



ADMINISTRATION GUIDE

Cisco Small Business

Cisco ProtectLink™ Web and Gateway 1.1

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco Ironport, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0907R)

Chapter 1: Introduction	5
Cisco ProtectLink Versions	5
Cisco ProtectLink Web	5
Cisco ProtectLink Gateway	6
How ProtectLink Web Works	6
How ProtectLink Gateway Protects Emails	7
Web Filtering and Threat Protection	8
Email Protection	12
How Email Protection Works	12
Email Protection in a Standard Service	14
Chapter 2: Deploying Cisco ProtectLink Web/Gateway	15
ProtectLink Web System Requirements	15
ProtectLink Gateway System Requirements	15
Email Protection	16
Web Protection	16
Setting Up the Router and Upgrading the Firmware	17
Using the ProtectLink Home Page in the Configuration Utility	17
Registering ProtectLink Web/Gateway	18
Activating ProtectLink Web/Gateway	26
Rerouting Your Mail through ProtectLink Gateway	29
Chapter 3: Configuring Cisco ProtectLink Web/Gateway	30
Configuring Approved Clients	31
Configuring Approved URLs	33
Configuring Overflow Control	35
Configuring Web Threat Protection (Web Reputation)	36
Configuring URL Filtering	37
Enabling the System Log and Outbound Blocking Event Log	40

Chapter 4: License Status and Renewal	42
Reviewing the License Status	42
Renewing the License	44
Renewing the License on SA 500 Series Routers	46
Renewing the License on RV Series Routers	51
Chapter 5: Configuring and Managing Email Protection	54
Launching the Web Portal for Email Protection	55
Features of the IMHS Web Portal	56
Viewing Reports	58
Working with Policies	61
Managing the Approved Senders	64
Managing the Quarantined Messages	66
Configuring the Summary Digest Mail for the Quarantine	67
Working with the Mail Tracking Logs	70
Administration Tasks in the IMHS Console	72
Managing Passwords	72
Importing User Directories	75
Co-Branding to Display a Company Logo in the Web Portal	77
Appendix A: Where to Go From Here	79

Introduction

This chapter includes the following topics:

- [Cisco ProtectLink Versions, page 5](#)
- [How ProtectLink Web Works, page 6](#)
- [How ProtectLink Gateway Protects Emails, page 7](#)
- [Web Filtering and Threat Protection, page 8](#)
- [Email Protection, page 12](#)

Cisco ProtectLink Versions

This guide describes how to configure and deploy the following versions of Cisco ProtectLink:

- [“Cisco ProtectLink Web” on page 5](#)
- [“Cisco ProtectLink Gateway” on page 6](#)

Cisco also provides the Cisco ProtectLink Endpoint. For more information about Cisco ProtectLink Endpoint, see *Cisco ProtectLink Endpoint 1.0 Administration Guide*.

Cisco ProtectLink Web

Cisco ProtectLink Web provides all users with the following:

- Web threat protection to prevent access to dangerous websites
- URL filtering to control employee access to non-business related websites

Cisco ProtectLink Web is a subset of Cisco ProtectLink Gateway, but provides Web threat protection to unlimited number of users, unlike Cisco ProtectLink Gateway, which is available in a 25-seat or 100-seat license.

Cisco ProtectLink Gateway

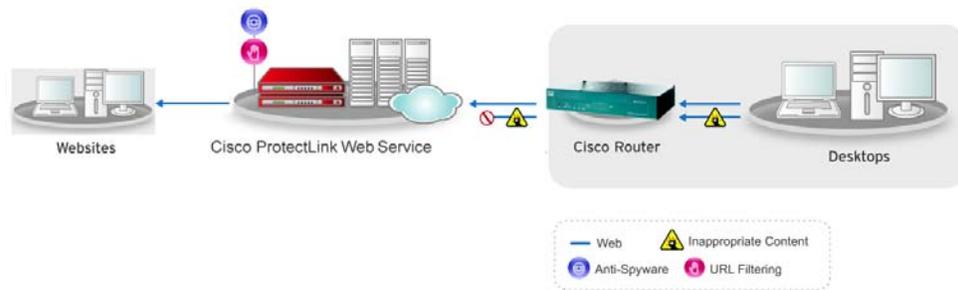
Cisco ProtectLink Gateway provides your Cisco Small Business router or security appliance with the Web security features of Cisco ProtectLink Web and combines it with email security to prevent spam, viruses, and phishing attacks in email.

However, unlike Cisco ProtectLink Web, Cisco ProtectLink Gateway is available in a 25-seat or 100-seat license.

How ProtectLink Web Works

Figure 2 shows the flow of website traffic as it moves from the Internet through the Cisco ProtectLink Web service and the router or security appliance. The router or security appliance blocks website threats.

Figure 1 How ProtectLink Web Works



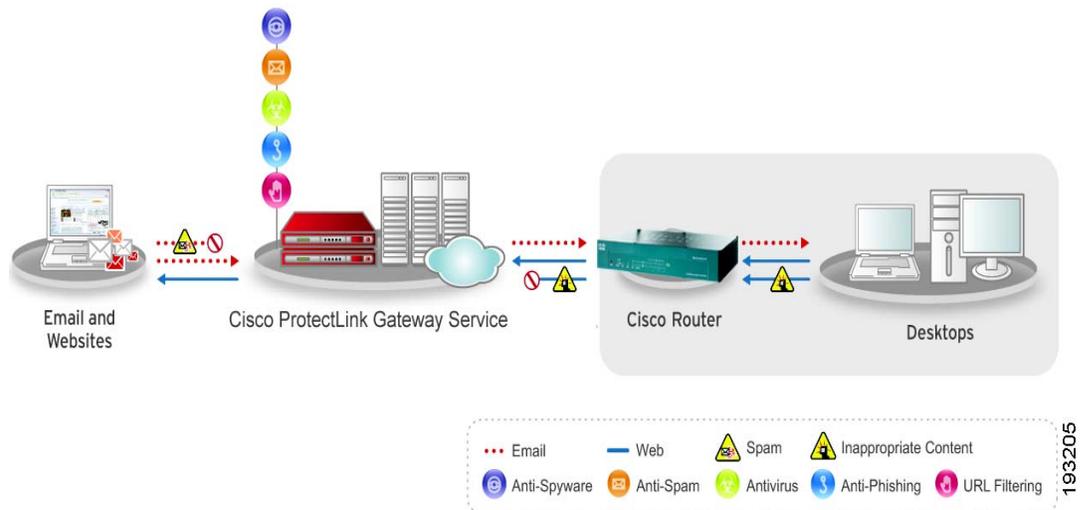
For more information about Cisco ProtectLink Web, go to the following URL:

<http://www.cisco.com/go/protectlink>

How ProtectLink Gateway Protects Emails

Figure 2 shows the flow of email traffic as it moves from the Internet through the Cisco ProtectLink Gateway service and the router or security appliance.

Figure 2 How ProtectLink Gateway Works



The ProtectLink Gateway Service stops email threats in the cloud by leveraging the Trend Micro IMHS capabilities.

Figure 2 also shows how Cisco ProtectLink Gateway provides web filtering and web threat protection.

For more information about Cisco ProtectLink Gateway, go to the following URL:

<http://www.cisco.com/go/protectlink>

Web Filtering and Threat Protection

Cisco ProtectLink Web/Gateway provides web filtering and web threat protection.

Web filtering allows you to:

- Manage Internet access.

For example, you can create policies that prohibit access to websites that your company considers non-work related.

- Create filters by category, time intervals, and days of the week.

For example, you can create filters that prohibit access to certain websites from 8:00 a.m. to 12 p.m. (0800 to 1200) and from 1:00 p.m. to 5 p.m. (1300 to 1700).

Web threat protection protects your network by blocking access to malicious websites. Web threat protection performs the following functions:

- Categorizes websites in real time.

Cisco ProtectLink Web/Gateway employs dynamic rating technology to categorize websites while users browse the Internet.

- Blocks malicious websites in real time.

Cisco ProtectLink Web/Gateway uses an extensive database to determine the reputation or rating of a requested URL. Then, ProtectLink Web/Gateway checks the rating against your company's defined restricted categories. If there is a match, ProtectLink Web/Gateway denies access to the website. ProtectLink Web/Gateway also evaluates the potential security risk of any requested URL by querying the web security database at the time of each HTTP request.

Depending on the Reputation Score of the website and the configured Security Level, Web Protection blocks websites that are known or suspected to be a threat.

- **Reputation Score:** This score determines whether a website is a threat or not. Cisco calculates the score using proprietary metrics. Based on the score, Cisco categorizes a URL as “likely to be a Web threat,” “very likely to be a Web threat,” or “a Web threat.” Cisco considers a URL safe to access if its score exceeds the configured Security Level, which is explained below.
- **Security Levels:** The configured Security Level and the Reputation Score determine whether Web Protection will allow or block access to a URL. Choose one of the following levels:
 - **High:** Blocks a greater number of website threats but increases the risk of false positives.
 - **Medium:** Blocks most website threats and does not create too many false positives. This is the recommended setting.
 - **Low:** Blocks fewer website threats but reduces the risk of false positives.

When ProtectLink Web/Gateway blocks a website, it sends a notification message to the browser to inform the user that access to the site is denied based on company policy.

NOTE If the URL Rating database does not return a rating result in time, the default action is to allow access to the URL.

The following figures, **Figure 3** and **Figure 4**, illustrate the flow of tasks in this process.

Figure 3 Web Protection Workflow—Part 1

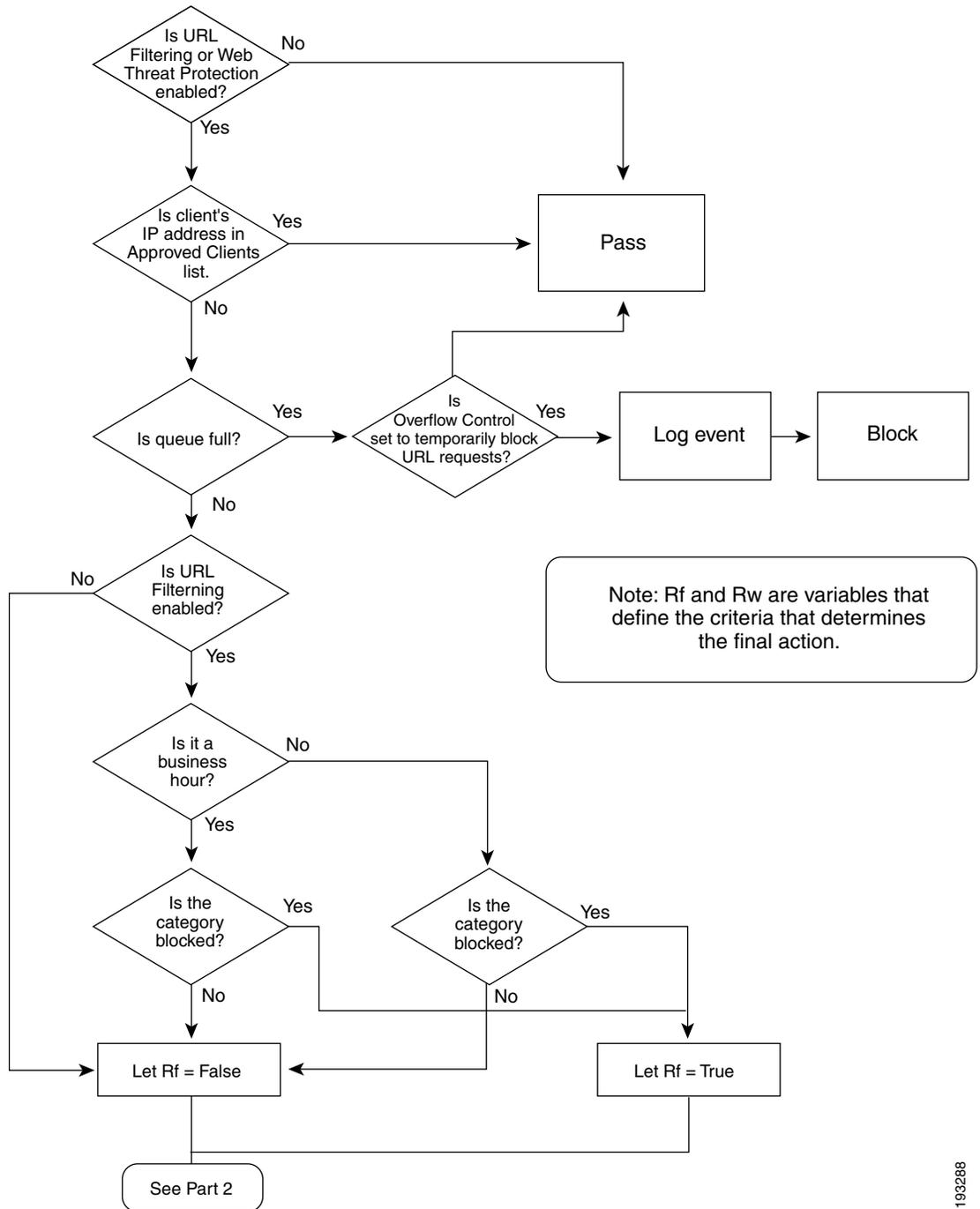
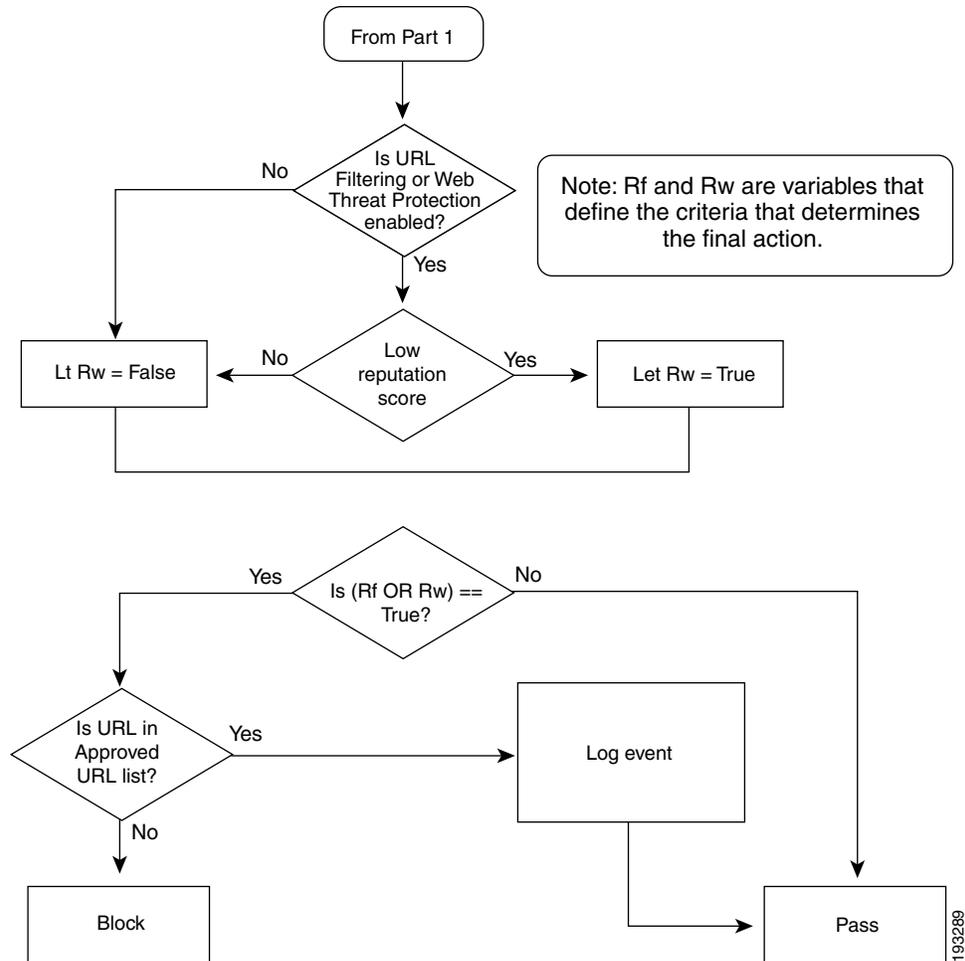


Figure 4 Web Protection Workflow - Part 2



Email Protection

This section includes the following topics:

- [How Email Protection Works, page 12](#)
- [Email Connection-Level Reputation-Based Filtering, page 13](#)
- [Email Protection in a Standard Service, page 14](#)

NOTE This section only applies to Cisco ProtectLink Gateway. Cisco ProtectLink Web does not provide email protection.

How Email Protection Works

The Cisco ProtectLink Gateway provides Email Protection through Trend Micro IMHS, a high-performance, cost-effective hosted security service that protects businesses against spam, viruses, and inappropriate content before they reach the network.

Email Protection proceeds in the following way when an email is sent to an email address at your company:

1. The originating mail server looks up the domain name that is specified in the email address.
2. Because your network is protected by IMHS, the Mail eXchange (MX) record for your domain causes the email to be redirected to IMHS.
3. IMHS servers accept the message and perform message filtering and policy matching on your behalf.
4. Assuming that a message is deliverable, the IMHS servers route the message to your email servers.

Additionally, two layers of protection are provided:

- [Email Connection-Level Reputation-Based Filtering, page 13](#)
- [Email Content-Based Filtering, page 13](#)

Email Connection-Level Reputation-Based Filtering

When an email server attempts to connect to an Email Protection server, the Email Protection server queries the Email Reputation Services (ERS) to determine whether the IP address of the sender is trustworthy.

Email Protection performs this first level of filtering prior to receiving the actual message. The content of the message is not scanned at this point.

The following tasks occur during the Email Protection process:

- If the sending server's IP address is a known source of spam, the sending server's IP address will be marked as untrustworthy. Email Protection permanently rejects connection attempts from this IP address.
- If the sender's computer is part of a botnet or is a zombie computer (both jargon terms for networks or computers that send malicious email automatically), the IP address will be in the ERS dynamic database. The ERS dynamic database identifies spam sources as they emerge and continues to track them for as long as they are active. Email Protection informs the sending server that the server is temporarily unavailable.
- If the server is legitimate, the server tries to re-send the message to the destination email server.

Email Content-Based Filtering

After the message passes the first layer of protection, Email Protection examines the message contents to determine whether the email is spam or contains a threat. The hosted service integrates anti-spam with antivirus, anti-phishing, and anti-spyware technologies.

Email Protection in a Standard Service

ProtectLink Gateway's Email Protection is provided as a Standard service-level offering through Trend Micro IMHS. As a Standard service, ProtectLink Gateway's Email Protection provides the following features:

- A simplified management console, which has pre-set protection defaults and is updated and tuned by Cisco.
- Multi-tiered anti-spam, antivirus, and anti-phishing protection for inbound email traffic, with streamlined management for complete security requiring minimal administration.
- The administrator can quickly create "white lists" of approved senders designated by email address or domain.
- Access to reports, email tracking, and password administration. Internet-based End-User Quarantine is also available for easy management.

Deploying Cisco ProtectLink Web/Gateway

This chapter describes how to deploy Cisco ProtectLink Web/Gateway:

- [ProtectLink Web System Requirements, page 15](#)
- [ProtectLink Gateway System Requirements, page 15](#)
- [Setting Up the Router and Upgrading the Firmware, page 17](#)
- [Registering ProtectLink Web/Gateway, page 18](#)
- [Activating ProtectLink Web/Gateway, page 26](#)
- [Rerouting Your Mail through ProtectLink Gateway, page 29](#)

ProtectLink Web System Requirements

Before you deploy ProtectLink Web, make sure that your system meets the requirements for Email Protection and Web Protection, as described below.

ProtectLink Gateway System Requirements

Before you deploy ProtectLink Gateway, make sure that your system meets the following requirements:

- Web Browser
Microsoft Internet Explorer 6.x or 7.0 or Mozilla Firefox 2.x or 3.0
- Internet connection

Email Protection

Email Protection does not require you to purchase additional hardware (other than your mail gateway and router) located on your premises. All scanning hardware is located offsite at Trend Micro's secure network operating centers. To access the Email Protection Administration console, a personal computer with access to the Internet is required:

- Web Browser: Microsoft™ Internet Explorer 6.x or 7.0 or Mozilla™ Firefox™ 2.x or 3.0
- Internet connection
- Access to the MX records on the DNS server in order to reroute email messages to Trend Micro servers. Contact your Internet Service Provider for more information or for help with the configuration.



WARNING Do not redirect your MX record until you receive confirmation that your account has been established. If you redirect your MX record before your account is set up, your email messages may be lost.

Web Protection

Web Protection does not require any additional hardware (other than your router) located at your premises.

Setting Up the Router and Upgrading the Firmware

Set up your router or security appliance and install the latest firmware by following the instructions in the documentation for your device. With the latest firmware installed, the Configuration Utility includes a ProtectLink module that you can find in the menu bar. Refer to the following examples:



NOTE If ProtectLink is supported on your router or security appliance and you do not see ProtectLink on the menu bar, upgrade the firmware. For more information, see the administration guide for the device.

Using the ProtectLink Home Page in the Configuration Utility

The Configuration Utility for your router or security appliance includes a page with links to the ProtectLink website. These links make it easy for you to buy, register, and activate ProtectLink services.

To open the page with links to the ProtectLink website:

- (SA 500 Series Security Appliances only) Click **Administration > License Management**.

The License Management page appears.

- (Cisco RV Series Routers only) Click **ProtectLink** in the menu bar. On some models, also click **ProtectLink** in the navigation tree.

The ProtectLink home page appears.

NOTE Different router models may have different configuration windows. Also, the windows might appear in an order different than the order in this chapter. For more information about the Configuration Utility, see the documentation for your router or security appliance. Also, for more information about a window, see the Configuration Utility's online Help.

Registering ProtectLink Web/Gateway

Register your service to activate your service and sign up for access to the web portal for online administration.

NOTE (ProtectLink Gateway only) Fully activating your service requires entering a list of the domains that you want to redirect for hosting to IMHS. IMHS then becomes the primary mail host for the Email Protection portion of the ProtectLink Gateway service. If you do not have this information, you can register the service now and add the missing information later. You will receive instructions in the post-registration email.

To register the service:

- STEP 1** Launch the Configuration Utility for your router or security appliance, and then log in.
- STEP 2** Open the ProtectLink Home page or License Management page, as described in [Using the ProtectLink Home Page in the Configuration Utility, page 17](#).

If you do not have a ProtectLink user account, the Configuration Utility opens the Register Your Product window.

Home > Support > [Online Registration](#) > **Register Your Product**

Register Your Product

Please enter your Registration Key (for example xx-xxxx-xxxxxx-xxxxxx) below and click **Next**. Contact your reseller if you cannot locate your Registration Key.

If you are a current ProtectLink Gateway user, and have purchased another router, [Click here](#) to register the new router.

For further assistance, contact www.cisco.com/support

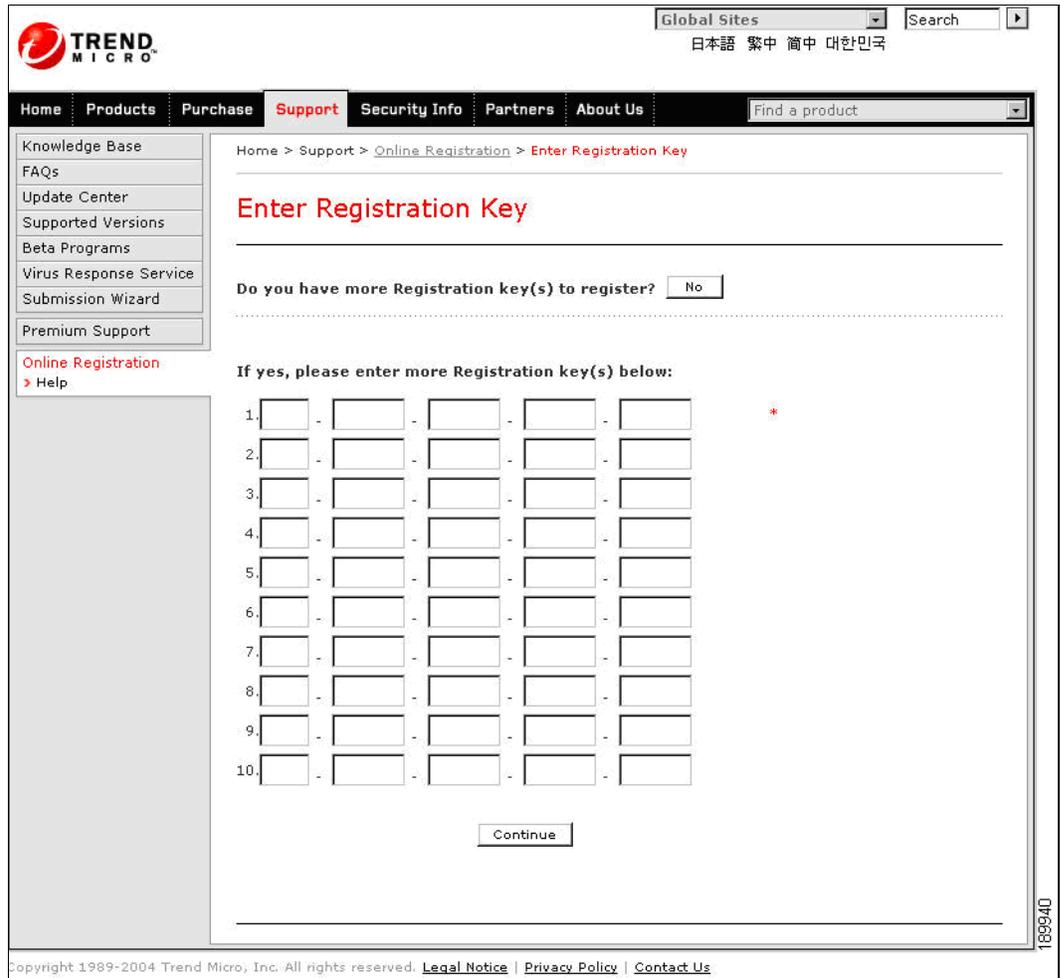
Enter your Registration Key:

[LR] - [RNSW] - [KPYM] - [SHUF] - [NUF]

Copyright 1989-2004 Trend Micro, Inc. All rights reserved. [Legal Notice](#) | [Privacy Policy](#) | [Contact Us](#)

STEP 3 Enter your **Registration Key**, and then click **Next**.

The Enter Registration Key page appears.



STEP 4 Enter additional **Registration Keys**, if necessary, and then click **Continue**.

The Confirm License Terms page appears.

The screenshot displays the Trend Micro website interface. At the top right, there is a 'Global Sites' dropdown menu with options for Japanese, Chinese, and Korean, and a search bar. Below this is a main navigation bar with links for Home, Products, Purchase, Support, Security Info, Partners, and About Us. A left sidebar contains a 'Knowledge Base' menu with various support links. The main content area is titled 'Confirm License Terms' and contains the following text:

Trend Micro licenses its products worldwide in accordance with certain terms and conditions. By breaking the seal on the CD jacket in the product box or registering the product's Registration Key, you or your company or organization accepted a Trend Micro license agreement.

Below you will find a representative Trend Micro License Agreement. If you or your company has already entered into a valid written license agreement with Trend Micro, click on the button below to confirm your acceptance of that original written agreement. If, for some reason, you have not already accepted a license agreement with Trend Micro, review the following Trend Micro License Agreement and click on the button below if you accept its terms. If not, or if you have any questions, contact Trend Micro before proceeding.

BY BUSINESS AND OTHER ENTITIES IS SUBJECT TO THE FOLLOWING LEGAL TERMS AND CONDITIONS

Enterprise and SMB Software and Services
Date: April 2007 v.1
English/Multi-country

1. Binding Contract. This License Agreement (Agreement) is a binding contract between Trend Micro Incorporated or a licensed affiliate (Trend Micro) and the legal entity that will be using Trend Micro Software or Services on a paid or trial use basis. An employee or other agent, including a reseller or contractor which installs or registers Software or Services, of this entity (Representative) must accept this Agreement on behalf of the entity before the Software or Service may be used. Entities whose Representative has validly accepted this Agreement are referred to as You. Please print this Agreement and save a copy electronically.

NOTE: SECTION 20 OF THIS AGREEMENT LIMITS TREND MICROS LIABILITY. SECTIONS 8, 16, 17 AND 18 LIMIT OUR WARRANTY OBLIGATIONS AND YOUR REMEDIES. SECTION 10 SETS FORTH IMPORTANT CONDITIONS OF USE FOR SOFTWARE AND SERVICES. SECTION 14 TELLS YOU WHAT INFORMATION WE COLLECT FROM THE SOFTWARE YOU INSTALL. READ THESE SECTIONS CAREFULLY.

At the bottom of the page, there are two radio buttons: I Accept and I Don't Accept *. Below these is a 'Submit' button. A 'Printer-Friendly Format' link is also visible.

STEP 5 Read the License Terms carefully. If you agree to the terms, select **I Accept**, and then click **Submit**. The Confirm Product or Service Information page appears.

TREND MICRO Global Sites Search

日本語 繁体中文 简体中文 대한민국

Home Products Purchase **Support** Security Info Partners About Us Find a product

Home > Support > Online Registration > Confirm Product Information

Confirm Product or Service Information

Thank you for choosing Trend Micro.
You get the following product/service:

Registration Key: UR-TONS-CL-17-11111-11111
Product name: ProtectLink
Version type: Full
Language: English
Operating system: Windows
Platform: Gateway Service

License start date: 1/4/2008
Maintenance end date: 1/4/2009

Account Activation
 Activating your service requires a list of the domains you wish to redirect for hosting by modifying your MX record to use Trend Micro InterScan Messaging Hosted Security as the primary domain host. We recommend further that you only accept mail from Trend Micro to limit authorized SMTP connections.

Domain 1	<input type="text"/>	IP Address 1	<input type="text"/>
Domain 2	<input type="text"/>	IP Address 2	<input type="text"/>
Domain 3	<input type="text"/>	IP Address 3	<input type="text"/>
Domain 4	<input type="text"/>	IP Address 4	<input type="text"/>

For additional domains, please contact support at imhs_support@trendmicro.com.

Messaging Environment:
 Please complete this section accurately. Incomplete or inaccurate information based on observed traffic for your account may require an adjustment in licensing terms.

Number of Users: *

Note: For significant changes in account size, please contact Support at imhs_support@trendmicro.com to discuss licensing requirements and future capacity needs.

For capacity planning purposes, do you expect any unusual message traffic events or content types that would generate increased traffic requirements? Yes No *

If YES, please explain:

For a copy of the Service Level Overview (SLO), please [click here](#).

If the above information is correct, please continue with the registration process; otherwise, please contact [Trend Micro](#).

Copyright 1989-2004 Trend Micro, Inc. All rights reserved. [Legal Notice](#) | [Privacy Policy](#) | [Contact Us](#)

198194

STEP 6 In the section **Do you have Domain/IP address now?**, choose one of the following options:

- **Yes:** Choose this option if you are ready to enter a list of the domains that you want to redirect for hosting to IMHS. To fully activate your service you must enter a list of your domains. Then enter each domain or IP address. If you need to enter more than four domain names or IP addresses, contact Cisco Support.
- **No:** Choose this option if you are not ready to enter a list of the domains now. In this case, the system will use temporary settings. You can update this info later by contacting Cisco support.

STEP 7 In the **Messaging Environment** section, enter the following information:

- **Number of Users:** Enter the number of users that will be registered with the service, according to your purchase agreement.
- Answer the capacity planning question by choosing one of the following options:
 - **Yes:** Choose this option if you expect unusual message traffic or content types that would generate increased traffic requirements. Enter an explanation of your situation in the text entry box.
 - **No:** Choose this option if you do not expect unusual message traffic or content types.

The Registration Information page appears.

TREND MICRO Global Sites 日本語 繁体中文 简体中文 대한민국 Search

Home Products Purchase **Support** Security Info Partners About Us Find a product

Home > Support > Online Registration > Registration Information

Registration Information

NOTICES: The following online form asks you for contact information, including certain personal data. By entering such information and clicking the Submit button at the bottom of the form, you are giving your express consent for Trend Micro and its authorized agents to collect such personal data and to process and store such personal data in countries, such as the United States, where Trend Micro has offices and where the personal data protection laws may not be as strict as in your home country.

As part of its compliance with U.S. export control laws, Trend Micro may also share certain information you provide below with a third-party service provider operating in the U.S. and Canada. This shared data is not retained by the third-party service provider once it verifies that your use of the software will not violate U.S. export control laws.

(Required fields *)

Company name: *

Company address: *

City: *

State/Province: *

ZIP/Postal code: *

Country/Region: *

Please create a logon ID for your company profile. A temporary password will be sent to you via email after registering, which you should change the first time you log on.

Logon ID: *
(6 to 25 characters)

+ Add Back Up Contact Information

Are you a Trend Micro reseller? Yes No *

Have you installed an evaluation copy of any of the products you are registering?

Linksys Router English Gateway Service, OS: Yes No
Windows

Copyright 1999-2004 Trend Micro, Inc. All rights reserved. [Legal Notice](#) | [Privacy Policy](#) | [Contact Us](#)

189694

STEP 8 Enter your contact details in full, including your email address and Logon ID for your company profile, and then click **Submit**.

The Confirm Registration page appears, with your contact and domain details.

TREND MICRO Global Sites: 日本語 繁體中文 简体中文 대한민국

Home Products Purchase **Support** Security Info Partners About Us Find a product

Home > Support > Online Registration > **Confirm Registration Information**

Confirm Registration Information

Please confirm that the information displayed below is correct:

Company: Trend Micro Inc.
Street: 10101 N. De Anza Blvd.
City: Cupertino
State/Province: California
Country/Region: United States
ZIP/Postal code: 95014

Maintenance expiration date: 1/4/2009
 An email notification will be sent to your contact email address before the product maintenance contract expires.

Account Administrator Contact
Name: [Your contact details]
Title:
Phone number:
Email address:
Mailing address:

Send email notifications before product Maintenance expires.
 I want to receive email virus alerts

Logon ID: [Your Logon ID]

Message Environment
 Number of users: 5
 unusual message traffic events: No
 Explanation: N/A

The list of the domains to redirect for hosting

Domain 1: [Your Domain]	IP 1: [Your IP Address]
Domain 2: N/A	IP 2: N/A
Domain 3: N/A	IP 3: N/A
Domain 4: N/A	IP 4: N/A

Copyright 1989-2004 Trend Micro, Inc. All rights reserved. [Legal Notice](#) | [Privacy Policy](#) | [Contact Us](#)

Activating ProtectLink Web/Gateway

After completing ProtectLink Web/Gateway registration, you should receive within 24 to 48 hours an email indicating successful registration of the service.

The email provides you with an Activation Code, affirming your Logon ID, and giving you a temporary password for your company. You should change the password after you log in.

The email also contains instructions for providing your email domains and mail server IP address for redirection, if you did not complete that portion during the registration process.

To activate the ProtectLink Web/Gateway service:

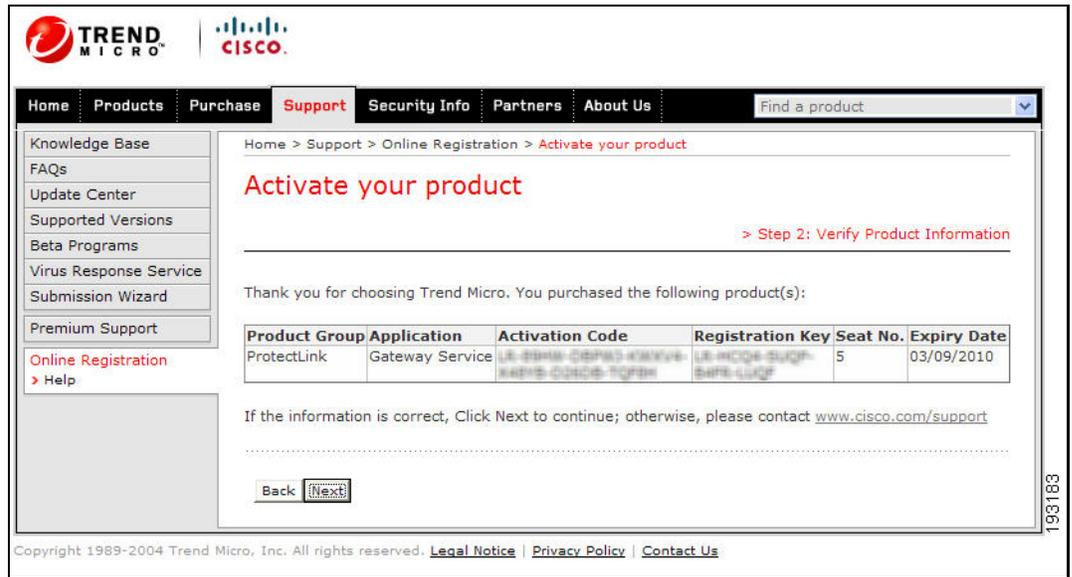
- STEP 1** Launch the Configuration Utility for your router or security appliance and then log in.
- STEP 2** Open the ProtectLink Home page, as described in [Using the ProtectLink Home Page in the Configuration Utility, page 17](#).
- STEP 3** At the bottom of the page, click the link to activate your service. The link may read **I have my Activation Code (AC) and want to activate ProtectLink Web/Gateway** or **Use the Activation Code (AC) to activate ProtectLink services**.

The Activate Your Product > Step 1: Enter Activation Code window appears.

The screenshot shows the 'Activate your product' page in the Trend Micro Cisco ProtectLink Web/Gateway interface. The page is titled 'Activate your product' and is part of a multi-step process, currently on 'Step 1: Enter Activation Code'. The navigation menu includes 'Home', 'Products', 'Purchase', 'Support', 'Security Info', 'Partners', and 'About Us'. A search bar is located in the top right corner. The main content area contains the following text: 'Your Activation Code(for example xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx) is located on the Product Registration Certificate you received. You can contact Trend Micro if you cannot locate your Activation Code. Enter your Activation Code below and click **Next**.' Below this text is a form with seven input fields separated by dashes, and a 'Next' button at the bottom. The footer of the page contains the copyright information: 'Copyright 1989-2004 Trend Micro, Inc. All rights reserved. [Legal Notice](#) | [Privacy Policy](#) | [Contact Us](#)'.

STEP 4 Enter your **Activation Code** and then click **Next**.

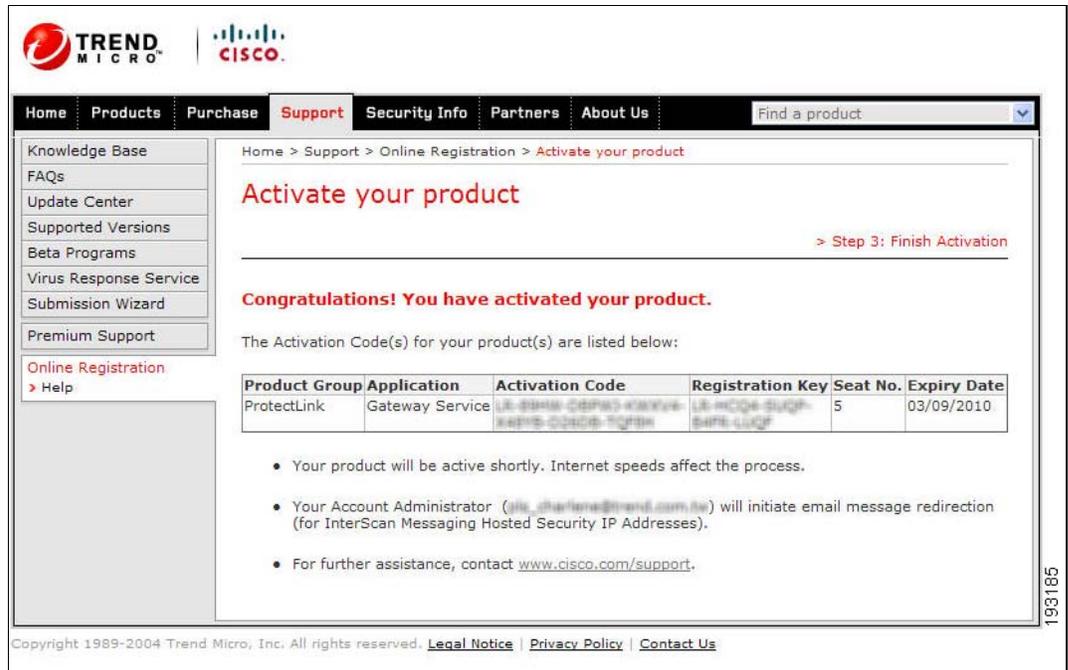
The Activate Your Product > Step 2: Verify Product Information window appears.



STEP 5 Verify that the product information is correct.

If the information is correct, click **Next**.

If you see a message indicating that the information needs to be corrected, click **Back**, and re-enter the activation code.



The Activate Your Product > Step 3: Finish Activation window appears.

You have successfully activated the product. Your service will be active by the next working day.

Rerouting Your Mail through ProtectLink Gateway

After Trend Micro receives your activation details, Trend Micro sends you additional emails.

- The Web Protection Activation email provides a Logon ID and temporary password, along with instructions to customize Web Protection for your company.
- The Email Protection Activation email includes your IMHS Username and temporary Password to access the IMHS web portal, with instructions on how to redirect your Mail Exchange (MX) record.
- When your Email Protection account is set up correctly, a Test Email is sent to ensure that email messages can flow through the Trend Micro servers properly.

NOTE If you did not provide the Domain Name and/or IP Address of your email server during registration, your Email Protection account is not created. Follow the instructions in the post-registration email to provide these details. Do not redirect your MX record until you receive the test email that your account has been properly established. If you redirect your MX record before your account is fully set up, your email messages may be lost.

Configuring Cisco ProtectLink Web/Gateway

After you activating your account, configure your router for Web Protection as described in the following sections:

- [Configuring Approved Clients, page 31](#)
- [Configuring Approved URLs, page 33](#)
- [Configuring Overflow Control, page 35](#)
- [Configuring Web Threat Protection \(Web Reputation\), page 36](#)
- [Configuring URL Filtering, page 37](#)
- [Enabling the System Log and Outbound Blocking Event Log, page 40](#)

NOTE Different router models may have different configuration windows. Also, the windows might appear in an order different than the order in this chapter. For more information about the Configuration Utility, see the documentation for your router or security appliance. Also, for more information about a window, see the Configuration Utility's online Help.

Configuring Approved Clients

The Approved Clients List details the computers that have unrestricted Web access. ProtectLink approves all URL requests from the specified IP addresses.

The Web Protection settings do not apply to the Internet requests of any computer whose IP address is in this list.

To configure the Approved Clients list:

STEP 1 Launch the Configuration Utility for your router or security appliance, and then log in.

STEP 2 (RV042/82/16 routers) Click **ProtectLink** on the menu bar.

The Web Protection window appears. The list of approved clients appears at the bottom of the page.

Approved Clients List		
<input type="checkbox"/>	Approved Client IP Addresses	Edit
<input type="checkbox"/>	1.1.1.2	
<input type="checkbox"/>	1.2.3.4	

STEP 3 (SA500 series routers) Click **ProtectLink** on the menu bar, and then click **Global Settings > Approved Clients** in the navigation tree to display the list of approved clients.

STEP 4 To enable the Approved Clients list, check the **Enable Approved Clients List** box, and then click **Apply** or **Save Settings**.

STEP 5 To add a new client, or multiple clients in an IP address range, click **Add**.

NOTE Other options: To edit an entry, click the pencil button in the **Edit** column. To delete an entry, click the check box and then click **Delete**. To select all entries in the table, check the box in the top left corner of the heading row.

STEP 6 To identify the client (or clients), enter the following information:

- **IP Address Type:** Choose **Single** to enter one IP address, or choose **Range** to specify a range of IP addresses.
- **Start IP Address:** For Single, enter the IP address. For Range, enter the first IP address in the range.
- **End IP Address:** For Single, leave this field blank. For Range, enter the last IP address in the range. ProtectLink will approve all URL requests from the specified IP addresses. For example, 1.1.1.2 - 1.1.1.10 will approve all the IP addresses that fall in the range.

STEP 7 Click **Apply** or **Save Settings**. The details will appear in the Approved Clients List.

NOTE If your Configuration Utility includes all Web Protection settings on one page, you can save the settings after configuring all of the desired features on the page.

Configuring Approved URLs

The Approved URLs List details the websites that always can be accessed. The approved sites are defined by specific URLs or keywords within URLs.

To configure Approved URLs:

- STEP 1** Launch the Configuration Utility for your router or security appliance, and then log in.
- STEP 2** Click **ProtectLink** on the menu bar, and then click **Global Settings > Approved URLs** in the navigation tree.

NOTE If your Configuration Utility does not include a left navigation tree, click **ProtectLink** and then choose **Web Protection**. Then scroll down to the **Approved URLs** area of the page. The layout will vary from the illustration.

<input type="checkbox"/>	Approved URL	Type	Edit
<input type="checkbox"/>	www.trendmicro.com	Web site	
<input type="checkbox"/>	cisco	URL keyword	

- STEP 3** To enable this feature, check the **Enable Approved URLs List** box, and then click **Apply**.
- STEP 4** To add a new URL or keyword to the list, click **Add**.

NOTE Other options: To edit an entry, click the pencil button in the **Edit** column. To delete an entry, click the check box and then click **Delete**. To select all entries in the table, check the box in the top left corner of the heading row.

STEP 5 To specify either the exact URL or a keyword, enter the following information:

- **URL:** Type the exact URL for the site (for example, *www.yahoo.com*) or enter partial URL for use as a keyword (for example, *yahoo*).
- **Match Type:** Choose one of the following options:
 - **Web site:** Choose this option if you want to allow access only to the exact URL that you entered in the URL box. For example, if you entered *www.yahoo.com* for the URL, then your users can access *www.yahoo.com*, but they will be blocked from *www.yahoo.com.uk* or *www.yahoo.co.jp*.
 - **URL keyword:** Choose this option if you want to allow access to any URL that includes the keyword that you entered in the URL box. For example, if you enter *yahoo* for the URL, then your users can access websites such as *www.yahoo.com*, *tw.yahoo.com*, *www.yahoo.com.uk*, and *www.yahoo.co.jp*.

STEP 6 Click **Apply** or **Save Settings** to save the settings. The details will appear in the Approved Clients List.

NOTE If your Configuration Utility includes all Web Protection settings on one page, you can save the settings after configuring all of the desired features on the page.

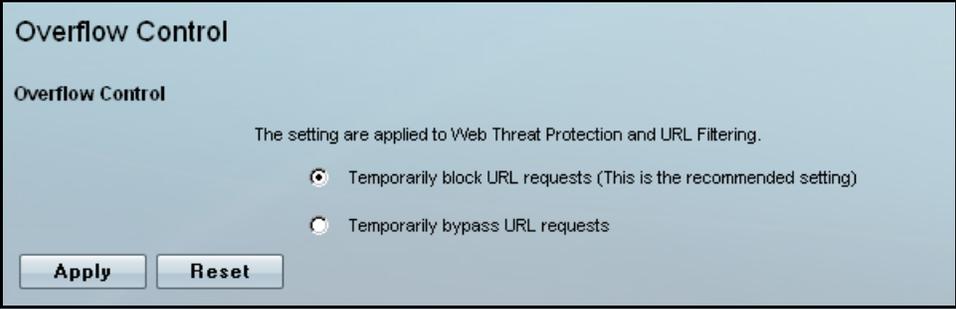
Configuring Overflow Control

Overflow Controls determines how ProtectLink handles excess URL requests. During periods of overflow, you can either block the requests or to bypass URL Filtering. Blocking the requests is the default setting and is recommended to ensure that URL Filtering continues to protect your business during busy periods.

To configure Overflow Control:

- STEP 1** Launch the Configuration Utility for your router or security appliance, and then log in.
- STEP 2** Click **ProtectLink** in the menu bar, and then click **Web Protection > Overflow Control** in the navigation tree.

NOTE If your Configuration Utility does not include a left navigation tree, click **ProtectLink** and then choose **Web Protection**. Then scroll down to the **Overflow Control** area of the page. The layout will vary from the illustration.



Overflow Control

Overflow Control

The settings are applied to Web Threat Protection and URL Filtering.

Temporarily block URL requests (This is the recommended setting)

Temporarily bypass URL requests

Apply Reset

- STEP 3** Choose one of the following options:
 - **Temporarily block URL requests:** Choose this option to manage overflow by temporarily blocking all new website requests. This setting is recommended.
 - **Temporarily bypass URL requests:** Choose this option to manage overflow by temporarily bypassing URL Filtering for new website requests.
- STEP 4** Click **Apply** or **Save Settings** to save the settings.

NOTE If your Configuration Utility includes all Web Protection settings on one page, you can save the settings after configuring all of the desired features on the page.

Configuring Web Threat Protection (Web Reputation)

If you enable Web Threat Protection (also called Web Reputation), you can choose the security level.

To configure Web Threat Protection:

- STEP 1** Launch the Configuration Utility for your router or security appliance, and log in.
- STEP 2** Click **ProtectLink** in the menu bar, and then click **Web Protection > Web Threat Protection** in the navigation tree.

NOTE If your Configuration Utility does not include a left navigation tree, click **ProtectLink** and then choose **Web Protection**. Then scroll down to the **Web Reputation** area of the page. The layout will vary from the illustration.



Web Threat Protection

Web Threat Protection

Enable Web Threat Protection:

Security Level

High Blocks a greater number of Web threats but increases the risk of false positives.

Medium Blocks most Web threats and does not create too many false positives. This is the recommended setting.

Low Blocks fewer Web threats but reduces the risk of false positives.

Apply **Reset**

- STEP 3** To enable this feature:

- Check the **Enable Web Threat Protection** check box.

NOTE On some models, this check box appears at the top of the Web Protection page.

- Select the **Security Level for Web Reputation**:
 - **High**: Blocks a greater number of web threats but increases the risk of false positives. In other words, you may block websites that are safe.
 - **Medium**: Blocks most web threats and does not create too many false positives. This setting is recommended.
 - **Low**: Blocks fewer web threats, but reduces the risk of false positives.

STEP 4 Click **Apply** to save your settings.

NOTE If your Configuration Utility includes all Web Protection settings on one page, you can save the settings after configuring all of the desired features on the page.

Configuring URL Filtering

You can use URL Filtering to restrict access to specified URLs. You can set different URL Filtering options for your business hours and your non-business hours.

To configure URL Filtering:

STEP 1 Launch the Configuration Utility for your router or security appliance, and then log in.

STEP 2 Click **ProtectLink** in the menu bar, and then click **Web Protection > URL Filtering** in the navigation tree.

NOTE If your Configuration Utility does not include a left navigation tree, click **ProtectLink** and then choose **Web Protection**. Then scroll down to the **URL Filtering** area of the page. The layout will vary from the illustration.

STEP 3 To enable URL Filtering, check the **Enable URL Filtering** box.

STEP 4 In the **Filtered Categories** table, choose the categories and hours for filtering.

- **Filtered Categories:** If you want to see the sub-categories, click the expansion + button next to the Category name.
- **Business Hours:** For each category or sub-category, check the box to activate URL Filtering during the Business Days and Business Times that you will define on this page.
- **Leisure Hours:** For each category or sub-category, check the box to activate URL Filtering during non-business hours. Non-Business Hours are the days and times that are not included in the specified **Business Days** and **Business Times**.

STEP 5 Define the Business Hours for URL filtering by choosing the **Business Days** and **Business Times**:

- **Business Days:** Check the box for each day that you want to include in your Business Hours. All days that are not selected will be considered Leisure Hours for the purpose of URL filtering.
- **Business Times:** Choose from the following options:
 - **All Day (24 hours):** Choose this option if you want your Business Hours to include all hours in the specified day.
 - **Specify Business Hours:** Choose this option if you want your Business Hours to be restricted to specified time periods. Then choose the **Morning** and **Afternoon** time periods. All hours that are not included in these ranges will be considered Leisure Hours for the purpose of URL filtering.

Morning: Check the box to specify the morning hours (before noon). Use the **From** and **To** drop-down lists to specify the range of Business Hours for the morning.

Afternoon: Check the box to specify the afternoon hours. Use the **From** and **To** drop-down lists to specify the range of Business Hours for the afternoon.

URL Filtering

Enable URL Filtering:

URL Categories	Filtering		Instances Blocked
	Business Hours	Leisure Hours	
+ Computers/Bandwidth	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0
+ Computers/Harmful	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0
+ Computers/Communication	<input type="checkbox"/>	<input type="checkbox"/>	0
+ Adult	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0
+ Business	<input type="checkbox"/>	<input type="checkbox"/>	0
+ Social	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0
+ General	<input type="checkbox"/>	<input type="checkbox"/>	0

Reset Counters:

Business Days

Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Business Times

All Day (24 hours):

Specify Business Hours: (Note: Time not designated as business time will be considered leisure time.)

Morning:

From: 08:00 To: 12:00

Afternoon:

From: 13:00 To: 18:00

© 2009 Trend Micro Incorporated. All rights reserved.

193208

STEP 6 Click **Apply** to save your settings.

NOTE If your Configuration Utility includes all Web Protection settings on one page, you can save the settings after configuring all of the desired features on the page.

Enabling the System Log and Outbound Blocking Event Log

ProtectLink Web/Gateway can provide a system log (syslog) as well as an Outbound Blocking Event log for all outbound events that it blocks. Enable these features to maintain the logs.

To enable the syslog and the Outbound Blocking Event Log:

- STEP 1** Launch the Configuration Utility of your router or security appliance, and then log in.
- STEP 2** Click the **Administration** on the menu bar, and then click **Logging > Remote Logging** in the navigation tree. The Remote Logging Config page appears.

NOTE If your Configuration Utility does not include a left navigation tree, click **Administration**, and then choose **Log**. Then scroll down to the **Syslog** area of the page. The layout will vary from the illustration.

Remote Logging Config

Log Options

Remote Log Identifier: SA520

Enable E-Mail Logs

Enable E-Mail Logs:

E-Mail Server Address:

Return E-Mail Address:

Send to E-Mail Address:

Authentication with SMTP Server: None

User Name:

Password:

Respond to Identd from SMTP Server:

Send E-mail logs by Schedule

Unit: Never

Day: Sunday

Time: 1:00 a.m. p.m.

Syslog Server

SysLog Server:

Apply **Reset**

STEP 3 In the **Syslog Server** field, enter the name or IP address of the syslog server.

NOTE If your Configuration Utility includes an Enable Syslog check box, check the box to enable this feature.

STEP 4 Click **Apply** or **Save Settings** to save your settings.

STEP 5 To view the logs, use one of the following methods, depending on the model:

- In a Configuration Utility with the left navigation tree, click **Status** on the menu bar, and then click **View Logs > Policy Enforcement Logs** in the navigation tree.
- In a Configuration Utility with the **Administration > Log** page, click the **View Log** button near the bottom of the page.

The Log page appears, where you can view All, System, Access, Firewall, and VPN logs page by page.

License Status and Renewal

Using the Configuration Utility of your router or security appliance, you can view your ProtectLink license status information and renew the license.

- [Reviewing the License Status, page 42](#)
- [Renewing the License, page 44](#)

Reviewing the License Status

To review license information:

- STEP 1** Launch the Configuration Utility for your router or security appliance, and then log in.
- STEP 2** Click the **ProtectLink** on the menu bar, and then click **License > Summary** in the navigation tree.

NOTE If your Configuration Utility does not include a left navigation tree, click **ProtectLink**, and then choose **License**, to view the License Information table. The layout will vary from the illustration.

License Summary

 Trend Micro ProtectLink Gateway is active.

License information last updated on: 03/19/2009 07:33:41 [Update Information](#)

License Information [View detailed license online](#)

Status:	Activated
Platform:	Gateway
License Expires On:	03/19/2010

The status of the license is indicated by the status icon and the status message near the top of the page.

- Cisco ProtectLink Service is Active.



- Cisco ProtectLink Service will expire in 30 days.



- Cisco ProtectLink Service has expired.



STEP 3 Click **Update Information** to update your license information. Your license information is updated and stamped with a date indicating when the license information was last updated.

STEP 4 Click the **View detailed license online** link to view more details of your product license.

The My Product Details Web page appears.

The screenshot shows the Trend Micro website interface. At the top right, there is a 'Global Sites' dropdown menu with options for Japanese, Chinese, and Korean. Below it is a search bar. The main navigation bar includes links for Home, Products, Purchase, Support, Security Info, Partners, and About Us. A 'Find a product' search box is also present. The left sidebar contains a 'Knowledge Base' section with links to FAQs, Update Center, Supported Versions, Beta Programs, Virus Response Service, Submission Wizard, and Premium Support. The main content area displays the 'My Product Details' page with the following information:

Product:	Linksys Router
Version:	Full
Operating system:	Windows
Platform:	Gateway Service
Language:	English
Licenses:	25
Activation Code:	[Your Activation Code]
License expiration:	1/4/2009 12:00:00 AM

At the bottom of the page, there is a copyright notice: 'Copyright 1989-2004 Trend Micro, Inc. All rights reserved. [Legal Notice](#) | [Privacy Policy](#) | [Contact Us](#)'. A vertical ID number '189920' is visible on the right side of the screenshot.

Renewing the License

Renewing the license, whether it is a 12-month license that you purchased or a 30-day trial license involves purchasing a new Registration Key (RK).

With the new RK, follow the steps below to generate a new Activation Code (AC).

- STEP 1** Log into the router.
- STEP 2** Click the **ProtectLink** tab.
- STEP 3** Click **License**.
- STEP 4** Click **Add a seat**.
- STEP 5** Log into TrendMicro Registration Server with your ProtectLink user ID.
- STEP 6** If necessary, open the My Products window (Support > Online Registration > My Products).

Home > Support > Online Registration > My Products

My Products

Company Name: Cisco Systems, Inc. [View/Edit Company Profile](#)

Register New Product/Add Seat Renew Product Merge Licenses

Item	Product	Sales Type	Registration Key	Registration Date	Activation Code	Expiration Date
1	ProtectLink	Retail Package	LR-7M4H-S9SH-VHVQ-CJFB	2/13/2010	XXXXXXXX-XXXX XXXXXXXXXXXX XXXXXXXX-XX	2/13/2011
2	ProtectLink	Retail Package	LR-Q2P5-X9DD-7SKU-HYRQ	2/15/2010	XXXXXXXX-XXXX XXXXXXXXXXXX XXXXXXXX-XX	3/15/2010

- STEP 7** Click **Register New Product/Add Seat**.

NOTE Do not click **Renew Product**.

- STEP 8** Enter the new RK you have received from Cisco.
- STEP 9** Click **Next**.

STEP 10 Click **Register New Product Separately**.

The screenshot shows the Trend Micro registration server interface. The main heading is "Register New Product". Below the heading, it indicates "Step 3: Similar Product Check". The text states: "These products are similar to the ProtectLink you are registering. If the new 5 seats of ProtectLink you are registering will be installed on the same network as one of the below existing registered products, select that product so their seats can be merged into one License and corresponding Activation Code." A table lists two existing products:

	Product Name	Activation Code	Registration Key	Seats	Maintenance Expiration
<input type="radio"/>	ProtectLink	LR-USVB-9W9WF-LTUXC-ZC6U4-GQHWX-Y84VE	XXXXXXXX-XXXXXXXXXXXXXXXX	5	2/13/2011
<input type="radio"/>	ProtectLink	LR-QCYR-RTWU4-D9GBT-G9DAW-E3VN7-U2T6C	XXXXXXXX-XXXXXXXXXXXXXXXX	5	3/15/2010

At the bottom of the page, there are two buttons: "Add Seats to Selected License" and "Register New Product Separately".

TrendMicro Registration Server generates a new AC.

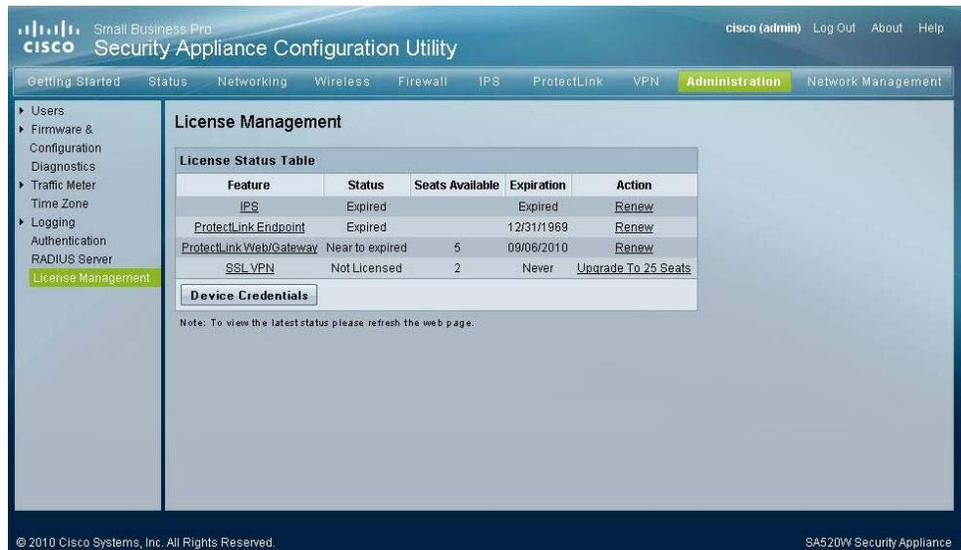
Using the new AC, follow the steps in the following sections to renew the license on your router.

- **“Renewing the License on SA 500 Series Routers” on page 46**
- **“Renewing the License on RV Series Routers” on page 51**

Renewing the License on SA 500 Series Routers

To renew the license on SA 500 Series routers, follow these steps:

- STEP 1** Log in to the SA500 Security Appliance Configuration Utility.
- STEP 2** Click **License Management** to open the License Management window.



Small Business Pro
 cisco Security Appliance Configuration Utility

Getting Started Status Networking Wireless Firewall IPS ProtectLink VPN **Administration** Network Management

Users
 Firmware & Configuration
 Diagnostics
 Traffic Meter
 Time Zone
 Logging
 Authentication
 RADIUS Server
License Management

License Management

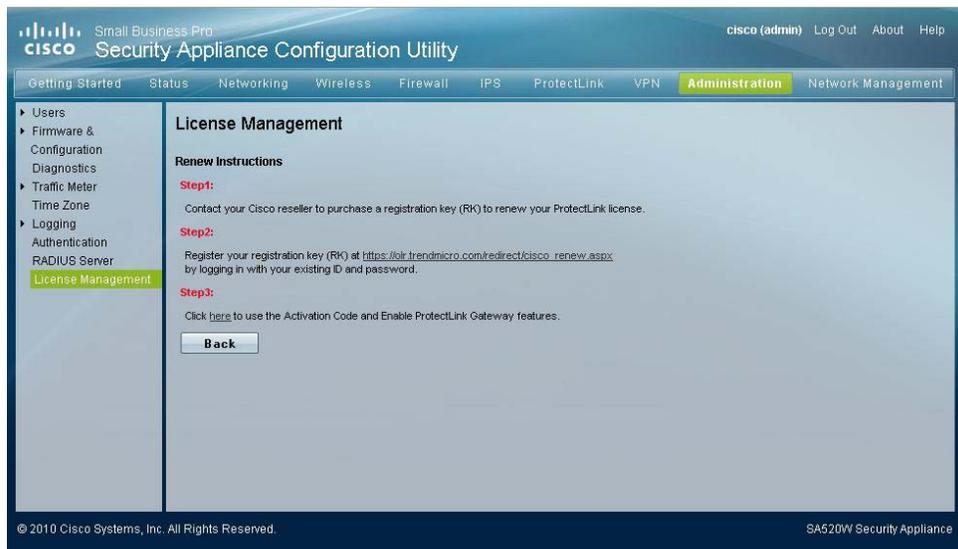
Feature	Status	Seats Available	Expiration	Action
IPS	Expired		Expired	Renew
ProtectLink Endpoint	Expired		12/31/1969	Renew
ProtectLink Web/Gateway	Near to expired	5	09/06/2010	Renew
SSLVPN	Not Licensed	2	Never	Upgrade To 25 Seats

Device Credentials

Note: To view the latest status please refresh the web page.

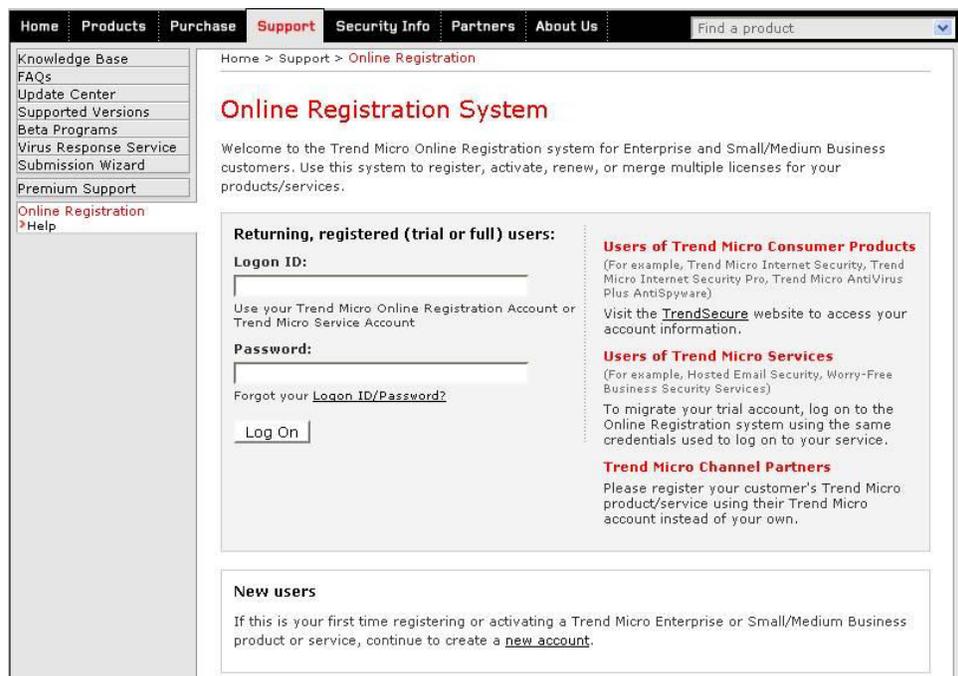
© 2010 Cisco Systems, Inc. All Rights Reserved. SA520W Security Appliance

STEP 3 In the License Management window, click the link in Step 2 to register your registration key.



This link opens the ProtectLink Online Registration window on the TrendMicro website.

STEP 4 In the Online Registration window, log in using your existing ProtectLink account.



After logging in, you should see a window like the following window:

Home > Support > Online Registration > My Products

My Products

Company Name: **Cisco Systems, Inc.** [View/Edit Company Profile](#)

[Register New Product/Renew](#)

Item	Product	Sales Type	Registration Key	Registration Date	Activation Code	Expiration Date
1	ProtectLink	Retail Package	LR-7M4H-S9SH-VHVQ-CJFB	2/13/2010	XX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX	2/13/2011
2	ProtectLink	Retail Package	LR-Q2P5-X9DD-7SKU-HYRQ	2/15/2010	XX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX	3/15/2011
3	ProtectLink	Retail Package	LR-MTE5-V4PQ-QDLC-QVNT	3/2/2010	XX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX	4/2/2010 (Expired!)
4	ProtectLink	Retail Package	LR-3SCV-RXUB-5LY9-EPAZ	3/16/2010	XX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX	3/16/2011
5	ProtectLink	Free	LR-885E-MFPA-RUPY-XQ56	5/11/2010	XX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX	6/11/2010 (Expired!)
6	ProtectLink	Retail Package	LR-EALS-97GN-DV35-T62P	5/26/2010	XX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX	5/26/2011
7	ProtectLink	Retail Package	LR-PJVZ-HKDM-4B3K-DCE5	5/27/2010	XX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX	6/27/2010 (Expired!)
8	ProtectLink	Retail Package	LR-959N-5345-M6DA-VUBT	6/30/2010	XX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX	7/30/2010 (Expired!)

* DD / MM / YYYY

Attention Worry Free Business Security Advanced Customers:

Have you recently upgraded to Worry Free Business Security Advanced but have not yet received instructions on how to activate the Trend Micro Hosted Email Security service that you are now entitled to?

If the answer is 'Yes', do not worry. Please go to <http://olr.trendmicro.com/redirect/cm5upgrade> to register your service and receive account login details. Don't forget to write down your Client Server Messaging Suite Activation Code listed in the products list above - you'll need it!!

NOTE You must have a separate Trend account for each device.

STEP 5 Click **Register New Product/Add Seat**.

Home > Products > Purchase > Support > Security Info > Partners > About Us

Activate your product

> Step 1: Enter Activation Code

Your Activation Code (for example xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx) is located on the Product Registration Certificate you received. You can contact Trend Micro if you cannot locate your Activation Code. Enter your Activation Code below and click **Next**.

Enter Activation code

- - - - - - -

STEP 6 Enter the new registration key and follow the online instructions.

STEP 7 Click **Next**.

Upon successful completion of the registration process, you receive an activation code onscreen. You also receive an email from TrendMicro with the new activation code. TrendMicro sends the email to the address associated with your ProtectLink account.

STEP 8 After obtaining the new activation code, log out.

STEP 9 Go back to the License Management window of the SA500 Configuration Utility.

STEP 10 In the License Management window, click the link in Step 3 to register your registration key.

This link opens the License Change window on the ProtectLink website.

STEP 11 In the License Change window, log in using the same login information you used in the registration process.

The screenshot shows the 'License Change' page on the Cisco ProtectLink website. The navigation bar includes Home, Products, Purchase, Support (highlighted), Security Info, Partners, and About Us. A search bar on the right says 'Find a product'. The left sidebar contains links for FAQs, Update Center, Supported Versions, Beta Programs, Virus Response Service, Submission Wizard, Premium Support, Online Registration, and Help. The main content area is titled 'License Change' and shows 'Step 2: Verify User ID'. Below the title, it says 'Enter your Logon ID and Password and click Next to continue.' There are two input fields: 'Logon ID:' and 'Password:'. Below the password field is a link for 'Forgot your ID/Password?'. At the bottom of the form are 'Back' and 'Next' buttons. A vertical ID number '236366' is visible on the right side of the screenshot.

Renewing the License on RV Series Routers

To renew the license on RVS4000, WRVS4400N, and RV042/82/16 routers, follow these steps.

STEP 1 Connect to the router you want to upgrade:

NOTE You must be on the LAN as the router to be able to complete this step.

- To connect to an RVS4000 or WRVS4400N router, enter the following URL in the Address field of your browser:

`http://router_address/new_purchase.htm`

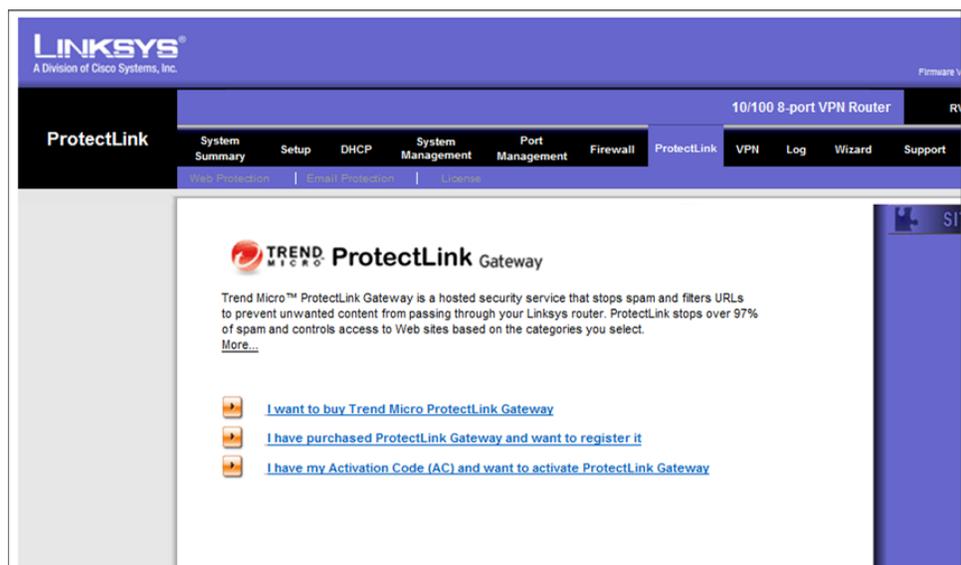
Replace *router_address* with the address of your router (for example, 192.168.1.1).

- To connect to an RV042/82/16 router, enter the following URL in the Address field of your browser:

`http://router_address/Security_Protection_new_purchase.htm`

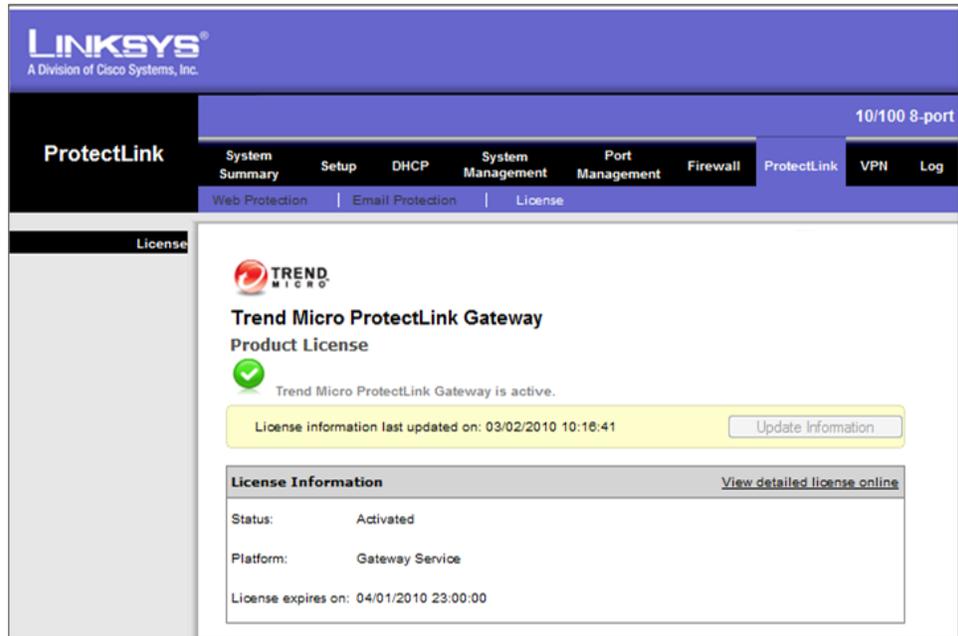
Replace *router_address* with the address of your router (for example, 192.168.1.1).

A window similar to the following appears:



STEP 2 In the ProtectLink Home window, click **I have my Activation Code (AC) and want to activate ProtectLink Gateway** to register the product online.

STEP 8 In the router's Configuration Utility, click the **ProtectLink** tab and verify the status of the license.



199854

Configuring and Managing Email Protection

NOTE This chapter applies to Cisco ProtectLink only.

Use the web portal to configure and manage email protection:

- [Launching the Web Portal for Email Protection, page 55](#)
- [Features of the IMHS Web Portal, page 56](#)
- [Viewing Reports, page 58](#)
- [Working with Policies, page 61](#)
- [Managing the Approved Senders, page 64](#)
- [Managing the Quarantined Messages, page 66](#)
- [Working with the Mail Tracking Logs, page 70](#)
- [Administration Tasks in the IMHS Console, page 72](#)

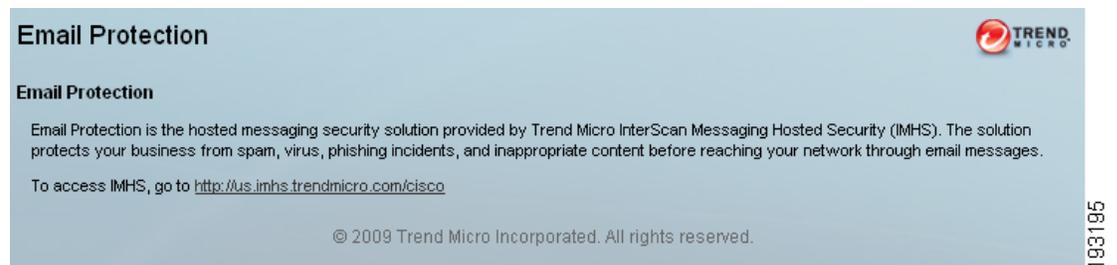
Launching the Web Portal for Email Protection

From the Configuration Utility for your router or security appliance, you can launch the web portal for Trend Micro IMHS.

- STEP 1** Launch the Configuration Utility for your router or security appliance, and then log in.
- STEP 2** Click **ProtectLink** in the menu bar, and then click **Email Protection** in the navigation tree.

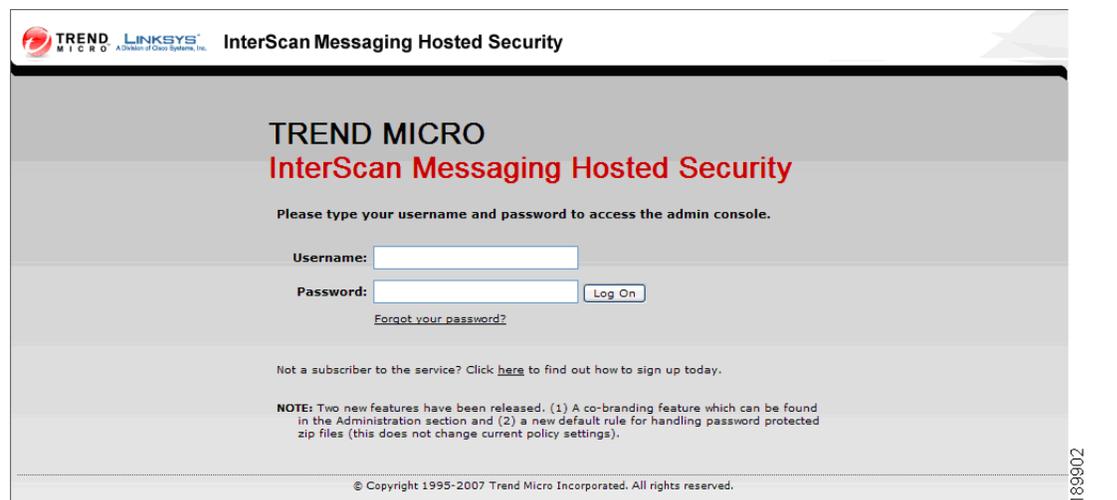
NOTE If your Configuration Utility does not include a left navigation bar, click **ProtectLink**, then choose **Email Protection**.

The Email Protection page appears.



- STEP 3** Click the link on the page to launch the web portal for Trend Micro IMHS: <https://us.imhs.trendmicro.com/cisco>.

The Trend Micro IMHS login page appears.



STEP 4 Enter the Username and Password that you received when you activated the Cisco ProtectLink Gateway, and then click **Log On**.

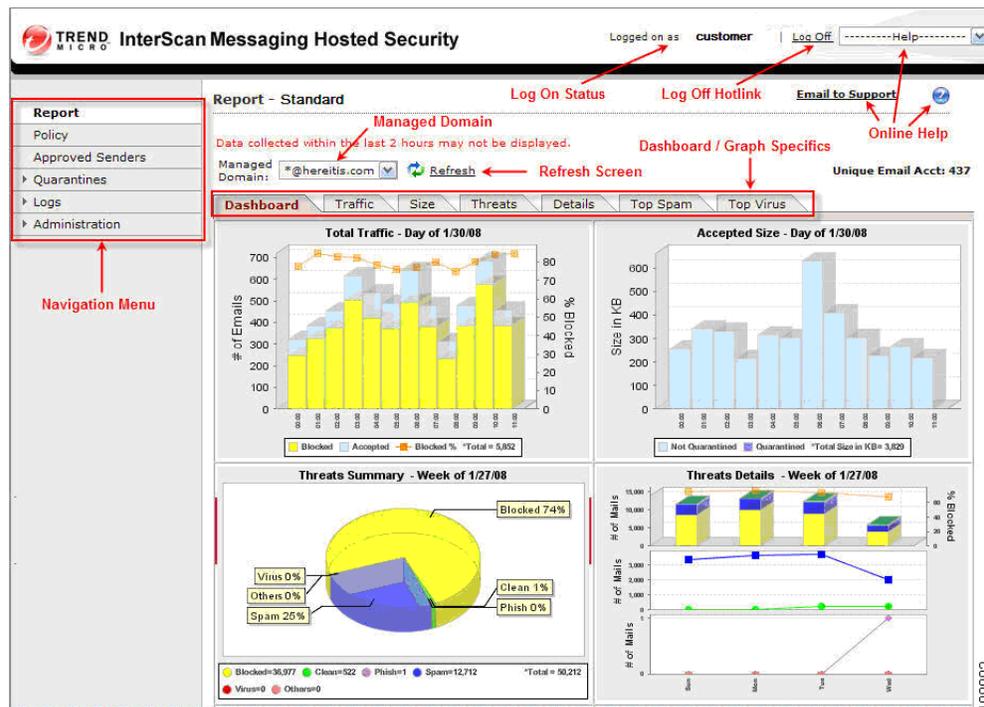
The IMHS web portal appears, with the **Report > Dashboard** displayed.

NOTE After you have logged onto IMHS for the first time, Cisco recommends changing your password to help ensure the security of your IMHS account. See the **“Changing a User Password”** section on page 74 for details.

Features of the IMHS Web Portal

The IMHS web portal allows you to create reports, view logs, perform administrative tasks, and review policies. The console is illustrated in **Figure 1**.

Figure 1 IMHS Web Portal



In the page displayed above, the user interface includes the following tools:

- **Navigation Menu:** Click menu items in the Navigation Menu to access working pages within the IMHS web portal. When clicked, menu items with right arrows open to reveal additional submenu items.
- **Dashboard / Tab Graph Specifics:** Click a graph in the Dashboard or its respective Tab, which displays details about the specific IMHS action.
- **Managed Domain:** The domain shown in the Dashboard is the current domain. Select other domains in the Managed Domain popup menu.
- **Online Help:** Help is available in three ways: through the Online Help popup menu, through the context-sensitive ? button, and through the **Email to support email** link. Using the Online Help popup menu you can download the IMHS manuals and access other help tools.
- **Log On Status:** Displays the name of the log on account.
- **Log Off Link:** Click the **Log Off** link to log out of the IMHS web portal.
- **Refresh page:** Click the **Refresh** link to refresh the page.

NOTE A full treatment of all the Email Protection features in IMHS is beyond the scope of this guide. For more details, refer to the *Trend Micro InterScan Gateway Hosted Security 1 Getting Started Guide* and the *Trend Micro InterScan Gateway Hosted Security 1 End User Guide* located at the following URL:
<http://www.trendmicro.com/download/>.

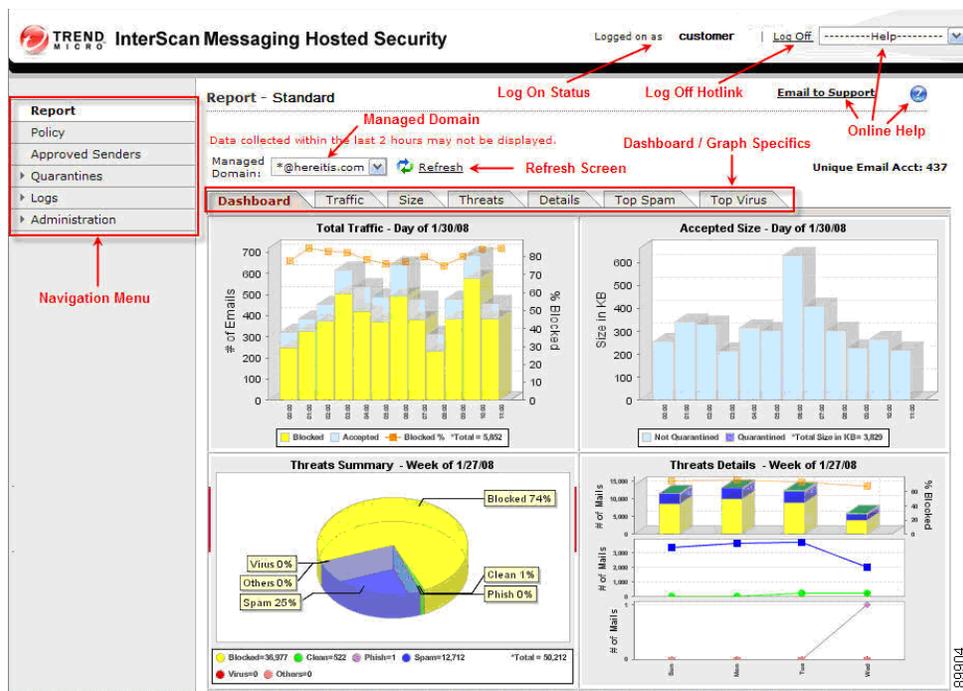
Viewing Reports

Many reports are available to help you analyze the results of your Email Protection.

STEP 1 Launch the web portal for IMHS, and log in.

NOTE For more information, see [Launching the Web Portal for Email Protection, page 55](#).

The **Report > Dashboard** page appears by default. You also can find this page by clicking **Reports** in the navigation menu.



STEP 2 For specifics concerning particular IMHS actions, click the appropriate tab or graphic in the Dashboard page. For example, click the **Traffic** or the **Total Traffic** graphic to view the details page.

The details page appears. Refer to the following example of the Total Traffic page.

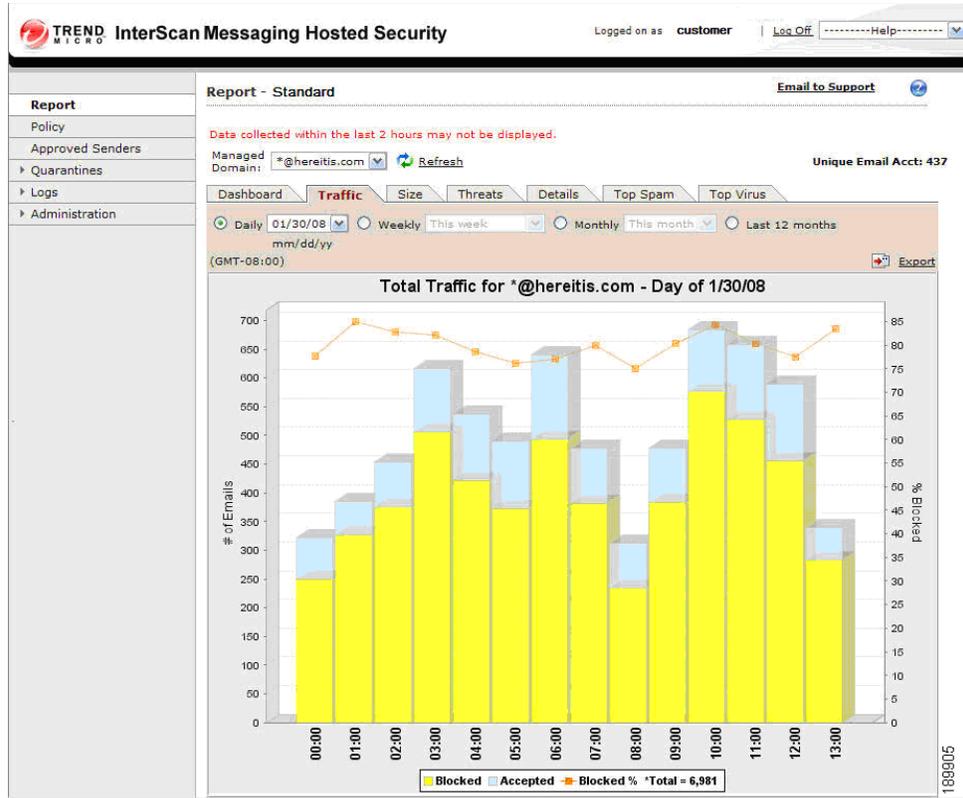


Table 1 describes the Dashboard / Tab page graphics.

Table 1 Dashboard / Tab page Graphics

Graphic Name	Tab Name	Description
Total Traffic	Traffic	Shows the total blocked and accepted email traffic for the selected domain
Accepted Size	Size	Shows the total size (in KB) of accepted email traffic for the selected domain
Threats Summary	Threats	Shows what percentage of specific types of messages make up the email traffic for the selected mail domain
Threats Details	Details	Shows detailed email traffic distribution for the selected mail domain
Top Spam Recipients	Top Spam	Shows the top spam message recipients for the selected mail domain
Top Virus Recipients	Top Virus	Shows the top virus message recipients for the selected mail domain

Working with Policies

An IMHS policy is defined as a set of rules for a specific mail domain. Multiple rules can exist for each domain (policy), but only a single policy can exist for any one domain. Use the Policy menu to view the predefined policies governing your Email Protection.

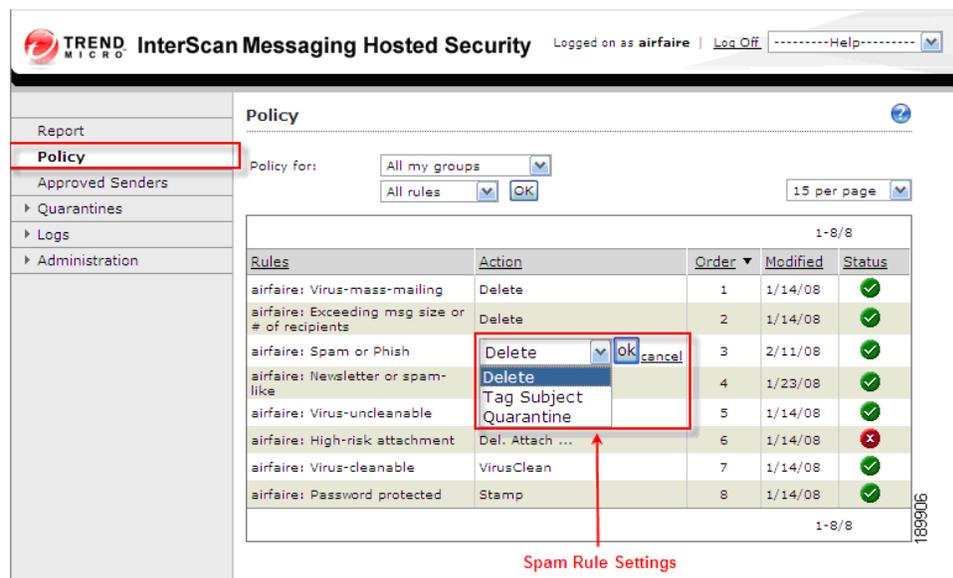
STEP 1 Launch the web portal for IMHS, and log in.

NOTE For more information, see [Launching the Web Portal for Email Protection, page 55](#).

STEP 2 Click **Policies** in the navigation menu.

The Policy page appears, displaying a list of the predefined Rules and the status of each.

Figure 2 IMHS Policy / Spam Rule Settings



NOTE The administrators can see the rules that apply to their organization. ProtectLink customers have read-only access and may view the default policy and modify the “Spam or Phish” and “Newsletter or spam-like” rules. The administrator may change the action taken on messages identified from the default action of Delete, Tag Subject, or Quarantine, as shown in the Spam Rule Settings popup menu above.

STEP 3 Use the following features, as needed:

- Use the column headings to change the sort order. The rules are displayed in a table, sorted by the order in which the rules are applied during scanning by IMHS. The contents of each table can be resorted by clicking a column heading. If you want to change the order of the information in the table, click any column heading. The information will be sorted in ascending order.
- Refer to the icons in the Status column to see the status of a rule.

Icon	Status
	Rule Enabled
	Rule Disabled

The ProtectLink (IMHS Standard) default policy settings are shown in [Table 2](#).

Table 2 Standard Service Default Policy Settings

Rule	Description
Rule 1	This rule is designed to protect the user from viruses that are often spread by mass mailing type campaigns. If a message is identified as containing a virus that cannot be cleaned and the message shows mass-mailing behavior, then the entire email message, along with the virus, is deleted.
Rule 2: Exceeding message size or allowed number of recipients.	This rule is designed to protect the system from Denial of Service (DOS) and Zip of Death attacks. If the size of the incoming message exceeds the default limit of 10MB or it has been sent to more than 50 recipients in the organization, then the message is deleted.

Table 2 Standard Service Default Policy Settings (Continued)

Rule (Continued)	Description (Continued)
<p>Rule 3: Spam or Phish</p>	<p>This rule is designed to catch spam or phishing email messages. The default action is to delete all messages identified as spam or phishing email messages. All IMHS customers have the ability to change the default action. It is highly recommend that only the Delete or Quarantine actions are used for this rule. All quarantined messages are saved for seven days in the IMHS web-accessible quarantine</p>
<p>Rule 4: Virus-uncleanable</p>	<p>This rule is designed to protect the user from viruses. If a message is identified as containing a virus that cannot by cleaned, then the virus attachment is deleted from the email message before it is delivered.</p>
<p>Rule 5: High-risk attachment</p>	<p>Disabled for Standard customers.</p>
<p>Rule 6: Virus-cleanable</p>	<p>This rule is designed to protect the user from viruses. If a message is identified as containing a virus that can by cleaned, then the virus is removed from the email message before it is delivered. If the virus cleaning process is unsuccessful, then the virus attachment is deleted.</p>
<p>Rule 7: Newsletter or spam-like</p>	<p>This rule is designed to catch “gray-mail” such as newsletters. The default action for these spam-like email messages is to Tag Subject (with “Spam>”). It is highly recommend that only the Tag Subject or Quarantine actions are used for this rule. All quarantined messages are saved for seven days in the IMHS web accessible quarantine.</p>

Table 2 Standard Service Default Policy Settings (Continued)

Rule (Continued)	Description (Continued)
Rule 8: Password-protected zipped file attachments	This rule is designed to allow advanced users to configure the action taken to handle email messages with password-protected zip file attachments. By default, messages with password-protected zip file attachment are passed through to the recipient and a notification is placed in the body of the mail stating that the attached file was not scanned.

Managing the Approved Senders

For each domain that you manage, you can specify the email addresses or domains that you approve as senders. The emails that are received from these approved senders will not be subject to all of the checks that are normally performed on incoming emails.

- ERS will not block any email messages from the senders (or domains) specified.
- Content-based heuristic spam rules will not apply to email messages received from the specified senders or domains.
- All virus, content-based, and attachment rules will apply.

To manage approved senders, follow these steps:

STEP 1 Launch the web portal for IMHS, and log in.

NOTE For more information, see [Launching the Web Portal for Email Protection, page 55](#).

STEP 2 Click **Approved Senders** in the navigation menu.

The Approved Senders page appears.



STEP 3 To display the approved senders for a different managed domain, complete the following tasks:

- a. From the Managed Domain list, choose a particular domain that you manage, or choose **All Domains** to see the Approved Senders for all domains.
- b. Click **Refresh** to display the approved senders for the selected domain.

STEP 4 To add a sender, complete the following tasks:

- a. From the Managed Domain list, choose whether to approve this sender for **All Domains** or for a particular domain.
- b. Click in the **Add** box, and then enter an email address (in the format *user@domain.com*) or enter a domain (such as *domain.com*).
- c. Click **Approve Sender** to add the sender to the list.

STEP 5 To edit an entry, complete the following tasks:

- a. Click the entry.
- b. Edit the text.
- c. Click **OK**.

STEP 6 To delete an entry, complete the following tasks:

- a. Click the check box for the entry.
- b. Click **Delete**.

Managing the Quarantined Messages

You can enter criteria to find quarantine messages for a particular recipient, domain, or sender. You can then choose whether to delete the messages or release them from the quarantine.

STEP 1 Launch the web portal for IMHS, and log in.

NOTE For more information, see [Launching the Web Portal for Email Protection, page 55](#).

STEP 2 Click **Quarantines** in the navigation menu, and then click **Query**.



STEP 3 Enter the search criteria.

- **Recipient (required):** Enter the recipient's email user name. For example, if the full email address is *user@domain.com*, you would enter *user*.
- **Domain (unlabeled):** Choose the domain from the drop-down list.
- **Sender (optional):** Enter the full email address or the domain of the sender.
- **Display:** Choose the number of messages to display per page. For faster display, choose a lower number of messages on each page. Buttons allow you to move through the pages.

STEP 4 Click **Search**.

The results appear in a table. The information includes that date, sender, and subject line. You can change the sort order by clicking a column heading. The results will be sorted in ascending order based on the selected heading.

STEP 5 To delete messages, complete the following tasks:

- a. For each message that you want to delete, check the box in the first column of the row.
—OR— Select all messages on the page by checking the box in the first column of the header row.
- b. Click the **Delete** button above the table. All selected messages will be deleted.
- c. Repeat for the other pages of the display, as needed.

STEP 6 To release an item from the quarantine, complete the following tasks:

- a. For each message that you want to release, check the box in the first column of the row.
—OR— Select all messages on the page by checking the box in the first column of the header row.
- b. Click the **Deliver (Not Spam)** button above the table.

NOTE When a message is released from the quarantine, IMHS processes the request but does not apply the anti-spam criteria. The message is then sent. However, be aware that a message may be blocked by the receiving email server, based on the messaging security policies that are in effect. IMHS does not control these policies. In this case, the email will not arrive in the recipient's email Inbox.

- c. Repeat for the other pages of the display, as needed.

Configuring the Summary Digest Mail for the Quarantine

Configure IMHS to send a summary digest email message to each recipient who has quarantined messages. You can choose the frequency, day of the week, and time to send this message. You also can control the content of the message. The digest mail can list up to 100 quarantined messages and provides a link for the recipient to access messages of interest.

A digest email is sent only if this feature is enabled.

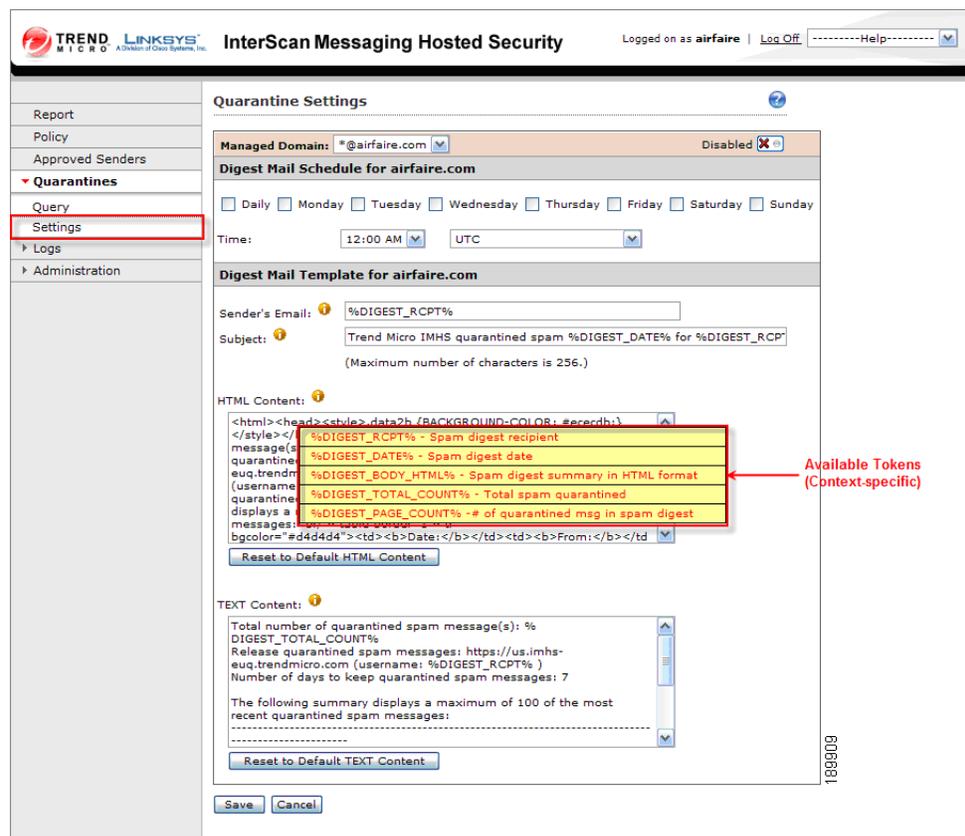
To configure the summary digest mail:

STEP 1 Launch the web portal for IMHS, and log in.

NOTE For more information, see [Launching the Web Portal for Email Protection, page 55](#).

STEP 2 Click **Quarantines** in the navigation menu, and then click **Settings**.

The Quarantine Settings window appears.



NOTE As illustrated in yellow, you can right-click any field in the Digest Mail Template area to view the available tokens. Tokens are codes that you can use to insert information such as the recipient's own email address, the date of the digest email, and other details. More information is provided in the step-by-step procedure below.

STEP 3 To enable this feature, click the **Disabled** icon in the upper right corner of the page. Now the button label is **Enabled**. You can disable the feature by clicking the button again. (This feature is disabled by default.)

STEP 4 From the **Managed Domain** drop-down list, choose the domain for which the digest email message will be created.

NOTE The domain used in the sender's email address must be the same as the domain to which the email will be delivered.

STEP 5 Select the frequency for sending the digest email message by checking the **Daily** check box or the individual boxes for the days of the week.

NOTE Quarantined email messages are retained for seven days.

STEP 6 Select a **Time** and **Time Zone** when the digest email message should be sent.

STEP 7 Enter the following information to configure the email message that will be sent:

NOTE To enter a token into a field, first click to place the cursor at the insertion point. Then right-click in that position to view the list of codes that can be used. Click a code on the list to insert it.

- **Sender's Email:** Enter the email address to display in the header as the sender of the email.

NOTE The default entry is the code `%DIGEST_RCPT%`, which automatically inserts the recipient's own email address in the From line of the message.

- **Subject:** Enter the text that appears in the digest email message subject line.

NOTE The default entry includes *Trend Micro IMHS quarantined spam*, with the code `%DIGEST_DATE%` to insert the date of the email and the code `%DIGEST_RCPT%` to automatically insert the recipient's own email address in the From line of the message.

- **HTML Content:** Enter the body of the HTML message, for users that can receive HTML email messages.

NOTE The default content includes HTML formatting tags that you can modify if you know HTML. The content of this message is the same as the default content in the TEXT Content box. The message includes the total number of quarantined messages, using the code `%DIGEST_TOTAL_COUNT%`. There is also a link that the user can click to connect to the IMHS Web EUQ login page. After logging in with the assigned username and password, the user can review the messages and specify any messages to release from the quarantine.

- **TEXT Content:** Enter a plain text version of the message, without HTML formatting tags, for users that cannot receive HTML email messages.

STEP 8 Click **Save** to save your changes.

Working with the Mail Tracking Logs

Use the Logs > Mail Tracking section to search for and view mail tracking logs based on a specific date or date range, sender, and/or recipient. Mail tracking information is only available for the previous five days.

The Mail Tracking feature allows you to locate any message within the system using sender and recipient information. It shows the status and the action taken on the message such as the following:

- Blocked or delayed at the system edge by reputation service
- Accepted for processing and deleted with a virus
- Accepted, processed, and delivered
- Unresolved

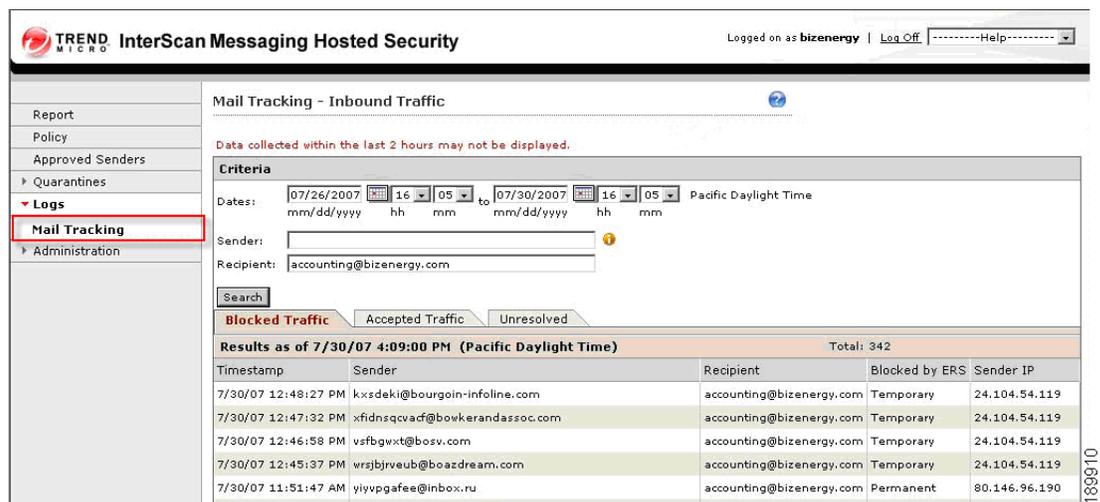
To view mail tracking logs:

STEP 1 Launch the web portal for IMHS, and log in.

NOTE For more information, see [Launching the Web Portal for Email Protection, page 55](#).

STEP 2 Click **Mail Tracking** in the navigation menu.

The Mail Tracking - Inbound Traffic page appears.



STEP 3 Enter the criteria for the logs that you want to view:

- **Dates:** Work from left to right to choose the start range and end range. Click the calendar button to choose a date. For time, use the **hh** drop-down list to choose the hour (from 0 to 23) and use the **mm** list drop-down list to choose the minutes (from 0 to 59). The displayed time zone is based on the settings for the computer that you are using.
- **Recipient:** Enter the recipient's email user name. For example, if the full email address is *user@domain.com*, you would enter *user*.
- **Sender (optional):** Enter the full email address or the domain of the sender.

STEP 4 Click **Search**.

The results appear.

STEP 5 Click a tab to choose the type of messages to view: **Blocked Traffic**, **Accepted Traffic**, or **Unresolved**.

Administration Tasks in the IMHS Console

This section includes the following tasks:

- [Managing Passwords, page 72](#)
- [Importing User Directories, page 75](#)
- [Co-Branding to Display a Company Logo in the Web Portal, page 77](#)

Managing Passwords

Administrators can change Admin Password and End User Passwords.

All IMHS passwords require between eight and 32 characters. Cisco strongly recommends the use of passwords that meet the following criteria:

- Include multiple character types (a mix of letters, numbers, and other characters).
- Do not use recognizable formats (for instance, your birthday, license number, or employee ID number).

Refer to the following topics:

- [Managing the Administrator Password, page 73](#)
- [Changing a User Password, page 74](#)

Managing the Administrator Password

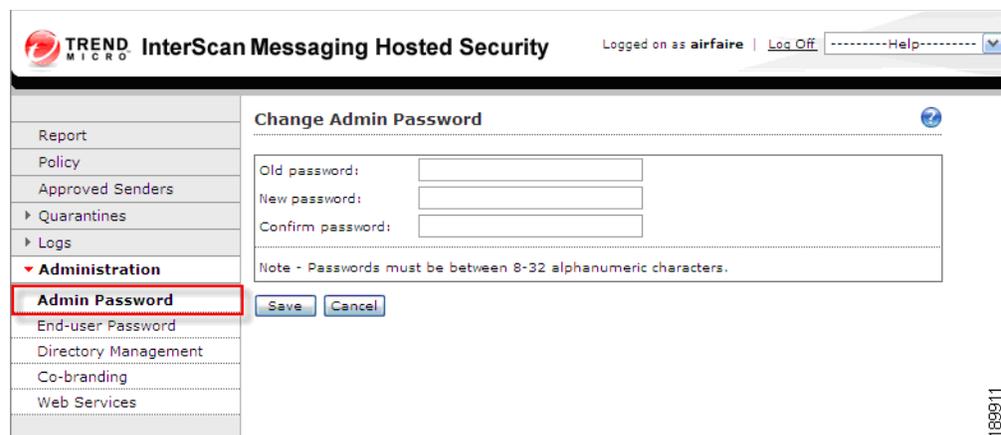
To change the Admin Password, follow these steps:

STEP 1 Launch the web portal for IMHS, and log in.

NOTE For more information, see [Launching the Web Portal for Email Protection, page 55](#).

STEP 2 Click **Administration** in the navigation menu, and then click **Admin Password**.

The Change Admin Password page appears.



STEP 3 Enter the following information:

- **Old password:** Enter your current password.
- **New password:** Enter a new password that includes between eight and 32 characters.
- **Confirm password:** Enter the new password again.

STEP 4 Click **Save**.

Changing a User Password

To reset an end-user password, follow these steps:

STEP 1 Launch the web portal for IMHS, and log in.

NOTE For more information, see [Launching the Web Portal for Email Protection, page 55](#).

STEP 2 Click **Administration** in the navigation menu, and then click **End-user Password**.

The Change End User Password page appears.

The screenshot shows the 'Change End User Password' page in the InterScan Messaging Hosted Security console. The page title is 'Change End User Password'. The navigation menu on the left includes 'Report', 'Policy', 'Approved Senders', 'Quarantines', 'Logs', 'Administration', 'Admin Password', 'End-user Password' (highlighted with a red box), 'Directory Management', 'Co-branding', and 'Web Services'. The main content area contains a form with the following fields: 'Registered end-user email address' (text input), 'Domain name' (dropdown menu showing 'airfaire.com'), 'New password' (text input), and 'Confirm password' (text input). A note below the form states: 'Note - Passwords must be between 8-32 alphanumeric characters.' There are 'Save' and 'Cancel' buttons at the bottom of the form. The top of the page shows the logo for TREND MICRO and the text 'InterScan Messaging Hosted Security'. The user is logged in as 'airfaire' and there are 'Log Off' and 'Help' links.

STEP 3 Enter the following information:

- **Registered end-user's email address:** Enter the first part of the email address. For example, if the address is *user@domain.com*, enter *user*.
- **New password:** Enter a new password that includes between eight and 32 characters.
- **Confirm password:** Enter the new password again.

NOTE The end-user will need to know the new password to log in. The system sends the end-user an email with an activation URL.

Importing User Directories

Importing user directories into IMHS can help prevent spam attacks that send emails to invalid addresses on your domain. For example, in a Directory Harvest Attack (DHA), a spammer sends emails to all possible user names on a domain. When the server returns “bounce” messages for the invalid addresses, the spammers can deduce which email addresses were valid, and can use this list of addresses for future attacks.

Importing user directories lets IMHS know legitimate email addresses and domains in your organization. IMHS will not forward messages for invalid addresses.

You can import directory files that are in the following formats:

- LDAP Data Interchange Format (LDIF: .ldf)
- Comma-separated Values (CSV: .csv) files.

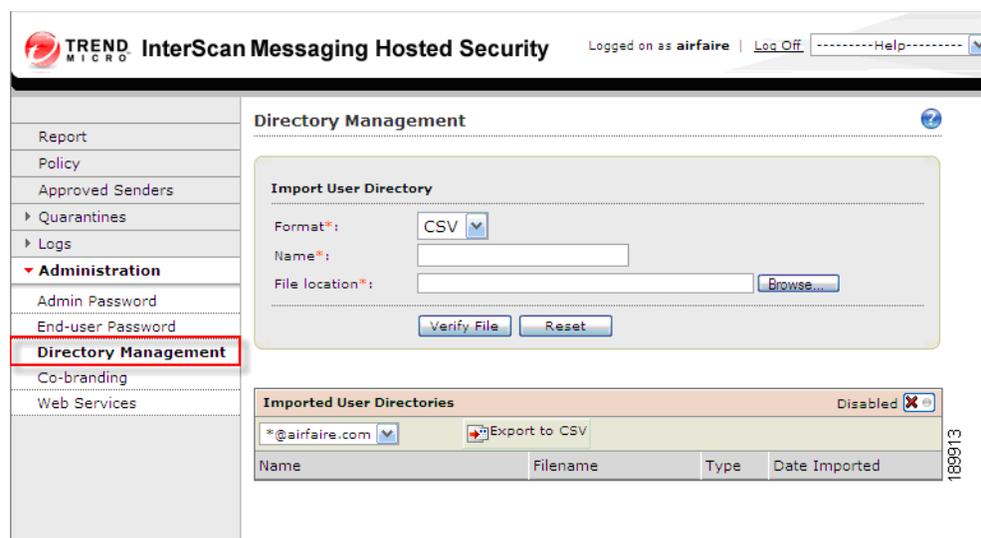
To import a user directory file, follow these steps:

STEP 1 Launch the web portal for IMHS, and log in.

NOTE For more information, see [Launching the Web Portal for Email Protection, page 55](#).

STEP 2 Click **Administration** in the navigation menu, and then click **Directory Management**.

The Directory Management page appears.



This page has two sections:

- **Import User Directory:** Selections for importing a new user directory file.
- **Imported User Directories:** The current user directory file(s) that IMHS is using. IMHS replaces one mail domain users at a time. Users may be a combination of multiple user directories.

STEP 3 In the **Import User Directory** section, enter the following information about the directory that you want to import:

- **Format:** Select the format type: **LDIF** or **CSV**.
- **Name:** Enter a descriptive name for the file.
- **File location:** Click **Browse** and select the file on your computer.

STEP 4 Click **Verify File**.

After the progress bar completes, a summary page appears, showing the following information:

- **Summary:** A summary of the information that you provided.
- **Domains and Number of Current Users to Replace Current Users:** The domains that you specified when you subscribed to the IMHS service.
- **Invalid domains:** Domains that are included in your directory file, but are not officially used on your IMHS service. IMHS cannot provide service for these domains and their corresponding email addresses.

STEP 5 Click **Import**.

NOTE There are best practices for exporting and importing directories in IMHS, as well as for administration and user directory verification. For details on these practices, see the [Trend Micro InterScan Messaging Hosted Security 1 Getting Started Guide](#), pages 3-23 to 3-26.)

Co-Branding to Display a Company Logo in the Web Portal

IMHS allows the user to display a company logo in various places within the web portal. When this feature is enabled, the selected logo appears in the following places:

- The banner bar of the IMHS login page
- The left navigation pane of the IMHS GUI after you log in
- The banner bar of the IMHS Web EUQ login page
- The left navigation pane of the IMHS Web EUQ GUI after you log in

NOTE Resellers can set different logos for different domains, or allow system administrators of the domain to set the logo for that domain, separately from the reseller logo. The logo selected for a domain also displays in the banner bar and navigation pane of the IMHS Web EUQ associated with that domain.

Users at the reseller level may set different domains with the same logo, different logos, or allow the domain administrators to set the logo to be displayed for their domain. Resellers can also leave the feature disabled.

Verify that your logo image meets the following requirements:

- Image height: 45 pixels
- Image width: 45-150 pixels
- Image file format: .gif, .jpg, or .png

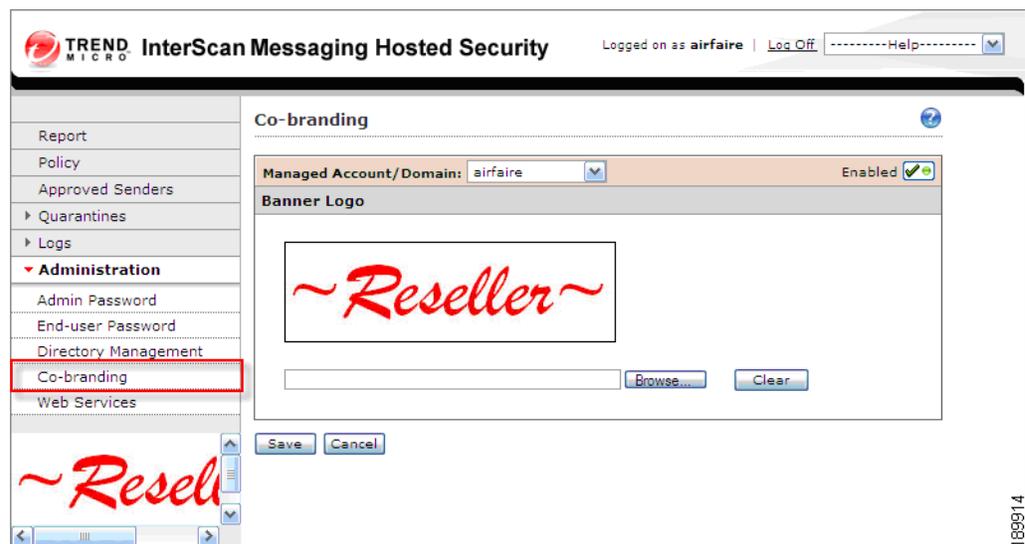
To display your logo, follow these steps:

STEP 1 Launch the web portal for IMHS, and log in.

NOTE For more information, see [Launching the Web Portal for Email Protection, page 55](#).

STEP 2 Click **Administration** in the navigation menu, and then click **Co-branding**.

The Co-branding page appears.



STEP 3 To enable this feature, click the **Disabled** icon in the right corner of the page. The icon label is now Enabled. Later if you need to disable this feature, click the **Enabled** icon. This feature is disabled by default.

STEP 4 From the **Managed Account/Domain** drop-down list, select the account or domain that will display the logo.

STEP 5 Click **Browse**, and select the logo file on your computer.

STEP 6 Click **Save**.

Where to Go From Here

Cisco provides a wide range of resources to help you and your customer obtain the full benefits of Cisco ProtectLink Web/Gateway.

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Online Technical Support and Documentation (Login Required)	www.cisco.com/support
Phone Support Contacts	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Software Downloads (Login Required)	Go to tools.cisco.com/support/downloads , and enter the model number in the Software Search box.
Product Documentation	
Technical Documentation	www.cisco.com/en/US/products/ps9952/tsd_products_support_series_home.html
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb
Marketplace	www.cisco.com/go/marketplace