▷ PROTECTION AT THE SPEED OF BUSINESS

SonicWALL Enforced Client Anti-Virus and Anti-Spyware Product Guide

Version 4.5

SONICWALL®

Enforced Client Anti-Virus and Anti-Spyware 4.5COPYRIGHT

Copyright © 2007 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of NcAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (AND IN KATAKANA), ACTIVESHIELD, CLEAN-UP, DESIGN (STYLIZED E), DESIGN (STYLIZED N), ENTERCEPT, EPOLICY ORCHESTRATOR, FIRST AID, FOUNDSTONE, GROUPSHIELD, GROUPSHIELD (AND IN KATAKANA), INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, MCAFEE, MCAFEE (AND IN KATAKANA), MCAFEE AND DESIGN, MCAFEE.COM, MCAFEE VIRUSSCAN, NET TOOLS, NET TOOLS (AND IN KATAKANA), NETSCAN, NETSHIELD, NUTS & BOLTS, OIL CHANGE, PRIMESUPPORT, SPAMKILLER, THREATSCAN, TOTAL VIRUS DEFENSE, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, VIRUSSCAN (AND IN KATAKANA), WEBSCAN, WEBSHIELD, WEBSHIELD (AND IN KATAKANA) are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. The color red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANIES YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Attributions

This product includes or may include:

• Software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/). • Cryptographic software written by Eric A. Young and software written by Tim J. Hudson. • Some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar Free Software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires that for any software covered under the GPL which is distributed to someone in an executable binary format, that the source code also be made available to those users. For any such software covered under the GPL, the source code is made available on this CD. If any Free Software licenses require that McAfee pro-+34vide rights to use, copy or modify a software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein. • Software originally written by Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer. • Software originally written by Robert Nordier, Copyright © 1996-7 Robert Nordier. • Software written by Douglas W. Sauder. • Software developed by the Apache Software Foundation (http://www.apache.org/). A copy of the license agreement for this software can be found at www.apache.org/licenses/LICENSE-2.0.txt. • International Components for Unicode ("ICU") Copyright ©1995-2002 International Business Machines Corporation and others. • Software developed by CrystalClear Software, Inc., Copyright ©2000 CrystalClear Software, Inc. • FEAD® Optimizer® technology, Copyright Netopsystems AG, Berlin, Germany. • Outside In® Viewer Technology ©1992-2001 Stellent Chicago, Inc. and/or Outside In® HTML Export, © 2001 Stellent Chicago, Inc. • Software copyrighted by Thai Open Source Software Center Ltd. and Clark Cooper, © 1998, 1999, 2000. • Software copyrighted by Expat maintainers. • Software copyrighted by The Regents of the University of California, © 1996, 1989, 1998-2000. • Software copyrighted by Gunnar Ritter. • Software copyrighted by Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A., © 2003. • Software copyrighted by Gisle Aas. © 1995-2003. • Software copyrighted by Michael A. Chase, © 1999-2000. • Software copyrighted by Neil Winton, ©1995-1996. • Software copyrighted by RSA Data Security, Inc., © 1990-1992. • Software copyrighted by Sean M. Burke, © 1999, 2000. • Software copyrighted by Martijn Koster, © 1995. • Software copyrighted by Brad Appleton, © 1996-1999. • Software copyrighted by Michael G. Schwern, ©2001. • Software copyrighted by Graham Barr, © 1998. • Software copyrighted by Larry Wall and Clark Cooper, © 1998-2000. • Software copyrighted by Frodo Looijaard, © 1997. • Software copyrighted by the Python Software Foundation, Copyright © 2001, 2002, 2003. A copy of the license agreement for this software can be found at www.python.org. • Software copyrighted by Beman Dawes, © 1994-1999, 2002. • Software written by Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame. • Software copyrighted by Simone Bordet & Marco Cravero, © 2002. • Software copyrighted by Stephen Purcell, © 2001. • Software developed by the Indiana University Extreme! Lab (http://www.extreme.indiana.edu/). • Software copyrighted by International Business Machines Corporation and others, © 1995-2003. • Software developed by the University of California, Berkeley and its contributors. • Software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/). • Software copyrighted by Kevlin Henney, © 2000-2002. • Software copyrighted by Peter Dimov and Multi Media Ltd. © 2001, 2002. • Software copyrighted by David Abrahams, © 2001, 2002. See http://www.boost.org/libs/bind/bind.html for documentation. • Software copyrighted by Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000. • Software copyrighted by Boost.org, © 1999-2002. • Software copyrighted by Nicolai M. Josuttis, © 1999. • Software copyrighted by Jeremy Siek, © 1999-2001. • Software copyrighted by Daryle Walker, © 2001. • Software copyrighted by Chuck Allison and Jeremy Siek, © 2001, 2002. • Software copyrighted by Samuel Krempp, © 2001. See http://www.boost.org for updates, documentation, and revision history. • Software copyrighted by Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002. • Software copyrighted by Cadenza New Zealand Ltd., © 2000. • Software copyrighted by Jens Maurer, ©2000, 2001. • Software copyrighted by Jaakko Järvi (jaakko.jarvi@cs.utu.fi), ©1999, 2000. • Software copyrighted by Ronald Garcia, © 2002. • Software copyrighted by David Abrahams, Jeremy Siek, and Daryle Walker, ©1999-2001. • Software copyrighted by Stephen Cleary (shammah@voyager.net), ©2000. • Software copyrighted by Housemarque Oy <http://www.housemarque.com>, © 2001. • Software copyrighted by Paul Moore, © 1999. • Software copyrighted by Dr. John Maddock, © 1998-2002. • Software copyrighted by Greg Colvin and Beman Dawes, © 1998, 1999. • Software copyrighted by Peter Dimov, © 2001, 2002. • Software copyrighted by Jeremy Siek and John R. Bandela, © 2001. • Software copyrighted by Joerg Walter and Mathias Koch, © 2000-2002. • Software copyrighted by Carnegie Mellon University © 1989, 1991, 1992. • Software copyrighted by Cambridge Broadband Ltd., © 2001-2003. • Software copyrighted by Sparta, Inc., © 2003-2004. • Software copyrighted by Cisco, Inc. and Information Network Center of Beijing University of Posts and Telecommunications, © 2004. • Software copyrighted by Simon Josefsson, © 2003. • Software copyrighted by Thomas Jacob, © 2003-2004. • Software copyrighted by Advanced Software Engineering Limited, © 2004. • Software copyrighted by Todd C. Miller, © 1998. • Software copyrighted by The Regents of the University of California, © 1990, 1993, with code derived from software contributed to Berkeley by Chris Torek.

PATENT INFORMATION

Protected by US Patents 6,006,035; 6,029,256; 6,035,423; 6,151,643; 6,266,774; 6,266,811; 6,269,456; 6,301,699; 6,457,076; 6,496,875; 6,510,448; 6,542,943; 6,550,012; 6,594,686; 6,611,925; 6,622,150; 6,668,289; 6,684,329; 6,697,950; 6,725,377; 6,728,885; 6,757,830; 6,763,403; 6,775,780; 6,782,527; 6,799,197; 6,823,460; 6,839,852; 6,907,396; 6,931,540; 6,931,546; 6,947,986; 6,966,059; 6,973,578; 6,976,068; 6,978,454; 6,988,209; 7,016,939; 7,058,975; 7,069,330.

Contents

1 Introduction

SonicWALL Enforced Client Anti-Virus and Anti-Spyware, referred to in this guide as Enforced Client, safeguards your computers automatically, and its advanced features let you customize your business's security strategy.

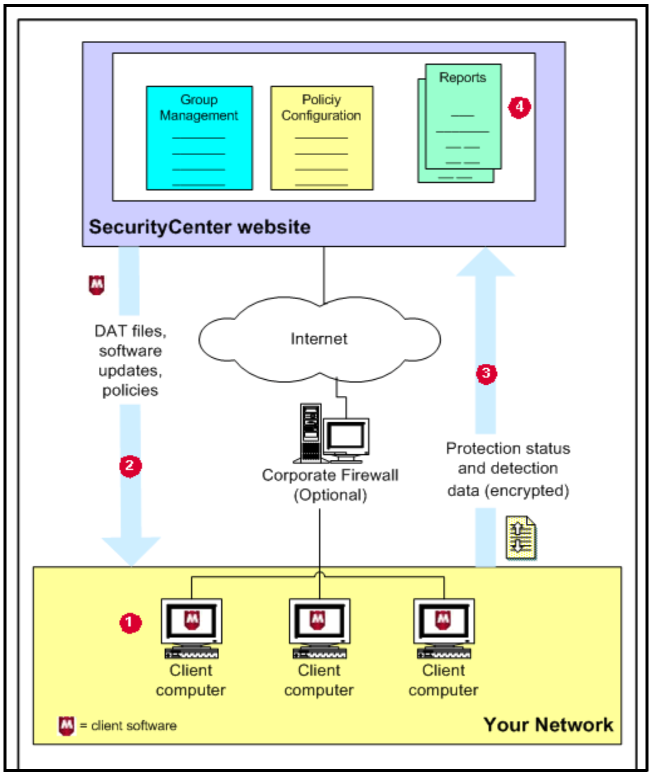
This section provides an overview of the product, its features, and how to use product resources for additional assistance.

- *What is Enforced Client?*
- *What is new in this release?*
- *How does the software work?*
- *Managing with the online SecurityCenter*
- *Using this guide*
- *Getting product information*

What is Enforced Client?

Enforced Client delivers comprehensive security as a service for all the computers on your account. These services automatically check for threats, intercept them, take the appropriate action to keep your data and your network safe, and track detections and security status for reports.

Figure 1-1 Enforced Client overview



1 The Enforced Client client software runs on each computer where it is installed.

2 The client software updates itself — automatically and silently — by downloading the latest detection definition (DAT) files from your account's administrative website, the SonicWALL SecurityCenter.

3 The client software uploads security information about each computer to the SecurityCenter for use in administrative reports.

4 As your account's administrator, you can use a web browser to visit the SecurityCenter, where you can access reports that detail the status of client computers and use tools for customizing and managing security.

- *Select the right version of Enforced Client*
- *Protect against many kinds of threats*
- *Ensure continuous, automatic protection*

Select the right version of Enforced Client

Select the version that best supports your needs.

Basic	Advanced
■ Virus and spyware protection for desktop computers and servers. ■ Firewall protection for desktop computers and servers. ■ Browser protection for desktop computers. ■ Access to the SonicWALL SecurityCenter for centralized management of your accounts.	■ Virus and spyware protection for desktop computers and servers. ■ Firewall protection for desktop computers and servers. ■ Browser protection for desktop computers. ■ Access to the SonicWALL SecurityCenter for centralized management of your accounts. ■ Email security: Email security service to protect all inbound email against virus, spam, and phishing attacks, or Email server security application for additional virus protection at the server level.

This guide focuses on the Enforced Client services for desktop computers and servers, and also contains instructions for setting up the email security service available in Enforced Client Advanced. Refer to your product CD or the SonicWALL download center for information about using the email server security application.

Protect against many kinds of threats

Enforced Client protects against a broad range of threats:

- The **virus and spyware protection service** checks for viruses, spyware, unwanted programs, and other potential threats borne on removable media or brought in from your network, including via email. Every time a file on your computer is accessed, your service scans the file to make sure it is free of viruses and spyware.
- The **firewall protection service** establishes a barrier between each computer and the Internet or other computers on your local network. It silently monitors communications traffic for suspicious activity and takes appropriate action, such as blocking.
- The **browser protection service** displays information to safeguard client computer users against web-based threats. Users can view website safety ratings and safety reports as they browse or search with Microsoft Internet Explorer or Mozilla Firefox.
- The **email security service** protects against email threats by scanning messages before they are received. It blocks or quarantines detections of directory harvest attacks, spam, phishing scams, viruses, and other email-borne threats in messages and attachments, to prevent them from reaching client computers. The email security service is available with Enforced Client Advanced.
- The **email server security application**, SonicWALL GroupShield® for Microsoft Exchange and Lotus Domino, provides comprehensive virus protection for the email and other content entering and leaving your Microsoft Exchange Server 2000/2003 environment. Proactive anti-virus scanning and an automatic outbreak manager prevent malicious code from disrupting the system, while advanced content filtering allows administrators to set up rules for inappropriate content, sensitive information, and adding disclaimers to messages.

The email server security application is available with Enforced Client Advanced. Detailed documentation on this application is available on the CD or in the downloadable installer accessible from the SonicWALL download center.

Ensure continuous, automatic protection

Enforced Client safeguards your computers with:

- Continuous protection — From the time a client computer is turned on until it is turned off, Enforced Client silently monitors all file input and output, downloads, program executions, inbound and outbound communications, and other system-related activities.
- Instant discovery — When Enforced Client detects a virus threat, it attempts to clean the item containing the threat before further damage can occur. If an item cannot be cleaned, a copy of it is placed in a quarantine folder and the original item is deleted.
- Customized threat response — By default, Enforced Client provides a high degree of protection against threats. You can also configure the response to detections of potentially unwanted programs and suspicious activity to suit the needs of your business: take immediate action to clean, quarantine, or block the detection; prompt users for a response; or only log the detection for administrative reports.
- Automatic updates — Enforced Client checks for product updates at regular intervals throughout the day, comparing security components against the latest releases. When a computer needs a newer version, the client software automatically retrieves it.
- Avert Early Warning system and outbreak response — Enforced Client uses the latest information about threats and outbreaks as soon as they are discovered by SonicWALL Avert Labs, a research division of SonicWALL. Whenever Avert Labs releases an outbreak detection definition (DAT) file, your network receives it promptly.

What is new in this release?

New features

New feature	Description
Browser protection service	Protects client computers against web-based threats while searching and browsing. Users can display a color-coded safety rating and detailed report for each website. See *Chapter 6, Using the Browser Protection Service*.
New policy options for greater control	Virus and spyware protection service: On-demand scans now scan all file types by default, or administrators can select a policy option to scan only certain types of files. See *Enable optional protection* on page 97. Firewall protection service: Select whether to use SonicWALL recommendations for safe Internet applications or allow only those you specify. See *Specify whether to use SonicWALL recommendations* on page 121.
Auto-renewal option	If your service provider has enabled this option, automatically renews your subscriptions before they expire.

Changes in support

Support for...	Description
Operating systems	■ Provides protection services for computers running Windows Vista. ■ Extends support to 64-bit versions of Windows XP and Windows Vista. See *Operating systems* on page 27. ■ Computers running older versions of Windows will continue to be supported against existing threats, but protection against new threats will be phased out as DAT files are no longer updated. See *Operating system support ending* on page 28. ■ Administrators can configure a policy option for displaying notifications on client computers to remind users that support is ending. See *Notifying users when support ends* on page 28.
Browsers	■ Installs on computers using Windows Internet Explorer version 7. See *Chapter 2, Installing Enforced Client*. ■ Adds browser protection for Mozilla Firefox. See *Chapter 6, Using the Browser Protection Service*.
Languages	With Enforced Client Advanced, **Quarantine Summary** emails generated by the email security service are now available in multiple languages. **Note:** No localized version is available for Brazilian Portuguese.

How does the software work?

Enforced Client implements a three-prong approach to security by:

1. Silently monitoring all file input and output, downloads, program executions, inbound and outbound communications, and other system-related activities on client computers.
    - Detected viruses are deleted or quarantined automatically.
    - Potentially unwanted programs, such as spyware or adware, are removed automatically unless you select a different response.
    - Suspicious activity is blocked unless you specify a different response.
2. Regularly updating detection definition (DAT) files and software components to ensure that you are always protected against the latest threats.
3. Uploading security information for each client computer to the SecurityCenter, then using this information to send emails and create reports that keep you informed about your account’s status.

In addition, it provides tools for managing client computers and customizing your security strategy.

- *The updating process*
- *Outbreak response*
- *Rumor technology*
- *Internet Independent Updating (IIU)*

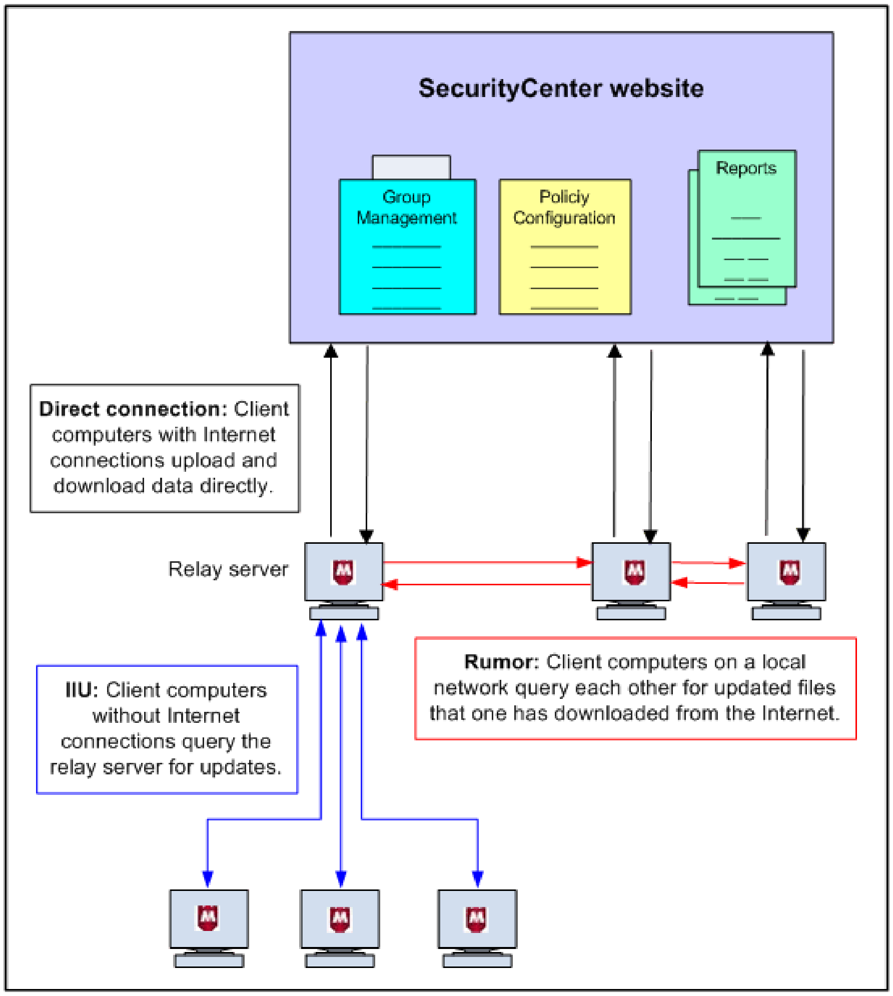
The updating process

Regular updates are the cornerstone of Enforced Client.

- Updates of its security components running on client computers. See *Retrieving updates*.
- Updates to the security data maintained on the SecurityCenter website and used in administrative reports. See *Uploading security information*.

Updates can occur in three ways, enabling you to use network resources efficiently.

Figure 1-2 Methods for updating client computers


SecurityCenter website
Group Management
Policiy Configuration
Reports
Direct connection: Client computers with Internet connections upload and download data directly.
Relay server
Rumor: Client computers on a local network query each other for updated files that one has downloaded from the Internet.
IIU: Client computers without Internet connections query the relay server for updates.

- In a simple scenario, each client computer on your account has a *direct connection* to the Internet and checks for new updates.
- *Rumor technology* enables all computers in a workgroup to share downloaded files, which controls Internet traffic and minimizes expensive downloads.
- *Internet Independent Updating (IIU)* enables any computer on the network to get information from the update site, even if that computer does not have an Internet connection, as long as at least one computer on the network is configured as a relay server.

Retrieving updates

Five minutes after a client computer starts, and at regular intervals throughout the day, the Enforced Client client software checks if updates are available. If they are, the client computer pulls them from another computer on the network (via *Rumor technology*) or downloads them directly from the Internet site.

The detection definition (DAT) files on the Internet site are regularly updated to add protection against new threats. When the client software connects to the update site on the Internet, it retrieves:

- Regular DAT files, which contain the latest definitions for viruses, potentially unwanted programs, and cookies and registry keys that might indicate spyware.
- Outbreak DAT files, which are high-priority detection definition files released in an emergency situation (see *Outbreak response*).
- Upgrades to the software if a newer version exists.
- Policy updates.

At any time, users can update manually by double-clicking M in the system tray.

> Update support for some operating systems is ending. After support ends, client computers running those operating systems will no longer be protected against new threats. See *Operating system support ending* on page 28 for more information.

Uploading security information

Client computers upload detection and status data hourly to the SecurityCenter website. This information is available to administrators in reports they can view on the SecurityCenter (see *Viewing reports* on page 78).

Outbreak response

When an outbreak of a new threat is identified by Avert Labs, they issue an *outbreak DAT*, which is a special detection definition (DAT) file marked as **Medium** or **High** importance. It is specially encoded to inform the first computer receiving it to share the update immediately with other client computers on the network. By default, client computers check for an outbreak DAT every hour.

Rumor technology

When one computer shares updates with other computers on the local area network (LAN), rather than requiring each computer to retrieve updates from the update website individually, the Internet traffic load on the network is reduced. This process of sharing updates is called *Rumor*.

1. Each client computer checks the version of the most recent *catalog* file on the Internet site. This catalog file contains information for every component in Enforced Client, and is stored in a digitally signed, compressed .CAB file format.
   - If the version is the same as the catalog file on the client computer, the process stops here.
   - If the version is different from the catalog file on the client computer, the client computer attempts to retrieve the latest catalog file from its peers. It queries if other computers on the LAN have already downloaded the new catalog file.
2. The client computer retrieves the required catalog file (directly from the Internet site or from one of its peers) and uses it to determine if new components are available for Enforced Client.
3. If new components are available, the client computer attempts to retrieve them from its peers. It queries if computers on the LAN have already downloaded the new components.

- If so, the client computer retrieves the update from a peer. (Digital signatures are checked to verify that the computer is valid.)
- If not, the client computer retrieves the update directly from the update site.

4 On the client computer, the catalog file is extracted and new components are installed.

Internet Independent Updating (IIU)

Internet Independent Updating enables computers to use Enforced Client when they are not connected to the Internet. At least one computer on the subnet must have an Internet connection to be able to communicate with the udpate site. That computer is configured as a *relay server*, and computers without an Internet connection retrieve updates locally from the relay server.

1 When a computer without Internet access fails to connect directly to the update site, it requests information from the relay server.

2 The relay server downloads a catalog of updates from the update site.

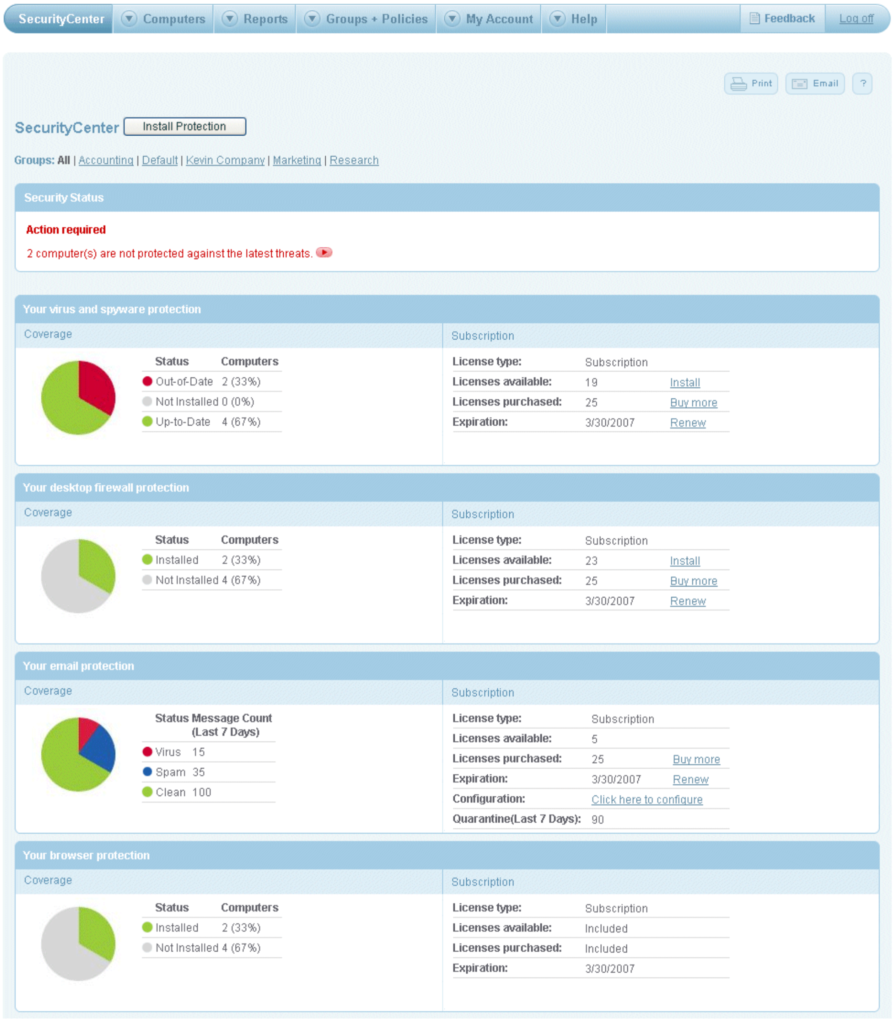
3 The computer with no Internet connection downloads the necessary updates from the relay server.

For more information, see *Enabling relay servers* on page 46.

Managing with the online SecurityCenter

To manage your account via the SecurityCenter, use the URL you received in an email message from your service provider. From the SecurityCenter, you can view the status of your protection services, access reports on client activity such as detections and suspicious activity, update your account data, and configure security settings. You can manage client computers by customizing how often they check for updates, changing the way they handle detections, and scheduling regular scans.

Figure 1-3 The online SecurityCenter



SecurityCenter

Groups: All | Accounting | Default | Kevin Company | Marketing | Research

Security Status

Action required

2 computer(s) are not protected against the latest threats.

Your virus and spyware protection

Coverage

Status	Computers
🟥 Out-of-Date	2 (33%)
○ Not Installed	0 (0%)
🟩 Up-to-Date	4 (67%)

Subscription

License type:	Subscription	
Licenses available:	19	Install
Licenses purchased:	25	Buy more
Expiration:	3/30/2007	Renew

Your desktop firewall protection

Coverage

Status	Computers
🟩 Installed	2 (33%)
○ Not Installed	4 (67%)

Subscription

License type:	Subscription	
Licenses available:	23	Install
Licenses purchased:	25	Buy more
Expiration:	3/30/2007	Renew

Your email protection

Coverage

Status	Message Count (Last 7 Days)
🟥 Virus	15
🟦 Spam	35
🟩 Clean	100

Subscription

License type:	Subscription	
Licenses available:	5	
Licenses purchased:	25	Buy more
Expiration:	3/30/2007	Renew
Configuration:	Click here to configure	
Quarantine(Last 7 Days):	90	

Your browser protection

Coverage

Status	Computers
🟩 Installed	2 (33%)
○ Not Installed	4 (67%)

Subscription

License type:	Subscription
Licenses available:	Included
Licenses purchased:	Included
Expiration:	3/30/2007

The SecurityCenter's main page shows a status summary for all the protection services you have purchased (except email server protection):

- **Security Status** — Indicates whether any action is required to address security issues, and links you to instructions for resolving them.
- **Your virus and spyware protection** — Illustrates the number of computers that are up-to-date and out-of-date, and where the virus and spyware protection service is not installed. Click a color in the pie chart to display a list of computers in that category.
- **Your desktop firewall protection** — Illustrates the number of computers where the firewall protection service is and is not installed. Click a color in the pie chart to display a list of computers in that category.
- **Your email protection** — Illustrates the number of messages delivered by category (clean, spam, virus detected). Click a color in the pie chart or select the **Click here to configure** link to open the email security service's web portal and view reports about your email.
- **Your browser protection** — Illustrates the number of computers where the browser protection service is and is not installed. Click a color in the pie chart to display a list of computers in that category.

See *Using the SecurityCenter* on page 55 for more information.

The SecurityCenter offers two powerful tools for displaying your computers in groups and fine-tuning their security settings.

- *User groups* enable you to effectively categorize and manage client computers that require different security settings or special monitoring.
- *Customized policies* allow you to specify security settings to meet the needs of your users and effectively use your network resources.

User groups

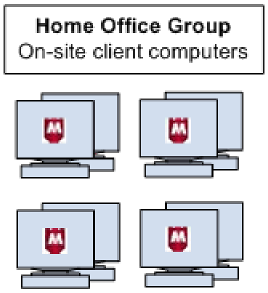
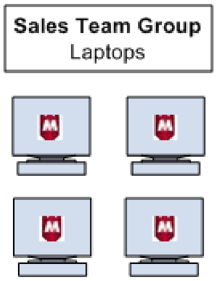
Each computer running the client software belongs to a group. A group consists of one or more computers using the same security settings (called *policies*). By default, computers are placed in the **Default** group.

Groups help you manage different types of computers effectively. You can base groups on geographic location, department, computer type, user tasks, or anything meaningful to your organization.

For example, you might place all laptops used by traveling sales representatives into a single group called Sales Team. You can then view details about this group of computers separately from other computers in your account. You can easily check detections for these computers or customize their security settings in a policy (see *Customized policies* on page 19) that accounts for specific circumstances and risks of a remote user.

To create groups, use the **Groups + Policies** tab on the SecurityCenter website. See *Creating groups to manage your site* on page 71 for more information.

The following example shows how an administrator might configure policies for three different groups of client computer users in an organization. You should configure policies for your users to meet your own company's needs.

Policy Setting			
	Weekly	Daily	Daily
Enable outbreak response	Enabled	Enabled	Enabled
Scan within archives during on-access scans	No	Enabled	Enabled
Check for updates every	12 hours	4 hours	4 hours
Spyware Protection Mode	Prompt	Protect	Prompt
Approved Programs	None	None	Nmap remote admin tool
Firewall Protection Mode	Protect	Protect	Prompt
Use Smart Recommendations to automatically approve common Internet applications	Enabled	No	Enabled
Connection Type	Trusted network	Untrusted network	Trusted network
Allowed Internet Applications	AOL Instant Messenger	None	AOL Instant Messenger GoogleTalk

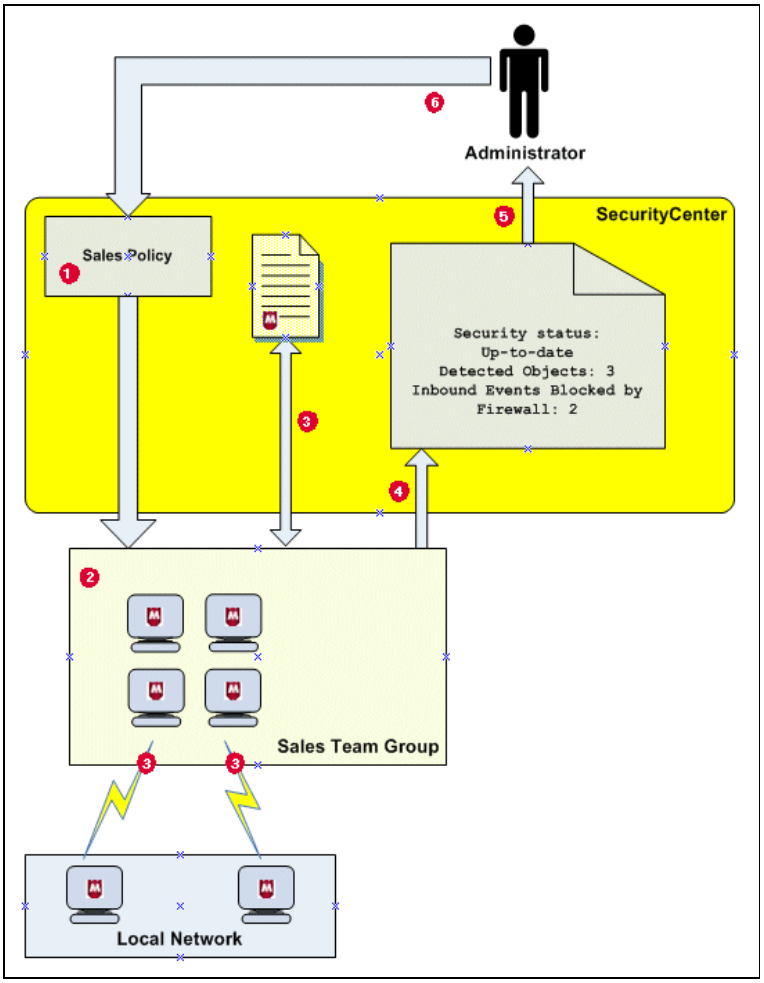
Customized policies

After installation, Enforced Client protects client computers from threats immediately using default security settings. However, you might want to change the way some features are implemented for some or all of your computers. For example, you might want the service to check for updates every four hours or set up a list of programs you consider safe.

Policies are made up of security settings that define how protection services operate on client computers. Policy management allows you to assign different levels and types of protection to different users. If you have created groups, you can assign a unique policy to each group or one policy to all groups.

For example, you can assign a Sales policy to your mobile Sales Team group, with security settings that protect against threats in unsecure networks such as airports and hotels.

Figure 1-4 Example: Sales Team group and Sales policy



1 Create a Sales Team group and a Sales policy.

2 Assign the Sales policy to the Sales Team group.

3 Client software running on computers in the Sales Team group performs the tasks defined in the Sales policy:

- Check for updates to software components and DAT files every 4 hours.
- Check for outbreak DAT file every hour.
- Scan for viruses and potentially unwanted programs daily.
- Block communication from computers on local network (untrusted network).

4 Client software sends security data for each client computer to the SecurityCenter.

5 Administrator checks the security status for the Sales Team group in reports on the SecurityCenter.

6 The administrator adjusts the Sales policy. The modified policy is downloaded automatically to client computers in the Sales Team group the next time they check for updates.

To create your own policies and assign them to computers or groups, use the **Groups + Policies** tab on the SecurityCenter website. See *Setting up policies* on page 75 for more information.

Using this guide

This guide provides information on installing, configuring, using, and troubleshooting Enforced Client.

- *Who should read this guide?*
- *Conventions*

Who should read this guide?

This information is designed for:

- System and network administrators who want to implement a proactive, hands-on approach to their security strategy.
- Partner Security Services (PSS) partners who remotely manage and monitor the SecurityCenter on behalf of their customer base.

Hands-off administrators who do not need to customize security settings can read an overview of basic features in the *Quick Start Guide*, which is available from the **Help** page on the SecurityCenter website.

Conventions

This guide uses the following conventions:

Bold Condensed

All words from the user interface, including options, menus, buttons, and dialog box names.

Example:
Type the **User** name and **Password** of the desired account.

`Courier`

The path of a folder or program; text that represents something the user types exactly (for example, a command at the system prompt).

Example:
The default location for the program is:

```
    C:\Program Files\McAfee\EPO\3.5.0
```

Run this command on the client computer:

```
    C:\SETUP.EXE
```

Italic

For emphasis or when introducing a new term; for names of product documentation and topics (headings) within the material.

Example:
Refer to the *VirusScan Enterprise Product Guide* for more information.

Blue

A web address (URL) and/or a live link.

Visit the SonicWALL website at:
http://www.mcafee.com

<TERM>

Angle brackets enclose a generic term.

Example:
In the console tree, right-click <SERVER>.

ⓘ **Note:** Supplemental information; for example, an alternate method of executing the same command.

💡 **Tip:** Suggestions for best practices and recommendations from SonicWALL for threat prevention, performance, and efficiency.

❗ **Caution:** Important advice to protect your computer system, enterprise, software installation, or data.

⚠ **Warning:** Important advice to protect a user from bodily harm when interacting with a hardware product.

Getting product information

Several types of information are available to meet the specific needs of client computer users and administrators.

Users — Client computer users can access online help from links in the client software.	
	Access online instructions for performing security tasks in two ways: ■ Click **help** on any window displayed by the client software. ■ Click M in the system tray and select **Help**. **Note:** If the product's built-in help system displays incorrectly on a client computer, its version of Microsoft Internet Explorer might not be using ActiveX controls properly. These controls are required to display the help file. Make sure the latest version of Internet Explorer is installed with its Internet security settings set to **Medium** or **Medium-high**.
Online Installation Instructions	Click the **help** link on any installation dialog box to display instructions for installing Enforced Client using the URL method. Also contains instructions for preparing for installation, testing, uninstalling, and troubleshooting installation issues.
Administrators — Unless otherwise noted, these product documents are Adobe Acrobat .PDF files available on the product CD or the **Help** page of the SecurityCenter.	
Product Guide	Product introduction and features, detailed instructions for configuring the software, information on deployment, recurring tasks, and operating procedures. Recommended for administrators who manage large organizations or multiple accounts, and for hands-on administrators who want to customize security settings and actively monitor client computers.
Quick Start Guide	A short "getting started" with information on basic product features, routine tasks that you perform often, and critical tasks that you perform occasionally. Recommended for first-time customers who need an overview of the product, and for hands-off administrators who plan to use the default security settings and monitor security status through their weekly status email.
Release Notes	*ReadMe*. Product information, resolved issues, known issues, and last-minute additions or changes to the product or its documentation. Available as a text document.
Online SecurityCenter help	For information about any page of your SecurityCenter website, click the help (**?**) link in the upper-right corner. You can access additional information with the table of contents, index, or search feature.
Online Push Install help	While running the Push Install utility, click the **help** link on any dialog box for information about deploying client software remotely to one or more computers without user intervention.
Avert Labs Threat Library	After an update, click **Avert Labs Threat Library** on the Enforced Client window to access the online SonicWALL Threat Library. This website has detailed information on where threats come from, how they infect your system, and how to remove them. The Avert Labs Threat Library contains useful information on hoaxes, such as virus warnings that you receive via email. *A Virtual Card For You* and *SULFNBK* are two of the best-known hoaxes, but there are many others. Next time you receive a well-meaning warning, view our hoax page before you pass the message on to your friends.

Enforced Client Advanced — With Enforced Client Advanced, additional documents are available.	
	See *Chapter 7, Using the Email Security Service* for instructions on setting up and using basic features of the email security service. Links are available from the SecurityCenter website to the email security service's web portal, where you can configure the service, access its administration guide, and view reports.
Email server security application	Detailed documentation for the email server security application is available on the product CD or in the downloadable installer accessible from the SonicWALL download center.

Contact information

Threat Center: SonicWALL Avert® Labs http://www.mcafee.com/us/threat_center/default.asp

Avert Labs Threat Library
http://vil.nai.com

Avert Labs WebImmune & Submit a Sample *(Logon credentials required)*
https://www.webimmune.net/default.asp

Avert Labs DAT Notification Service
http://vil.nai.com/vil/signup_DAT_notification.aspx

Download Site http://www.mcafee.com/us/downloads/

Product Upgrades *(Valid grant number required)*

Security Updates (DATs, engine)

HotFix and Patch Releases

- **For Security Vulnerabilities** *(Available to the public)*
- **For Products** *(ServicePortal account and valid grant number required)*

Product Evaluation

SonicWALL Beta Program

Technical Support http://www.mcafee.com/us/support/

KnowledgeBase Search
http://knowledge.mcafee.com/

SonicWALL Technical Support ServicePortal *(Logon credentials required)*
https://mysupport.mcafee.com/eservice_enu/start.swe

Customer Service

Web
http://www.mcafee.com/us/support/index.html
http://www.mcafee.com/us/about/contact/index.html

Phone — US, Canada, and Latin America toll-free:
+1-888-VIRUS NO or **+1-888-847-8766** Monday – Friday, 8 a.m. – 8 p.m., Central Time

Professional Services

Small and Medium Business: http://www.mcafee.com/us/smb/services/index.html

Enforced Client

Beta Site
http://betavscan.mcafeeasap.com

Beta Feedback
DL_ToPS_SMB_Beta@mcafee.com

2 Installing Enforced Client

This section describes what happens after you purchase the hosted services in Enforced Client and Enforced Client Advanced, provides system requirements, and explains how to install the virus and spyware protection service, firewall protection service, and browser protection service.

> ℹ If you purchased Enforced Client Advanced, refer to emails and materials from SonicWALL for instructions on installing the email security service or email server security application. See *Chapter 7, Using the Email Security Service* for information about activating and setting up the email security service.

- *After you place your order*
- *System requirements*
- *Before you install*
- *Installing Enforced Client*
- *Completing the installation*
- *What should I do after installing?*

After you place your order

When you place an order for Enforced Client, you supply an email address, and your account is associated with that email address. After you submit your order:

1 SonicWALL processes your order.

2 You receive three emails:

This email...	**Contains...**
Welcome	The download URL and instructions for installing the protection services, accessing documentation, and contacting customer support.
Login credentials	Instructions for logging on to the SonicWALL SecurityCenter administrative website and changing your password.
Grant letter	The grant number for the order, which is required for customer support.

3 If you purchased Enforced Client Advanced, you also receive an email with instructions for changing your MX (Mail eXchange) records. See *Update your MX records* on page 135.

If you purchased Enforced Client from a SonicWALL partner who manages security for you, the partner usually receives these emails. If you have questions about which emails you should receive, contact the partner.

Placing multiple orders

If you placed more than one order using different email addresses, you have more than one Enforced Client account. To merge them so that all your security information and emails are sent to a single email address, contact the SonicWALL partner from whom you ordered, or SonicWALL customer support if you ordered directly from SonicWALL.

System requirements

Enforced Client is designed for Microsoft Windows operating systems running on a PC platform. It installs and runs on computers equipped with:

- An Intel Pentium processor or compatible architecture.
- Microsoft Internet Explorer 5.5 SP2 or later.
- *Operating systems*
- *RAM*
- *Email security service*
- *Email server security application*
- *Terminal servers*

Operating systems

	Protection services		
Operating system	**Virus and spyware**	**Firewall**	**Browser**
Client computers			
Windows 2000 Professional with Service Pack 3 or later	✓	✓	✓
Windows XP Home Windows XP Professional (32-bit)	✓	✓	✓
Windows Vista (32-bit)	✓	✓	✓
Windows XP Windows Vista (64-bit)	✓		
Servers			
Windows 2000 Server Advanced Server Small Business Server with Service Pack 3 or later	✓	✓	
Windows 2003 Standard Server Enterprise Server Web Edition Small Business Server	✓	✓	

If you upgrade the operating system on a client computer (for example, from Windows 2000 to Windows XP) and you want to leave your existing files and programs intact during the upgrade, you must first uninstall Enforced Client, then reinstall it after the upgrade is complete.

Support for some operating systems is ending. After support ends, client computers running those operating systems will no longer be protected against new threats. See *Operating system support ending* for more information.

Operating system support ending

Support for these Windows operating systems is ending with Enforced Client version 4.5.

- Windows 95
- Windows 98
- Windows ME
- Windows NT 4.x

For more information about support for these operating systems, visit http://www.mcafee.com/us/enterprise/support/customer_service/end_life.html, then look for Enforced Client under **Managed Services Matrix**.

See *Notifying users when support ends* for information about notifying users when support for their operating system is ending.

Notifying users when support ends

By default, Enforced Client displays notifications on client computers to remind users that support is ending for their operating system.

- When upgrades to product components, such as the scanning engine, are scheduled to end or will end within 30 days.
- When updates to detection definition (DAT) files have ended or will end within 30 days.

A policy option determines whether support notifications are displayed.

> Notifications are not displayed for computers running Windows 95 because support for that operating system has already ended.

To enable or disable notifications:

1 On the **Groups + Policies** page, click **Add Policy** (or click **Edit** to modify an existing policy).

2 Click the **Advanced Settings** tab.

3 Select or deselect **Display support notifications on client computers**, then click **Save**.

RAM

	Minimum virus and spyware protection	Minimum firewall protection*	Recommended
Windows 2000	64 MB	256 MB	256 MB
Windows XP	128 MB	256 MB	256 MB
Windows 2003	256 MB	512 MB	512 MB
Windows Vista	512 MB	512 MB	1 GB
Servers	256 MB	512 MB	512 MB
* Use the value listed for the firewall protection service whether installing that service alone or with other protection services.			

Email security service

Enforced Client Advanced includes the additional email security service. To set up and run this service, you need:

- A dedicated email server, either in-house or hosted by an ISP.
- A company email domain, such as *yourdomain*.com, with a static IP address.

Email server security application

Enforced Client Advanced gives you the option to install the SonicWALL GroupShield email server security application.

Minimum requirements for Microsoft Exchange Server 2003:

- Intel Pentium or compatible 133MHz processor.
- 128 MB of RAM (512 MB recommended).
- 740 MB free disk space.
- One of these operating systems:
  - Microsoft Windows 2000 Server with Service Pack 4.
  - Microsoft Windows 2000 Advanced Server with Service Pack 4.
  - Microsoft Windows Server 2003 Standard Edition (32-bit).
  - Microsoft Windows Server 2003 Enterprise Edition (32-bit).

Minimum requirements for Microsoft Exchange Server 2000 with Service Pack 3:

- Intel Pentium or compatible 133MHz processor.
- 128 MB of RAM (256 MB recommended).
- 740 MB of free disk space.
- Microsoft Windows 2000 Server with Service Pack 4.

Terminal servers

Enforced Client supports terminal servers and the Windows fast user switching feature in most scenarios, with these limitations:

- Enforced Client must be installed on the server by someone with local administrator privileges.
- When an installation or update occurs on a terminal server, one session is designated as the primary update session (see *Update computers where no user is logged on* on page 55 for restrictions that apply to automatic updates).
- For all user sessions, the Enforced Client icon is removed from the system tray during the installation or update. The icon is restarted only for the user logged on to the primary update session. All user sessions are protected, and other users can manually redisplay their icons (see *Removing and displaying the icon* on page 52 for more information).
- Detection notifications are not displayed on the desktop of all computer users if the fast user switching feature is enabled.
- If you use an authenticating proxy server, disable the policy option **Update client computers where users are not logged in** on the SecurityCenter’s **Advanced Settings** tab (see *Set advanced virus protection options* on page 97).

Before you install

Complete these procedures on each computer to prepare for installing the client software:

- *Uninstall existing virus protection software*
- *Uninstall existing firewall software*
- *Configure your browser*
- *Install the standalone installation agent* — Required if users will install protection services on client computers where they do not have administrator rights.

Uninstall existing virus protection software

Other virus protection software might conflict with the advanced features of Enforced Client virus protection. When multiple virus scanning engines try to access the same files on your computer, they interfere with each other.

Uninstall all virus protection software before installing the Enforced Client virus and spyware protection service. If you are notified of existing virus protection software on a computer during installation, follow these instructions to remove it.

To uninstall existing virus protection software:

1. In the Windows **Control Panel**, open **Add/Remove Programs**.
2. In the list of programs, locate any virus protection software (including Enforced Client), then click **Remove**.

The following lists include products that Enforced Client detects. In some cases, Enforced Client uninstalls the software automatically; in other cases, it prompts you to uninstall it.

If you have virus protection software that does not appear on these lists, you must manually uninstall it before installing Enforced Client.

SonicWALL products automatically detected

SonicWALL Enterprise
- Anti-Spyware Enterprise (all editions)
- ePO agent
- Managed VirusScan (previous editions)
- Enforced Client Enterprise
- VirusScan Enterprise 8.5*i* / 8.0*i* / 7.1 / 7.0
- VirusScan 4.5.1
- VirusScan 4.0.3

SonicWALL Retail
- Internet Security Suite
- SonicWALL SecurityCenter
- Enforced Client for Home Users
- VirusScan Retail 8.0
- VirusScan Professional Edition 7.0 / 6.0
- VirusScan Home Edition 7.0 / 6.0
- VirusScan Retail 5.1.X
- VirusScan Retail 5.0 for 9x
- VirusScan Retail-OEM 4.0.3 for 9x

Non-SonicWALL products automatically detected

Computer Associates
- eTrust AntiVirus 7.1
- eTrust AntiVirus 7.0
- Inoculate IT 3.5.1
- Inoculate IT 4.5.3
- Pest Patrol for spyware (compatibility)

Finjan
- SurfinGuard

F-Secure
- AntiVirus 5.52
- Antivirus 2004 (home)
- Antivirus Client Security (uninstalls AV only)
- F-Secure Internet Security 2006

Kaspersky
- AntiVirus Personal
- AntiVirus Personal Pro
- Antivirus Business Optimal

Microsoft
- Live OneCare

Panda
- BusinesSecure 2006 (with TruPrevent) (ClientShield is the AV portion)
- ClientShield (with TruPrevent)
- EnterpriSecure 2006 (with TruPrevent)
- FileSecure
- Platinum Internet Security
- Titanium Antivirus 2006/2004/2003
- WebAdmin Antivirus

Sophos
- Sophos Antivirus

Symantec
- NAV 2006/2004 Internet Security Edition (uninstalls AV only)
- NAV 2006/2004 Professional (uninstalls AV only)
- NAV 2002
- NAV 8.0
- NAV 7.6 for Windows for 9x
- NAV 7.6 for Windows for NT
- NAV 7.5.1/7.5
- NAV Central Quarantine
- Norton Internet Security 2006/2004 home & small office editions (uninstalls AV only)
- Norton Internet Security 2006/2004 Professional home & small office editions (uninstalls AV only)
- Norton Mobile Update Agent
- Norton Mobile Update Distribution Console
- Norton Rescue Disk
- Norton Systemworks 2006/2004 (uninstalls AV only)
- Symantec Antivirus 10.3, 10.1, 9.x, 8.1 (all editions)

Trend
- Micro HouseCall (On-Line)
- OfficeScan
- PC-Cillin Internet Security 2006
- PC-Cillin 2004
- Virusbuster Corporate Edition

Uninstall existing firewall software

Before installing the firewall protection service, we recommend that you uninstall any other firewall programs on your computer. Follow your firewall program's instructions for uninstalling or use the Windows Control Panel.

To uninstall existing firewall software:

1 In the Windows **Control Panel**, open **Add/Remove Programs**.

2 In the list of programs, locate any firewall software (including Enforced Client), then click **Remove**.

> On computers running Windows XP and Windows Vista, the Windows firewall is disabled automatically during installation of Enforced Client.

Configure your browser

Enforced Client requires Microsoft Internet Explorer 5.5 SP2 or later during installation.

- *Internet Explorer*
- *Non-Microsoft browsers*

Internet Explorer

Enforced Client works with the default security settings in Internet Explorer. If you are unsure of your settings, use the following steps to verify and configure them.

version 5.5

1 From the Windows **Control Panel**, open **Internet Options**.

2 On the **Security** tab, select **Internet Zone**.

3 Click **Default Level**.

4 Drag the scrollbar to **Medium**, then click **OK**.

version 6.x

1 From the Windows **Control Panel**, open **Internet Options**.

2 On the **Security** tab, select **Custom Level**.

3 From the **Reset to** menu, select **Medium**, then click **Reset**.

version 7.x

1 From the Windows **Control Panel**, open **Internet Options**.

2 On the **Security** tab, select **Medium-high**.

Non-Microsoft browsers

If on your administrative or client computers you typically use a non-Microsoft browser, such as Mozilla Firefox or Opera, you must install Internet Explorer before installing Enforced Client. After the software is installed, you can continue to use your default Internet browser. You can access the SecurityCenter with Internet Explorer (version 5.5 or later) or Firefox (version 1.5 or later).

Install the standalone installation agent

To allow users without administrator rights to install Enforced Client on client computers using the URL method, you must first load a standalone installation agent on their client computers. You can use a deployment tool to install it from your administrative computer, or you can download it directly onto the client computers. You must have administrator rights on the client computer to install this file.

To deploy the installation agent from your administrative computer:

1 From the SecurityCenter website, click the **Help** tab, select **Utilities**, then click **installation agent** to download the installation agent.

2 Deploy and execute the file on client computers using your customary deployment tools, such as Microsoft Systems Management Server (SMS) installer, Windows NT login scripts, or Tivoli IT Director.

To deploy the installation agent from the client computer:

1 From the SecurityCenter website, click the **Help** tab, select **Utilities**, then click **installation agent** to download the installation agent.

2 When the download is complete, double-click the file.

After the standalone installation agent is installed on a client computer, any user can install Enforced Client client software on that computer.

Installing Enforced Client

Install the client software in any of the following ways:

Standard URL installation
Use the URL you received in your welcome email message to install the software on your computer and access the SecurityCenter website. Then install the software on other computers using a standard or customized URL, or send the URL to users with instructions on how to install.

Advanced Installation options
From an administrative computer, visit the SecurityCenter website and use these methods to remotely install the software on one or more computers simultaneously without user interaction.

Silent installation
Download a program called VSSETUP.EXE, then run it at the command line. This method requires a third-party deployment tool, a login script, or a link to an executable file in an email message.

Push installation
Download the Push Install utility, then deploy the software directly from your service provider's website.

Standard URL installation

URL installation is the most common installation method. Users install the client software individually, by downloading it from a company-specific URL.

- *Requirements*
- *Sending an installation URL to users*
- *Installing on client computers*

Requirements

To use the Internet URL installation method, the client computer's user must have:

- Local administrator rights.

> Administrator rights are not the default. You need to change the Windows configuration or deploy a standalone installation agent (see *Install the standalone installation agent* on page 34 for more information).

- Sufficient rights to install an ActiveX control and a product to the system. (This is not required for computers running Windows Vista.)
- An Internet connection.

Sending an installation URL to users

As the administrator, you can obtain the company-specific installation URL in two ways:

- After signing up for Enforced Client, you receive an email message containing the URL that has been set up for your company. This installation URL installs all the services you have subscribed to into your account's default group in your account's default language. You can copy this URL into an email message to send to the client computer users at your company.
- At any time, you can log on to your SecurityCenter and create a customized URL to send to users. This enables them to install specific services in a designated group and language.

To create a customized installation URL:

1. In your web browser, log on to your SecurityCenter website.
2. From the **Computers** page, click **Add Computer**.
3. Select the group to place the client computers in, the services to install, and a language for the software, then click **Next**.

   A customized URL is displayed, along with simple instructions for users.
4. Click **Select Text and Copy to Clipboard**.
5. In your local email application, open a new message and paste the text you have copied.
6. Revise the instructions if needed, then send the email to the users who need to install the software.

Installing on client computers

Administrators and users follow the same procedure for installing the client software.

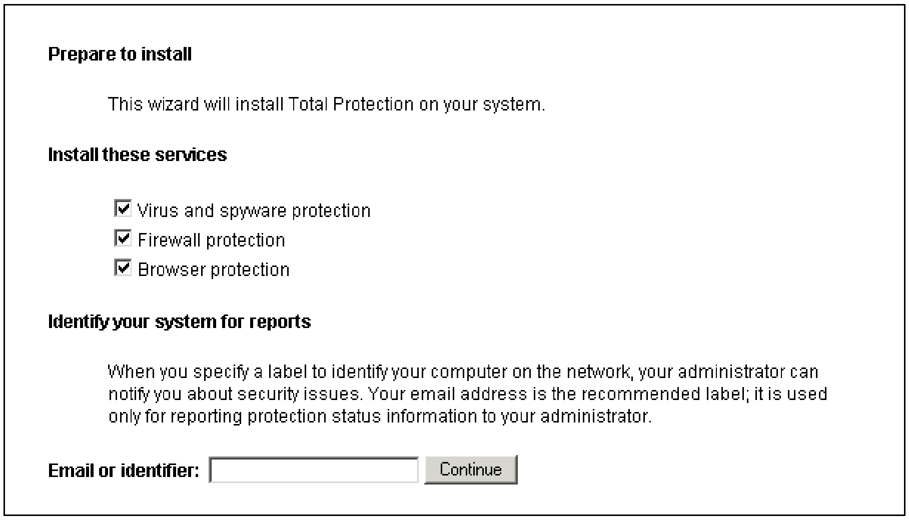
To install using the URL method:

1. On the client computer, open the email message and click the installation URL.

   > The URL installation method can be used only by client computers with a connection to the Internet, and users must have local administrator rights (see *Requirements*.)

   Enforced Client installs automatically.

Figure 2-1 Internet URL installation



Prepare to install

This wizard will install Total Protection on your system.

Install these services

☑ Virus and spyware protection
☑ Firewall protection
☑ Browser protection

Identify your system for reports

When you specify a label to identify your computer on the network, your administrator can notify you about security issues. Your email address is the recommended label; it is used only for reporting protection status information to your administrator.

Email or identifier: ________ Continue

2 Select the services to install if you are prompted to do so, type your email address in the **Email or identifier** field, and click **Continue**.

What is the email address used for?
The information entered here identifies the computer where the installation is taking place. The SecurityCenter uses it to identify that computer in reports. If reports indicate a problem with a computer, you can use the email address to notify the user. If the user does not enter an email address, it is important to know how to contact the user when security issues arise.

3 When you are prompted to do so, click **Install**.

4 In the **File Download** dialog box, click **Run**.

For installation, Enforced Client uses a cookie created at this time. The cookie expires after 24 hours. If you save the installation file and then try to install it after 24 hours have passed, or delete the cookie, you are prompted to begin the installation process again.

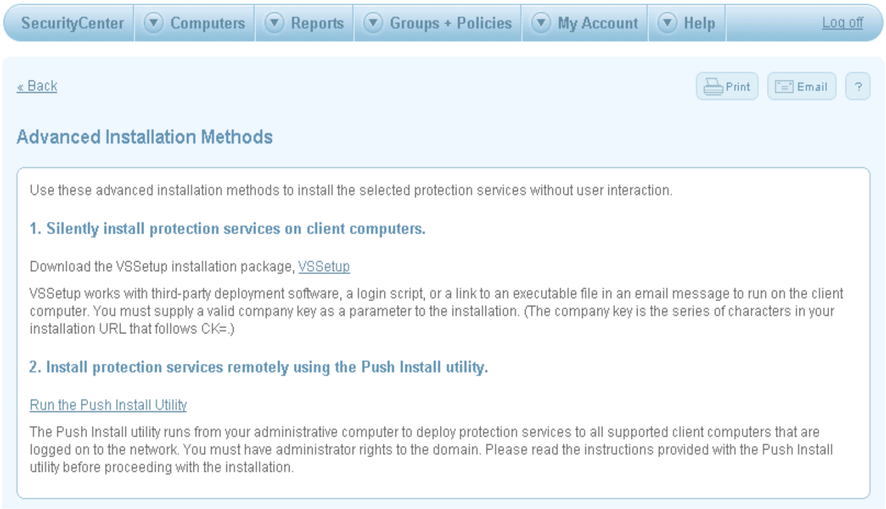
5 On computers running Windows Vista, if the **User Account Control** dialog box appears, click **Continue**.

6 Select **Restart** when prompted to reboot after installing the firewall protection service.

Advanced installation methods

Administrators can use the advanced installation methods to install the Enforced Client client software without user interaction.

Figure 2-2 Advanced installation methods



Advanced Installation Methods

Use these advanced installation methods to install the selected protection services without user interaction.

1. Silently install protection services on client computers.

Download the VSSetup installation package, VSSetup

VSSetup works with third-party deployment software, a login script, or a link to an executable file in an email message to run on the client computer. You must supply a valid company key as a parameter to the installation. (The company key is the series of characters in your installation URL that follows CK=.)

2. Install protection services remotely using the Push Install utility.

Run the Push Install Utility

The Push Install utility runs from your administrative computer to deploy protection services to all supported client computers that are logged on to the network. You must have administrator rights to the domain. Please read the instructions provided with the Push Install utility before proceeding with the installation.

Two advanced installation methods are available: *Silent installation* and *Push installation*. Select the one that works best for your network.

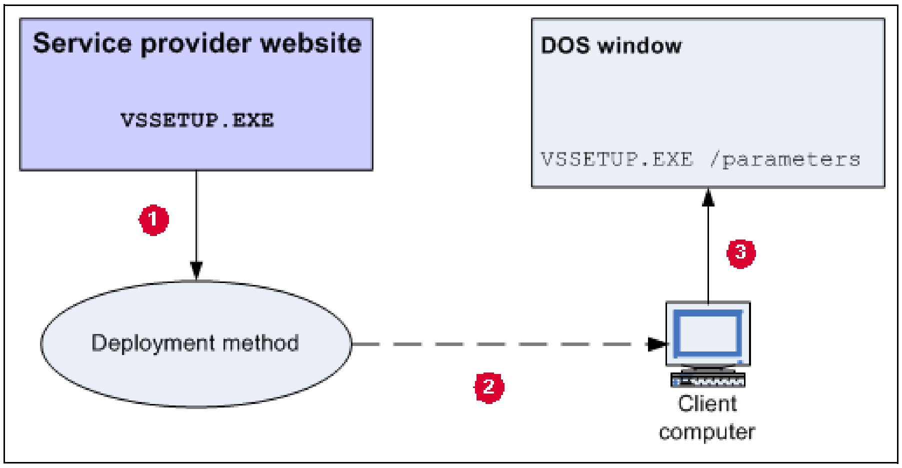
	Advanced installation method	
The administrator...	**Silent**	**Push**
	Client computer	Administrative computer
Downloads this file	VSSETUP.EXE	Push Install utility
Installs the client software on	One computer	One or more computers
Installs remotely	No	Yes
Can designate relay servers (optional)	Yes	Yes (separately from client computers)

Some network configurations require additional information to ensure that client software operates correctly (see *If you use a corporate firewall or proxy server* on page 45).

Silent installation

VSSETUP is an executable file for installing Enforced Client on a client computer with no user interaction. This installation method is not network-specific and installs the software on any Windows operating system.

Figure 2-3 How silent installation works



To use silent installation:

1 Download VSSETUP from the SecurityCenter.

2 Deploy to each computer where you want to install the client software.

3 On the computer, open a DOS window and run the VSSETUP command using the appropriate parameters.

- *Requirements*
- *Installation*

Requirements

To use the silent installation method:

- You must have a method for installing executable files on your network computers. For example:
  - A third-party deployment tool, such as Novell NAL, ZenWorks, Microsoft Systems Management Server (SMS) installer, or Tivoli IT Director.
  - A login script.
  - A link to an executable file in an email message.
  - A portable medium such as a CD.
- You should run this program using an account with sufficient rights to install the product. Typically local administrator rights are required, and some methods require remote execution rights.

- You must know your company key (the series of characters in the installation URL after the characters `CK=`).

Installation

To install Enforced Client silently:

1. From your web browser, log on to your SecurityCenter.
2. On the **Computers** page, click **Add Computer**.
3. Select the group to place the user's computer in, the services to install, and a language for the software, then click **Next**.
4. Under **Additional Installation Options**, click **Display advanced installation methods**.
5. Under method 1, click **VSSETUP** to save the VSSETUP.EXE file to your hard drive.
6. Deploy the program to each client computer using your customary deployment tool, such as those listed under *Requirements*.
7. On a client computer, open a DOS window and run the following command:

   ```
   VSSETUP.EXE /CK=<your company key> /<parameters>
   ```

   As shown in this example, you must include your company key (`CK`) as a parameter. See *VSSETUP parameters* for a list of optional parameters you can add to your command line.

   #### What is my company key?

   Your company key is included in the URL that you received when you subscribed to Enforced Client. It is the hexadecimal value that follows the characters `CK=` at the end of the URL.

8. Reboot the client computer after installing the firewall protection service.

VSSETUP parameters

For a silent installation, use this command line and any of the following parameters (which are not case-sensitive):

```
VSSETUP.EXE /CK=<your company key> /<parameters>
```

`/CK=XYZ`	Required. Launches Setup using the company key.
`/Email=x@y.com`	Identifies the user's email address in administrative reports. **Note:** Despite its name, the email variable does not need to be an email address. Do not use a string containing non-standard characters, because they might display incorrectly in reports.
`/Uninstall`	Uninstalls Enforced Client.
`/SetRelayServerEnable=1`	Sets a computer with a connection to the Internet as a relay server. If the computer is not used as a relay server, set to `0`.
`/Reinstall`	Reinstalls Enforced Client, leaving the previous values for company key, email address, and machine ID intact.
`/Groupid=[group number]`	Places the computer into any group you have created. You can find the number associated with a group by generating a customized URL (see *To create a customized installation URL:* on page 36). **Note:** If you designate a group that does not exist, users are placed in the **Default** group.

`/P=b`
`/P=f`
`/P=v`
`/P=bf`
`/P=bv`
`/P=fv`
`/P=vfb`
	Selects the protection service(s) to install:
	■ `b` — browser protection service.
	■ `f` — firewall protection service.
	■ `v` — virus and spyware protection service.
	Note: If you omit the `/P` parameter, only the virus and spyware protection service is installed.

Examples

- `VSSETUP.EXE /vfb /CK=abcd /Email=joe@example.com /Groupid=3`

  The virus and spyware, firewall, and browser protection services are installed. The company key is `abcd`, the user's email address is `joe@example.com` for reporting purposes, and this user is placed in an existing group represented by the number `3`. Generate a customized URL, as described in *Sending an installation URL to users* on page 36, to find the correct numeric groupid.

- `VSSETUP.EXE /CK=abcd /Email=joe@example.com`

  Only the virus and spyware protection service is installed. The company key is `abcd` and the user's email address is `joe@example.com` for reporting purposes.

Push installation

Push means deploying remotely to one or more computers in a network. This method uses the Push Install utility to deploy the client software directly from your service provider's website to client computers on your network. Push installation does not require third-party deployment software or interaction with users.

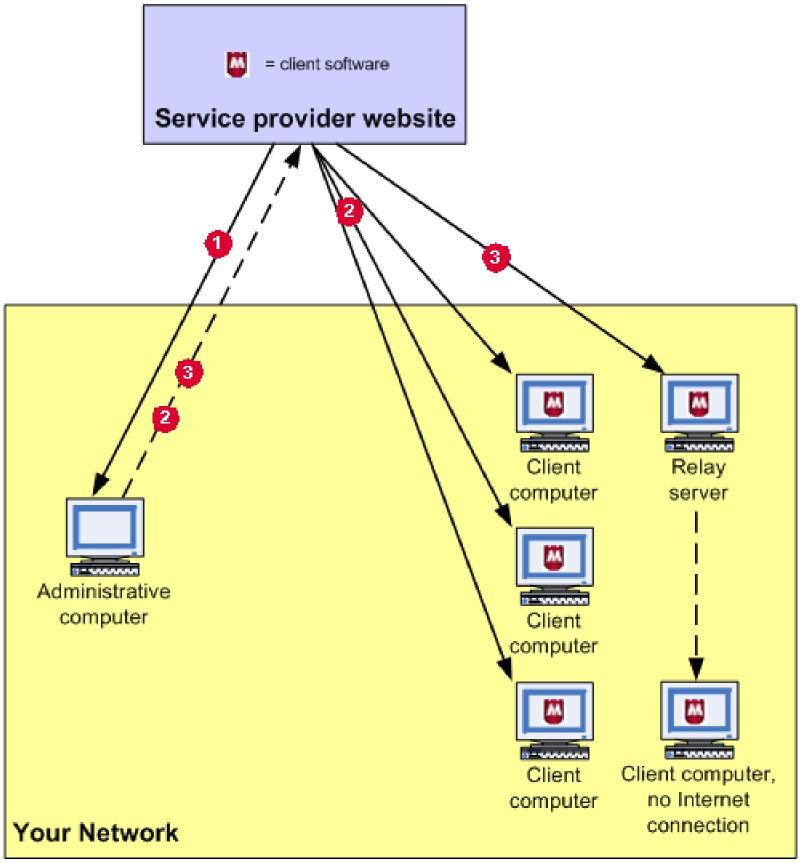
To perform a push installation:

- Designate an *administrative computer*, where you will download the Push Install utility and initiate the push.
- Select the *target computers*, which are client computers on your network that will receive the software.

The Push Install utility is essentially an ActiveX control that runs on an administrative computer. It installs client software on all target computers that are online when the push takes place. Use push installation to install client software on new network computers or to install additional protection services on computers with existing client software.

The Push Install utility allows you to specify one or more network computers with an Internet connection as relay servers. You must do so in a separate push operation, because you cannot push to relay servers and non-relay servers at the same time. See *Enabling relay servers* on page 46 for more information.

Figure 2-4 How push installation works



To perform a push installation:

1. Download the Push Install utility from the SecurityCenter.
2. Initiate a push to one or more client computers.
3. Optional. Initiate a push to one or more relay servers.

- *Requirements*
- *Installation*

ℹ Online help for the Push Install utility is available by clicking the **help** link in any dialog box during installation.

Requirements

To use the push installation method:

- The administrative computer must be running the Windows 2000, Windows XP Professional, or Windows Vista operating system.

ℹ Push installation is not supported on Microsoft Windows XP Home Edition because Windows XP Home Edition cannot log on to an Active Directory domain.

- The administrative computer must be running Internet Explorer 5.5 SP2 or later, with ActiveX enabled.
- At the administrative computer, you must be logged on with domain administrator privileges for the domain being installed.
- Administrative computers running the Windows firewall and Windows XP Professional or Windows Vista must add File and Print Sharing to the firewall's Exceptions list. For instructions, see the *Push Install Help*, available by clicking the **help** link in any dialog box when you run the Push Install utility.
- All target computers must be logged on to the same Windows domain as the administrator.

Considerations for scheduling push installations

When scheduling push installations:

- **Consider other network tasks.** Pushing to a large number of computers simultaneously can produce a high volume of network traffic, so schedule push installations for times when they will not affect other network tasks.
- **Make sure the target computers are turned on.** The Push Install utility installs client software on target computers that are online when the push takes place.
- **Make sure users are not using the target computers.** Restarting a client computer while a push installation is in progress can cause the computer to become unstable, so schedule push installations for times when users will not be turning off or restarting their computers.

Installation

Back up any vital data on your critical servers before pushing software to them.

To install Enforced Client using the Push Install utility:

1 On the administrative computer, open the web browser, log on to the SecurityCenter, then click **Install Protection**.

2 Select the type of computers to install software on, then click **Next**.

3 If you are installing to new computers (where no Enforced Client services are currently installed), select the group where you want to assign the computers.

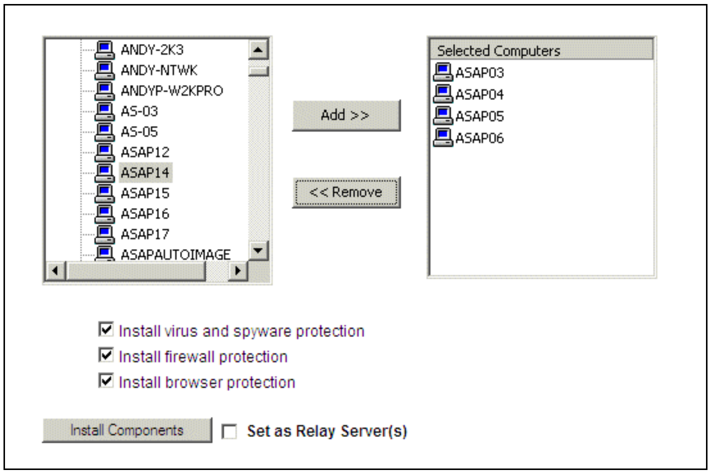
4 Select the services to install and their language, then click **Next**.

5 Under **Additional Installation Options**, click **Display advanced installation methods**.

6 Under **method 2**, click **Run Push Install utility**.

A window displays a list of visible computers in your domain.

Figure 2-5 Select target computers and protection services



☑ Install virus and spyware protection
☑ Install firewall protection
☑ Install browser protection
□ Set as Relay Server(s)

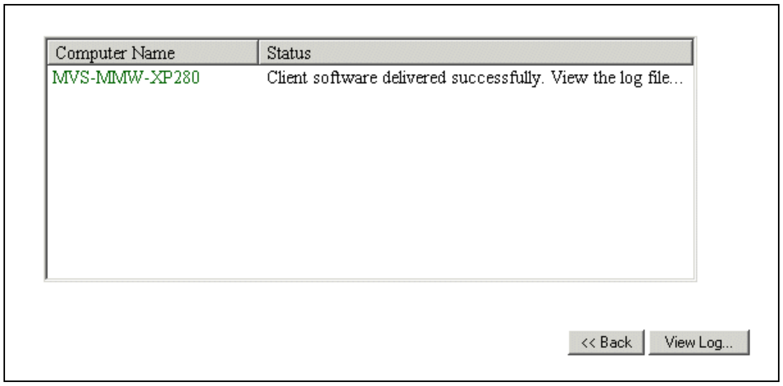
7 From the left pane, select the target computer(s), then click **Add**.

8 Optionally, select **Set as Relay Server(s)** to configure the selected computers as relay servers, which can distribute updates to other computers on the network. See *Enabling relay servers* on page 46 for details.

9 Select the Enforced Client service(s) to install, then click **Install Components**.

After installation is complete, a status for each target computer is displayed.

Figure 2-6 Status for target computers



Computer Name	Status
MVS-MMW-XP280	Client software delivered successfully. View the log file...

10 Click **View Log** to open a log file in Microsoft Notepad that shows the status of the current session, then save the file.

The dialog box indicates only whether the files were pushed to the target computers. It is important to review the log file to verify that the files were installed and updated successfully. You can also use the log file for troubleshooting. (The contents of the log file are deleted when you close the Push Install utility or perform another push.)

11 Optionally, click **Back** to return to the previous screen and push to more computers.

12 If you have installed the firewall protection service, restart the client computers.

If you use a corporate firewall or proxy server

Enforced Client downloads components directly from SonicWALL servers to client computers. If you are behind a corporate firewall, or are connected to the Internet by a proxy server, you might need to provide additional information for your service to work properly.

- Authentication support is limited to anonymous authentication or Windows domain challenge/response authentication. Basic authentication is not supported.
- Advanced installation methods and automatic updating do not support a CHAP or NTLM proxy.
- If you use an authenticating proxy server, disable the policy option **Update client computers where users are not logged in** on the SecurityCenter's **Advanced Settings** tab (see *Set advanced virus protection options* on page 97).

Contact product support if you have proxy questions while installing or updating Enforced Client.

Enabling relay servers

If any computers on your network do not have a direct connection to the Internet, the Internet Independent Updating (IIU) feature allows them to receive software updates from another local computer. In that case, you must specify at least one computer in your LAN as a relay server.

If all the computers on your network connect to the Internet, you do not need to set up any relay servers. However, you might want to specify relay servers to reduce Internet traffic on your LAN. See *Internet Independent Updating (IIU)* on page 15 for information on using relay servers.

You can specify one or more computers as a relay server in two ways:

- *Using the Push Install utility*
- *Using VSSETUP*

Using the Push Install utility

During the push installation procedure, select **Set as Relay Server(s)** before clicking **Install Enforced Client** (see step 10 under *Installation* on page 44).

You must perform a separate push operation to push files to relay servers and non-relay servers, because you cannot push to both at the same time.

Using VSSETUP

During a silent installation, or at any time after Enforced Client has been installed on a computer, you can run the `vssetup` command with the variable that specifies a computer as a relay server. The `vssetup` syntax differs, depending on whether this is an initial installation or an existing installation. (See *Silent installation* on page 39 for more information.)

Initial installation

During an installation, `vssetup` uses the following syntax to specify a computer as a relay server:

```
VSSETUP.EXE /RelayServer=1
```

If you do not specify the computer as a relay server during the installation process, the default is **0** (off), and the computer is not a relay server.

Changing an existing configuration

You can edit an existing installation using `vssetup` with the **SetRelayServerEnable** parameter.

- Specify a computer as a relay server:

  ```
  VSSETUP.EXE /SetRelayServerEnable=1
  ```

- Change a current relay server computer so that it is no longer a relay server:

  ```
  VSSETUP.EXE /SetRelayServerEnable=0
  ```

Completing the installation

After installing Enforced Client, perform these procedures on each client computer to ensure that the software is working correctly and the computer is protected. (Users can read instructions for performing these procedures in the online *Installation Instructions* or *User Help*.)

- *Test virus protection*
- *Scan the client computer*
- *Scan the email Inbox*
- *Set up the default firewall*

Test virus protection

Test the virus-detection feature of the virus and spyware protection service at any time by downloading the EICAR Standard AntiVirus Test File at the client computer. Although it is designed to be detected as a virus, the EICAR test file is not a virus.

To run a test:

1 Download the EICAR file from the following location:

http://www.eicar.org/download/eicar.com

If installed properly, the virus and spyware protection service interrupts the download and displays a threat detection dialog box.

2 Click **OK**, then select **Cancel**.

> If installed incorrectly, the virus and spyware protection service **does not** detect the virus or interrupt the download process. In this case, use Windows Explorer to delete the EICAR test file from the client computer. Then reinstall Enforced Client and test the new installation.

Scan the client computer

After installing the virus and spyware protection service for the first time, we recommend running an on-demand scan of all client computer drives before proceeding. This checks for and cleans or deletes existing threats in files. In the future, files are scanned when they are accessed, downloaded, or saved.

To scan your computer:

1 Click M in the system tray.

2 Select **Scan Tasks**, then select **Scan My Computer**.

Scan the email Inbox

After installing the virus and spyware protection service for the first time, we recommend running an on-demand email scan before proceeding. This checks for threats in email already in the client's Microsoft Outlook Inbox. Future emails are scanned before they are placed in the Inbox.

To run an on-demand email scan:

- From the **Tools** menu in Outlook, select **Scan for Threats**.

  The **On-Demand Email Scan** dialog box appears when the scan starts. You can stop, pause, and restart the scan. You can also check the results of the scan.

Set up the default firewall

To ensure complete protection on computers running Windows XP or Windows Vista, the firewall protection service automatically disables the Windows firewall and configures itself as the default firewall. This enables it to monitor communications for Internet applications and track events for reporting purposes, even if the Windows firewall is also running.

We recommend that you do not re-enable the Windows firewall while the Enforced Client firewall is enabled.

> If both firewalls are enabled, the Enforced Client firewall lists only a subset of the blocked IP addresses in its **Inbound Events Blocked by the Firewall** report. The Windows firewall blocks some of these addresses; however, it does not report them because event logging is disabled in the Windows firewall by default. If both firewalls are enabled, you must enable Windows firewall logging to view a list of all blocked IP addresses. The default Windows firewall log is C:\Windows\pfirewall.log. Enabling both firewalls also results in duplicate status and alert messaging.

What should I do after installing?

After installing Enforced Client, client computers are protected immediately and no further setup is required for the virus and spyware protection service, the firewall protection service, or the browser protection service. You will receive regular status emails with details about your account. (If you purchased Enforced Client from a SonicWALL partner who manages security for you, the partner usually receives these emails.)

> If you purchased Enforced Client Advanced, refer to emails and other materials from your service provider for instructions on installing and configuring the additional services. See *Chapter 7, Using the Email Security Service* for information about activating and setting up the email security service.

You might want to take advantage of additional features to more easily manage your account and customize a security strategy for your specific needs:

- *Setting up your account* on page 62.
- *Viewing your security services at-a-glance* on page 63.
- *Managing your computers* on page 65.
- *Creating groups to manage your site* on page 71.
- *Setting up policies* on page 75.
- *Viewing reports* on page 78.

For guidelines on administering an effective security strategy:

- For virus and spyware protection, see *Manage your protection strategy with best practices* on page 108.
- For firewall protection, see *Managing suspicious activity with best practices* on page 125.

Users configure most browser protection settings on their computers. For descriptions of these features and recommended settings, see *Configuring browser protection on the client computer* on page 131.

3 Using Enforced Client

Enforced Client consists of two main components for managing security:

- **The client software:** Software installed on each client computer. The client software runs in the background to download updates and protect the computer from threats. It also provides users access to the basic functions of their SonicWALL protection services, such as scanning files, folders, and email messages.
- **The SonicWALL SecurityCenter:** A website for administrative functions, where you can centrally manage the protection services for your account. Most administrative tasks are performed from the SecurityCenter.

Enforced Client is designed for hands-off management. After installing the software on client computers, you receive regular emails that summarize the security status of all client computers on your account, and notify you of actions required to address vulnerabilities. Status emails contain a link to your SecurityCenter website, where you can view detailed reports and instructions for resolving problems.

In small organizations, status emails might be all that is needed to assure you that your computers are safe. If you manage a large account or want more proactive, hands-on involvement, you can take advantage of the tools available on the SecurityCenter.

Using the client software

After installing Enforced Client, the software runs on each client computer to immediately protect it from threats such as viruses and intrusions.

Typically, users have little interaction with the client software unless they want to manually scan for threats. User tasks are documented in the online *User Help* on client computers.

As an administrator, you can most easily use the SecurityCenter website to configure settings and monitor detections for client computers. Occasionally, you might work directly on a client computer.

Users and administrators access the client software's features through these components on a client computer:

- *Enforced Client system tray icon*
- *Client menu*
- *Administrative menu and tasks*

Enforced Client system tray icon

When Enforced Client is running on a client computer, the Enforced Client icon M appears in the system tray and indicates the status of the services.

This icon...	....indicates:
M⬇	An update is in progress. Do not interrupt the Internet or LAN connection, or log off the computer.
M⊘	■ The last update failed to complete. Check the Internet or LAN connection, then double-click the icon to perform a manual update. ■ On-access scanning is disabled (see *Disabling on-access scanning* on page 110). ■ The firewall protection service is disabled (see *Enable firewall protection* on page 114). ■ The service subscription is expired (see *Managing your subscriptions* on page 83).

See *Removing and displaying the icon.*

Removing and displaying the icon

When you remove the Enforced Client icon, the protection services continue to protect the client computer by blocking detections, but do not display any user prompts.

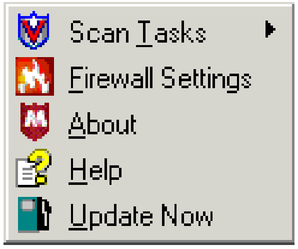
To remove the icon from the system tray:

1 On the client computer, hold down the **Ctrl** and **Shift** keys and click M in the system tray.

2 Select **Exit**.

To display the icon in the system tray:
On the client computer, select **Start | Programs | SonicWALL | Enforced Client Anti-Virus and Anti-Spyware | SonicWALL Enforced Client**.

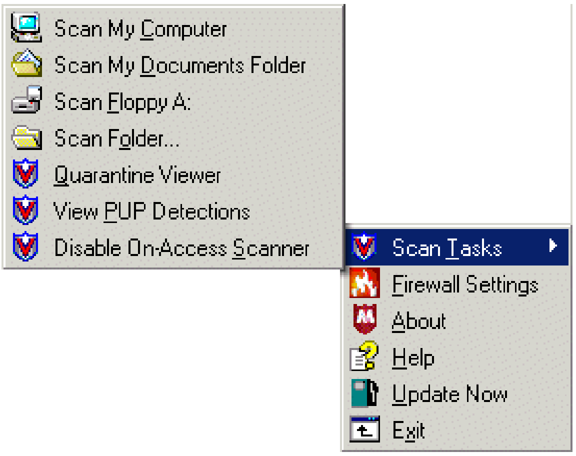
Client menu



Click in the system tray to access these options:

- Scan Tasks: Displays a submenu for accessing features of the virus and spyware protection service.
- Firewall Settings: Displays the current status, mode, and connection type for the firewall protection service. If the policy allows users to configure firewall protection, a dialog box for changing settings appears instead.
- About: Displays information about the software, including the current version of the detection definition (DAT) file.
- Help: Displays the built-in *User Help* file, which contains basic information about using product features.
- Update Now: Checks whether a new update is available; if so, the update downloads automatically.

Administrative menu and tasks



Access administrative features by holding down both the **Ctrl** and **Shift** keys when clicking in the system tray:

- Exit: Removes the Enforced Client icon from the system tray. See *Removing and displaying the icon* on page 52 for more information.
- Scan Tasks | Disable On-Access Scanner: Turns off the automatic on-access scanner. To re-enable the scanner, reopen the administrative menu and select **Enable On-Access Scanner**. See *Disabling on-access scanning* on page 110 for more information.
- Scan Tasks | Quarantine Viewer: Opens the quarantine folder, which contains possible threats detected on the computer. See *Manage quarantined files* on page 109 for more information.

Administrative tasks for client computers are also described in the online *User Help* on the client computer. However, instructions for accessing the administrative menu are provided only in this *Product Guide*.

Updating client computers

Enforced Client automatically updates client computers with new detection definition (DAT) files and other software components.

Users can check for updates manually at any time. In addition, you can configure optional policy settings for updating tasks.

Update support for some operating systems is ending. Once support ends, client computers running those operating systems will no longer be protected against new threats. See *Operating system support ending* on page 28 for more information.

- *Update automatically*
- *Update manually*
- *Update during an outbreak*
- *Update computers where no user is logged on*

Update automatically

The software on each client computer automatically connects to the Internet directly or to a relay server and checks for updated components. Enforced Client checks for updates five minutes after a user logs on and at regular intervals thereafter. For example:

- If a computer is normally connected to the network all the time, it checks for updates at regular intervals throughout the day.
- If a computer normally connects to the network each morning, it checks for new updates five minutes after the user logs on each day, then at regular intervals throughout the day.
- If a computer uses a dial-up connection, the computer checks for new updates five minutes after dialing in, then at regular intervals throughout the day.

By default, computers check for new updates every 12 hours. You can change this interval by configuring a policy setting (see *Select your update frequency* on page 97).

On computers where a CHAP or NTML proxy is set up in Internet Explorer, automatic updates do not work.

Update manually

At times, users might want to check for udpates manually. For example, when a computer appears to be out-of-date in your administrative reports, users might need to update manually as part of the troubleshooting process.

To update manually:
Double-click M in the system tray, or click the icon and select **Update Now**.

Update during an outbreak

When an outbreak is identified by SonicWALL Avert Labs, they issue an *outbreak DAT*, which is a special detection definition (DAT) file marked as **Medium** or **High** importance. It is specially encoded to inform the first computer receiving it to share the update immediately with other client computers on the network.

In rare cases, SonicWALL might send an EXTRA.DAT file with instructions for manually installing it.

For maximum protection, configure your policies to check for an outbreak DAT file every hour (see *Enable optional protection* on page 97). This feature is enabled by default.

Update computers where no user is logged on

In most scenarios, Enforced Client supports terminal servers and the Windows fast user switching feature. When an update occurs, one session is designated as the primary update session. A pseudo user is defined, which enables automatic updates to occur on computers where no user is logged on.

For certain configurations, automatic updates cannot occur. Enforced Client cannot create the pseudo user when:

- The computer is a domain controller.
- Local security policies, including password restrictions, prevent the user's creation.

When the pseudo user cannot be created, automatic updates do not occur. The pseudo user also cannot update if the computer is behind an authenticating proxy server.

For these situations, you can disable the **Update client computers where users are not logged in** policy setting on the SecurityCenter's **Advanced Settings** tab (see *Set advanced virus protection options* on page 97). This prevents automatic update attempts from being reported as errors.

To disable updates for non-logged-on users:

1. On the **Groups + Policies** page, click **Add Policy** (or click **Edit** to modify an existing policy).
2. Click the **Advanced Settings** tab.
3. Deselect **Update client computers where users are not logged in**, then click **Save**.

Using the SecurityCenter

Access the administrative features of Enforced Client from the online SecurityCenter.

The SecurityCenter offers tools for administrators who manage many computers or want to assume a proactive role in overseeing their corporate security strategy.

Use the SecurityCenter to centrally manage the client computers and information for your account. For every category of account management, you can access all the tasks you need to perform from the SecurityCenter:

When you are...	Perform these tasks from the SecurityCenter
	■ *Set up your profile* ■ *Change your SecurityCenter password* ■ *Sign up for email notifications*
Viewing your security services at-a-glance	■ *Install protection services* ■ *View and resolve action items* ■ *View security coverage for your account*
	■ *Search for computers* ■ *Display details for a computer* ■ *View detections for a computer* ■ *View user-approved applications for a computer* ■ *Send email to computers* ■ *Block computers from receiving updates* ■ *Delete computers from your reports* ■ *Move computers into a group*
Creating groups to manage your site	■ *Create or edit a group* ■ *Delete a group*
	■ *Create or edit a group administrator* ■ *Delete a group administrator*
Setting up policies	■ *Create or edit a policy* ■ *Assign a policy to a group* ■ *Restore default policy settings* ■ *Delete a policy*
	■ *View detections* ■ *View unrecognized programs* ■ *View unrecognized Internet applications* ■ *View inbound events blocked by the firewall* ■ *View duplicate computers* ■ *View computer profiles* ■ *View your detection history*
Managing your correspondence	■ *Send email to users* ■ *Update user email addresses* ■ *Update your account's email address* ■ *Add your logo to reports*
	■ *View your service subscriptions* ■ *Update subscription information* ■ *Purchase, add, and renew services* ■ *Request a trial subscription* ■ *Receive subscription notifications*
Getting assistance	■ *View printed and online documents* ■ *Download utilities* ■ *Contact product support*

Getting started

The SecurityCenter website helps you locate information easily.

- *Log on to the SecurityCenter*
- *Access online features and functions*
- *Make the most of your online data*
- *Customize listings and reports*
- *Using the online help*

Log on to the SecurityCenter

You must use your unique user name and password to log on to the SecurityCenter.

1 Obtain the URL for your SecurityCenter in the login credentials email you received from your service provider (see *After you place your order* on page 26).

2 Paste or type the URL into your browser.

3 Type your login credentials:

Email Address	The email address that you used to sign up for Enforced Client.
Password	In most cases, the password that you created when signing up.

4 Click **Log In**.

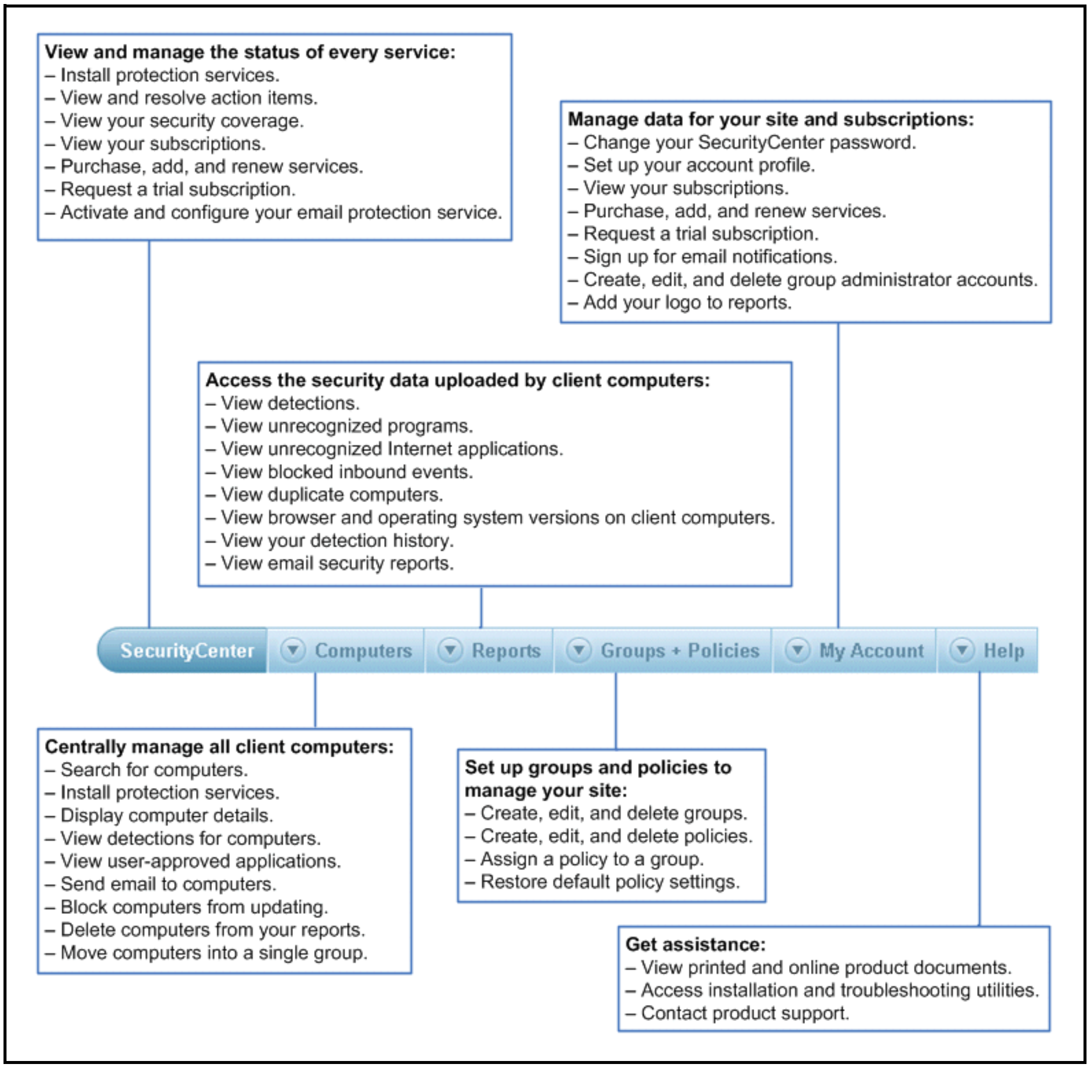
At any time after logging on, you can change your password by updating your user profile (see *Change your SecurityCenter password* on page 62). Your password is case-sensitive and must be a minimum of six characters.

Access online features and functions

Administrative features are divided among six pages:

- **SecurityCenter**
- **Computers**
- **Reports**
- **Groups + Policies**
- **My Account**
- **Help**

Figure 3-1 SecurityCenter tabs



View and manage the status of every service:
– Install protection services.
– View and resolve action items.
– View your security coverage.
– View your subscriptions.
– Purchase, add, and renew services.
– Request a trial subscription.
– Activate and configure your email protection service.

Manage data for your site and subscriptions:
– Change your SecurityCenter password.
– Set up your account profile.
– View your subscriptions.
– Purchase, add, and renew services.
– Request a trial subscription.
– Sign up for email notifications.
– Create, edit, and delete group administrator accounts.
– Add your logo to reports.

Access the security data uploaded by client computers:
– View detections.
– View unrecognized programs.
– View unrecognized Internet applications.
– View blocked inbound events.
– View duplicate computers.
– View browser and operating system versions on client computers.
– View your detection history.
– View email security reports.

Centrally manage all client computers:
– Search for computers.
– Install protection services.
– Display computer details.
– View detections for computers.
– View user-approved applications.
– Send email to computers.
– Block computers from updating.
– Delete computers from your reports.
– Move computers into a single group.

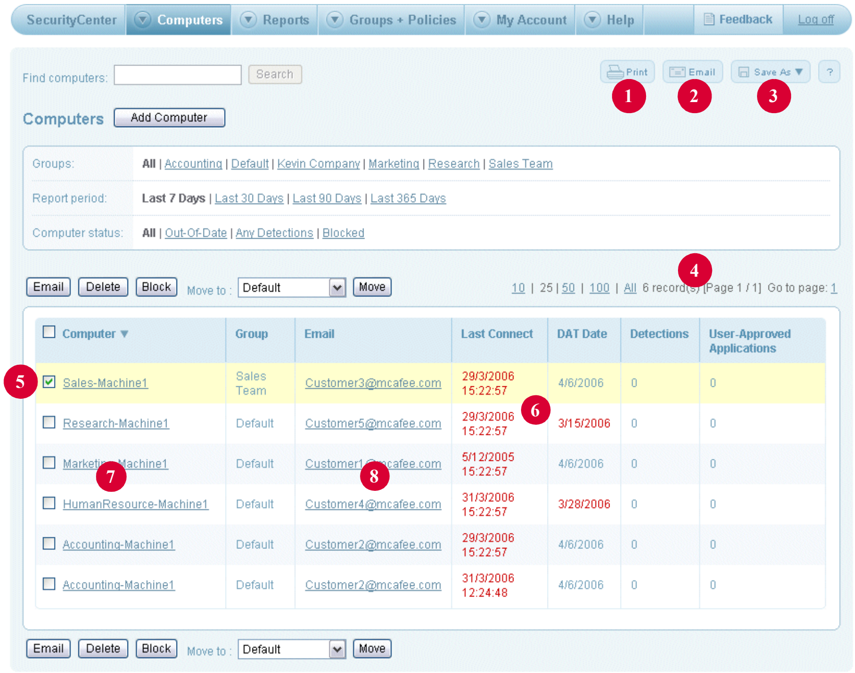
Set up groups and policies to manage your site:
– Create, edit, and delete groups.
– Create, edit, and delete policies.
– Assign a policy to a group.
– Restore default policy settings.

Get assistance:
– View printed and online product documents.
– Access installation and troubleshooting utilities.
– Contact product support.

Make the most of your online data

Each SecurityCenter page includes features for displaying the exact data you need and using it efficiently.

Figure 3-2 Page controls for listings and reports



Find computers:

Computers

Groups: **All** | Accounting | Default | Kevin Company | Marketing | Research | Sales Team

Report period: **Last 7 Days** | Last 30 Days | Last 90 Days | Last 365 Days

Computer status: **All** | Out-Of-Date | Any Detections | Blocked

Move to : Default

10 | 25 | 50 | 100 | All 6 record(s) [Page 1 / 1] Go to page: 1

□ Computer ▼	Group	Email	Last Connect	DAT Date	Detections	User-Approved Applications
☑ Sales-Machine1	Sales Team	Customer3@mcafee.com	29/3/2006 15:22:57	4/6/2006	0	0
□ Research-Machine1	Default	Customer5@mcafee.com	29/3/2006 15:22:57	3/15/2006	0	0
□ Marketing-Machine1	Default	Customer1@mcafee.com	5/12/2005 15:22:57	4/6/2006	0	0
□ HumanResource-Machine1	Default	Customer4@mcafee.com	31/3/2006 15:22:57	3/28/2006	0	0
□ Accounting-Machine1	Default	Customer2@mcafee.com	29/3/2006 15:22:57	4/6/2006	0	0
□ Accounting-Machine1	Default	Customer2@mcafee.com	31/3/2006 12:24:48	4/6/2006	0	0

Move to : Default

	When you want to...	**Do this...**
1	Print the current page.	Click **Print** to open the page in a separate browser window, then select **Send to printer** to open the Windows **Print** dialog box.
2	Send the current page as an email attachment.	Click **Email** to open a blank email message to fill out, then click **Send**. (You must have a local email application installed to use this feature.)
3	Save the current page.	Click **Save As**, then select the file format you want.
4	Navigate in multiple-page listings.	Click the number of entries to display, or click **Go to page** to display a specific page.
5	Select computers to manage.	Select the checkbox for individual computers, or select the checkbox in the heading to select all computers.
6	Check your action items.	Problems that require your attention appear in red. Display instructions for resolving them by clicking the corresponding action item. See *View and resolve action items* on page 64.
7	Display details about a computer.	Click a computer name in a listing.
8	Send email to a computer.	Click an email address in the listing to open a blank, preaddressed message. (You must have a local email application installed to use this feature.)

Customize listings and reports

Select the information to display or the order in which it appears.

To filter information:
At the top of a page, select the information to display (group name, period of time, or type of information).

To sort information in listings:
Click a column heading to sort by that column. Click it again to switch the order in which it is displayed (ascending order ▲ or descending ▼).

Using the online help

Online help is available from any page on the SecurityCenter website by clicking the **help** (**?**) link in the top-right corner of the page. The help window provides information about the page from which it was called. You can access additional information with the table of contents, the index, or the search feature.

Help navigation procedures

To...	**Do this...**
	Click **Back** on the shortcut menu. **Note:** Do not use the **Previous** or **Next** buttons. They are used to navigate through the linear order of pages in the table of contents.
View the table of contents, index, and search from a single help pane	Click (**Show Navigation**).
Page through the help as ordered in the table of contents	Click ∧ ∨ (**Previous** and **Next)**.
View related how-to topics	Click (**Related Links**).
Locate an item alphabetically within the index	Click **Index** in the left pane.
Print a page	Click (**Print**), or click **Print** on the shortcut menu.
Create a bookmark of a page for an HTML browser	Click (**Bookmark**).
Conduct a search	Click **Search** in the navigation pane, enter the word or words to search on, and click **Go**.
Remove highlighted text on a page after a search	Click **Refresh** on the shortcut menu.

Setting up your account

Configure your contact information so that you receive important notices from your service provider.

- *Set up your profile*
- *Change your SecurityCenter password*
- *Sign up for email notifications*

Set up your profile

Your profile contains the information your service provider needs to contact you about your account. Initially, information supplied during your product purchase is placed into your profile. It is important to keep this information up-to-date to prevent a disruption in your services.

We recommend changing the administrator’s email address that you use to access the SecurityCenter (for example, admin@example.com), so that if the current administrator for Enforced Client leaves the company, the administrative email address is easily transferred to the new administrator.

To configure your profile:
On the **My Account** page under **My Profile**, click **Edit**.

Change your SecurityCenter password

We recommend that you change your password when you first visit the SecurityCenter and at regular intervals thereafter.

To change your password:

1. On the **My Account** page under **My Profile**, click **Edit**.
2. Under **Your Contact Information**, type and confirm a new password.

Sign up for email notifications

Sign up for email notifications about your account status, service expiration, and service utilization.

Status emails keep you informed about detections and coverage for your account. It is important to receive status emails at regular intervals that are appropriate for your account, based on the frequency with which you need to review detection information. By default, you receive status emails **Weekly**.

To configure your notification preferences:
On the **My Account** page under **My Preferences**, click **Edit**.

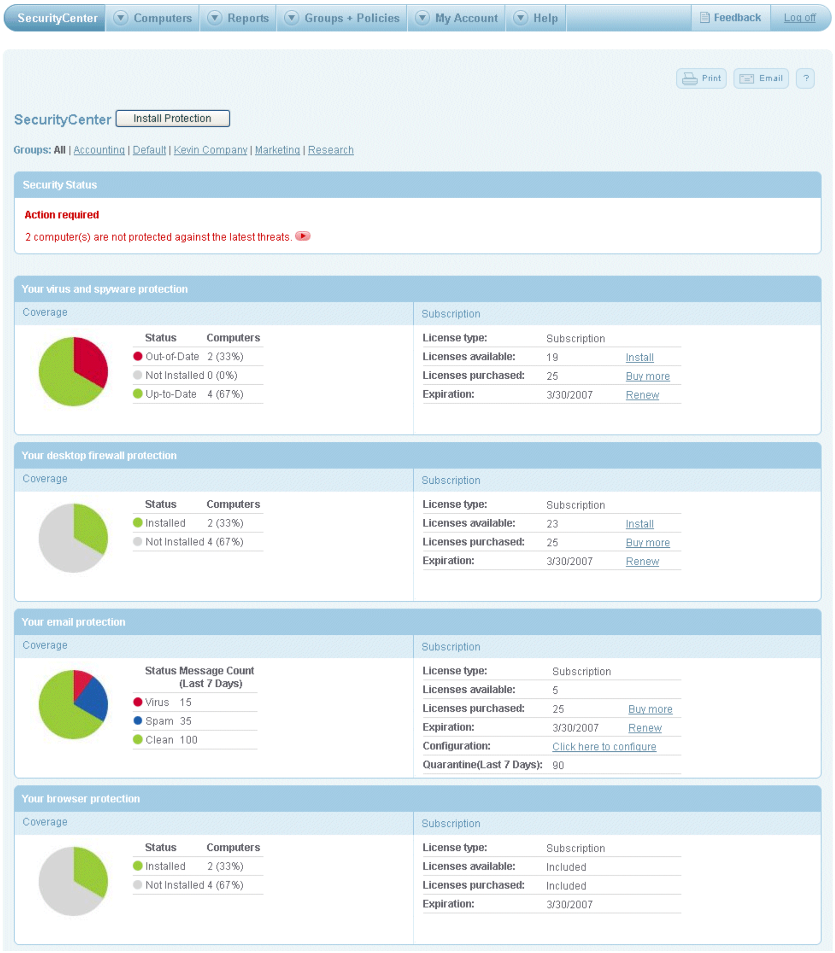
Viewing your security services at-a-glance

The **SecurityCenter** page is your “home” page on the SecurityCenter website — a graphical overview of your coverage with instant access to summary information about the computers and service subscriptions in your account.

Your status emails contain an overview of the information shown on the **SecurityCenter** page and notify you when you need to check your SecurityCenter website.

What can I do from the SecurityCenter page?
The **SecurityCenter** page shows the current status for your account. It’s your “one-stop service center,” where you can install services, check for problems, check your security coverage, or check and update your subscriptions. Access the **SecurityCenter** page at any time by clicking the **SecurityCenter** tab.

Figure 3-3 SecurityCenter page



SecurityCenter

Groups: All | Accounting | Default | Kevin Company | Marketing | Research

Security Status

Action required

2 computer(s) are not protected against the latest threats.

Your virus and spyware protection

Coverage

Status	Computers
● Out-of-Date	2 (33%)
● Not Installed	0 (0%)
● Up-to-Date	4 (67%)

Subscription

License type:	Subscription	
Licenses available:	19	Install
Licenses purchased:	25	Buy more
Expiration:	3/30/2007	Renew

Your desktop firewall protection

Coverage

Status	Computers
● Installed	2 (33%)
● Not Installed	4 (67%)

Subscription

License type:	Subscription	
Licenses available:	23	Install
Licenses purchased:	25	Buy more
Expiration:	3/30/2007	Renew

Your email protection

Coverage

Status	Message Count (Last 7 Days)
● Virus	15
● Spam	35
● Clean	100

Subscription

License type:	Subscription	
Licenses available:	5	
Licenses purchased:	25	Buy more
Expiration:	3/30/2007	Renew
Configuration:	Click here to configure	
Quarantine(Last 7 Days):	90	

Your browser protection

Coverage

Status	Computers
● Installed	2 (33%)
● Not Installed	4 (67%)

Subscription

License type:	Subscription
Licenses available:	Included
Licenses purchased:	Included
Expiration:	3/30/2007

Select the information that appears on this page:

Groups — Display only the computers in a group or display all computers.

From the **SecurityCenter** page, you can:

- *Install protection services*
- *View and resolve action items*
- *View security coverage for your account*
- *Purchase, add, and renew services*
- *Request a trial subscription*

Install protection services

From the SecurityCenter, you can begin the installation process in two ways:

- On the **SecurityCenter** page, click **Install Protection**.

  OR

- On the **Computers** page, click **Add Computer**.

See *Chapter 2, Installing Enforced Client* for more information.

View and resolve action items

Action items are security issues that need your immediate attention and are listed in red on the **SecurityCenter** page or **Computer Details** page. Whenever you see information highlighted in red, check for a corresponding action item on one of those pages. Possible action items are:

Computers are not protected against the latest threat.
One or more computers are not updated with the latest detection definition (DAT) files or software components.

You have no virus and spyware protection installed. Click here to install protection.
Either you have not installed the virus and spyware protection service on client computers or the installation failed. Click the action item to begin installation.

You have no desktop firewall protection installed. Click here to install protection.
Either you have not installed the firewall protection service on client computers or the installation failed. Click the action item to begin installation.

Too many subscriptions in use.
You have installed Enforced Client on more computers than you are licensed for. You need to uninstall from some computers or purchase additional licenses.

Your subscription is about to expire.
Your subscription to one or more protection services will expire soon and needs to be renewed.

Your subscription has expired.
Your subscription to one or more protection services is no longer valid and needs to be renewed.

Your email is being spooled. Please check your email server.
Your organization’s email is being stored temporarily on your service provider’s server because your email server is not accepting email.

Your email security service needs to be activated.
Your subscription to the email security service has not been activated; you need to proceed with the activation process.

To view instructions for resolving an action item:
On the **SecurityCenter** page or the **Computer Details** page, click an action item.

View security coverage for your account

For each protection service, a pie chart shows the status of client computers in your account.

This color...	Indicates...
Red	Out-of-date or unprotected computers.
Green	Up-to-date or protected computers.
Gray	Computers where the protection service is not installed.

To view details about protection coverage for your account:
Click a color to show details about computers in a category.

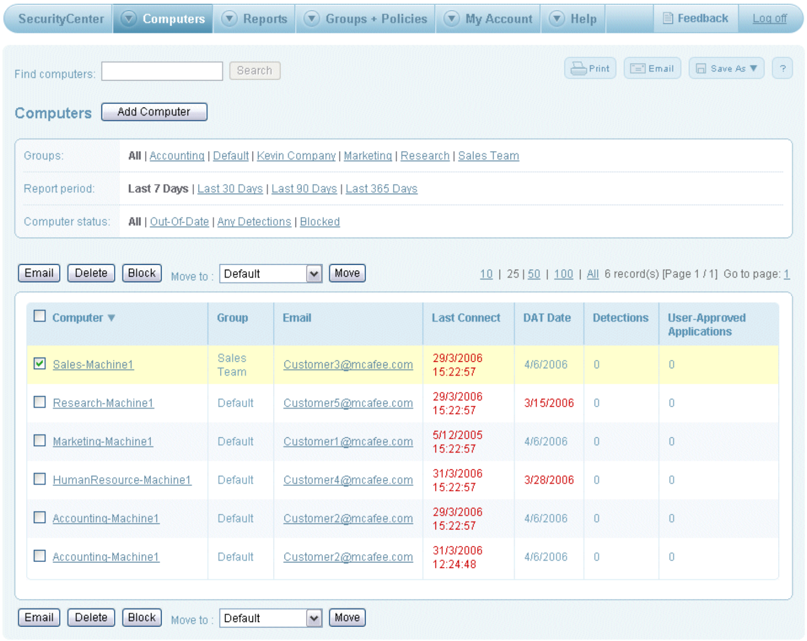
The **Product Coverage** page lists details about the computers with the corresponding level of coverage.

Managing your computers

The SecurityCenter provides a centralized location for working with all the computers in your account. You can instantly view each computer’s group and email address, when it last connected to the network, whether its detection definition (DAT) file is current, the number of detections, and the number of Internet applications approved by its user. You can easily see which computers need your attention, display additional information, and perform necessary management tasks.

Click the **Computers** tab to display the **Computers** page, which lists all the computers in your account or only the computers in a selected group.

Figure 3-4 Computers page



Find computers: [ ] Search

Computers [Add Computer]

Groups:	All | Accounting | Default | Kevin Company | Marketing | Research | Sales Team
Report period:	Last 7 Days | Last 30 Days | Last 90 Days | Last 365 Days
Computer status:	All | Out-Of-Date | Any Detections | Blocked

Email Delete Block Move to : Default Move   10 | 25 | 50 | 100 | All 6 record(s) [Page 1 / 1] Go to page: 1

□ Computer ▼	Group	Email	Last Connect	DAT Date	Detections	User-Approved Applications
☑ Sales-Machine1	Sales Team	Customer3@mcafee.com	29/3/2006 15:22:57	4/6/2006	0	0
□ Research-Machine1	Default	Customer5@mcafee.com	29/3/2006 15:22:57	3/15/2006	0	0
□ Marketing-Machine1	Default	Customer1@mcafee.com	5/12/2005 15:22:57	4/6/2006	0	0
□ HumanResource-Machine1	Default	Customer4@mcafee.com	31/3/2006 15:22:57	3/28/2006	0	0
□ Accounting-Machine1	Default	Customer2@mcafee.com	29/3/2006 15:22:57	4/6/2006	0	0
□ Accounting-Machine1	Default	Customer2@mcafee.com	31/3/2006 12:24:48	4/6/2006	0	0

Email Delete Block Move to : Default Move

Select the information that appears on this page:

Groups — Display only the computers in a group or display all computers.

Report period — Specify the length of time for which to display information.

Computer status — Show all computers, or only out-of-date computers, computers with detections, or computers you have blocked from receiving updates.

For example, you can check whether there are security issues within specific groups. For groups that regularly download files from Internet sites, you might want to monitor the number and type of detections, then modify the security settings to approve safe programs and block communications from sites you distrust.

From the **Computers** page, you can:

- *Search for computers*
- *Install protection services*
- *Display details for a computer*
- *View detections for a computer*
- *View user-approved applications for a computer*
- *Send email to computers*
- *Block computers from receiving updates*
- *Delete computers from your reports*
- *Move computers into a group*

What computer management reports are available?
Use the **Reports** page to access two reports that can assist you with computer management:

- *View duplicate computers*
- *View computer profiles*

Search for computers

Use this feature to find a particular computer in your listings. Site administrators can search the entire account; group administrators can search only the groups their site administrator has assigned to them. (See *Designating group administrators* on page 72 for information on group administrators.)

To search for a computer:
At the top of the **Computers** page, type a full or partial computer name, email address, IP address, or relay server name in the **Find computers** box, then click **Search**.

> The computer search feature does not recognize wildcard characters. You must use only letters or numbers.

Install protection services

From the SecurityCenter, you can begin the installation process in two ways:

- On the **SecurityCenter** page, click **Install Protection**.

  OR

- On the **Computers** page, click **Add Computer**.

See *Chapter 2, Installing Enforced Client* for more information.

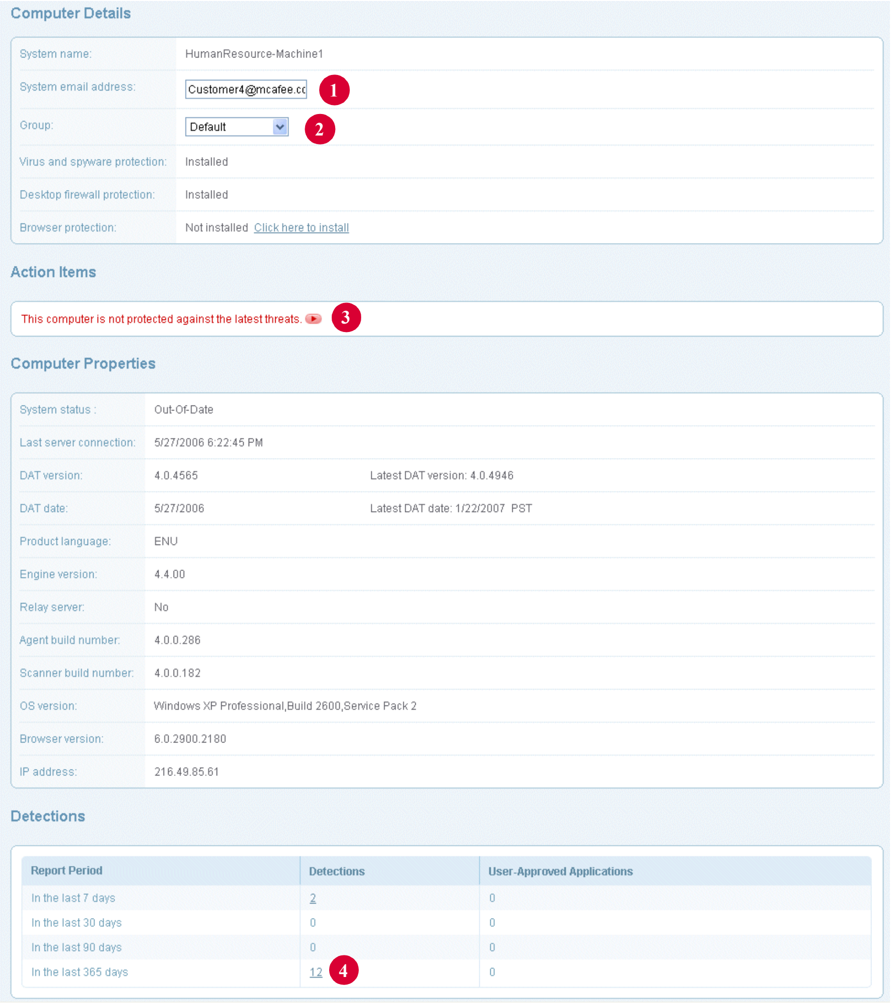
Display details for a computer

Use the **Computer Details** page to check information about a computer and manage its security.

To display details about a computer:
On the **Computers** page, click a computer name.

The **Computer Details** page displays information about the computer, its service components, and its detections.

Figure 3-5 Computer Details page



Computer Details

System name:	HumanResource-Machine1
System email address:	Customer4@mcafee.cc
Group:	Default
Virus and spyware protection:	Installed
Desktop firewall protection:	Installed
Browser protection:	Not installed Click here to install

Action Items

This computer is not protected against the latest threats.

Computer Properties

System status :	Out-Of-Date	
Last server connection:	5/27/2006 6:22:45 PM	
DAT version:	4.0.4565	Latest DAT version: 4.0.4946
DAT date:	5/27/2006	Latest DAT date: 1/22/2007 PST
Product language:	ENU	
Engine version:	4.4.00	
Relay server:	No	
Agent build number:	4.0.0.286	
Scanner build number:	4.0.0.182	
OS version:	Windows XP Professional,Build 2600,Service Pack 2	
Browser version:	6.0.2900.2180	
IP address:	216.49.85.61	

Detections

Report Period	Detections	User-Approved Applications
In the last 7 days	2	0
In the last 30 days	0	0
In the last 90 days	0	0
In the last 365 days	12	0

	When you want to...	Do this...
1	Update the email address.	For **System email address**, type a new email address, then click **Save**.
2	Move the computer into a new group.	For **Group**, select a group from the list, then click **Save**.
3	Display instructions for resolving an action item.	Click the red action item.
4	Display details about detections.	Under **Detections**, click a quantity in the **Detections** or **User-Approved Applications** column, then click **Save**. (To approve any detections for use by adding them to a policy, see *Specify approved programs* on page 101 and *Set up allowed Internet applications* on page 121.)

View detections for a computer

Use this feature to view all the detections for a single client computer.

To view detections:

1. On the **Computers** page, click a quantity under **Detections** to display a list of detected items and their status.
2. From the **Detection List**, click the name of a detection to display detailed information from the SonicWALL Avert Labs Threat Library.

View user-approved applications for a computer

Use this feature to see which programs users have approved. Users can add approved programs and allowed Internet applications only if their policy permits.

To view user-approved applications:
On the **Computers** page, click a quantity under **User-Approved Applications** to display a list of potentially unwanted programs detected by the virus and spyware protection service and Internet applications detected by the firewall protection service.

These programs were detected as potential threats, but users have approved them to run on their computers.

To approve or allow a program:
To allow a user-approved program to run on other client computers, add it to a policy. (See *Specify approved programs* on page 101 or *Set up allowed Internet applications* on page 121 for more information.) Approved programs are no longer detected or blocked on any computers using the updated policy.

Send email to computers

Use this feature to notify users about problems with their computers or tasks they need to perform. You must have a local email application installed on your administrative computer.

To send email to computers:
On the **Computers** page, click an email address for a computer in the listing.

OR

Select the checkbox next to each computer you want to send email to, then click **Email**.

Your local email application opens a blank message, preaddressed (in the BCC field) to the selected computers.

Block computers from receiving updates

Use this feature to prevent unauthorized computers that are connecting to your network (sometimes called *rogue systems*) from receiving service updates.

To block computers:
On the **Computers** page, select the computers you want to block, then click **Block**.

To unblock computers:
On the **Computers** page, select **Blocked** to list all blocked computers, then select the computers you want to unblock and click **Unblock**.

Delete computers from your reports

Use this feature to remove obsolete computers and duplicate computers from your listings. Duplicates typically appear when the Enforced Client client software has been installed more than once on a single computer or when users install it on their new computers without uninstalling it from their previous computers.

> Deleting a computer does not uninstall the Enforced Client client software. If you mistakenly delete a computer with working client software from the report, it automatically reappears in your listing the next time its report data is uploaded. However, you will no longer be able to view the historical detection data for that computer.

To delete computers:
On the **Computers** page, select the computers you want to delete, then click **Delete**.

See *View duplicate computers* on page 80 for information on displaying a complete listing of duplicate computers in a report.

Move computers into a group

Every client computer is part of a group (see *Creating groups to manage your site* on page 71 for more information). Initially, you assign computers to a group when installing Enforced Client. If no group is specified, computers are placed in the **Default** group.

You can move computers into a different group at any time.

To move computers:

1. On the **Computers** page, select the computers you want to move.

2. From the **Move to** list, select the group you want to move the computers to.

   You must create the group before you can move computers into it. See *Create or edit a group* on page 72.

3. Click **Move**.

Creating groups to manage your site

A group consists of one or more computers that use the same policy of security settings. You can base groups on geographic location, department, computer type, the tasks performed by the users, or anything meaningful to your organization.

By default, every computer in your account is placed into a group called **Default**. You can create other groups to place them in instead.

Why use groups?

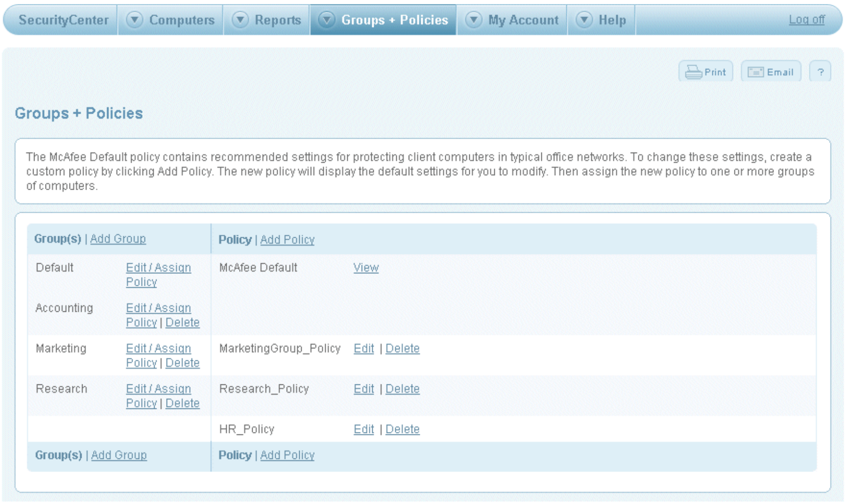
Groups help you manage large numbers of computers or computers that use different security settings (defined in *policies*). Groups are particularly helpful in larger organizations or companies that are widely distributed geographically. Placing similar computers into a single group enables you to view and manage security issues for the group separately from the other computers in your account.

For example, you might place all laptops used by traveling sales representatives into a single group called Sales Team. Then you can configure special security settings for those computers to provide greater protection against threats in unsecure networks such as airports and hotels. You can also track the number of detections on those computers through more frequent reports and adjust the security settings as needed. See *User groups* on page 18 for an illustration.

How can I manage groups?

Click the **Groups + Policies** tab to display the groups in your organization and the policies assigned to them. If you have not created any groups or policies, only the **Default** group and the **SonicWALL Default** policy are displayed.

Figure 3-6 Groups + Policies tab



Groups + Policies

The McAfee Default policy contains recommended settings for protecting client computers in typical office networks. To change these settings, create a custom policy by clicking Add Policy. The new policy will display the default settings for you to modify. Then assign the new policy to one or more groups of computers.

Group(s) | Add Group		Policy | Add Policy	
Default	Edit / Assign Policy	McAfee Default	View
Accounting	Edit / Assign Policy | Delete		
Marketing	Edit / Assign Policy | Delete	MarketingGroup_Policy	Edit | Delete
Research	Edit / Assign Policy | Delete	Research_Policy	Edit | Delete
		HR_Policy	Edit | Delete
Group(s) | Add Group		Policy | Add Policy	

From the **Groups + Policies** page, you can:

- *Create or edit a group*
- *Delete a group*

Computers are assigned to a group when protection services are installed. You can also move computers to different groups using the **Computers** page.

The Default group

Until you create additional groups, all computers where you install your security services are assigned to the **Default** group. You cannot change the name of the **Default** group.

The **Default** group uses the **SonicWALL Default** policy, which is configured with settings recommended by SonicWALL to protect most organizations. You can assign a different policy to the **Default** group.

Create or edit a group

Use this procedure to assign a name and a policy to a group. See *Move computers into a group* on page 70 for instructions on assigning computers to the group.

To create or edit a group:
On the **Groups + Policies** page, click **Add Group** or **Edit/Assign Policy**, specify a name and a policy for the group, then click **Save**.

Only one policy can be assigned to a group. Any existing policy is removed from that group when you click **Save**.

Delete a group

You must move all computers out of a group before you can delete it. See *Move computers into a group* on page 70 for instructions.

To delete a group:
On the **Groups + Policies** page, click **Delete** next to the group you want to delete.

You cannot delete the **Default** group.

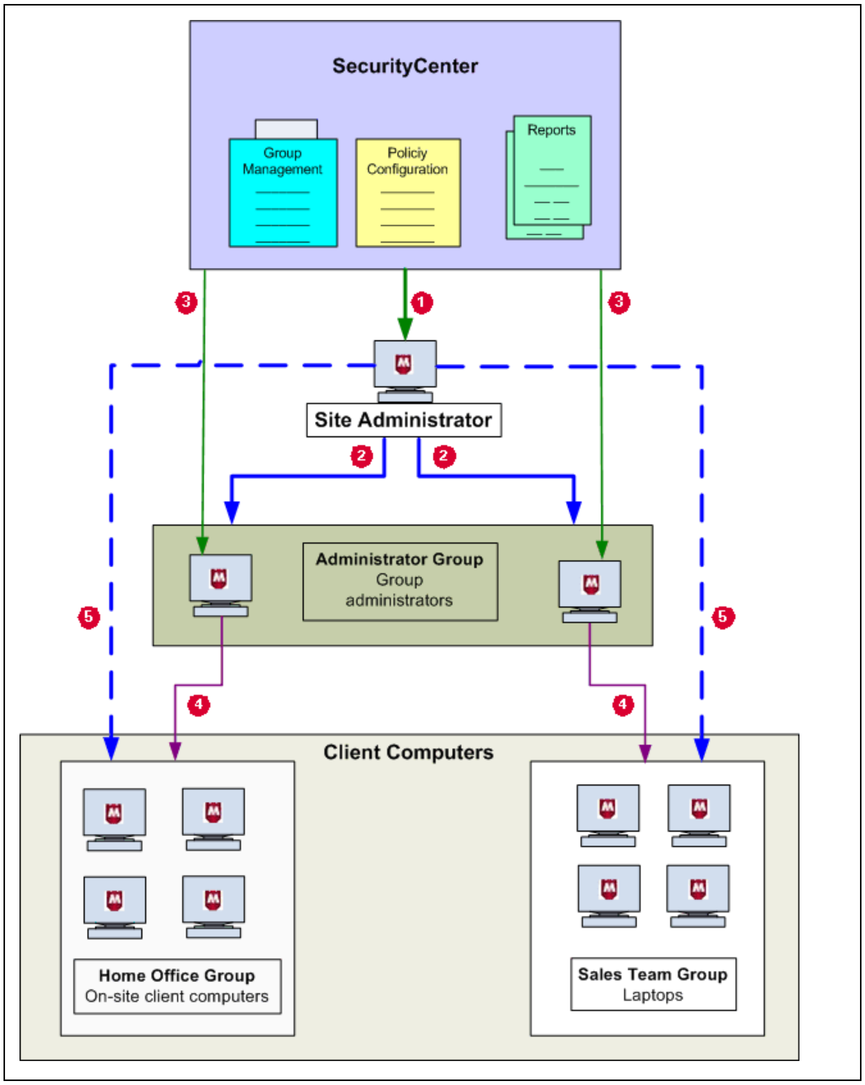
Designating group administrators

Group administrators oversee and manage the groups that you, the site administrator, assign to them. When creating group administrators, you specify which groups they manage, a password they use to access the SecurityCenter, and their access level.

Why use group administrators?
Create group administrators to distribute security management in large organizations.

Group administrators have fewer access rights than the site administrator. While the site administrator can access all security information for all client computers in the account, group administrators can access information only for client computers in the groups they are assigned to.

Figure 3-7 Site and group administrators



1 The site administrator communicates directly with the SecurityCenter to create policies, check reports, and maintain the Enforced Client account.

2 The site administrator creates and manages group administrators.

3 Group administrators communicate directly with the SecurityCenter to access security data for the groups they are assigned to.

4 Group administrators manage the client computers in their assigned groups. The management tasks they can perform and the information they can access on the SecurityCenter depend on the type of group administrator account set up for them.

5 The site administrator can manage all client computers in all groups.

What can group administrators do?
The access level you assign determines which tasks group administrators can perform for their groups.

Basic tasks for Read Only	Additional tasks for Read & Modify Reports
■ Access the SecurityCenter website (see *Getting started*). **Note**: No subscription information is visible. Only the assigned groups are visible. ■ Manage from client computers (using the administrative menu): *Manage quarantined files*. *Disabling on-access scanning*. ■ View computers from the SecurityCenter (see *Display details for a computer*). ■ Check data in reports (see *Viewing reports*).	■ *Install protection services*. ■ View and manage computers from the SecurityCenter (see *Managing your computers*). ■ View policies (see *Setting up policies*). ■ Rename groups (see *Create or edit a group*). ■ Modify the information in listings and reports: *Send email to computers*. *Block computers from receiving updates*. *Delete computers from your reports*. ■ Move computers in and out of groups (see *Move computers into a group*). ■ *Send email to users*. ■ Send reports to users in email (see *Make the most of your online data*).

You specify the access level when you create the group administrator's account, and you can edit it at any time.

- *Create or edit a group administrator*
- *Delete a group administrator*

Create or edit a group administrator

Use the **My Account** page to manage group administrators. Up to six group administrators can be listed on this page. If you have created more than six group administrator accounts, click **All group administrators** to display a complete listing.

To create or edit a group administrator:

1 On the **My Account** page, in the **Group Administrator** section, click **Add** or **Edit**.

2 On the **Manage Group Administrators** page, select **Create New** or select the name of an existing group administrator.

3 Type the group administrator's name, email address, and password.

The password you assign is used to log on to the SecurityCenter and must be different from your password. Administrative rights based on the group administrator's access level will be assigned to this password.

4 Select an access level and which groups to manage.

5 Click **Save** to return to the **My Account** page.

6 On the line where the new group administrator's name appears, click **Email Password**.

Your local email application opens a preaddressed message explaining how to log on to the SecurityCenter, assigned groups, and instructions for accessing information about their responsibilities. (You can use this feature only if you have a local email application installed.)

7 Send the email message.

Delete a group administrator

For security purposes, be sure to delete obsolete accounts for group administrators.

To delete a group administrator:
On the **My Account** page, in the **Group Administrators** section, click **Delete**.

Setting up policies

Policies are made up of security settings for all of your protection services. These settings define how your services operate on client computers.

Why use policies?
Policies enable you to customize security settings for your entire organization or for different computers in your organization. Each policy is assigned to a group of computers. If you have created multiple groups, you can assign a unique policy to each group or allow them to share a single policy.

For example, you might place all laptops used by traveling sales representatives into a single group called Sales Team. You can then assign a policy with high security settings that will provide greater protection against threats in unsecure networks such as airports and hotels. Whenever you want to adjust those setting, simply change the policy. Your changes will be applied to all the computers in the Sales Team group automatically. There is no need to update each computer's setting individually. See *Customized policies* on page 19 for an illustration.

How can I manage policies?
Click the **Groups + Policies** tab to display the groups in your organization and the policies assigned to them. If you have not created any groups or policies, only the **Default** group and the **SonicWALL Default** policy are displayed (see *The SonicWALL Default policy*). From this page, you can:

- *Create or edit a policy*
- *Assign a policy to a group*
- *Restore default policy settings*
- *Delete a policy*

Can users change their security settings?
The policy determines whether users can change their security settings.

The SonicWALL Default policy

Until you create additional policies, all computers are assigned the **SonicWALL Default** policy, which is configured with settings recommended by SonicWALL to protect many environments. You cannot rename or modify the **SonicWALL Default** policy.

When you create a new policy, the default settings appear as a guideline. This enables you to configure only the settings you want to change without having to configure them all.

Tab	Default setting
	On-Demand Scan: Off
Spyware Protection	**Spyware Protection Status:** On **Spyware Protection Mode:** Prompt
Desktop Firewall	**Automatically install the desktop firewall on all computers using this policy:** Disabled **Use Smart Recommendations to automatically approve common Internet applications:** Enabled **Firewall Configuration:** User configures firewall **Firewall Status:** On **Firewall Protection Mode:** Prompt **Connection Type:** Untrusted
Browser Protection	**Automatically install browser protection on all computers using this policy:** Enabled
Advanced Settings	**Update client computers where users are not logged in:** Enabled **Display support notifications on client computers:** Enabled Virus protection: ■ **Enable outbreak response:** Enabled ■ **Enable buffer overflow protection:** Enabled ■ **Enable script scanning:** Enabled ■ **Scan email (before delivering to the Outlook Inbox):** Enabled ■ **Scan all file types during on-access scans:** Enabled ■ **Scan compressed archives during on-access scans:** Disabled ■ **Scan compressed archives during on-demand scans:** Enabled ■ **Check for updates every:** 12 hours Spyware protection: All programs types are enabled.

With the default **Advanced Settings** configuration, it is possible for an on-demand scan to detect threats in archived files that are not detected during an on-access scan. This is because on-access scans do not look at compressed archives by default. If this is a concern for your organization, you should enable this option.

Create or edit a policy

Use this procedure to name a policy and configure its security settings.

To create or edit a policy:

1 On the **Groups + Policies** page, click **Add Policy** (or click **Edit** to modify an existing policy).

2 In the **Add Policy** window, type a name in the **Policy name** box. (If you are editing an existing policy, the name appears automatically in the **Edit Policy** window.)

3 Configure the settings on each tab.

Initially, options are configured with the **SonicWALL Default** policy settings.

- See *Set basic virus protection options* on page 95 and *Set advanced virus protection options* on page 97 to configure virus protection settings.
- See *Set basic spyware protection options* on page 99 and *Set advanced spyware protection options* on page 102 to configure spyware protection settings.
- See *Configuring policies for firewall protection* on page 112 to configure firewall protection settings.
- See *Configuring browser protection from the SecurityCenter* on page 130 to configure browser protection settings.
- See *Update computers where no user is logged on* on page 55 to prevent error logging for computers that are unable to update automatically.
- See *Notifying users when support ends* on page 28 to display a message on client computers when support for the operating system is changing.

4 Click **Save**.

Assign a policy to a group

After you create a policy, assign it to a group by editing the group. See *Create or edit a group* on page 72 for instructions.

Restore default policy settings

Use this procedure to change all settings on all tabs of a custom policy to the original **SonicWALL Default** policy settings.

To restore a policy to the SonicWALL Default settings:

1 On the **Groups + Policies** page, click **Edit** next to the policy you want to modify.

2 On any tab, click **Reset to Defaults** to restore all the settings for all tabs.

3 Make adjustments to any of the default settings as needed.

4 Click **Save**.

These changes do not take effect until you click **Save**. You have the opportunity to cancel the changes or to modify individual settings before saving.

Delete a policy

Use this procedure to remove a policy you have created from your account. You cannot delete the **SonicWALL Default** policy.

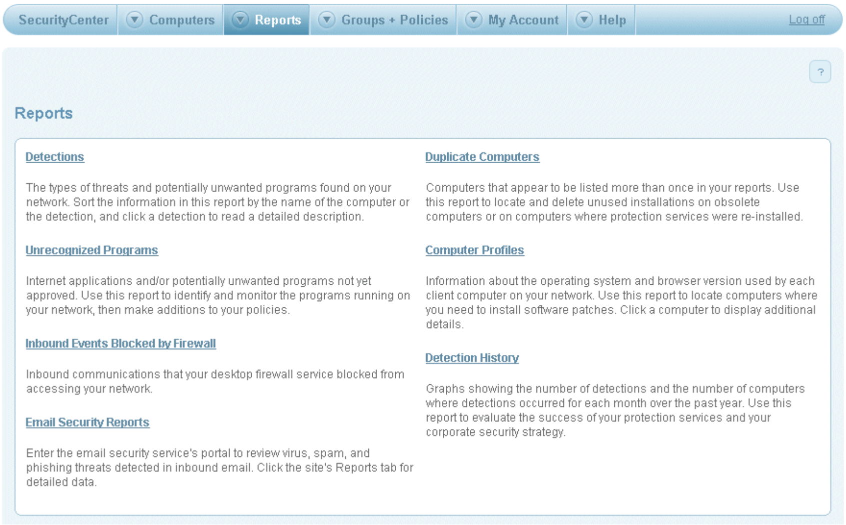
To delete a policy:
On the **Groups + Policies** page, next to a policy name click **Delete**.

If you delete a policy that is assigned to one or more groups, the **SonicWALL Default** policy will be assigned to those groups.

Viewing reports

Whenever a client computer checks for updates, it also sends its scanning history, update status, and detections to the SecurityCenter website in encrypted XML files. It uploads the data directly through an Internet connection or via a relay server. You can view this data in reports accessed from the **Reports** page. All client computers on your account (using the same company key) appear in the reports.

Figure 3-8 Reports page



Reports

Detections

The types of threats and potentially unwanted programs found on your network. Sort the information in this report by the name of the computer or the detection, and click a detection to read a detailed description.

Unrecognized Programs

Internet applications and/or potentially unwanted programs not yet approved. Use this report to identify and monitor the programs running on your network, then make additions to your policies.

Inbound Events Blocked by Firewall

Inbound communications that your desktop firewall service blocked from accessing your network.

Email Security Reports

Enter the email security service's portal to review virus, spam, and phishing threats detected in inbound email. Click the site's Reports tab for detailed data.

Duplicate Computers

Computers that appear to be listed more than once in your reports. Use this report to locate and delete unused installations on obsolete computers or on computers where protection services were re-installed.

Computer Profiles

Information about the operating system and browser version used by each client computer on your network. Use this report to locate computers where you need to install software patches. Click a computer to display additional details.

Detection History

Graphs showing the number of detections and the number of computers where detections occurred for each month over the past year. Use this report to evaluate the success of your protection services and your corporate security strategy.

Why use reports?

Reports provide valuable tools for managing your security strategy. Only the reports available for the installed protection services appear on this page.

Use this report...	To view...
	The types of potentially malicious code or unwanted programs that have been found on your network. Use this report to manage detections of viruses and potentially unwanted programs. See *View detections* on page 103 for instructions.
Unrecognized Programs	Programs that your spyware protection or firewall protection detected on your network. Use this report to manage your potentially unwanted program detections and Internet applications blocked by the firewall protection service. See *View unrecognized programs* on page 105 and *View unrecognized Internet applications* on page 123 for instructions.
Inbound Events Blocked by Firewall	Computers where inbound or outbound communications were blocked by the firewall protection service. Use this report to manage blocked communications. See *View inbound events blocked by the firewall* on page 124 for instructions.
Duplicate Computers	Computers that appear more than once in administrative reports. Use this report to track down obsolete computers and those where Enforced Client has been incorrectly overinstalled and tracked as multiple installations. See *View duplicate computers* on page 80 for detailed instructions.
Computer Profiles	The version of the Windows operating system and the Internet Explorer web browser running on each client computer. Use this report to locate computers where you need to install software patches for a specific browser or operating system. See *View computer profiles* on page 81 for detailed instructions.
Detection History	A graphical summary of the number of detections and the number of computers where detections occurred on your network over the past year. Use this report to evaluate the effectiveness of your security strategy. See *View your detection history* on page 107 for instructions.
Email Security Reports	A page on the email security service’s portal, where you can access reports on your site’s mailflow and detections. Use these reports to monitor email activity and detections. See *Viewing reports for the email security service* on page 141 for instructions.

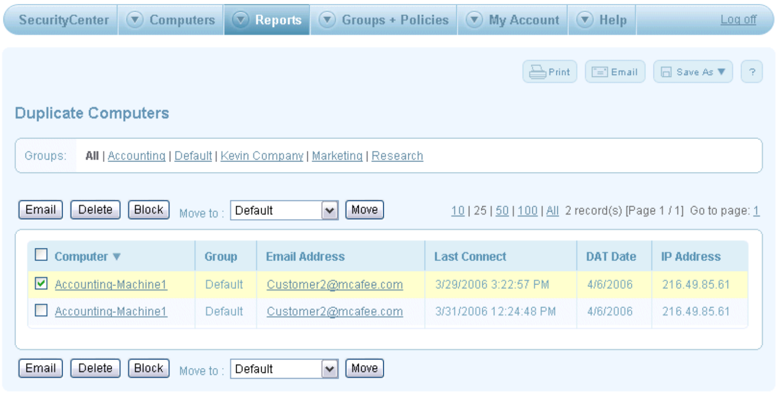
Can I customize reports?

- Select the data to display (see *Customize listings and reports* on page 60).
- Print a report, save it, or send it to users (see *Make the most of your online data* on page 59).
- Add a customized logo (see *Add your logo to reports* on page 82).

View duplicate computers

Use the **Duplicate Computers** report to locate computers that are listed more than once in your reports. Duplicate listings usually result when the Enforced Client client software has been installed more than once on a single computer or when users install it on their new computers without uninstalling it from their previous computers.

Figure 3-9 Duplicate Computers report



Duplicate Computers

Groups: **All** | Accounting | Default | Kevin Company | Marketing | Research

10 | 25 | 50 | 100 | All 2 record(s) [Page 1 / 1] Go to page: 1

□ Computer ▼	Group	Email Address	Last Connect	DAT Date	IP Address
☑ Accounting-Machine1	Default	Customer2@mcafee.com	3/29/2006 3:22:57 PM	4/6/2006	216.49.85.61
□ Accounting-Machine1	Default	Customer2@mcafee.com	3/31/2006 12:24:48 PM	4/6/2006	216.49.85.61

Select the information that appears in this report:

Groups — Display only the computers in a group or display all computers.

To delete a duplicate computer:

Select the duplicate computer in the report, then click **Delete**.

> Deleting a computer does not uninstall the Enforced Client client software. If you mistakenly delete a computer with working client software from the report, it automatically reappears in your listing the next time its report data is uploaded. However, you will no longer be able to view the historical detection data for that computer.

To view details about a computer:

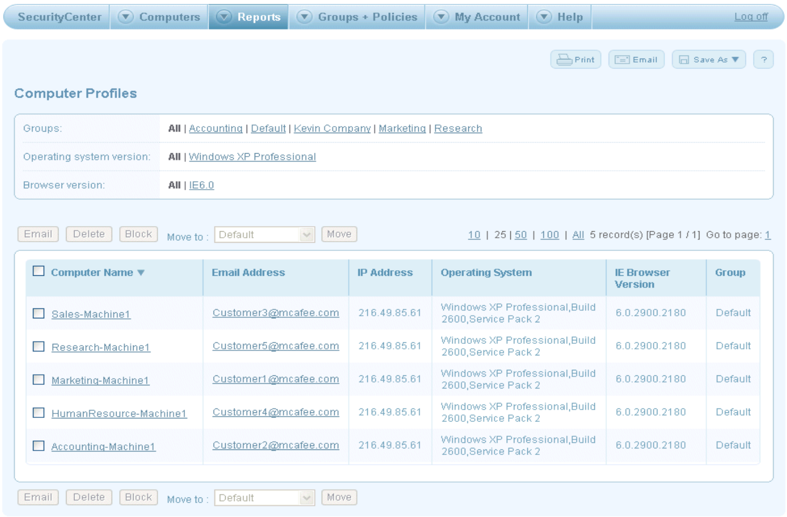
Click a computer name to display the **Computer Details** page.

The **Computer Details** page displays information about the computer, its service components, and its detections. See *Display details for a computer* on page 67 for information about tasks you can perform from this page.

View computer profiles

Use the **Computer Profiles** report to view the version of the Windows operating system and the Internet Explorer web browser running on client computers. This helps you locate computers for maintenance, such as installing Microsoft software patches.

Figure 3-10 Computer Profiles report



Computer Profiles

Groups:	All | Accounting | Default | Kevin Company | Marketing | Research
Operating system version:	All | Windows XP Professional
Browser version:	All | IE6.0

10 | 25 | 50 | 100 | All 5 record(s) [Page 1 / 1] Go to page: 1

□ Computer Name ▼	Email Address	IP Address	Operating System	IE Browser Version	Group
□ Sales-Machine1	Customer3@mcafee.com	216.49.85.61	Windows XP Professional,Build 2600,Service Pack 2	6.0.2900.2180	Default
□ Research-Machine1	Customer5@mcafee.com	216.49.85.61	Windows XP Professional,Build 2600,Service Pack 2	6.0.2900.2180	Default
□ Marketing-Machine1	Customer1@mcafee.com	216.49.85.61	Windows XP Professional,Build 2600,Service Pack 2	6.0.2900.2180	Default
□ HumanResource-Machine1	Customer4@mcafee.com	216.49.85.61	Windows XP Professional,Build 2600,Service Pack 2	6.0.2900.2180	Default
□ Accounting-Machine1	Customer2@mcafee.com	216.49.85.61	Windows XP Professional,Build 2600,Service Pack 2	6.0.2900.2180	Default

Select the information that appears in this report:

Groups — Display only the computers in a group or display all computers.

Operating system version — Display computers running all Windows operating systems or only those running the selected version.

Browser version — Display computers running all versions of Internet Explorer or only those running the selected version.

Managing your correspondence

Use SecurityCenter features to simplify and customize your correspondence with users, customers, and your service provider.

- *Send email to users*
- *Update user email addresses*
- *Update your account's email address*
- *Add your logo to reports*

Send email to users

Use email to send important information about corporate security to your users:

- Send reports or listings as an attached archived web page in .MHTM format (see *Make the most of your online data* on page 59).
- Send descriptions of security issues on client computers or instructions for required maintenance (see *Send email to computers* on page 69).

> You can use this feature only if you have a local email application installed.

Update user email addresses

Users can enter their email address when installing Enforced Client. It is important for you to update their email addresses as they change.

To update a user's email address:

1 In any listing, click a computer name link.

2 On the **Computer Details** page, type a new email address, then click **Save**.

Update your account's email address

Keep the email address for your account up-to-date to prevent lapses in receiving your status emails and other account correspondence from your service provider.

To update your account's email address:

1 On the **My Account** page, in the **My Profile** section, click **Edit**.

2 On the **Customer Profile** page, type your new email address in the first text box, then click **Save**.

Add your logo to reports

To customize your correspondence, you can upload a logo that appears in the upper-right corner of the SecurityCenter website, including reports you send to users.

Logo files can be .GIF, .JPEG, .JPG, or .PNG format. Logo dimensions must be 175 x 65 pixels with a file size under 500 KB. Other dimensions will result in a stretched or shrunken logo.

To upload a logo:

1 On the **My Account** page, in the **My Logo** section, click **Edit**.

2 On the **Manage Logo** page, click **Upload Logo**. (To replace an existing logo, click **Upload New Logo**.)

3 On the **Upload Your Logo** page, type the name of the file you want to upload or browse to locate the file.

4 In the **Verification Code** box, type the characters displayed in the black box. (Alphabetic characters are not case-sensitive.)

5 Click **Upload Logo**.

If your logo file is not the correct size, the SecurityCenter resizes it to fit the allotted area and displays a preview of how it will appear on reports. Click **Approve** to accept the resized logo, or **Delete and Resubmit** to select a different file.

6 Click **Close Window**.

To delete a logo:

1 On the **My Account** page, in the **My Logo** section, click **Edit**.

2 On the **Manage Logo** page, click **Delete Logo**.

3 Click **Cancel** to return to the **My Account** page.

Managing your subscriptions

The SecurityCenter includes tools to help you keep track of your service subscriptions.

- *View your service subscriptions*
- *Update subscription information*
- *Purchase, add, and renew services*
- *Request a trial subscription*
- *Receive subscription notifications*

View your service subscriptions

Check the status of your subscriptions to ensure your protection services remain active and you have the right number of licenses to protect new computers as your organization grows.

To view your protection services summary:
Click the **My Account** tab.

The **Service Summary** lists details about each subscription, including the number of licenses and the expiration date.

To view your subscription history:

1 On the **My Account** page, in the **Service Summary** section, select **View subscription history**.

The **Subscription History** page lists details for each service subscription.

2 Select **View Cancelled Subscriptions** to display a list of subscriptions that are no longer current.

Update subscription information

Use the **Subscription History** page to update the contact and account information for each of your protection service subscriptions. This is useful for administrators who manage multiple accounts.

> Your service provider determines whether this feature is available to you. Typically, the **Edit** link is available only to SonicWALL partners who oversee security for multiple accounts.

To update information for a subscription:

1. On the **My Account** page, in the **Service Summary** section, select **View subscription history**.

   The **Subscription History** page lists details for each service subscription.

2. In the listing, select **Edit** for the subscription you want to update.

3. In the **Edit Subscription Information** page, type new information for:

   - Email address
   - Company name
   - First name
   - Last name

4. Click **Submit** to return to the **Subscription History** page and view the updated entry.

Purchase, add, and renew services

To ensure that additional or renewed services remain on the same account with your existing services, follow these guidelines:

- Submit your order through the same SecurityCenter website you use to maintain your original subscriptions.
- Submit your order with the same email address you used to register and maintain your original subscriptions.

> If you customized an administrator email address that is different than the email address you used to place your original order, be sure you use the original email address to place your new order.

By keeping all your service subscriptions on the same account, all your client computers report to the same SecurityCenter website, and your service provider sends all correspondence and notifications to one email address.

To purchase, add, or renew services:

1. On the **My Account** page, locate the **Service Summary** section.

2. In the **Add Service** column, click **Buy**, **Buy More**, or **Renew**.

3. Follow the instructions on the **Product Purchase** page.

> You can also access the **Product Purchase** page from the **SecurityCenter** page or the **Subscription History** page.

Request a trial subscription

To try a protection service free of charge for 30 days, you can request a trial subscription. You'll have the opportunity to try all the features. You can then purchase the service and continue using it with no interruption in protection.

To request a free trial:

1 On the **My Account** page or the **SecurityCenter** page, click **Buy** or **Try**.

2 Follow the instructions on the **Product Purchase** page.

Receive subscription notifications

Configure your notification preferences to receive an email whenever the expiration date for a service approaches. See *Sign up for email notifications* on page 62 for more information.

Getting assistance

Click the **Help** tab to display the **Help** page, where you can access additional resources for Enforced Client and your SecurityCenter website.

- *View printed and online documents*
- *Download utilities*
- *Contact product support*

View printed and online documents

Several documents are available to assist you with installing, configuring, and using your protection services.

To view online documents:
On the **Help** page, click a link for this *Product Guide*, the *Quick Start Guide*, or the *Release Notes*.

To view context-sensitive online help:
Click the **help** link (**?**) at the upper right of any page of the SecurityCenter to view information specific for that page.

Download utilities

Access utilities to assist with installing client software and troubleshooting installation problems from the **Utilities** page.

To download utilities:
On the **Help** page, click **Utilities**, then click a link.

To do this...	Click this link...
	VSSetup Downloads the silent installation package for deploying client software to a single computer without user interaction. Download to the administrative computer. Requires a method for moving the installation package to a client computer, such as a third-party deployment tool, a login script, a link to an executable file in an email message, or a portable medium such as a CD. See *Silent installation* on page 39 for more information.
Install client software remotely using the Push Install utility.	**Run the Push Install Utility** Downloads a utility for remotely deploying client software directly from your service provider's website to multiple computers simultaneously. Download to the administrative computer. See *Push installation* on page 42 for more information.
Uninstall components left from a previous installation.	**MVSUninstall** Downloads a utility that cleans up registry keys and files from a previous installation of Enforced Client or competitive software. Download directly to the client computer, then double-click.
Enable users without administrator rights to install client software.	**installation agent** Downloads the standalone installation agent. Download directly to the client computer and install locally, or download to the administrative computer and use deployment tools to install on clients. Required only when you want users without administrator rights to use the URL method to install client software. You must have local administrator rights on the client computer to install this file. See *Install the standalone installation agent* on page 34 for more information.

Contact product support

If you cannot find an answer to a question in the product documentation, send it directly to a product support representative.

To contact product support:
On the **Help** page, click **Contact Support** to display a form where you can submit a description of your problem to a product support representative.

4 Using the Virus and Spyware Protection Service

The virus and spyware protection service in Enforced Client safeguards client computers against threats, such as viruses and potentially unwanted programs, by scanning files and email messages as they are accessed.

This section describes features of the virus and spyware protection service:

- *Accessing client features (Scan Tasks menu)*
- *Scanning client computers*
- *Configuring policies for virus and spyware protection*
- *Viewing reports for virus and spyware detections*
- *Managing detections*
- *Disabling on-access scanning*

Accessing client features (Scan Tasks menu)

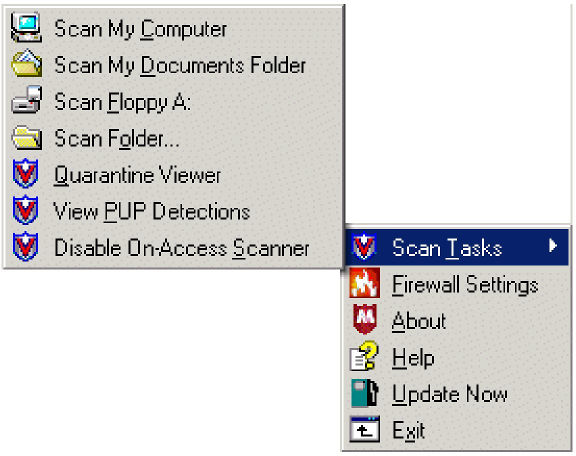
Use the **Scan Tasks** menu to access client features of the virus and spyware protection service. You can also access advanced features from an administrative version of the menu.

To display the Scan Tasks menu:
On the client computer, click M in the system tray, then select **Scan Tasks**.

OR

To display the administrative version of the menu, hold down **Ctrl** and **Shift**, click M in the system tray, then select **Scan Tasks**.)

Figure 4-1 Scan Tasks menu



Select this command...	To do this...
	Select a location to scan (**My Computer**, **My Documents Folder**, or **Floppy A**). Click **Scan Folder...** to browse to a folder of your choice.
Quarantine Viewer (administrative menu only)	Open the quarantine folder, which contains possible threats detected on the computer (see *Manage quarantined files* on page 109).
View PUP Detections	Display a list of potentially unwanted programs that the virus and spyware protection service has detected (see *Scan for spyware* on page 93).
Disable On-Access Scanner (administrative menu only)	Turn off the automatic on-access scanner. To re-enable the scanner, reopen the administrative menu and select **Enable On-Access Scanner** (see *Disabling on-access scanning* on page 110). **Note:** The computer is vulnerable to attack if you disable the on-access scanning feature. Be sure to enable the feature again as soon as possible.

Scanning client computers

The virus and spyware protection service safeguards computers by automatically scanning for viruses and spyware. At any time, users can perform manual scans of files, folders, or email, and administrators can set up scheduled scans.

- *Scan automatically (on-access scans)*
- *Scan manually (on-demand scans)*
- *Schedule on-demand scans*
- *Scan email*
- *Scan for spyware*

The behavior of the scanning features on client computers is defined in the policies that you configure using the SecurityCenter. Policy settings determine the types of files, programs, and other items detected; whether users can manage their detections; how frequently computers check for updates; and when scheduled scans occur. See *Configuring policies for virus and spyware protection* on page 95 for instructions on configuring these settings in policies.

Scan automatically (on-access scans)

The virus and spyware protection service scans files and folders on client computers whenever they are accessed, which is referred to as an *on-access scan*.

The default on-access scanning policy is:

- All types of files are scanned when opened, and again when closed (if they were modified).
- All email attachments are scanned when accessed and when saved to the hard drive, protecting the computer from email infections.
- Programs are scanned for spyware identifiers, to detect if a spyware program attempts to run or a program attempts to install spyware.

To customize on-access scans, administrators can:

- Exclude certain folders, file types, or programs from on-access scanning by configuring the virus and spyware protection settings in policies (see *Specify approved programs* on page 101).
- Select an option to scan only files meeting the current file extension criteria specified in the detection definition (DAT) files (see *Set advanced virus protection options* on page 97).
- Select an option to scan compressed archives (see *Set advanced virus protection options* on page 97).
- Specify other options for scanning email attachments and spyware (see *Configuring policies for virus and spyware protection* on page 95).
- *How detections are handled*

Scan manually (on-demand scans)

The virus and spyware protection service automatically scans most files when they are accessed. However, users can scan a particular drive or folder at any time. This is referred to as an *on-demand scan*.

The default on-demand scanning policy is:

- All processes running in memory are scanned.
- All files are scanned.
- All critical registry keys are scanned.

In addition, during an on-demand scan of **My Computer**, the drive where Windows is installed, or the Windows folder:

- All cookies are scanned.
- All registry keys are scanned.

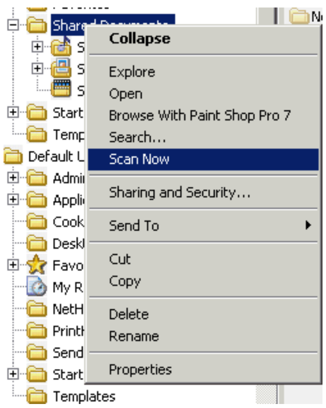
Administrators can set a schedule for some or all computers to run an on-demand scan automatically. See *Schedule on-demand scans* on page 95 for more information.

To perform a manual scan using the icon:

1. Click M in the system tray, then select **Scan Tasks**.
2. Select **Scan My Computer, Scan My Documents Folder,** or **Scan Floppy A:,** or select **Scan Folder** and browse for a drive or folder.

To perform a manual scan from Windows Explorer:
In Windows Explorer, click any drive or folder, then select **Scan Now** from the menu.

Figure 4-2 Scan Now option



- *View scan results*
- *How detections are handled*

View scan results

After completing an on-demand scan, Enforced Client stores results in a **Scan Statistics** report on the computer where the scan was performed. The number and type of detections are uploaded to the SecurityCenter for inclusion in administrative reports.

To view results of a manual scan:
In the **Scan Completed** dialog box, click **Report** to display the **Scan Statistics** report.

What is in a Scan Statistics report?
The **Scan Statistics** report opens in the default browser and displays the following information:

- Date and time the scan was started.
- Elapsed time for the scan.
- Version of the scanning engine software and DAT file.
- Date of the last update.
- Completion status of the scan.
- Location of the scanned items.
- Status for scanned files, registry keys, and cookies:

Scanned Number of items scanned.

Detected The item is still a threat and still resides on the system. *For files*, they are most likely contained within a compressed archive (for example, a .ZIP archive) or on write-protected media. *For registry keys and cookies*, the file it is associated with has a status of **Detected**.

Cleaned The item was cleaned of the threat. An encrypted backup copy of the original item was saved in a quarantine folder, where it can be accessed only with the **Quarantine Viewer** (see *Manage quarantined files* on page 109).

Deleted The item could not be cleaned; it was deleted instead. An encrypted copy was saved in a quarantine folder, where it can be accessed only with the **Quarantine Viewer** (see *Manage quarantined files* on page 109).

How detections are handled

The type of threat and the policy settings determine how the virus and spyware protection service handles a detection:

Items with detections	How the service handles the detections
	Virus detections: The virus and spyware protection service attempts to clean the file. If it can be cleaned, the user is not interrupted with an alert. If it cannot be cleaned, an alert appears, and the detected file is deleted. A copy is placed in the quarantine folder. **Potentially unwanted program detections:** If the virus and spyware protection service is set to **Protect** mode, detections are cleaned or deleted. If set to **Prompt** mode, users must select the response. See *Select a spyware protection mode* on page 100 for details. In all cases, an encrypted backup copy of the original item is saved in a quarantine folder (see *Manage quarantined files* on page 109). Data for all activity is uploaded to the SecurityCenter for use in reports.
Registry keys and cookies	Detections initially appear as **Detected**. See *Scan for spyware* on page 93 for instructions on cleaning the detections. Cleaning detected files also cleans their associated registry keys and cookies. Their status is then reported as **Cleaned**.

Schedule on-demand scans

Schedule an on-demand scan to occur at a specific date and time, either once or on a recurring basis. For example, you might want to scan client computers at 11:00 P.M. each Saturday, when it is unlikely to interfere with other client processes. Scheduled scans are configured as part of a policy and run on all computers using that policy. See *Schedule on-demand scans* on page 95.

> At the start of an on-demand scan, all previous detections of potentially unwanted programs are cleared from the **Potentially Unwanted Program Viewer**.

Scan email

By default, the virus and spyware protection service scans all email messages and attached files as they are accessed. It also scans messages before they reach a user's Inbox (see *Enable optional protection* on page 97).

Users can scan their Microsoft Outlook folders or individual messages manually.

To scan an email message manually:

1. In the Microsoft Outlook Inbox, highlight one or more messages in the right pane.
2. Under **Tools**, select **Scan for Threats**.

   The **On Demand Email Scan** window displays any detections. If the window is empty, no threats were detected.

Scan for spyware

As part of its automatic scans, the virus and spyware protection service scans for spyware whenever programs are installed or run, and during manual scans. Its response to detections depends on the spyware mode configured in the client computer's policy (see *Set basic spyware protection options* on page 99). Three responses are possible:

- Attempt to clean the program (**Protect** mode).
- Prompt the user for a response (**Prompt** mode).
- Log the detection and take no further action (**Report** mode).

Cookies and registry keys that indicate spyware are also detected. Deleting a potentially unwanted program deletes any associated cookies and registry keys.

All detections are listed in administrative reports available from the SecurityCenter. On client computers, you can view and manage detections using the **Potentially Unwanted Program Viewer**.

> At the start of an on-demand scan, all previous detections of potentially unwanted programs are cleared from the **Potentially Unwanted Program Viewer**. For on-access scans, previous detections remain in the **Potentially Unwanted Program Viewer**.

To manage spyware detections on client computers:

1. On the client computer, open the **Potentially Unwanted Programs Viewer**. Either:

   - In the **Detection Alert** dialog box, click **Yes**.
   - Click M in the system tray, then select **Scan Tasks | View PUP Detections**.

   The **Potentially Unwanted Program Viewer** lists each detected program.

2 Select one or more detections, then select an action:

Clean Place an encrypted original copy of each selected item in a quarantine folder, then attempt to clean it. If it cannot be cleaned, delete the item.

Approve Add each selected item to the user's list of approved programs. These programs will not be detected as spyware during future scans. (Clicking **Approved** displays a list of all currently approved programs on the client computer.)

Close Allow the items to remain on the computer and close the **Potentially Unwanted Program Viewer**. They will be detected again during the next scan.

3 Check the status of each item, then click **Close**.

Action Required You have not performed any action on this item since it was detected.

Approved The item was added to the list of user-approved programs and will no longer be detected as spyware on this computer.

Cleaned The item was cleaned successfully and can be used safely. An encrypted, backup copy of the original item was placed in a quarantine folder.

Quarantined The item could not be cleaned. The original item was deleted, and an encrypted copy was placed in a quarantine folder. If the item was a program, all associated cookies and registry keys were also deleted.

Note: Items are placed into the quarantine folder in a format that is no longer a threat to the computer. After 30 days, these items are deleted. You can manage these items using the **Quarantine Viewer** (see *Manage quarantined files* on page 109).

Delete failed The item could not be cleaned or deleted. If it is in use, close it and attempt the clean again. If it resides on read-only media, such as CD, no further action is required. The virus and spyware protection service has prevented the original item from accessing the computer, but it cannot delete the item. Any items copied to the computer have been cleaned.

Note: If you are not sure why the item could not be cleaned, it is possible that a risk still exists. If you cannot determine why the delete failed, contact product support.

Configuring policies for virus and spyware protection

Policies define the operational settings for all your protection services. See *Setting up policies* on page 75 for general information about using policies.

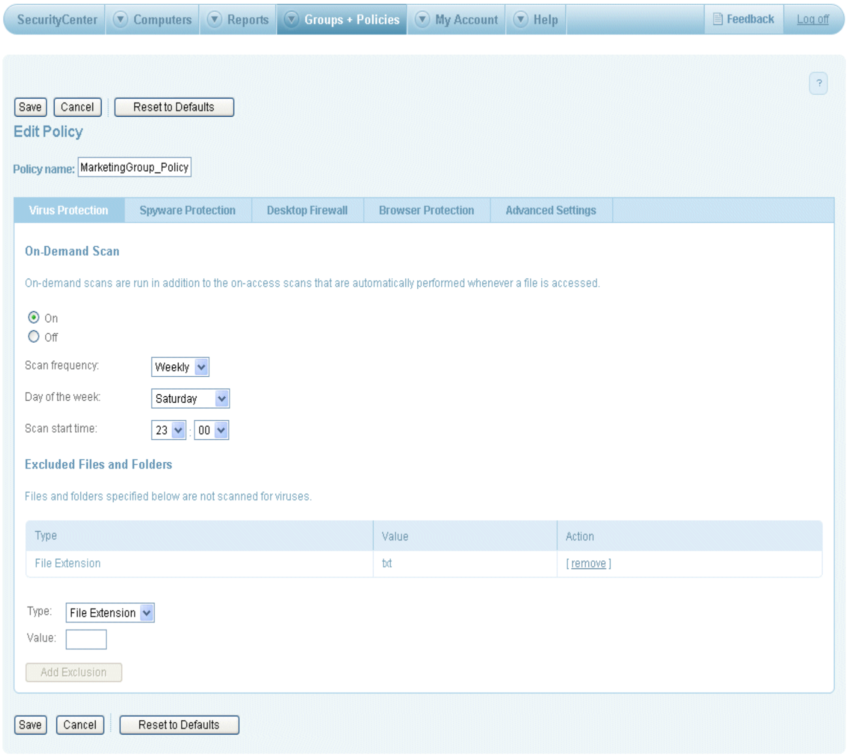
Three tabs are used to configure the features for virus and spyware protection. See *The SonicWALL Default policy* on page 76 for a list of the virus and spyware protection settings in the **SonicWALL Default** policy.

Set basic virus protection options

On the **Groups + Policies page**, use the **Virus Protection** tab to configure basic settings for virus protection.

- *Schedule on-demand scans*
- *Exclude files and folders from virus scans*

Figure 4-3 Virus Protection policy tab



Edit Policy

Policy name: MarketingGroup_Policy

On-Demand Scan

On-demand scans are run in addition to the on-access scans that are automatically performed whenever a file is accessed.

● On
○ Off

Scan frequency: Weekly

Day of the week: Saturday

Scan start time: 23 : 00

Excluded Files and Folders

Files and folders specified below are not scanned for viruses.

Type	Value	Action
File Extension	txt	[remove]

Type: File Extension

Value:

Schedule on-demand scans

You can force a computer to scan all files, folders, and programs by scheduling an on-demand scan to occur at a specific date and time, once or on a recurring basis. These scans are performed in addition to the regular on-access scans.

To schedule an on-demand scan:

1 On the **Groups + Policies** page, click **Add Policy** (or click **Edit** to modify an existing policy).

2 Click the **Virus Protection** tab.

3 Under **On-Demand Scan**, click **On**.

4 Select a frequency, day, and time for the scan to run, then click **Save**.

Exclude files and folders from virus scans

You can create a custom list of files, paths, and file extensions to exclude from both on-access and on-demand scans for *viruses*. By selecting a file here, you request that it *not* be scanned for viruses.

> You can exclude a particular type of file you know is not vulnerable to attack or a folder you know is safe. If you are unsure, we recommend not setting exclusions.

To specify exclusions:

1 On the **Groups + Policies** page, click **Add Policy** (or click **Edit** to modify an existing policy).

2 Click the **Virus Protection** tab.

3 Under **Excluded Files and Folders**, select the type of exclusion you want to create.

4 Specify the value (browse for a file or folder, or type a file extension).

5 Click **Add Exclusion**.

The new exclusion appears in a list.

6 Click **Save**.

To remove an exclusion from the list:

1 On the **Groups + Policies** page, click **Add Policy** (or click **Edit** to modify an existing policy).

2 Click the **Virus Protection** tab.

3 Under **Excluded Files and Folders**, in the table listing for the exclusion you want to remove, click **remove**, then click **Save**.

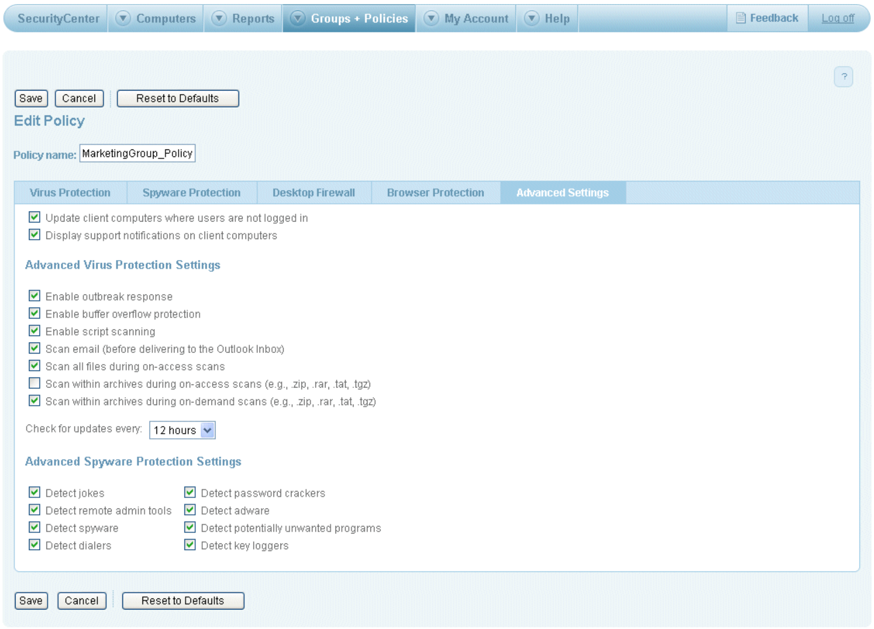
Set advanced virus protection options

On the **Groups + Policies** page, use the **Advanced Settings** tab to configure enhanced protection and safeguard against additional threats lurking in out-of-the-way locations.

- *Select your update frequency*
- *Enable optional protection*

> See *Update computers where no user is logged on* on page 55 for information about the **Update client computers where users are not logged in** policy setting.

Figure 4-4 Advanced virus protection policy settings



Edit Policy

Policy name: MarketingGroup_Policy

☑ Update client computers where users are not logged in
☑ Display support notifications on client computers

Advanced Virus Protection Settings

☑ Enable outbreak response
☑ Enable buffer overflow protection
☑ Enable script scanning
☑ Scan email (before delivering to the Outlook Inbox)
☑ Scan all files during on-access scans
□ Scan within archives during on-access scans (e.g., .zip, .rar, .tat, .tgz)
☑ Scan within archives during on-demand scans (e.g., .zip, .rar, .tat, .tgz)

Check for updates every: 12 hours

Advanced Spyware Protection Settings

☑ Detect jokes
☑ Detect remote admin tools
☑ Detect spyware
☑ Detect dialers
☑ Detect password crackers
☑ Detect adware
☑ Detect potentially unwanted programs
☑ Detect key loggers

Select your update frequency

By default, computers check for updates every 12 hours. You can specify that they check as often as every four hours or as infrequently as once a day.

> An update is not necessarily downloaded every time the computer checks for updates. Checking can reveal that no new update is available.

To select an update frequency:

1 On the **Groups + Policies** page, click **Add Policy** (or click **Edit** to modify an existing policy).

2 Click the **Advanced Settings** tab.

3 For **Check for updates every**, select a setting, then click **Save**.

Enable optional protection

Specify additional updates and advanced scanning to increase protection on client computers.

To specify optional scans:

1 On the **Groups + Policies** page, click **Add Policy** (or click **Edit** to modify an existing policy).

2 Click the **Advanced Settings** tab, select each scan you want to enable, then click **Save**.

Enable outbreak response Check for an outbreak DAT file every hour.

Enable buffer overflow protection Detect code starting to run from data in reserved memory and prevent that code from running. This feature protects against buffer overflow in more than 30 most commonly used Windows-based programs. SonicWALL updates this list as it adds buffer overflow protection for additional programs.

Important: Buffer overflow protection does not stop data from being written. Do not rely on the exploited application remaining stable after being compromised, even if buffer overflow protection stops the corrupted code from running.

Enable script scanning Detect harmful code embedded in web pages that could cause unauthorized programs to run on client computers.

Scan email (before delivering to the Outlook Inbox) Detect viruses and harmful code in email messages before they are placed in the user’s Inbox.

Scan all file types during on-access scans Inspect all types of files, instead of only default types, when they are downloaded, opened, or run. (Default file types are defined in the DAT files.)

Scan within archives during on-access scans (e.g., .zip, .rar, .tat, .tgz) Detect viruses and harmful code in compressed archive files (such as .ZIP files) during on-demand scheduled or **Scan Now** scans.

Scan within archives during on-demand scans (e.g., .zip, .rar, .tat, .tgz) Detect viruses and harmful code in compressed archive files (such as .ZIP files) as they are saved, uncompressed, or opened.

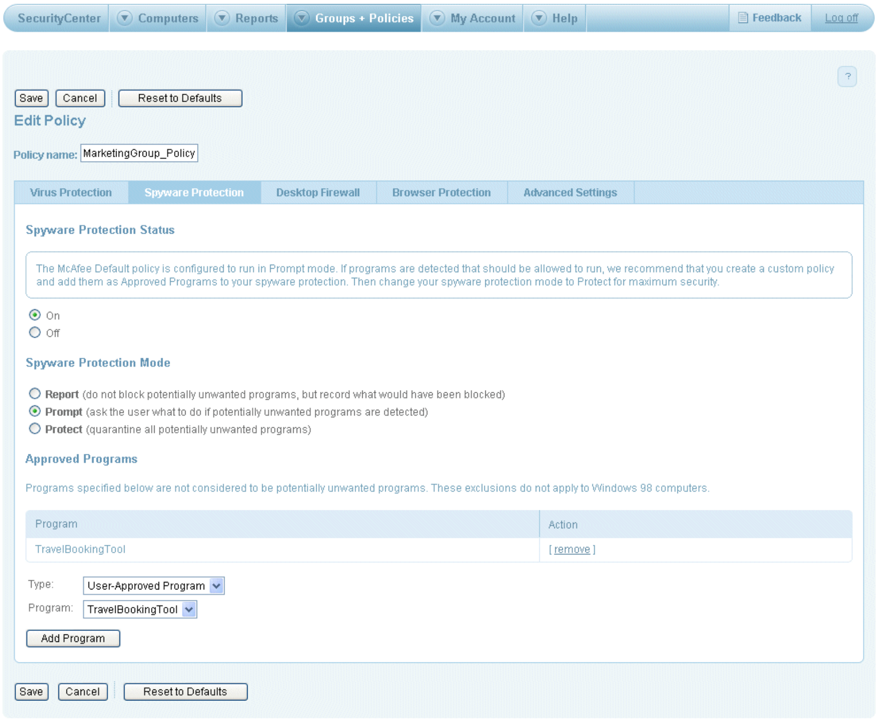
> With the default settings, it is possible for an on-demand scan to detect threats in archived files that are not detected during an on-access scan. This is because on-access scans do not look at compressed archives by default. If this is a concern for your organization, you should enable this option.

Set basic spyware protection options

On the **Groups + Policies** page, use the **Spyware Protection** tab to configure basic settings for spyware protection.

- *Enable spyware protection*
- *Select a spyware protection mode*
- *Specify approved programs*

Figure 4-5 Spyware Protection policy tab



Edit Policy

Policy name: MarketingGroup_Policy

Spyware Protection Status

The McAfee Default policy is configured to run in Prompt mode. If programs are detected that should be allowed to run, we recommend that you create a custom policy and add them as Approved Programs to your spyware protection. Then change your spyware protection mode to Protect for maximum security.

● On
○ Off

Spyware Protection Mode

○ **Report** (do not block potentially unwanted programs, but record what would have been blocked)
● **Prompt** (ask the user what to do if potentially unwanted programs are detected)
○ **Protect** (quarantine all potentially unwanted programs)

Approved Programs

Programs specified below are not considered to be potentially unwanted programs. These exclusions do not apply to Windows 98 computers.

Program	Action
TravelBookingTool	[remove]

Type: User-Approved Program
Program: TravelBookingTool

Enable spyware protection

You can specify whether the virus and spyware protection service looks for spyware and other potentially unwanted programs during scans. By default, this option is enabled.

To enable and disable spyware protection:

1 On the **Groups + Policies** page, click **Add Policy** (or click **Edit** to modify an existing policy).

2 Click the **Spyware Protection** tab.

3 For **Spyware Protection Status**, select **On** or **Off**, then click **Save**.

Select a spyware protection mode

You can specify how the virus and spyware protection service responds to detections of potentially unwanted programs on client computers.

- **Protect**: It attempts to clean the detected item. If the item cannot be cleaned, a copy of the item is placed in a quarantine folder and the original item is deleted.
- **Prompt**: It displays a dialog box with information about the detection, and allows the user to select a course of action. This option is the default.
- **Report**: It reports detections to the SecurityCenter and takes no additional action.

For all modes, detections are reported to the SecurityCenter, where you can view information about them in reports.

To prevent popup prompts from appearing on client computers when threats are detected, and for highest security, we recommend using **Protect** mode.

To specify a response to potentially unwanted program detections:

1 On the **Groups + Policies** page, click **Add Policy** (or click **Edit** to modify an existing policy).

2 Click the **Spyware Protection** tab, select a **Spyware Protection Mode**, then click **Save**.

Use the following table to determine how policy options are implemented in the different protection modes.

Mode	Behavior of protection service
Report	■ No user prompts. ■ Detections reported to SecurityCenter. ■ Administrator can select approved programs, which are not reported as detections. ■ Can be used as a *Learn mode*.
Prompt	■ Users prompted about detections. ■ Detections reported to SecurityCenter. ■ Administrator can select approved programs. These programs are not reported as detections, and users are not prompted for a response to them. ■ Users can approve additional programs in response to prompts. These are reported to SecurityCenter.
Protect	■ Users not prompted about detections. ■ Users notified about deleted or quarantined programs. ■ Detections reported to SecurityCenter. ■ Administrator can select approved programs. These programs are not reported as detections.

If the policy is changed from **Prompt** mode to **Protect** mode or **Report** mode, the virus and spyware protection service saves user settings for approved programs. If the policy is then changed back to **Prompt** mode, these settings are reinstated.

Learn mode

Report mode can be used as a "learn mode" to help you determine which programs to approve (see *Specify approved programs* on page 101). In **Report** mode, the virus and spyware protection service tracks but does not delete unrecognized programs. You can review detected programs in the **Unrecognized Programs** report (see *View unrecognized programs* on page 105) and approve those that are appropriate for your policy. When you no longer see programs you want to approve in the report, change the policy setting to **Prompt** or **Protect** mode.

Specify approved programs

On client computers, the virus and spyware protection service maintains a list of *approved programs* that are not identified as potentially unwanted programs. You can configure the list of approved programs for all computers using a policy. In addition, users can approve programs for individual client computers when the firewall protection service is set to **Prompt** mode.

> Exclude only programs you know are safe. If you are unsure about a program, we recommend not adding it to the approved programs list.

To configure approved programs in a policy:

1 On the **Groups + Policies** page, click **Add Policy** (or click **Edit** to modify an existing policy).

2 Click the **Spyware Protection** tab.

3 Under **Approved Programs**, select the type of program (a detected program or a user-approved program).

4 Select a program, then click **Save**.

The selected program is added to the list of allowed programs. (No list appears until you have added at least one approved program to the policy.)

> Use the **Unrecognized Programs** report to view a complete listing of all programs detected on client computers.

To remove an approved program from a policy:

1 On the **Groups + Policies** page, click **Add Policy** (or click **Edit** to modify an existing policy).

2 Click the **Spyware Protection** tab.

3 In the list of **Approved Programs**, click **remove** for each program you want to delete from the list, then click **Save**.

Set advanced spyware protection options

On the **Groups + Policies** page, use the **Advanced Settings** tab to select the types of potentially unwanted programs to search for during scans.

Threat type	Description
Jokes	Programs designed to be mistaken for a virus. They might alarm or annoy a user but do not harm files or data. They are intended to waste time and resources.
Remote admin tools	Programs that can be used from a remote location to access a computer. Some remote administration tools serve useful purposes, such as allowing users to access their files from home, but others can be used by unauthorized persons to monitor user activities and take control of a computer.

Threat type	Description
Spyware	Programs that covertly gather user information through the user’s Internet connection without the user’s knowledge. Once installed, spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can gather information such as email addresses, websites visited, passwords, and credit card numbers.
Dialers	Programs that hijack a user’s modem and dial premium-rate phone numbers, such as those required to access pornographic websites.
Password crackers	Programs that find passwords or encryption keys by trying every possible combination of characters until the code is broken.
Adware	Programs that display unsolicited advertisements. Adware often includes code that tracks a user's personal information and transmits it to someone else, without the user's knowledge.
Potentially unwanted programs	Programs such as viruses, worms, and Trojan horses that perform some unauthorized (and often harmful or undesirable) act.
Key loggers	Programs that record every keystroke a user makes. They can be used to steal passwords and other confidential information.

To specify programs to detect:

1. On the **Groups + Policies** page, click **Add Policy** (or click **Edit** to modify an existing policy).
2. Click the **Advanced Settings** tab.
3. Select each type of program you want to detect, then click **Save**.

Viewing reports for virus and spyware detections

Whenever a client computer checks for updates, it also sends data to the SecurityCenter in encrypted XML files. You can view this data in reports accessed from the **Reports** page. Three reports contain information about virus or spyware detections:

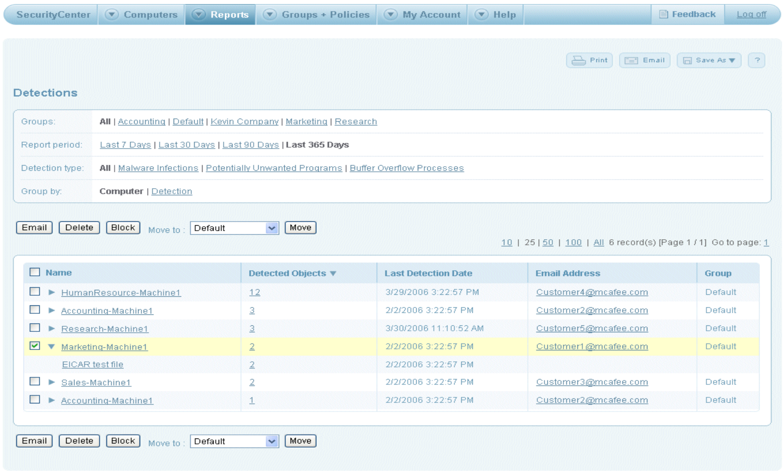
- **Detections** (see *View detections*).
- **Unrecognized Programs** (see *View unrecognized programs* on page 105).
- **Detection History** (see *View your detection history* on page 107).

View detections

Use the **Detections** report to view and manage the types of potentially malicious code or unwanted programs that have been found on your network.

> Specify the types of unwanted programs the virus and spyware protection service will detect in a policy (see *Set advanced spyware protection options* on page 102).

Figure 4-6 Detections report



Detections

Groups:	**All** | Accounting | Default | Kevin Company | Marketing | Research
Report period:	Last 7 Days | Last 30 Days | Last 90 Days | **Last 365 Days**
Detection type:	**All** | Malware Infections | Potentially Unwanted Programs | Buffer Overflow Processes
Group by:	**Computer** | Detection

Email Delete Block Move to : Default Move

10 | 25 | 50 | 100 | All 6 record(s) [Page 1 / 1] Go to page: 1

□ Name	Detected Objects ▼	Last Detection Date	Email Address	Group
□ ▶ HumanResource-Machine1	12	3/29/2006 3:22:57 PM	Customer4@mcafee.com	Default
□ ▶ Accounting-Machine1	3	2/2/2006 3:22:57 PM	Customer2@mcafee.com	Default
□ ▶ Research-Machine1	3	3/30/2006 11:10:52 AM	Customer5@mcafee.com	Default
☑ ▼ Marketing-Machine1	2	2/2/2006 3:22:57 PM	Customer1@mcafee.com	Default
EICAR test file	2	2/2/2006 3:22:57 PM		
□ ▶ Sales-Machine1	2	2/2/2006 3:22:57 PM	Customer3@mcafee.com	Default
□ ▶ Accounting-Machine1	1	2/2/2006 3:22:57 PM	Customer2@mcafee.com	Default

Email Delete Block Move to : Default Move

Select the information that appears in this report:

Groups — Display only the computers in a group or display all computers.

Report period — Specify the length of time for which to display information.

Detection type — Show all threat detections or a particular type:

Malware Infections Known threats that would infect your computer if they were not caught.

Potentially Unwanted Programs Programs that you defined as unwanted. Configure the types of programs on the **Advanced Settings** tab (see *Set advanced spyware protection options* on page 102).

Buffer Overflow Processes Unwanted code that attempted to run in reserved memory but was stopped.

Group by — List detections by the computer where they occurred or by the name of the detection.

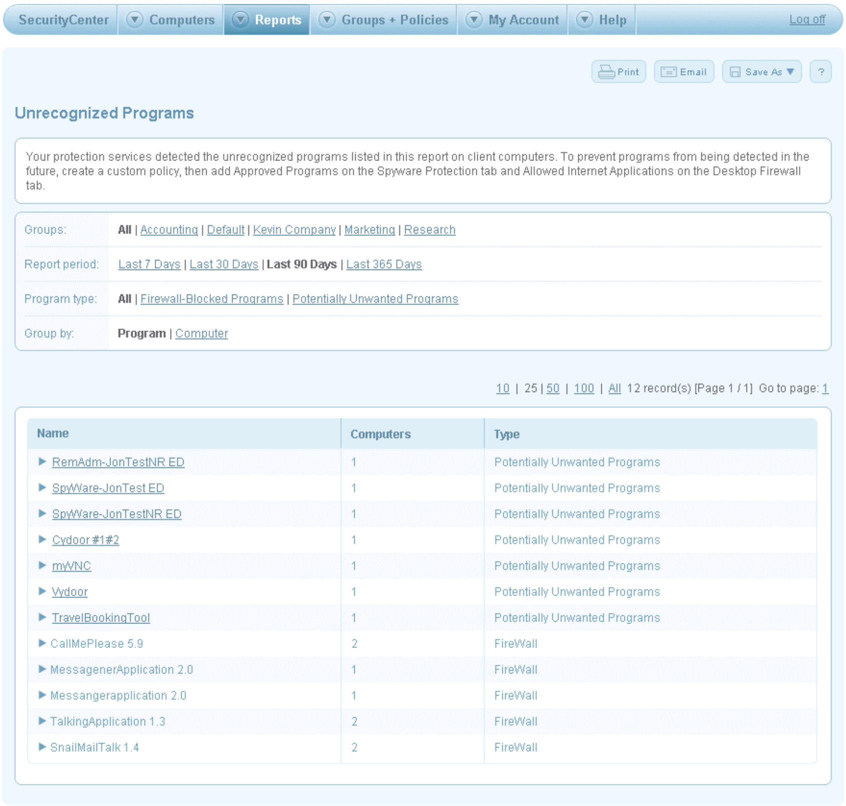
Using the Detections report

When you want to...	**Do this...**
	Click ▶ next to a name: ■ Under a computer name, show which detections were found. ■ Under a detection name, show the computers where it was found.
View details about detections	If detections are listed for a computer, click a quantity to display details. 1 On the **Detections** report, click a quantity for **Detected Objects** to display a list of detected threats and their status. 2 From the **Detection List**, click the name of a detection to display detailed information from the SonicWALL Avert Labs Threat Library.
	On the **Detections** report, click a computer name to display the **Computer Details** page. The **Computer Details** page displays information about the computer, its service components, and its detections (see *Display details for a computer* on page 67).

View unrecognized programs

Use the **Unrecognized Programs** report to view a list of unapproved programs that the spyware protection service or firewall protection service detected on your network.

Figure 4-7 Unrecognized Programs report



Unrecognized Programs

Your protection services detected the unrecognized programs listed in this report on client computers. To prevent programs from being detected in the future, create a custom policy, then add Approved Programs on the Spyware Protection tab and Allowed Internet Applications on the Desktop Firewall tab.

Groups:	**All** | Accounting | Default | Kevin Company | Marketing | Research
Report period:	Last 7 Days | Last 30 Days | **Last 90 Days** | Last 365 Days
Program type:	**All** | Firewall-Blocked Programs | Potentially Unwanted Programs
Group by:	**Program** | Computer

10 | 25 | 50 | 100 | All 12 record(s) [Page 1 / 1] Go to page: 1

Name	Computers	Type
▶ RemAdm-JonTestNR ED	1	Potentially Unwanted Programs
▶ SpyWare-JonTest ED	1	Potentially Unwanted Programs
▶ SpyWare-JonTestNR ED	1	Potentially Unwanted Programs
▶ Cydoor #1#2	1	Potentially Unwanted Programs
▶ myVNC	1	Potentially Unwanted Programs
▶ Vydoor	1	Potentially Unwanted Programs
▶ TravelBookingTool	1	Potentially Unwanted Programs
▶ CallMePlease 5.9	2	FireWall
▶ MessagenerApplication 2.0	1	FireWall
▶ Messangerapplication 2.0	1	FireWall
▶ TalkingApplication 1.3	2	FireWall
▶ SnailMailTalk 1.4	2	FireWall

Select the information that appears in this report:

Groups — Display only the computers in a group or display all computers.

Report period — Specify the length of time for which to display information.

Program type — Show all unrecognized programs, only programs blocked by the firewall protection service, or only potentially unwanted programs.

Group by — List unrecognized programs by the computer where they were detected or by the name of the program.

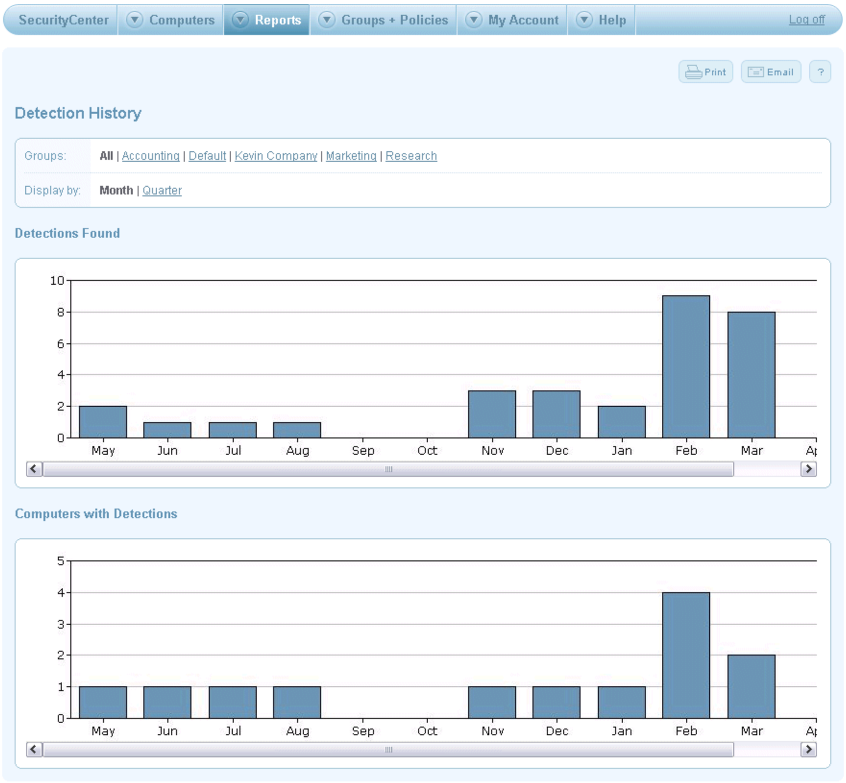
Using the Unrecognized Programs report

When you want to...	Do this...
Display computers or detections	Click ▶ next to a name: ■ Under a computer name, show which detections were found. ■ Under a detection name, show the computers where it was found.
View details about detections	On the **Unrecognized Programs** report, click the name of a potentially unwanted program to display detailed information from the SonicWALL Avert Labs Threat Library.
View details about a computer where a detection occurred	On the **Unrecognized Programs** report, click a computer name to display the **Computer Details** page. The **Computer Details** page displays information about the computer, its service components, and its detections (see *Display details for a computer* on page 67).
Approve a program	To add unrecognized programs to the list of approved programs for other users, add them to a new or existing policy (see *Specify approved programs* on page 101). Approved programs will no longer be detected as a threat by the virus and spyware protection service on computers using the policy.

View your detection history

Check the **Detection History** report for a graphical overview of the number of detections and the number of computers where detections occurred over the past year on your network. This information can help you determine how successfully your protection services have performed, and whether strategies you have implemented such as user education or policy adjustments have been effective.

Figure 4-8 Detection History report



Detection History

Groups: All | Accounting | Default | Kevin Company | Marketing | Research

Display by: Month | Quarter

Detections Found

Computers with Detections

Select the information that appears in this report:

Groups — Display only the computers in a group or display all computers.

Display by — Display information for the last year in monthly or quarterly increments.

Managing detections

To effectively manage your strategy for virus and spyware protection, we recommend that you proactively track the types of threats being detected and where they are occurring.

- *Manage your protection strategy with best practices*
- *Manage quarantined files*
- Manage potentially unwanted program detections (see *Scan for spyware* on page 93)

Manage your protection strategy with best practices

1. Check your status emails or the SecurityCenter website for an overview of your account's status. (See *Sign up for email notifications* on page 62 to request status emails.)
   - Ensure that your computers are up-to-date.
   - Ensure that protection services are installed on all computers.
2. Check the **Detections** report and **Unrecognized Programs** report regularly to see what is being detected (see *View detections* on page 103 and *View unrecognized programs* on page 105).
3. Check the **Unrecognized Programs** report frequently to monitor the programs that users are allowing on client computers.
4. To centralize management and more easily monitor the types of programs allowed on client computers, define client security settings in a policy.
5. If particular types of detections are occurring frequently or certain computers appear vulnerable, update the policy to resolve these issues.
   - Schedule scans or add exclusions (see *Set basic virus protection options* on page 95).
   - Enable advanced scanning options (see *Set advanced virus protection options* on page 97).
   - Ensure that spyware protection is enabled (see *Set basic spyware protection options* on page 99).
   - For maximum protection, set your spyware protection to **Protect** mode to automatically clean potentially unwanted programs (see *Set basic spyware protection options* on page 99).

   Protect mode is not the default setting. For maximum protection, create a policy that includes **Protect** mode.

   - Enable all advanced spyware options (see *Set advanced spyware protection options* on page 102).
6. Use "learn" mode to identify which programs to add to the **Approved Programs** list, (see *Learn mode* on page 101). This ensures that no required programs are deleted before you have the opportunity to authorize their use. Then change your protection mode to **Protect**.
7. View the **Detection History** report periodically to discover trends specific to your network, and verify your strategy's success in reducing detections.

Manage quarantined files

When the virus and spyware protection service detects a threat on a client computer, it attempts to clean the item where the threat is detected. The item might be a file, cookie, or registry key.

- If it cannot clean the item, it deletes the original item and places an encrypted copy in a quarantine folder.
- If it can clean the item, it places an encrypted copy of the original detected item in a quarantine folder. This copy serves as a backup.

Once quarantined, these items pose no threat to client computers. It is not necessary to view or delete them, but you might occasionally want to do so. In these situations, you must view the files on the client computer using the **Quarantine Viewer**.

> Files are placed into the **Quarantine Viewer** in a format that is no longer a threat to the client computer. After 30 days, these files are deleted. Only users with administrator rights can access the **Quarantine Viewer**.

To check quarantined files:

1 On the client computer, hold down the **Ctrl** and **Shift** keys and click M in the system tray.

2 Select **Scan Tasks | Quarantine Viewer**.

The **Quarantine Viewer** lists all the items in the quarantine folder and their status.

3 Select one or more items, then click an action:

Rescan Scan each selected item again. This option is useful when new detection definition (DAT) files include a method of cleaning a detection that could not be cleaned previously. In this case, rescanning the file cleans it and allows you to restore it for normal use.

Restore Place each selected item back in its original location on the computer. The restored item will overwrite any other items with the same name in that location.

Note: The virus and spyware protection service detected this item because it considers the item to be a threat. Do not restore the item unless you are sure it is safe.

Delete Remove each selected item from the quarantine folder, along with all associated registry keys and cookies. No copy will remain on the computer.

4 Check the status of each item:

Cleaned The rescan action was successful. You can safely restore the item.

Clean failed The item cannot be cleaned.

Delete failed The item cannot be cleaned or deleted. If it is in use, close it and attempt the clean again. If it resides on read-only media, such as CD, no further action is required. The virus and spyware protection service has prevented the original item from accessing the computer, but it cannot delete the item. Any items copied to the computer have been cleaned.

Note: If you are not sure why the item could not be cleaned, it is possible that a risk still exists.

Quarantined You have not performed any action on this item since it was placed in the quarantine folder.

5 Click **OK** to close the **Quarantine Viewer**.

Disabling on-access scanning

Temporarily disabling the automatic on-access scanner on client computers can be useful when working with product support to troubleshoot issues with scanning and cleaning files.

> The computer is vulnerable to attack if you disable the on-access scanning feature. Be sure to enable the feature again as soon as possible.

To disable and enable on-access scans:

1 On the client computer, hold down the **Ctrl** and **Shift** keys and click M in the system tray.

2 Select **Disable On-Access Scanner** or **Enable On-Access Scanner**.

> Only on-access scanning is disabled. Buffer overflow protection continues to function. To disable buffer overflow protection, you must update the policy (see *Set advanced virus protection options* on page 97).

5 Using the Firewall Protection Service

The firewall protection service in Enforced Client safeguards against intrusions by monitoring inbound and outbound communications on client computers. It checks:

- IP addresses and communication ports that attempt to communicate with your computer.
- Applications that attempt to access the Internet.

As the administrator, you can define what constitutes suspicious activity and the firewall protection service's response. You can specify specific IP addresses, reports, and applications to allow or to block. By defining firewall protection settings in a policy, you can centrally manage the firewall protection service for your organization.

If you prefer a more hands-off approach, you can allow users to decide which communications and applications the firewall protection service allows.

This section describes these features of the firewall protection service:

- *Accessing client features (Firewall Settings command)*
- *Configuring policies for firewall protection*
- *Viewing reports for firewall protection*
- *Managing suspicious activity with best practices*

Accessing client features (Firewall Settings command)

Use the client menu to access client features of the firewall protection service.

To display firewall settings:
On client computers, click M in the system tray and select **Firewall Settings**:

- On computers where the policy does not allow users to configure settings, a summary of current settings is displayed.
- On computers where the policy does allow users to configure settings, a dialog box with configuration options is displayed.

Client procedures for configuring firewall settings are documented in the *User Help* on the client computer.

Configuring policies for firewall protection

Policies define the operational settings for all your protection services. See *Setting up policies* on page 75 for general information about using policies.

See *The SonicWALL Default policy* on page 76 for a table listing the firewall protection settings in the **SonicWALL Default** policy.

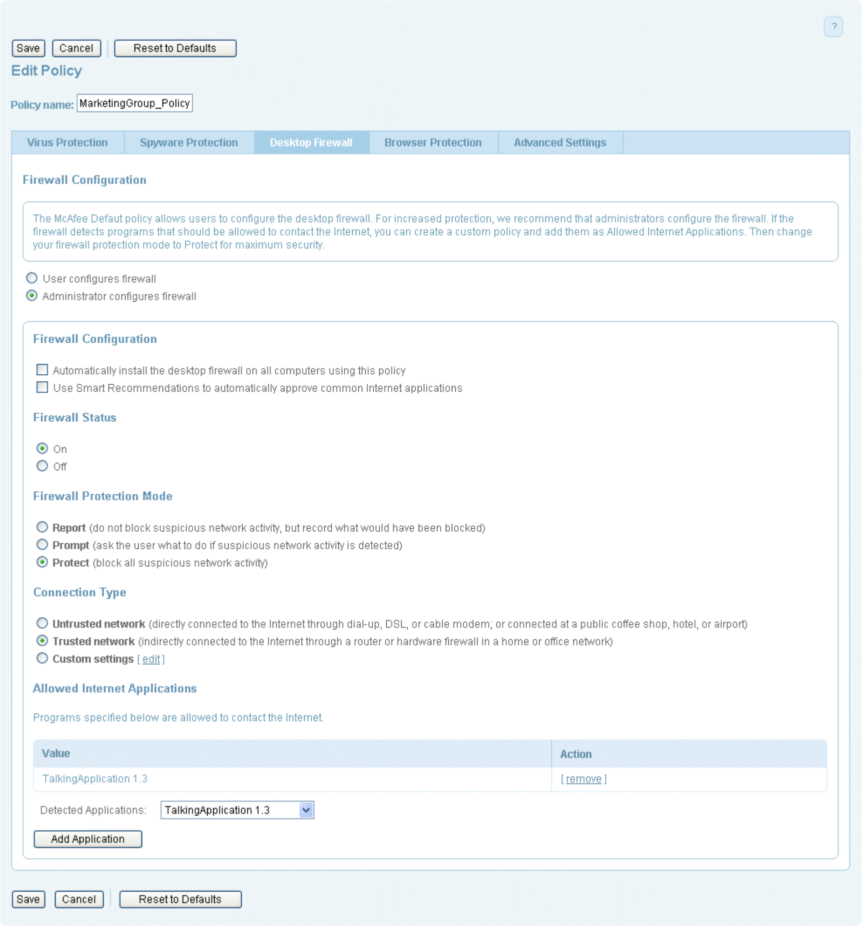
By default, users configure their own firewall protection settings. When you set up a policy, you can specify whether to allow users to change their settings.

> For maximum protection, we recommend that you configure firewall protection settings. If users change their settings, we recommend that you review their changes regularly. It is important that mobile users who connect to both secure (trusted) and unsecure (untrusted) networks be able to update the settings as their location changes.

On the **Groups + Policies** page, use the **Desktop Firewall** tab to configure basic settings for the firewall protection service.

- *Specify who configures firewall protection settings*
- *Install the firewall protection service via policy*
- *Enable firewall protection*
- *Select a firewall protection mode*
- *Specify a connection type*
- *Set up allowed Internet applications*
- *Specify whether to use SonicWALL recommendations*

Figure 5-1 Desktop Firewall policy tab



Edit Policy

Policy name: MarketingGroup_Policy

Firewall Configuration

The McAfee Defaut policy allows users to configure the desktop firewall. For increased protection, we recommend that administrators configure the firewall. If the firewall detects programs that should be allowed to contact the Internet, you can create a custom policy and add them as Allowed Internet Applications. Then change your firewall protection mode to Protect for maximum security.

○ User configures firewall
● Administrator configures firewall

Firewall Configuration

□ Automatically install the desktop firewall on all computers using this policy
□ Use Smart Recommendations to automatically approve common Internet applications

Firewall Status

● On
○ Off

Firewall Protection Mode

○ **Report** (do not block suspicious network activity, but record what would have been blocked)
○ **Prompt** (ask the user what to do if suspicious network activity is detected)
● **Protect** (block all suspicious network activity)

Connection Type

○ **Untrusted network** (directly connected to the Internet through dial-up, DSL, or cable modem; or connected at a public coffee shop, hotel, or airport)
● **Trusted network** (indirectly connected to the Internet through a router or hardware firewall in a home or office network)
○ **Custom settings** [edit]

Allowed Internet Applications

Programs specified below are allowed to contact the Internet.

Value	Action
TalkingApplication 1.3	[remove]

Detected Applications: TalkingApplication 1.3

Specify who configures firewall protection settings

Configuring settings for the firewall protection service enables you to control which applications and communications are allowed on your network. It provides the means for you to ensure the highest level of security.

You can also allow users to configure their own firewall protection settings. In this case, no other options are available on this tab for you to select.

To specify who configures firewall settings:

1 On the **Groups + Policies** page, click **Add Policy** (or click **Edit** to modify an existing policy).

2 Click the **Desktop Firewall** tab.

3 Under **Firewall Configuration**, select **Administrator configures firewall** or **User configures firewall**, then click **Save**.

> To ensure the highest level of security, we recommend that administrators configure firewall protection. If you allow users to configure the settings, it is important to educate them about threats and strategies for avoiding intrusions.

How do user settings and administrator settings coexist?
When you select **Administrator configures firewall**, any firewall settings that users have configured on their computers are saved.

- If you also select **Prompt** mode, user settings are merged with your policy settings on each client computer. When they differ, user settings take precedence over administrator settings.
- If you select **Protect** mode or **Report** mode, user settings become inactive.

Saved settings configured by users become active again only when you reconfigure the policy for **Prompt** mode or **User configures firewall**.

Install the firewall protection service via policy

Use this option to install the firewall protection service automatically whenever client computers check for an updated policy. You might want to use this feature for adding the firewall protection service on computers where the Enforced Client client software is already installed. By default, this option is disabled.

> ! Enabling this feature can result in unattended installations on computers where no one is available to authorize communications that are consequently blocked by the firewall. If this feature is used to install the firewall protection service on a server, it is important to configure essential system services first, to prevent disruptions.

To install the firewall protection service via policy:

1. On the **Groups + Policies** page, click **Add Policy** (or click **Edit** to modify an existing policy).
2. Click the **Desktop Firewall** tab.
3. Under **Firewall Configuration**, select **Automatically install the desktop firewall on all computers using this policy**, then click **Save**.

Enable firewall protection

Specify whether the firewall protection service monitors inbound communications and Internet applications. By default, this feature is enabled.

To enable the firewall protection service:

1. On the **Groups + Policies** page, click **Add Policy** (or click **Edit** to modify an existing policy).
2. Click the **Desktop Firewall** tab.
3. Under **Firewall Status**, select **On**, then click **Save**.

Select a firewall protection mode

Specify how the firewall protection service responds to suspicious activity on client computers.

- **Protect**: It blocks the suspicious activity.
- **Prompt**: It displays a dialog box with information about the detection, and allows the user to select a response. This option is the default.
- **Report**: It reports suspicious activity to the SecurityCenter and takes no additional action.

For all modes, detections are reported to the SecurityCenter, where you can view information about them in reports.

To prevent popup prompts from appearing on client computers when applications are detected, and for highest security, we recommend using **Protect** mode.

To specify a response to firewall detections:

1 On the **Groups + Policies** page, click **Add Policy** (or click **Edit** to modify an existing policy).

2 Click the **Desktop Firewall** tab, select a **Firewall Protection Mode**, then click **Save**.

Use the following table to determine how policy options are implemented in the different protection modes.

Mode	Behavior of protection service
Report	■ No user prompts. ■ Detections reported to SecurityCenter. ■ Administrator can select allowed applications, which are not reported as detections. ■ Can be used as a *Learn mode*.
Prompt	■ Users prompted about detections. ■ Detections reported to SecurityCenter. ■ Administrator can select allowed applications. These applications are not reported as detections, and users are not prompted for a response to them. ■ Users can approve additional applications in response to prompts. These are reported to SecurityCenter.
Protect	■ Users not prompted about detections. ■ Users notified about deleted or quarantined applications. ■ Detections reported to SecurityCenter. ■ Administrator can select allowed applications. These applications are not reported as detections.

If the policy is changed from **Prompt** mode to **Protect** mode or **Report** mode, the firewall protection service does not save user settings for allowed applications. If the policy is then changed back to **Prompt** mode, users need to specify allowed applications again.

Learn mode

Report mode can be used as a "learn mode" to help you determine which applications to allow (see *Set up allowed Internet applications* on page 121). In **Report** mode, the firewall protection service tracks but does not block unrecognized Internet applications. You can review detected applications in the **Unrecognized Programs** report (see *View unrecognized Internet applications* on page 123) and approve those that are appropriate for your policy. When you no longer see applications you want to allow in the report, change the policy setting to **Prompt** or **Protect** mode.

Specify a connection type

The connection type defines the environment where client computers are used and determines which IP addresses and ports the firewall protection service allows to communicate with them. This option defines what the firewall protection service considers to be suspicious activity. The default setting is **Untrusted**.

> ❗ For client computers used in multiple environments, it is important to update the connection type whenever the working environment changes. For example, mobile users who connect to both secure (trusted) and unsecure (untrusted) networks must be able to change their setting accordingly.

Select from three connection environments:

Select this...	When the computer...	Then the firewall service...
	Is connected directly to the Internet. For example: through a dial-up connection, a DSL line, or a cable modem; through any type of connection in a coffee shop, hotel, or airport.	Blocks communications with all other computers, including those on the same subnet.
Trusted	Is connected indirectly to a network that is separated from the Internet by a hardware router or firewall. For example: in a home or office network.	Allows communications with other computers on the same subnet, but blocks all other network communications.
Custom	Should communicate only through specific ports or with a specific range of IP addresses, or the computer is a server providing system services. You also need to configure additional options (see *Configure a custom connection* on page 117).	Allows communications only with the ports and IP addresses you specify, and blocks all other network communications.

> ℹ This feature does not affect Internet applications running on client computers. To configure Internet applications, see *Set up allowed Internet applications* on page 121.

To specify a connection type:

1 On the **Groups + Policies** page, click **Add Policy** (or click **Edit** to modify an existing policy).

2 Click the **Desktop Firewall** tab, select a **Connection Type**, then click **Save**.

Configure a custom connection

Configure a custom connection type to designate:

- Ports through which your computer can receive communications. This is required to set up your computer as a server that provides system services. Your computer will accept communications through any open port from any computer.
- IP addresses from which your computer can receive communications. This allows you to limit communications to specific IP addresses.

From the **Firewall Custom Settings** page, you can define exactly which communications the firewall protection service allows:

- *Configure system services for a custom connection*

- *Configure IP addresses for a custom connection*

Custom settings configured on the SecurityCenter are ignored on client computers if the **Firewall Protection Mode** is set to **Prompt** mode. In **Prompt** mode, settings configured by users override administrator settings.

Configure system services for a custom connection

Certain applications, including web servers and file-sharing server programs, must accept unsolicited connections from other computers through designated system service ports. When configuring a custom operating mode, you can:

- Allow applications to act as servers on the local network or the Internet.
- Add or edit a port for a system service.
- Disable or remove a port for a system service.

Select a port for system services only if you are certain it must be open. You will rarely need to open a port. we recommend that you disable unused system services.

Examples of system services that typically require ports to be opened are:

Email server — You do not need to open a mail server port to receive email. You need to open a port only if the computer running the firewall protection service acts as an email server.

Web server — You do not need to open a web server port to run a web browser. You need to open a port only if the computer running the firewall protection service acts as a web server.

An opened service port that does not have an application running on it poses no security threat.

This section explains the following concepts and tasks relevant to configuring service ports:

- *Standard system service ports*
- *Open a service port*
- *Add and edit service ports*
- *Close a service port*

Standard system service ports

System services communicate through *ports*, which are logical network connections. Common Windows system services are typically associated with particular *service ports*, and your computer’s operating system or other system applications might attempt to open them. Because these ports represent a potential source of intrusions into a client computer, you must open them before the computer can communicate through them.

These commonly used standard service ports are listed by default on the **Firewall Custom Settings** page, where you can open or close them:

- File and Print Sharing
- Remote Desktop

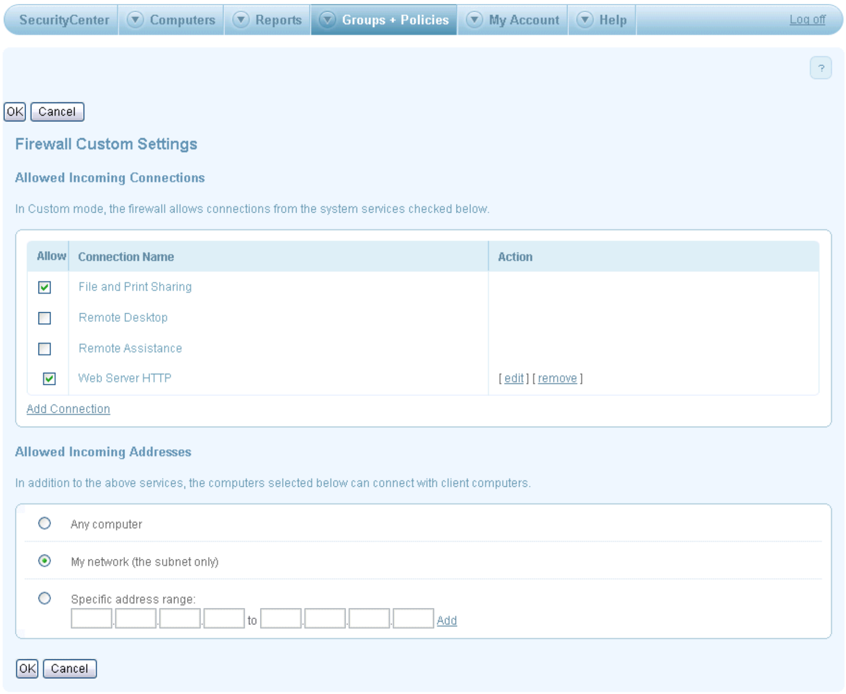
- Remote Assistance

You can add other service ports as needed. Standard service ports for typical system services are:

- File Transfer Protocol (FTP) Ports 20-21
- Mail Server (IMAP) Port 143
- Mail Server (POP3) Port 110
- Mail Server (SMTP) Port 25
- Microsoft Directory Server (MSFT DS) Port 445
- Microsoft SQL Server (MSFT SQL) Port 1433
- Remote Assistance / Terminal Server (RDP) Port 3389 (same as *Remote Assistance* and *Remote Desktop*)
- Remote Procedure Calls (RPC) Port 135
- Secure Web Server (HTTPS) Port 443
- Universal Plug and Play (UPNP) Port 5000
- Web Server (HTTP) Port 80
- Windows File Sharing (NETBIOS) Ports 137-139 (same as *File and Print Sharing*)

To ensure that a port is blocked, you must add it to this list and make sure it is deselected.

Figure 5-2 Firewall Custom Settings page



Firewall Custom Settings

Allowed Incoming Connections

In Custom mode, the firewall allows connections from the system services checked below.

Allow	Connection Name	Action
☑	File and Print Sharing	
□	Remote Desktop	
□	Remote Assistance	
☑	Web Server HTTP	[edit] [remove]

Add Connection

Allowed Incoming Addresses

In addition to the above services, the computers selected below can connect with client computers.

○ Any computer

● My network (the subnet only)

○ Specific address range:
□.□.□.□ to □.□.□.□ Add

Open a service port

Opening a system service port on a client computer allows it to act as a server on the local network or the Internet.

To open a service port:

1 On the **Groups + Policies** page, click **Add Policy** (or click **Edit** to modify an existing policy).

2 Click the **Desktop Firewall** tab.

3 Under **Connection Type**, select **Custom settings**, then click **edit**.

4 On the **Firewall Custom Settings** page, select the checkbox next to the service port(s) you want to open, then click **Save**. Client computers using this policy will accept all communications through these ports.

5 On the **Desktop Firewall** tab, click **Save**.

! Select a port in the **Allowed Incoming Connections** list only if you are sure it must be open.

Add and edit service ports

If a service port does not appear in the **Allowed Incoming Connections** list, you need to add it to the list manually.

To add or edit a system service:

1 On the **Groups + Policies** page, click **Add Policy** (or click **Edit** to modify an existing policy).

2 Click the **Desktop Firewall** tab.

3 Under **Connection Type**, select **Custom settings**, then click **edit**.

4 On the **Firewall Custom Settings** page, click **Add Connection**, or select an existing service and click **edit**.

5 On the **Add or Edit Incoming Connection** page, specify the service name.

6 Specify the port(s) through which this service will communicate, then click **OK**.

7 On the **Firewall Custom Settings** page, select the checkbox next to the service, then click **OK**.

8 On the **Desktop Firewall** tab, click **Save**.

Close a service port

If you are not sure that a service port needs to be open, or when you stop using a service, we recommend that you close the port to prevent intrusions.

To close a service port:

1 On the **Groups + Policies** page, click **Add Policy** (or click **Edit** to modify an existing policy).

2 Click the **Desktop Firewall** tab.

3 Under **Connection Type**, select **Custom settings**, then click **edit**.

4 On the **Firewall Custom Settings** page, for the port you want to close, click **remove**, then click **OK**.

5 On the **Desktop Firewall** tab, click **Save**.

Configure IP addresses for a custom connection

In addition to accepting communications through the selected service ports, client computers accept communications originating from designated IP addresses.

To add one or more IP addresses:

1. On the **Groups + Policies** page, click **Add Policy** (or click **Edit** to modify an existing policy).
2. Click the **Desktop Firewall** tab.
3. Under **Connection Type**, select **Custom settings**, then click **edit**.
4. On the **Firewall Custom Settings** page, select which IP addresses can communicate with client computers:

   Any computer All IP addresses.

   My network All computers with IP addresses on your local network.

   Specific address range Only computers with IP addresses specified here. When you select this option, you must specify an address range and click **Add**. Address ranges that you enter appear in an **Allowed IP Address Range** table.

> When using a computer in multiple locations, you might want to specify more than one range of IP addresses. For example, you might want one IP address range for office use and another for home use. To specify multiple address ranges, repeat step 4, enter another address range, then click **Add** again.

5. Click **OK**.
6. On the **Desktop Firewall** tab, click **Save**.

To remove a range of IP addresses:

1. Click M in the system tray, then select **Firewall Settings**.
2. Click the **Desktop Firewall** tab.
3. Under **Connection Type**, select **Custom settings**, then click **edit**.
4. On the **Firewall Custom Settings** page, under **Allowed IP Address Range**, click **remove** for each range you want to delete from the list, then click **OK**.
5. On the **Desktop Firewall** tab, click **Save**.

Set up allowed Internet applications

The firewall protection service monitors communications with Internet applications, which connect to the Internet and communicate with client computers. When it detects an Internet application running on a computer, it allows the application to connect to the Internet or blocks the connection. Its response is based on these factors in this order:

1. A policy-specific list of *allowed Internet applications* created by the administrator. The administrator creates this list as part of a policy, then assigns the policy to groups of computers (see *Specify Internet applications in a policy*).

2 A list of safe applications that SonicWALL maintains on the www.hackerwatch.org website. By default, the firewall protection service allows applications that appear on this list. If the administrator does not want the firewall protection service to consult this list, he can configure a policy option (see *Specify whether to use SonicWALL recommendations*).

3 A computer-specific list of allowed Internet applications created by user responses to detection prompts. Users are prompted for a response to application detections when their policy is configured for **Prompt** mode (see *Select a firewall protection mode* on page 115).

Specify Internet applications in a policy

When you authorize Internet applications in a policy, the firewall protection service allows the applications to connect to the Internet whenever they run on computers using the policy.

> Authorize only applications you know are safe. If you are unsure an application is safe, we recommend not adding it to the allowed Internet applications list.

To configure allowed Internet applications in a policy:

1 On the **Groups + Policies** page, click **Add Policy** (or click **Edit** to modify an existing policy).

2 Click the **Desktop Firewall** tab.

3 Under **Allowed Internet Applications**, select the type of application (a detected application or a user-approved application).

4 Select an application, then click **Save**.

The selected application is added to the list of allowed programs for computers using this policy. (No list appears until you have added at least one allowed application to the policy.)

To remove an allowed Internet application from a policy:

1 On the **Groups + Policies** page, click **Add Policy** (or click **Edit** to modify an existing policy).

2 Click the **Desktop Firewall** tab.

3 In the list of **Allowed Internet Applications**, click **remove** for each application you want to delete from the list, then click **Save**.

Specify whether to use SonicWALL recommendations

SonicWALL maintains a whitelist of Internet applications it has determined to be safe at the www.hackerwatch.org website. By default, the firewall protection service checks this website whenever it detects an Internet application that the administrator has not specified as an approved Internet application. You can change the setting of this option in a policy.

To ignore SonicWALL recommendations for Internet applications:

1 On the **Groups + Policies** page, click **Add Policy** (or click **Edit** to modify an existing policy).

2 Click the **Desktop Firewall** tab, deselect the **Use Smart Recommendations to automatically approve common Internet applications** checkbox, then click **Save**.

Viewing reports for firewall protection

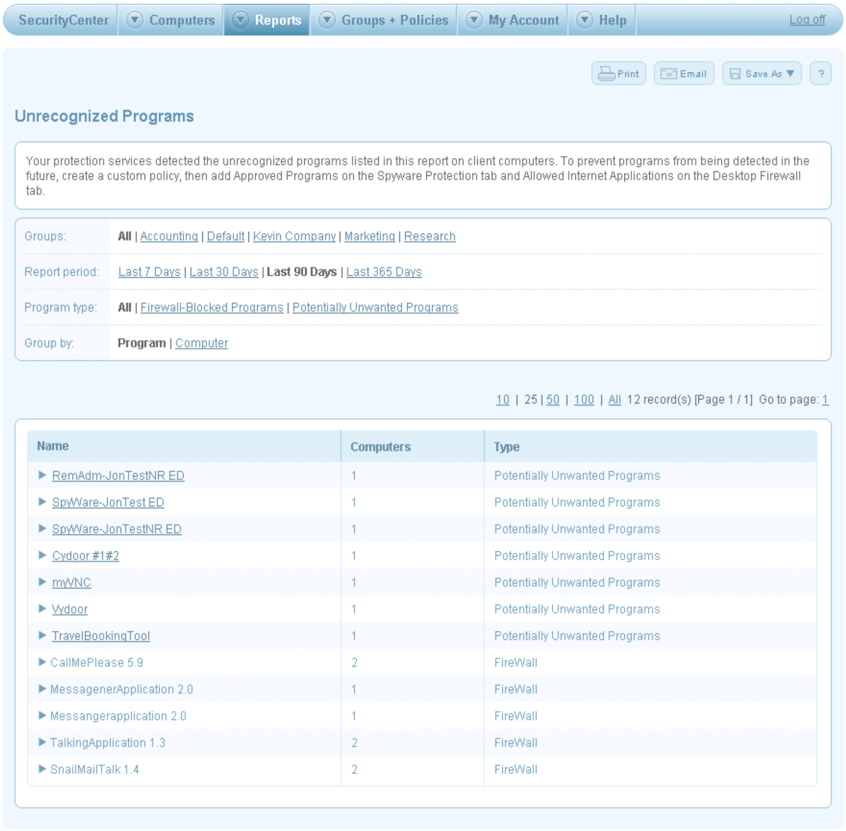
Whenever it checks for updates, each client computer also sends data to the SecurityCenter website in encrypted XML files. You can view this data in reports accessed from the **Reports** page. Two reports contain information about detected suspicious activity:

- **Unrecognized Programs** (see *View unrecognized Internet applications*).
- **Inbound Events Blocked by Firewall** (see *View inbound events blocked by the firewall*).

View unrecognized Internet applications

Use the **Unrecognized Programs** report to view a list of unapproved Internet applications that the firewall protection service detected on your network.

Figure 5-3 Unrecognized Programs report



Unrecognized Programs

Your protection services detected the unrecognized programs listed in this report on client computers. To prevent programs from being detected in the future, create a custom policy, then add Approved Programs on the Spyware Protection tab and Allowed Internet Applications on the Desktop Firewall tab.

Groups:	**All** | Accounting | Default | Kevin Company | Marketing | Research
Report period:	Last 7 Days | Last 30 Days | **Last 90 Days** | Last 365 Days
Program type:	**All** | Firewall-Blocked Programs | Potentially Unwanted Programs
Group by:	**Program** | Computer

10 | 25 | 50 | 100 | All 12 record(s) [Page 1 / 1] Go to page: 1

Name	Computers	Type
▶ RemAdm-JonTestNR ED	1	Potentially Unwanted Programs
▶ SpyWare-JonTest ED	1	Potentially Unwanted Programs
▶ SpyWare-JonTestNR ED	1	Potentially Unwanted Programs
▶ Cydoor #1#2	1	Potentially Unwanted Programs
▶ myVNC	1	Potentially Unwanted Programs
▶ Vydoor	1	Potentially Unwanted Programs
▶ TravelBookingTool	1	Potentially Unwanted Programs
▶ CallMePlease 5.9	2	FireWall
▶ MessagenerApplication 2.0	1	FireWall
▶ Messangerapplication 2.0	1	FireWall
▶ TalkingApplication 1.3	2	FireWall
▶ SnailMailTalk 1.4	2	FireWall

Select the information that appears in this report:

Groups — Display only the computers in a group or display all computers.

Report period — Specify the length of time for which to display information.

Program type — Show all unrecognized programs, only programs blocked by the firewall protection service, or only potentially unwanted programs.

Group by — List unrecognized programs by the computer where they were detected or by the name of the program.

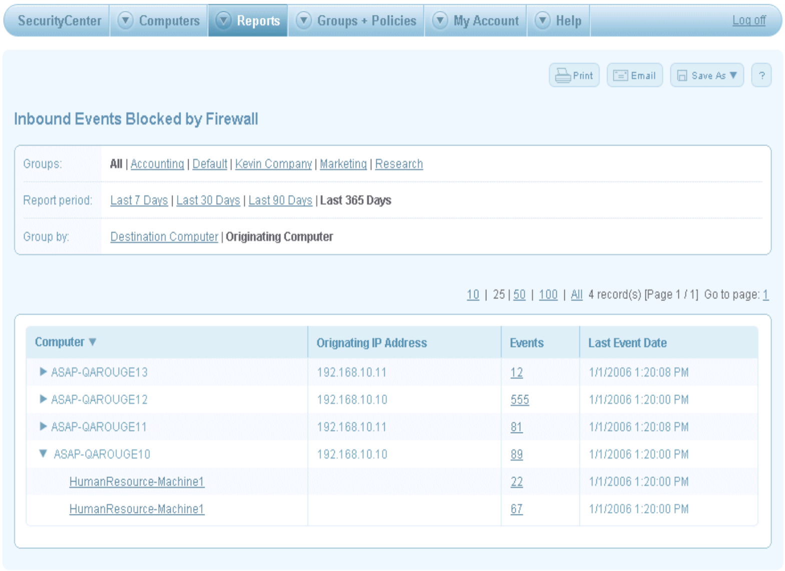
Using the Unrecognized Programs report

When you want to...	Do this...
Display computers or detections	Click ▶ next to a name: ■ Under a computer name, show which detections were found. ■ Under a detection name, show the computers where it was found.
View details about a computer where a detection occurred	On the **Unrecognized Programs** report, click a computer name to display the **Computer Details** page. The **Computer Details** page displays information about the computer, its service components, and its detections (see *Display details for a computer* on page 67).
Allow an Internet application	To add unrecognized Internet applications to the list of allowed applications for other users, add them to a new or existing policy (see *Set up allowed Internet applications* on page 121). Allowed applications will no longer be detected or blocked by the firewall protection service for computers using the policy.

View inbound events blocked by the firewall

Use the **Inbound Events Blocked by Firewall** report to view a list of programs that the firewall protection service prevented from communicating with client computers.

Figure 5-4 Inbound Events Blocked by Firewall report



Inbound Events Blocked by Firewall

Groups: All | Accounting | Default | Kevin Company | Marketing | Research

Report period: Last 7 Days | Last 30 Days | Last 90 Days | Last 365 Days

Group by: Destination Computer | Originating Computer

10 | 25 | 50 | 100 | All 4 record(s) [Page 1 / 1] Go to page: 1

Computer ▼	Orignating IP Address	Events	Last Event Date
▶ ASAP-QAROUGE13	192.168.10.11	12	1/1/2006 1:20:08 PM
▶ ASAP-QAROUGE12	192.168.10.10	555	1/1/2006 1:20:00 PM
▶ ASAP-QAROUGE11	192.168.10.11	81	1/1/2006 1:20:08 PM
▼ ASAP-QAROUGE10	192.168.10.10	89	1/1/2006 1:20:00 PM
HumanResource-Machine1		22	1/1/2006 1:20:00 PM
HumanResource-Machine1		67	1/1/2006 1:20:00 PM

Select the information that appears in this report:

Groups — Display only the computers in a group or display all computers.

Report period — Specify the length of time for which to display information.

Group by — List inbound events blocked from accessing client computers or list the computers where inbound events originated.

Using the Inbound Events Blocked by Firewall report

When you want to...	Do this...
Display computers or detections	Click ▶ next to a name: ■ Under a computer name, show which detections were found. ■ Under a detection name, show the computers where it was found.
View details about events	In the **Inbound Events Blocked by Firewall** report, click a quantity under **Events** to display the **Inbound Event List**. The **Inbound Event List** shows the name of the event, the number of occurrences, and the date on which it was detected.
View details about a computer	In the **Inbound Events Blocked by Firewall** report, click a computer name to display the **Computer Details** page. The **Computer Details** page displays information about the computer, its service components, and its detections (see *Display details for a computer* on page 67).

Managing suspicious activity with best practices

To effectively manage your strategy for guarding against suspicious activity, we recommend that you proactively track the types of suspicious activity being detected and where they are occurring.

To effectively manage your firewall protection strategy:

1. Check your status emails or the SecurityCenter website for an overview of your account's status. See *Sign up for email notifications* on page 62 to request status emails.

2. Check the **Unrecognized Programs** report and **Inbound Events Blocked by Firewall** report regularly. See *View unrecognized Internet applications* on page 123 and *View inbound events blocked by the firewall* on page 124.

3. To centralize management and more easily monitor the types of applications and communications allowed on client computers, configure client firewall protection settings in a policy.

4. Decide whether to use SonicWALL's recommendations for commonly used, safe Internet applications (see *Specify whether to use SonicWALL recommendations* on page 121). When this option is enabled, applications on SonicWALL's whitelist are approved automatically, minimizing the need for you or users to approve applications manually.

5. Use "learn" mode to identify which applications to add to the Allowed Internet Applications list (see *Learn mode* on page 116). This ensures that no applications required for your business are blocked before you have the opportunity to authorize their use. Then change your protection mode to **Protect**.

6. If particular types of intrusions are occurring frequently or certain computers appear vulnerable, update the policy to resolve these issues.

   - Ensure that the firewall protection service is enabled. See *Enable firewall protection* on page 114.

   - Carefully specify the environment where client computers are used. For users with mobile computers, ensure that they know how to select the correct connection type each time their environment changes and their policy allows them to do so. See *Specify a connection type* on page 116.

- Before installing the firewall protection service on a server, ensure that the server's system services and Internet applications are configured correctly. If there is a possibility the service might be installed when no user is present to monitor the installation, disable the policy setting for **Automatically install the desktop firewall on all computers using this policy**. (See *Install the firewall protection service via policy* on page 114).

- When running the firewall protection service on a server, ensure that service ports are configured correctly to prevent disruption of system services (see *Configure system services for a custom connection* on page 117). Ensure that no unnecessary ports are open.

- For maximum protection, set the firewall protection service to **Protect** mode to automatically block suspicious activity (see *Select a firewall protection mode* on page 115).

6 Using the Browser Protection Service

The browser protection service in Enforced Client, based on SonicWALL SiteAdvisor™, displays information to safeguard client computer users against web-based threats:

- A safety rating for each website (see *How safety ratings are compiled* on page 128).
- A safety report for each website that includes a detailed description of test results and feedback submitted by users and site owners.

The browser protection service supports Microsoft Internet Explorer (version 5.5 or later) and Mozilla Firefox (version 1.5 or later).

This section describes these features of the browser protection service:

- *Accessing site safety information*
- *Configuring browser protection settings*
- *Submitting feedback*

Accessing site safety information

On client computers, the safety data compiled by the browser protection service can be used as:

- A browser plugin or extension to stay safe during searches (see *Staying safe during searches*).
- A browser plugin or extension to stay safe while browsing (see *Staying safe while browsing*).
- A resource for detailed analysis, provided in site safety reports (see *Viewing safety reports*).

See *How safety ratings are compiled.*

How safety ratings are compiled

Safety ratings are derived by testing criteria for each website and evaluating the results to assess whether the site poses a risk and, if so, what type of risk.

Automated tests compile safety ratings for a website by checking for:

- Viruses and potentially unwanted programs bundled with downloaded files.
- Spam or a high volume of non-spam emails sent after submitting contact information in a signup form.
- Excessive popup windows.
- Attempts by the site to exploit browser vulnerabilities.
- Deceptive or fraudulent practices employed by a site.

Test results are compiled into a safety report that can also include:

- Feedback submitted by site owners, which might include descriptions of safety precautions used by the site or responses to user feedback about the site.
- Feedback submitted by site users, which might include reports of phishing scams or bad shopping experiences.
- Analysis by SonicWALL employees.

Staying safe during searches

When users enter keywords into a popular search engine such as Google, Yahoo!, MSN, Ask, or AOL.com, color-coded safety icons appear next to sites listed in the Search Results page:

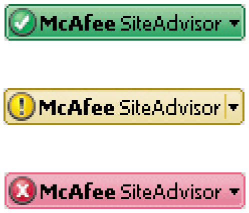
✅	No significant problems.
⚠️	Some issues users should know about. For example, the site tried to change the testers’ browser defaults or sent them a high volume of non-spam email.
❌	Some serious issues that users should consider carefully before accessing the site. For example, the site sent testers spam emails or bundled adware with a download.

To view a site’s safety balloon:
Hold the cursor over the safety icon.

To view a site’s safety report:
Click the safety icon or select **More info** in the safety balloon.

Staying safe while browsing

When users browse to a website, the SiteAdvisor toolbar displays a color-coded menu button (the location depends on the browser):



To display the SiteAdvisor toolbar:
In Internet Explorer, select **View | Toolbars | SonicWALL SiteAdvisor**.

The SiteAdvisor toolbar is always displayed in Firefox.

To display the SiteAdvisor menu:
Click the **SiteAdvisor** menu button.

Available menu commands depend on the browser.

To do this...	Select this option...	
	Internet Explorer	Firefox
	Show balloon	
Display the safety report for the current site. Not available when the browser protection service is disabled (Internet Explorer) or the **Enable safe browsing button** option is not selected (Firefox).	**View site details**	**View Site Details**
Configure settings for browser protection (see *Configuring browser protection on the client computer* on page 131).	**Settings**	**Settings**
Add a website to the list of approved sites. The user will not receive warnings when viewing or downloading from sites on this list.	**Do Not Warn list**	
	Disable/Enable	
Send an email to a friend explaining how to download a free trial version of the browser protection service.	**Tell a friend**	**Tell a Friend**
Open a form to submit a site for testing, submit user or owner feedback about a site, or contact product support (see *Submitting feedback* on page 132).	**Send feedback**	**Send Feedback**
Install the latest version of the browser protection service or check whether the latest version is running.	**Get latest version**	
	Help	**Help**
Access a brief description of the browser protection service, its license agreement, and its privacy policy.	**About**	**About**

Viewing safety reports

Users can supplement the color-coded safety information for a site by viewing its detailed safety report. These reports describe specific threats discovered by testing and include feedback submitted by site owners and users.

To view the safety report for the current site:
From the SiteAdvisor menu, select **View Site Details**.

OR

Click the safety icon in a Search Results page.

To view a safety report from the www.siteadvisor.com website:
On the www.siteadvisor.com Home page or Analysis page, enter a URL into the **Look up site report** box.

Configuring browser protection settings

Policies define the operational settings for all your protection services. See *Setting up policies* on page 75 for general information about using policies.

In this release, users configure most browser protection features at their computers. From the SecurityCenter, administrators can configure whether to install the browser protection service automatically as part of a policy.

- *Configuring browser protection from the SecurityCenter*
- *Configuring browser protection on the client computer*

Configuring browser protection from the SecurityCenter

Currently, administrators can configure one option on the **Browser Protection** tab of the SecurityCenter.

- *Installing via policy*

Installing via policy

Use this option to install the browser protection service on client computers automatically whenever they check for an updated policy. This feature is useful for adding only the browser protection service on computers where the Enforced Client client software is already installed. In the **SonicWALL Default** policy, this feature is enabled.

To add this feature to other policies, you must edit an existing policy or set up a new policy and then assign it to one or more groups of computers (see *Creating groups to manage your site* on page 71 and *Setting up policies* on page 75).

To install the browser protection service via policy:

1 On the **Groups + Policies** page, click **Add Policy** (or click **Edit** to modify an existing policy).

2 Click the **Browser Protection** tab.

3 Select **Automatically install browser protection service on all computers using this policy**, then click **Save**.

The browser protection service will be installed on all computers using this policy the next time they check for an updated policy.

Configuring browser protection on the client computer

Users can configure settings for additional browser protection features.

To configure browser protection settings:

1 From the SiteAdvisor menu, select **Settings**.

2 Select one of the available commands, then click **OK**.

To do this...	Select this option...	
	Internet Explorer	Firefox
	Participate in product improvement program	
Highlight the entire link that appears in the Search Results page with green, yellow, or red.	**Highlight search result links**	**Highlight search result links**
Enable or disable the display of safety icons next to website links in a Search Results page.	**Show verdict in Safe Search**	**Display safe search icons**
Encrypt the data sent to the server using the Secure Sockets Layer protocol. This prevents intruders from tracking user browsing patterns.	**Use SSL communications to server**	**Use SSL communications to server**
Enable or disable the color coding for the **SiteAdvisor** menu button.		**Enable safe browsing button**

Submitting feedback

SonicWALL encourages feedback about websites:

- Users can describe suspicious or dangerous behavior they encounter when visiting a site.
- Site owners can provide helpful information or respond to user feedback about their site.

Feedback is displayed in the site's safety report.

> Users and site owners must register before submitting information to SonicWALL. A link is provided in the feedback form.

Users can also use the feedback feature to offer general suggestions, report problems, and contact product support.

> The feedback feature requires the browser to accept cookies. For instructions, select **Help** from the **SiteAdvisor** menu.

To submit feedback:

1 From the SiteAdvisor menu, select **Send Feedback**.

2 From the drop-down list, select the appropriate action.

Submit a site for testing	Enter the URL for a website you would like SonicWALL to test.
Leave user comments about a site	Enter your contact information, the website's URL, and your comments.
Leave comments as a site owner	Enter your contact information, your website's URL, and your comments.
General SonicWALL Product Support	Select a link for customer service, technical support, virus removal services, or support for software installed by a SonicWALL partner. A page appears with answers to common questions and links for assistance.
Contact our business team	Click **send an e-mail** to open a preaddressed message for discussing business partnerships or requesting the use of SiteAdvisor data.

7 Using the Email Security Service

The email security service in Enforced Client Advanced scans messages before they are received by client computers and quarantines detections. Your service checks for spam, phishing scams, viruses, directory harvest attacks, and other email-borne threats in messages and attachments.

The email security service resides outside your network, requiring no system resources. Your company's mail exchange (MX) record is redirected through SonicWALL's servers. There, your email traffic is scanned before entering your network, with less than a one-second delay in transit.

The email security service provides:

- **Protection from email-borne threats** — The flood of email threats is stopped before entering your network.
- **Real-time, around-the-clock email security** — Email is processed all day, every day in real time through a highly secure system architecture that operates with no detectable latency.
- **Simplified management** — Centralized, web-based policy management allows you to configure comprehensive policies for spam, viruses, and content-filtering (for inappropriate words and phrases). You can also view reports on email usage and check quarantined messages.

To use the email security service, your company needs to have its own mail domain, such as *yourdomain*.com, with a static IP address and a dedicated email server, either in-house or hosted by an ISP.

This section describes these features of the email security service:

Activating the email security service

Activate your email security service through a unique registration website, which you access from the SecurityCenter website.

To activate your account:

1 On the SecurityCenter website, click the **SecurityCenter** tab.

2 Click **Install Protection**.

3 Select **Install email security service**.

4 Click the URL to open the activation wizard.

5 From the SecurityCenter, copy the activation key, then paste it into the field in the activation wizard.

6 Answer the questions in the wizard.

Activation takes about an hour to complete. When it is complete, reporting information appears on the SecurityCenter page, and you receive an email with instructions for changing your mail exchange (MX) records. At this point, you can set up and configure your account through the service's portal.

Using the portal

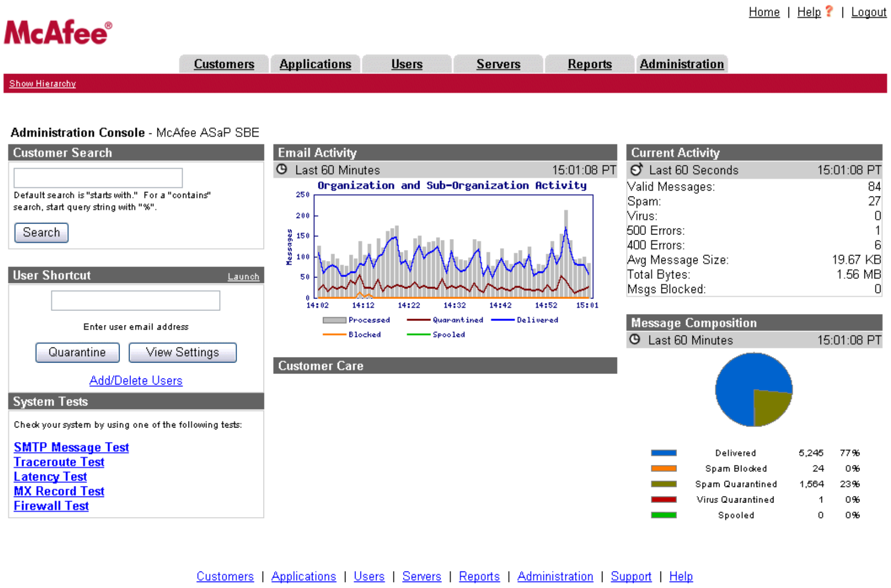
The portal is a website, which you access from the SecurityCenter, where you perform most management functions for the email security service. You can configure your service, check email statistics and activity, and view reports through the portal.

To access the portal:

1 On the SecurityCenter website, click the **SecurityCenter** tab.

2 Under **Your email protection**, select **Click here to configure**, or click an area of the pie chart.

Figure 7-1 Email security service's portal



Administration Console - McAfee ASaP SBE

Default search is "starts with." For a "contains" search, start query string with "%".

Enter user email address

Check your system by using one of the following tests:

Valid Messages:	84
Spam:	27
Virus:	0
500 Errors:	1
400 Errors:	6
Avg Message Size:	19.67 KB
Total Bytes:	1.56 MB
Msgs Blocked:	0

🟦	Delivered	5,245	77%
🟧	Spam Blocked	24	0%
🟫	Spam Quarantined	1,564	23%
🟥	Virus Quarantined	1	0%
🟩	Spooled	0	0%

Setting up your account

When your account is activated, you can set it up to filter email for users in its activation domain, the domain you specified in the activation wizard.

- *Update your MX records*
- *Customize your account settings*
- *Configure general administration settings*

Update your MX records

To filter email for users in the activation domain, you must change the domain's mail exchange (MX) records to direct email flow to SonicWALL servers. These records might be managed by you or your service provider. You need to change them as instructed in the last step of the activation wizard or in the email you received after activating your account. You can also view instructions on the **Administration** tab under **DNS Instructions**.

Customize your account settings

From the portal, you can customize the email security service to better suit your company's needs. For example, you can add more domains, add users, and set up additional filters.

- *Default settings*
- *Recommended first steps*
- *Optional customization*

Default settings

As soon as your email security service is activated, default functionality and features are configured.

- Two users appear on the **Users** tab:
  - Your administrator login address.
  - A default user (whose name begins with *pdefault*), which you should ignore.

> Do not delete the *pdefault* entry.

- Users in the activation domain automatically receive virus protection and basic attack blocking. However, your users *will not* receive spam filtering protection until they are added to the email security service.
  - Registered users receive a daily **Quarantine Summary** email, which lists recent spam detections. Users can review the list and optionally forward any false positives to their Inbox (see *Managing quarantined email* on page 142).
- The activation domain is entered on the **Domains** page (on the **Administration** tab), and your email server is entered under **Delivery Manager** (on the **Servers** tab).
- Users can contact you for assistance via a support address, which initially is your administrator login address.
- Automatic disaster recovery is enabled via *spooling:* Should your email server stop functioning, messages are temporarily saved to the SonicWALL server, then automatically delivered when your server begins functioning again.

Recommended first steps

We recommend you follow these steps to configure your service for enhanced security, quick response to problems, and disaster recovery.

1 **Add your other domains.**

If users in multiple domains need email protection, add those domains to your email security service. (You don’t need to add subdomains, such as corp.yourdomain.com or sales.yourdomain.com. Instead, set up subdomain stripping for the primary domain.)

> SmartCreate, which automatically adds users accounts, works only for domains that have been added to the email protection service.

2 **Add partners, associates, and other friendly addresses to the Approved Senders list.**

This helps prevent false positives.

3 **Set up your email server to prevent spam and viruses from circumventing the email security service.**

Some virus and spam senders specifically target email servers using low-priority DNS MX records or by looking up a server directly with an intuitive name like mail.*yourdomain*.com. To prevent them from bypassing the email security service, we recommend that you add all your domains to the email protection service, and configure your email server to accept mail only from the email security service.

4 **Configure alerts about significant server events to be sent to your (the administrator's) wireless device.**

To ensure that you are alerted immediately to significant server events, such as when a host stops functioning or spooling begins, we recommend setting up alerts for both Delivery Manager and Spool Manager. Also, it's important to send alerts to an address at a wireless device rather than an address routed through the data center, because the data center would potentially be disabled by the event triggering the alert.

5 **If your email server receives valid traffic from trusted relay severs, use Connection Manager to allow those servers' IP addresses, so their traffic is not misinterpreted as an attack and blocked.**

A trusted relay server passes significantly more traffic to your email server than other servers. Therefore, its traffic is likely to be blocked by Connection Manager. To prevent this from happening, specifically allow those servers' IP addresses.

Optional customization

Answer these questions to fine-tune your email security settings.

1 **Do you want to add users to the service manually, rather than having them added automatically?**

By default, users in your domains are added automatically to the email security service, using SmartCreate (under **General Settings** on the **Administration** tab). If you do not want this to happen, disable SmartCreate and add users manually. You might want to do this if you do not want all users to receive spam filtering. (Users you do not add will still receive virus protection.)

2 **Do you want to filter a specific category of spam more or less aggressively than average?**

Spam filters are initially adjusted to catch as much spam as possible without falsely tagging legitimate messages as spam. You might need to fine tune these settings, or adjust sensitivity of filters for individual spam categories, including sexually explicit or racially insensitive messages, get-rich-quick offers, and special commercial offers. For example, you might want to filter sexually explicit messages more aggressively, while allowing special offers.

3 **Do you want to prevent users from delivering quarantined messages to their Inboxes? Do you want to deny them access to quarantined messages altogether?**

Initially, users receive a **Quarantine Summary** email listing recently quarantined messages, and they can optionally deliver legitimate messages from their quarantine to their Inbox.

You can turn off the **Quarantine Summary** or block users from delivering quarantined messages to their Inbox (in this case, users will have to contact an administrator to forward legitimate messages for them).

4 **Do you want to manage all users' quarantined messages in one central quarantine, rather than separate user quarantines?**

Initially, each user's detected spam is quarantined in an individual user quarantine, where you can go to manage that user's spam. If you prefer to manage all your organization's spam from one location, you can divert all spam to a central quarantine by changing your *spam disposition*.

5 **Do you want to allow attachments larger than 200 MB, or block attachments smaller than that?**

By default, the protection service blocks all messages containing attachments that are larger than 200 MB. These messages are not delivered to users and cannot be retrieved. You can change this size limit using **Attachment Manager** on the **Applications** tab.

6 **Do you want to prohibit or approve messages based on the file type of any attachment?**

On the **Applications** tab, enable **Attachment Manager** and configure a custom filter or one of the file type filters. For example, you might want to block potentially dangerous executable attachments, such as .EXE files, but specifically allow certain image file types.

7 **Do you want to prohibit or approve messages based on text in the message?**

On the **Applications** tab, create **Content Manager** filters. For example, you might want to allow all messages containing the text "résumé" to make sure that no incoming resumes are accidentally filtered as spam.

8 **Do you want to adjust sensitivity for blocking specific types of server attacks?**

Connection Manager automatically detects attacks against your email server, including directory harvest attacks, virus outbreaks, and spam attacks. You can optionally detect email bombs and change the sensitivity of blocking for individual types of attacks.

Configure general administration settings

Manage general system administration of the email security service on the **Administration** page.

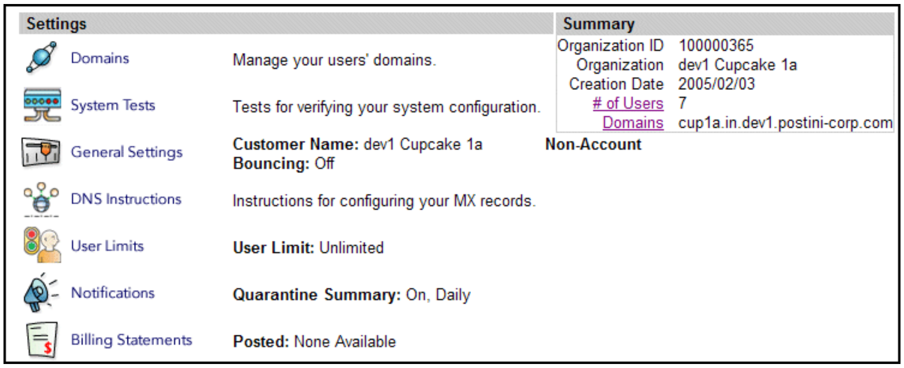
To configure administrative settings:

1 On the SecurityCenter website, click the **SecurityCenter** tab.

2 Under **Your email protection**, select **Click here to configure**.

3 On the portal, click the **Administration** tab.

Figure 7-2 Administration page



Settings	
Domains	Manage your users' domains.
System Tests	Tests for verifying your system configuration.
General Settings	**Customer Name:** dev1 Cupcake 1a **Bouncing:** Off
DNS Instructions	Instructions for configuring your MX records.
User Limits	**User Limit:** Unlimited
Notifications	**Quarantine Summary:** On, Daily
Billing Statements	**Posted:** None Available

Summary	
Organization ID	100000365
Organization	dev1 Cupcake 1a
Creation Date	2005/02/03
# of Users	7
Domains	cup1a.in.dev1.postini-corp.com

Non-Account

Access basic administration features on the Administration page:

Use this feature...	To...
Domains	■ View your current domains. ■ Add or delete a domain. ■ Enable/disable subdomain stripping for a domain.
System Tests	■ Test and trace mailflow. ■ Test server latency. ■ Verify your MX record configuration.
General Settings	■ Modify your company name or support address. ■ Choose how to handle messages to unrecognized addresses in your domains.
DNS Instructions	■ Configure your domain's MX records to point to the email security service's primary and backup data centers.
User Limits	■ Track how many users are receiving email protection. ■ Check whether you have reached any prescribed limit. ■ Send automatic administrator alerts.
Notifications	■ Send users a periodic email summary of recently quarantined messages. ■ Turn off the Quarantine Summary.
Usage Details	■ View a monthly summary of usage of the email security service.
Summary	This chart can be helpful for Help Desk personnel. ■ View your organization's unique ID (created automatically). ■ View your organization name, which you can change under **General Settings**. ■ View the date your service was established. ■ View the number of users currently added to the email security service and a link to listing them. ■ View the domains that have been added to your service and a link to managing them.

Viewing your email protection status

Once your email security service is running, check the **SecurityCenter** page of the SecurityCenter website to view your email traffic, including spam, viruses, and delivered messages from the prior seven days. Data on the last 60 minutes of your email traffic is available by clicking the pie chart. Key issues that require attention are noted in the action items at the top of the **SecurityCenter** page (see *View and resolve action items* on page 64).

To view the status of your service:

1 On the SecurityCenter website, click the **SecurityCenter** tab.

2 Under **Your email protection**, check your email statistics.

3 Click the pie chart to open the portal, where you can view data for the last seven days of email activity.

To resolve action items:
Click an action item to display instructions for resolving it.

Configuring a policy for email security

Configure security settings for your email security service by setting up a policy. (You can set up only one policy for your email security service account.)

To set up a policy for email security:

1. On the SecurityCenter website, click the **Groups + Policies** tab.

2. Select **Add Email Security Policy**.

   - If you have purchased only the email security service, this option appears on the page.

   - If you have purchased multiple protection services, click the down arrow ▼ on the **Groups + Policies** tab, then select **Add Email Security Policy** from the menu.

3. On the portal, click the **Applications** tab.

4. Select type of settings you want to configure:

   - **Spam Filtering** — Enable spam filtering, specify the type of messages to filter, specify how to handle detections, then click **Save**.

   - **Virus Blocking** — Enable virus protection and specify how to handle detections, then click **Save**.

   - **Sender Lists** — Add email addresses to allow or block.

Viewing reports for the email security service

Check the **Reports** page of the SecurityCenter website to access report data from the email security service.

To view report data:

1. On the SecurityCenter website, click the **Reports** tab.

2. Select **Email Security Reports**.

3. On the portal, click the **Reports** tab.

4. Click the name of a report.

You can click the **Help** link for more information about the data in each type of report.

Managing quarantined email

The email security service quarantines email messages that contain detected spam, phishing, and virus threats. Several tools are available for managing these messages:

- *View and manage quarantined user messages*
- *Check the Quarantine Summary*
- *View quarantined mail deliveries*

View and manage quarantined user messages

For each primary user email account, you can check the status of quarantined messages, view details about them, and specify processing tasks.

To manage user messages:

1. On the portal, click the **Users** tab.
2. Select a user’s email address.
3. Select **Quarantine**.

   From the listing, you can sort, filter, and process messages.

You can click the **Help** link for more information about managing quarantined messages.

Check the Quarantine Summary

The email security service sends users a **Quarantine Summary**, which lists the messages that have been quarantined for them since they last received a summary. These messages have not yet been delivered or deleted.

The **Quarantine Summary** enables users to quickly determine the type and number of messages that were quarantined. It lists:

- Sender, subject, and time received.
- Total number of quarantined messages.
- Messages containing detected viruses.
- Messages containing detected spam or phishing scams.

Users can check the **Quarantine Summary** to detect any false positives that were quarantined by mistake and restore those messages to their email Inbox. Messages containing viruses are cleaned before they are restored.

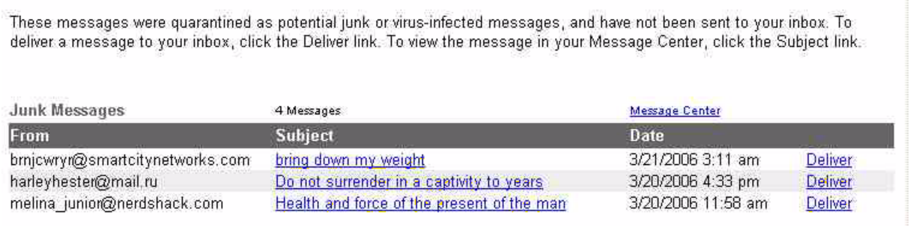
As the administrator, you determine how often users receive the **Quarantine Summary**. It is sent to each user’s primary email address, which you register with the email security service. If the service does not detect and quarantine any email threats, it does not send a **Quarantine Summary**. Quarantined messages are deleted automatically after two weeks.

You also configure whether users can deliver quarantined email to their Inboxes. (If they cannot deliver email, the **Deliver** link does not appear in the **Quarantine Summary**.) Click the **Help** link on the portal for more information.

To restore quarantined email to an Inbox:
Provide these instructions to your users:

1 Open the **Quarantine Summary**.

2 To restore a message, click **Deliver**.



These messages were quarantined as potential junk or virus-infected messages, and have not been sent to your inbox. To deliver a message to your inbox, click the Deliver link. To view the message in your Message Center, click the Subject link.

Junk Messages 4 Messages Message Center

From	Subject	Date	
brnjcwryr@smartcitynetworks.com	bring down my weight	3/21/2006 3:11 am	Deliver
harleyhester@mail.ru	Do not surrender in a captivity to years	3/20/2006 4:33 pm	Deliver
melina_junior@nerdshack.com	Health and force of the present of the man	3/20/2006 11:58 am	Deliver

View quarantined mail deliveries

Administrators can track the number and type of quarantined messages that users deliver to their Inboxes by viewing **Quarantine Delivery** reports. Use these reports to determine whether too many false positives are being detected and quarantined, and whether users are delivering inappropriate messages.

To view quarantine deliveries:

1 On the portal, click the **Reports** tab.

2 Under **Quarantine Delivery**, select **Activity Log**.

3 Select **Inbound Weekly Log** or **Inbound Daily Log**, depending on the number of days for which you want to view data.

You can click the **Help** link for more information about managing quarantined messages.

Getting more information

Detailed information, instructions, and troubleshooting procedures are available in the *Administration Guide*.

To access the Administration Guide:
On the portal, click the **Help** link in the top right corner of any page.

Context-sensitive information appears, and you can navigate to any topic in the guide.

8 Troubleshooting

For help installing, using, and maintaining Enforced Client, refer to frequently asked questions or specific error messages and their solutions.

- *Uninstalling protection services*
- *Frequently asked questions (FAQ)*
- *Error messages*
- *Contacting product support*

Uninstalling protection services

For testing purposes or before reinstalling the client software, you might need to uninstall the client software.

> ! If you uninstall the client software, the computer is no longer protected. we recommend that you reinstall as soon as possible.

To uninstall the client software from a client computer:

1. Close the Microsoft Outlook and Internet Explorer applications.
2. In the Windows **Control Panel**, open **Add/Remove Programs**.
3. Select **SonicWALL Virus and Spyware Protection Service** from the list, then click **Remove**.
4. Select **SonicWALL Firewall Protection Service** from the list, then click **Remove**.

> i On computers running Windows XP or Windows Vista, the Windows firewall is automatically re-enabled when the Enforced Client firewall protection service is uninstalled. This ensures that the computer is always protected by a firewall program.

5. Select **SonicWALL Browser Protection Service** from the list, then click **Remove**.

Frequently asked questions (FAQ)

This section includes questions asked by administrators and client computer users.

- *Installing*
- *Adding, renewing, and moving licenses*
- *Configuring and managing policies*
- *Scanning*
- *Reporting*
- *Updating*
- *Firewall protection*
- *Browser protection*
- *Email*
- *General*

Installing

How do users without administrator rights install the service with an Internet URL?
To allow users without administrator rights to install protection services, you must first load a standalone installation agent on their client computers. See *Install the standalone installation agent* on page 34 for more information.

Does it matter which email address or identifier I enter when installing Enforced Client?
No. Any description can be entered in the field, or it can be left blank. However, an email address provides a link for notifying the principal user about security issues for the computer. The information entered identifies the client computers in administrative reports.

While installing Enforced Client, the installation process appears to stop responding.
The installation might take a few minutes to complete. However, if the status bar stops moving and nothing in the installation window has changed in more than five minutes, close the window and start the installation process again (for example, by clicking the installation URL).

Do access protection or behavior blocking rules in other applications affect installation of Enforced Client?
Yes. If users are unable to install the client software and you have defined access protection or behavior blocking rules, such as those that would prevent binaries from executing from the TEMP folder, disable them and try installing again.

Adding, renewing, and moving licenses

I purchased licenses for new computers, but the new computers don't show up on my reports.
When you purchase additional services or renew services, use the same email address that you used when purchasing the original services. Also, place your order from the same SecurityCenter website where you purchased your original services. This ensures that your new services have the same company key (CK) as your existing service and show up on the same reports. Contact product support for assistance with merging multiple accounts.

Can I move a license from one computer to another?
Yes. You can uninstall Enforced Client from one computer and install it on a new computer without affecting the total number of licenses you are using. The old computer is automatically subtracted from your total license count on the service's accounting system, and the new one added, so that your license number remains constant.

1. Uninstall the software from the old computer (see *Uninstalling protection services* on page 145).
2. From the SecurityCenter, click the **Computers** tab.
3. For **Groups**, select **All**, then select the old computer in the listing and click **Delete**.
4. Install the software on the new computer (see *Installing Enforced Client* on page 35).

The new computer appears in your reports after it uploads its status information to the SecurityCenter. This usually takes about 20 minutes.

My computer crashed and I had to reinstall the operating system and start over. Will this affect my license number?
No. The old computer is automatically subtracted from your total license count on the service's accounting system, and the new one added, so that your license number remains constant.

1. From the SecurityCenter, click the **Computers** tab.
2. For **Groups**, select **All**, then select the old computer in the listing and click **Delete**.
3. Install the software on the reformatted computer (see for *Installing Enforced Client* on page 35).

The new computer appears in your reports after it uploads its status information to the SecurityCenter. This usually takes about 20 minutes.

Configuring and managing policies

How can I prevent popup prompts from appearing when unrecognized programs are detected?
The virus and spyware protection service and the firewall protection service prompt users for a response to a potentially unwanted program or Internet application detection when set to **Prompt** mode. To prevent popups, select **Protect** or **Report** mode. For highest protection, select **Protect** to automatically delete unrecognized programs (virus and spyware protection service) or block unrecognized Internet applications (firewall protection service). For more information, see *Select a spyware protection mode* on page 100 or *Select a firewall protection mode* on page 115.

Why would I want to specify excluded files and folders or approved programs?
Specifying excluded files and folders from scanning can be useful if you know a particular type of file is not vulnerable to attack, or a particular folder is safe. If you use a program or Internet application to conduct your business, adding it to a list of approved programs or allowed Internet applications keeps it from being detected as unrecognized and deleted or blocked. If you are unsure, it is best not to specify exclusions.

Why does the firewall protection service ignore user settings, such as allowed Internet applications? It did not ignore them last week.
If the previous policy allowed users to configure settings and the current policy does not, user settings are ignored. However, user settings are saved on client computers. If the policy is later updated to allow users to configure settings, their firewall protection service again recognizes their settings, such as allowed Internet applications.

Scanning

How do I prevent certain files or folders from being scanned for viruses?
The policy management feature allows you to specify files, folders, or types of files to exclude from scanning for viruses (see *Exclude files and folders from virus scans* on page 96).

How do I prevent certain programs from being scanned for spyware?
The policy management feature allows you to specify approved programs that will not be detected as potentially unwanted programs (see *Specify approved programs* on page 101). Users can also specify approved programs on their own computers.

Is there a “learn mode” to help me discover which programs I need to approve?
Yes. When you first install the virus and spyware protection service, select **Prompt** mode, then check the **Unrecognized Programs** reports frequently to see which programs are detected on client computers (see *Learn mode* on page 101). After you add the ones you need to your list of approved programs, you can change to **Protect** or **Report** mode.

Can I stop a scheduled scan once it has started?
No. Once a scheduled, on-demand scan has started, you cannot stop the scan unless you restart the computer.

Why do on-demand scans sometimes detect items that on-access scans don’t detect?
With the default policy settings, on-access scans do not look at compressed archives and on-demand scans do. If this is a concern for you, reconfigure these policy settings (see *Enable optional protection* on page 97). If the policy does not use default settings, options might be selected to scan different files during on-access and on-demand scans. See *Scan automatically (on-access scans)* on page 89 and *Scan manually (on-demand scans)* on page 90 for more information.

Reporting

How do I find my reports?
Log on to the SecurityCenter, then click the **Reports** tab to display links to available reports.

I’m looking at my report and some of my computers don’t show up there.
If your company added more computers, or upgraded from trial to full product, some computers might not appear in your reports.

If you upgraded or purchased additional services using a new email address, you received a new company key and URL for a new account instead of adding licenses to your existing account. (The company key appears after the characters `CK=` in the URL.) Because you have two company keys, reports appear in two places. Make sure all your trial users reinstall with the installation URL associated with the new key. Contact product support for assistance with merging multiple accounts.

Can I use a non-Microsoft browser to view reports?
Yes. You can view the SecurityCenter website using Internet Explorer (version 5.5 or later) or Firefox (version 1.5 or later).

My cloned systems all report as the same computer.
Enforced Client generates a unique system identifier when it is installed. If a drive is imaged after the software was installed, all the cloned systems have the same system identifier. To avoid this problem, the software must be installed *after* the new systems are restarted. You can do this automatically using the silent installation method.

How long does the server save old report data?
Your data is saved for your full license period, and continues if the license is renewed.

I just installed Enforced Client and don't have much information on my SecurityCenter website. Can I view sample reports?
Yes. Sample reports are available at:

http://www.mcafeeasap.com/intl/EN/content/virusscan_asap/samplereports.asp

Sample reports are useful for new administrators who do not have many users or much detection data and, therefore, cannot view some advanced reporting features.

Sample reports are available in all product languages. Select the language from the **Global Sites** pull-down list in the upper right corner of the page.

Updating

When does Enforced Client check for updates?
Client computers check for new updates five minutes after connecting to the network, and at regular intervals throughout the day. You can specify the interval in the computer's policy (see *Select your update frequency* on page 97).

To run an update manually on a client computer, double-click M in the system tray.

If there is an outbreak, how soon will client computers receive an updated detection DAT file?
SonicWALL Avert Labs provides updates as soon as possible after an outbreak. To ensure that client computers receive them promptly, make sure the policy's **Enable outbreak response** option is selected (see *Enable optional protection* on page 97).

During an update, I get a message that one or more Enforced Client windows are open, but I don't see any windows open. What should I do?
This occurs when a task that cannot be stopped, such as a scheduled scan, is running in the background. Wait for the task to complete, or restart the computer to proceed with the update.

How can I stop errors from showing up in my reports when automatic updates fail on systems where no user is logged on?
For certain system configurations, automatic updates do not occur on systems where no user is logged on. You can prevent these failed updates from being reported by configuring a policy setting (see *Update computers where no user is logged on* on page 55).

Firewall protection

Is there a "learn mode" to help me discover which Internet applications I need to approve?
Yes. When you first install the firewall protection service, select **Prompt** mode, then check the **Unrecognized Programs** reports frequently to see which applications are detected on client computers (see *Learn mode* on page 116). After you add the ones you need to your list of allowed applications, you can change to **Protect** or **Report** mode.

Is it okay to run the Windows firewall and the firewall protection service at the same time?
We recommend that you disable the Windows firewall when the firewall protection service is running. (It is disabled automatically when the firewall protection service is installed.)

If both firewalls are enabled, the firewall protection service lists only a subset of the blocked IP addresses in its **Inbound Events Blocked by the Firewall** report. The Windows firewall blocks some of these addresses; however, it does not report them because event logging is disabled in the Windows firewall by default. If both firewalls are enabled, you must enable Windows firewall logging to be able to view a list of all blocked IP addresses. The default Windows firewall log is C:\Windows\pfirewall.log. In addition, there will be some duplication of status and alert messaging.

How do I keep the firewall protection service from blocking certain Internet applications?
The policy management feature allows you to specify allowed Internet applications that will not be blocked (see *Set up allowed Internet applications* on page 121). Users can also specify allowed Internet applications on their own computers if their policy allows.

I blocked Internet Explorer on a client computer, and then temporarily disabled the firewall protection service. When I re-enabled the service, why was Internet Explorer no longer blocked?
The firewall protection service uses Internet Explorer to update product components. Whenever you enable the service, Internet Explorer is given **Full Access** in order to check for updates.

Why does the firewall protection service ignore user settings, such as allowed Internet applications? It did not ignore them last week.
If the previous policy allowed users to configure settings and the current policy does not, user settings are ignored. However, user settings are saved on client computers. If the policy is later updated to allow users to configure settings, their firewall protection service again recognizes their settings, such as allowed Internet applications.

Why does the firewall protection service ignore settings configured by the administrator?
If the administrator configures **Prompt** mode, user settings take precedence over administrator settings. The administrator can always add to the list of **Allowed Applications**.

Browser protection

Can users run the browser protection service for Internet Explorer and Firefox on the same computer?
Yes. The browser protection service for Internet Explorer and Firefox are compatible on the same computer. Users can install protection for both browsers. (If both browsers are present on a computer when browser protection is installed, protection for both browsers is installed automatically.)

Is it safe to use the browser protection service as my only source of security against web-based threats?
No. The service tests a variety of threats, and constantly adds new threats to its testing criteria, but it cannot test for all threats. Users should continue to employ traditional security defenses, such as the virus, spyware, and firewall protection services in Enforced Client, for a multi-tiered defense.

Email

Is my computer protected from email viruses?
Yes. The virus and spyware protection service (on desktop client computers) features an on-access scanner that scans email messages and attachments as they are accessed or opened. It also cleans infected email messages before they are delivered to the user's Inbox when the **Scan email option** on the **Advanced Settings** tab is enabled (see *Enable optional protection* on page 97).

For enhanced email security, SonicWALL offers Enforced Client Advanced. With this solution, you have the power of an email security service that routes email messages through SonicWALL servers and scans them for spam, viruses and other threats before they are received by client computers. Detections are blocked or quarantined. An email server security application can also be implemented to protect Microsoft Exchange and Lotus Domino email servers against viruses.

Can I scan email messages on demand?
Yes. In your Microsoft Outlook Inbox, select one or more messages, then from the **Tools** menu, select **Scan for Threats**.

After installing the email security service, why am I not receiving email or seeing any charts on the email service's portal?
To determine and resolve the problem, visit the email security service's portal (see *Using the portal* on page 134) and run the **System Tests** listed on the home page. Refer to the *Administration Guide* for more information on the tests (see *Getting more information* on page 143).

General

Can I use a non-Microsoft browser, such as Mozilla Firefox or Opera?
Yes. The client computer must use Microsoft Internet Explorer 5.5 SP2 or later to install the client software. However, once the client software is installed, the default Internet browser can be used for other purposes. You can view the SecurityCenter using Internet Explorer or Firefox.

I use Windows XP Service Pack 2, and I get a message that my computer may be at risk. What does this mean?

This is a known problem with Microsoft Security Center, because Microsoft cannot determine that Enforced Client is installed and up-to-date. If you get this message when starting your computer, click the message balloon to open the **Recommendation** window, select **I have an antivirus program that I'll monitor myself**, then click **OK**.

I want to update the Windows operating system on my client computer. Do I need to reinstall Enforced Client?

Yes. If you upgrade a client computer's operating system (for example, from Windows 2000 to Windows XP) and you want to leave your existing files and programs intact during the upgrade, you must first uninstall Enforced Client, then reinstall it after the upgrade is complete.

Is it okay to delete the Temp folder in my program's directory structure?

No. Updates might fail if the Temp folder does not exist. If you delete the folder inadvertently, restart the computer to re-create the folder automatically, or manually create a Temp folder under the Program Files\McAfee\Managed VirusScan directory.

I copied a virus to my computer as a test and nothing seemed to happen. Why didn't my virus protection service detect it?

The virus and spyware protection service quietly detects and cleans most types of viruses without notifying users. This reduces help desk calls and minimizes user interruptions. However, virus detections are always noted on the administrative reports. Verify that the virus was found by checking the reports from the SecurityCenter website.

The system tray icon is missing. How do I make it appear again?

On the client computer, click **Start | Programs | SonicWALL | Enforced Client | SonicWALL Enforced Client** to display M in the system tray.

Why does the online help not display correctly?

If the built-in help system displays incorrectly on a client computer, its version of Microsoft Internet Explorer might not be using ActiveX controls properly. These controls are required to display the help file. Make sure that you install the latest version of Internet Explorer with its Internet security settings set to **Medium** or **Medium-high**.

Error messages

Click these links to see details about common error messages and solutions:

- *A file needed to install the software is not available. Please click the installation URL to begin the installation process again*
- *Cannot find remote shared directory*
- *File does not exist*
- *Installation cannot proceed because you have selected not to accept a vital agent component...*
- *Installation Declined*
- *Installation Denied*
- *Invalid Entitlement Error*

- *MyASUtil.SecureObjectFactory error message*
- *MyINX Error*
- *Unable to connect to the Enforced Client update server*
- *Unable to create Cab Installer Object*
- *Your current security settings prohibit running ActiveX controls on this page*

A file needed to install the software is not available. Please click the installation URL to begin the installation process again

When a user clicks the installation URL to download the installation file, a cookie is created. The cookie expires after 24 hours. If the user saves the installation file and then tries to install it after 24 hours have passed, or deletes the cookie, that user must download the file and begin the installation process again.

Cannot find remote shared directory

This error appears during a failed push installation. The target computers did not meet one or more of the following requirements:

- File and Print Sharing must be enabled.
- User-level access control must be configured.
- The person initiating the push must have domain administrator rights.
- They must not be running Microsoft Windows XP Home Edition, which does not support Windows NT Domain logins.

Check if the client computer you are pushing to has the appropriate shares enabled, and if you have appropriate administrator rights to perform a push installation to that computer. To check:

1 On the client computer, select **Start | Run**.

2 In the **Open** text box, type `\\CPUNAME\ADMIN$` (where `CPUNAME` is the name of the computer to which you are pushing); then click **OK**.

   The \WINDOWS directory of the computer to which you are trying to push should be displayed. If you do not have sufficient administrator rights to that computer, or if that computer does not have appropriate user-level access and sharing enabled, a **Network path not found** error dialog box appears.

3 See your Windows networking documentation for information on fixing your network administrative settings.

File does not exist

This Microsoft Windows error might appear in the foreground at the same time the threat detection dialog box displayed by the virus and spyware protection service appears in the background. This error verifies that the service is protecting your computer from threats. When you clicked to open an infected file from Windows Explorer, the service’s on-access scanner immediately detected and deleted the file, so that Windows could not open it.

Installation cannot proceed because you have selected not to accept a vital agent component...

The full text of the error message is **Installation cannot proceed because you have selected not to accept a vital agent component, you don’t have administrative rights to your machine, or other issues occurred**. This error message can be caused by several different problems:

The security level of the browser is too high.
Set the browser's security level to **Medium** or **Medium-high** (see *Configure your browser* on page 33).

Internet Explorer is blocking ActiveX controls.
Click the narrow bar at the top of the **Installation Denied** page and select **Install ActiveX Control**. This returns you to the original installation page, where you can enter an email address and proceed successfully.

The user doesn't have administrator rights.
Users must have administrator rights to install protection services on client computers. If they do not, you need to install the standalone installation agent (see *Install the standalone installation agent* on page 34).

A registry file is missing.
The system file REGEDIT.EXE might be missing. Search for that file in the client computer's \WINDOWS folder. If the file is missing, replace it using the original Windows install media or copy it from another computer that is running the same operating system.

The browser cache is full.
Empty the Internet Explorer cache:

versions 5.5 and 6.x

1. Open the **Internet Properties** dialog box. Either:
   - Right-click the **Internet Explorer** icon on the desktop and select **Properties**.
   - From Windows **Control Panel**, open **Internet Options.**
2. Under **Temporary Internet Files**, click the **Delete Files** button.
3. Select **Delete all offline content**, then click **OK**. An hourglass appears while the files are being deleted.
4. Under **Temporary Internet Files**, click **Settings**, then click **View Files**.
5. Select **Edit | Select All.**
6. Select **File | Delete**. It might take a while for all the files to be deleted. When the deletions are complete. you are returned to the **Internet Properties** dialog box.
7. Click **OK**.

version 7.0

1. Open the **Internet Properties** dialog box. Either:
   - Right-click the **Internet Explorer** icon on the desktop and select **Properties**.
   - From Windows **Control Panel**, open **Internet Options.**
2. Under **Browsing history**, click **Delete**.
3. Under **Temporary Internet Files**, click the **Delete files** button.

Installation Declined
This message can appear after a failed installation or uninstallation of Enforced Client. It indicates that leftover product files need to be removed from the client computer. Remove these components by downloading and running the MVSUninstall cleanup utility on the computer where you need to install (see *Download utilities* on page 86).

Installation Denied

Common causes and solutions:

- When you begin the installation, Internet Explorer displays a dialog box asking you to verify that you want to install Enforced Client. You must click **Yes**.
- The browser must be able to run ActiveX controls.
  - Set the browser's Internet security setting to **Medium** or **Medium-high** (see *Configure your browser* on page 33).
  - If the narrow bar at the top of the **Installation Denied** web page displays a message about ActiveX controls, click the bar and select **Install ActiveX Control**. You return to the original installation page, where you can enter an email address and proceed successfully.
- Users must have administrator rights to install protection services on client computers. If they do not, you need to install the standalone installation agent (see *Install the standalone installation agent* on page 34).
- Check to be sure the system drive has enough free space. When installing all the protection services, a maximum of 50 MB might be required.
- The Windows system file REGEDIT.EXE must be present in the Windows directory. If it is missing, replace it using the original Windows install media or copy it from another computer that is running the same operating system.

Invalid Entitlement Error

The installation URL in your email message might have been truncated or badly formatted. Make sure that you are using the entire URL with no spaces, and that the company key at the end of the URL is complete. (The company key is the value after the characters `CK=`.) You might need to paste the URL into your web browser if you cannot click it from your email message.

This error can also indicate that the trial evaluation period or subscription has expired, or that you are attempting to install protection services on more computers than you have purchased licenses for.

MyASUtil.SecureObjectFactory error message

The SecureObjectFactory Class program might have become corrupted. To verify this, check the status of the SecureObjectFactory Class program file:

1. Launch Internet Explorer.
2. From the **Tools** menu, select **Internet Options**.
3. In the **Temporary Internet Files** section of the dialog box, click **Settings** to display the **Settings** dialog box.
4. Click **View Objects** to open the **Downloaded Program Files** folder.
5. Find the entry for **SecureObjectFactory Class**. Make note of the information in the **Status** and **Creation Date** columns:
   - If the status and dates are listed as **Unknown**, delete the SecureObjectFactory Class program file. Uninstall and reinstall Enforced Client to reload the file.
   - If the status is listed as **Installed**, with valid dates, the file is not damaged.

- If there is another comment in the **Status** column, contact product support with that information.

> If you do not see a **Status** column, set your view options to **Details**.

MyINX Error
The installer has detected other virus protection software on the computer, which you must uninstall:

1 From the Windows **Control Panel**, open **Add/Remove Programs**.

2 In the list of programs, locate any virus protection software (including Enforced Client), then click **Remove**.

3 Begin the installation process again.

If you have uninstalled Enforced Client and still receive this error, some components might be installed but not visible, because the installation was only partially completed. Remove these components by downloading and running the MVSUninstall cleanup utility on the computer where you need to install (see *Download utilities* on page 86).

Unable to create Cab Installer Object
One possible cause is that the service MYAGTSVC.EXE is no longer running on the computer. You must manually restart it:

1 Select **Start | Run**.

2 Type the path to MYAGTSVC.EXE (you can use **Browse** to locate the file) and add the option `/start`. For example:

```
C:\winnt\mycio\agent\myagtsvc.exe /start
```

3 Click **OK**.

If that does not solve the problem, contact product support.

> This is a Microsoft Internet Explorer error, and might require installing a Microsoft patch.

Unable to connect to the Enforced Client update server
This error can be caused by several different problems:

The computer is not connected to the Internet.
Check the computer's connection to the Internet. It must be able to connect to the Internet directly or through a relay server.

The security level of the browser is too high.
Set the browser's security level to **Medium** or **Medium-high** (see *Configure your browser* on page 33).

You need to empty the Internet Explorer cache.

versions 5.5 and 6.x
1 Open the **Internet Properties** dialog box. Either:

- Right-click the **Internet Explorer** icon on the desktop and select **Properties**.

- From Windows **Control Panel**, open **Internet Options.**

2 Under **Temporary Internet Files**, click the **Delete Files** button.

3 Select **Delete all offline content**, then click **OK**. An hourglass appears while the files are being deleted.

4 Under **Temporary Internet Files**, click **Settings**, then click **View Files**.

5 Select **Edit | Select All.**

6 Select **File | Delete**. It might take a while for all the files to be deleted. When the deletions are complete. you are returned to the **Internet Properties** dialog box.

7 Click **OK**.

version 7.0

1 Open the **Internet Properties** dialog box. Either:

- Right-click the **Internet Explorer** icon on the desktop and select **Properties**.
- From Windows **Control Panel**, open **Internet Options.**

2 Under **Browsing history**, click **Delete**.

3 Under **Temporary Internet Files**, click the **Delete files** button.

You might need to adjust your corporate firewall or proxy settings.
See *If you use a corporate firewall or proxy server* on page 45.

Your current security settings prohibit running ActiveX controls on this page
Click the narrow bar at the top of the **Installation Denied** page and select **Install ActiveX Control**.

Contacting product support

There are three ways to contact product support.

By email
To contact product support via email, refer to your welcome email for your service provider's support address.

By phone
To access a list of current phone numbers for product support, visit:

http://www.mcafee.com/us/about/contact/index.html

From the web

1. Log on to the SecurityCenter with your user name and password.
2. Click the **Help** tab, then select **Contact Support** to display a form where you can submit a description of your problem to a product support representative.

Browser protection support
Before using the feedback feature to submit a question to product support, check the online list of frequently asked questions for the browser protection service. This list contains answers to the most common questions from users, organized by topic.

To view frequently asked questions:
From the SiteAdvisor menu, select **Help**.

Additional sources of support are available for the browser protection service.

To request support for SiteAdvisor:

1. From the SiteAdvisor menu, select **Send feedback**.
2. Select **General SonicWALL Product Support**.
3. Click a link for **Customer Service**, **Technical Support**, **Virus Removal Services**, or a SonicWALL partner company.

   A corresponding page appears with frequently asked questions and additional links for assistance.

Glossary

action item

Indicator of a potential vulnerability in your organization’s security that requires attention. Action items appear in red on the SecurityCenter website in three locations: **SecurityCenter** page, **Computer Details** page, and in reports (as dates).

action taken

How SonicWALL protection services handle or respond to detections; for example, **Cleaned** indicates that the detected threat was successfully removed.

administrative reports

See *reports*.

administrator

A user account with read, write, and delete permissions that manages an organization’s Enforced Client account. The administrator installs the software, receives status emails, and can access the SecurityCenter website.

Compare to *group administrator* and *user*.

agent

See *client software*.

allowed Internet application

An application, detected by the firewall protection service, that is specified as safe for contacting the Internet. Administrators make this selection in a policy; users respond to a prompt.

approved program

A program, detected by the virus and spyware protection service, that is specified as safe and should not be detected. Administrators make this selection in a policy; users respond to a prompt.

Avert Labs

SonicWALL Avert Labs; a research center that supports the computing public and SonicWALL customers by researching the latest threats, and by uncovering threats that may arise in the future.

blocking

Action taken by the firewall protection service to intercept and prevent a communication attempt.

browser protection service

A service that provides safety ratings for websites and reports detailing known website threats.

Compare to *email security service*, *firewall protection service*, and *virus and spyware protection service*.

catalog file

A file on the Internet *update site* that contains version information for every component in Enforced Client. Client computers check the latest catalog file to determine if their software components are up-to-date. The catalog file is stored in a compressed, digitally signed .CAB file format.

Clean Failed

The virus and spyware protection service could not clean or delete the item. This might indicate that the item is in use; if so, close it and attempt the clean again. This might also indicate that the item resides on read-only media, such as a CD. If so, no further action is required. The virus and spyware protection service has prevented the original file from being accessed by the client computer, but it cannot delete the item. Any files copied to the computer have been cleaned. If the item is not in use or on read-only media, further action might be required to ensure the computer is not at risk.

clean, cleaning

(1) Action taken by the virus and spyware protection service when it detects a threat such as a virus, Trojan horse, or worm. The cleaning action can include removing the threat from a file and restoring the file to usability; removing references to the threat from system files, system .INI files, and the registry; ending the process generated by the threat; deleting a macro or a Microsoft Visual Basic script that is infecting a file; deleting a file if it is a Trojan horse or a worm; renaming a file that cannot be cleaned.

(2) A label applied to email that has been inspected by the email security service and found free of inappropriate content such as spam, phishing attempts, viruses, or particular content identified by your organization as undesirable.

client computer

A computer on which the Enforced Client client software is installed.

client software

The Enforced Client software module installed on each client computer. It serves as an intelligent link between the client computer and the SecurityCenter website by performing tasks (such as scanning and updating) on the client computer and sending report data to the SecurityCenter.

Compare to *SecurityCenter website*.

configuration settings

See *policy*.

connection type

The type of network environment to which a client computer is connected; used by the firewall protection service to determine whether to trust communications from other computers on the same network.

See also *custom connection type, trusted connection,* and *untrusted connection*.

custom connection type

A network environment where only specified communications are allowed. The firewall protection service allows communications only from IP addresses and ports defined by the administrator.

Compare to *trusted connection* and *untrusted connection*.

Customer Home site

See *SecurityCenter website*.

deployment

Distributing and installing the Enforced Client client software to computers from a central location, such as the administrative computer, via the silent installation or push installation method.

Compare to *URL installation*.

detection definition files

DAT files (also referred to as signatures) that identify the code which anti-virus and anti-spyware software detect to repair viruses, Trojan horses and potentially unwanted programs (PUPs).

directory harvest attacks (DHA)

Attempts to retrieve lists of valid email addresses from email servers. The email security service analyzes every IP address that connects to an email server and blocks messages that exhibit the characteristics of a directory harvest attack.

download site

The SonicWALL website for retrieving product, DAT file, and engine updates.

EICAR test file

European Institute of Computer Anti-Virus Research has developed a file consisting of a string of characters that can be used to test the proper installation and operation of anti-virus and anti-spyware software.

email security service

A web-based service that safeguards small business computers by automatically routing email messages through SonicWALL's servers and scanning for dangerous and inappropriate content before delivering the messages to the local network.

Compare to *browser protection service, firewall protection service,* and *virus and spyware protection service*.

event

See *inbound event*.

firewall protection service

A web-based service that safeguards small business computers by automatically monitoring communications from other computers and Internet applications to check for suspicious activity, then generating reports.

Compare to *browser protection service, email security service,* and *virus and spyware protection service*.

group

One or more client computers defined by a system administrator for managing security settings and analyzing report data. Groups can be determined by geographic location, department, computer type, or anything meaningful to your organization.

group administrator

A user account with permissions to monitor one or more assigned groups of computers. The account administrator sets up a group administrator account, assigns a password for accessing the SecurityCenter website, and specifies an access level that determines which tasks the group administrator is authorized to perform. Access levels are **Read Only** and **Read & Modify Reports**.

Compare to *administrator* and *user*.

inbound event

An attempt by another computer to send data to a client computer. The firewall protection service running on the client computer intercepts this attempt and responds according to policy settings.

installation

Installing the Enforced Client client software on computers.

See also *push installation*, *silent installation*, and *URL installation*.

installation URL

A company-specific URL for installing Enforced Client software on client computers.

See also *URL installation*.

Internet application

An application that communicates with both the Internet and a client computer.

Internet Independent Updating (IIU)

A method that allows computers not connected to the Internet to use Enforced Client. At least one computer on the subnet needs to have an Internet connection to be able to communicate with the SonicWALL update site. This computer is configured as a relay server, and other computers communicate with the update site through it.

See also *relay server*, *rumor technology*, and *update site*.

license

An agreement to install SonicWALL software on a single client computer. When you purchase a subscription for SonicWALL protection services, you designate a specific number of licenses for the computers where the software using those services will be installed. You can also add and renew licenses for your subscription.

Compare to *subscription*.

mail exchange record

MX record; a software entry in your email domain name database that controls where email is routed.

MX record

See *mail exchange record*.

notification preferences

Information designating which automatically generated account emails, such as status emails and notices of account expiration, should be sent by the service provider. Administrators can configure notification preferences on the **My Account** page of the SecurityCenter website.

outbreak DAT file

A special detection definition file marked as **Medium** or **High** importance and released by SonicWALL Avert Labs in response to an outbreak. It is specially encoded to inform the first computer receiving it to share the update immediately with other client computers on the network. Administrators can configure a policy setting to check for outbreak DAT files more frequently than regular updates.

See also *detection definition files*.

policy

A group of security settings that define how each SonicWALL protection service operates on client computers. Policies determine which programs and communications are detected as threats, the response to detections, the frequency of tasks such as scans and updates, and the implementation of many other features. A policy can be assigned to one or more client computers.

portal, email security service

A website where administrators can customize and view reports for the email security service. The portal's home page is accessed through links on the SecurityCenter website.

profile

Information for contacting a designated recipient (usually the account administrator) with information about a Enforced Client subscription. Administrators can configure profile data on the **My Account** tab of the SecurityCenter website.

prompt mode

An operating mode in which the client software prompts the user for a response to each detection; can be configured for spyware protection and for the firewall protection service in a policy.

Compare to *protect mode* and *report mode*.

protect mode

An operating mode in which the client software blocks or attempts to clean detections automatically. Administrators can configure Prompt mode for spyware protection and for the firewall protection service in a policy. If the firewall protection service detects an unrecognized program, it blocks it. If the virus and spyware protection service detects a potentially unwanted program, it attempts to clean it.

Compare to *prompt mode* and *report mode*.

push installation

Remotely deploying the Enforced Client software directly from the service provider's website to one or more client computers, eliminating the need for any user interaction.

Compare to *silent installation* and *URL installation*.

quarantine

Enforced isolation of a file or folder — for example, to prevent a threat or to isolate a spam email message — until action can be taken to clean or remove the item.

quarantine folder

The location on a computer system for storing email messages that might contain virus or other suspicious code; messages are stored until they can be reviewed and a course of action determined.

registry keys

Information stored in the Microsoft Windows system registry, which is a database containing the information required to configure a client system. Registry keys identify installed hardware, installed applications and their configuration settings, registered ports, and much more. Unwanted programs can change the value of registry keys or create new ones to execute malicious code.

relay server

A network computer with an Internet connection that downloads updated files from the SonicWALL update site for retrieval by other network computers without Internet connections.

See also *Internet Independent Updating (IIU)*, *rumor technology*, and *update site*.

report mode

An operating mode in which the client software logs detections for reporting purposes but does not take additional action; can be configured for spyware protection and for the firewall protection service in a policy.

Compare to *prompt mode* and *protect mode*.

reports

Data uploaded by client computers to the SecurityCenter and formatted for the administrator; information on the account's security status for the administrator.

response

How SonicWALL protection services handle or take action on detections; for example, **Cleaned** indicates that the detected threat was successfully removed from the item where it was found.

rumor technology

A method that allows all computers on a subnet to share downloaded files, saving each computer from having to download from the update site on the Internet every time it needs an updated file.

See also *Internet Independent Updating (IIU)*, *relay server*, and *update site*.

scan

An examination of files to determine if a threat is present.

See *on-access scanning* and *on-demand scanning*.

scanning engine

The mechanism that drives the scanning process.

script scanning

A protection method that detects harmful scripts contained in files, emails, and web pages. Scripts are programs or sequences of instructions that are run by other programs instead of by a computer's processor.

SecurityCenter website

A website containing the administrative features of Enforced Client, where administrators can centrally manage protection services on client computers. Formerly known as the *Customer Home site*.

Compare to *client software*.

silent installation

Remotely deploying Enforced Client software onto a client computer, eliminating the need for any user interaction.

Compare to *push installation* and *URL installation*.

spooling

Storing data at an alternate location so that it can be processed later. When your local email server is not accepting email, the email security service spools your organization's email to SonicWALL's server, then delivers the email when your local email server is functioning properly again. SPOOL stands for Simultaneous Peripheral Operations On Line.

subscription

An agreement to receive access to electronic protection services for a specified period of time. While your subscription is active, you receive regular updates

Compare to *license*.

system services

Functionality provided by software running on the network that performs essential tasks, such as transmitting or converting data in a network, delivering and receiving email, or interacting with applications on the Internet.

task

An activity (both one-time such as *on-demand scanning*, and routine such as *updating*) that is scheduled to occur at a specific time, or at specified intervals.

Compare to *policy*.

Enforced Client icon

The icon that appears in the system tray of client computers running the Enforced Client software. Click the icon to display a menu of commands, or double-click the icon to manually update the computer.

trusted connection

A connection to a home or office network that is protected from the Internet by hardware such as a router or firewall. The firewall protection service allows communications from other devices on a trusted network (it considers them to be safe).

Compare to *untrusted connection*.

untrusted connection

A direct connection to the Internet, such as a wireless network in a public airport or hotel. The firewall protection service blocks communications from other devices on an untrusted network (it considers them to be unsafe).

Compare to *trusted connection*.

update site

A repository on the Internet from which a client computer retrieves updates.

updates

Files from SonicWALL that provide more current information to a product. Updates can include upgraded software components and definition detection (DAT) files containing revised information about existing threats and new information about recently identified threats.

See *detection definition files*.

updates

Files from SonicWALL that provide more current information to a product. Updates can include upgraded software components and DAT files containing revised information about existing threats and new information about recently identified threats.

See also *detection definition files*.

updating

The process of installing updates to existing products or upgrading to new versions of products.

URL installation

Installing the Enforced Client client software locally on a client computer by clicking a link to a unique website, sent via email from an administrator. The URL determines the protection services installed, the language for Enforced Client services, and the group where the computer is placed.

Compare to *push installation* and *silent installation*.

user

The person who uses the Enforced Client software on a client computer.

Compare to *administrator* and *group administrator*.

utilization

The way in which your licenses for SonicWALL protection services are being used. Enforced Client issues utilization action items and notifications when you attempt to install client software on more computers than you have purchased licenses for, or when the number of computers you have installed client software on approaches the number of licenses you have purchased.

virus and spyware protection service

A web-based service that safeguards small business computers by automatically checking files and email messages for viruses and spyware, then generating reports.

Compare to *browser protection service*, *email security service* and *firewall protection service*.

A User Interface Definitions

Login page

Use this page to log on to the SonicWALL SecurityCenter website, where you can manage your account and view reports.

- *Log on to the SecurityCenter*
- *Change your SecurityCenter password*

Item	Description
	Type the email address for your account. In most cases, this is the email address you used when registering for Enforced Client.
Password	Type the password for your account. See your welcome email from your service provider for your initial password.
Remember me on this computer	Select this option if you want to access this site in the future without signing in. Do not select this option if you share this computer with non-administrative co-workers.
Add this page to your favorites	Select this option to add this page to your browser's Favorites list.
Log In	Click to open the SecurityCenter.

SecurityCenter tab

Use this page to see an overview of your account's protection services. You can display the status of all computers or select one of the groups you have created.

- *Viewing your security services at-a-glance*
- *Install protection services*
- *View and resolve action items*
- *View security coverage for your account*

Item	Description
Install Protection	Click to install Enforced Client services on one or more client computers. The installation wizard will display and step you through the process of selecting the computers and services to install.
Groups	Select which group of computers to display. If you have not created any groups, this option does not appear and all your computers are displayed.
Security Status	Lists security issues that require you to take action. Click a red action item to display instructions for resolving the problem.

Item	Description
Coverage	Shows the protection status for your computers. Click a color in the pie chart to open the **Product Coverage** page, which lists details about the computers with the corresponding status. The pie chart appears only for services you have installed. For other services, a status message appears.
Subscription	Shows the status of your subscriptions and licenses for protection services.
Buy **Buy More** **Renew** **Try**	Select a link to open the **Product Purchase** page, where you can buy new or additional services, renew services, or sign up for a trial subscription.
Install	Select this link to install the protection service on one or more client computers. The installation wizard will display and step you through the process of selecting the computers and services to install.
Subscribe	Select this link to subscribe to the email protection service.
Click here to configure	Select this link to configure the email protection service.

Computers tab

Use this page to manage client computers where Enforced Client is installed. You can display all computers or one of the groups you have created, then select individual computers to manage or view details.

Select a checkbox next to a computer name to select that computer; select the checkbox in the heading to select all computers.

- *Managing your computers*
- *Install protection services*
- *Display details for a computer*
- *View detections for a computer*
- *View user-approved applications for a computer*
- *Send email to computers*
- *Block computers from receiving updates*
- *Delete computers from your reports*
- *Move computers into a group*
- *Make the most of your online data*
- *Customize listings and reports*
- *Specify approved programs*
- *Set up allowed Internet applications*

Item	Description
Find computers	Type a full or partial computer name, email address, IP address, or relay server name in the box, then click **Search** to display computers matching your search criteria. **Note:** All the client computers in your account are searched.
Add Computer	Click to install Enforced Client services on one or more new client computers. The installation wizard will display and step you through the process of selecting the group and services to install.
Groups	Select which group of computers to display. If you have not created any groups, this option does not appear. All your computers are displayed.
Report period	Select the time period to display.
Computer status	Select the type of detections to display.
Email button	Click to open a blank email message addressed to the selected computers. (You must have a local email application installed to use this feature.)
Delete	Click to delete the selected computers from your listing. Use this feature to delete duplicate and obsolete computers. If you delete a computer where a valid service is installed, it will be added back to your listing the next time you log on.
Block	Click to prevent the selected computers from receiving product updates. Use this feature to keep unauthorized computers from using your protection services.
Move to	Select a group to move selected computers into. To create a group, go to the **Groups + Policies** page. Then use this **Move to** list to move computers into the new group.
Move	Click to move the selected computers into the selected group.
Computer	Lists each computer where Enforced Client is installed. Select a computer's name to display detailed information about it.
Group	Shows which group each computer belongs to.
Email	Shows the email address for each computer. Select an address to open a blank email message addressed to that computer. (You must have a client email application installed to use this feature.) To send an email message to multiple computers instead, select the computers, then click the **Email** button.
Last Connect	Shows when a computer last connected to the network. The date appears in red for out-of-date computers. To view instructions for updating an out-of-date computer, select the computer name to open the **Computer Details** page, then click the red action item.
DAT Date	Shows when the detection definition (DAT) file was last updated. The date appears in red for out-of-date computers. To view instructions for updating an out-of-date DAT file, select the computer name to open the **Computer Details** page, then click the red action item.

Item	Description
Detections	Shows the total number of detections for each computer during the selected time period. Select the quantity to display a list of the detections.
User-Approved Applications	Shows the number of detected applications the user approved to run on each computer. Select the quantity to display details about the applications. To approve an application for other users, you need to add it to a policy. After you approve detected programs and Internet applications, they are no longer detected as threats on client computers using the policy.

Reports tab

Use this page to access administrative reports. The information in these reports is uploaded from client computers hourly.

- *Viewing reports*
- *View detections*
- *View unrecognized programs*
- *View unrecognized Internet applications*
- *View inbound events blocked by the firewall*
- *View duplicate computers*
- *View computer profiles*
- *View your detection history*
- *Viewing reports for the email security service*
- *Make the most of your online data*
- *Customize listings and reports*
- *Manage your protection strategy with best practices*
- *Managing suspicious activity with best practices*

Item	Description
Detections	Select this link to display a report listing viruses, potentially unwanted programs, and buffer overflow processes detected on your computers.
Unrecognized Programs	Select this link to display a report on potentially unwanted programs blocked by the virus and spyware protection service and Internet applications blocked by the firewall protection service.
Inbound Events Blocked by Firewall	Select this link to display information about incoming communications blocked by the firewall protection service.
Duplicate Computers	Select this link to display a list of computers that appear to be listed more than once for your account. Duplicates might indicate obsolete computers of those where Enforced Client was installed more than once.
Computer Profiles	Select this link to display the operating system and browser versions running on your computers.

Item	Description
Detection History	Select this link to display a graphical overview of your detections for the past year.
Email Security Reports	Select this link to open the email security service's portal, where you can access reports about email traffic and detections.

Groups + Policies tab

Use this page to create and manage groups and policies:

- A **group** consists of one or more computers that use the same security settings. Create groups to organize computers so that you can manage them more easily. You might create groups based on physical locations (for example, Home Office and Travel Team) or the types of tasks performed (for example, Accounting and Online Marketing Research).
- A **policy** is made up of security settings that define how the protection services operate on client computers. Create policies to regulate security settings for different types of users. You might create one policy for desktop computers in the office and another policy for laptop computers that are used outside the office.
- *Creating groups to manage your site*
- *Setting up policies*
- *Configuring policies for virus and spyware protection*
- *Configuring policies for firewall protection*
- *Configuring a policy for email security*

Item	Description
	Lists the groups defined for your account. If you have not created any groups, only the **Default** group appears.
Add Group	Select this link to create a group.
Edit/Assign Policy	Select this link to rename a group or change the policy assigned to it. You cannot rename the **Default** group.
Delete	Select this link to remove a group you have created. You cannot delete the **Default** group.
Policy section	Lists the policies defined for your account. If you have not created any policies, only the **SonicWALL Default** policy appears.
Add Policy	Select this link to create a policy. The new policy initially contains the default settings, which you can change.
View	Select this link to display settings for the **SonicWALL Default** policy.
Edit	Select this link to rename a policy or change its settings. You cannot edit the **SonicWALL Default** policy.
Delete	Select this link to remove a policy you have created. You cannot delete the **SonicWALL Default** policy.

My Account tab

Use this page to manage information for your protection services account.

- *Setting up your account*
- *Change your SecurityCenter password*
- *Managing your subscriptions*
- *Designating group administrators*
- *Sign up for email notifications*
- *Add your logo to reports*

My Profile section

Shows contact information associated with your account. Your service provider uses this information to communicate with you. It is important to keep this information up-to-date.

Item	Description
	Select this link to modify the contact settings for your account, including your password for accessing the SecurityCenter.

Service Summary section

Shows an overview of each subscription that includes the type, the number of licenses in use, the number of licenses purchased, and the expiration date for the licenses that will expire first. Expiration dates less than 60 days in the future appear in red.

Item	Description
	Select this link to open the **Subscription History** page, with details about your previous service subscriptions.
Buy **Buy More** **Renew** **Try**	Select a link to open the **Product Purchase** page, where you can buy new or additional licenses, renew licenses, or sign up for a trial subscription.

Group Administrators section

Lists the group administrators defined for your account. Group administrators help to distribute administrative tasks within an organization by managing their assigned groups.

If you have created more group administrators than can be displayed on this page, the most recently viewed administrators appear here. Select All Group Administrators to view a complete list.

Item	Description
	Select this link to create a new group administrator account or edit an existing account.
All group administrators	Select this link to open a page where you can view and edit all groups administrator accounts for your organization.
Name	Shows the name you entered for identification purposes when you created the group administrator's account.
Email Address	Select an address to open a blank email message addressed to the group administrator. (You must have a local email application installed to use this feature.)
Groups	Lists the groups assigned to the group administrator account. The group administrator can manage only the assigned groups.
Access Level	Shows the access level assigned to the group administrator account: ■ **Read only**: The group administrator can access group and report information. ■ **Read and modify reports**: The group administrator can access and modify group and report information.
	Shows the date and time the group administrator last logged on to the SecurityCenter.
Edit	Select this link to modify the settings for the group administrator.
Email Password	Select this link to open an email message addressed to the group administrator that includes the password, assigned groups, and instructions for accessing information about responsibilities. (You must have a local email application installed to use this feature.)
Delete	Select this link to remove the group administrator account.

Notification Preferences section

Shows which account emails you have selected to receive. Your service provider determines which emails are available for you to select.

Item	Description
	Select this link to modify your notification preferences for receiving account emails.

My Logo section

Shows the logo that currently displays when you send reports to users or customers.

- If you have not uploaded a logo, a placeholder appears.
- If your service provider has uploaded a customized logo to the SecurityCenter, this feature is not available for your logo.

Item	Description
	Select this link to open a page that allows you to upload a new logo or delete a logo.

Help tab

Use this page to access online product documentation and to contact customer support.

- *View printed and online documents*
- *Download utilities*
- *Contact product support*

Item	Description
	Select this link to display a document that describes how to use the basic features of Enforced Client. This document is recommended for new administrators and those who want an overview of changes to the product. You can view and print this document in PDF format.
Product Guide	Select this link to display an in-depth guide to product features. This document is recommended for hands-on administrators and Partner Security Services administrators who want to understand how Enforced Client works, to set up groups and policies, or to use advanced features. You can view and print this document in PDF format.
Release Notes	Select this link to display the ReadMe file shipped with Enforced Client. You can view and print this document in text format.
Utilities	Select this link to open a page where you can download software tools for installing Enforced Client and troubleshooting installation problems.
Contact Support	Select this link to open a form where you can enter a description of your problem to submit to product support.

Email Page

Use this page to send data from the SecurityCenter to users and customers in email. The page you are sending will be attached to an email message in .MHTM format.

Item	Description
	Shows which SecurityCenter page you are sending.
From email address	Displays the email address for this account.
To email address(es)	Type email addresses where you want to send the data, or select them from the list on the right and click **Add**. If you type addresses, separate them with a comma.
Subject	Displays the name of the page you are sending. Edit this information if needed.
Your message	Type a description of the information you are sending or any other message.
Send	Click to send the message.
Cancel	Click to return to the previous page without sending a message.

Install Protection

Use this page to select the computers where you want to install protection services or to install the email security service.

- *Installing Enforced Client*
- *Standard URL installation*
- *Using the portal*

Item	Description
	Select this option to install one or more protection services onto one or more computers where Enforced Client *is not* already installed.
Install additional protection onto existing computers (already managed by SecurityCenter)	Select this option to install one or more protection services onto one or more computers where Enforced Client *is* already installed.
Install email security service (email protection)	Select this option to view your Mail eXchange (MX) record settings, contact product support, or access the email security service's portal. If you have not purchased and activated the email security service, this option does not appear.
Next	Click to proceed to the next page. You must select an option before proceeding.
Cancel	Click to end the installation process.

Install Protection: New Computers

Use this page to select your installation settings.

- *Standard URL installation*

Item	Description
	Select the group to place the new computer(s) in.
Products	Select the protection service(s) to install.
Language	Select the language of the protection service(s).
Back	Click to return to the previous page.
Next	Click to proceed to the next page, where you can select an installation method. You must select at least one protection service to install before proceeding.
Cancel	Click to end the installation process.

Install Protection: New Computers: Email Text

Use this page select and proceed with an installation method.

- *Standard URL installation*
- *Advanced installation methods*

Item	Description
	To send users a URL they can use to install on their computers, first click this button. Then open a blank email message, paste the text you copied into its body, and send it to users who need to install the protection service(s). You will have the opportunity to edit the instructions in your email message before sending. **Note:** This button does not appear in the Firefox browser. In that case, you need to copy the text manually.
Install now on this computer	Select this link to install the selected protection service(s) on the local computer using the selected options.
Display advanced installation methods	Select this link to open a page where you can use the silent installation method or Push Install utility to deploy protection services on client computers without user interaction.
Cancel	Click to end the installation process.

Install Protection: Existing Computers

Use this page to select the protection services to install and the language.

- *Standard URL installation*

Item	Description
	Select the protection service(s) to install.
Language	Select the language of the protection service(s).
Back	Click to return to the previous page.
Next	Click to proceed to the next page, where you can select an installation method. You must select at least one protection service before proceeding.
Cancel	Click to end the installation process.

Install Protection: Existing Computers: Email Text

Use this page select and proceed with an installation method.

- *Standard URL installation*
- *Advanced installation methods*

Item	Description
Select Text and Copy to Clipboard	To send users a URL they can use to install on their computers, first click this button. Then open a blank email message, paste the text you copied into its body, and send it to users who need to install the protection service(s). You will have the opportunity to edit the instructions in your email message before sending. **Note:** This button does not appear in the Firefox browser. In that case, you need to copy the text manually.
Install now on this computer	Select this link to install the selected protection service(s) on the local computer using the selected options.

Item	Description
Display advanced installation methods	Select this link to open a page where you can use the silent installation method or Push Install utility to deploy protection services on client computers without user interaction.
Cancel	Click to end the installation process.

Install Email Security Service

Use this page to reference configuration information for your Mail eXchange (MX) records, contact support, and access the email security service's portal, where you can manage and view reports for the email security service.

- *Using the portal*
- *Update your MX records*
- *Viewing reports for the email security service*
- *Getting more information*

Item	Description
	Select this link to contact product support.
click here	Select this link to open the email security service's portal.

Advanced Installation Methods

Use this page to select an installation method for remotely deploying protection services on client computers without user interaction.

- *Advanced installation methods*
- *Silent installation*
- *Push installation*

Item	Description
	Select **VSSetup** to download an executable file that enables you to install protection services on a client computer without user interaction. The silent installation method requires a method for installing executable files on your network computers. For example: - A third-party deployment tool, such as Novell NAL, ZenWorks, Microsoft Systems Management Server (SMS) installer, or Tivoli IT Director. - A login script. - A link to an executable file in an email message.
Install protection services remotely using the Push Install utility	Select **Run the Push Install utility** to download and run a utility from your administrative computer that *pushes* the client software directly from your service provider's site to one or more client computers without user interaction. To use the Push Install utility, the administrative computer must be running Windows 2000, Windows XP Professional, or Windows Vista.

Product Purchase

Use this page to purchase new or additional licenses for SonicWALL protection services or sign up for a trial subscription.

- *Managing your subscriptions*
- *Purchase, add, and renew services*
- *Request a trial subscription*

Item	Description
	Select this link if you purchased Enforced Client from a SonicWALL reseller.
Click here to...	Select this link for the region where you are located.
If you wish to update your email address, click here	Select this link to update the email address associated with your account. The current email address is displayed on this page. Your account is associated with a unique email address, which your service provider uses to contact you about issues specific to your account. It is important to use to keep this email address up-to-date, and use it when renewing or adding licenses and subscriptions to your existing account.

Product Coverage

Use this page to manage client computers with a particular status. You can display all computers with this status or a subset, then select individual computers. To select a computer, select the checkbox next to its name.

The **Group** and **Service** you selected on the **SecurityCenter** page determine which computers appear on this page. Depending on the **Status** you selected, computers on this page can be:

- **Up-to-Date**: The virus and spyware protection service is installed and the latest components have been downloaded.
- **Out-of-Date**: The virus and spyware protection service is installed, but newer versions of one or more components, such as the detection definition (DAT) file, are available from the update site.
- **Installed**: The firewall protection service is installed.
- **Not Installed**: The firewall protection service is not installed.
- *View security coverage for your account*
- *View and resolve action items*
- *Display details for a computer*
- *Make the most of your online data*
- *Customize listings and reports*

Item	Description
	Click to open a blank email message addressed to the selected computers. (You must have a client email application installed to use this feature.)
Delete	Click to delete the selected computers from your listing. Use this feature to delete duplicate and obsolete computers. If you delete a computer where a valid service is installed, it will be added back to your listing the next time you log on.
Block	Click to prevent the selected computers from receiving product updates. Use this feature to keep unauthorized computers from using your protection services.
Move to	Select a group to move selected computers into. To create a group, go to the **Groups + Policies** page. Then use this **Move to** list to move computers into the new group.
Move	Click to move the selected computers into the selected group.
Computer	Lists each computer where Enforced Client is installed. Select a computer's name to display detailed information about it.
Group	Shows which group each computer belongs to.
Email	Shows the email address for each computer. Select an address to open a blank email message addressed to that computer. (You must have a client email application installed to use this feature.) To send an email message to multiple computers instead, select the computers, then click the **Email** button.
Last Connect	Shows when a computer last connected to the network. The date appears in red for out-of-date computers. To view instructions for updating an out-of-date computer, select the computer name to open the **Computer Details** page, then click the red action item.
DAT Date	Shows when the detection definition (DAT) file was last updated. The date appears in red for out-of-date computers. To view instructions for updating an out-of-date DAT file, select the computer name to open the **Computer Details** page, then click the red action item.

Computer Details

Use this page to view detailed information about a single computer and manage the computer.

- *Managing your computers*
- *Make the most of your online data*
- *Customize listings and reports*
- *Specify approved programs*
- *Set up allowed Internet applications*

Item	Description
	Lists information about the computer and protection services.
System email address	Shows the email address used to contact the user. To change the address, type a new address.
Group	Shows the group to which this computer belongs. To move this computer to another group, select one from the list.
(Services)	Shows the status of each protection service. If a service you have subscribed to is not installed, a link appears that allows you to install it.
Action Items section	Lists security issues that require you to take action. Click an action item to display instructions for resolving the problem.
Computer Properties section	Lists information about software components on this computer, including the protection services, operating system, and web browser. Lists the computer's IP address.
Detections	Shows the total number of detections on this computer during several time periods. Select the quantity to display a list of the detections.
User-Approved Applications	Shows the number of detected applications the user approved to run on this computer. Select the quantity to display details about the applications. To approve an application for other users, you need to add it to a policy. When you approve detected programs and Internet applications, they are no longer detected as threats.
Save	Click to save changes you made to this page and return to the previous page.
Cancel	Click to return to the previous page without saving changes.

Detection List

Use this page to view detailed information about detections.

The **Computer**, **Report period**, and **Detection type** selected on the previous page determine the content of this listing.

- *View detections for a computer*

Item	Description
	Shows the name of the item that contains the detected threat. The item might be a file, cookie, or registry entry.
Detection	Select the name of the detected threat to display a detailed description from the SonicWALL Avert Threat Labs.
Date Found	Shows when the detection occurred.
Status	Shows the current status of the detection. Status can be: **Cleaned**, **Quarantined**, or **Buffer Overflow Blocked**.

User-Approved Application List

Use this page to view detailed information about detected programs and Internet applications that users have approved to run on their computers. These applications are no longer detected as threats on the computers where they are approved.

To approve these applications for use on other computers, you need to add them to a policy. After you approve detected programs and Internet applications, they are no longer detected as threats on any computers using the policy.

- *View user-approved applications for a computer*
- *Specify approved programs*
- *Set up allowed Internet applications*

Item	Description
	Shows the name of the detected application. For potentially unwanted programs, select the name of the detected threat to display a detailed description from the SonicWALL Avert Threat Labs.
Type	Shows the type of application: ■ Potentially unwanted program detected by the virus and spyware protection service. ■ Internet application detected by the firewall protection service.

Search Results

Use this page to locate and manage all client computers in your account that meet your search criteria.

- *Managing your computers*
- *Search for computers*
- *Display details for a computer*
- *Make the most of your online data*
- *Customize listings and reports*

Item	Description
Find computers	Shows the search criteria. To perform another search, type another full or partial computer name, email address, IP address, or relay server name in the box, then click **Search**.
Email button	Click to delete the selected computers from your listing. Use this feature to delete duplicate and obsolete computers. If you delete a computer where a valid service is installed, it will be added back to your listing the next time you log on.
Delete	Click to prevent the selected computers from receiving product updates. Use this feature to keep unauthorized computers from using your protection services.
Block	Select a group to move selected computers into. To create a group, go to the **Groups + Policies** page. Then use this **Move to** list to move computers into the new group.
Move to	Click to move the selected computers into the selected group.
Computer	Lists each computer where Enforced Client is installed. Select a computer's name to display detailed information about it.
Group	Shows which group each computer belongs to.

Item	Description
Email	Shows the email address for each computer. Select an address to open a blank email message addressed to that computer. (You must have a client email application installed to use this feature.) To send an email message to multiple computers instead, select the computers, then click the **Email** button.
Last Connect	Shows when a computer last connected to the network. The date appears in red for out-of-date computers. To view instructions for updating an out-of-date computer, select the computer name to open the **Computer Details** page, then click the red action item.
DAT Date	Shows when the detection definition (DAT) file was last updated. The date appears in red for out-of-date computers. To view instructions for updating an out-of-date DAT file, select the computer name to open the **Computer Details** page, then click the red action item.

Detections report (by computer)

Use this report to view and manage detections and the computers where detections occurred. You can display all computers or a subset, then select individual computers for managing or viewing details. To select a computer, select the checkbox next to its name.

- *View detections*
- *Make the most of your online data*
- *Customize listings and reports*
- *Manage your protection strategy with best practices*

Item	Description
Groups	Select which group of computers to display. If you have not created any groups, this option does not appear. All your computers are displayed.
Report period	Select the time period to display.
Detection type	Select the type of detections to display.
Group by	■ Select **Computer** to list the computers where detections occurred. ■ Select **Detection** to list the detections.
Email button	Click to open a blank email message addressed to all selected computers. (You must have a local email application installed to use this feature.)
Delete	Click to delete the selected computers from your listing. Use this feature to delete duplicate and obsolete computers. If you delete a computer where a valid service is installed, it will be added back to your listing the next time you log on.
Block	Click to prevent the selected computers from receiving product updates. Use this feature to keep unauthorized computers from using your protection services.

Item	Description
Move to	Select a group to move selected computers into. To create a group, go to the **Groups + Policies** page. Then use this **Move to** list to move computers into the new group.
Move	Click to move the selected computers into the selected group.
Name	Lists each computer where a detection occurred. ■ Select a computer to display detailed information about it. ■ Click the arrow next to a computer to display or hide a list of its detections. ■ Select a detection name to display details about it from the SonicWALL Avert Threat Labs Library.
Detected Objects	Shows the total number of detections. Select a quantity to display the **Detection List**, showing which items contained the detected threats.
Last Detection Date	Shows the most recent date that a detection occurred.
Email	Shows the email address for the computer. Select an address to open a blank email message addressed to that computer. (You must have a local email application installed to use this feature.) To send an email message to multiple computers instead, select the computers, then click the **Email** button.
Group	Shows which group the computer is assigned to.

Detections report (by detection)

Use this report to view and manage detections and the computers where detections occurred.

- *View detections*
- *Make the most of your online data*
- *Customize listings and reports*
- *Manage your protection strategy with best practices*

Item	Description
Groups	Select the group of computers to display. If you have not created any groups, this option does not appear.
Report period	Select the time period to display.
Detection type	Select the type of detections to display.
Group by	■ Select **Computer** to list the computers where detections occurred. ■ Select **Detection** to list the detections.
Name	Lists the name of each detected threat. ■ Select a detection to display detailed information about it. ■ Click the arrow next to a detection to display or hide a list of computers where it occurred. ■ Select a computer name to display details about it.

Item	Description
Detected Objects	Shows the number of occurrences for this detection. Select a quantity to display the **Detection List**, showing which items contained the detected threats.
Last Detection Date	Shows the most recent date that a detection occurred.

Unrecognized Programs report (by computer)

Use this report to view and manage detected programs that were not recognized by the virus and spyware protection service or firewall protection service, and the computers where these programs were detected.

You can display all computers or a subset, then select individual computers for managing or viewing details. To select a computer, select the checkbox next to its name.

To approve any of these applications for use on client computers, you need to add them to a policy. After you approve detected programs and Internet applications, they are no longer detected as threats on the computers using the policy.

- *View unrecognized programs*
- *Make the most of your online data*
- *Customize listings and reports*
- *View user-approved applications for a computer*
- *Specify approved programs*
- *View user-approved applications for a computer*
- *Set up allowed Internet applications*
- *Manage your protection strategy with best practices*
- *Managing suspicious activity with best practices*

Item	Description
Groups	Select the group of computers to display. If you have not created any groups, this option does not appear.
Report period	Select the time period to display.
Program type	Select the status of detections to display: ■ **All**: All detected programs. ■ **Firewall-Blocked Programs**: Internet applications blocked by the firewall protection service. ■ **Potentially Unwanted Programs**: Programs detected by the virus and spyware protection service as possible spyware.
Group by	■ Select **Computer** to list the computers where detections occurred. ■ Select **Detection** to list the detections.

Item	Description
Computer	Lists each computer where a detection occurred. ■ Select a computer to display detailed information about it. ■ Click the arrow next to a computer to display or hide a list of its detections. ■ Select the name of a potentially unwanted program to display details about it from the SonicWALL Avert Threat Labs Library.
Programs	Shows the number of detections that occurred on the computer.
Type	Shows the type of program detected: **Firewall-Blocked Programs** or **Potentially Unwanted Programs** detected by the virus and spyware protection service. **Mixed** indicates that both types of programs were detected.

Unrecognized Programs report (by program)

Use this report to view and manage detected programs not recognized by the virus and spyware protection service or firewall protection service, and the computers where these programs were detected.

To approve any of these applications for use on client computers, you need to add them to a policy. After you approve detected programs and Internet applications, they are no longer detected as threats on the computers using the policy.

- *View unrecognized programs*
- *View user-approved applications for a computer*
- *Specify approved programs*
- *Set up allowed Internet applications*
- *Manage your protection strategy with best practices*
- *Managing suspicious activity with best practices*

Item	Description
Groups	Select the group of computers to display. If you have not created any groups, this option does not appear.
Report period	Select the time period to display.
Program type	Select the status of detections to display: ■ **All**: All detected programs. ■ **Firewall-Blocked Programs**: Internet applications blocked by the firewall protection service. ■ **Potentially Unwanted Programs**: Programs detected the by virus and spyware protection service as possible spyware.
Group by	■ Select **Program** to sort the list by the name of the unrecognized program. ■ Select **Computer** to sort the list by the computers on which programs were detected.

Item	Description
Name	Lists the name of each detected program. - Select the name of a program to display detailed information about it. - Click the arrow next to a program to display or hide a list of computers where it was detected. - Select a computer name to display details about it.
Computers	Shows the number of computers where the program was detected.
Type	Shows the type of program detected: **Firewall-Blocked Programs** or **Potentially Unwanted Programs** detected by the virus and spyware protection service.

Inbound Events Blocked by Firewall report (by originating computer)

Use this report to view and manage blocked communications sent to client computers, and the computers where these communications originated. Each attempt at communication is reported as a single *event*.

- *View inbound events blocked by the firewall*

Item	Description
	Select the group of computers to display. If you have not created any groups, this option does not appear.
Report period	Select the time period to display.
Group by	- Select **Originating Computer** to list the computers where events originated. - Select **Destination Computer** list the computers where events were targeted.
Computer	Lists the name of each originating computer. - Click the arrow next to the event name to display or hide a list of computers where the event was targeted. - Select a computer name to display details about it.
	Lists the IP address of the computer where the event originated.
Events	Shows the number of inbound events blocked. Select the quantity to display a list of the blocked events.
Last Event Date	Shows the date when the event was last blocked.

Inbound Events Blocked by Firewall report (by destination computer)

Use this report to view and manage blocked communications sent to client computers, and the computers where these communications were targeted. Each attempt at communication is reported as a single *event*.

- *View inbound events blocked by the firewall*

Item	Description
Groups	Select the group of computers to display. If you have not created any groups, this option does not appear.
Report period	Select the time period to display.

Item	Description
Group by	■ Select **Originating Computer** to list the computers where events originated. ■ Select **Destination Computer** to list the computers where events were targeted.
Computer	Lists the name of each target computer. ■ Click the arrow next to the event name to display or hide a list of computers where the event originated. ■ Select a computer name to display details about it.
Originating IP Address	Lists the IP address of the computer where the event originated.
Events	Shows the number of inbound events blocked. Select the quantity to display a list of the blocked events.
Last Event Date	Shows the date when the event was last blocked.

Inbound Event List

Use this page to view detailed information about inbound communications that were blocked by the firewall protection service.

The **Computer** and **Report period** selected on the previous page determine the content of this listing.

- *View inbound events blocked by the firewall*

Item	Description
	Shows the type of event that was blocked.
Event Count	Shows the number of times this type of event was blocked.
Last Event Date	Shows the date when the event was last blocked.

Duplicate Computers report

Use this report to investigate computers suspected to be duplicates. Duplicate listings usually result when the Enforced Client client software has been installed more than once on a single computer, or when users install it on their new computers without uninstalling it from their previous computers.

If you delete a computer where a valid service is installed, it will be added back to your listing the next time you log on. However, you will no longer be able to view historical report data for that computer.

- *View duplicate computers*
- *Display details for a computer*
- *View and resolve action items*
- *Make the most of your online data*
- *Customize listings and reports*

Item	Description
	Select the group of computers to display. If you have not created any groups, this option does not appear.
Email button	Click to open a blank email message addressed to the selected computers. (You must have a local email application installed to use this feature.)
Delete	Click to delete the selected computers from your listing.
Block	Click to prevent the selected computers from receiving product updates. Use this feature to keep unauthorized computers from using your protection services.
Move to	Select a group to move selected computers into. To create a group, go to the **Groups + Policies** page. Then use this **Move to** list to move computers into the new group.
Move	Click to move the selected computers into the selected group.
Computer	Lists each computer suspected to be a duplicate. Select a computer's name to display detailed information about it.
Group	Shows which group a computer belongs to.
Email	Shows the email address for a computer. Select an address to open a blank email message addressed to that computer. (You must have a client email application installed to use this feature.) To send an email message to multiple computers instead, select the computers, then click the **Email** button.
Last Connect	Shows when a computer last connected to the network. The date appears in red for out-of-date computers. To view instructions for updating an out-of-date computer, select the computer name to open the **Computer Details** page, then click the red action item.
DAT Date	Shows when the detection definition (DAT) file was last updated. The date appears in red for out-of-date computers. To view instructions for updating an out-of-date DAT file, select the computer name to open the **Computer Details** page, then click the red action item.
IP Address	Shows the IP address of a computer.

Computer Profiles report

Use this report to check the version of the Microsoft Windows operating system and the Microsoft Internet Explorer browser running on each computer. This can help you locate computers that require maintenance, such as installing software patches.

In this report, you can display all computers or one of the groups you have created, then select individual computers for managing or viewing. To select a computer, select the checkbox next to its name.

- *View computer profiles*

Item	Description
	Select the group of computers to display. If you have not created any groups, this option does not appear.
Operating system version	Select a version to display only the computers running that version. Only the operating systems running on client computers are listed here.
Browser version	Select a version to display only the computers running that version. Only the web browsers running on client computers are listed here.
Email button	Click to open a blank email message addressed to the selected computers. (You must have a local email application installed to use this feature.)
Delete	Click to delete the selected computers from your listing. Use this feature to delete duplicate and obsolete computers. If you delete a computer where a valid service is installed, it will be added back to your listing the next time you log on.
Block	Click to prevent the selected computers from receiving product updates. Use this feature to keep unauthorized computers from using your protection services.
Move to	Select a group to move selected computers into. To create a group, go to the **Groups + Policies** page. Then use this **Move to** list to move computers into the new group.
Move	Click to move the selected computers into the selected group.
Computer Name	Lists each computer in the selected group. Select a computer name to display detailed information about it.
Email Address	Shows the email address for a computer. Select an address to open a blank email message addressed to that computer. (You must have a client email application installed to use this feature.) To send an email message to multiple computers instead, select the computers, then click the **Email** button.
IP Address	Shows the IP address of a computer.
Operating System	Shows the name and version of Windows running on a computer.
IE Browser Version	Shows the name and version of Internet Explorer running on a computer.
Group	Shows which group a computer belongs to.

Detection History report

Use this report to create a graphical representation of detections for your account over the past year. This information can assist you in detecting trends specific to your network and evaluating the success of your corporate security strategy in reducing threats for your business.

- *View your detection history*
- *Manage your protection strategy with best practices*

Item	Description
	Select the group of computers to display. If you have not created any groups, this option does not appear.
Display by	Select increments in which to display historical information: ■ **Month**: Each bar in the graphs represents data for a month. ■ **Quarter**: Each bar in the graphs represents data for a 3-month period.
	Shows the total number of detections for your account over the past year.
Computers with Detections	Shows the total number of computers where detections occurred over the past year.

Edit Default Group

When you first install Enforced Client, only the **Default** group is defined. By default, every computer in your account is placed into the **Default** group. You can also create other groups for your computers.

Initially, the **Default** group uses the **SonicWALL Default** policy. If you create other policies, you can use this page to assign a different policy to the **Default** group.

- *Creating groups to manage your site*
- *Setting up policies*
- *Assign a policy to a group*

Item	Description
	Shows the **Default** group name. You cannot edit the name of this default group or select another group. To edit a different group, click **Cancel** to return to the **Groups + Policies** page, then select that group.
Policy	Select a policy from the list. The current policy is displayed, and all available policies appear in the list. If you have not created any policies, only the **SonicWALL Default** policy appears. **Note:** You must create a policy before you can assign it to a group.
Save	Click to update the **Default** group with the selected policy and return to the previous page.
Cancel	Click to return to the previous page without changing the policy.

Edit Group

Use this page to rename a group or assign a different policy.

- *Creating groups to manage your site*
- *Setting up policies*

Item	Description
	Type a new name for the group if you want to rename it.
Policy	Select a policy from the list if you want to assign a different one. The current policy is displayed, and all available policies appear in the list. If you have not created any policies, only the **SonicWALL Default** policy appears. **Note:** You must create a policy before you can assign it to a group.
Save	Click to update the group and return to the previous page.
Cancel	Click to return to the previous page without saving changes.

Add Group

Use this page to create a group.

A group consists of one or more computers that use the same security settings (known as a *policy*). You can create groups based on geographic location, department, computer type, the tasks performed by the users, or anything meaningful to your organization.

- *Creating groups to manage your site*
- *Move computers into a group*
- *Setting up policies*
- *Assign a policy to a group*

Item	Description
	Type a name for the new group.
Policy	Select a policy from the list. If you have not created any policies, only the **SonicWALL Default** policy appears. **Note:** You must create a policy before you can assign it to a group.
Save	Click to add the group and return to the previous page.
Cancel	Click to return to the previous page without saving changes.

View Default Policy

Use this page to view the protection settings for the **SonicWALL Default** policy.

Policies are made up of security settings for all of your protection services. These settings define how your services operate on client computers.

When you first install Enforced Client, only the **SonicWALL Default** policy is defined and every computer in your account uses this policy. You can also create other policies.

You cannot change the settings for the **SonicWALL Default** policy. For different settings, you need to create a new policy.

- *Setting up policies*
- *Set basic virus protection options*
- *Set advanced virus protection options*
- *Set basic spyware protection options*
- *Set advanced spyware protection options*

- *Configuring policies for firewall protection*
- *Configuring browser protection from the SecurityCenter*
- *The SonicWALL Default policy*

Item	Description
Virus Protection	
Scheduled On-Demand Scan	**Disabled**: No *on-demand* scan is scheduled. *On-access* scans still occur every time users run, open, or download files.
Spyware Protection	
Spyware Protection Status	**Enabled**: The spyware scanning feature of the virus and spyware protection service is turned on. It will check for potentially unwanted programs during on-access and on-demand scans.
Spyware Protection Mode	**Prompt:** The virus and spyware protection service asks users how to respond when potentially unwanted programs are detected. **Note:** To prevent prompts from displaying, create a new policy with a different setting. For maximum protection, we recommend selecting **Protect** mode to automatically delete potentially unwanted programs.
Desktop Firewall Protection	
Automatically install the desktop firewall on all computers using this policy	**Disabled.** Installs the browser protection service automatically whenever client computers check for an updated policy.
Use Smart Recommendations to automatically approve common Internet applications	**Enabled.** Whenever it detects an Internet application that the administrator has not specified as an approved Internet application, the firewall protection service checks a whitelist of Internet applications that SonicWALL has determined to be safe.
Firewall Configuration	**User configures firewall**: Users must configure the firewall protection service for their computers. When this option is selected, other firewall protection options do not appear on this page. **Important:** To ensure the highest level of security, we recommend that administrators create a new policy and configure the firewall protection service. If you allow users to configure their settings, it is important to educate them about threats and strategies for avoiding intrusions.
Firewall Status	**Enabled**: The firewall protection service is turned on.
Firewall Protection Mode	**Prompt:** The firewall protection service asks users how to respond when suspicious activity is detected. **Note:** To prevent prompts from displaying, create a new policy with a different setting. For maximum protection, we recommend selecting **Protect** mode to automatically block suspicious activity.
Firewall Connection Type	**Untrusted network:** The computer connects to a network that might not be secure, such as an airport or hotel network. The firewall protection service should block communications from IP addresses on that network.
Browser Protection	
Automatically install browser protection on all computers using this policy	Select this option to install the browser protection service automatically whenever client computers check for an updated policy.
Advanced Settings	

Item	Description
Update client computers where users are not logged in	**Enabled.** Automatic updates occur on computers where no user is logged on, for example, terminal servers and computers where the fast user switching feature is used.
Display support notifications on client computers	**Enabled.** Notification dialog boxes warn client computer users when software upgrades and DAT file updates are being discontinued for their operating system.
Enable outbreak response	**Enabled**: Client computers check for an outbreak detection definition (DAT) file every hour.
Enable buffer overflow protection	**Enabled**: Detect code starting to run from data in reserved memory and prevent that code from running. The virus and spyware protection service protects against buffer overflow in more than 30 most commonly used Windows-based programs. SonicWALL updates this list as it adds buffer overflow protection for additional programs. **Important:** Buffer overflow protection does not stop data from being written. Do not rely on the exploited application remaining stable after being compromised, even if buffer overflow protection stops the corrupted code from running.
Enable script scanning	**Enabled**: Detect harmful code embedded in web pages that would cause unauthorized programs to run on client computers.
Scan email (before delivering to the Outlook Inbox)	**Enabled**: Look for threats in email before it is placed into the user's Inbox.
Scan all file types during on-access scans	**Enabled**: Look for threats in all types of files, instead of only default types, when they are downloaded, opened, or run. (Default file types are defined in the DAT files.).
Scan within archives during on-access scans (e.g., .zip, .rar, .tat, .tgz)	**Disabled**: Look for threats in compressed archive files when the files are accessed.
Scan within archives during on-demand scans (e.g., .zip, .rar, .tat, .tgz)	**Enabled**: Do not look for threats in compressed archive files when files are scanned manually.

Item	Description
Check for updates every	**12 hours**: Client computers check for updated detection definition (DAT) files and product components every 12 hours.
Detect ...	**Enabled**: The following threats are detected during scans: ■ **Jokes**: Programs designed to be mistaken for a virus. They may alarm or annoy a user but do not harm files or data. They are intended to waste time and resources. ■ **Remote admin tools**: Programs that can be used from a remote location to access a computer. Some remote administration tools serve useful purposes, such as allowing users to access their files from home, but others can be used by unauthorized persons to monitor user activities and take control of a computer. ■ **Spyware**: Programs that covertly gather user information through the user's Internet connection without the user's knowledge. Once installed, spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can gather information such as email addresses, websites visited, passwords, and credit card numbers. ■ **Dialers**: Programs that hijack a user's modem and dial premium-rate phone numbers, such as those required to access pornographic websites. ■ **Password crackers**: Programs that find passwords or encryption keys by trying every possible combination of characters until the code is broken. ■ **Adware**: Programs that display unsolicited advertisements. Adware often includes code that tracks a user's personal information and transmits it to someone else, without the user's knowledge. ■ **Potentially unwanted applications**: Programs that perform some unauthorized (and often harmful or undesirable) act such as viruses, worms, and Trojan horses. ■ **Key loggers**: Programs that record every keystroke a user makes. They can be used to steal passwords and other confidential information.

Edit Policy: Virus Protection Settings

Policies are made up of security settings for all of your protection services. These settings define how your services operate on client computers.

Use this page to rename a policy or modify its virus protection settings. Changes do not take effect until you click **Save**.

- *Set basic virus protection options*
- *Assign a policy to a group*

Item	Description
Policy name	Type a new name for the policy if you want to rename it.
On-Demand Scan	■ Select **On** to schedule an *on-demand* scan, then select the time and frequency. ■ Select **Off** to schedule no on-demand scans. Regardless of this setting, *on-access* scans occur every time users run, open, or download files.

Item	Description
Excluded Files and Folders	Lists files, folders, and file name extensions that the virus and spyware protection service does not scan for viruses. If you have not designated any files or folders to exclude, no list appears here. Only files that you know are safe should be excluded from on-access and on-demand virus scans.
Type	Select the type of exclusion: ■ **File**: The file will not be scanned. ■ **Folder**: No files or subfolders in this folder will be scanned. ■ **File Extension**: No files using this extension will be scanned. The selected type determines the contents of the **Value** field.
Value	Specify the file, folder, or file extension. You can browse to select a file.
Add Exclusion	Click to add the specified folder, file, or file extension. Once it is added, it appears in the list on this tab.
remove	Select this link to delete the file, folder, or file extension from the list. During future scans, this item is checked for threats.
Save	Click to update the policy and return to the **Groups + Policies** page.
Cancel	Click to return to the **Groups + Policies** page without changing the policy.
Reset to Defaults	Click to assign the original **SonicWALL Default** policy settings to this policy. **Note**: This resets all settings on all tabs. Settings will not take effect until you click **Save**.

Edit Policy: Spyware Protection Settings

Policies are made up of security settings for all of your protection services. These settings define how your services operate on client computers.

Use this page to rename a policy or modify its spyware protection settings. Changes do not take effect until you click **Save**.

- *Set basic spyware protection options*
- *Assign a policy to a group*

Item	Description
Policy name	Type a new name for the policy if you want to rename it.
Spyware Protection Status	■ Select **On** to enable the spyware scanning feature of the virus and spyware protection service. ■ Select **Off** to disable it. When enabled, the virus and spyware protection service checks for potentially unwanted programs during on-access and on-demand scans.

Item	Description
Spyware Protection Mode	Select the response when a potentially unwanted program is detected: ■ **Report:** Allow the program to run. Do not notify the user. ■ **Prompt:** Ask the user how to respond. ■ **Protect:** Block the program. Detections of potentially unwanted programs always appear in administrative reports when the spyware protection feature is enabled.
Approved Programs	Lists previously detected programs that will no longer be detected as potentially unwanted on computers using this policy. If you have not specified any approved programs, no list appears here. Only programs that you know are safe should appear here. In essence, these programs are excluded from on-access and on-demand scans for spyware.
Type	Select the type of program to approve: ■ **Detected Program**: A potentially unwanted program detected by the virus and spyware protection service. ■ **User-Approved Program**: A detected program that a user has subsequently approved to run on a client computer. The selected type determines the programs displayed in the **Program** list.
Program	Select a program.
Add Program	Select this link to allow the selected program. Once it is added, it appears in the list on this tab.
remove	Select this link to delete the program from the list. During future scans, it is treated as a new detection on computers using this policy, and the virus and spyware protection service responds according to the **Spyware Protection Mode** selected.
Save	Click to update the policy and return to the **Groups + Policies** page.
Cancel	Click to return to the **Groups + Policies** page without changing the policy.
Reset to Defaults	Click to assign the original **SonicWALL Default** policy settings to this policy. **Note**: This resets all settings on all tabs. Settings will not take effect until you click **Save**.

Edit Policy: Desktop Firewall Settings

Policies are made up of security settings for all of your protection services. These settings define how your services operate on client computers.

Use this page to rename a policy or modify its settings for the firewall protection service. Changes do not take effect until you click **Save**.

- *Configuring policies for firewall protection*
- *Learn mode*
- *Assign a policy to a group*

Item	Description
Policy name	Type a new name for the policy if you want to rename it.
Firewall Management	Select who manages the firewall protection service's settings for client computers: ■ **Administrator configures firewall**: You configure the policy settings that determine how the firewall protection service operates. When this option is selected, other firewall protection options appear on this page. ■ **User configures firewall**: Users must configure the firewall protection service for their computers. When this option is selected, other firewall protection options do not appear on this page. **Important:** To ensure the highest level of security, we recommend that administrators configure the firewall protection service. When enabling users to configure their settings, it is important to educate them about threats and strategies for avoiding intrusions. a **Notes:** When you update a policy to **Administrator configures firewall**, any firewall protection settings that users have configured previously on computers using this policy are saved. ■ If you also select **Prompt** mode, user settings are merged with your policy settings on each client computer. ■ If you select **Protect** mode or **Record** mode, user settings are inactive. Saved settings configured by users become active again when you update the policy to **User configures firewall**.
Automatically install the desktop firewall on all computers using this policy	Select this option to install the firewall protection service automatically whenever client computers check for an updated policy. **Important:** Enabling this feature can result in unattended installations on computers where no one is available to authorize communications that are consequently blocked by the firewall. If this feature is used to install the firewall protection service on a server, it is important to configure essential system services first, to prevent disruptions.
Use Smart Recommendations to automatically approve common Internet applications	Select this option to use SonicWALL recommendations for approved Internet applications. When the firewall protection service detects an Internet application, it first checks the approved applications specified by the administrator. If the detected application is not on that list, it checks the list of SonicWALL recommendations when this option is enabled.
Firewall Status	■ Select **On** to enable the firewall protection service. ■ Select **Off** to disable it.
Firewall Protection Mode	Select the response when suspicious activity is detected: ■ **Report:** Allow the activity. Do not notify the user. (This setting can be used as a "learn mode" to help you determine which applications to approve.) ■ **Prompt:** Ask the user how to respond. ■ **Protect:** Block the activity. Suspicious activity always appears in administrative reports when the firewall's status is enabled. **Note:** See *Firewall Management* for related information.

Item	Description
Connection Type	Select the environment where a client computer is used: ■ **Untrusted network:** The computer connects to a network that might not be secure, such as an airport or hotel network. The firewall protection service should block communications from IP addresses on that network. ■ **Trusted network:** The computer connects to a network that is protected from the Internet by a hardware firewall or router. The firewall protection service should allow communications from IP addresses on the same subnet. ■ **Custom settings:** The computer should communicate only with specified ports and IP addresses. Click **Edit** to configure the settings.
Allowed Internet Applications	Lists previously detected Internet applications that you have approved to run on computers using this policy. If you have not specified any allowed applications, no list appears here. Only Internet applications that you know are safe should appear here.
Detected Applications	Select an application that you want to approve from the list. The list shows all the Internet applications detected on client computers by the firewall protection service.
Add Application	Click to allow the specified application on computers using this policy. Once it is added, it appears in the list on this tab.
remove	Click to delete the application from the list. If this application attempts to contact the Internet in the future, it is treated as a new detection on computers using this policy. At that time, the firewall protection service responds according to the **Firewall Protection Mode** selected.
Save	Click to update the policy and return to the **Groups + Policies** page.
Cancel	Click to return to the **Groups + Policies** page without changing the policy.
Reset to Defaults	Click to assign the original **SonicWALL Default** policy settings to this policy. **Note**: This resets all settings on all tabs. Settings will not take effect until you click **Save**.

Firewall Custom Settings

Use this page to define custom settings for the environment where client computers operate. Custom settings are typically recommended when computers using this policy meet one of these criteria:

- They should allow communications from system services only through specific ports or from a specific range of IP addresses.
- They function as servers that provide system services.

Custom settings specify:

- Which system service ports client computers are allowed to communication through.
- Which IP addresses client computers are allowed to accept communications from.

Changes you make to custom settings do not take effect until you click **Save** on the **Desktop Firewall** tab.

- *Configure system services for a custom connection*

- *Configure IP addresses for a custom connection*

Item	Description
	Specifies the system service ports through which computers using this policy can communicate.
Allow	Select the checkbox next to each port you want to enable. The firewall protection service allows communications through the selected ports. It blocks communications through unselected ports.
Connection Name	Identifies the system service using the port. Three commonly used ports appear by default: ■ **File and Print Sharing** ■ **Remote Desktop** ■ **Remote Assistance** You can edit the configuration for these services and define additional services.
edit	Select this link to open a page where you can modify the configuration for an incoming connection.
remove	Select this link to remove an incoming connection from the list.
Add Connection	Select this link to open a page where you can configure a new incoming connection.
Allowed Incoming Addresses	Select which IP addresses computers using this policy can accept communications from: ■ **Any computer:** All IP addresses. ■ **My network (the subnet only):** Only IP addresses on the local subnet. This settings is the same as **Trusted network** on the **Desktop Firewall** tab. ■ **Specific address range:** Only the IP addresses you designate here. Type a beginning and ending IP address in the boxes provided.
Add	Select this link to add the range of IP addresses you have entered to the list of **Allowed incoming IP address ranges**. If you have not added any address ranges, this list does not appear.
remove	Select this link to remove a range of IP addresses from the list.
OK	Click to update the policy and return to the **Desktop Firewall** tab. **Note:** You must also click **Save** on the **Desktop Firewall** tab to update the policy.
Cancel	Click to return to the **Desktop Firewall** tab without saving changes.

Add or Edit Incoming Connection

Use this page to add a service port through which the firewall protection service will allow communication, or update the information about a port. In most cases, this will be a system service port.

- *Configure system services for a custom connection*

Item	Description
Name	Type the name of the service port through which system services can communicate with the computer. This can be a standard name or one that is meaningful to your business.
Port(s)	Type the port number(s).

Item	Description
OK	Click to add the port configuration and return to the **Firewall Custom Settings** page.
Cancel	Click to return to the **Firewall Custom Settings** page without adding a port.

Edit Policy: Browser Protection Settings

Policies are made up of security settings for all of your protection services. These settings define how your services operate on client computers.

Use this page to rename a policy or modify its settings for the browser protection service. Changes do not take effect until you click **Save**.

- *Configuring browser protection from the SecurityCenter*
- *Assign a policy to a group*

Item	Description
	Type a new name for the policy if you want to rename it.
Automatically install browser protection service on all computers using this policy	Select this option to install the browser protection service automatically whenever client computers check for an updated policy.
Save	Click to update the policy and return to the **Groups + Policies** page.
Cancel	Click to return to the **Groups + Policies** page without changing the policy.
Reset to Defaults	Click to assign the original **SonicWALL Default** policy settings to this policy. **Note**: This resets all settings on all tabs. Settings will not take effect until you click **Save**.

Edit Policy: Advanced Settings

Policies are made up of security settings for all of your protection services. These settings define how your services operate on client computers.

Use this page to rename a policy or modify its advanced virus and spyware protection settings. Changes do not take effect until you click **Save**.

- *Set advanced virus protection options*
- *Set advanced spyware protection options*
- *Update computers where no user is logged on*
- *Notifying users when support ends*
- *Assign a policy to a group*

Item	Description
Policy name	Type a new name for the policy if you want to rename it.
Update client computers where users are not logged in	Select this option to automatically update terminal servers and other client computers where no user is logged on to a current session.
Display support notifications on client computers	Select this option to display dialog boxes that notify users when upgrades or updates will end for the operating system running on their client computers.

Item	Description
Advanced Virus Protection Settings	Select additional protection features for the virus and spyware protection service. If none of these features are selected, the service still detects viruses. ■ **Enable outbreak response**: Check for an outbreak detection definition (DAT) file every hour. ■ **Enable buffer overflow protection**: Detect code starting to run from data in reserved memory and prevent that code from running. The virus and spyware protection service protects against buffer overflow in more than 30 most commonly used Windows-based programs. SonicWALL updates this list as it adds buffer overflow protection for additional programs. **Important:** Buffer overflow protection does not stop data from being written. Do not rely on the exploited application remaining stable after being compromised, even if buffer overflow protection stops the corrupted code from running. ■ **Enable script scanning**: Detect harmful code embedded in web pages that would cause unauthorized programs to run on client computers. ■ **Scan email (before delivering to the Outlook Inbox)**: Look for threats in email before it is placed into the user's Inbox. ■ **Scan all file types during on-access scans**: Inspect all types of files, instead of only default types, when they are downloaded, opened, or run. (Default file types are defined in the dat files.) ■ **Scan within archives during on-access scans (e.g., .zip, .rar, .tat, .tgz)**: Look for threats in compressed archive files when the files are accessed. ■ **Scan within archives during on-demand scans (e.g., .zip, .rar, .tat, .tgz)**: Look for threats in compressed archive files when they are scanned manually.
Check for updates every	Select how often client computers should check for updates.

Item	Description
Advanced Spyware Protection Settings	Select potentially unwanted program threats to detect. If no threats are selected, the virus and spyware protection service does not detect any potentially unwanted programs. ■ **Jokes**: Programs designed to be mistaken for a virus. They may alarm or annoy users but do not harm files or data. They are intended to waste time and resources. ■ **Remote admin tools**: Programs that can be used from a remote location to access a computer. Some remote administration tools serve useful purposes, such as allowing users to access their files from home, but others can be used by unauthorized persons to monitor user activities and take control of a computer. ■ **Spyware**: Programs that covertly gathers user information through the user's Internet connection without the user's knowledge. Once installed, spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can gather information such as email addresses, websites visited, passwords, and credit card numbers. ■ **Dialers**: Programs that hijack a user's modem and dial premium-rate phone numbers, such as those required to access pornographic websites. ■ **Password crackers**: Programs that find passwords or encryption keys by trying every possible combination of characters until the code is broken. ■ **Adware**: Programs that display unsolicited advertisements. Adware often includes code that tracks a user's personal information and transmits it to someone else, without the user's knowledge. ■ **Potentially unwanted applications**: Programs that perform some unauthorized (and often harmful or undesirable) act such as viruses, worms, and Trojan horses. ■ **Key loggers**: Programs that record every keystroke a user makes. They can be used to steal passwords and other confidential information.
Save	Click to update the policy and return to the **Groups + Policies** page.
Cancel	Click to return to the **Groups + Policies** page without changing the policy.
Reset to Defaults	Click to assign the original **SonicWALL Default** settings to this policy. **Note**: This resets all settings on all tabs. Settings will not take effect until you click **Save**.

Add Policy: Virus Protection Settings

Policies are made up of security settings for all of your protection services. These settings define how your services operate on client computers.

Use this page to create a policy and configure its virus protection settings. Changes do not take effect until you click **Save**.

- *Set basic virus protection options*
- *Assign a policy to a group*

Item	Description
	Type the name of the new policy.
On-Demand Scan	■ Select **On** to schedule an *on-demand* scan, then select the time and frequency. ■ Select **Off** to schedule no on-demand scans. Regardless of this setting, *on-access* scans occur every time users run, open, or download files.
Excluded Files and Folders	Lists files, folders, and file name extensions that the virus and spyware protection service does not scan for viruses. If you have not designated any files or folders to exclude, no list appears here. Only files that you know are safe should be excluded from on-access and on-demand virus scans.
Type	Select the type of exclusion: ■ **File**: The file will not be scanned. ■ **Folder**: No files or subfolders in this folder will be scanned. ■ **File Extension**: No files using this extension will be scanned. The selected type determines the contents of the **Value** field.
Value	Specify the file, folder, or file extension.
Add Exclusion	Click to add the specified file, folder, or file extension. Once it is added, it appears in the list on this tab.
remove	Click to delete the file, folder, or file extension from the list. During future scans, it will be checked for threats.
Save	Click to update the policy and return to the **Groups + Policies** page.
Cancel	Click to return to the **Groups + Policies** page without changing the policy.
Reset to Defaults	Click to assign the original **SonicWALL Default** policy settings to this policy. **Note**: This resets all settings on all tabs. Settings will not take effect until you click **Save**.

Add Policy: Spyware Protection Settings

Policies are made up of security settings for all of your protection services. These settings define how your services operate on client computers.

Use this page to create a policy and configure its spyware protection settings. Changes do not take effect until you click **Save**.

- *Set basic spyware protection options*
- *Assign a policy to a group*

Item	Description
Policy name	Type a name for the new policy.
Spyware Protection Status	■ Select **On** to enable the spyware scanning feature of the virus and spyware protection service. ■ Select **Off** to disable it. When enabled, the virus and spyware protection service checks for potentially unwanted programs during on-access and on-demand scans.

Item	Description
Spyware Protection Mode	Select the response when a potentially unwanted program is detected: ■ **Report:** Allow the program to run. Do not notify the user. ■ **Prompt:** Ask the user how to respond when a potentially unwanted program is detected. ■ **Protect:** Block the program. Detections of potentially unwanted programs always appear in administrative reports when the spyware protection feature is enabled.
Approved Programs	Lists previously detected programs that will no longer be detected as potentially unwanted on computers using this policy. If you have not specified any approved programs, no list appears here. Only programs that you know are safe should appear here. In essence, these programs are excluded from on-access and on-demand scans for spyware.
Type	Select the type of program to approve: ■ **Detected Program**: A potentially unwanted program detected by the virus and spyware protection service. ■ **User-Approved Program**: A detected program that a user has subsequently approved to run on a client computer. The selected type determines the programs displayed in the **Program** list.
Program	Select a program.
Add Program	Select this link to allow the selected program. Once it is added, it appears in the list on this tab.
remove	Select this link to delete the program from the list. During future scans, it is treated as a new detection on computers using this policy, and the virus and spyware protection service responds according to the **Spyware Protection Mode** selected.
Save	Click to update the policy and return to the **Groups + Policies** page.
Cancel	Click to return to the **Groups + Policies** page without changing the policy.
Reset to Defaults	Click to assign the original **SonicWALL Default** policy settings to this policy. **Note**: This resets all settings on all tabs. Settings will not take effect until you click **Save**.

Add Policy: Desktop Firewall Settings

Policies are made up of security settings for all of your protection services. These settings define how your services operate on client computers.

Use this page to create a new policy and configure its settings for the firewall protection service. Changes do not take effect until you click **Save**.

- *Configuring policies for firewall protection*
- *Learn mode*
- *Assign a policy to a group*

Item	Description
Policy name	Type a name for the new policy.
Firewall Configuration	Select who manages the firewall protection service's settings for client computers: ■ **Administrator configures firewall**: You configure the policy settings that determine how the firewall protection service operates. When this option is selected, other firewall protection options appear on this page. ■ **User configures firewall**: Users must configure the firewall protection service for their computers. When this option is selected, other firewall protection options do not appear on this page. **Important:** To ensure the highest level of security, we recommend that administrators configure the firewall protection service. When enabling users to configure their settings, it is important to educate them about threats and strategies for avoiding intrusions. **Notes:** When you update a policy to **Administrator configures firewall**, any firewall protection settings that users have configured previously on computers using this policy are saved. ■ If you also select **Prompt** mode, user settings are merged with your policy settings on each client computer. ■ If you select **Protect** mode or **Record** mode, user settings are inactive. Saved settings configured by users become active again when you update the policy to **User configures firewall**.
Automatically install the desktop firewall on all computers using this policy	Select this option to install the firewall protection service automatically whenever client computers check for an updated policy. **Important:** Enabling this feature can result in unattended installations on computers where no one is available to authorize communications that are consequently blocked by the firewall. If this feature is used to install the firewall protection service on a server, it is important to configure essential system services first, to prevent disruptions.
Use Smart Recommendations to automatically approve common Internet applications	Select this option to use SonicWALL recommendations for approved Internet applications. When the firewall protection service detects an Internet application, it first checks the approved applications specified by the administrator. If the detected application is not on that list, it checks the list of SonicWALL recommendations when this option is enabled.
Firewall Status	■ Select **On** to enable the firewall protection service. ■ Select **Off** to disable it.
Firewall Protection Mode	Select the response when suspicious activity is detected: ■ **Report:** Allow the activity. Do not notify the user. (This setting can be used as a "learn mode" to help you determine which applications to approve.) ■ **Prompt:** Ask the user how to respond. ■ **Protect:** Block the activity. Suspicious activity always appears in administrative reports when the firewall's status is enabled. **Note:** See *Firewall Configuration* for related information.

Item	Description
Connection Type	Select the environment where a client computer is used: ■ **Untrusted network:** The computer connects to a network that might not be secure, such as an airport or hotel network. The firewall protection service should block communications from IP addresses on that network. ■ **Trusted network:** The computer connects to a network that is protected from the Internet by a hardware firewall or router. The firewall protection service should allow communications from IP addresses on the same subnet. ■ **Custom settings:** The computer should communicate only with specified ports and IP addresses. Click **Edit** to configure the settings.
Allowed Internet Applications	Lists previously detected Internet applications that you have approved to run on computers using this policy. If you have not specified any allowed applications, no list appears here. Only Internet applications that you know are safe should appear here.
Detected Application	Select an application that you want to approve from the list. The list shows all the Internet applications detected on client computers by the firewall protection service.
Add Application	Click to allow the specified application on computers using this policy. Once it is added, it appears in the list on this tab.
remove	Click to delete the application from the list. If this application attempts to contact the Internet in the future, it is treated as a new detection on computers using this policy. At that time, the firewall protection service responds according to the **Firewall Protection Mode** selected.
Save	Click to update the policy and return to the **Groups + Policies** page.
Cancel	Click to return to the **Groups + Policies** page without changing the policy.
Reset to Defaults	Click to assign the original **SonicWALL Default** policy settings to this policy. **Note**: This resets all settings on all tabs. Settings will not take effect until you click **Save**.

Add Policy: Browser Protection Settings

Policies are made up of security settings for all of your protection services. These settings define how your services operate on client computers.

Use this page to create a new policy and configure its settings for the browser protection service. Changes do not take effect until you click **Save**.

- *Configuring browser protection from the SecurityCenter*
- *Assign a policy to a group*

Item	Description
Policy name	Type a new name for the policy if you want to rename it.
Automatically install browser protection service on all computers using this policy	Select this option to install the browser protection service automatically whenever client computers check for an updated policy.
Save	Click to update the policy and return to the **Groups + Policies** page.

Item	Description
Cancel	Click to return to the **Groups + Policies** page without changing the policy.
Reset to Defaults	Click to assign the original **SonicWALL Default** policy settings to this policy. **Note**: This resets all settings on all tabs. Settings will not take effect until you click **Save**.

Add Policy: Advanced Settings

Policies are made up of security settings for all of your protection services. These settings define how your services operate on client computers.

Use this page to create a policy and configure its advanced virus and spyware protection settings. Changes do not take effect until you click **Save**.

- *Set advanced virus protection options*
- *Set advanced spyware protection options*
- *Update computers where no user is logged on*
- *Notifying users when support ends*
- *Assign a policy to a group*

Item	Description
Policy Name	Type a name for the new policy.
Update client computers where users are not logged in	Select this option to automatically update terminal servers and other client computers where no user is logged on to a current session.
Display support notifications on client computers	Select this option to display dialog boxes that notify users when upgrades or updates will end for the operating system running on their client computers.

Item	Description
Advanced Virus Protection Settings	Select additional protection features for the virus and spyware protection service. If none of these features are selected, the service still detects viruses. ■ **Enable outbreak response**: Check for an outbreak detection definition (DAT) file every hour. ■ **Enable buffer overflow protection**: Detect code starting to run from data in reserved memory and prevent that code from running. The virus and spyware protection service protects against buffer overflow in more than 30 most commonly used Windows-based programs. SonicWALL updates this list as it adds buffer overflow protection for additional programs. **Important:** Buffer overflow protection does not stop data from being written. Do not rely on the exploited application remaining stable after being compromised, even if buffer overflow protection stops the corrupted code from running. ■ **Enable script scanning**: Detect harmful code embedded in web pages that would cause unauthorized programs to run on client computers. ■ **Scan email (before delivering to the Outlook Inbox)**: Look for threats in email before it is placed into the user's Inbox. ■ **Scan all file types during on-access scans**: Inspect all types of files, instead of only default types, when they are downloaded, opened, or run. (Default file types are defined in the dat files.) ■ **Scan within archives during on-access scans (e.g., .zip, .rar, .tat, .tgz)**: Look for threats in compressed archive files when the files are accessed. ■ **Scan within archives during on-demand scans (e.g., .zip, .rar, .tat, .tgz)**: Look for threats in compressed archive files when they are scanned manually.
Check for updates every	Select how often client computers should check for updates.

Item	Description
Advanced Spyware Protection Settings	Select potentially unwanted program threats to detect. If no threats are selected, the virus and spyware protection service does not detect any potentially unwanted programs. ■ **Jokes**: Programs designed to be mistaken for a virus. They may alarm or annoy users but do not harm files or data. They are intended to waste time and resources. ■ **Remote admin tools**: Programs that can be used from a remote location to access a computer. Some remote administration tools serve useful purposes, such as allowing users to access their files from home, but others can be used by unauthorized persons to monitor user activities and take control of a computer. ■ **Spyware**: Programs that covertly gather user information through the user's Internet connection without the user's knowledge. Once installed, spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can gather information such as email addresses, websites visited, passwords, and credit card numbers. ■ **Dialers**: Programs that hijack a user's modem and dial premium-rate phone numbers, such as those required to access pornographic websites. ■ **Password crackers**: Programs that find passwords or encryption keys by trying every possible combination of characters until the code is broken. ■ **Adware**: Programs that display unsolicited advertisements. Adware often includes code that tracks a user's personal information and transmits it to someone else, without the user's knowledge. ■ **Potentially unwanted applications**: Programs that perform some unauthorized (and often harmful or undesirable) act such as viruses, worms, and Trojan horses. ■ **Key loggers**: Programs that record every keystroke a user makes. They can be used to steal passwords and other confidential information.
Save	Click to update the policy and return to the **Groups + Policies** page.
Cancel	Click to return to the **Groups + Policies** page without changing the policy.
Reset to Defaults	Click to assign the original **SonicWALL Default** settings to this policy. **Note**: This resets all settings on all tabs. Settings will not take effect until you click **Save**.

Subscription History

Use this page to view all your existing and previous licenses for SonicWALL protection services.

Your service provider determines what type of information appears on this page, so you might not see some of the columns described below.

If you are viewing this page after selecting **View Cancelled Subscriptions**, only the subscriptions that have been cancelled appear.

- *Managing your subscriptions*

Item	Description
	Select this link to open a page listing service subscriptions that are no longer current. If you are already viewing a list of cancelled subscriptions, a link to display current subscriptions appears instead.
Managed Services	Lists the name of the SonicWALL protection service.
Quantity	Shows the number of licenses allocated to the subscription. This determines how many computers can have the service installed.
Service Start Date	Shows when protection coverage for the service began.
Service Expiration Date	Shows when protection coverage for the service ends. After this date, the subscription can no longer download updates. Expiration dates less than 60 days in the future appear in red. To view instructions for renewing or purchasing a new subscription, select the computer name to open the **Computer Details** page, then click the red action item.
Status	Shows the current status of the subscription: ■ **Active**: The service is installed. ■ **Inactive**: The service is not installed on any computers. ■ **Evaluation**: The subscription is for a free, 30-day trial. ■ **Expired**: The subscription is no longer valid. This status appears in red.
	Shows the name of the contact person for the subscription.
Company Name	Shows the name of the company that purchased the subscription.
Order ID	Shows the order identification number generated by the website hosting Enforced Client.
Grant/Partner Order #	Shows either a grant number from SonicWALL, or an order that a partner supplies to the website hosting Enforced Client while placing the subscription order.
Customer Email Address	Shows where to send messages regarding the subscription.
Edit	Select this link to update the information for the subscription.

Edit Subscription Information

Administrators who manage multiple subscription accounts can use this page to update the contact information and other details for an individual account.

- *Update subscription information*

Item	Description
Quantity	Shows the number of licenses allocated for the subscription. This determines how many computers can have the service installed.
Start Date	Shows when protection coverage for the service began.
Expiration Date	Shows when protection coverage for the service ends. Expiration dates less than 60 days in the future appear in red.
Order ID	Shows the order identification number generated by the website hosting Enforced Client.
Email address	If needed, enter a new email address for sending messages about the account. Status emails are sent to this address.
Company Name	If needed, enter a new name for the company that purchased the subscription.

Item	Description
First Name	If needed, enter a new first name for the subscription's primary contact.
Last Name	If needed, enter a new last name for the subscription's primary contact.
Submit	Click to save the changes and return to the previous page.
Cancel	Click to return to the previous page without updating the subscription information.

Manage Group Administrators

Use this page to add a group administrator account or modify the settings for an existing account.

You can distribute management tasks within your organization by creating group administrators. Group administrators can oversee and manage only the groups assigned to them. The types of tasks they can perform depends on the access level you assign to them.

- *Designating group administrators*

Item	Description
	Select a group administrator from the list, or select **Create New**. Group administrators are listed by their email address. If you select an existing group administrator, the rest of the information on this page is filled in.
Name	Type an optional name to identify the group administrator.
Email address	Type the email address you will use to contact the group administrator about protection issues.
Enter password	Type the password the group administrator uses to log on to the SecurityCenter. Administrative rights based on the group administrator's access level are assigned to this password. Therefore, it must be different from your password.
Re-enter password	Type the password again for verification.
Access level	■ Select **Read only** to allow the administrator to view group and report information. ■ Select **Read and modify reports** to allow the administrator to view and change group and report information. For example, these group administrators can add computers to their groups.
	Select each group the administrator is authorized to manage.
Save	Click to update the group administrator account and return to the **My Account** page.
Cancel	Click to return to the **My Account** page without updating the group administrator account.

Manage All Group Administrators

This page lists information for all the group administrator accounts you have created. Use this page to add a group administrator account or modify the settings for an existing account. The types of tasks they can perform depends on the access level you assign to them.

- *Designating group administrators*

Item	Description
	Click to create a group administrator account.
Name	Shows the name you entered for identification purposes when you created the group administrator account.
Email Address	Select an address to open a blank email message addressed to the group administrator. (You must have a local email application installed to use this feature.)
Groups	Lists the groups assigned to the group administrator account. The group administrator can manage only the assigned groups.
Access Level	Shows the access level assigned to the group administrator account: ■ **Read only**: The group administrator can view group and report information. ■ **Read and modify reports**: The group administrator can view and change group and report information.
Last Logon	Shows the date and time the group administrator last logged on to the SecurityCenter.
Edit	Click to modify the settings for the group administrator account.
Email Password	Click to open an email message addressed to the group administrator that includes the account password, assigned groups, and instructions for accessing information about responsibilities. (You must have a local email application installed to use this feature.)
Delete	Click to remove the group administrator account.

Notification Preferences

Use this page to select the email notifications you would like to receive from your service provider.

Your service provider determines which email notifications appear on this list, so you might not see some of the types described below.

- *Sign up for email notifications*

Item	Description
	Select how often you want your service provider to send status emails about your account. **Important:** Status emails keep you informed about the status of your account. It is important to receive them at regular intervals that are appropriate for your account, based on how often you need to review detection information. By default, you will receive status emails **Weekly**.
Trial expiration notice	Select a checkbox to receive an email reminder when your trial service subscription is about to expire.
Subscription expiration notice	Select a checkbox to receive an email reminder when your service subscription is expired.
Utilization notice	Select a checkbox to receive an email reminder when the number of licenses in use for a subscription approaches the total number of licenses purchased.
Save	Click to save your changes and return to the **My Account** page.
Done	Click to return to the **My Account** page without saving changes.

Edit Profile

Use this page to modify the information your service provider uses to notify you about issues related to your account. Some fields are optional; fields that you must fill in are labeled as required.

- *Set up your profile*
- *Change your SecurityCenter password*

Item	Description
	This information is used to log on to the SecurityCenter.
Email address	Type the email address your service provider uses to contact you about your account. Initially, this is the email address you used when you purchased your protection services.
Password	Type a new password for accessing the SecurityCenter.
Confirm password	Re-type the new password.
Mailing Address section	This information is used to contact your company about your protection services account.
Primary Contact Information section	This information is used to contact a company's designated account representative by telephone.
Language Information	Select the default language for your account. Your SecurityCenter and notification emails use this language.
Save	Click to save your changes and return to the **My Account** page.
Cancel	Click to return to the **My Account** page without saving changes.

Manage Logo

Use this page to upload a customized logo to appear on reports that you email to users and customers. The logo will appear in the upper-right corner of each SecurityCenter page.

You will be able to preview the appearance of your logo before saving it.

- *Add your logo to reports*

Item	Description
	Shows the logo now used for your account. If you have not uploaded a logo, a placeholder appears.
Upload New Logo	Click to open a window that allows you to select a new logo.
Delete Logo	Click to remove your logo from the site. If you have not uploaded a logo, this button does not appear.
Cancel	Click to return to the **My Account** page. Any changes you made on this page are saved.

Utilities

Use this page to download software tools for installing Enforced Client and for troubleshooting installation problems.

- *Download utilities*
- *Silent installation*
- *Push installation*

- *Install the standalone installation agent*

Item	Description
	Select the **VSSetup** link to download the silent installation package, which enables you to remotely deploy Enforced Client on a client computer with no user interaction. Download the utility to the administrative computer or client computer.
Install protection services remotely using the Push Install utility	Select **Run the Push Install utility** to download a program that enables you to deploy Enforced Client directly from the service provider's server onto multiple client computers. Download the utility to the administrative computer.
Uninstall components from a previous installation	Select the **MVSUninst** link to download a cleanup utility that removes components left from a previous installation of Enforced Client or another vendor's protection software. Download the utility directly to a client computer, then double-click to begin installation.
Download the standalone installation agent	Select the **installation agent** link to download software that you can install on client computers to allow users without administrative rights to install Enforced Client.