



SmartFilter Software Overview

This chapter describes Secure Computing Corporation SmartFilter Software, Release 3.1.2 for Cisco Content Engines running ACNS software, Release 5.0. This chapter provides an overview of SmartFilter software, including the SmartFilter Control List. This chapter contains the following sections:

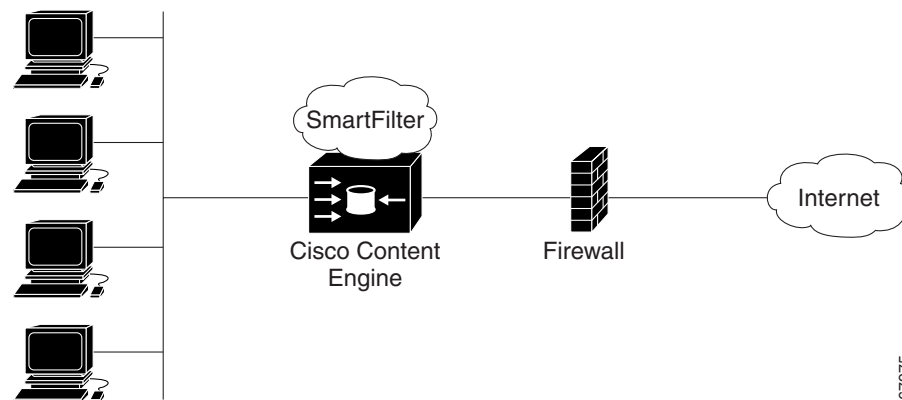
- [About This SmartFilter Software Release, page 1-1](#)
- [Inside the SmartFilter Software, page 1-7](#)

About This SmartFilter Software Release

SmartFilter software is a specialized URL filtering software product installed on Cisco Content Engines that operate with Cisco ACNS software. SmartFilter software operates inside your network to control user access to outside Internet resources and allows you to restrict access to World Wide Web pages.

SmartFilter software transparently controls access to HTTP resources by network users internal to your organization and allows you to implement an Internet access policy for your organization. SmartFilter software integrates seamlessly with the Cisco Content Engine behind the firewall or router, as shown in [Figure 1-1](#).

Figure 1-1 SmartFilter Software Installed on the Cisco Content Engine Running Behind a Firewall



License Activation Certificate

Cisco Systems provides you with an activation certificate that contains a unique SmartFilter software license number. When the SmartFilter software license number is entered into the <http://www.smartfilter.com/cisco> website, it allows you to obtain a SmartFilter software login username, password, and license activation keys. The license activation keys are for SmartFilter software and the Cyfin Reporter for SmartFilter software.

SmartFilter Administration Software

SmartFilter software running on a Cisco Content Engine is controlled by configuration files that are generated and distributed to individual Content Engines by the SmartFilter Administration Console graphical user interface application through the SmartFilter Administration Server. The SmartFilter Administration Console communicates through the SmartFilter Administration Server directly with the Cisco Content Engines.

The SmartFilter Administration Console and SmartFilter Administration Server run on a UNIX (Linux or Solaris) or Microsoft Windows (NT or 2000) operating system of your network host. Your Content Engines use the SmartFilter Administration Console to perform the following tasks:

- Download the most recent list of blocked URLs (the SmartFilter Control List).
- Customize the Control List of blocked URLs for your enterprise organization.
- Distribute (through the SmartFilter Administration Server) the updated configuration to each Cisco Content Engine (one at a time or as a group) in the form of SmartFilter software configuration files exported to the Cisco Content Engine *local1/smartfilter* system file system (sfs) directory, as shown in [Example 1-1](#).

Example 1-1 Location of SmartFilter Software Configuration Files on the Cisco Content Engine

```
ContentEngine# cd smartfilter
ContentEngine# pwd
/local1/smartfilter
ContentEngine# dir
      size      time of last change      name
-----
      161   Sun Jan 19 21:13:36 2003   README
     16804   Sun Jan 19 21:13:36 2003   config.txt
      3386   Sun Jan 19 21:13:36 2003   patterns.txt
      2087   Sun Jan 19 21:13:36 2003   search.txt
     118289  Thu Jan 16 21:44:43 2003   sf.log
    1567337   Sun Jan 19 21:13:36 2003   sfagent
       371   Sun Jan 19 21:13:36 2003   sfagent.txt
       951   Sun Jan 19 21:13:36 2003   sfagent_control
        52   Sun Jan 19 21:13:36 2003   sfcontrol
         12   Sun Jan 19 03:00:04 2003   sfcontrol.current
         84   Sun Jan 19 21:14:50 2003   sfftp.stat
      3054   Sun Jan 19 21:13:36 2003   site.txt
        981   Sun Jan 19 21:13:36 2003   users.txt
ContentEngine#
```

Comments within the text files provide additional guidelines for configuring SmartFilter software.

Key Benefits

SmartFilter software delivers exceptional flexibility and performance.

- The most accurate URL Control List in the industry eliminates user frustration and minimizes help desk calls.
- SmartFilter software’s customizable filtering policy allows you to make the right enforcement choices for your organization.
- The SmartFilter software On-Box architecture requires no additional hardware.
- On-Box filtering has a nearly transparent impact on proxy server and network performance.
- Management-ready reports are delivered directly to the manager’s desktop without the need for Information Technology (IT) involvement.
- Minimal IT administration is required after installation.
- Remote management allows you to configure and manage multiple SmartFilter software plug-in proxy servers, regardless of platform, from one vantage point.
- SmartFilter software preserves network bandwidth otherwise consumed by unauthorized Internet surfing.
- 24 x 7 “live answer” support is always there when you need it—at no extra cost.

Key Features

SmartFilter software supports a variety of monitoring and control features designed to ensure that Internet use is productive and appropriate for your organization.

You can enable or disable the individual SmartFilter software configuration options to tailor Internet use to your organization’s unique access policies and network environment. This allows you to modify your SmartFilter software configuration as your organization’s Internet usage evolves. [Table 1-1](#) highlights the key SmartFilter software features.

Table 1-1 SmartFilter Software Key Features

Feature	Summary
Remote administration	Simplifies administration of large-scale installations. Plug-ins can be configured individually or in groups.
Filtering and blocking	Allows you to define the specific types of URLs that you want to filter from a list of 30 pre-defined categories plus 10 user-defined categories in the SmartFilter Control List. Standard blocking feature of the SmartFilter software allows you to create customized messages that are displayed to users who attempt access to blocked sites.
Coaching	Allows you to specify a predefined message or warning that is displayed to users informing them that the site has been filtered, but giving them the option to proceed at their own risk.

Table 1-1 SmartFilter Software Key Features (continued)

Feature	Summary
Delay	Allows you to slow the downloading of filtered sites. This delay feature is unique to SmartFilter software. By deliberately slowing the download process, SmartFilter software discourages users from browsing nonbusiness or objectionable Internet sites in the workplace or educational environment while preserving network bandwidth for business- or education-related applications.
Redirect blocked URLs	Enables you to “redirect” a user to a separate web page containing a blocking message or additional information on your company’s Internet usage policy. This feature is useful if you have more advanced messaging requirements.
Custom restrictions on identified workstations or users	<p>Allows you to restrict Internet access through the use of configurable policies that are grouped based on client usernames or workstation IP addresses. For example, you can:</p> <ul style="list-style-type: none"> • Create a global policy to restrict access to URLs across the company. • Permit unrestricted access to a group of users such as your internal administrators. • Permit less restricted access to a series of workstations in your company, such as those workstations located on a test lab network.
Directory services integration	Supports dynamic querying of user group information from one or more user directories, such as Lightweight Directory Access Protocol (LDAP), Active Directory, or the internal SmartFilter software database. These directories can be configured and ordered for query precedence—eliminating the need to duplicate user data.
Time of day restrictions	Defines both the type of access for a URL and the specific time of day during which the access applies. For instance, an organization might deny access to certain URLs only during work or school hours or during high-traffic periods.
Automated FTP or HTTP Control List download	Configures SmartFilter software to automatically download the SmartFilter Control List twice a week, once a week, or once a month. Or, you can choose to update the file manually, at any time, with the click of a button.
Incremental Control List download	<p>Downloads the difference between your existing SmartFilter Control List and the most recent SmartFilter Control List. These changes are represented by incremental files that are appended to your existing Control List to produce a new list.</p> <p>Note If you use this option without having an existing SmartFilter Control List, a full Control List is downloaded.</p>
Customizable categories	Allows you to create user-defined categories as well as use the 30 predefined SmartFilter Control List categories.
Reporting and logging	Creates a variety of HTML-based reports showing detailed, outbound Internet usage activities with the Secure Computing Cyfin Reporter for SmartFilter software. When Cyfin Reporter is integrated with SmartFilter software, it delivers a complete Internet management solution.

SmartFilter Software Deployment

A Cisco Content Engine with SmartFilter software can filter both proxy-style and transparently received HTTP requests. SmartFilter software analyzes requests and determines, based on content category rules and corporate guidelines, whether or not URLs are business-related and allows or denies requests as appropriate. For further information on proxy-style and transparent cache deployments of the Content Engine, refer to the *Cisco ACNS Software Caching Configuration Guide*.

Informing Users About Your Access Policy

We strongly recommend that your organization disclose to network users the nature of your site's Internet access policy. For example, inform your network users that Internet activity is being monitored, and that management has access to a log of visited sites. It is also recommended that you create a "Corporate Acceptable Use Statement" in HTML and link it to the user-definable SmartFilter software error message. To do this with the SmartFilter software product, see the "[Creating a Message for a Coached Category](#)" section on page 7-18.

SmartFilter Remote Administration

SmartFilter software remote administration consists of a three-tiered architecture, including a Java-based client user interface (called the SmartFilter Administration Console), a Java-based Administration Server, and lightweight administration agents, which reside on the proxy platforms.

Administration Server

All configuration data is stored in the Administration Server and is deployed to the various proxy plug-ins through the administration agents when required.

Administration Console

Configuration data is modified through the Administration Console, which interacts with the Administration Server through the network. Other than the IP address of the Administration Server, the Administration Console does not store any configuration data locally.

Administration Agent and Proxy Plug-In

The administration agent and proxy plug-in are always installed in and reside on the same Cisco Content Engine. In addition to communicating with the Administration Server, the administration agent is responsible for Control List downloads.

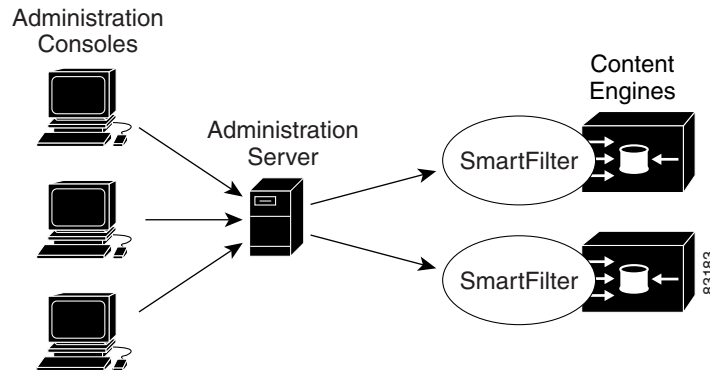
Administration Options

This section provides an illustration and a description for each of the supported administration configuration options.

Enterprise Configuration

The Administration Server, Administration Console, and administration agents or proxy plug-ins can each be installed on different hosts connected through an IP network, as shown in [Figure 1-2](#), allowing your SmartFilter software administrator to manage SmartFilter software from anywhere in the world.

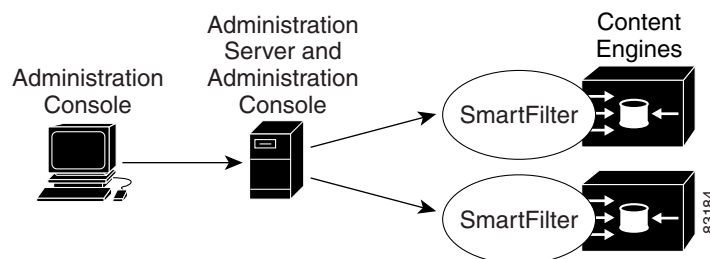
Figure 1-2 Enterprise Configuration



Large Company Configuration

The Administration Server and Administration Console can be installed on the same device, as shown in [Figure 1-3](#), with each administration agent located on a separate proxy server host connected through an IP network. Using this configuration does not preclude you from adding a remote Administration Console.

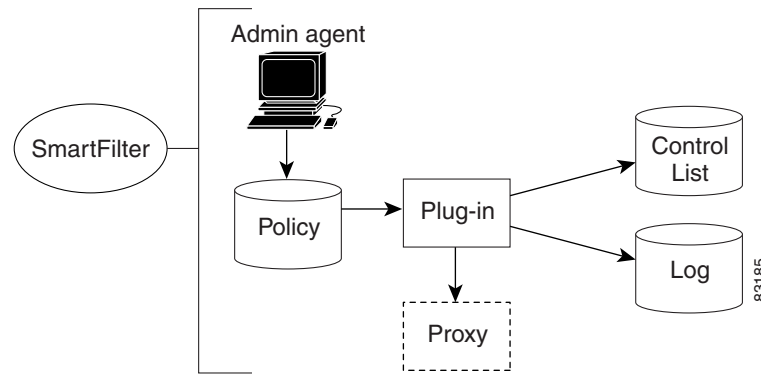
Figure 1-3 Large Company Configuration



Inside the SmartFilter Software

As shown in [Figure 1-4](#), SmartFilter software consists of an operating system-specific SmartFilter program (or plug-in) and a SmartFilter Control List installed on a system in your network.

Figure 1-4 SmartFilter Software Components



SmartFilter Administration Software

You must download both SmartFilter administration components from the Secure Computing website (<http://www.securecomputing.com>) and install them on your workstation before you can use the SmartFilter software. The SmartFilter administration components include the SmartFilter Administration Server software and SmartFilter Administration Console software. SmartFilter administration software is available at no charge.

SmartFilter Plug-In Software

The latest SmartFilter plug-in software comes preinstalled on the Cisco Content Engine.

Control List Subscription

Purchasing a SmartFilter Control List subscription is required to successfully deploy SmartFilter software. Twice a week, Secure Computing Corporation posts an updated Control List to the SmartFilter FTP server. As shown in [Figure 1-5](#), you can keep your company's Control List up to date by downloading the Control List from <http://list.smartfilter.com/cgi-bin/getlist.cgi>.

Figure 1-5 Subscription to the Control List Allows Access to the Latest URL Database



**Tip**

The Internet is dynamic and ever-changing, and you are encouraged to update the Control List twice a week from Secure Computing Corporation's download server. For instructions on using SmartFilter software to connect to the download site, see the [“Scheduling Control List Downloads”](#) section on [page 6-2](#).
