Symantec™ Client Firewall Policy Migration Guide

Symantec Client Firewall Policy Migration Guide

Documentation version 12.01.00.00

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Managed Services	Managed Services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Education Services	Education Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about enterprise services, please visit our Web site at the following URL:

www.symantec.com/business/services/

Select your country or language from the site index.

Migrating policies from Symantec Client Firewall Administrator to Symantec Endpoint Protection Manager

This document includes the following topics:

Migrating Symantec Client Firewall policies

You can use the Symantec Client Firewall Migration Wizard to migrate your Symantec Client Firewall policies to Symantec Endpoint Protection Manager for Symantec Endpoint Protection or Symantec Endpoint Protection Small Business Edition. The wizard converts a Symantec Client Firewall policy into multiple policies that you can import into Symantec Endpoint Protection Manager.

Table 1-1 describes the process that you use to migrate a Symantec Client Firewall policy to Symantec Endpoint Protection Manager.

Table 1-1 Process for migrating Symantec Client Firewall policies

Step	Task
Step 1	Export the Symantec Client Firewall policy file that you want to migrate to the computer on which you run the migration wizard. See "About the policies that the Symantec Client Firewall Migration Wizard generates" on page 8. For more information on how to save a policy, see the *Symantec Client Firewall Administrator Help*.
Step 2	Install the migration wizard on either the computer that runs Symantec Endpoint Protection Manager or another computer. See "Installing the Symantec Client Firewall Migration Wizard" on page 12.
Step 3	Run the migration wizard to convert the Symantec Client Firewall policy file into multiple policy files. See "Converting a Symantec Client Firewall policy to multiple Symantec Endpoint Protection Manager policies" on page 13.
Step 4	Import the output policy files into Symantec Endpoint Protection Manager. See "Importing migrated policies into Symantec Endpoint Protection Manager" on page 14.

About the policies that the Symantec Client Firewall Migration Wizard generates

The migration wizard converts a single Symantec Client Firewall policy file into two types of Symantec Endpoint Protection Manager policies: a Firewall policy and an Intrusion Prevention policy.

For each Symantec Client Firewall policy, the migration wizard creates the following firewall policies:

- **Firewall Policy** for the default location
- **Firewall Policies** for each additional location
- **Firewall Policy** for pRules

For each Symantec Client Firewall policy, the migration wizard creates an Intrusion Prevention policy.

The exported Symantec Client Firewall Administrator policies use the following formats:

- The .cfp and .xml formats are full policy files with all the settings.
- The .cfu format is an updated policy file.

From these files, the migration wizard generates .dat files that are stored in a .zip format.

Table 1-2 lists the policy files that the migration wizard generates from the .cfp and .xml formats, their corresponding output file names, and the file content.

Table 1-2 Output policy file name and content

Symantec Client Firewall Migration Wizard output	Output file name	Description of Symantec Client Firewall Administrator content
Firewall Policy—Default Location	<*input file name*>.dat	Contains all of the Rules and Zone settings that are associated with the Default Location and the Client Settings.
Firewall Policy—All Locations	<*input file name*>_<location>.dat	One Symantec Endpoint Protection Manager Firewall policy is created for each location in the input policy. Each location-specific policy contains all of the Rules and Zone information that is associated with that location and the Client Settings from the input policy.
Firewall Policy—pRules	<*input file name*>_prule.dat	Contains all of the pRules and the Client Settings in the input policy.

Table 1-2 Output policy file name and content *(continued)*

Symantec Client Firewall Migration Wizard output	Output file name	Description of Symantec Client Firewall Administrator content
IPS Policy	<*input file name*>_ips.dat	Contains the following intrusion protection system settings: ■ Addresses on the **Zones** > **AutoBlock Exclusions** tab. ■ Signatures on the **IPS** tab. Symantec Endpoint Protection Manager does not migrate intrusion protection system V1.x signatures. ■ Intrusion Prevention settings on the **Client Settings** > **General** tab.

The migration wizard generates Symantec Client Firewall Administrator policies in the .cfu format to **Firewall Policy—Default Location** and **Firewall Policy—pRules** policies only.

See "Converting a Symantec Client Firewall policy to multiple Symantec Endpoint Protection Manager policies" on page 13.

See "Migrating Symantec Client Firewall policies" on page 8.

About the order in which firewall rules are generated

The migration wizard converts Symantec Client Firewall tab settings to firewall rules in the Symantec Endpoint Protection Manager Firewall policies. The migration wizard also places these firewall rules in a specific order. This order is based on the tab from which the content came in Symantec Client Firewall Administrator.

Table 1-3 describes the order in which the migration wizard places the rules and settings from Symantec Client Firewall into the **Firewall Policy—Default Location** policy and the **Firewall Policy—All Locations** policy.

Table 1-3 Location-specific firewall policies

Order	Symantec Client Firewall Administrator tab
1	**Zones** ■ **Restricted Zone** ■ **Trusted Zone** **Note:** The settings on the AutoBlock Exclusions and Zone Settings tabs do not migrate.
2	**Client Settings** ■ **Client Settings** > **Protocol Filtering** ■ Other settings on the **Client Settings** tab
3	**Rules** ■ **General Rules** ■ **Program Rules** ■ **Trojan Rules** ■ Default rule The migration wizard adds a default rule to the bottom of the policy. For any traffic that the other migrated firewall rules ignore, the default rule asks users to allow or blocks the traffic.

Table 1-4 displays the order in which the migration wizard places the pRules policy from Symantec Client Firewall into the **Firewall Policy—pRules** policy.

Table 1-4 pRules policy order

Order	Symantec Client Firewall Administrator tab
1	**pRules**
2	Default rule

See "Importing migrated policies into Symantec Endpoint Protection Manager" on page 14.

About installing the Symantec Client Firewall Migration Wizard

The Symantec Client Firewall Migration Wizard includes two files, `SCFMigrationTool.bat` and `SCFMigrationTool.jar`. These files are available in

the TOOLS folder on the installation product disc and from Symantec Technical Support.

The migration wizard also requires Java Runtime Environment (JRE) 1.6 or later and does not include this software. The wizard runs on all operating systems that Symantec Endpoint Protection Manager supports. Symantec Endpoint Protection Manager does not run on Windows Vista, and Windows Vista is not supported.

If you install the migration wizard on a computer that runs Symantec Endpoint Protection Manager, installing JRE 1.6 is not necessary. Symantec Endpoint Protection Manager automatically installs JRE 1.6. If you install the migration wizard on a computer that does not run Symantec Endpoint Protection Manager, you must install JRE 1.6 or later on that computer.

You can download JRE 1.6 from http://www.sun.com.

If you install the Symantec Client Firewall Migration Wizard on a computer that does not run Symantec Endpoint Protection Manager, you must set the PATH environment variable. The PATH environment variable must point to the JRE run-time folder. An example of a PATH command that you run from a command prompt follows:

```
PATH=%PATH%;c:\Program Files\Java\jre1.6.0_07\bin
```

The %PATH%; entry preserves the existing path information, and the JRE folder information is appended to the existing path information. You can display the current path information with the PATH command.

Symantec recommends that you install the Symantec Client Firewall Migration Wizard on the same computer as Symantec Endpoint Protection Manager. You also need to copy the Symantec Client Firewall policies to the same computer on which you run the migration wizard.

See "Converting a Symantec Client Firewall policy to multiple Symantec Endpoint Protection Manager policies" on page 13.

Installing the Symantec Client Firewall Migration Wizard

Symantec recommends that you install the Symantec Client Firewall Migration Wizard on the same computer as Symantec Endpoint Protection Manager. You also need to copy the Symantec Client Firewall policies to the same computer on which you run the migration wizard.

See "Converting a Symantec Client Firewall policy to multiple Symantec Endpoint Protection Manager policies" on page 13.

To install the Symantec Client Firewall Migration Wizard

- On a computer that runs Symantec Endpoint Protection Manager, copy `SCFMigrationTool.bat` and `SCFMigrationTool.jar` to the following directory:

  drive:\Program Files\Symantec\Symantec Endpoint Protection Manager\bin

Converting a Symantec Client Firewall policy to multiple Symantec Endpoint Protection Manager policies

You can use the migration wizard to convert an exported Symantec Client Firewall policy to multiple Symantec Endpoint Protection Manager policies. The migration wizard requires that you select an input policy file and an output folder to place the converted policy files.

See "About the policies that the Symantec Client Firewall Migration Wizard generates" on page 8.

To convert a Symantec Client Firewall policy to multiple Symantec Endpoint Protection Manager policies

1. Copy the policies to migrate to an output folder on the same computer as you installed the migration wizard.

   See "Installing the Symantec Client Firewall Migration Wizard" on page 12.
2. Browse to and double-click `SCFMigrationTool.bat`.
3. In the **Welcome** panel, click **Next**.
4. In the **Policy File Selection** panel, click **Browse** to locate a policy file to migrate from.
5. In the **Output Directory Selection** panel, click **Browse** to locate the output folder, and then click **Next**.
6. In the **Options and Migration** panel, optionally uncheck the policy files that you do not want to create, and then click **Migrate**.
7. When the migration completes, in the **Migration Status** panel, click **Report** to review the rules and options that were migrated.

8 Click **Finish**.

9 Review the .dat files that are created in your output folder.

You can then import these files into Symantec Endpoint Protection Manager.

See "Importing migrated policies into Symantec Endpoint Protection Manager" on page 14.

Importing migrated policies into Symantec Endpoint Protection Manager

The migration wizard generates two types of policies that you can import: multiple firewall policies and an Intrusion Prevention policy.

Note: Make sure that you import a Firewall policy as a Firewall policy and not as an Intrusion Prevention policy. Make sure that you import an Intrusion Prevention policy as an Intrusion Prevention policy and not as a Firewall policy. Otherwise, the policies do not migrate correctly.

When you convert policies from Symantec Client Firewall Administrator to Symantec Endpoint Protection Manager, the following changes occur:

- Zone Rules and pRules that were locked when migrated from the Symantec Client Firewall Administrator are unlocked in the Symantec Endpoint Protection Manager. They can be modified after they are imported.
- All Symantec Client Firewall Administrator rules with the **Monitor** action are disabled when they are migrated to the Symantec Endpoint Protection Manager. The action is reset to **Allow** and logging is enabled.
- **Custom Alert Text** entries are truncated to 127 characters in Symantec Endpoint Protection Manager.

Note: Symantec Endpoint Protection Small Business Edition has one location only. Because the Symantec Client Firewall Migration Wizard creates one policy file for each location, you can import one location-specific policy file only.

See "About the policies that the Symantec Client Firewall Migration Wizard generates" on page 8.

To import migrated policies into Symantec Endpoint Protection Manager

1 Log on to Symantec Endpoint Protection Manager.

2 In the console, click **Policies**.

3. Do one of the following tasks:
   - Under **Policies**, click **Firewall**.
   - Under **Policies**, click **Intrusion Prevention**.
4. Do one of the following tasks:
   - Under **Tasks**, click **Import a Firewall policy**.
   - Under **Tasks**, click **Import an Intrusion Prevention policy**.
5. In the **Import Policy** dialog box, browse to and select a migrated policy in your output folder.
6. In the right pane, click the imported policy.
7. Under **Tasks**, click **Edit the policy** and review the migrated policy.

About the firewall rules for an imported location-specific policy

For each location, Symantec Endpoint Protection Manager creates firewall rules with an Allow, Block, or Ask action that duplicates the behavior of settings in Symantec Client Firewall Administrator.

The firewall rules are based on the combined values that you specified in the following Symantec Client Firewall Administrator settings:

- **Rule exception handling** setting for a location on the **Locations** > **Connection Management** tab.
- **Custom Security Level - Firewall Level** on the **Client Settings** > **General** tab.
- **Custom Security Level - Access Control Alerts** on the **Client Settings** > **General** tab.

See "About the policies that the Symantec Client Firewall Migration Wizard generates" on page 8.

Table 1-5 shows the firewall rules that Symantec Endpoint Protection Manager creates for each location.

Table 1-5 Firewall rules that the management server creates for a location-based policy

If the rule exception handling setting is...	The firewall level setting is...	The access control alert setting is...	Then the Symantec Endpoint Protection Manager firewall rule action is...
BLOCK	Ignored	Ignored	**Block**
PERMIT	Ignored	Ignored	**Allow**
PROMPT	Ignored	**ENABLE**	**Ask**
PROMPT	**Medium**	**DISABLE**	**Allow**
PROMPT	**High**	**DISABLE**	**Block**

For example, if the rule exception handling setting is **PROMPT** and the access control alert setting is **ENABLE**, the firewall rule action is converted to **Ask** in Symantec Endpoint Protection Manager. If the rule exception handling setting is **BLOCK**, the firewall rule action is converted to **Block**.

Note: For Symantec Endpoint Protection Small Business Edition, you cannot create a firewall rule with an **Ask** action, you can only import a rule with an **Ask** action.

Migrating failed policies

Five security policies have failed migration from Symantec Client Firewall Administrator to Symantec Endpoint Protection Manager.

Table 1-6 shows the failed policies and the versions in which they are found.

Table 1-6 Failed policies

Defect number	Security policy	Symantec AntiVirus version
1142104	retailprules.cfu	9.x
1142133	VeryHighSecurity.xml	10 or 10.1
1142130	HighSecurity.xml	10 or 10.1
1142126	MediumSecurity.xml	10 or 10.1
1142121	LowSecurity.xml	10 or 10.1

The following procedure details a workaround that enables you to migrate these security policies.

To migrate the failed policies

1. Open the Symantec Client Firewall Administrator.
2. If you migrate from Symantec AntiVirus 9.x, select the retailprules.cfu policy from the cd4 folder.
3. If you migrate from Symantec AntiVirus 10 or 10.1, select one of the following security policies from the cd4 folder:
   - VeryHighSecurity.xml
   - HighSecurity.xml
   - MediumSecurity.xml
   - LowSecurity.xml
4. Import the security policy into the Symantec Client Firewall Administrator.
5. Export the security policy from the Symantec Client Firewall Administrator using the **Save As...** command.

   The firewall administrator saves the file with a .cfp file extension.
6. Open the Symantec Client Firewall Migration Wizard using the `SCFMigrationTool.bat` file from the command prompt.
7. In the migration wizard, browse and select the security policy file with the .cfp file extension.
8. Specify an output folder.
9. Click **Next** and **Migrate**.
10. Click **Finish**.

    The .dat files appear in your output folder and can be used in Symantec Endpoint Protection Manager.

See "Importing migrated policies into Symantec Endpoint Protection Manager" on page 14.