SecureWay™ Firewall Plus for Tivoli®

User's Guide

Version 1.2

July 2000

First Edition

ITM-SWF-TIVG-1.2

Legal Notices

Copyright Notice

Warranty Notice

NOTICE: The information and specifications in this document are subject to change without notice. Please consult your IT Masters representative for the latest edition or supplements that are applicable and current. This document is intended to present a clear and comprehensive guide to the use of the product it describes. IT Masters, however, makes no representation or warranty except as outlined in the product License Agreement.

Trademark Notices

IT Masters and the IT Masters logo are trademarks or registered trademarks of IT Masters.

Tivoli Management Environment, Tivoli Management Framework, Tivoli Management Platform, Tivoli Enterprise Console, Tivoli Manager, Tivoli Plus, Tivoli Sentry, TME, and TME 10 are trademarks or registered trademarks of Tivoli Systems, Inc.

SecureWay and eNetwork are trademarks of International Business Machines Corporation in the United States or other countries or both. AIX, RS/6000, TrackPoint, S/390, AIX/6000, and AS/400 are registered trademarks of International Business Machines Corporation in the United States or other countries or both. All other trademarks or registered trademarks are the property of their respective owners.

Preface

The SecureWay Firewall Plus for Tivoli User’s Guide describes specific features and procedures for using the SecureWay™ Firewall Plus for Tivoli® (“Firewall Plus”) module. This module provides an integration of IBM Corporation’s IBM SecureWay™ Firewall version 4.1 (“IBM SecureWay Firewall”) product with the Tivoli Management Environment™ (TME 10™) product. Through this integration, the Firewall Plus module delivers the system management capabilities of the TME 10 product for specific use with the IBM SecureWay Firewall product. Through this integration the Firewall Plus module provides management capabilities across a multiplatform network.

Who should read this guide

This guide is for system administrators who use the Firewall Plus module to manage the operation of the SecureWay Firewall product. Readers of this guide should be familiar with the Tivoli TME 10 product, the IBM SecureWay Firewall product, and concepts such as directories, files, and symbolic links. Readers of this guide should also be familiar with the operating systems running on the machines on which they will be using the Firewall Plus module, the TME 10 product, and the IBM SecureWay Firewall application.

Prerequisite and related documents

The information in the SecureWay Firewall Plus for Tivoli User’s Guide complements information presented in the

- *IBM SecureWay Firewall User’s Guide for Windows NT,*
- *IBM SecureWay Firewall Reference for Windows NT,*
- *IBM SecureWay Firewall User’s Guide for AIX,*
- *IBM SecureWay Firewall Reference for AIX,*
- *Tivoli TME 10 Framework User’s Guide, and*
- *Tivoli Plus User’s Guide.*

You should be familiar with these guides before attempting to use the information in the SecureWay Firewall Plus for Tivoli User’s Guide.

What this guide contains

The SecureWay Firewall Plus for Tivoli User's Guide contains the following chapters:

- Chapter 1, "Getting Started."
- Chapter 2, "Features of the Firewall Plus Module."
- Chapter 3, "Software Distribution."
- Chapter 4, "Distributed Monitoring."
- Chapter 5, "TEC Events."
- Chapter 6, "Task Operations."
- Chapter 7, "Uninstalling the Firewall Plus Product."

Typeface conventions

- Key names appear in small capital letters: ESCAPE, ENTER
- The following appear in monoface font:
  - Path names and URLs

    `www.itmasters.com, C:\Program Files\IT Masters`
  - Code and executables

    `mcstat -n <CellName>`
  - File names that are part of a path name:

    `MCELL_HOME/etc/mcell.dir`
- File names not part of a path are in boldface (**config.sys**) and GUI elements such as buttons, fields, and menu options: **Add** button, **Source** field, **Add Cell** menu option

Contacting customer support

Americas (USA, Canada, Central, and South America) and Pacific Rim

- Toll-Free Phone within USA: 1-888-ITM-0234
- Phone Outside USA: 1-512-219-5086
- Fax: 1-512-219-5087
- E-mail: `support@us.itmasters.com`

EMEA

- Phone: +32-16-39-64-44
- Fax: +32-16-39-64-74
- E-mail: `support@itmasters.com`

General information

General information about IT Masters and our products can be obtained from our Web site:

```
http://www.itmasters.com/
```

Comments on this document

Please address any questions or comments you may have regarding this document to the IT Masters documentation department at:

```
docs@us.itmasters.com
```

Contents

1 Getting Started

The Firewall Plus module provides an integration of the Tivoli Management Environment product with the IBM SecureWay Firewall 4.2 (“IBM SecureWay Firewall”) product. This module provides the following features for managing the IBM SecureWay Firewall product:

- Subscription lists for clients and servers
- SecureWay Firewall application distribution and installation
- Monitoring of key processes or services
- Monitoring SecureWay Firewall clients through the Tivoli Enterprise Console
- Tasks and jobs for starting and stopping processes or services from the Tivoli desktop

Caution Be certain you have a current backup of the Tivoli database and the Tivoli binary directories before proceeding.

Note

The Tivoli Software Distribution application, the Tivoli Distributed Monitoring application, and the Tivoli Enterprise Console application must be installed and configured before their corresponding Firewall Plus module functions are operational. If the Firewall Plus module is installed before these Tivoli applications are installed, you must reinstall the Firewall Plus module in order for these features to be operational.

Installation requirements

Before attempting to install the Firewall Plus module into the Tivoli Management Environment product, make certain you review the requirements in this section. Also review the *SecureWay Firewall Plus for Tivoli Release Notes* shipped with the product.

The following table provides the context and authorization role required to install the Firewall Plus module.

Activity	Context	Required Role
Installing Firewall Plus	TME	**super**

In order for the Firewall Plus module to function correctly, it must be installed on the following machines:

- The TMR (Tivoli Managed Region) server
- The TEC server
- The IBM SecureWay Firewall server. This server can be either a Tivoli managed node or an LCF (Light Client Framework) endpoint
- Any Tivoli managed nodes that also act as gateways and service endpoints that have a need for some or all of the Firewall Plus module's features. These managed nodes must also have the Tivoli Enterprise Console Adapter Configuration Facility installed

Software requirements

The Firewall Plus module has features that use the Tivoli Software Distribution application, the Tivoli Distributed Monitoring application, the TME 10 Enterprise Console, the TME 10 Enterprise Console interface, and the TME 10 Enterprise Console Adapter Configuration Facility. If these applications are not installed, then the icons referring to these features do not display on the desktop and many of the components do not function correctly.

Area	Requirement
TME Distributed Monitoring TME 10 Software Distribution TME 10 Enterprise Console TME 10 Framework	Version 3.6, 3.6.1 or 3.6.2 for all four
IBM SecureWay Firewall 4.2 software	AIX 4.3.2 or 4.3.3 Windows NT 4.0, service pack 4, 5 and 6

Hardware requirements

The following table provides the client and server disk space requirements for the Firewall Plus module.

Supported Platform	Libraries	Binaries	Database	Man Pages	Message Catalogs
AIX	0 MB	635 KB	† 0	0 MB	18 KB
Windows NT	0 MB	635 KB	† 0	0 MB	18 KB

† Not Appreciable

Upgrading to 1.2 of the SecureWay Firewall Plus Module

You must back up the Tivoli database before removing the previous version of the SecureWay Firewall Plus module. It is highly *recommended* that you also have a current backup of the Tivoli binary directories.

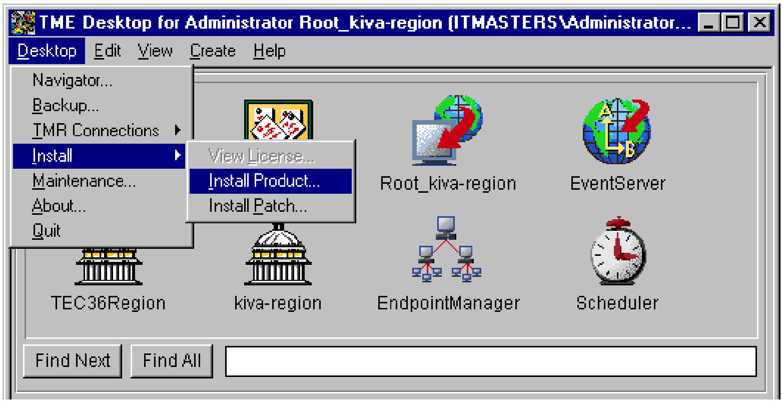
Upgrading from Version 1.1

In order to upgrade from version 1.1 of the SecureWay Firewall Plus module, please follow the instructions from Chapter 7 of this user’s guide, “Uninstalling the Firewall Plus Product” on page 75. After you have uninstalled the 1.1 module, you may proceed to the next section in order to install the 1.2 version of the module.

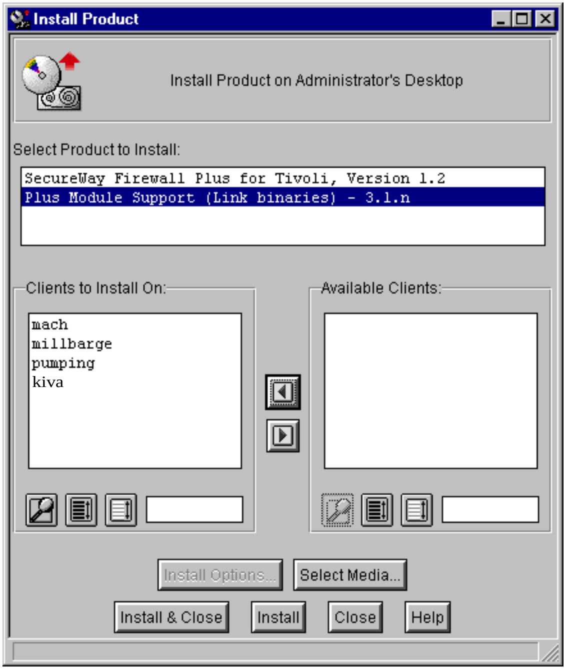
Installing from the desktop

Use the following steps to install the Firewall Plus module from the Tivoli desktop:

1 Select **Desktop** > **Install** > **Install Product...** .



This option displays the Install Product window.



Install Product

Install Product on Administrator's Desktop

Select Product to Install:

```
SecureWay Firewall Plus for Tivoli, Version 1.2
Plus Module Support (Link binaries) - 3.1.n
```

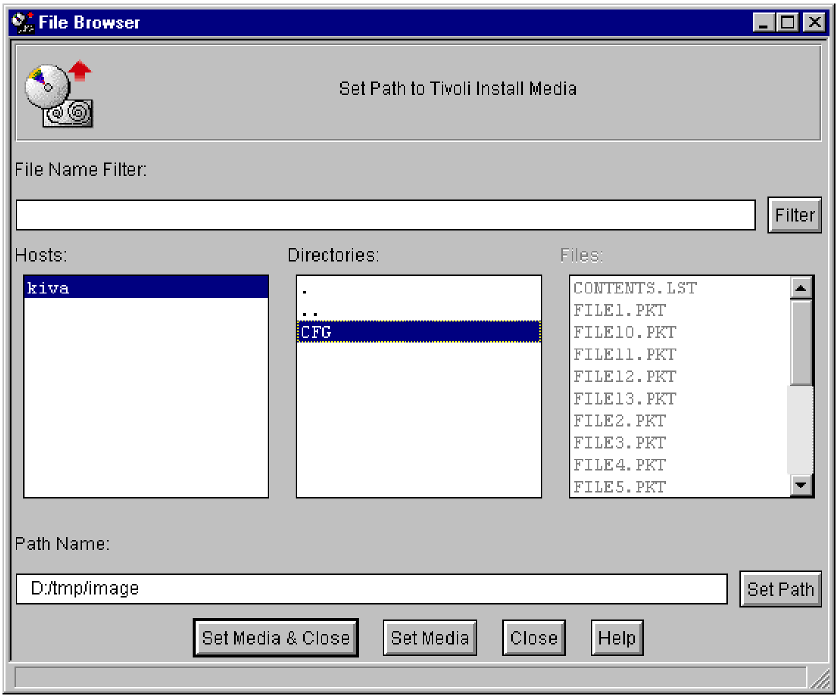
Clients to Install On:

```
mach
millbarge
pumping
kiva
```

Available Clients:

If the Firewall Plus module and the Plus Module Support link binary files are listed in the **Select Product to Install** scrolling list, skip to step 3. If they are not listed, proceed to step 2.

2 Click on the **Select Media...** button to display the File Browser window.



File Name Filter:

Hosts:

kiva

Directories:

.
..
CFG

Files:

CONTENTS.LST
FILE1.PKT
FILE10.PKT
FILE11.PKT
FILE12.PKT
FILE13.PKT
FILE2.PKT
FILE3.PKT
FILE4.PKT
FILE5.PKT

Path Name: D:/tmp/image

The File Browser window enables you to identify or specify the path to the installation media.

If you already know the path to the CD-ROM image:

a. Enter the full path in the **Path Name** field.

b. Click the **Set Path** button to change the path to the specified directory.

c. Click the **Set Media & Close** button to save the new media path and return to the Install Product window. The window now contains a list of products that are available for installation.

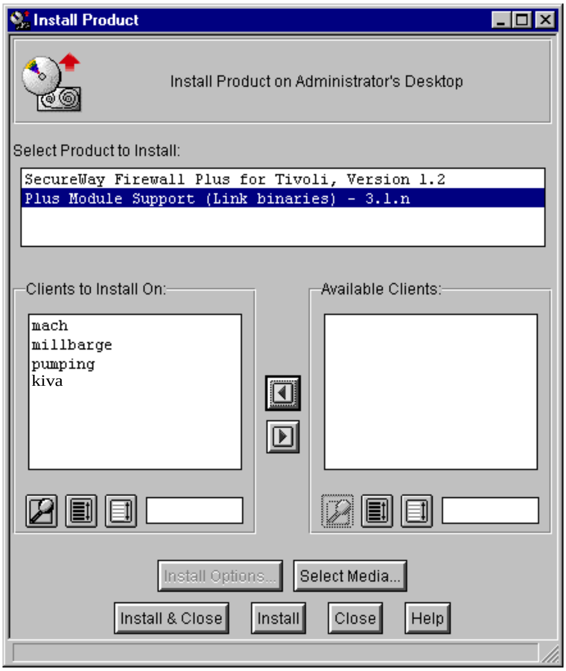
If you do not know the exact path to the CD-ROM image:

a. Select the host on which the install media is mounted from the **Host** scrolling list. Selecting a host updates the **Directories** scrolling list to show the directories of the host you chose.

b. Select the directory containing the install media from the **Directories** scrolling list.

c. Click the **Set Media & Close** button to save the new media path and return to the Install Product window. The window now contains a list of products that are available for installation.

3 Select **Plus Module Support (link binary files)** from the **Select Product to Install** list.



Select Product to Install:

```
SecureWay Firewall Plus for Tivoli, Version 1.2
Plus Module Support (Link binaries) - 3.1.n
```

Clients to Install On:

```
mach
millbarge
pumping
kiva
```

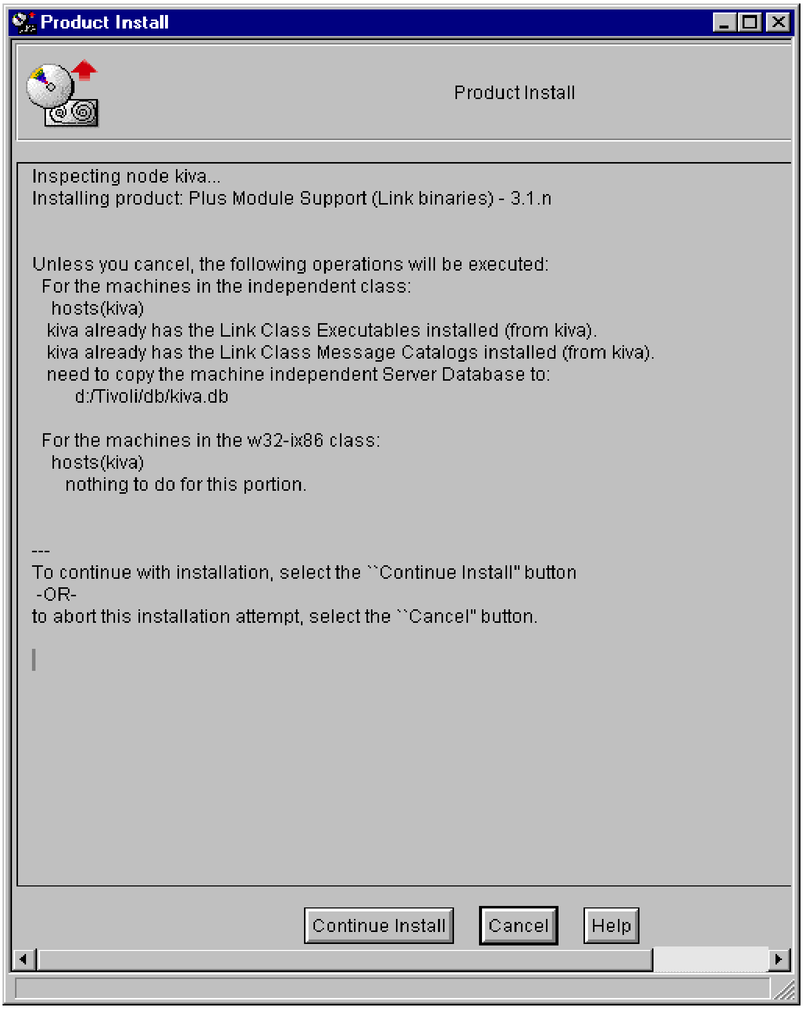
Available Clients:

4 Click the **Install & Close** button to install the link binary files and close the Install Product window.

— OR —

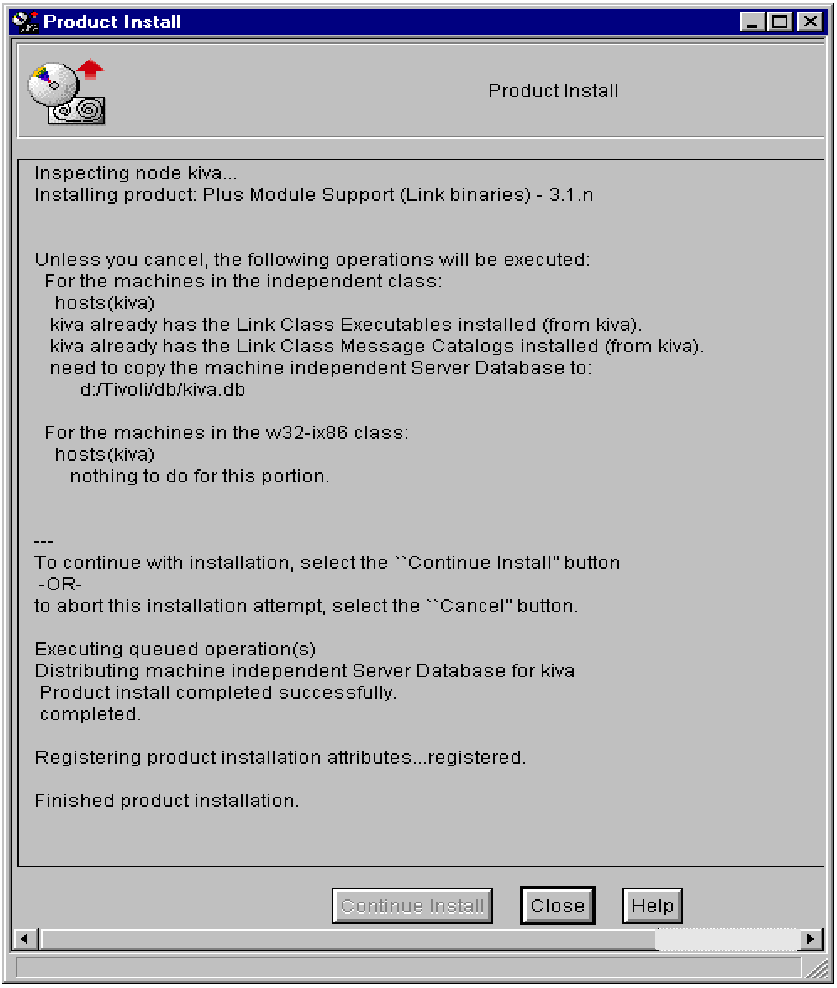
Click the **Install** button to install the link binary files and keep the Install Product window open. You can then install the Firewall Plus module on another set of clients, or you can install another product.

The installation process prompts you with a Product Install window similar to the following:



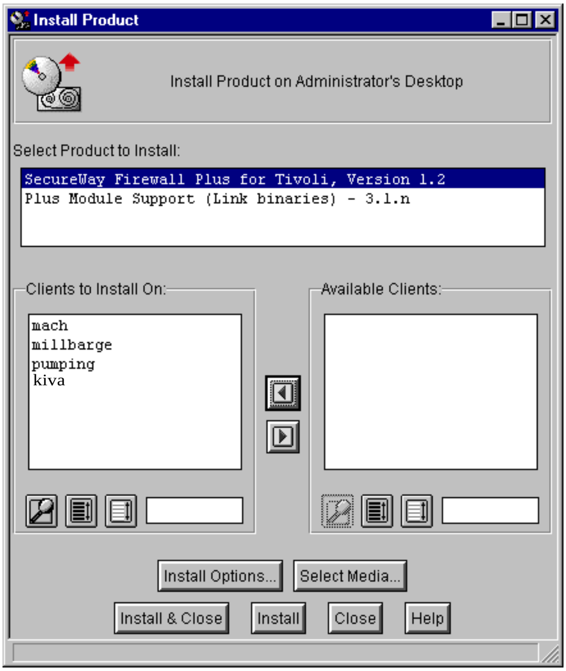
```
Inspecting node kiva...
Installing product: Plus Module Support (Link binaries) - 3.1.n


Unless you cancel, the following operations will be executed:
 For the machines in the independent class:
  hosts(kiva)
  kiva already has the Link Class Executables installed (from kiva).
  kiva already has the Link Class Message Catalogs installed (from kiva).
  need to copy the machine independent Server Database to:
      d:/Tivoli/db/kiva.db

 For the machines in the w32-ix86 class:
  hosts(kiva)
    nothing to do for this portion.


---
To continue with installation, select the ``Continue Install'' button
 -OR-
to abort this installation attempt, select the ``Cancel'' button.
```

This window provides the list of operations that take place when installing the software. This window also warns you of any problems that you may want to correct before you install the **Plus Module Support (link binary files)**.



```
Inspecting node kiva...
Installing product: Plus Module Support (Link binaries) - 3.1.n


Unless you cancel, the following operations will be executed:
 For the machines in the independent class:
  hosts(kiva)
   kiva already has the Link Class Executables installed (from kiva).
   kiva already has the Link Class Message Catalogs installed (from kiva).
   need to copy the machine independent Server Database to:
      d:/Tivoli/db/kiva.db

 For the machines in the w32-ix86 class:
  hosts(kiva)
     nothing to do for this portion.


---
To continue with installation, select the ``Continue Install'' button
 -OR-
to abort this installation attempt, select the ``Cancel'' button.

Executing queued operation(s)
Distributing machine independent Server Database for kiva
 Product install completed successfully.
 completed.

Registering product installation attributes...registered.

Finished product installation.
```

5 Select the **SecureWay Firewall Plus for Tivoli** entry from the **Select Product to Install** list.



Select Product to Install:

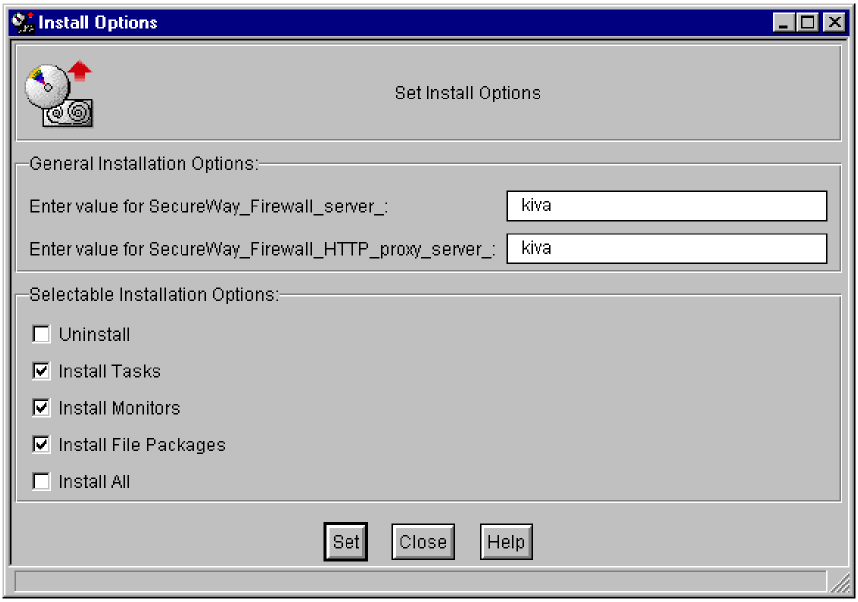
SecureWay Firewall Plus for Tivoli, Version 1.2
Plus Module Support (Link binaries) - 3.1.n

Clients to Install On:

mach
millbarge
pumping
kiva

Available Clients:

The Install Options dialog displays.



Set Install Options

General Installation Options:

Enter value for SecureWay_Firewall_server_: kiva

Enter value for SecureWay_Firewall_HTTP_proxy_server_: kiva

Selectable Installation Options:

☐ Uninstall

☑ Install Tasks

☑ Install Monitors

☑ Install File Packages

☐ Install All

The install options are:

a. **SecureWay Firewall Server**- The host name of the machine on which the IBM SecureWay Firewall product is installed.

b. **SecureWay Firewall HTTP Proxy**- The host name of the machine on which the IBM SecureWay Firewall HTTP proxy is installed.

c. In the **Selectable Installation Options** portion of the Set Install Options dialog do ***not*** check the **Uninstall** checkbox. Instead, choose *one* of the following:

- **Install Monitors** checkbox.
- **Install Tasks** checkbox.
- **Install File Packages** checkbox.

–OR–

- **Install All** checkbox to install the module in its entirety.

d. When finished click the **Set** button to return to the Install Product window.

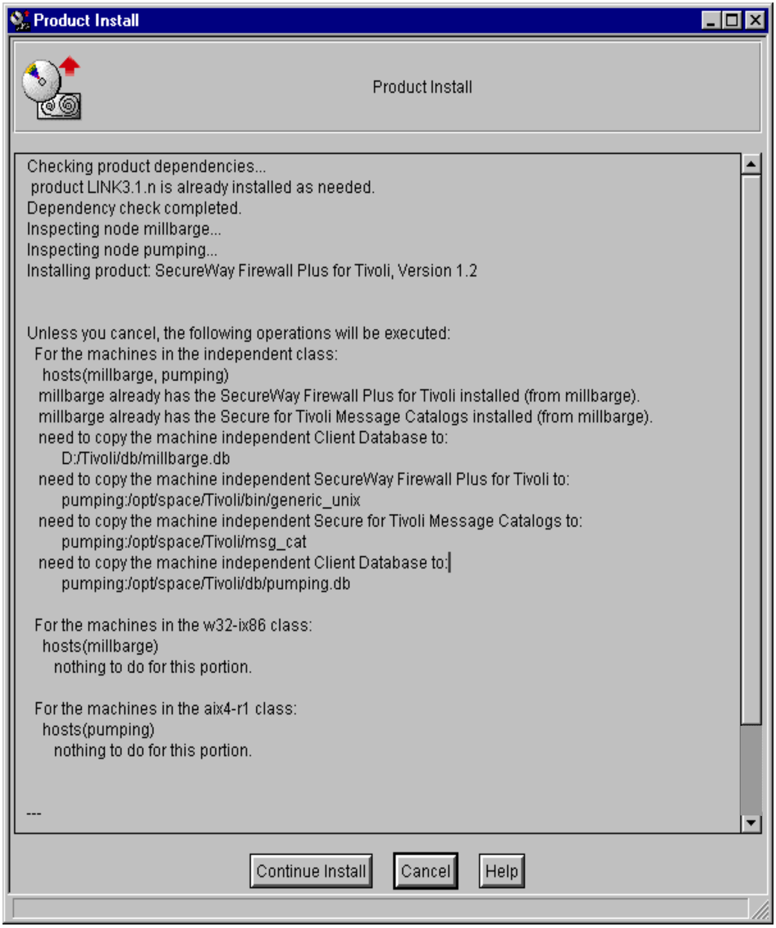
Note

If the IBM SecureWay Firewall server changes machines after the Firewall Plus module has been installed, you can reset these values by double-clicking on the **Set Install Options** icon in the Firewall Plus collection once the module has been completely installed.

6 Specify the clients on which the module will be installed by using the arrow keys to move machine names between the **Clients to Install On** scrolling list and the **Available Clients** scrolling list.

By default, all machines in the current Tivoli Management Region are listed in the **Clients to Install On** scrolling list. Move a machine name to the **Available Clients** list by choosing one or more clients from the **Clients to Install On** scrolling list and clicking the **left-arrow** button. The chosen clients are moved to the **Available Clients s**crolling list.

7 Click the **Install** button to begin the installation process.

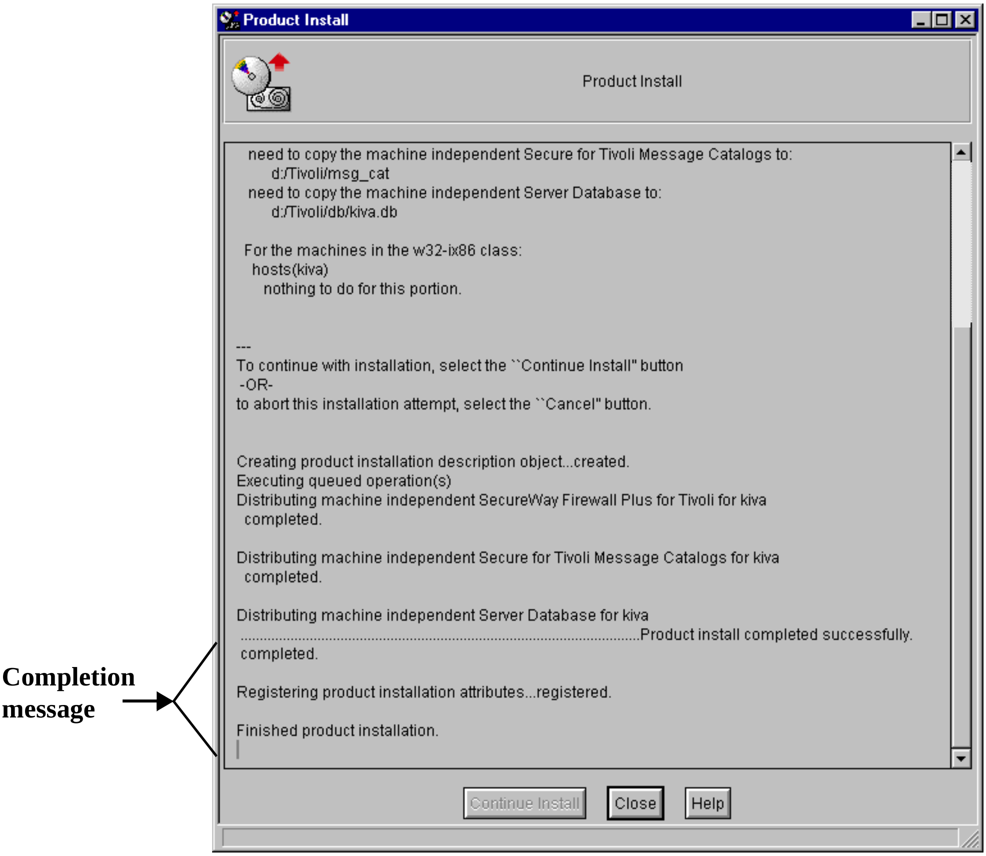


```
Checking product dependencies...
 product LINK3.1.n is already installed as needed.
Dependency check completed.
Inspecting node millbarge...
Inspecting node pumping...
Installing product: SecureWay Firewall Plus for Tivoli, Version 1.2


Unless you cancel, the following operations will be executed:
  For the machines in the independent class:
    hosts(millbarge, pumping)
   millbarge already has the SecureWay Firewall Plus for Tivoli installed (from millbarge).
   millbarge already has the Secure for Tivoli Message Catalogs installed (from millbarge).
   need to copy the machine independent Client Database to:
         D:/Tivoli/db/millbarge.db
   need to copy the machine independent SecureWay Firewall Plus for Tivoli to:
         pumping:/opt/space/Tivoli/bin/generic_unix
   need to copy the machine independent Secure for Tivoli Message Catalogs to:
         pumping:/opt/space/Tivoli/msg_cat
   need to copy the machine independent Client Database to:
         pumping:/opt/space/Tivoli/db/pumping.db

  For the machines in the w32-ix86 class:
    hosts(millbarge)
       nothing to do for this portion.

  For the machines in the aix4-r1 class:
    hosts(pumping)
       nothing to do for this portion.


---
```

—OR—

Click the **Cancel** button to abort the installation process.

When the installation is complete, the Product Install window displays a completion message similar to the following.



```
  need to copy the machine independent Secure for Tivoli Message Catalogs to:
      d:/Tivoli/msg_cat
  need to copy the machine independent Server Database to:
      d:/Tivoli/db/kiva.db

 For the machines in the w32-ix86 class:
   hosts(kiva)
     nothing to do for this portion.


---
To continue with installation, select the ``Continue Install" button
 -OR-
to abort this installation attempt, select the ``Cancel" button.


Creating product installation description object...created.
Executing queued operation(s)
Distributing machine independent SecureWay Firewall Plus for Tivoli for kiva
  completed.

Distributing machine independent Secure for Tivoli Message Catalogs for kiva
  completed.

Distributing machine independent Server Database for kiva
 ..........................................................................................Product install completed successfully.
 completed.

Registering product installation attributes...registered.

Finished product installation.
```

8 Click the **Close** button when the Product Install status window indicates that the installation is complete.

Installing from the command line

The following example command installs the Firewall Plus module:

```
winstall -c cdrom_path [managed node] \
-i index_file DOTASKS=1 DOMONS=1 DOFPS=1 \
SecureWay_Firewall_Server_=[Firewall Server hostname] \
SecureWay_Firewall_HTTP_proxy_server_=[Firewall HTTP Server
hostname]
```

where:

-c *cdrom_path* — Specifies the path to the CD-ROM image.

-i *index_file* — Specifies the index file from which the product is to be installed.

managed node — Specifies the node on which to install. If no managed node is specified, the module is installed on all managed nodes.

DOTASKS=1 — Specifies that the module's tasks are to be removed. This item is optional and can be omitted if you do not wish to uninstall the module's tasks.

DOMONS=1 — Specifies that the module's monitors are to be removed. This item is optional and can be omitted if you do not wish to uninstall the module's monitors.

DOFPS=1 — Specifies that the module's file packages are to be removed. This item is optional and can be omitted if you do not wish to uninstall the module's file packages.

`SecureWay_Firewall_server_ = [Firewall serer hostname]`

Specifies the hostname of the SecureWay Firewall Server.

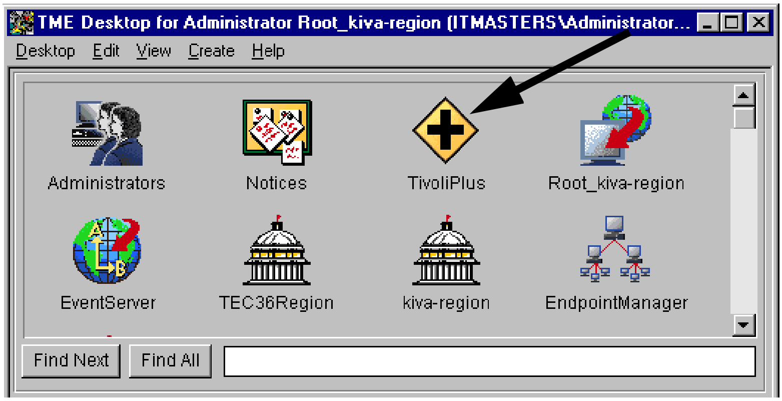
`SecureWay_Firewall_HTTP_proxy_server_ = [Firewall HTTP sever hostname]`

Specifies the hostname of the SecureWay Firewall HTTP proxy server.

See the `winstall` command in the *Tivoli Management Platform Reference Manual* for more information.

Viewing the Firewall Plus module

All Tivoli Plus modules are kept in a collection under the **TivoliPlus** icon. The following icon represents the TivoliPlus collection:



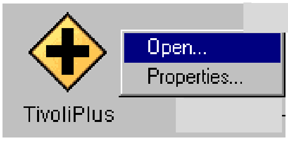
After the Firewall Plus module is installed, its components appear in the TivoliPlus collection. Also, all of the solutions associated with this specific integration module are placed in the TivoliPlus collection.

Use the following steps to view the solutions provided by the Firewall Plus module:

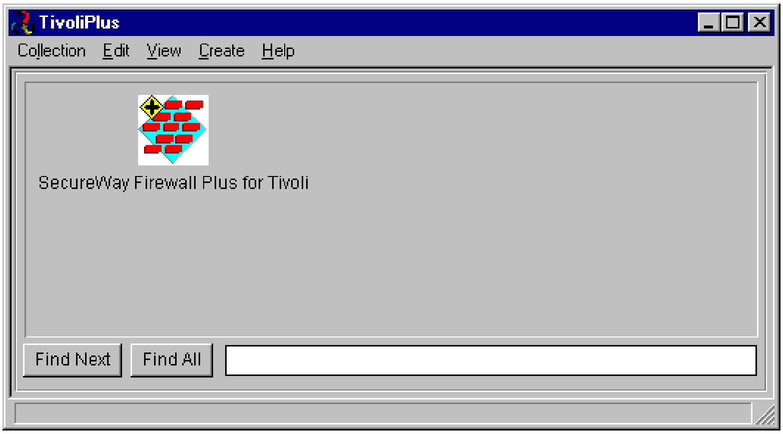
1 From the TME desktop, double-click on the **TivoliPlus** icon

—OR—

Select **Open** from the **TivoliPlus** icon pop-up menu



to display the TivoliPlus window.

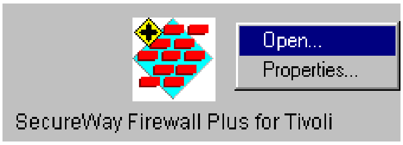

TivoliPlus
Collection Edit View Create Help
SecureWay Firewall Plus for Tivoli
Find Next
Find All

The TivoliPlus window displays all the Tivoli Plus module solutions that are presently installed.

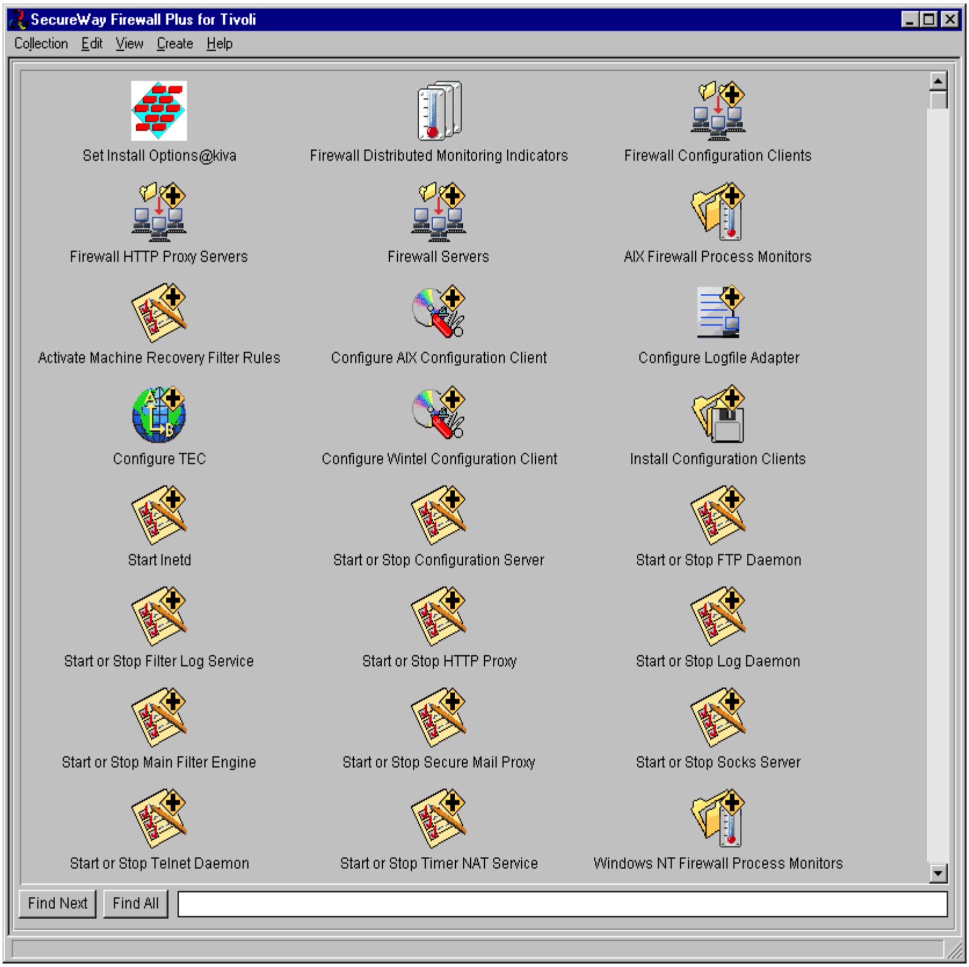
2 Open the Firewall Plus module window by double-clicking on the icon

—OR—

Select **Open** from the **Firewall Plus** icon pop-up menu



to display the Firewall Plus window, which contains the icons for the Firewall Plus integration module.


SecureWay Firewall Plus for Tivoli
Collection Edit View Create Help
Set Install Options@kiva
Firewall Distributed Monitoring Indicators
Firewall Configuration Clients
Firewall HTTP Proxy Servers
Firewall Servers
AIX Firewall Process Monitors
Activate Machine Recovery Filter Rules
Configure AIX Configuration Client
Configure Logfile Adapter
Configure TEC
Configure Wintel Configuration Client
Install Configuration Clients
Start Inetd
Start or Stop Configuration Server
Start or Stop FTP Daemon
Start or Stop Filter Log Service
Start or Stop HTTP Proxy
Start or Stop Log Daemon
Start or Stop Main Filter Engine
Start or Stop Secure Mail Proxy
Start or Stop Socks Server
Start or Stop Telnet Daemon
Start or Stop Timer NAT Service
Windows NT Firewall Process Monitors
Find Next
Find All

2 Features of the Firewall Plus Module

The Firewall Plus module provides numerous pre-configured, custom solutions to help you manage the IBM SecureWay Firewall product. The Firewall Plus module provides you with the *out-of-the-box* ability to use both the Tivoli and the IBM SecureWay Firewall applications simultaneously to identify potential problems, determine the source, and respond quickly.

The Firewall Plus module

The Firewall Plus module provides a centralized configuration mechanism for the deployment of all out-of-the-box solutions for the Firewall Plus module. The module includes the following:

- A task to configure IBM SecureWay Firewall interface with the TEC software
- Two tasks to configure the client distributions of the IBM SecureWay Firewall application to AIX and Windows machines
- Three subscriber lists for the IBM SecureWay Firewall client and servers
- Tivoli Software Distribution hierarchical file package for distributing the IBM SecureWay Firewall client application clients to Windows and AIX platforms
- Twelve Tivoli tasks for automating common, repetitive IBM SecureWay Firewall activities
- Two Tivoli Distributed Monitoring collections, one each for Windows and AIX, to hold the IBM SecureWay Firewall monitor feedback.
- One logfile adapter to monitor the SecureWay Firewall logfile and send to the TEC server the events that are generated from specific logfile messages and a task to configure it.

Note

Each Tivoli application must be installed and configured *before* the Firewall Plus collection will contain icons/tasks pertaining to them.

Although each Firewall Plus module also includes a TEC adapter, various filters, and event correlation rules, these only appear on the Enterprise Console itself.

Profile manager subscription lists

A profile is a set of application-specific information about a particular type of resource, as defined by the Tivoli TME 10 product. A profile is created in the context of a profile manager. The profile manager is a TME 10 software entity that links a profile to a set of resources called “subscribers.” Subscribers can be managed nodes or other profile managers and can contain profiles of multiple types, or multiple profiles of the same type.

The TME 10 administrators organize and distribute profiles via the profile manager(s). A profile manager is created in the context of a policy region and is a managed resource in the policy region of the TME 10 resource that uses the profile’s information. A profile, itself, has no direct subscribers.

The Firewall Plus module includes pre-configured subscription lists for both clients and servers, called **Firewall Configuration Clients**, **Firewall HTTP Proxy Servers**, and **Firewall Servers**.

Most of the pre-configured solutions provided by the Firewall Plus module use the client and server subscription lists as the default for their distributions. Although each solution can be distributed to a separate set of subscribers, we recommend you set up these subscription lists initially and use them for the majority of your distributions for consistency.

3 Software Distribution

The Firewall Plus module helps you manage, monitor, and distribute software across a multi-platform network.

The Firewall Plus module includes a hierarchical, pre-configured Tivoli Software Distribution file package for distributing and installing the IBM SecureWay Firewall client software. The Firewall Plus software supports AIX platforms, as well as Windows NT 4.0.

Tivoli software distribution setup

After the Firewall Plus module has been successfully installed, you must configure the location of the installation directories so you can set up the Tivoli Software Distribution file packages for each platform type. This allows the Tivoli Software Distribution file packages to locate the installation binary files. There are two IBM SecureWay Firewall
CD-ROMs, one for Windows NT and one for AIX that includes a Windows NT client. The Windows NT files are slightly different between the two CD-ROMs.

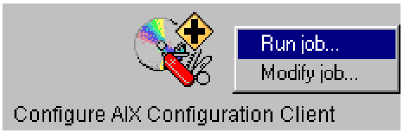
AIX client setup

Use the following procedure to set up the Tivoli software file package distribution for the IBM SecureWay Firewall client software on a AIX client.

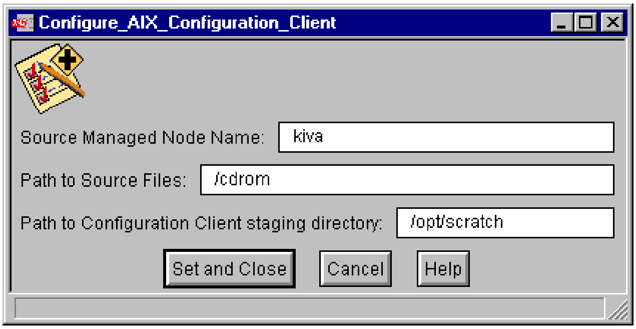
1 Double-click on the **Configure AIX Configuration Client** icon in the Firewall Plus collection window.

—OR—

Right-click on the **Configure AIX Configuration Client** icon and select the **Run job** option from the pop-up menu



to display the Configure_AIX_Configuration_Client window.



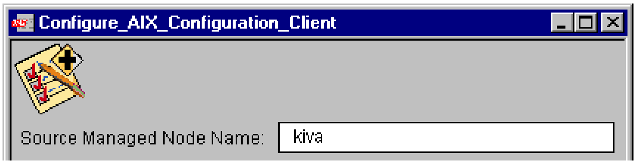
Source Managed Node Name: kiva

Path to Source Files: /cdrom

Path to Configuration Client staging directory: /opt/scratch

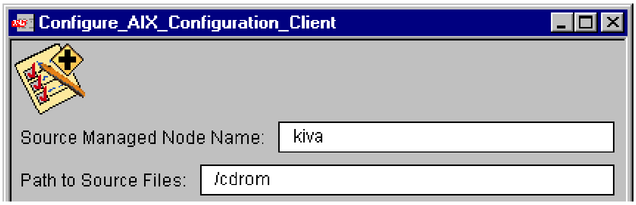
This window allows you to configure the file package information for all AIX platforms.

2 Enter the name of the TME managed node that has the client binary files to install in the **Source Managed Node Name:** field.



Source Managed Node Name: kiva

3 Enter the path on the source host where the files reside for installing the Configuration Client. Usually this is your CD-ROM drive. In the graphic shown below it is ‘/cdrom’ in the **Path to Source Files:** field.



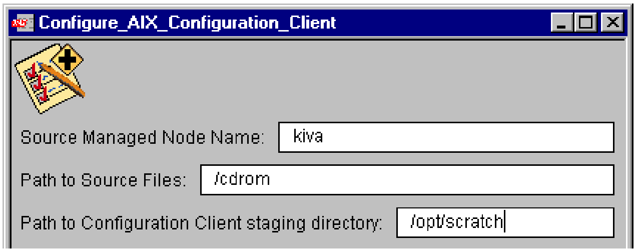
Source Managed Node Name: kiva

Path to Source Files: /cdrom

4 Enter the path to a scratch area in the **Path to Configuration Client staging directory:** field. This is the directory on the client machine where the files are placed temporarily in order to install the SecureWay Configuration Client.

Note

The IBM SecureWay Firewall application requires you to have 55 MB available in the scratch are for the installation of the AIX Configuration Client.



Source Managed Node Name: kiva

Path to Source Files: /cdrom

Path to Configuration Client staging directory: /opt/scratch

5 Click the **Set and Close** button to set all the information you have entered and return to the Tivoli Plus module window.

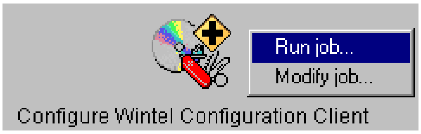
PC client setup

Use the following procedure to set up the Tivoli software file package distribution of the IBM SecureWay Firewall client software version 4.2 on a PC client. You need to use this dialog only once to set up a file package distribution for all of your PC clients using Firewall Plus version 4.2 software.

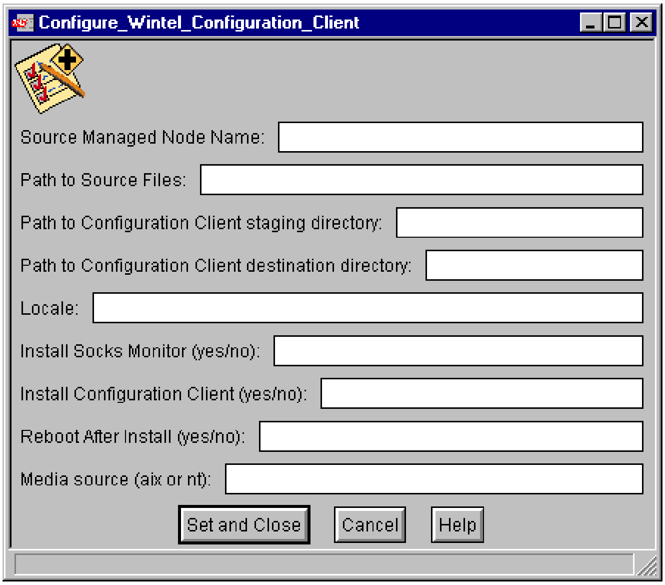
1 Double-click the **Configure Wintel Configuration Client** icon in the **Tivoli Plus** module window.

—OR—

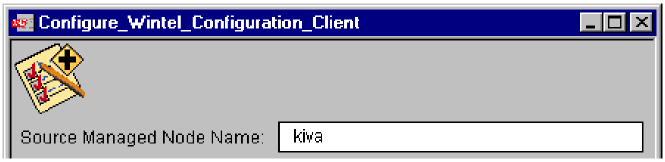
Right-click on the **Configure Wintel Configuration Client** icon and select **Run job** from the pop-up menu



to display the Configure_Wintel_Configuration_Client window.

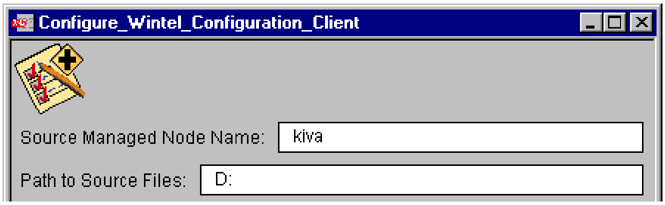

Configure_Wintel_Configuration_Client
Source Managed Node Name:
Path to Source Files:
Path to Configuration Client staging directory:
Path to Configuration Client destination directory:
Locale:
Install Socks Monitor (yes/no):
Install Configuration Client (yes/no):
Reboot After Install (yes/no):
Media source (aix or nt):
Set and Close
Cancel
Help

2 Enter the name of the TME managed node that has the client binary files and library files to install in the **Source Managed Node Name:** field.



Source Managed Node Name: kiva

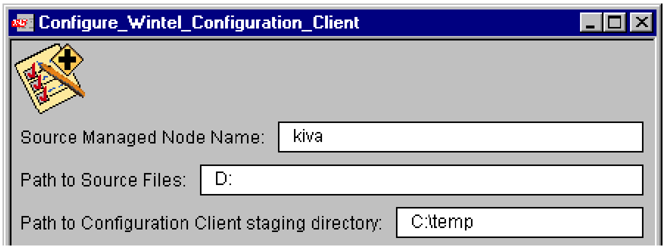
3 Enter the path on the source host where the files reside for the installation of the Configuration Client. Usually this will be your CD-ROM drive, i.e., “D:” in the **Path to Source Files:** field.



Source Managed Node Name: kiva

Path to Source Files: D:

4 Enter the path to a scratch area in the **Path to Configuration Client staging directory:** field. This is the directory on the client machine where files will be placed temporarily in order to install the SecureWay Configuration Client.



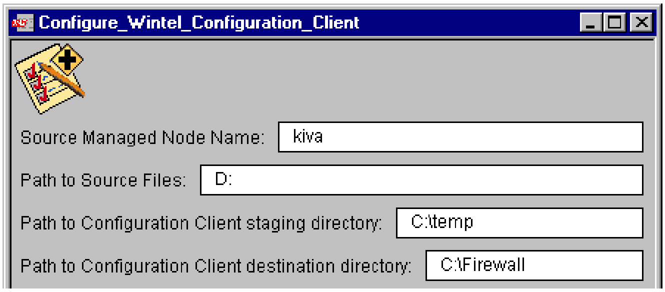
Configure_Wintel_Configuration_Client

Source Managed Node Name: kiva

Path to Source Files: D:

Path to Configuration Client staging directory: C:\temp

5 Enter the path to the destination directory where the IBM SecureWay Firewall Configuration Client will be installed in the **Path to Configuration Client destination directory:** field.



Configure_Wintel_Configuration_Client

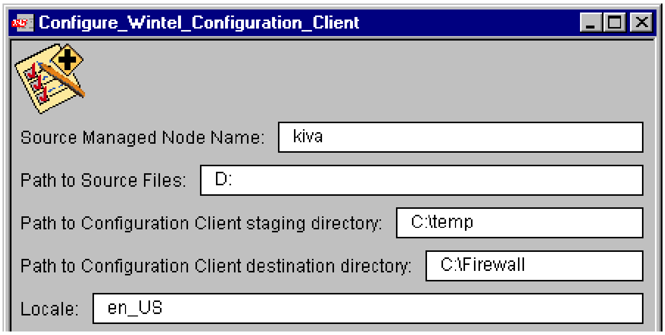
Source Managed Node Name: kiva

Path to Source Files: D:

Path to Configuration Client staging directory: C:\temp

Path to Configuration Client destination directory: C:\Firewall

6 Enter the locale where the IBM SecureWay Firewall is installed in the **Locale:** field. For example, en_US is the locale for English language installations.



Configure_Wintel_Configuration_Client

Source Managed Node Name: kiva

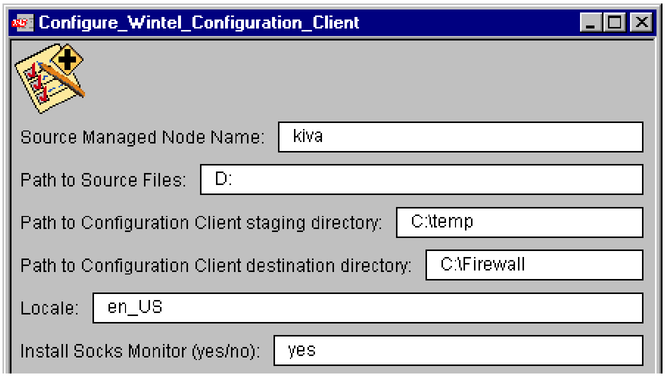
Path to Source Files: D:

Path to Configuration Client staging directory: C:\temp

Path to Configuration Client destination directory: C:\Firewall

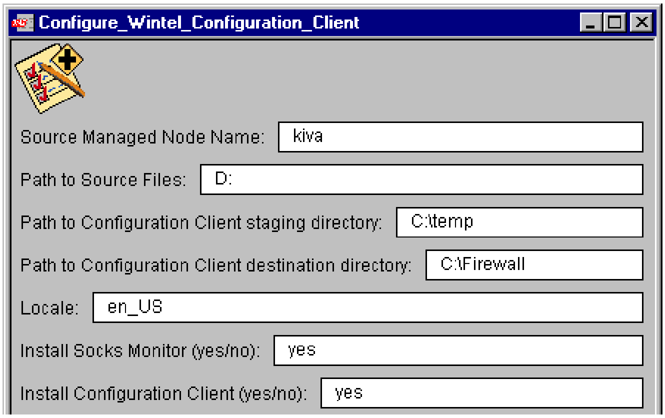
Locale: en_US

7 Enter either ‘yes’ or ‘no’ in the **Install Socks Monitor (yes/no):** field to indicate whether or not the Socks Monitor should be installed along with the Configuration Client.



Source Managed Node Name:	kiva
Path to Source Files:	D:
Path to Configuration Client staging directory:	C:\temp
Path to Configuration Client destination directory:	C:\Firewall
Locale:	en_US
Install Socks Monitor (yes/no):	yes

8 Enter either ‘yes’ or ‘no’ in the **Install Configuration Client (yes/no):** field to indicate whether or not the Configuration Client should be installed.

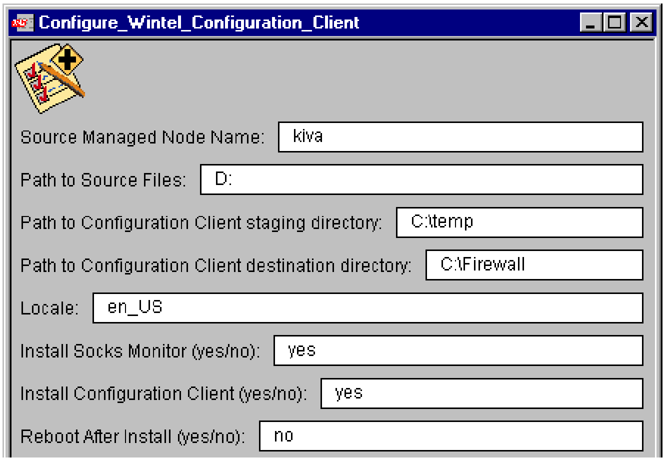


Source Managed Node Name:	kiva
Path to Source Files:	D:
Path to Configuration Client staging directory:	C:\temp
Path to Configuration Client destination directory:	C:\Firewall
Locale:	en_US
Install Socks Monitor (yes/no):	yes
Install Configuration Client (yes/no):	yes

Note

By default the Report Utilities are installed, so it is not necessary to install the Configuration Client.

9 Enter either ‘yes’ or ‘no’ in the **Reboot After Install (yes/no):** field to indicate whether or not the managed nodes on which the Configuration Client is installed should be rebooted after the installation.



Configure_Wintel_Configuration_Client

Source Managed Node Name: kiva

Path to Source Files: D:

Path to Configuration Client staging directory: C:\temp

Path to Configuration Client destination directory: C:\Firewall

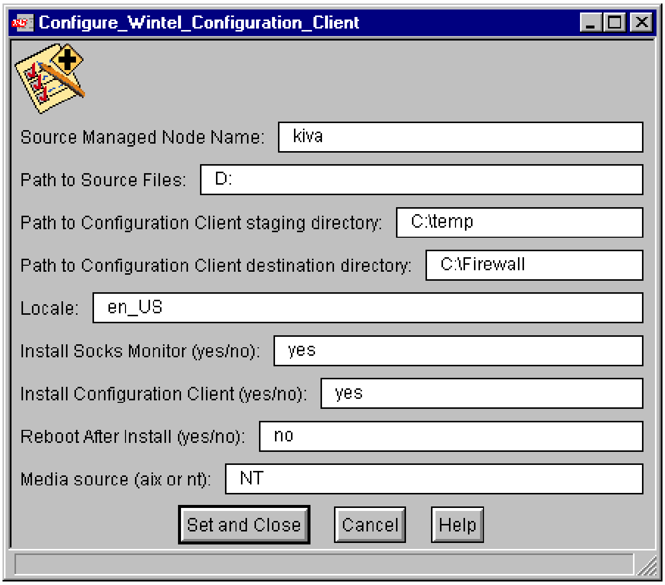
Locale: en_US

Install Socks Monitor (yes/no): yes

Install Configuration Client (yes/no): yes

Reboot After Install (yes/no): no

10 Enter either ‘nt’ or ‘aix’ in the **Media source:** field. The entry in this field determines whether or not you will be configuring the File Packages using the Windows NT source media or the AIX source media for the SecureWay Firewall Configuration Client installation. The Windows NT Configuration Client is included on both CDs.



Configure_Wintel_Configuration_Client

Source Managed Node Name: kiva

Path to Source Files: D:

Path to Configuration Client staging directory: C:\temp

Path to Configuration Client destination directory: C:\Firewall

Locale: en_US

Install Socks Monitor (yes/no): yes

Install Configuration Client (yes/no): yes

Reboot After Install (yes/no): no

Media source (aix or nt): NT

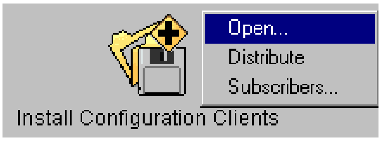
11 Click **Set and Close** to set all of the information you have entered and return to the Tivoli Plus module window.

You can change the server and location of the binaries destination directory at any time.

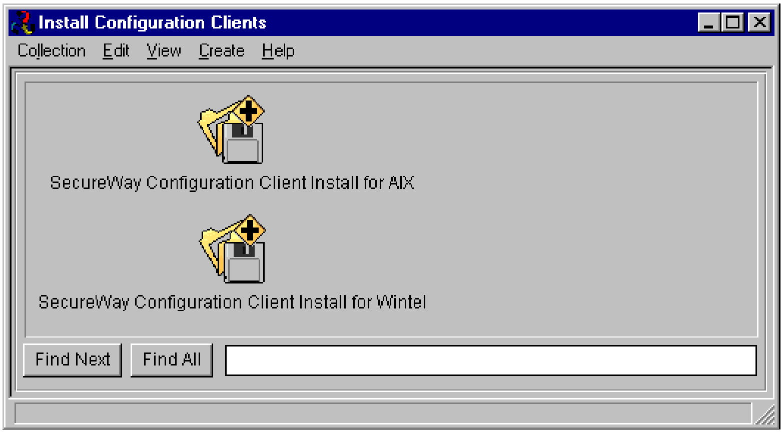
Distributing file packages

After you have configured the desired file packages you are ready to distribute them. During distribution the Firewall Plus module performs pre-installation checks, such as verifying available disk space and memory. If any problems are encountered during file package distribution a window appears containing detailed information. If you wish, you can save this information in an output file for reference.

To begin the software distribution right-click on the **Install Configuration Clients** icon in the Firewall Plus window and select **Open...**



to display the Install Configuration Clients window.


Install Configuration Clients
Collection
Edit
View
Create
Help
SecureWay Configuration Client Install for AIX
SecureWay Configuration Client Install for Wintel
Find Next
Find All

This window contains the two icons used to distribute the file packages to the appropriate Firewall Plus clients.

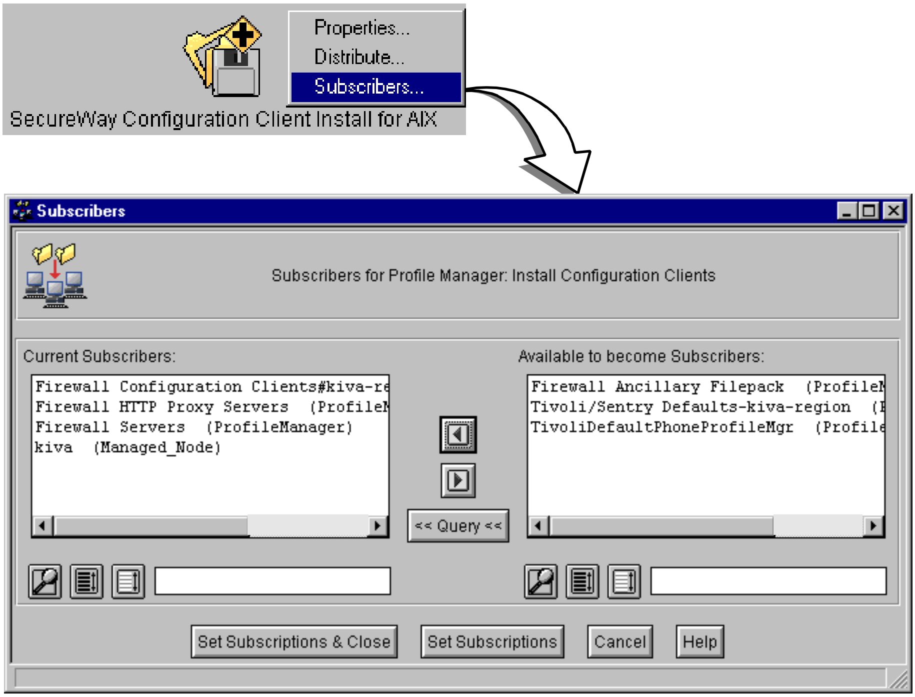
AIX client file package distribution

In the Install Configuration Clients window:

1 Double-click on the **SecureWay Configuration Client Install for AIX** icon to bring up the Subscribers dialog.

–OR–

Right-click the **SecureWay Configuration Client Install for AIX** icon and select **Subscribers** from the pop-up menu.


Properties...
Distribute...
Subscribers...
SecureWay Configuration Client Install for AIX
Subscribers
Subscribers for Profile Manager: Install Configuration Clients
Current Subscribers:
Available to become Subscribers:
<< Query <<
Set Subscriptions & Close
Set Subscriptions
Cancel
Help

```
Firewall Configuration Clients#kiva-re
Firewall HTTP Proxy Servers  (ProfileM
Firewall Servers  (ProfileManager)
kiva  (Managed_Node)
```

```
Firewall Ancillary Filepack  (ProfileM
Tivoli/Sentry Defaults-kiva-region  (P
TivoliDefaultPhoneProfileMgr  (Profile
```

2 Specify the subscription lists to which you want to distribute by highlighting each choice and using the left and right arrow keys to place your choice in the appropriate pane of the window.

3 When you have made your choices, click on **Set Subscriptions & Close**.

4 Distribute the file packages to your selected subscribers by right-clicking on the **SecureWay Configuration Client Install for AIX** icon in the Install Configuration Clients window and selecting **Distribute...** from the pop-up menu.

After distribution:

For IBM SecureWay Firewall version 4.2 software on AIX platforms only, the **Distribute...** task runs `installp`, the package installation program on the AIX managed node or endpoint to which the file package is distributed.

Note

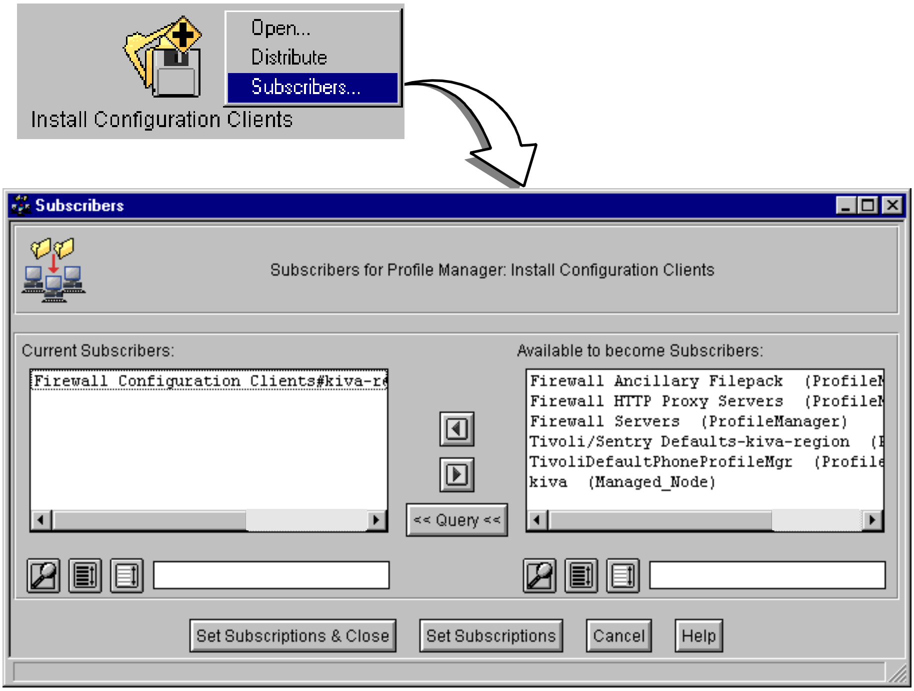
Approximately 160 MB of disk space in the /usr filesystem is required for installation of the Configuration Client.

PC client 4.2 file package distribution

1 Double-click on the **Install Configuration Clients** icon to display the Subscribers dialog.

–OR–

Right-click the **Install Configuration Clients** icon and select **Subscribers** from the pop-up menu



Subscribers for Profile Manager: Install Configuration Clients

Current Subscribers:

```
Firewall Configuration Clients#kiva-re
```

Available to become Subscribers:

```
Firewall Ancillary Filepack   (ProfileM
Firewall HTTP Proxy Servers   (ProfileM
Firewall Servers  (ProfileManager)
Tivoli/Sentry Defaults-kiva-region   (P
TivoliDefaultPhoneProfileMgr   (Profile
kiva  (Managed_Node)
```

2 Specify the subscription lists to which you want to distribute by highlighting each choice and using the left and right arrow keys to place your choice in the Current Subscribers pane of the window.

3 When you have made your choices, click on **Set Subscriptions & Close**.

4 Distribute the file packages to your selected subscribers by right-clicking on the **Install Firewall Wintel Configuration Client** icon in the Install Firewall Wintel Configuration Clients window and selecting **Distribute...** from the pop-up menu.

File package distribution copies the setup installation files to the distribution target in a temporary staging directory.

4 Distributed Monitoring

Monitors must be distributed to make them active. Each monitor checks the status of a specific resource based on a pre-defined frequency and can trigger responses once a certain threshold or condition is met.

This chapter shows how the Firewall Plus module uses the Tivoli Distributed Monitoring application to provide resource monitoring capabilities.

This chapter describes the following:

- IBM SecureWay Firewall product monitors
- Distributing monitors
- Changing monitor properties
- Viewing monitor status
- Properties of the pre-configured IBM SecureWay Firewall product monitors provided with the Firewall Plus module

IBM SecureWay Firewall product monitors send TEC events as part of their default response.

Firewall Plus Monitors

Overview

The Firewall Plus module has three basic monitors. They are:

- FilterStatus
- CoreProcessStatus
- HTTPProxyProcessStatus

Monitored resources

The following table indicates the IBM SecureWay Firewall server resources that the SecureWay Firewall Plus for Tivoli product monitors on Windows NT platforms.

Monitoring Source	Monitors	Platform
CoreProcessStatus (smtpsb)	Secure Mail Proxy	AIX
CoreProcessStatus (fwsocks5)	Socks Server	Windows NT AIX
CoreProcessStatus (inetd)	Inetd	AIX
CoreProcessStatus (ibmfwncs)	Configuration Server	Windows NT
CoreProcessStatus (securemail)	Secure Mail Proxy	Windows NT AIX
CoreProcessStatus (fwfiltlgs)	Filter Log Service	Windows NT
CoreProcessStatus (fwtimernats)	Timer NAT Service	Windows NT
CoreProcessStatus (pftpd)	Proxy FTP Daemon	Windows NT
CoreProcessStatus (ptelnetd)	Proxy Telnet Daemon	Windows NT
CoreProcessStatus (fwlogds)	Log Daemon	Windows NT
HTTPProxyProcessStatus (ibmproxy)	Web Traffic Express 3.0 HTTP Proxy	Windows NT AIX
FilterStatus	Filter	Windows NT AIX

Default Properties

By default the monitors are enabled when distributed. It is possible to disable them and to configure responses when you edit monitor properties.

Note

You should analyze the pre-configured monitor properties as a set before changing them. Review the section “Monitored Conditions” on page 52.

Responses

The following list identifies the possible responses for monitors and indicates whether the response is on by default for Firewall Plus monitors.

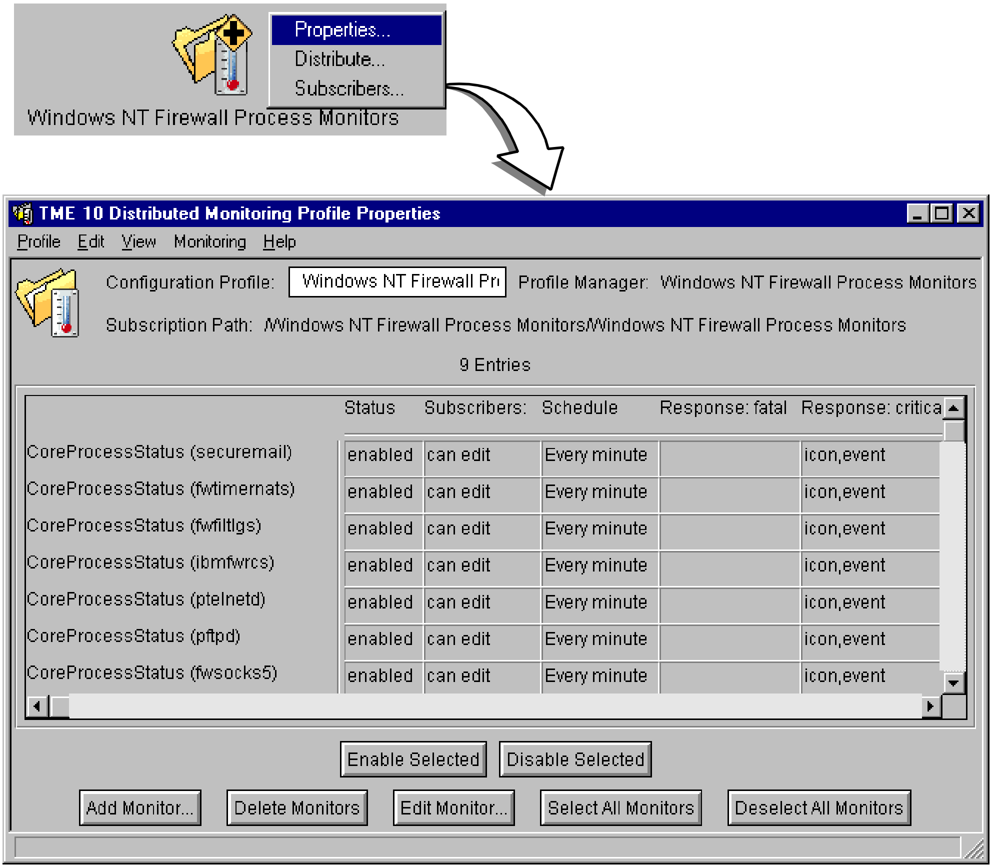
- ***TEC Event***: **YES**
- ***Sentry Indicator***: **YES**
- ***Pop-up***: **NO**
- ***Tivoli Notice***: **NO**
- ***Automated Actions***: **NO** — however, the TEC server may still respond automatically to TEC events sent by the monitors.

Changing Monitor Properties

The server monitors for the Firewall Plus module are pre-configured for immediate use.

Customizing Specific Monitor Properties

1 Right-click on the desired monitor icon, then choose **Properties...** from the pop-up menu. The TME 10 Distributed Monitoring Profile Properties window appears.



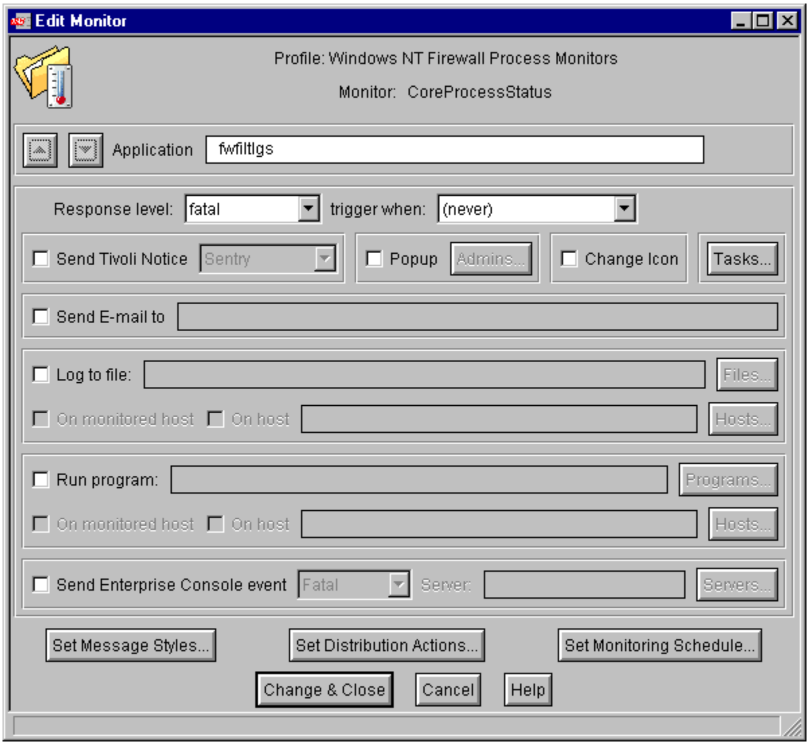
Configuration Profile: Windows NT Firewall Pr Profile Manager: Windows NT Firewall Process Monitors

Subscription Path: /Windows NT Firewall Process Monitors/Windows NT Firewall Process Monitors

9 Entries

	Status	Subscribers:	Schedule	Response: fatal	Response: critica
CoreProcessStatus (securemail)	enabled	can edit	Every minute		icon,event
CoreProcessStatus (fwtimernats)	enabled	can edit	Every minute		icon,event
CoreProcessStatus (fwfiltlgs)	enabled	can edit	Every minute		icon,event
CoreProcessStatus (ibmfwrcs)	enabled	can edit	Every minute		icon,event
CoreProcessStatus (ptelnetd)	enabled	can edit	Every minute		icon,event
CoreProcessStatus (pftpd)	enabled	can edit	Every minute		icon,event
CoreProcessStatus (fwsocks5)	enabled	can edit	Every minute		icon,event

2 Select the desired monitor, then click **Edit Monitor**. The Edit Monitor window appears.



Edit Monitor

Profile: Windows NT Firewall Process Monitors

Monitor: CoreProcessStatus

Application fwfiltlgs

Response level: fatal trigger when: (never)

□ Send Tivoli Notice Sentry □ Popup Admins... □ Change Icon Tasks...

□ Send E-mail to

□ Log to file: Files...

□ On monitored host □ On host Hosts...

□ Run program: Programs...

□ On monitored host □ On host Hosts...

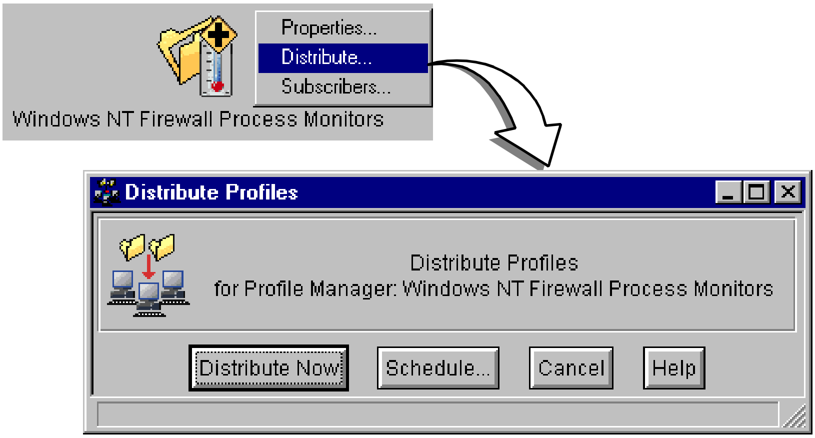
□ Send Enterprise Console event Fatal Server: Servers...

3 You can change trigger levels and responses for each monitor.

4 Modify the properties as desired, then click **Change and Close**. In the Profile Properties window, note that a change bar now appears next to the monitor that you edited.

5 In the TME 10 Distributed Monitoring Profile Properties window **Profile** menu, select **Profile** > **Save**, then choose **Profile** > **Close**.

6 Distribute the monitors. Right-click on the desired monitor icon, then choose **Distribute...**. In the dialog that appears, click **Distribute Now** or schedule the distribution.



Distribute Profiles
for Profile Manager: Windows NT Firewall Process Monitors

Polling Intervals

The Firewall Plus product monitors are pre-configured to poll at specified intervals. Polling intervals can be modified for each individual monitor, as illustrated in the Edit Monitor window above.

Viewing Monitor Status

Monitor status may be viewed in any of several ways. Each monitor can be configured to use one or more methods to signal its status.

- Pop-ups
- Tivoli Notices
- TEC Events
- Distributed Monitoring indicators

Pop-ups

When enabled, a pop-up dialog appears on the administrator's screen whenever a monitor trigger is activated.

Tivoli Notices

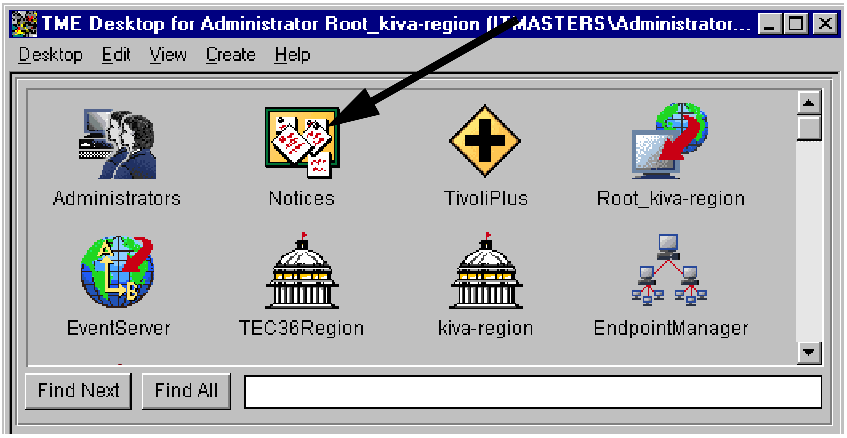
When enabled, a notice is posted to Tivoli Notices whenever a monitor trigger is activated.

Note

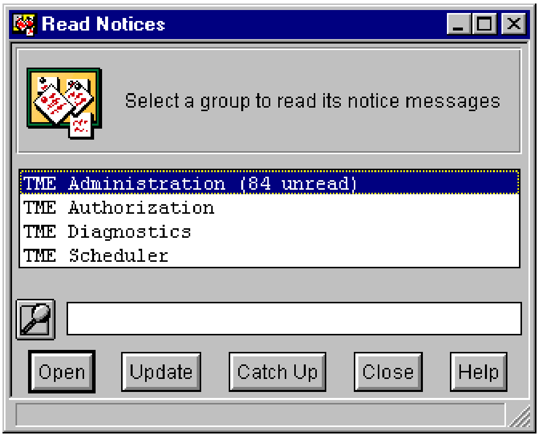
An administrator must be granted access to the Tivoli Notice Group to view notices from their TME Desktop.

To view notices:

1 On the TME Desktop, double-click **Notices**.



A list of notice groups appears.



TME Administration (84 unread)
TME Authorization
TME Diagnostics
TME Scheduler

Each item in the list identifies a group and the number of unread notices for the group.

2 Double-click on the desired group entry. A message window appears that contains all the information in the notice relating to that group.

3 Click **Close** when finished.

TEC Events

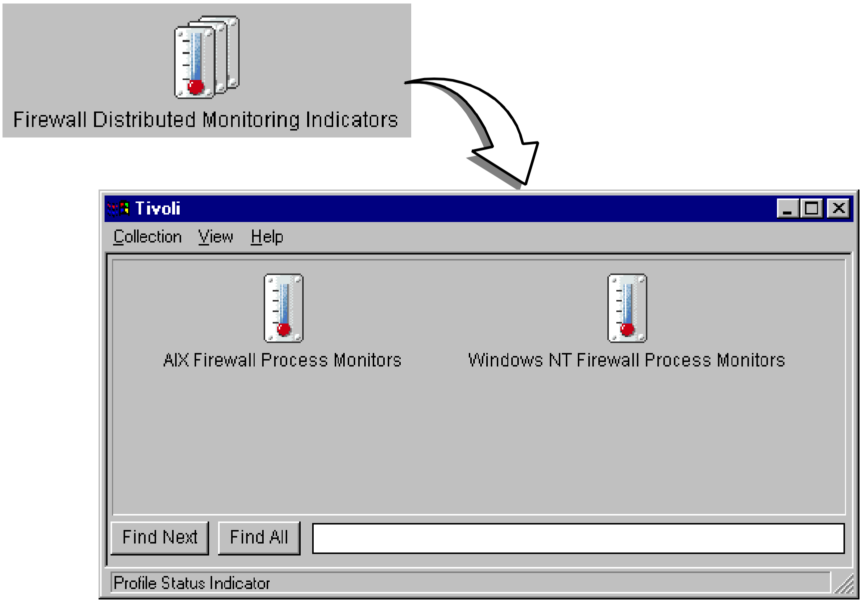
Some monitors have TEC events associated with them. If the monitor is configured to generate TEC events, then an event is sent to the TEC server whenever the monitor threshold is reached that activates TEC event generation.

Monitor Indicators

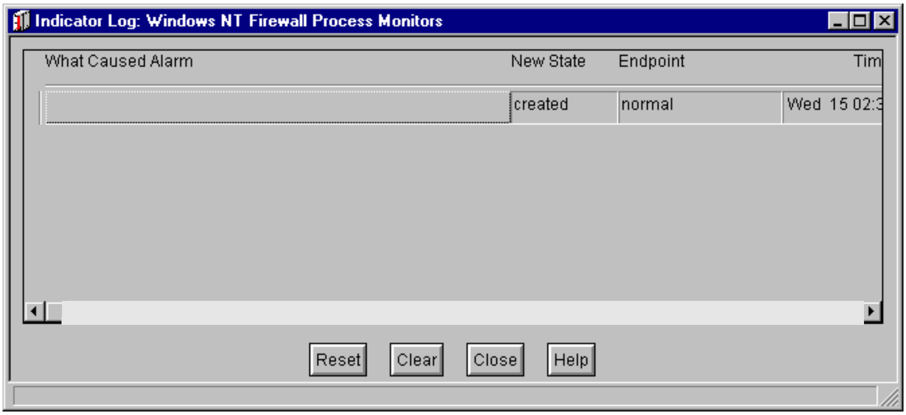
When monitor indicators are enabled, changes in an **Indicator** thermometer icon on the Firewall Plus desktop identify the severity level of a trigger whenever a condition is met.

To use the monitor indicators when enabled:

1 In the Firewall Plus window, double-click the **Firewall Distributed Monitoring Indicators** icon. A window containing monitor indicators appears for each group of monitors.


Firewall Distributed Monitoring Indicators
Tivoli
Collection
View
Help
AIX Firewall Process Monitors
Windows NT Firewall Process Monitors
Find Next
Find All
Profile Status Indicator

2 Double-click on an indicator icon to see a log of monitor alarms. A log window appears.



What Caused Alarm	New State	Endpoint	Tim
	created	normal	Wed 15 02:3

3 The following are choices you may make in this log window:

- Click the **Reset** button to reset the indicator.
- Click the **Clear** button to clear all entries in the log.

- Click the **Close** button when finished.

Monitored Conditions

The tables in this chapter show the relationship of monitored conditions to triggered actions as the monitors are provided. Triggers and responses can be customized as required. See “Firewall Plus Monitors” on page 53 for details on status changes.

Summary

This is a brief summary of monitored conditions:

- status of the filter
- status of specific processes in the table on AIX and on NT
- status of HTTP proxy process

The tables on the following pages correspond to the tables of conditions and responses that appear for the monitors when you edit their properties. Monitors can have a trigger and response for each of four severity levels.

The trigger response has the following components:

- **Severity**: Individual triggers can be configured for each severity. In the table, the severity columns identify each level of severity for Distributed Monitoring (Sentry) and for the TEC interface. The six severity levels are:
  - Critical
  - Severe
  - Warning
  - Normal
  - Reset
  - Always
- **Threshold** has one value that is expressed in specific units.
- **Response -** Entries in this column indicate the monitor’s action when it is triggered. Response has five parts:

- Send notice
- Pop-up window
- Change Indicator
- TEC Event - generate a TEC event if indicated in the table for the distributed monitor.
- Auto(matic) Action - any additional action taken as noted in the table for the monitor.

Firewall Plus Monitors

The Firewall Plus module has three monitors. The tables below show the trigger response for each monitor.

Definitions that apply to monitor status are:

- Triggers: never, up/available, down/unavailable, becomes available, becomes unavailable.
- Triggers: >, <, =, !=, increases beyond, decreases below, increase of, % increase of, changes by, and outside range

FilterStatus

Table 1:

Monitor Name	FilterStatus			
Description	Monitors the status of the filter.			
Collection	AIX/NT			
Frequency	1 minute			
			Response	
Severity	**Triggers when**	**Threshold value**	**TEC Event**	**Auto Action**
Critical	Becomes	Unavailable	Sends event `Firewall_FilterProcessStatus`.	
Severe				
Warning				
Normal				
Reset	Becomes	Available	Sends event `Firewall_FilterProcessStatus`.	
Always				

CoreProcessStatus

Table 2:

Monitor Name	CoreProcessStatus

Table 2:

Description	Monitors the status of specific processes in the table on AIX and on NT.
Collection	AIX/NT
Frequency	1 minute

Severity	**Triggers when**	**Threshold value**	**Response**	
			TEC Event	**Auto Action**
Critical	Becomes	Unavailable	Sends event `Firewall_CoreProcessStatus`.	
Severe				
Warning				
Normal				
Reset	Becomes	Available	Sends event `Firewall_CoreProcessStatus`.	
Always				

HTTPProxyProcessStatus

Table 3:

Monitor Name	HTTPProxyProcessStatus
Description	Monitors the status of the HTTP proxy process.
Collection	AIX/NT
Frequency	1 minute

			Response	
Severity	**Triggers when**	**Threshold value**	**TEC Event**	**Auto Action**
Critical	Becomes	Unavailable	Sends event `Firewall_HTTPProxyStatus`.	
Severe				
Warning				
Normal				
Reset	Becomes	Available	Sends event `Firewall_HTTPProxyStatus`.	
Always				

5 TEC Events

This chapter describes setting up the Tivoli Enterprise Console (TEC) server and the logfile adapter to receive and process events sent by the distributed monitors. It contains the following:

- Configuring the TEC server
- Configuring the Logfile Adapter
- Viewing Firewall Plus events in a TEC interface
- Listings of events, rules, and automatic actions

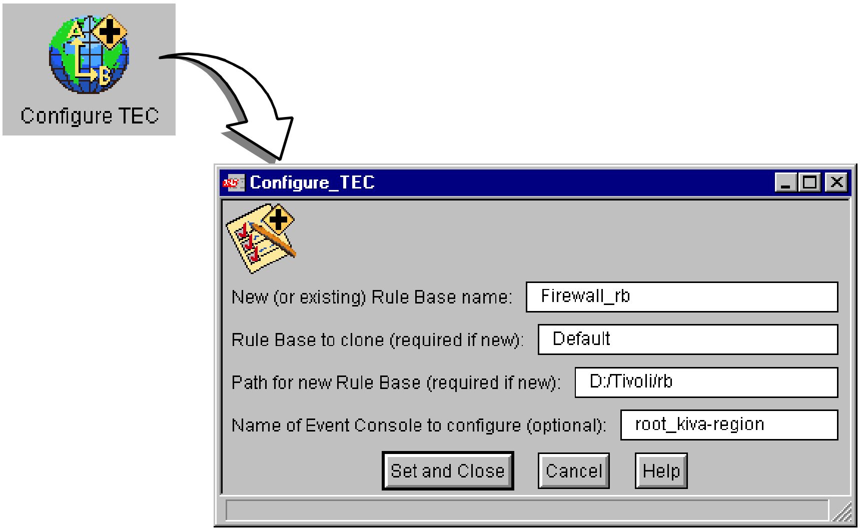
The event server processes events sent to it by distributed monitors and the Firewall Plus module. It processes the events according to a rule base. Depending on the event and the rule used to handle it, the server can forward the event to a TEC interface or perform actions in response.

At least one event console must be installed before the event server can be set up.

Configuring the TEC Server

The TEC server must be configured to use the Firewall Plus event classes and rule base before Firewall Plus events can be monitored from the TEC interface. To configure the server, do the following:

1 In the Firewall Plus desktop, double-click on the **Configure TEC** icon. The Configure TEC window appears.



New (or existing) Rule Base name: Firewall_rb

Rule Base to clone (required if new): Default

Path for new Rule Base (required if new): D:/Tivoli/rb

Name of Event Console to configure (optional): root_kiva-region

2 Fill in the information:

- **New (or existing) Rule Base name**: Enter a unique rule base name or the name of a rule base that already exists, e.g., **Firewall_rb,** in this field.

Caution Do not use “Default” as the Rule Base name in this field.

- **Rule Base to clone (required if new):** Enter the name of your current rule base in this field. If one has not been defined, use **Default.**
- **Path for new Rule Base (required if new):** Enter the path to the directory for the rule base files.

Caution The directory for the rule base files **must** not exist or the run will fail and an error message appears.

- **Name of Event Console to configure (optional):** Type the name of the event console to be configured, e.g., `Root_<host machine name>-region`.

Alternatively, you can "discover" the name of the event console by typing the following command in the CLI of the sourced Tivoli environment:

wlookup -ar EnterpriseClient

3 Click on the **Set and Close** button. The rule base files are configured. An output window appears; check it for errors.

Configuring the Logfile Adapter

In order to monitor the SecureWay Firewall's main logfile, you must configure the logfile adapter that is included with the plus module.

To configure the logfile adapter, do the following:

1 On the **SecureWay Firewall Plus for Tivoli** collection, right-click the **Configure Logfile Adapter** icon and select the **Run Job** option. The Configure Logfile Adapter dialog displays.

2 In the **TEC Server** text field, enter the name of the TEC server where the events are sent from the logfile.

3 In the **TEC Server Port** text field, enter the port number through which the TEC server receives events. The default port used by TEC when installed on Windows NT is 5529, and 0 (zero) on UNIX. You must enter a value in this field.

4 In the **Path to (and including) perl** text field, enter the path to the perl executable and the name of the executable.

This perl installation must be on the same machine where the SecureWay Firewall server is installed. An example value for this field, if the SecureWay Firewall server is installed on a Windows NT machine is: `C:/Perl/Perl.exe`.

Note

The logfile adapter requires the installation of Perl 5 or higher.

5 Click the **Set and Close** button to begin the logfile adapter configuration.

After the completion of the logfile adapter configuration, it automatically starts and subsequently starts every time the machine starts.

If any of the values that have been entered in the Configure Logfile Adapter dialog have changed, you may rerun the Configure Logfile Adapter job. If you are using Windows NT the service that was created to run the logfile adapter will be deleted and replaced with the new values.

The logfile adapter and its configuration files are then located in the following directories depending on your Tivoli environment:

SecureWay Firewall server is a Windows NT Tivoli endpoint:

```
%System Root%\System32\drivers\etc\Tivoli\lfa
```

SecureWay Firewall server is a UNIX Tivoli endpoint:

```
\etc\Tivoli\lfa
```

SecureWay Firewall server is a Tivoli managed node:

```
$BINDIR/../generic_unix/TME/PLUS/SECUREWAY_FIREWALL/
lfa
```

Viewing Firewall Plus Events

When the **Configure TEC** task executes, it sets up the following on the TEC server:

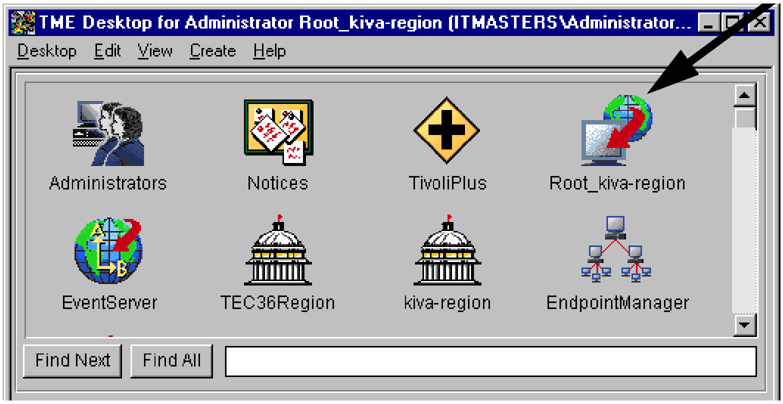
- An event group for Firewall Plus events: FIREWALL_PLUS
- An event source for all Distributed Monitor sources: FIREWALL_DM. This event source may already exist.
- An event source for all Firewall Plus Logfile Adapter sources: FIREWALL_ADAPTER. This event source may already exist.

The task also configures the event console selected to subscribe to the event group. All administrators are subscribed to all sources by default.

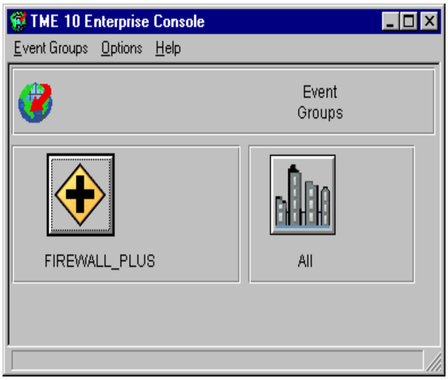
Viewing Events

To view Firewall Plus events:

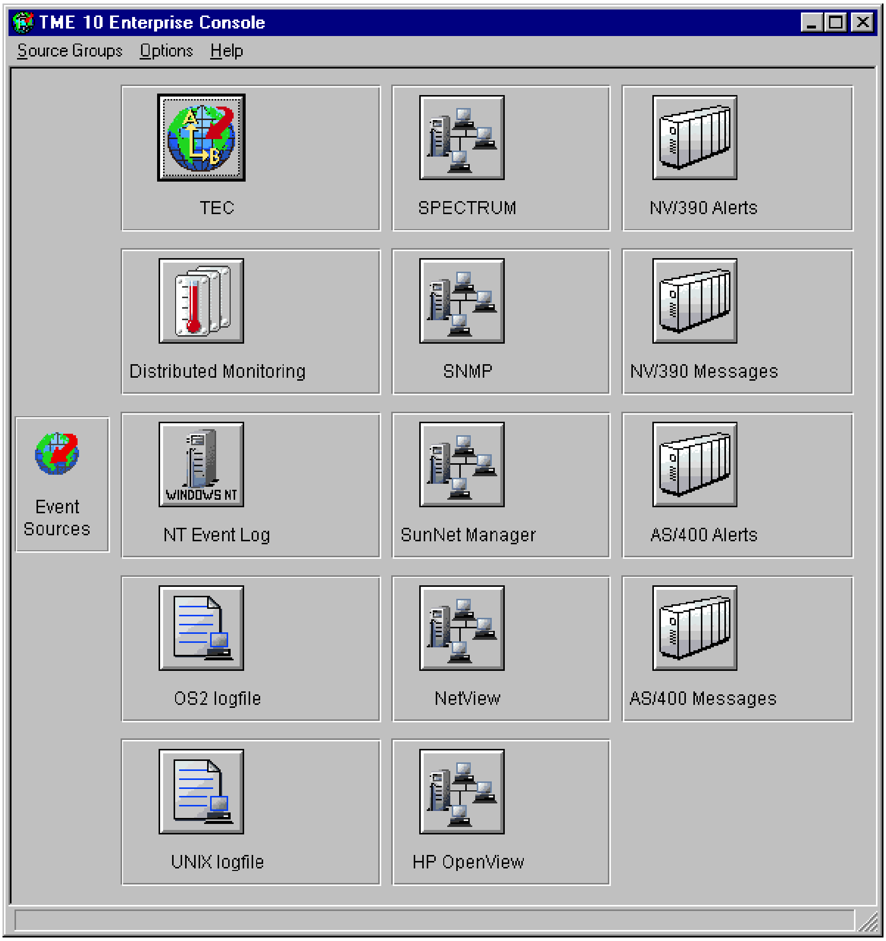
1 On the TME desktop, double-click the event console configured in the **Configure TEC** task.



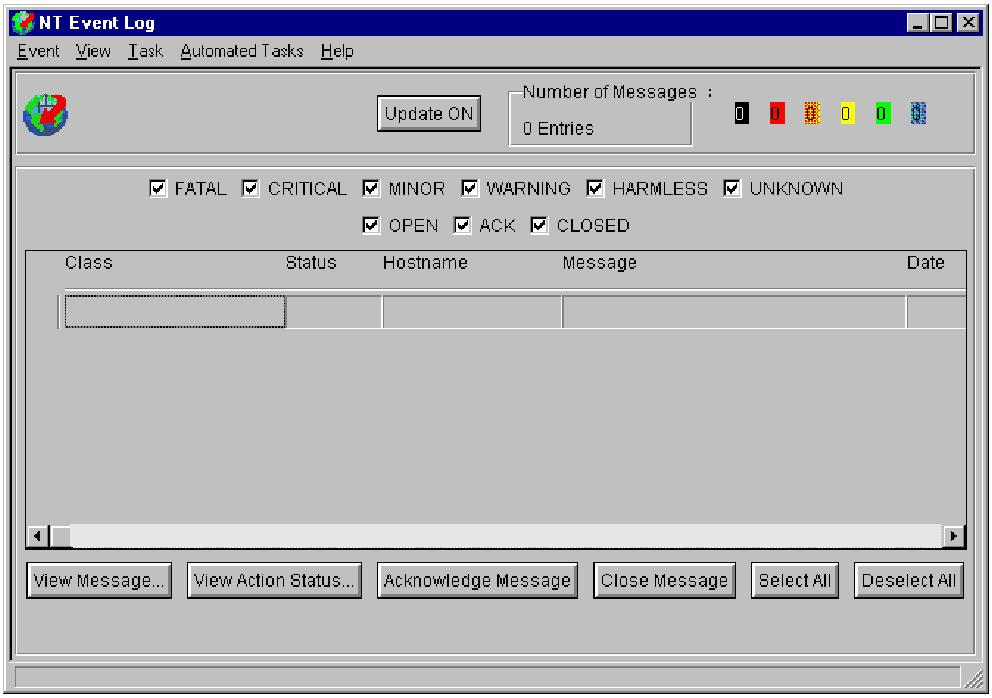
Two windows display: Event Groups**.**



and Event Sources.



2 Click the event button to view its assigned events. An events dialog appears. (The dialog for the NT Event Log event source is shown below.)



Number of Messages : 0 Entries

☑ FATAL ☑ CRITICAL ☑ MINOR ☑ WARNING ☑ HARMLESS ☑ UNKNOWN

☑ OPEN ☑ ACK ☑ CLOSED

Class	Status	Hostname	Message	Date

Firewall Plus for Tivoli events can be viewed and managed in this window. See Tivoli documentation for more details.

Note

When the Distributed Monitoring event source is selected, all Distributed Monitoring events are visible, not just the Distributed Monitoring events for the Firewall Plus module.

Configuring Other TEC Consoles

The FIREWALL_PLUS event group and the Distributed Monitoring event sources may be assigned to other TEC interfaces. Consult Tivoli documentation for information about how to assign them.

TEC Events and Rules

The distributed monitors and the logfile adapter send events to the TEC interface. The “TEC event messages listing” section below lists all of the event classes used. In the previous chapter, the section “Monitored conditions” lists the severity of the events. When an event is received by the TEC event server, a rule base is consulted to determine how to handle the event. The “TEC rules and actions listing” section below lists the rules and actions that can be triggered by an event or combination of events.

The rule base can be customized. Consult Tivoli documentation for details.

TEC Event Messages Listing

Event Class	Condition
IBM Firewall Event Base Class	Base class definition upon which all other events are dependent.
Firewall_CoreProcessStatus	Event definition for many of the processes that the SecureWay Firewall product uses.
Firewall_FilterProcessStatus	Event definition for the FilterStatus monitor-generated event.
Firewall_HTTPProxyStatus	Event Definition for the status of the HTTPProxy server.
Firewall_IntrusionDetection	Event definition for messages received from the logfile adapter indicating that attempts are being made to breach the security of the SecureWay Firewall server.
Firewall_AdministratorNotification	Event definition for messages received from the logfile adapter indicating isolated Firewall events such as a failed login.
Firewall_UserRequestFailure	Event definition for messages received from the logfile adapter indicating that a particular user operation failed.
Firewall_Performance	Event definition for messages received from the logfile adapter indicating the SecureWay Firewall has a load that it cannot handle.

TEC Rules and Actions Listing

Event Class/Rule	Event/Action
AllFirewallEvents	Remove if duplicate.
FilterProcessAvailable	If the Filter Process becomes available, close all previous events stating that it was down.

Event Class/Rule	Event/Action
CoreProcessAvailable	If one of the IBM SecureWay Firewall core processes becomes available, close all previous events stating that it was down.
HTTPProxyAvailable	If the HTTP proxy becomes available, close all previous events stating that it was down.
PerformanceEscalation	If a Firewall_Performance event is received more than 2 times in 10 minutes and not less than 30 seconds, escalate the severity of the event from a WARNING level to a CRITICAL level.

6 Task Operations

The Firewall Plus module can perform day-to-day management operations as jobs or as tasks from the task icons in the Firewall Plus window. The following topics are described:

- **Firewall Plus Tasks**: lists each operation and any required arguments for the task.
- **Overview**: describes how to run the operations as jobs or as tasks.
- **Jobs**: describes how to run an operation as a job and how to modify job options.
- **Tasks**: describes how to run an operation as a task and how to modify task options.

Overview of Jobs and Tasks

Management operations are represented as task icons in the SecureWay Firewall Plus for Tivoli window.

From a task icon, operations can run as jobs or tasks. A job is intended to be run repeatedly as a routine operation or as a means of controlling an entire service. It typically is executed on multiple subscribers. A task is intended to be run as a special one-time operation on one or more selected hosts or task endpoints.

- **Job**: To run an operation as a job, double-click the task icon, or right-click the task icon and choose **Run Job** from the pop-up menu. If options must be supplied, a dialog appears and prompts for them.
- To specify how the job is executed, right-click the task icon and choose **Modify Jobs** from the pop-up menu before running the job.
- **Task**: To run an operation as a task, right-click the task icon and choose **Run on Selected Hosts** from the pop-up menu. A dialog appears asking how the task is to be run and what hosts to run it on. When the task executes, another dialog asks for options, if needed.

Firewall Plus Tasks

Note

Spaces are *not* allowed in path names.

Start or Stop Main Filter Engine

This task starts or stops the main filter engine.

Argument:

Start or Stop.

Enter “Start” or “Stop” to start or stop the main filter engine.

Start or Stop Socks Server

This task starts or stops the Socks server.

Argument:

Start or Stop.

Enter “Start” or “Stop” to start or stop the Socks server.

Start or Stop Secure Mail Proxy

This task starts or stops the Secure Mail Proxy.

Argument:

Start or Stop.

Enter “Start” or “Stop” to start or stop the Secure Mail Proxy.

Activate Machine Recovery Filter Rules

This task enables a SecureWay Firewall administrator to recover from catastrophic situations on the Firewall server by enabling all secure connections.

Caution This task puts the SecureWay Firewall in an insecure state for recovery purposes only, and it will be necessary to manually re-configure the server to re-secure it.

Start Inetd

This task starts inetd on AIX, which is required to run many SecureWay Firewall services.

Start or Stop HTTP Proxy

This task starts or stops the SecureWay Firewall HTTP Proxy server.

Argument:

Start or Stop.

Enter “Start” or “Stop” to start or stop the HTTP Proxy server.

Start or Stop Configuration Server

This task starts or stops the Configuration Server on a Windows NT SecureWay Firewall server.

Argument:

Start or Stop.

Enter “Start” or “Stop” to start or stop the Configuration server.

Start or Stop Filter Log Service

This task starts or stops the Filter Log Service on a Windows NT SecureWay Firewall server.

Argument:

Start or Stop.

Enter “Start” or “Stop” to start or stop the Filter Log service.

Start or Stop Log Daemon

This task starts or stops the Log Daemon on a Windows NT SecureWay Firewall servers.

Argument:

Start or Stop.

Enter “Start” or “Stop” to start or stop the Filter Log service.

Start or Stop FTP Daemon

This task starts or stops the FTP Daemon on Windows NT SecureWay Firewall servers.

Argument: Start or Stop. Enter “Start” or “Stop” to start or stop the FTP Daemon.

Start or Stop Proxy Telnet Daemon

This task starts or stops the Proxy Telnet Daemon on Windows NT SecureWay Firewall servers.

Argument:

Start or Stop.

Enter “Start” or “Stop” to start or stop the Proxy Telnet Daemon.

Start or Stop Timer NAT Service

This task starts or stops the Timer NAT Service on Windows NT SecureWay Firewall installations.

Argument:

Start or Stop.

Enter “Start” or “Stop” to start or stop the Timer NAT Service.

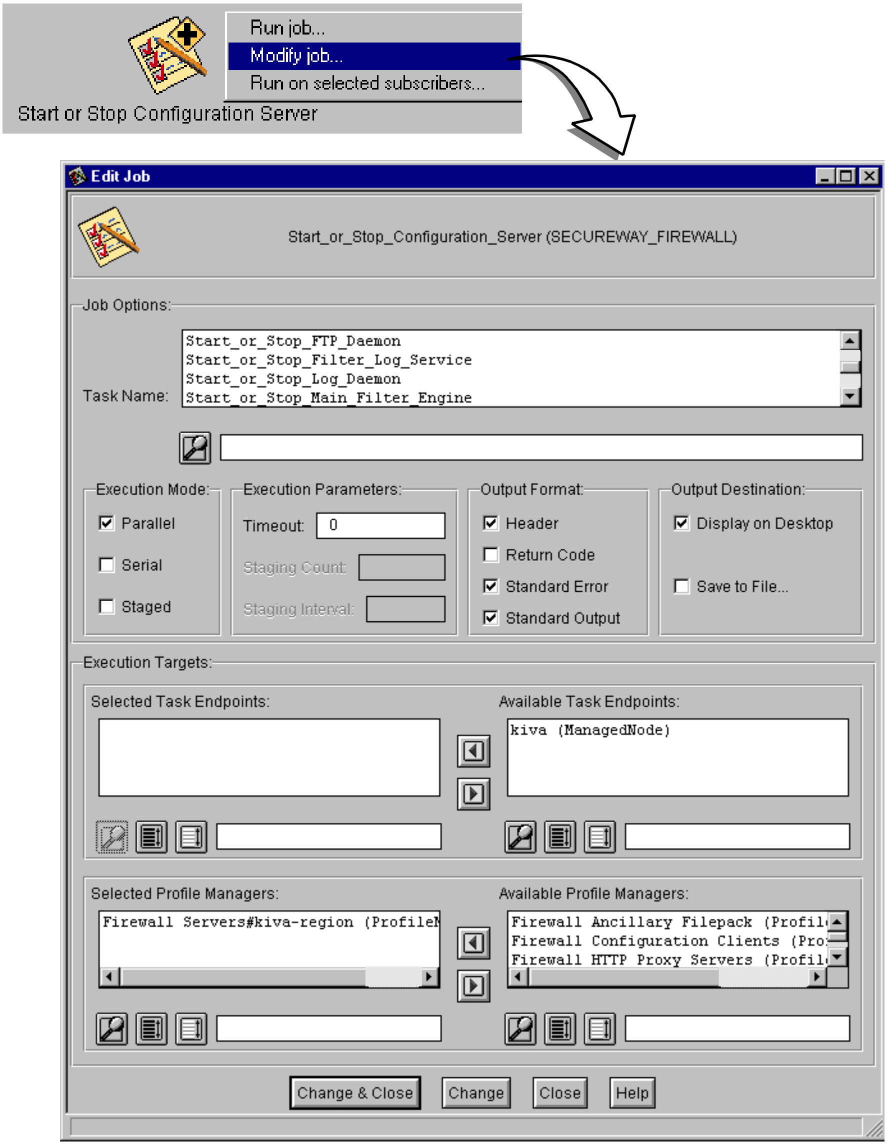
Jobs

A job usually runs on a set of default subscribers and typically produces output in a window on the desktop.

Modifying a Job Configuration

To modify a job, follow these steps before running the job:

1 Right-click the desired task icon, then choose **Modify Job** from the menu. The Edit Job window appears.


Run job...
Modify job...
Run on selected subscribers...
Start or Stop Configuration Server
Edit Job

Start_or_Stop_Configuration_Server (SECUREWAY_FIREWALL)

Job Options:

Task Name:

```
Start_or_Stop_FTP_Daemon
Start_or_Stop_Filter_Log_Service
Start_or_Stop_Log_Daemon
Start_or_Stop_Main_Filter_Engine
```

Execution Mode:

☑ Parallel

☐ Serial

☐ Staged

Execution Parameters:

Timeout: 0

Staging Count:

Staging Interval:

Output Format:

☑ Header

☐ Return Code

☑ Standard Error

☑ Standard Output

Output Destination:

☑ Display on Desktop

☐ Save to File...

Execution Targets:

Selected Task Endpoints:

Available Task Endpoints:

```
kiva (ManagedNode)
```

Selected Profile Managers:

```
Firewall Servers#kiva-region (ProfileM
```

Available Profile Managers:

```
Firewall Ancillary Filepack (Profil
Firewall Configuration Clients (Pro
Firewall HTTP Proxy Servers (Profil
```

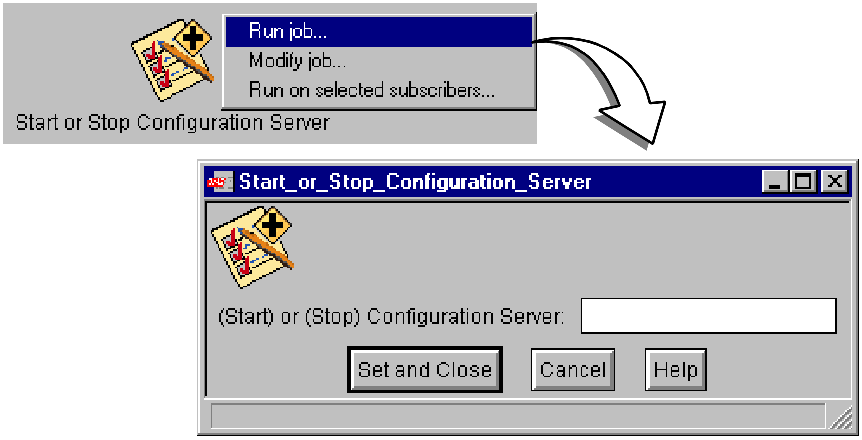
2 Change the parameters as desired, then click **Change & Close**. The job parameters remain in effect each time the job is run.

The default output is sent to a window, from which it can be saved.

Running a Job

To run a job:

1. Right-click the desired task icon and choose **Run Job** from the menu. If job options are required, a prompt appears.


Run job...
Modify job...
Run on selected subscribers...
Start or Stop Configuration Server
Start_or_Stop_Configuration_Server
(Start) or (Stop) Configuration Server:
Set and Close
Cancel
Help

2. Set the options as desired, then click on the **Set and Close** button. An output window appears.
3. Save the output to a file by clicking the **Save to File...** button.
4. Click **Close** when finished.

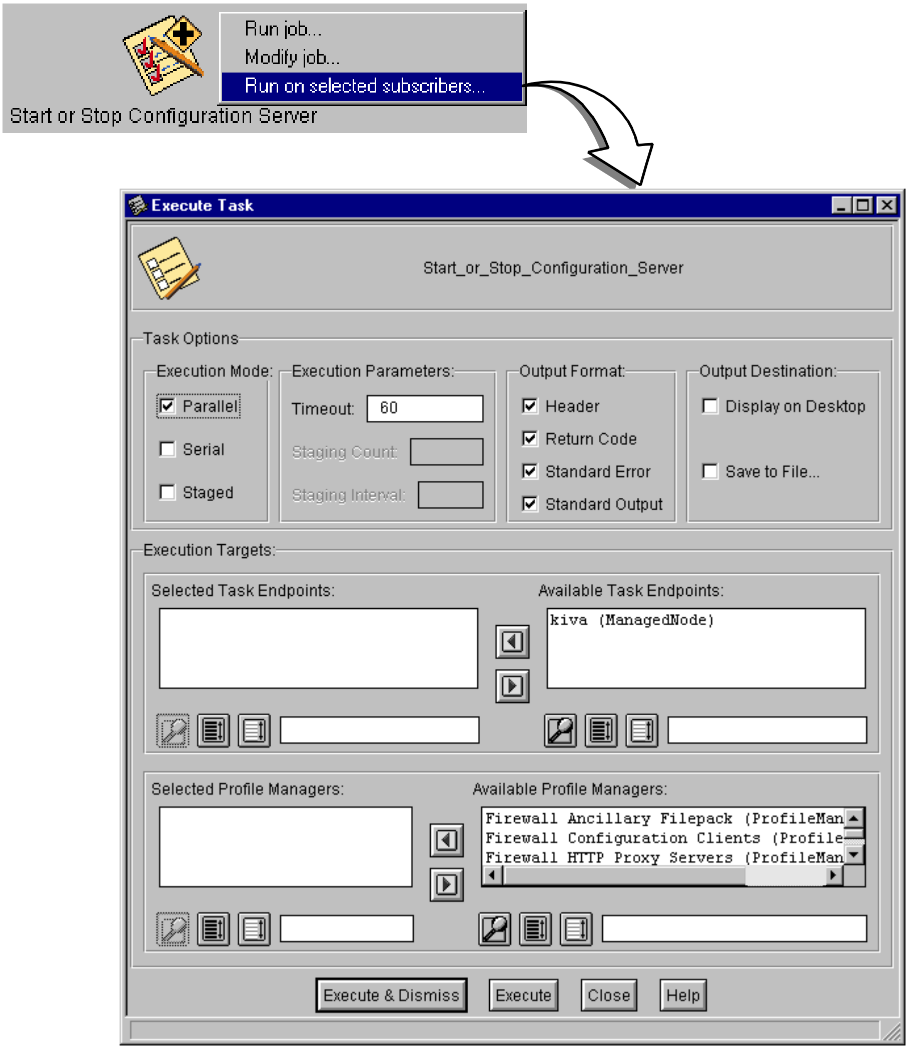
Creating Scheduled Jobs

Sets of operations can be scheduled to run at a particular time. Consult the *TME 10 Framework User's Guide* for details on job scheduling.

Tasks

To run an operation as a task:

1 Right-click the task icon, then choose **Run on selected subscribers**.The Execute Task window appears.



Start_or_Stop_Configuration_Server

Task Options

Execution Mode: ☑ Parallel ☐ Serial ☐ Staged

Execution Parameters: Timeout: 60; Staging Count: ; Staging Interval:

Output Format: ☑ Header ☑ Return Code ☑ Standard Error ☑ Standard Output

Output Destination: ☐ Display on Desktop ☐ Save to File...

Execution Targets:

Selected Task Endpoints:

Available Task Endpoints:

```
kiva (ManagedNode)
```

Selected Profile Managers:

Available Profile Managers:

```
Firewall Ancillary Filepack (ProfileMan
Firewall Configuration Clients (Profile
Firewall HTTP Proxy Servers (ProfileMan
```

Note

Select the desired Task options, then click **Execute & Dismiss**. Note that for a task there are no default subscribers and that, by default, no output is specified.

2 A prompt appears if job options are required.

3 Set the options as desired, then click on the **Execute & Dismiss** button. An output window appears.

4 Click **Save to File** to save the output, if desired.

5 Click **Close** when finished.

7 Uninstalling the Firewall Plus Product

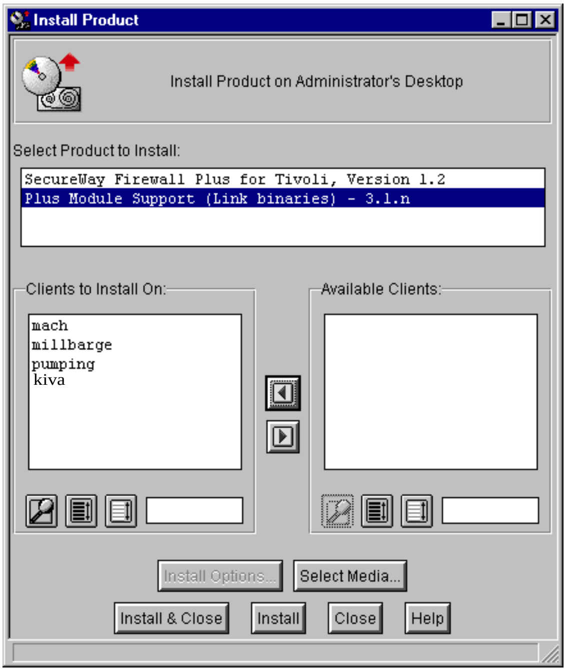
Note

This chapter can also be used to uninstall 1.1 version of the plus module. Please refer to Chapter 1, “Getting Started”, for additional information.

Uninstalling the Firewall Plus module with the GUI

Uninstall SecureWay Firewall Plus for Tivoli version 1.2 with the steps on the following pages.

From the Tivoli desktop select **Desktop** > **Install** > **Install Product...** . The Install Product window appears.

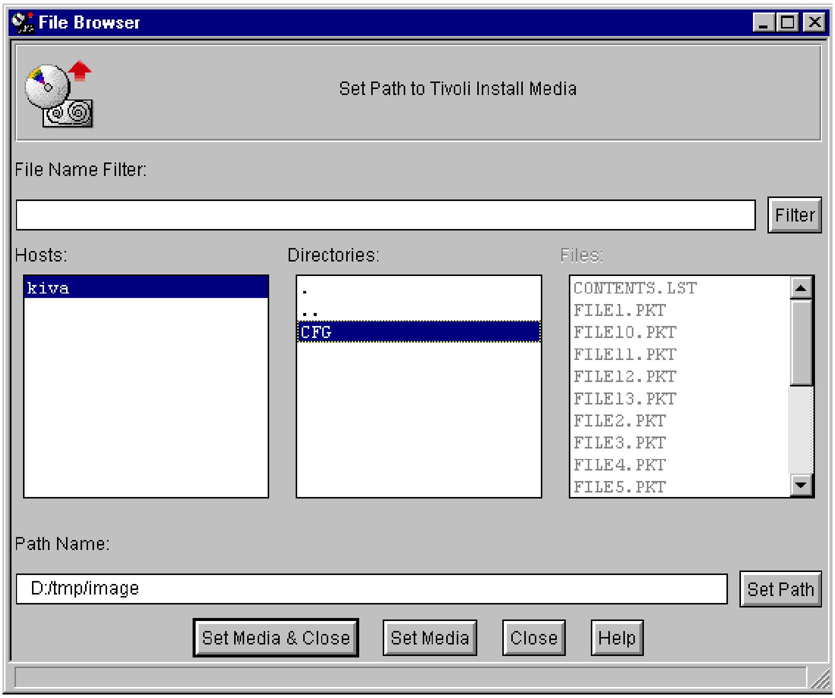


SecureWay Firewall Plus for Tivoli, Version 1.2
Plus Module Support (Link binaries) - 3.1.n

mach
millbarge
pumping
kiva

If the SecureWay Plus for Tivoli module and the Plus Module Support link binary files are listed in the **Select Product to Install** scrolling list, skip to step 3. If they are not listed, proceed to step 2.

6 Click on the **Select Media...** button to display the File Browser window.



Set Path to Tivoli Install Media

File Name Filter:

Hosts:

kiva

Directories:

.
..
CFG

Files:

CONTENTS.LST
FILE1.PKT
FILE10.PKT
FILE11.PKT
FILE12.PKT
FILE13.PKT
FILE2.PKT
FILE3.PKT
FILE4.PKT
FILE5.PKT

Path Name: D:/tmp/image

7 The File Browser window enables you to identify or specify the path to the installation media.

If you already know the path to the CD-ROM image

a. Enter the full path in the **Path Name** field.

b. Click the **Set Path** button to change to the specified directory.

c. Click the **Set Media & Close** button to save the new media path and return to the Install Product window. The window now contains a list of products that are available for installation.

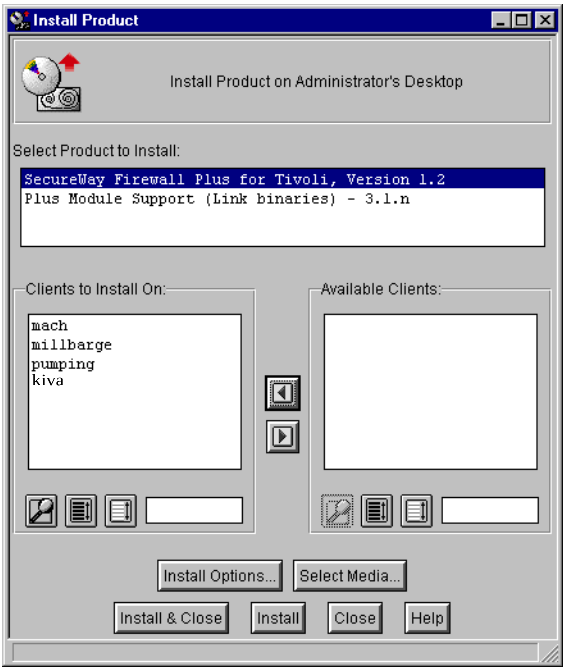
If you do not know the exact path to the CD-ROM image

a. Select the host on which the install media is mounted from the **Host** scrolling list. Selecting a host updates the **Directories** scrolling list to show the directories of the host you chose.

b. Select the directory containing the install media from the **Directories** scrolling list.

c. Click the **Set Media & Close** button to save the new media path and return to the Install Product window. The window now contains a list of products that are available for installation.

8 Select the **SecureWay Plus for Tivoli** entry from the **Select Product to Install** list.



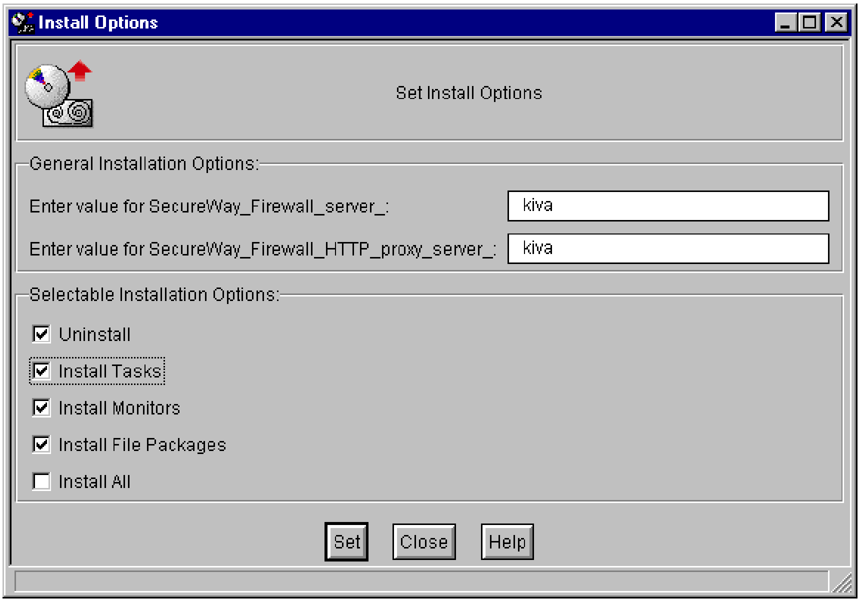
Select Product to Install:

SecureWay Firewall Plus for Tivoli, Version 1.2
Plus Module Support (Link binaries) - 3.1.n

Clients to Install On:

mach
millbarge
pumping
kiva

9 The Set Install Options dialog will appear.



General Installation Options:

Enter value for SecureWay_Firewall_server_: kiva

Enter value for SecureWay_Firewall_HTTP_proxy_server_: kiva

Selectable Installation Options:

☑ Uninstall

☑ Install Tasks

☑ Install Monitors

☑ Install File Packages

□ Install All

In the **Selectable Installation Options** portion of the dialog, check the **Uninstall** box, and any of the boxes below it.

For example:

a. if you wanted to uninstall just the monitors, you would check the **Uninstall** box as well as the **Install Monitors** box.

b. if you wanted to uninstall the entire plus module, you would check the **Uninstall** box and the **Install All** box.

c. alternatively, you could also check the **Uninstall** box, the **Install Tasks** box, the **Install Monitors** box, and the **Install File Packages** box to uninstall the entire plus module.

10 Click the **Set** button to return to the Install Product window.

11 Specify the clients on which the module will be uninstalled by using the arrow keys to move machine names between the **Clients to Install On** scrolling list and the **Available Clients** scrolling list.

a. By default, only the machines in the current Tivoli Management Region that do not have the plus module installed are listed in the **Clients to Install On** scrolling list.

b. Move a machine name to the **Available Clients** list by choosing one or more clients from the **Clients to Install On** scrolling list and clicking the **right-arrow** button. The chosen clients are moved to the **Available Clients** scrolling list.

c. When there are no machine names in the **Clients to Install On** list, move the TMR server in the **Available Clients** list to it, in order to uninstall the plus module on the TMR server.

12 Click the **Continue Install** button to begin the uninstall process.

—OR—

Click the **Cancel** button to abort the uninstall process.

13 When the uninstall process is complete, the Product Install window displays a completion message.

14 Click the **Close** button when the Product Install window indicates that the uninstall process is complete.

Uninstalling the Firewall Plus module from the command line

The following example command uninstalls the Secureway Firewall Plus module:

```
winstall -c cdrom_path [managed node] \
-i index_file UNINSTALL=1 DOTASKS=1 DOMONS=1 DOFPS=1
```

where:

-c *cdrom_path* Specifies the path to the CD-ROM image.

-i *index_file* Specifies the index file from which the product is to be installed.

managed node Specifies the node to uninstall on, which should be your TMR Server.

UNINSTALL=1 Specifies that the module be uninstalled. This must be specified if the module is to be uninstalled.

DOTASKS=1 Specifies that the module’s tasks are to be removed. This item is optional and can be omitted if you do not wish to uninstall the module’s tasks.

DOMONS=1	Specifies that the module's monitors are to be removed. This item is optional and can be omitted if you do not wish to uninstall the module's monitors.
DOFPS=1	Specifies that the module's file packages are to be removed. This item is optional and can be omitted if you do not wish to uninstall the module's file packages.

See the `winstall` command in the *Tivoli Management Platform Reference Manual* for more information.

1 Ensure the correct TMR ("Tivoli Management Region") environment shell script is sourced:

UNIX:

```
. /etc/Tivoli/setup_env.sh
```

Windows NT:

```
%SystemRoot%\system32\drivers\etc\Tivoli\setup_env.cmd
```

2 If you are completely uninstalling SecureWay Plus for Tivoli, remove product-specific binary files on the TMR server and on every node that you uninstalled the SecureWay Plus for Tivoli module:

```
rm -rf $BINDIR/../generic_unix/TME/PLUS/SECUREWAY_FIREWALL
rm -f $BINDIR/../generic_unix/.installed/Secure*
rm -f $DBDIR/.installed/Secure_ALIDB*
rm -rf $BINDIR/../../msg_cat/C/SECUREWAY*
rm -f $BINDIR/../../msg_cat/.installed/Secure*
```

3 You must run the `wchkdb` command after the remove script to verify and modify database resources in the Tivoli environment. (See the *Tivoli Framework Reference Manual* for more information about using the `wchkdb` command.) Run wchkdb on the TMR server with the `-u` argument:

```
wchkdb -u
```

Index