Compliant Enterprise

The Compliant Enterprise Active Control System

Release 2.0

Product Overview

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: PO2.0-B02

Contents

Preface

Welcome to the Compliant Enterprise Active Control System, the information control platform that provides broad insight into and control over how information is used in your enterprise. Compliant Enterprise not only protects information from unauthorized access, it lets you control how files are used after access is granted.

What's New in the 2.0 Framework

Release 2.0 of Compliant Enterprise is based on a revised framework architecture that decouples the components of the product so that they can be developed and released on schedules that are independent of each other. Specifically, this framework allows the following new features and improvements over the 1.6 release:

- Support for Policy Author 2.0, which includes an overall redesign of the interface: look and feel, menu structure, generic controls, and organization of the components panels and action types. This redesign is geared toward increasing overall usability, and also supporting policy enforcement on collaboration portals.
- Support for policy enforcement on collaboration portals, including release 1.0 of the SharePoint Server Enforcer. In Policy Author 2.0, this support is reflected in the new Portal Content component type, and in a redefinition of the Basic Actions.
- Support for release 1.6 of the File Server Enforcer for Linux, which extends the functionality of the 1.6 Windows File Server Enforcer to Linux-based servers.
- Support for Custom Obligations. You can write custom executables or batch files to perform any kind of behavior you like, which can then be invoked as a result of policy enforcement. Examples of custom obligations might be sending a page message, encrypting some specified documents, or automatically scanning documents and flagging those with sensitive contents. Note that this feature is only available with enforcers that also support it.
- Ability to export defined policies and components from one instance of Compliant Enterprise and import them into another.
- Reorganization of the product documentation set, as described below.

Feature Dependencies Matrix

Compliant Enterprise consists of a central framework or platform, known as the Control Center, plus peripheral components that include Policy Author, pre-built enforcers, and custom-built enforcers. Due to the new framework mentioned above, each release of the framework will support a given set of features, but it is important to realize that some features may require specific version of other components.

For example, if you have the 1.6 framework installed you can upgrade to 2.0 and continue using the 1.6 Policy Author with it—the new framework is backward compatible in that sense. If you do, however, you are limited to the features that are supported by the earlier version of the Policy Author. For instance, you will not be able to take advantage of the custom obligations feature of the 2.0 framework, since the earlier version of Policy Author does not display the field where you add custom obligations to policies.

For each release of the framework, some features will have such dependencies and other will not. For this reason it is important to bear this possibility in mind, and to keep the components of your system synchronized whenever this is required for supporting new features. Table 2-1, below, summarizes the requirements of the 2.0 framework.

Table 2-1: 2.0 Framework, Dependencies Matrix

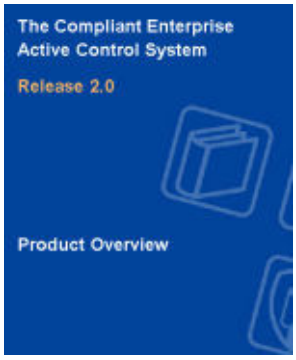
Feature	Supported By	
	Policy Author	Enforcers
Exporting and importing policies	Any version (no dependencies)	Any version (no dependencies)
Custom obligations	2.0 or higher	• SharePoint Server v. 1.0 • Windows Desktop v. 1.7
Policy enforcement on collaboration portals	2.0 or higher	SharePoint Server v. 1.0

Product Documentation

The Compliant Enterprise documentation set consists of eight manuals: this 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 this product overview carefully, in order to acquaint themselves with the high-level architecture and function of the platform as a whole.

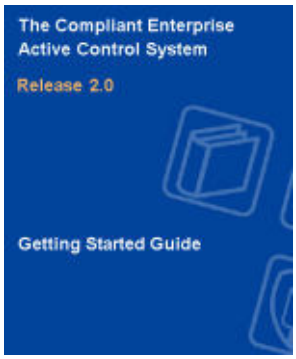


Getting Started Guide

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

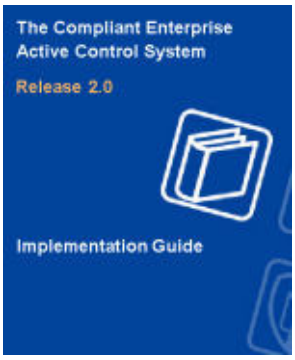
The installation procedures for all policy enforcers are provided separately, in the *Enforcer Administrator's Guide*.

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



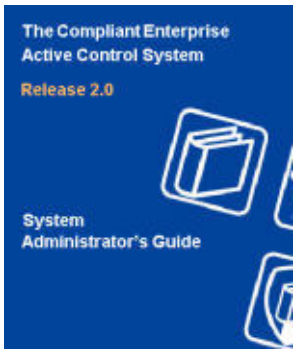
Implementation Guide

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.



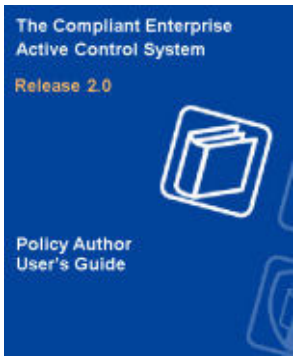
System Administrator's Guide

This *System Administrator's Guide* provides information required for managing and maintaining the Compliant Enterprise system once it is set up. It provides complete instructions 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.



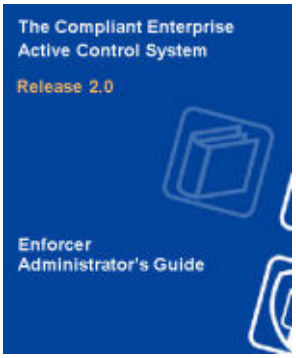
Policy Author User's Guide

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.



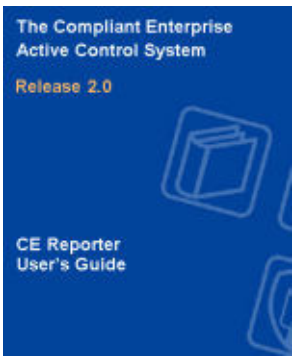
Enforcer Administrator's Guide

The *Enforcer Administrator's Guide* provides information on using and maintaining all the types of enforcers currently available for ***Compliant Enterprise***: for Windows file servers, Linux file servers, 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.



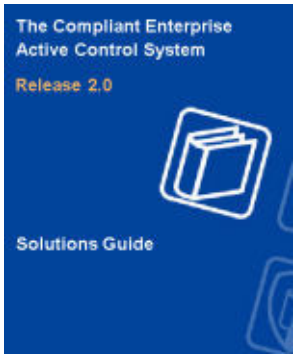
CE Reporter User's Guide

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 Compliant Enterprise

This chapter presents an introductory description of what Compliant Enterprise is and how it can help your organization regain control over the way confidential information is accessed, used and shared. It contains the following topics:

What is Compliant Enterprise?

The Compliant Enterprise Information Control Platform is an enterprise-grade software solution that provides insight into and control over how information assets are used throughout an organization. It consists of the platform itself, multiple enforcers distributed to points of information use, and a set of resource kits that let you customize and extend the platform's powerful features to suit your specific requirements. This book provides an overview of the platform and enforcers, and how they work together. The SDK is discussed separately, in its own documentation set.

What it Does

Compliant Enterprise can perform several fundamental functions in any organization: it can monitor and record how people anywhere are accessing and using information resources, and it can prevent people from accessing or using information resources in unauthorized or potentially harmful ways. It can also display various kinds of notifications to users, for example to remind users of workflow requirements or deadlines, or to remind authorized users about company policies on how to handle sensitive resources. Lastly, using custom obligations, it can automatically execute processes such as encryption, interactive user prompting, deletion, or sending customized pager messages, in response to the context in which a user accesses some resources. We refer to these as the platform's *auditing*, *control*, *education*, and *automation* capabilities.

Auditing

Compliant Enterprise enables you to gather comprehensive data on information access and use throughout your organization: in short, who is using which documents, what they are doing with them, and when. This is helpful both initially, in assessing risk and designing information control policies, and continuously

afterwards, to monitor the effectiveness of those policies and detect new sources of risk as they arise.

Control

Once you have identified risk areas, you can design information use policies that will enable you to control your organization's information use. Compliant Enterprise allows you to create policies that control how specific kinds of users can access or use specific kinds of information resources, under various specific conditions—which application or computer is used, what network location is being accessed, and even what time of day or day of the week or month it is. When a user's actions are in conformance with the policy, they are allowed; but if someone tries any action prohibited by the policy, he or she is blocked, and is reminded about the policy by a pop-up message.

Education

Of course, all kinds of users in an organization are constantly accessing and handling information resources they are authorized to use. Even if control policies are deployed, they allow authorized user to open the most sensitive files or other resources. You can design policies that display notification messages to the user, to remind him or her of use policies that apply specifically to the resources, time context, user, computer or application being used, or some combination of all those. This represents a valuable tool for educating your workforce on the proper ways of handling any information resources, or of disseminating any other information—policy workflow requirements, upcoming deadlines, lockout time windows, etc.—to users in a context-sensitive way.

Automation

Custom obligations, a new feature in Compliant Enterprise 2.0, allow you to attach any executable program to a policy, so that it will be invoked in response to the actions and context specified in that policy. For example, you can write an obligation that automatically encrypts documents, and then use it in a policy that allows certain users to post certain files on a SharePoint portal, but only on certain secure sites; and when they do, the files will be automatically encrypted first. This has the benefit of automating a control mechanism so that users retain flexible use of the resources, while security measures are automatically applied, eliminating the potential for human error. Because any action or series of actions that can be carried out by an executable file (an .exe or batch file) can be included in policies as a custom obligation, this feature offers enormous potential for powerful, proactive policies.

The Abstraction Layer

An integral part of designing policies is mapping your physical environment to a set of components. Components are logical entities you define, which represent categories of physical entities such as computers, users or documents. These can then represent individual entities in a flexible and powerful way, allowing for policies to be defined without worrying about changes to the physical business environment.

For example, you could define a component representing all members of an advanced concepts development team, one representing all sensitive design spec documents, and one representing both laptop computers and removable media such as USB thumb drives, CDs and ZIP drives. You can then use these components to build a policy that will stop any members of the advanced development team from copying design specs onto removable media or laptops. Once this policy is deployed, it will perform the assigned function on the basis of these categories, regardless of which individual document or user is involved. This allows the policy to remain effective regardless of changes in personnel, creation and deletion of documents, or acquisition of new hardware peripherals.

You create both policies and components in a simple, drag-and-drop user interface called Policy Author. To do this, you use Active Control Policy Language, or ACPL, which allows you to define components based on basic properties, then combine them in straightforward, English-like strings that represent the policies. We'll look more closely at ACPL a bit later.

The Implementation Cycle

Each of the functions that Compliant Enterprise provides is extremely useful on its own, but they provide even more power in the way they work together in a kind of operational cycle, represented by Figure 1-1.

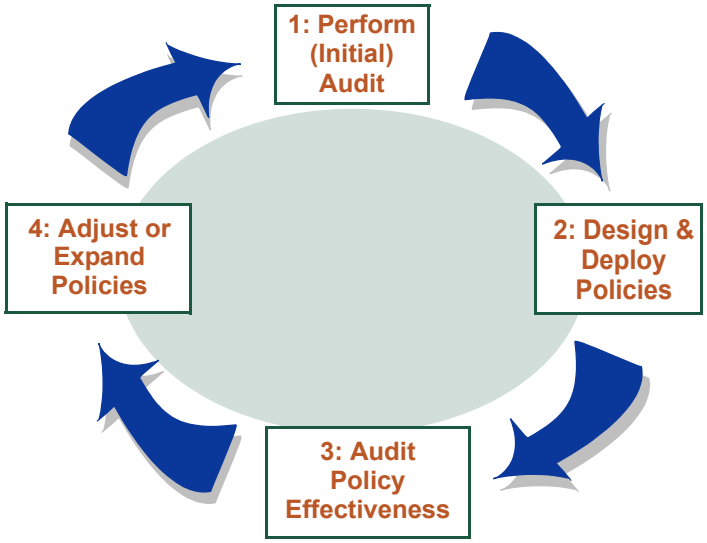


Figure 1-1: The Implementation Cycle

1. You generally start using Compliant Enterprise by running an initial system audit, which can identify who is using which documents, what they are doing with them, and when. You can start such an audit with a few mouse clicks, and let it run for as long as you think appropriate. This resulting data can then be queried and analyzed in flexible charts and detail tables,

that will help you identify areas where information use policies could be helpful.

2. Based on your analysis of these reports, you then design, create and deploy a set of enforcement policies along with the components they require. (Although components provide the building blocks of policies, as a rule the two are designed and created simultaneously, rather than in sequence.)

3. When the policies are deployed and placed into effect throughout the network, they begin controlling information use according to their design. At this point the platform's monitoring tools are very valuable for monitoring how well the policies are working, whether they are delivering their intended results, and how comprehensively they cover all potential risks in the network.

4. Based on analysis of the results of this ongoing monitoring, you can debug and fine-tune the deployed policies, and to add new ones to address problems you had not initially anticipated or recognized. In this way the ongoing information control needs can be more and more effectively met as your deployed policy set is refined and perfected.

System Architecture

From a functional perspective, Compliant Enterprise consists of a platform and a set of enforcers. Let's take a closer look at the platform first.

The Platform

The platform is a set of software components that work together to provide the functions required to implement and support comprehensive information auditing and enforcement. These functions are represented in Figure 1-2.

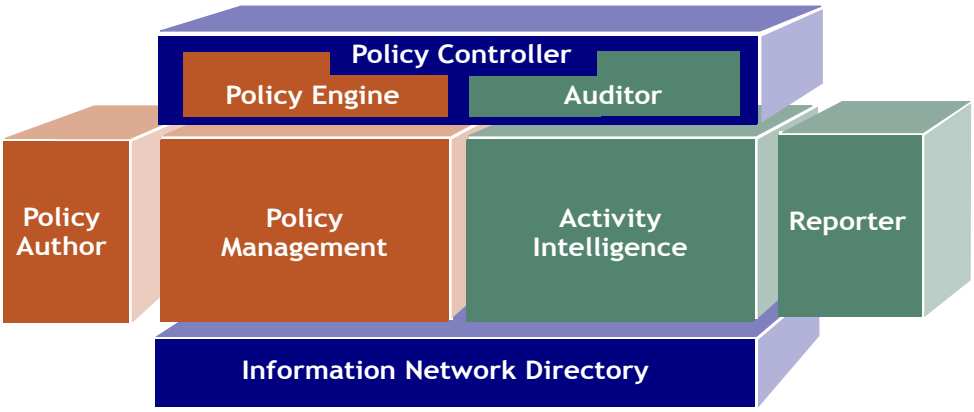


Figure 1-2: The Compliant Enterprise Platform

These functions do not necessarily correspond to physical software components, but rather may be thought of as logical components of the overall operation of the platform. They include:

Information Network Directory: Involves gathering, maintaining and updating information about the physical entities—users, computers, file servers, applications, and so on—present in the network. The platform needs to keep track of this information so it can map it to the virtual components you define to represent these entities. This mapping is referred to as the platform's *Information Resource Model*.

Auditor: Involved in monitoring how all users in the system are accessing and using information resources, and recording it at a central location for later export and analysis. This function is independent of any policy enforcement—it can be used simply for monitoring activity in the network.

Activity Intelligence: Refers to the platform's ability to capture and analyze information in real time on how users are accessing and using information resources. The Policy Engine uses this information to make decisions about enforcing current policies.

Reporter: The ability to express queries to the audit information base, extract the relevant information from it, and export it in a useful format, for analysis. This function, too, is independent of any policy enforcement.

Policy Author: The user interface where authorized personnel can define the policies Compliant Enterprise will enforce.

Policy Management: Refers to a set of functions required to store and maintain policies once they are defined, keep track of the current status of all policies; and know which enforcement points each policy should be deployed to, based on its content.

Policy Engine: Concerned with evaluating the available information every time a user attempts to open or use a document, reviewing the policies currently in effect, deciding whether to permit or deny the action, and determining what responses to take in the course of each enforcement decision. In policy enforcement terms, the Policy Engine represents the Policy Decision Point (PDP) in the system.

Note that the first three functions—those on the right in the figure—are concerned primarily with the platform's auditing and monitoring activity, while the last three, on the left, are connected with the definition, management, and enforcement of information use policies. The platform, obviously, is responsible for both of these areas; however, for both it requires the assistance of enforcers distributed throughout the network.

Policy Enforcers

If the platform components constitute the brain of Compliant Enterprise, enforcers provide its eyes and ears, as well as its muscle. They are the software components that monitor how people are using documents, continuously send that information to the platform for processing, carry out whatever enforcement decisions the platform makes, and then relay information on the enforcement results. There are three kinds of enforcers:

- **File Server Enforcers** run on Windows or Linux file servers to control access to documents stored there, by anyone in the network.
- **Desktop Enforcers** run on desktop or laptop PCs to control both access to and use of documents by individual PC users.
- **SharePoint Enforcers** run on SharePoint servers and control access to all contents available there, similar to the files on a file server.

Enforcers operate as remote clients of the central platform. They provide the multiple Policy Enforcement Points (PEPs) of the system, but they rely on the decision-making intelligence and management controls of the platform for their operation. This centralized architecture significantly simplifies the administration and management of the system, and allows multiple administrators to work collaboratively designing and deploying policies.

Enforcers receive messages from and send data back to the Policy Controllers. These in turn communicate with the Control Center server components through a special protocol called the Information Control Enforcement Network, or *ICENet*.

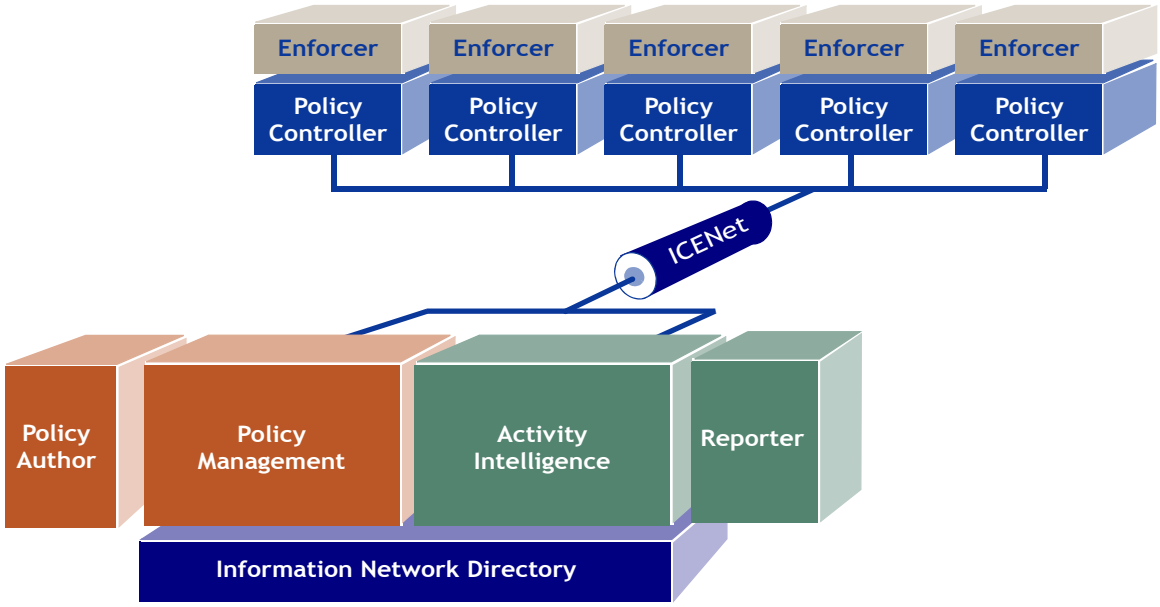


Figure 1-3: Compliant Enterprise Enforcers

Information Use Auditing

As the discussion earlier in this chapter should make clear, Compliant Enterprise's auditing function is valuable both in performing an initial audit independent of any policy enforcement, and in combination with deployed policies. The auditing function continuously gathers data about how documents are being accessed and used throughout the network, and stores them in the Activity Journal database. From there, authorized users can generate reports using the flexible querying tool called Reporter, to produce summary charts and detailed reports of information use over time. Figure 1-4 shows a sample report.

The Activity Journal

The Activity Journal database is the repository for cumulative data about information use and policy enforcement activity. An internal database is provided with the Compliant Enterprise; it installs automatically, is completely integrated with the other components, and is transparent to users. However, as an alternative you can also configure the system to use an external database to store the Activity Journal. The supported DB types are Oracle and PostgreSQL.

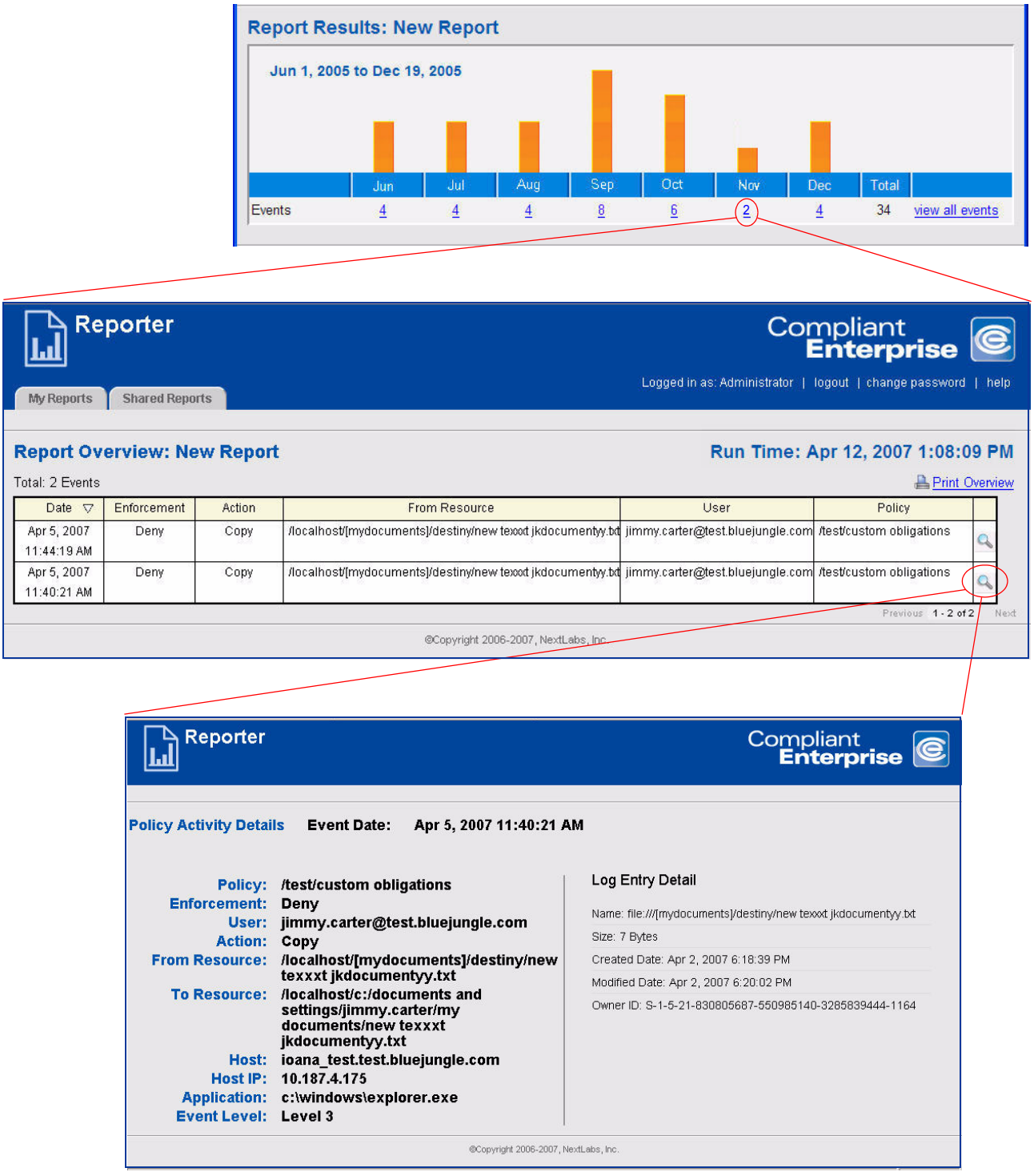


Figure 1-4: Using Reports

Active Enforcement

Enforcing a corporate-wide information protection policy has traditionally been a manual process, relying on employees and contractors to know what needs protection and what actions are necessary to safeguard that information. Compliant Enterprise takes the burden of information policy compliance away from individual employees by automating policy enforcement to prevent malicious information misuses, policy misinterpretations, and even information handling mistakes. Active policy enforcement keeps confidential documents uncompromised and safe from exposure.

As we have seen, Compliant Enterprise relies on a set of deployed policies and policy components as guidelines for recognizing what kinds of activity are permissible, and which are not. When any user attempts to violate a policy, he is stopped from doing so and reminded about the policy. This active, preemptive approach is obviously more effective than relying on auditing alone, which can detect information risks only after the fact. Most effective of all is the combination of active enforcement policies and continuous auditing to monitor the effectiveness of your policies, and identify ways to fine-tune them.

The component\policy architecture of Compliant Enterprise delivers two considerable benefits: flexibility, and ease of use. The system's flexibility is a product its reliance on an Information Resource Model; its ease of use derives from the Active Control Policy Language (ACPL). Let's discuss each of these in turn.

The Information Resource Model

Within Compliant Enterprise, the term *information network* refers to an organization's information resource servers, desktops, network configuration, applications, and organizational structure. Every organization's information network is constantly evolving. To internally represent and organize diverse and unpredictable information networks, Compliant Enterprise creates a consistent internal model called the *Information Resource Model*.

When Compliant Enterprise is deployed, one or more network domains are *enrolled*—that is, imported—into the Information Network Directory. You can enroll multiple network domains to control resources across internal and external networks, for example networks belonging to partners or contractors. User and host data is imported into Compliant Enterprise from LDAP directory systems such as Active Directory, organized, and structured into a common model. As the information network changes, the information resource model is automatically updated.

The Compliant Enterprise policy component model works together with the imported information resource model, to insulate information control policies from information network changes and allow policies to automatically adapt as the information network evolves. This is illustrated by the scenario represented by Figure 1-5. Note that new laptops might be added or old ones subtracted, employees can come and go, and new documents may be created; these changes will be picked up by the information network directory, but they will not require any changes to the defined components, nor interrupt the continuous enforcement of the policy.

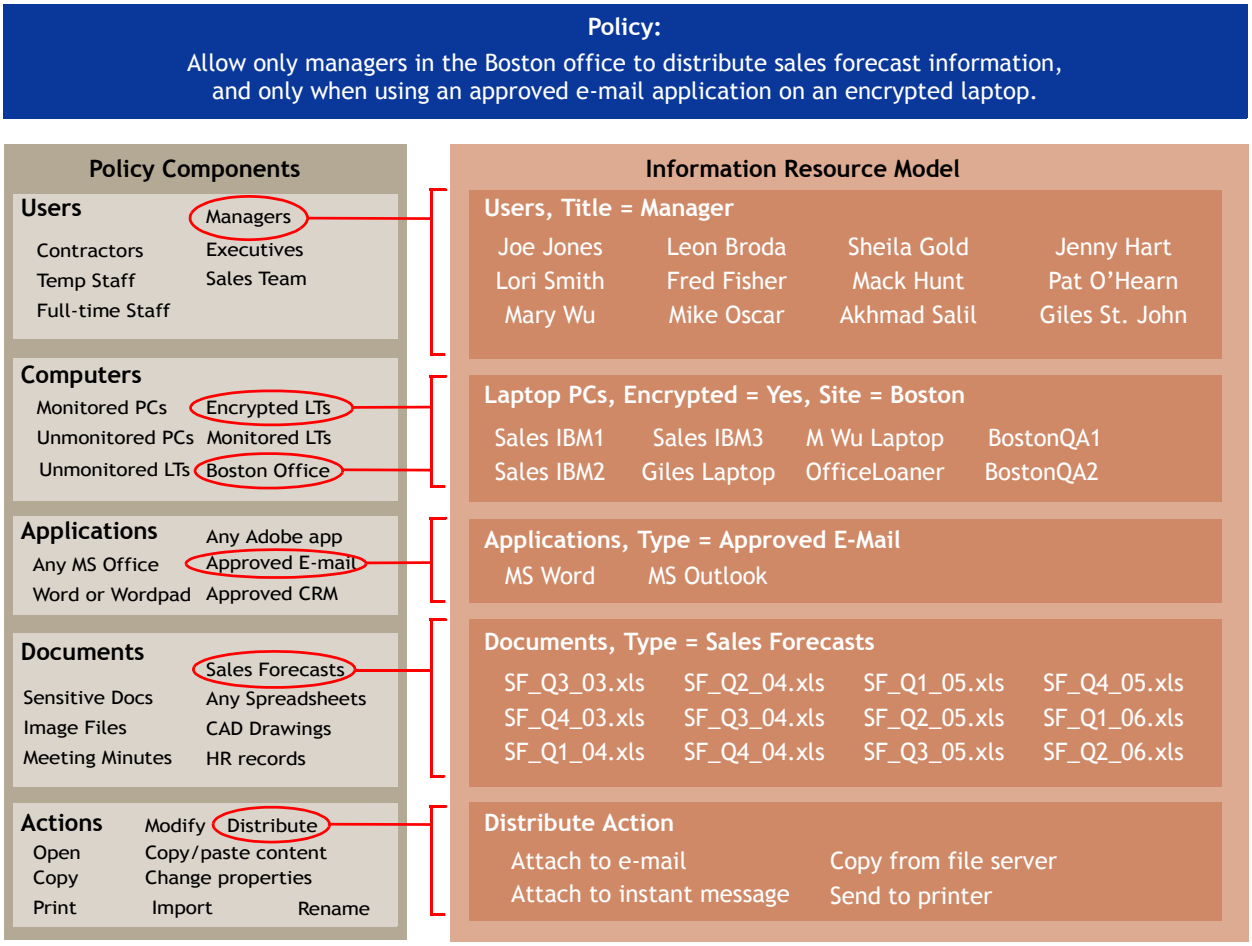


Figure 1-5: Policy Components and the Information Resource Model

The ACPL Language

Compliant Enterprise uses an internal policy language to represent, store, and manage policy components and policies. Active Control Policy Language (ACPL) is designed to allow compliance teams to author policies in business terms. Its system-independent grammar allows a single policy to be applied consistently across multiple heterogeneous systems.

ACPL is based on a natural language syntax, combining several predefined "parts of speech" into statements that follow a given grammar to create meaningful expressions of policy concepts.

Compliant Enterprise users do not need to know or directly manipulate ACPL; the platform provides policy design and management tools. Compliant Enterprise translates user choices in these tools into ACPL for internal use.

ACPL and Policy Components

With ACPL, organizations can define policy components to represent classes or categories of business-level concepts such as “Confidential Information” or “Offsite Contractors,” then use those components as building blocks for policies that reflect categories rather than individual entities. This approach allows each policy to automatically adapt as underlying systems, organizational structures, or document locations change. The following example shows a simple policy:

Allow only product managers to download confidential product information.

“Product managers,” “download,” and “confidential product information” are examples of concepts that can be represented by policy components. These components are defined once in Policy Author and then stored in ACPL, so they are available for use in many policy definitions. If you decide to change the definition of a component later, all policies using that component are automatically updated to reflect the change. In addition, changes to users and computers, which are maintained in your LDAP directory, can be automatically propagated to Compliant Enterprise, so that active policies will reflect them without any need to redefine either policies or components.

Figure 1-6 provides some examples of the different types of policy components that can be defined using the ACPL policy elements:

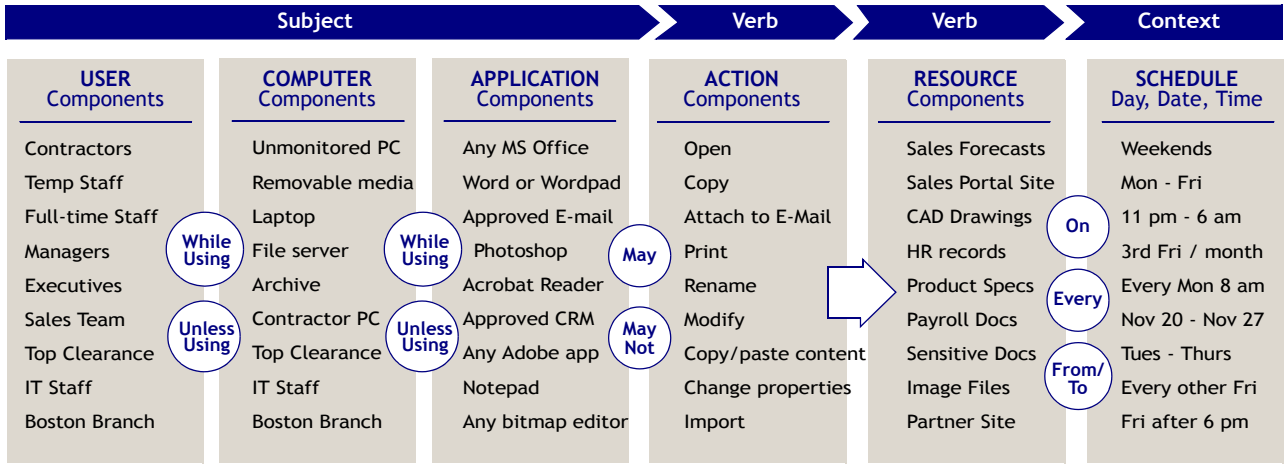


Figure 1-6: Policy Elements and Structure

In addition to components, each policy can have an *obligation*—that is, the action Compliant Enterprise will take after enforcing the policy—and an *effect*: whether to block the specified action, allow it but only if all conditions of the policy apply, or allow it in all cases and perform some specified obligation. Obligations can include displaying a policy reminder to the user, sending a notification e-mail to an administrator, writing the details of the event to the event log, or some combination of these. They can also call a custom-built executable, which allows you to initiate complex actions as a result of policy enforcements.

ACPL Policy Grammar

The ACPL grammar enables Compliant Enterprise users to define policies in the same terms which a compliance officer would use to express enterprise policies in a written document.

For example, a simple policy could be expressed as follows: *Allow only HR staff to access salary records; if anyone else tries, send an e-mail alert to IT Security.*

Within Compliant Enterprise, this policy would be represented by one ACPL statement. A ACPL statement comprises the following parts:

- **Subject** (in the example, "HR staff"): The noun performing an action. Can be a person, computer, or application, or a list including one or more of each
- **Action** ("access"): The verb that describes what user activity should be controlled
- **Resource** ("salary records"): The information resource that is being controlled
- **Effect** ("Allow only"): The enforcement result that should be performed (either allow or deny)
- **Obligation** ("if anyone else . . . "): Specify event logging and/or e-mail notification whenever the policy is enforced.

ACPL is flexible and extensible, and supports sophisticated sentence construction including compound parts of speech, contextual evaluation, and specification of both source and target resources. Here is an example of a more sophisticated policy:

Allow only Brand Managers or product management executives using corporate desktops and approved e-mail to distribute confidential product information between 9:00 am and 5:00 pm.

Overview of Components

The following brief overview of the architecture of the Compliant Enterprise platform should help clarify the above discussion of how the system works. we will provide a more detailed discussion of the system architecture in Chapter 2.

Compliant Enterprise consists of the following software components:

The Control Center: A set of central server components, that work together as the heart of the platform. They may be installed on one host or distributed among many.

Policy Enforcers: Tamper-resistant software components you can install on one or more file servers, and on desktop and laptop PCs in your network. Enforcers run continuously as Windows services, to monitor and control information access as needed. You can install two types of enforcers:

- **File Server Enforcers** run on Windows file servers to control access to documents stored there, by anyone in the network.
- **Desktop Enforcers** run on desktop or laptop PCs to control both access to and use of documents by individual PC users.

Ordinarily you will have both kinds of enforcers present in your network, but which file servers you need to protect, and how many PCs you want to monitor, depends on you individual requirements.

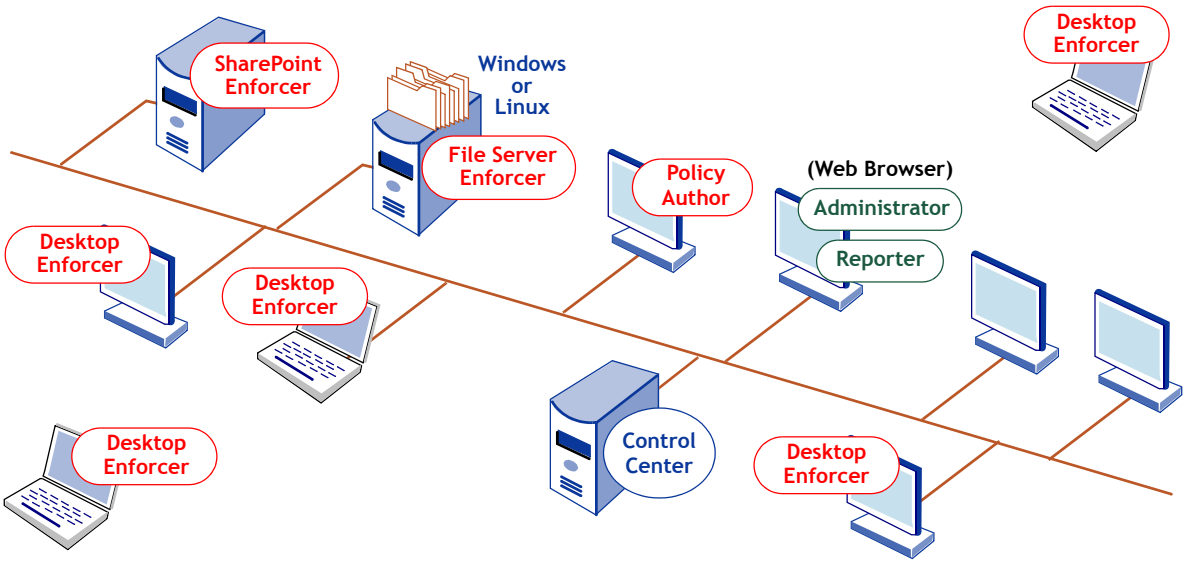


Figure 1-7: Compliant Enterprise Components

Policy Author, **Reporter**, and **Administrator**: A suite of graphical interface tools that allow you to define and implement your control policies, monitor policy enforcement and other system activity, and administer the system. Policy

Author is locally installed on an authorized user's PC; Reporter and Administrator are Web applications that can be opened anywhere, through a Web browser.

Compliance personnel use Policy Author construct your organization's information control policies and specify what action Compliant Enterprise should take in each case. Once defined, policies are managed in the Control Center, which deploys them to the enforcers running on file servers, SharePoint serves, or desktops throughout your organization.

All policy enforcers constantly monitor user actions and enforce policies as needed; they also periodically check in with the Control Center to see whether updated policies are available. The tamper prevention capabilities of Compliant Enterprise ensure that the policy enforcers are not stopped or uninstalled without authorization.

Whenever a user attempts to use a document in a way that is prohibited by a current policy—to open a SharePoint library item he is not authorized to use, for example, or to attach a sensitive document to an e-mail—the system prevents him from doing so, and displays a notification message explaining that the action is unauthorized. It also logs the event in the Activity Journal and, depending on the policy's configuration, can send an e-mail notification of the attempted unauthorized action, or invoke a custom-built piece of executable code.

As Figure 1-7 illustrates, once Desktop Enforcers are installed on mobile laptops, they continue enforcing document access and use policies whether they are connected to the network or not. This allows, for example, a policy that permits a sales rep to copy a sensitive product presentation onto his laptop so he can show it to a client in another city, but prevents him from copying, printing, e-mailing or renaming it, or even from cutting and pasting any content from it.

To monitor and configure the system, administrative and IT personnel can use the Administrator, with its status indicators, system statistics, and screens for configuring user permissions and policy enforcer behavior. Finally, to measure policy effectiveness or investigate suspected instances of information misuse, executives and audit personnel can use the Reporter to create ad-hoc queries or generate reports.

2 System Architecture

In the previous chapter we described the Compliant Enterprise Information Control Platform in terms of the logical or functional components that combine to provide its auditing and enforcement power. In this chapter, we will look at the software components that make up the system, and how they relate to one another. Bear in mind this is a rather different perspective, and in some cases the software components do not directly map to the logical components we discussed in Chapter 1.

This chapter is organized into the following topics:

Architecture Overview

Compliant Enterprise comprises a number of distributed software modules that interface with different types of desktop computers, file servers, and servers. As we mentioned in the previous chapter, the components include the following:

- A set of server components called the **Control Center**, which provides central policy management, reporting, and system management. These may be installed on a single physical server, or distributed among many.
- **Enforcers**, which are the components that reside out in the network and perform the work of monitoring use and restricting or allowing it in conformance with all currently deployed use and access policies. There are three varieties of enforcers:
  - **Desktop Enforcers**, which provide distributed audit, policy evaluation, and policy enforcement at the desktop or laptop PC level. You install these on as many PCs as you wish.
  - **File Server Enforcers**, which provide distributed audit, policy evaluation, and policy enforcement at the file server level. You install these on whichever file servers you want to monitor and/or control.
  - **SharePoint Enforcers**, which control access to SharePoint portal content, the same way File Server Enforcers control files.

- Three user applications, called **Policy Author**, **Reporter**, and **Administrator**, which provide an interface where administrators can construct and deploy policies, report on activity and policy effectiveness, and perform administration tasks.

Figure 2-1, below, illustrates the connections among these components, showing the Control Center servers in a distributed architecture.

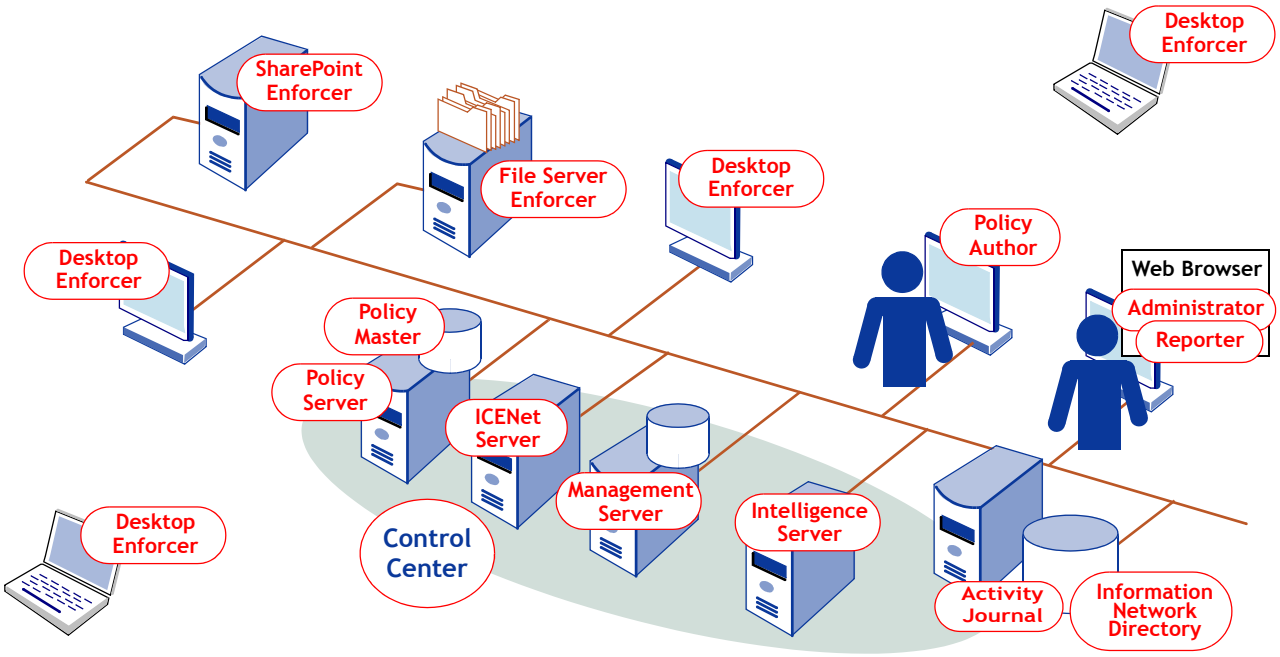


Figure 2-1: System Architecture

The Control Center

The Control Center comprises a number of components and data repositories, including the following:

- Policy Server and Policy Master
- ICENet Server
- Management Server and Information Network Directory
- Intelligence Server
- Activity Journal

Each installation of Control Center has one or more of each of these components, but can have only one Policy Server and Policy Master. Let's take a minute to describe each of these in turn.

Policy Server

The Policy Server is responsible for policy management, including policy definition, lifecycle, and deployment. The Policy Server maintains a Policy Master data store that is used to centrally create and deploy policies. This means that no matter how large your Control Center is, it can have only one Policy Master. The Policy Server is packaged as a J2EE application and communicates via web services.

The Policy Server provides the following functions:

- Policy Construction
- Access Control
- Lifecycle Management
- Policy Component Model
- Deployment

Users access the Policy Server through the Policy Author application, which provides a graphical user interface to author policies and manage the policy lifecycle, from creation through deployment and eventual retirement. Finished policies are stored in a central data store called the Policy Master.

Constructing Policies

The Policy Author tool provides an interface to the Policy Server, making it simple to create valid ACPL statements. Policy Author is used to organize policies into folders, write policy and policy component definitions to the Policy Master, validate the grammar of a policy, and manipulate an object throughout its lifecycle.

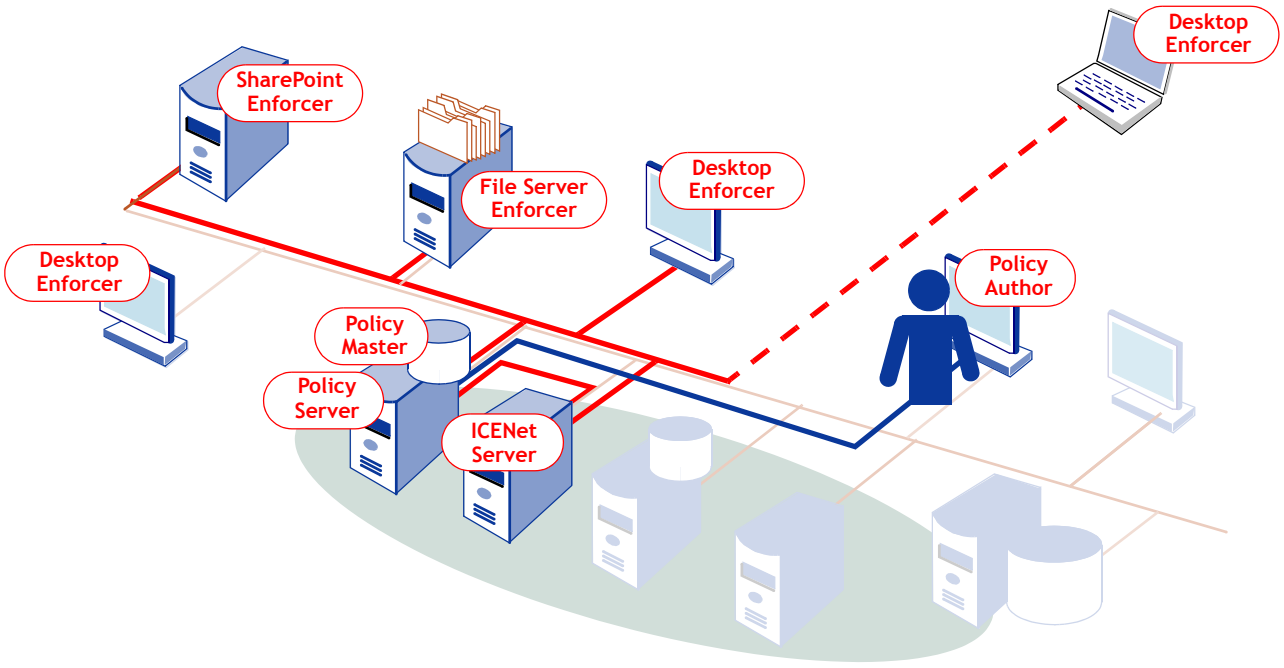


Figure 2-2: The Policy Server

Controlling Access

The Policy Server controls access to policies and policy components, ensuring that only authorized personnel are able to access, manipulate, and deploy policies and policy components.

Lifecycle Management

The Policy Server manages the lifecycle of each policy and policy component. Each object follows a lifecycle from creation to retirement, which enables teams to work collaboratively and minimizes the chance of incomplete or unapproved policy changes being deployed to production systems.

Policy Component Model

The Policy Server manages the Policy Component Model, which is simply the set of components you define to represent the entities in your physical environment.

Deploying Policies

The Policy Server is responsible for storing and implementing deployment specifications for policies and policy components. There are several ways to do this, including:

- **Manual Targeting**: Deploy policies and components to an explicit list of enforcers.
- **Smart Deployment**: Automatically deploy each policy component or policy to those file server or desktop computers where it is needed, based on the documents stored on that system or the type of usage that occurs on a particular desktop.
- **Default Scheduling:** Deploy policies and components based on a default IT schedule maintained for the entire system.
- **Explicit Scheduling**: Deploy policies and components at a specific date and time.

Information Network Directory

The Information Network Directory is a central repository for data about entities in the organization, including users, computers, groups, applications, document resources, sites, etc. This data must be enrolled using various enrollment utilities, and is stored as a separate database schema, on the same DB host as the Activity Journal.

You can use theCompliant Enterprise enrollment utility called Enrollment Manager to enroll one or more of your organization's information networks with the directory. As your organization's infrastructure changes over time, you can automatically update the information resource model by repeating the enrollment process, typically through a script that runs as a nightly scheduled process.

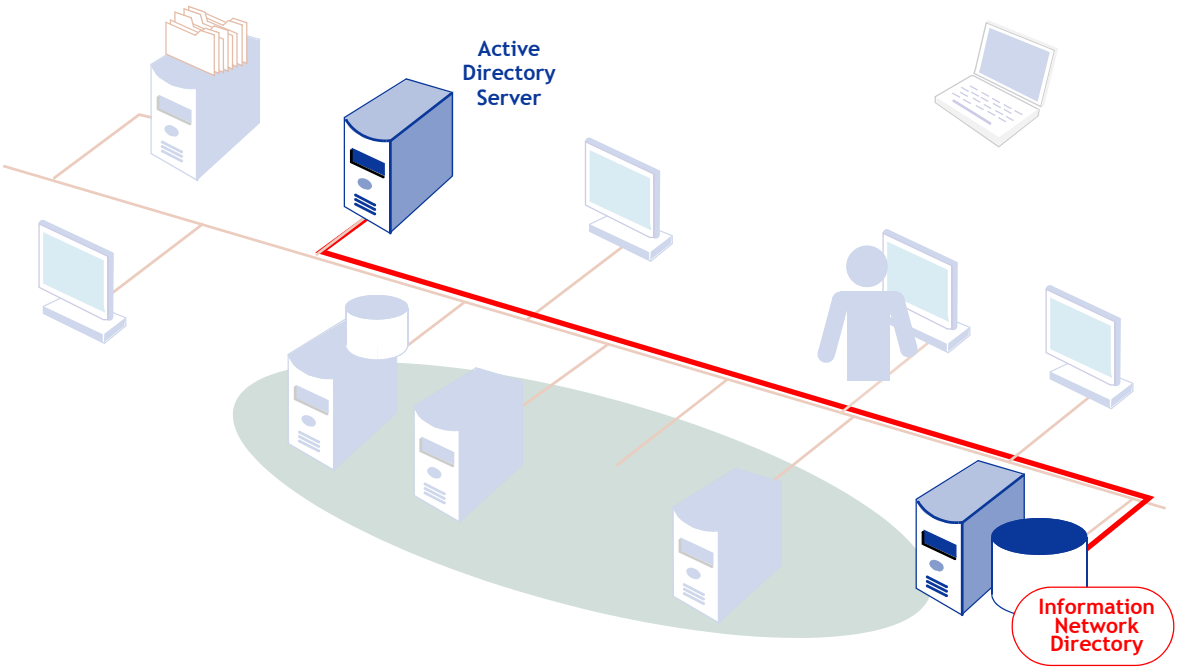


Figure 2-3: The Information Network Directory

The Enrollment Manager utility connects to one or more LDAP directory servers in your environment, such a Microsoft Active Directory server, or to LDIF files you provide, and imports information about the underlying information network. The types of entities that can be enrolled include the following:

- **Users and user groups**: When you enroll users and user groups from an LDAP directory, they are available in Policy Author for constructing User components, which you can then use to construct policies.
- **Computers and computer groups**: When you enroll computers and computer groups from an LDAP directory, they are available for creating Computer components.
- **Sites**: You have the option of enrolling network address ranges that represent physical or logical locations such as Headquarters, Boston Office, or a VPN. These are referred to as *sites*, and they can be used to define location-based Computer components. Site information is not LDAP-based, but is imported from a text file you create, listing the machines included in each site.
- **File Shares**: File share information is enrolled to facilitate mapping to specific resource paths. To enroll file shares, you use a special utility to query the servers in your network.
- **Applications**: You can enroll whatever applications you want to make available for constructing Application components, for use in policies. This process uses a pair of special utilities: one to discover applications on a source PC and generate an LDIF file with information about them, and another to enroll the information from that LDIF file into the Information Network Directory.

Intelligence Server

The Intelligence Server provides summary, trend, and detailed analysis of user activity and policy enforcement. The Intelligence Server is accessed using the Reporter Web application or through Web services, allowing business users to create graphical reports to demonstrate compliance, understand information usage, and investigate cases of information misuse. The Intelligence Server analyzes comprehensive audit information captured in a centralized activity journal, providing insight and accountability for information handing. The

Intelligence Server is packaged as a J2EE Web Application and communicates via web services.

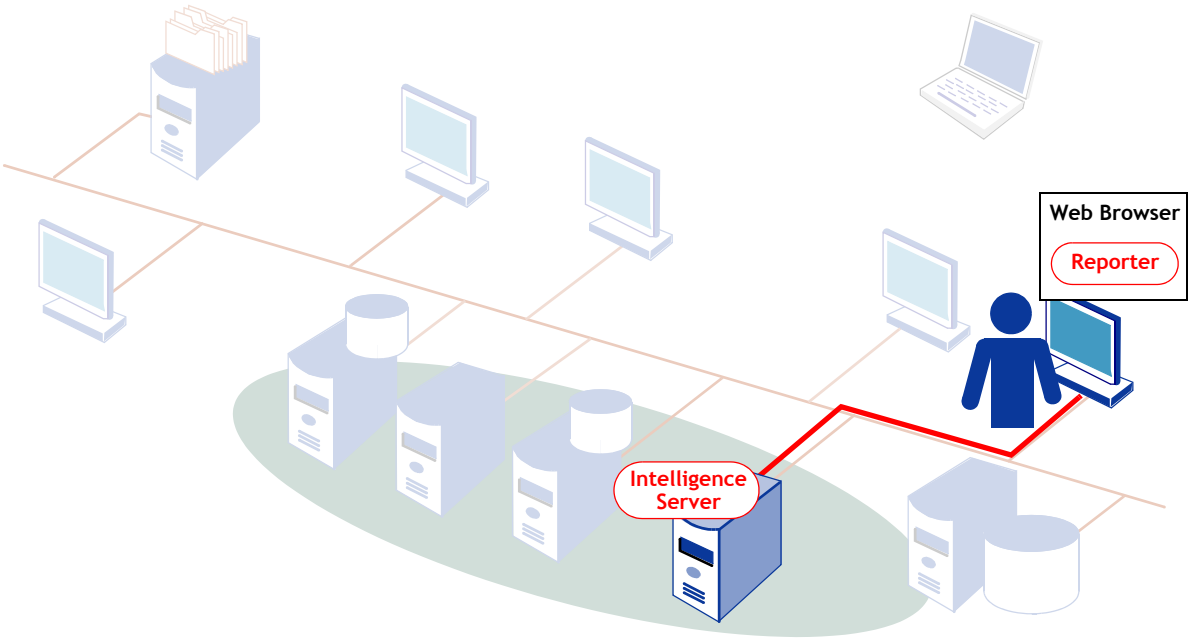


Figure 2-4: The Intelligence Server

The Intelligence Server provides several types of analysis:

- **Summary Analysis**: Activity or policy effectiveness summarized by user, document, document component, or policy.
- **Trend Analysis**: Activity or policy effectiveness for a given time period. The analysis can be explored by zooming in and out on different time periods.
- **Detailed Event Forensics**: Event information for specific user actions or policy enforcements. Detailed reports show the event-level details for document activity or policy enforcement. Compliance officers can use event forensics to investigate specific incidents of information misuse. For each event, the Intelligence Server provides user, resource, destination, time and date, application, policy, and action information.
- **Personal and Shared Reports**: Queries can be saved and shared with other users.

The Intelligence Server exposes this functionality as a set of web services that can be used to integrate this information with other applications or build custom reporting applications. The Reporter tool is a pre-built web application that exposes Intelligence Server functionality.

Management Server

The Management Server is the center of a Compliant Enterprise system. It centralizes the management of all system components, providing a single location to view system status, modify configuration, and manage users. The Management Server includes a central server component, called Management Server, and one or more enforcer communication servers, called ICENet Servers. The ICENet servers manage the communication between the enforcers and the Compliant Enterprise Control Center, and are designed to allow multiple servers to be deployed for large-scale deployments with a large number of enforcers. The Management Server is packaged as a J2EE Web Application and communicates via web services.

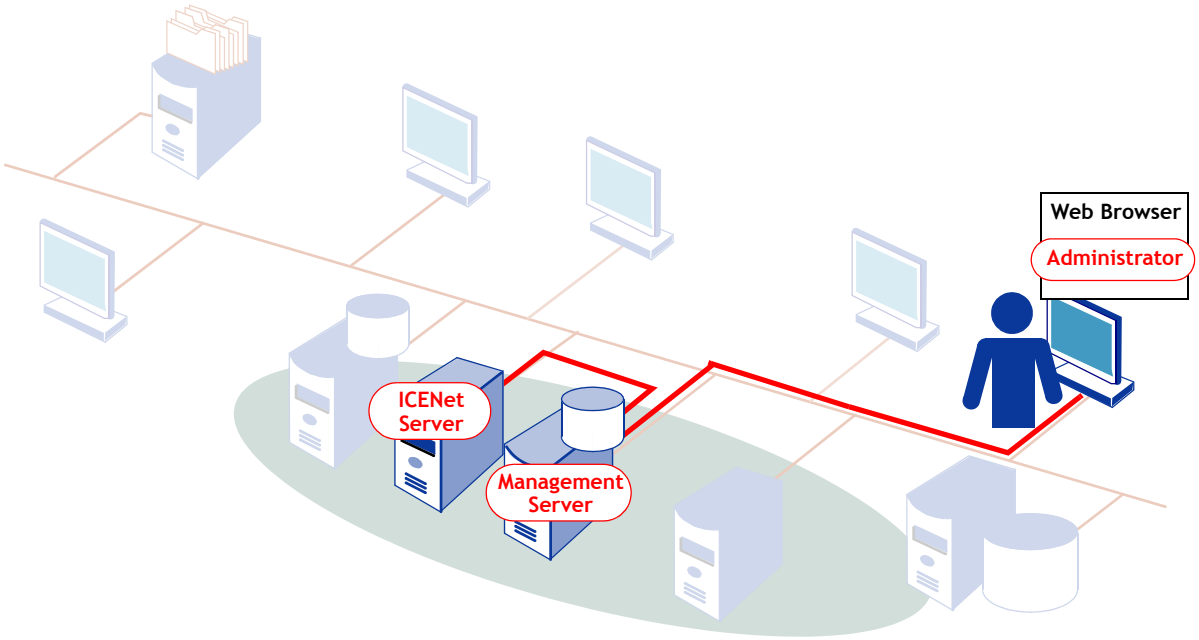


Figure 2-5: The Management Server

The Management Server is accessed through the Administrator Web application, which provides a graphical user interface to management services.

The Management Server provides the following services:

- Monitors all other Compliant Enterprise components, including servers and enforcers. Displays status of each component through the Administrator tool.
- Registers new enforcers and maintains a registry of all enforcers.
- Orchestrates policy deployment.
- Manages users, user groups, and roles.
- Manages the configuration for all servers.

- Manages configuration profiles for enforcers.

ICENet Server

As we mentioned above, the ICENet Server brokers communications between enforcers and the Control Center, including distribution of configuration profiles, policy deployments, and the upload of audit information to the Activity Journal. The ICENet Server is also responsible for creating deployment bundles for each enforcer, containing the current versions of all policies and policy components targeted to that enforcer.

While it is logically part of the Management Server, the ICENet Server is a separate J2EE Web Application that can be deployed on one or more machines based on your organization's scalability requirements.

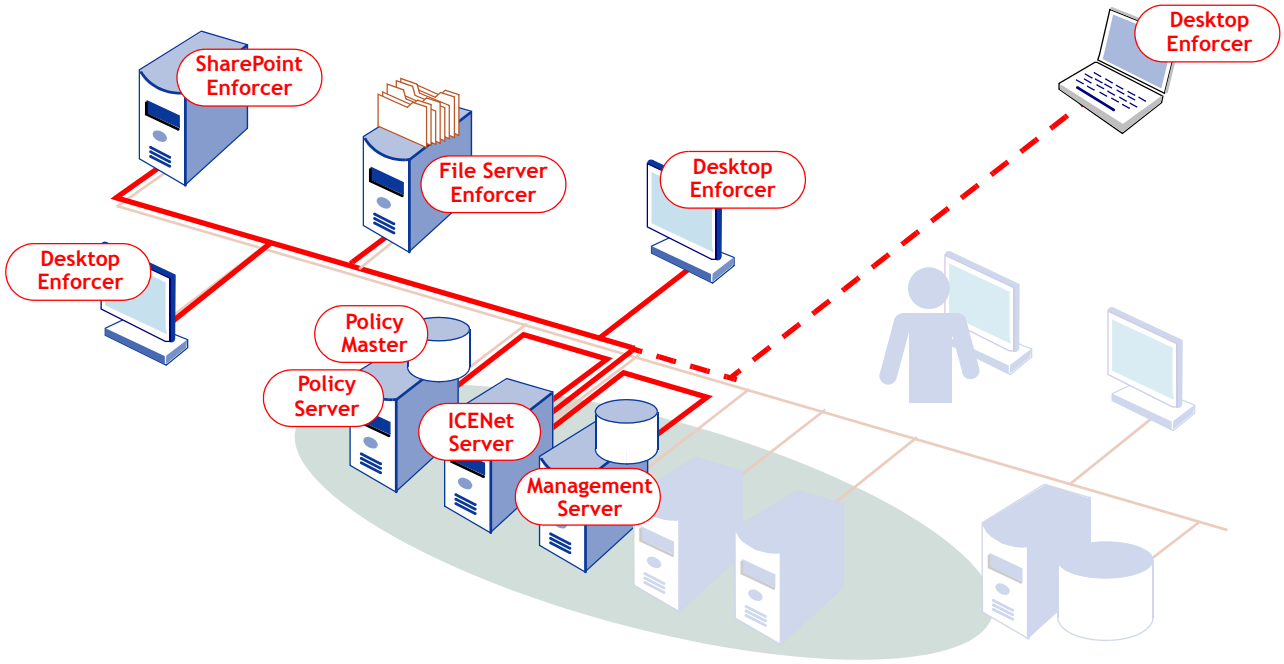


Figure 2-6: The ICENet Server

The ICENet Server builds customized and optimized policy bundles for each enforcer. These customized policy bundles are compiled into policy maps, an optimized format that enables real-time policy evaluation, even on PCs that are disconnected from the network. Because this allows policies to be distributed only to those enforcers that will be actually enforcing them (based on the content of the policies), this is referred to as *smart deployment*. In addition, updated policy bundles are distributed to the appropriate enforcers whenever a change is deployed; the exact moment of distribution depends on the deployment scheduling technique that has been selected.

Enforcers

Enforcers are the part of the system responsible for monitoring how users are attempting to access information resources, and what they are doing with them once they get access; and also for actively preventing any access or use that violates a currently deployed policy. They they are responsible not only for enforcing policy in this way, but also for continuously collecting audit information for their respective host systems, regardless of whether any policies are being enforced or not.

Compliant Enterprise provides three types of enforcers, for a multi-layer approach to information control and compliance enforcement.

- File Server Enforcers are installed on Windows or Linux file servers, and can only enforce policies concerned with uses' access to the information stored on that server.
- SharePoint Enforcers are installed on SharePoint servers, and work in a similar way.

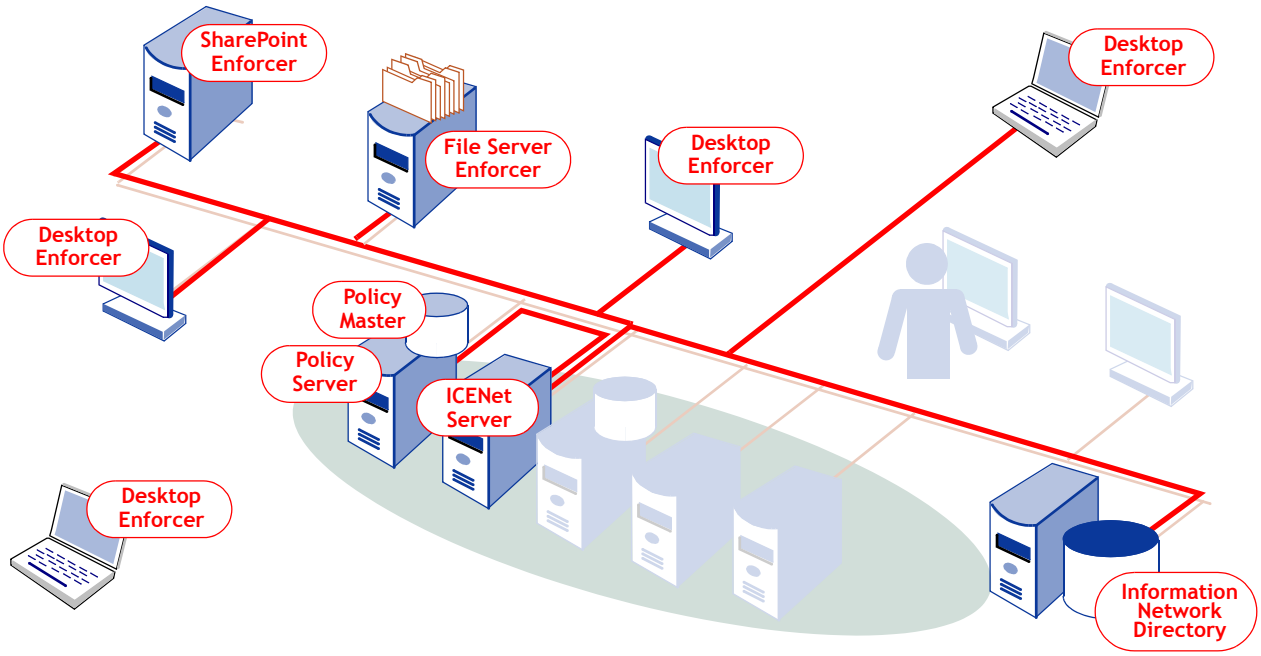


Figure 2-7: Policy Enforcers

- Desktop Enforcers are installed on desktop or laptop PCs, and can control both whether users can access specified information, and also what they can do with it once they get access.

  Desktop Enforcers on laptop PCs continue enforcing policies whether they are connected to the network or not; whenever they do connect, they can receive any updates to their policies from the Policy Server.

Combining all three types of enforcers in a Compliant Enterprise deployment provides control over both document access and the use of information by organization personnel.

File Server Enforcers

File Server Enforcers controls file resources on Windows- or Linux-based file servers. They are installed on file server hosts and enforce document access policies as organization personnel interact with the file server. Access policies control whether users are allowed to create, read, update, or delete documents. The table below summarizes all the actions that File Server Enforcers can control.

Table 2-1: 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
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.

In addition to controlling access to files, File Server Enforcers also can gather information about how documents and folders are used, and about how and when policies are enforced, and save it in the Activity Journal.

File Server Enforcers can be installed on some or all of the file servers within an enterprise, depending on which file servers contain documents for which the organization wishes to enforce document access policy. Each File Server Enforcers affects only the file server where it is installed.

File Server Enforcers must be installed if you want to allow or deny access to document resources on a particular server by users who do not have Desktop Enforcers installed on their PCs. 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.

SharePoint Enforcers

SharePoint Enforcers run on Windows SharePoint servers, and their function is analogous to that of File Server Enforcers. They monitor access to all content available on the server, and can enforce policies that allow specific groups of users to access or post any type of content—portals, sites, library or lists, or library or list items, and so on—depending on the context. This represents a very powerful way to regain control of the access to and use of SharePoint content, without losing the flexibility that makes SharePoint such a useful collaboration

tool. The table below summarizes all the actions that SharePoint Enforcers can control.

Table 2-2: Functions of SharePoint 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 spreadsheet
Attach to Item	Attach one portal list item to another.

Desktop Enforcers

Desktop Enforcers control end-user access to and usage of documents on Windows-based desktop or laptop PCs. They are installed on the desktop or laptop PC, and control both access to and usage of documents, regardless of whether those documents are stored on the PC or remotely, and whether the PC is connected to the network or not.

Desktop Enforcers enforce usage policies, which control whether users of that PC are allowed to open files and perform various actions such as sending, printing, or copying particular types of files. The following table summarizes all the actions that Desktop Enforcers can control:

Table 2-3: 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

Table 2-3: Functions of Desktop Enforcers (Continued)

Action	Description
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

Desktop Enforcers also collect information about each enforcement event for the Compliant Enterprise Activity Journal.

Desktop Enforcers can be installed on anywhere from none to all of the PCs within an enterprise. Each Desktop Enforcer affects only the PC where it is installed.

Policy Enforcer Architecture

Both types of enforcers have a similar architecture which includes the following components, delivered as a single software package:

- Policy Engine: a policy decision point (PDP) that is responsible for evaluating policy and managing the local set of policies, or policy bundle.
- Policy Enforcement Point (PEP): a system-specific policy enforcement point that is responsible for detecting events and enforcing policy decisions made by the Policy Engine. Enforcers are built specifically for each target system to provide tight levels of integration with the host platform.
- Auditor: logs all end-user document activity. The behavior of the Auditor is controlled from the Administrator tool as described in the Administrator's Guide.
- Manager: manages enforcer configuration and self-monitors the enforcer by preventing tampering and restarting the enforcer in cases where it is shut down unexpectedly.
- Compliance Notifications: an optional component that can be used to present a message when an enforcement action has taken place.
- ICENet Client: controls remote communication with the ICENet Server.

What Enforcers Do

This section describes the functions performed by enforcers in the course of their routine operation.

Policy Enforcement

The Policy Enforcement Point (PEP) detects end-user or system events that may be subject to information control policies. The contexts of these events are provided to the Policy Engine, which is responsible for evaluating any relevant policy. The effect of the policy is communicated back to the PEP, which contains system-specific logic to apply the enforcement. If the policy evaluation results in the requested event being denied, the enforcer typically returns a standard system error that indicates that access is denied or that the requested action cannot be performed.

Auditing

The Auditor receives its settings from the enforcer configuration profile, which indicates what actions should be audited on the current system. Any event that matches the Activity Journal 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 central Activity Journal.

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

Tamper Resistance

Enforcers are protected from tampering by unauthorized personnel; they can not be stopped, started, or uninstalled except through the appropriate administration channels. The following features contribute to the tamper resistance capabilities:

- Automatic startup of the enforcer service or daemon to protect information immediately and continuously
- Password protected service to prevent other programs and users from stopping the service
- Self-recovery service automatically restarts itself whenever it terminates improperly
- Protected installation directory and system files to prevent unauthorized uninstallation, deletion, or modifications
- Activity logging to track all tampering activities

How File Server Enforcers Work

File Server Enforcers are designed for the multi-user, high performance environment of enterprise file servers. They are application independent, functioning at the file server level. They monitor the access to all files by all users, and prevent unauthorized access or use whenever detected, based on the policies currently deployed to that server. Whenever they enforce a policy, a standard Windows notification message (“You do not have permission to read the con-

tents of this folder," "This file is read-only and may not be copied," and so on) displays to the end user.

Three components are installed with the File Server Enforcer:

- A Windows Service or Linux daemon process, which provides Policy Engine, Manager, Auditor, and ICENet services
- A TDI Driver, which monitors network requests for files
- An IFS driver, which monitors file system requests

This architecture allows the File Server Enforcer to evaluate policies based on the greatest amount of context for each request, since it can use both network-level and file system-level information.

The File Server Enforcer is self-monitoring and self-protecting. When it is running, no user or process can modify, delete, or access the File Server Enforcer system files including the binaries, log files, and policy bundle. If the File Server Enforcer is stopped unexpectedly, it is automatically restarted.

How Desktop Enforcers Work

Desktop Enforcers are application- and file format-independent modules installed on a desktop or laptop PC, which detect file activity for all applications running on that PC. Desktop Enforcers run as a Windows service and can only be stopped by using an administrative password on the host machine. Once stopped, they will automatically restart when the host reboots, or it can be manually restarted by a user with local administrator privileges.

During installation, Desktop Enforcers can be configured to run silently, with no notification or feedback for the personnel who are subject to the policies being enforced; or they can be configured to run with notifications turned on. In the latter case, the Notification component runs as a separate executable process, and can be seen as an icon in the Windows system tray. Whoever is using this PC can right-click on the icon to display a menu of local controls, as shown in Figure 2-8.

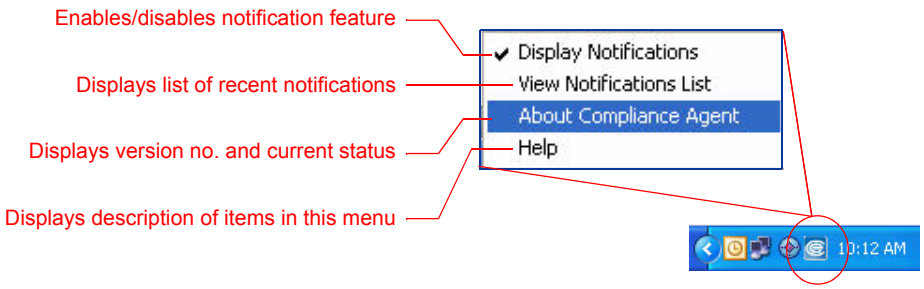


Figure 2-8: Desktop Enforcer Local Controls

When a policy is enforced at this host, whether preventing or allowing a user action, a notification message appears in an information balloon, as shown below.

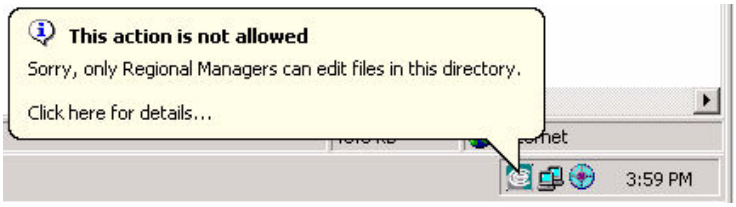


Figure 2-9: Sample Desktop Enforcement Notification

At any time, the user can view the list of policies that have been enforced by right-clicking on the CE icon and choosing View Notification List. The user also has the option of disabling these notifications, and later re-enabling them.

The 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 bundle. If the Desktop Enforcer is stopped unexpectedly, it is automatically restarted.

Applications

This section provides an overview of the three applications you use to interact with Compliant Enterprise:

- Policy Author
- Administrator (page 46)
- Reporter (page 48)

Bear in mind that you cannot start using any of these three until you have installed the Control Center components and enrolled all information about your environment into Compliant Enterprise.

Policy Author

Policy Author is an application that runs on Windows and is used by policy designers and administrators for modeling and for constructing and deploying policies.

Modeling

Modeling refers to the process of defining of policy components—the representations of various parts of the enterprise environment, such as users, user actions, documents, and applications, as well as hardware such as file servers and desktop PCs.

Each policy component represents a class or category of real entities, such as a given set of file servers or users that share certain characteristics. For example, a policy component representing one or more files can be defined based on the

location of the file, document name, owner, or creation and modification dates. The actual files corresponding to a given policy component may change over time as the location and attributes of files change.

The use of modeling allows the policy author to create policies based on logical rather than physical entities. This kind of abstraction is useful in a complex environment, where employees, documents, and machines are in a constant state of flux, entering and leaving the organization or moving about within it. When policies are based on the policy component model, changes to the underlying physical resources or users do not necessitate changes to policies.

Figure 2-10 shows the workspace in Policy Author where you define components.

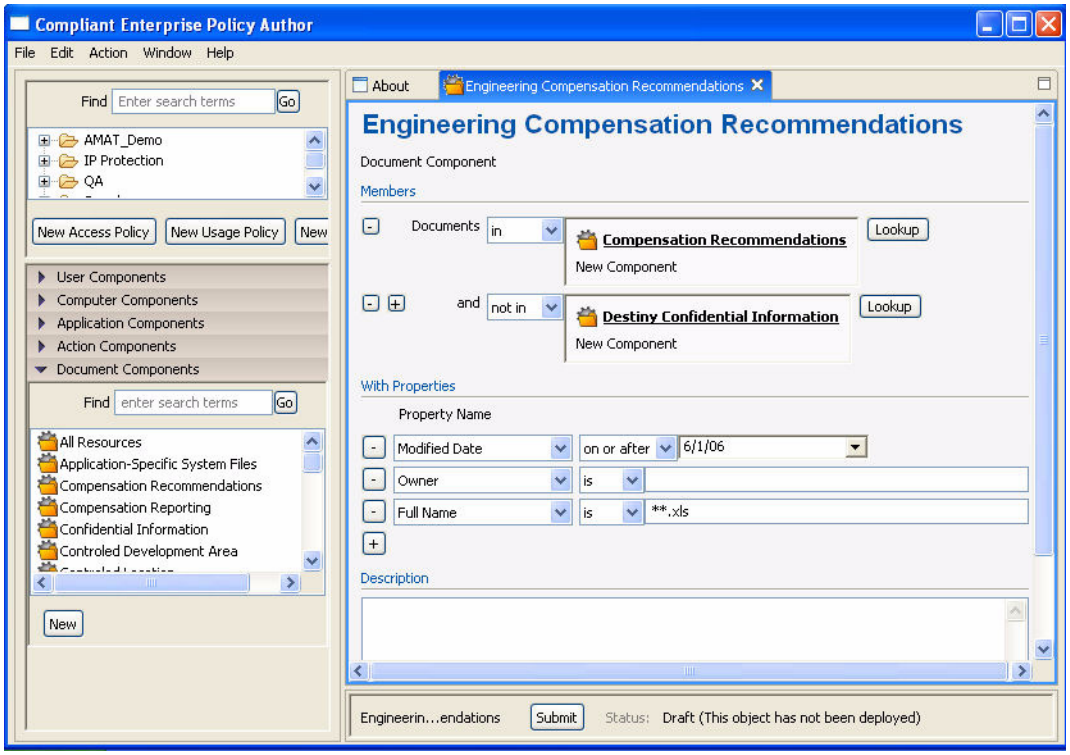


Figure 2-10: Working with Policy Components

Constructing Policies

Once you have defined components, you can use them as the building blocks for policies, specifying which components are involved and how, and what consequences occur when users attempt to perform certain actions. Constructing policies involves putting the appropriate policy components together, along with a predefined set of possible actions and conditional expressions. For example, an organization might develop a policy that allows people on the graphic design and training development staffs to create media files, but denies all others permission to do so.

As we discussed in the previous chapter, policies are based on an underlying language called ACPL, with a strict grammar which dictates the structure of each policy. Every Compliant Enterprise policy is made up of the following:

- The *resource*, meaning the category of files that will be covered by the policy. Resources are represented by the policy components defined during the modeling process.
- The *action*, such as opening or editing a file, that triggers the policy.
- The *subject*, meaning the category of users to whom the policy applies. Subjects are also represented by policy components.
- Optionally, the policy can include additional contextual conditions that must be met in order for the policy to be enforced; for example, a policy might be enforced only between the hours of 11 p.m. and 7 a.m.
- Each policy also specifies the enforcement *effect*: whether to permit or prevent the specified action on the specified resource.
- The policy also specifies any additional follow-up tasks to be done after the policy is evaluated, such as adding a record of this policy event to the log file or sending a notification e-mail to a particular user. We refer to these follow-up tasks as *obligations*.

Figure 2-11 shows the workspace in Policy Author where you define policies.

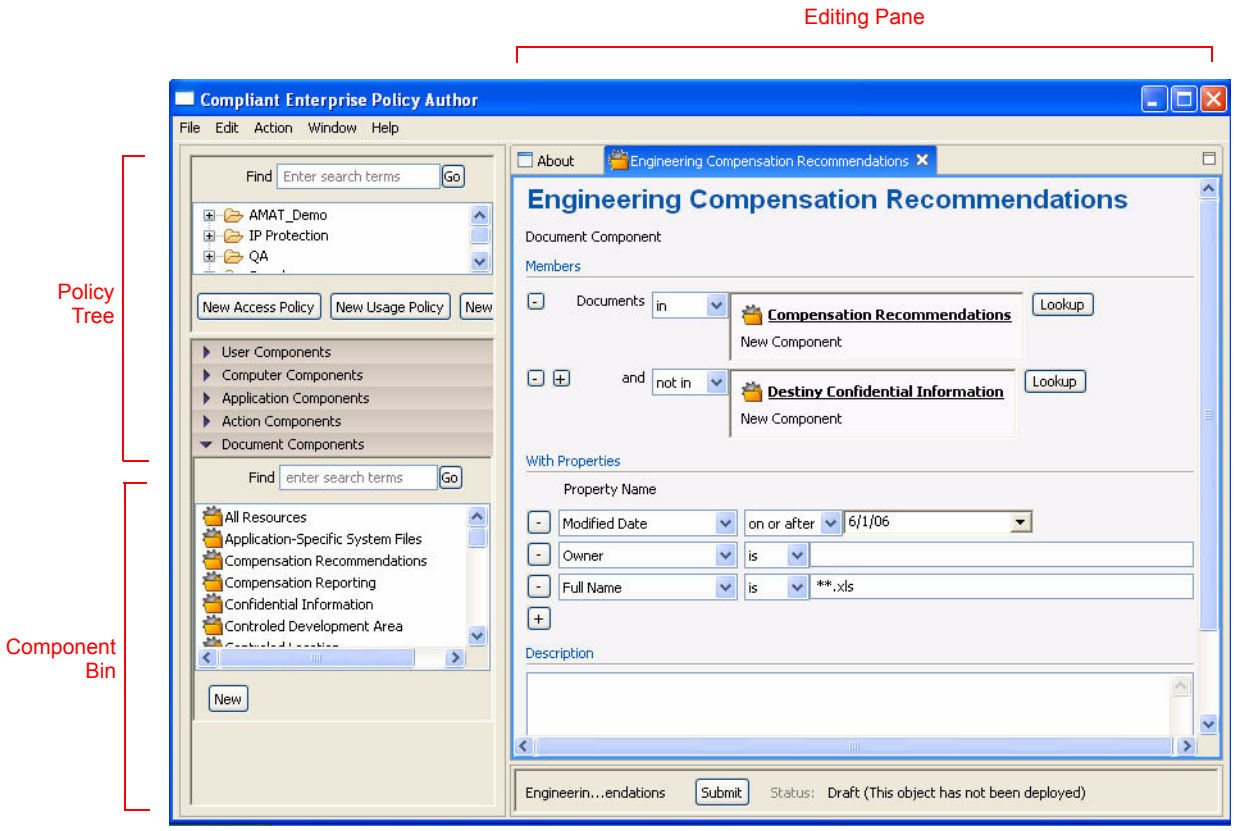


Figure 2-11: The Policy Author Workspace

As the figure shows, the Policy Author window is divided into three panes.

- The **Editing Pane** is where you specify the properties of components and policies as you construct them initially, or refine or change them later.
- The **Policy Tree** pane is where all currently defined policies are organized, in a standard folder tree structure.
- The **Component Bin** is where all currently defined components are organized, available to use as building blocks for policies. To build a policy, you simple drag components from the bin into the appropriate fields on the Editing pane.

A fourth pane, **Preview**, is available when you need it. It is used to preview the actual results of defining a component a certain way. For example, if you define a User component as anyone whose last name start with the letter M, you can

open the Preview pane to view a list of all the individual users that component would represent.

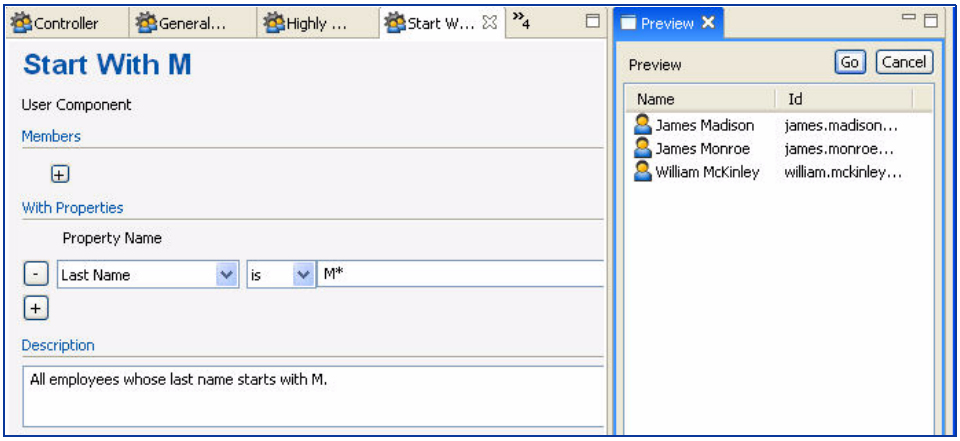


Figure 2-12: Policy Author: The Preview Pane

Deploying Policies

Deployment is the process of distributing new or revised components and policies to the appropriate desktop PCs and file servers throughout your organization, where enforcers are installed. After constructing a policy, the Policy Author user submits it for deployment. The person managing deployment can view a list of all policies and policy components awaiting deployment and make decisions about when to schedule each requested deployment. Deployment can be scheduled immediately, at a default interval, or at a particular future date and time.

In addition, you can either specify that a new policy or component be distributed to specific hosts, or allow Compliant Enterprise to intelligently determine where it needs to be deployed.

More comprehensive information on how Policy Author works and how to use it is provided in the *Policy Author 2.0 User's Guide*.

Administrator

Administrator is a Web application used by a system administrator or policy administrator for the following tasks:

- Monitoring the status of the system.
- Managing users, user groups, and roles.
- Setting up Compliant Enterprise user roles and assigning roles to users. Each role consists of a set of permissions, such as which Compliant Enterprise applications can be accessed (and which cannot), what types of Compliant Enterprise objects the role can work on (such as policies or specific types of policy components), and

whether others are allowed to view and modify the objects created by users in this role.

- Setting up enforcer profiles and assigning profiles to hosts. Each profile consists of a set of options that affect how enforcer software modules behave on that host.

You open Administrator in your Web browser, by entering the URL where the Intelligence server is installed. Typically, the URL is in the form *https://hostname/administrator*.

Figure 2-13 shows Administrator's main window.

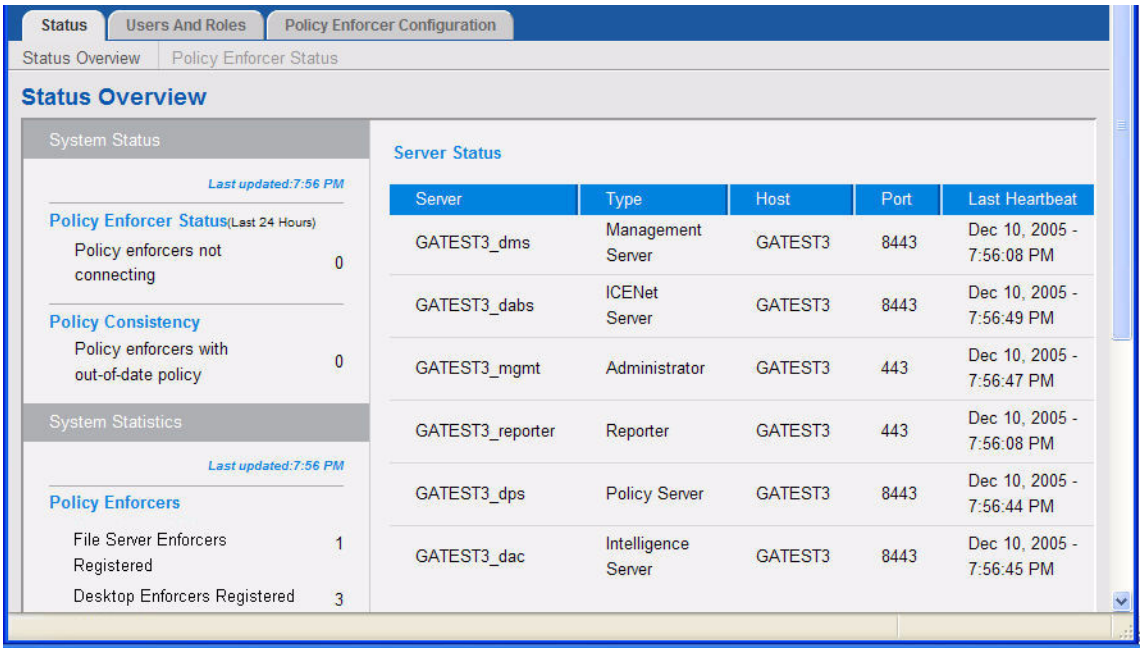


Figure 2-13: The Administrator Main Window

As the figure shows, Administrator's controls are organized onto three tabs.

- The **Status** tab displays cumulative information about policy enforcement, and the current status of the various distributed components of Compliant Enterprise.
- The **Users and Roles** tab is where you define and manage Users, User Groups, and Roles—the virtual entities representing the administrators who actually use Compliant Enterprise.

- The **Enforcer Configuration** tab is where you create and manage enforcer profiles, which are groups of configuration settings that you can share among many enforcers.

More comprehensive information on how Administrator works and how to use it is provided in the *System Administrator's Guide*.

Reporter

Reporter is a Web application used by compliance executives and others to create reports about policy-related events or other activities logged by Compliant Enterprise. A report is a set of filter criteria that express a question about the audit data recorded by Compliant Enterprise. When a Reporter user runs a particular report, the information to answer the question is retrieved from the Compliant Enterprise Activity Journal and presented in the Reporter user interface. For example, by creating filtered views of the data, it is possible to find out what enforcement actions have been taken in a given time period, for a given user, or for a given type of document.

Reporter is packaged as a J2EE Web Application and communicates with the Control Center and Intelligence Server via web services.

As with Administrator, you open Reporter in your Web browser by entering the URL where the Intelligence Server is installed. The URL is in the form *https://hostname/reporter*.

Figure 2-13 shows the interface where you can define reports in Reporter.

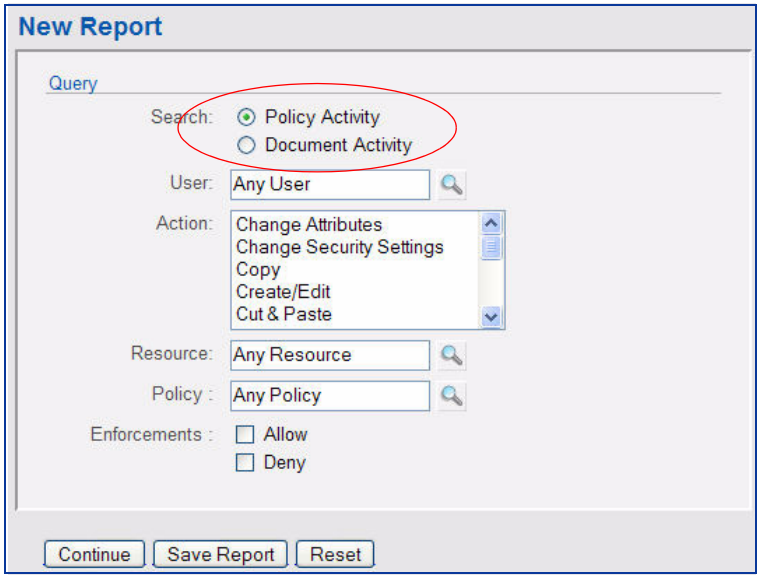


Figure 2-14: Defining a Report with Reporter

Reporter provides a powerful tool for forensics and incident response activities, such as the investigation of possible breaches of security or misuse of informa-

tion. As the figure shows, you can define reports to retrieve information on two types of activity:

- **Policy Activity**: Events in the system that are directly related to policies you have deployed—for example, how often a particular policy is used, how often a particular user has been the subject of policy enforcement, or how many policy enforcements have occurred in a given time period.
- **Document Activity**: All events in the system, regardless of whether they are covered by any policies. By default, Compliant Enterprise creates a record of these access and usage events, but you can configure the Activity Journal to customize the specific types of information you wish to record.

The Document Activity feature allows you to use Compliant Enterprise for purely auditing purposes, to analyze what is happening with your users and documents. This can be very helpful in designing appropriate policies. Once you then deploy the policies, you can run Policy Activity reports to analyze how effective the policies are.

More comprehensive information on how Reporter works and how to use it is provided in the *Reporter 2.0 User's Guide*.

3 Using Compliant Enterprise

This chapter gives an overview of the entire cycle of designing, implementing, and use a Compliant Enterprise system at your organization. It includes the following topics:

- Getting Started
- Implementing Compliant Enterprise (page 53)

Getting Started

If your organization already has defined a set of document use policies and knows where and how they need to be enforced, you can start using Policy Author to construct and deploy policies and policy components. More commonly, however, use and access policies are undefined or inadequately defined, and you will need to perform some system auditing to help formulate them. As we discussed in Chapter 1, Compliant Enterprise has powerful capabilities for monitoring information use and access throughout an organization, and generating reports that provide valuable tools in identifying your information control needs and how to define policies that can meet them.

This initial information audit is actually only one part of a properly designed Compliant Enterprise implementation. A thorough design phase should consist of several steps, as represented at right.

Figure 3-1: Design Phase

Designing your Implementation

As you prepare to implement your Compliant Enterprise system, you should proceed along the following sequence:

1. Identify your **requirements and objectives.** What are you trying to achieve, and what are the desired end results when your Compliant Enterprise system is up and running? This is the point where an initial information use audit can provide help.
2. Map your **objectives** to a **physical deployment**. What Compliant Enterprise software components, and how many, will you need to install, and on what machines?
3. Map your **objectives** to a set of **information policies**. What are the individual document control and compliance policies that, when combined, can achieve the desired results?
4. **Identify the components and policies** that will be required to translate your organization's information control policies into implementable units.
5. Create an **auditing and reporting strategy**. What types of logging and reports do you need?
6. Create a **testing strategy**. What type of hardware can you dedicate as a test system, and what tests will you run to be sure the policy components and policies are working?
7. Create a **change management strategy**. Who will have permission to modify policies once they are deployed? How will you manage the change process?

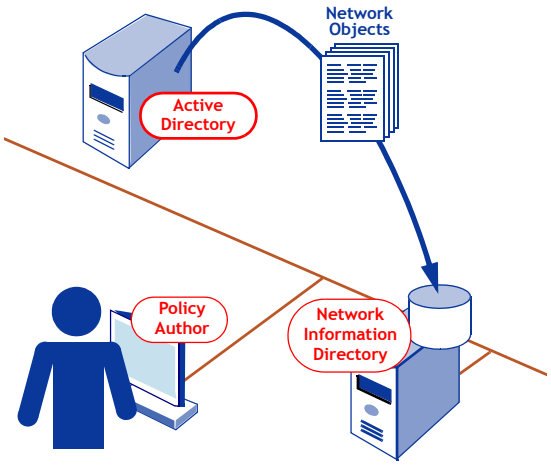
Implementing Compliant Enterprise

Compliant Enterprise allows you to control your organization's information by automating several aspects of the policy definition and execution process. Adopting and implementing Compliant Enterprise involves several steps.

1. Install Software

Obviously, you must start by installing the components of the suite. As we discussed in the previous chapter, this involves the Control Center components, one or more File Server Enforcers and Desktop Enforcers, and one or more Policy Author clients.

2. Enroll Network Information

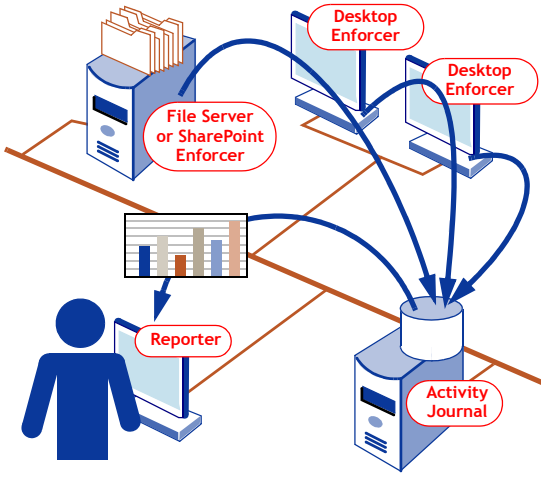


During the initial installation of the Compliant Enterprise Control Center, information about the organization's Information Network (users, desktop computers, applications, location sites, and SharePoint sites) is *enrolled*—that is, imported from an LDAP directory, such as Active Directory, or from input files—into Compliant Enterprise, creating an information resource model. As we have noted, this information is stored in the Network Information Directory database. Compliant Enterprise can enroll one or more network domains, in order to control resources across internal and external (for example, partner or contractor) networks. After the initial enrollment, information from a single domain may be automatically updated, allowing policies to adapt to changes in the information network.

To enroll network information, you use a special set of utilities provided with Compliant Enterprise. The enrollment process gathers information about the following entities within the enterprise:

- Desktop and laptop PCs, and host groups
- Enterprise users and user groups
- Applications available to organization personnel
- File shares, on both Windows and Linux systems
- SharePoint sites
- Location sites, which are physical or logical locations or connection types such as *Headquarters*, *Boston Office*, or *All PCs connecting via VPN*.

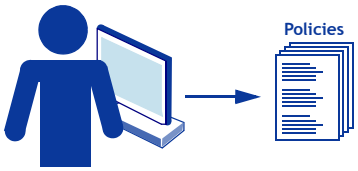
3. Run an Information Use Audit



Even if an organization has some idea about current risks to its information security, it will usually benefit from performing a thorough audit of the ways documents are being used throughout the organization.

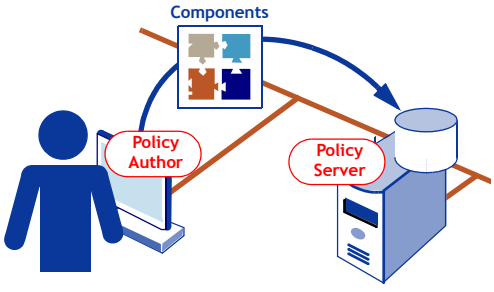
Without defining a single component or policy, you can use Compliant Enterprise to gather this information transparently and efficiently. You can record what documents all users are accessing, what they are doing with them, and when. By generating and analyzing sophisticated reports from this data, you can identify precisely where enforcement policies are required, and what they should be.

4. Design Policies



Someone familiar with business practices and processes, and with the structure of the organization, must define logical rules that Compliant Enterprise will have to enforce. These may be based on current company rules about using and distributing information, or they may be designed specifically for the Compliant Enterprise implementation, on the basis of an information use audit. They can be written in plain English, but they should be designed with an eye to the general way Policy Author works, and the capabilities and limitations of the Compliant Enterprise Policy Language (ACPL). For this reason, whoever conducts this design task should be familiar with the design chapters of the *Implementation Guide*.

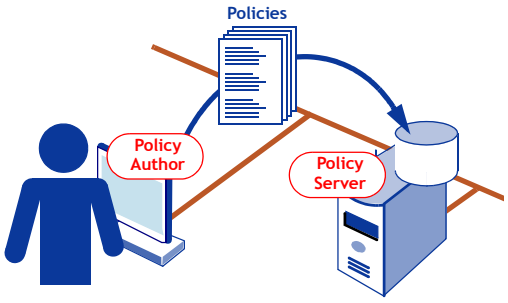
5. Define Policy Components



To provide the building blocks for constructing policies, you define a set of *policy components*. Each policy component is a model that represents a category or class of real entities, such as users, user actions, file servers, or information resources such as files or portal items. Modeling is performed by a policy analyst, using the Policy Author. As a rule, you need to use the logical policies designed in the previous step as a basis for identifying these components. The logical policies reveal the components required

to build them, but the actual building with the Policy Author tool requires the components as building blocks.

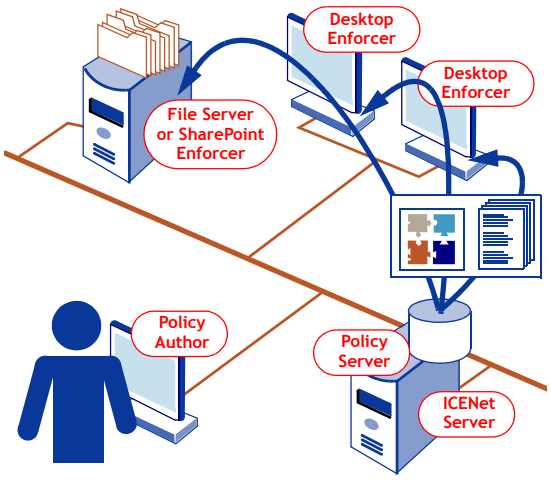
6. Construct Policies



Once you have defined components, you can use them to actually construct policies in Policy Author that represent the logical rules governing document access and use within your organization. Policy Author lets you write policies business terms, eliminating the need to translate corporate information policy to system-level rules. Each policy specifies which components (users, computers, actions, and documents) are involved and what the consequences are when the policy is enforced. All policies are stored centrally within a master repository, and are enforced by distributed Enforcers. They can be defined in one Compliant Enterprise implementation—a design and test environment, for example—and later exported to the production system in the form of XML files.

The person who constructs the policies at this point must be familiar not only with the logical policies defined earlier on, but also with the overall network topology, the policy components already defined, and the and the network objects that have been imported from your LDAP directory into the platform's Information Resource Model.

7. Deploy Components and Policies

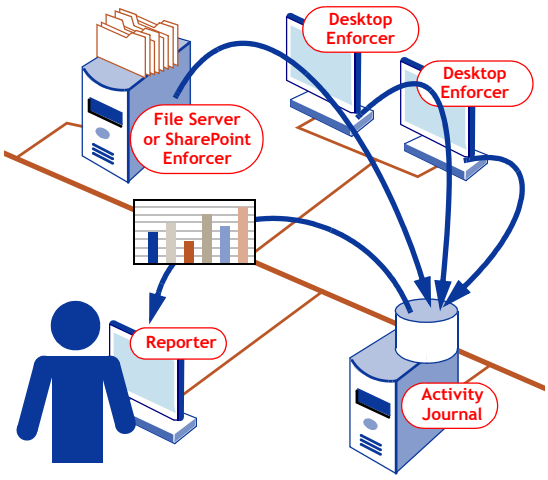


When you finish defining a component or policy and it is ready to use, you can then schedule it for *deployment*. Typically, a policy administrator manages deployment, because the administrator is responsible for changes to the production environment. Once scheduled, the deployment is handled automatically by Compliant Enterprise. You can deploy locally to a test machine first, as part of the testing phase. As policies or components change over time, the modeling and definition steps are repeated, and the modified policies and components are redeployed using the change management process that you planned for in the design phase earlier.

During deployment, business-level policy is automatically and intelligently translated into enforceable rules. As enforcers check in with the Control Center, updated policy packages are sent to each enforcer so that each enforcer has a complete copy of relevant policy for real-time, pervasive enforcement. The Policy Engine builds customized policy packages for each enforcer based on the information known about policy, policy components, and information resource model using Smart Deployment technology. Policies can be automatically delivered to those systems where they are relevant or specifically targeted to a specific set of enforcers. Deployment can occur based on a default IT schedule, or it can be scheduled for a specific date and time.

8. Enforcement and Audit

As organization personnel interact with documents, the policies that refer to those documents are enforced. For example, when a user attempts an operation that is not permitted by a given policy, the policy is automatically enforced by Compliant Enterprise, and the operation is denied.



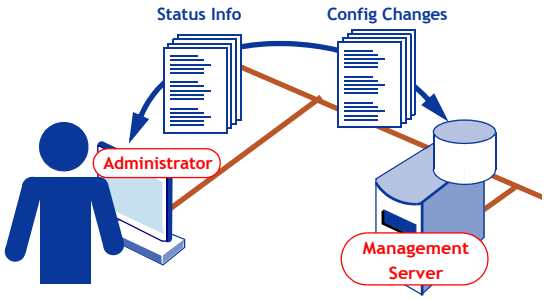
Depending on how a given policy was written, enforcement of the policy can result in various outcomes. For example, the user might be allowed to perform the action as usual, but the fact that they did so might be recorded in the Activity Journal and an e-mail might be sent to their manager.

As enforcement proceeds, audit logs of user activity and policy enforcement are captured by the individual enforcers, and this audit trail is periodically uploaded to the central Compliant Enterprise Activity Journal for analysis. The level of audit can be controlled centrally for each enforcer, making it easy to turn up or down the level of audit based on need.

9. Reporting and Forensics

Using the Reporter application, business analysts can view summary, trend, and detailed charts and reports on user activity and policy effectiveness. Compliant Enterprise records policy enforcement events and any normal user activity that is set up to be recorded in the Activity Journal. An organization's chief security officer or other executives and personnel can run reports to assess the effectiveness of the currently-deployed policies, and also to detect anomalies and possible threats. If policy effectiveness does not meet expectations, if problems are found, or if the needs of the organization change, you can add new policies or make changes to the definitions of your components and/or policies, and redeploy the new versions.

10. Ongoing System Monitoring and Maintenance



System administrators can use the Administrator application to monitor the status of hosts on which Compliant Enterprise components are running, manage Compliant Enterprise users, and configure the behavior of enforcer software by creating enforcer profiles. Enforcer profiles are groups of settings that determine how enforcers behave on host machines assigned to each profile. Enforcer profiles control logging, heartbeats, and which ICENet Server component the Enforcers communicate with.

A Glossary of Terms

This appendix provides definitions for some of the specialized terminology and concepts used throughout the Compliant Enterprise documentation set.

ACPL

The language Compliant Enterprise uses to internally represent, store, and manage policy components and policies.

Administrator

The web-based software tool provided with Compliant Enterprise, which you use to monitor and configure the system.

Auditor

A component of enforcer software. Logs end-user document activity and policy enforcements.

Control Center

The server architecture of Compliant Enterprise.

Desktop Enforcer

Enforcer software designed for use on Windows PCs.

Enrollment

The process by which an organization's existing information network of users, hosts, and other entities are imported into Compliant Enterprise.

File Server Enforcer

Enforcer software designed for use on Windows or Linux file servers.

ICENet

Protocol used to communicate between enforcers and the Compliant Enterprise Control Center.

ICENet Client

A component of the enforcer software architecture. Controls remote communication with the ICENet Server.

ICENet Server

Component of the Control Center. Manages communication between enforcers and the Control Center.

Information Network

An organization's information resource servers, desktops, network configuration, applications, and organizational structure.

Information Network Directory

Internal model Compliant Enterprise uses to represent the organization's information network. Stores data about entities including users, computers, applications, and documents.

Intelligence Server

A component of the Control Center. Contains the Activity Journal and provides user activity and policy enforcement data and analysis. See also Reporter.

Management Server

A component of the Control Center. Centralizes management of all system components.

Modeling

The process of defining policy components to represent real entities.

PDP

Policy decision point. A component of enforcer software. Evaluates policies and manages the local set of policies.

PEP

Policy enforcement point. A component of enforcer software.Intercepts user events and makes policy decisions.

Policy Administrator

Person who manages the deployment of policies.

Policy Analyst

Person who authors and edits policies.

Policy Author

Software tool provided by Compliant Enterprise. Used for modeling, policy construction, and component and policy deployment.

Policy Enforcement Point (PEP)

A component of enforcer software. A system-specific policy enforcement point that is responsible for detecting events and enforcing policy decisions.

Policy Enforcer

Software module installed on a Windows file server or PC to monitor user activity and take action if policies are triggered. See also *Desktop Enforcer*, *File Server Enforcer*, and *SharePoint Enforcer.*

Policy Engine

An ACPL execution engine found in the Policy Server and in the PDP within each enforcer. Creates policy maps and evaluates policies in real time.

Policy Maps

The optimized policy bundles that are deployed to each enforcer and allow real-time evaluation and enforcement even when disconnected from the network.

Policy Master

A database within the Control Center in which the Policy Server maintains central creation and deployment of policies.

Policy Server

A component of the Control Center. Responsible for policy management, including authoring, lifecycle, and deployment.

Reporter

A software tool provided by Compliant Enterprise. Reporter is a web application for creating reports and performing forensics. It obtains data from the Intelligence Server.

Index

Numerics

A

C

D

E

U

Index