Compliant Enterprise

The Compliant Enterprise Active Control System

Release 2.0

Enforcer Administrator's Guide

May 2007

NextLabs welcomes comments or suggestions regarding this manual or any of our product documentation. Please send an e-mail to info@nextlabs.com.

TRADEMARKS

LICENSE AGREEMENT

Published in San Mateo, CA, by NextLabs, Inc.
www.nextlabs.com
info@nextlabs.com
650.577.9101

Document Revision Number: EAG2.0-B03

Contents

Preface

Welcome to the Compliant Enterprise Active Control System, the information control platform that eliminates policy silos, controls information disclosure inside and outside the enterprise, and provides universal control over information access and use along with real-time enforcement. Only NextLabs delivers an Active Control System that can comprehensively enforce information access entitlements, protect end points while data is in use, and maintain reliable information barriers.

Available Enforcers

This manual combines information about all Compliant Enterprise policy enforcers available as of publication date. The most recent releases of these include:

- Windows Desktop Enforcer, release 1.6
- Windows File Server Enforcer, release 1.6
- Linux File Server Enforcers, release 1.0
- SharePoint Server Enforcers, release 1.0

Chapter 1 provides an overview of enforcers and describes the administrative procedures common to all types. The remaining chapters provide installation instructions and other administrative information specific to each type.

Product Documentation

The Compliant Enterprise documentation set consists of eight titles: an introductory *Product Overview*; a *Getting Started Guide* with installation and configuration instructions; an *Implementation Guide* to help with strategies for auditing information use and designing policies; an administrator's guide for all enforcers and one for the system overall; user's guides for Policy Author and Reporter; and a guide to the predefined active control solutions available with release 2.0.

Product Overview

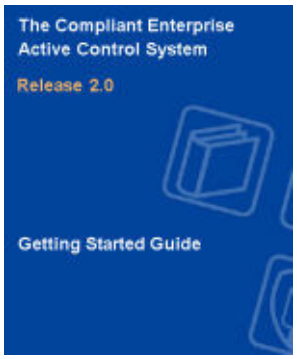
Because Compliant Enterprise is a powerful, distributed enterprise product, its components are likely to be used by a number of different users in any given organization. Even though various users may be engaged exclusively with individual components of the suite and may not be interested in any others, we strongly recommend that all users read the *Product Overview* carefully, in order to acquaint themselves with the high-level architecture and function of the platform as a whole.

Getting Started Guide

The *Getting Started Guide* provides instructions on planning your system architecture and installing the Control Center and Policy Author.

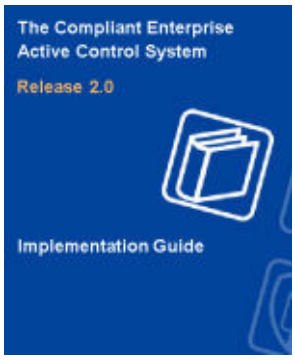
The installation procedures for all policy enforcers are provided separately, in the *Enforcer Administrator's Guide*.

Instructions on enrolling network entities, which is required after installation, are also provided separately, in the *System Administrator's Guide*.



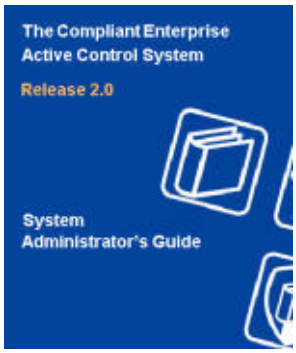
Implementation Guide

The *Implementation Guide* provides a high-level approach to designing and implementing the information control policies that best suit your enterprise's needs. It offers generic advice on analyzing your needs through information use audits, approaches to designing appropriate policies, and optimizing those policies based on ongoing monitoring.



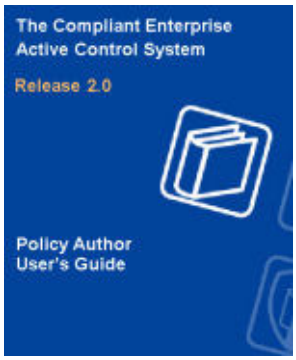
System Administrator's Guide

The *System Administrator's Guide* provides information required for managing and maintaining the Compliant Enterprise system once it is set up. It provides complete instructrions on enrolling all kinds of network entities, which is required after the initial software installation. It also includes all user information for the administrative web application called Administrator, as well as for all utilities and other tools provided with the product. It is directed at the IT specialists who will be responsible for maintaining the Control Center after it has been installed.



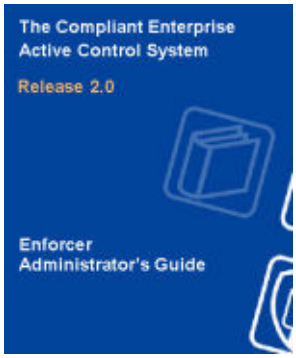
Policy Author User's Guide

The *Policy Author User's Guide* provides complete information on how to use Policy Author, the user interface where you build, deploy, and manage your information control policies and the library of policy components they are built upon. It is intended for the Compliant Enterprise user who will be responsible for converting generically expressed information policy goals into the specific, ACPL-based policy controls that are actually distributed to enforcement points throughout the enterprise.



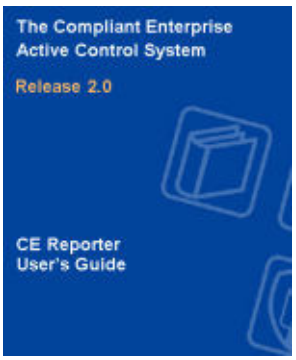
Enforcer Administrator's Guide

This *Enforcer Administrator's Guide* provides information on installing, using and maintaining all the types of enforcers currently available for Compliant Enterprise: for file servers (Windows and Linux), Windows desktops, and SharePoint servers. It is intended for the technical specialists who will be managing the enforcers; these may be the same as the Control Center administrators, or they may be different.



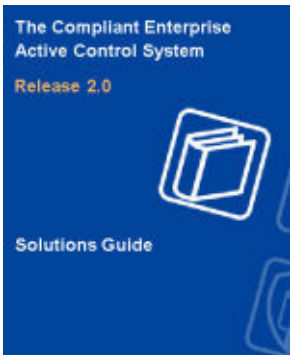
CE Reporter User's Guide

The *Reporter User's Guide* provides complete information on how to use Reporter, the web-based application that lets you easily generate reports on information use and access in your enterprise, and on the performance of your deployed policies. It is required reading for anyone with permission to generate or view Compliant Enterprise reports.



Solutions Guide

The *Solutions Guide* provides detailed information on customizing and using the pre-designed Active Control Solutions that are included with Compliant Enterprise: for Information Entitlements, for Endpoint Data Protection, and for Business Information Barriers.



Current Versions

Documents distributed in PDF format can become obsolete as subsequent versions are released. If you would like to check whether you are using the most current version of this or any manual, check the Document Control Number (DCN) at the bottom right of the inside cover, then click here to view a table of the most current versions of all Compliant Enterprise manuals. If the version listed in that table is later than the one in this manual, contact info@nextlabs.com to request the more recent version.

Release Notes

The release notes for each release of Compliant Enterprise are available directly on the installation CD, from the link on the splash screen or from the Docs directory. They describe any features or changes that could not be included in the documentation, and provide a list of known problems with the current version, along with suggested workarounds when appropriate.

Feedback

Feedback from Compliant Enterprise users is a valuable resource in helping our Product Information group provide you with the highest quality documentation as our product line develops. To this end, we would appreciate any comments you have on this manual or on any other Compliant Enterprise documentation; please send all feedback to info@nextlabs.com.

1 Introducing Policy Enforcers

In this chapter we provide a brief description of the role of Policy Enforcers within the Compliant Enterprise system, and an overview of some of the administrative procedures that are common to all types. The chapter has the following sections:

Additional information specific to each type of enforcer is provided in the later chapters of this manual.

About Enforcers

Policy Enforcer is the generic term for the Compliant Enterprise clients that monitor and enforce access to and use of information sources. The rules that govern such access and use are referred to as *policies*. We use the term *subject* to mean to any network user whose activity is controlled by currently defined policies.

As we mentioned earlier in this manual, there are three types of Policy Enforcers: File Server Enforcers, Desktop Enforcers, and SharePoint Enforcers. File Server Enforcers are available for Windows or Linux; Desktop and SharePoint Enforcers run on Windows only.

- **File Server Enforcers** are installed on Windows or Linux file servers in your network, and run continuously to enforce any policies governing the files stored on that server. They control various kinds of access to that location only—whether a given subject can open, edit, save, or rename files there, or create and save new files.
- **Desktop Enforcers** are installed on desktop or laptop PCs, and run continuously to monitor and enforce all policies that govern any user logging onto that individual device. They control not only whether subjects can access files from a specific location, but also how they can use them after making a local copy—including such actions as renaming, copying and pasting contents, and sending as an e-mail or instant message attachment.

- **SharePoint Enforcers** are installed on the server where Microsoft SharePoint is running, and monitor and control users' access to the contents of the portal. The kind of access control they provide is very similar to the way file server enforcers control access to file server resources.

Enforcers are responsible for both enforcing policy and collecting audit information about their respective host systems. Working together, the three types can provide seamless control over document access and use by all personnel in an organization, whether they are using monitored or unmonitored PCs (i.e., with or without a Desktop Enforcer installed).

About Context-Based Enforcement

Like standard access control mechanisms, Compliant Enterprise provides control over information access based on user, user group, and document location. In addition to that, however, Compliant Enterprise considers context: the type of device being used, the application being used, the location of the user, and when the event occurs. In addition, Compliant Enterprise can control not just access to documents, but the actual *usage* of documents as well.

For example, you can set a policy that allows a class of documents to be opened and edited, but only using specific authorized applications. Or, you can allow a specific category of employees to open a document, but then control whether they can copy it (and where), e-mail it, attach it to an instant message, print it, or even cut and paste contents from it. Or you can allow them to do any or all of these, but only during certain hours, or days of the week, or dates. This kind of context-based usage control gives Compliant Enterprise much more power and flexibility than simple access controls or document-based permissions do.

How it Works

Once you have constructed and deployed your policies, they are evaluated and enforced by the policy enforcers running on file servers and desktops throughout the network. Each policy enforcer includes a *policy enforcement point* (PEP), which intercepts user events, and a *policy decision point* (PDP), which makes policy decisions. These decisions include dynamic evaluation of the context in which the event occurs.

For example, Desktop Enforcers provide application-level context that allows policy decisions to be made based not only on file system events, but also on which application is being used and even the user action within the file. This level of integration allows the PEP to determine, for example, whether users are attaching a document to instant messages or e-mail.

File Server Enforcers can correlate events that occur at the network level with those that occur at the file system level. This provides greater context about the network request, so that the PEP can use information about the network location of the requesting user to add context to policy decisions. In addition, both kinds of enforcers can factor time of day, day of the week, or date into decisions on access or use. This type of contextual enforcement provides more sophisticated control than ordinary file system access control mechanisms.

How Policy Enforcers Work

Now let's take a closer look at the common functions of both types of enforcers, and then turn to a more detailed discussion of the functions of each type in turn. For our purposes here, there is no distinction between Linux and Windows versions.

Common Features

Both types of enforcers have several features that provide basic functionality. These features are implemented through a number of software sub-components within each enforcer. (All such sub-components are transparent to the users and policy subjects, and do not require any individual attention; we describe them here just for background information.)

Policy Enforcement

Both types of enforcers contain a policy enforcement point (PEP) component that monitors all end-user or system events to determine whether they need to be checked for conformity to information control policies. The PEP is implemented in as a set of libraries that interface directly with (known as *hooking into*) the application, file system, or SharePoint portal that is being monitored.

If an event is in some category that may cause it to be covered under some policy, the PEP sends a request to another component called the Policy Controller, which is a service or daemon that acts as the policy decision point (PDP). The Policy Controller applies all context information to the events, and makes decisions on what policy applies and how. It then relays the effects of any relevant policy back to the PEP, which contains system-specific logic to apply the enforcement.

The PEP then instructs the application or file system to respond to the user's action as the policy requires—either allow or deny. If the policy evaluation results in the action being denied, the enforcer returns a message indicating that access is denied or that the requested action cannot be performed. These may take the form of standard system errors and/or the customized text balloon that was defined with the policy being enforced.

Monitoring and Auditing

Every enforcer perform continuous monitoring of document access and use, so that even if it never blocks any actions by policy subjects, it is still providing a valuable service of capturing who is using what information, how, and when.

To do this, a component called the Auditor receives its settings from the policy enforcer configuration profile, which indicates what actions should be audited on the current system. Any event that matches the Activity Journal's settings is captured by the Auditor and written to the local audit log. Periodically, as determined by the configuration profile, this log information is uploaded and inserted into the Activity Journal.

All policy enforcers automatically log activity at a minimum level. At this level, attempts to stop or start the policy enforcer or tamper with enforcer-managed files (policy enforcer binaries, configuration, policy, or logs) are logged.

Tamper Resistance

All Policy Enforcers are protected from tampering by unauthorized personnel. They can not be stopped, started, or uninstalled except by an authorized Administrator using the password assigned to that enforcer. This tamper resistance includes the following features:

- They start automatically as soon as installed, to protect information immediately and continuously.
- They run as password protected Windows services, to prevent users or other programs from shutting them down.
- They are controlled by a transparent self-recovery mechanism that automatically restarts them if they are ever terminated improperly.
- They have specially protected installation directory and system files to prevent unauthorized uninstallation, deletion, or modification.
- Their activity logging system tracks all attempts at tampering; this information which can be easily output to reports for analysis.

File Server Enforcers

File Server Enforcers control file resources on Windows- or Linux-based file servers. They are installed on the file server host, and enforce document access policies whenever anyone in your organization requests a file. Access policies control whether users are allowed to create, read, update, rename, or delete documents.

Because they run on file servers, File Server Enforcers are designed for the multi-user, high performance environment of enterprise file servers. The technology is application independent, functioning at the file system level.

In addition, File Server Enforcers are self-monitoring and self-protecting. When an enforcer is running, no user or process can modify, delete, or access its system files, including the binaries, log files, and policy bundle. If the File Server Enforcer is stopped unexpectedly, it is automatically restarted—by the OS if running on Windows, or by a special guardian process, if running on Linux.

Table 1-1 summarizes all the actions that File Server Enforcers can control:

Table 1-1: Functions of File Server Enforcers

Action	Description
Read	Open file
Delete	Permanently remove a file from storage. This includes moving a file to the Recycle bin.
Move	Delete a file from its current storage location and place it in a different location

Table 1-1: Functions of File Server Enforcers (Continued)

Action	Description
Create/Edit	Create a new file or change the contents of a file, including its file name or extension
Change Attributes	Modify the file attributes. This includes all properties on the General and the Custom tabs under File, Properties, but not those on the Summary tab.
Change Permissions	Modify the file security attributes, which includes all properties on the Security tabs under File, Properties.

File Server Enforcers also log all users' access to documents and folders and information about each enforcement event, and write it to the Activity Journal.

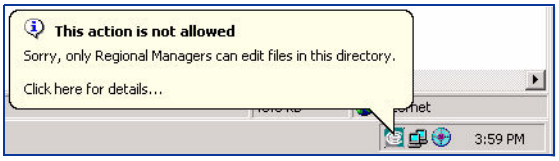
File Server Enforcers can be installed on one or all file servers in an organization, depending on which file servers contain documents that require document access policies. Each File Server Enforcer controls only the file server where it is installed.

You must install at least one File Server Enforcer in your system if you want to control access to document resources on a particular server by users with unmonitored PCs—that is, PCs without a Desktop Enforcer installed. If you also want to enforce what tasks users can do with resources once they access them, you must also install Desktop Enforcers on PCs.

Desktop Enforcers

Desktop Enforcers control how policy subjects can access and use documents on Windows-based desktop or laptop PCs. As soon as a Desktop Enforcer is installed and started, it runs continuously as a service, controlling both access to and use of documents, whether those documents are stored on the PC or remotely, and whether the PC is connected to a network or not.

The Desktop Enforcer is an application- and file format-independent policy enforcer installed on a desktop or laptop PC that detects file activity for each application running on the PC. It runs as a Windows service and can only be stopped by using an administrative password on the host machine.



At installation, the Desktop Enforcer can be configured to run silently, with no notification or feedback for the subjects of the policies being enforced; or it can be configured to run with notifications turned on. In the latter case, the Notification component runs as a separate executable process, and displays as an icon in the Windows system tray. Whenever a policy prevents a subject from performing an action, the subject's PC displays a message in an information balloon. The text of this message is defined as one of the properties of the policy being enforced, and is fully configurable. In addition, the subject can view the list of policies that have been enforced by right-clicking on the Notify icon and choosing View Notifications.

Each Desktop Enforcer is self-monitoring and self-protecting. When it is running, no user or process can modify, delete, or access the Desktop Enforcer's system files, including the binaries, log files, and policy bundles. If the Desktop Enforcer is ever stopped unexpectedly, it automatically restarts immediately.

Table 1-2 summarizes all the actions that Desktop Enforcers can control, involving both access and use.

Table 1-2: Functions of Desktop Enforcers

Action	Description
Read	Open file
Delete	Permanently remove a file from storage. This includes moving a file to the Recycle bin.
Move	Delete a file from its current storage location and place it in a different location
Create/Edit	Create a new file or change the contents of a file, including its file name or extension
Copy	Make a duplicate of a file, or insert one file into another file, such as by using the Insert File menu item to embed a spreadsheet in a word processor document. Includes copying to USB drives or CD/DVD burners.
Print	Print a file to a printer device or print to an output file
Change Attributes	Modify file attributes, such as whether the file is read-only or hidden (using Windows file property dialogs)
Change Permissions	Change permissions granted to users of a file (using Windows security dialogs)
Attach to E-mail	Attach a file to an outgoing message in Microsoft Outlook
Attach to IM	Attach a file to an outgoing instant message in Yahoo Instant Messenger, AOL Instant Messenger (AIM), Microsoft MSNMessenger, or Microsoft Windows Messenger
Paste	Copy or cut and paste a portion of the file's contents to a location outside the file

Like File Server Enforcers, Desktop Enforcers also collect information about each enforcement event for the Activity Journal.

Depending on your information control requirements, you can install Desktop Enforcers on none, a few, or all PCs within your organization. Each Desktop Enforcer affects only the PC where it is installed.

SharePoint Enforcers

SharePoint Enforcers are installed on the SharePoint server, to monitor and control users' access to the contents of the portal in very much the same way file server enforcers control access to resources in the server's directory structure.

Like all enforcers, SharePoint Enforcers are self-monitoring and protected by tamper-resistance features. When an enforcer is running, no user or process can modify, delete, or access its system files including the binaries, log files, and policy bundle. If the enforcer stops unexpectedly, it is automatically restarted.

Table 1-3 summarizes all the actions that SharePoint Enforcers can control:

Table 1-3: Functions of SharePoint Server Enforcers

Action	Meaning
Read	Open a portal item for viewing. This includes accessing a site, workspace, structure, list, or library item on a portal.
Delete	Permanently remove a file or portal item (site, workspace, structure, list, or library item) from storage.
Move	Delete a site, workspace, structure, list, or library item from its current storage location within the portal server and place it in a different location on the same server. Not to be confused with exporting or attaching, which are different actions.
Create/Edit	Create a new file or item, rename, or change the contents of an existing one. Specific actions include: • Create a portal site, page, list, library, library item, or column • Edit the content of an existing document or portal element • Rename an existing document or portal element • Overwrite an existing document by any means: copying a file with the same name from another location, renaming another file, etc. • Edit a portal site, page, list, library, library item, or column, by any means (in datasheet, in spreadsheet, etc.) • Upload any item to a portal
Export	Export a portal item. Specific actions include: • Export list to datasheet • Export library to speadsheet
Attach to Item	Attach one portal list item to another.

Like all enforcers, SharePoint Enforcers log all users' access to resources and information about each enforcement event, whether Allowed or Denied, and write it to the Activity Journal.

SharePoint Enforcers can be installed on one or more servers in an organization; each SharePoint Enforcer controls only the server where it is installed. In the case of server farm architecture, where one logical server is actually running on many physical server hosts, an enforcer must be installed on each physical host.

About Bundle Encryption

Control Center continuously updates enforcers, of all kinds, with any newly-defined or modified policies relevant to them. Each enforcer periodically sends a heartbeat message to the ICENet Server, which then checks whether any new or changed policies are in queue to be sent to that enforcer. If there are, it sends them, in the form of a file called *bundle.bin*; this file is referred to as a *policy bundle*.

All policy bundles sent from the Control Center to enforcers are encrypted using standard SSL protocols. When they arrive at the enforcer, the enforcer authenticates them with digital certificates to ensure that they were indeed created by the Control Center server, and that they have not been modified by any other processes. This protects against the possibility of anyone deploying spoof policies designed to open security holes in your enterprise.

Authentication Failure

Whenever a bundle file arrives at an enforcer client and cannot be authenticated, a Level 3 document activity event is written to the Windows Event Log:

```
policy bundle authentication failed
```

This event will also be displayed by Reporter, if your query includes Level 3 events. The most likely cause of such failure is that the file is corrupted in some way; in such cases you should examine the file contents.

Bundle files are encrypted, but administrators can decrypt them for troubleshooting purposes. For this purpose, a special utility called *decrypt.bat* is available in the Bin directory of each host where an enforcer is installed. To use this utility,

1. Stop the enforcer on the host where the encrypted bundle file is located. You cannot decrypt any bundles while the enforcer is running.
2. From a command line window, run the utility, supplying the arguments shown below.

```
decrypt -b <path>\bundle.bin -f <OutputFile.txt> -k <InstallPath>
```

In this command,

- **-b** is the path and name of the encrypted bundle file. The path typically will be C:\Program Files\Compliant Enterprise\WindowsDesktopEnforcer; the file name will always be *bundle.bin*.
- **-f** is the name of the output (decrypted) file.
- **-k** is the actual installation directory for the enforcer, which the utility needs in order to load the security keys from the keystore on the file system. If the enforcer is installed in the default path (C:\Pro-

gram Files\Compliant Enterprise\Windows Desktop Enforcer), this argument is optional.

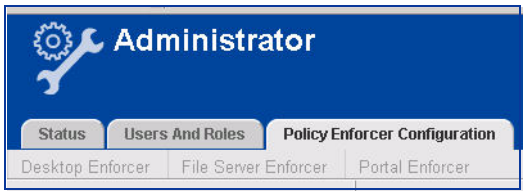
Here is an example:

```
Decrypt –b "C:\Program Files\Info Security\Compliant Enter-
    prise\Windows Desktop Enforcer\bundle.bin" –f bundle.txt –k
    "C:\Program Files\Info Security\Compliant Enterprise\Windows
    Desktop Enforcer"
```

3. When the utility starts, it prompts you for the standard utility password, which is the same as the password required to stop the enforcer.

4. After the utility runs, the clear-text output file will be available for analysis.

Managing Enforcer Profiles



All policy enforcers are governed by a number of configuration settings that control such aspects as logging behavior, heartbeat rates, tamper-prevention passwords, and network configuration. These are assigned default values when you first install an enforcer, but they can be changed manually at any time. To simplify this, Administrator allows you to create named sets of configuration settings, which you can then assign to one or more enforcers in your network. These are referred to as *enforcer profiles*, and you manage them in Administrator, with the settings on the Policy Enforcer Configuration tab. Profiles make no distinction between Windows- and Linux-based enforcers; you can assign the same profile to enforcers on either platform, or both at the same time.

The settings controlled by enforcer profiles include the following:

- Which ICENet server the enforcer will use to communicate with the Control Center
- How often the enforcer sends heartbeat signals to the Control Center to indicate it is operating normally

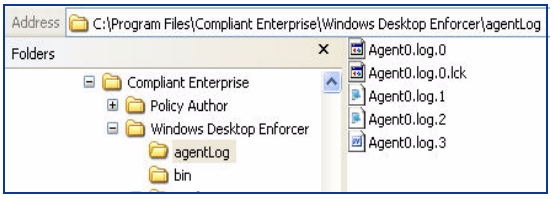
For more details on defining and using enforcer profiles, refer to the “Introducing” chapter in the *Compliant Enterprise 2.0 Administrator’s Guide*.

Managing Log Files

Each kind of policy enforcer maintains a set of local log files, which can be useful for troubleshooting, or when communicating with Compliant Enterprise technical support. Both kinds of enforcers save their log files at

```
<InstallDir>\agentLog
```

Because of the tamper-resistance features, you must stop any enforcer before you can view or open its log files.



Desktop Enforcers maintain a log file called *Agent0.log.0* until the file reaches its specified maximum size, the file is saved as *Agent0.log1*, and current logging continues in the original file name. Every time the file reaches its maximum size it is closed and saved, and the ending integer in all existing files is incremented. That is, the file ending in 0 will always contain the latest information, and the one ending in the highest integer will contain the oldest information.

Logging Settings

For both File Server Enforcers and Desktop Enforcers, you can configure the limit on the number and size of log files each enforcer maintains by editing the file *logging.properties* in the following directory:

```
<InstallDir>\config
```

The following properties control the number and size of log files maintained by each policy enforcer:

- **java.util.logging.FileHandler.count**: Specifies the maximum number of log files that can be archived at any given time. When this maximum is reached, the oldest file is discarded so that a new file can be started. Default = 10.
- **java.util.logging.FileHandler.limit**: Specifies the maximum size of each log file, in bytes.When this limit is reached, the current file is archived and a new log file is started. Default = 500K.

Changing Logging Levels

You can configure enforcers to the following levels of event logging, in order of increasing verbosity:

- Severe
- Warning
- Info
- Fine
- Finest

By default, the logging level is set to Severe, but if you wish you can change this individually for each policy enforcer. It is controlled by three parameters in the logging.properties file:

- java.util.logging.ConsoleHandler.level
- com.bluejungle.level
- .level

You should always set the first two to the same value. The .level parameter represents a restraint on the other two; they cannot operate at a higher verbosity level than is set there. This means that if you increase the verbosity for the other two, you must reset the .level value at least as high for the change to take effect. Figure 1-1 shows an example of this file.

Note that increasing the logging level of Desktop Enforcers may slow their performance noticeably. As a rule, you should leave these both at the default setting unless a technical support engineer asks you to change them.

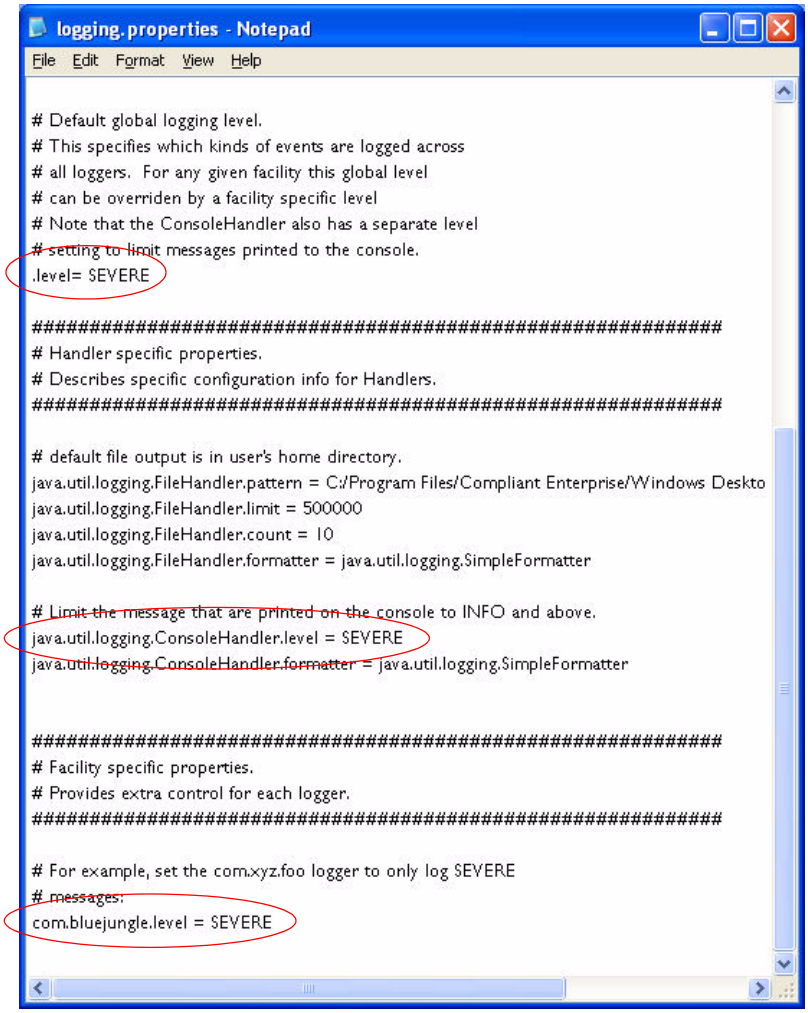


Figure 1-1: Changing Enforcer Logging Levels

Compliant Enterprise

2 Windows File Server Enforcer 1.6

In this chapter we provide information on installing and managing the File Server Enforcer for Windows. It includes the following sections:

Installing Windows File Server Enforcers

You can install the Windows File Server Enforcer 1.6 locally on each host, or you can push out multiple installations from a central location. In most cases, the latter will be the preferred option. The installation is quick and simple, but before you do it you should spend some time planning your installation.

Specifically, you need to decide the following:

- Which hosts you want enforcers to run on
- Which ICENet Server each enforcer will connect to. As we have seen, each enforcer works with one ICENet Server, which acts as its gateway to the Control Center.

Installing Enforcers Locally

You can use the installation wizard to install enforcers locally on each server host, using the following procedure:

1. Place the installation CD in the host where you want to install a file server enforcer. The installation splash screen should launch automatically; if it does not, open Windows Explorer and double-click on the autorun.exe file on the root of the CD. Click on the Install Windows File Server Enforcer link to launch the install wizard.

   Alternatively, copy the file **WindowsFileServerEnforcer-setup.exe** to the target host, or to a network shared folder. Launch the install wizard by double-clicking this file.
2. When the wizard's splash screen appears, click Next.
3. On the **Licence Agreement** screen, read the license agreement, choose "I Accept," and click Next.
4. On the **Destination Folder** screen, specify the path and directory where you want to install the enforcer, and click Next.

5. On the **ICENet Server Location** screen, use the drop-down list to select the ICENet Server this enforcer will use for its connection when it registers itself with the Control Center. (After it registers, it will use whatever ICENet Server is specified in the default profile.) This list will display all the ICENet Servers detected in the network; however, you can also type in a different value (if your ICENet Server is not currently running).

   If you are using load-balanced ICENet servers, type in the virtual IP address or virtual host name of the load balancer here.

Note: In order to view all active servers in this list, you should make sure the autodiscovery port (19888) on the server host is not blocked by a firewall. For details, refer to the *Getting Started Guide*.

Figure 2-1: Choosing Setup Type (Desktop Enforcer Only)

6. On the **Setup Type** screen, select Complete or Custom, and click Next. (This choice is available only for Desktop Enforcers; it will not display if you are installing a File Server Enforcer.)

   - **Complete**: Installs all software features. If you choose this option, the installation begins after this screen.
   - **Custom**: Allows you to select optional features. In the current release, there is only one such feature: the ability to enable or disable compliance notification. When enabled, the CE logo will display in this desktop's system tray, and the enforcer will display any On Deny messages defined in the policies whenever they are enforced. When disabled, the enforcer will run in silent mode: the CE logo will not display, and there will be no enforcement notification on this PC, even if an On Deny message is defined in the policy.

The Custom Setup Screen

1. If you are installing a Desktop Enforcer and select a Custom installation, the **Custom Setup** screen prompts you to choose the features you want to enable.

This screen allows you to check if your destination location has enough space. To do this, select one or more features and click the Space button.

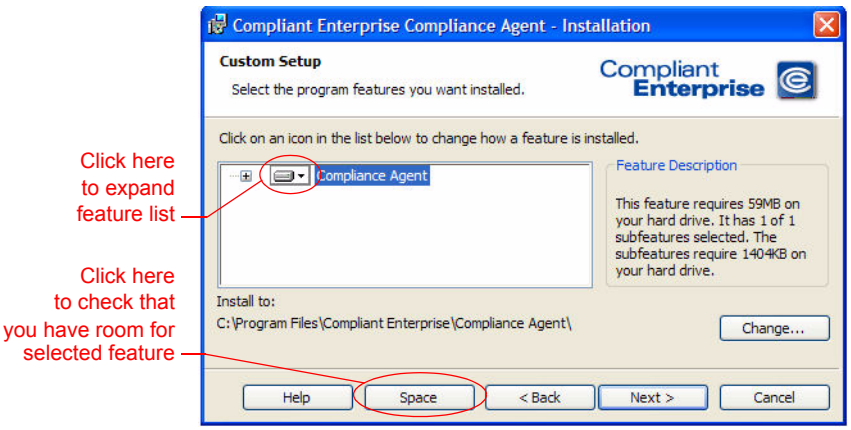


Figure 2-2: The Desktop Enforcer Custom Setup Screen

2. Expand the feature menu Compliance Notification feature menu and select one of the options, to either enable or disable the feature.

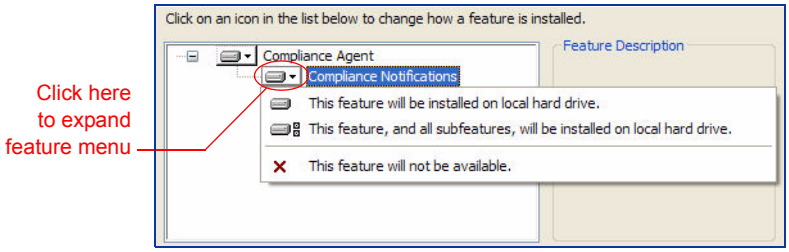


Figure 2-3: Enabling Desktop Enforcer Features

After you make a new choice in this menu, the icon next to the component name changes to reflect your choice.

3. In the final Wizard screen, click Install.

A notification message lets you know when installation is complete.

Start Enforcers

Note that desktop enforcers must be manually started the first time they are installed; they are designed to run continuously thereafter. They can be started like any standard Windows service, either from the Administrative Tools, Services window under Control Panel, or by rebooting the host PC.

Installing Enforcers Centrally

Any number of enforcers can be installed from a central location, using managed installation methods such as a login script or Windows Group Policy Object (GPO). The Compliant Enterprise installation package includes an .MSI installation file that can be used with these installation methods.

This section provides general instructions for performing a managed installation using GPO. For details about GPO, refer to Microsoft documentation.

1. Use Microsoft Group Policy Object on the domain controller and register each target machine on which you want to install enforcer software.
2. Create an .MSI transform file (.MST file) to set the value of the ICENet Server Location installation parameter to the machine where you installed the ICENet Server. Use the format <machine-Name>:<port>. If you use the default port number 8443, you can omit it from the value and simply set the machineName.
3. Use any desired transformation tool to create the file, and consult the documentation for that tool for details on how to set up the file.

Configure GPO to run the appropriate .MSI and .MST files whenever each machine is booted up: WindowsDesktopEnforcer-setup-setup.msi for desktop or laptop PCs, WindowsFileServerEnforcer-setup.msi for file servers.

Uninstalling SharePoint Enforcers

If you need to uninstall a Windows File Server Enforcer for any reason—for example, if you are upgrading to a later version—perform the following procedure.

1. If the enforcer is running, stop it with the Stop utility, available in the Start, All Programs, Compliant Enterprise menu (see page 28). You will require the security password to do this.
2. In the Windows Control panel, open the Add or Remove Programs utility.
3. From the list of programs, select Compliant Enterprise SharePoint Enforcer, then click the Remove button.
4. What's the catch here?

Routine Operation

The first time you install file server enforcers, you must start them manually (see page 28). After that they should run continuously as standard Windows services, and will be restarted automatically if they ever shut down for any reason.

Processes

The file server enforcer consists of one Windows process, called **Compliant Enterprise File Server Enforcer.**

When the enforcer is running normally, this will display in the list in the Windows Services Control Panel window, and also on the Processes tab in Windows Task Manager.

NEED TO CONFIRM THIS

Configuration and Management

No configuration changes are required for running file server enforcers once they have been installed. There are some configuration controls available through the Administrator web application, and there are some minimal management activities that enforcer administrative personnel may need to perform from time to time.

Configuration Tools

The only configuration settings available for file server enforcers are the enforcer profile settings and the log file management settings. These are the same for all enforcers, and are described in Chapter 1; see "Managing Enforcer Profiles" (page 20) and "Managing Log Files" (page 20).

Management Activities

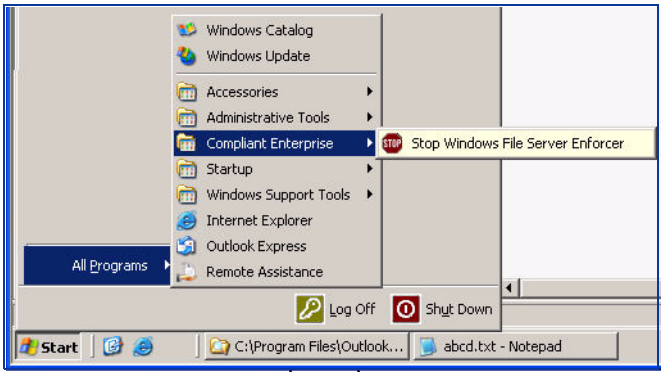
Because enforcers are designed to run continuously with no complications, there are very few management functions required from system administrators. These include stopping enforcers that are currently running, restarting enforcers after they have been stopped, and monitoring the status of currently running enforcers.

Stopping and Restarting

Because all enforcers are designed to resist tampering, no user can stop them through the standard services manager or through any registry settings. They can be stopped only with a special, password-protected utility.

Note that as a tamper resistance feature, no one can even view the contents of an enforcer's installation directory while the enforcer is running. This means that you must stop the enforcer before you can, for example, examine log files in the logs directory.

File Server Enforcers are tamper resistant, and to stop them you must use a special executable, ***Stop Windows File Server Enforcer***. You launch this from the Compliant Enterprise group in the Windows Start, All Programs menu, as shown at right.



After stopping a File Server Enforcer, you can restart it again locally with the standard Services manager in Windows Control Panel, or by rebooting the host server.

Monitoring Enforcers

You can always check the status of a file server enforcer locally by opening the Services management window and checking the list of services on the Extended tab. The service is called Compliance Enterprise File Server Enforcer; its status should always be Started, and its startup type is Automatic.

Remote Monitoring

You can monitor the status of all enforcers in the network—on file servers and on PCs—by opening CE Administrator, going to the Status tab, and clicking the Policy Enforcer Status link. By default, this tab displays the status of all enforcers

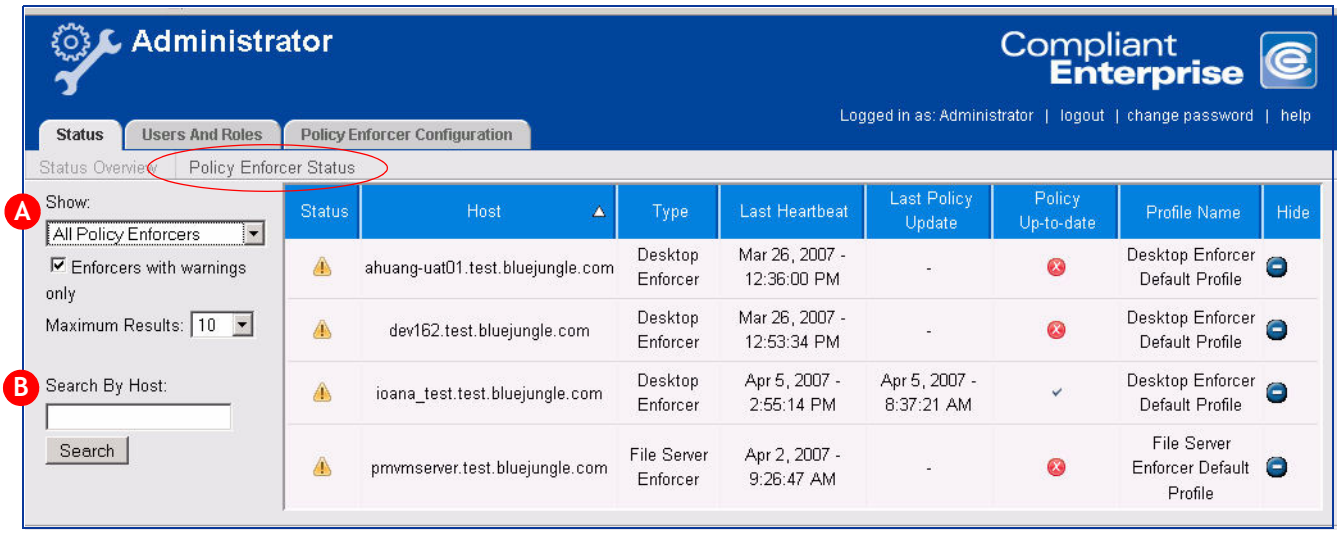


Figure 2-4: Monitoring the Status of File Server Enforcers

in the system; to view only file server enforcers, select *All File Server Enforcers* from the Show combo-box list at the left (**A**). Note that there is no distinction between Windows- and Linux-based file server enforcers—both will be displayed together. in the Status grid.

You can also filter by host name (**B**), if you are interested in the status of enforcers on a specific enforcer host or host group. This provides a way to limit the display to Windows-based enforcers, if you know which hosts they are running on.

The status grid displays the following information about the status of each enforcer:

Table 2-1: Information on Policy Enforcer Status

Column	Description
Status	Indicates the current status of this enforcer, which may be either of the following: Green light = Clear: the policy enforcer is sending normal heartbeats. Exclamation point = Warning: the policy enforcer has not sent a heartbeat in the last 24 hours.
Host	Name of the machine where the policy enforcer is installed.
Type	Indicates the policy enforcer type: File Server Enforcer or Desktop Enforcer.
Last Heartbeat	Time stamp of the last heartbeat generated by this policy enforcer. If the policy enforcer is running normally, this time should correspond to the configured heartbeat interval. However, keep in mind that this does not necessarily indicate a problem, since certain policy enforcers—in particular, those on laptop computers used by remote personnel or computers that are turned off when not in use—might not be able to send a heartbeat for an extended period of time even though they are operating normally.
Last Policy Update	Tells when a new or modified policy or policy component was last deployed to this policy enforcer.
Policy Up to Date	A check mark appears if the policy enforcer has received the latest version of the policies that are targeted for deployment to it.
Profile Name	Tells which policy enforcer profile is assigned to this host. This profile determines behavior such as logging and heartbeat frequency.
Hide	Click to remove this host from the display. This is useful when the policy enforcer software has been uninstalled, and you therefore no longer need to monitor that host. If a policy enforcer is ever reinstalled on this host, the host will reappear on the list. If you click Hide by mistake on a host with an active policy enforcer, it will reappear automatically the next time the policy enforcer sends a heartbeat.

Checking Deployment

At any time, administrators can check which policies are deployed on which enforcers throughout the enterprise. There are two ways to approach this:

- Check which policies and components have been deployed to a specific file server or PC;
- Check which servers and PCs a specific policy or component has been deployed to.

You use Policy Author for both approaches.

Checking by Host

To find out which policies and components have been deployed to a specific policy enforcer host,

1. In Policy Author's Tools menu, select Deployment Status. A pop-up window appears, displaying all currently scheduled and past deployments for all hosts. For each host, the total number of policies and policy components deployed is displayed.

As Figure 2-5 shows, the hosts are organized on thee tabs:

- **Desktop Enforcers**: Displays all hosts with Desktop Enforcers running on them.
- **File Server Enforcers**: Displays all hosts, both Windows and Linux, with File Server Enforcers running on them.

.

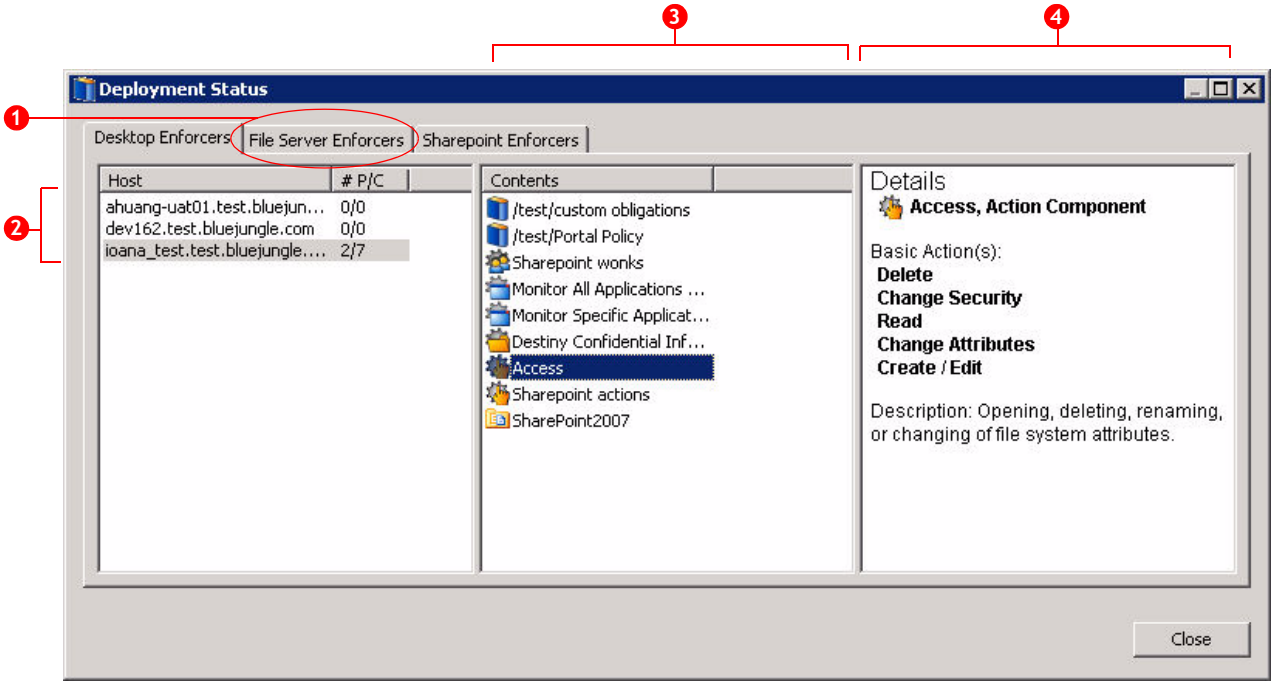


Figure 2-5: Displaying Deployment Status in Policy Author

2. Click the tab you are interested in, to display all hosts of that type in the Host column.
3. Select the host you want to examine, and a list of policies and policy components deployed on that machine displays in the Contents pane, in the center.
4. To display the actual definition of any policy or component deployed on the selected machine, select it in the Contents pane, and the definition displays in the Details pane, at the right.

Checking by Policy or Component

Administrators can use this approach to find out which hosts have received deployment of a particular policy or policy component and when, and to view each of multiple deployed versions (which can occur if different versions are deployed to different machines).

1. In Policy Author, display the policy or component.
2. In the Action menu, choose Version History. A pop-up window displays the currently scheduled and past deployments of the policy or component you are editing. Each deployment is represented by a time in the list in the left pane. Bear in mind that a *deployment* usually is not the same as a policy or a component; it may represent one component or policy, or many that were deployed together.

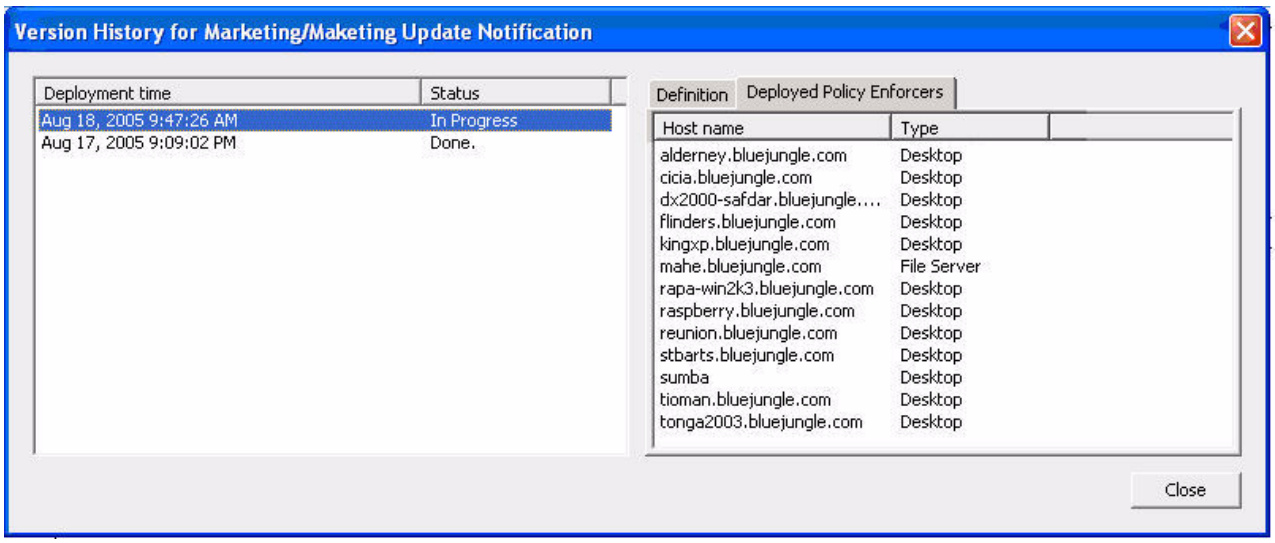


Figure 2-6: Viewing Deployed Version History

3. In the left pane, click the deployment time you are interested in. Details on the version deployed at that time display on the Definition tab, in the right-hand pane.
4. To see which machines this version of the policy or component was deployed to, click the Deployed Policy Enforcers tab. Note that the type of each host is displayed—either Desktop or File Server.
5. When you are finished with this window, click Close.

3 Linux File Server Enforcer 1.0

In this chapter we provide information on installing and managing the Compliant Enterprise enforcer for Linux file servers. The chapter has the following sections:

Installing Linux File Server Enforcers

The installation procedure for the Linux File Server Enforcer 1.0 is quick and very simple.

1. Copy the installation executable from the Installers directory on the installation CD, to the Linux host where you want to install the enforcer. This file is called `CE-fse-1.00-nnnnnn.i386.bin` (**n** represents variables that depend on build version and release date).
2. From the Linux command line, run the installation executable.
3. Review the license agreement (you will have to scroll down through multiple screens) and when you are finished, type **yes** to accept the terms.
4. In response to the next prompt, specify the name of the ICENet Server the enforcer will use for its connection when it registers itself with the Control Center. (After it registers, it will use whatever ICENet Server is specified in the default profile.)
5. In response to the next prompt, specify the connection port to the ICENet server, or accept the default, 8443.
6. At this point the installation runs. When it finishes, the enforcer starts automatically.

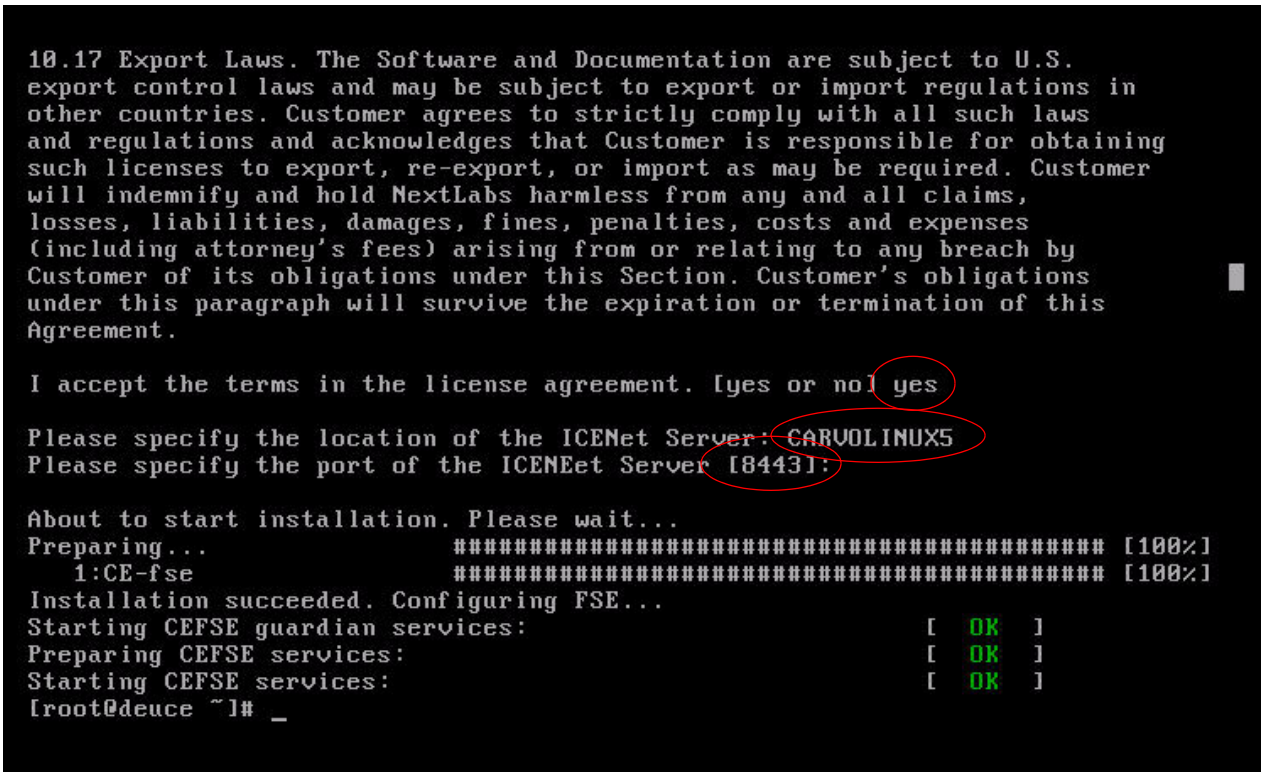


Figure 3-1: Installing the Linux File Server Enforcer

Uninstalling Linux File Server Enforcers

If you need to uninstall a SharePoint Enforcer for any reason—for example, if you are upgrading to a later version—perform the following procedure.

1. If the enforcer is running, stop it with the `cefse_stop` command (see page 35). You will require the security password to do this.

2. Then what?

Routine Operation

The Linux File Server Enforcer runs continuously as a service, and will restart automatically if it ever fails or stops running abnormally for any reason. When running normally, it consists of a pair of processes:

- **/usr/local/ce/bin/controlmodule** is the enforcer itself
- **/bin/sh/etc/init.d/CEFSE-guardian start** is the guardian process that will restart the enforcer whenever necessary, to ensure continuous operation

Both processes are tamper-resistant, and cannot be stopped without the administrative password.

Configuration and Management

No configuration changes are required for running Linux File Server Enforcers once they have been installed. There are some configuration controls available through the Administrator web application, and there are some minimal management activities that enforcer administrative personnel may need to perform from time to time. These are described below.

If you are running Linux file server enforcer in your network, there is one special enrollment procedure you need to perform, in order to discover and enroll the file shares on the Linux side and add them to the aliases.txt file on the Windows side. All details about enrollment are presented in the System Administrator's Guide; for this particular topic, refer to the "Enrolling Other Entities" chapter. File shares are the only enrolled entities that have special procedures for Linux enforcers.

Configuration Tools

There is no required configuration for the Linux File Server Enforcer, and once it is installed it should need little or no attention. One aspect of the enforcer's operation that might need changing is the is the ICENet server each enforcer connects to. This is set during installation, but you can use CE Administrator to redirect it at any point after that. For more information, see "Managing Enforcer Profiles" (page 20).

Management Activities

Because enforcers are designed to run continuously with no complications, there are very few management functions required from system administrators. These include stopping enforcers that are currently running, restarting enforcers after they have been stopped, and monitoring the status of currently running enforcers.

Stopping and Restarting

Because all enforcers are designed to resist tampering, no user can stop them through the standard services manager or through any registry settings. They can be stopped only with the superuser password.

To stop a Linux File Server Enforcer, log into the local host and type the command:

```
cefse_stop
```

then provide the superuser administrator's password when prompted.

To restart the enforcer, use the command:

```
service cefse start
```

Monitoring Enforcers

To check the current status of a Linux File Server Enforcer, log in locally and type the command:

```
cefse_status
```

There are only two possible statuses: Stopped or Running. The enforcer should be running at all times, unless it has been manually stopped by an authorized administrator.

Remote Monitoring

You can monitor the status of all enforcers in the network—on file servers and on PCs—by opening Administrator, going to the Status tab, and clicking the Policy Enforcer Status link.

By default, this tab displays the status of all enforcers in the system; to view only file server enforcers, select *All File Server Enforcers* from the Show combo-box list at the left (**A**). Note that there is no distinction between Windows- and Linux-based file server enforcers here—both will be displayed together.

You can also filter by host name (**B**), if you are interested in the status of enforcers on a specific enforcer host or host group. This provides a way to limit the display to Linux-based enforcers, if you know which hosts they are running on.

For descriptions of the contents of the enforcer status grid, see Table 2-1 on page 30.

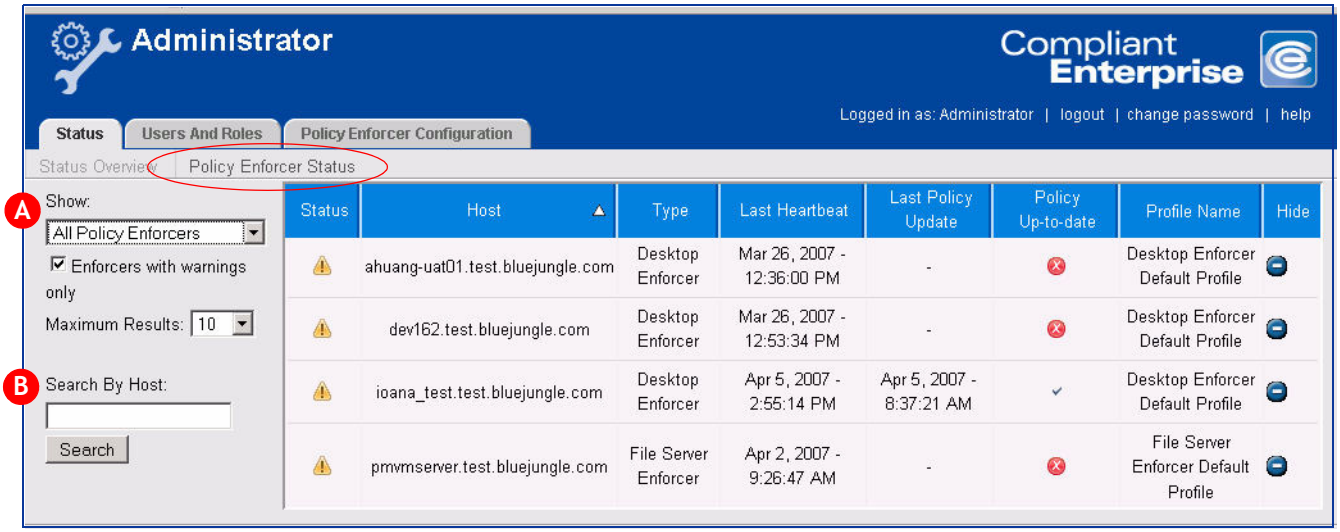


Figure 3-2: Monitoring the Status of File Server Enforcers

4 Windows Desktop Enforcer 1.6

This chapter describes the installation and management of desktop enforcers, which run on Windows desktop or laptop PCs. The chapter has the following sections:

Installing Desktop Enforcers

You can install the Windows Desktop Enforcer 1.6 locally on each host, or you can push out multiple installations from a central location. In most cases, the latter will be the preferred option. The installation is quick and simple, but before you do it you should spend some time planning your installation. Specifically, you need to decide the following:

- Which PCs you want enforcers to run on.
- Which ICENet server each enforcer will initially connect to as its gateway to the Control Center. This can be selected from a list of all ICENet servers currently running in the network, which is automatically detected during installation.

Installing Enforcers Locally

You can use the installation wizard to install enforcers locally on each server host, using the following procedure:

1. Place the installation CD in the host where you want to install a file server enforcers. The installation splash screen should launch automatically; if it does not, open Windows Explorer and double-click on the autorun.exe file on the root of the CD.

   Alternatively, copy the file **WindowsDesktopEnforcer-setup.exe** to the target host, or to a network shared folder.
2. Launch the install wizard by double-clicking this file.
3. When the wizard's splash screen appears, click Next.
4. On the **Licence Agreement** screen, read the license agreement, choose "I Accept," and click Next.

5. On the **Destination Folder** screen, specify the path and directory where you want to install the enforcer, and click Next.
6. On the **ICENet Server Location** screen, use the drop-down list to select the ICENet Server this enforcer will use for its connection when it registers itself with the Control Center. (After it registers, it will use whatever ICENet Server is specified in the default profile.) This list will display all the ICENet Servers detected in the network; however, you can also type in a different value (if your ICENet Server is not currently running).

   If you are using load-balanced ICENet servers, type in the virtual IP address or virtual host name of the load balancer here.

Note: In order to view all active servers in this list, you should make sure the autodiscovery port (19888) on the server host is not blocked by a firewall. For details, refer to the Getting Started Guide.

Figure 4-1: Choosing Setup Type

7. On the **Setup Type** screen, select Complete or Custom, and click Next.
   - **Complete**: Installs all software features. If you choose this option, the installation begins after this screen.
   - **Custom**: Allows you to select optional features. In the current release, there is only one such feature: the ability to enable or disable compliance notification. When enabled, the CE logo will display in this desktop's system tray, and the enforcer will display any On Deny messages defined in the policies whenever they are enforced. When disabled, the enforcer will run in silent mode: the CE logo will not display, and there will be no enforcement notification on this PC, even if an On Deny message is defined in the policy.

The Custom Setup Screen

1. If you select a Custom installation, the **Custom Setup** screen prompts you to choose the features you want to enable.

This screen allows you to check if your destination location has enough space. To do this, select one or more features and click the Space button.

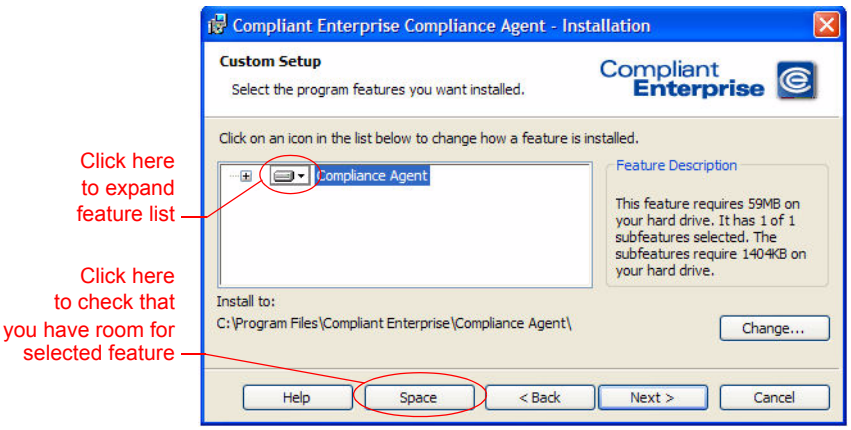


Figure 4-2: The Desktop Enforcer Custom Setup Screen

2. Expand the feature menu Compliance Notification feature menu and select one of the options, to either enable or disable the feature.

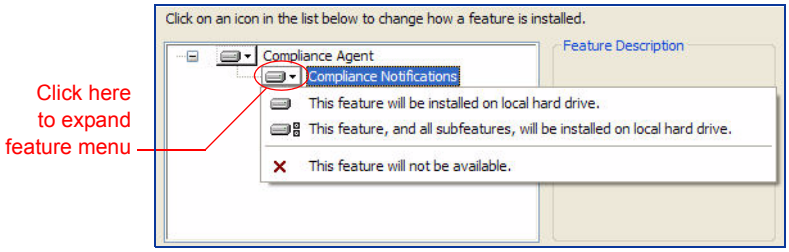


Figure 4-3: Enabling Desktop Enforcer Features

After you make a new choice in this menu, the icon next to the component name changes to reflect your choice.

3. In the final Wizard screen, click Install.

A notification message lets you know when installation is complete.

Installing Enforcers Centrally

Any number of enforcers can be installed from a central location, using managed installation methods such as a login script or Windows Group Policy Object (GPO). The Compliant Enterprise installation package includes an .MSI installation file that can be used with these installation methods.

This section provides general instructions for performing a managed installation using GPO. For details about GPO, refer to Microsoft documentation.

1. Use Microsoft Group Policy Object on the domain controller and register each target machine on which you want to install enforcer software.
2. Create an .MSI transform file (.MST file) to set the value of the ICENet Server Location installation parameter to the machine where you installed the ICENet Server. Use the format <machine-Name>:<port>. If you use the default port number 8443, you can omit it from the value and simply set the machineName.
3. Use any desired transformation tool to create the file, and consult the documentation for that tool for details on how to set up the file.

Configure GPO to run the appropriate .MSI and .MST files whenever each machine is booted up: `WindowsDesktopEnforcer-setup-setup.msi` for desktop or laptop PCs, `WindowsFileServerEnforcer-setup.msi` for file servers.

Uninstalling SharePoint Enforcers

If you need to uninstall a Windows Desktop Enforcer for any reason—for example, if you are upgrading to a later version—perform the following procedure.

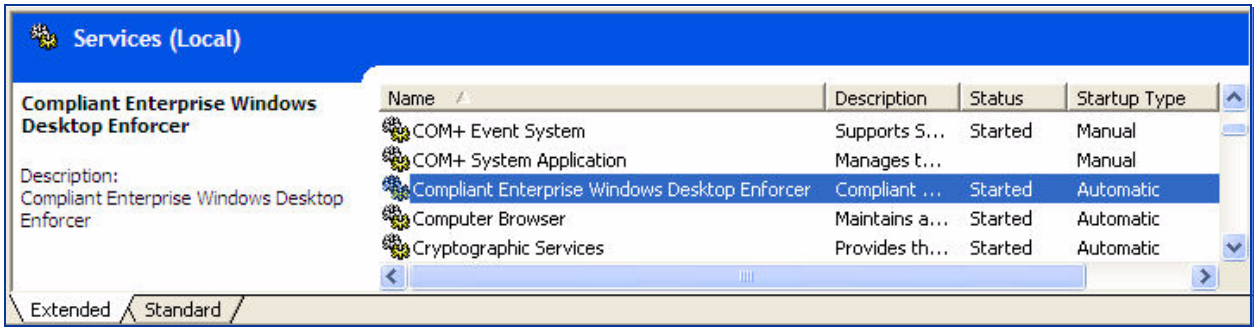
1. If the enforcer is running, stop it with the Stop utility, available at Program Files\Compliant Enterprise\Windows Desktop Enforcer\public bin. (see page 44). You will require the security password to do this.
2. In the Windows Control panel, open the Add or Remove Programs utility.
3. From the list of programs, select Compliant Enterprise SharePoint Enforcer, then click the Remove button.
4. What's the catch here?

Routine Operation

After you install a desktop enforcer, you must manually start it (see page 44); thereafter, it runs continuously as a standard Windows service. It sends the Compliant Enterprise Control Center a regular heartbeat signal every hour, by default, to indicate that it is connected to the network and running normally. The Control Center sends back policy bundles whenever policies are deployed that require enforcement at that host.

Processes

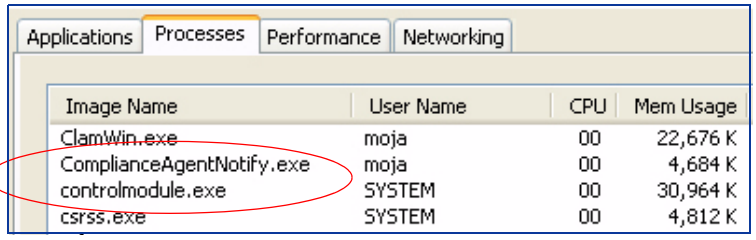
The Windows Desktop Enforcer runs as a Windows service called **Compliant Enterprise Windows Desktop Enforcer**.



The enforcer comprises two separate processes:

- **ComplianceAgentNotify.exe**: Controls all the display functions, such as the CE icon in the system tray and the menu of display right-click functions.
- **ControlModule.exe**: This is the main process of the enforcer itself.

When the enforcer is running normally, these will display on the Processes tab in Windows Task Manager. Note, however, that only the ControlModule process runs when desktop enforcers installed in silent mode.



Configuration and Management

No configuration changes are required for running desktop enforcers once they have been installed. There are some configuration controls available through Administrator, and there are some minimal management activities that enforcer administrative personnel may need to perform from time to time.

Configuration Tools

The only configuration settings available for desktop enforcers are the enforcer profile settings, and the log file management settings. These are the same for all enforcers, and are described in Chapter 1; see Managing Enforcer Profiles (page 20) and Managing Log Files (page 20).

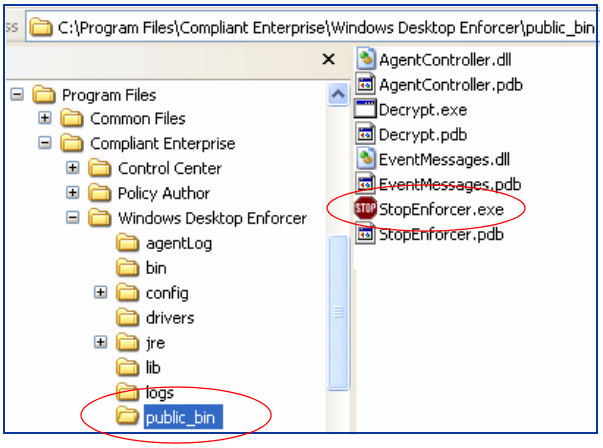
Management Activities

Because enforcers are designed to run continuously with no complications, there are very few management functions required from system administrators. These include stopping enforcers that are currently running, restarting enforcers after they have been stopped, and monitoring the status of currently running enforcers.

Stopping and Restarting

Because Desktop Enforcers are designed to resist tampering, no user can stop them through the standard services manager or through any registry settings. They can be stopped only with a special, password-protected utilities.

Note that as a tamper resistance feature, no one can even view the contents of an enforcer's installation directory while the enforcer is running. This means that you must stop the enforcer before you can, for example, examine log files in the logs directory.



Administrators can manually stop each individual enforcer at the local host using a utility called ***StopEnforcer.exe***, installed on each Desktop Enforcer host at *C:\Program Files\Compliant Enterprise\Windows Desktop Enforcer\ public_bin*, as shown at right. This utility requires the administrative password set for whatever profile is assigned to the enforcer. This means you need to know which profile is in use, and what its password is, before you can stop an enforcer.

Once you stop the enforcer with this utility, you can restart it again manually with the standard Services manager in Windows Control Panel, or by rebooting the PC.

Monitoring Enforcers

You can monitor the status of all enforcers in the network—on file servers and on PCs—by opening Administrator, going to the Status tab, and clicking the Policy Enforcer Status link. By default, this tab displays the status of all enforcers in the system; to view only desktop server enforcers, select *All Desktop Enforcers* from the Show combo-box list at the left (A). You can also filter by host name (B), if you are interested in the status of enforcers on a specific enforcer host or host group. For descriptions of the contents of the enforcer status grid, see Table 2-1 on page 30.

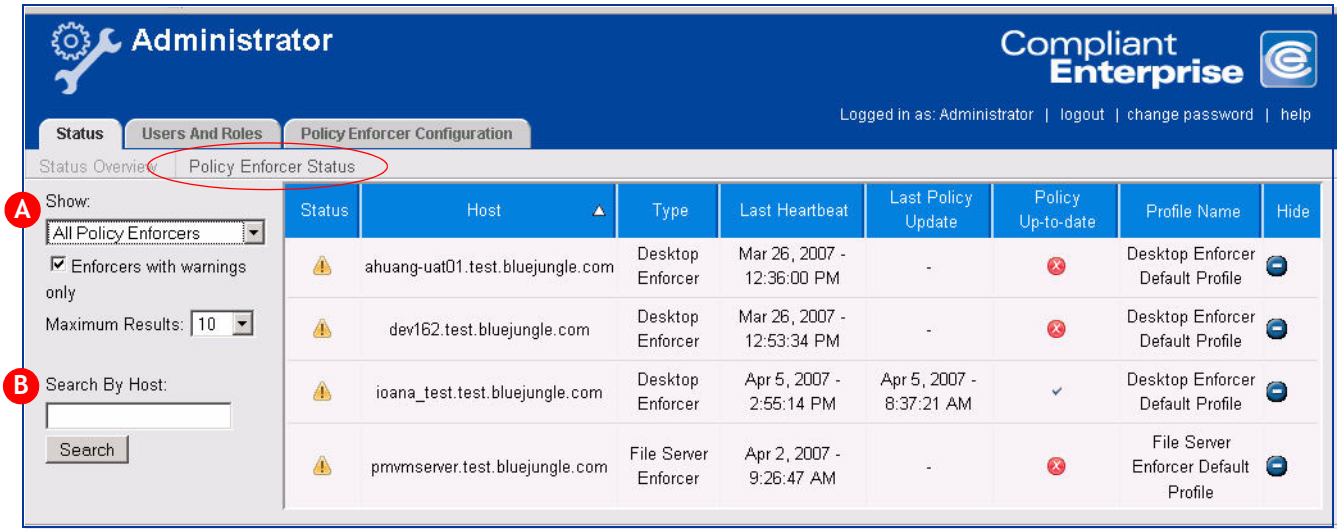


Figure 4-4: Monitoring the Status of File Server Enforcers

Compliant Enterprise

5 SharePoint Enforcer 1.0

In this chapter we discuss the installation and management of SharePoint enforcers, which run on the SharePoint server. The chapter has the following sections:

Installing SharePoint Enforcers

There are two basic architectural scenarios for the SharePoint server you might want to control with a SharePoint Server Enforcer 1.0:

- A single-server architecture, where the server is running on one IIS host
- A server-farm architecture, where a single logical server is running on a number of physical hosts

For either case, the installation process is the same. In the former case, you run it on the single host; in the latter, you must run it locally on every host where an IIS is running.

The installation runs from an installer wizard, available from the Install Enforcers link on your installation CD.

1. Place the installation CD in the host where you want to install a SharePoint enforcer. The installation splash screen should launch automatically; if it does not, open Windows Explorer and double-click on the file *autorun.exe* on the root of the CD. Right-click on the Install Enforcers link, then select SharePoint Enforcer to launch the install wizard.

   Alternatively, you can copy the file *SharePointServerEnforcer-setup.exe* to the target host, or to a network shared folder. Launch the install wizard by double-clicking this file.
2. When the wizard's splash screen appears, click Next.
3. On the **Licence Agreement** screen, read the license agreement, choose "I Accept," and click Next.

4. On the **Destination Folder** screen, accept the default install directory, or click the Change button to specify a different location, then click Next.
5. On the **ICENet Server Location** screen, use the drop-down list to select the ICENet Server this enforcer will use for its connection when it registers itself with the Control Center. (After it registers, it will use whatever ICENet Server is specified in the default profile.) This list will display all ICENet Servers detected in the network; however, you can also type in a different value (if your ICENet Server is not currently running).

   If you are using load-balanced ICENet servers, type in the virtual IP address or virtual host name of the load balancer here.

   Note: In order to display all active servers in this list, you should make sure the autodiscovery ports on the server host is not blocked by a firewall. Control Center uses port 9233 for the SharePoint Enforcer and 19888 for all others. For details, refer to the *Getting Started Guide*.
6. On the next screen, click the Install button to begin the installation process.
7. After the installation finishes, the IIS running on the install host will have to be restarted. On the next screen, click Yes to restart it now, or No if your prefer to restart it at a later time. (Note that this refers specifically to restarting the IIS; there is no need to reboot the host machine.) You will not be able to use the enforcer until you do this.

Uninstalling SharePoint Enforcers

If you need to uninstall a SharePoint Enforcer for any reason—for example, if you are upgrading to a later version—perform the following procedure.

1. If the enforcer is running, stop it with the Stop utility, available in the Start, All Programs, Compliant Enterprise menu (see page 50). You will require the security password to do this.
2. In the Windows Control panel, open the Add or Remove Programs utility.
3. From the list of programs, select Compliant Enterprise SharePoint Enforcer, then click the Remove button.
4. What's the catch here?

Routine Operation

One it has been installed, the SharePoint Enforcer runs continuously, and should require little or no attention from an administrator. Like other enforcers, it consists of two logical parts: a policy decision point, or PDP, and a policy enforcement point, or PEP. The PDP—also known as the Policy Controller—runs as a standard Windows service, and will be visible as an item in the list in the Services management window, called **Compliance Enterprise SharePoint Enforcer**. On the Processes tab in the Windows Task Manager, it displays as **cepdpman.exe**.

If the service ever stops for an abnormal reason, the Windows operating system will automatically restart it immediately.

The PEP is not an active process but rather a set of DLLs that are written to the required locations on the server, and are then called by the IIS whenever requests come in for access to SharePoint content. The PEP makes a decision on whether the request is something that might be covered by a current policy, and if so it passes the information to the Policy Controller, where rules for enforcing currently deployed polices at that server. The Policy Controller passes its enforcement decision—Allow or Deny—back to the PEP, which passes it to the IIS.

Configuration and Management

No configuration changes are required for running desktop enforcers once they have been installed. There are some configuration controls available through Administrator, and there are some minimal management activities that enforcer administrative personnel may need to perform from time to time.

Configuration Tools

The only configuration settings available for SharePoint enforcers are the enforcer profile settings, and the log file management settings. These are the same for all enforcers, and are described in Chapter 1; see Managing Enforcer Profiles (page 20) and Managing Log Files (page 20).

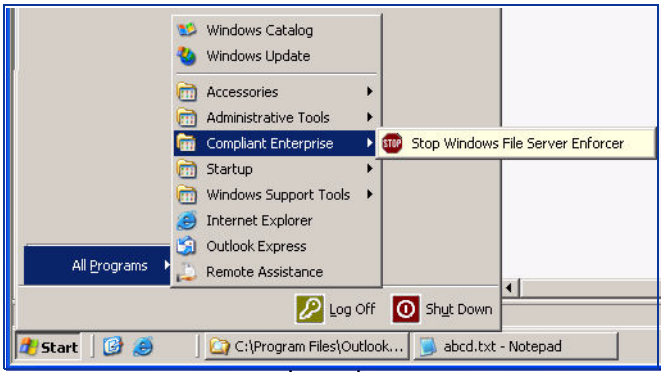
Management Activities

Because enforcers are designed to run continuously with no complications, there are very few management functions required from system administrators. These include stopping enforcers that are currently running, restarting enforcers after they have been stopped, and monitoring the status of currently running enforcers.

Stopping and Restarting

SharePoint Enforcers are protected by the same tamper-resistance features as file server and desktop enforcers. This means that no user can stop them through the standard services manager or through any registry settings. They can be stopped only with a special, password-protected utility.

Like other types, SharePoint Enforcers are tamper resistant. To stop them, you must use a special executable, ***Stop SharePoint Enforcer***. You launch this from the Compliant Enterprise group in the Windows Start, All Programs menu, as shown at right, on the server host where the enforcer is running.



After stopping a SharePoint Enforcer, you can restart it again manually with the standard Services manager in Windows Control Panel, or by rebooting the host server.

If the enforcer ever stops for any reason other than the Stop utility, it automatically restarts, and the event is logged in the activity Journal as an Abnormal Restart event.

Monitoring Enforcers

You can always check the status of a SharePoint Enforcer locally by opening the Services management window and checking the list of services on the Extended tab. The service is called *Compliance Enterprise SharePoint Enforcer*; its status should always be Started, and its startup type is Automatic.

Remote Monitoring

You can monitor the status of all enforcers in the network—on file servers and on PCs—by opening Administrator, going to the Status tab, and clicking the Policy Enforcer Status link.

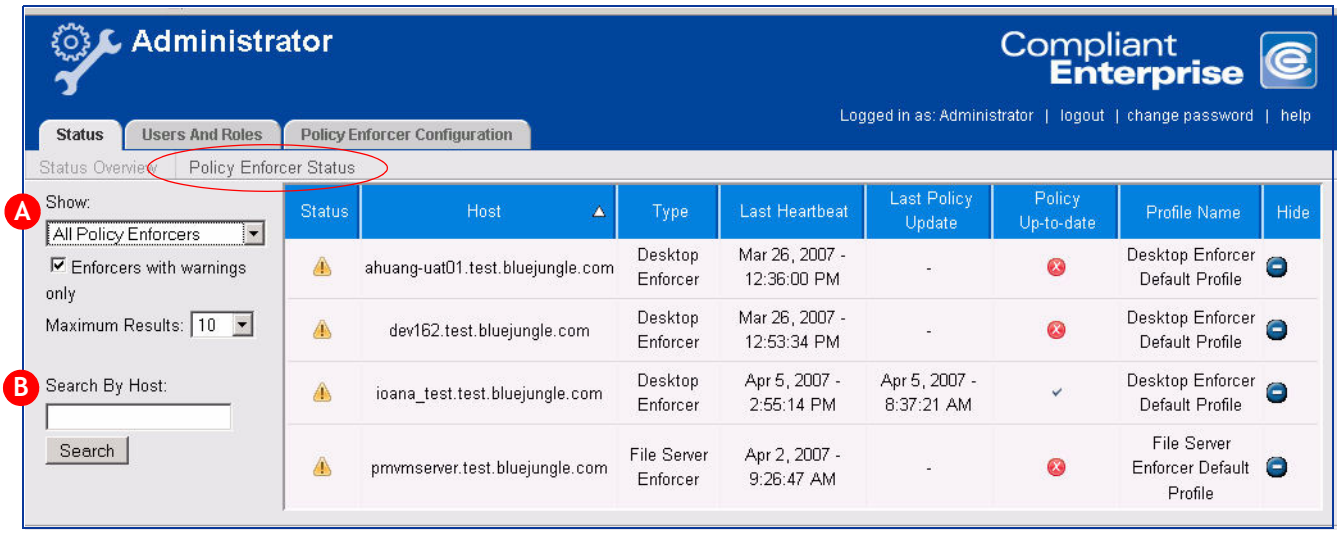


Figure 5-1: Monitoring the Status of Enforcers

By default, this tab displays the status of all enforcers in the system; to view only SharePoint Enforcers, select that item from the Show combo-box list at the left (A). You can also filter by host name (B), if you are interested in the status of enforcers on a specific enforcer host or host group. For descriptions of the contents of the enforcer status grid, see Table 2-1 on page 30.

Index

H

I

L

M

N

P

R

S

T

U

V

W

Index