



The Compliant Enterprise Active Control System

Release 2.0

System Administrator's Guide



May 2007

Copyright © 2007 NextLabs, Inc. All rights reserved.
The information in this document is subject to change without notice.

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

TRADEMARKS

Compliant Enterprise™, ACPL™ and the Compliant Enterprise logo are registered trademarks of NextLabs, Inc. All other brands or product names used herein are trademarks or registered trademarks of their respective owners.

LICENSE AGREEMENT

This documentation and the software described in this document are furnished under a license agreement or nondisclosure agreement. The documentation and software may be used or copied only in accordance with the terms of those agreements. No part of this manual may be reproduced, stored in a retrieval system or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's use, without the prior written permission of NextLabs, Inc.

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

Document Revision Number: SAG2.0-B05

Preface	9
What's New in the 2.0 Framework	9
Feature Dependencies Matrix	10
Product Documentation	11
Product Overview	11
Getting Started Guide	11
Implementation Guide	11
System Administrator's Guide	12
Policy Author User's Guide	12
Enforcer Administrator's Guide	12
CE Reporter User's Guide	12
Document Versions	13
Release Notes	13
Feedback	13
1. Enrolling Users, Hosts and Groups	15
About Enrollment	15
About the Information Network Directory	16
What To Enroll	16
Required Entities	16
Optional Entities	16
Windows and Linux	18
Enrollment Failures	18
The Enrollment Manager	19
Before You Enroll	19
LDAP Directory Requirements	19
Other Requirements	20
Using the Enrollment Manager	20
Auxiliary Input Files	22

Connection Files	22
Definition Files	24
Directory Definition Files	25
LDIF Definition File for Users, Hosts, and Groups	26
Filter Files	27
Filter Properties	28
Enrolling Users and Hosts	29
Enrolling from a Directory	29
Enrolling from Files	30
Maintaining Enrollments	32
Updating vs. Synchronizing	32
Updating Directory Enrollments	33
Updating LDIF File Enrollments	34
Synchronizing Enrollments	35
Manual Synchronization	35
Scheduled Synchronization	36
Other Management Functions	38
Checking Enrollments	38
Deleting Enrollments	39
2. Enrolling Other Entities	41
Enrolling Applications	41
The Definition File	42
Multiple Application Versions	43
Enrolling File Shares	44
About Resource Path Discovery	44
Enrolling Windows Shares	44
Linux File Servers	47
Microsoft Distributed File System	48
Enrolling Location Sites	49
Enrolling SharePoint Sites	51
Setting the Enrollment Utility Password	53
3. Completing Your Setup	55
Using Compliant Enterprise	55
Authorized Users	55
Location Sites	56
Enforcer Profiles	56
Default Profiles and Passwords	56
Components and Policies	56
4. Introducing Administrator	59
Using Administrator	59

Opening Administrator	59
Changing Passwords	60
Administrator's Tab Structure	60
The Status Tab	61
Status Overview	61
Policy Enforcer Status	63
The Users and Roles Tab	65
About Users	65
About Groups	65
About Roles	66
Managing Users	67
Adding a New User	67
Deleting a User	69
Managing User Groups	69
Creating a New Group	69
About Default Access Control Groups	70
Linking to an Existing Windows Group	72
Modifying a Group	73
Deleting a Group	73
Managing Roles	73
Assigning Roles to Users	75
The Enforcer Configuration Tab	76
About Profiles	76
Initial Registration	77
Profiles, ICENet Servers, and Hosts	77
Load-Balanced ICENet Servers	78
Working with Profiles	79
Defining a New Profile	79
Using Profiles for Auditing	81
Removing a Host from a Policy Enforcer Profile	81
Modifying a Policy Enforcer Profile	82
Deleting a Policy Enforcer Profile	83
Moving Profiles between ICENet Servers	83
5. Routine Management	85
Managing Control Center	85
Starting and Stopping	85
Exporting and Importing Policies	86
Exporting	86
Displaying a List	88
About Shallow Export	88
File Overwrite Default Behavior	88
Importing	89
Viewing the Contents of an Export File	90

Managing Policy Enforcers	91
Adding Additional Enforcers	91
Load Balancing	91
At Initial Installation	92
After Initial Installation	93
Stopping Policy Enforcers	93
Desktop Enforcers	93
File Server Enforcers	94
SharePoint Enforcers	95
Confirming Status	95
Restarting Policy Enforcers	95
Uninstalling Policy Enforcers	95
Reconfiguring Enforcers	96
Policy Enforcer Profiles	97
Managing Security Certificates	98
Database Administration	99
6. Configuration Tools	101
About Configuration Files	101
The Compliant Enterprise Config File	103
The Tomcat App Server Config File	103
Configuration Settings	104
Configuring the User Repository	104
Configuring Authentication	104
Choosing Local or Remote Authentication	104
Configuring the External Domain Authentication	105
Configuring Trusted Domains	106
Configuring Control Center Components	108
The From Address	109
Configuring Data Access	111
About Connection Pools	111
Adjusting Connection Pool Size	113
The Database Connection Bottleneck	114
Changing Database Connect Strings	114
Tomcat Settings	115
Location	115
Config File Structure	115
Encrypting Passwords for the Configuration File	118
Event Log Settings	119
Desktop Enforcer Logging	119
7. Defining Custom Properties	121
User, Host, and Group Properties	121
About Property Manager	122

Adding Properties	123
Deleting Properties	124
Listing Properties	124
Document Properties	125
Defining Custom Document Properties	126
Portal Content Properties	129
Defining Custom Portal Properties	129
8. Using Custom Obligations	133
About Custom Obligations	133
Writing Custom Obligations	134
Configuration	135
Application-Specific Arguments	136
Staging and Testing	137
Design Considerations	137
Sequential Behaviors	138
Appendix A: How Do I . . . ?	139
Appendix B: Passwords and Users	143
Initial Default	143
How to Change	144
Comments	144
References	145
Enforcer Profile Security Passwords	146
Initial Default	146
How to Change	146
Other Comments	146
References	147
Utility Security Password	148
Initial Default	148
How to Change	148
References	148
Active Directory Access Password	149
Initial Default	150
How to Change	150
References	151
Initial Default	151
How to Change	151
References	151
Appendix C: Glossary	153
Acronyms	153
Terms	154

Appendix D: Administrator’s Reference163

 Intra-System Communication163

 Web Services Communications165

 Web Application Communications165

 Native Data Server Protocols165

 Communication Ports166

Index169

Preface

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

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.

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	<ul style="list-style-type: none">• 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 seven titles: an introductory *Product Overview*; a *Getting Started Guide* with installation and configuration instructions; an *Implementation Guide* to help with strategies for auditing information use and designing policies; an administrator's guide for all enforcers and one for the system overall; and user's guides for Policy Author and Reporter.

Product Overview

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

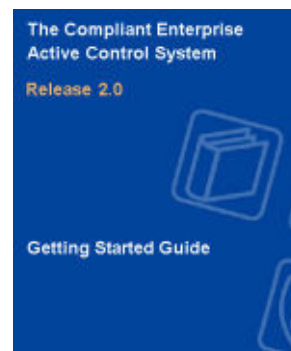


Getting Started Guide

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

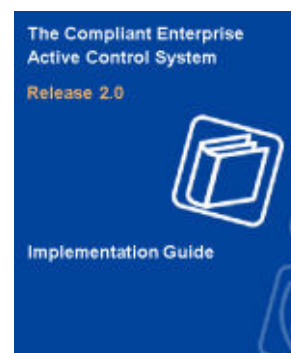
The installation procedures for all policy enforcers are provided separately, in the *Enforcer Administrator's Guide*.

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



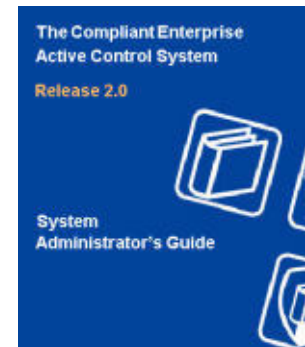
Implementation Guide

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



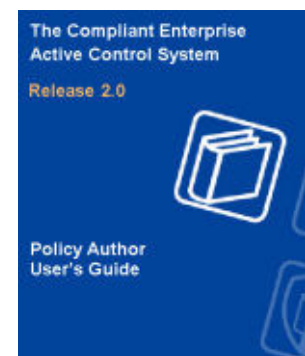
System Administrator's Guide

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.



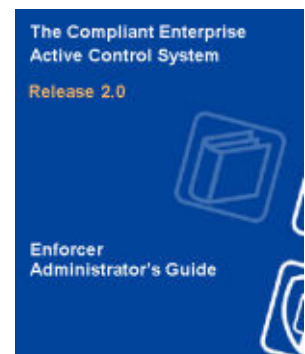
Policy Author User's Guide

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.



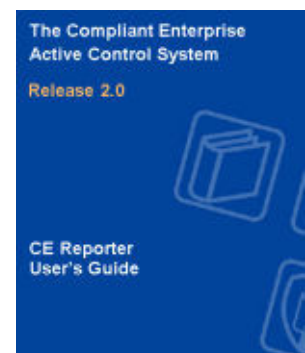
Enforcer Administrator's Guide

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.



Document 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

Enrolling Users, Hosts and Groups

Among the most important activities for Compliant Enterprise administrators is enrolling—that is, importing—various entities into the system’s internal database. This must be performed after the basic installation procedure that is covered in the *Getting Started Guide*, and it is a crucial step in setting up your Compliant Enterprise system initially. However, it is also an important part of ongoing administrative responsibilities, as you may need to enroll entities such as sites, applications or SharePoint sites at any time after your initial installation.

This chapter covers all aspects of enrolling users, user groups, hosts, and host groups from your LDAP directory. To do that, you must use a utility called Enrollment Manager. In addition, you can enroll applications, file shares, location sites, and collaboration portal sites. For those entities, you must use the other specialized utilities provided along with Compliant Enterprise; these will be covered in the following chapter.

This chapter is organized into the following sections:

- About Enrollment
- The Enrollment Manager ([page 19](#))
- Auxiliary Input Files ([page 22](#))
- Enrolling Users and Hosts ([page 29](#))
- Maintaining Enrollments ([page 32](#))
- Other Management Functions ([page 38](#))

About Enrollment

In Compliant Enterprise, *enrollment* refers to the process of importing information about your environment into the Compliant Enterprise system so it is available for use by Compliant Enterprise components. This includes both LDAP directory entities, and other kinds of information you enroll from text files. When you perform either kind of enrollment, information about the entities in your system is copied and stored in the Information Network Directory, one of Compliant Enterprise’s internal databases.

After enrollment is complete, the enrolled data is available for use in Policy Author. For example, you will have access to users so you can write policies that restrict the document usage permissions of certain users.

About the Information Network Directory

The Information Network Directory is the database schema where Compliant Enterprise stores its information about the entities in your organization, including users, computers, groups, applications, and so on. This data is organized according to a structured information resource model, which provides consistent definition and organization to make it possible to define policy components. The Information Network Directory is installed on the same database host as the Activity Journal, either in Postgres or Oracle.

You should perform your initial enrollments right after you install Compliant Enterprise. You can enroll entities from any number of domains, but each requires a separate operation. As your organization's infrastructure changes over time, you can manually update the information whenever you need to, and you can also configure the Enrollment Manager to automatically synchronize the information resource model at regular intervals.

What To Enroll

The Compliant Enterprise enrollment utilities import information about the underlying information network, including the entities listed below. Note that most are mandatory, and will have to be imported in all installations. Only location sites and portal sites are optional, meaning they may or may not need to be enrolled, depending on your requirements.

Required Entities

Users and User Groups: To be able to create user components in Policy Author, you must use the Enrollment Manager utility to enroll users and user groups. With the Enrollment Manager, you have the choice of enrolling entities directly from an LDAP server (such as Microsoft Active Directory) or from any correctly formatted LDIF (Lightweight Directory Interchange Format) file.

Hosts: To be able to create computer components, you must enroll hosts and host groups, also using Enrollment Manager. Like users and user groups, you can enroll them either from an LDAP server directory or from an LDIF file.

Applications: In order to be able to create Application Components, you must enroll any applications you will want to monitor. This topic will be covered in the following chapter.

File Shares: You must enroll file share information to facilitate mapping to specific resource paths. File shares are enrolled by querying the servers in your organization. To do this, you must manually run a utility called Resource Path Discovery. This topic also will be covered in the following chapter.

Optional Entities

Portal Sites: You will need to enroll portal sites only if you have installed one or more enforcers for SharePoint or other portal servers, and plan to design policies to monitor and control those sites. You enroll portal sites with the Enrollment Manager; details are provided in the following chapter.

Location Sites: Location sites are physical or logical locations (such as Headquarters, Boston Office, VPN), expressed as one or more ranges of IP addresses,

that you can enroll and use to define location-based computer components. Site information is gathered from a text file you create manually, specifying the computers included in each site. You enroll location sites with a utility called Import Locations; this topic will be covered in the following chapter.

Table 1-1 illustrates where you can locate all the utilities and template files required for enrolling various entities.

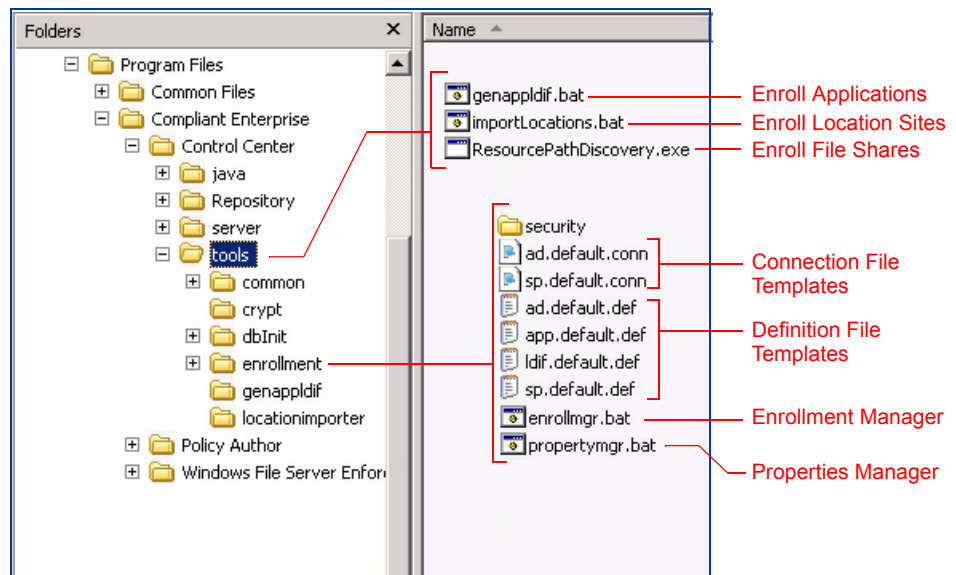


Figure 1-1: Locations of Enrollment Utilities

Table 1-1: Enrolling Compliant Enterprise Entities

Entity Type	Enrollment Method	Required?	Refer to:
Users & User Groups	Enrollment Manager utility (\tools\enrollment\enrollmgr.bat), Type = DIR or LDIF	YES	page 29
Hosts & Host Groups	Enrollment Manager utility (\tools\enrollment\enrollmgr.bat), Type = DIR or LDIF	YES	page 29
Applications	Application Discovery utility (\appdiscovery\ appdiscovery.cmd, on the installation CD) to generate an LDIF file; then Enrollment Manager utility (\tools\enrollment\enrollmgr.bat), Type = LDIF	YES	page 41 & page 29
File Shares	Windows: Resource Path Discovery utility (\tools\ResourcePathDiscovery.exe) Linux: Samba Directory mapping utility (/usr/local/ce/bin/smbDirMapping)	YES	page 44 & page 47
Location Sites	Manually create a plain-text Locations file, then Import Locations utility (\tools\importLocations.bat)	NO	page 49
Portal Sites	Enrollment Manager utility (\tools\enrollment\enrollmgr.bat), Type = PORTAL	NO	page 51

Windows and Linux

You enroll entities into your Compliant Enterprise system the same way regardless of whether you will be installing enforcers on Windows file servers, Linux file servers, or a mixture of both. That is, there is no such thing as “Windows enrollment” or a “Linux enrollment.” Rather, you just have to be sure your Samba server is configured so it can map the LDAP users in your Active Directory on the Windows side, to the users defined on the Linux side. This normally has to be done in any case, so the two systems can work together. As long as this is configured properly, Compliant Enterprise will manage all enrolled entities internally, and policies will be enforced properly on both Linux and Windows servers.

The one exception to this is discovering and enrolling file shares, which requires that you run separate utilities on the Windows and Linux environments. For details, see “About Resource Path Discovery” ([page 44](#)).

Enrollment Failures

Compliant Enterprise considers each instance of enrolling a specified set of LDAP data as a distinct metadata entity called an *enrollment*. Information about enrollments is saved internally, independent of the actual data that was imported, and you can refer later to enrollments as you manage the system.

It is possible that an enrollment may fail for various reasons—a connectivity problem, improper syntax in a connection file or definition file, a typo in the command line parameters, and so on. Even if an enrollment attempt fails, it is still recorded as an enrollment, and is present in the management data repository. In such cases, once you discover and correct the problem that caused the failure, you must use the *Delete* command to manually delete the failed enrollment before you re-attempt it. For details on deleting enrollments, see [page 39](#).

The Enrollment Manager

As we have seen, you can use the Enrollment Manager utility to enroll entities into the Network Information Directory, either directly from an LDAP directory or from an LDIF or a plain text file. These entities include users and user groups, hosts and host groups, applications, location sites, and portal sites. The Enrollment Manager can also be used for a number of enrollment management functions, described later in this chapter. It is not used in enrolling file shares; they have their own special utilities, for Windows and Linux.

Before You Enroll

Before you enroll LDAP data, you must run the Control Center installation wizard, and then start Control Center. Specifically, the Management Server component must be installed and running before you begin your enrollment.

LDAP Directory Requirements

Before you start, be sure any data to be enrolled from your LDAP directory meets the following requirements:

- All entries must have an *objectClass* attribute.
- All entries must belong to the corresponding object class, as shown below:

Entry	objectClass
User	person
Host	computer
Structural group	organization or organizationalUnit
Enumerated group	group

- All entries must have an *objectGUID* attribute, which holds the static identifier of that entry in the source directory.
- All user and host entries (also called “terminal” entries) must have an *objectSid* attribute. This attribute holds the system reference information for that entry—that is, the token or identifier that is used to identify the entity within the Windows system. This attribute is assigned to each user and host by the LDAP directory. If this attribute is not present, the entry will be ignored and a warning will be logged.
- User entries must have a *userPrincipalName* attribute that serves as a unique, user-friendly name for this entry within the directory.
- Host entries must have a *dnsHostName* attribute that serves as a unique, user-friendly name for this entry within the directory.
- If you will be combining a Linux file server with a Windows AD system, you must configure your Samba server so that all users and groups users map properly between the Windows and Linux.

Other Requirements

In addition, note the following points:

- If your directory data is large, we recommend that you create a filter file to selectively enroll only the user/host/group data that you require for policy enforcement. To do this, you need to know which data is required. For more on filter files, see [page 27](#).
- For best results, all entries in the directory tree should refer only to other entries in the same tree. For example, if a user group refers to users that are located outside the tree being enrolled, those user references will be ignored. Before you enroll data into Compliant Enterprise, take these considerations into account and select an appropriate root node. However, note too that enrolling from a root node that has too much information will make the pick lists in Policy Author so long that creating policy definitions becomes cumbersome.
- You will have to create one or more auxiliary input files before you are ready to enroll. Compliant Enterprise provides templates for these files; details are provided below ([page 22](#)).

Using the Enrollment Manager

The Enrollment Manager is automatically installed on the Control Center host, at

```
Program Files\Compliant Enterprise\Control Center\  
tools\enrollment
```

(If you divided your Control Center components among several hosts in a distributed installation, this refers to the server where the Management Server is installed.)

To use the Enrollment Manager, open a command line window, navigate to this location, and use the command *enrollMgr* plus the specific command and arguments for the function you want. All commands are described in [Table 1-2](#), below; descriptions of all command line arguments are provided in [Table 1-3](#). Note that *-f*, filter file name, is the only optional argument (as indicated by the square brackets); all others are required for their respective functions.

The *Enroll* and *Update* commands require a reference to a definition file and/or a connection file. Definition files provide information on how information elements in your source directory or file will map to the data structures inside Compliant Enterprise's data tables; for details, see [page 24](#). Connection files provide information necessary to connect to the LDAP directory data source; for details, see [page 22](#).

[Table 1-2](#) represents an overview of all available functions; more detailed information on enrolling each type of entity is provided in the following sections of this chapter.

Note that however they are represented throughout this manual, the commands themselves are *not* case-sensitive. Of the command argument values, only the User and Password are case-sensitive.

Table 1-2: CLI Commands, Enrollment Manager

Command	Purpose	Full Command String	Refer to:
enroll	Enroll entities from an LDAP directory server or a source file	enrollmgr enroll -t <type> -n <domain_name> -s <server> -p <port> -u <ceuser> -w <cepwd> -a <ad_connection_file> -d <definitionfile> [-f <filterfile>] Note that not all arguments are required for all enrollment types.	page 29
update	Update an existing enrollment from an LDAP directory or a source file	enrollmgr update -t <type> -n <name> -s <server> -p <port> -u <ceuser> -w <cepwd> -a <ad_connection_file> -d <definitionfile> [-f <filterfile>] Note that not all arguments are required for all enrollment types.	page 33
sync	Synchronize an enrollment	enrollmgr sync -n <domain_name> -s <server> -p <port> -u <ceuser> -w <cepwd>	page 35
delete	Delete an enrollment	enrollmgr delete -n <domain_name> -s <server> -p <port> -u <ceuser> -w <cepwd>	page 39
list	List enrollments	enrollmgr list -s <server> -p <port> -u <ceuser> -w <cepwd>	page 38

Table 1-3: Command Line Arguments, Enrollment Manager

Argument	Description
-t	Used with the enroll and update commands to specify the type of enrollment. Valid values are: <ul style="list-style-type: none"> • DIR: enrolling from an LDIF directory • PORTAL: the path and name of a collaboration portal site • LDIF: enrolling from an LDIF file • TEXT: enrolling from a plain text file
-n <domain_name>	The name of the enrollment. (Each enrollment needs a unique name, so you can identify it in various management functions, such as confirming, synchronizing, and updating.) This value must be the name of the domain from which you are enrolling. Accordingly, you cannot perform more than one enrollment from a single domain; rather, you can perform an enrollment, then later update it (using the same name) to incorporate any changes. Be careful with this when you type this value, since if the name does not exactly match the domain name as defined in your DNS, the enrollment will not fail, but Compliant Enterprise will be unable to deploy any policies to any of the enforcers in this domain. Note that in the case of applications, the enrollment name, -n, does not have to be the same as the domain name; you can use any unique string you like. This is an exception to the rule for all other kinds of enrollments.
-s <server>	The name or URL of the host where your Control Center is running.
-p <port>	The port of the Control Center host—8443, by default.
-u <ceuser>	User name of a Compliant Enterprise user with administrator privileges.
-w <cepwd>	The Compliant Enterprise utility password. (For details, see page 148 .)
-a <connection_file>	The name of the directory connection file. Required for enrolling or updating with an LDAP directory and for enrolling portal sites; see "Connection Files" (page 22).
-d <definitionfile>	The name of the definition file, which is required for all enrollments and updates. You use one of several provided template or default files depending on which kind of entity you are enrolling; for a detailed explanation, see "Definition Files" (page 24).
-f <filterfile>	The name of the LDAP filter file, if you are using one. Optional in all cases; see "Filter Files" (page 27).

Auxiliary Input Files

The command lines for enrolling and updating users, hosts and groups have three filename parameters, which refer to the following kinds of auxiliary input files:

- Connection Files
- Definition Files
- Filter Files

Connection Files

Connection files, as the name implies, contain the information Compliant Enterprise needs to locate and connect to some information source your system will need: either to the LDAP directory tree from which you want to enroll information, or to the SharePoint server you want to enroll. You must specify a directory connection file whenever you use the Enroll or Update commands and type = DIR, but it is not required when type = LDIF or TEXT.

This file also controls the automatic directory synchronization feature, which is available only for directory enrollments, not LDIF file enrollments. For details, see [page 36](#).

For an LDAP directory, you can use the sample file *ad.default.conn* as a template for your directory connection files. For SharePoint sites (described in the following chapter), you use the file *sp.default.conn*. During installation, these template files are placed in the tools\enrollments directory on the Control Center host. [Figure 1-2](#) shows the elements in the *ad.default.conn* file; note that your actual file will contain a number of commented lines explaining how to use the elements. You should make a copy of this template, rename it however you wish and, for all the elements indicated by rectangles in the figure, replace the dummy values with your actual values. You may also wish to change one or more of the optional settings, indicated by the ovals in the example.

For details on how the elements in this file function, see [Table 1-4](#).

```

server      moscow.widgetco.com
port        389
login       jimmy.carter@test.widgetco.com
password     rozzy.amy

roots       ou=fixed,dc=test,dc=widgetco,dc=com \n\
            ou=bulk3000,dc=test,dc=widgetco,dc=com \n\
            ou=mytest,dc=test,dc=widgetco,dc=com

filter      objectclass=*

IsPagingEnabled      true
EnableADDirChgReplications      false

ScheduledSyncTime     Sep 27, 2006 1:00 AM
ScheduledSyncInterval 360

```

Figure 1-2: Sample Directory Connection File (ad.default.conn)

Table 1-4: Elements of Directory Connection Files

Element	Description
server	Specifies the host name of the LDAP server to which you want to connect.
port	Specifies the port on this LDAP server, where you want to connect.
login	Specifies a user name with access privileges sufficient to connect to the LDAP server and access the information you want to enroll.
password	Specifies a valid password for this user, for connecting to the LDAP server. This parameter is optional. Because it is an unencrypted string, you may prefer not to expose it in the connection file this way. If the parameter is not present in the file, the user will be prompted for the connection at the time when he performs the enrollment. If the parameter is present, it will simply be read, with no such prompt. This latter may be preferable for the sake of convenience, during testing or in other restricted-use context when security is not a concern.
roots	Each line describes one branch in the LDAP directory tree you want to enroll. Although you technically can list any number of root elements in a single connection file, as long as they are separated by the escape string <code>\n\</code> at the end of each line. (There are three root elements listed in the example above). However, if you specify only one branch per enrollment, they are generally easier to keep track of and manage (update and synchronize, for example) in the future.
filter	You can define one or more LDAP filter strings in this file—for example, <code>objectclass=user</code> and <code>department=HR</code> . The default value, <code>objectclass=*</code> , means no filters will apply.
IsPagingEnabled	A flag that indicates whether LDAP paging control is supported by your LDAP server. Change this flag to false if your LDAP server does not support this function.

Table 1-4: Elements of Directory Connection Files (Continued)

Element	Description
EnableADDirChgReplications	A flag that controls Compliant Enterprise's synchronization autotracking feature. When left at the default, false, Compliant Enterprise will reenroll all entities from your Active Directory source during every synchronization. (This is specific to Active Directory.) When changed to true, the feature is enabled, and during synchronization Compliant Enterprise will enroll only new entities and those whose properties have changed since the last sync operation. This feature makes sync procedures more efficient and faster, but it requires special permissions.
ScheduledSyncTime	Allows you to set a specific time when the enrollment will be automatically synchronized with its source. After this date and time, the enrollment will autosynchronize at the interval specified by the ScheduledSyncInterval parameter. Note that you must use exactly the format specified in the template file. Specifically, <ul style="list-style-type: none"> Each date and time element must be space delimited The month must be expressed as the first three letters of the month name The year must be represented in four digits The hour must be represented in 12-hour notation, with AM or PM specified This value is only active if the Scheduled Sync Interval is set to some positive value. If you leave ScheduledSyncInterval at the default, 0, the synchronization feature is disabled.
ScheduledSyncInterval	When left at the default, 0, disables the automatic synchronization feature. When changed to any positive value, specifies a regular re-synchronization schedule, expressed in minutes following the time specified by the ScheduledSyncTime. This setting has no influence until after the ScheduledSyncTime passes. That is, in the example above Compliant Enterprise would wait until 1 a.m. on September 26 to synchronize the enrollment to its source, and then would re-sync it every 6 hours (360 minutes) thereafter. Manual synchronization is possible only if this value is set to zero. If you have changed it to enable automatic synchronization, you must change it back to zero to run a manual sync.

Definition Files

Definition files contain all information required to map the data you are enrolling from some information source to the format Compliant Enterprise uses in its Information Network Directory tables. Templates for these files are automatically copied to your Control Center host during installation.

Note that the format and content of these files will differ, depending on whether you are enrolling from an LDAP server, from an LDIF file containing users, hosts and groups; or from an LDIF file containing applications. For this reason, three specialized definition file templates are provided during installation; these are placed in the `\tools\enrollments` directory (see Figure 1-1 on page 17). They are:

- **ad.default.def**, for use with Active Directory or other LDAP directories
- **ldif.default.def**, for use with LDIF files for users, hosts, and groups
- **app.default.def**, for use with LDIF files for applications, generated with the AppDiscovery utility
- **site.default.def**, for use in enrolling host sites
- **sp.default.def**, for use in enrolling collaboration portal sites

To use these templates, copy them to a known location, make the changes specified in the procedures outlined below, and then point to them (by file name and path) in the `-d <definitionfile>` parameter in your *Enroll* or *Update* command lines.

Directory Definition Files

The figure below shows a sample Directory Definition file. The actual file, when you open it, will display additional comments and instructions for editing.

Ordinarily you will not need to change any elements in this file, *unless* you are changing the mappings. You might do this if you know that you have made changes to your Active Directory that diverge from the default schema, or if you are using some LDAP directory other than Active Directory, that has a different schema.

```
# This is the definition file for a default Active Directory enrollment. It assumes
# a default Active Directory schema.

enroll.users                true
enroll.computers            true
enroll.applications         false

#
# Required attributes
#

entry.attributeFor.staticid  objectGUID
computer.requirements       (objectClass=Computer)
user.requirements            (&(objectClass=User) (!(objectClass=Computer)))
group.requirements           (objectClass=Group)
group.attributeFor.enumeration member

#
# Attribute mappings
#

user.string.principalName    userPrincipalName
user.string.displayName      name
user.string.firstName        givenName
user.string.lastName         sn
user.string.title            title
user.string.company          company
user.string.department       department
user.string.accountName      SAMAccountName
user.string.countryName      co
user.string.icoCountryCode    c
user.string.email            mail
user.string.windowsSid        objectSid

computer.string.dnsName      dnsHostName
computer.string.machineName  dnsHostName
computer.string.os           dnsHostName
computer.cs-string.windowsSid objectSid

entry.attributeFor.parentid  parentGUID
entry.attributeFor.isdeleted isDeleted
```

Figure 1-3: Directory Definition File Template (ad.default.def)

LDIF Definition File for Users, Hosts, and Groups

The figure below shows the default LDIF definition file *ldif.default.def*, which you should use as the template for your definition file when you enrolling or updating users, hosts and groups from an LDIF file. (There is a different template for applications; see [page 43](#).) The actual file, when you open it, will display additional comments and instructions for editing.

Normally you will have to edit only the last element in this file, *ldif.filename*, which tells the enrollment utility which file you want to enroll. Note that you must provide the full path to your LDIF file, and you must use front-slash characters rather than backslashes for the path separators.

This file is based on the default Active Directory schema. If you know that the directory from which you exported the LDIF file is different from this default, you will need to edit other elements in this file accordingly.



```
# This is the definition file for an LDIF file enrollment.
# It assumes a default Active Directory schema.

enroll.users                true
enroll.computers            true

#
# Required attributes
#
computer.requirements      (objectClass=Computer)
user.requirements          (&(objectClass=User) (!(objectClass=Computer)))
group.requirements         (objectClass=Group)
group.attributeFor.enumeration member

#
# Attribute mappings for user type
#
user.string.principalName  userPrincipalName
user.string.displayName    name
user.string.firstName      givenName
user.string.lastName       sn
user.string.windowsSid     objectSid

#
# Attribute mappings for host type
#
computer.string.dnsName    dnsHostName
computer.cs-string.windowsSid objectSid

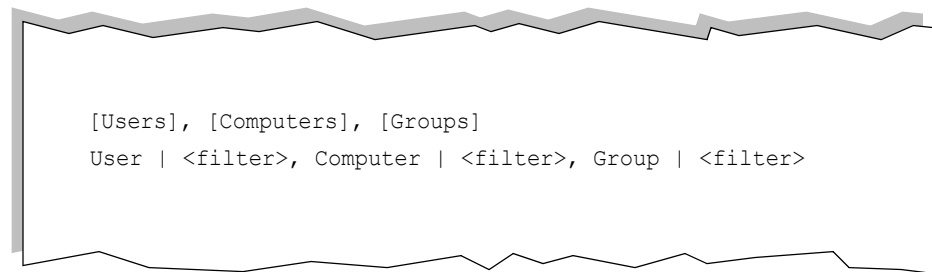
ldif.filename               e:/p4_ajones_1.0/personal/ldifoutput.ldif
```

Figure 1-4: LDIF Definition File Template (*ldif.default.def*)

Filter Files

A filter file allows you to selectively import leaf element—users, hosts, and groups—from a directory server. If the directory being enrolled contains a large amount of data, you can create a filter file to selectively enroll only those users, hosts, and groups that are relevant to your policy enforcement requirements. You can do this by creating a filter file in comma-separated value (CSV) format. It is easiest to set up the filters using a spreadsheet program like MS Excel and then save it as a .csv file, but you can also create the CSV file directly in any text editor.

Note: A new filter file can be defined only during the initial enrollment of a given domain. Once you enroll a domain using a filter file, you can use the same filter when you synchronize, but you cannot apply a different filter, or define a new one, when synchronizing an already enrolled domain.



```
[Users], [Computers], [Groups]
User | <filter>, Computer | <filter>, Group | <filter>
```

Figure 1-5: LDAP Filter File Format

The CSV file must use the format shown in the figure above, where <filter> is a search specification in LDAP format. When placed in the Users column, the filter is applied within the set of all users in the directory; if under Computers, within all computers; and so on. The filter can be based on any attributes of objects, such as job titles of users, e.g., (*title=Manager*). Here are some examples of filters you could put in the Users column:

- (lastName=M*) Everyone whose last name begins with the letter M
- (firstName=Jack)(firstName=Terry): Everyone whose first name is Jack OR Terry
- (!firstName=Amy) Everyone but Amy

As shown in the example above, the first row must contain the header cells, including square brackets:

```
[Users], [Computers], [Groups]
```

The remaining rows list the following information:

- Under the [Users] header, each cell is either the login name of a user to be enrolled, or a filter in LDAP format, specifying which users to enroll from the set of all users in the directory.
- Under the [Computers] header, each cell is either the name of a computer, or a filter in LDAP format, specifying which computers to enroll from the set of all computers in the directory.
- Under the [Groups] header, each cell is either the name of a group to be enrolled (for example, Hardware Upgrade Project), or a filter in LDAP format, specifying which groups to enroll from the set of all groups in the directory.

The same search filter syntax can be used in every column. The headers Users, Computers, and Groups are provided so that you can omit filter criteria based on the objectClass or objectCategory attributes, since the type of object is already known from the column header. For example, to enroll all managers in an organization, you could use the filter (title=Manager) in a cell in the [Users] column.

When the spreadsheet is complete, save it as a CSV file (with commas as the delimiters between cells).

For more information about the LDAP filter syntax, consult LDAP documentation or see the proposed standard from the Internet Engineering Task Force.

Filter Properties

When you use a filter, you may need to edit the content of a special file called *selectivefilter.properties*, which is stored under the \tools\enrollment directory. This file contains several settings that control filtering behavior.

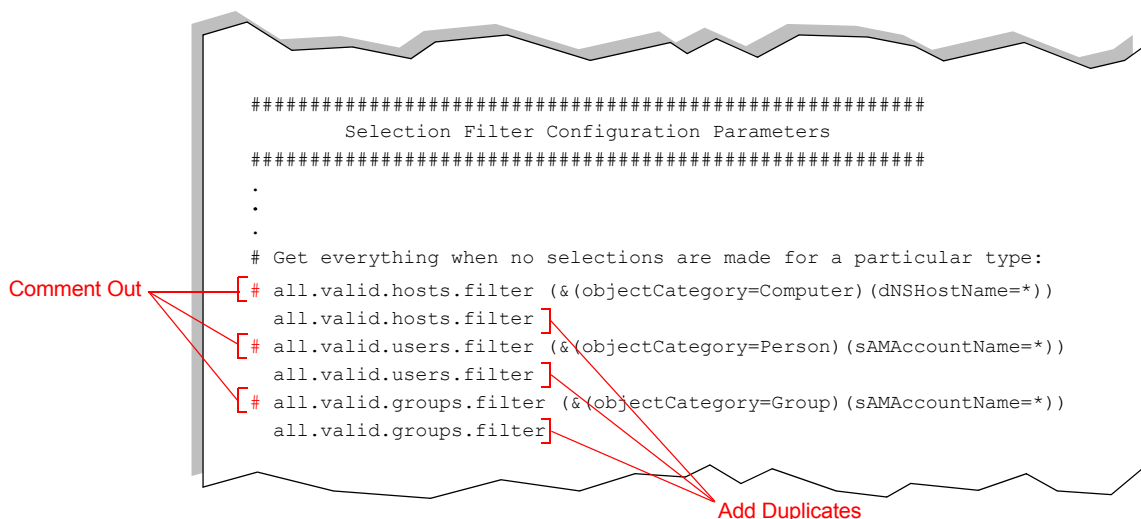


Figure 1-6: Selective Filter Properties File

By default, the filter sample file specifies three entities in the header: users, computers, and groups. If you are going to filter by all three, you do not need to change any filter properties. If you want to filter by only one or two—say, only by users, or only by users and groups—then you must make the following change to the Filter Properties file:

1. Open the file with any text editor.
2. Comment out *all three* lines in the last section of the file, as shown in [Figure 1-6](#), above.
3. For each line, copy the line and paste a duplicate below it, containing only the first element, but not the second (the actual LDAP filter, in parentheses), as shown in the figure.
4. Save your changes and close this file.

Once you have edited the filter properties in this way, you can proceed with your enrollment.

Enrolling Users and Hosts

You can use the Enrollment Manager utility to manually enroll users, user groups, hosts, and host groups directly from an LDAP server, as well as any information from an LDIF file. By default, the utility is installed in the <installDirectory>\ControlCenter\tools\enrollment folder. You should run it from that location.

Enrolling from a Directory

Before you can enroll user and host data directly from a live LDAP directory, you need to prepare both a definition file and a connection file, and specify them in the command line. In this case, you should use the `ad.default.def` file, located in the `\tools\enrollment` directory as your template. Make a copy of this file, and replace the default values there with your actual values (see [Figure 1-2](#) on page 23).

The process is as follows:

1. Make sure you have the information you will need to supply the required arguments to the enrollment utilities. This includes:
 - The domain name containing the objects to be enrolled. This is also used as a unique name assigned to this enrollment.
 - The host name of the Control Center server, and its port number (8443, by default). In many cases this is the same host where you are running command window, but you may be running the enrollment remotely.
 - The user name of an authorized Compliant Enterprise administrator.
 - The utility security password.
 - The name of the connection and definition files you have prepared for this enrollment. (See [page 22](#).)

- Optionally, the name of your filter file, if you are using one. (See [page 22.](#))

2. On the Control Center host, open a console window.
3. Change to the directory where the Enrollment Manager is installed—by default,

Program Files\Compliant Enterprise\Control Center\tools\enrollment

4. At the prompt, run the Enroll Manager using the following command, filling in the appropriate values for the arguments:

```
enrollmgr enroll -t DIR -n <domain_name> -s <server> -p <port> -u <ceuser>  
-w <cepwd> -a <ad_connection_file> -d <definitionfile> [-f <filterfile>]
```

When this utility runs, it reads the entries in your organization's LDAP directory, transforms them into the format Compliant Enterprise requires, and performs the enrollment. For descriptions of all command line arguments, see Table 1-3 on [page 21](#).

When this step is complete, a success message will display.

5. (Optional) If you want to review your progress so far, you can see a list of enrollments you've created by running the command:

```
enrollMgr list -s <server> -p <port> -u <ceuser> -w <cepwd>
```

For details on the *List* command, see [page 38](#).

6. If you are enrolling data from more than one domain, repeat step 4 for each domain, using the domain name of each for the -n argument.
7. After each enrollment, you must use the *Sync* command to synchronize the data in the enrollment. This is because the enrollment itself only imports metadata and sets up the required data structures in the Information Network Directory; the structures are populated only during synchronization procedure. For details on the *Sync* command, see [page 35](#).

Enrolling from Files

Before you can enroll user and host data directly from a file in standard LDIF format, you need to prepare a definition file, and specify it in the command line. In this case, you should use the *ldif.default.def* file, located in the `\tools\enrollment` directory as your template. Make a copy of this file, and edit the *ldif.filename* setting (the last line) to reflect the name of the LDIF file you are enrolling (see [Figure 1-4](#) on [page 26](#)).

You use the same procedure for enrolling applications as for users, groups and hosts. The only difference is that you use a different template for the definition file, called *app.default.def*.

To enroll data from LDIF files, perform the following steps.

1. Make sure you have the information you will need to supply the required arguments to the enrollment utilities. This includes:
 - The domain name, which is the unique name that will be assigned to this enrollment.
 - The host name of the Control Center server, and its port number (8443, by default). In many cases this is the same host where you are running command window, but you may be running the enrollment remotely.
 - The user name of an authorized Compliant Enterprise administrator.
 - The utility security password.
 - The name of the definition file you have prepared for this enrollment. (See [page 22](#).)
2. On the Control Center host, open a console window.
3. Change to the directory where the Enrollment Manager is installed—by default,

Program Files\Compliant Enterprise\Control Center\tools\enrollment

4. At the prompt, run the *Enroll* command as follows, filling in the appropriate values for the arguments:

```
enrollmgr enroll -t LDIF -n <domain_name> -s <server>
-p <port> -u <ceuser> -w <cepwd> -d <definitionfile>
```

When this utility runs, it reads the LDIF file specified in the definition file, transforms its contents into the format Compliant Enterprise requires, and performs the enrollment. For descriptions of all command line arguments, see Table 1-3 on [page 21](#).

When this step is complete, a success message will display.

5. (Optional) If you want to review your progress so far, you can see a list of enrollments you've created by running the command:

```
enrollmgr list -s <server> -p <port> -u <ceuser> -w <cepwd>
```

For details on the *List* command, see [page 38](#).

6. After each enrollment, you must use the *Sync* command to synchronize the data in the enrollment. This is because the enrollment itself only imports metadata and sets up the required data structures in

the Information Network Directory; the structures are populated only during synchronization procedure. For details on the *Sync* command, see [page 35](#).

Maintaining Enrollments

Once you have enrolled users, groups and hosts into your system, you will need to keep the information about them up to date. To help with this, Compliant Enterprise provides utilities for updating and synchronizing enrollments.

Updating vs. Synchronizing

Because the enrollment name is the same as the domain name, you can only perform one enrollment from each domain. If you later want to change the entities enrolled from a domain—for example, add new entity types or different roots—you must perform an *Update*. Note that this command changes only the data structure of the enrollment; it does not import the data itself. For this reason, you must run a *Sync* command after all updates.

If you only need to refresh the enrolled data without redefining the structure of the enrollment—that is, leaving the entity types and other metadata the same—you can use the *Sync* command. This is the reason why the *Update* command requires the definition file in the command line, while the *Sync* command does not.

The table below summarizes the various options available for updating and synchronizing your enrollments. Details on all procedures are provided in the following sections of this chapter.

Table 1-5: User, Host and Group Synchronization Options

	Update	Manual Sync	Scheduled Sync
LDAP Directory	YES: Run <i>enrollMgr update</i> with Type=DIR, and specify the enrollment name. Both definition and connection files are required. Also, you must run the Sync procedure after updating.	YES: Run <i>enrollMgr sync</i> , and specify enrollment name. No auxiliary files are required.	YES: Sync time and interval are based on the last two parameters in the definition file.
	Effect: The data structure for this enrollment is replaced in the Information Network Directory, with the metadata from the directory specified in the connection file, according to the syntax specified in the definition file. Update does not import the data itself; this is why you must run a Sync after updating.	Effect: Based on the enrollment name, Compliant Enterprise retrieves the connection and definition information from its internal tables, and synchronizes its Information Network Directory data to the data in the specified LDAP directory. No change can be made to the structure of the entities. Any changed information is updated, any entities that have been removed from the directory are removed from the IND, and any entities that have been added to the directory are added to the IND.	

Table 1-5: User, Host and Group Synchronization Options (Continued)

	Update	Manual Sync	Scheduled Sync
LDIF File	YES: Run <i>enrollMgr update</i> with type=LDIF and specify enrollment name. The definition file is required, and you must run a <i>Sync</i> command after the update.	YES: Run <i>enrollMgr sync</i> , and specify enrollment name. No auxiliary files are required.	NO: The scheduled sync depends on a connection file, which LDIF File enrollments do not use. Instead of syncing to a static file, which makes little sense, manually update the enrollment procedure using <i>enrollMgr update</i> , with type=DIR.
	Effect: The data structure for this enrollment is replaced in the Information Network Directory, by the metadata from the LDIF file specified in the definition file, according to the syntax specified in the definition file.	Effect: Based on the enrollment name, Compliant Enterprise retrieves the LDIF file name and path from its internal tables, and synchronizes its Information Network Directory data to the contents of the LDIF file. Any changed information is updated, any entities that are no longer present in the LDIF file are removed from the IND, and any that have been added to the file are added to the IND.	n/a

Updating Directory Enrollments

You should use the *Update* command whenever you want to enroll different types of entities or a changed data structure from a domain you have already enrolled. This requires a definition file, where the different entities are specified. Note that the update process imports new metadata from the source into CE; to import the data itself, you must perform a manual sync after the update.

To update user, group and host data from an LDAP directory, perform the following steps.

1. Make sure you have the information you will need to supply the required arguments to the enrollment utilities. This includes:
 - The unique name of the enrollment you are updating, which is the same as the domain name.
 - The host name of the Control Center server, and its port number (8443, by default). In many cases this is the same host where you are running command window, but you may be running the enrollment remotely.
 - The user name of an authorized Compliant Enterprise administrator.
 - The utility security password.
 - The name of the connection and definition files you have prepared for this enrollment. (See [page 22.](#))
 - Optionally, the name of the filter file, if you are using one. (See [page 22.](#))
2. On the Control Center host, open a console window.
3. Change to the directory where the Enrollment Manager is installed—by default,

```
Program Files\Compliant Enterprise\Control Center\tools\enrollment
```

4. At the prompt, run the *Update* command as follows, filling in the appropriate values for the arguments:

```
enrollmgr update -t DIR -n <domain_name> -s <server> -p <port> -u <ceuser>  
-w <cepwd> -a <ad_connection_file> -d <definitionfile> [-f <filterfile>]
```

When this utility runs, it reads the directory specified in the connection file, transforms its contents into the format Compliant Enterprise requires, and performs the enrollment. For descriptions of all command line arguments, see Table 1-3 on [page 21](#).

When this step is complete, a success message will display.

5. When the update is finished, you will have updated the data structure in CE, but no new data content has been imported. To do that, you have to run the *Sync* command as a separate operation. For details, see [page 35](#).

Updating LDIF File Enrollments

You can also use the *Update* command to update user and host information in the Compliant Enterprise Information Network Directory, based on the content of an LDIF file. Again, this command updates metadata only; the *Sync* command updates the data itself.

1. Make sure you have the information you will need to supply the required arguments to the enrollment utilities. This includes:
 - The unique name of the enrollment you are updating, which is the same as the domain name.
 - The host name of the Control Center server, and its port number (8443, by default). In many cases this is the same host where you are running the command window, but you may be running the enrollment remotely.)
 - The user name of an authorized Compliant Enterprise administrator.
 - The utility security password.
 - The name of the definition file you have prepared for this enrollment. (See [page 22](#).)
2. On the Control Center host, open a console window.
3. Change to the directory where the Enrollment Manager is installed—by default,

```
Program Files\Compliant Enterprise\Control Center\tools\enrollment
```

- At the prompt, run the *Enroll* command as follows, filling in the appropriate values for the arguments:

```
enrollmgr update -t LDIF -n <domain_name> -s <server> -p <port>
-u <ceuser> -w <cepwd> -d <definitionfile>
```

When this command runs, it reads the specified LDIF file, transforms its contents into the format Compliant Enterprise requires, and performs the enrollment. For descriptions of all command line arguments, see Table 1-3 on [page 21](#).

When this step is complete, a success message will display.

- When the update is finished, you will have updated the data structure in Compliant Enterprise, but no new data content has been imported. To do that, you have to run the *Sync* command as a separate operation. For details, see below.

Synchronizing Enrollments

The entities in network domains change frequently, and you need to ensure that any changes are updated into Compliant Enterprise. To do this, you can use the *Sync* command, which synchronizes one or more enrollments with their originating domains in the LDAP directory. By using this command, you can keep the Compliant Enterprise Information Network Directory up to date with changes in your organization. Bear in mind you can only synchronize the same data you have already enrolled; if you need to change the structure of the entities enrolled from a domain, you need to use the *Update* command.

You can synchronize enrollments either manually, at the current time, or automatically, at scheduled intervals. You can perform manual synchronizations for either directory- or file-based enrollments, but you can schedule automatic synchronizations only for directory-based ones.

Manual Synchronization

The *Sync* command reuses the parameters provided the last time the enroll command was called for the specified enrollments—including the references to the appropriate definition and connection files—based on the enrollment name parameter (-n). For LDAP enrollments, the connection file will provide the information for the LDAP directory you want to sync to; for LDIF files, the definition file contains the required file and path information.

If you need to change the parameters for any of the enrollments (for example, to change the security password), use the *enroll* command again with the desired enrollment name, using the new parameters.

To synchronize your user and host data from an LDAP directory, perform the following steps.

1. Make sure you have the information you will need to supply the required arguments to the enrollment utilities. This includes:
 - The unique name of the enrollment you are updating, which is the same as the domain name.
 - The host name of the Control Center server, and its port number (8443, by default). In many cases this is the same host where you are running command window, but you may be running the enrollment remotely.)
 - The user name of an authorized Compliant Enterprise administrator.
 - The utility security password.
2. On the Control Center host, open a console window.
3. Change to the directory where the Enrollment Manager is installed—by default,

```
Program Files\Compliant Enterprise\Control Center\tools\enrollment
```

4. At the prompt, run the *Sync* command as follows, filling in the appropriate values for the arguments:

```
enrollmgr sync -n <domain_name> -s <server> -p <port> -u <ceuser> -w <cepwd>
```

(For descriptions of all command line arguments, see Table 1-3 on [page 21](#).) When this utility runs, it reads either the LDAP directory or the LDIF file on which the specified enrollment is based (the connection and file information is stored in Compliant Enterprise's internal tables), and refreshes all relevant information in the Network Information Directory.

When this step is complete, a success message will display.

5. (Optional) If you want to review your progress so far, you can see a list of enrollments you've created by running the command:

```
enrollmgr list -s <server> -p <port> -u <ceuser> -w <cepwd>
```

For details on the *List* command, see [page 38](#).

Scheduled Synchronization

It is very simple to configure an enrollment to be automatically synchronized on a regular schedule. To do this, simply provide a value for the last two parameters in the connection file:

- **ScheduledSyncTime:** The date and time when the first autosynchronization will be performed;

- **ScheduledSyncInterval:** The interval, in minutes, at which the sync will occur, after the time specified in the previous parameter. A zero value here disables the autosync feature. (You must reset this to zero if you want to run a manual sync.)

For an example, see [Figure 1-2](#) on page 23.

Scheduled synchronizations should be done frequently, to ensure that your Compliant Enterprise policies are consistent with the actual network entities. As a rule, you should configure this to run at least every 24 hours (ScheduledSyncInterval = 1440).

Note, however, that this option is available only for enrollments from LDAP directories, not from LDIF files. For those, you can perform a manual synchronization, using the *enrollMgr syncLDIF* command.

Other Management Functions

The last two of the Enrollment Manager commands are provided not for enrolling entities per se, but to help with managing your enrollments in various ways, later on. These include:

- Checking Enrollments ([page 38](#))
- Deleting Enrollments ([page 39](#))

Checking Enrollments

You can use the Enrollment Manager's *List* command at any time to check which domains have been enrolled. This command generates a list of all current enrollments that were created with the *Enroll* command; each of these represents one domain. Note that the list does not include any domains that were enrolled but later dropped using the *Delete* command.

Note also that this command returns a list of *enrollments*, not of the network objects (users, PCs, servers, etc.) actually imported. To confirm these, you can open Policy Author and use the *Browse* command to view enrolled entities of each type.

To use the *List* command:

1. On the host where the Management Server component of the Compliant Enterprise Control Center is installed, open a console window.
2. Change to the directory `<InstallDir>\tools\enrollment`. By default, this is:

```
Program Files\Compliant Enterprise\Control Center\tools\
enrollment
```

3. At the prompt, run the *List* command as follows, filling in the appropriate values for the arguments:

```
enrollmgr list -s <server> -p <port> -u <ceuser> -w <cepwd>
```

This will return a list of all enrollments, with the following information:

- Name of the enrollment
- Source of the enrolled data
- A (filtered) tag indicates that the data was enrolled using an inclusive filter, as described on [page 27](#).
- A (pending) tag indicates that the enrollment will not occur until the next time `synchronize.bat` runs; that is, `enroll.bat` was called with the argument `-z TRUE`.

- Date when the enrollment was last updated

Deleting Enrollments

If you want to delete an enrollment from your Compliant Enterprise system for any reason, you can use the Enrollment Manager's *Delete* command. This command removes the enrollment entry from the Information Network Directory tables, so that no more updates or syncs can be performed on it. Thus if the enrollment was set up to be automatically synchronized, Delete cancels that feature.

Note: An important case where you would need to use the delete command, is any time an enrollment fails and you need to perform it again. In such cases, the failed enrollment must be manually deleted before any subsequent attempt can succeed.

You should run the *Delete* command from wherever the Enrollment Manager is installed—by default, <installDirectory>\ControlCenter\tools\enrollment. You should run it from that location.

To use the *Delete* command:

1. On the host where the Management Server component of the Compliant Enterprise Control Center is installed, open a console window.
2. Change to the directory <InstallDir>\tools\enrollment. By default, this is:

```
Program Files\Compliant Enterprise\Control Center\tools\
enrollment
```

3. At the prompt, run the *Delete* command as follows, filling in the appropriate values for the arguments:

```
enrollmgr delete -n <domain_name> -s <server> -p <port>
-u <ceuser> -w <cepwd>
```

Once the enrollment has been deleted, you will see a confirmation message. If you wish, you can use the *List* command to check the deletion.

Note that after you have deleted an enrollment, any policy components based on the objects in that enrollment will no longer work. For this reason, if you need to change the contents of an enrollment, it is preferable to use Enrollment Manager to update and then resync it, rather than deleting altogether.

Enrolling Other Entities

In the previous chapter we discussed the procedures for enrolling users, groups and hosts, and for managing these entities after enrolling them. In this chapter, we turn to the other three types of entities you can enroll: file shares, applications, and sites. The chapter is organized into the following sections:

- Enrolling Applications ([page 41](#))
- Enrolling File Shares ([page 44](#))
- Enrolling Location Sites ([page 49](#))
- Enrolling SharePoint Sites ([page 51](#))
- Setting the Enrollment Utility Password ([page 53](#))

Enrolling Applications

Applications, unlike users, cannot be automatically enrolled from your LDAP directory. In order to be able to define application-type components, you must manually enroll your applications into the Compliant Enterprise Information Network Directory. Once you have enrolled an application, it becomes available in the lookup list of applications displayed in Policy Author, and you can use it to define application components.

To enroll applications into your information network directory, you use a special utility called **App Discovery**. This utility provides a UI where you can select the applications you want to enroll, then generate an LDIF file containing all the required fields for the specified applications. You then enroll this file into your Compliant Enterprise Information Network Directory using Enrollment Manager's standard *Enroll LDIF* and *Sync* commands.

Normally you will perform this action on a PC or laptop where all the standard applications you want to monitor are installed. One convenient option is to use a standard PC image that system administrators use for setting up standard desktops in your organization.

To enroll applications:

1. Copy the AppDiscovery folder from the installation CD to any host location where you want to search for applications to enroll.
2. At the command prompt, run the following command:

```
<LocationCopiedTo>\appDiscovery>appdiscovery.cmd
```

This will launch the Application Discovery window, as shown in [Figure 2-1](#), displaying a Windows browser.

3. In this window, navigate to the Program Files directory (or wherever else application EXE files are installed), and check the box next to all the applications you want to enroll.
4. In the File menu, use the *GenerateLDIF* command to generate an output LDIF file.
5. Close the AppDiscovery window.
6. Copy your generated LDIF file onto the host where Control Center is running, in the same directory as the Enrollment Manager.
7. Use Enrollment Manager's *Enroll LDIF* and *Sync* commands to enroll the LDIF file. For a detailed explanation of how you use these commands, see "Enrolling from Files" ([page 30](#)). Note that for this process you will need to prepare a definition file, specifying the name of the LDIF file you are enrolling (see "The Definition File", below).

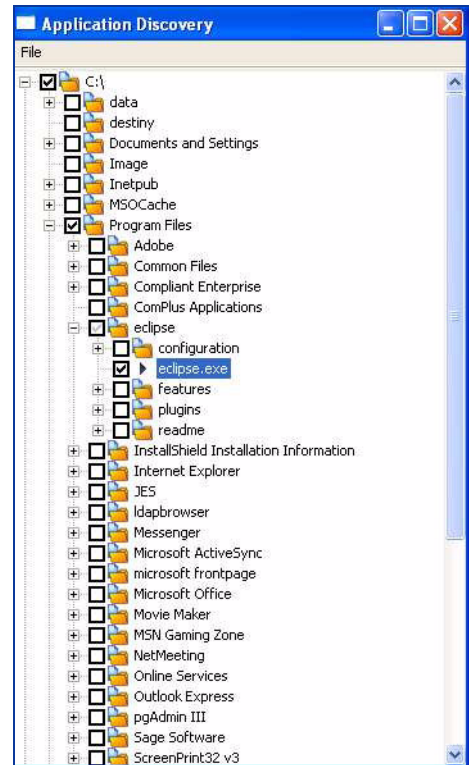


Figure 2-1: Enrolling Applications

The Enrollment Manager is installed on the Control Center host machine, in the Control Center\tools\enrollment\ directory. You can run it there, or copy it to some other location to run it; just be sure you copy your LDIF file to the same directory before you run the utility.

The Definition File

As we just mentioned, the *enrollLDIF* command requires a definition file. The figure below shows the default LDIF definition file *app.default.def*, which you should use as the template for your definition file when enrolling or updating applications from an LDIF file. It differs slightly from the one you use for users, hosts and groups. (The actual file, when you open it, will display additional comments and instructions for editing.)

In this file you will definitely need to edit only the *ldif.filename* element, since the syntax mapping will be consistent with the AppDiscovery utility's LDIF output. (For more details on definition files generally, see [page 24](#).)

```
# This is the definition file for an LDIF file enrollment.
# It assumes a default Active Directory schema.

enroll.users                false
enroll.computers            false
enroll.applications         true
#
# Required attributes
#
entry.attributeFor.staticid  uniqueGlobalIdentifier
app.requirements             (objectClass=Application)
user.requirements            (objectClass=User)
computer.requirements        (objectClass=Computer)
group.requirements           (objectClass=Group)
group.attributeFor.enumeration member
#
# Attribute mappings
#
application.string.uniqueName  fullyQualifiedNames
application.string.displayName cn
application.cs-string.appFingerPrint applicationFingerPrint
application.cs-string.systemreference sn
isRecurring                   false
ldif.filename                 e:/p4_ajones_1.0/personal/applications.ldif
```

Supply name and location of LDIF file here. Note front slashes!

Figure 2-2: LDIF Definition File Template for Applications (*app.default.def*)

Multiple Application Versions

It is important to understand that Compliant Enterprise considers different versions of an application as entirely independent of one another. If you have more than one version of an application running in your environment and you want to write policies against them, you must import each version separately, just as though they were different applications.

When you enroll an application, Compliant Enterprise automatically assigns a default name to it based on the executable file name. Since this name does not take account of application version, it will be the same regardless of the ver-

sion. This means that if you need to enroll more than one version of an application, you need to manually change the default name of the first one in the LDIF file, then perform your enrollLDIF, then generate an LDIF file for the other version of the application and enroll it. If you do not make this name change, the second application will overwrite the first, and you will not have both versions to work with.

Enrolling File Shares

By enrolling information about your organization's file shares, you can ensure that the use of differing file share paths to access the same document does not result in inconsistent policy enforcement. In a policy definition, a policy might identify a file by specifying a particular drive and path; however, in a real world organization, users might use various shared drive configurations to access that file. Compliant Enterprise needs to be aware of all the various file shares that are in use in your organization, so that it can consistently apply the correct policies to any given document, no matter which file share is used to access the document.

File shares typically are defined on file servers, but by definition they also include directories on any PC, that have been opened for sharing by other users. Note that if you are running policy enforcers on both Windows and Linux file servers, file shares have to be discovered on both platforms.

About Resource Path Discovery

The enrollment process involves discovering file shares defined on network hosts, and then enrolling them into the Information Network Directory. Because this requires active discovery on the live network, it requires separate procedures for Windows and Linux.

Enrolling Windows Shares

To enroll file shares, you use a utility called **Resource Path Discovery**. When you give this utility a list of servers in your network, it runs a discovery procedure and generates a complete list of file shares on those servers, showing the actual network and directory path for each share, with the duplicate shares (different shares that refer to the same actual directory) grouped together. This list is referred to as a *MachineList file*.

It is important to note that this procedure requires some special permissions, since it relies on visibility into multiple machines in the network. For details, see [page 47](#).

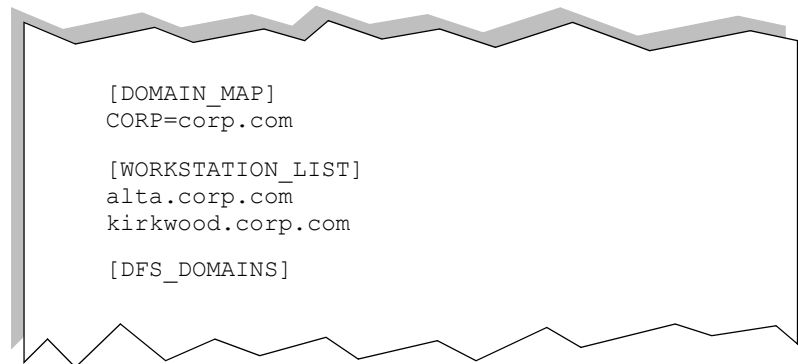
As new file shares are added to your system or existing ones are deleted, it is important to periodically run Resource Path Discovery to update your file share enrollment. This is why it's a good idea to set this up in a script that can run on a schedule—every week, for example.

By default, the Resource Path Discovery utility (ResourcePathDiscovery.exe) is installed in the <installDirectory>\ControlCenter\tools folder. You should run it from that location.

To enroll file shares for all file servers:

1. Create a text file containing a list of any hosts in your organization where you want to search for file shares. Again, this should definitely include all monitored file servers, but also any PCs where file shares may have been defined. This file, called the *MachineList file*, can contain three sections:
 - [DOMAIN_MAP] is an optional section which is used in the case where DFS shares span multiple domains (for example, //sand.mycompany.com/dfsroot/dfslink --> c:/share on machinec.child.mycompany.com). In this example, CHILD is the domain name and child.mycompany.com is how the domain is referenced in DNS.
 - [WORKSTATION_LIST] is the list of computers you want to search for file shares, and is the only required section. Each machine name must be on a separate line and specified by the full DNS name.
 - [DFS_DOMAINS] is an optional section which lists the domains that contain domain-based DFS shares (for example, //mycompany.com/dfsroot . . .).

Figure 2-3 shows a file that would be used to enroll two computers named Alta and Kirkwood, in a single domain. When creating your MachineList file, be sure to use the uppercase, square-bracket format for group headings, exactly as shown.



```
[DOMAIN_MAP]
CORP=corp.com

[WORKSTATION_LIST]
alta.corp.com
kirkwood.corp.com

[DFS_DOMAINS]
```

Figure 2-3: Sample Resource Path Discovery MachineList File

2. On any machine in your network that can connect to all the hosts listed in the file, log in as administrator of the domain that contains the listed servers. You must be logged in with one of the privileges required by Resource Path Discovery (see "Permission Requirements", below).
3. Change to the directory <InstallDir>\tools. For example:

```
cd Program Files\Compliant Enterprise\Control Center\tools
```

4. Run the Resource Path Discovery utility, using the following syntax:

```
ResourcePathDiscovery aliases.txt <MachineListFile>
```

where `aliases.txt` is the output file, and `<MachineListFile>` is the name of the text file you created in Step 1.

5. When Resource Path Discovery finish, open the output file and check its contents to be sure the utility completed the file correctly. The file should contain a section for each host listed in the MachineList file, with all of its file shares listed below it. The first line of each section should end with 0, indicating that no errors occurred during discovery. In the example in [Figure 2-4](#), there are two hosts, Alta and Kirkwood.



```
alta.corp.com 0
'\\alta.corp.com\nestedshare' 'C:\Public\nestedshare'
'\\alta.corp.com\Public\nestedshare' 'C:\Public\nestedshare'
'\\kirkwood.corp.com\DFSRoot\DFSLink\nestedshare' 'C:\Public\nestedshare'
'\\kirkwood.corp.com\DFSRoot\DFSLink' 'C:\Public'
'\\alta.corp.com\Public' 'C:\Public'

kirkwood.corp.com 0
'\\kirkwood.corp.com\SYSVOL\corp.com\SCRIPTS' 'C:\WINDOWS\SYSVOL\sysvol\corp.com\SCRIPTS'
'\\kirkwood.corp.com\NETLOGON' 'C:\WINDOWS\SYSVOL\sysvol\corp.com\SCRIPTS'
'\\kirkwood.corp.com\DFSRoot' 'C:\DFSRootShare'
'\\kirkwood.corp.com\SYSVOL' 'C:\WINDOWS\SYSVOL\sysvol'
```

Figure 2-4: Sample Resource Path Discovery Output File

6. When you are satisfied that the output file (`aliases.txt`) has been correctly generated, put it into production by copying it to the `aliased_shared` directory on the your Management Server host, like this:

```
<InstallationDirectory>\server\aliased_shares\aliases.txt
```

Note that you must restart Control Center at this point, so the Management Server rereads this file. This is the case whenever you make any subsequent changes to the `aliases.txt` file as well.

At this point, all Windows file shares have been discovered and enrolled, and will be handled properly by Compliant Enterprise policies for your Windows file servers.

Permission Requirements

As we mentioned, the Resource Path Discovery utility has special permission requirements in order to examine multiple hosts in the Windows network. For every host listed in the MachineList file, the administrator running Resource Path Discovery must be a member of *one* of the following:

- The local Power Users group;
- The local Print Operators group;
- The local Server Operators group (for domain controllers, the only type of host that has a Server Operators group);
- The local Administrators group;
- The Domain Administrators group;
- The Enterprise Administrators group.

Again, any of these six conditions would give the user sufficient permission to search a host for file shares. Such permission is required for all machines where the Resource Path Discovery utility is going to search for file shares—that is, all the hosts listed in the MachineList file.

Linux File Servers

If you have any Linux servers in your environment, there are a two remaining steps in the enrollment process, which you must perform after enrolling the Windows file shares:

7. From the Linux host, generate a second list of file shares, for the Linux server, using a utility called Samba Directory Mapping. To do this, type the following command on the Linux file server:

```
# /usr/local/ce/bin/smbDirMapping >~/aliases.txt
```

This creates an output file on the Linux host, also called aliases.txt. Note that this procedure, unlike the Windows discovery, does not require any MachineList file.

8. Next, append this new file to your Windows aliases.txt file, using the following commands from the Linux host:

```
# mkdir ~/mnt/aliased_shares  
  
# mount -t cifs //ICENet-server/aliased_shares  
~/aliased_shares -o user=valid_user_on_ICENet_server  
  
# cat ~/aliases.txt >> ~/aliased_shares/aliases.txt
```

```
# umount ~/aliased_shares
```

At this point, the file shares discovered on the Linux server have been added to the enrolled Windows file shares, and will be enforced properly by your policies. Note that if you run enforcers on more than one Linux server, you must repeat this procedure for each.

Microsoft Distributed File System

Microsoft Distributed File System, or dFS, aggregates Windows file share names into a single machine or domain name with links to various physical shares. In order to enforce policy on the various physical shares when it is access through a dFS share, Control Center must maintain a map of the share paths.

The list of share paths can be obtained by using the Resource Path Discovery utility, as described in the previous section. The following procedure is specific to using Resource Path Discovery with dFS shares.

Resource Path Discovery syntax:

```
ResourcePathDiscovery <outputfile name> <config file name>
```

The configuration file is a text file with the following sections:

```
[DOMAIN_MAP]
CORP=myco.corp.com
TEST=test.corp.com

[WORKSTATION_LIST]
lindsey.myco.corp.com
jasmine.myco.corp.com
natlie.test.corp.com

[DFS_DOMAINS]
corp.com
```

[DOMAIN_MAP] section lists the domains for a dFS share that spans multiple domains, e.g. \\myco.corp.com\dfsroot\dfslink is a dFS share in the CORP domain but it points to a physical share in another domain such as \\tahiti.test.corp.com\myshare in the TEST domain. The list maps the NetBIOS domain name to the DNS domain name, e.g. CORP=myco.corp.com.

[WORKSTATION_LIST] is the list of stand-alone dFS machine names. There are two types of dFS shares: domain-based and stand-alone with the following UNC formats.

- Domain-based: \\myco.corp.com\dfsroot\dfslink
- Stand-alone: \\jasmine.myco.corp.com\dfsroot\dfslink

This list contains only stand-alone dFS machines names, e.g. jasmine.myco.corp.com. If domain-based dFS is used, the following section is used instead.

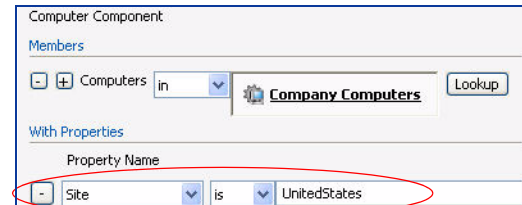
[DFS_DOMAINS] section lists the domains that use domain base dFS shares, e.g. \\myco.corp.com.com\dfsroot\dfslink.

The output file must be incorporated into the aliases.txt file as described above (see [page 46](#)).

Enrolling Location Sites

A *location site* is a Compliant Enterprise term referring to a group of hosts that you want to consider as a single location because they share certain characteristics. These may be physical, such as all computers at the Boston branch office, or virtual, such as all users connecting via a VPN. You define a site simply by creating a locations file that specifies one or more IP addresses or ranges of addresses and gives each a name, then enrolling the information from this file, using a utility called Import Locations.

Once defined and enrolled, sites are not themselves components, but rather are available as a property of computer components, allowing you to write policies that refer to a group of hosts based on their location.



To enroll sites, you use the Import Locations utility to extract site information from a locations file you provide and add it to the Compliant Enterprise Information Network Directory. Before you do this, you need to prepare the locations file.

By default, the Import Locations utility (importLocations.bat) is installed in the <installDirectory>\Control Center\tools folder. You should run it from that location.

To enroll a site, perform the following procedure:

1. Create your locations file. This is a text file containing any number of location definitions, one per line. Each line has the format

<LocationName> <AddressMask>

where <LocationName> is the name by which you want to refer to the site when referring to it in Compliant Enterprise tools such as Policy Author, and <AddressMask> is a CIDR-like mask for the 32-bit IP address of a machine that is in the given location. Note that the Location Name may not contain spaces.

For example, to define a location called VPN that represents a machine connecting through a virtual private network, you might create the following entry:

```
VPN 192.168.254.0/24
```

Create additional similar lines for all the other hosts that are part of the VPN group. Here is another example:

```
intranet 10.0.0.0/8
```

You can also put comments in the file by beginning each comment line with #. For example:

```
# The following lines define the machines in the  
# Boston office
```

2. Change to the directory *<InstallDir>\tools*. By default, this is:

```
Program Files\Compliant Enterprise\Control Center\tools\
```

3. Run the Import Locations utility with appropriate values for all parameters, as shown below. Note that this line must provide the name and path of the locations file, and connection information for your system database. The last parameter, *-instance*, is required only if database type is Oracle

```
importLocations.bat -locations <LocationsFile> -user <DB_user> -password <DB_password>  
-host <DB_host> -port <DB_port> -database <oracle|postgres> [-instance <instance>]
```

When the utility finishes running, all the locations defined in your input file will be present in the Information Network Directory, and you can use the sites you enrolled as values for the Site property when defining Computer components in Policy Author.

Enrolling SharePoint Sites

If you plan to deploy policies that will control access to content on SharePoint collaboration portals, you must enroll each individual site whose content you want to control. These are the same as the sites you define in SharePoint; you can enroll as many as you need. The procedure for doing this somewhat resembles that for enrolling users and groups, as described in the previous chapter: you use the Enrollment Manager to enroll the sites, based on a connection file and a definition file. For SharePoint sites, however, you need not make any changes to customize the definition file—only the connection file.

If you need to enroll more than one site in Compliant Enterprise, you must do them one at a time, whether they are running on the same logical portal or not.

To enroll one or more SharePoint sites,

1. Open the sample SharePoint connection file *sp.default.conn*, and edit the elements as shown in [Figure 2-5](#). Required elements are indicated by rectangles; optional ones, by ovals. (Descriptions of these elements are provided in [Table 2-1](#).) Save your changes when you have finished. You can rename this file or keep the default name; just be sure you specify the name properly with the *-a* flag in the Enroll command line (Step 4).

```
# This is a template connection file for enrolling SharePoint Sites.

domain          sharepoint2007
login           Administrator
*password       mYpAsSwOrD345

sites            http://sharepoint2007/sites/MySite \n\
                 http://sharepoint2007/MyOtherSite

ScheduledSyncTime      Sep 27, 2006 1:00 AM
ScheduledSyncInterv    360
```

Figure 2-5: Sample SharePoint Connection File (*site.default.conn*)

Table 2-1: Elements of SharePoint Connection Files

Element	Description
domain	Specifies the domain of the SharePoint server where the site you want to register is defined.

Table 2-1: Elements of SharePoint Connection Files (Continued)

Element	Description
login	Specifies a user name with access privileges to connect to the SharePoint server.
password	<p>Specifies a valid password for this user, for connecting to the portal server.</p> <p>This parameter is optional. Because it is an unencrypted string, you may prefer not to expose it in the connection file this way. If the parameter is not present in the file (i.e., if you leave it commented out), the user will be prompted for the connection at the time when he performs the enrollment. If the parameter is present, it will simply be read, with no such prompt. This latter may be preferable for the sake of convenience, during testing or in other restricted-use context when security is not a concern.</p> <p>If you want to define an unencrypted password here, be sure to remove the # character at the beginning of the line.</p>
portals	Each line here represents one site on the SharePoint site collection, which you want to enroll. It must contain the full URL delimited by backslash characters, as shown in the dummy values in the template file.
ScheduledSyncTime	<p>Optional parameter, allows you to set a specific time when the enrollment will be automatically synchronized with its source. After this date and time, the enrollment will autosynchronize at the interval specified by the ScheduledSyncInterval parameter. Note that you must use exactly the format specified in the template file. Specifically,</p> <ul style="list-style-type: none"> • Each date and time element must be space delimited • The month must be expressed as the first three letters of the month name • The year must be represented in four digits • The hour must be represented in 12-hour notation, with AM or PM specified <p>This value is only active if the Scheduled Sync Interval is set to some positive value. If you leave ScheduledSyncInterval at the default, 0, the synchronization feature is disabled.</p>
ScheduledSyncInterval	<p>Optional parameter. When left at the default, 0, disables the automatic synchronization feature. When changed to any positive value, specifies a regular re-synchronization schedule, expressed in minutes following the time specified by the ScheduledSyncTime.</p> <p>This setting has no influence until after the ScheduledSyncTime passes. That is, in the example above Compliant Enterprise would wait until 1 a.m. on September 26 to synchronize the enrollment to its source, and then would re-sync it every 6 hours (360 minutes) thereafter.</p> <p>Manual synchronization is possible only if this value is set to zero. If you have changed it to enable automatic synchronization, you must change it back to zero to run a manual sync.</p>

2. You ordinarily do not need to make any changes to the content of the definition file, `sp.default.def`, but you do need to place it somewhere where you can point to it in the Enroll command line (Step 4).
3. Change to the directory `<InstallDir>\tools`. By default, this is:

```
Program Files\Compliant Enterprise\Control Center\tools\enrollment
```

4. Run the Enroll Manager's Enroll command with the Type = PORTAL along with the other standard arguments, as follows:

```
enrollmgr.bat enroll -t PORTAL -s <Moskau> -p 8443 -u Administrator
-w mYpAsSwOrD345 -a sp.default.conn -d sp.default.def
```

Note that this line must specify the name and port of the SharePoint server, a user and password, and the names and paths of the connection

and definition files. For descriptions of all Enrollment Manager command line arguments, see Table 1-3 on [page 21](#).)

5. Run the Enroll Manager's Sync command, as follows. Note that neither connection nor definition file is required for this command:

```
enrollmgr.bat sync -s <host> -p 8443 -u <Admin> -w <securityPwd>
```

At this point the SharePoint sites will be available for use in defining components in Policy Author. You can use the Lookup button to display all portal content in a tree structure, so you can browse it directly as you define portal components.

Setting the Enrollment Utility Password

Some of the enrollment utilities require a password. The default is the password for the super user *Administrator* account, which is specified during installation of the Compliant Enterprise Control Center.

You can very easily change this password by logging in as the super user *Administrator*, then clicking on the Change Password link at the upper right of the main screen of both Administrator and Reporter. This will change the utility security password for all utilities and the password for the super user Administrator, but will not affect the passwords of any other authorized application users who may be defined in the system.

For complete information on all Compliant Enterprise passwords, refer to [Appendix B](#), "Passwords and Users".



Completing Your Setup

This chapter presents a concise summary of the sequence of tasks involved in starting to use Compliant Enterprise, assuming the system has been installed and all required entities have been enrolled, as described in the previous two chapters. Once this sequence is clear, we turn in the following chapter to a more detailed description of the controls and features in Administrator, which is where you will perform most of the administrative tasks outlined here.

Using Compliant Enterprise

Once the Compliant Enterprise system is installed and the mandatory enrollment has been performed is finished, you can start using the system by performing the following:

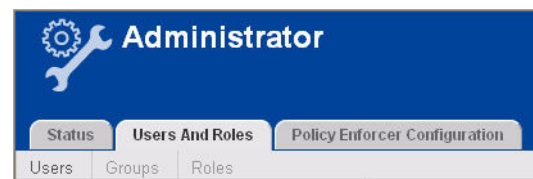
1. Define users, groups, and roles
2. Define location sites (optional)
3. Define enforcer profiles (optional)
4. Design, construct and deploy components and policies

Authorized Users

The first thing to do is open Administrator and define one or more users and, optionally, organize them into user groups. Users represent people in your enterprise who are authorized to open and use Administrator, Reporter, and Policy Author. The platform provides one default user, *Administrator*, but in practice various people will need to use these applications for different purposes, and you will need a more nuanced arrangement of user permissions.

Part of creating users and groups is defining generic *roles*, which are sets of permissions that can be granted to one or more users. Compliant Enterprise provides four roles with preset default permission levels, but you can customize these to best suit your needs. Roles are somewhat analogous to policy components, in that they can be independently customized and applied to users and groups, providing a level of abstraction between roles and users.

You define and manage users on the Users and Roles tab in Administrator. For details, refer to [page 65](#).



Location Sites

Location Sites—so called to distinguish them from SharePoint or other portal sites—are groups of computer resources you can manually define based on geographical proximity or any other characteristic you like. They can be very useful for defining policies that cover, for instance, branch offices or organizational units, or buildings on a campus. You may have already defined the sites you need when you performed your initial enrollment of all other entities (technically we refer to defining sites as *enrolling*); but they are not required, and can be defined at any time.

You create sites by specifying one or more ranges of IP addresses and using the enrollment utilities to enroll network information about them as single network entities. These entities are then available in Policy Author, as properties of computer components. For details, see [page 49](#).

Enforcer Profiles

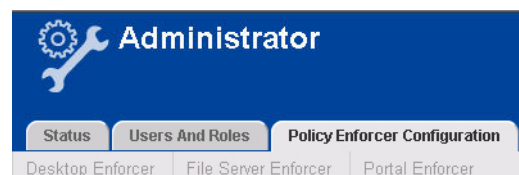
If your system has a relatively large number of Policy Enforcers, or if you anticipate adding more, you may benefit by defining multiple *enforcer profiles*. Profiles are simply named sets of property definitions that, once defined and saved, can be applied to any policy enforcer in the system. This simplifies configuration process, and allows you to ensure that several enforcers are definitely configured exactly the same way.

Default Profiles and Passwords

If you don't explicitly define any enforcer profiles, all enforcers in your system will be automatically assigned the settings of the default profile that is automatically created in Administrator. Although you do not technically need to change any settings, as a security precaution we recommend that you change the default password for this default profile. (It is "password"). This is the password you need to stop or uninstall any enforcer.

In addition, if you have more than one ICENet Server in your system, one of them will be assigned to each enforcer by default. It is strongly recommended that you examine the default profile, to confirm that the assigned ICENet Server is the one you want to use.

You define enforcer profiles on the Policy Enforcer Configuration tab in Administrator. For details, see [page 76](#).



Components and Policies

Once your enforcer profiles are defined, you can start defining components and using them to build policies, though in practice this will require some detailed policy design beforehand. It is possible that the design work based on your organization's business needs, and the mechanical effort of actually constructing and deploying the policies in Policy Author, will constitute two distinct efforts, involving different personnel.

Although components are used as building blocks for policies, in practice the two tend to be designed simultaneously. This is so because components aren't always obvious, based simply on an organization's assets; often the policies themselves are helpful in illuminating or revealing what components will be required to implement them.

Depending on your organization's needs, you may want to divide the policy definition effort into two phases:

- **Information Use Audit:** Define a set of audit policies that cover some definite set of documents, users, or assets. An audit policy does not stop any user from accessing or using a document; its purpose is to capture information about how, when, and by whom all covered documents are being used. This information can provide valuable analytical insights into what kind of document control policies you should implement.

(Defining and using audit policies is similar to running an information use audit without any policies at all; the difference is that it allows you to focus the audit as precisely and narrowly as you need to. If you do not need this kind of focus, a standard global audit is an easier approach.)

- **Information Use Control:** Once you have analyzed more precisely how documents are being used in your organization, you will better understand what kind of policies you need to control document use that may be harmful in one way or another. This second phase involves designing, deploying, and monitoring policies that do restrict people from using or accessing documents in specific ways.

For help designing audit strategies and policy sets, see the *Compliant Enterprise 2.0 Implementation Guide*. For complete details on using Policy Author to construct policies, refer to the *Policy Author 2.0 User's Guide*.

Introducing Administrator

In this chapter we introduce Administrator, the user interface available to system administrators for performing all kinds of configuration and routine administrative tasks. The chapter is organized into the following sections:

- Using Administrator ([page 59](#))
- The Status Tab ([page 61](#))
- The Users and Roles Tab ([page 65](#))
- The Enforcer Configuration Tab ([page 76](#))

For a quick reference to many of the features of Administrator, see Table A-3 on [page 140](#).

Using Administrator

Compliant Enterprise administrators will use the Administrator interface for various kinds of routine system management, including:

- Monitoring the operational status of control center processes, File Server Enforcers, Desktop Enforcers, and SharePoint Enforcers
- Monitoring statistical summaries of the policy enforcement activity of the system
- Monitoring the status of policies deployed to enforcers—that is, whether they are up-to-date, or have been revised but are awaiting deployment
- Defining and managing administrative users authorized to access the Compliant Enterprise tools
- Defining and assigning the configuration profiles that control several aspects of enforcer behavior

Opening Administrator

Because Administrator runs as a web application, it can be opened from any web browser that can connect to the server where the Administrator Server is running.

Note: If you are using Firefox as your Web browser, you cannot access Administrator unless you enable TLS 1.0 (under Tools, Options, Security). This is not required with Internet Explorer.

To open Administrator,

1. In your Web browser, enter the URL where Administrator is installed at your organization. Typically, the URL is in the form

`https://<hostname>/administrator`

The Login dialog appears.

2. Type your user name and password. If you have not yet been assigned a user name and password, see your system administrator.

You can also use the built-in super administrator, *Administrator*, along with the password set during Control Center installation. Typically, only a Compliant Enterprise system administrator would know this password and be able to use this account.

3. Click Login, and the Administrator main window will appear.

To exit Administrator, click the *Logout* link in the upper right of the screen. This will take you back to the Login screen. (You can also simply close your browser.)



Changing Passwords

The *Change Password* link at the upper right of the screen can be used to change the password of whatever user is logged in. Note that if you are logged in as the super user, Administrator, you can change the super user password. Bear in mind that this password is also used for system utilities such as Enrollment Manager and Property Manager.

Administrator's Tab Structure

When you open Administrator, you will see that the work space is organized into three tabs:

- Status
- Users and Roles
- Policy Enforcer Configuration

Let's examine the controls available on each tab, and describe how they are used in routine administrative tasks.

The Status Tab

The controls available on this tab are designed to help you monitor current system activity. It is organized into two screens, which you access by clicking the links at the top of the tab:



- **Status Overview:** Displays a diagnostic overview that informs you at a glance of potential problems, statistical totals for various types of activity throughout Compliant Enterprise, and the current status of each Control Center component. This screen displays in front by default.
- **Policy Enforcer Status:** Displays current status of each host where policy enforcer software is installed, and shows which policy enforcer profile is assigned to each host.

Status Overview

The Status Overview screen presents a high-level summary of the current status of the whole Compliant Enterprise system.

1. System Status

2. System Statistics

3. Server Status

System Status		Server Status				
Policy Enforcer Status (Last 24 Hours) Policy enforcers not connecting: 0		Server	Type	Host	Port	Last Heartbeat
Policy Consistency Policy enforcers with out-of-date policy: 0		GATEST3_dms	Management Server	GATEST3	8443	Dec 10, 2005 - 7:56:08 PM
System Statistics Last updated: 7:56 PM		GATEST3_dabs	ICENet Server	GATEST3	8443	Dec 10, 2005 - 7:56:49 PM
Policy Enforcers File Server Enforcers Registered: 1 Desktop Enforcers Registered: 3		GATEST3_mgmt	Administrator	GATEST3	443	Dec 10, 2005 - 7:56:47 PM
		GATEST3_reporter	Reporter	GATEST3	443	Dec 10, 2005 - 7:56:08 PM
		GATEST3_dps	Policy Server	GATEST3	8443	Dec 10, 2005 - 7:56:44 PM
		GATEST3_dac	Intelligence Server	GATEST3	8443	Dec 10, 2005 - 7:56:45 PM

Figure 4-1: The Status Overview Screen

As [Figure 4-1](#) shows, the screen is divided into three areas:

- **System Status:** The upper left pane, displays summary statistics indicating whether any issues require attention around policy enforcers or policy deployment. Any sudden, large drop in these totals can indicate that an unexpected event has occurred, such as policy enforcers going down or policy deployments not reaching their targets. For example, a 30% change in value over 24 hours would qualify as a sudden, large drop which would merit further investigation.
- **System Statistics:** The lower left pane, displays statistical totals, giving an overview of the amount of activity in the system.
- **Server Status:** The large pane at center right, displays the current status and configuration of each Control Center component.

[Table 4-1](#) provides a summary of all statistics displayed in all three areas on this tab.

Table 4-1: Status Overview Statistics

Statistic	Description
1. System Status: Small pane in the upper left of the main window	
Policy Enforcer Status	Tells how many of the installed policy enforcer modules have failed to communicate with the Compliant Enterprise Control Center within the past 24 hours. If the total is not 0, click the Policy Enforcer Status link at the top of the tab and identify the policy enforcers that have not connected. See "Policy Enforcer Status" (page 63). However, keep in mind that certain policy enforcers, such as those on laptop computers used by remote personnel or computers that are turned off when not in use, should not be expected to connect during every 24-hour period.
Policy Consistency	Tells how many policy enforcers have not received their most recent deployment of new or modified policies or policy components. For example, if one of the policy enforcers is on a laptop PC, and the user has not attached the laptop to the organization's network since the last policy deployment, that PC contains outdated policies.
2. System Statistics: Small pane in the lower left of the main window	
Policy Enforcers	Total number of policy enforcers installed on Windows file servers and PCs throughout the organization, and total heartbeats received by the Compliant Enterprise Control Center in the past 24 hours. Each policy enforcer is a software module that is responsible for detecting and responding to events that are covered by currently-deployed information control policies. Each heartbeat is a periodic communication received from a policy enforcer, indicating that the policy enforcer is running normally. When a heartbeat occurs, the policy enforcer receives any pending policy deployments or configuration updates. In a typical installation, the number of heartbeats received in each 24-hour period should be relatively consistent over time. Severe deviations from the expected value could indicate a system issue and should be investigated. To see status information for each policy enforcer, click the Policy Enforcer Status link at the top of the tab.
Policies	Total number of policies deployed within the organization. This total includes every policy that is deployed to any Windows file server or desktop PC in the organization.
Activity Journal	Tells how many messages have been stored in the logs that Compliant Enterprise maintains for reporting purposes: <ul style="list-style-type: none"> • Policy Activity: total number of entries that are automatically created whenever any policy denies a requested action, or whenever a policy is triggered that has a Log obligation defined. • Document Activity: total number of entries about various occurrences within the organization that are not related to policy enforcement. The precise set of activities to be logged depends on how the audit level of the Activity Journal is configured; see "Specifying Policy Enforcer Profile Settings" on page 29. • Total Activity: Sum of both items above. The log messages are counted and added to the Status tab's total when the logs are uploaded from the policy enforcers. Logs are uploaded periodically at a configurable time interval.

Table 4-1: Status Overview Statistics (Continued)

Statistic	Description
3. Server Statistics: Large pane on the right side of the main window	
Server	Name of the Control Center server component, including the host and domain where it is installed.=.
Type	The type of this Control Center component: Policy Server, Management Server, Administrator, Reporter, Intelligence Server, Information Network Directory, or ICENet Server.
Host	Machine where the software component is running. This is useful in that there may be more than one instance of a given server component, distributed on more than one host.
Port	Web services communication port where this component is listening for communication requests.
Last Heartbeat	Time stamp of the last heartbeat sent by the Control Center component. All these components send heartbeat signals to Administrator to indicate that they are running normally. In contrast to policy enforcer heartbeats, component heartbeats do not imply any download of policies or configuration changes; they serve merely as a notification that the software component is present.
Expected Heartbeat	Time the last heartbeat should have been sent by the Control Center, given current configuration settings. To check whether a component is up and running, compare this value to Last Heartbeat.

Policy Enforcer Status

When you click the Policy Enforcer Status link at the top of the Status tab (A), a screen displays status information for each file server and desktop PC where a policy enforcer is running.

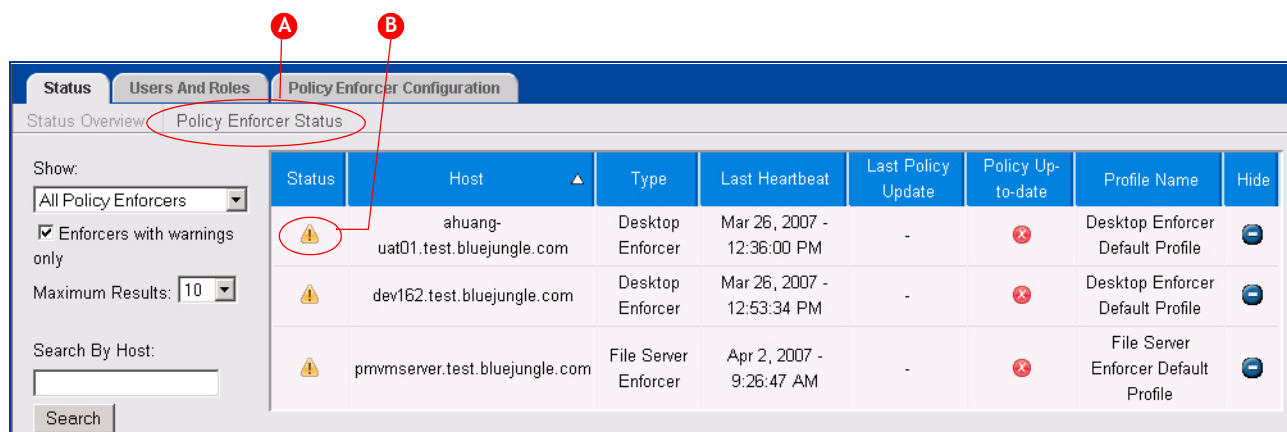


Figure 4-2: The Policy Enforcer Status Screen

To monitor policy enforcers,

1. Check the Status Summary indicator (B) in the Status column:
 - **Green Light:** All policy enforcers are operating normally.
 - **Warning** (exclamation point icon): One or more of the policy enforcers listed has not sent a heartbeat in the past 24 hours. Note that this may not necessarily indicate a problem, since certain policy enforcers, such as those on laptop computers used by remote personnel or computers that are turned off when not in use, may not connect as often as every 24 hours.

2. Optionally, you can select a filter in the Show combo-box, to narrow down the rows displayed. Available filters include:



- All Policy Enforcers
- All Desktop Enforcers
- All File Server Enforcers
- Policy Enforcers with Warnings
- Desktop Enforcers with Warnings
- File Server Enforcers with Warnings

For example, if the Status Summary shows a Warning icon, and you want to find out which policy enforcer(s) are triggering the warning, you could choose the Policy Enforcers With Warnings filter.

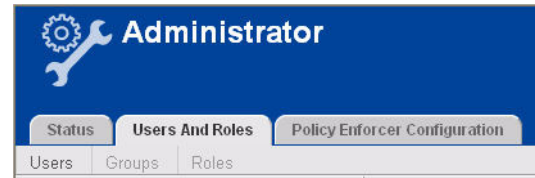
3. Read the detailed information about each policy enforcer in the list. [Table 4-2](#) summarizes all information given for each policy enforcer:

Table 4-2: Information on Policy Enforcer Status

Column	Description
Status	Indicates the current status of this enforcer, which may be either of the following: Green light = Clear: the policy enforcer is sending normal heartbeats. Exclamation point = Warning: the policy enforcer has not sent a heartbeat in the last 24 hours.
Host	Name of the machine where the policy enforcer is installed.
Type	Indicates the enforcer type: File Server Enforcer or Desktop Enforcer.
Last Heartbeat	Time stamp of the last heartbeat generated by this enforcer. If the enforcer is running normally, this time should correspond to the configured heartbeat interval. However, keep in mind that this does not necessarily indicate a problem, since certain policy enforcers—in particular, those on laptop computers used by remote personnel or computers that are turned off when not in use—might not be able to send a heartbeat for an extended period of time even though they are operating normally.
Last Policy Update	Tells when a new or modified policy or component was last deployed to this enforcer.
Policy Up to Date	A check mark appears if the enforcer has received the latest version of the policies that are targeted for deployment to it.
Profile Name	Tells which enforcer profile is assigned to this host. This profile determines behavior such as logging and heartbeat frequency. For more information about enforcer profiles, see page 76 .
Hide	Click to remove this host from the display. This is useful when the enforcer software has been uninstalled, and you therefore no longer need to monitor that host. If a enforcer is ever reinstalled on this host, the host will reappear on the list. If you click Hide by mistake on a host with an active policy enforcer, it will reappear automatically the next time the enforcer sends a heartbeat.

The Users and Roles Tab

The controls available on this tab allow you define and manage *users*, *user groups*, and *roles* for the Compliant Enterprise UI tools—Policy Author, Administrator, and Reporter.



Before we proceed, let's explain the meaning of each of these terms.

Note: The term *users* in this context is distinct from the two default user accounts that are available as soon as you initially install Compliant Enterprise: one for logging in to the platform's software tools, and one for logging in to the Information Network Directory's underlying data server. These accounts are not managed with the Administrator tool, and therefore are not covered in this section.

About Users

Within the Administrator tool, the term *user* refers to people who need to use the Compliant Enterprise tools—Policy Author, Administrator, and Reporter. For example, users include policy designers, Compliant Enterprise administrators, and executives or auditors running reports. Each user has a login name and password, which is used to verify the identity of the person attempting to use a Compliant Enterprise tool.

These users can be defined in or imported into Compliant Enterprise, which stores them in the Information Network Directory. The stored user information can come from the following sources:

- **Imported** into Compliant Enterprise from an organization's Active Directory. You can use this technique to grant existing Windows users access to Compliant Enterprise applications.
- **Manually added** as a New User, through Administrator's Users and Roles tab.

Both types of user can be set up as Compliant Enterprise users through the Users and Roles tab in Administrator.

For information about how users are authenticated, and how to authenticate them locally (within Compliant Enterprise) or using a live connection to the organization's information network, see "Configuring Authentication" on [page 104](#).

About Groups

A *group* is a set of users who have similar responsibilities and require similar rights to Compliant Enterprise objects (folders, policy components, policies, and reports). Rather than setting these rights for each user individually, you can set rights for the group and then assign users to the appropriate group and reassign them at will.

If you create a new group (using the New button), it is created strictly within Compliant Enterprise and does not have any relation to the LDAP groups you may have imported from Active Directory. If you prefer to create a group whose membership is based on an LDAP group, use the Add Windows Group feature. For example, if you already have a group called System Administrators, you can leverage this group as a source of Compliant Enterprise users. The benefit of linking Compliant Enterprise groups to existing Windows groups is that if the group membership changes in Windows, Compliant Enterprise automatically picks up the change. You can continue to manage the group on the Windows side.

About Roles

In Compliant Enterprise, a *role* refers to a set of permissions that determine which tasks individual users assigned to that role can do with Compliant Enterprise. Permissions within each role include which Compliant Enterprise applications can be used and what permission is granted for editing policies and components in Policy Author.

Compliant Enterprise provides four pre-defined roles: System Administrator, Policy Administrator, Policy Analyst, and Business Analyst. The roles would typically be used as follows:

- **System Administrator:** System administrators or other IT professionals who need to use Administrator to monitor the Compliant Enterprise system and manage users and policy enforcer profiles. These users may also need to use Policy Author and Reporter, and have full editing privileges.
- **Policy Administrator:** These users have responsibility for managing the lifecycle of policies and policy components, including deployment, so they would need access to Policy Author, with full editing privileges. These users might also want access to Reporter.
- **Policy Analyst:** Users with access to Policy Author in order to construct policies and submit them for deployment. These same people might also want to use Reporter to see how their policies are working out in practice.
- **Business Analyst:** Managers, executives, or other security personnel who will monitor and analyze how Compliant Enterprise functions within the organization. These people would need to use only Reporter.

These typical responsibilities are reflected by the default permissions assigned to the four roles when Compliant Enterprise is first installed. [Table 4-3](#) summarizes these roles.

Table 4-3: Roles: Default Permissions

Role	Can Use Reporter	Can Use Administrator	Can Use Policy Author	Policy Author Editing Privileges
System Administrator	Yes	Yes	Yes	All policies, All component types
Policy Administrator	Yes	No	Yes	All policies, All component types
Policy Analyst	Yes	No	Yes	All policies, No component types
Business Analyst	Yes	No	No	none

You can leave these default settings as they are, or you can modify them to suit your needs. However, you cannot delete roles or create additional ones.

Managing Users

Managing users involves two basic procedures: adding and defining new users, and deleting existing ones.

Adding a New User

You can use Administrator to create new Compliant Enterprise user accounts for users from two sources:

- Users enrolled from your organization's Active Directory and authenticated using integrated Windows authentication.
- New users added manually to Compliant Enterprise. These accounts are in addition to those imported from your organization's Active Directory and are kept in a separate, local domain. This is useful when, for example, you want to provide a unique login name and password that can be used to log in to Policy Author (or another Compliant Enterprise tool). Such accounts are always authenticated locally, even if Compliant Enterprise as a whole has been configured for remote authentication (see "Configuring Authentication" on [page 104](#)).

To set up a new Compliant Enterprise user account:

1. On the Users and Roles tab, click the Users link.
2. Click one of the following buttons:
 - **New** to create a new user within Compliant Enterprise.
 - **Add Windows User** to set up an account for a user enrolled from your Active Directory.

A user editing area appears in the right pane.

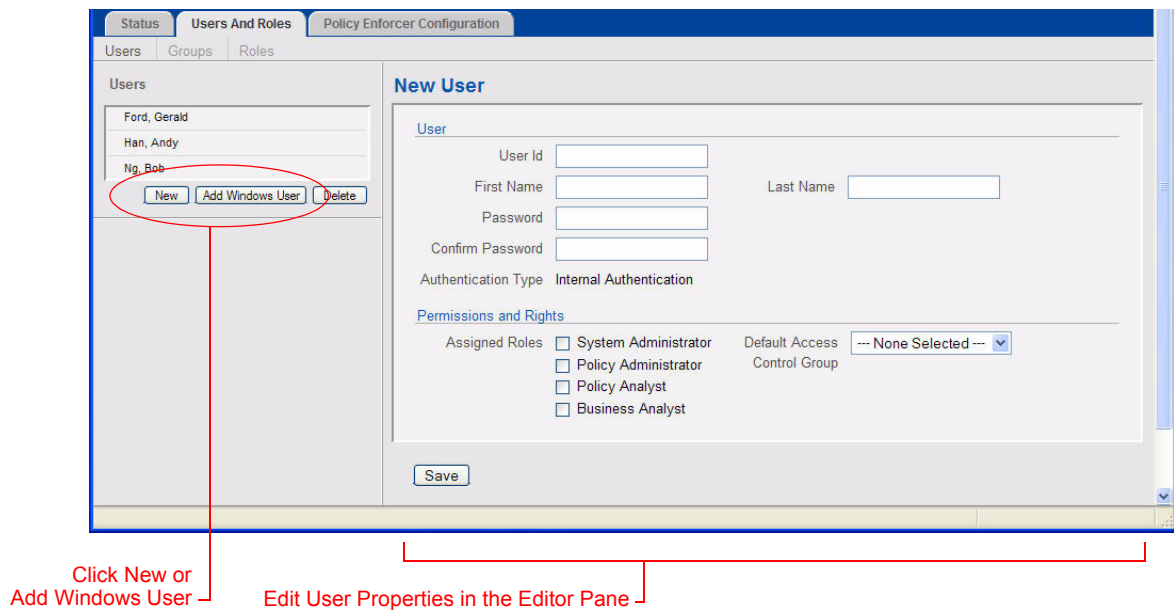


Figure 4-3: The Users Screen

3. In the Editor pane, define the basic characteristics of the user account. (Some of these fields will not be available if you clicked Add Windows User to grant access to an existing user, because in that case the user authentication is set up outside of Compliant Enterprise.)
 - In **User ID**, type the user account name the user will type into the Login dialog box when starting Administrator, Reporter, or Policy Author.
 - In **First Name** and **Last Name**, type the user's real name.
 - Define the **Password** that will allow this user to log in. Note that this must contain 7-12 characters, at least one number, at least one letter, and at least one non-alphanumeric character other than underscore.
4. In Assigned Roles (under Permissions and Rights), check one or more boxes to define what actions the user is allowed to take when using Compliant Enterprise applications.
5. (Optional) In Default Access Control Group, you can define which default access control (DAC) group you want this user to belong to. You specify this by choosing one of the user groups in the drop-down list, which displays all groups to which this user belongs.
 The drop-down list will be empty if this user is not assigned to any groups. That is, you can only use this feature if the user belongs to at least one group.

For more details on how DAC groups work, see [page 70](#).

- Click Save. Once the new user is saved, you will see the green confirmation message.

✓ Your changes were saved successfully.

Deleting a User

You might need to delete a user if that person leaves your organization or is reassigned to another project and is no longer working with Compliant Enterprise. When you delete a user, it only affects their ability to use Compliant Enterprise applications; the user is not deleted from your organization as a whole.

To delete an existing user, simply select it in the list of Users, and click the Delete button.

Managing User Groups

Managing user groups involves three operations: creating new groups, importing existing groups from your enterprise, and modifying existing groups in Administrator.

Creating a New Group

To create a new group,

- Go to the Users and Groups tab and click the Groups link. This will display the Groups screen, with the General tab in front as shown in [Figure 4-4](#).

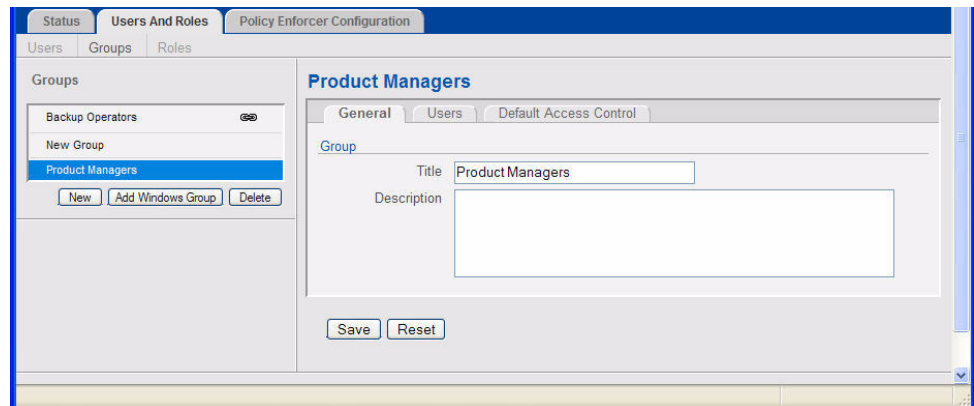


Figure 4-4: The Groups Screen, General Tab

- Type a name and description for this group, and click Save.

3. Go to the Users tab, where you can select the users you want to add to the group. You do this by clicking the Add button at the right, to display an index of available users.

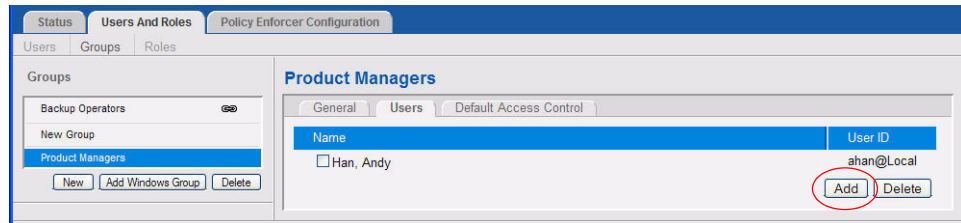


Figure 4-5: The Users Screen, Users Tab

4. In this index, click the hyperlinked letters to find the name you want, then click the name. The name appears in the Users to Add list at the left side of the window.

Note: You can only add users to groups if they have already been defined on the Users screen. If no names are available for adding to a group, you must first define them as users.

5. When you have added all the users you want, click the Add button at the left.

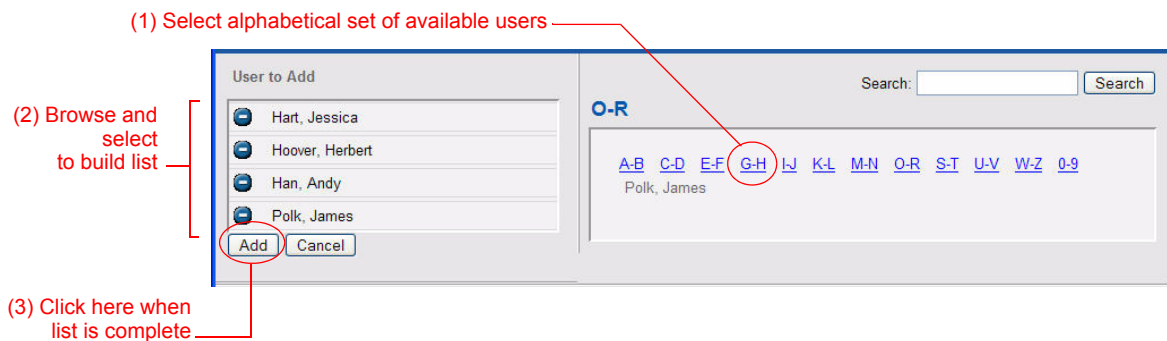


Figure 4-6: Adding New Users

6. (Optional) If you wish, you can assign default access control permissions to this group as a whole, and/or to any individual members of it.

About Default Access Control Groups

Once you define a group, you can assign the permissions you want other people to have on components and policies created by any user in that group. Assigning default access control (or DAC) at the group level makes it easier for different teams within your organization to work together—or to keep their work sepa-

rate, as desired. This feature lets you selectively grant access from all users in one group, to all users in that group or in other groups, or to selected individual users. Once you define DACs, you can assign them to individual users.

You define permissions for access groups on the Default Access Control tab of the Groups screen, as shown in [Figure 4-7](#). You have the option to allow other users or groups to do any of the following to components and policies:

- Set Access
- Read
- Write
- Delete
- Submit
- Deploy

Again, though these permissions are set at the group level, they only have meaning insofar as they apply to all the members of that group. (After all, groups don't define components or policies, individual users do.) Membership in a group determined by the Default Access Control Group field on the Users screen (see [Figure 4-3](#) on [page 68](#)), which you can use to associate each user with a DAC group.

There are two reasons this explicit association is required even though a user may be assigned to a standard user group, on the Groups tab. First, a user may belong to more than one user group with different DAC permissions defined for them, and this field allows you to designate which permissions will apply to this user. (Each user can belong to only one DAC group.) Second, you have the option of not assigning a user to any DAC group, by simply leaving this field blank. This allows a sort of override mechanism: even if a user belongs to a group and that group has DAC permissions defined for it, that user's components and policies will not be subject to those permissions.

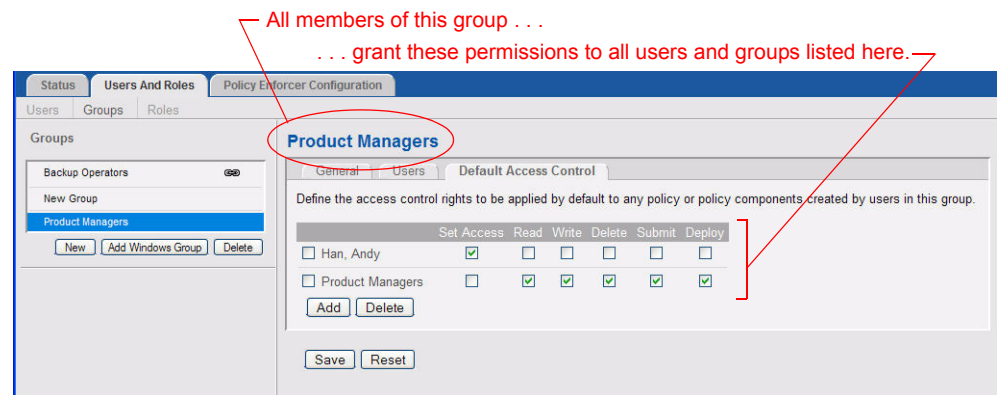


Figure 4-7: The Users Screen, Default Access Control Tab

As we mentioned, these DAC permissions may be granted to groups or individuals. To do this, you use the Add button to browse for a user or a group, add it to

the list on the Default Access Control tab, and check the kinds of permissions you want to grant to that group.

The groups given permission may include the group itself—in which case all members of that group will be given the specified permission to any objects others in the group created—but this is not necessary. To do this, the group itself must be added to the list and checkboxes checked, just as for any other group or user. This is the case in the example shown in [Figure 4-7](#): the Product Managers group permissions list includes the Product Managers group itself.

The example shown defines the following situation: whenever any user in the Product Managers group creates a component or a policy, all other users in that group have permission to read, write, delete, submit, and deploy it. In addition, the individual user Andy Han has permission to set access for those components or policies, even though he is not a member of the Product Managers group.

To assign default access controls to a group,

1. On the Groups screen, go to the Default Access Control tab. Click Add. An index of users and groups appears.
2. Click the hyperlinked letters to find the name of a user or group to which you want to grant access, then click the name. The name appears in the Principals to Add list at the left side of the window.
3. When all the desired names are in the list, click Add.
4. Check one or more boxes next to each principal to indicate what you want that user (or users in that group) to be able to do with objects created by users in the group you are editing.

One last point: the reason these are called *default* access controls, is that they automatically apply when a component or policy is created, but they can always be overridden by defining a custom set of permissions for the component or policy, using the Access Control tab of the object's Properties window.

Linking to an Existing Windows Group

1. On the Groups screen, click Add Windows Group.
2. Specify the group(s) you want to link to. An alphabetized index of hyperlinks appears, showing groups that exist in your Windows domain.
3. Click the hyperlinked letters to find the name you want, then click the name. The name appears in the list at the left side of the window.
4. When all the desired names are in the list, click Add.
5. On the General tab, give a name and description for the group. The source of the group is displayed in External Link.

Modifying a Group



If the link icon appears, you cannot modify the membership of a group; it is linked to a group in your Windows domain and is managed there, not from within Compliant Enterprise.

1. Click the Groups tab. If this group is imported from your Windows domain, its source is displayed in External Link.
2. Make the desired modifications.
3. Click Save.

Deleting a Group

To delete a group, simply select it in the list of groups, and click the Delete button.

Managing Roles

As we mentioned earlier, a *role* is simply a named set of permissions for working with the three Compliant Enterprise applications, which you can define independently and then assign to users and groups as appropriate. (It is somewhat analogous to the way components and policies work in Policy Author, in that it provides a layer of abstraction between the users and groups and the permissions assigned to them.)

You can use roles as intensively as you wish to suit your needs. However, there are certain circumstances when you definitely should modify them:

Initial Implementation. When Compliant Enterprise is first installed, the role definitions are not assigned to any users. Before any system administrators in your organization can start using the Policy Author, Reporter, and Administrator tools, you must set up the Compliant Enterprise roles and assign each role to at least one user. (In order to gain initial access to the Administrator tool in order to set up and assign roles, you can use the built-in Administrator account.)

Shifting Responsibilities. Change the roles to set up the division of labor that reflects the changing conditions at your organization. The permissions granted in each role represent the tasks that can be done by users assigned to that role. In any given organization, at one point in time, the different tasks that can be accomplished with the Compliant Enterprise tools (Policy Author, Administrator, and Reporter) might be carried out by different people, while in another organization or at a different time, all of these tasks might be carried out by one person.

Note that as you modify a role, your work is not automatically saved as you go. If you are interrupted while working on a role, or if you want to work on another task and return to modifying the role later, click Save before you stop work.

To modify a role,

1. On the Users and Roles tab, click the Roles link.

2. Click the name of the role you want to modify, to display the current settings for that role.

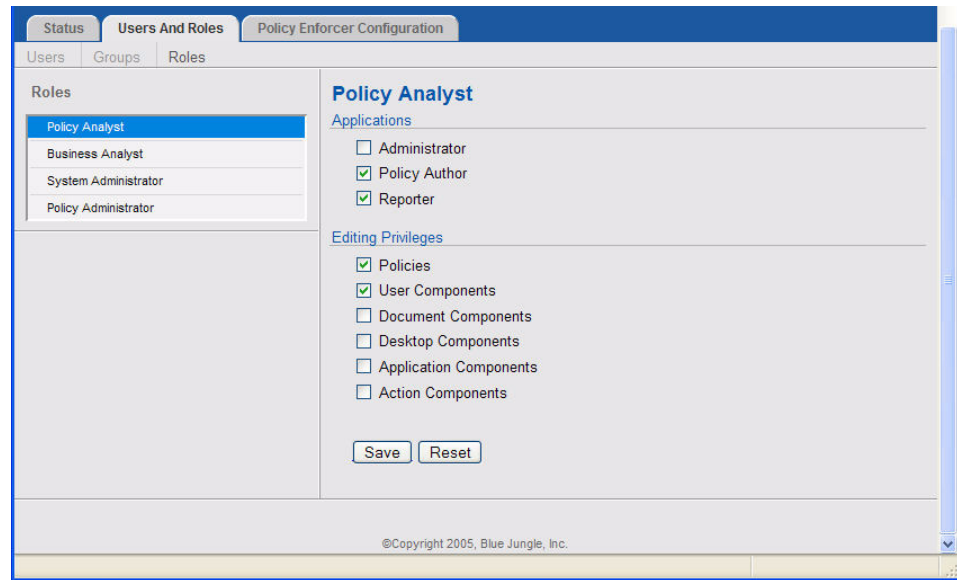


Figure 4-8: The Roles Screen

3. In Applications, select the Compliant Enterprise tools that you want users in this role to be able to run. For example, for the Business Analyst role, you would typically check Reporter.
4. In Editing Privileges, select what types of objects users in this role can modify. If you checked Policy Author in step 3, but you don't check any objects in this step, then users in this role can view but not edit policies and policy components.
5. Click Save.

Assigning Roles to Users

Once you have defined users, groups, and (optionally) roles, you need to give each user appropriate access the Compliant Enterprise tools (Policy Author, Administrator, and Reporter). You do this by assigning one or more roles to each user. To do this,

1. On the Users and Roles tab, click the Users link.
2. In the list under Users, click the name of the user to whom you want to assign one or more roles. (The first time you use Administrator, this list might be empty.)

If you do not see the user you want, click the Add Windows User button and select the user from the Add Users dialog box. Compliant Enterprise creates the Add Users list by doing a live check of the domain controller in your organization's Active Directory and importing an up-to-date list of users.

3. In Permissions and Rights, under Assigned Roles, check one or more boxes next to the roles you want this user to have.
4. From the Default Access Control Group combo-box, select the DAC group (see [page 70](#)) you want this user to belong to. You can also leave this blank if you do not want the user to belong to any DAC group.
5. Click Save.

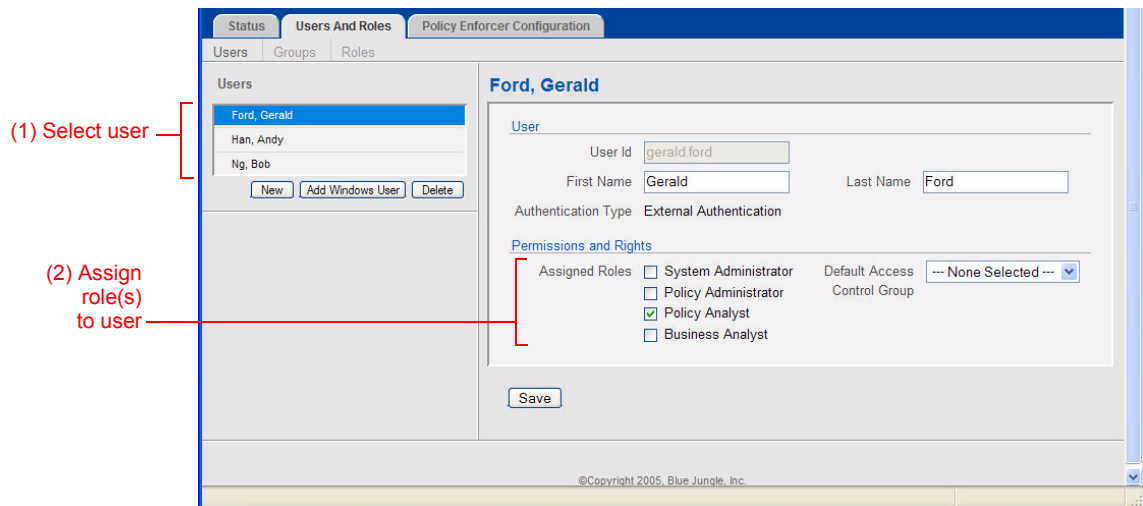
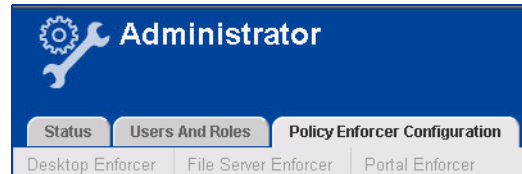


Figure 4-9: Assigning Roles to Users

The Enforcer Configuration Tab

The controls available on this tab allow you to define and manage enforcer profiles.



About Profiles

All policy enforcers are governed by a number of configuration settings that control such aspects as logging behavior, heartbeat rate, tamper-prevention password, and network configuration. These are assigned default values when you first install an enforcer, but they can be changed manually at any time.

To simplify this, Administrator allows you to create named sets of configuration settings, which you can then assign to one or more enforcers in your network. These are referred to as *enforcer profiles*, and you can manage them here on the Policy Enforcer Configuration tab. You can define profiles for each of the three types of enforcers; you do this by clicking on the corresponding link on the Policy Enforcer Configuration tab.

Note that on the File Server Enforcer page, profiles make no distinction between Windows- and Linux-based enforcers; you can assign the same profile to enforcers on either platform.

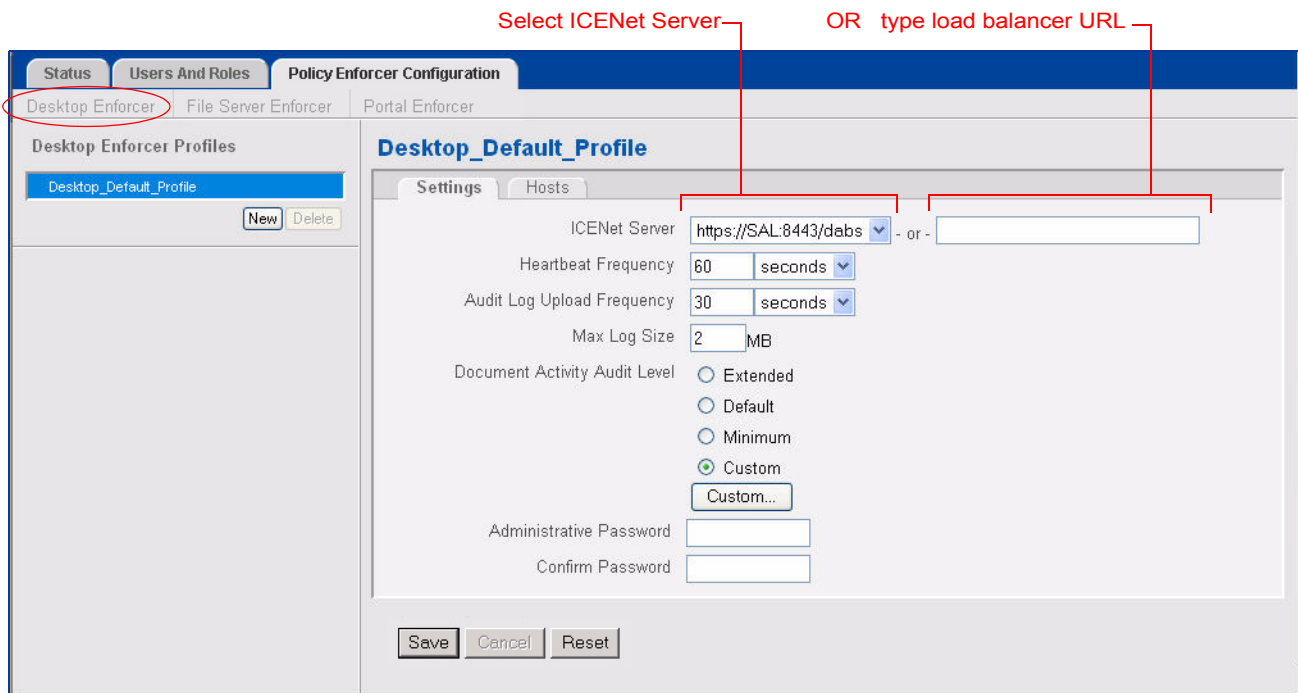


Figure 4-10: The Policy Enforcer Configuration Tab

For each enforcer type, one default profile containing all default settings is available after installation, and it is automatically applied to any enforcer you install. If you wish to create more profiles and assign them to various enforcers, you can do so here. This is not strictly mandatory, but it is strongly recommended that you at least change the administrator password, as a security precaution.

Initial Registration

When you install any enforcer, the installation wizard prompts you for an ICENet Server to connect to. This does not necessarily represent the ICENet server the server will always connect to, but rather the one it will connect to the first time it starts up, in order to register itself with the Control Center. When an enforcer registers, it informs the Control Center of its location and status, and acquires the operating parameters specified by its assigned profile—in most cases, the default profile for its type.

From that point on, the enforcer will connect to the Control Center through the ICENet server specified in its assigned profile. This may be the same ICENet server as was specified during enforcer installation, but it may be different, and in the latter case the ICENet server specified during installation will not be used any longer by that enforcer. The important point here is that just because you specified some ICENet server during installation, that does not mean the enforcer will necessarily continue to connect through that one for anything but its initial registration.

Profiles, ICENet Servers, and Hosts

It is important to understand the relationship between enforcer profiles, ICENet Servers, and enforcer hosts.

- Each enforcer host in the network—file servers, desktops or laptops—is a client of only one ICENet Server. You specify this when you install the enforcer.
- Each profile can be associated with only one ICENet Server (or with one cluster of load-balanced servers). You can think of this as the profile's parent ICENet Server. This is set as a property of the profile.
- This means that any profile is available only to those enforcers running on hosts that are served by the ICENet Server of which they are clients. Or, looking at it from the other direction, any enforcer can be assigned only those profiles that belong to its ICENet Server.
- However, each ICENet Server may have multiple profiles associated with it, just as it may have multiple enforcer hosts as clients.
- You can define a profile and assign it to one or more of the hosts belonging to its parent ICENet Server. You can reassign a different hosts to a profile.
- You can associate a different ICENet Server to an existing profile. When you do that, the profile is automatically made available for assigning to all the enforcer clients of that server. You can think of

this as moving the profile from one ICENet Server to another. It has the effect of removing the profile from all enforcers served by the previous ICENet Server (it is replaced by the appropriate default profile), and making it available to assign to all enforcers served by the new ICENet Server.

Load-Balanced ICENet Servers

As far as profiles are concerned, each cluster of load-balanced ICENet Servers behaves like a single one. You can associate a load balancer with a profile by typing its virtual IP address or virtual host name into the OR field (see Figure 4-10 on [page 76](#)). In this case, all hosts of all the ICENet servers in the cluster will have the profile available to them—that is, they can be added on the profile's Hosts tab.

For details on setting up load sharing, see [page 91](#).

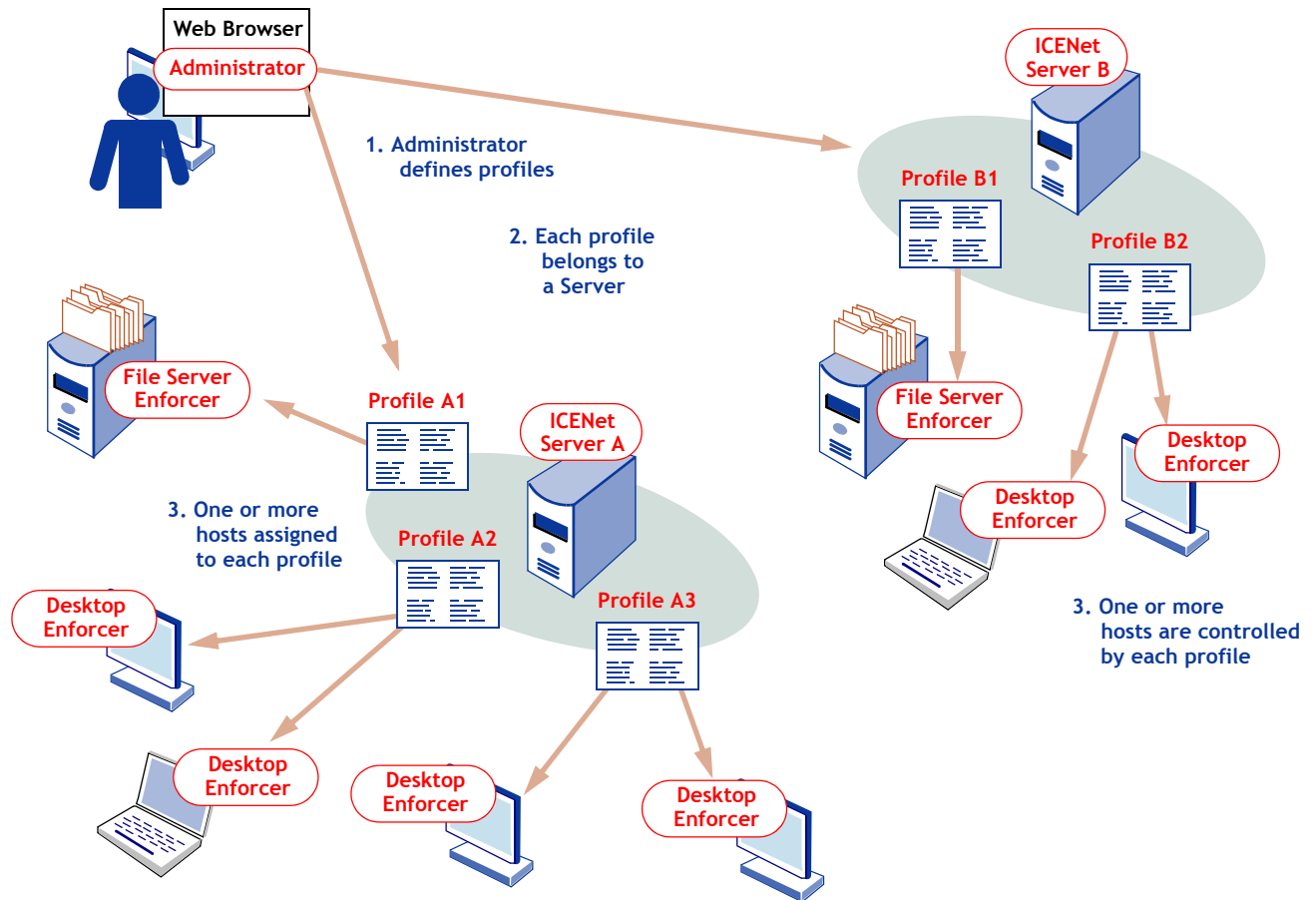


Figure 4-11: Profiles, ICENet Servers, and Hosts

Working with Profiles

Administrators can work with enforcer profiles in several ways, including defining them, changing which enforcers belong to them, modifying them, and deleting them.

Defining a New Profile

Defining a new profile is very simple.

1. At the top of the tab, specify which kind of profile you want to create by selecting one of the three sub-tab links: Desktop Enforcer, File Server Enforcer, or Portal Enforcer.
2. In the left-hand pane of the screen, click the New button.
3. Assign a descriptive name to the new profile.

4. On the Settings tab in the right-hand pane, specify all settings as needed for the new profile. As a practical rule, the settings you will be most interested in—that is, the ones that are most useful in distinguishing one profile from another—are the ICENet Server and the password. [Table 4-4](#) provides descriptions of all settings.

Table 4-4: Enforcer Profile Settings

Setting	Description
ICENet Server	Specifies the ICENet Server that this profile is associated with. That is, this profile will be available to all the clients of the ICENet Server selected here. Choose one of the following: <ul style="list-style-type: none"> From the drop-down list, select the URL where the ICENet Server component is installed; or, If you have set up load balancing for the ICENet Server, type the URL of the load balancer in the OR field.
Heartbeat Frequency	Specifies the frequency, in seconds, of the heartbeats the policy enforcer sends to the server. A heartbeat is a signal that lets the server know the policy enforcer is running and provides an opportunity to download a policy deployment or new policy enforcer profile to the policy enforcer. Default value = 3600 [one hour]
Audit Log Upload Frequency	Specify the interval, in minutes, at which policy enforcers send their activity logs to the server. Default value = 30 Note that frequent log uploads might affect the speed of your network.
Max Log Size	Specify the maximum allowed sized, in MB, of the current policy enforcement log is allowed to become. Default value = 2 If the log reaches the Max Log Size before the scheduled upload time, logs are uploaded immediately, unless the machine is not connected to the network. In that case, logging is suspended, while policy enforcement continues.
Document Activity Audit Level	Defines the kinds of actions that will be written to the Activity Journal for the purposes of running document activity audits. Details are provided below, under "Using the Document Activity Auditing Level".
Administrative Password	Assign a password to tamper-protect policy enforcers installed under this profile. This password will be needed to stop or uninstall any policy enforcer covered by this profile. For both the Desktop Default Profile and the File Server Default Profile, and whenever you create a new profile, this password is initially set to "password". You should replace this default whenever you actually apply any profile to enforcers.

Note: If you are setting up a profile for a global audit, be sure to set the Document Activity Audit Level to Extended.

5. Once you have changed all settings you need, click the Save button to save the new profile.
6. On the Hosts tab, select all enforcers you want this profile to control. You can apply a profile to as many enforcers as you like.
7. When you are finished selecting hosts, click the Save button.

Using the Document Activity Auditing Level

For each profile you define, you can specify exactly which user or system activity is recorded in the Activity Journal for all enforcers governed by that profile. You use the radio buttons to choose one of four levels:

- **Minimum:** Records any attempts to tamper with the policy enforcer installed on this host, including all actions listed under Minimum Options in the Custom Journaling window. These events are always recorded; they cannot be disabled.
- **Default:** Records all events included under Minimum Options in the Custom Journaling Options window, plus those listed under Default Options.
- **Extended:** Records all events included under Minimum Options and Default Options the Custom Journaling Options window, plus those listed under Extended Options.
- **Custom:** Records whatever combination of events you select the Custom Journaling Options window. To open this window, click the Custom button. Check the boxes next to the actions that you want included in the log. If you leave all the boxes unchecked, the logging feature is set to Minimum.

Since the three types of enforcers work in different ways, the list of activities available to monitor is different for each enforcer type. [Figure 4-12](#), below, shows the list in the Options window for each type of enforcer.

Using Profiles for Auditing

You can also define a profile purely for the purpose of gathering data for what we refer to as a *targeted audit*. To do this, simply create only one profile, select only those activities you want to audit (under Custom Journaling Options) and assign only those hosts you want to include in the audit. Or if you prefer you can use more than one profile, with certain actions audited on certain hosts and other actions on other hosts. You can then generate reports to analyze the data collected in the Activity Journal. The benefit of this strategy is that it requires less system resources than an unfiltered, global audit.

Removing a Host from a Policy Enforcer Profile

Every policy enforcer host in the network can belong to only one profile at any time. If you decide to change the policy enforcer settings for a particular host, you do it by simply assigning the host to a different profile. In other words, the procedure for removing a host from a profile is the same as for assigning a host. Whenever you assign a host to a profile, it is automatically removed from any other profile to which it may have previously belonged.

Desktop Enforcers	File Server Enforcers	Portal Enforcers
<p>Custom Journaling Options</p> <p>Extended</p> <p><input type="checkbox"/> Create/Edit</p> <p><input type="checkbox"/> Delete</p> <p><input type="checkbox"/> Open</p> <p>Default</p> <p><input type="checkbox"/> Move</p> <p><input type="checkbox"/> Attach to email</p> <p><input type="checkbox"/> Copy</p> <p><input type="checkbox"/> Change File Permissions</p> <p><input type="checkbox"/> Print</p> <p><input type="checkbox"/> Attach to instant messenger</p> <p><input type="checkbox"/> Change Attributes</p> <p>Minimal</p> <p><input type="checkbox"/> Abnormal Enforcer Shutdown</p> <p><input type="checkbox"/> Enforcer Configuration File Access</p> <p><input type="checkbox"/> User Login</p> <p><input type="checkbox"/> Policy Bundle File Access</p> <p><input type="checkbox"/> Enforcer Startup</p> <p><input type="checkbox"/> Enforcer Shutdown (normal)</p> <p><input type="checkbox"/> Enforcer Log File Access</p> <p><input type="checkbox"/> User Logout</p> <p><input type="checkbox"/> Policy Bundle Authentication Failed</p> <p><input type="checkbox"/> Enforcer Binary File Access</p> <p><input type="checkbox"/> Policy Bundle Authentication Succeeded</p> <p>OK Cancel</p>	<p>Custom Journaling Options</p> <p>Extended</p> <p><input type="checkbox"/> Create/Edit</p> <p><input type="checkbox"/> Delete</p> <p><input type="checkbox"/> Open</p> <p>Default</p> <p><input type="checkbox"/> Move</p> <p><input type="checkbox"/> Change File Permissions</p> <p><input type="checkbox"/> Change Attributes</p> <p>Minimal</p> <p><input type="checkbox"/> Abnormal Enforcer Shutdown</p> <p><input type="checkbox"/> Enforcer Configuration File Access</p> <p><input type="checkbox"/> User Login</p> <p><input type="checkbox"/> Policy Bundle File Access</p> <p><input type="checkbox"/> Enforcer Startup</p> <p><input type="checkbox"/> Enforcer Shutdown (normal)</p> <p><input type="checkbox"/> Enforcer Log File Access</p> <p><input type="checkbox"/> User Logout</p> <p><input type="checkbox"/> Policy Bundle Authentication Failed</p> <p><input type="checkbox"/> Policy Bundle Authentication Succeeded</p> <p><input type="checkbox"/> Enforcer Binary File Access</p> <p>OK Cancel</p>	<p>Custom Journaling Options</p> <p>Extended</p> <p><input type="checkbox"/> Create/Edit</p> <p><input type="checkbox"/> Delete</p> <p><input type="checkbox"/> Open</p> <p>Default</p> <p><input type="checkbox"/> Move</p> <p><input type="checkbox"/> Copy</p> <p><input type="checkbox"/> Download/Export</p> <p><input type="checkbox"/> Upload/Attach to Item</p> <p><input type="checkbox"/> Print</p> <p>Minimal</p> <p><input type="checkbox"/> Abnormal Enforcer Shutdown</p> <p><input type="checkbox"/> Enforcer Configuration File Access</p> <p><input type="checkbox"/> User Login</p> <p><input type="checkbox"/> Policy Bundle File Access</p> <p><input type="checkbox"/> Enforcer Startup</p> <p><input type="checkbox"/> Enforcer Shutdown (normal)</p> <p><input type="checkbox"/> Enforcer Log File Access</p> <p><input type="checkbox"/> User Logout</p> <p><input type="checkbox"/> Policy Bundle Authentication Failed</p> <p><input type="checkbox"/> Policy Bundle Authentication Succeeded</p> <p><input type="checkbox"/> Enforcer Binary File Access</p> <p>OK Cancel</p>

Figure 4-12: Custom Journaling: Actions Available for Different Enforcers

Modifying a Policy Enforcer Profile

As company conditions change over time, you might want to change a policy enforcer profile. For example:

- You may want to change the security password.
- You may want to change the level of Activity Journaling that the policy enforcers perform.
- If you expand your hardware infrastructure and install policy enforcers on additional machines, and you don't want to use the default policy enforcer profiles which are assigned automatically, you will need to assign each of those new hosts to a policy enforcer profile.

The modifications go into effect the next time the policy enforcer sends a heartbeat to Compliant Enterprise.

To edit an existing profile,

1. Click the link for the type of policy enforcer profile you want to modify, either Desktop Enforcers or File Server Enforcers.
2. Click one of the profile in the list to display its details in the editing pane.
3. Click the Settings or Hosts tab, depending on what part of the profile you want to modify.
4. Make the desired changes.
5. When you are finished, go to the Settings tab and click Save.

Deleting a Policy Enforcer Profile

You can delete any profile that is currently defined. Bear in mind that deleting means just that—removing it from the Compliant Enterprise system altogether. It should not be confused with “deleting” the profile from a specific host; for information on how to do that, see “Removing a Host from a Policy Enforcer Profile”, above.

When you delete a policy enforcer profile, any hosts that were assigned to that profile are reassigned to the default profile. You cannot delete the default profile.

To delete a profile, simply select the profile in the left-hand pane, and click the Delete button as shown below.

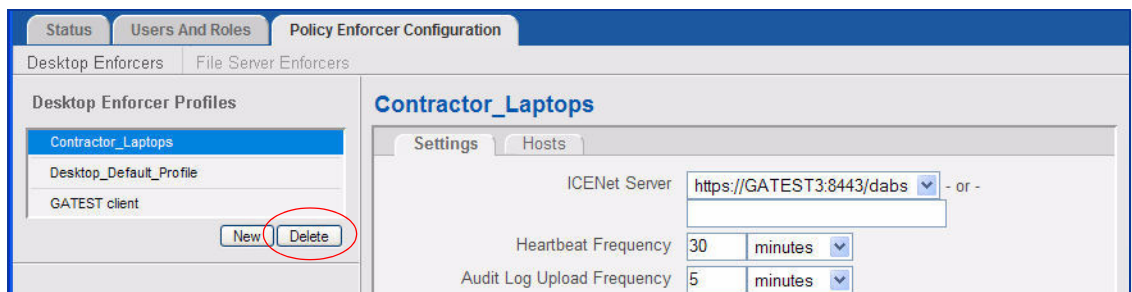


Figure 4-13: Deleting an Enforcer Profile

Moving Profiles between ICENet Servers

As we mentioned above, you can in effect move a profile from one ICENet Server to another, by assigning a new server to the profile. This has the effect of removing the profile from all enforcers served by the previous ICENet Server, and making it available to be assigned to all enforcers served by the new ICENet Server. However, it is not actually assigned to any of these clients until you do so explicitly, by adding them to the list on the profile’s Hosts tab.

Bear in mind that moving profiles in this way involves a delay, due to the reliance on heartbeat messages. If you ever decide to move the profiles associated with one server over to another server, you should leave both servers running long enough to allow all client hosts to receive the instructions about the han-

dover. Clients connected to the network will receive the update with their next heartbeat message (30 seconds, by default); but any mobile clients that are not connected to the network will not get this update until they connect. If the old server is shut down before mobile clients reconnect, they will continue to enforce policies but will be cut off from the Compliant Enterprise system: they will not be able to receive any new policy updates, or send their audit data back to the Activity Journal.

In the previous chapter, we discussed the tools that are available for reconfiguring the system, either during initial installation or at any time during routine operation. In this chapter we discuss several management activities that may be required from administrators in the course of routine operation. These fall into the following categories:

- Managing Control Center
- Exporting and Importing Policies ([page 86](#))
- Managing Policy Enforcers ([page 91](#))
- Managing Security Certificates ([page 98](#))
- Database Administration ([page 99](#))

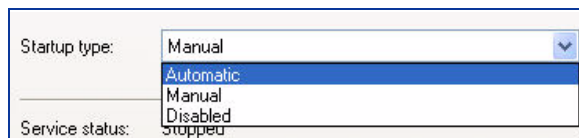
Managing Control Center

All the server and database components of Control Center are designed to start once and run continuously as a Windows service. Users should note that the name of this service does not reflect the individual server components. In fact, although (depending on your configuration) you may have several or even all of the Control Center servers installed on the same host, they will all appear in the Windows Services manager as a single service, called Compliant Enterprise Control Center. Similarly, no matter how you distribute components across several hosts, each host will display only one Compliant Enterprise Control Center service in the Windows Services list, representing one or more server components.

Note however that the embedded databases—the Administrator database and the network directory—do appear as separate services in the list, and may be restarted manually if necessary.

Starting and Stopping

Whether single-host or distributed, this service must be manually started after the initial installation. By default, it is not set to restart automatically if it fails, but like any service you can change that if you wish, by changing the Startup Type from Manual to Automatic.



You can use the Status tab in Administrator (see [page 61](#)) to keep an eye on whether the individual components are running normally. If one fails and you

need to restart it, you can do so by restarting the Control Center service, regardless of whether that service represents more than one Control Center server component.

Similarly, if you ever need to stop any server process, you must stop the service even though this will stop all Control Center components running on that host.

Exporting and Importing Policies

Components and policies require time and effort to design and construct. However, there may be cases where you want to distribute the components and policies defined in one implementation of Compliant Enterprise and deploy them in another. For example, you may have a separate test environment where you have fine-tuned your policies, and you now need to transfer them to your production network.

To avoid having to manually redefine all the components and policies in the second system, Compliant Enterprise provides a CLI-based import/export utility. The feature allows you to export any policies in one implementation, along with their folder structure, so you can import them elsewhere. Although all components required by exported policies are automatically included, you have the option of manually specifying components to export as well. All objects are exported to an XML file, which you can then import into the policy repository of another Compliant Enterprise system.

Specifically, this feature allows you to:

- Export all policies from a given Control Center
- Export selected policies by folder, either recursively or not
- Export selected individual policies
- Export specified components
- Perform a *shallow export*, which strips policies of any leaf wirings that tie them to the physical system
- Generate a list of components and/or policies, without exporting
- Import the contents of XML files generated by exporting
- View the contents of such XML files, without importing

Exporting

To export an existing set of policies and/or components from Policy Author:

1. Log in to the host of the Control Center from which you want to export policies, or to a computer that can connect to it, and open a command line window.
2. Make sure the Export utility (**export.exe**) is present on the host where you will be working. By default, it is placed in the Control Center host at Program Files\Compliant Enterprise\tools, and is also available on the installation CD.

3. Navigate to the location of the utility, and type the export command with the three required connection arguments and whichever of the optional arguments you want to use, using the format below. The optional arguments allow you to specify what content you want to export, and what to do in case of conflicts. [Table 5-1](#) provides details on all available arguments.

```
% export -s <host> [-p <port>] -a <admin> -w <password> [-f | -x] [-v | -l ] [-d <dirName>] <filename>
```

Connection arguments (port is optional)
Optional controls
Required

4. When the export finishes, it displays one of the following return codes:

```
0: Export successful

-1: Unknown host

-2: Connection refused. Check the credentials and try again.

-3: Target not found, export aborted.

-4: Cannot create export file. Check for disk full, or inadequate permissions. Export aborted.
```

If the export was successful, the exported objects are available in an XML file with the name you specified, which can be imported into another Control Center.

Table 5-1: Command Line Arguments, Export Command

Argument		Description
Connection	-s <server>	The name or URL of the host where the Control Center is running, from which you want to export the policies. This argument is required.
	-a <adminName>	User name of a Compliant Enterprise user with administrator privileges. This argument is required.
	-w <password>	The Compliant Enterprise utility password. This argument is required.
	-p <port>	The port of the Control Center host. If not specified, the default 8443 is used.
Controls	-h	Help: displays the syntax of this command, as a reminder to the user. Supersedes any other arguments.
	-v	Displays a list of all folders, policies and components specified by the target. Details are not displayed.
	-l	Displays a list of all folders, policies and components specified by the target, including details. Details include path/name, version, and author. Supersedes -v.
	-f	If a file with the same name as the export file already exists, the earlier version will be overwritten. Cannot be used together with the -x flag.
	-x	If a file with the same name as the export file already exists, the export operation will be cancelled. Cannot be used together with the -f flag.

Table 5-1: Command Line Arguments, Export Command (Continued)

Argument		Description
Export Target Specifications	-u	Export file will include all folders, policies and components in the Policy Master database. Supersedes any other target specification.
	-d <dirName>	Include specified directory, exporting all policies and their dependent components. May be used more than once, and in conjunction with any other target specifier. Non-recursive—does not follow into sub-folders.
	-r <dirName>	Include specified directory, as well as all its subdirectories, exporting all policies and their dependent components. May be used more than once, and in conjunction with any other target specifier.
	-p <path/policy>	Include the policy specified by path/policy, including all of its dependent components. The path is the folder hierarchy of this policy. May be used more than once, and in conjunction with any other target specifier.
	-c <[type]:<name>	Include the component specified by the qualified name, which consists of the component type and the name. Valid values for type include: <i>user, computer, application, action, file, or portal</i> .
	-n	Perform a <i>shallow export</i> , which unwires components and policies from the actual system environment (see below).
	<filename>	The name you want to assign to the export file. The value specified here will be appended with an .xml extension. This argument is required, and must be the last string in the line.

Displaying a List

If you only want to generate a list of policies and/or components, you can use one of the List flags:

- **-l** displays a list of all folders, policies and components specified by the export target specification elements, along with path/name, version, and author.
- **-v** displays a list of all folders, policies and components specified by the export target specification elements, but without the details—just the names.

Note that in either case you must specify the target policies or folders you want to list.

About Shallow Export

The shallow export flag, **-n**, commands the utility to perform a special kind of export: for any components or policies that are defined with reference to specific user or group names or to network hosts or paths, the utility will remove those references, saving only those aspects of the definitions, such as LDIF metadata and file or user properties, that do not tie the definitions to the physical environment.

File Overwrite Default Behavior

As shown in the table above, the **-f** and **-x** flags provide instructions on what the export utility will do when a file with the same name as the specified export file already exists: either overwrite, or cancel the export. Even if you do not specify

either of these flags, if the utility finds that the output file already exists, it prompts the user for permission to overwrite. If the user specifies No, it then asks for a new file to write to, proposing a default name. Here is a typical scenario (user actions are in bold):

```
% export -s begemot -a Admin -w 123passw!d -u foo.xml <CR>
Foo.xml already exists. Overwrite Y/N (N)? <N> <CR>
New output file (foo (1).xml) : <CR>
Export successful.
%
```

Note that in this situation, the utility offered an alternative file name based on the original one, in the same directory. The user has the option of accepting that, or supplying a different name and/or path.

Importing

Once you have generated an XML file through the export procedure, you can import it to another Control Center, where the policies and components will then be available for use in Policy Author. For this, you use a separate import utility called `import.exe`, which is also placed on the Program Files\Compliant Enterprise\tools directory during Control Center installation. To use this utility,

1. Open a command line window, on a computer with a network connection to the Control Center where you want to import the policies and components.
2. Navigate to the location of the utility, and type the import command line, specifying the required connection arguments, controls, and name of the source file you want to import. Use the following format:

Connection arguments (port is optional)	Optional controls	Required
% import -s <host> [-p <port>] -a <admin> -w <password>	[-o -u -d -x]	<filename>

3. When the import finishes, it displays one of the following return codes:

```
0: Import successful
-1: Unknown host
-2: Connection refused. Check the credentials and try again.
-3: Cannot open export file. File does not exist, or user has
    inadequate permissions. Import aborted.
-4: Import canceled by user.
-5: Import canceled by server.
```

If the import was successful, at this point the objects you imported are available for use in Policy Author, and are displayed in the policy tree and component panels.

Table 5-2: Command Line Arguments, Import Command

Argument		Description
Connection	-s <server>	The name or URL of the host where the Control Center is running, to which you want to import the policies. This argument is required.
	-a <adminName>	User name of a Compliant Enterprise user with administrator privileges. This argument is required.
	-w <password>	The Compliant Enterprise utility password. This argument is required.
	-p <port>	The port of the Control Center host. If not specified, the default 8443 is used.
Controls	-h	Help: displays the syntax of this command, as a reminder to the user. Supersedes any other arguments.
	-v	Displays a list of all folders, policies and components in the specified export file. Details are not displayed.
	-l	Displays a list of all folders, policies and components in the specified export file, including details. Details include path/name, version, and author. Supersedes the -v flag.
	-o	Resolve all data conflicts by overwriting the existing data on the server with the imported data from the file. Cannot be used together with the -u or -d flags.
	-u	Resolve all data conflicts by adding the imported data to the server, with auto-generated new names. Cannot be used together with the -o or -d flags.
	-d	Resolve all data conflicts by keeping the names of existing policies and components, but overwriting their definitions when necessary, based on the imported data. Cannot be used together with the -o or -u flags.
	-x	In the event of data conflict, cancel the import operation. Supersedes the -o, -u, and -d flags.
	<filename>	The name of the file you want to import. This argument is required, and must be the last string in the line.

Viewing the Contents of an Export File

As with the Export command, the -l and -v flags allow you to review the contents of the file—with or without details, respectively—before you actually run an import procedure.

Managing Policy Enforcers

There are a number of procedures that a system administrator may need to perform from time to time, regarding the policy enforcers in the system. These include:

- Adding Additional Enforcers ([page 91](#))
- Load Balancing ([page 91](#))
- Stopping Policy Enforcers ([page 93](#))
- Restarting Policy Enforcers ([page 95](#))
- Uninstalling Policy Enforcers ([page 95](#))
- Reconfiguring Enforcers ([page 96](#))

We'll examine each of these in turn.

Adding Additional Enforcers

If you need to install additional enforcers of either type you can do so at any time using managed installation methods, such as a login script or Windows Group Policy Object (GPO). Compliant Enterprise provides an .msi installation file that can be used with these installation methods. The rest of this section provides general instructions for performing a managed installation using GPO. For details about GPO, refer to Microsoft documentation.

1. Use Microsoft Group Policy Object (GPO) to set the domain controller and register each target machine on which you want to install policy enforcer software.
2. Create an .MSI transform file (.MST file) to set the value of the required installation parameter ICENET_SERVER_LOCATION to the host where the ICENet Server is installed. Use the format machine-Name:port. If you use the default port number 8443, you can omit it from the value and simply set the machineName.
3. Use any desired transformation tool to create the file, and consult the documentation for that tool for details on how to set up the file.
4. Configure GPO to run the appropriate .msi and .mst files whenever each machine is booted up:
 - **Desktop or laptop PCs:** WindowsDesktopEnforcer-setup.msi
 - **File servers:** WindowsFileServerEnforcer-setup.msi

The domain server will automatically send the binary to the target computer and run the installer.

Load Balancing

As we have seen, the ICENet Server controls all communication between the Control Center and all the enforcers running in your network. It also handles a good deal of the inter-server data transfer within Control Center. For this reason, it represents the most likely performance bottleneck in the system. To improve performance, you may decide to install several ICENet Servers on distributed hosts. If you do this, you must use a load balancer to divide the workload among all ICENet Servers.

You can either set up load balancing when you first install Compliant Enterprise software, or set it up at a later time. Install the load balancer between the desktops or file servers on which policy enforcers are installed and the machines on which the ICENet Servers are installed. Note that you can set up load balancing among many ICENet Servers regardless of whether they are running on separate hosts, or many on the same host.

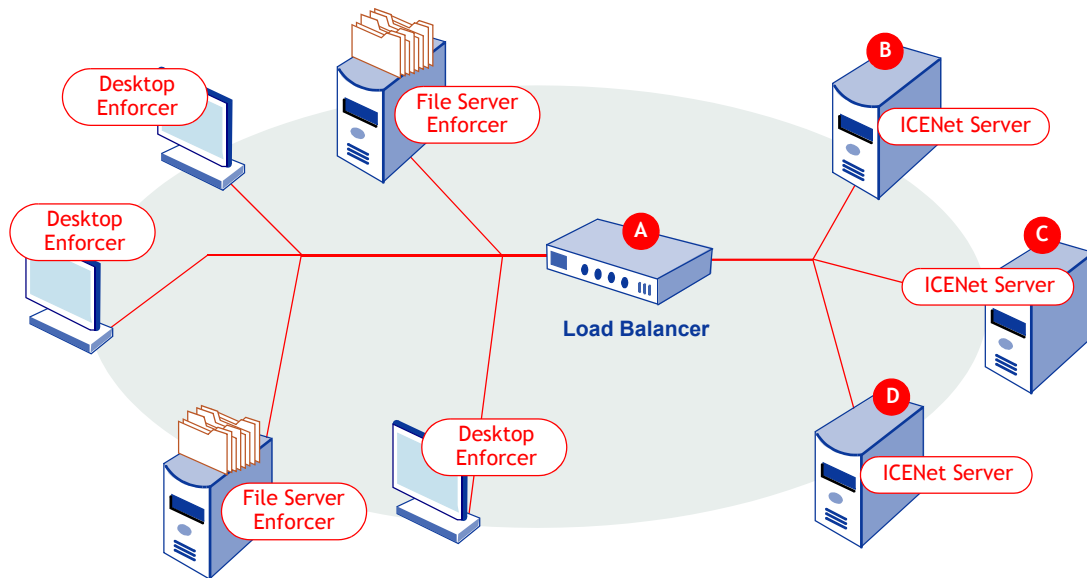


Figure 5-1: Load Balancing ICENet Servers

At Initial Installation

To set up load balancing during your initial installation,

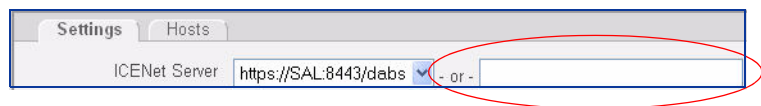
1. Before you install the Control Center, install a load balancer on a separate server host, Server A.
2. Run the Control Center installation wizard. When the wizard prompts you for the location of the ICENet Server, give the virtual IP address or virtual host name of the load balancer, rather than the actual location of the ICENet Server.
3. Install ICENet Server components as required on additional machines—lets's say, hosts B, C, and D.
4. Configure the load balancer on host A to balance requests among machines B, C, and D.

Note that any enforcers you want to use the load balanced ICENet servers, should be configured with the virtual IP address or virtual host name of the load balancer, rather than the actual IP addresses of the ICENet Servers. (For details, see [page 78](#).)

After Initial Installation

To set up load balancing at any point after your initial installation:

1. Install the ICENet Server components on several server hosts.
2. Set up the load balancer so that it refers to the ICENet Servers. Configure the load balancer to use stateless (“non-sticky”) load balancing.
3. Use Administrator to modify all your currently defined policy enforcer profiles, changing the ICENet Server location from its actual location to the load balancer’s virtual IP address or virtual host name. Note that because Administrator cannot autodiscover the load balancer, it will not appear in the list in the ICENet Servers combo-box. You must type it manually in the OR field, as shown.



Note: If you make a mistake when specifying the load balancer location, policy enforcers will not be able to find the load balancer, and won't be able to communicate with the Control Center. This will cause serious problems in your Compliant Enterprise system.

4. Monitor the policy enforcers to ensure that they all receive the new profile.

Note that each policy enforcer will not start using load balancing until it receives the new policy enforcer profile, and the new profile will not likely be communicated to all the policy enforcers immediately. Some of the currently deployed policy enforcers will continue to use the old ICENet Server location until they have received the updated policy enforcer profile.

When all policy enforcers have received the new profile, remove the old ICENet Server host if you are no longer using it. Of course, you have the option of leaving the old ICENet Server in operation and make it part of the server pool behind the load balancer.

Stopping Policy Enforcers

There are occasions when you might want to stop the execution of the policy enforcer on a particular machine without uninstalling it.

Desktop Enforcers

To stop a Desktop Enforcer, you can locally run a special executable called *StopEnforcer.exe*. You can find this at C:\<InstallDirectory>\Windows Desktop Enforcer\public_bin, as shown in [Figure 5-2](#).

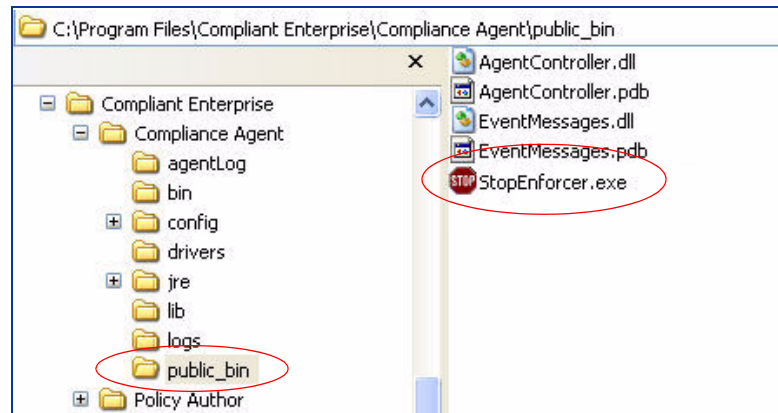
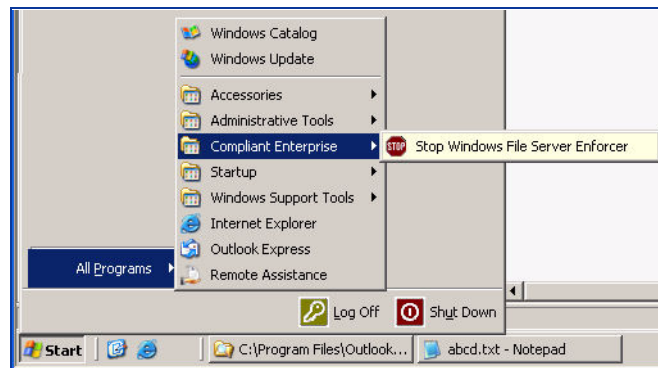


Figure 5-2: Stopping Policy Enforcers

To run this executable, you will need to provide the policy enforcer administrative password, set as part of whichever policy enforcer profile applies to the host where this enforcer is running. Before you can uninstall, you must know which profile is being used on the machine so you can have the appropriate password ready.

File Server Enforcers

The executable that stops a Windows File Server Enforcer is launched from Compliant Enterprise group in the Windows Start, All Programs menu, as shown at right. As with Desktop Enforcers, it prompts you for the password of the profile assigned to the enforcer you are trying to shut down.



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

```
cefse_stop
```

then provide the superuser administrator's password when prompted.

SharePoint Enforcers

The procedure for stopping SharePoint Enforcers is the same as for Windows File Server Enforcers.

Confirming Status

Once you run this executable, it should display a notification window stating that the process was successfully terminated. If you wish, you can positively verify that the policy enforcer software has stopped.

All Enforcers, remotely: Use Administrator to view the list of deployed policy enforcers. The policy enforcer you stopped will still appear in the list, but should no longer be sending heartbeats. For details, see "Policy Enforcer Status" ([page 63](#)).

Desktop Enforcers, locally: The CE icon will continue to display in the Windows system tray, even after the enforcer is stopped. You can right-click on it, select About Desktop Enforcer; the About screen should have a line reading *Enforcer Status: Not Running*.

Windows File Server and SharePoint Enforcers, locally: Open the standard Services window under Control Panel, Administrative Tools, and check the status of the service in the list on the Extended tab.

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

```
cefse_status
```

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

Restarting Policy Enforcers

To restart a Windows enforcer of any type, open the Services window from the Windows Control Panel, Administrative Tools, and restart the corresponding service. As with any Windows service, you must have local administrator privileges to do this. You can also restart the enforcers by rebooting the host machine.

To restart a Linux File Server Enforcer, log into the local host and use the command:

```
service cefse start
```

Uninstalling Policy Enforcers

Before you can uninstall any enforcer you must stop it, as described above ([page 93](#)).

If the policy enforcers were installed using Group Policy Object (GPO), you can remove them the same method, in reverse. In the list of machines that are signed up for automatic managed installation, remove the names of the

machines where you want to uninstall the software. The next time any of those machines is rebooted, the user will see a message indicating that policy enforcer software is being uninstalled, and the machine will auto-reboot. Then the user will be allowed to log in.

If you only want to remove the policy enforcer from a single machine, you can do so using the Add/Remove Programs functionality of the Windows Control Panel. When you request to remove the policy enforcer, you will be prompted for the policy enforcer administration password. This password is set as part of the policy enforcer profile. Before you can uninstall, you must know which profile is being used on the machine so you can have the appropriate password ready. If the policy enforcer was installed via GPO, be sure to also delete the machine name from the GPO installation list, or the software will automatically be reinstalled the next time the machine is rebooted.

To verify that the policy enforcer software has been uninstalled, use the Administrator tool to view the list of deployed policy enforcers. The policy enforcer you uninstalled will still appear in the list, but should no longer send heartbeats.

Reconfiguring Enforcers

For whatever reason—for example, moving a PC from one domain to another—you may need to move a desktop or file server enforcer from one Control Center to another. To do this, you need to reconfigure the enforcer so that it connects to a different ICENet Server. To do this, perform the following procedure:

1. Stop the enforcer you want to reconfigure.
2. On the enforcer host, delete the following four files from the install directory, as shown in [Figure 5-3](#):
 - bundle.bin
 - \config\registration.info
 - \config\security\agent-truststore.jks
 - \config\security\agent-keystore.jks
3. Open the configuration file \config\commprofile.xml, and find the DABSLocation element.
4. Replace the host name within this element with the name of the new ICENet host you want to connect to. For example, change

```
<DABSLocation value="https://Grande:8443/dabs"/>
```

to

```
<DABSLocation value="https://Guernsey:8443/dabs"/>
```
5. Restart the enforcer service.

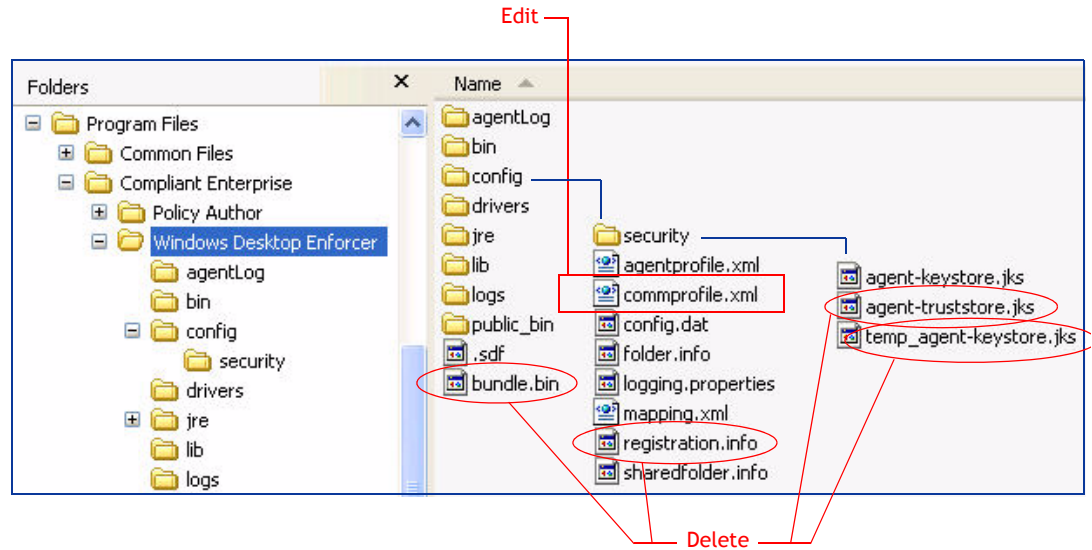


Figure 5-3: Configuring an Enforcer to a new ICENet Server

Policy Enforcer Profiles

An important aspect of managing policy enforcers is defining and assigning enforcer profiles. This is discussed in detail elsewhere in this manual; see "Working with Profiles" ([page 79](#)).

Managing Security Certificates

Two types of security certificates are provided to ensure security throughout Compliant Enterprise:

- Component-to-component certificates provide certification between Compliant Enterprise software components, such as between policy enforcers and ICENet Servers or between distributed Control Center components.
- Web application certificates support HTTPS for the Administrator and Reporter applications.

The provided certificates are issued at the time of installation, are self-signed by NextLabs, and expire in ten years. A set of certificates is issued for each installation. The certificates are kept in a keystore file, whose location is stored in the configuration file *server.xml*.

You might want to replace the provided Web application certificates; for example, if you already have a website of your own and you want to use your own certificates. You can create your own certificates using any certificate generation tool.

To replace security certificates:

1. Place the certificates in a keystore file.
2. Open the configuration file *server.xml* on the machine where one or more Web application server components (Intelligence Server or Management Server) are installed.
3. Find the `<Service>` tag where the Name attribute is "CE-Apps."
4. Find the `<Connector>` tag within that `<Service>` tag, and change the value of its `keystoreFile` attribute to the name of the file where your certificates are stored.
5. Set the `keystorePass` attribute to a new password to protect the security certificates. The password must be encrypted. For information, see "Encrypting Passwords for the Configuration File" ([page 118](#)).

To confirm that the new certificates are in use, open the Web application and click View Certificate.

Database Administration

As we have noted, you have the option of using an external database for storing your Activity Journal and your Information Network Directory data. Both Oracle and PostgreSQL are supported; the installation default is PostgreSQL.

If you are using PostgreSQL, it is a good idea to clean up the database periodically, by running the *vacuum* command. The more you use Compliant Enterprise, the more often you should use this utility—for example, anywhere from once a week to once a month.

The Compliant Enterprise installation package includes the VACUUM executable, which is installed by default in the following location:

```
<InstallDirectory>\Control Center\Repository\bin\vacuumdb.exe
```

The recommended options to use are:

```
vacuumdb -a -U root -W <Administrator password>
```

You must supply the password of the Administrator account.

For more information about what this utility does, refer to the PostgreSQL online help, which you can open from the command line by typing:

```
vacuumdb.exe -?
```


This chapter describes the tools available for modifying the configuration of Compliant Enterprise after it is installed. None of the available configuration settings are strictly mandatory, in that all have default settings that you do not necessarily need to change. However, you may wish to change some settings either during your initial installation, or at any later time.

Note that this chapter describes only those configuration settings you may want to modify, under certain specified conditions. You should not make any changes to settings that are not explicitly described here. All configuration files contain many settings that you should not change; doing so could seriously disrupt the operation of your Compliant Enterprise system.

The chapter is organized into the following sections:

- About Configuration Files
- Configuration Settings ([page 104](#))
- Tomcat Settings ([page 115](#))
- Event Log Settings ([page 119](#))

About Configuration Files

You perform all configuration by editing various Compliant Enterprise configuration files directly, and saving your changes.

The platform uses two main XML files that contain configuration settings you can view or modify in order to tune your system's performance, scale the system by adding or removing modules, or address various administration tasks and issues. The two configuration files are:

- **configuration.xml**: The main configuration file for Compliant Enterprise. This file contains settings for Compliant Enterprise software behavior, such as policy enforcer heartbeat frequency and other settings that are required for the various Compliant Enterprise software components to communicate.
- **server.xml**: The configuration file for the Tomcat application server, which is part of the Compliant Enterprise platform. You will only need to edit this file if you install additional instances of the Tomcat server.

Both files begin with a set of initial configuration settings, which are based partly on responses provided to on-screen prompts during installation, but mostly to default values in the config files. In order to modify those initial settings, or to access settings that are not included in the installation wizards, you can edit the configuration files directly.

Each feature is associated with a section in the file, and focuses on the functions of each information element (marked by its XML tag) in that section. An element may or may not have one or more Properties sections within it, which control aspects of the corresponding feature's operation. [Figure 6-1](#) shows an example of one of these sections.

```
-->
Repository & Connection Pool configuration
<!--
<Repositories>
  <Repository>
    <Name>management.repository</Name>
    <ConnectionPoolName>management.connection.pool</ConnectionPoolName>
    <Properties>
      <Property>
        <Name>hibernate.dialect</Name>
        <Value>net.sf.hibernate.dialect.PostgreSQLDialect</Value>
      </Property>
    </Properties>
  </Repository>
  <Repository>
    <Name>activity.repository</Name>
    <ConnectionPoolName>activity.connection.pool</ConnectionPoolName>
    <Properties>
      <Property>
        <Name>hibernate.dialect</Name>
        <Value>net.sf.hibernate.dialect.PostgreSQLDialect</Value>
      </Property>
    </Properties>
  </Repository>
</Repositories>
```

Figure 6-1: Sample Section from the Configuration.xml File

To change any aspect of your configuration:

1. Open the file with any text editor.
2. Find the setting you are interested in by searching for its tag.
3. Change the value between the open and close tags.
4. Close the file, saving your changes.

The Compliant Enterprise Config File

The main Compliant Enterprise configuration file, *configuration.xml*, is placed on the host machine when you first install the Control Center. It controls the behavior of all Control Center components throughout your system, even if they are installed on different hosts. During installation, the file is placed at

```
<InstallDir>\server\configuration\configuration.xml
```

You can use this file to change the configuration of the following:

- the user repository
- authentication
- Compliant Enterprise components
- data access
- the Information Network Directory

The Tomcat App Server Config File

Compliant Enterprise uses the Tomcat open-source application server to provide a platform for the Compliant Enterprise server components. If you install Control Center server components in a distributed architecture rather than on a single host, Tomcat is installed on each of the host machines.

Every installation of Tomcat has its own configuration file, called *server.xml*. This file informs a given instance of Tomcat about which applications it will be serving on that machine. During installation, the file is placed at

```
<InstallDir>\server\configuration\server.xml
```

The Compliant Enterprise implementation of the Tomcat configuration file contains many standard Tomcat settings, which you can modify to tune your system. For example, you can change the default number of threads and various time-outs. More specifically to Compliant Enterprise, the file contains `<Service>` sections that provide settings for two services, *DCC-Core* and *DCC-Apps*. You must not delete either of these sections, but you can modify some of their properties. For more details, see "Tomcat Settings" on [page 115](#).

Configuration Settings

The main Compliant Enterprise configuration file, *configuration.xml*, is copied to the host server when you first install the Control Center. It controls the behavior of all Control Center components throughout your system, even if they are installed on different hosts. During installation, the file is placed at

```
<InstallDir>\server\configuration\configuration.xml
```

You can use this file to change the settings that control various functions of the system. These include the configurations of the following:

- The User Repository, the logical database where information on users and user groups is stored;
- User authentication ([page 104](#)), external domain authentication ([page 105](#)), and trusted domain configuration ([page 106](#));
- Individual Control Center software components ([page 108](#));
- Connections between Control Center and the four data stores required by Compliant Enterprise ([page 111](#)).

Configuring the User Repository

The settings that capture information about the internal directory server hosting Compliant Enterprise user information are organized in the <UserRepository-Configuration> section. [Table 6-1](#) describes the elements in this section.

Table 6-1: User Repository Configuration Elements

Element	Description
server.name	Name of the machine hosting the User Repository server. This will be the same as the machine hosting the DMS (Management Server).
server.port	Port for the User Repository server. Set by the installer.
useSSL	Specifies whether the server being accessed is SSL enabled.
login.dn	The distinguished name or user principal name (for example, <code>jdoe@bluejungle.com</code>) of the account that will be used to gain access to the user repository. This property is initially set through the Compliant Enterprise Control Center installation wizard.
login.password	Password for the user in <code>login.dn</code> . This property is the same as the Administrator password, which is specified during Control Center installation. The value must be encrypted. For information about how to change the value at any time after your initial installation, see page 118 .

Configuring Authentication

Authentication is the process of checking to be sure that a person who is trying to log in to Policy Author, Administrator, or Reporter is authorized to do so. Compliant Enterprise integrates with the existing security infrastructure, eliminating the need to manage user account information in multiple systems.

Choosing Local or Remote Authentication

Compliant Enterprise supports the following types of authentication:

- **Local** authentication: Users are authenticated directly against Compliant Enterprise’s local Information Network Directory.
- **Remote** authentication: Users are authenticated against a Kerberos server in the organization’s network.
- **Hybrid** authentication: Users are first authenticated against the manually created users within Compliant Enterprise. If no such user is found or if the credentials do not match, the credentials are verified remotely (as in Remote authentication) if an imported user is found with the same login name.

The type of authentication you will use is controlled by the `<AuthenticationMode>` element, which looks like this:

```
<ApplicationUserConfiguration>

    <AuthenticationMode>Hybrid</AuthenticationMode>

    . . .

</ApplicationUserConfiguration>
```

This is initially set during installation. It is set to *Local* if the user skips the Application User Authentication screen during installation, and to *Hybrid* if the user provides the requested information in that screen. If you want to change it manually any time after installation, you can do so by changing this value.

Configuring the External Domain Authentication

Another section, `<ExternalDomainConfiguration>`, contains several properties that are used to configure information about the external domain for user and group information retrieval, and for remote authentication of users logging into Reporter and Administrator. During Compliant Enterprise installation, this section is commented out if the Application User Authentication screen of the installation wizard is skipped.

In this section, the name of the security domain, authentication server, and connectivity information are configured, as follows:

Table 6-2: External Domain Configuration Settings

Element	Description
<code><DomainName></code>	The name of the security domain against which the user will be authenticated. The login name which the user attempts to use must exist within this domain. You can specify only one domain.
<code><AuthenticatorConfiguration></code>	Contains two properties relevant to domain authentication.
<code>java.security.krb5.kdc</code>	Kerberos Domain Controller. The name of the primary domain controller for the domain specified in the <code>java.security.krb5.realm</code> property. The primary domain controller contains credentials for all web application users.
<code>java.security.krb5.realm</code>	The domain name. Should be the same as specified in the <code><DomainName></code> subsection described earlier, except that it must be in all capital letters.

Table 6-2: External Domain Configuration Settings

Element	Description
<code><UserAccessConfiguration></code>	This element has four properties that control connectivity to the Active Directory server hosting the user and group information. These settings allow Compliant Enterprise to display and enroll external users and groups from your organization's domain into Compliant Enterprise.
<code>server.name/server.port</code>	Name and port of the Active Directory server hosting the information.
<code>useSSL</code>	Whether to use SSL when connecting to the Active Directory server.
<code>root.dn</code>	The distinguished name of the root node from which to start retrieval of user/group data entries.
<code>login.dn</code>	The principal name of a user with read privileges on the external domain.

Configuring Trusted Domains

During normal operation, Compliant Enterprise keeps track of users and hosts according to the domain where they are enrolled, for the purposes of preparing policy bundles. It needs this information so that it can include in policy bundles only the information that is relevant to a particular policy enforcement point.

For example, policy bundles deployed to file servers in the `test.widgetco.com` domain need to contain users and hosts only from that domain. Ordinarily, the information about users and hosts from one domain, `widgetco.com`, is irrelevant to file servers in another, `test.widgetco.com`, because the operating system denies logon to users from `widgetco.co`—making it impossible to perform any further actions on file servers of the `test.widgetco.com` domain.

However, there is one important exception. When there is a trust relation between the `widgetco.com` and `test.widgetco.com` domains, file servers from `test.widgetco.com` must know about hosts and users of the `widgetco.com`, and vice versa. Compliant Enterprise will distribute policy bundles correctly across domains in such cases, but only if you inform Compliant Enterprise about any such trust relationships. To do this, you use a configuration setting, `<MutuallyTrusted>`, found in the in the DABS section of the configuration file.

```

<DABS>
  <HeartbeatRate>30</HeartbeatRate>

  <MailServerConfiguration>
    .
    .
  </MailServerConfiguration>

  <TrustedDomainsConfiguration>
    <MutuallyTrusted>publishing.widgetco.com,test.widgetco.com,widgetco.com</MutuallyTrusted>
    <MutuallyTrusted>partners.cyberdyne.com,widgetco.com</MutuallyTrusted>
  </TrustedDomainsConfiguration>
</DABS>

```

Figure 6-2: Sample Trusted Domains Configuration

Each element in this section can contain two or more domains, and represents a trust relationship between or among them. Note the following syntactical points about this section:

- Domains with mutual trust relations are specified as comma-separated lists within the <MutuallyTrusted> tags.
- Each of these lists is logically separate: a domain with more than one trusted relationship may be included in multiple lists, without joining the lists. For example, the sample configuration above creates trust relationships between widgetco.com and partners.cyberdyne.com and between widgetco.com and publishing.widgetco.com, but it does not create a trust relationship between partners.cyberdyne.com and publishing.widgetco.com.
- Empty lists or lists with only one domain will be ignored, but are allowed.
- Blank spaces around commas are ignored; however, blank spaces around dot separators will produce an error.

Configuring Control Center Components

A set of sections in Configuration.xml control the various components of the Compliant Enterprise Control Center. All instances of each software component share the configuration settings of a single section in the configuration file. For example, if you have a distributed system where several ICENet Servers divide the traffic from the policy enforcer software modules in your organization, all the ICENet components use the same configuration.

Table 6-3 lists these sections and the elements and properties in each, and summarizes their functions.

Table 6-3: Configuring Control Center Components

Section	Purpose	Element or Property	Function
<DMS>	Governs the operation of the Management Server	<HeartbeatRate>	Specifies the frequency, in seconds, of the Management Server's own heartbeat signal. This value should not be changed. Minimum = 15; default = 60
		<LDAPPollInterval>	Specifies how often, in seconds, the Management Server queries the Information Network Directory to find out whether there has been a change to enrolled data. Enrolled data is user and host data imported from your organization's Active Directory, as well as enrolled application information. Default = 60
<DCSF>	Governs the operation of the core server framework, which relays information across machines between components, relays license key enforcement, and performs other tasks.	<HeartbeatRate>	Specifies the frequency, in seconds, of the heartbeat signal sent to the Management Server. Minimum = 15; default = 60
<DABS>	Governs the operation of the ICENet Server, which manages communication between the Control Center and all policy enforcers.	<HeartbeatRate>	Specifies the frequency, in seconds, of the heartbeat signal the ICENet Server sends to the Management Server. Minimum = 15; default = 60
		<MailServer Configuration>	Contains settings that control the ICENet Server's connection to your mail server, for e-mail notification purposes.
		<Server>	Specifies the name of the network host where the mail sever is running.
		<Port>	The port where the ICENet will connect to the mail server.
		<MailFrom>	Specifies the content of the From field of all e-mail notifications sent by this server.
		<Username>	The username required for this connection. If your SMTP server does not require authentication, this may be left blank.
		<Password>	The password required for this connection. If your SMTP server does not require authentication, this may be left blank.
		<TrustedDomains Configuration>	Allows you to specify trust relationships among domains in your network. For any trusted domains listed here, policy bundles applying to a file server in one domain will include user and host information for the other domain. This allows Compliant Enterprise to enforce policies across domains (this happens only in the case of trusted domains).

Table 6-3: Configuring Control Center Components (Continued)

Section	Purpose	Element or Property	Function
<DPS>	Governs the operation of the Policy Server, the server for the Policy Author application.	<HeartbeatRate>	Specifies the frequency, in seconds, of the heartbeat signal the Policy Server sends to the Management Server. Minimum = 15; default = 60
		<DeploymentTime>	Specifies the default deployment time for policy enforcers. Value is case-insensitive. (For examples, see Table 6-4 .) Required syntax: [(ordinal last)] [day of week] HH24:MM
<DAC>	Governs the operation of the Intelligence Server, the server for the Reporter application.	<HeartbeatRate>	Specifies the frequency, in seconds, of the heartbeat signal the Intelligence Server sends to the Management Server. Minimum = 15; default = 60
<Management Console>	Governs the operation of the Administrator.	<HeartbeatRate>	Specifies the frequency, in seconds, of the heartbeat signal Administrator sends to the Management Server. Minimum = 15; default = 60
<Reporter>	Governs the operation of the Reporter.	<HeartbeatRate>	Specifies the frequency, in seconds, of the heartbeat signal Reporter sends to the Management Server. Minimum = 15; default = 60

Table 6-4: Examples, Deployment Time Settings

Example	Explanation
00:00	Next midnight (default value of <DeploymentTime>)
wednesday 1:20	1:20 AM every Wednesday
first monday 1:15	1:15 AM on the first Monday of each month
Last Saturday 22:30	10:30 PM on the last Saturday of each month
3rd FRIDAY 0:10	10 minutes past midnight on the third Friday of each month
fourth SATURDAY 12:30	12:30 PM on the fourth Saturday of each month
fifth Monday 23:59	11:59 PM on the fifth Monday of each month

If the required day of the current month has already passed, the corresponding day of the next month is taken. If the next month does not have the specified day (for example, the next February to have the fifth Sunday will be February of 2032) the following month is checked.

The From Address

By default, the From address field in all e-mail notifications contains a dummy value that will not be valid. You can replace this with a real address by manually editing the Control Center configuration file. This is strongly recommended, since it will help you catch any instances when notification messages might bounce back from undeliverable addresses. To define a From address,

1. Open the configuration.xml file for the server your Policy Author is working with.
2. Locate the <DABS> section in the file. ([Figure 6-3](#), below, shows an example of this section.)

3. In the <MailFrom> element, replace the default string with the actual e-mail address you want to appear in the From field.
4. Close the file, saving your changes.
5. Shut down and then restart the Control Center service, so the new configuration can take effect.

The image shows a code editor window with a jagged, torn-paper-like border. Inside, there is an XML configuration snippet. The snippet is as follows:

```
- <DABS>
  <HeartbeatRate>30</HeartbeatRate>
  <MailServerConfiguration>
    <Server>begemot.bluejungle.com</Server>
    <Port>25</Port>
    <MailFrom>HelpDesk@[129.0.0.1]</MailFrom>
    <Username />
    <Password />
  </MailServerConfiguration>
</DABS>
- <!--
```

The line containing the <MailFrom> element is circled in red. The text inside the circle is <MailFrom>HelpDesk@[129.0.0.1]</MailFrom>. The word 'Username' in the line below is crossed out with a red line.

Figure 6-3: Configuring the E-mail From Address

Configuring Data Access

The configuration.xml file also contains settings for connecting to the four databases Control Center requires. Each of these connections is controlled by a group of parameters, in one of the four <repository> sections of the file.

The four databases include:

- **Management Database:** The Management Database contains runtime information such as which components are running, how many policy enforcers have registered with the server, etc. This will always be an internal, PostgreSQL database. The connection to this database is defined in the **management.repository** section of the file, as shown in [Figure 6-4](#)).
- **Policy Master:** The Policy Master contains policy component definitions and policy definitions created by users of the Policy Author application. This will always be an internal, Postgres database. The connection to this database is defined in the **policyframework.repository** section of the file.
- **Activity Journal:** The Activity Journal contains user events, policy enforcement data, and notifications, which are used by the Reporter application. This may be either an internal, Postgres database, or an externally hosted Oracle or Postgres database. It will always be the same location as the Information Network Directory. The connection to this database is defined in the **activity.repository** section of the file.
- **Information Network Directory** The Information Network Directory stores information about directory entities—users, hosts, groups, and so on—that have been enrolled into the Compliant Enterprise system. This may be either an internal, Postgres database, or an externally hosted Oracle or Postgres database. It will always be the same location as the Activity Journal. The connection to this database is defined in the **dictionary.repository** section of the file.

About Connection Pools

The four repository sections contain just a few settings—basically just the <name>, and a pointer to a *connection pool* section, where the actual connection information for that repository is stored. Accordingly, there are four <ConnectionPool> sections, one associated with each of the repositories. [Figure 6-4](#) illustrates this relationship.



Figure 6-4: Configuring Data Access: <Repositories> and <ConnectionPools>

Each <ConnectionPool> section contains six elements, whose functions are explained in [Table 6-5](#).

Table 6-5: Connection Pool Settings

Tag	Description
Name	Name of the connection pool. This name should match the ConnectionPoolName setting in one of the <Repository> sections.
Username	User name for a database account that can access the database specified in the Name property. This property is initially set during installation, when you fill in the database connection screen of the Control Center installation wizard. If you want to change this setting, for example, to change to a user with fewer privileges, you can do so.

Table 6-5: Connection Pool Settings (Continued)

Tag	Description
Password	Password that goes with the user account specified in Username. You can change this password later; for example, if the user changes his password or if you change the user on this data source to a different one. The value must be encrypted. For information about how to change the value, see page 118 .
ConnectionString	For the Management DB and Policy Master, which use Postgres, the database connect string will be in the PostgreSQL format <code>machine:port/databaseName</code> The other two databases, Activity Journal and the Information Network Directory, may use either Postgres or Oracle. The host and port are initially set during installation, but you can change the machine and port in the connect string at any time after installation—for example, if you move the database server to a different machine.
DriverClassName	Name of the database driver used by this connection. Valid values are: Postgres: <code>org.postgresql.Driver</code> Oracle: <code>oracle.jdbc.driver.OracleDriver</code>
MaxPoolSize	Sets a maximum number of connections that are simultaneously available for accessing this data source from a given Control Center instance. For more detail on using this setting, see below.

Adjusting Connection Pool Size

The last element, `<MaxPoolSize>`, specifies the maximum number of simultaneous data connections available for each of the four databases. By default, the values for this setting are not the same for each of the four connection pools. They are:

- `management.connection.pool` (for the Management DB): **8** connections;
- `policyframework.connection.pool` (for the Policy Master): **8** connections;
- `activity.connection.pool` (for the Activity Journal): **20** connections;
- `dictionary.connection.pool` (for the Information Network Directory): **14** connections.

Note that the sum of these connections is 50, which is half the maximum supported by Compliant Enterprise's internal Postgres database. This is based on the common installation architecture of one physical host for the ICENet Server, and one for all other Control Center components: two server hosts x 50 connections apiece, matches the database's own default limit.

The way these 50 are divided among the four pools is based on the relative amounts of database activity you can anticipate for each repository, during normal use. If you need to adjust these settings you can do so by editing these connection pool definitions, but remember that you can only reallocate them from one pool to another. That is, if you increase the max for one pool, you should decrease it for another, so that the total doesn't exceed 50 (in the case of the internal Postgres database; this may be different for external databases).

When to Adjust

You will need to reallocate connections whenever the operational requirements for one of the repositories start exceeding the number of connections allocated. When this happens, database operations for that repository will begin timing out, producing the following error message in your system log:

```
java.sql.SQLException: An attempt by a client to checkout a Connection has timed out.
```

The Database Connection Bottleneck

Bear in mind, these maximum connection values apply per each server instance, rather than to the Control Center as a whole. If you install multiple ICENet Servers, each will have the same default number of connections to access each given repository. Therefore, the sum total of maximum available connections to a given data source is $(N * \text{MaxPoolSize})$, where 'N' is the number of ICENet Servers you are running. (This does not mean that all these connections will be used; some ICENet Servers might not use all the provided data sources.) The total connections will be $50 * (\text{the number of servers you deploy})$.

However, the databases themselves support only a finite, maximum number of connections. Compliant Enterprise's internal Postgres database supports 100 connections; if you are using an external Postgres or Oracle database, it may support a different number. This means that if you deploy multiple ICENet Servers, it is possible that the number of their combined connection pools will exceed the actual capabilities on the database side. In such cases, you will see an error message like the following in your log:

```
org.postgresql.util.PSQLException: Backend start-up failed: FATAL: sorry, too many clients already.
```

If you are using an external database, you should know what its connection maximum is, and make sure that you do not exceed it by the aggregate connection pools of all ICENet servers in the system. You can do this either by increasing it on the database side, or reducing your configuration.xml connection pool sizes to something below the default levels.

Changing Database Connect Strings

If you change the database name portion of the connect string, be extremely careful. This part of the connect string must match the name of the database itself. There is no reason to change the names of the Management and Policy Master repositories, because these are set up by the installer and are managed internally by Compliant Enterprise. However, the Activity Journal and the Information Network Directory can be managed externally, and in this case you might need to change their connect strings.

Tomcat Settings

Compliant Enterprise's UI applications work through the Tomcat web-based application server, included in every Control Center installation. During installation, all required configuration settings are supplied by prompts in the install wizard, and all optional ones are assigned with default values. Accordingly, there is no technical need to change any configuration settings after installation, but they are available if you ever have need of them. This section provides details about all available configuration settings, both required and optional.

Location

The settings described in this section can be changed by opening and editing the Tomcat configuration file. During installation, this file is placed on the target host, at

```
<InstallDir>\ControlCenter\server\tomcat\conf\server.xml
```

If you distribute the components of Control Center, this host will be the one where the Management Server is installed.

Config File Structure

The Tomcat configuration file contains two Service sections with the following names:

- **DCC-Core** contains settings for the core server framework, which relays information across machines between components, relays license key enforcement, etc.
- **DCC-Apps** contains settings for Compliant Enterprise web applications (Administrator and Reporter).

You can find these sections in the file by searching for the tags `<Service name="DCC-Core">` and `<Service name="DCC-Apps">`. Both contain the following subsections, containing additional settings:

- `<Connector>`
- `<Host configuration>`
- `<Default Context for Components>`
- `<Component Context Settings>`

[Table 6-6](#), below, describes the function and use of the settings available in each of these sections.

Table 6-6: Connector Section Properties

Setting	Description
port	<p>If you want to change the port number later, you must propagate the change consistently to any other settings that refer to the same port. Be sure to update the port property in every Tomcat configuration file throughout your organization. You must also update the value wherever it is used in other properties throughout the file (for example, DCLocation) so that other components can start to communicate using the new port. It is recommended that you do this by examining each property one by one, rather than by using a global “search and replace” strategy. Remember that you must bounce Tomcat before the new settings will take effect.</p> <p>In addition, if you are using load balancing and you change the application port number, you will need to inform the load balancer of the new location.</p> <p>If you do not properly reconfigure all components, the fact that one or more is unable to connect should be apparent from a message in the log file. Similarly, if you choose a port number that is already in use by a different application, and a port conflict arises, this should be reflected in the log file.</p>
keystoreFile	Specifies the path to the keystore file where the security certificate is stored. In the DCC-Apps section, keystoreFile, keystorePass, and keystoreType are useful when you want to exchange the supplied Web application security certificates for certificates of your own. It is not recommended that you change this setting within the DCC-Core section, which configures the security certificates for communication between components of Compliant Enterprise. For information about security certificates and how to change them, see “Managing Security Certificates” on page 41.
keystorePass	The password used to access the server certificate from the specified keystore file. This password is encrypted during installation. If you later change the password, you must run the encryption utility to re-encrypt the password (see page 118).
keystoreType	The type of keystore file to be used for the server certificate. The value should always remain set to “JKS” for Java Key Store.
truststoreFile	Contains a list of trusted entities. Do not change this setting; however, you might need to look at the value to find out where the truststore file is located.
truststorePass	The password used to access the server certificate from the specified truststore file. This password is encrypted during installation. If you later change the password, you must run the encryption utility to re-encrypt the password (see page 118).
truststoreType	The type of truststore file to be used for the server certificate. The value should always remain set to “JKS”.
clientAuth	<p>To keep your server secure, the connector for the web service port should always have this attribute set to true.</p> <p>When true, the clients of this service that make an application request must be authenticated (by verification of a valid certificate chain) before a connection is made. This ensures that only trusted clients ever make requests to Compliant Enterprise Control Center internal applications.</p>
maxThreads	The maximum number of request processing threads to be created, which determines the maximum number of simultaneous requests that can be handled.
minSpareThreads	The number of request processing threads that will be created when this connector is first started. The connector will also make sure it has the specified number of idle processing threads available.
maxSpareThreads	The maximum number of unused request processing threads that can exist at any given time. If this number is exceeded, the thread pool will stop the unnecessary threads.
enableLookups	Set to true in order to perform DNS lookups to return the actual host name of the remote client. By default, for performance improvement, this value is set to false.
acceptCount	The maximum queue length for incoming connection requests when all possible request processing threads are in use. Any requests received when the queue is full will be refused.
connectionTimeout	The number of milliseconds this connector will wait, after accepting a connection, for the request URI line to be presented.
scheme	The name of the protocol to be used. To keep the server secure at all times, the value should always be “https” and should not be changed.
secure	
Host configuration	The <Host> section within each <Service> section contains the following properties to configure the host of the service:

Table 6-6: Connector Section Properties (Continued)

Setting	Description
Name	The virtual host name. This value should remain set to “localhost” at all times.
autoDeploy	Determines whether new Web applications added to the appBase directory while Tomcat is running should be automatically deployed. Since no new Web applications are expected while Tomcat is running, this value can remain set to false.
unpackWARs	Set to true if you want Web applications that are placed in the appBase directory as Web application archive (WAR) files to be unpacked into a corresponding disk directory structure. Set to false to run such Web applications directly from a WAR file. Default: false.
xmlValidation	Set to true if you want to enable validation of XML configuration files validation. Default: false.
appBase	
Default Context for Components	The <DefaultContext> section configures server resources shared by all Compliant Enterprise components. You should never modify any of these settings.

Table 6-7: The Component Context Section

Setting	Description
<Context>	
The configuration file contains one <Context> section for each Control Center component that is installed on this host; normally there will only be one. The file may contain other <Context> sections that are commented out; these allow you to add more Control Center components later simply by uncommenting the appropriate <Context> section(s). Note: Do not comment out the <Context> section for DCSF. Every machine must have this component.	
path	The context path of this Web application, which is matched against the beginning of each request URI to select the appropriate Web application for processing. For example, when path=“/administrator”, this <Context> section contains settings for the Administrator application. Each context path value must be unique. In the DCC-Core service, the context path values should not be changed, as Compliant Enterprise expects these values to be present. In the DCC-Apps service, you can change the Web application context paths to different values; for example, “/console” instead of “/administrator”. When path=“/reporter”, this <Context> section contains settings for the Reporter application. This <Context> section has no ComponentName property, because the Reporter application is not always part of the Compliant Enterprise installation; it could be replaced by a custom application built using the Compliant Enterprise API. Therefore, Reporter can not necessarily be monitored using the Administrator application, and therefore does not need a display name for use on screen in that application.
reloadable	Set to true if you want to monitor classes in /WEB-INF/classes/ and /WEB-INF/lib for changes and automatically reload the Web application if a change is detected. To optimize the server performance, this value should be set to false at all times.
docBase	Absolute path name to the application Web Archive (WAR) file. This value is set at installation based on the Compliant Enterprise Control Center installation location. This value should not be changed.
workDir	Path name to a scratch directory to be provided by this context for temporary read-write use by servlets within the associated Web application. This value is set at installation based on the Control Center installation location. This value should not be changed.
ComponentName Parameter	The value, in the format machine_component, is the component name that will display in Administrator. A default name is provided during installation. You can change this value, but it must be unique over all Tomcat configuration files. That is, no two Control Center component instances can have the same component name.
Location Parameter	The location where the component can be reached. This value is set at installation and should not be modified.
DACLocation Parameter	Used only where path=“/reporter”. Specifies the location of the Intelligence Server (DAC) as part of the settings for the Reporter application. If you have installed multiple instances of the Intelligence Server and are using a load balancer to distribute Reporter requests among them, change the value of DACLocation to the location of the load balancer.

Encrypting Passwords for the Configuration File

Whenever you generate a new password for the configuration file, you should encrypt it using the following procedure:

1. Open a console window.
2. Change directories to <InstallDir>/tools.
3. Run the following command, where <password> is the new password you want to place in the configuration file:

```
mkpassword.bat -p <password>
```

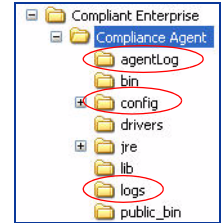
4. An encrypted version of the password appears on the screen. The encrypted value is random; if you run the command again for the same password, a different encrypted version will be generated.
5. Copy the encrypted password from the screen and paste it into Configuration.xml at the desired location.

Event Log Settings

Compliant Enterprise has an extensive event logging mechanism that can captures all events relevant to policy enforcement. Each log is associated with one installation of a policy enforcer, and all events are captured in a log file. By default, these files are maintained on the local host, at

`<InstallDir>\agentLog`

Since you use Reporter to generate reports on system events and the performance of enforcers, you will usually not have any need to use these files directly. One exception might be during troubleshooting, in which case you should follow instructions from Compliant Enterprise technical support representatives.



Desktop Enforcer Logging

If you do not change any log settings for Desktop Enforcers, the default behavior will be as follows:

- Level of verbosity = Severe
- max size of file = 500K

If you wish to change any of this behavior at any time, you can edit the file `logging.properties`, in the `config` directory. The available levels, in order of increasing verbosity, are:

- Severe
- Warning
- Info
- Fine
- Finest

For details on changing these settings, see the “Enforcer Administration” chapter of the *Compliant Enterprise 2.0 Enforcers Administrator’s Guide*. Note that if a Desktop Enforcer is running, it will prevent you from opening any of the local configuration files. To edit them, you must first stop the enforcer (see [page 93](#)).

Defining Custom Properties

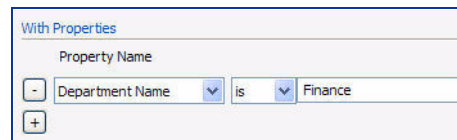
This chapter describes the procedures for defining custom properties for various kinds of entities you define as components in Policy Author. It is organized into the following sections:

- User, Host, and Group Properties
- Document Properties ([page 125](#))
- Portal Content Properties ([page 129](#))

Note that you cannot define custom properties for Application or Action components.

User, Host, and Group Properties

Each of the three LDAP entity types Users, Hosts and Groups has a default set of properties (technically, LDAP attributes), which display in Policy Author in the Property Name combo-box list. These are stored in internal tables in the Information Network Directory. Each property has both a logical name, which is the actual column name in the database table, and a display name, which is the label that shows in the combo-box list. (Host properties are displayed in the combo-box list for Computer components.)



[Table 7-1](#) describes the default properties available for defining Computer components. [Table 7-2](#) describes the default properties available for defining User components.

Table 7-1: Computer Components: Default Properties

Property	Description
DNS Host	Name of this computer, which the DNS uses for resolving IP addresses in order to find this computer in the network.
Machine Name	The permanent name assigned to this computer.
Network Address	The network name assigned to the PC, which will be resolved by a DNS. You may also use the direct numeric IP representation.
Operating System	Operating system of this computer.
Site	The name of the site where the desktop is located. Sites are defined as one or more ranges of IP addresses.

Table 7-2: User Components: Default Properties

Property	Description
Account Name	Account with which this user is associated.
Company	Company with which this user is associated.
Country Name	Country of this user.
Department Name	Department with which this user is associated.
First Name	This user's first name.
Full Name	This user's whole name.
ISO Country Code	The ISO code of this user's country.
Last Name	This user's last name.
Numeric Country Code	Numeric code of this user's country.
Title	Title assigned to this user: Mr., Mrs., Ms., Dr., etc.
User Principal Name	This user's LDAP principal name—a unique identifier for a user in Active Directory, typically in the form of an e-mail address; for example, jdoe@yourcompany.com.

About Property Manager

If you want to define additional, custom properties for either User or Computer components, or for user or host groups, Compliant Enterprise provides a utility called Property Manager (propertymgr.bat). The Property Manager, like the Enrollment Manager, is automatically installed on the Control Center host, at

Program Files\Compliant Enterprise\Control Center\tools\enrollment

[Table 7-3](#) describes the three functions of this tool; for explanations of all arguments, see [Table 7-4](#).

Table 7-3: Property Manager: CLI Commands

Command	Use	Full Command String	See:
add	Add a custom property to users, hosts or applications	propertymgr add -s <server> -p <port> -u <ceuser> -w <cepwd> -t <type> -l <logicalname> -i <displayname> -e <entitytype>	page 123
delete	Delete a property from users, hosts or applications	propertymgr delete -s <server> -p <port> -u <ceuser> -w <cepwd> -l <logicalname> -e <entitytype>	page 124
list	List all current properties of users, hosts and applications	propertymgr list -s <server> -p <port> -u <ceuser> -w <cepwd>	page 124

Table 7-4: Property Manager: Command Arguments

Argument	Description
-s <server>	The name or URL of the host where your Control Center is running.
-p <port>	The port of the Control Center host—8443, by default.

Table 7-4: Property Manager: Command Arguments (Continued)

Argument	Description
-u <ceuser>	User name of a Compliant Enterprise user with administrator privileges.
-w <cepwd>	The Compliant Enterprise utility password. (For details, see page 148 .)
-l <logicalname>	The logical name of the property you are adding or deleting. This is the actual column name in the internal data tables; it must be unique, and may not include spaces or special characters.
-i <displayname>	The display name you want to assign to the property you are adding. This is the string that displays in Policy Author, in the list in the Properties combo-box. It is cap-sensitive, and may contain spaces.
-t <type>	Specifies the data type of the property you want to add; valid values are <i>string</i> , <i>cs-string</i> , <i>number</i> or <i>date</i> . Used only with the <i>Add Property</i> command.
-e <entitytype>	Specifies the type of entity to which you want to add a property; valid values are <i>user</i> , <i>host</i> , or <i>application</i> . Used only with <i>Add Property</i> command.

Adding Properties

You can use the *Add* command to add a new property to users, hosts, and groups. (Of course, this procedure applies only to Compliant Enterprise; any properties you add should also be supported by your LDAP back end.) Whenever you add a property, you must specify the entity type—that is, whether it is a new property of users, hosts, or groups—and supply both a logical name and a display name.

To use this feature,

1. On the host where the Management Server component of the Compliant Enterprise Control Center is installed, open a console window.
2. Change to the directory <InstallDir>\tools\enrollment. By default, this is:

```
Program Files\Compliant Enterprise\Control Center\tools\ enrollment
```

3. At the prompt, run the *Add* command as follows, filling in the appropriate values for the arguments:

```
propertymgr add -s <server> -p <port> -u <ceuser> -w <cepwd>
-l <logicalname> -i <displayname> -e <entitytype>
```

Once the property has been added, you will see a confirmation message.

4. In order to add the new property to the appropriate table in the Information Network Directory, you have to edit the default defini-

tion file to include the new property as an element in the Attribute Mappings section (see [Figure 1-3](#) on page 25).

5. Next, run the Enrollment Manager's standard *Update* command, as described on [page 33](#). This step updates the table structure, but does not import the actual data values to for the new property.
6. To import the data values, run the Enrollment Manager's standard *Sync* command, as described on [page 35](#). When this finishes running, the new property is available for constructing components in Policy Author. You can confirm this by opening Policy Author and opening the Properties combo-box list for a user or host component, or a group. If you wish, you can use the *List Properties* command to check your addition.

Deleting Properties

You can use the *Delete* command to delete a property from any type of entity. You must specify the logical name of the property, and the entity type. To use this feature,

1. On the host where the Management Server component of the Compliant Enterprise Control Center is installed, open a console window.
2. Change to the `\enrollment` directory.
3. At the prompt, run the *Delete* command as follows, filling in the appropriate values for the arguments:

```
propertymgr delete -s <server> -p <port> -u <ceuser> -w <cepwd>  
-l <logicalname> -e <entitytype>
```

Once the properties have been deleted, you will see a confirmation message. If you wish, you can use the *List Properties* command or Policy Author to check the deletion.

Listing Properties

You can use the *List* command to display a list of all properties currently defined for all three entity types. To use this feature,

1. On the host where the Management Server component of the Compliant Enterprise Control Center is installed, open a console window.
2. Change to the directory `<InstallDir>\tools\enrollment`. By default, this is:

```
Program Files\Compliant Enterprise\Control Center\tools\  
enrollment
```

3. At the prompt, run the *List Properties* command as follows, filling in the appropriate values for the arguments:

```
propertymgr list -s <server> -p <port>
-u <ceuser> -w <cepwd>
```

All properties will display in a single list, sorted by entity type. Each line shows the data type, logical name, display name, and data type. The display format is:

```
<TYPE>.<logicalName> - <displayName>: <dataType>
```

Document Properties

Table 7-5, below, describes the default properties available for defining document components. These are the properties that will display by default in the Property Name combo-box for document components, in Policy Author.

Table 7-5: Document Components: Default Properties

Property	Description
Access Date	The date and time the document was last opened.
Created Date	The date and time the document was created.
Full Name	The name of the document, without the directory path but including the extension.
Include Only Directories	This is a special property that allows you to control how any policies with this component will handle directories.
Modified Date	The date and time the document was last modified.
Type	The type of the document (i.e., its extension).
Directory	The full name of the directory where the document is located.
Owner	The owner of this file.
Owner User Component	Name of the user component of which the owner of this file is a member.
Owner LDAP Group	The name of an LDAP or Active Directory group of which the owner of this file is a member. This is the name of a group that has been enrolled with the Information Network Directory. The value should be specified as a principal name in the format company.com:Groups:Group Name.
Size	The size of the document, expressed in bytes.

Compliant Enterprise allows you to define custom properties and attach them to document components. This feature is very useful in combination with third-party content analysis tools that can scan the content of documents and categorize them based on, for example, the presence of sensitive strings such as account numbers or other personal information. You might run such a tool to identify all files with such confidential content, then add a custom property to those files, “IsConfidential = Y”. You could then define a document component called *Confidential Files* (*.*, With Properties: IsConfidential is Y), and then write policies using this component.

The values for custom properties can be any data string—for example, “Export = USOnly | NorthAmOnly | NorthAmEUOnly.” Once defined, the property is available in the Properties combo-box list in Policy Author, along with the default properties like File Size and Owner.

Note that the properties you define in this way are valid for NTFS file systems only; they will not be usable in a Linux environment, and they will not correspond to the OLE properties that are accessible on a file’s Properties tabs in Windows.

In addition, bear in mind the following two caveats:

- Whenever a file with custom properties is sent as an e-mail attachment, the properties are stripped from it and will no longer be available for policy enforcement.
- When you attach custom properties to a file, the file’s Last Modified date is changed to reflect that operation. This may create problems or unexpected behavior in enforcing policies that include document components based on the Last Modified property.

Defining Custom Document Properties

Adding custom documents properties involves two steps: attaching the property to the files themselves, once you have identified them using some 3rd-party tool; and then exposing the property for use in Policy Author. For the first, you use a utility called Custom Attribute Setter (*customAttrSetter.exe*); for the second, you need to edit the configuration file *configuration.xml*.

All the files you want to mark with a custom property must be located on the same host, and you run the Custom Attribute Setter on that host. If the files are located on different hosts, you must run the utility on each one for the files there.

1. By whatever means you like, identify the files you want to mark with a custom attribute. This may be done with a content-analysis tool, or in any other way that suits your purposes.
2. Create a plain-text input file that simply contains a list of these files, one per line. For example, you might call this input file *confidentialFiles.txt*.
3. Copy this input file to the host where the files you want to mark are located.
4. Copy the Custom Attribute Setter to the same host. (You can find the utility on the Compliant Enterprise installation CD, in the Tools directory.)

5. On that host, open a command line window and run the *customAttrSetter.exe*, supplying the arguments shown below.

```
<LocationCopiedTo>\customAttrSetter.exe <InputFile.txt> <attribute> <value>
```

In this command,

- *<InputFile.txt>* is the plain text input file you created; for example, *confidentialFiles.txt*
- *<attribute>* is the name of the attribute you are adding; for example, *IsConfidential*
- *<value>* is the value of the attribute, for these files; for example, *Y*

When the utility finishes running, all files listed in your input file will have this new attribute, with the specified value.

6. Next, open the *configuration.xml* file on the Control Center host, locate the *<CustomAttributes>* section within *<DPS>*, and add a *<ResourceAttribute>* section to describe the attribute you are adding. As [Figure 7-1](#) shows, this section has three required elements:
 - *<DisplayName>* is the name that will display in the Policy Author properties combo-box;
 - *<Name>* is the name of the attribute, as you defined it with the *-a* argument in the Set Attributes utility. Note that you must prepend this value with *document:* as shown in the example below; this is required to differentiate between custom properties of document and those of other types of resources, such as portal content. (All kinds of resources are listed together in this section of the config file.)
 - *<Type>* is the data type of this attribute; currently *STRING* is the only supported type.
7. Close the configuration file, saving your changes, and restart the Management Server.



```

<DPS>
.
.
.
  <CustomAttributes>
    <ResourceAttribute>
      <DisplayName>Confidential</DisplayName>
      <Name>document:confidentialMarker</Name>
      <Type>STRING</Type>
    </ResourceAttribute>
    <ResourceAttribute>
      <DisplayName>Keyword</DisplayName>
      <Name>portal:CompletedDate</Name>
      <Type>STRING</Type>
    </ResourceAttribute>
  </CustomAttributes>
.
.
.
</DPS>

```

Figure 7-1: Defining Custom Document Properties

At this point when you open Policy Author, the new attribute is available to use in defining document components. To test it, create a new document component and drop down the Property Name combo-box.

You can define multiple custom attributes in the configuration file (the example in [Figure 7-1](#) has one for documents and one for portal content), and all will display in Policy Author. However, when you actually attach attributes to files, you must do so one at a time. That is, you must run the Set Attribute utility separately for each attribute you want to add. Also, you can only set one value at a time for all files; if you want to define an attribute and assign different values to several sets of files, you must run the utility repeatedly for those as well.

Portal Content Properties

Table 7-6, below, describes the default properties available for defining portal content components. These are the properties that will display by default in the Property Name combo-box of the component definition, in Policy Author.

Table 7-6: Portal Content Components: Default Properties

Property	Description	Allowed Operators
Created	Date when the content item was created.	'after', 'on or before'
Created by	User who initially created the content item.	'is', 'is not'
Description	Text description of the content item, if one has been supplied.	'matches', 'contains'
File Size	The file size of the content item.	'=', '>', '<', '>=', '<=', '!=', '!='
Modified	Date when the content item was most recently modified.	'after', 'on or before'
Modified by	User who most recently modified the content item.	'is', 'is not'
Name	The file name of the content element. Wildcards are supported.	'is', 'is not'
Sub-type	Sub-type of the content item; required only for types List Item and Library Item. Valid values include ??	'is', 'is not'
Title	The title string that has been applied to the content item. Wildcards are supported.	'is', 'is not'
Type	Type of content item. Valid values include: <ul style="list-style-type: none"> • Portal • Site • Web page • Portlet • Library item? • List item? • CLARIFY THIS! 	'is', 'is not'

Defining Custom Portal Properties

As with other component types, you can define custom properties for portal content components. You define the properties as you work in the portal itself—for example, by adding a list or a library in SharePoint.

In the course of day-to-day work in a portal, users may define large numbers of custom properties. (After all, the structural flexibility and decentralized control of portals is an important part of their collaborative value.) For this reason, you may not want to expose all custom properties in Policy Author, since the Property Name drop-down list could become unmanageably long. To help with this, the Property Name field is an open text input, where the user can type any property name he wants. This means that any custom property that has been defined in the portal can be used in policies, whether it is exposed in the Property Name drop-down list or not.

For whichever custom properties you do want to expose in Policy Author,

1. Open the *configuration.xml* file on the Control Center host, locate the `<CustomAttributes>` section within `<DPS>`, and add a `<ResourceAttribute>` section to describe the attribute you are adding. As [Figure 7-2](#) shows, this section has three required elements:
 - `<DisplayName>` is the name that will display in the Policy Author properties combo-box.
 - `<Name>` is the name of the attribute, as you defined it in the portal. Note that you must prepend this value with “portal:” as shown in the example below; this is required to differentiate between portal content properties and those of other types of resources, such as documents. (All kinds of resources are listed together in this section of the config file.)
 - `<Type>` is the data type of this attribute; currently `STRING` is the only supported type.
2. Close the configuration file, saving your changes, and restart your Control Center.

```

<DPS>
.
.
.
  <CustomAttributes>
    <ResourceAttribute>
      <DisplayName>Confidential</DisplayName>
      <Name>document:confidentialMarker</Name>
      <Type>STRING</Type>
    </ResourceAttribute>
    <ResourceAttribute>
      <DisplayName>Keyword</DisplayName>
      <Name>portal:CompletedDate</Name>
      <Type>STRING</Type>
    </ResourceAttribute>
  </CustomAttributes>
.
.
.
</DPS>

```

Figure 7-2: Portal Content: Custom Properties

At this point when you open Policy Author, the new attribute is available to use in defining portal content components. To test it, create a new portal content component and drop down the With Properties combo-box.

You can define multiple custom attributes in the configuration file, for different kinds of resources. The example above has two, one for documents and one for portal content. All will display in Policy Author, for their respective component types.

Using Custom Obligations

This chapter explains how you define custom obligations and use them to enormously expand the power of information control policies. It includes the following topics:

- About Custom Obligations
- Writing Custom Obligations ([page 134](#))
- Configuration ([page 135](#))
- Design Considerations ([page 137](#))

About Custom Obligations

As we have explained earlier, the practical result that ensues when a policy resolves to true is referred to as the policy's *obligation*. By default, the standard structure of a Compliant Enterprise policy allows you to specify three kinds of obligations: write the event to a log, display a notification to the end user, and send an e-mail to one or more specified targets. With release 2.0, Compliant Enterprise supports a fourth option, custom obligations.

A custom obligation is a custom-defined executable program—an .exe file or a script—that is invoked when the policy with which it is associated resolves to true. The possibilities for what this might specifically involve are very broad; examples include prompting the end user to encrypt some resource before proceeding, notifying some administrator by pager, or offering the blocked end user to e-mail a network administrator, requesting access. Basically, anything that can be handled by an executable program or script, and runs as a non-authenticated session (that is, as a local system user, in background), can be called as a custom obligation. Note that this does *not* include batch files, shell command lines, or graphical user interfaces.

Custom obligations are enforced in the following sequence:

1. Any enforcer in the system enforces a policy that has a custom obligation defined for it. It may be either an On Allow or On Deny obligation.
2. Based on the obligation's display name, included in the policy, the enforcer checks the configuration file to map the display name to the executable's full name and install path. (The executable must be installed on the same host as the enforcer.)
3. The enforcer (specifically, the PDP within it) then passes a set of arguments to the executable. The first of these arguments is the command

that invokes the executable; the others provide information about the event that was enforced against—what action was attempted, by whom, on what host, at what time, and so on.

4. The executable is invoked by the command argument, and performs its special function, incorporating the arguments it was passed: sends a message to the specified user, compresses the specified file, etc.

Accordingly, custom obligations require the following components:

- The executable itself, which is written independently of Compliant Enterprise or Policy Author. It may be an .exe or a script, and must be installed on every host where enforcers are installed.
- The custom obligation must be specified in any policies that should trigger it. This is just a display name, such as “Encrypt,” “Compress,” or “Delete All.”
- The *configuration.xml* file must be edited to include a section for each custom obligation. This is where the enforcer maps the obligation’s display name to the actual executable name (this is the <command> argument), and it is how the enforcer knows the path to the executable. As always, the Control Center must be restarted before any config file changes will take effect.

In addition, custom obligations can only be enforced on release versions of enforcers that support this feature (see Table 2-1 on [page 10](#)).

Writing Custom Obligations

You must design and code the custom obligations outside of Compliant Enterprise. There are several points to bear in mind if you want to take advantage of custom obligations:

- The executable you design must expect a call with the following format:

```
% <command> <argument1> <value> <argument2> <value> . . . <argumentN> <value>
```

- The executable should be expecting a list of the command-line arguments containing at least the following. That is, it need not use all of them, but it should be able to handle them:
 - CEstimestamp <timestamp>: Date and time at which the action was requested (time has .1 second precision)
 - CEaction <action>: The action that triggered the enforcement
 - CEuser <user>: Login name of the user requesting the action
 - CEhost <host>: Full name of the host the user is logged onto
 - CEsitename <site>: Site the host is currently plugged in

- CEapp <path/app_exe>: The application, with path, which attempted the action. Path uses forward slashes.
 - CEsouce <source>: Resource the action was applied to (source)
 - CEdest <destination> [optional]: If logically appropriate, the destination resource
- Optionally, you can include additional application-specific arguments. They can be added using any syntax, space delimited, as in the example above. You must define these in the configuration file section for each custom obligation (see below).

Configuration

For each custom obligation you want to use in any policy, you must add a <CustomObligations> subsection to the DABS section of the configuration file, *configuration.xml*. Each such subsection must contain the three elements shown in the [Figure 8-1](#); descriptions of each are provided below. Note that the sequence of these three elements is very important, and must not be altered.

```

<DABS>
.
.
.
<CustomObligations>
  <DisplayName>obligation1Name</DisplayName>
  <RunAt>PDP</RunAt>
  <ExecPath>obligation1Path</ExecPath>
</CustomObligations>

<CustomObligations>
  <DisplayName>obligation2Name</DisplayName>
  <RunAt>PDP</RunAt>
  <ExecPath>obligation2Path</ExecPath>
</CustomObligations>
.
.
.
</DABS>

```

Note: Do not change the sequence of these three elements

Figure 8-1: Configuring Custom Obligations

- **DisplayName:** This is the shorthand name for the obligation, which can be typed into the Custom Obligation Name field in the policy you want to associate this obligation with.
- **RunAt:** This is reserved for future use; “PDP” is currently the only supported value.

- **ExecPath:** This is the full path and name of the executable, plus any arguments, delimited by spaces. For example:

```
<ExecPath>"C:\encryption tools\encryptfile.vbs RC4"</ExecPath>
```

Path and file of executable

Argument

Note that any value that includes one or more spaces must be enclosed in double quotes, as shown.

As with any time you edit the config file, you must restart the Control Center before your changes will take effect.

Application-Specific Arguments

If you want to define additional arguments that are used by your executable, you must specify them at the end of the ExecPath element in the configuration file. This feature allows you to leverage an executable you define once but use in slightly different ways in many different custom obligations.

For example, you may write a script, *SendPageAlert.exe*, that composes a pager message and sends it to some administrator whenever some policy is enforced. The message might include the action that triggered the enforcement, and the user who performed the action; this information is provided by the enforcer and can be inserted using variables. However, you might want to send the alert to Jeff Jones in certain cases, and to Lois Smith in other cases, depending on what policies are enforced.

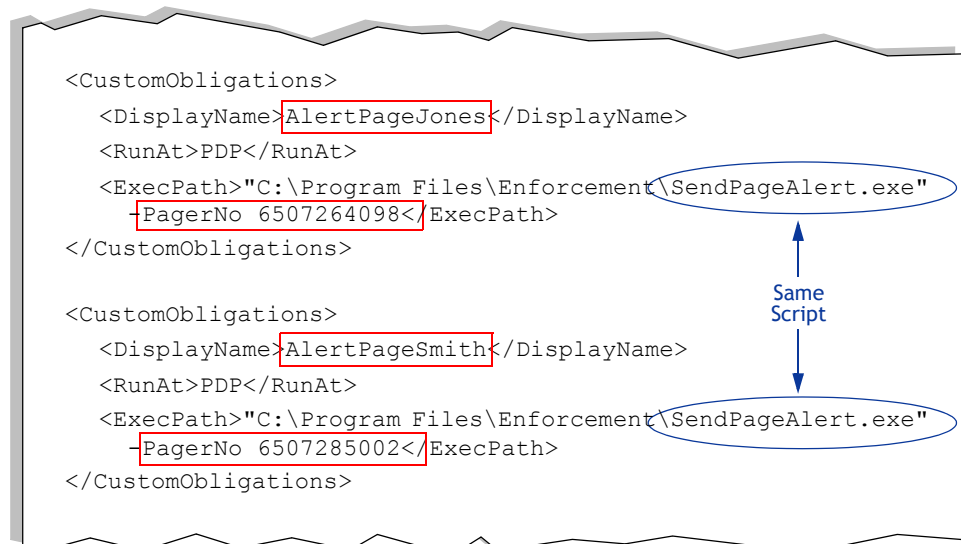


Figure 8-2: Adding Application-Specific Arguments

To do this, you can use your `SendPageAlert` script in two custom obligations, called *PageAlertJones* and *PageAlertSmith*. Each would have its own section in the config file, distinguished by the different display names and the additional argument *PagerNo*, specified in the `ExecPath` argument as shown in [Figure 8-2](#). When a policy with the *PageAlertJones* obligation is enforced, the executable will place a page call to Jones's number; when one with the *PageAlertSmith* obligation is enforced, the same executable will be called, but it will call Smith's number instead.

Staging and Testing

The application's success is evaluated and the command returns 0 if successful, something else otherwise.

The developer may create multiple binaries, for supporting multiple types of platforms.

To test the custom obligation, an administrator can deploy a key set of executables on a few of the desktops observed by Compliant Enterprise, then deploy a test policy with the appropriate custom obligation to those hosts. The administrator can then verify that the intended command line can start the executables. In particular, verify that:

- Correct binary was deployed, and is compatible with the platform;
- If an absolute path is to be used, then the binary was deployed in the expected position; otherwise, it is in the path for the administrator (or the user who runs the enforcer).
- Any external dependencies are satisfied (required libraries and resources, if any, exist in the expected places).

Policy analyst then creates policy using the Policy Author. For each decision branch, it adds appropriate obligations, including custom obligations (see [Feature 5](#)), using agreed-upon command lines. The CE arguments need not be explicitly written in the interface, they will be added by the infrastructure to the set of arguments the Policy Analyst has already given. These policies are then deployed.

Design Considerations

As the above description should make clear, you can design a custom obligation to do anything a standard executable file can do. Though there is a set of default arguments, you can add as many additional custom ones as you like, which can enable a broad variety of possibilities. Here are some suggestions enforcement behaviors that could be performed by custom obligations:

Zip Files: Compress/Uncompress files automatically, or notify the end user that the requested files must be compressed before proceeding, and prompt for a confirmation.

Encrypt Files: Encrypt/Decrypt files automatically, or notify the end user that the requested files must be encrypted before proceeding, and prompt for a confirmation.

License Management: Automatically check out or check in a license from a pool of floating application licenses.

Third-Party Integration: Invoke a third-party application to automatically generate an entry, document, incident report, helpdesk request, export record, inventory item, etc.

Scrub Lost Laptop: Delete all files from some location—for example, a laptop that has gone missing.

Sequential Behaviors

Note that all custom obligations are enforced asynchronously. The enforcer does not expect to receive any response from the executable about the outcome of the event, and so does not wait for any result before continuing with other enforcement actions. This means that a single obligation cannot control the sequence of events down a branching logic tree, by acting on the basis of an earlier obligation. For example, you can't design an On Deny obligation that can check Active Directory for the employment status of a user and then send a pager alert to a security officer if he is a contractor, or to the user's superior if he is full-time.

However, you can design obligations that work in a complex sequential ways as long as they involve the end user. For example, for a policy that blocks someone from opening a document on SharePoint site, you might design a custom obligation that pops up an HTML page to prompt the user with a few choices: click *here* to view the details of the policy that blocked access, click *here* to send an access request to the site's owner, or click *here* to cancel and continue. The user's response might then be either used by another executable, or covered by another policy which can include another custom obligation.

A

How Do I . . . ?

This appendix provides quick reminder of how to perform commonly required actions or procedures. It is organized in tables, focusing on the following areas:

- Controlling System Components ([page 139](#))
- Monitoring the System ([page 140](#))

Table A-1: Enrolling Entities

How do I . . .	Procedure
Enroll users and user groups?	Use the Enrollment Manager utility, with Type = DIR (for LDAP directories) or Type = LDAP (for LDAP output files). From LDAP directory, requires a connection file and a definition file; from LDIF file, requires only a definition file. See page 29 .
Enroll hosts and host groups?	Use the Enrollment Manager utility, with Type = DIR (for LDAP directories) or Type = LDAP (for LDAP output files). From LDAP directory, requires a connection file and a definition file; from LDIF file, requires only a definition file. See page 29 .
Enroll applications ?	Use the AppDiscovery utility, as described on page 41 .
Enroll Windows file shares ?	Use the Resource Path Discovery utility, as described on page 44 .
Enroll Linux file shares ?	Enroll Windows file shares, then use the Samba Directory Mapping utility as described on page 47 .
Enroll location sites ?	Use the Enrollment Manager utility with Type = TEXT. Requires a definition file containing a list of one or more sites, expressed as ranges of IP addresses. See page 49 .
Enroll SharePoint sites?	Use the Enrollment Manager utility with Type = PORTAL. Requires a connection file and a definition file, as described on page 51 .

Table A-2: Controlling System Components

How do I . . .	Procedure
Stop a Desktop Enforcer?	<ol style="list-style-type: none"> 1. In Administrator, find which profile the enforcer is using: Status tab, Policy Enforcer Status link: set Show filter to <i>All Desktop Enforcers</i>, check Profile Name column. 2. Find out the administrative password for that profile. (These do not display anywhere; they must be stored outside of Compliant Enterprise. The default is <i>password</i>.) 3. Use the StopDesktopEnforcer.exe utility, at C:\Program Files\Compliant Enterprise\Desktop Enforcer\public_bin (profile password is required). For details, see the <i>Enforcer Administrator's Guide</i>.
Start a Desktop Enforcer?	Runs as a Windows service. Manually restart the service under Control Panel, Administrative Tools, Services; or restart the host PC. For details, see the <i>Enforcer Administrator's Guide</i> .
Stop a Desktop Enforcer from displaying enforcement messages ?	Right-click on the CE icon in the system tray, and uncheck Display Notifications.

Table A-2: Controlling System Components (Continued)

How do I . . .	Procedure
Stop a File Server Enforcer?	<ol style="list-style-type: none"> 1. In Administrator, find which profile the enforcer is using: Status tab, Policy Enforcer Status link: set Show filter to <i>All File Server Enforcers</i>, check Profile Name column. 2. Find out the administrative password for that profile. (These do not display anywhere; they must be stored outside of Compliant Enterprise. The default is <i>password</i>.) 3. Windows: Use the <i>StopFileServerEnforcer.exe</i> utility, under Start, All Programs, Compliant Enterprise (profile password is required). Linux: Log in as local administrator and use the <i>cefse_stop</i> command. For details, see the <i>Enforcer Administrator's Guide</i> .
Restart a File Server Enforcer?	Windows: Runs as a Windows service. Manually restart the service under Control Panel, Administrative Tools, Services; or restart the host computer. Linux: Log in as local administrator and use the <i>service cefse start</i> command. For details, see the <i>Enforcer Administrator's Guide</i> .
Stop a SharePoint Enforcer?	<ol style="list-style-type: none"> 1. In Administrator, find which profile the enforcer is using: Status tab, Policy Enforcer Status link: set Show filter to <i>All Desktop Enforcers</i>, check Profile Name column. 2. Find out the administrative password for that profile. (These do not display anywhere; they must be stored outside of Compliant Enterprise. The default is <i>password</i>.) 3. Use the <i>StopSharePointEnforcer.exe</i> utility, under Start, All Programs, Compliant Enterprise (profile password is required). For details, see the <i>Enforcer Administrator's Guide</i>.
Restart a SharePoint Enforcer?	Runs as a Windows service. Manually restart the service under Control Panel, Administrative Tools, Services; or restart the host PC. For details, see the <i>Enforcer Administrator's Guide</i> .
Change the security password for any enforcer?	<ol style="list-style-type: none"> 1. In Administrator, find which profile the enforcer is using: Status tab, Policy Enforcer Status link: set Show filter to <i>All Desktop Enforcers</i>, check Profile Name column. 2. On the Policy Enforcer Configuration tab, select that profile, and provide a new password in the Administrative Password and Confirm Password fields (lower right). See page 82.
Point an enforcer to a different ICENet Server after it has been installed?	Associate the enforcer host to a different enforcer profile, which is associated with the new ICENet Server. See page 83 .

Table A-3: Monitoring the System

How do I . . .	In Administrator:
Check how many policies are deployed in my network?	Status tab, Status Overview link, Policies statistic (lower left).
Find out what hosts my Control Center server components are installed on?	Status tab, Status Overview link, Server Status pane (at right): Host column.
Check the health of all my Control Center server components?	Status tab, Status Overview link, Server Status pane at right: Last Heartbeat value turns red if expected interval has been exceeded.
Check how many enforcers are currently running?	Status tab, Status Overview link, Policy Enforcers statistics (middle left): shows File Server Enforcers, Desktop Enforcers, and Total.
Find out which enforcers are currently running?	Status tab, Policy Enforcer Status link: set Show filter to <i>All Policy Enforcers</i> .
Check if any enforcers are disconnected?	Status tab, Status Overview link, Policies Statistics (lower left). See page 61 .
Find out which enforcers are disconnected?	Status tab, Policy Enforcer Status link: set Show filter to <i>All Policy Enforcers with Warnings</i> ; then check the leftmost column for enforcers with Warning icons (exclamation points). See page 61 .

Table A-3: Monitoring the System (Continued)

How do I . . .	In Administrator:
Check for enforcers that are using obsolete policies ?	Status tab, Status Overview link, Policy Consistency statistic (upper left). See page 61 .
Find out which enforcers are using obsolete policies ?	Status tab, Policy Enforcer Status link: set Show filter to <i>Policy Enforcers with Warnings</i> , look for red X icon in Policy Up-to-Date column. See page 63 .
Tell how often policies are being enforced?	Status tab, Status Overview link, Policies statistic (lower left). See page 61 .
Find out which profile an enforcer is using?	Status tab, Policy Enforcer Status link: set Show filter to <i>All Policy Enforcers</i> , check Profile Name column. See page 63 .
Find out current heartbeat setting for an enforcer?	<ol style="list-style-type: none"> 1. Find which profile the enforcer is using (see above). 2. Policy Enforcer Configuration tab, Desktop Enforcers or File Server Enforcers link, locate the profile in the list at left, click the Settings tab, check the Heartbeat Frequency setting.

Compliant Enterprise uses several different passwords for various restricted activities, and they are maintained in different ways. Because this can be confusing, this appendix provides a concise summary of how all passwords work, how the default values are set, and how you can change them.

There are five distinct ways passwords are required in Compliant Enterprise:

- Authorized Application Users ([page 143](#))
- Enforcer Profile Security Passwords ([page 146](#))
- Utility Security Password ([page 148](#))
- Active Directory Access Password ([page 149](#))
- Database Password ([page 151](#))

Authorized Application Users

These refer to user/password pairs that allow users to access and use the three Compliant Enterprise applications: Policy Author, Reporter, and Administrator.

One or more separate user/password pairs can be defined for each application, by defining new users and assigning different roles to them. In turn, depending on how roles are defined, each user may have full or limited editing permissions within Policy Author. (Permissions for Administrator and Reporter are all-or-nothing; there are no levels of usage permission inside them.)

Initial Default

There is one hard-coded super user, *Administrator*, whose password is set during the initial installation of Control Center, in response to a prompt on the Super User Password screen of the install wizard as shown below. This user has full permissions for all three applications. Anyone logging in as this user can create and manage additional authorized application users, and can also change the password for this super user; but this user name itself cannot be deleted or changed.

Note that the super user password also serves as the default for all enrollment utilities, as described in the on [page 148](#). If the super user logs into Reporter or Administrator and changes the super user password, that change will also apply to the security password for all utilities.

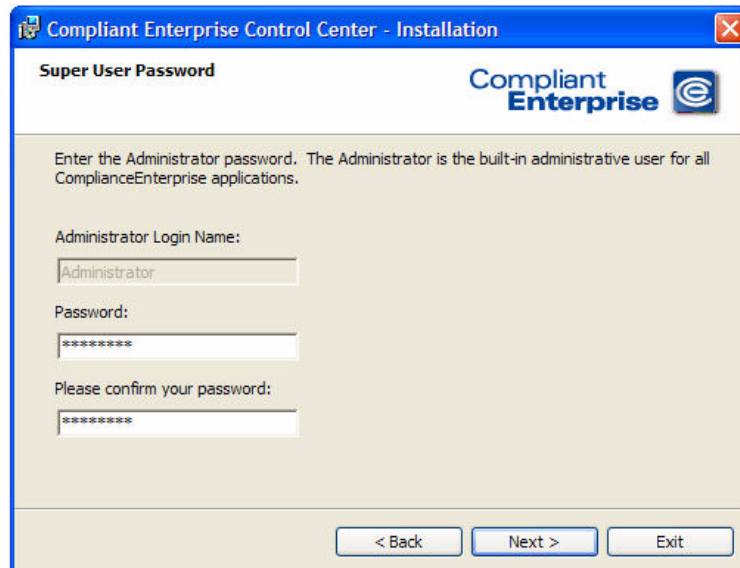


Figure B-1: Setting the Authorized Application User Password

How to Change

The super user *Administrator* cannot be deleted or renamed. However, you can change its password by logging into either Administrator or Reporter as this super user, then manually clicking the Change My Password link at the upper right of the screen (see references, below.) As we mentioned above, this change will also pertain to the security password for using all utilities.



Anyone logged in with the super user permission can create additional application users in Administrator, and also change the passwords of existing users. Any application user so defined, can also change his own password, also by logging in to Administrator or Reporter and clicking the Change My Password link. Authorized users can also change passwords on the Users and Roles tab (Figure B-2), which is also where you can create new users and groups, delete users and groups, assign different roles to existing users, and redefine the permissions associated with a role.

Comments

The default user *Administrator* is not displayed in the Users list on this tab, even though that is where you create and manage additional users of the same type. It cannot be deleted.

All passwords, whether defined during the install wizard or manually in the Administrator, are never visible anywhere, and cannot be looked up by anyone.

This means you must keep track of passwords somewhere outside of Compliant Enterprise, or change them if they are lost.

References

- Changing the Administrator password: [page 118](#)
- Creating and editing authorized application users: [page 67](#)

The screenshot shows the 'New User' form in the 'Users And Roles' tab of the Compliant Enterprise 2.0 Administrator's Guide. The form is divided into two main sections: 'User' and 'Permissions and Rights'. The 'User' section contains fields for 'User Id', 'First Name', 'Last Name', 'Password', and 'Confirm Password'. The 'Authentication Type' is set to 'Internal Authentication'. The 'Permissions and Rights' section includes a list of 'Assigned Roles' with checkboxes for 'System Administrator', 'Policy Administrator', 'Policy Analyst', and 'Business Analyst'. A 'Default Access Control Group' dropdown menu is set to '--- None Selected ---'. A 'Save' button is located at the bottom of the form.

Figure B-2: Users and Groups Tab in Administrator

Enforcer Profile Security Passwords

Each policy enforcer profile has a security password defined for it, to support the tamper-proof feature. This password is not associated with a single user; rather, it allows anyone to shut down and uninstall any enforcer using that profile. It is required by the StopDesktopEnforcer.exe and StopFileServerEnforcer.exe tools, and also during an uninstallation using the standard Windows Add/Remove Programs tool.

Initial Default

All enforcers are assigned a default profile, depending on their type; either File_Server_Default_Profile, or Desktop_Default_Profile.

You can create different, custom profiles and assign them to enforcers at any time, instead of the default profiles. For both the initial default profiles and any that you create, a default password string *password* applies, until you provide a different password string. This means that this default password will apply to an enforcer unless you have:

- changed this default password of the default profiles, or
- defined a new profile with a different password and assigned the new profile to the enforcer.

Because this default password can represent a security gap, we strongly recommend that you change it for both these default profiles as soon as you install Control Center.

How to Change

You can change the password for any enforcer profile, including the two default profiles. You do this by opening Administrator, going to the Policy Enforcer Configuration tab, selecting the profile in the list on the left, and typing the new password in the Administrative Password and Confirm Password fields.

Other Comments

You should change the passwords of the default profiles as soon as you install Control Center, since leaving the default could represent a security hole.

Like application user passwords, enforcement passwords are never visible anywhere, and cannot be looked up by anyone. This means you must keep track of passwords somewhere outside of Compliant Enterprise, or change them if they are lost.

This is especially important for enforcer profiles, since there may be many profiles, each with a different password. If an administrator needs to shut down a desktop enforcer, for example, he needs to find out which profile is assigned to

that enforcer, but he then needs to be able to find out the password for that profile.

The screenshot shows the 'Policy Enforcer Configuration' window with the 'Desktop Enforcer Profiles' tab selected. The 'Desktop_Default_Profile' is highlighted in the list on the left. The 'Settings' tab is active for this profile. The 'Administrative Password' and 'Confirm Password' fields are circled in red, indicating they are the focus of the configuration.

Setting	Value
ICENet Server	https://SAL8443/dabs
Heartbeat Frequency	60 seconds
Audit Log Upload Frequency	30 seconds
Max Log Size	2 MB
Document Activity Audit Level	Custom
Administrative Password	[Empty]
Confirm Password	[Empty]

Figure B-3: Changing Enforcer Profile Passwords

References

- Stopping enforcers: Enforcer Administrator's Guide
- Changing enforcer profile passwords: [page 82](#)

Utility Security Password

This password allows anyone to use several Compliant Enterprise utilities. This password must be provided as one of the arguments in the command line used to launch each utility. The specific argument used by each utility is provided in the list below.

- enrollmgr (-w)
- propertymgr (-w)
- ImportLocations (-password)

Initial Default

By default, this password is the same as the password string defined for application super user during initial installation.

How to Change

Anyone logged into Administrator or Reporter as this super user can manually change this password by clicking on the Change Password link at the upper right of the main screen. Once you change this password, it will apply to all utilities that require it; you cannot define different passwords for separate utilities.

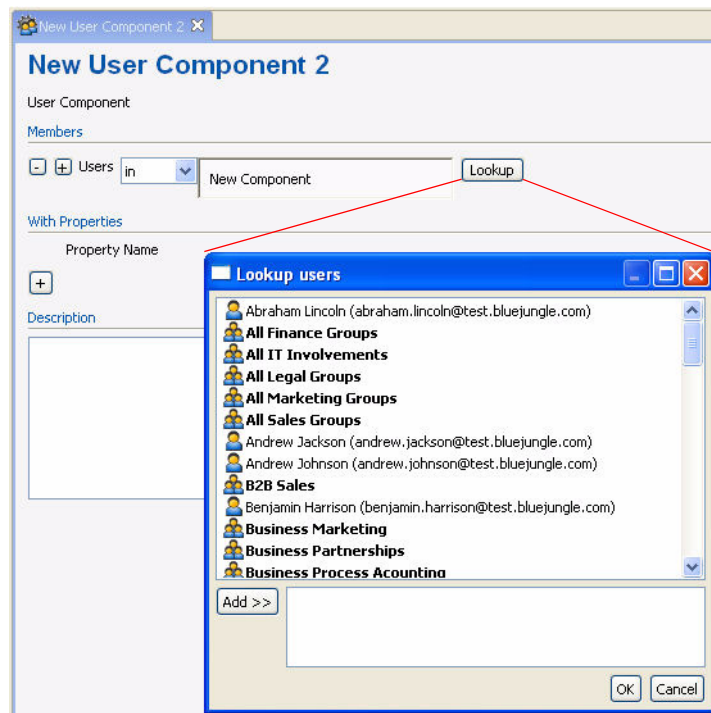
References

- Enrollment Manager utility: [page 19](#)
- ImportLocations utility: [page 49](#)
- Changing the security password: [page 53](#)

Active Directory Access Password

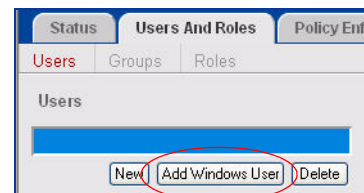
This user name and password pair is required whenever a Compliant Enterprise server component needs to acquire data from the network Active Directory. This access occurs transparently—the user is not prompted for a password—but nonetheless the password is required. Specifically, this occurs in the following cases:

- An Administrator user, defining a new user component, clicks the Lookup button to check the currently defined Users or Computers



- A Policy Author user clicks the New Windows User or New Windows Group button, to define a new user group based on Active Directory entities.

In either of these cases, Compliant Enterprise uses the stored user name and password to access Active Directory for the requested information. Because the user does not need to provide a password, this is ordinarily not a problem. However, if this password is ever changed on the AD server, these lookup features will be broken unless the new password is updated in Compliant Enterprise.



Initial Default

This user authentication does not require any user action, but occurs transparently based on the username and password saved in Compliant Enterprise's configuration file. These values are supplied during initial Control Center installation, at the following screen:

Figure B-4: Setting the AD Access User Name and Password

How to Change

You can supply a new value for one or both of these values by directly editing the configuration.xml file. However, since the password value should be encrypted, you need to run the crypt.jar utility to generate a new password string, which you then paste into the XML file. (This is the same basic procedure as for generating a new password for the Administrator user.)

You may need to change just the password, or the password and user name both. The elements you need to replace in the XML file is in the <UserAccess-Configuration> section, and looks like this:

```
<Property>
  <Name>login.dn</Name>
  <Value>jimmy.carter@test.bluejungle.com</Value>
</Property>
```

```
<Property>
  <Name>login.password</Name>
  <Value>5d5f5069375d365f3d5004036572c5e2b5f3d582f5d</Value>
</Property>
```

References

- Generating a new encrypted password: [page 118](#)
- The Administrator users and groups Lookup feature: [page 67](#)

Database Password

There is a username and password required whenever Compliant Enterprise connects to the database it is using to store Activity Journal data. This connection is performed transparently during normal Compliant Enterprise operation, but if you ever change the location of the Activity Journal, this connection will need to be reconfigured.

These settings are stored in the ConnectionPools section of the configuration XML file. This section has three ConnectionPool sections, one each for the Policy Master, Activity Journal, and Management DB—in that order. [Figure B-5](#) shows an example of these sections.

Initial Default

This connect string and password are set in response to prompts from the install wizard, during the initial installation of Control Center.

How to Change

If you need to change the database connection at any time after initial installation of Control Center, edit the <UserName>, <Password>, and <ConnectionString> elements in this file, for the **activity.connection.pool** (the second one in the section). As with other passwords, you can use the crypt.jar utility to generate a new encrypted password.

References

- Initial installation: Getting Started Guide
- Generating a new encrypted password: [page 118](#)

```

<ConnectionPools>

  <ConnectionPool>
    <Name>policyframework.connection.pool</Name>
    <Username>root</Username>
    <Password>66437346074625490d7810755776</Password>
    <ConnectionString>jdbc:postgresql://GRANDE9:5432/pf</ConnectionString>
    <DriverClassName>org.postgresql.Driver</DriverClassName>-
    <MaxPoolSize>30</MaxPoolSize>
  /ConnectionPool

  <ConnectionPool>
    <Name>activity.connection.pool</Name>
    <Username>qa3</Username>
    <Password>4c4f414c3d4c2e4f7841</Password>
    <ConnectionString>jdbc:oracle:thin:@HostName:1521:orcl</ConnectionString>
    <DriverClassName>oracle.jdbc.driver.OracleDriver</DriverClassName>
    <MaxPoolSize>30</MaxPoolSize>
  </ConnectionPool>

  <ConnectionPool>
    <Name>management.connection.pool</Name>
    <Username>root</Username>
    <Password>5866627a695854665162187a05690b7e00656b4a</Password>
    <ConnectionString>jdbc:postgresql://GRANDE5:5432/management</ConnectionString>
    <DriverClassName>org.postgresql.Driver</DriverClassName>
    <MaxPoolSize>30</MaxPoolSize>
  </ConnectionPool>
</ConnectionPools>

```

Figure B-5: Database Connection Pool Settings

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

The first section just lists acronyms, which are cross-referenced to the second section where the full terms are defined.

Acronyms

ACPL	See "Active Control Policy Language" (page 154)
AD	Active Directory, the standard Microsoft network entity management system.
CC	See "Control Center" (page 155)
IND	See "Information Network Directory" (page 157)
PDP	See "Policy Decision Point" (page 158)
PEP	See "Policy Enforcement Point" (page 159)

Terms

Active Control Policy Language	The language Compliant Enterprise uses internally to represent, store, and manage components and policies. Referred to as <i>ACPL</i> for short. The syntax ACPL uses is partially exposed in the Policy Author user interface; beyond this, it is not something policy designers or constructors need be concerned about.
Action Component	One of the five types of components you can build in <i>Policy Author</i> . (The other four types, collectively, are referred to as <i>Object Components</i> .) You define an action component by checking one or more of the available <i>Basic Actions</i> within it. Once defined, action components are available as the logical verbs in <i>ACPL</i> , the language in which policies are expressed.
Activity Journal	<p>One of the three databases used by Compliant Enterprise. The Activity Journal stores information from all <i>File Server Enforcers</i> about how subjects access and use information, and also on policy enforcement. When you use <i>Reporter</i> to generate reports, you are querying data from the Activity Journal.</p> <p>The Activity Journal can be maintained either on the internal database supplied with Compliant Enterprise, or on an external Oracle or Postgre-SQL database.</p>
Administrator	One of the three user applications in Compliant Enterprise. Allows you to configure various aspects of the system's operation, and monitor current operation.
Application Component	One of the five types of components you can build in <i>Policy Author</i> . Application components represent individual applications or categories of applications in the physical network.
Auditor	A logical component of Policy Enforcer software, responsible for capturing document access and use by policy subjects, as well as all policy enforcement events, and writing them to the <i>Activity Journal</i> database.
Basic Action	One of the set of irreducible actions, such as <i>open</i> , <i>copy</i> , <i>paste</i> , and <i>send by e-mail</i> , that are available for combining into <i>Action Components</i> in <i>Policy Author</i> . Each action component can consist of one or more basic actions.
Business Analyst	One of the four roles available in <i>Administrator</i> . (See <i>Roles</i> .)
Cancel	One of the actions you can take to change the deployment status of objects (policies and components). You can cancel an object if it has been submitted and scheduled for deployment, but not if it has already been deployed. Deployed objects must be <i>Deactivated</i> before they can be cancelled.

Component Bin	The pane in the lower left area of the <i>Policy Author</i> window, which displays all currently defined <i>Components</i> . Users create new policies by dragging components from the bin up into the main editing pane.
Component	Components are the building blocks of policies; they represent classes or categories of entities in the physical network environment. There are five types of components, represented by window-shade lists in the <i>Policy Author</i> component bin: Actions, Applications, Computers, Documents, and Users.
Computer Component	One of the five basic types of <i>Component</i> you can define in <i>Policy Author</i> to represent classes of entities in the physical environment—in this case, computers.
Connection File	A plain-text file that is used in connection with the Enrollment Manager utility to provide the information Compliant Enterprise needs to connect to the LDAP directory you are using as an enrollment source. The name and path of this file are specified as a command line argument in several enrollment-related commands, and is then stored in Compliant Enterprise’s internal tables for use in updating and synchronizing. A template for this file is provided during installation; users can change values in the file as necessary.
Control Center	The set of software servers and other modules that constitute the heart of the Compliant Enterprise platform. The main components of the Control Center are the Policy Server and Policy Master DB, the Management Server and Information Network Directory, the Intelligence Server and Activity Journal, one or more ICENet Servers, and the Reporter and Administrator servers.
Deactivate	One of the actions you can take to change the deployment status of objects (policies and components). If you want to delete an object that has already been deployed, you must first deactivate it. Once it is no longer in an active state, you can either leave it deactivated, to be able to reactivate it later; or delete it permanently, if you know you will not want to use it again.
Definition File	A plain-text file that is used in connection with the Enrollment Manager utility to provide the information Compliant Enterprise needs to map the data you are enrolling from LDAP directories or LDIF files, to the format Compliant Enterprise uses in its Information Network Directory tables. This file is specified as a command line argument for both enrolling and updating/synchronizing procedures. Like the <i>Connection File</i> , it is provided as a template that users can edit and save for their use.
Delete	See <i>Deactivate</i> .
Deployed	One of the possible states of a <i>Policy Author</i> object (a component or policy). When an object is deployed, it is distributed to all relevant enforcers in the system, where it comes into effect governing the way <i>Subjects</i> access and/or use information <i>Resources</i> .

Desktop Enforcer	One of two types of Policy Enforcers ; application that runs on Windows desktop or laptop PCs to monitor and enforces how any subject using that PC accesses and uses document resources.
Document Component	One of the five basic types of Component you can define in Policy Author to represent classes of entities in the physical environment—in this case, documents. Document components may be defined based on a number of properties such as extension, name (using wildcard characters), and date created or last changed; but most common is probably directory path where they are located.
Editor	The main pane on the right side of the Policy Author interface. This is where you define newly created components and policies, or change the definition of existing ones.
Effect	Every policy starts with an effect, which is the result that will ensue when the policy is enforced. There are three possible effects: Deny, Allow Only, and When. The last is used for policies that do not restrict anyone's use, but are intended for pure audit or subject notification purposes.
Enforcer Status	Policy Enforcers can be in either of two states: running, or not running. You can check this with the local controls for Desktop Enforcers , and for all enforcers by checking the latest heartbeat displayed on the Enforcers Status tab in Administrator . When an enforcer is running, this tab displays a policy status as well—that is, whether the most recently submitted version of all policies have been deployed to that enforcer, or not. You can also view summaries of policy status per enforcer by using the Deployment Status command from the Window menu, in Policy Author .
Enrollment	The process by which an organization's existing information network of users, hosts, and other entities are imported from LDAP directories or LDIF files, into Compliant Enterprise.
Enrollment Manager	A system utility that provides a unified tool for enrolling data from LDAP directories or LDIF files, updating and synchronizing enrollments of users, groups, and hosts.
File Server Enforcer	One of two types of Policy Enforcers ; a collection of software processes that run on Windows file servers to monitor and control the way all users access the files stored on that server.
Filter File	A plain-text file where users can define any set of LDAP filters. This file can be specified as a command line argument in enrollment procedures, so the enrollment will only be performed on entities meeting the filter criteria.
Folder	You can define folders in Policy Author for organizing your policies as you construct them. Folders can be assigned levels of access permission for various actions; these are configurable on the Access Control tab under Properties.

ICENet	Protocol used to communicate between <i>Policy Enforcers</i> and the <i>Control Center</i> . All such communication passes through the <i>ICENet Server</i> on the Control Center side; each enforcer is equipped with an <i>ICENet Client</i> .
ICENet Client	The component of the <i>Policy Enforcer</i> software architecture that controls remote communication with the <i>ICENet Server</i> .
ICENet Server	The <i>Control Center</i> server component that manages communication between all policy enforcers and the Control Center.
Information Network	The collective term that refers to all of an organization's information resource servers, desktops, network configuration, applications, and organizational structure.
Information Network Directory	The internal model Compliant Enterprise uses to represent the organization's information network. It can be thought of as a repository that maps to the data that is enrolled from your LDAP directory or LDIF files, about physical entities in the network including users, computers, groups, and applications. Physically, the IND is stored in the same database as the Activity Journal—either Compliant Enterprise's embedded database, or an external Oracle or Postgres DB.
Intelligence Server	The <i>Control Center</i> component that sends data to the <i>Activity Journal</i> and provides user activity and policy enforcement data and analysis.
MachineList File	The manually created file listing all PCs and servers in a given domain, which you must compose in order to enroll file shares using the Resource Path Discovery utility.
Management Database	One of the three databases employed by the <i>Control Center</i> to store the information Compliant Enterprise needs as it operates. Management Database stores the data about authorized users and the operation of <i>Administrator</i> .
Management Server	The <i>Control Center</i> component that centralizes management of all system components.
Manager	A software component of <i>Policy Enforcers</i> that manages their configuration and self-monitors the enforcer to prevent tampering.
Modeling	The process of defining policy components to represent classes of entities in the physical environment.
Modify	Whenever you want to change the state of any component or policy that has been submitted or deployed, you must click the Modify button in <i>Policy Author</i> . This puts the object into Draft state, meaning you must resubmit when you are finished modifying it.
My Reports	One of two tabs on the main screen of the <i>Reporter</i> application. This tab displays details about all reports created and owned by the user currently logged

into the application. The other tab, [Shared Reports](#), shows all report created and owned by all other authorized users, to which the currently logged in user has read access only.

Object Component	There are two general categories of components: <i>action</i> and <i>object</i> . Action components serve as the verbs in policies: read, copy, print, cut & paste, attach to e-mail, and so on. Object components provide the subjects and objects in policies, and fall into four categories: Applications, Computers, Documents, and Users. It is helpful to group these four together conceptually because you define and use them in a similar way, which is very different from how you build and use action components.
Obligation	These are the actions that Compliant Enterprise is to take whenever a policy is enforced. There are three types: make log entry (in the Activity Journal), display a notification to the subject, and send an e-mail notification to a specified recipient. For any policy, you can include one or more of these three. Log entries are required for all On Deny enforcements.
Policy	A rule you define in Policy Author to control information use in your organization. Policies consist of Components strung together with logical operators, along with other variables such as Obligations and time-based contexts.
Policy Administrator	One of the four roles available in Administrator . (See Roles .)
Policy Analyst	One of the four roles available in Administrator . (See Roles .)
Policy Author	One of the three user applications in Compliant Enterprise. Used for modeling components, constructing policies, and managing the deployment of components and policies.
Policy Component	See Component .
Policy Decision Point	The logical point, at each Policy Enforcer where the Policy Engine evaluates the action some subject is performing or requesting, weighs it against all currently deployed policies relevant to that action, and decides whether to enforce a policy or not.
Policy Enforcer	The generic term for the Compliant Enterprise clients that monitor document access and use, and enforce policies at the point of user. There are two types of Policy Enforcers: File Server Enforcers for file servers, and Desktop Enforcers for desktops and laptops.
Policy Engine	An ACPL execution engine found in the Policy Server and in the PDP within each policy enforcer. Creates policy maps and evaluates policies in real time.
Policy Enforcer Configuration	The third tab in the Administrator main window, where you define and apply Policy Enforcer Profiles .

Policy Enforcement Point	The software component within each Policy Enforcer that intercepts user events and makes policy decisions.
Policy Enforcer Profile	A named set of configuration settings you can define in Administrator , then assign to any policy enforcers in your network. You define profiles on the Policy Enforcer Configuration tab.
Policy Enforcer Status	One of sub-tabs available on the Administrator 's Status tab. The grid on this page lets you monitor various useful indicators of the status of all enforcers in the network, and also provides a filter that lets you focus in on only certain categories of enforcers.
File Server Enforcer	Software module installed on a Windows file server to monitor user activity and take action if access policies are triggered.
Policy Map	The optimized policy packages that are deployed to each policy 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 policy creation and editing, deployment and status tracking, and lifecycle management.
Policy Subject	Any person using a Resource or a computer that is under the control of one or more policies.
Policy Tree	The upper of the two small panes at the left side of the Policy Author main screen, displaying the folder structure where your policies are organized.
Preview Pane	An secondary pane in Policy Author main window that you can open to view the actual entities that would be represented by a component, or governed by a policy, as it is currently expressed. This pane is a useful tool for testing and debugging your policies as you work, though generally it is only opened when it is directly needed.
Profile	See Policy Enforcer Profile .
Property Manager	A system utility that provides simple way to view and customize the properties (technically, LDAP attributes) of users, hosts and applications enrolled in Compliant Enterprise.
Report	The results of a query run on the information stored in the Activity Journal , showing some combination of details about information access and use and policy enforcement in the network. Reports can be displayed in detail (grid) format, or as bar charts.

Report Query	The group of filter settings available in Reporter that control how a report content will be extracted from the Activity Journal .
Report Settings	The group of format settings available in Reporter that control how a report's output will be displayed.
Reporter	One of the three user applications in Compliant Enterprise. Reporter is a web application for creating reports and performing forensics. It obtains data from the Intelligence Server.
Resource	In the Compliant Enterprise system, information resources are document components that may be included in policy definitions. They provide the grammatical object of actions in the ACPL language.
Roles	There are four roles—Business Analyst, Policy Administrator, Policy Analyst, and System Administrator—available to be assigned to the users defined in Administrator . They are simply named sets of permission settings governing how a user can access Compliant Enterprise applications and edit components and policies. There are default settings for each, but they can be customized however you like. You control these settings on the Roles sub-tab of the Users and Roles tab.
Scheduled	You can deploy components and policies either immediately, or at some specified future time. In the latter case, the object is in a distinct state, Scheduled for Deployment.
Shared Reports	Whenever you define a report in Reporter , you have the option of marking it as shared, which makes it available (but not editable) to other users. All shared reports organized on a separate tab in the application.
Site Component	A collection of computer components with shared characteristics that represents some logical entity, such as a branch office or a building on a corporate campus. Sites are not imported from your LDAP directory directly; rather they are manually defined as one or more ranges of IP addresses, whose properties are then imported and marked as a special kind of component, available for use when defining policies.
States	Policy Author objects—policies and components—go through various states in their life cycle. There are seven possible states: Editing, Submitted for Deployment, Pending Deployment, Deployed, Submitted for Deactivation, Pending Deactivation, Deactivated, and Deleted. The state an object is currently in limits the kinds of actions you can perform on it.
Status Bar	The bar at the very bottom of the editing pane in Policy Author , which displays the current status of the currently active object, along with buttons for performing any status change actions appropriate at a given time.
Subject	(1) See Policy Subject .

(2) The components of a policy that, taken together, provide the grammatical subject. They are grouped together at the top of the policy editing pane in [Policy Author](#).

Submit	The action Policy Author users take to mark a policy or component as being finished and ready to deploy. When you click the Submit button, the active object is placed in Submitted state, and may be deployed.
System Administrator	One of the four roles available in Administrator . (See Roles .)
System Status	The upper left pane on the Status tab in Administrator 's main window, displaying the number of enforcers that have failed to connect within the last 24 hours, and the number to which the latest version of some policy or component has not yet been deployed.
User Component	One of the five basic types of Components you can define in Policy Author to represent classes of entities in the physical environment—in this case, people in the organization. User components can be defined based on any of the properties your network users have defined in your LDAP directory: name, title, department, salary, and so on.
Users and Roles	The middle tab on the Administrator main window. This is where you define and configure Compliant Enterprise users, user groups, and roles. Compliant Enterprise Users refer to the personnel authorized to access and use the three applications in Compliant Enterprise. They should not be confused with the User Components you define in Policy Author .
Window Shades	The stack of horizontal bars you use to open and close the five lists of components in the Component Bin, in the lower left corner of the Policy Author window.

This appendix provides miscellaneous reference material that may be of use for Compliant Enterprise system administrators, but is not commonly required for routine operation.

Intra-System Communication

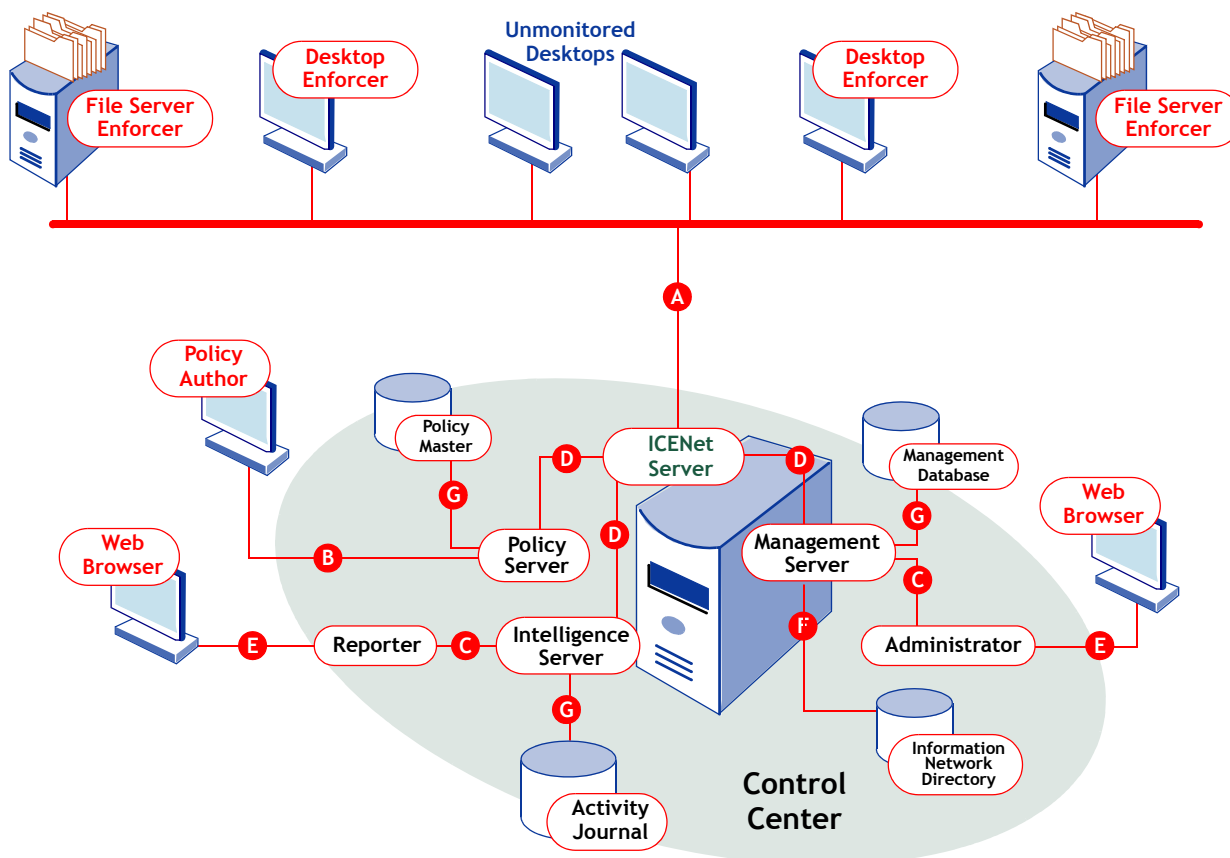
Compliant Enterprise is designed to be deployed and managed as a distributed system. Communications between the various servers and clients in Compliant Enterprise is accomplished via three communication models:

Web Services: Communications between the Policy Server and the Policy Author application, as well as between the policy enforcers and the ICENet Servers, is accomplished using the standard Web Services protocols SOAP and HTTPS. By default, these connections are encrypted and authenticated using SSL.

Web Application: The browser-based applications, Reporter and Administrator, are accessed using a standard HTML web browser using HTTPS. HTTPS allows communication between the Web browser and the Web applications to be encrypted.

Native data server protocols: Communications between Control Center servers and embedded data repositories such as the Information Network Directory and the relational database use native LDAP and RDBMS connectors respectively.

[Figure D-1](#) represents the connections among all components in Compliant Enterprise network.



CONNECTION DETAILS:

- A = ICENet communications for policy deployment, central management, and health monitoring; Web svcs port (8443)
- B = Client-Server communications (8443)
- C = Application-Application Service communications; Web services port (8443)
- D = Health monitoring (8443)
- E = HTTP with SSL; Web applications port (443)
- F = Open LDAP port (389)
- G = PostgreSQL embedded database port (5432)

Figure D-1: Compliance Enterprise Component Connections

Web Services Communications

The following component-to-component connections leverage Web Services standards:

Table D-1: Intra-system Communication Types

Component 1	Component 2	Description
Policy Author	Policy Server	Client-Server communications
Reporter Web Application	Intelligence Server	Application-Application Service communications
Administrator Web Application	Management Server	Application-Application Service communications
Policy Enforcers	ICENet Server	ICENet communications for policy deployment, central management, and health monitoring
Policy Server	Management Server	Health monitoring
Intelligence Server	Management Server	Health monitoring
ICENet Server	Management Server	Health monitoring

The Web Services communication is based on the Web Services standard Simple Object Access Protocol (SOAP) using the HTTP transport with SSL to both authenticate and encrypt communications between components. SSL is a commonly used communications security mechanism that is familiar to most Internet users. Each component is automatically issued a digital certificate at installation. These certificates contain the public-private key material used in the SSL handshake process and are used to authenticate both the client and the server. The certificates and the necessary certificates corresponding to the trust chain are managed in keystore files provided by the Java platform.

Web Application Communications

Web Application communications are used between standard, supported Web browsers and the Administrator and Reporter Web applications. By default, both of these Web applications are made available over HTTPS (HTTP with SSL) to provide encryption and server authentication. The Reporter and Administrator applications are issued default digital certificates. These can be replaced by certificates issued by a public certificate authority or a corporate certificate authority if desired.

Native Data Server Protocols

The Information Network Directory is implemented on a standard LDAP directory server, which provides standards-based access to hierarchical data. Communication with the Information Network Directory is based on the LDAP protocol and encrypted using SSL.

The Policy Master, Management Database, and Activity Journal are all managed within an embedded relational database. Communication with the database is managed using the PostgreSQL JDBC database driver, and uses the native database access protocol.

[Table D-2](#) provides a summary of the functions of the three databases used by Compliant Enterprise.

Table D-2: Database Functions

Component	Database	Description
Policy Server	Policy Master	Management of Policy and Policy Components
ICENet Server	Policy Master	Deployment of policy bundles
Management Server	Management Database	Heartbeat and policy enforcer health status
ICENet Server	Activity Journal	Application of audit logs to Activity Journal
Intelligence Server	Activity Journal	Analysis of Activity Journal
Management Server	Management Database	Component status, configuration, and user management
Policy Server	Policy Master	Management of Policy and Policy Components

Communication Ports

The following communication ports are used for internal communications:

- The Web Services Port (by default, port 8443) is used for a wide variety of connections to various Control Center components.
- The Web Applications Port (by default, port 443) is used for SSL-encrypted communications between the Reporter and Administrator applications and a Web browser.
- The OpenLDAP port (by default, port 389) is used for communication between the Management Server component and the LDAP server.
- The Autodiscovery port (19888) is used by components (Policy Author and policy enforcers) when they scan the network looking for a running Control Center to connect to.

[Figure D-2](#) illustrates how these ports are used by the various components of Compliant Enterprise.

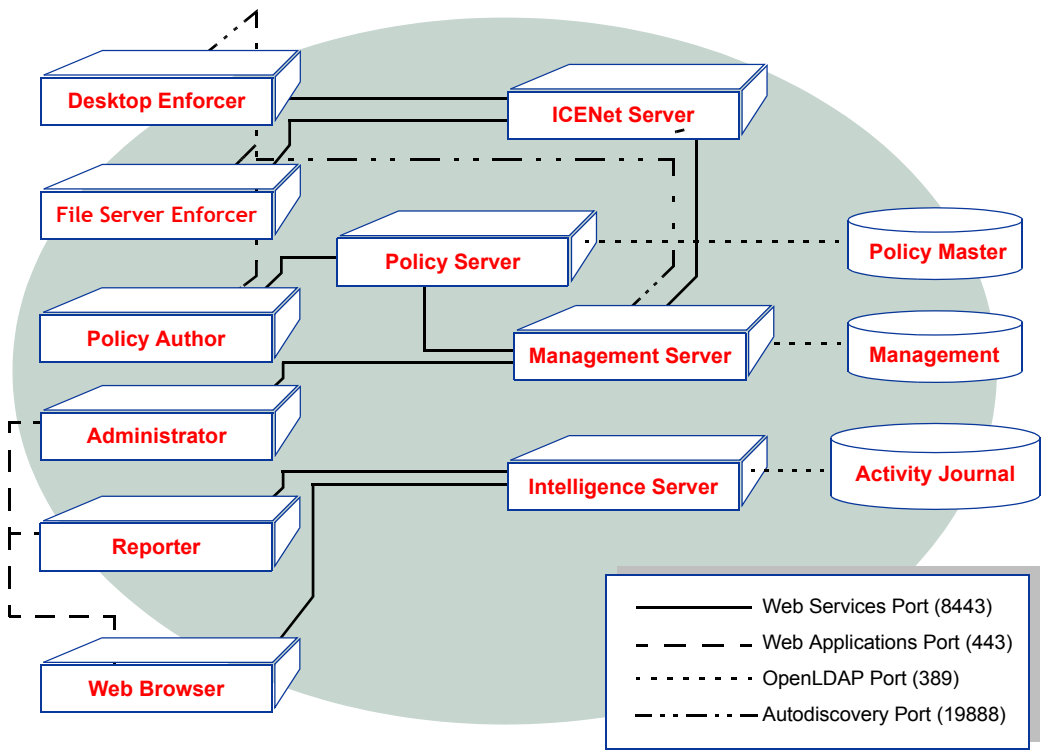


Figure D-2: Communications Ports



A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Numerics

2.0 framework
feature dependencies 9

A

ACPL 154
action components 154
Active Directory 65
Activity Audit Level 80
Activity Journal 154, 165, 166
administration 99
setting custom audit level options 80
viewing # of entries in 62
ad.default.conn (connection file) 22
example of 23, 51
ad.default.def (definition file) 24
example of 25
Add button 70, 72, 75
add command (Property Mgr) 123
Add Windows Group 66
adding
groups 69
users 67
Windows group 72
Windows user 67
Administrative Password (profiles) 80
Administrator
starting 59
users 65
Administrator user
changing password 60, 144
alerts 62

aliases.txt 46, 49
app.default.def (definition file) 24, 31, 42
app.default.def (definition file) example of 43
AppDiscovery 41
application components 154
applications
discovering and enrolling 41
enrolling different versions 43
Applications checkboxes 74
Assigned Roles 75
attributes
custom
for documents 126
Audit Log Upload Frequency 80
Auditor 154
audits
targeted 81
using enforcer profiles 81
authentication
config settings 104
autodiscovery port 166

B

basic actions 154
Business Analyst role 66, 154

C

cancelling deployment 154
case sensitivity
of utility command-line strings 20
command line arguments
of custom obligation executables 134

Index

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

- component bin 155
- components 155
 - computers
 - custom properties 121, 123
 - document 156
 - custom properties 125
 - object 158
 - sites 160
 - user
 - custom properties 121, 123
- computer components
 - custom properties 123
 - defining custom properties 121, 123
 - properties of 121
- configuration files
 - encrypting passwords 118
 - overview 101
 - Tomcat server 103
- configuration.xml
 - section 104
 - editing for custom obligations 135
- connection files
 - description of 22
- connection pools 111
 - adjusting max size 113
- Control Center 155
 - starting and stopping 85
- crypt.jar 53
- custom obligation
 - definition of 133
- custom obligations
 - configuring 135
 - requirements for using 134
 - version dependencies 10
- custom properties
 - documents 125
 - of document components 125
 - defining 126
 - of users, hosts and groups 123
 - users, computers, & groups 121, 123
- customAttrSetter.exe 126
 - using 127

D

- DABS section 135
- data sever protocols 163

- databases
 - and connection pools 111
 - description of 111
- deactivating 155
- default
 - properties
 - of computer components 121
 - of user components 122
- default access control groups 70
 - assigning to users 75
 - assigning users to 68
 - setting permissions 71
- Default Access Control tab 70
- Default Access Group 68
- definition files
 - for LDAP directories 25
 - for LDIF files
 - applications 42
 - users, hosts and groups 26
- delete command (Enrollment Mgr) 39
 - after failed enrollment 18
- delete command (Property Mgr) 124
- deleting
 - groups 73
 - hosts from profiles 81
 - users 69
- deployment 155
- Desktop Enforcers
 - reconfiguring 96
 - stopping 93
 - uninstalling 95
- dFS 48
- DisplayName
 - config file element 135
- Distributed File System (Microsoft) 48
- document activity
 - audits
 - setting options 80
- document components 156
 - custom properties 125
 - defining 126
 - defining custom properties 125

E

- Editing Privileges 74

- e-mail
 - configuration settings 108
 - setting the From field 109
- EnableADDirChgReplications 24
- encrypt utility 53
- encrypting passwords 118
- enforcer profiles
 - assigning to enforcers 64
 - defining 79
- Enroll Manager
 - enrolling
 - users and hosts 30
- enrolling
 - applications 41
 - file shares
 - Linux servers 47
 - Windows hosts 45
 - filter files for 27
 - location sites 49
 - users and hosts
 - manually 29
- enrollment
 - definition 15
 - failures 18, 39
 - manual 15
 - prerequisites 19
- Enrollment Manager
 - delete command 39
 - after failed enrollment 18
 - description of 19
 - enrolling
 - applications 42
 - list command 38
 - summary of CLI command arguments 21
 - summary of CLI commands for 21
 - sync command 35
- ExecPath
 - config file element 136
- executables
 - for custom obligations 134
- exiting
 - Administrator 60
- Expected Heartbeat (server statistic) 63
- exporting
 - policies 86
- exporting policies 86
 - CLI command arguments 87
 - command line arguments 87, 90
 - file overwrite behavior 88

- external domain authentication
 - configuring 105

F

- features, new in 2.0 9
- File Server Enforcers
 - reconfiguring 96
 - stopping 94
 - uninstalling 95
- filter files 27
- filters
 - in AD connection file 23
 - setting properties 28
- Firefox browser
 - TLS 1.0 required 59
- From field (notification e-mail)
 - configuring 108, 109
- Full Name (document property) 125

G

- global audit
 - setting activity audit level for 80
 - setting audit level 80
- groups
 - creating 69
 - default access control 70
 - deleting 73
 - in Administrator 65, 69

H

- heartbeat
 - enforcers
 - changing default value 80
 - of Control Center servers 108
 - of enforcers 76
 - policy enforcers, monitoring 64
- HeartbeatRate (config setting) 108
- heartbeats
 - description of 62
 - monitoring 63
 - total received in last 24 hrs 62
- Hide
 - in enforcer status display 64
- host
 - of policy enforcers 64

Index



hosts
 enrolling manually 29

HTML 163

HTTP 165

HTTPS 163, 165

I

ICENet Servers 165

 associating with a profile 80

 database functions 166

 initial registration 77

 install wizard vs. profile 77

 load balancing 91

 moving enforcers among 96

 reassigning profiles to 83

Import Locations

 enrolling

 sites 49

 syntax 50

importing

 policies 86

 See enrollment

importing policies 89

 CLI command arguments 90

Information Network Directory 16, 65

 administration 99

Intelligence Server 165, 166

IsPagingEnabled 23

J

java.security.krb5.kdc (config setting) 105

java.security.krb5.realm (config setting) 105

L

Last Heartbeat

 of policy enforcers 64

Last Heartbeat (server statistic) 63

Last Policy Update

 policy enforcers 64

LDAP 163, 165

 filter files 27

LDAP directory

 definition files 25

LDAPPollInterval (config setting) 108

LDIF

 enrolling applications 41

LDIF definition files

 for applications 42

 for users, hosts and groups 26

ldif.default.def (definition file) 24, 30

 example of 26

Linux

 enrollments for 18

Linux file servers

 enrolling file shares 47

list command (Enrollment Mgr) 38

list command (Property Mgr) 124

load balancing

 ICENet Servers 78, 91

location sites

 definition of 49

 enrolling 49

logging in

 Administrator 59

logging out

 Administrator 60

login.password (config setting) 104

logs

 setting upload frequency 80

M

MachineList file 44, 45, 157

MailFrom (config setting) 108

Management Database 165, 166

Management Server 165, 166

MaxPoolSize (config setting) 113

Microsoft Distributed File System 48

modeling 157

N

name

 document component property 125

native database access protocol 165

Network Information Directory
 and Enrollment Manager 19

New button 67

new features in 2.0 9

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------	----------

new in this release 9

NTFS

custom document properties 126

O

object components 158

properties of 122

OpenLDAP port 166

P

password

default for enforcer profiles 80

for stopping enforcers 56

for uninstalling enforcers 56

in LDAP directory connection file 23

in portal connection file 52

to stop enforcers 94

to uninstall enforcers 96

passwords

changing for Administrator account 60, 144

description of all 143

encrypting 53, 118

enrollment utilities 53

for stopping enforcers 80

for uninstalling enforcers 80

for using CE applications

defining 68

of enforcer profiles 80

changing 146

permissions

for Resource Path Discovery 47

modifying 73

Permissions and Rights 75

policies

displaying list for export 88

exporting 86

command line arguments 87, 90

file overwrite behavior 88

importing 89

importing and exporting 86

total number deployed 62

Policy Administrator role 66

Policy Analyst role 66

Policy Consistency 62

Policy Enforcer Status 62, 63

Policy Enforcers

total number installed 62

policy enforcers

reconfiguring 96

Policy Master 159, 165, 166

Policy Server 165, 166

policy subject 159

Policy Up to Date, monitoring 64

port numbers, default 164

portal content components

custom properties 129

properties of 129

portals

in connection file 52

ports 166

19888 166

diagram 167

Principals to Add 72

Profile Name

of policy enforcers 64

profiles

changing passwords 146

defining 79

moving between ICENet servers 83

setting password 56

using in audits 81

properties

deleting 124

listing 124

of computer components 121

custom 123

of document components

custom 125

defining 126

of portal content components 129

custom 129

of user components

custom 123

default 122

of user components (custom) 123

Property Manager

add command 123

delete command 124

list command 124

summary of CLI command arguments 122

summary of CLI commands for 122

using 122

propertymgr.bat 122

protocols 163

R

RDBMS 163

registration
 of ICENet Servers 77

Reporter 74

Resource Path Discovery 157
 description of 44
 MachineList file 45
 output file 46
 permission requirements 47
 using with dFS 48

roles
 modifying 73
 types 66
 what is? 66

Roles link 73

RunAt
 config file element 135

S

Samba Directory Mapping utility 47

ScheduledSyncInterval
 for AD enrollments 24
 for portal enrollments 52

ScheduledSyncTime
 for AD enrollments 24
 for portal enrollments 52

selectivefilter.properties file 28

server statistics
 viewing in Administrator 63

Server Status 62

shallow export
 definition 88

Simple Object Access Protocol 165

site.default.def (definition file) 24

sites 160
 description of 56

smbDirMapping utility 47

SOAP 163

sp.default.conn (connection file) 22

sp.default.def (definition file) 24

SSL 165

starting
 Administrator 59
 Control Center 85
 policy enforcers 95

status
 of policy enforcers 64

Status Overview 61

Status Summary 63

stopping
 Control Center 85
 policy enforcers 93

synchronizing enrollments
 automatically 22, 36
 manually 35
 vs. updating 32

System Administrator role 66

system alerts 62

System Statistics 62

System Status 62

T

tamper prevention
 enforcers
 setting password 80

targeted audits 81

TLS 1.0
 required with Firefox 59

trusted domains, configuring 106, 108

type
 of policy enforcers 64

U

uninstalling
 Policy Enforcers 95

updating enrollments
 from LDAP directory 33
 from LDIF file 34
 vs. synchronizing 32

upgrading
 dependencies 10

URL 60, 80

- user components
 - custom properties 123
 - default properties 122
 - defining custom properties 121, 123

- User Id field 68

- User Principal Name 122

- user repository
 - config settings 104

- users 65
 - adding 67
 - deleting 69
 - enrolling manually 29
 - groups 65, 69
 - what is? 65

- Users and Roles tab 67, 73, 75

- Users link 67, 75

- Users tab 70

- Users to Add 70

- useSSL (config setting) 104, 106

- utilities

- AppDiscovery 41
- customAttrSetter.exe 126
- Enrollment Manager 30
- Import Locations 50
- Property Manager 122
- Samba Directory Mapping 47

V

- version
 - of enrolled applications 43

W

- Web Applications 163, 165

- web applications port 166

- Web Services 163, 165

- web services port 166

X

- XML files

- in importing/exporting policies 86

Index

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---