ADMINISTRATION GUIDE

Cisco Small Business

Cisco ProtectLink™ Endpoint 1.0

OL-21461-01

Contents

1

An Introduction to Cisco ProtectLink Endpoint

This chapter contains the following topics:

Cisco ProtectLink Overview

You can use two Cisco ProtectLink services to provide an integrated, multi-layer security solution for protecting your business and your users:

- ProtectLink Endpoint
- ProtectLink Gateway

ProtectLink Endpoint

Cisco ProtectLink Endpoint is a hosted security service powered by Trend Micro Worry-Free™ Business Security Hosted. This service, working along with your Cisco security appliance, protects Microsoft™ Windows™ PCs and servers against spyware, viruses and other malware. ProtectLink Endpoint allows for security appliance-based network access policy enforcement.

As a hosted service, Cisco ProtectLink Endpoint provides significant benefits over an on-site solution:

- Allows access to the console from anywhere.
- Decreases on-site hardware and software maintenance.
- Optimizes protection with updates and tuning by Cisco.
- Reduces infrastructure costs, while easing deployment and administration.

ProtectLink Gateway

Cisco ProtectLink Gateway offers comprehensive spam and web protection from your Cisco security appliance. This service integrates anti-spam with antivirus and anti-spyware, and Web Threat Protection with URL Filtering. As a result, you can protect your network from email threats in the Internet "cloud" and web threats in the Cisco security appliance, providing access only to email and websites that are appropriate for your business.

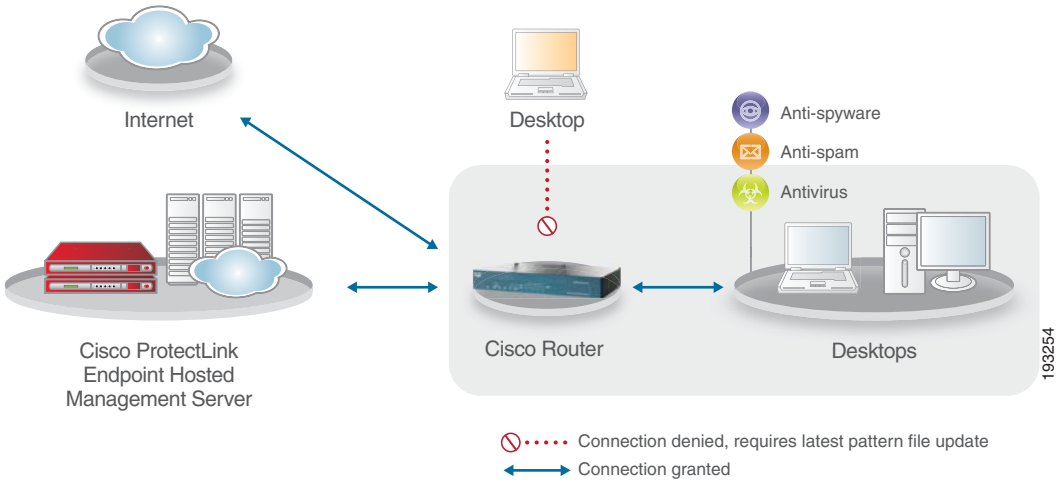
As a hosted service, ProtectLink Gateway provides significant benefits over an on-site solution:

- Keeps email and web threats completely off the network.
- Preserves Internet connection bandwidth and reduces storage.
- Decreases on-site hardware and software maintenance.
- Optimizes protection with updates and tuning by Cisco.
- Reduces infrastructure costs, while easing deployment and administration.

How Cisco ProtectLink Endpoint Works

Figure 1 shows the flow of web and email traffic as it moves from the Internet through the Cisco ProtectLink Endpoint Service and the Cisco Small Business security appliance. Cisco ProtectLink Endpoint Service protects desktops using Trend Micro WFBS-H.

Figure 1 How ProtectLink Endpoint Works



Desktop Protection

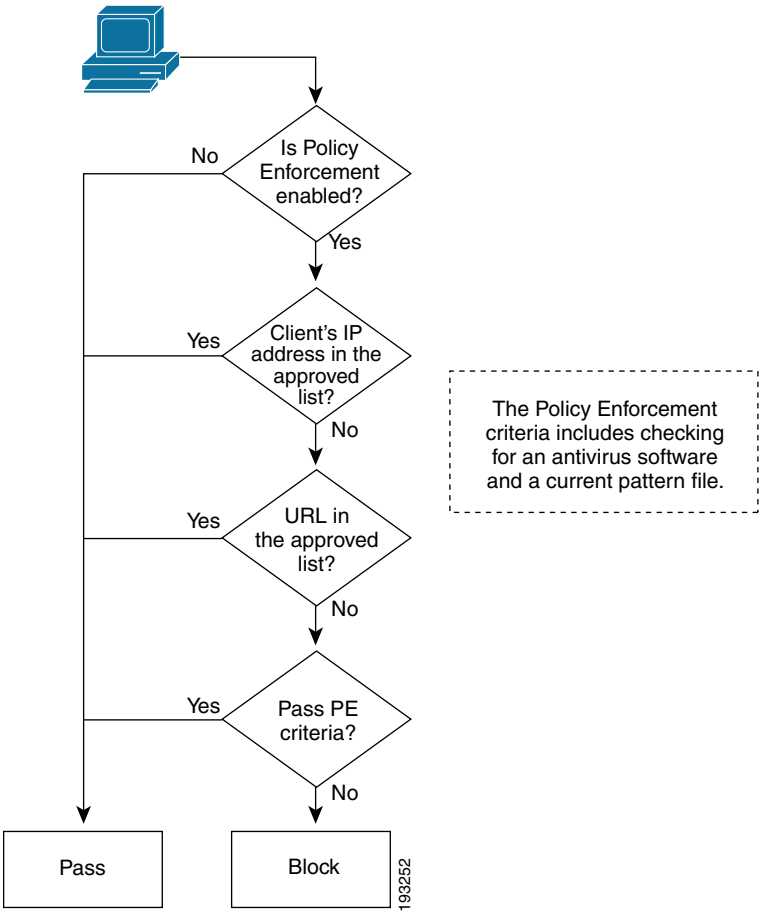
Cisco ProtectLink Endpoint integrates with Trend Micro WFBS-H to provide desktop protection.

TIP For information or documents about Worry-Free Business Security Hosted, visit http://us.trendmicro.com/us/products/sb/worry-free-business-security-hosted.

Administrators can automatically prevent threats on networks using WFBS-H, a hosted solution. They can also create reports, view summarized and complete threat status, security risk status, and system updates.

After installing the WFBS-H Agent on a computer, next install the Threat Management Agent (TMAgent). The TMAgent ensures that each computer has an antivirus solution. If a computer does not have the TMAgent installed, the security appliance blocks access to the web. This feature provides protection by preventing attacks on vulnerable computers that would expose your network to threats. **Figure 2** illustrates the workflow.

Figure 2 Endpoint Protection Workflow



Benefits of Using ProtectLink Endpoint

Hosted services provide significant benefits over an on-site solution:

- Keeps email and web threats completely off the network.
- Preserves Internet connection bandwidth.
- Decreases on-site hardware and software.
- Optimizes protection with updates and tuning by Cisco.
- Reduces infrastructure costs, while easing deployment and administration.

NOTE For information regarding ProtectLink Gateway, please see the *ProtectLink Gateway Administration Guide*.

2

Deploying Cisco ProtectLink Endpoint

You can deploy the Cisco ProtectLink Endpoint through a straightforward process described in the following sections:

- **System Requirements, page 9**
- **Setting Up the Router and Upgrading the Firmware, page 11**
- **Registering ProtectLink Endpoint, page 12**
- **Activating ProtectLink Endpoint, page 19**

NOTE Before following these instructions, you must first complete the initial configuration tasks for your security appliance. For more information, refer to the documentation for your security appliance.

System Requirements

You can use this service on computers that meet the following system and web browser requirements:

- Operating System:

  Windows 2000 32-bit Edition

  - Microsoft Windows 2000 Professional Edition with Service Pack 4 or later
  - Microsoft Windows 2000 Server Edition with Service Pack 4 or later
  - Microsoft Windows 2000 Advanced Edition with Service Pack 4 or later

  Windows XP 32-bit or 64-bit Edition

  - Microsoft Windows XP Professional with Service Pack 2
  - Microsoft Windows XP Home Edition with Service Pack 2

- Microsoft Windows XP Tablet PC Edition with Service Pack 2

Windows Server 2003 32-bit or 64-bit Edition

- Microsoft Windows Server 2003 Standard Edition (with Service Pack 1)
- Microsoft Windows Server 2003 Enterprise Edition (with Service Pack 1)
- Microsoft Windows Server 2003 R2 Standard Edition (with Service Pack 1)
- Microsoft Windows Server 2003 R2 Enterprise Edition (with Service Pack 1)

Windows Small Business Server 2003 R2 32-bit or 64-bit Edition

- Microsoft Windows Small Business Server 2003 R2 Standard Edition
- Microsoft Windows Small Business Server 2003 R2 Premium Edition

Windows Vista 32-bit or 64-bit Edition

- Microsoft Windows Vista Home Basic Edition
- Microsoft Windows Vista Home Premium Edition
- Microsoft Windows Vista Business Edition
- Microsoft Windows Vista Enterprise Edition
- Microsoft Windows Vista Ultimate Edition

Windows Server 2008 32-bit or 64-bit Edition

- Microsoft Windows Server 2008 Standard Edition
- Microsoft Windows Server 2008 Datacenter Edition
- Microsoft Windows Server 2008 Enterprise Edition

Windows Small Business Server 2008 32-bit or 64-bit Edition

- Microsoft Windows Small Business Server 2008 Standard Edition
- Microsoft Windows Small Business Server 2008 Premium Edition

Windows Essential Business Server 2008 32-bit or 64-bit Edition

- Microsoft Windows Essential Business Server 2008 Standard Edition
- Microsoft Windows Essential Business Server 2008 Premium Edition

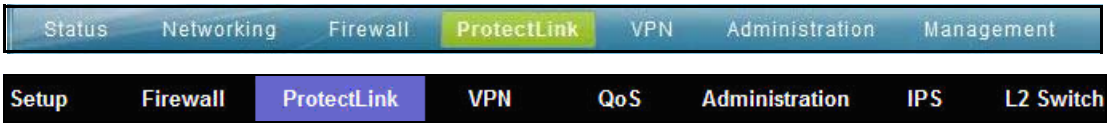
Windows Home Server 32-bit Edition

- Microsoft Windows Home Server

- Processor: Intel™ Pentium™ or AMD™
- RAM: 256 MB or more (operating system dependent)
- Disk space: 350 MB
- Web Browser: Microsoft Internet Explorer 6.0 or 7.0
- Monitor that supports 800 x 600 resolution with 256 colors
- Internet connection
- Adobe™ Acrobat™ Reader 7.0 or 8.0 to view reports

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.

Registering ProtectLink Endpoint

Register your service to activate it and sign up for access to the web portal for online administration. To register a service, follow these steps:

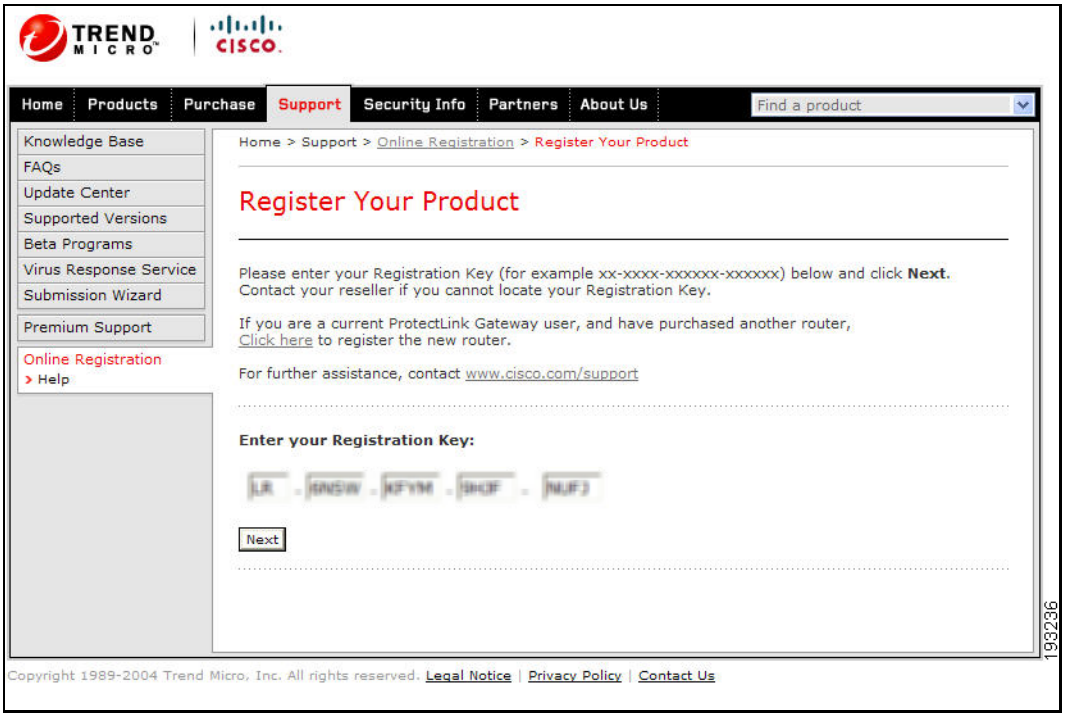
STEP 1 Launch the Configuration Utility for your security appliance, and then log in.

STEP 2 Click **ProtectLink** in the menu bar, and then click **ProtectLink** in the navigation tree.

The ProtectLink page appears.

STEP 3 Click the link: **Register ProtectLink services and obtain an Activation Code (AC)**.

The Register Your Product page appears.

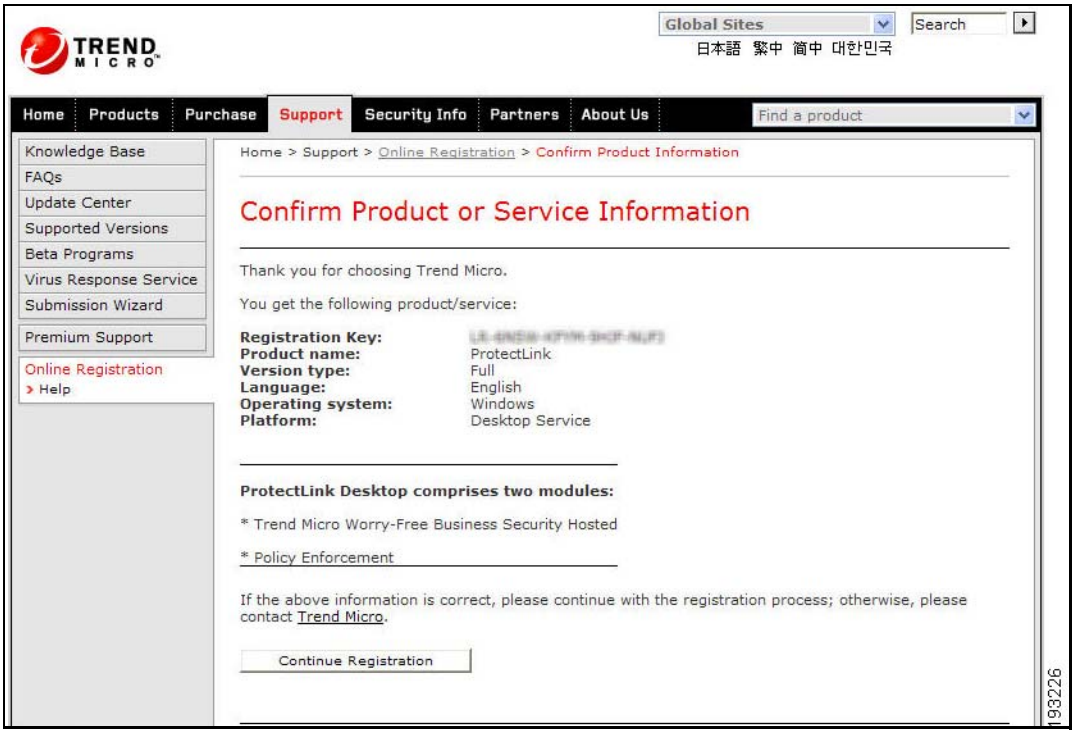


STEP 4 Enter your **Registration Key**, and then click **Next**.

The Confirm License Terms page appears.

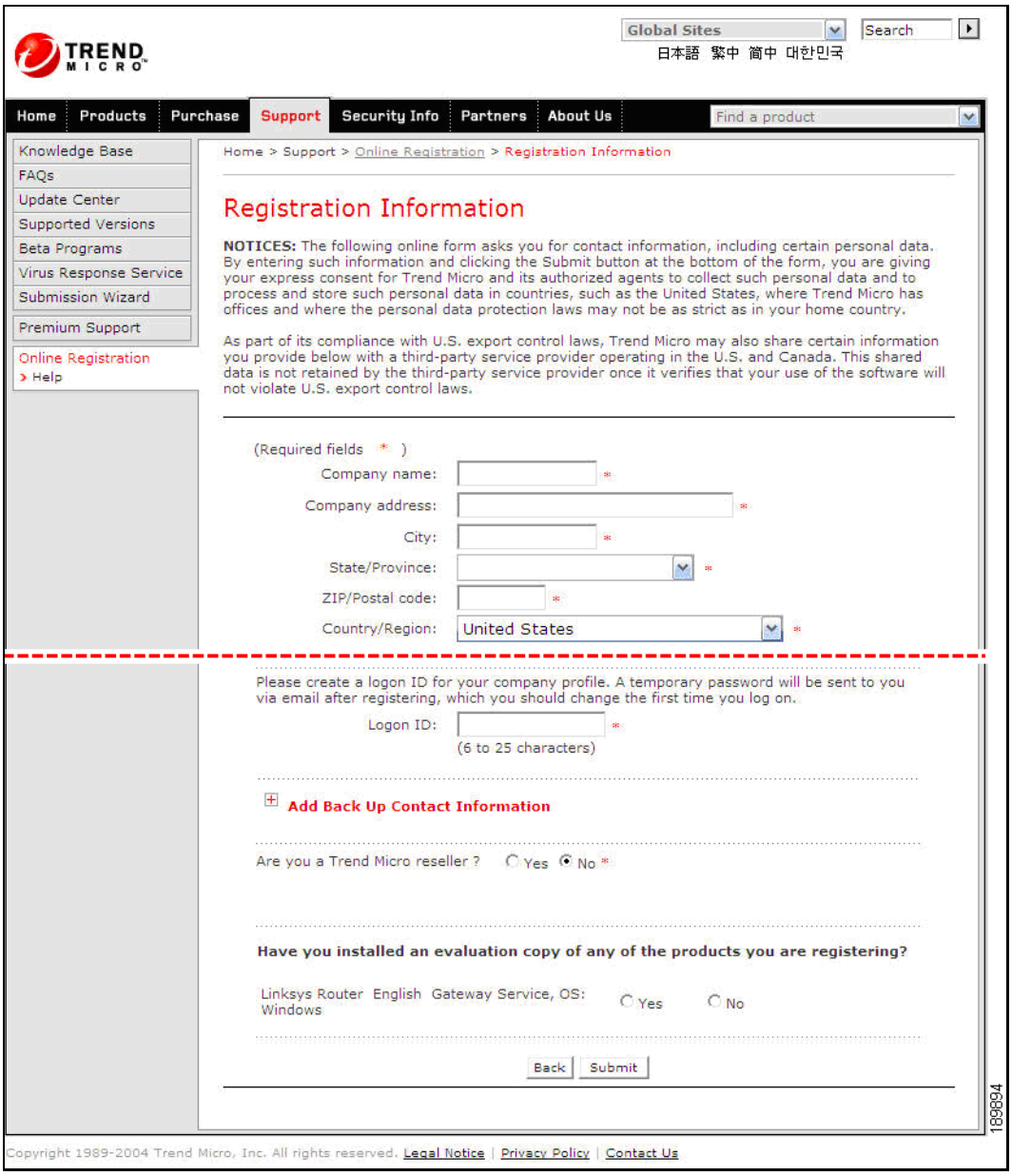
STEP 5 Read the License Terms carefully. If you agree to the terms, select **I Accept**, and then click **Submit**.

The Confirm Product or Service Information page appears.



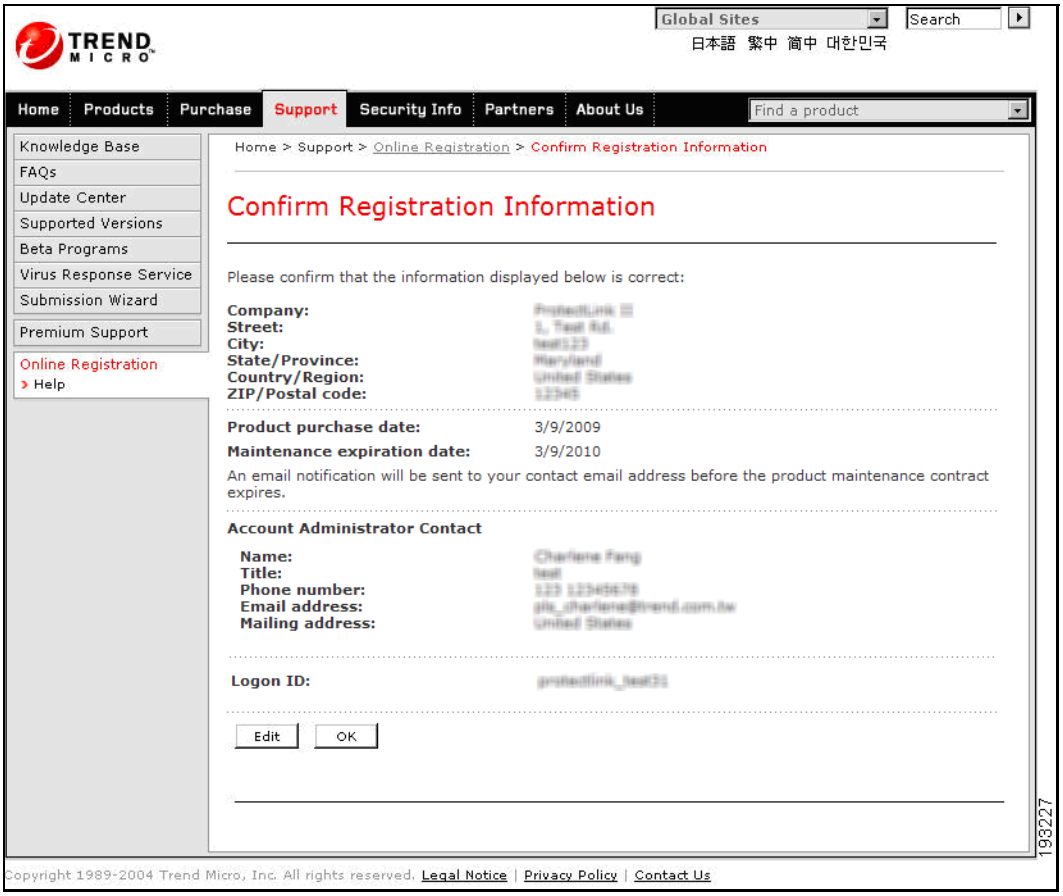
STEP 6 Click **Continue Registration**.

The Registration Information page appears.



STEP 7 Enter your contact details in full, including your email address and a logon ID for your company profile, and then click **Submit**.

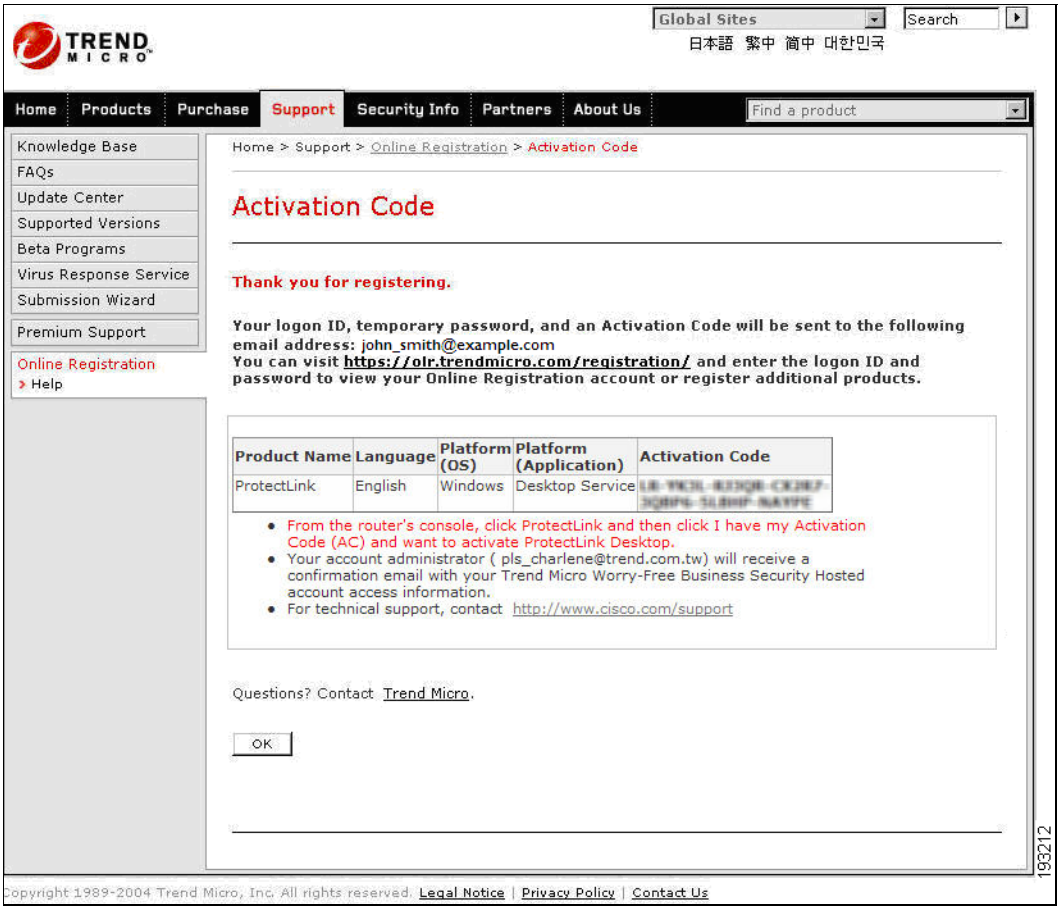
The Confirm Registration page appears, with your contact and domain details.



STEP 8 Make sure the information is correct.

- Click **Edit** if you need to make changes.
- If the information is correct, click **OK**. ProtectLink Endpoint is activated.

The Activation Code page appears and displays your Activation Code. You may print this page for your records.



NOTE **In the future**, you can visit https://olr.trendmicro.com/registration/ to view your Online Registration Account or to register additional Cisco ProtectLink products.

STEP 9 Click **OK** to finish the registration process.

Activating ProtectLink Endpoint

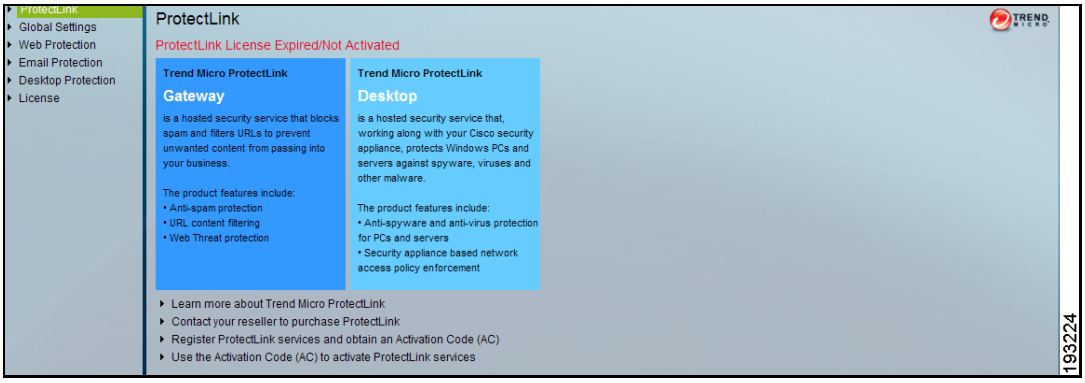
You should receive an email indicating you have successfully registered your ProtectLink Endpoint account within 24 hours (See **Appendix 6, "Post-Registration and Post-Activation Emails"**). The email includes the URL to access the console, your logon ID, and a temporary password, which you should change the next time you log on.

To start using ProtectLink Endpoint, follow these steps:

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

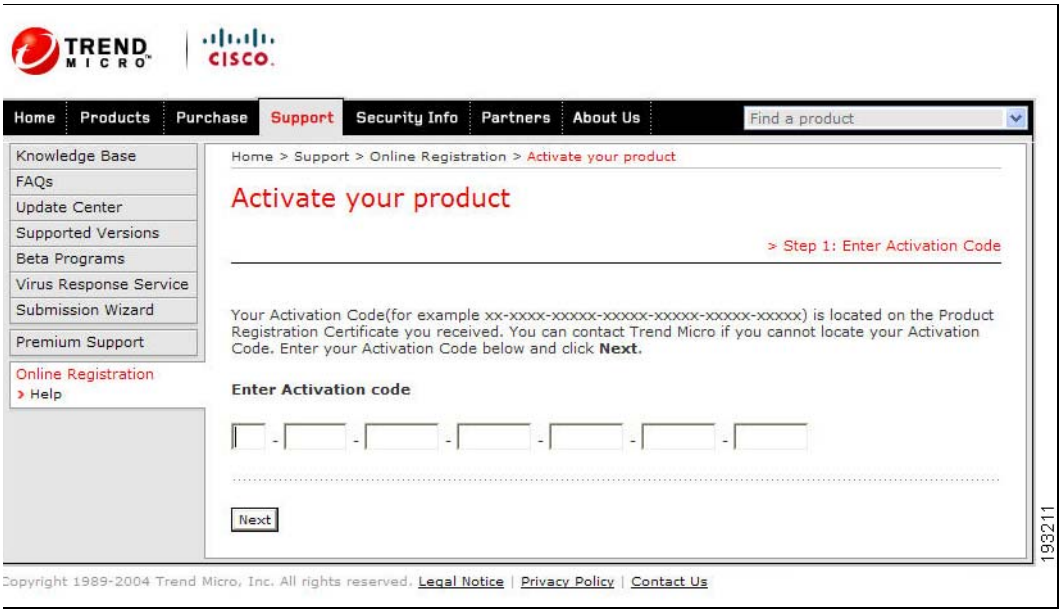
STEP 2 Click **ProtectLink** on the menu bar.

The ProtectLink page appears.



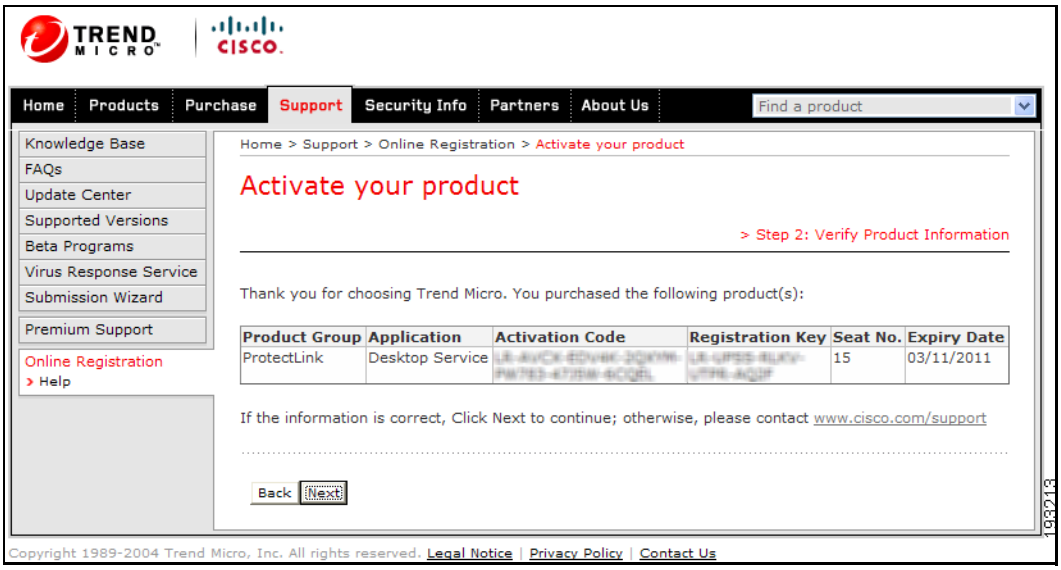
STEP 3 At the bottom of the page, click the link: **Use the Activation Code (AC) to activate ProtectLink services**.

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



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

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



STEP 5 Verify that the details are correct.

- A message appears if the details need to be corrected. You can click **Back** and edit your details.
- If the details are correct, click **Next**.

The Activate Your Product: > Step 3: Finish Activation page appears. You have successfully activated the product.

3

Configuring Cisco ProtectLink Endpoint

After you have activated your account, configure your security appliance for Desktop Protection, as described in the following sections:

- **Providing Desktop Protection to the Computers on the Network, page 22**
- **Enabling Policy Enforcement, page 30**
- **Configuring Global Settings, page 31**
- **License Status and Renewal, page 34**
- **Enabling the Syslog > Outbound Blocking Event Log, page 52**

Providing Desktop Protection to the Computers on the Network

Desktop Protection is powered by Trend Micro WFBS-H. Before enabling policy enforcement, you must install the required components on all computers that use the security appliance for Internet access. When policy enforcement is enabled, only computers with a Worry-Free Business Security Hosted Agent (or any other antivirus application) with updated pattern files and a Threat Management Agent are allowed to access the web.

The following list summarizes the required tasks. Detailed procedures are provided below this summary.

1. Create the WFBS-H Packages.

2. Install the Packages on the Computers.

3. Download and Install the TMAgent on all computers.

1. Create the WFBS-H Packages.

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

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

STEP 3 On the ProtectLink Endpoint page, click the WFBS-H link to connect to the WFBS-H web portal at the following URL:

https://wfbs-h.trendmicro.com/wfbsh/protectlinklogin.aspx

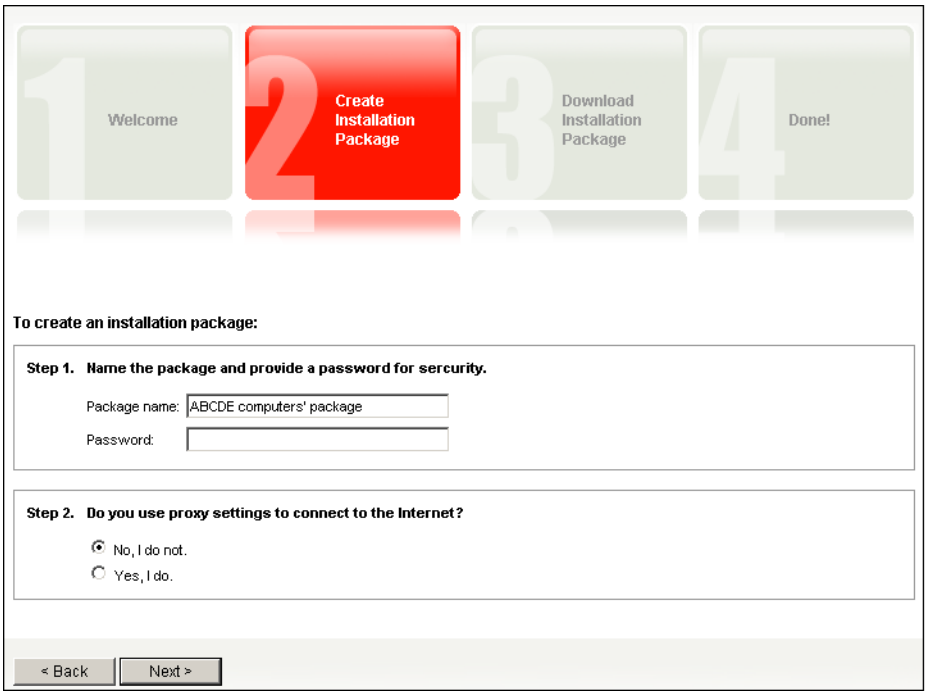
The login page appears.

STEP 4 Enter the **WFBS-H User name** and temporary **Password** that you received when you activated the Cisco ProtectLink Endpoint. Click **Log on**.

The Welcome page appears. You can view your Activation Code on the Welcome page.

STEP 5 Click **Next** to create packages.

The Create Installation Package page appears.

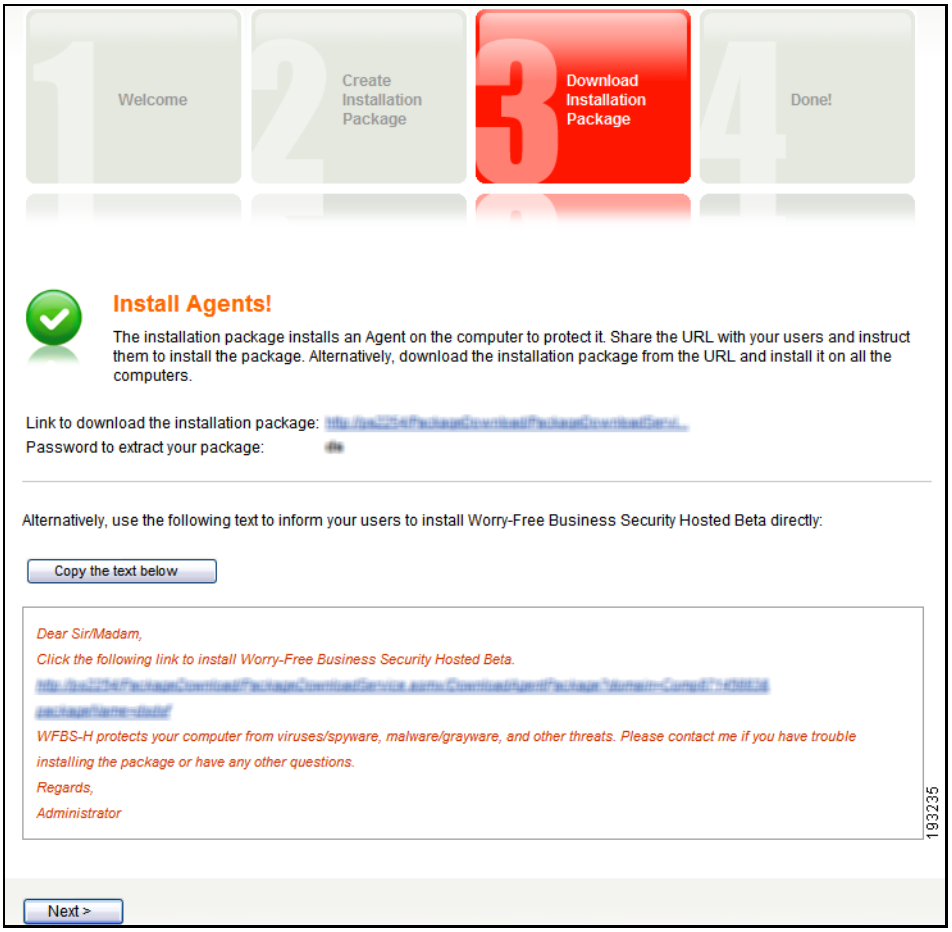


STEP 6 To create the packages that install the Agents on the client computers, enter the following information:

- **Package Name**: Enter a name for the package.
- **Password**: Enter a password to be used when extracting the package.
- **Do you use proxy settings to connect to the Internet?**:
  - If you do not use proxy settings, click **No, I do not**.
  - If you use proxy settings, click **Yes, I do**. The configuration options appear.
- If you use proxy settings, select the required proxy settings for the agents to communicate with the WFBS-H server:
  - **Automatically detect settings**: Agent installer automatically detects the settings required to install the package.
  - **Automatic configuration script**: WFBS-H updates the location of the configuration script in the Address field. It uses the configuration script from this URL to install the package.
  - **Manual configuration**: WFBS-H updates the following proxy configuration in the Manual configuration field.
- If you chose manual configuration, enter the following information:
  - **Server IP Address**: Enter the IP address of the proxy server. You can get the IP address for the proxy server from the Internet Explorer settings.
  - **Port**: Enter the port number that is used by the proxy server for client connections.
  - **User ID**: Enter the account name used by the client machine to connect to the proxy server.
  - **Password**: Enter the password for the User ID.

STEP 7 Click **Next**.

The Download Installation Package page appears.



STEP 8 To download the installation package, click the **Link to download the installation package**.

Alternatively, click **Copy the text below** to copy the text in the box. You can use this text to inform your users to install the Agent.

STEP 9 Click **Next**.

The Done page appears.

STEP 10 Click **OK**.

The Summary page appears.

NOTE Next, continue to **2. Install the Packages on the Computers.**

2. Install the Packages on the Computers.

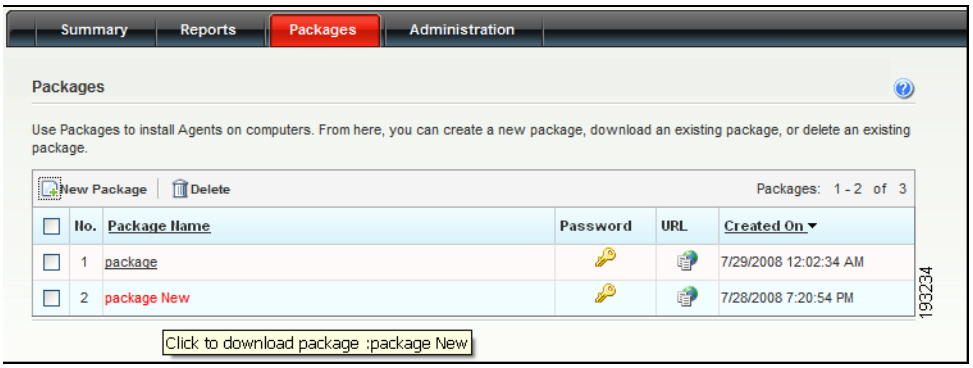
After creating a package, follow these steps to download and install these packages on computers that connect to your security appliance.

NOTE After installing a package, it takes approximately one hour for the agents to start reporting to WFBS-H.

STEP 1 Continuing from the previous procedure, click the **Packages** tab in the WFBS-H web portal.

> **NOTE** To connect to the WFBS-H web portal, launch the Configuration Utility for your security appliance, and then log in. Click **ProtectLink** in the menu bar, and then click **Web Protection > Desktop Protection** in the navigation tree. On the ProtectLink Endpoint page, click the WFBS-H link. Then log on to the WFBS-H web portal.

The Packages page appears.



STEP 2 Click the package name from the list. A **File Download** dialog box appears.

STEP 3 Click **Save** to save the package on your machine.

STEP 4 Install these packages on computers you want to protect.

> **NOTE** On Windows Vista computers, install the package with Administrator rights (using the **Run as administrator** option).

NOTE Next, continue to **3. Download and Install the TMAgent on all computers.**

3. Download and Install the TMAgent on all computers.

The TMAgent ensures the client has an antivirus solution installed. If a computer does not have an antivirus solution installed, the TMAgent alerts the security appliance. When policy enforcement is enabled on the security appliance, unprotected computers are prevented from accessing the web.

STEP 1 Download the TMAgent from the following URL:

http://www.trendmicro.com/download/product.asp?productid=94

STEP 2 Click the link for the file (.MSI).

STEP 3 When the Security Warning appears, click **Save**, and then choose a location on your computer.

STEP 4 After the file is downloaded, double-click it to run the installation program.

STEP 5 Install the TMAgent on all computers that connect to your security appliance.

Enabling Policy Enforcement

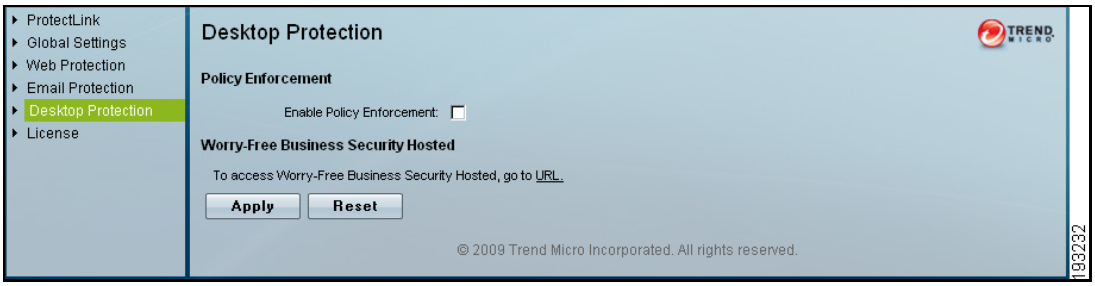
Enable policy enforcement to ensure that only protected computers can access the Internet.

To enable policy enforcement, follow these steps:

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

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

The Desktop Protection Policy Enforcement page appears.



STEP 3 Check the **Enable Policy Enforcement** box. When this feature is enabled, only computers with a Worry-Free Business Security Hosted Agent (or any other antivirus application) with updated pattern files and a Threat Management Agent are allowed to access the web.

> **NOTE** Only port 80 will be blocked on computers not meeting these requirements.

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

Configuring Global Settings

This section contains the following tasks:

- Configuring Approved Clients, page 31
- Configuring Approved URLs, page 32

Configuring Approved Clients

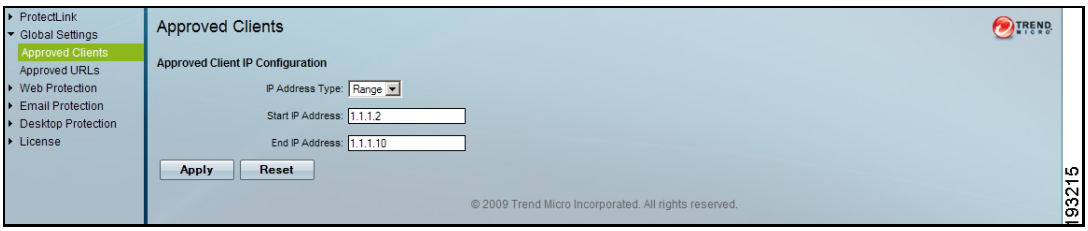
- The Approved Clients List details the computers that have unrestricted web access. To configure Approved Clients, follow these steps:

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

STEP 2 Click **ProtectLink** on the menu bar, then click **Global Settings > Approved Clients**.

STEP 3 To enable this feature, check the **Enable Approved Clients List** box, and click **Apply**.

STEP 4 To add a new computer to the list, click **Add**.



STEP 5 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 6 Click **Apply** to save the settings. The details appear in the Approved Clients List on the Approved Clients page.

Configuring Approved URLs

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

To configure Approved URLs, follow these steps:

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

STEP 2 Click **ProtectLink** on the menu bar, then click **Global Settings > Approved URLs**.

STEP 3 To enable this feature, check the **Enable Approved URLs List** box, and click **Apply**.

STEP 4 To add a new URL or keyword to the list, click **Add**.

STEP 5 Enter the following information:

- **URL**: Enter the name of the site or keyword.
- **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 contains 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** to save the settings. The details appear in the Approved Clients List on the Approved Clients page.

License Status and Renewal

From the Configuration Utility for your security appliance or router, you can review your license status, renew your license, and to add seats to your ProtectLink account.

This section contains the following tasks:

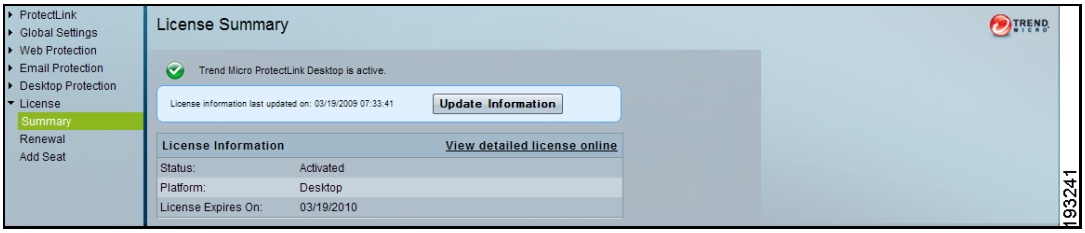
- **Renewing a License, page 36**
- **Adding Seats, page 43**

To review license information, follow these steps:

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

STEP 2 Click the **ProtectLink** on the menu bar, and then click **License > Summary** in the navigation tree.

The License Summary page appears, displaying the status of the license.



You can perform the following tasks:

- View detailed license information
- Renew your license
- Add seats to your existing license

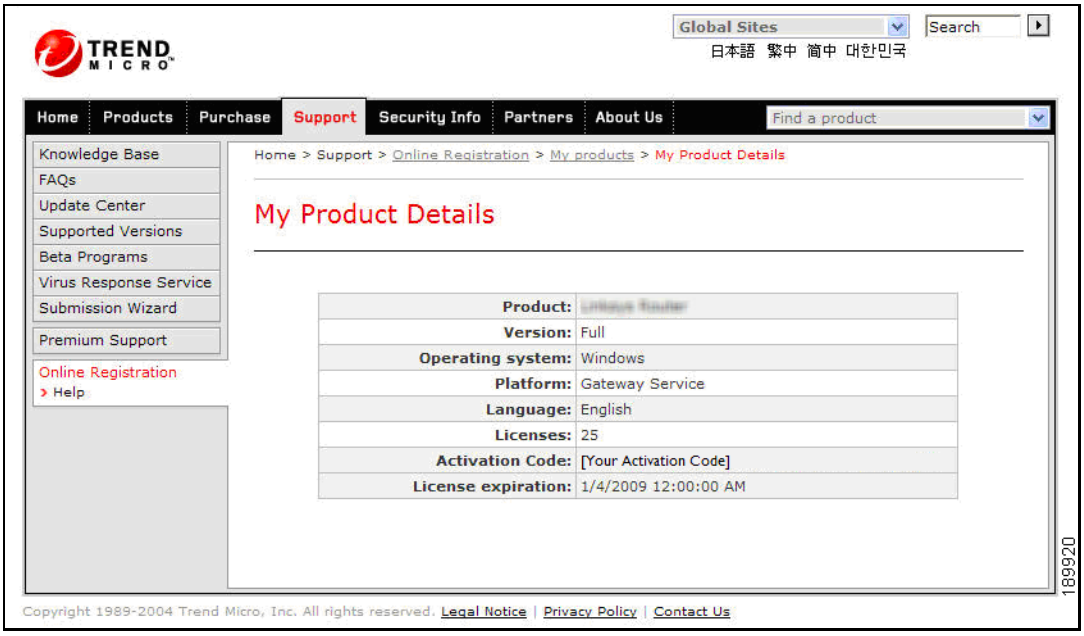
The Status Icon and the message indicate the status of the license.

Icon	Message
	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 page appears.



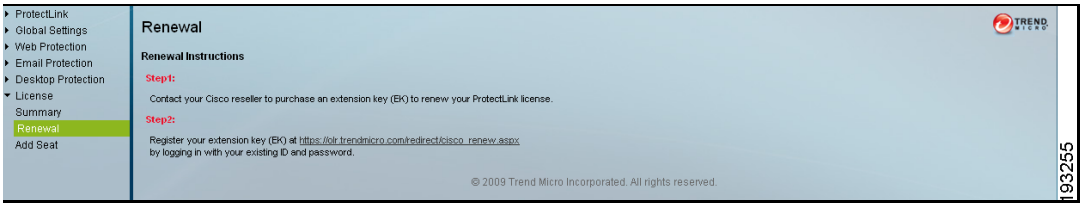
Renewing a License

NOTE You must first purchase an Extension Key (EK) from your Cisco reseller.

To renew your license, follow these steps:

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

STEP 2 Click **ProtectLink** on the menu bar, and then click **License > Renewal**.

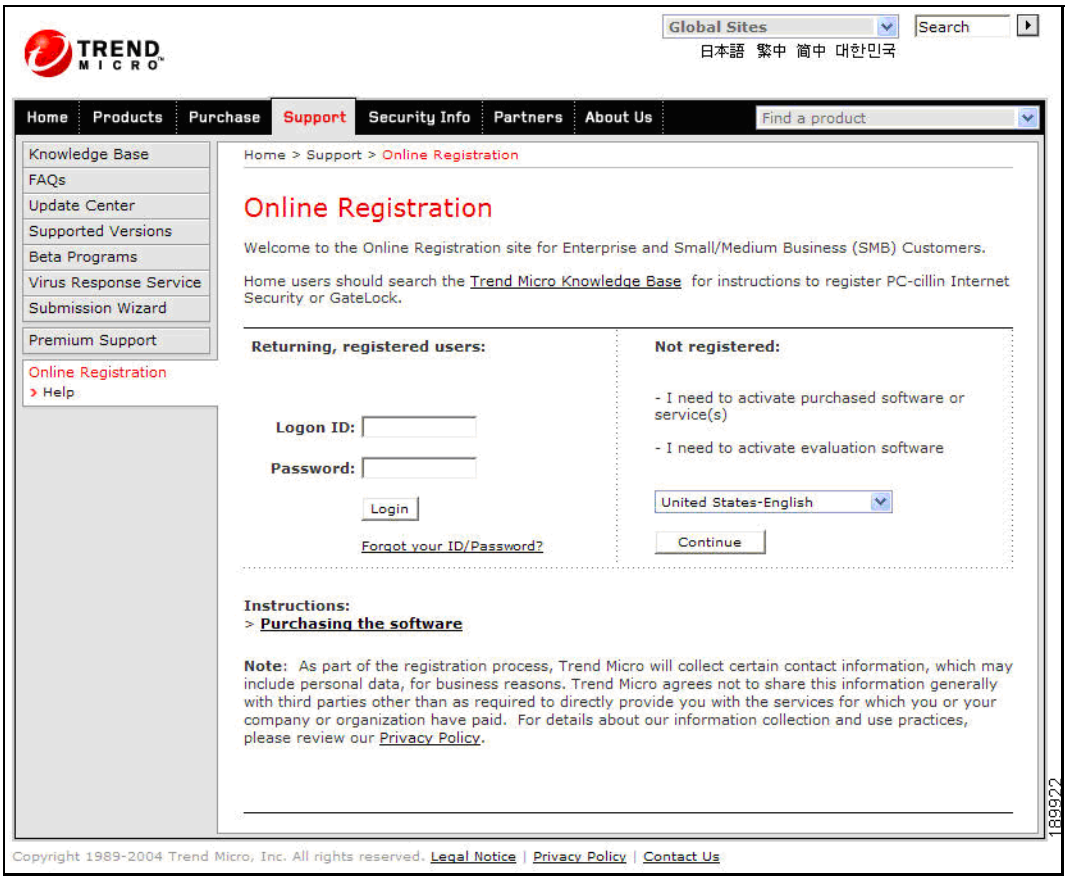


STEP 3 Proceed by following the instructions on the page:

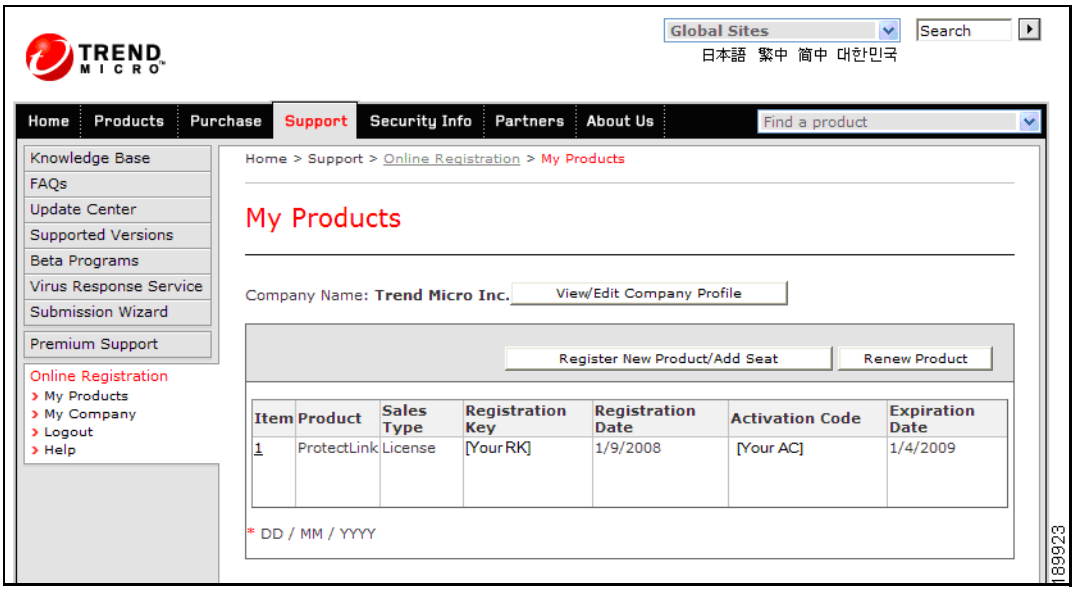
a. Contact your Cisco reseller to purchase an extension key (EK) to renew your ProtectLink license.

b. Click the Cisco link to launch the Cisco web portal and register your extension key.

The Cisco Online Registration page appears.

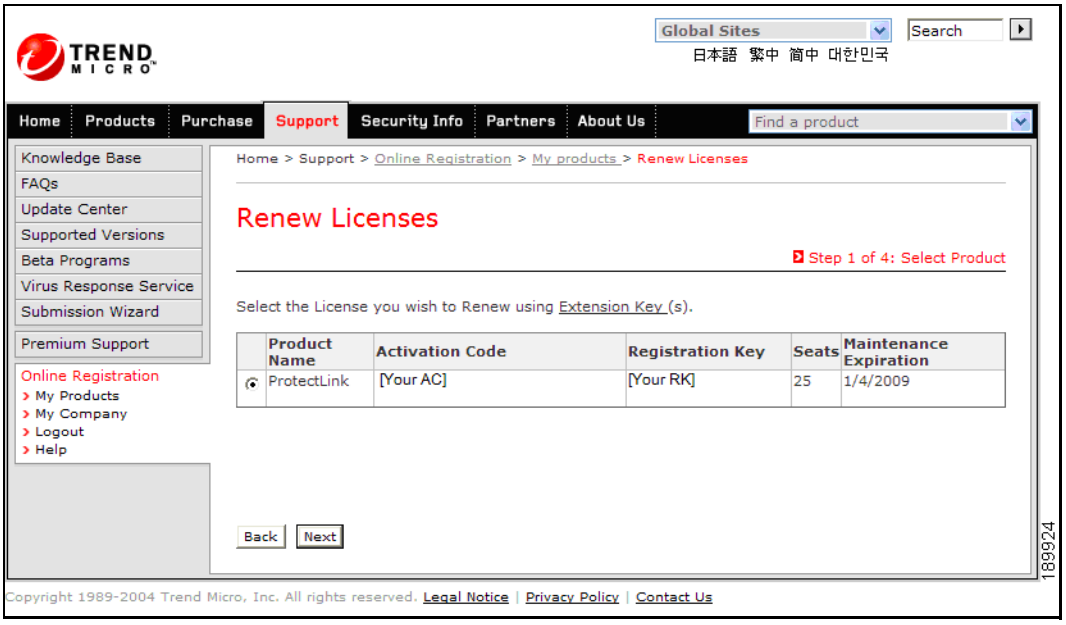


STEP 4 Enter your ProtectLink Logon ID and Password, then click **Login**.



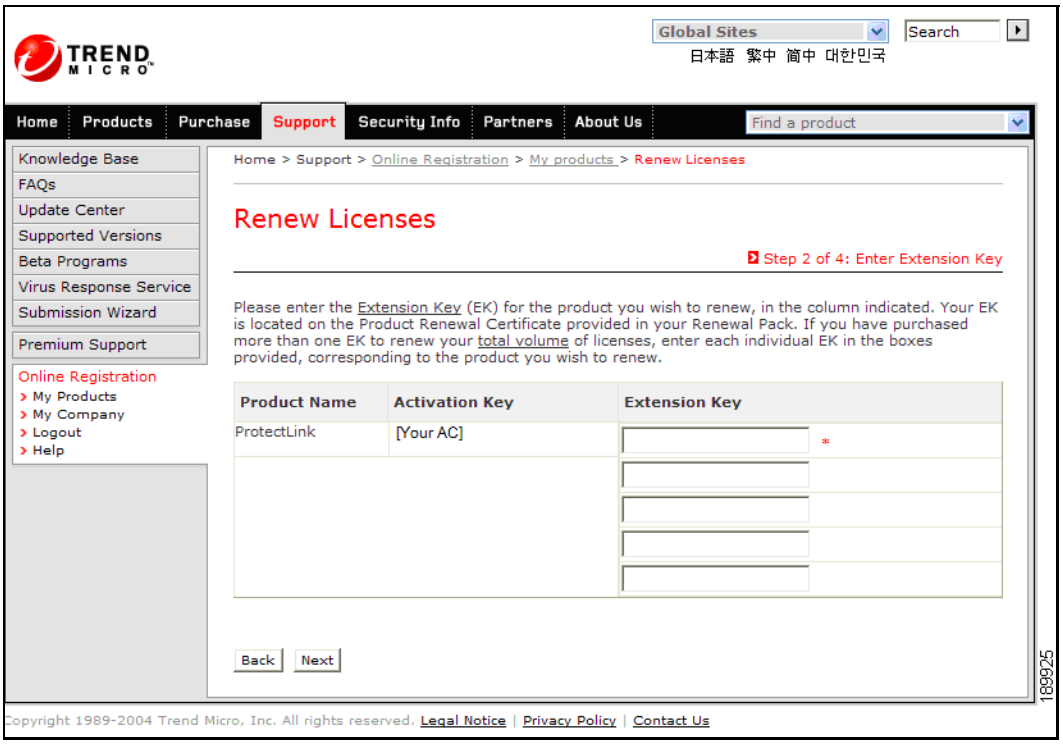
STEP 5 Click **Renew Product**.

The Renew Licenses > Step 1 of 4: Select Product page appears.



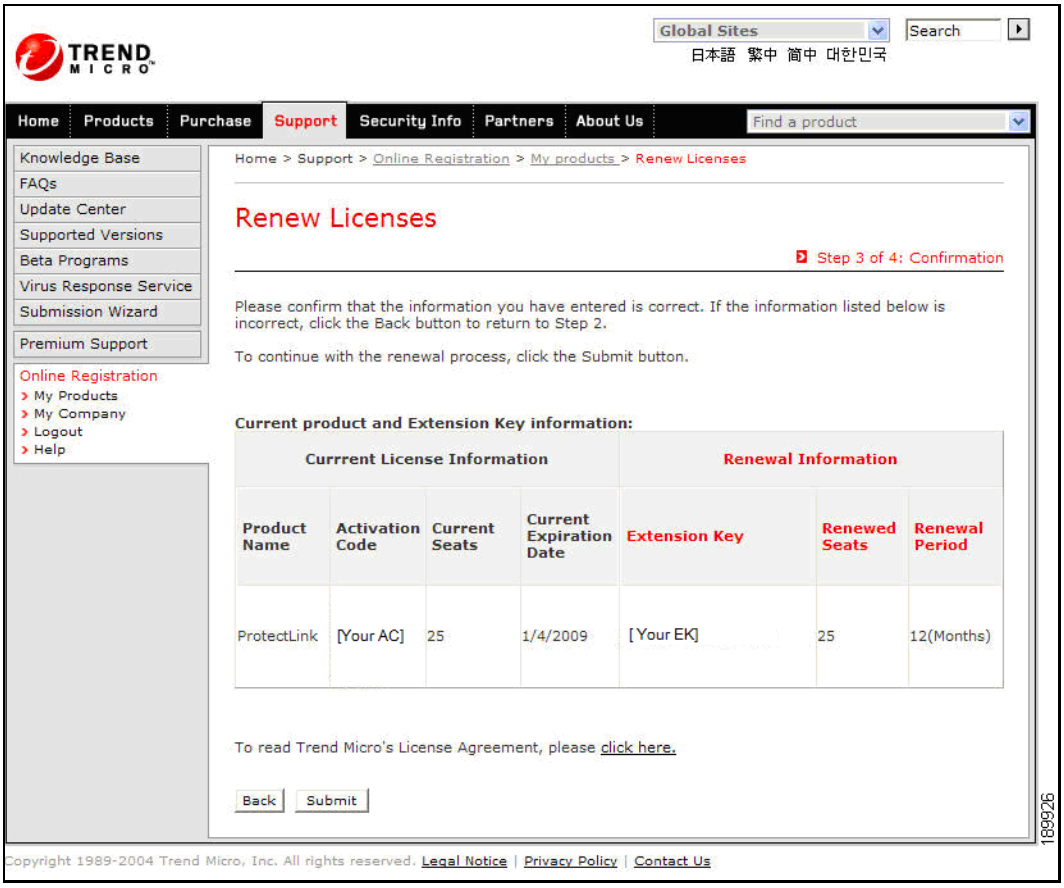
STEP 6 Select the license to renew, and then click **Next**.

The Renew Licenses > Step 2 of 4: Enter Extension Key page appears.



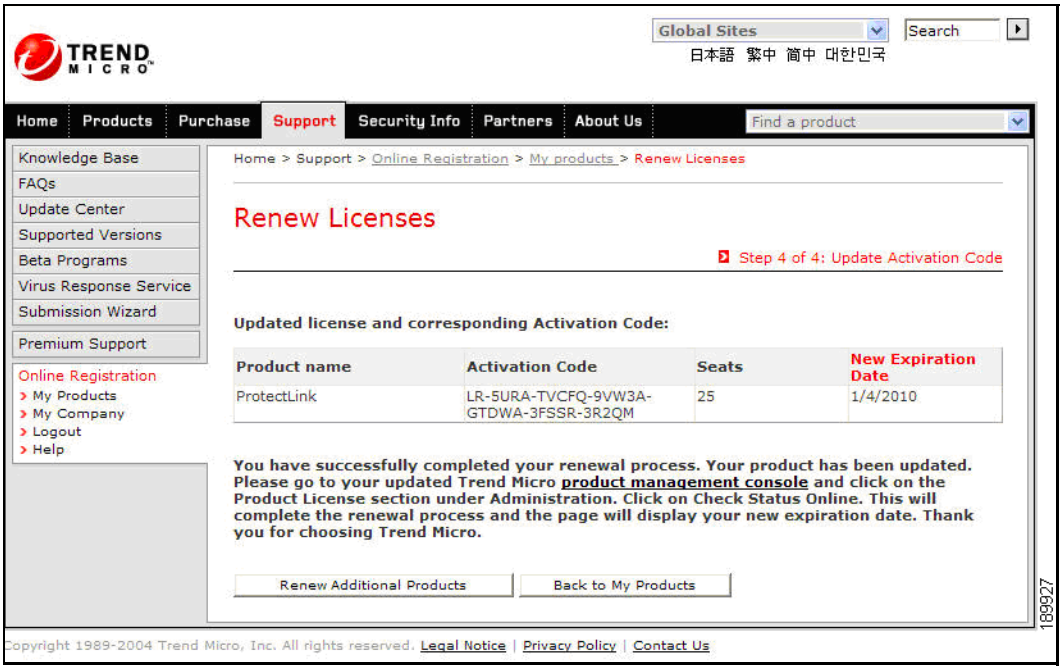
STEP 7 Enter the **Extension Key** for the product you wish to renew (ProtectLink), and then click **Next**.

The Renew Licenses > Step 3 of 4: Confirmation page appears.



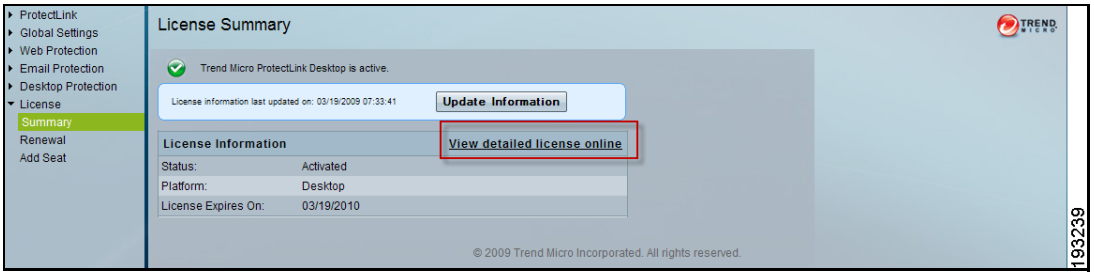
STEP 8 Check your current product and Extension Key information, and then click **Submit**.

The Renew Licenses > Step 4 of 4: Update Activation Code page appears, indicating that you have successfully renewed your license.



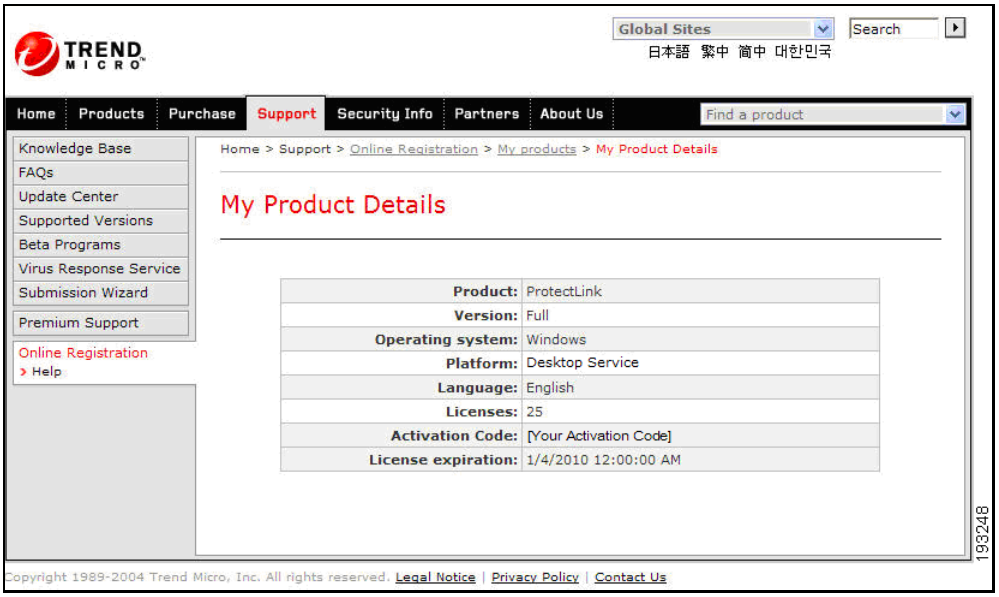
STEP 9 To complete the renewal process, return to the security appliance Configuration Utility.

STEP 10 Click **ProtectLink** on the menu bar, and then click **License > Summary**.



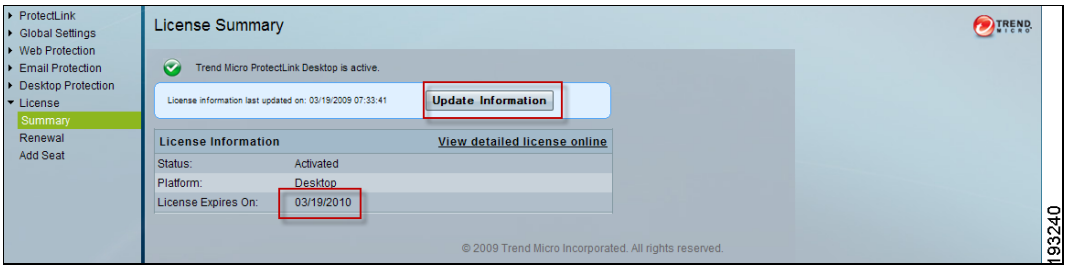
STEP 11 Click **View detailed license online**.

The My Product Details page appears, indicating your ProtectLink product details and the new license expiration date.



STEP 12 Return to the security appliance Configuration Utility.

STEP 13 Click **ProtectLink** on the menu bar, and then click **License > Summary**.



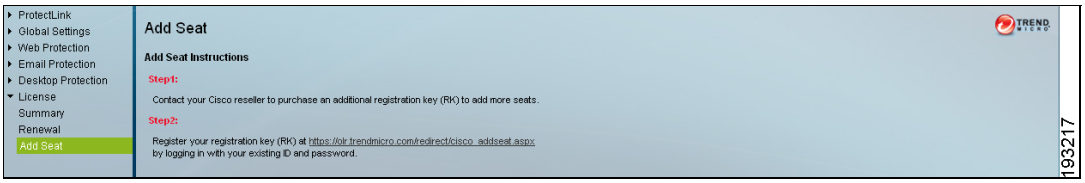
STEP 14 Click **Update Information**. Your License Information is updated, indicating your new ProtectLink expiration date.

Adding Seats

When you purchase ProtectLink services, you can choose from the 5-seat or the 25-seat option. To add seats to your license, allowing additional computers to be protected, follow these steps:

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

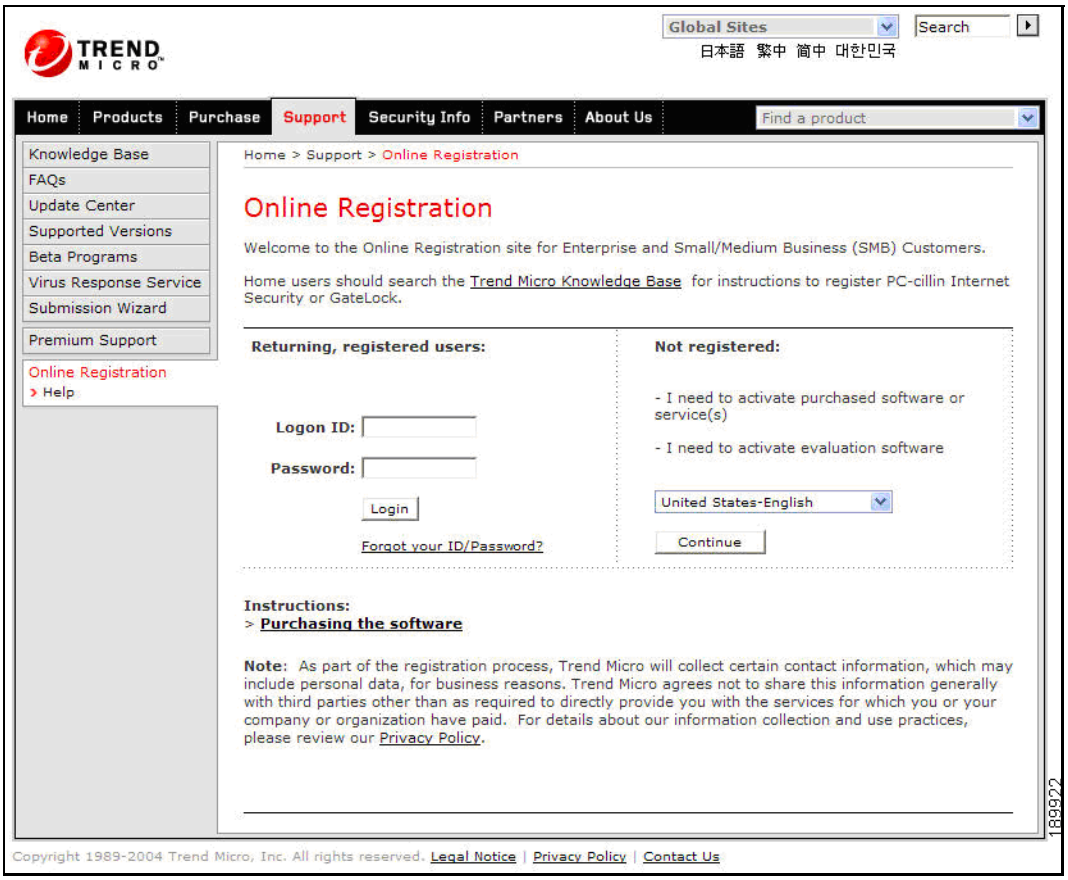
STEP 2 Click **ProtectLink** on the menu bar, and then click **License > Add Seat**.



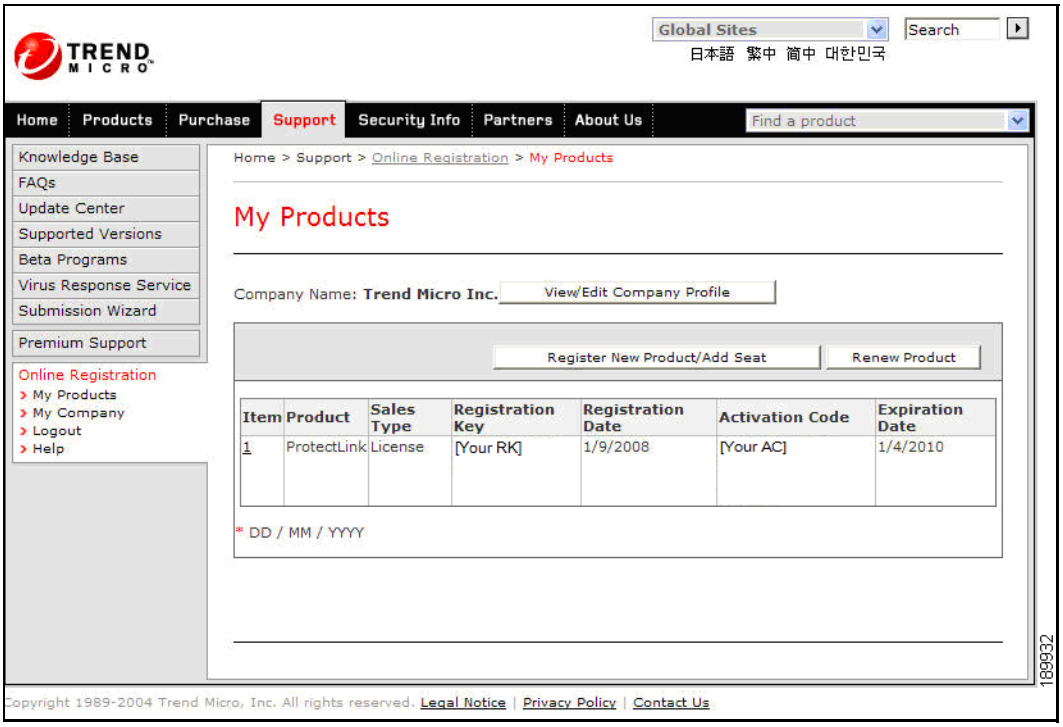
STEP 3 To proceed, follow the instructions on the page:

a. Contact your Cisco reseller to purchase an additional registration key (RK) to add more seats.

b. Click the link to log in to the web portal and register the product.

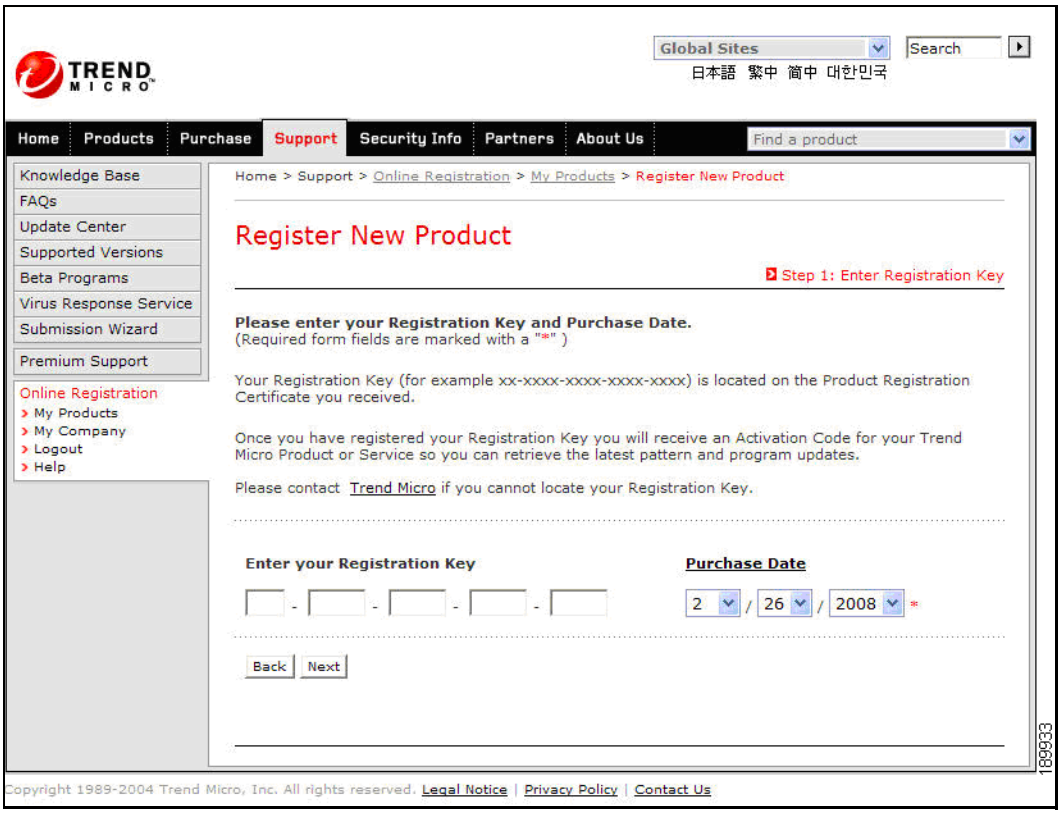


STEP 4 Enter your Logon ID and Password, and then click **Login**.



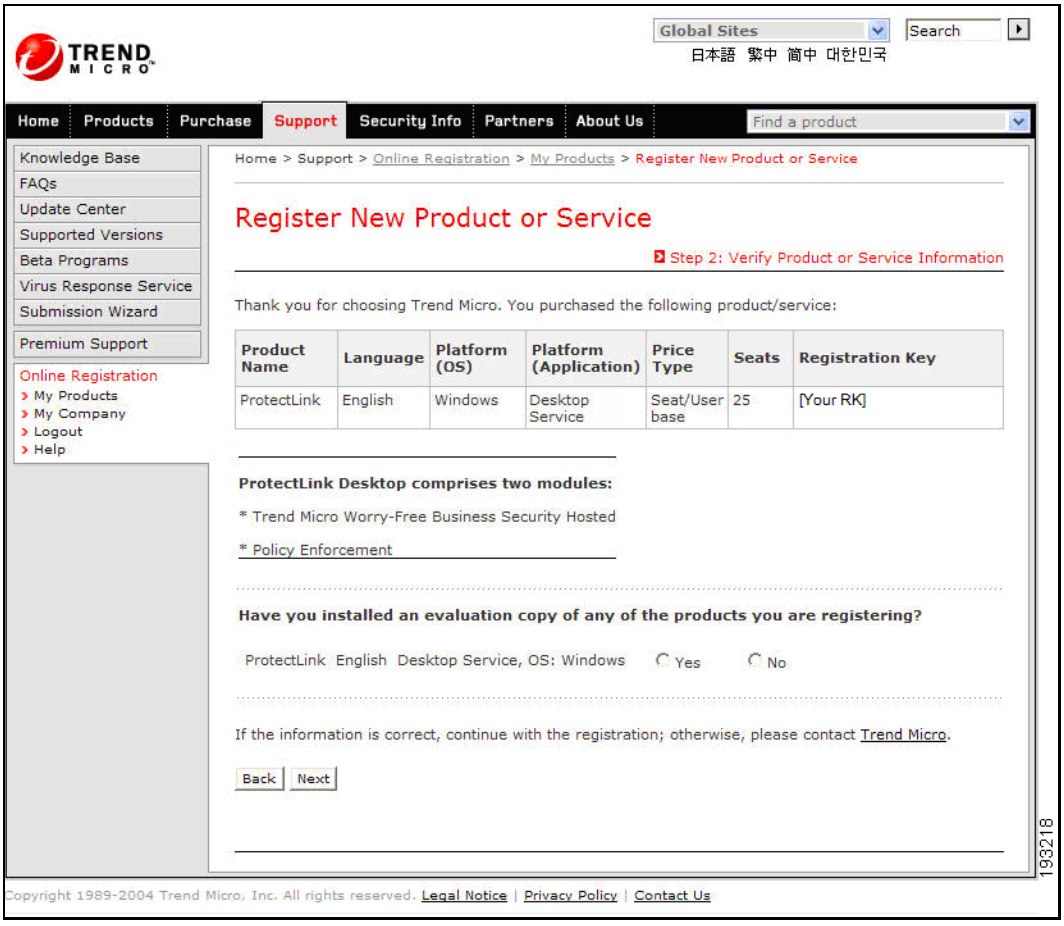
STEP 5 Click the **Register New Product/Add Seat** button above the table.

The Register New Product > Step 1: Enter Registration Key page appears.



STEP 6 Enter your **Registration Key** and **Purchase Date**, and then click **Next**.

The Register New Product > Step 2: Verify Product or Service Information page appears, with the new Seats showing in the Registration table.

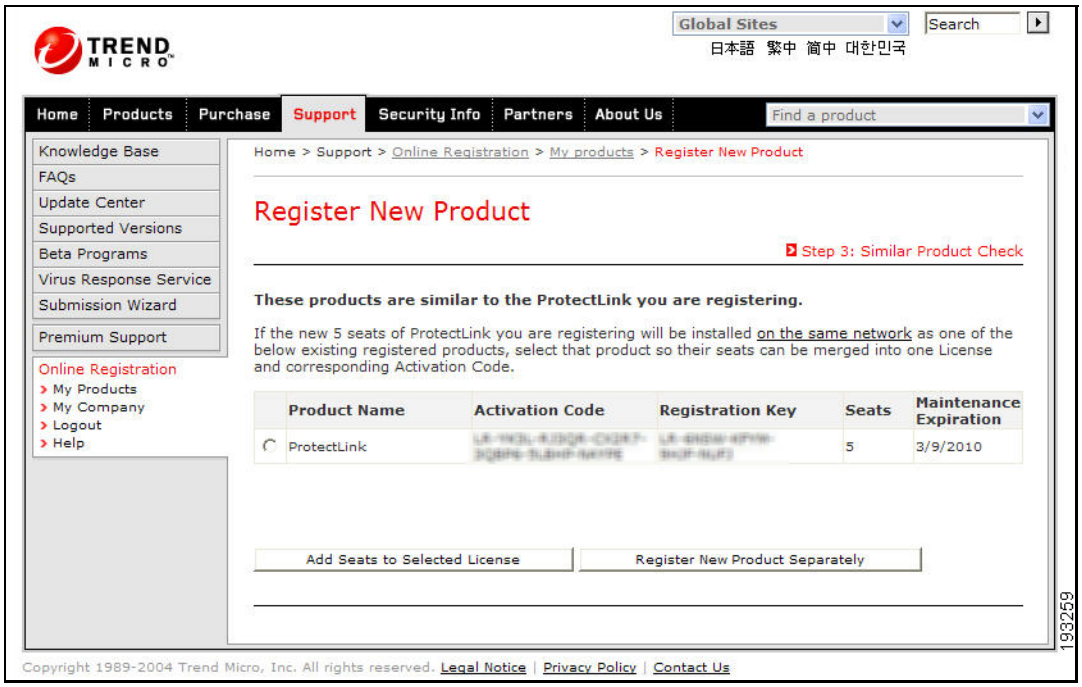


STEP 7 Verify your product or service information.

STEP 8 Click **Yes** or **No** to answer the question: Have you installed an evaluation copy of any of the products you are registering?

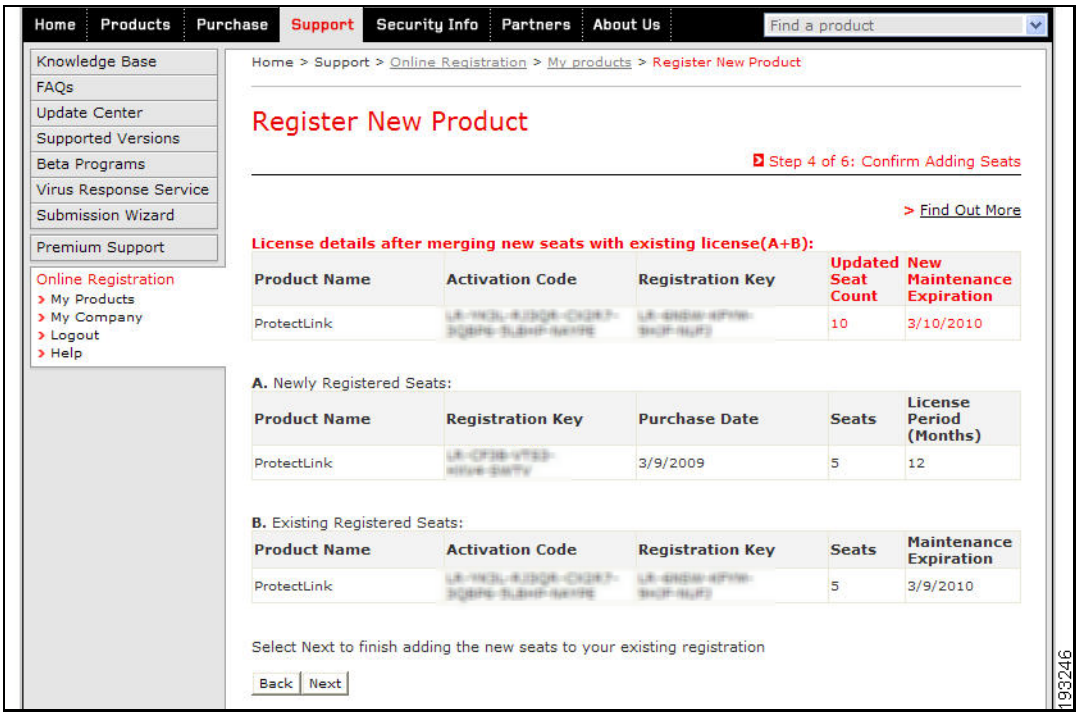
STEP 9 If the information is correct, click **Next**.

The Register New Product > Step 3: Similar Product Check page appears.



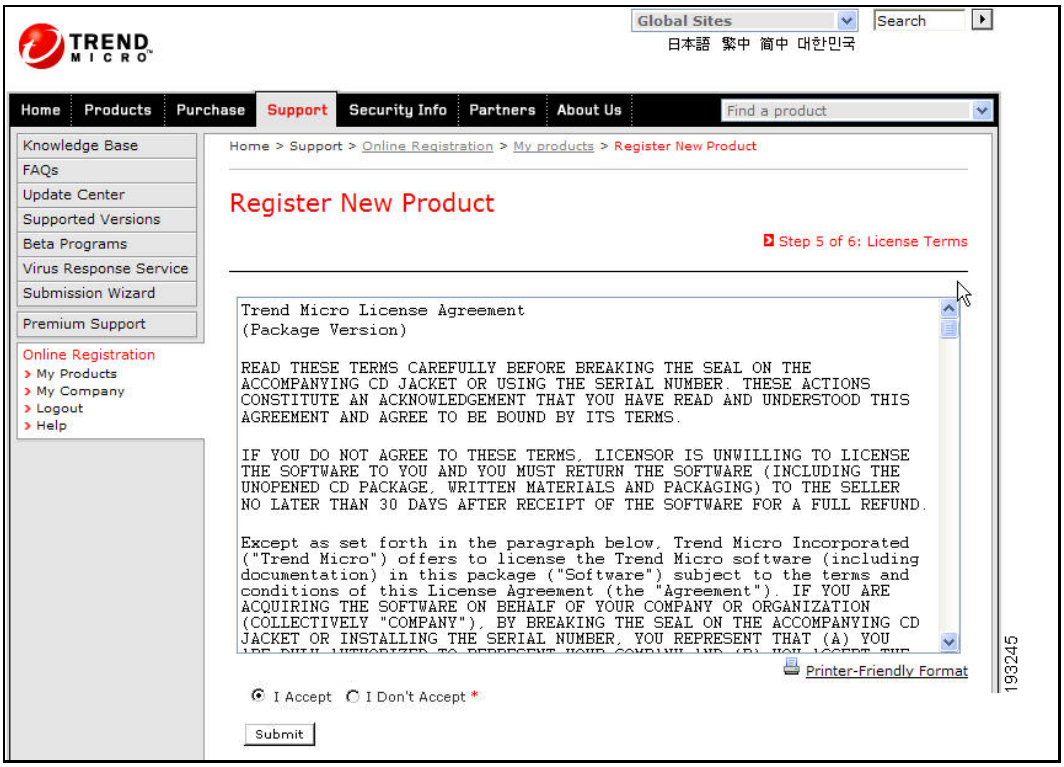
STEP 10 Select the required license, and then click **Add Seats to Selected License**.

The Register New Product > Step 4 of 6: Confirm Adding Seats page appears.



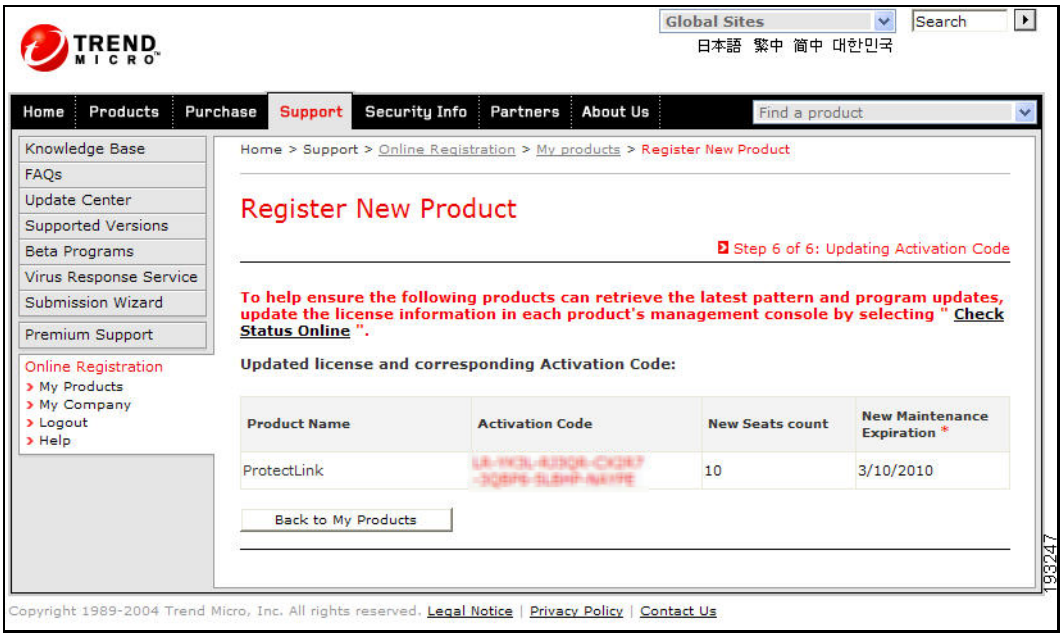
STEP 11 Click **Next** to confirm the changes highlighted in red.

The Register New Product > Step 4 of 6: License Terms page appears.



STEP 12 Click **I Accept**, and then click **Submit**.

The Register New Product > Step 6 of 6: Updating Activation Code page appears.



STEP 13 When these steps are completed, your ProtectLink Endpoint account is updated and will accommodate the new seats.

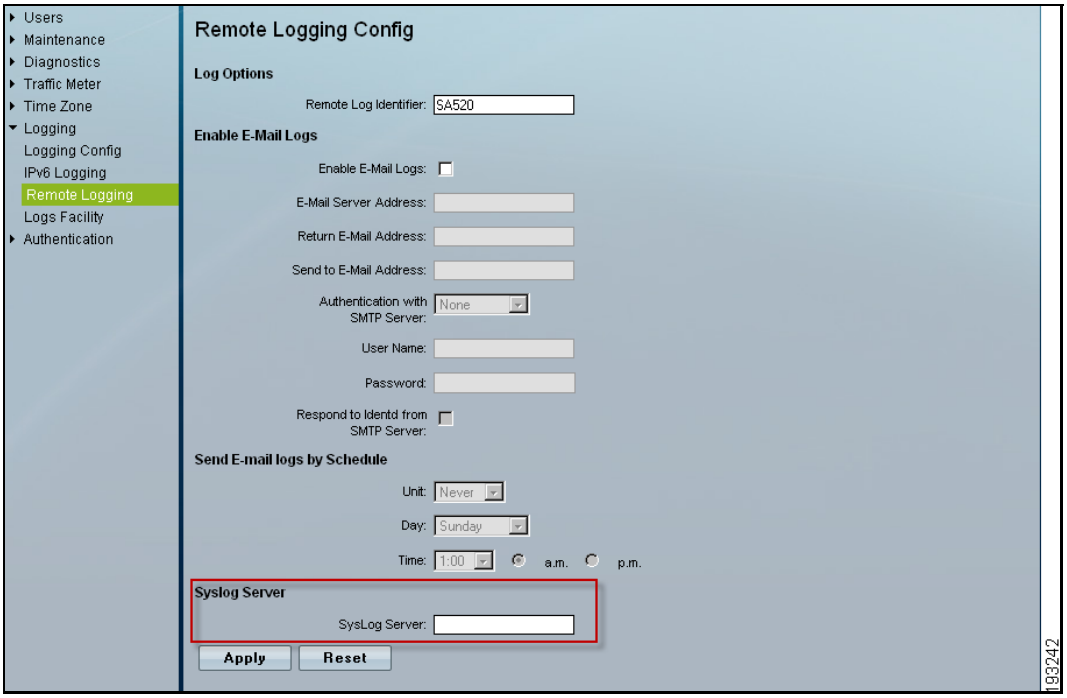
Enabling the Syslog > Outbound Blocking Event Log

ProtectLink Endpoint 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, follow these steps:

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

STEP 2 Click the **Administration** on the menu bar, and then click **Logging > Remote Logging** link.



STEP 3 In the **Syslog Server** section, enter the **Name or IP Address** of the Syslog Server.

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

STEP 5 When you have log data, click **View Log** to view your logs.

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

4

Using the Web Portal for Administration

Use the web portal for the following administrative tasks:

Launching the Web Portal

You can launch the web portal from the Configuration Utility for your security appliance. The web portal provides access to summaries, packages, reports, and administrative features for WFBS-H.

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

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

STEP 3 On the ProtectLink Endpoint page, click the WFBS-H link to go to the following URL:

https://wfbs-h.trendmicro.com/wfbsh/protectlinklogin.aspx

STEP 4 When the WFBS-H web portal log in page appears, enter your login ID and password, and then click **Log on**.

You are now ready to start using the web portal.

Working with Summaries

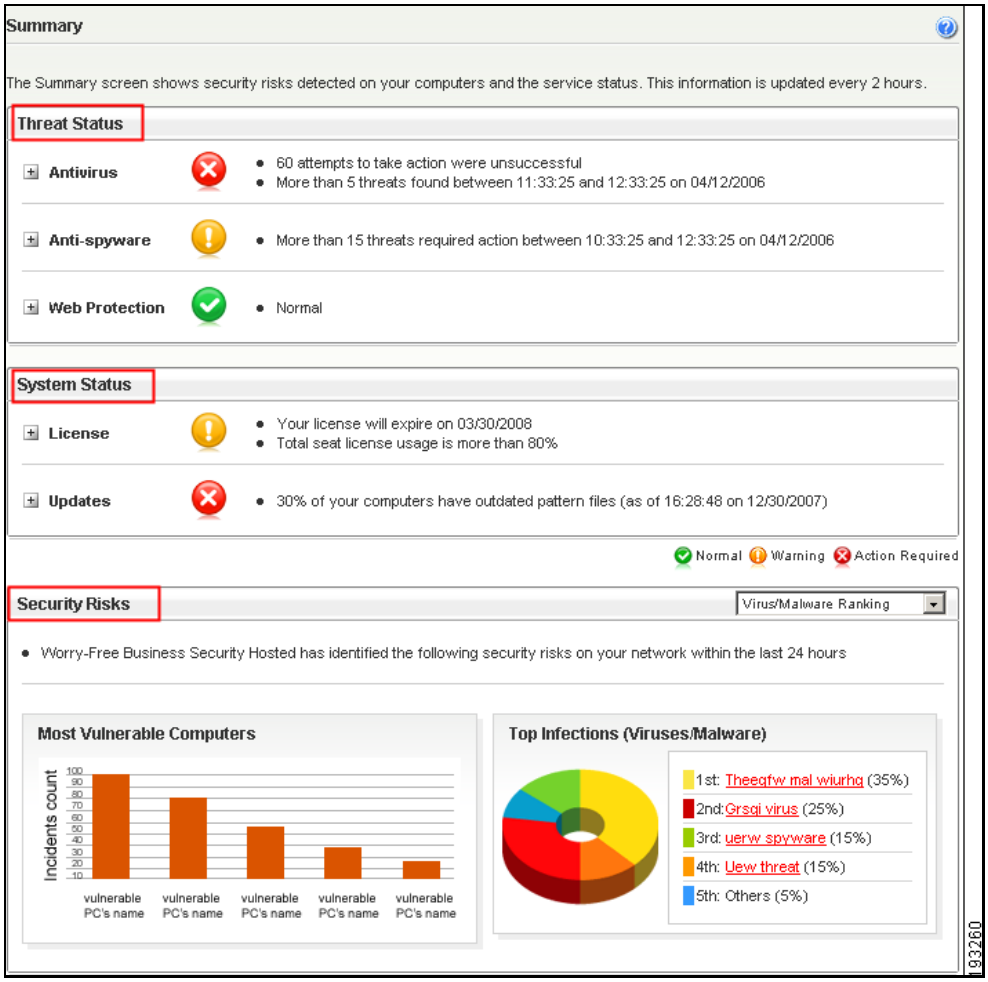
Open the Summary page to display the security risks detected on computers and the status of the service.

To open the Summaries page:

STEP 1 Launch the WFBS-H web portal.

NOTE For more information, see Launching the Web Portal, page 53.

STEP 2 Click the **Summary** tab.



NOTE WFBS-H updates the summary information every two hours.

STEP 3 Click the buttons and the links on the page to view more information.

Refer to the following topics for details:

- **Notification Icons, page 55**
- **Threat Status, page 56**
- **System Status, page 57**
- **Security Risks, page 58**

Notification Icons

The notification icons on the Summary page indicate the status of the Worry-Free Business Security Hosted service on your computer, and also alerts you when a virus or spyware is detected.

The following table describes the notification icons status.

Table 1 Notification Icons

Icon	Status Description
	**Normal**: No action required.
	**Warning:** Typically, a warning icon means that you have many vulnerable computers that are reporting too many virus/malware or spyware incidents.
	**Action Required:** Take action to prevent further risk to your network.

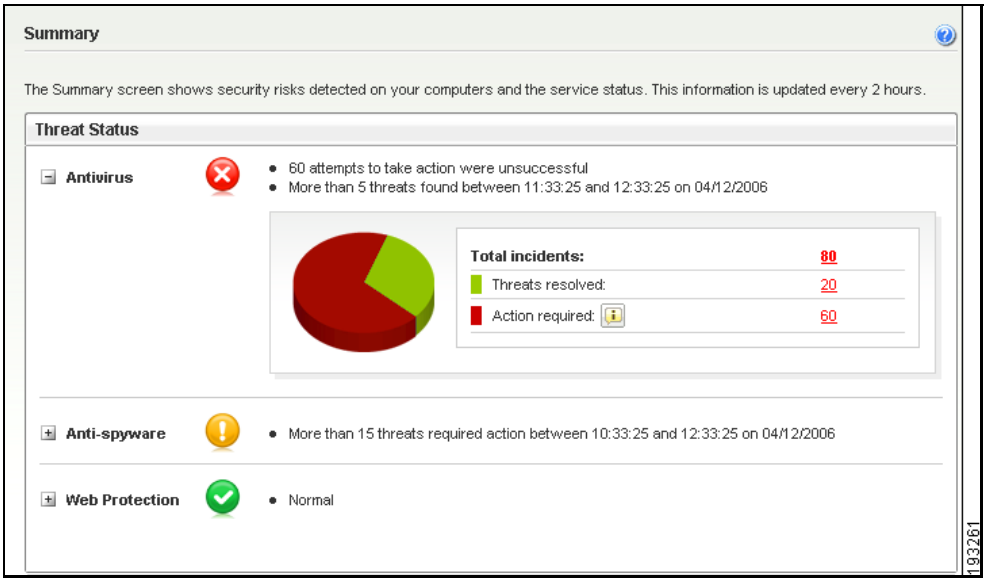
Threat Status

The Threat Status section of the Summary page indicates the total incidents found on your network, the number of threats resolved, and the number of threats that require action. This section includes the following sub-sections:

- Antivirus
- Anti-spyware
- Web Protection

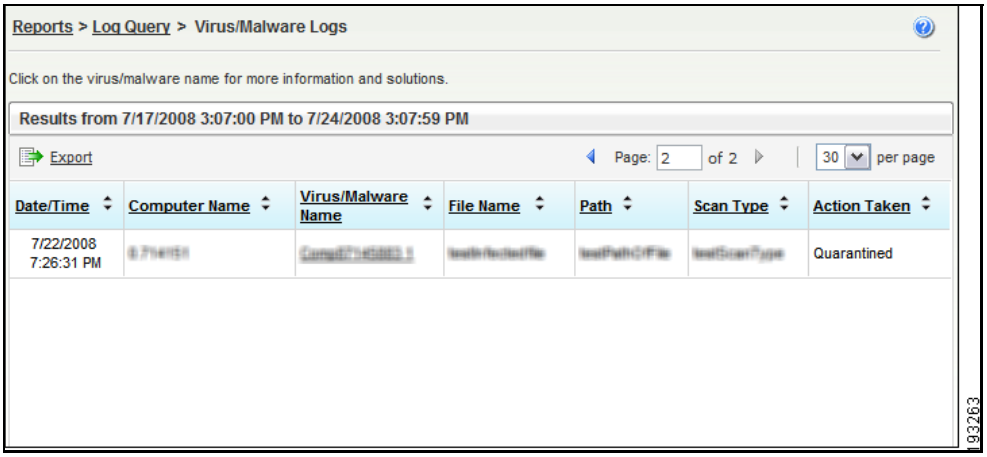
To view details of a particular threat type, click ⊞ next to the subheading. **Figure 1** shows an example of the information that appears.

Figure 1 Threat Status for Antivirus section



To view detailed information including the name of the computer and the number of threats found, click the incident count. **Figure 2** shows an example of the information that appears.

Figure 2 Detailed Virus/Malware Status page



The generated log contains information about the name of the virus/malware or spyware found in the specified time range, and actions taken. Click on the virus/malware or spyware/grayware name for more information and solutions.

System Status

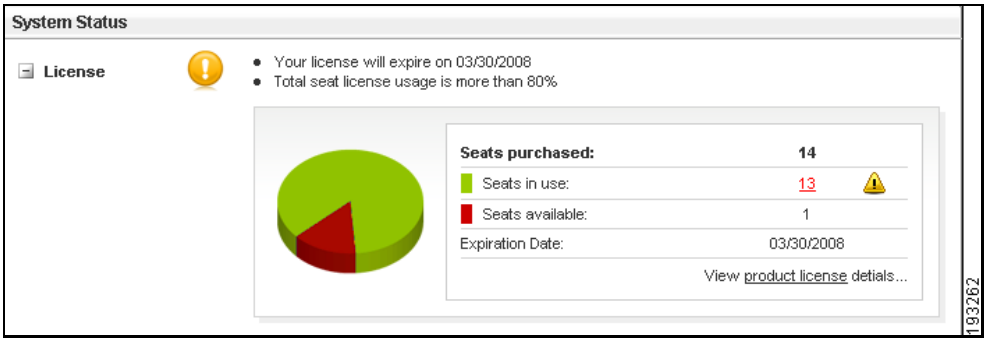
In the System Status section of the Summary page, you can view the status for the license and the file updates.

- **Licenses**: This section includes information about the number of seats purchased, the number of seats in use, and the number of seats available. It also provides information about the license expiration date.
- **Updates**: The updates summary provides the updates on the outdated computers in your network.

  NOTE Outdated computers are the computers that do not have latest virus pattern updates from WFBS-H.

To view the license information, click ⊞ next to the **License** sub-heading. A detailed graphical representation is displayed with information about the number of seats purchased, seats in use, seats available, and the Expiration date. **Figure 3** shows an example of the information that appears.

Figure 3 License System Status section



You can perform the following tasks:

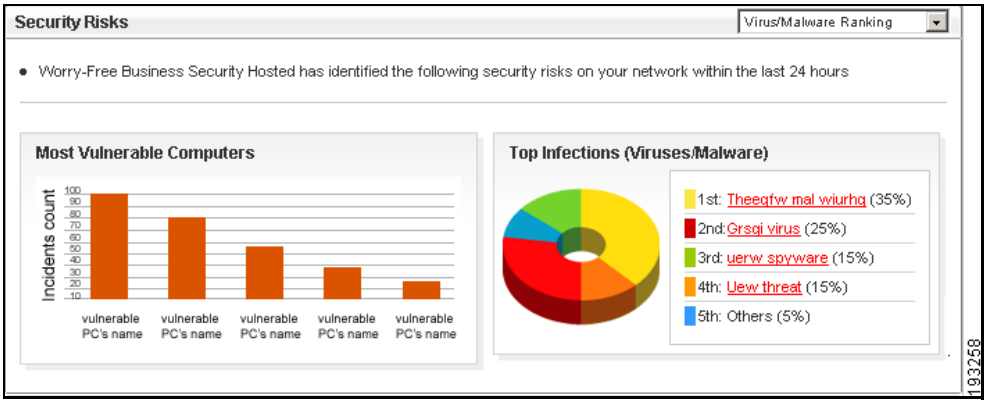
- Click the underlined seat count to view details about the name of each computer and the version of the installed WFBS-H Agent.
- Click the **product license** link to view details about the license.

Security Risks

The Security Risks section of the Summary page displays the status of the security risks found on your network. It displays a list of most common infections, which may include virus/malware, spyware/grayware, or malicious URLs. This section also displays a graphical representation of the most vulnerable computers on your network. You control the display by choosing one of the options from the drop-down list in the section heading:

- Virus/Malware Ranking
- Spyware/Grayware Ranking
- Malicious URLs Ranking

Figure 4 Security Risks section



Working with Packages

Packages are programs that install the agents on the client computers. Use WFBS-H to create, configure, and download packages to computers on your network.

NOTE After installing a package, it takes approximately one hour for the agents to start reporting to WFBS-H.

Refer to the following topics:

- **Creating New Packages, page 60**
- **Downloading Existing Packages, page 62**
- **Deleting Existing Packages, page 62**

WARNING Users can uninstall the Agent without a password.

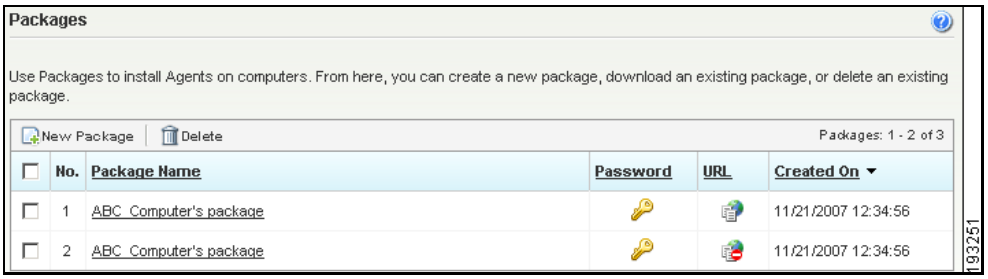
Creating New Packages

You can create new packages to store different connection settings. To create a new package:

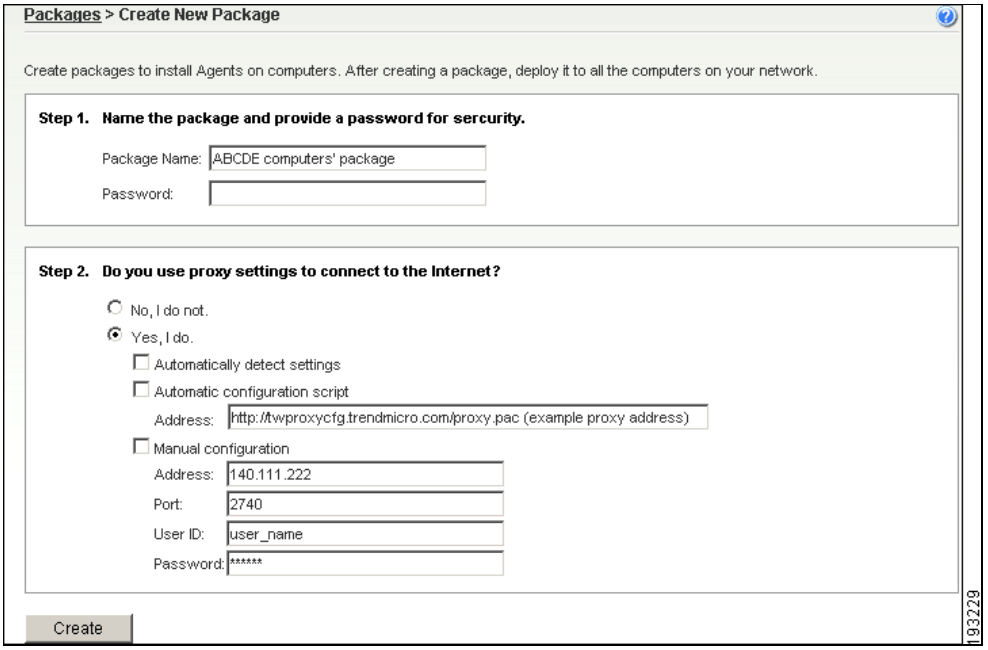
STEP 1 Launch the WFBS-H web portal.

NOTE For more information, see Launching the Web Portal, page 53.

STEP 2 Click the **Packages** tab.



STEP 3 Click the **New Package** button above the table.



STEP 4 Enter the following information:

- **Package Name**: Enter a name for the package.
- **Password**: Enter a password to be used when extracting the package.

- **Do you use proxy settings to connect to the Internet?**:
  - If you do not use proxy settings, click **No, I do not**.
  - If you use proxy settings, click **Yes, I do**. The configuration options appear.
- If you use proxy settings, select the required proxy settings for the agents to communicate with the WFBS-H server:
  - **Automatically detect settings:** Agent installer automatically detects the settings required to install the package.
  - **Automatic configuration script:** WFBS-H updates the location of the configuration script in the Address field. It uses the configuration script from this URL to install the package.
  - **Manual configuration**: WFBS-H updates the following proxy configuration in the Manual configuration field.
- If you chose manual configuration, enter the following information:
  - **Server IP Address**: Enter the IP address of the proxy server. You can get the IP address for the proxy server from the Internet Explorer settings.
  - **Port**: Enter the port number that is used by the proxy server for client connections.
  - **User ID**: Enter the account name used by the client machine to connect to the proxy server.
  - **Password:** Enter the password for the User ID.

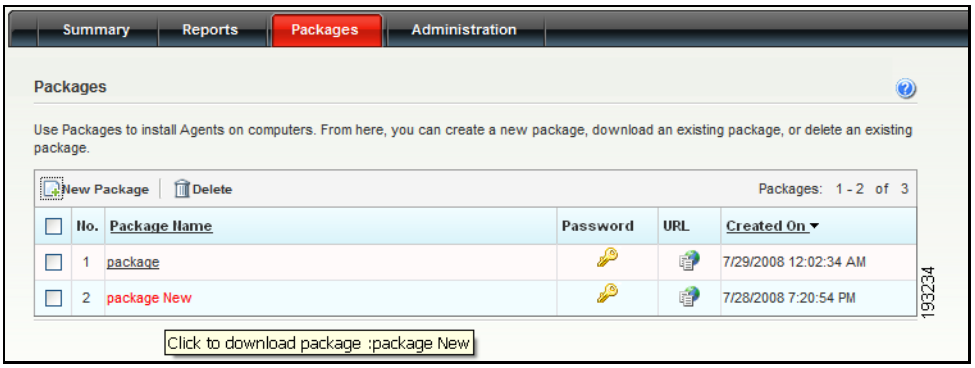
STEP 5 Click **Create**.

A link for a new package with specified name is created. Click the package name link to download the package.

Downloading Existing Packages

After creating a package, follow these steps to download these packages on computers you want to protect:

STEP 1 Launch the web portal, and then click the **Packages** tab to see this page.



STEP 2 Find the package that you want to download, and then click the link in the Package Name column.

A **File Download** dialog box appears.

STEP 3 Click **Save** to save the package on your machine.

STEP 4 Install these packages on computers you want to protect.

NOTE On Windows Vista computers, install the package with Administrator rights (using the **Run as administrator** option).

Deleting Existing Packages

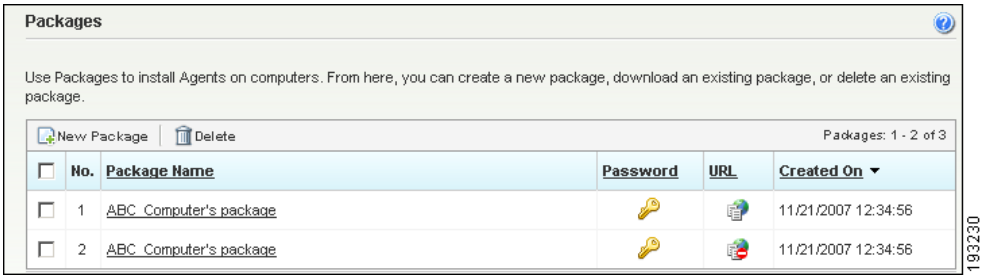
Follow these steps to delete an existing package:

STEP 1 Launch the WFBS-H web portal.

NOTE For more information, see **Launching the Web Portal, page 53**.

STEP 2 Click the **Packages** tab.

STEP 3 Check the box for each package that you want you want to delete. To select all packages, check the box at the top of the first column.



STEP 4 Click the **Delete** button above the table.

Working with Reports

Worry-Free Business Security Hosted allows you to create and view reports that contain detailed information about detected threats. Reports also include ranking to identify the most vulnerable computers. WFBS-H generates reports as a PDF.

You can generate a log query from the Reports page. A log query displays information about the virus/malware, spyware/grayware, or malicious URLs detected on your network for the specified time. It also provides detailed information about the names of the affected computers, threats, and affected files. It also lists the scan type and action taken on that particular threat.

Refer to the following topics:

- **Creating Reports, page 64**
- **Deleting Existing Reports, page 67**
- **Generating a Log Query, page 67**

Creating Reports

You can create a report for files and data that were collected during the previous 90 days.

NOTE WFBS-H stores files and data for a maximum of 90 days.

You can create reports for a specific time period or time zone depending on your needs. The reports contain the following information:

Time, date, and time zone for which the report is generated.

- **Virus/Malware Summary**:
  - The activities, number of incidents, and percentage of the virus/malware
  - Rankings for the virus/malware based on the number and percentage of incidents
  - A graphical representation of the activities
- Most Vulnerable Computers to Virus/Malware Infection:
  - A graphical representation of the virus/malware count for each computer
  - Rankings based on the number and percentage of incidents
- **Spyware/Grayware Summary**:
  - The activities, number of incidents and percentage of the spyware/grayware
  - Rankings for the spyware/grayware based on the number and percentage of incidents
  - A graphical representation of the activities
- **Most Vulnerable Computers to Spyware/Grayware**:
  - A graphical representation of the spyware/grayware count for each computer
  - Rankings for the computers based on the number and percentage of incidents

- **Malicious URL Summary**: Ranks malicious URLs based on number of incidents and percentage
- **Top Computers Accessing Malicious URLs**:
  - Rankings for computers based on the number of malicious URLs accessed
  - A graphical representation of the malicious URLs count for each computer

Follow these steps to create a new report:

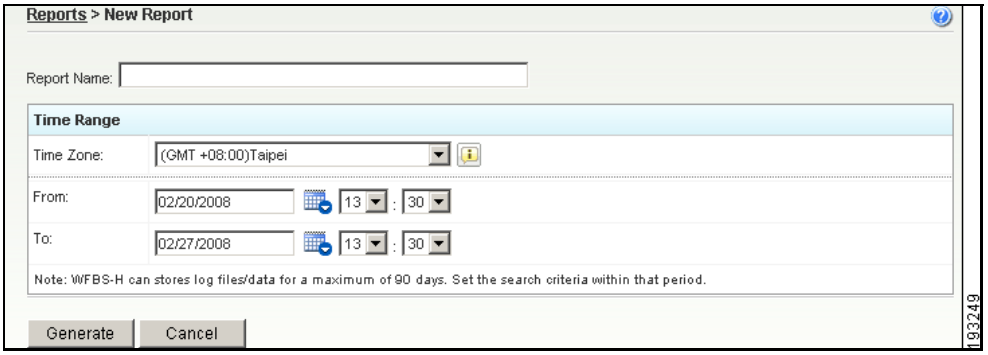
STEP 1 Launch the WFBS-H web portal.

NOTE For more information, see **Launching the Web Portal, page 53**.

STEP 2 Click the **Reports** tab.

The Reports page appears.

STEP 3 Click the **New Report** button above the table.



STEP 4 Enter the following information:

- **Report Name:** Enter a descriptive name for this report.
- **Time Range**: Choose the time zone, dates, and times for the content that you want to include in the report.
  - **Time Zone**: Choose the correct time zone for the location.
  - **From**: Choose the start date for the report contents by clicking the calendar icon. Enter the start time by using the drop-down lists for hours (0 to 24) and minutes (0 to 60).
  - **To**: Choose the end date for the report contents by clicking the calendar icon. Enter the end time by using the drop-down lists for hours (0 to 24) and minutes (0 to 60).

STEP 5 Click **Generate**. When the report is successfully generated, click the report name to view it. WFBS-H requires Adobe Acrobat Reader 7.0 or later to view reports.

STEP 6 If needed, save the report locally.

Deleting Existing Reports

WARNING Deleted reports cannot be recovered. Cisco recommends downloading reports before deleting them.

Follow these steps to delete an existing report:

STEP 1 Launch the WFBS-H web portal.

NOTE For more information, see **Launching the Web Portal, page 53**.

STEP 2 Click the **Reports** tab.

STEP 3 On the **Reports** page, check the box for each report that you want to delete. To select all reports, check the box at the top of the first column.

STEP 4 Click the **Delete** button above the table.

Generating a Log Query

A log query displays information about the virus/malware, spyware/grayware, or malicious URLs detected on your network at the specific time. It also provides detailed information about the names of computers, threats, files, scan type and action taken on that particular threat.

The data is exported in the CSV (Comma Separated Values) format, which can be open for analysis in various third-party spreadsheet programs and database programs.

WFBS-H can query the logs for the following types:

- Virus/Malware
- Spyware/Grayware
- Malicious URLs

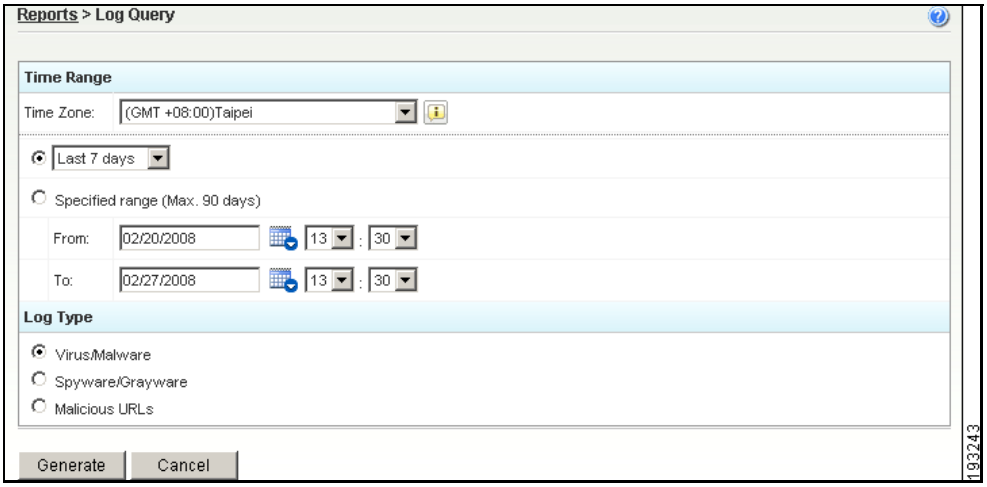
Follow these instructions to generate a log query:

STEP 1 Launch the WFBS-H web portal.

NOTE For more information, see **Launching the Web Portal, page 53**.

STEP 2 Click **Reports** tab.

STEP 3 Click the **Log Query** button above the table.



STEP 4 In the **Time Range** section, enter the following parameters for the query:

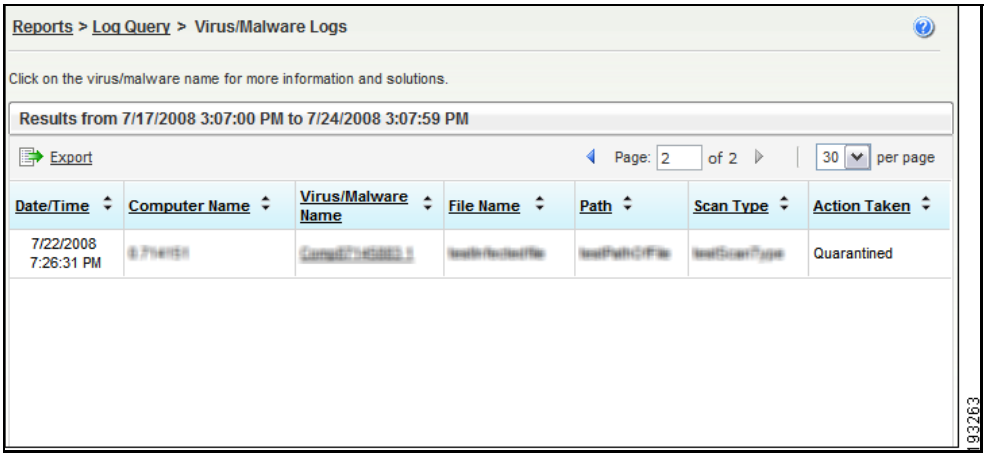
- **Time Zone**: Choose the correct time zone for the location.
- **Range**: Use the drop-down list or specify a range.
  - **Drop-down list**: Choose **All dates**, **Today**, **Last 7 days**, or **Last 30 days**.
  - **Specified Range**: Click the button and then enter the date range by specifying the **From** and **To** values. Choose the dates by clicking the calendar icons. Enter the times by using the drop-down lists for hours (0 to 24) and minutes (0 to 60).

    NOTE By default, the Last 7 days option is selected.

STEP 5 In the **Log Type** section, select the type of threat to include in the log: **Virus/ Malware, Spyware/Grayware**, or **Malicious URLs**.

STEP 6 Click **Generate**. A log for the selected type and time range is displayed.

The generated log contains information about the name of the virus/malware or spyware found in the specified time range, and actions taken.



NOTE By default, you can view 10 records per page. You can select the number of records you want to view from the per page list. You can also browse through the pages using the pagination option.

STEP 7 Click the **Export** button above the table to export the data in the CSV format.

Administering Cisco ProtectLink Endpoint

Worry-Free Business Security Hosted needs minimal administration. From the Administration page you can:

- View the product, license, and account related information. You can view when your license is expiring and renew your service agreement to protect your computers from the latest threats.
- Add or renew the service to the existing WFBS-H services using the Renewal/Additional Service link on the Administration page. The Administration page displays information about your activation code, product version, seats purchased, registration status, and license expiration date.

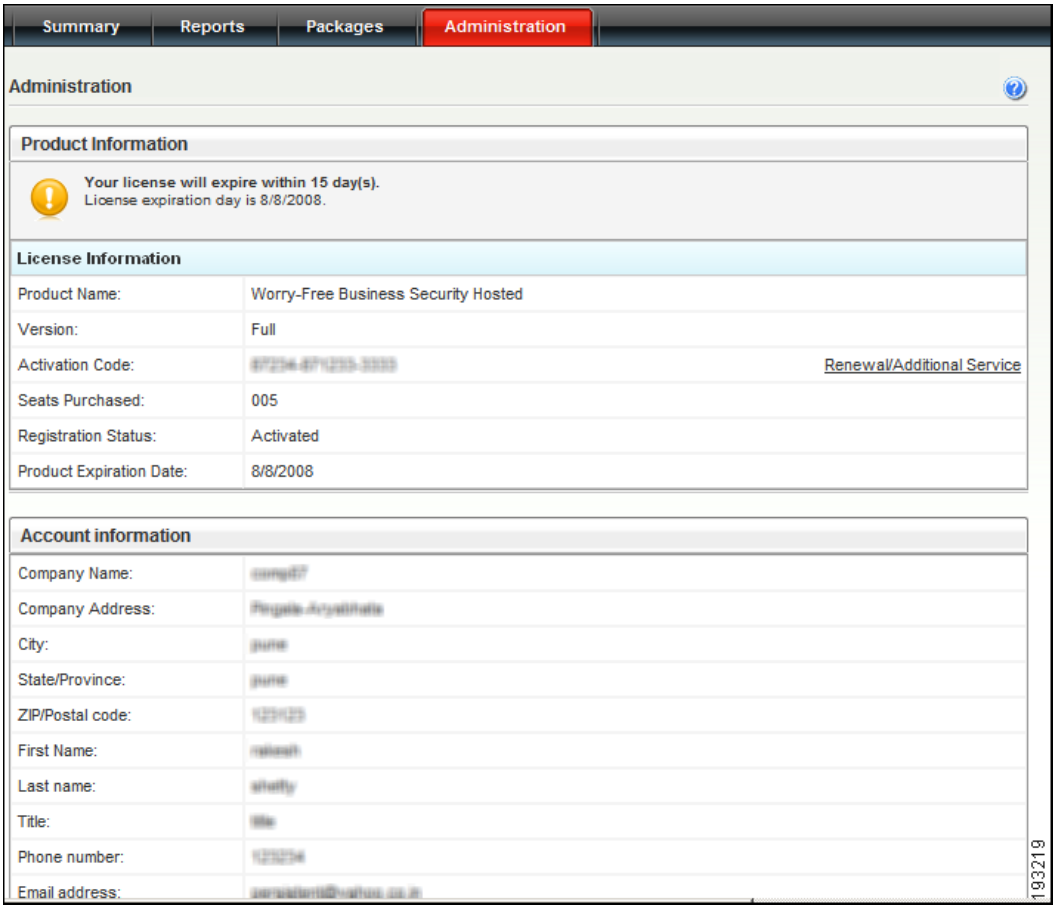
Managing Licenses

Follow these steps to renew or add a service:

STEP 1 Launch the WFBS-H web portal.

NOTE For more information, see **Launching the Web Portal, page 53**.

STEP 2 Click the **Administration** tab.



STEP 3 Click the **Renewal/Additional Service** link next to the activation code.

The registration website appears. You can renew your license on this website.

Using WFBS-H Agent Proxy Configuration Tool

If the proxy settings have changed, use the proxy configuration tool to reconfigure an Agent's proxy settings.

NOTE On Windows Vista computers, run this program as an Administrator.

Follow these steps to reconfigure an Agent's proxy settings:

STEP 1 On your computer, click the **Windows Start** button.

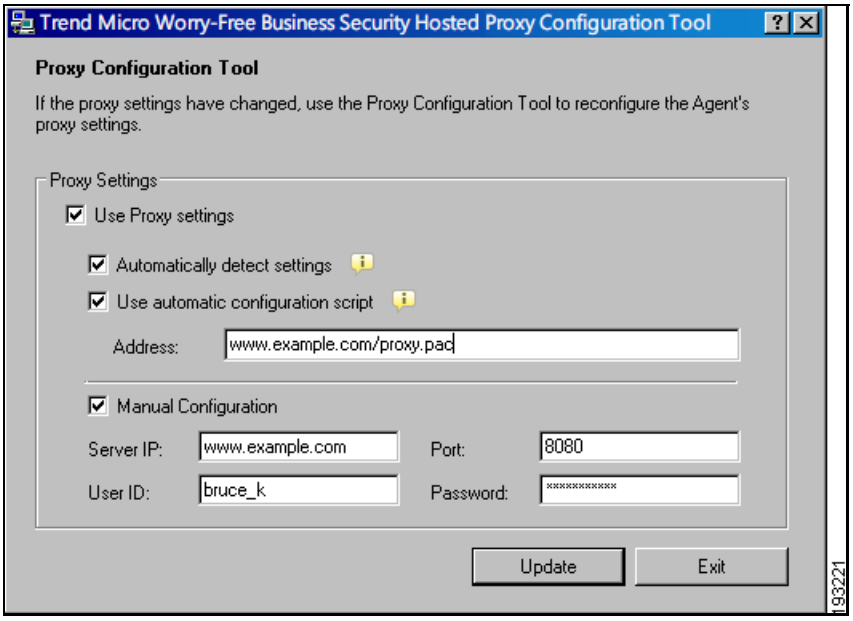
STEP 2 Choose **My Computer** and then choose the drive where you installed the files, typically Local Disk (C:).

A window appears, displaying the files and folders on the selected drive.

STEP 3 Open **Program Files > Trend Micro > RAgent**.

STEP 4 Double-click **ProxyCfg.exe**.

The Worry-Free Business Security Hosted Agent Proxy Configuration Tool window appears.



STEP 5 Configure the required connection options:

- **Automatically detect settings**: The Agent gets the settings from the DHCP and DNS.

- **Use automatic configuration script**: Enter the location of the configuration script in the Address text box.
- **Use HTTP Proxy**: Provide the Server IP, Port, User ID, and Password for the HTTP proxy.
- **Automatic configuration may override manual settings**: To ensure the use of manual settings, disable automatic configuration.

STEP 6 Click **Apply**. The changes take effect immediately.

5

Terminology

Computer security is a rapidly changing subject. Administrators and information security professionals invent and adopt a variety of terms and phrases to describe potential risks or uninvited incidents to computers and networks. The following is a discussion of these terms and their meanings as used in this document:

Viruses/Malware

A computer virus is a program that has the unique ability to replicate. Viruses can attach themselves to almost any type of executable file and are spread as files that are copied and sent from individual to individual. In addition to replication, some computer viruses also include a damage routine that delivers the virus payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage.

ProtectLink Endpoint can detect viruses/malware. The Cisco recommended action for viruses/malware is clean.

You should be aware of additional terms related to viruses and malware:

- Backdoors—A backdoor is a method of bypassing normal authentication, securing remote access to a computer, and/or obtaining access to information, while attempting to remain undetected.
- Macro Viruses—Macro viruses are application-specific. The viruses reside within files for applications such as Microsoft Word (.doc) and Microsoft Excel (.xls). Therefore, they can be detected in files with extensions common to macro capable applications such as .doc, .xls, and .ppt. Macro viruses travel amongst data files in the application and can eventually infect hundreds of files if undeterred.

- Malware—Malware is software designed to infiltrate or damage a computer system without the owner's consent.
- Rootkit—A rootkit is a set of programs designed to corrupt the legitimate control of an operating system by its users. Usually, a rootkit will obscure its installation and attempt to prevent its removal through a subversion of standard system security.
- Trojans—A Trojan is a malicious program that masquerades as a harmless application. Unlike viruses, Trojans do not replicate but can be just as destructive. An application that claims to rid your computer of viruses when it actually introduces viruses onto your computer is an example of a Trojan.
- Worms—A computer worm is a self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems. The propagation usually takes place through network connections or email attachments. Unlike viruses, worms do not need to attach themselves to host programs.

Spyware/Grayware

ProtectLink Endpoint can detect spyware/grayware. The Cisco recommended action for spyware/grayware is clean.

- Spyware—Spyware is computer software that is installed on a computer without the user's consent or knowledge and collects and transmits personal information.
- Grayware—Grayware is a program that performs unexpected or unauthorized actions. It is a general term used to refer to spyware, adware, dialers, joke programs, remote access tools, and any other unwelcome files and programs. Depending on its type, it may or may not include replicating and non-replicating malicious code.
- Adware—Adware, or advertising-supported software, is any software package, which automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while the application is being used.
- Bots—A bot (short for “robot”) is a program that operates as an agent for a user or another program or simulates a human activity. Bots, once executed, can replicate, compress, and distribute copies of themselves. Bots can be used to coordinate an automated attack on networked computers.

- Dialers—Dialers are necessary to connect to the Internet for non-broadband connections. Malicious dialers are designed to connect through premium-rate numbers instead of directly connecting to your ISP. Providers of these malicious dialers pocket the additional money. Other uses of dialers include transmitting personal information and downloading malicious software.
- Hacking Tools—A hacking tool is a program, or a set of programs, designed to assist hacking.
- Keyloggers—A keylogger is computer software that logs all the keystrokes of the user. This information could then be retrieved by a hacker and used for his/her personal use.

6

Post-Registration and Post-Activation Emails

Upon registering for Cisco ProtectLink Endpoint, you are automatically sent post-registration and post-activation emails that provide instructions on the next step. Below are samples of these emails.

This chapter contains the following sections:

Registration and Activation Email—ProtectLink Endpoint

```
Subject: Successful Cisco ProtectLink Endpoint - Registration

Greetings from Cisco!

You have successfully registered ProtectLink(TM) Endpoint – an online hosted
service powered by Trend Micro(TM) Worry-Free(TM) Business Security Hosted.

ProtectLink Endpoint comprises two modules:
* Worry-Free Business Security - Hosted
* Policy Enforcement
Worry-Free Business Security – Hosted has been activated. Refer to the
following instructions to activated Policy Enforcement:

1. From the security appliance's configuration page, click ProtectLink and
then click I have my Activation Code (AC) and want to activate ProtectLink
services.
2. Activate Policy Enforcement using the following Activation Code:
ProtectLink Endpoint Service:

Logon information
* ProtectLink Endpoint Web console URL: http://WFBS-H.trendmicro.com
* User name: #LOGINID#
* Password: #PWD#

To log onto the Worry-Free Business Security - Hosted console:
1. Access the ProtectLink Endpoint console URL to view the logon page.
2. Use the above logon information to log onto the console.
```

```
For more details, refer to the resources below:

* ProtectLink Administrator's Guide - <Link>
Tip: Refer to Chapter 2 of the Administrator's Guide to help you get started
using ProtectLink Endpoint.

* ProtectLink Endpoint landing page: http://www.trendmicro.com/go/wfbsh

If you have any technical issues with your product, please contact the Cisco
helpdesk.
http://www.cisco.com/support

Best regards,
Cisco

This message was automatically issued by the Cisco Registration services. The
account is not attended. Please do not reply to this message.
```

Policy Enforcement Activation

```
Greetings from Cisco!

Congratulations. You have successfully activated Cisco ProtectLink Endpoint -
Policy Enforcement.

Policy Enforcement is now active. From the security appliance's configuration
page, click ProtectLink > Desktop Protection > Policy Enforcement to
customize the settings.

To view your customer profile, modify your profile, or register additional
Cisco ProtectLink products, visit: https://olr.trendmicro.com/registration/

Logon ID: #Logon ID#

For more details, refer to the resources below:

* ProtectLink Administrator's Guide - <New Link>
Tip: Refer to Chapter 2 of the Administrator's Guide to help you get started
using ProtectLink Endpoint.

If you have any technical issues with your product, please contact the Cisco
helpdesk.
http://www.cisco.com/support

Best regards,
Cisco

This message was automatically issued by the Cisco Registration services. The
account is not attended. Please do not reply to this message.
```

A

Where to Go From Here

Cisco provides a wide range of resources to help you and your customer obtain the full benefits of the <edit PRODUCT NAME>.

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