Option 1 - Using the Firstboot wizard to configure RiskFilter

This option gives you an easy to use wizard interface with which to configure your appliance. To use the Firstboot wizard, you must temporarily add a workstation to the same network as the appliance, then connect to the appliance via this computer. To do this:

- 1 Connect the workstation to the appliance. You must use a CAT-5 crossover cable and plug it into the port labelled LAN1. Your hardware documentation contains details of rear panel cable connections.



Note: This workstation must have an operating system with a GUI and be able to run a browser, for example: Microsoft Windows.

- 2 Power up the appliance. The power button is behind the front panel.

- 3 Carry out the following:
 - **If you are using Windows** – double-click **Local Area Connection**.
 - **If you are using LINUX** – change the workstation's IP to an IP address on the 192.168.1.0 network. This will enable it to access the RiskFilter appliance (RiskFilter's default IP address is 192.168.1.200).
- 4 In the **Local Area Connection Status** dialog box that follows select the **General** tab and click **Properties**.
- 5 Select 'Internet Protocol (TCP/IP)' in the Local Area Connection Properties dialog.



Note: Do NOT clear the check box alongside this option.

- 6 Click **Properties**.
- 7 Log in to the appliance using a web browser by typing in the URL:
https://192.168.1.200/admin
- 8 Accept the certificate that appears and enter your login details. The default settings are:
 - User name = administrator
 - Password = admin



Note: For security reasons SurfControl recommends that you change this default authentication as soon as possible.

- 9 The Firstboot wizard will appear. Proceed through the wizard until you have entered all your configuration details.
- 10 Once complete, the Firstboot Wizard will attempt to log you back into the Administrator Console using the new IP address. Use your new administrator login details to log in.

Option 2 - Using Hyper Terminal to configure RiskFilter

If you do not have access to the wizards, option 2 enables you to use Windows Hyper Terminal to act as a console for the appliance.



Note: If you are running Windows Server 2003 you must install Hyper Terminal before you start.

To set up your Hyper Terminal connection:

- 1 On the workstation, select **Start > Programs > Accessories > Communications > Hyper Terminal**.
- 2 The **Connection Description** dialog box is displayed. Enter a name for the Hyper Terminal connection. If the **Connection Description** dialog box doesn't display automatically, select **New Connection** from the File menu.
- 3 Click **OK**.
- 4 Select the communication port that the computer will use to connect to the appliance. You can choose either COM1 or COM2.
- 5 Click **OK**.
- 6 A property sheet for the port you specified in step 4 will display. Fill in the fields as follows:
 - Bits per second: 38400
 - Data bits: 8
 - Parity: None
 - Stop bits: 1
 - Flow control: None
- 7 Click **OK**.
- 8 From the File menu, select **Save**.
- 9 Power up the RiskFilter – E-mail appliance. The power button is behind the front panel.
- 10 Open your Hyper Terminal connection and log in as `rfmnggr` with the password `$rfmnggr$`.
- 11 Type `firstboot.pl` then follow step 5 - 19 of procedure 2.
- 12 Disconnect the serial cable from the appliance.

Now that you have configured the RiskFilter – E-mail appliance hardware, you must configure its software. Proceed to Stage 3.

Option 3 - Using a console to configure RiskFilter

You can use the appliance itself as a console to configure RiskFilter, if there is no computer running Windows available:

- 1 Connect a monitor and keyboard to the appliance.
- 2 Power up the RiskFilter appliance. The power button is behind the front panel.
- 3 Log in to the console as `rfmngr` with the password `$rfmngr$`.
- 4 Type `firstboot.pl`
- 5 Press **Enter**. The RiskFilter configuration screen will display.
- 6 Type the host name of the appliance.
- 7 Press **Enter**.
- 8 Type the name of the domain in which the RiskFilter appliance is positioned.
- 9 Press **Enter**.
- 10 Type the IP address of your appliance.
- 11 Type the subnet mask of the network you want the RiskFilter appliance to connect to.
- 12 Press **Enter**.
- 13 Type the gateway address of the network you want RiskFilter to connect to.
- 14 Press **Enter**.
- 15 A list of timezones will display. Choose the number that corresponds to your time zone:
 - Select your Primary time zone region, e.g. 8 for Europe
 - Select your Secondary region, e.g. 21 for London.
- 16 A confirmation screen will show the settings you have chosen. It will also show the IP address of your DNS server. You will now be asked if you are satisfied with these settings. Type **Y**.
- 17 Type a new password for the `rfmngr` account and confirm it.
- 18 The RiskFilter Services will restart with your new settings in place.
- 19 Plug the network cable into the LAN 1 port of the appliance. This is the left port, when viewed from the rear.
- 20 Disconnect the monitor and keyboard from the appliance.

STAGE 3: UPDATING THE SOFTWARE

Before updating your software, read knowledge base article 1534, at <http://kb.surfcontrol.com>.

To update your RiskFilter software:

- 1 Open a Web browser and enter the following URL:
https://<hostname or IP address of appliance>:10000
- 2 Log in using your rfmngr username and password.
- 3 The System Management console will display. Click **RiskFilter**.
- 4 The **RiskFilter** tab will display. Click **Update RiskFilter – E-mail**.
- 5 The Update tab will display. Select the following checkboxes:
 - RiskFilter – E-mail
 - SurfControl OS
- 6 Click **OK**.
- 7 RiskFilter will download the latest software and OS updates, and also the latest Administrator's Guide. You will see a message on the screen to confirm that the update was successful.

Now activate your RiskFilter – E-mail license by using the Configuration Wizard – proceed to Stage 4.

STAGE 4: RUNNING THE CONFIGURATION WIZARD

Once you have configured the hardware of the appliance and updated the software, you can run the Configuration Wizard to finish the setup of RiskFilter. You can use this wizard to license the appliance as well as setting up routing and protected domains.



Note: Pop-up blockers will stop the RiskFilter wizards from launching. Ensure that you disable all pop-up blockers on any computer that need to run the RiskFilter wizards.

To start the wizard:

- 1 In a Web browser, enter the URL:
https://<hostname or IP address of appliance>/admin
- 2 The RiskFilter Administrator login page will appear. Type the username **administrator** and the password **admin**.
- 3 Click **Log In**.
- 4 Select **Help > Configuration Wizard** from the left-hand menu. The Configuration wizard will start.
- 5 Follow the instructions in the Configuration wizard which will enable you to:
 - License the appliance
 - Configure protected domains
 - Configure MX records

Activating your license without the Configuration Wizard

To activate your license without using the Configuration wizard:

- 1 In a Web browser, enter the URL:
https://<hostname or IP address of appliance>/admin
- 2 In the login page that follows type the username **administrator** and the password **admin**.
- 3 Click **Log In**.
- 4 The License Status page is displayed. Click the **View** button next to **Component License**.
- 5 Enter your Serial Number and Activation Code, then click **Submit**.

- 6 Fill out the user information form to complete the license registration and click **Submit**.
- 7 You will see a message to confirm that your license registration has been successful.

You must now update the Anti-Virus Agent (AVA) and Anti-Spam Agent (ASA) software. Proceed to Stage 5.

STAGE 5: AVA AND ASA UPDATES

Update the AVA and ASA files regularly to maintain the best protection against viruses and spam. To update the Anti-Virus Agent and Anti-Spam Agent pattern files:

- 1 In a Web browser enter the URL:
https://<hostname or IP address of appliance>/admin
- 2 In the login page that follows enter the default username **administrator** and the default password **admin**. Click **Login**.
- 3 On the System Settings tab, select **Update Now** from the **Update** menu.
- 4 Select the **Anti-Virus Definitions** and **Anti-Spam Definitions** checkboxes.
- 5 Click **Submit**. A message will confirm that the updates have been successful.

SETUP COMPLETE

You have now finished setting up RiskFilter – E-mail, and the appliance is ready to begin filtering e-mail. Consult the Administrator's Guide for information on how to:

- Create and apply policies.
- Fine-tune and optimize the RiskFilter – E-mail appliance for your corporate policy.
- Manage and monitor e-mail.

To view the Administrator's Guide, log in to the Administrator screen and select **Admin Guide** from the **Help** menu.

INTERFACE OVERVIEW

Now that you have the appliance installed and SurfControl RiskFilter up and running you can start to create filtering policies and run reports on the way your e-mail system is being used. There are two interfaces with which you can manage SurfControl RiskFilter:

- **SurfControl System Management Console (RiskFilter Management Console)** - Configures the RiskFilter appliance.
- **RiskFilter Console (Administrator)** - Configures the filtering settings on the appliance.

RISKFILTER CONSOLE

The SurfControl RiskFilter Console is where you manage the RiskFilter software. You can use this interface to:

- Manage user accounts and licensing.
- Schedule updates to Anti-Virus and Anti-Spam agents.
- Manage servers and connection issues.
- Set up policies to manage how users send and receive e-mail.
- Run reports on these users and their messages

As soon as the RiskFilter Administrator opens, you will see the Dashboard containing brief information about servers used, as well as a report showing general e-mail use: The Administrator's Guide contains detailed information on how to use all of RiskFilter Management Console's functionality. To access the RiskFilter Console:

- 1 Open a web browser and type **https://<hostname_or_ipaddress>/admin** where '<hostname_or_ipaddress>' is the name or IP address of your RiskFilter appliance.
- 2 At the RiskFilter Console login page enter the user name and password that you want to use to access the account. The default user name and password for the RiskFilter Console are:
 - User name = `administrator`
 - Password = `admin`
- 3 Click **Log in**.

This Management console interface consists of three tabs, each with its own set of menus.

The System Settings tab

The System Settings tab is where you configure the receiving and delivery of messages to and from the RiskFilter appliance:

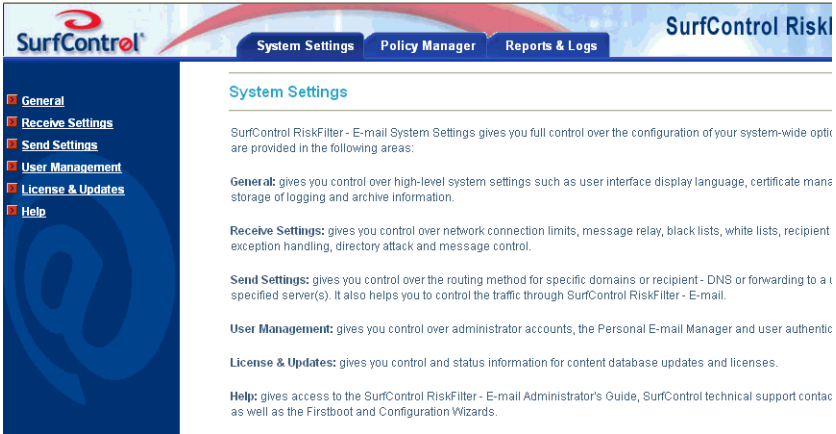


Figure 1 The System Settings Tab

Items that can be configured here include:

- User authentication and directories for storing messages and log files
- Personal E-mail Manager (PEM)
- Postmaster e-mail address
- Sending and receiving information
- Licensing and updates
- Proxy servers
- Certificates (using TLS)

The Policy Manager tab

The Policy Manager tab is where you set up your filtering policies using ready-made filters supplied with the product, plus filters that you can create yourself.

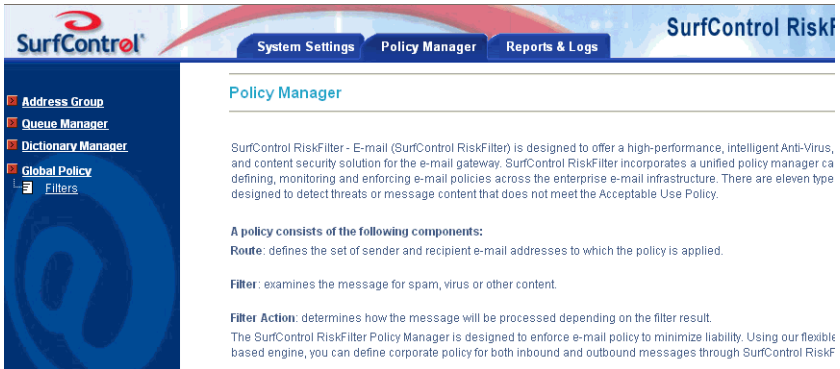


Figure 1 The Policy Manager tab

In this tab you can configure:

- Groups of users and addresses.
- Create and manage queues for isolated e-mails to be stored in.
- Dictionaries that enable RiskFilter to search for specific words in a message.
- Global policies that apply to everyone.

The Reports and Logs tab

The Reports and Logs tab enables you to run reports on how your users are using the e-mail system.

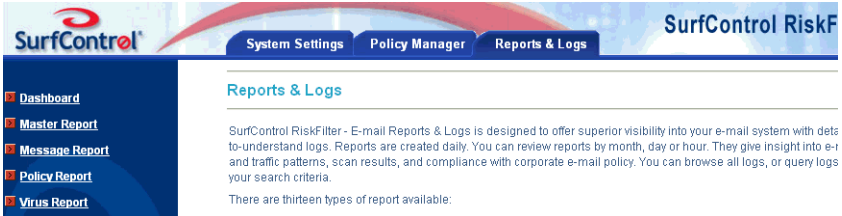


Figure 1 The Reports and Logs tab

This tab enables you to set up reports and logs for:

- General messages
- Messages that have been isolated to different queues
- Messages that have violated policies
- Messages that have been categorized as Spam or Virus

RISKFILTER SYSTEM MANAGEMENT CONSOLE

The RiskFilter Management Console enables you to configure the RiskFilter appliance itself as well as its interaction with the surrounding network. With RiskFilter Management Console you can:

- Use IP Access Control to only allow access to those IP addresses that you trust. This will prevent unauthorized access being gained by anyone who guesses your password.
- Make changes to the language that titles, prompts and messages etc will be displayed in within the RiskFilter appliance interfaces.
- Make network specific changes such as adding RiskFilter Management Console servers and specifying which IP addresses and port RiskFilter Management Console will bind to.
- Keep records of the various actions taken by administrators of the RiskFilter Management Console server.
- Check things like historic system settings and running processes.
- Change passwords.

To open the RiskFilter System Management Console:

- 1 Open a web browser and type
`https://<hostname_or_ipaddress>:10000/`
where '`<hostname_or_ipaddress>`' is the name or IP address of your RiskFilter appliance.
- 2 At the RiskFilter Management Console login page enter that username and password. The default username and password are:
 - Username = `rfmngr`
 - Password = `$rfmngxr$`
- 3 Click **Login**.

The RiskFilter Console interface consists of three tabs with which you can configure the RiskFilter system and environment.

The Webmin tab

The Webmin tab contains modules with which you can manage the RiskFilter System Management console and its connections.

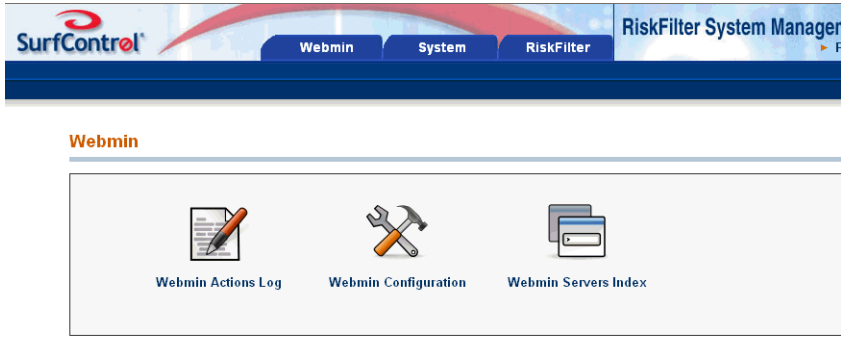


Figure 1 Webmin

- **Webmin Actions Log** - Generate reports on actions carried out by users within any of the modules, such as changing passwords, booting up/shutting down the computer or any configuration within the console.
- **Webmin Configuration** - Access modules to manage IP access, the language of messages from Webmin, ports and addresses, logging and proxy servers.
- **Webmin Servers Index** - Monitor multiple RiskFilter appliances without having to remember the password for each appliance.

The System tab

The System Tab gives you access to operating system level configuration such as Network Interfaces, System Time and passwords. It also contains modules to allow for monitoring of system processes and resources:

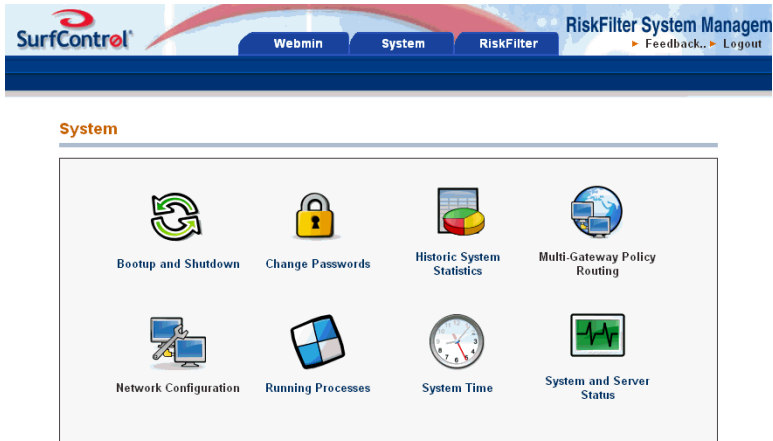


Figure 1 The System tab

- **Bootup and Shutdown** - Instantly reboot or shut down the system.
- **Change Passwords** - Change the password of the rfmngr account.
- **Historic System Statistics** - View real time and historic monitors of system usage.
- **Multi Gateway Policy Routing** - Set up dynamic routing to preserve ipv4 source addresses.
- **Network Configuration** - Specify how the RiskFilter System Management Console server connects and interacts with the network using network interfaces, routing and gateways, DNS client, host addresses, running processes, system time, system and server status.

The RiskFilter tab

The RiskFilter tab enables you to manage the configuration of services, backing up and updating of the software:

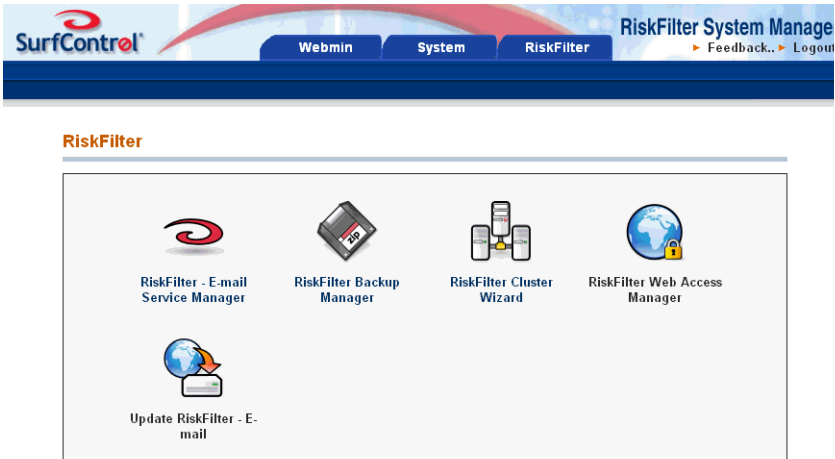


Figure 1 The RiskFilter tab

In this tab you can configure:

- **RiskFilter Services Manager** - Start, stop and restart RiskFilter. You can also see the status of:
 - Msoftsmg service - The mail processor and SMTP server
 - Msoftadmin service - The user interface
 - Msoftnp.dc service - The document convertor (extracts text from .docs/.pdfs/.exl files)
 - Avagent.mcafee service - the McAfee Anti-Virus engine.
- **RiskFilter Backup Manager** - Make copies of your RiskFilter configuration. Back up files on a real-time basis, or set a schedule so these files are backed up automatically at pre-set times.
- **RiskFilter Cluster Wizard** - Set up the RiskFilter appliance as a node in a cluster. The appliance can be configured into three modes:
 - Master - a server that gathers all logging information, the master may or may not process spam.
 - Slave - a server that processes e-mail and reports everything to a master server.
 - Original configuration - the 'out of the box' configuration

- **RiskFilter Web Access Manager** - Manage access to the two HTTP servers: Webmin and the Administrator Console. Access can be set to be by HTTP and HTTPS.
- **Update RiskFilter** - Download the latest version of the RiskFilter software as you did when you first set up RiskFilter.

FURTHER READING

The following provide more information on configuring and using RiskFilter.

- **RiskFilter Administrator's Guide V5.2** - this is supplied with the software and can be accessed from the Help menu in the RiskFilter Management Console.
- **Knowledge base articles** - Visit <http://kb.surfcontrol.com> and search for the following ID Numbers:
 - 1534 - information about the latest version of the software.

TECHNICAL SUPPORT

Visit www.surfcontrol.com/support. To speak to a technical support representative, call SurfControl Technical Support:

Table 1 Technical Support contact details

Region	Hours of Operation	Number
USA	8:00 AM - 8:00 PM (EST)Monday - Friday	(831) 440-2700
Europe	9:00 AM - 5:30 PM (GMT)Monday - Friday	+44 1260 296 259
Asia	9:00 AM - 5:30 PM (Beijing, Hong Kong, Taiwan, Singapore, GMT +8) Monday - Friday	+65 6823 1313
Australia	7:30 AM - 6:00 PM (Australia Eastern) Monday - Friday	+61 2941 40033