



# **Probix Trustee**

User's Guide

**Release 2.1**

**July 9, 2003**

**Probix, Inc.**

**[www.probix.com](http://www.probix.com)  
883 N. Shoreline Blvd, Bldg. A  
Mountain View, CA, 94043 USA**

**Phone: (650) 691-1700**

**Information contained in this document is subject to change.**

## **DISCLAIMER**

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. Probix shall have neither liability nor responsibility to any person or entity with respect to loss or damages arising from the information contained in this document.

# Table of Contents

---

---

<b>Chapter 1: Theory of Operations</b> . . . . .	<b>9</b>
SYSTEM REQUIREMENTS . . . . .	10
Probix Server Requirements . . . . .	10
Content Server Requirements . . . . .	10
UNIX (Solaris) Configuration . . . . .	10
Linux Configuration . . . . .	10
Windows Configuration . . . . .	10
Client Requirements . . . . .	11
PROBIX TRUSTEE CONCEPTS . . . . .	12
PROBIX CONTENT PROTECTION NETWORK OVERVIEW . . . . .	13
PCPN TOOLS . . . . .	15
<b>Chapter 2: Creating a Custom Probix Adaptor</b> . . . . .	<b>17</b>
OVERVIEW . . . . .	18
PROBIX ADAPTOR ARCHITECTURE . . . . .	19
Solaris/Linux . . . . .	19
CREATING AN ADAPTOR FOR SOLARIS OR LINUX . . . . .	20
SOLARIS AND LINUX ADAPTOR INTERFACES . . . . .	21
CPcpnAdaptor Class Definition . . . . .	21
RegisterAdaptor() . . . . .	22
Syntax . . . . .	22
Return Value . . . . .	22
UnRegisterAdaptor() . . . . .	23
Syntax . . . . .	23
Return Value . . . . .	23
CPcpnAdaptor() . . . . .	23
Syntax . . . . .	23
Parameters . . . . .	24
Remarks . . . . .	24
~CPcpnAdaptor() . . . . .	24
Syntax . . . . .	24
Remarks . . . . .	24
AdaptorIsProtectedResource() . . . . .	24
Syntax . . . . .	24

Parameters . . . . .	25
Return Value . . . . .	25
AdaptorGetUserName() . . . . .	25
Syntax . . . . .	25
Parameters . . . . .	25
Return Value . . . . .	25
AdaptorGetPolicy() . . . . .	26
Syntax . . . . .	26
Parameters . . . . .	26
Remarks . . . . .	26
Return Value . . . . .	26
CREATING AN ADAPTOR FOR MS WINDOWS . . . . .	27
WINDOWSADAPTOR INTERFACES. . . . .	28
PROBIX ADAPTOR FUNCTIONS FOR WINDOWS . . . . .	29
pcpnmodInitialize . . . . .	29
Syntax . . . . .	29
Remarks . . . . .	29
Return Values . . . . .	29
pcpnmodUninitialize . . . . .	29
Syntax . . . . .	29
Remarks . . . . .	29
Return Values . . . . .	29
pcpnmodIsContentProtected . . . . .	29
Syntax . . . . .	30
Parameters . . . . .	30
Return Values . . . . .	30
pcpnmodGetUserName . . . . .	30
Syntax . . . . .	30
Parameters . . . . .	30
Remarks . . . . .	30
Return values . . . . .	30
pcpnmodCanPrint . . . . .	31
Syntax . . . . .	31
Parameters . . . . .	31
Remarks . . . . .	31
Return Values . . . . .	31
pcpnmodIsWatermark . . . . .	31
Syntax . . . . .	31
Parameters . . . . .	31
Remarks . . . . .	32
Return Values . . . . .	32
pcpnmodGetRenderInterval . . . . .	32
Parameters . . . . .	32
Return Value . . . . .	32

## **Chapter 3: Using the Probix Trustee Logger . . . . . 33**

THE PHP LOGGER MENU . . . . .	34
View All Logs . . . . .	34
Log Fields and Meanings . . . . .	34

Performing a Customized Query . . . . .	37
View Logs by Customer . . . . .	39
DECODING LOGS CREATED BY THE PHP LOGGER . . . . .	40
DECODING OTHER LOGS . . . . .	42
<b>Chapter 4: Administering Probix Trustee . . . . .</b>	<b>43</b>
PROBIX TRUSTEE ADMINISTRATION CONCEPTS . . . . .	44
Right . . . . .	44
Customer . . . . .	44
Manager . . . . .	44
Content Server . . . . .	44
Probix Server . . . . .	44
STARTING THE PROBIX TRUSTEE ADMINISTRATION TOOL . . . . .	45
ADMINISTERING CUSTOMERS . . . . .	46
Adding a Customer . . . . .	46
Activating or Suspending a Customer . . . . .	49
Modifying a Customer . . . . .	49
Removing a Customer . . . . .	52
Exporting a Customer . . . . .	52
ADMINISTERING MANAGERS . . . . .	53
Adding a Manager . . . . .	54
Activating or Suspending a Manager . . . . .	54
Modifying a Manager . . . . .	55
Removing a Manager . . . . .	55
ADMINISTERING PROBIX SERVERS . . . . .	57
Adding a Probix Server . . . . .	58
Modifying a Probix Server . . . . .	59
Removing a Probix Server . . . . .	60
ADMINISTERING ADMINISTRATORS . . . . .	61
Adding an Administrator . . . . .	61
Activating or Suspending an Administrator . . . . .	62
Modifying an Administrator . . . . .	63
Removing an Administrator . . . . .	63
ADMINISTERING RIGHTS . . . . .	64
Adding Rights . . . . .	65
Activating or Suspending a Right . . . . .	65
Modifying a Right . . . . .	66
Removing a Right . . . . .	66
<b>Chapter 5: Managing Probix Trustee Policies . . . . .</b>	<b>67</b>
POLICY MANAGER CONCEPTS . . . . .	68
Content . . . . .	68
User . . . . .	68
Group . . . . .	68
Members . . . . .	68

Policy . . . . .	68
Schedule . . . . .	68
Active/Suspended . . . . .	68
STARTING THE PROBIX TRUSTEE POLICY MANAGER . . . . .	69
MANAGING USERS . . . . .	70
Adding a User . . . . .	71
Activating and Suspending Users . . . . .	71
Modifying a User. . . . .	72
Removing a User . . . . .	73
MANAGING GROUPS . . . . .	74
Adding a Group . . . . .	75
Activating and Suspending Groups . . . . .	75
Modifying a Group . . . . .	76
Removing a Group . . . . .	76
MANAGING GROUP MEMBERS. . . . .	78
MANAGING CONTENT. . . . .	80
Limitations of Support of Some Content Types . . . . .	80
HTML Support . . . . .	80
MS Word File Support. . . . .	80
MS Excel File Support. . . . .	81
HWP File Support. . . . .	82
Adding Content . . . . .	83
Adding Portable Content . . . . .	84
Activating and Suspending Content . . . . .	85
Modifying Content. . . . .	85
Removing Content . . . . .	86
MANAGING POLICIES . . . . .	87
Adding a Policy. . . . .	88
Displaying Policies. . . . .	92
Activating or Suspending Policies . . . . .	93
Modifying a Policy. . . . .	93
Editing a Policy Name or Description . . . . .	94
Adding Content to an Existing Policy . . . . .	95
Removing Content from a Policy . . . . .	95
Adding Accounts to an Existing Policy. . . . .	95
Removing Accounts from a Policy . . . . .	96
Adding Rights to an Existing Policy . . . . .	96
Removing Rights from a Policy . . . . .	96
Adding a Schedule to an Existing Policy . . . . .	96
Editing a Schedule within a Policy . . . . .	97
Removing a Schedule From a Policy. . . . .	98
Removing a Policy . . . . .	98
USING THE IIS IMPORT TOOL . . . . .	99
<b>Chapter 6: Probix Trustee Command-Line Utilities . . . . .</b>	<b>101</b>

PCPNCUSTCFG . . . . .	102
SAVE_LOGS . . . . .	104
CHECK_PCPN . . . . .	105
CHECK_PCPN_PKG . . . . .	106
WEBSTART . . . . .	107
WEBSTOP . . . . .	108
WEBRESTART . . . . .	109
WEBSTAT . . . . .	110
MYSQLSTART . . . . .	111
MYSQLSTOP . . . . .	112
MYSQLSTAT . . . . .	113
<b>Chapter 7: Troubleshooting Messages . . . . .</b>	<b>115</b>
PROBIX-SPECIFIC HTTP STATUS CODES . . . . .	116
WINDOWS ACTIVEX APPLICATION ERROR MESSAGES . . . . .	121
APPLICATION ERRORS . . . . .	124
Probix PowerPoint Plugin Errors . . . . .	124
Probix Word Plugin Errors . . . . .	125
Probix Hangul Plugin Errors . . . . .	126
Probix Acrobat Plugin Errors . . . . .	127
Probix JPG and Text Viewer Plugin Errors . . . . .	128
Probix Excel Plugin Errors . . . . .	129
JAVA STATUS MESSAGES . . . . .	130
PROBIX TRUSTEE FOR OUTLOOK ERROR MESSAGES . . . . .	132
HTTP STATUS CODES . . . . .	133
<b>Appendix A: Glossary . . . . .</b>	<b>139</b>
<b>Index . . . . .</b>	<b>141</b>





# Chapter 1

## *Theory of Operations*

---

---

This chapter gives an overview of Probix Trustee™ and what hardware and software you need to run it.

The topics covered in this chapter are:

- “System Requirements” on page 10
- “Probix Trustee Concepts” on page 12
- “Probix Content Protection Network Overview” on page 13
- “PCPN Tools” on page 15

# SYSTEM REQUIREMENTS

Probix Trustee involves running a Probix Server, a Content Server, and a Client running a browser. The Probix Server can be run either at your site, or you can use Probix's Server as a service.

## Probix Server Requirements

The Probix Trustee server has the following hardware and software requirements:

- Sun Microsystems SPARC ULTRA 10 or higher
- 512K RAM plus additional memory based on the amount of content you plan to host
- Solaris 8.x plus all security patches
- Tomcat
- Apache web server
- MySQL Database Server version 3.23 or higher
- At least 500 megabytes of disk space for the software

Tomcat, Apache, and MySQL are part of the default installation package.

## Content Server Requirements

The Probix Trustee Content Server can run under either of the following hardware and software configurations:

### UNIX (Solaris) Configuration

- Sun Microsystems SPARC ULTRA 10 or higher
- 512K RAM plus additional memory based on the amount of content you plan to host
- Solaris 8.x plus all security patches
- Apache web server
- At least 500 megabytes of disk space for the software

Apache is part of the default installation package.

### Linux Configuration

- Red Hat Linux version 7.3
- Apache web server version 1.3.x
- ModSSL for Apache

### Windows Configuration

- Windows 2000
- Microsoft Internet Information Services 6.0

## Client Requirements

Probix Trustee supports the following operating systems and content types:

<b>Platform</b>	<b>Supported Versions</b>
OS	Windows 98, Windows ME, Windows NT 4.0, Windows 2000, Windows XP
Language	English, Japanese, Korean
MS Office	2000, XP
Adobe Acrobat	Acrobat Reader 5.0, 5.1; Adobe Acrobat 5.0, 5.05
Browser	MS Internet Explorer 5.0, 5.1, 5.5, 6.0
MS Outlook	2000, 2002
Hangul Word	HWP 2002
Content Type	PDF, Word, PPT, Excel, TXT, JPG, HWP 2002, HTML

## PROBIX TRUSTEE CONCEPTS

Probix allows customers to set content use policies, enforces those policies at all times, and provides the content owner with a detailed audit trail of any operation performed on protected content.

Trustee drastically reduces the risk of authorized users from knowingly or unknowingly misusing valuable proprietary information. It extends the security measures you already have in place, to protect and monitor the use of confidential content after it has been delivered to an authorized end-user.

Probix Trustee lets you:

- **Manage Content**

You may protect a wide variety of digital *content*, which can be one or more files, directories, or a web page.

- **Assign Usage Policies**

You can define a *policy*, which lets you define the length of access that an individual or group has to a particular document, and the types of operations that may be performed.

- **Review Audit Trail**

You can track how your confidential information is disseminated, who accessed the information, and what operations were performed.

- **Revoke Access Rights**

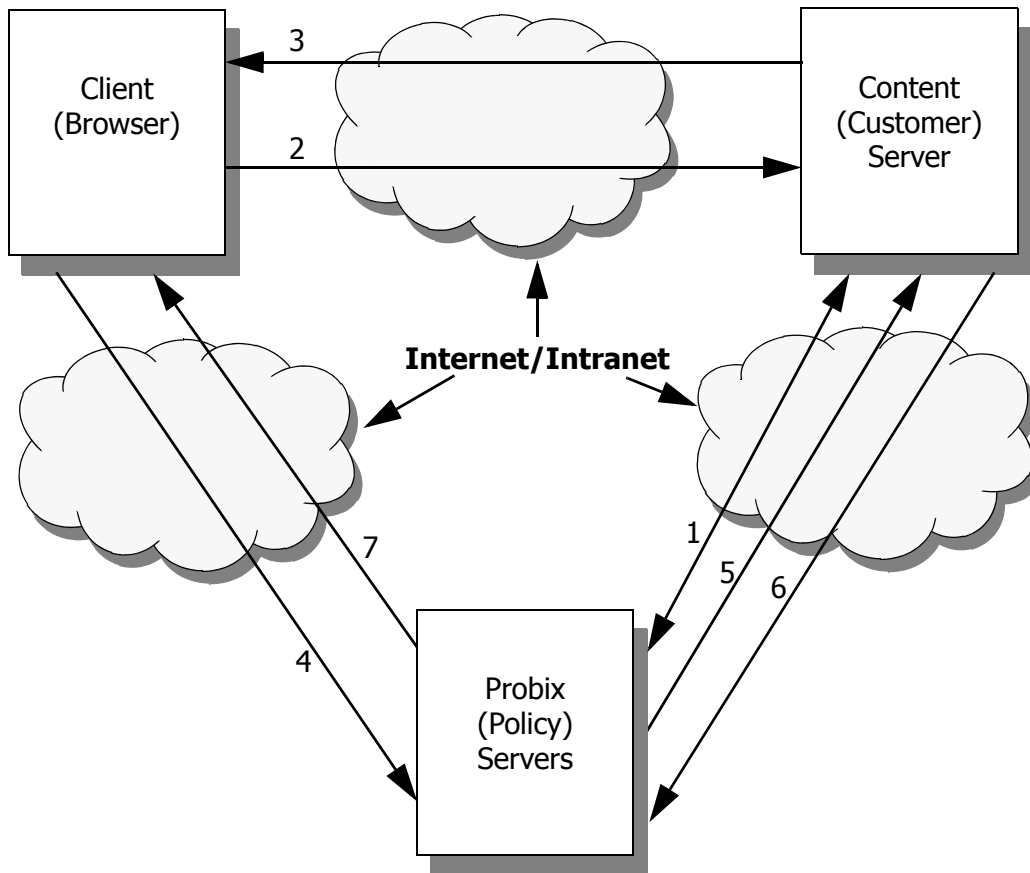
You may revoke access to confidential information even after that content has been distributed electronically.

## PROBIX CONTENT PROTECTION NETWORK OVERVIEW

Probix Trustee involves running a Probix Server, a Content Server, and a Client running a browser. The Probix Server can be run either at your site, or you can use Probix's Server as a service. You also need to run an adaptor to provide an interface between the client and the Content Server. The adaptor can be an existing one, such as Netegrity Siteminder™, or it can be one you create using the Probix Adaptor API discussed in Chapter 2, "Creating a Custom Probix Adaptor" on page 17.

The sum of the client, Content Server, Probix Server, adaptor, and the Internet as a transport medium is the *Probix Content Protection Network*, or PCPN.

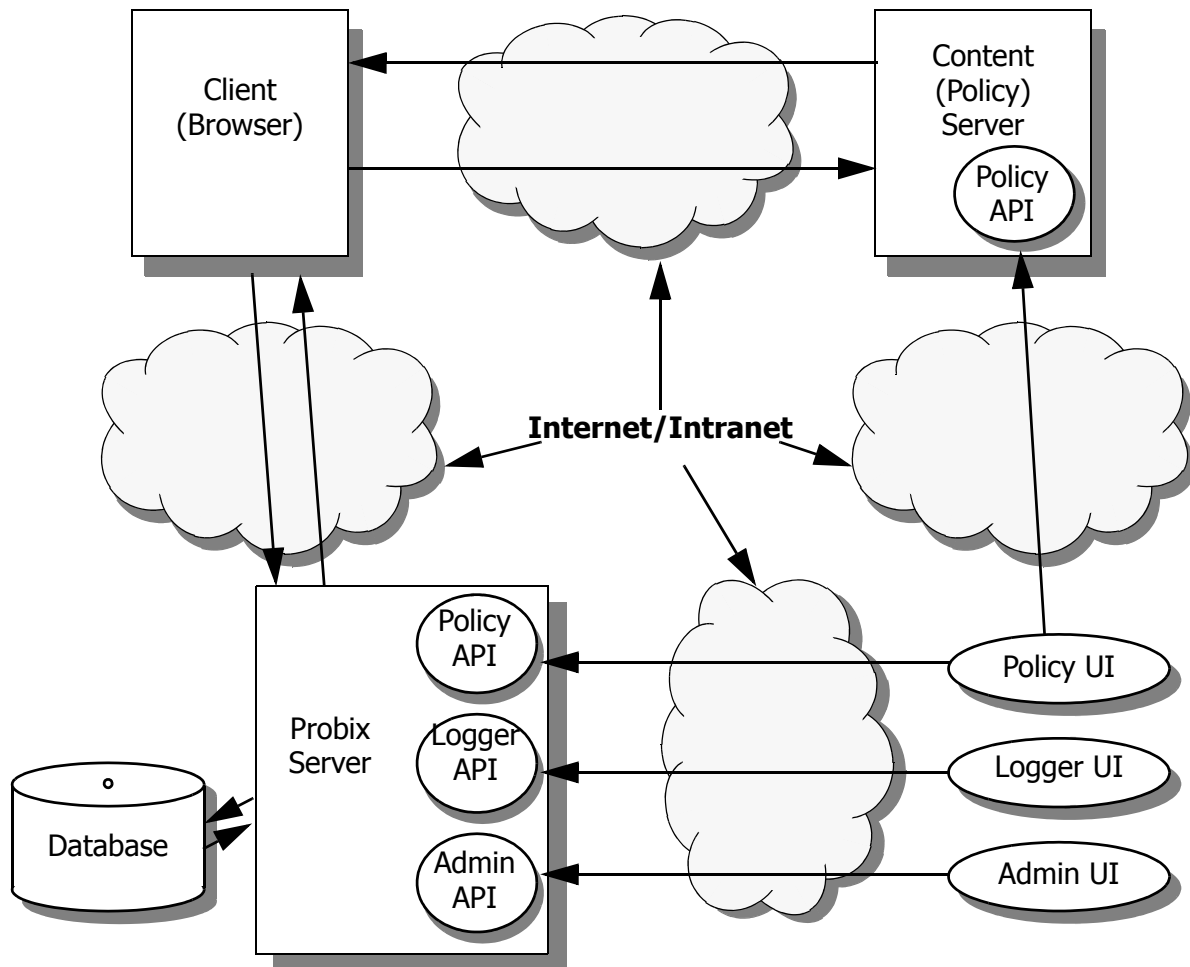
The following figure illustrates the flow of data in the PCPN.



The steps are:

1. The Probix Server and Content Server are initialized.
2. The client requests content from the Content Server.
3. The Probix Server sends a modified URL to the client.
4. The client's request is redirected to the Probix Server.
5. The Probix Server requests content from the Content Server.
6. The Content Server sends the content to the Probix server.

7. The Probix Server "wraps" the content into an ePouch and sends it to the Client.  
The following illustrates the flow of data in the PCPN system.



## PCPN TOOLS

The PCPN Administration Tool lets you administer customers, log in as one to verify and set up a customer site, administer managers of a Probix Trustee site, administer Probix Trustee servers, and set up rights available to the Policy Manager.

To authenticate users accessing Probix Trustee through Netegrity's Siteminder™ or other third-party business software platforms, you need an adaptor. This can be a third-party adaptor, or it can be one you develop yourself. For information on developing your own authentication function to work with Probix Trustee, see Chapter 2, "Creating a Custom Probix Adaptor" on page 17.

For more information on administering Probix Trustee, see Chapter 4, "Administering Probix Trustee" on page 43.

The PCPN Policy Manager is designed to create and manage your policies, as well as the accounts (users and groups) and rights that secure your content. This utility enables you to assign permissions to users, define groups of users and simultaneously set access permissions to all members of those groups, and develop schedules for accessing content.

For more information on managing Probix Trustee policies, see Chapter 5, "Managing Probix Trustee Policies" on page 67.

In addition to the GUI interfaces provided for managing Probix Trustee, Probix provides several UNIX command-line utilities you can use to manage policies and administer your site. These are discussed in Chapter 6, "Probix Trustee Command-Line Utilities" on page 101.

Probix Trustee logs all transactions made to the Probix Server. To view logs of these transactions, use the PCPN Logger. For information on using the PCPN Logger, see Chapter 3, "Using the Probix Trustee Logger" on page 33.

To help debug problems that may occur while running Probix Trustee, or to understand error-type messages that occur when users try to access content protected against them, see "Troubleshooting Messages" on page 115.





# Chapter 2

## *Creating a Custom Probix Adaptor*

---

---

This chapter describes the Probix API for Solaris, Linux, and Windows environments for developing your own adaptor to further customize the behavior of the Content Server.

This chapter contains the following:

- an overview of Probix Adaptor
- a description of the Probix Adaptor architecture
- an explanation of how to use the adaptor interfaces
- descriptions of the Probix Adaptor functions you need to implement for Solaris and Linux
- descriptions of the Probix Adaptor functions you need to implement for MS Windows

If you have any feedback you would like to send us regarding the Probix Content Protection Network (PCPN), or if you would like more information about other Probix products, please send e-mail to [info@probix.com](mailto:info@probix.com).

## OVERVIEW

Probix has partnered with numerous security providers to offer an integrated solution where web administrators can centrally manage not only who can access the content, but also what they can do with it.

- Probix supplies adaptors that can integrate with:
- Probix Adaptor™ for Check Point FireWall-1
- Probix Adaptor™ for Netegrity SiteMinder™
- Probix Adaptor™ for Tivoli Securway™ Policy Directory
- Probix Adaptor™ for Verisign Digital Certificates

Probix Adaptor™ integrates Probix Trustee™ with an existing user authentication or authorization system already deployed as part of a web server environment.

The functions documented in this chapter are prototypes of functions you must implement to customize the functionality of the Probix software to operate without one of these adaptors. Using these functions you can write an interface with a different adaptor.

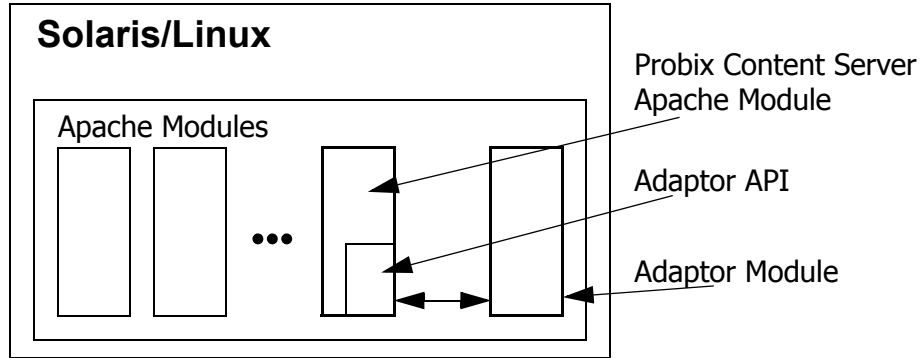
The functions documented here determine how the customer server modules behave. If you do not implement these functions, the behavior of the Probix software will remain unchanged.

When called, these functions determine whether content needs to be protected, what rights the end-users have (such as whether they can print the content), and who is requesting the document. Once you have implemented these functions, the Probix software can hook into them to adapt to different authentication and authorization systems.

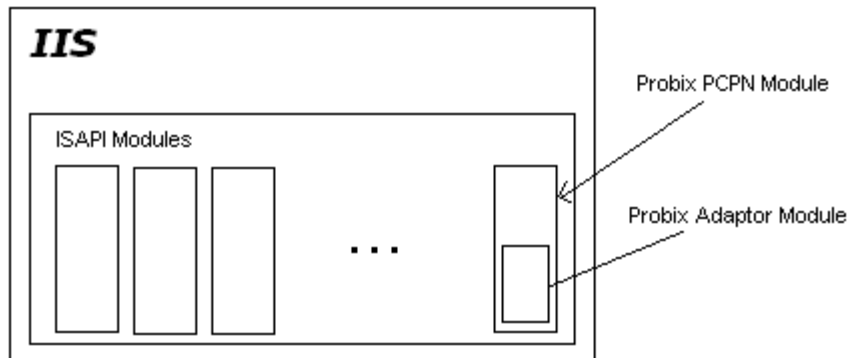
**Note:** The MS Windows functions must be implemented in a Microsoft Foundation Class (MFC) Dynamic Link Library (DLL) on a Microsoft platform, and these functions must be exported. Under MS Windows, the adaptor functionality only works with the Probix Internet Information Server (IIS) software module.

# PROBIX ADAPTOR ARCHITECTURE

The following figures illustrate how the Probix Adaptor module interfaces with an adaptor. Under Solaris and Linux:



Under Microsoft Windows:



## CREATING AN ADAPTOR FOR SOLARIS OR LINUX

The custom adaptor must be developed as an Apache module (so module). Use the C++ interface provided by Probix to interact with the Probix Content Server. The interface definition resides in the `PcpnAdaptor.h` and `PcpnBaseAdaptor.h` files provided by Probix. Your custom adaptor module must include these header files in the code.

The file `PcpnAdaptor.h` contains the `CPcpnAdaptor` class definition you need to implement to create a custom adaptor.

Follow these steps to implement your own adaptor for Solaris or Linux:

1. Create an empty Apache module.
2. Define an adaptor class inherited public from the `CPcpnAdaptor` class, including its constructor and virtual functions, such as `"class CAdaptor public CPcpnAdaptor{}`".
3. Develop constructor and virtual functions.
4. Declare an object of this class. It can be a static object.
5. Register this object using the base root class `RegisterAdaptor()` function. You can do this using the adaptor module `mod_init()` function.
6. Build the adaptor module, and put it into the `$APACHE_DIR/libexec` directory.
7. Create appropriate configuration directives for the `$APACHE_DIR/httpd.conf` file to cause apache to load the module upon restart.
8. Stop and restart Apache on the Customer Server.

In the `mod_init()` function the adaptor registers its registration object in the PCPN Customer server module. During the processing of any URL, the Content Server module calls overloaded virtual functions of the adaptor module and operates accordingly using the return values from these functions.

Each adaptor is identified by its name declared in its constructor function of its `CAdaptor` class.

More than one adaptor can be developed and attached to operate with Probix Content Server software at the same time. Each must be distinguished by its name and the protection logic provided when responding to URLs.

Notes:

- You have to provide a `LoadModule` directive in the `$APACHE_DIR/httpd.conf` file for Apache to load and run the adaptor module.
- Multiple adaptor modules can be deployed on the same Probix Content Server.
- The Probix Content Server calls the adaptor modules interface functions in the order they registered their registration objects.
- Probix provides the `PcpnAdaptor.h` and `PcpnBaseAdaptor.h` header files in the `$APACHE_DIR/include/pcpn` directory.
- Probix provides a full functional Sample Adaptor module with sources and make file that serve as an example you can use in developing your own custom adaptor module.
- A custom adaptor module is a normal Apache module that can use any module specific interface function as desired. The only requirement is it must follow the adaptor registration procedure call to be able accept requests from the Content Server.

## SOLARIS AND LINUX ADAPTOR INTERFACES

The following functions must be implemented and by your custom adaptor module.

The CPcpnAdaptor class is the base class for creating a custom adaptor. The rest of these are the prototype functions you must implement from this base class.

- CPcpnAdaptor Class Definition
- RegisterAdaptor()
- UnRegisterAdaptor()
- CPcpnAdaptor()
- ~CPcpnAdaptor()
- AdaptorIsProtectedResource()
- AdaptorGetUserName()
- AdaptorGetPolicy()

This section describes these functions.

### CPcpnAdaptor Class Definition

This class presents a registration object and functions for creating adaptors. Custom adaptors must define their own registration object class inherited from the CPcpnAdaptor class and implement the virtual functions defined in this class.

```
class CPcpnAdaptor: public CPcpnBaseAdaptor
{
public:
    CPcpnAdaptor(const char* a_szAdaptorName);
    ~CPcpnAdaptor();

    static PCPN_ADAPTOR_CODE GetAproprateAdaptor(
request_rec* r,
                CPcpnAdaptor** a_pAdaptor,
bool& a_bIsProtect,
int& iCustomerID);

// Virtual functions that can be overloaded by third party Adaptors classes

virtual PCPN_ADAPTOR_CODE AdaptorIsProtectedResource(
request_rec* r,
bool& bProtected,
int& iCustomerID);
virtual PCPN_ADAPTOR_CODE AdaptorGetUserName(
request_rec* r,
const char*& a_szUserName);
virtual PCPN_ADAPTOR_CODE AdaptorGetPolicy(
request_rec* r,
CPcpnAdapterPolicy& a_policy);
};
```

All overloaded virtual functions of the `CPcnpAdaptor` class return the `PCPN_ADAPTOR_CODE` type defined in the `PcnpAdaptor.h` file.

```
enum PCPN_ADAPTOR_CODE
{
    PCPN_ADAPTOR_OK           = 0,
    PCPN_ADAPTOR_DECLINED    = 1,
    PCPN_ADAPTOR_ERROR       = 2
};
```

`PCPN_ADAPTOR_OK` is returned when the implementation of the custom adaptor virtual function successfully processes an operation.

`PCPN_ADAPTOR_DECLINED` is returned when the implementation of the custom adaptor virtual function that this request is not supported by the adaptor module and needs to be processed by other modules.

`PCPN_ADAPTOR_ERROR` or a higher value is returned when the implementation of the custom adaptor virtual function could not process the operation for some error conditions.

Custom adaptors must define their own registration object class inherited from the `CPcnpAdaptor` class and implement the virtual functions described in this section.

**Note:** The `GetAproprateAdaptor` function is implemented in the Probix Customer Server Software. Your custom adaptor module does *not* need to define or declare this function.

## RegisterAdaptor()

Call the base class `RegisterAdaptor()` member function of its registration object to register the object. This can be done inside the `mod_init` function.

### Syntax

```
PCPN_ADAPTOR_REG_CODE    RegisterAdaptor()
```

### Return Value

A registration value in the form of a `PCPN_ADAPTOR_REG_CODE` type defined in the `PcnpBaseAdaptor.h` header file. This code type has the following definition:

```
enum PCPN_ADAPTOR_REG_CODE
{
    PCPN_ADAPTOR_REG_OK = 0,
    PCPN_ADAPTOR_REG_NOT_FOUND = 1,
    PCPN_ADAPTOR_REG_DUPLICATE = 2,
    PCPN_ADAPTOR_REG_WRONG_VERSION = 3
};
```

- `PCPN_ADAPTOR_REG_OK` – the adaptor is successfully registered or unregistered.
- `PCPN_ADAPTOR_REG_NOT_FOUND` – you are trying to deregister an object that has not been registered.
- `PCPN_ADAPTOR_REG_DUPLICATE` – returned when you are trying to register an object that is already registered.
- `PCPN_ADAPTOR_REG_WRONG_VERSION` – returned during registration when the internal API version is wrong.

**Note:** The internal API version is set by Probix and cannot be modified by your custom adaptor module. This internal versioning feature enables upwards compatibility of custom adaptor binary files with future

versions of this API.

## UnRegisterAdaptor()

Call the base class UnRegisterAdaptor() member function of its registration object to deregister itself from the Content Server software.

### Syntax

```
PCPN_ADAPTOR_REG_CODE    UnRegisterAdaptor()
```

### Return Value

A deregistration value in the form of a PCPN\_ADAPTOR\_REG\_CODE type defined in the PcpnBaseAdaptor.h header file. This code type has the following definition:

```
enum PCPN_ADAPTOR_REG_CODE
{
    PCPN_ADAPTOR_REG_OK = 0,
    PCPN_ADAPTOR_REG_NOT_FOUND = 1,
    PCPN_ADAPTOR_REG_DUPLICATE = 2,
    PCPN_ADAPTOR_REG_WRONG_VERSION = 3
};
```

- PCPN\_ADAPTOR\_REG\_OK – the adaptor is successfully registered or unregistered.
- PCPN\_ADAPTOR\_REG\_NOT\_FOUND – you are trying to deregister an object that has not been registered.
- PCPN\_ADAPTOR\_REG\_DUPLICATE – returned when you are trying to register an object that is already registered.
- PCPN\_ADAPTOR\_REG\_WRONG\_VERSION – returned during registration when the internal API version is wrong.

**Note:** The internal API version is set by Probix and cannot be modified by your custom adaptor module. This internal versioning feature enables upwards compatibility of custom adaptor binary files with future versions of this API.

## CPcpnAdaptor()

Constructor function.

### Syntax

```
CPcpnAdaptor(const char* a_szAdaptorName)
```

## Parameters

`a_szAdaptorName` a null-terminated character string containing the name of your custom adaptor. This name with the returned error code that equal or higher `PCPN_ADAPTOR_ERROR` value appears in the Apache `error_log` when any error condition is returned from your adaptor's implemented virtual functions.

## Remarks

Your custom adaptor module must provide its own constructor function that calls the base class constructor. It can also initialize itself.

## **~CPcpnAdaptor()**

Destructor function.

### Syntax

```
~CPcpnAdaptor()
```

## Remarks

Your custom adaptor module must provide its own constructor function, but you are not required to provide a destructor function.

## **AdaptorIsProtectedResource()**

Asks the adaptor whether the URL is to be protected.

### Syntax

```
PCPN_ADAPTOR_CODE AdaptorIsProtectedResource (  
    request_rec* r,  
    bool& bProtected,  
    int& iCustomerID);
```



## Parameters

<code>r</code>	the pointer to Apache <code>request_rec</code> structure that contains all the information about the received request
<code>bProtected</code>	a boolean set when the function returns <code>PCPN_ADAPTOR_OK</code> . The value "true" means the URL must be protected; "false" means the URL must not be protected and content is sent to the client unprotected (clear).
<code>iCustomerID</code>	an integer set by the adaptor module when the function returns the <code>PCPN_ADAPTOR_OK</code> return code. The Customer ID may be any valid customer ID registered in the Probix Server database.  <b>Note:</b> In the Customer configuration database for this customer, "Policy Source" must <i>not</i> be set to "Probix Database".

## Return Value

One of the following:

- `PCPN_ADAPTOR_OK` - the adaptor owns this request and will protect the content.
- `PCPN_ADAPTOR_DECLINED` - the adaptor does not own this request, thus the Content Server must use its native configuration for protection.
- `PCPN_ADAPTOR_ERROR` - an error occurred during the processing of this function.

## AdaptorGetUserName()

Gets the user name of the person trying to access protected content.

### Syntax

```
PCPN_ADAPTOR_CODE AdaptorGetUserName(  
    request_rec* r,  
    const char*& a_szUserName);
```

## Parameters

<code>r</code>	the pointer to Apache <code>request_rec</code> structure that contains all the information about the received request
<code>a_szUserName</code>	a zero-terminated ASCII string containing the user name. Memory for this field must be allocated from the Apache pool referenced by <code>r-&gt;pool</code> .

## Return Value

One of the following:

- `PCPN_ADAPTOR_OK` - success.
- `PCPN_ADAPTOR_DECLINED` - use the default user name "user" instead.
- `PCPN_ADAPTOR_ERROR` - an error occurred during the processing of this function.

## AdaptorGetPolicy()

Gets the policy information for the specified resource.

### Syntax

```
PCPN_ADAPTOR_CODE AdaptorGetPolicy(  
    request_rec* r,  
    CPcpnAdapterPolicy& a_policy);
```

### Parameters

<code>r</code>	the pointer to Apache <code>request_rec</code> structure that contains all the information about the received request
<code>a_policy</code>	the <code>CPcpnAdapterPolicy</code> structure that must be filled by policy information. It is defined in the <code>PcpnAdaptor.h</code> header file.

### Remarks

Use this function after you have a return value of `PCPN_ADAPTOR_OK` from a previous function.

### Return Value

One of the following:

- `PCPN_ADAPTOR_OK` - success.
- `PCPN_ADAPTOR_DECLINED` - use the default policy instead, which is No Print, No Watermark, and unlimited Render Interval.
- `PCPN_ADAPTOR_ERROR` - an error occurred during the processing of this function.

## CREATING AN ADAPTOR FOR MS WINDOWS

Follow these steps to implement your own adaptor on Windows:

- 1. Create an MFC DLL that implements the Probix adaptor functions specified in this document.**
- 2. Install the adaptor module:**
  - a. Start the registry editor.
  - b. In the file `HKEY_LOCAL_MACHINE\SOFTWARE\Probix\PCPN`, add a string value called `modulefile` where the value is the full path to the adaptor module.
- 3. Restart the IIS.**

The PCPN module loads the new adaptor and calls its interfaces to determine the behavior of PCPN. When you write an adaptor, you change the way the PCPN behaves when determining whether content is protected and what policies apply to the content. Without the adaptor, the PCPN module defaults to its own behavior.

The policies for the content are read from the `pcpncust.cfg` and `pcpnpolicy.cfg` files in the PCPN module installation directory. The interfaces in the adaptor can change this behavior.

## WINDOWSADAPTOR INTERFACES

The following functions must be implemented and exported by the adaptor module. The following are the function prototypes of the functions.

```
#ifdef __cplusplus
extern "C"
{
#endif

int WINAPI pcpnmodInitialize(void);

int WINAPI pcpnmodUninitialize(void);

int WINAPI pcpnmodGetUserName(
    CHttpFilterContext *lpContext /* [in] */,
    LPTSTR lpszUserName/* [in/out] */);

bool WINAPI pcpnmodIsContentProtected(
    CHttpFilterContext *lpContext /* [in] */,
    PHTTP_FILTER_URL_MAP pMapInfo /* [in] */,
    void *lpVoid /* [in] */);

bool WINAPI pcpnmodCanPrint(
    CHttpFilterContext *lpContext /* [in] */,
    const char* lpszURI/* [in] */,
    void* lpVoid/* [in] */);

bool WINAPI pcpnmodIsWatermark(
    CHttpFilterContext *lpContext /* [in] */,
    const char* lpszURI /* [in] */,
    void* lpVoid /* [in] */);

int WINAPI pcpnmodGetRenderInterval(
    CHttpFilterContext *lpContext /* [in] */,
    const char* lpszURI/* [in] */,
    void* lpVoid/* [in] */);

#ifdef __cplusplus
}
#endif
```

See Microsoft Developer Network (MSDN) documentation for information related to MFC classes and data structures.

## PROBIX ADAPTOR FUNCTIONS FOR WINDOWS

The following functions need to be implemented for the Probix Adaptor code to work properly on Windows:

- `pcpnmodInitialize`
- `pcpnmodUninitialize`
- `pcpnmodIsContentProtected`
- `pcpnmodGetUserName`
- `pcpnmodCanPrint`
- `pcpnmodIsWatermark`
- `pcpnmodGetRenderInterval`

**Note:** The Probix Adaptor functions use the following Microsoft classes and data structures:

- `CHttpFilterContext`
- `PHTTP_FILTER_URL_MAP`

See Microsoft documentation for more information about these data structures.

### **pcpnmodInitialize**

Initializes the adaptor.

#### **Syntax**

```
int WINAPI pcpnmodInitialize(void);
```

#### **Remarks**

Call this function when you load the adaptor module to initialize variables for the module.

#### **Return Values**

Returns 0 for success and any other values for failure. If this fails, the entire PCPN module is unloaded.

### **pcpnmodUninitialize**

Cleans up system states after the adaptor has been used.

#### **Syntax**

```
int WINAPI pcpnmodUninitialize(void);
```

#### **Remarks**

Call this function when you unload the adaptor module to do clean up.

#### **Return Values**

The return value is ignored.

### **pcpnmodIsContentProtected**

This function determines whether or not content is protected.

## Syntax

```
bool WINAPI pcpnmodIsContentProtected(  
    CHttpFilterContext *lpContext /* [in]  
    PHTTP_FILTER_URL_MAP pMapInfo /* [in] */,  
    void *lpVoid /* [in] */);
```

## Parameters

lpContext

[in] Pointer to the `CHttpFilterContext` structure that contains the context to be set in the specified thread.

pMapInfo

[in] Pointer to the structure that contains the information Probix IIS needs to map the URL to a physical path and file.

lpVoid

[in] Reserved for use with the PCPN module's default behavior.

See Microsoft documentation for details about the first two parameters.

## Return Values

The value **true** indicates the content is protected; **false** indicates otherwise.

**Note:** Do not protect requests that go to `/pcpn/probixprotflt.dll` and `/pcpn/probixprotsrv.dll`; these libraries are necessary for PCPN to work.

## pcpnmodGetUserName

Determines the name of the end-user making the request for protected content.

## Syntax

```
int WINAPI pcpnmodGetUserName(  
    CHttpFilterContext *lpContext /* [in] */,  
    LPTSTR lpszUserName/* [in/out] */);
```

## Parameters

lpContext

[in] Pointer to the `CHttpFilterContext` structure that contains the context to be set in the specified thread. Request information can be retrieved from the `lpContext` parameter.

lpszUserName

[in/out] Pointer to a string value that contains the user name.

## Remarks

See Microsoft documentation for details about the parameters.

## Return values

Request information can be retrieved from the `lpContext` parameter.

The user name is returned in the `lpszUserName` parameter. The buffer passed in has a maximum size of 256 characters.

The return value of this function is ignored. The user name is used in the logs to determine who accessed what content.

## pcpnmodCanPrint

Determines whether or not the specified user can print the protected content.

### Syntax

```
bool WINAPI pcpnmodCanPrint(  
    CHttpFilterContext *lpContext /* [in] */,  
    const char* lpszURI/* [in] */,  
    void* lpVoid/* [in] */);
```

### Parameters

lpContext

[in] Pointer to the **CHttpFilterContext** structure that contains the context to be set in the specified thread. Request information can be retrieved from the lpContext parameter.

lpszURI

[in/out] Pointer to a string value that contains the request URL.

lpVoid

[in] Reserved for use with the PCPN module's default behavior.

### Remarks

See Microsoft documentation for details about the first parameter.

### Return Values

A value of **true** allows printing of protected content; a value of **false** prevents printing.

## pcpnmodIsWatermark

Determines whether or not the printed document will have a watermark.

### Syntax

```
bool WINAPI pcpnmodIsWatermark(  
    CHttpFilterContext *lpContext /* [in] */,  
    const char* lpszURI/* [in] */,  
    void* lpVoid/* [in] */);
```

### Parameters

lpContext

[in] Pointer to the **CHttpFilterContext** structure that contains the context to be set in the specified thread. Request information can be retrieved from the lpContext parameter.

lpszURI

[in/out] Pointer to a string value that contains the request URL.

lpVoid

[in] Reserved for use with the PCPN module's default behavior.

## Remarks

See Microsoft documentation for details about the first parameter.

## Return Values

A value of **true** shows a watermark on printed documents; a value of **false** to print documents without a watermark.

**Note:** Watermarking only works when printing is enabled.

## pcpnmodGetRenderInterval

Determines the length of time the user can view the protected document.

```
int WINAPI pcpnmodGetRenderInterval(  
    CHttpFilterContext *lpContext /* [in] */,  
    const char* lpszURI/* [in] */,  
    void* lpVoid/* [in] */);
```

## Parameters

lpContext

[in] Pointer to the `CHttpFilterContext` structure that contains the context to be set in the specified thread. Request information can be retrieved from the `lpContext` parameter.

lpszURI

[in/out] Pointer to a string value that contains the request URL.

lpVoid

[in] Reserved for use with the PCPN module's default behavior.

See Microsoft documentation for details about the first parameter.

## Return Value

Returns the number of seconds the user is permitted to view the content. For example, if the user can view the content for five minutes, the value is 300.



# Chapter 3

## ***Using the Probix Trustee Logger***

---

---

The Probix Trustee™ logger enables you to monitor access to content on the Probix server.

This chapter describes the various options under each of these options, along with how to use the logs created.

To access the Probix Trustee logger, enter the URL:

`https://mysite/phplogger`

where *mysite* is the name of the site on which you are running the PCPN software.

The following topics are covered in this chapter:

- The PHP Logger Menu
- Decoding Logs Created by the PHP Logger
- Decoding Other Logs

# THE PHP LOGGER MENU

The Log Menu has two options:

- View All Logs
- View Logs by Customer

This section describes the various options under each of these options, along with how to use the logs created.

## View All Logs

When you select View All Logs, the following choices appear:

- Today - a log of all events that have occurred since 00:00:00 today.
- Current Week - a log of all the events that have occurred since 00:00:00 Monday of the present week.
- Current Month - a log of all the events that have occurred since 00:00:00 of the first day of the present month.
- Current Year - a log of all the events that have occurred since 00:00:00 of the first day of this year.
- View All Logs - all events that have occurred since the system was installed.
- View by User - a list of all events from Start Date and End Date (entered in the format YYYY-MM-DD HH:MM:SS) grouped by each user of the Probix Trustee system.
- View by Session ID - a list of all events from Start Date and End Date (entered in the format YYYY-MM-DD HH:MM:SS) grouped chronologically by session ID and displayed in chronological order.
- View by IP Address - a list of all events from Start Date and End Date (entered in the format YYYY-MM-DD HH:MM:SS) grouped by the IP address of the client accessing Probix Trustee.
- Customize - perform a query of the logs based on a specific set of dates, displaying only specified parameters, sorted by a compound list of parameters. For more details, see "Performing a Customized Query" on page 37.

To return to the main logger menu, select **Log Menu**.

## Log Fields and Meanings

The order of records in the log is relevant to when the record is received or generated by the Probix Server. Sometimes Probix Trustee is running when the client appears to have finished. For example, when a Probix Trustee user prints a document and close their browser. Although to the Probix Trustee user the transaction appears complete, the print job might not start on the Probix Server until after the browser has been closed. While the browser on the MS Windows client may no longer be running, the application performing the print may still be running. Thus, although the end user may believe Probix Trustee has completed all actions, print activities running in the background may continue to generate log entries.

The log contains the following columns:

- CID - the Customer ID number. This maps to the customer names in the Probix Trustee database.
- Event - the type of interaction. The following table contains the list of interactions:

<b>Probix Server Log Record (In typical order)</b>	<b>Description</b>
GET	A standard redirect request has been received from a client machine and processed on the Probix Server.
REQCONTENT	The Probix Server has sent a request to Content Server to obtain the protected content.
RECVCONTENT	The Probix Server has received a response to the request for protected content from the Content Server.
SENDLOADER	The Probix Server has prepared a protected document for the client machine and has initiated the opening of the protected content by sending an HTML page to the client machine that causes the Probix protection to be started on the client machine.
JSJARRESP	The Probix Server has sent a JavaScript-signed JAR file. This is only seen only when a network device is attempting to verify the signed JavaScript that is present in the LoaderHTML. Typically this is the client-side browser, but it can also originate with a firewall or other network security device.
BIXRESP	This is received when the client machine is opening the protected content. The client makes a request to the Probix Server for the protected content. The protected content is delivered within the body of the reply.
GETKEY	The client machine has completed the initiation of the secure transaction and is requesting a decryption key.
SENDKEY	The Probix Server has verified the decryption key request and has sent the decryption key to the Client machine.
CLIENTAUDIT	A client-audit message has been received from the client. This tracks document viewing, printing, and the presence of rogue applications. This also includes messages sent from the client side application that are relevant to security threats that may be present on that platform.
POLICYREQ	A policy request has been sent from the client to Probix Server. This request implements policies with some right that must be counted at the client. For example, if a protected document may be printed once, since the document may be viewed from multiple browsers at the same time by the same individual, the request for printing must be performed when the attempt to print is made.
POLICYAUDIT	A policy audit sent from the client to the Probix Server to track policy-related activities. This request is only used when a cardinal policy is in use.

<b>Probix Server Log Record (In typical order)</b>	<b>Description</b>
BIXDESTROY	The secure content has been closed either by user action on the client or because of a security threat. This message is sent by the Probix software surrounding the secure content to tell the Probix Server the secure session is being ended.
WRONGREQ	A request was received at the Probix Server that cannot be processed. The next table contains common requests that cannot be processed.
WRONGREQ_REALDOWNLOAD	This special error message is recorded when the Probix Server detects the RealDownload utility has been invoked to transfer the secure content. This is <i>not</i> allowed. To stop the RealDownload program from retrying the transfer, the Probix Server sends the HTTP status messages "403 = HTTP_FORBIDDEN" to the client.
TEST	During the installation of a Content Server, the TEST request verifies secure communications can be accomplished between the Probix Server and the Content Server. The TEST operation can also be used to help diagnose network connection problems.
RESPTEST	The Probix Server indicates it has sent a response to the Content Server TEST request.

The following table lists the most common requests that cannot be processed by the Probix Server:

<b>Typical WRONGREQ requests</b>	<b>Description</b>
400	A malformed HTTP request, compare with records for the same time in the <code>access_log</code> and <code>error_log</code> files in the <code>\$APACHE_DIR/logs</code> directory.
403	This is usually a result of an attempt to transfer protected content via RealDownload.
443	A malformed HTTP request; compare with records for the same time in the <code>access_log</code> and <code>error_log</code> files in the <code>\$APACHE_DIR/logs</code> directory.
455	An authentication-related problem.
456	An attack by an attempt to replay the key exchange protocol was detected and rejected.
457	An attack by an attempt to replay a redirection request from the content server was detected and rejected. Usually this is merely the user refreshing their browser address line

Typical WRONGREQ requests	Description
458	The client user does not have to rights to perform the operation. Typically this is a user that has used up their view or print rights. Possibly they are trying to view an expired document.
500	Server Error. Compare with records for the same time in the <code>access_log</code> and <code>error_log</code> files in the <code>\$APACHE_DIR/logs</code> directory.
555	Possible attack by access to a secure session after it has been closed. Typically, this can be as a result of HTTP requests that arrive out of order. For example, if the client software sends a CLIENTAUDIT request and a BIXDESTROY request around the same time and the network transport delivers them in a different order, the CLIENTAUDIT request gets rejected if it arrives after the BIXDESTROY request is processed.
557	The client user does not have to rights to perform the operation. Typically this can be a user that has used up their view or print rights, or possibly they are trying to view an expired document.
954	The protected content cannot be retrieved from the content server.

- Time - the time, in the ISO 8601 format YYYY-MM-MM HH:MM:SS, for example, "2002-06-06 00:43:06".

**Note:** The time stamps of the form 20021231005209 are in one of the ISO 8601 time formats. These timestamps are relative to the Probix Server rather than the client.

- Status - the HTTP status.
- Session ID - the eight-digit hexadecimal ID representing the session in which the transaction took place.
- IP Address - the IP address of the client calling the Probix Server.
- User - the e-mail address of the user who initiated the transaction.
- Browser - the browser under which the transaction took place.
- Query - either the URL submitted by the browser, or the action that took place on the client system.

Clicking on the heading of a column sorts the display by that field.

## Performing a Customized Query

To perform a customized query:

1. Click **Customize**.
2. Enter the **Start Date** and **End Date** in the format YYYY-MM-DD HH:MM:SS.
3. From the following list, select the Fields you want displayed:
  - Customer ID
  - Event

- Time
- Status
- Session ID
- IP
- User
- Requester Agent
- Query

You can use up to ten conditions and operands and nine “and/ors” in your query.

4. Select any of the following **Conditions** from the pull-down menu:

- Customer ID
- Event
- Time
- Status
- Session ID
- Requester IP
- User
- Requester Agent
- Query

5. Select any of the following operands from the pull-down menu:

- equal
- not equal to
- less than
- less than or equal to
- greater than
- greater than or equal to
- contains
- begins with
- ends with

Add queries with one of the following pull-down operands:

- And
- Or

6. Under **Categorize by**, select up to five of the following to group the resulting logs:

- Year
- Month
- Day

- Date
- Customer ID
- Event
- Time
- Status
- Session ID
- Requester IP
- User
- Requester Agent

7. Click **Submit Query** to perform the custom query.

## **View Logs by Customer**

When you select View Logs by Customer, the logs are ordered by customer ID.

## DECODING LOGS CREATED BY THE PHP LOGGER

The log reports created by the PHP Logger can help you debug problems that may occur during the running of Probix Trustee. Understanding the fields of a log can help you figure out where a problem in a given Probix Trustee session or configuration is occurring.

When you run a query, the log returns the following fields:

- CID

This is the Customer ID number. This maps to the customer names in the Probix Trustee database. The UNIX command `pcpnCustCfg -print` returns a mapping of customer ID to customer name. Most installations outside of Probix have only one "customer" with ID "0001".

- Event

This is the type of interaction. The following types of events occur:

- GET - a GET request; a client is requesting content from the content server. The GET and WRONGREQ transactions are the only ones directly originated by the user from the client.
- SENDLOADER - the Probix server is sending the HTML code that starts the protection to the content server.
- BIXRESP - the Probix server sends the protected content.
- GETKEY - the client sends a request to the Probix server for the key to decrypt the protected content.
- SENDKEY - the Probix server sends the key from the previous request to the client.
- CLIENTAUDIT - audit messages from the client showing what activity has taken place (for example, viewed, printed, tried to print screen).
- BIXDESTROY - the file containing the protected content is destroyed on the client.
- WRONGREQ - a wrong request. This has a variety of meanings.

The user was trying to retrieve content from the same URL using the same redirected URL

The encryption keys might be wrong

Something does not match the expected values or the original content

The URL has been modified

- Time - the time, in the format YYYY-MM-MM HH:MM:SS, for example, "2002-06-06 00:43:06".
- Status - the HTTP status; if the value is anything other than "HTTP\_OK", your problem is with that transaction.
- Session ID - the eight-digit hexadecimal ID representing the session in which the transaction took place. Session IDs are unique; you can use them to follow the transaction history of a particular session.
- IP Address - the IP address of the client calling the Probix server.
- User - the e-mail address of the user who initiated the transaction. When a transaction originates from the content server or Probix server, "N/A" appears in this field.
- Browser - the type of browser under which the transaction took place, along with the OS on which



the browser was running. If the transaction was controlled by an applet, the version of Java under which the applet was running is listed instead.

- Query - either the URL submitted by the browser, or the action that took place on the client system. This string often explains in detail the nature of the transaction.

Combining information from these fields can help you figure out where things went wrong.

### **1. Determine which session contains the problem transaction.**

Ask the user with the problem transaction for the following information:

- Their user name
- The IP address of the client system (less crucial, as you can often figure this out from the logs)
- The time (approximately) at which the offending transaction took place
- The nature of the transaction
- A description of the symptoms

### **2. Search the logs for the session.**

You may want to do a "View by User", "View by Today", or "View by Current Week" query to view the transactions. "View by User" might not be the most useful query if you are trying to find a transaction in a session not initiated by the user.

### **3. Perform a custom query.**

Once you know the session ID of the session in which the offending transaction occurred, you can perform a custom query for transactions involving that session ID.

### **4. Follow the transaction history.**

The problem transaction is usually the last transaction in the session; occasionally it is the transaction before the last one in the session. Based upon which parts of the software and hardware were involved in that transaction, you can run diagnostic tools to determine:

- whether the problem is hardware or software related
- if software, whether the problem was caused by Probix software or third-party software
- if hardware, where in the PCPN the error occurred

## DECODING OTHER LOGS

In addition to the log reports created by the PHP Logger, Probix Trustee and Apache create other logs that can help you debug problems that may occur during the running of Probix Trustee. Checking actions and activities against time stamps in various logs can help you determine when an error occurred and what may have caused it.

The PHP Logger and the `/usr/local/apache/pcpn/pcpn_log` file contain similar information, but in a different format. For example, given the following date and time:

- Friday, July 4th, 2003, 11:55:03am EDT

In GMT, that becomes:

- Friday, July 4th, 2003, 16:55:03

The PHP Logger representation of that is:

- 2003-07-04 19:55:03

The `/usr/local/apache/pcpn/pcpn_log` file representation of that is:

- 20030704T185503Z

The `/usr/local/apache/logs/access_log` representation of that time stamp is also expressed as GMT, so it appears as:

- [2003-07-04T22:55:03Z (GMT)]

The `/usr/local/apache/logs/error_log` file has time stamps expressed as GMT, but in more UNIX-like time format. In this file, the same time stamp is:

- [Fri Jul 04 22:55:03 2003]

# Chapter 4

## *Administering Probix Trustee*

---

---

Administering a Probix Trustee site involves adding, modifying, activating, suspending, and removing:

- customers
- managers of a Probix Trustee site
- Probix Trustee servers
- administrators of a Probix Trustee site
- rights on a Probix Trustee site

This chapter discusses the following concepts and tasks involved in administering a Probix Trustee site:

- "Probix Trustee Administration Concepts" on page 44
- "Starting the Probix Trustee Administration Tool" on page 45
- "Administering Customers" on page 46
- "Administering Managers" on page 53
- "Administering Probix Servers" on page 57
- "Administering Administrators" on page 61
- "Administering Rights" on page 64

## PROBIX TRUSTEE ADMINISTRATION CONCEPTS

You need to understand the following concepts before you administer a Probix Trustee site.

### **Right**

A *right* is a permission given to a user or group to perform a specific action within a policy. Some examples of rights include print, transfer, and watermark.

### **Customer**

A *customer* is an enterprise or entity using Probix Trustee.

### **Manager**

A *manager* is a user who can manage a Probix Trustee customer.

### **Content Server**

A *content server* is a server that contains the customer content. This server is also referred to as a *customer server*. A content server can be run either by you at your site or by Probix offsite.

### **Probix Server**

A *Probix server* is a server running the Probix Trustee server software for content protection. This server is also referred to as a *policy server*. A Probix server can be run either by you at your site or by Probix offsite.

## STARTING THE PROBIX TRUSTEE ADMINISTRATION TOOL

To start the Probix Trustee Administration tool, enter the URL:

`https://myhost:port/trustee/admin/`

where:

*myhost* is the name of your host

*port* is the port number on which you are running Probix Trustee

A welcome screen similar to the following appears.

The screenshot shows the Probix Trustee Administrator web interface. The page title is "Probix Trustee Administrator" and it includes "Home" and "Logout" links. The main content area features a large "Probix Trustee Admin" logo. On the left, there is a navigation menu with the following items:

- Customers**
  - Customer Management
  - Managers
- Probix Servers**
  - Probix Servers Management
  - Administrators
- Rights**
  - Rights Management
- Help**

Annotations on the left side of the image point to these menu items with the following text:

- Click to administer customers (points to Customer Management)
- Click to administer managers. (points to Managers)
- Click to administer Probix Servers. (points to Probix Servers Management)
- Click to administer Probix administrators. (points to Administrators)
- Click to administer Probix administrators. (points to Rights Management)
- Click to administer rights. (points to Help)

At the bottom of the page, the footer reads: "Probix ©2001-2002, All Rights Reserved Probix, Inc. 1-650-691-1700"

From here you can perform customer, Probix Server, and rights administration tasks.

# ADMINISTERING CUSTOMERS

To administer customers of your Probix Trustee system, select **Customers** from the navigation bar on the left to access the Customers Administration tool.

Click to sort column.

Suspended customers; left-click to select.

Active customers; left-click to select.

Click to add a customer.

Click to activate or suspend a customer.

Click to modify a customer.

Click to remove a customer.

Click to export customers.

Click to show descriptions of customers.

Descriptions of customers.

The first Probix Trustee customer is automatically created with the same name as the Customer Server when you install Probix Trustee. You can change the name of this customer using the directions in "Modifying a Customer" on page 49.

- The **Active** column on the left shows all *active* customers. These are all customers who can use Probix Trustee.
- The **Suspended** column on the right shows all *suspended* customers. These are all customers who cannot use Probix Trustee.
- Clicking on the **Active** or **Suspended** heading sorts the list alphabetically in ascending order; clicking on the heading a second time sorts the list in descending order.
- Checking the **Show Descriptions** box causes the text from the Description of a customer to be displayed when you select that user.

## Adding a Customer

To add a customer:

1. Click **Add**.

The Add Customer form appears.

The screenshot shows the 'Add Customer' form with the following fields and instructions:

- \*Customer:** MyCo (Enter customer name (case-insensitive).)
- \*Expiration Date:**  Never  2004-07-04 (YYYY-MM-DD) (Check **Never** or enter an expiration date.)
- Auth Name:** (Enter the user name for the authentication server.)
- Password:** (New) (Confirm) (Enter the customer password in both boxes (case-sensitive).)
- \*Probix Server Address:** 192.168.100.214 (Enter the IP address of the Probix Server.)
- Probix Server Port:** 80 (Enter the Probix Server HTTP port.)
- Encryption Algorithm:** AES (Select algorithms and policy source.)
- Hash Algorithm:** SHA (Select algorithms and policy source.)
- Policy Source:** Database on Probix Server (Select algorithms and policy source.)
- Server Location:** Egg Crate, NJ (Enter physical location of the Probix Server (text).)
- Time Zone:** (GMT-05:00) Eastern Time (US & Canada) (Select a time zone.)
- Description:** My Company (Enter text description of Probix Server.)
- Reseller Company Name:** My Company (Enter the name of the reseller company.)
- Reseller Company URL:** http://www.my\_co.com (Enter a valid URL for the reseller's Web site.)
- Reseller Sales E-mail Address:** sales@my\_co.com (Enter a valid e-mail address for the reseller's sales department.)
- Reseller Notification E-mail Address:** support@my\_co.com (Enter the return e-mail address on notifications.)
- Reseller Diagnostic Page URL:** http://www.my\_co.com/support (Enter a valid URL for the reseller's support site.)
- Reseller Logo Text:** My Company (Enter reseller's corporate slogan or motto.)
- Reseller Alternate Logo Text:** My Company's Slogan (Enter reseller's corporate slogan or motto.)
- Reseller Partnership Text:** in partnership with (Enter reseller's corporate slogan or motto.)
- Trusted Exception List:** snagit.exe (Enter text explaining the relationship between Probix and the reseller.)

Buttons: OK, Cancel

*\*Required fields.*

Enter applications to be ignored by Probix Trustee.

2. Enter the following fields:

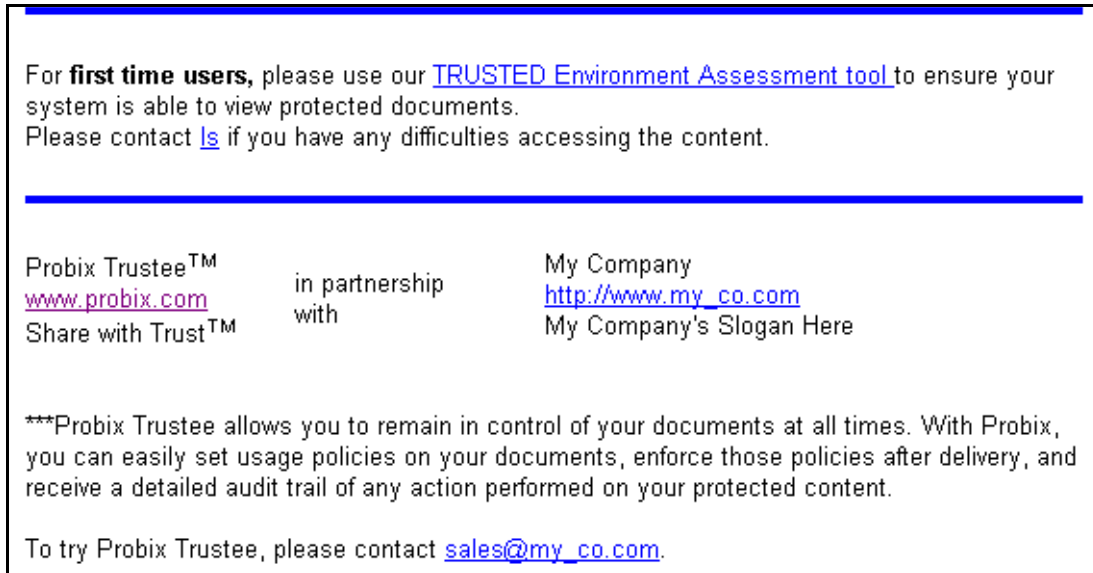
**Note:** Fields marked with \* are required fields.

<b>*Customer:</b>	the name of the customer as it will appear in the <b>Active</b> and <b>Suspended</b> columns, as well as in the <b>Manager</b> pull-down menu
<b>*Expiration Date:</b>	a date upon which the customer can no longer send protected content. ( <b>Note:</b> The customer can still <i>access</i> protected content.)
<b>Auth Name:</b>	the user name needed to access content on the content server (optional)
<b>Password:</b>	the password for the content server. Enter it under the "New" and "Confirm" boxes
<b>*Probix Server Address:</b>	the IP address of the Probix Trustee policy server
<b>Probix Server Port:</b>	the HTTP port (default value:80)
<b>Encryption Algorithm</b>	from the pull-down menu, select <b>AES, DES, or Triple DES</b>
<b>Hash Algorithm:</b>	from the pull-down menu, select <b>SHA</b> or <b>MD5</b>
<b>Policy Source:</b>	from the pull-down menu, select <b>Database on Probix Server, Redirect URL, or Protected Content.</b>
<b>Server Location:</b>	the physical location of the server (text).
<b>Time Zone:</b>	from the pull-down menu, select the appropriate time zone.
<b>Description:</b>	an optional text description of the customer.
<b>Reseller Company Name:</b>	the name of the company from which the documents are delivered. Appears in the phrase, "Documents protected by Probix Trustee™ have been delivered to you by <i>reseller</i> " (optional).
<b>Reseller Company URL:</b>	a valid URL for the reseller's Web site; this appears on invitations and notifications (optional).
<b>Reseller Sales E-mail Address:</b>	a valid e-mail address for the reseller's sales department to which people can send e-mail to to request more information (optional).
<b>Reseller Notification E-mail Address:</b>	the return e-mail address on notifications (optional).
<b>Reseller Diagnostic Page URL:</b>	a valid URL for the Probix Trustee diagnostic software (support) page on the reseller's system (optional).
<b>Reseller Logo Text:</b>	Trademarked spelling of the reseller company's name (optional).
<b>Reseller Alternate Logo Text:</b>	corporate slogan or motto used by the reseller (optional).
<b>Reseller Partnership Text:</b>	text explaining the relationship between Probix and the reseller. For example, "partnered with" as in "Probix Trustee partnered with <i>reseller</i> " (optional).



**Trusted Exception List:** any executables you want Probix Trustee to not treat as a "rogue application." Note that screen capturing is totally disabled while protected content is being accessed (optional).

**Note:** The Reseller fields, when entered, cause messages sent by Probix Trustee for Meetings, Probix Trustee for Notes, and Probix Trustee for Outlook to have lines at the bottom similar to the following:



Click **OK** to add the customer, or **Cancel** to return to the Customers Administration tool.

## Activating or Suspending a Customer



To activate or suspend a customer:

**1. In the Customer Administration tool, select one or more customers to be activated or suspended.**

Use the left mouse button to select each customer you want to activate or suspend.

Left-clicking on a user name and pressing the **Shift** key as you move your cursor selects a consecutive set of customers. Press the **Ctrl** key and left-click individual customers to select multiple non-consecutive customers.

**2. Change the status of the selected customers.**

Click the  button to move customers from the **Active** column to the **Suspended** column, thus suspending them, or click the  button to move customers from the **Suspended** column to the **Active** column, thus activating them.

## Modifying a Customer

To modify a customer:

**1. In the Customer Administration tool, click **Modify**.**

The Modify Customer form appears.

**Modify Customer**

\*Customer:  ID:

\*Expiration Date:  Never  2004-07-04 (YYYY-MM-DD)

---

Auth Name:

\*\*Password:

---

\*Probix Server Address:

Probix Server Port:

---

Encryption Algorithm:

Hash Algorithm:

Policy Source:

---

Server Location:

Time Zone:

Description:

---

Reseller Company Name:

Reseller Company URL:

Reseller Sales E-mail Address:

Reseller Notification E-mail Address:

Reseller Diagnostic Page URL:

Reseller Logo Text:

Reseller Alternate Logo Text:

Reseller Partnership Text:

---

Trusted Exception List:

*\*Required fields. \*\*Current password is preserved if empty.*

- Enter new customer name (case-insensitive).
- Check **Never** or enter an expiration date.
- Customer ID number (cannot be edited).
- Enter the user name for the authentication server.
- (Optional) Enter new customer password in both boxes (case-)
- Enter a new IP address for the Probix Server.
- Enter the Probix Server HTTP port.
- Select algorithms and policy source.
- Enter physical location of the Probix Server (text).
- Select a time zone.
- Enter text description of Probix Server (optional).
- Enter the name of the reseller company.
- Enter a valid URL for the reseller's Web site.
- Enter a valid e-mail address for the reseller's sales department.
- Enter the return e-mail address on notifications.
- Enter a valid URL for the reseller's support site.
- Enter the reseller's corporate slogan or
- Enter text explaining the relationship between Probix and the reseller.
- Enter applications to be ignored by Probix Trustee.

2. Edit whichever of the following fields you want to change:

**Note:** Fields marked with \* are required fields.

<b>*Customer:</b>	the name of the customer as it will appear in the <b>Active</b> and <b>Suspended</b> columns, as well as in the <b>Manager</b> pull-down menu
<b>*Expiration Date:</b>	a date upon which the customer can no longer send protected content. ( <b>Note:</b> The customer can still <i>access</i> protected content.)
<b>Auth Name:</b>	the user name needed to access content on the content server (optional)
<b>Password</b>	the password for the content server. Enter it under the " <i>New</i> " and " <i>Confirm</i> " boxes. If there are two asterisks (**) by Password, the password is preserved and cannot be changed.
<b>*Probix Server Address:</b>	the IP address of the Probix Trustee policy server
<b>Probix Server Port:</b>	the HTTP port (default value:80)
<b>Encryption Algorithm</b>	from the pull-down menu, select <b>AES, DES, or Triple DES</b>
<b>Hash Algorithm:</b>	from the pull-down menu, select <b>SHA</b> or <b>MD5</b>
<b>Policy Source:</b>	from the pull-down menu, select <b>Database on Probix Server, Redirect URL, or Protected Content</b>
<b>Server Location:</b>	the physical location of the server (text)
<b>Time Zone:</b>	from the pull-down menu, select the appropriate time zone
<b>Description:</b>	an optional text description of the customer
<b>Reseller Company Name:</b>	the name of the company from which the documents are delivered. Appears in the phrase, "Documents protected by Probix Trustee™ have been delivered to you by <i>reseller</i> " (optional).
<b>Reseller Company URL:</b>	a valid URL for the reseller's Web site; this appears on invitations and notifications (optional).
<b>Reseller Sales E-mail Address:</b>	a valid e-mail address for the reseller's sales department to which people can send e-mail to to request more information (optional).
<b>Reseller Notification E-mail Address:</b>	the return e-mail address on notifications (optional).
<b>Reseller Diagnostic Page URL:</b>	a valid URL for the Probix Trustee diagnostic software (support) page on the reseller's system (optional).
<b>Reseller Logo Text:</b>	Trademarked spelling of the reseller company's name (optional).
<b>Reseller Alternate Logo Text:</b>	corporate slogan or motto used by the reseller (optional).

**Reseller Partnership Text:**

text explaining the relationship between Probix and the reseller. For example, "partnered with" as in "Probix Trustee partnered with reseller" (optional).

**Trusted Exception List:**

any executables you want Probix Trustee to not treat as a "rogue application." Note that screen capturing is totally disabled while protected content is being accessed (optional).

Click **OK** to modify the customer, or **Cancel** to return the the Customers Administration tool.

## Removing a Customer

To remove one or more customers:

**1. In the Customer Administration tool, select the customers you want to remove.**

Use the left mouse button to select the customer you want to remove. Left-clicking on a customer and pressing the **Shift** key as you move your cursor selects a consecutive set of customers. Press the **Ctrl** key and left-click individual customers to select multiple non-consecutive customers.

**2. Remove the selected customers.**

Click **Remove**. A confirmation box appears.

**3. Confirm the removal.**

Click **OK** to remove the selected customers, or **Cancel** to cancel the removal.

## Exporting a Customer

Use this command to export the encryption keys for the specified customer into a file. This file is then imported into the customer server software. When you import keys onto the customer server, this command creates the file you import.

To export the encryption keys for a customer:

**1. Select a customer.**

**2. Click Export.**

The Export Customer form appears.



Enter new password in boxes (case-sensitive).

Enter and re-enter the password (appears as asterisks – "\*\*") for the customer encryption key.

**Note:** The password fields protect the encryption keys. You must have the correct password for the keys to be imported properly; otherwise, the customer server cannot properly encrypt content.

**3. Confirm.**

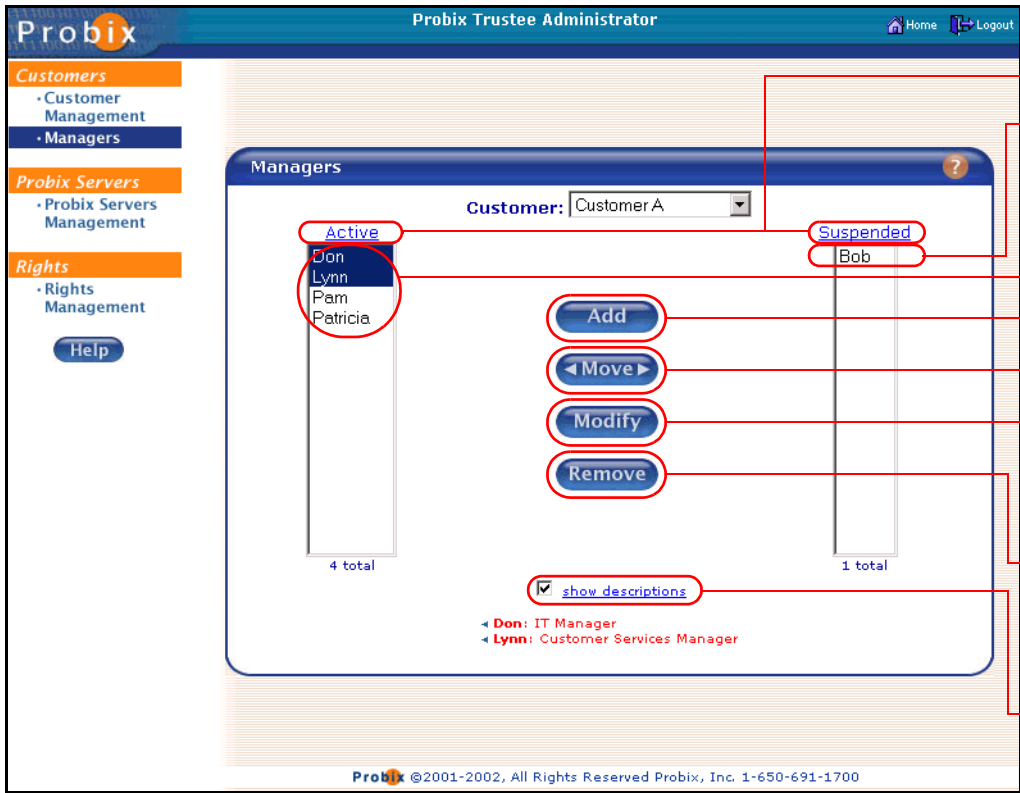
Click **OK** to export the selected customer to a file on your client, or **Cancel** to cancel the export.

# ADMINISTERING MANAGERS

A *manager* is a user who can manage a Probix Trustee customer.

**Note:** You must create at least one Customer before you can select a Manager.

Each Probix Trustee Customer needs at least one manager. A Customer can have more than one managers. To administer managers of a Probix Trustee site, select **Managers** from the navigation bar on the left to access the Managers Administration tool.



- Pull-down to select customer.
- Click to sort column.
- Suspended customers; left-click to select.
- Active customers; left-click to select.
- Click to add a customer.
- Click to activate or suspend a customer.
- Click to modify a customer.
- Click to remove a customer.
- Click to show descriptions of customers.

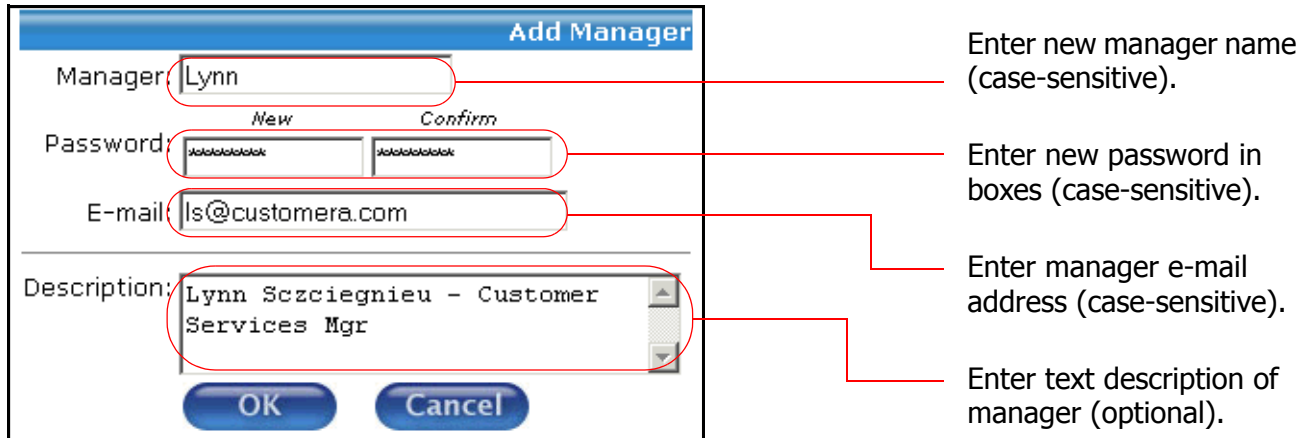
- Use the pull-down menu to select a Customer. The list of managers for that customer site appears.
- The **Active** column on the left shows all *active* managers. These are all users who can manage this Probix Trustee customer.
- The **Suspended** column on the right shows all *suspended* managers. These are all users who cannot manage this Probix Trustee customer.
- Clicking on the **Active** or **Suspended** heading sorts the list alphabetically in ascending order; clicking on the heading a second time sorts the list in descending order.
- Checking the **Show Descriptions** box causes the text from the Description of a manager to be displayed when you select that manager.

## Adding a Manager

To add a manager:

1. In the Manager Administration tool, select a **Customer:** from the drop-down menu.
2. Click **Add** to add a manager.

The Add Manager form appears.



The screenshot shows the 'Add Manager' dialog box with the following fields and annotations:

- Manager:** Lynn (Annotation: Enter new manager name (case-sensitive).)
- Password:** Two boxes labeled 'New' and 'Confirm' (Annotation: Enter new password in boxes (case-sensitive).)
- E-mail:** ls@customera.com (Annotation: Enter manager e-mail address (case-sensitive).)
- Description:** Lynn Szczegnieu - Customer Services Mgr (Annotation: Enter text description of manager (optional).)

Buttons: OK, Cancel

3. Enter the following in the **Add Manager** form:

- Manager:** enter the person's name as will appear in the Active and Suspended columns
- Password:** enter the password in the *New* and *Confirm* boxes
- E-mail:** person's e-mail address
- Description:** optional text description

4. Click **OK** to add the manager, or **Cancel** to return to the Managers Administration tool.

## Activating or Suspending a Manager

To activate or suspend a manager:

- 1. In the Manager Administration tool, select a customer.**



Use the pull-down **Customer:** menu to select a Customer from which the manager is to be suspended.

- 2. Select one or more managers to be activated or suspended.**

Use the left mouse button to select each manager you want to activate or suspend.

Left-clicking on a user name and pressing the **Shift** key as you move your cursor selects a consecutive set of managers. Press the **Ctrl** key and left-click individual managers to select multiple non-consecutive managers.

### 3. Change the status of the selected managers.

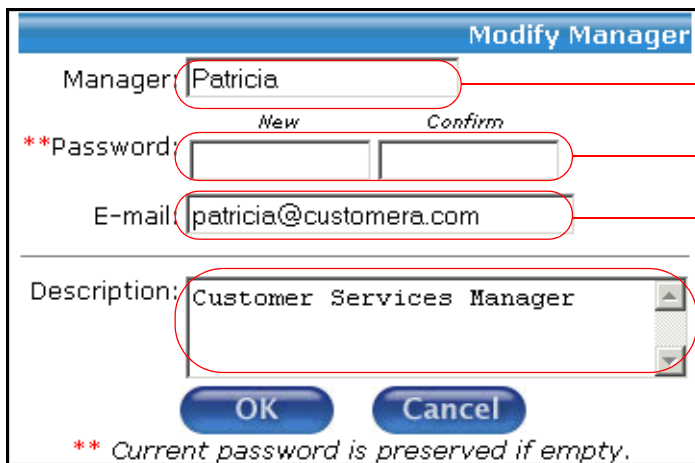
Click the  button to move managers from the **Active** column to the **Suspended** column, thus suspending them, or click the  button to move managers from the **Suspended** column to the **Active** column, thus activating them.

## Modifying a Manager

To modify a manager:

1. In the Manager Administration tool, select a **Customer:** from the drop-down menu.

The Modify Manager form appears.



Enter new manager name (case-insensitive).

Enter new password in boxes (case-sensitive).

Enter manager e-mail address (case-sensitive).

Enter text description of manager (optional).

2. Click **Modify** to modify a manager.
3. Change any of the following fields in the **Modify Manager** form:

- Manager:** change the person's name as it appears in the Active and Suspended columns
- Password:** enter a new password in the *New* and *Confirm* boxes
- E-mail:** change the person's e-mail address
- Description:** enter or change the optional text description

4. Click **OK** to modify the manager, or **Cancel** to return to the Managers Administration tool.

## Removing a Manager

To remove a manager:

1. **Select a manager to be removed.**

In the Manager Administration tool, select a **Customer:** from the drop-down menu. Then use the left mouse button to select one or more managers for removal.

2. **Remove the selected managers from that customer.**

Click **Remove**. A confirmation box appears.

### 3. Confirm the removal.

Click **OK** to remove the selected managers, or **Cancel** to cancel the removal.



# ADMINISTERING PROBIX SERVERS

A *Probix Server* is a server running the Probix Trustee server software for content protection. This is also referred to as Probix Content Protection Network (PCPN) software.

The screenshot shows the 'Probix Trustee Administrator' interface. On the left is a sidebar with sections: 'Customers' (Customer Management, Managers), 'Probix Servers' (Probix Servers Management, Administrators), and 'Rights' (Rights Management, Help). The main area is titled 'Probix Servers' and contains a table with one entry: 'Dragon Backup Server'. Below the table are buttons for 'Add', 'Modify', 'Remove', and a checked 'show locations' checkbox. A callout box shows details for the selected server: 'Dragon: Outer Monrovia Backup Server: Egg Beater, NJ'. Red lines connect callouts to the 'Server' heading, the table, the details box, and the action buttons.

- Click to sort column.
- Probix Servers; left-click to select.
- Physical locations of selected Probix Servers.
- Click to add a Probix Server.
- Click to modify a Probix Server.
- Click to remove a Probix Server.
- Click to show physical locations of Probix Servers.

- Clicking on the **Server** heading sorts the list alphabetically in ascending order; clicking on the heading a second time sorts the list in descending order.
- Checking the **show location** box causes the text describing the physical Location of a server to be displayed when you select that server.

## Adding a Probix Server

To add a Probix Server, in the Server Administration tool, click **Add**. The **Add Probix Server** form appears.

The screenshot shows the 'Add Probix Server' dialog box. It contains the following fields and controls:

- \*Server Name:** A text input field with a red circle around it. An annotation points to it: "Enter Probix Server name (case-insensitive)."
- \*Server IP Address:** A text input field with a red circle around it. An annotation points to it: "Enter the IP address for the Probix Server."
- TCP/IP Port:** A text input field with a red circle around it. An annotation points to it: "Enter the TCP/IP port of the Probix Server."
- Update Time:** A text input field containing '300' and a 'sec' label. A red circle is around the input. An annotation points to it: "Enter the update time (in seconds)."
- Time Window:** A text input field containing '15' and a 'sec' label. A red circle is around the input. An annotation points to it: "Enter the time window (in seconds)."
- Incremental Download:** Radio buttons for 'On' (selected) and 'Off'. An annotation points to the 'On' button: "Select whether to allow incremental downloads."
- Max Bix Chunk Size:** A text input field containing '1000' and a 'kbyte' label. A red circle is around the input. An annotation points to it: "Enter the time window (in seconds)." (Note: This annotation is likely a typo in the original document).
- Server Location:** A text input field with a red circle around it. An annotation points to it: "Enter physical location of the Probix Server (text)."
- Remarks:** A large text area with a red circle around it. An annotation points to it: "Enter text description of Probix Server (optional)."

At the bottom, there are 'OK' and 'Cancel' buttons, and a note: *\*Required field.*

Enter:

- \*Server Name:** the name of the Probix Server
- \*Server IP Address:** the IP address of the server ("nnn.nnn.nnn.nnn")
- TCP/IP Port:** the TCP/IP port of the server
- Update Time:** in seconds, indicates the period of time after which the time difference between the Probix Server and Customer Server is updated (default value is 300 seconds)
- Time Window:** in seconds, the time window in which the timestamp can vary from the time difference.
- Incremental Download:** Select either **On** or **Off** to determine whether to download the protected content incrementally.
- Max Bix Chunk Size:** in kbytes, the maximum size of an encrypted (protected) data packet.

**Server Location:** the physical location of server (text)  
**Remarks:** text remarks about the server (optional)

Fields marked with \* are required.

Click **OK** to add the server, or **Cancel** to leave the form and return the the Server Administration tool.

## Modifying a Probix Server

To modify a Probix Server, in the Server Administration tool, click **Modify**. The **Modify Probix Server** form appears.

The screenshot shows the 'Modify Probix Server' dialog box with the following fields and callouts:

- \*Server Name:** Backup Server. Callout: Enter Probix Server name (case-insensitive).
- \*Server IP Address:** 192.168.100.200. Callout: Enter the IP address for the Probix Server.
- TCP/IP Port:** 80. Callout: Enter the TCP/IP port of the Probix Server.
- Update Time:** 300 sec. Callout: Enter the update time (in seconds).
- Time Window:** 15 sec. Callout: Enter the time window (in seconds).
- Incremental Download:**  On  Off. Callout: Select whether to allow incremental downloads.
- Max Bix Chunk Size:** 1000 kbyte.
- Server Location:** Egg Beater, NJ. Callout: Enter physical location of the Probix Server (text).
- Remarks:** Backup Server. Callout: Enter text description of Probix Server (optional).

Buttons: OK, Cancel. Note: \*Required fields.

Modify any of the following:

**\*Server Name:** the name of the server  
**\*Server IP Address:** the IP address of the server ("nnn.nnn.nnn.nnn")  
**TCP/IP Port:** the TCP/IP port of the server  
**Update Time:** in seconds, indicates the period of time after which the time difference between the Probix Server and Customer Server is updated (default value is 300 seconds)

<b>Time Window:</b>	in seconds, the time window in which the timestamp can vary from the time difference.
<b>Incremental Download:</b>	Select either <b>On</b> or <b>Off</b> to determine whether to download the protected content incrementally.
<b>Max Bix Chunk Size:</b>	in kbytes, the maximum size of an encrypted (protected) data packet.
<b>Server Location:</b>	the physical location of server (text)
<b>Remarks:</b>	text remarks about the server (optional)

Fields marked with \* are required.

Click **OK** to add the server, or **Cancel** to leave the form and return the the Server Administration tool.

## Removing a Probix Server

To remove a Probix server, in the Server Administration tool:

### 1. Select a server to be removed.

Use the left mouse button to select one or more servers for removal.

### 2. Remove the selected servers.

Click **Remove**. A confirmation box appears.

### 3. Confirm the removal.

Click **OK** to remove the selected servers, or **Cancel** to cancel the removal.

# ADMINISTERING ADMINISTRATORS

An *administrator* is someone who can administer your Probix Trustee site.

Click to sort column.

Probix Trustee administrators ; left-click to select.

Click to add an administrator.

Click to activate or suspend an administrator.

Click to modify an administrator.

Click to remove an administrator.

Click to show descriptions of Probix Trustee administrators.

- The **Active** column on the left shows all *active* administrators. These are all users who can administer this Probix Trustee customer.
- The **Suspended** column on the right shows all *suspended* administrators. These are all users who cannot administer this Probix Trustee customer.
- Clicking on the **Active** or **Suspended** heading sorts the list alphabetically in ascending order; clicking on the heading a second time sorts the list in descending order.
- Checking the **Show Descriptions** box causes the text from the Description of an administrator to be displayed when you select that administrator.

## Adding an Administrator

To add an administrator to your Probix Trustee site:

1. In the Administrator Administration tool, click **Add** to add an administrator.

The Add Administrator form appears.

The screenshot shows the 'Add Administrator' form with the following fields and callouts:

- Administrator:** admin\_3 (Callout: Enter new administrator name (case-sensitive).)
- Password:** Two boxes labeled 'New' and 'Confirm' containing asterisks (Callout: Enter new password in boxes (case-sensitive).)
- E-mail:** ls@probix.com (Callout: Enter administrator e-mail address (case-sensitive).)
- Description:** Lynn Szczegnieu (Callout: Enter text description of administrator (optional).)

Buttons: OK, Cancel

2. Enter the following in the **Add Administrator** form:

- Administrator** enter the person's name as will appear in the Active and Suspended columns :
- Password:** enter the password in the *New* and *Confirm* boxes
- E-mail:** person's e-mail address
- Description:** optional text description

3. Click **OK** to add the manager, or **Cancel** to return the the Administrator Administration tool.

## Activating or Suspending an Administrator

**WARNING:** *Do not suspend the last administrator.* If you do, you will no longer be able to administer your Probix Trustee site unless you reinstall Probix Trustee.



To activate or suspend an Administrator:

**1. In the Administrator Administration tool, select one or more administrators to be activated or suspended.**

Use the left mouse button to select each administrator you want to activate or suspend.

Left-clicking on a user name and pressing the **Shift** key as you move your cursor selects a consecutive set of administrators. Press the **Ctrl** key and left-click individual administrators to select multiple non-consecutive administrators.

**2. Change the status of the selected administrators.**

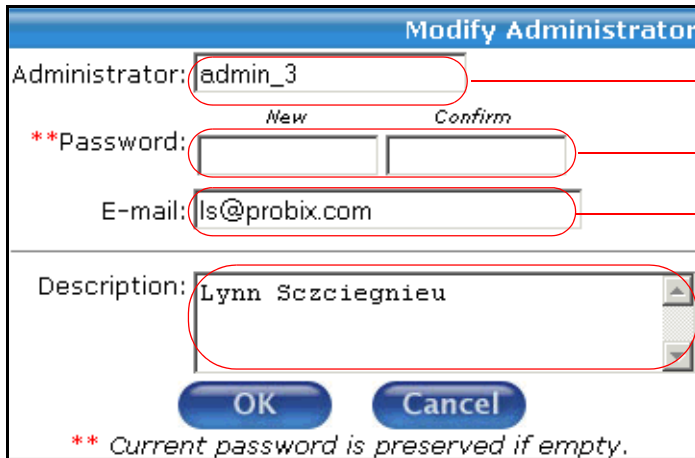
Click the  button to move administrators from the **Active** column to the **Suspended** column, thus suspending them, or click the  button to move administrators from the **Suspended** column to the **Active** column, thus activating them.

## Modifying an Administrator

To modify an administrator:

1. In the Administrator Administration tool, select an administrator to be modified.
2. Click **Modify** to modify an administrator.

The Modify Administrator form appears.



Change administrator name (case-insensitive).

Change password in boxes (case-sensitive).

Change administrator e-mail address (case-

Change text description of administrator

3. Change any of the following fields in the **Modify Administrator** form:

- Administrator** change the person's name as it appears in the Active and Suspended columns :
- Password:** enter a new password in the *New* and *Confirm* boxes
- E-mail:** change the person's e-mail address
- Description:** enter or change the optional text description

4. Click **OK** to modify the manager, or **Cancel** to return the the Administrator Administration tool.

## Removing an Administrator

**WARNING:** *Do not remove the last administrator. If you do, you will no longer be able to administer your Probix Trustee site unless you reinstall Probix Trustee.*

To remove an administrator:

1. **Select an administrator to be removed.**

In the Administrator Administration tool, use the left mouse button to select one or more administrators for removal.

2. **Remove the selected administrators.**

Click **Remove**. A confirmation box appears.

3. **Confirm the removal.**

Click **OK** to remove the selected administrators, or **Cancel** to cancel the removal.

# ADMINISTERING RIGHTS

A *right* is a permission given to a user or group to perform a specific action within a policy. Rights are the core of Probix Trustee.

Some rights are preloaded into the MySQL database when the Probix Trustee software is installed. You can add or remove rights, but they are non-functional unless the PCPN software already supports them.

The rights currently supported by Probix Trustee are:

- *print* - make a permanent copy of the content outside of control of the repository
- *view* - view the content
- *watermark* - enable watermarking when documents are printed

To administer rights on your Probix Trustee system, select **Rights Management** from the navigation bar on the left to access the Rights Management Administration tool.

- Clicking on the **Active** or **Suspended** heading sorts the list alphabetically in ascending order; clicking on the heading a second time sorts the list in descending order.
- Checking the **Show Descriptions** box causes the text from the Description of a user to be displayed when you select that user.

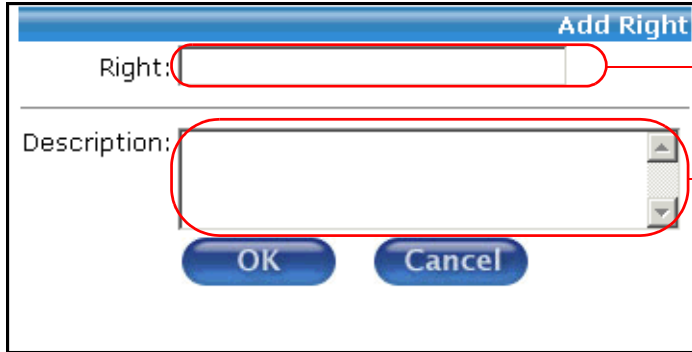


## Adding Rights

To add a right, in the Rights Administration tool:

1. Click **Add**.

The Add Right form appears.



Enter the name of the right being added.

Enter a text description of the right being added (optional).

2. In the **Add Right** form, enter the following fields:
  - **Right:** - the name of the right being added
  - **Description:** - a text description of the right being added
3. Confirm by clicking **OK** to add the right, or **Cancel** to cancel the form and return to the Rights Administration tool.

**Note:** Rights must be loaded using MySQL and must be implemented to work.

## Activating or Suspending a Right



To activate or suspend a right, in the Rights Administration tool:

1. **Select one or more rights to be activated or suspended.**

Use the left mouse button to select each right you want to activate or suspend.

Left-clicking on a right and pressing the **Shift** key as you move your cursor selects a consecutive set of rights. Press the **Ctrl** key and left-click individual rights to select multiple non-consecutive rights.

2. **Change the status of the selected rights.**

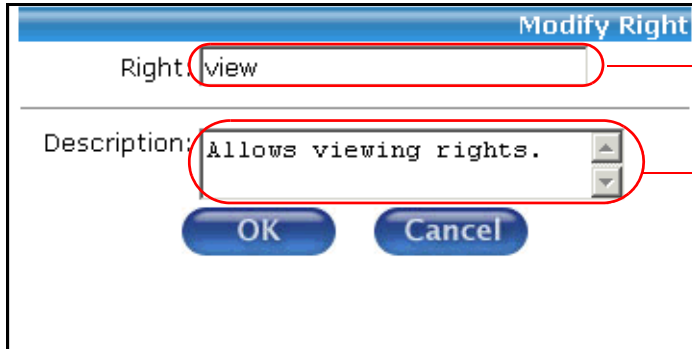
Click the  button to move rights from the **Active** column to the **Suspended** column, thus suspending them, or click the  button to move rights from the **Suspended** column to the **Active** column, thus activating them.

## Modifying a Right

To modify a right, in the Rights Administration tool:

1. Select the right to be modified, then click **Modify**.

The Modify Right form appears.



Enter the name of the right being added.

Enter a text description of the right being added (optional).

2. In the **Modify Right** form, change either or both of the following fields:
  - **Right:** - the name of the right being added
  - **Description:** - a text description of the right being added
3. Confirm by clicking **OK** to modify the right, or **Cancel** to cancel the form and return to the Rights Administration tool.

## Removing a Right

To remove a right, in the Rights Administration tool:

1. **Select a right to be removed.**

Use the left mouse button to select one or more rights for removal.

2. **Remove the selected rights.**

Click **Remove**. A confirmation box appears.

3. **Confirm the removal.**

Click **OK** to remove the selected rights, or **Cancel** to cancel the removal.

# Chapter 5

## ***Managing Probix Trustee Policies***

---

---

Probix Trustee™ extends existing online security measures to protect and monitor the use of confidential content after delivery to an authorized end-user. Managing a Probix Trustee site involves granting and denying access to users and content.

The Probix Content Protection Network (PCPN) Policy Manager lets you create and manage *policies*, *users*, and *groups* of users, granting and denying them access to *content* for your site.

This chapter discusses the following concepts and tasks involved in managing a Probix Trustee site:

- “Policy Manager Concepts” on page 68
- “Starting the Probix Trustee Policy Manager” on page 69
- “Managing Users” on page 70
- “Managing Groups” on page 74
- “Managing Group Members” on page 78
- “Managing Content” on page 80
- “Managing Policies” on page 87
- “Using the IIS Import Tool” on page 99

# POLICY MANAGER CONCEPTS

You need to understand the following concepts before you use the Probix Trustee Policy Manager.

## Content

*Content* is one or more files or directories to which access is being granted by Probix Trustee.

Probix Trustee supports the following types of content:

- One or more directories
- HTML, including web pages and dynamic files created by ASP, PHP, JSP, and CGI scripts

**Note:** Sessions are not supported. Applets are supported, but are displayed in clear (unprotected).

- Adobe Acrobat (PDF) versions 4.0 and 5.0
- Microsoft Office 2000 and Office XP (Word, Excel, and PowerPoint)
- HWP 2000 files (also HWP 97 files via the HWP 2000 plugin)
- ASCII text, including web pages and dynamic files created by ASPs or CGI scripts
- JPEG files
- GIF files
- BMP files

For more details on support of content types, see "Managing Content" on page 80.

## User

A *user* is an individual to whom access to your content is granted. Users can be added to groups.

## Group

A *group* is a collection of users over which you can simultaneously distribute access permissions. A group is comprised of a group name, a group description, and users.

## Members

*Members* are users who belong to a group.

## Policy

A *policy* is a collection or organization of the groups, custom rights, groupings, and schedules of access to your content. A policy lets you define the length of time an individual or group can access content and the types of access granted to the content.

## Schedule

A *schedule* is a window of time during which a user is granted access to secured content.

## Active/Suspended

The terms *active* and *suspended* have varying meanings depending upon the context in which they are used. An active user has access to the PCPN; a suspended user has had that access denied. Similarly, an active piece of content can be accessed by users of the PCPN; a suspended piece of content is one on which access has been revoked. Suspended items often appear in grayed-out text.

This chapter explains why you might want to activate or suspend a user, content, or access rights, as well as what those terms mean in those contexts.

## STARTING THE PROBIX TRUSTEE POLICY MANAGER

To use the Probix Trustee Policy Manager, enter the URL:

`https://myhost:port/trustee/`

where:

*myhost* is the name of your host

*port* is the port number on which you are running Probix Trustee

Enter the following:

- **Customer ID** - the name of the customer. This can be entered case-insensitive, but it appears in whatever case it was entered into the Customer database.
- **User Name** - the user name of the Probix Trustee Policy Manager user; case-sensitive.
- **Password** - the password of the Probix Trustee Policy Manager user; case-sensitive

After you click Login, a welcome screen similar to the following appears.

Click to manage users.

Click to manage groups.

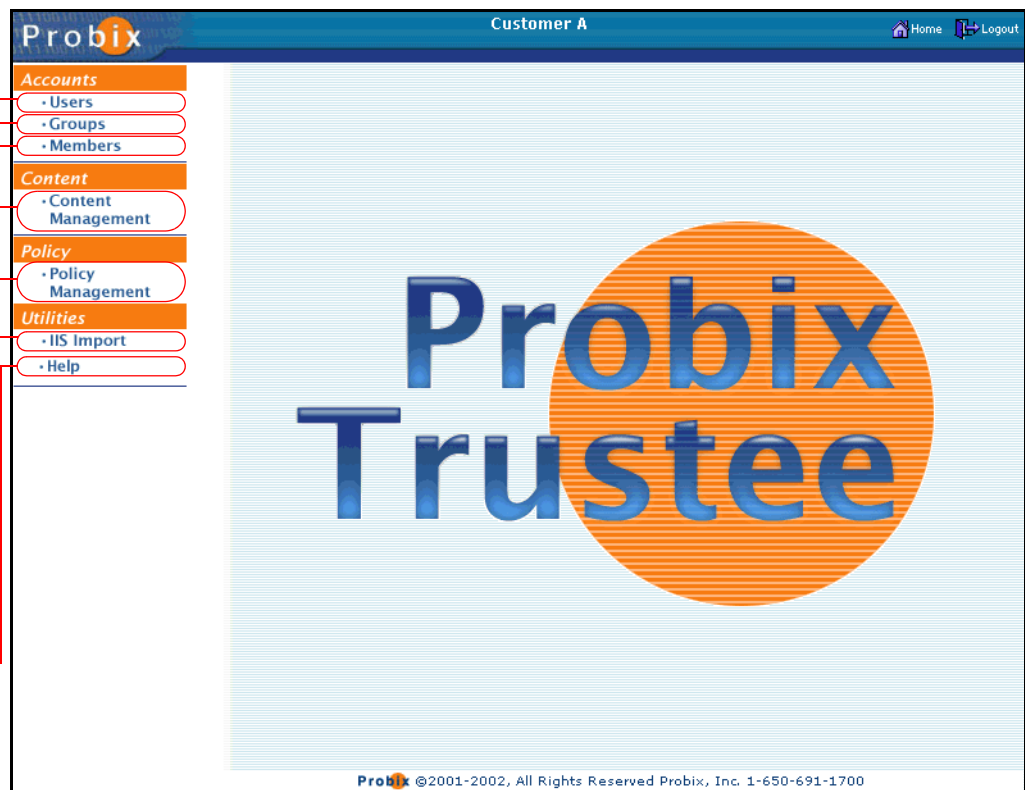
Click to manage members.

Click to manage content.

Click to manage policies.

Click to manage rights.

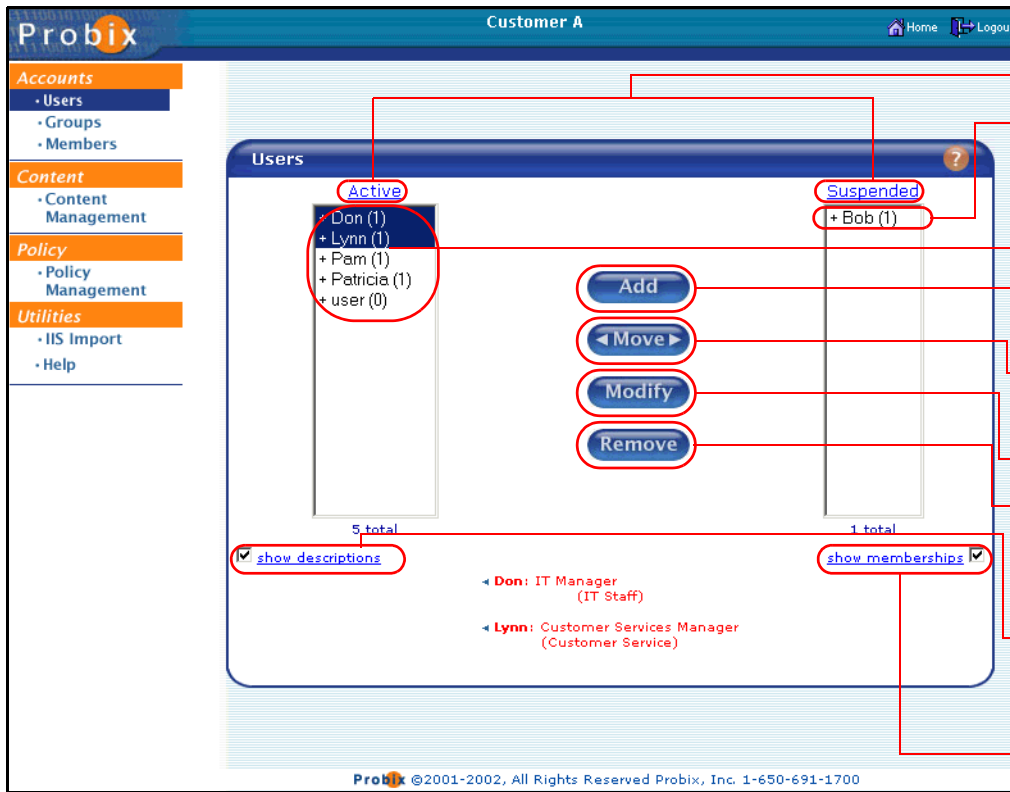
Click for online help.



From here you can manage users, groups of users, members of groups, content, and policies.

# MANAGING USERS

To manage users of your Probix Trustee system, select **Users** from the navigation bar on the left to access the Users Administration tool.



- Click to sort column.
- Suspended users; left-click to select.
- Active users; left-click to select.
- Click to add a user.
- Click to activate or suspend a user.
- Click to modify a user.
- Click to remove a user.
- Click to show descriptions of users.
- Click to show memberships in groups.

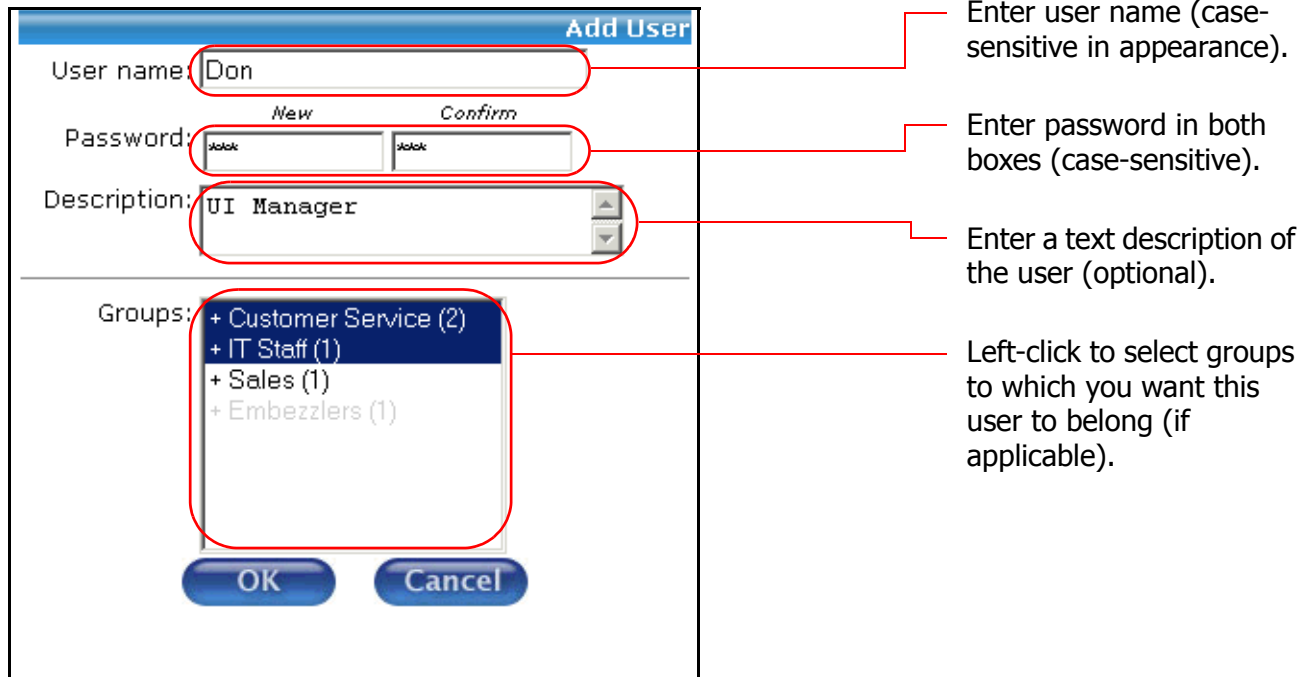
The first Probix Trustee user (Default user) is automatically created when you install Probix Trustee.

- The **Active** column on the left shows all *active* users. These are all users who can use Probix Trustee.
- The **Suspended** column on the right shows all *suspended* users. These are all users who cannot use Probix Trustee.
- Clicking on the **Active** or **Suspended** heading sorts the list alphabetically in ascending order; clicking on the heading a second time sorts the list in descending order.
- Checking the **Show Descriptions** box causes the text from the Description of a user to be displayed when you select that user.
- Checking the **Show Memberships** box lets you view Descriptions of groups to which the selected users belong.

To view the list of groups to which a user belongs, double-click on the user name. To collapse the list, double-click on the name again. The number to the right of the (#) next to the name in the listing is the number of groups to which the specified user belongs.

## Adding a User

To add a user, in the User Administration tool, click the **Add** button. The Add User form appears.



The screenshot shows the 'Add User' dialog box. It has a title bar 'Add User' and four main sections: 'User name:' with a text box containing 'Don'; 'Password:' with two sub-boxes labeled 'New' and 'Confirm', both containing '123456'; 'Description:' with a text box containing 'UI Manager'; and 'Groups:' with a list box containing four items: '+ Customer Service (2)', '+ IT Staff (1)', '+ Sales (1)', and '+ Embezzlers (1)'. The 'IT Staff (1)' item is highlighted in blue. At the bottom are 'OK' and 'Cancel' buttons. Red lines connect text boxes to descriptive annotations on the right.

- In the **User name:** box enter the name of the user. The name is case-sensitive for appearance in Probix Trustee, but case-insensitive when you login as that user.
- Enter the password into the **Password:** box and again in the **Confirm Password:** box.
- You can also enter an optional text description of the user in the **Description:** box; this is displayed when the **Show Descriptions** box is checked.
- Highlight any **Groups:** in which this user is to belong (if applicable). Note that suspended groups are grayed-out.

Click **OK** to save the new user, or click **Cancel** to abort the changes.

## Activating and Suspending Users

When users are created they are automatically active and appear in the left, or **Active** column. When you want to terminate a user's access to Probix Trustee, you suspend them, and they appear in the right, or **Suspended** column.

There are reasons you might prefer to suspend, rather than delete, a user of Probix Trustee. Possible scenarios include:

- One of the users left their password written on a paper on their desk, and a disgruntled employee saw the sheet of paper and gained access to their account.
- A user is going on a Leave of Absence.
- A user is leaving your company, but other people still need access to the same documents the user can access.



To activate or suspend a user:

### 1. Select one or more users to be activated or suspended.

Use the left mouse button to select each user name you want to activate or suspend.

Left-clicking on a user name and pressing the **Shift** key as you move your cursor selects a consecutive set of user names. Press the **Ctrl** key and left-click individual user names to select multiple non-consecutive user names.

### 2. Change the status of the selected users.

Click the  button to move users from the **Active** column to the **Suspended** column, thus suspending them, or click the  button to move users from the **Suspended** column to the **Active** column, thus activating them.

## Modifying a User

There are times when you may want to change a user's access privileges. For example:

- A user is promoted to management and needs more access to privileged data.
- A user changes departments and needs different kinds of access.
- A user leaves the company as an employee, but remains on in an advisory capacity.

To modify a user:

### 1. In the User Administration tool, select the user you want to modify.

Use the left mouse button to select the user name of the user you want to modify.

### 2. Enter changes to the user.

Click **Modify**. The Modify User form appears.

Enter new user name (case-sensitive in appearance).

Enter new password in both boxes (case-sensitive).

Enter a new text description of the user (optional).

Select groups to which you want this user to belong; deselect groups to remove user from them.

- To change the user name, enter a different user name in the **User name:** box.



- To change the password, enter the password into the **Password:** box and the **Confirm Password:** box.
- To change the text description of the user, edit the text in the **Description:** box. This text appears when the user is selected and the **Show Descriptions** box is checked.
- To add this user to one or more **Groups**, highlight the names of groups to which you want the user to belong, *including* those groups to which this user is already assigned. Note that suspended groups are grayed-out.
- To remove this user from groups, press Ctrl and left-click on each highlighted group from which you want to remove the user.

### 3. Confirm.

Click **OK** to save the modified user, or **Cancel** to abort the changes and return to the User Administration tool.

## Removing a User

To remove one or more users:

### 1. In the User Administration tool, select the users you want to remove.

Use the left mouse button to select the user name you want to remove. Left-clicking on a user name and pressing the **Shift** key as you move your cursor selects a consecutive set of user names. Press the **Ctrl** key and left-click individual user names to select multiple non-consecutive user names.

### 2. Remove the selected users.

Click **Remove**. A confirmation box appears.

### 3. Confirm the removal.

Click **OK** to remove the selected users, or **Cancel** to cancel the removal.

## MANAGING GROUPS

A *group* is a collection of rights given to a user. Groups enable you to manage the types of operations that can be performed on your content.

To manage groups of your Probix Trustee system, select **Groups** from the navigation bar on the left to access the Group Administration tool. The Group Administration tool appears.

The screenshot shows the Probix Group Administration tool interface. The top navigation bar includes 'Customer A', 'Home', and 'Logout'. The left sidebar contains menu items: 'Accounts' (Users, Groups, Members), 'Content' (Content Management), 'Policy' (Policy Management), and 'Utilities' (IIS Import, Help). The main content area is titled 'Groups' and is divided into two columns: 'Active' and 'Suspended'. The 'Active' column lists three groups: 'Customer Service (2)', 'IT Staff (1)', and 'Sales (1)'. The 'Suspended' column lists one group: 'Embezzlers (1)'. Below the lists are buttons for 'Add', 'Move', 'Modify', and 'Remove'. At the bottom, there are checkboxes for 'show descriptions' and 'show memberships'. Callouts with red lines point to various elements: 'Active' and 'Suspended' headings, the group names and counts, the 'Add', 'Move', 'Modify', and 'Remove' buttons, the 'show descriptions' and 'show memberships' checkboxes, and the footer text.

Click to sort column.

Suspended group; left-click to select.

Active groups; left-click to select.

Click to add a group.

Click to activate or suspend a group.

Click to modify a group.

Click to remove a group.

Click to show descriptions of groups.

Click to show users with memberships in selected groups.

- Clicking on the **Active** or **Suspended** heading sorts the list alphabetically in ascending order; clicking on the heading a second time sorts the list in descending order.
- Checking the **Show Descriptions** box causes the text from the Description of a group to be displayed when you select that group.
- Checking the **Show Memberships** box lets you view the members of the selected group.
- To view the list of users that belong to a selected group, double-click on the group name. To collapse the list, double-click on the name again. The number to the right of the (#) next to the group name in the listing is the number of users that belong to that group.

## Adding a Group

To add a group, in the Group Administration tool, click the **Add** button.

The Add Group form appears.

The screenshot shows the 'Add Group' dialog box with the following fields and options:

- Group:** A text input field containing 'Customer Service'.
- Description:** A text input field containing 'Customer Service Managers'.
- Users:** A list box containing the following entries: '+ Don (0)', '+ Lynn (0)', '+ Pam (0)', '+ Patricia (0)', '+ user (0)', and '+ Bob (0)'. The entries '+ Lynn (0)' and '+ Patricia (0)' are selected.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom.

Red circles highlight the 'Group:', 'Description:', and 'Users:' sections. Red lines connect these circles to explanatory text on the right:

- Enter group name (case-sensitive).
- Enter a text description of the group (optional).
- Select users to belong to this group; deselect users to remove them from this group (if applicable)

- In the **Group:** box enter the name of the group.
- You can also enter an optional text description of the group in the **Description:** box; this is displayed when the **Show Descriptions** box is checked.
- In the **Users:** box, select the users to belong to this group. Note that suspended users are grayed-out.

Click **OK** to save the new group, or click **Cancel** to abort the changes and return to the Group Administration tool.

## Activating and Suspending Groups

When groups are created they are automatically active and appear in the left, or **Active** column. When you want to terminate a group's access to Probix Trustee, you suspend it, and it appears in the right, or **Suspended** column.

There are reasons you might prefer to suspend, rather than delete, a Probix Trustee group. Possible scenarios include:

- A group of users were given access to content via Probix Trustee that had been intended for a smaller audience.
- Part of your company has been sold to another company, and some of the information previously available to a group needs to be made unavailable.



To activate or suspend a group:

### 1. Select one or more groups to be activated or suspended.

Use the left mouse button to select each group you want to activate or suspend.

Left-clicking on a group and pressing the **Shift** key as you move your cursor selects a consecutive set of groups. Press the **Ctrl** key and left-click individual groups to select multiple non-consecutive groups.

## 2. Change the status of the selected groups.

Click the  button to move groups from the **Active** column to the **Suspended** column, thus suspending them, or click the  button to move groups from the **Suspended** column to the **Active** column, thus activating them.

## Modifying a Group

There are times when you may want to change the name or description of a group of users. For example:

- A group of users are reorganized under a different division.
- A group of users have been moved to a different organization.

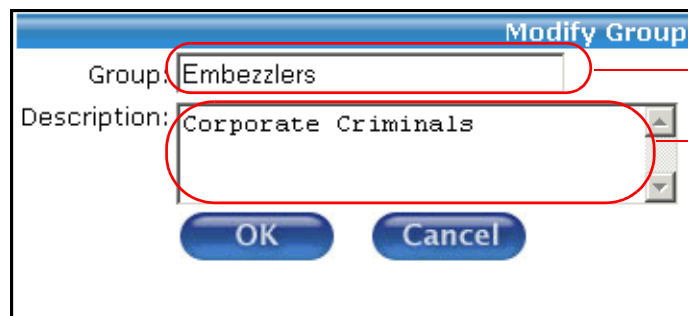
To modify a group:

### 1. In the Group Administration tool, select the group you want to modify.

Use the left mouse button to select the group you want to modify.

### 2. Modify the group.

Once you have selected the group to be changed, click **Modify**. The Modify Group form appears.



Enter a new group name (case-sensitive).

Enter a new text description of the group (optional).

- To change the the name of the group, enter a different group name in the **Group:** box.
- To change the text description of the group, edit the text in the **Description:** box. This text appears when the group is selected and the **Show Descriptions** box is checked.

### 3. Confirm.

Click **OK** to save the modified group, or **Cancel** to abort the changes and return the the Group Administration tool.

## Removing a Group

To remove one or more groups of users:

### 1. In the Group Administration tool, select the groups you want to remove.

Use the left mouse button to select the group you want to remove. Left-clicking on a group name and pressing the **Shift** key as you move your cursor selects a consecutive set of groups. Press the **Ctrl** key and left-click individual group names to select multiple non-consecutive groups.

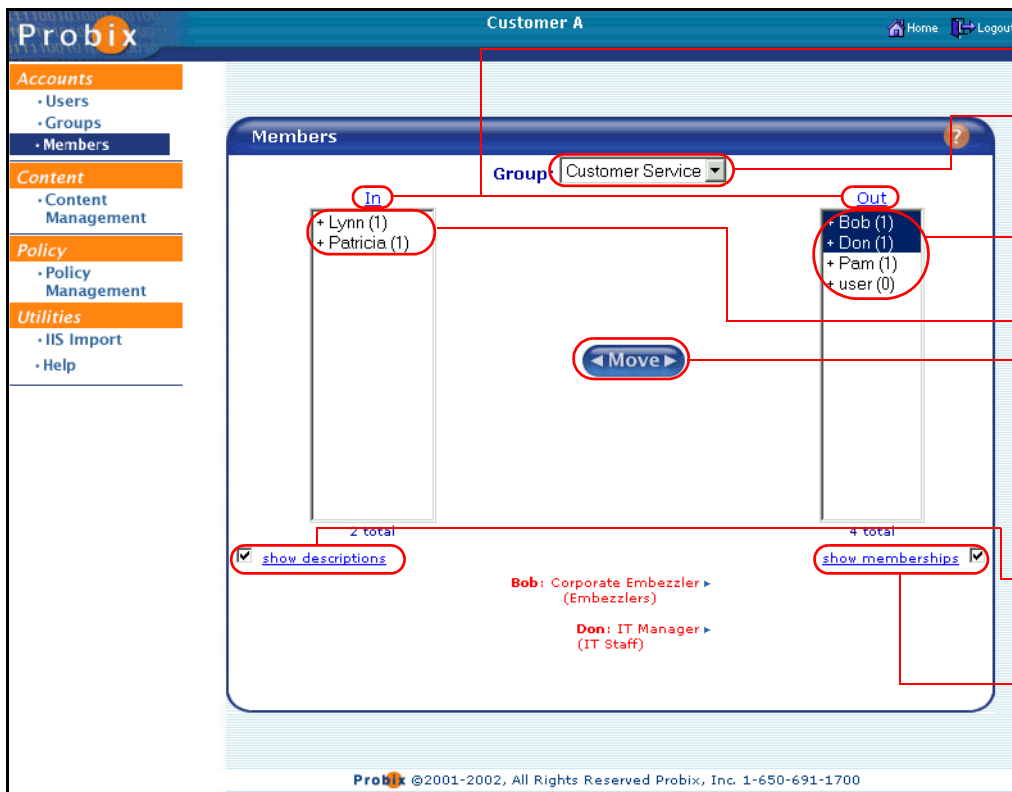
## 2. Remove the selected groups.

Click **Remove**. A confirmation box appears.

Click **OK** to remove the selected groups, or **Cancel** to cancel the removal and return to the Group Administration Tool.

## MANAGING GROUP MEMBERS

To manage group members of your Probix Trustee system, select **Members** from the navigation bar on the left to access the Members Administration tool.



Click to sort column.

Use pull-down menu to select the active group.

Suspended users; left-click to select.

Active groups; left-click to select.

Click to move a member in or out of a group.

Click to show descriptions of groups.

Click to show users with memberships in selected groups.

**Note:** You must have at least one group created before you can add members to it. If you select **Members** and no groups exist, you are automatically navigated into the Group Administration tool.

- The **In** column on the left shows all users who are members of the specified group.
- The **Out** column on the right shows all users who are not members of the specified group.
- Clicking on the **In** or **Out** heading sorts the list alphabetically in ascending order; clicking on the heading a second time sorts the list in descending order.
- Checking the **Show Descriptions** box causes the text from the Description of a group to be displayed when you select that user.
- Checking the **Show Memberships** box lists all groups of which the selected users are members.

**Note:** Suspended users are grayed-out.

To move a user in or out of a group:

### 1. Select a group.



Use the drop-down **Group** menu to select the active group.

### 2. Select one or more group members to be moved.

Use the left mouse button to select each group member you want to move in or out of the selected group.

Left-clicking on a group member and pressing the **Shift** key as you move your cursor selects a consecutive set of group members. Press the **Ctrl** key and left-click individual group members to select multiple non-consecutive group members.

### 3. Change the status of the selected users.

Click the  button to move group members from the **In** column to the **Out** column, thus suspending them, or click the  button to move group members from the **Out** column to the **In** column, thus making them members of the selected group.

## MANAGING CONTENT

*Content* is one or more files or directories to which access is being granted by Probix Trustee.

Probix Trustee supports the following types of content:

- One or more directories
- HTML, including web pages and dynamic files created by ASP, PHP, JSP, and CGI scripts
- Adobe Acrobat (PDF) versions 4.0 and 5.0
- Microsoft Office 2000 and Office XP (Word, Excel, and PowerPoint)
- HWP 2002 files (also HWP 97 files via the HWP 2002 plugin)
- ASCII text, including web pages and dynamic files created by ASPs or CGI scripts
- JPEG files
- GIF files
- BMP files

### Limitations of Support of Some Content Types

The following types of content have limited support:

#### HTML Support

HTML files are supported with the following restrictions:

- JavaScript functions that manipulate windows (window.\*) are not supported.
- Applets are supported, but are unprotected (clear).
- Sessions are not supported.
- GET and POST requests are sent unencrypted, but GET and POST responses requesting content protected by Probix are sent encrypted. Content that is not protected by Probix cannot be retrieved using these methods on a protected HTML page
- Embedded objects, including third-party plugins, are supported, but are not always protected.

#### MS Word File Support

Most MS Word features are supported in protected documents, but with the following restrictions:

- Saving is disabled.
- Printing is allowed per the print policy set by the sender.
- Cut and copy are disabled.
- Print screen is disabled.
- Screen captures are prevented.
- Drag and drop is disabled.
- The document is covered when the browser plugin window is not the focus window.
- Toolbars are disabled.
- You cannot add toolbars from the **View->Toolbars** menu.



- The formula bar does not appear, even from the **View->Toolbars** menu.
- Hot keys (such as **Ctrl-P** for print) are disabled.

Probix Trustee for Outlook does not allow recipients to edit (modify) the Word documents. Probix Trustee for Outlook uses MS Word's native "Comments" protection capability as found in the **Tools->Protection** menu. In this mode:

- editing of the document is not allowed
- some types of embedded images can be moved inside the document, such as MS Word Art objects
- you cannot hide lower level sentences in Outline mode
- the filename field in the document is incorrect
- in Office 2000, page numbering is incorrect

### **MS Excel File Support**

Most Excel features are supported in protected documents, but with the following restrictions:

- Saving is disabled.
- Printing is allowed per the print policy set by the sender.
- Cut and copy are disabled.
- Print screen is disabled.
- Screen captures are prevented.
- Drag and drop is disabled.
- The document is covered when the browser plugin window is not the focus window.
- Toolbars are disabled.
- You cannot add toolbars from the **View->Toolbars** menu.
- The formula bar does not appear, even from the **View->Toolbars** menu.
- Hot keys (such as **Ctrl-P** for print) are disabled.

Probix Trustee for Outlook allows recipients to edit (modify) the Excel documents, depending upon whether the sender gives them the option to do this, by using Excel's native protection capabilities. Probix Trustee for Outlook enables the integrity of documents but does not require it. A recipient may also modify an Excel document and print it with a watermark, if allowed.

Probix Trustee for Outlook uses MS Excel's native "Protect Sheet" and "Protect Workbook" capabilities as found in the **Tools->Protection** menu. In this mode:

- Hyperlinks within Excel document are supported.
- Links from a protected Excel document to an unprotected Excel document are supported.
- All other behaviors expected from a Sheet-Protected Excel document.
- At "Protect Sheet" level, sheets set within Workbooks can be altered (insert, remove, rename).
- At "Protect Workbook" level, the aforementioned applies, except sheets set within Workbooks cannot be altered.

## HWP File Support

Probix Trustee for Outlook supports HWP 2000 protected documents, but with the following restrictions:

- Saving is disabled.
- Printing is allowed per the print policy set by the sender.
- Cut and copy are disabled.
- Print screen is disabled.
- Screen captures are prevented.
- Drag and drop is disabled.
- The document is covered when the browser plugin window is not the focus window.
- Toolbars are disabled.
- Hot keys (such as **Ctrl-P** for print) are disabled.

**Note:** You must have HWP 2000 installed to view HWP 2000 or HWP 97 format files.

To manage content on your Probix Trustee system, select **Content** from the navigation bar on the left to access the Content Administration tool.

Click to sort column.

Suspended content; left-click to select.

Active content; left-click to select.

Click to add a content item.

Click to activate or suspend content.

Click to modify a content item.

Click to remove selected content.

Click to show descriptions of selected content items.

- The **Active** column on the left shows all *active* content items. These are all content items that can be accessed by using Probix Trustee.
- The **Suspended** column on the right shows all *suspended* content items. These are all content items that can no longer be accessed by using Probix Trustee.

- Clicking on the **Active** or **Suspended** heading sorts the list alphabetically in ascending order; clicking on the heading a second time sorts the list in descending order.
- Checking the **Show Descriptions** box causes the text from the Description of a content item to be displayed when you select that content item.

## Adding Content

**Note:** Before you add content here, you must have the Probix Trustee Customer Server package installed, and your file must be accessible by the Probix Trustee Customer Server.

To add a content item to Probix Trustee, as the Apache user, first copy it to the content directory on the Customer Server. This is usually `$APACHE_DIR/htdocs/secure/customer_ID` where `$APACHE_DIR` is the location of your Apache directory and `customer_ID` is your customer ID.

Next, in the Content Administration tool, click the **Add** button. The Add Content form appears.

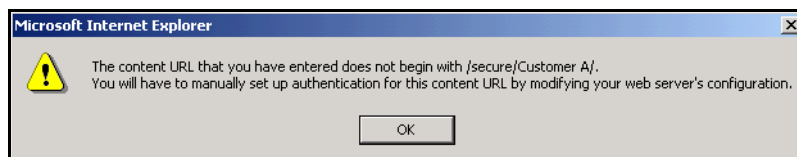
Enter the path to the content directory or file (case-sensitive).

Enter a text description of the content directory or file (optional).

- In the **URL:** box, enter the path of the content directory or file.
- You can also enter an optional text description of the content item in the **Description** box; this is displayed when the **Show Descriptions** box is checked.

Click **OK** to save, or **Cancel** to abort the adding of content and return to the Content Administration tool.

**Note:** If you are adding content to a directory other than the default protected directory, a pop-up window appears similar to the following:



Click **OK** to continue.

The directory is created, and the content is added, but the content cannot be accessed until you enable file authentication for the directory on the content server as follows:

1. As the root user, log into the server on which the content is stored.
2. Edit the file `$APACHE_DIR/conf/httpd.conf`.
  - a. Search for the string "secure" until you are above a `Directory` block similar to the following:

```
#Require authentication on Trustee secure folder
<Directory /usr/local/apache/htdocs/secure>
    AuthName "Probix Protected Document."
    AuthType Basic
```

```
SSLRequireSSL
PCPNCustAuthBy user
require valid-user
</Directory>
```

- b. Duplicate this Directory block, changing the directory name in the duplicated block to the directory you entered in the Policy Manager. For example, if you entered `myDirectory` in the Policy Manager, you need to change the first line in the new block to:

```
<Directory /usr/local/apache/htdocs/myDirectory>
```

3. Stop and restart the apache server by entering:

```
cd $APACHE_DIR/bin
webstop
webstart
```

## Adding Portable Content

This feature lets you physically separate the delivery of your important documents from delivery of the decryption keys that enable it to be viewed. If you have a lot of data your users do not need to access often, you may want use this feature to store the content on a portable device, such as a CD-ROM, floppy disk, or downloadable file, and just keep the encryption keys for the content on the Content Server, saving on disk space. The content formats supported for this feature are:

- Files with extensions `.doc`, `.ppt`, `.pps`, `.pdf`
- Adobe Acrobat (PDF) versions 4.0 and 5.0
- Microsoft Office 2000 and Office XP (Word, Excel, and PowerPoint)
- HWP 2002 files (also HWP 97 files via the HWP 2002 plugin)

To use this feature:

### 1. Use the `pmm-tool` to encrypt the PDF files and generate keys for them.

The `pmm-tool` utility is located in the `$APACHE_DIR/pcpncust` directory. It takes three parameters - a `doc_root` directory path, the Volume label ( `Volume`), and an encryption algorithm (`-alg DES | TDES | AES`), and creates the following directories:

- `doc_root/clear/Volume/` - source files
- `doc_root/encrypt/Volume/` - encrypted files
- `doc_root/secure/Volume/` - pmm placeholders

The `pmm-tool` utility scans `doc_root/clear/Volume/` for all supported file types. It then prepares and puts corresponding encrypted file in the `doc_root/encrypt/Volume/` directory and `*.pmm` files in the `doc_root/secure/CD_Volume/` directory.

For example, if you have a file called `"x.pdf"` in the directory `/usr/bob/portable` and you enter on one line:

```
$APACHE_DIR/pcpncust/pmm-tool -root /usr/bob/portable -label
my_portable_files -alg DES
```

The `pmm-tool` creates the following:

- `/usr/bob/portable/clear/my_portable_files/x.pdf` - source file
- `/usr/bob/portable/encrypt/my_portable_files/x.pdf` - encrypted file
- `/usr/bob/portable/secure/my_portable_files/x.pmm-_pdf` - pmm placeholder

## 2. Move the files to the distribution media and Content Server.

Move the files from `doc_root/encrypt/Volume/` to the distribution media (CD-ROM, memory stick, floppy disk, etc.).

Move the files from `doc_root/secure/Volume/` to your Content Server.

## Activating and Suspending Content

When content is added to the server it is automatically active and appears in the left, or **Active** column. When you want to quickly terminate access to one or more Probix Trustee content items, you suspend them, and they appear in the right, or **Suspended** column.

There are reasons you might prefer to suspend, rather than delete, a Probix Trustee content item. Possible scenarios include:

- The content item contains a fact error that needs to be corrected; it can then be uploaded and reactivated.
- The wrong file was uploaded to the Probix Trustee server.



To activate or suspend one or more content items, in the Content Administration tool:

### 1. Select one or more content items to be activated or suspended.

Use the left mouse button to select each content item you want to activate or suspend.

Left-clicking on a content item and pressing the **Shift** key as you move your cursor selects a consecutive set of content items. Press the **Ctrl** key and left-click individual content items to select multiple non-consecutive content items.

### 2. Change the status of the selected content items.

Click the  button to move content items from the **Active** column to the **Suspended** column, thus suspending them, or click the  button to move content items from the **Suspended** column to the **Active** column, thus activating them.

## Modifying Content

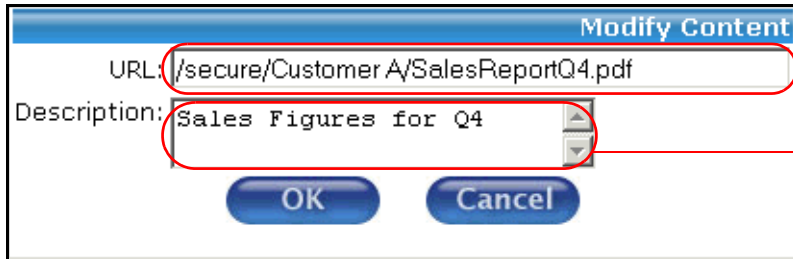
To modify the description of a content item:

### 1. In the Content Administration tool, select the content item you want to modify.

Use the left mouse button to select the content item you want to modify.

## 2. Modify the content description.

Once you have selected the content to be changed, click **Modify**. The Modify Content form appears.



Change the path to the content item (case-sensitive).

Enter a new text description of the content item (optional).

Here you can edit:

- the **URL**.
- the text description of the content item in the **Description** box. This text appears when the group is selected and the **Show Descriptions** box is checked.

## 3. Confirm.

Click **OK** to save, or **Cancel** to abort the change and return to the Content Administration tool.

## Removing Content

**Note:** Content that is removed from the list is permanently removed from the Probix Trustee server. To be active again, content must be readded to the Probix Trustee server.

To remove one or more content items from the Probix Trustee server:

### 1. In the Content Administration tool, select the content items you want to remove.

Use the left mouse button to select the content items you want to remove. Left-clicking on a content item and pressing the **Shift** key as you move your cursor selects a consecutive set of content items. Press the **Ctrl** key and left-click individual content items to select multiple non-consecutive content items.

### 2. Remove the selected content items.

Click **Remove**. A confirmation box appears.

### 3. Confirm.

Click **OK** to remove the selected content items, or **Cancel** to leave the content items on the Probix Trustee server and return to the Content Administration Tool.

# MANAGING POLICIES

A *policy* is a collection or organization of the groups, custom rights, groupings, and schedules of access to your content. A policy lets you define the length of time a user or group of users can access content, along with the types of access granted to the content.

To manage policies on your Probix Trustee system, select **Policy Management** from the navigation bar on the left to access the Policy Manager. The policies that exist on your Probix Trustee system appear in descending priority order under the **Active** and **Suspended** columns.

The screenshot shows the Probix Policy Management interface. On the left is a navigation menu with categories: Accounts (Users, Groups, Members), Content (Content Management), Policy (Policy Management), and Utilities (IIS Import, Help). The main area is titled 'Policies' and is split into two columns: 'Active' (containing one policy, 'Sample Policy') and 'Suspended' (empty). Between the columns are buttons for 'Add', 'Move', 'Modify', and 'Remove'. Below the columns are a 'show descriptions' checkbox (checked) and a 'Sample Policy: Example of a policy' link. A 'PRIORITY' arrow is on the left of the Active column. Callouts on the right explain: 'Click to sort column.' (points to the priority arrow), 'Suspended policies; left-click' (points to the Suspended column), 'Active policies; left-click to select.' (points to the Sample Policy), 'Click to add a policy.' (points to the Add button), 'Click to activate or suspend a policy.' (points to the Move button), 'Click to modify a policy.' (points to the Modify button), 'Click to remove a policy.' (points to the Remove button), and 'Click to show descriptions of selected policies.' (points to the show descriptions checkbox).

**Note:** When setting relative priorities of your policies, position the stricter policies above looser ones so the stricter policies are not overridden. A less restrictive policy with a higher priority than a more restrictive one overrides the restrictions of the more restrictive policy.

- Checking the **Show Descriptions** box causes the text from the Description of a content item to be displayed when you select that content item.
- Clicking the **Edit** tab displays the details of a policy (the Description, Content, Accounts, Rights, and Schedules), highlight the policy name, click **Modify**, then click the **Display** tab. To exit the screen and view another policy, you must click **Close**.

**Note:** Although you can grant print access to secure content, there are restrictions:

- If print access is not granted to a document, the print commands and icons are grayed out.
- If "print once" access is granted to a document, the print commands and icons remain after the document has been printed, but the end user is no longer able to print the document.
- Printing overlapping ranges in programs that normally permit it is disabled. This affects printing of PowerPoint, MS Word, HWP, ASCII text, JPG, and GIF files.

## Adding a Policy

To add a policy, in the Policy Manager, click the **Add** button. The Add Policy form appears.

Enter policy name (case-sensitive).

Use the drop-down menu to select the policy position relative to other policies

Enter a text description of the user (optional).

### 1. Name the policy.

- In the **Policy** box enter the name of the policy.
- In the **Priority** box, use the drop-down menu to set the priority.
- You can also enter an optional text description of the policy in the **Description** box; this is displayed when the **Show Descriptions** box is checked.

Click **OK** to add the policy and proceed to the **Edit** tab, or click **Cancel** to abort the addition.

Policy name and description; click to view policy.

Click to save the policy.

Click to close the policy without saving changes.

Click to add or remove policy content

Click headings to sort columns alphabetically.

Click to add users and groups to the policy or remove them.

Click to add, edit, or remove policy rights.

Click to add notification users to the policy.

Click to add, edit, or remove policy schedules



## 2. In the Edit Policy tab, add content to the policy.

To the left of the **Content** link, click **Add**.

The screenshot shows a dialog box titled "Content" with a blue header. Below the header, there is a list of content items: "/secure/CustSvc/Customers-Apr02.xls", "/secure/CustSvc/Customers-May02.xls", "/secure/SalesReport.pdf", and "/secure/CustSvc/Customers-Jun02.xls". A red circle highlights the first three items. Below the list, there is a search box labeled "Content Search" with the text "4 total" above it. To the right of the search box are "OK" and "Cancel" buttons. Below the search box, there is a note: "\* denotes a folder of content."

Select content to add to policy.

Enter content to search for by name; press Enter or Return (depending on your system) to begin the search.

In the Content form, select one or more content items from those loaded onto the Content Server to be appended to this policy. You can also use the **Content Search** box to search for an exact URL. Click **OK** to add the content, or click **Cancel** to abort the addition.

**Note:** Suspended content items are grayed-out.

### 3. Add users to the policy.

Below and to the left of Accounts, click **Add**.

The screenshot shows a dialog box titled "Accounts" with the instruction "Select an individual or group of accounts to be appended to the open active policy." Below this is a list of accounts: "+ Customer Service (2)", "+ IT Staff (1)", "+ Sales (1)", "Don", "Lynn", "Pam", "Patricia", "+ Embezzlers (1)", and "Bob". The "Pam" entry is highlighted. At the bottom of the list is "9 total". Below the list is a "User Search" text box, which is circled in red. To the right of the text box are "OK" and "Cancel" buttons. Below the buttons is the text "+ denotes a group of users." A red line points from the "User Search" box to the text "Enter user to search for by name; press Enter or Return (depending on your system) to begin the search." Another red line points from the list of accounts to the text "Select content to add to policy."

Select content to add to policy.

Enter user to search for by name; press Enter or Return (depending on your system) to begin the search.

In the Accounts form, select one or more groups or users to be appended to this policy. You can also use the **User Search** box to search for an exact user name. Click **OK** to add the accounts, or click **Cancel** to abort the addition.

**Note:** Suspended users and groups are grayed-out.

#### 4. Add rights to the policy.

Below and to the left of Accounts, click **Add**.

Select an individual or group of rights to be appended to the open active policy.

print  
watermark

2 total

Allow infinite right invocations

Limit max number of right invocations to

Send notification when right is invoked

Right Search

OK Cancel

+ denotes a custom rights grouping.

Select rights to be added to the policy.

Click to allow infinite invocations of rights.

Click button to limit rights invocations; enter number of invocations allowed.

Click to notify sender and other users when rights are invoked.

Enter right to search for by name; press Enter or Return (depending on your system) to begin the search.

Note that **view** is a part of your policy by default. In the Rights form:

- Select one or more rights to be appended to this policy. You can also use the **Right Search** box to search for an exact right.
- Select one of the following:
  - Select the box to the left of **Allow infinite right invocations** to grant the users and groups in this policy no limit to the number of times they can access the content as specified in this policy.
  - Select the box to the left of **Limit max number of right invocations** to limit the number of times the users and groups in this policy can access the content. If you select this button, you must enter an integer specifying the number of times the users and groups can access the content.
- Click the **Send notification when right is invoked** if you want one or more users to be notified when the content is accessed.

**Note:** Suspended rights are grayed-out.

Click **OK** to add the rights, or click **Cancel** to abort the addition.

#### 5. Add a notification user to the policy.

If you checked the **Send notification when right is invoked** in the previous step you must complete this step; otherwise, this step is optional.

To the left of the **Notification** link, click **Add**.

Enter the name of the user to be notified when rights are invoked.

Enter the e-mail address of the user to be notified when rights are invoked.

In the Add Notification User form, enter a **Name** and **E-Mail** address of a user to be notified when content is accessed. Click **OK** to add the notification, or click **Cancel** to abort the addition.

## 6. Add a schedule to the policy.

To the left of the **Schedules** link, click **Add**. The Add Schedule form appears.

Use the pull-down menus to select the start and end dates and times.

Click to use the Calendar tool to select the start and end dates.

Use the pull-down menu to select a duration of access to the protected content.

Enter the name of the new schedule.

Use the pull-down menus and calendar picker to pick a start and end date and time. Then use the **Duration** pull-down menus to determine the amount of time the document is available when it is being accessed (this can keep someone from leaving the office with a protected document visible on their screen).

Enter a **Name** for the schedule, then click **OK** to save or **Cancel** to abort the changes and return to the Policy Administration tool.

## 7. Save the policy.

Click the flashing **Record** button in the upper right-hand portion of the **Edit** tab to save your policy.

## Displaying Policies

Use either of the following methods to display a policy:

- Click **Display** under **Policy Management** in the left menu, or if in the **Edit** tab, click the **Display** tab in the Policy Manager to display the most recently accessed policy.
- Click **Policy Management** in the left menu, then select the policy to be displayed, then click **Display** under **Policy Management** in the left menu. A listing of the Content, Accounts, Rights, and Schedules for that policy appears.

## Activating or Suspending Policies



When you create a policy, it is automatically active and appears in the left, or **Active** column. When you want to terminate a Probix Trustee policy, you suspend it, and it appears in the right, or **Suspended** column.

To activate or suspend policies:

### 1. In the Policy Manager, select one or more policies you want to activate or suspend.

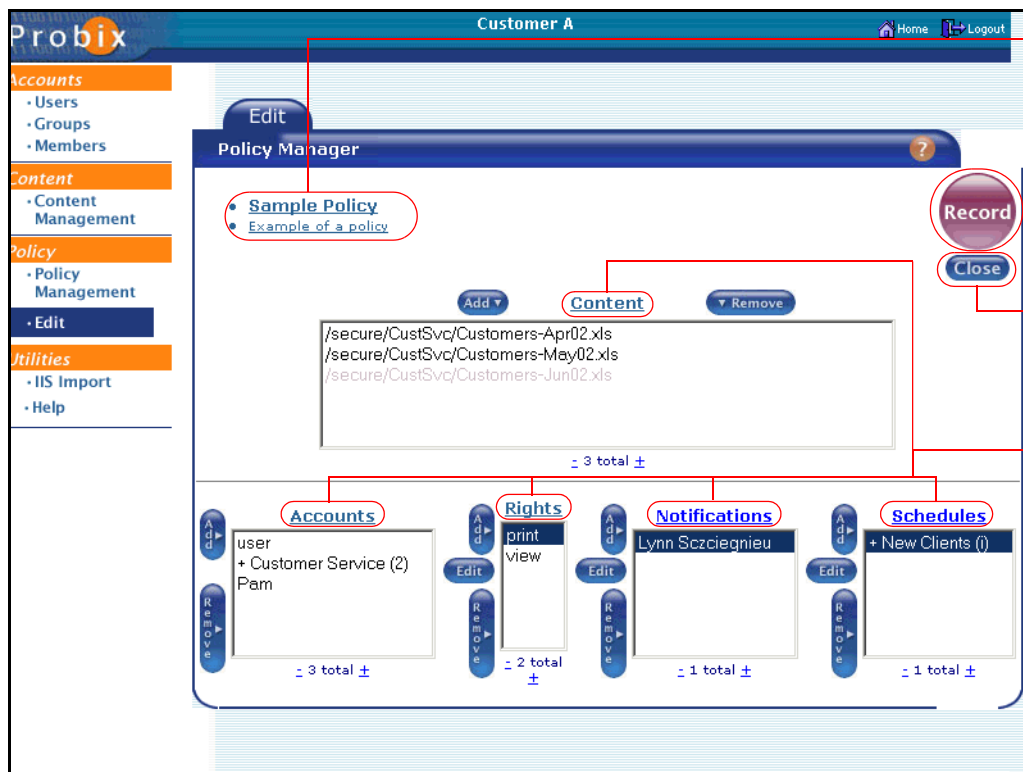
Use the left mouse button to select each policy you want to activate or suspend. Left-clicking on a group and pressing the **Shift** key as you move your cursor selects a consecutive set of policies. Press the **Ctrl** key and left-click individual policies to select multiple non-consecutive policies.

### 2. Change the status of the selected policy.

Click the  button to move policies from the **Active** column to the **Suspended** column, thus suspending them, or click the  button to move policies from the **Suspended** column to the **Active** column, thus activating them.

## Modifying a Policy

To modify a policy, in the Policies Administration tool, select the name of the policy you want to modify, then click **Edit** in the left column of the screen. The Edit Policy tab appears.



The screenshot shows the Probix Policy Manager interface. The top navigation bar includes "Customer A", "Home", and "Logout". The left sidebar contains menu items: Accounts (Users, Groups, Members), Content (Content Management), Policy (Policy Management, Edit), and Utilities (IIS Import, Help). The main area is titled "Policy Manager" and shows an "Edit" tab. A list of policies is displayed, with "Sample Policy" and "Example of a policy" selected. Below the list are buttons for "Add", "Content", and "Remove". The "Content" column shows a list of files: "/secure/CustSvc/Customers-Apr02.xls", "/secure/CustSvc/Customers-May02.xls", and "/secure/CustSvc/Customers-Jun02.xls". Below this list are four columns for "Accounts", "Rights", "Notifications", and "Schedules", each with "Add" and "Remove" buttons. The "Accounts" column shows "user", "+ Customer Service (2)", and "Pam". The "Rights" column shows "print" and "view". The "Notifications" column shows "Lynn Szczegnieu". The "Schedules" column shows "+ New Clients (0)".

Annotations on the right side of the screenshot:

- Policy name and description; click to view policy.
- Click to save the policy.
- Click to close the policy without saving changes.
- Click headings to sort columns alphabetically.

To display the Contents, Accounts, Rights, Notifications, and Schedules in ascending or descending alphabetical order, click on the respective heading.

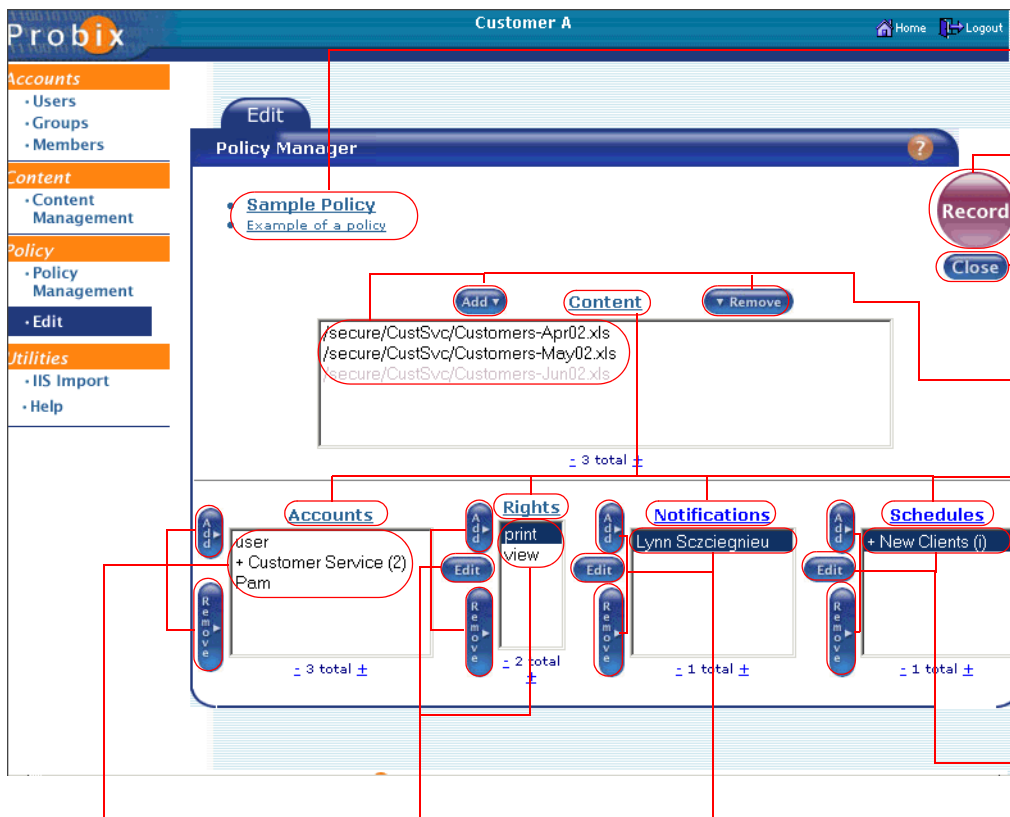
- Clicking on the **Contents** heading sorts the contents alphabetically in ascending order; clicking on the heading a second time sorts the list in descending order.
- Clicking on the **Accounts** heading sorts the accounts alphabetically in ascending order; clicking on

the heading a second time sorts the list in descending order.

- Clicking on the **Rights** heading sorts the rights alphabetically in ascending order; clicking on the heading a second time sorts the list in descending order.
- Clicking on the **Notifications** heading sorts the notifications alphabetically in ascending order; clicking on the heading a second time sorts the list in descending order.
- Clicking on the **Schedules** heading sorts the schedules chronologically in ascending order; clicking on the heading a second time sorts the list in descending order.

**Note:** Suspended content items, accounts, rights, notification users, and schedules are grayed-out.

From this tab you can edit policy Rights, Notifications, and Schedules; you can also add and remove policy Content, Accounts, Rights, Notifications, and Schedules.



Policy name and description; click to view policy.

Click to save the policy.

Click to close the policy without saving changes.

Click to add content to policy, or select then remove policy content.

Click headings to sort columns alphabetically.

Click to add users and groups to the policy, or select and remove them.

Click to add rights to the policy, or select then edit or remove rights.

Click to add notification users to the policy, or select then edit and remove them.

Click to add schedules to the policy, or select then edit or remove schedules.

## Editing a Policy Name or Description

To edit a policy name or description:

### 1. In the Edit tab of the Policy Management tool, select the policy you want to modify.

Use the left mouse button to select the policy you want to modify.

### 2. Modify the policy description.

Once you have selected the policy to be changed, click **Modify**. A new dialog window appears.

- To change the the name of the policy, enter a different policy name in the **Policy** box.
- To change the text description of the policy, edit the text in the **Description** box. This text appears when the policy is selected and the **Show Descriptions** box is checked.

### 3. Confirm.

Click **OK** to save, or **Cancel** to abort the changes.

### Adding Content to an Existing Policy

To add content to an existing policy:

#### 1. In the Edit tab of the Policy Management tool, select the policy to which you want to add content.

Use the left mouse button to select the policy to which you want to add content, then click **Add**. A new dialog window appears.

#### 2. Add the content.

Use the left mouse button to select each content item to be added. Left-clicking on a content item and pressing the **Shift** key as you move your cursor selects a consecutive set of content items. Press the **Ctrl** key and left-click individual content items to select multiple non-consecutive content items.

#### 3. Confirm.

Click **OK** to add the content, or **Cancel** to abort adding the content.

**Note:** Suspended content items are grayed-out.

### Removing Content from a Policy

To remove content from a policy:

#### 1. In the Edit tab of the Policy Management tool, select the policy from which you want to remove content.

Use the left mouse button to select the policy to which you want to remove content. Left-clicking on a content item and pressing the **Shift** key as you move your cursor selects a consecutive set of content items. Press the **Ctrl** key and left-click individual content items to select multiple non-consecutive content items. Next, click **Remove**. A confirmation box appears.

#### 2. Confirm.

Click **OK** to remove the content, or **Cancel** to abort removing the content.

### Adding Accounts to an Existing Policy

To add accounts to an existing policy:

#### 1. In the Edit tab of the Policy Management tool, select the policy to which you want to add accounts.

Use the left mouse button to select the policy to which you want to add accounts, then click **Add**. A new dialog window appears.

#### 2. Add the accounts.

Use the left mouse button to select the accounts to be added. Left-clicking on an account and pressing the **Shift** key as you move your cursor selects a consecutive set of accounts. Press the **Ctrl** key and left-click individual accounts to select multiple non-consecutive accounts.

### 3. Confirm.

Click **OK** to add the accounts, or **Cancel** to abort adding the accounts.

**Note:** Suspended users and groups are grayed-out.

#### Removing Accounts from a Policy

To remove accounts from a policy:

##### 1. In the Edit tab of the Policy Management tool, select the policy from which you want to remove accounts.

Use the left mouse button to select the policy to which you want to remove one or more accounts. Left-clicking on an account and pressing the **Shift** key as you move your cursor selects a consecutive set of accounts. Press the **Ctrl** key and left-click individual accounts to select multiple non-consecutive accounts. Next, click **Remove**. A confirmation box appears.

##### 2. Confirm.

Click **OK** to remove the accounts, or **Cancel** to abort removing the accounts.

#### Adding Rights to an Existing Policy

To add accounts to an existing policy:

##### 1. In the Edit tab of the Policy Management tool, select the policy to which you want to add rights.

Use the left mouse button to select the policy to which you want to add rights, then click **Add**. A new dialog window appears.

##### 2. Add the rights.

Use the left mouse button to select the rights to be added. Left-clicking on a right and pressing the **Shift** key as you move your cursor selects a consecutive set of rights. Pressing the **Ctrl** key and left-click individual rights selects multiple non-consecutive rights.

##### 3. Confirm.

Click **OK** to add the rights, or **Cancel** to abort adding the rights.

**Note:** Suspended rights are grayed-out.

#### Removing Rights from a Policy

To remove rights from a policy:

##### 1. In the Edit tab of the Policy Management tool, select the policy from which you want to remove rights.

Use the left mouse button to select the policy to which you want to remove one or more rights. Left-clicking on an account and pressing the **Shift** key as you move your cursor selects a consecutive set of rights. Pressing the **Ctrl** key and left-click individual rights selects multiple non-consecutive rights. Next, click **Remove**. A confirmation box appears.

##### 2. Confirm.

Click **OK** to remove the rights from the policy, or **Cancel** to abort removing the rights from the policy.

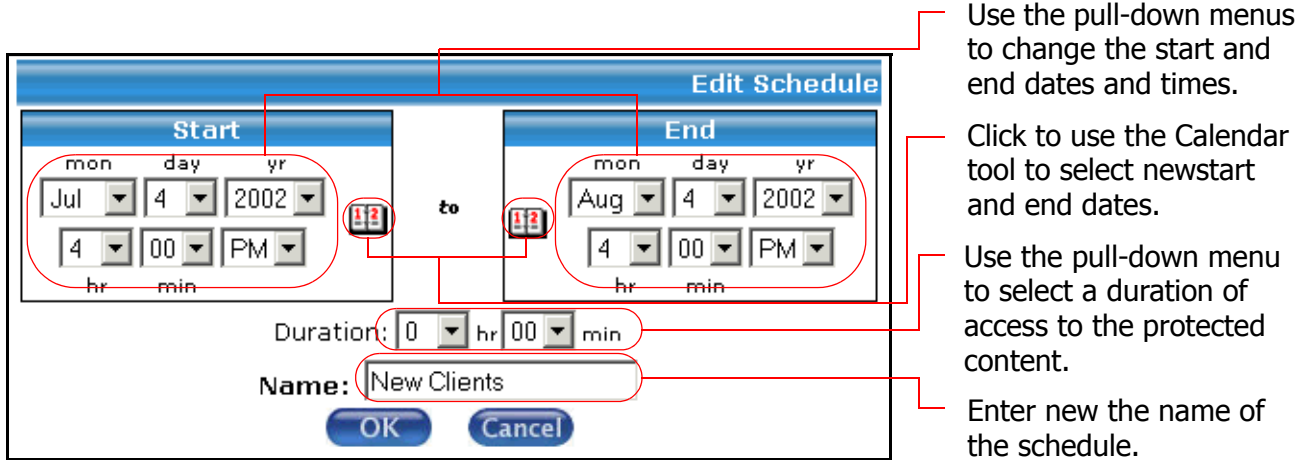
#### Adding a Schedule to an Existing Policy

To add a schedule to an existing policy:



**1. In the Edit tab of the Policy Management tool, select the policy to which you want to add a schedule.**

Use the left mouse button to select the policy to which you want to add a schedule, then click **Add**. A new dialog window appears.



**2. Add the schedule.**

Use the pull-down menus and calendar picker to pick a start and end date and time. Then use the **Duration** pull-down menus to determine the amount of time the document is available when it is being accessed (this can keep someone from leaving the office with a protected document visible on their screen).

**3. Confirm.**

Click **OK** to add the schedule, or **Cancel** to abort adding the schedule.

**Editing a Schedule within a Policy**

To edit a schedule within a policy:

**1. In the Edit tab of the Policy Management tool, select the policy within which you want to edit a schedule.**

Use the left mouse button to select the policy within which you want to modify a schedule, then click **Modify**. A new dialog window appears.

**2. Modify the schedule.**

From the drop-down box, select an **Interval** or **Metered** schedule. If **Metered**, set the duration for the policy and set the **Name**. If **Interval**, set the start and end dates and times and set the **Name**.

**3. Confirm.**

Click **OK** to change the schedule, or **Cancel** to abort the changes.

## Removing a Schedule From a Policy

To remove a schedule from a policy:

1. **In the Edit tab of the Policy Management tool, select the policy from which you want to remove a schedule.**

Left-clicking on a group and pressing the **Shift** key as you move your cursor selects a consecutive set of policies. Press the **Ctrl** key and left-click individual policies to select multiple non-consecutive policies. Next, click **Remove**. A confirmation box appears.

2. **Confirm.**

Click **OK** to remove the schedule from the policy, or **Cancel** to abort removing the schedule.

**Note:** The Record button changes color between red and blue to prompt you to click on it to save any changes made to a policy prior to closing the screen.

To exit the Policy Manager and edit another policy, click **Close**.

## Removing a Policy

To remove a policy:

1. **In the policy manager, select the policies you want to remove.**

Use the left mouse button to select the policies you want to remove. Left-clicking on a policy and pressing the **Shift** key as you move your cursor selects a consecutive set of policies. Pressing the **Ctrl** key and left-clicking individual policies selects multiple non-consecutive policies. Next, click **Remove**. A confirmation box appears.

2. **Confirm.**

Click **OK** to remove the policies, or **Cancel** to abort removing the policies.

## USING THE IIS IMPORT TOOL

You can use the IIS Import tool to import users and groups from the Microsoft Domain server.

**Note:** The `users.asp` file must be installed on the Microsoft IIS server.

To use the IIS Import tool, click IIS Import in the left menu. The IIS Import form appears:

The screenshot shows the Probix web interface with the IIS Import form open. The form contains the following fields and labels:

- URL:** A text input field with a red line pointing to the text: "Enter the URL for the Microsoft IIS server."
- User Name:** A text input field with a red line pointing to the text: "Enter the User Name for the Microsoft IIS server."
- Password:** A text input field with a red line pointing to the text: "Enter the password for the Microsoft IIS server user."
- Domain:** A text input field with a red line pointing to the text: "Enter the domain for the Microsoft IIS server."

The form also includes an "OK" button at the bottom. The background shows the Probix navigation menu and a footer with copyright information: "Probix ©2001-2002, All Rights Reserved Probix, Inc. 1-650-691-1700".

Enter the following fields:

**Note:**

- URL** the URL for the Microsoft IIS server in the form `"/hostname/users.asp"`
- User Name:** the user name needed for the Microsoft IIS server
- Password:** the password for the Microsoft IIS server user.
- Domain** the domain for the Microsoft IIS server.

Click OK to import the data. When you are finished, a message indicating the data has been imported appears. Click any item on the left menu under Accounts, Content, or Policy to continue managing your Probix Trustee site.



# Chapter 6

## *Probix Trustee Command-Line Utilities*

---

---

This chapter lists and discusses the following Solaris command-line utilities you can use to manage and administer a Probix Trustee site:

- `pcpnCustCfg`
- `save_logs`
- `check_pcpn`
- `check_pcpn_pkg`
- `webstart`
- `webstop`
- `webrestart`
- `webstat`
- `mysqlstart`
- `mysqlstop`
- `mysqlstat`

**Note:** In these examples, `$APACHE_DIR` refers to the directory in which you have installed the Apache server.

# PCPNCUSTCFG

Create and modify the customer configuration files.

## Location

`$APACHE_DIR/bin/pcpnCustCfg`

## Syntax

`pcpnCustCfg -option`

where *option* is one of the parameter/argument combinations.

**import *import\_file\_name password***

Imports a file containing a customer using the specified password.

**address *customerID file\_or\_folder\_name***

Adds a file or directory to the list of protected resources (viewable with the -print option).

**delres *customerID protected\_resource\_ID***

Deletes a file or directory from the list of protected resources (viewable with the -print option).

**srvaddr *customerID server\_address[:port\_number]***

Sets the Probix Server address [and port number] for that customer ID.

**print**

Displays the customer configuration file.

**test *customerID***

Tests the connection between the content server and the Probix Server.

**remove *customerID***

Removes the customer specified by the customer ID from the content server.

**encalg *customerID { DES | TDES | AES }***

Sets the encryption algorithm for content for the specified customer to either DES, Triple DES (TDES), or AES.

**policysrc *customerID {protCont | redirURL | psDB}***

The source for the policy. One of:

- *protCont* - the policy is in the back end of the customer server and is sent with the protected content
- *redirURL* - the policy is in the front end of the customer server and is sent via a redirect URL
- *psDB* - the policy comes from the Probix Server database

## Parameters

*import\_file\_name*

the name of the file containing the customer ID

<i>password</i>	the password needed to access the data in the <i>import_file_name</i>
<i>customerID</i>	the customer ID number
<i>file_or_folder_name</i>	file or directory being added to the list of protected resources
<i>protected_resource_ID</i>	protected resource ID number for a specific <i>file_or_folder_name</i>
<i>server_address</i> [: <i>port_number</i> ]	the Probox Server IP address [and port number]

## **SAVE\_LOGS**

Creates an archive folder of the current Apache and PCPN log files and zeroes the current logs. The archive folder is located in `$APACHE_DIR/log.date-and-time`.

### **Location**

`$APACHE_DIR/pcpn/save_logs`

### **Syntax**

`save_logs`

### **Parameters**

None.



## **CHECK\_PCPN**

Check the installation of the PCPN software to make sure the files and permissions are correct.

### **Location**

`$APACHE_DIR/bin/check_pcpn`

### **Syntax**

`check_pcpn`

### **Parameters**

None.

## **CHECK\_PCPN\_PKG**

Check the installation of the Sun PCPN packages to make sure the files and permissions are correct.

### **Location**

`$APACHE_DIR/pcpncust/check_pcpn_pkg`

### **Syntax**

`check_pcpn_pkg`

### **Parameters**

None.

## **WEBSTART**

Start the Apache and Tomcat servers needed for PCPN to work properly.

### **Location**

`$APACHE_DIR/bin/webstart`

### **Syntax**

`webstart`

### **Parameters**

None.

## **WEBSTOP**

Stop the Apache and Tomcat servers needed for PCPN to work properly.

### **Location**

`$APACHE_DIR/bin/webstop`

### **Syntax**

`webstop`

### **Parameters**

None.

## **WEBRESTART**

In case of configuration changes, gracefully restart the Apache and Tomcat servers needed for PCPN to work properly.

### **Location**

`$APACHE_DIR/bin/webrestart`

### **Syntax**

`webrestart`

### **Parameters**

None.

## **WEBSTAT**

Check the status of the Apache and Tomcat servers needed for PCPN to work properly.

### **Location**

`$APACHE_DIR/bin/webstat`

### **Syntax**

`webstat`

### **Parameters**

None.

## **MYSQLSTART**

Start the MySQL database server needed for PCPN to work properly.

### **Location**

`/usr/local/mysql/bin/mysqlstart`

### **Syntax**

`mysqlstart`

### **Parameters**

None.

## **MYSQLSTOP**

Stop the MySQL database server needed for PCPN to work properly.

### **Location**

`/usr/local/mysql/bin/mysqlstop`

### **Syntax**

`mysqlstop`

### **Parameters**

None.



## **MYSQLSTAT**

Check the status of the MySQL database server needed for PCPN to work properly.

### **Location**

`/usr/local/mysql/bin/mysqlstat`

### **Syntax**

`mysqlstat`

### **Parameters**

None.



# Chapter 7

## *Troubleshooting Messages*

---

---

This chapter contains a list of messages that may appear when using Probix Trustee, what causes them to occur, and the proper response to them. Some of these messages are standard HTTP status codes discussed in greater detail in RFC 2621, available at <http://www.w3.org/Protocols/rfc2616/rfc2616.html>. They are included here for your reference.

When troubleshooting problems you may encounter while using Probix Trustee you may also find it helpful to view the logs as described in Chapter 3, "Using the Probix Trustee Logger" on page 15.

If you have any questions regarding the Probix Content Protection Network (PCPN), or if you would like more information about other Probix products, please send e-mail to [customer-support@probix.com](mailto:customer-support@probix.com).

## PROBIX-SPECIFIC HTTP STATUS CODES

The following are Probix-specific status codes that may be encountered while running Probix Trustee. If the suggested response does not fix the problem, note the status code and details, and call Probix Customer Support.

Status Code	Description	Response
106 - General Error	There are some (required) PCPN-specific HTTP headers missing in the response from the Probix Server.	Have the user quit and restart the browser, then try to retrieve the content again.
119 - General Error	Something went wrong during the download of the protected content from the Probix Server. This can happen when a user refreshes the window because the packet containing the encrypted content is already in use.	Have the user quit and restart the browser, then try to retrieve the content <i>without</i> refreshing the screen.
441 - PCPN bad request: no parameters	The request from the client was supposed to contain parameters but did not.	Make sure the Content Server and Probix Server have compatible software versions.
442 - PCPN bad request: parameters count	The request from the client contained a different number of parameters than the PCPN was expecting.	Make sure the Content Server and Probix Server have compatible software versions.
443 - PCPN bad request: parameters list	The request from the client contained the wrong type of parameters.	Make sure the Content Server and Probix Server have compatible software versions.
444 - PCPN bad request: customer ID	The user listed as owning the content is not registered.	Make sure the Content Server and Probix Server have compatible software versions.
445 - PCPN bad request: nonce length	There was a problem with the security information sent to the client, or there may have been an attack on the PCPN.	Make sure the Content Server and Probix Server have compatible software versions.
446 - PCPN bad request: hash length	There was a problem with the security information sent to the client, or there may have been an attack on the PCPN.	Make sure the Content Server and Probix Server have compatible software versions.
447 - PCPN bad request: authorized redirect	The client was redirected to the wrong server.	Have the user retry the request. Use network monitoring tools to confirm the URL the user requested arrives at the Content Server unaltered.

Status Code	Description	Response
448 - PCPN bad request: time stamp	The user tried to obtain expired content, or there may have been an attack on the PCPN.	Make sure the Content Server and Probix Server have compatible software versions.
449 - PCPN bad request: original URL	The original URL sent from the client was malformed, or there may have been an attack on the PCPN.	Have the user retry the request. Use network monitoring tools to confirm the URL the user requested arrives at the Content Server unaltered.
450 - PCPN bad request: information	There was a problem with the security information sent to the client, or there may have been an attack on the PCPN.	Have the user retry the request. Use network monitoring tools to confirm the URL the user requested arrives at the Content Server unaltered.
451 - PCPN bad request: SID length	There was a problem with the security information sent to the client, or there may have been an attack on the PCPN.	Make sure the Content Server and Probix Server have compatible software versions.
452 - PCPN bad request: public key length	There was a problem with the security information sent to the client, or there may have been an attack on the PCPN.	<ol style="list-style-type: none"> <li>1. Make sure the Content Server and Probix Server have compatible software versions.</li> <li>2. Use network monitoring tools to confirm the URL the user requested arrives at the Content Server unaltered.</li> </ol>
453 - PCPN bad request: authentication test	The user was testing the code.	<ol style="list-style-type: none"> <li>1. Make sure the Content Server and Probix Server have compatible software versions.</li> <li>2. Use network monitoring tools to confirm the URL the user requested arrives at the Content Server unaltered.</li> </ol>
454 - PCPN bad request: version	There was a problem with the security information sent to the client, or there may have been an attack on the PCPN.	Make sure the Content Server and Probix Server have compatible software versions.
455 - PCPN bad request: authentication client	There was a problem with the security information sent to the client, or there may have been an attack on the PCPN.	<ol style="list-style-type: none"> <li>1. Make sure the Content Server and Probix Server have compatible software versions.</li> <li>2. Use network monitoring tools to confirm the URL the user requested arrives at the Content Server unaltered.</li> </ol>

Status Code	Description	Response
456 - PCPN bad request: key exchange replay	The user tried to obtain protected content by replaying protected network traffic, usually by using the address line of the browser.	<ol style="list-style-type: none"> <li>1. Make sure the Content Server and Probix Server have compatible software versions.</li> <li>2. Use network monitoring tools to confirm the URL the user requested arrives at the Content Server unaltered.</li> </ol>
457 - PCPN bad request: redirection replay	The user tried to obtain protected content by replaying protected network traffic, usually by using the address line of the browser.	<p>The redirected URL can be used only once. If the user has not tried to reuse a redirected URL:</p> <ol style="list-style-type: none"> <li>1. Make sure the user's browser is not caching the redirected URL.</li> <li>2. Use network monitoring tools to identify the source using the redirected URL.</li> </ol>
500 - HTTP internal server error	The server encountered an unexpected condition which prevented it from fulfilling the request.	Make sure the Content Server and Probix Server have compatible software versions.
551 - internal WWW root error	The server encountered an error while processing the URL.	Have the user retry the request. Note that the Content Server or Probix Server may need to be restarted.
552 - internal configuration error	Server error.	Make sure the Content Server and Probix Server have compatible software versions.
553 - internal allocation error	Server error.	Make sure the Content Server and Probix Server have compatible software versions.
554 - internal socket error	Server error.	<ol style="list-style-type: none"> <li>1. Make sure the Content Server and Probix Server have compatible software versions.</li> <li>2. Use network monitoring tools to confirm the URL the user requested arrives at the Content Server unaltered.</li> </ol>
555 - internal get state error	This is typically caused by a long (many minutes) delay by the user when answering a dialog question presented during the display of content.	Use network monitoring tools to identify the source of the long communication times.

Status Code	Description	Response
556 - internal save state error	Server error.	Make sure the Content Server and Probix Server have compatible software versions.
557 - internal no policy error	Server error.	Use network monitoring tools to confirm the URL the user requested arrives at the Content Server unaltered.
900 - PCPN-specific error	Server error.	Make sure the Content Server and Probix Server have compatible software versions.
901 - time response error	Server error.	Make sure the Content Server and Probix Server have compatible software versions.
902 - time authentication content error	Server error.	Make sure the Content Server and Probix Server have compatible software versions.
951 - customer request URL error	Server error.	Make sure the Content Server and Probix Server have compatible software versions.
952 - customer request address error	Server error.	Use network monitoring tools to identify the source of the communication problem from the Probix Server to the Content Server.
953 - customer connect error	Server error.	Use network monitoring tools to identify the source of the communication problem from the Probix Server to the Content Server.
954 - customer read from error	Server error.	Use network monitoring tools to identify the source of the communication problem from the Probix Server to the Content Server.
955 - customer no data error	Server error.	Use network monitoring tools to identify the source of the communication problem from the Probix Server to the Content Server.

Status Code	Description	Response
956 - customer HTTP verified error	Server error.	Use network monitoring tools to identify the source of the communication problem from the Probix Server to the Content Server.
957 - customer read header error	Server error.	Use network monitoring tools to identify the source of the communication problem from the Probix Server to the Content Server.
958 - customer zero header error	Server error.	Use network monitoring tools to identify the source of the communication problem from the Probix Server to the Content Server.
959 - customer zero content error	Server error.	Use network monitoring tools to identify the source of the communication problem from the Probix Server to the Content Server.
960 - customer content error	Server error.	Examine the protected document on the Content Server and confirm that it has a correct file extension and is not corrupted.
961 - customer cont authentication error	Server error.	<ol style="list-style-type: none"> <li>1. Use network monitoring tools to identify the source of the communication problem from the Probix Server to the Content Server.</li> <li>2. Use network monitoring tools to confirm the URL the user requested arrives at the Content Server unaltered.</li> </ol>



## WINDOWS ACTIVEX APPLICATION ERROR MESSAGES

Error Code	Description	Response
001 - Failed to retrieve IShellBrowser	There is a problem with the plugin.	Have the user retry the request. Note that the content server or policy server may need to be restarted.
000 - second create	There is a problem with the plugin.	Have the user retry the request. Note that the content server or policy server may need to be restarted.
002 - fail to create IStorage object	There is a problem with the plugin.	Have the user retry the request. Note that the content server or policy server may need to be restarted.
003 - cannot retrieve content from server	There is a problem with the plugin.	Have the user retry the request. Note that the content server or policy server may need to be restarted.
004 - security update is available; please restart your browser	The plugin needs to be updated.	<ol style="list-style-type: none"> <li>1. Quit and restart the browser.</li> <li>2. Run the <code>probix_cleanup.htm</code> utility. At the end of the utility you are prompted to close the browser.</li> <li>3. Quit and restart the browser.</li> </ol>
005 - Could not initialize Probix protection	There is a problem with the plugin.	Have the user retry the request. Note that the content server or policy server may need to be restarted.
006 - Probix cxa8() function failed	The user used the Back or Forward arrow button in the browser.	Have the user retry the request. Note that the content server or policy server may need to be restarted.
007 - Could not start Probix Protection	There is a problem with the plugin.	Have the user retry the request. Note that the content server or policy server may need to be restarted.

<b>Error Code</b>	<b>Description</b>	<b>Response</b>
008 - Could not load corresponding *P2.dll file	There is a problem with the plugin.	Have the user retry the request. Note that the content server or policy server may need to be restarted.
009 - Could not load Probix01.dll	There is a problem with the plugin.	Have the user retry the request. Note that the content server or policy server may need to be restarted.
010 - Failed to start corresponding application	The client system is having problems with the native application (for example, Acrobat, MS Word, or PowerPoint)	Make sure the application is installed properly. The user may need to reinstall the application.
011 - Failed to get application pointer	There is a problem with the plugin.	Have the user try to restart the corresponding native application.
013 - Could not set protection	There is a problem with the plugin.	Have the user try to restart the corresponding native application.
014 - Could not detect corresponding process	There is a problem with the plugin.	Have the user try to restart the corresponding native application.
015 - Could not load target file	There is a problem with the plugin.	Have the user try to restart the corresponding native application.
016 - Cannot get IDispatch pointer	There is a problem with the plugin.	Have the user try to restart the corresponding native application.
017 - Error to get IPersistStorage interface pointer	There is a problem with the plugin.	Have the user try to restart the corresponding native application.
018 - Error to get IHlink interface pointer	There is a problem with the plugin.	Have the user try to restart the corresponding native application.
019 - PostThreadMessage failed	This error is highly unlikely to occur.	Have the user try to restart the corresponding native application.
020 - SetClientSite failed	There is a problem with the plugin.	Have the user try to restart the corresponding native application.
021 - Error navigating to target file	There is a problem with the plugin.	Have the user try to restart the corresponding native application.
022 - Detected rogue application	Probix Trustee has detected an application running that could threaten the security of the PCPN, such as a screen capture program.	Have the user close all programs that can capture screens. If the problem persists, note the error code and call Probix Customer Support.

Error Code	Description	Response
023 - probixapp.exe shutdown	The ProbixApp.exe program has quit unexpectedly.	Have the user close and reopen their browser. If the problem persists, note the error code and details, and call Probix Customer Support
027 - rogue port	A rogue port has been detected.	Have the user close and reopen their browser. If the problem persists, note the error code and details, and call Probix Customer Support
029 - Injection into specific failed	An injection into the specific application failed.	Have the user close and reopen their browser. If the problem persists, note the error code and details, and call Probix Customer Support
030 - attempt screen capture	An application is attempting to capture the screen.	Close the application that is a threat. If the problem persists, note the error code and details, and call Probix Customer Support

## APPLICATION ERRORS

The following errors may occur while running Probix Trustee. If the response does not work, note the error code and any details and call Probix Customer Support.

### Probix PowerPoint Plugin Errors

Error Code	Description	Response
1001 - Couldn't get PowerPoint Application Interface	Microsoft PowerPoint is not loaded on the client.	If Microsoft PowerPoint is already installed on the client system: <ol style="list-style-type: none"> <li>1. Quit PowerPoint.</li> <li>2. Quit and restart the browser.</li> <li>3. Try requesting the document again.</li> </ol>
1002 - Failed to get PowerPoint Window HWND	Either Microsoft PowerPoint is not loaded on the client or the installation has been corrupted.	If Microsoft PowerPoint is already installed on the client system: <ol style="list-style-type: none"> <li>1. Quit PowerPoint.</li> <li>2. Quit and restart the browser.</li> <li>3. Try requesting the document again.</li> </ol>
1003 - Failed to get PowerPoint version	Either Microsoft PowerPoint is not loaded on the client or the installation has been corrupted.	If Microsoft PowerPoint is already installed on the client system: <ol style="list-style-type: none"> <li>1. Quit PowerPoint.</li> <li>2. Quit and restart the browser.</li> <li>3. Try requesting the document again.</li> </ol>
1004 - Could not disable menu	Either Microsoft PowerPoint is not loaded on the client or the installation has been corrupted.	If Microsoft PowerPoint is already installed on the client system: <ol style="list-style-type: none"> <li>1. Quit PowerPoint.</li> <li>2. Quit and restart the browser.</li> <li>3. Try requesting the document again.</li> </ol>
1005 - No child window found	Microsoft PowerPoint is not operating properly.	If Microsoft PowerPoint is already installed on the client system: <ol style="list-style-type: none"> <li>1. Quit PowerPoint.</li> <li>2. Quit and restart the browser.</li> <li>3. Try requesting the document again.</li> </ol>

## Probix Word Plugin Errors

Error Code	Description	Response
2001 - failed to set Word Document protection	Microsoft Word is not properly installed on the client.	If Microsoft Word is already installed on the client system: <ol style="list-style-type: none"> <li>1. Quit Word.</li> <li>2. Quit and restart the browser.</li> <li>3. Try requesting the document again.</li> </ol>
2002 - could not find child window	Microsoft Word is not properly installed on the client.	If Microsoft Word is already installed on the client system: <ol style="list-style-type: none"> <li>1. Quit Word.</li> <li>2. Quit and restart the browser.</li> <li>3. Try requesting the document again.</li> </ol>
2003 - failed to remove key binding	Microsoft Word is not properly installed on the client.	If Microsoft Word is already installed on the client system: <ol style="list-style-type: none"> <li>1. Quit Word.</li> <li>2. Quit and restart the browser.</li> <li>3. Try requesting the document again.</li> </ol>
2004 - failed to disable menu items	Microsoft Word is not properly installed on the client.	If Microsoft Word is already installed on the client system: <ol style="list-style-type: none"> <li>1. Quit Word.</li> <li>2. Quit and restart the browser.</li> <li>3. Try requesting the document again.</li> </ol>

## Probix Hangul Plugin Errors

Error Code	Description	Response
3001 - QueryInterface IPersist Memory failed	Hangul is not properly installed on the client.	If the client system is running Hangl 2002: 1. Quit Hangul. 2. Quit and restart the browser. 3. Try requesting the document again.
3002 - Couldn't activate object in place	Hangul is not properly installed on the client.	If the client system is running Hangl 2002: 1. Quit Hangul. 2. Quit and restart the browser. 3. Try requesting the document again.
3003 - Invoke "LoadFile" failed	Hangul is not properly installed on the client.	If the client system is running Hangl 2002: 1. Quit Hangul. 2. Quit and restart the browser. 3. Try requesting the document again.
3004 - Failed to get IOleInPlaceObject interface	Hangul is not properly installed on the client.	If the client system is running Hangl 2002: 1. Quit Hangul. 2. Quit and restart the browser. 3. Try requesting the document again.
3005 - Failed to hook authentication server	Hangul is not properly installed on the client.	If the client system is running Hangl 2002: 1. Quit Hangul. 2. Quit and restart the browser. 3. Try requesting the document again.

## Probox Acrobat Plugin Errors

Error Code	Description	Response
3001 - QueryInterface IPersistMemory failed	The client is either running an unsupported or improperly installed version of Adobe Acrobat.	<p>If the user is already running Adobe Acrobat 4.0 or higher on the client:</p> <ol style="list-style-type: none"> <li>1. Quit Acrobat.</li> <li>2. Quit and restart the browser.</li> <li>3. Try requesting the document again.</li> </ol>
3002 - Couldn't activate object in place	The client is either running an unsupported or improperly installed version of Adobe Acrobat.	<p>If the user is already running Adobe Acrobat 4.0 or higher on the client:</p> <ol style="list-style-type: none"> <li>1. Quit Acrobat.</li> <li>2. Quit and restart the browser.</li> <li>3. Try requesting the document again.</li> </ol>
3003 - Invoke "LoadFile" failed	The client is either running an unsupported or improperly installed version of Adobe Acrobat.	<p>If the user is already running Adobe Acrobat 4.0 or higher on the client:</p> <ol style="list-style-type: none"> <li>1. Quit Acrobat.</li> <li>2. Quit and restart the browser.</li> <li>3. Try requesting the document again.</li> </ol>
3004 - Failed to get IOleInPlaceObject interface	The client is either running an unsupported or improperly installed version of Adobe Acrobat.	<p>If the user is already running Adobe Acrobat 4.0 or higher on the client:</p> <ol style="list-style-type: none"> <li>1. Quit Acrobat.</li> <li>2. Quit and restart the browser.</li> <li>3. Try requesting the document again.</li> </ol>
3005 - Failed to hook authentication server	The client is either running an unsupported or improperly installed version of Adobe Acrobat.	<p>If the user is already running Adobe Acrobat 4.0 or higher on the client:</p> <ol style="list-style-type: none"> <li>1. Quit Acrobat.</li> <li>2. Quit and restart the browser.</li> <li>3. Try requesting the document again.</li> </ol>

<b>Error Code</b>	<b>Description</b>	<b>Response</b>
3006 - ProgIDFromCLSID with CLSID PDF failed	The client is either running an unsupported or improperly installed version of Adobe Acrobat.	If the user is already running Adobe Acrobat 4.0 or higher on the client: <ol style="list-style-type: none"> <li>1. Quit Acrobat.</li> <li>2. Quit and restart the browser.</li> <li>3. Try requesting the document again.</li> </ol>
3007 - version of Acrobat is less than 4.0	The client is running an unsupported version of Adobe Acrobat.	If the user is already running Adobe Acrobat 4.0 or higher on the client: <ol style="list-style-type: none"> <li>1. Quit Acrobat.</li> <li>2. Quit and restart the browser.</li> <li>3. Try requesting the document again.</li> </ol>

## Probix JPG and Text Viewer Plugin Errors

<b>Error Code</b>	<b>Description</b>	<b>Response</b>
4001 - Stream for html is not created		<ol style="list-style-type: none"> <li>1. Quit and restart the browser.</li> <li>2. Try requesting the document again.</li> </ol>
4002 - Writing base text into html wasn't succeeded		<ol style="list-style-type: none"> <li>1. Quit and restart the browser.</li> <li>2. Try requesting the document again.</li> </ol>
4003 - Stream for PCPNHTML Reader Info is not created		<ol style="list-style-type: none"> <li>1. Quit and restart the browser.</li> <li>2. Try requesting the document again.</li> </ol>
4004 - Write PCPNHTML Reader Info into stream was not succeeded		<ol style="list-style-type: none"> <li>1. Quit and restart the browser.</li> <li>2. Try requesting the document again.</li> </ol>
4005 - OleLoad Picture in Image wasn't reached		<ol style="list-style-type: none"> <li>1. Quit and restart the browser.</li> <li>2. Try requesting the document again.</li> </ol>



## Probix Excel Plugin Errors

Error Code	Description	Response
5001 - Failed to get application pointer	The client is either running an unsupported or improperly installed version of MS Excel.	<p>If the user is already running MS Excel on the client:</p> <ol style="list-style-type: none"> <li>1. Quit Excel.</li> <li>2. Quit and restart the browser.</li> <li>3. Try requesting the document again.</li> </ol>
5002 - Unable to set Excel document Sheets protection	The client is either running an unsupported or improperly installed version of MS Excel.	<p>If the user is already running MS Excel on the client:</p> <ol style="list-style-type: none"> <li>1. Quit Excel.</li> <li>2. Quit and restart the browser.</li> <li>3. Try requesting the document again.</li> </ol>
5003 - Unable to remove dangerous hotkeys	The client is either running an unsupported or improperly installed version of MS Excel.	<p>If the user is already running MS Excel on the client:</p> <ol style="list-style-type: none"> <li>1. Quit Excel.</li> <li>2. Quit and restart the browser.</li> <li>3. Try requesting the document again.</li> </ol>
5004 - Failed to disable dangerous menu items.	The client is either running an unsupported or improperly installed version of MS Excel.	<p>If the user is already running MS Excel on the client:</p> <ol style="list-style-type: none"> <li>1. Quit Excel.</li> <li>2. Quit and restart the browser.</li> <li>3. Try requesting the document again.</li> </ol>

## JAVA STATUS MESSAGES

<b>Error Code</b>	<b>Description</b>	<b>Response</b>
1501 - Unsafe Screen	Software on the client system (such as a screen capture program) is attacking protection.	Have the user close the offending application, then try again.
1502 - Incorrect URL	The client supplied an incorrect URL.	Have the Probix Administrator verify the configuration is correct.
1503 - General error	This error is unlikely to occur.	No action is required.
1504 - Connection Failed	The connection to the Probix Server was interrupted.	Have the user try to connect to the server again.
1505 - Decryption Error	The connection to the Probix Server was interrupted.	Have the user try to connect to the server again.
1506 - Action Not Allowed	The user tried to take an action not supported by the content owner's policy.	Have the content owner verify the policy on the content.
1507 - Content Type Not Supported	Protected delivery of the type of content being requested is not supported.	Unsupported content types can be added; call Probix Customer Support for details.
1508 - Character Encoding Error	The character set is not supported by Probix Trustee.	Unsupported character sets can be added; call Probix Customer Support for details.
1509 - Temporarily Unsafe Screen	Software on the client system (such as a screen capture program) is attacking protection.	Have the user close the offending application, then try again.
1510 - Time Expired	Client is trying to access protected content after the time period when the content was available.	This is not an error; Have the user retry the request. Note that the content server or policy server may need to be restarted.
1511 - Loading	Java is loading.	This is a status message.
1512 - Unsupported Browser	The browser the client is using is not supported by Probix Trustee.	Unsupported browsers can be added; call Probix Customer Support for details.
1513 - Unsupported OS	The operating system the client is using is not supported by Probix Trustee.	Unsupported operating systems can be added; call Probix Customer Support for details.
1514 - 16-bit Application	Protected content is under attack by a 16-bit application.	Have the user close the offending application, then try again.

<b>Error Code</b>	<b>Description</b>	<b>Response</b>
1515 - Certificate Denied	The user has either rejected the certificate or has not responded to the certificate prompt before it timed out.	Tell the user to accept the certificate to view the page.

## PROBIX TRUSTEE FOR OUTLOOK ERROR MESSAGES

These error messages may appear while running Probix Trustee for Outlook. If the suggested response does not work, note the error code and details, and call Probix Customer Support.

<b>Error Code</b>	<b>Description</b>	<b>Response</b>
-1 - PT40_ERR_PARAM	Internal error.	Have the user retry sending the message.
-2 - PT40_ERR_NOFILE	Internal error.	Have the user retry sending the message.
-3 - PT40_ERR_OPEN	Internal error.	Have the user retry sending the message.
-4 - PT40_ERR_READ	Internal error.	Have the user retry sending the message.
-5 - PT40_ERR_WRITE	Internal error.	Have the user retry sending the message.
-6 - PT40_ERR_STAT	Internal error.	Have the user retry sending the message.
-7 - PT40_ERR_PARSE	The message has been corrupted into an unrecognized format.	Have the user retry sending the message.
-8 - PT40_ERR_TEMP	Internal error.	Have the user retry sending the message.
-9 - PT40_ERR_MEMORY	Internal error.	Have the user retry sending the message.
-10 - PT40_ERR_MESSAGE	The message has been corrupted into an unrecognized format.	Have the user retry sending the message.
-11 - PT40_ERR_ENCODING	An attachment uses an unsupported coding algorithm.	Have the user retry sending the message.
-12 - PT40_ERR_DATABASE	Internal error.	Have the user retry sending the message.
-13 - PT40_ERR_AUTH	In the initial setup of Probix Trustee for Outlook after adding the add-in, the user entered the manager account name or password incorrectly.	Have the user correct the settings for the manager account in the settings for the add-in.
-14 - PT40_ERR_HASH	The message has somehow been altered or corrupted.	Have the user retry sending the message.

## HTTP STATUS CODES

These are standard HTTP status codes provided for your convenience. Most of these will only be encountered by someone developing code to interface with the PCPN.

If the suggested response does not work, note the error code and details, and call Probix Customer Support.

Error Code	Description	Response
100 - HTTP continue	The client software has determined the server will not accept the request.	Have the user quit and restart the browser and resubmit the request.
101 - HTTP switching protocols	The server is switching to a different protocol.	Have the user retry the request. Note that the content server or policy server may need to be restarted.
102 - HTTP processing	The server is processing the request.	Have the user retry the request. Note that the content server or policy server may need to be restarted.
200 - HTTP ok	The client request has succeeded.	Have the user retry the request. Note that the content server or policy server may need to be restarted.
201 - HTTP created	The client request has been fulfilled and has resulted in a new resource being created.	Have the user retry the request. Note that the content server or policy server may need to be restarted.
202 - HTTP accepted	The request has been accepted for processing, but the processing has not been completed. This is often used when the server response is to be processed later, such as a batch job that runs once a day.	Have the user retry the request. Note that the content server or policy server may need to be restarted.
203 - HTTP non authoritative	The returned metainformation in the entity-header is not the definitive set as available from the origin server, but is gathered from a local or a third-party copy.	Have the user retry the request. Note that the content server or policy server may need to be restarted.
204 - HTTP no content	The server has fulfilled the request but does not need to return an entity-body.	Have the user retry the request. Note that the content server or policy server may need to be restarted.

<b>Error Code</b>	<b>Description</b>	<b>Response</b>
205 - HTTP reset content	The server has fulfilled the request; the user needs reset the document view which caused the request to be sent.	Have the user refresh the browser window.
206 - HTTP partial content	The connection to the server broke before the data could be transferred.	Have the user resubmit the request.
300 - HTTP multiple choices	The requested resource corresponds to any one of a set of representations, each with its own specific location, and agent- driven negotiation information	Have the user choose any of the hyperlinks supplied by the server.
301 - HTTP moved permanently	The requested resource has been assigned a new permanent URI;	Have the user follow the new hyperlink.
302 - HTTP moved temporarily	The requested resource resides temporarily under a different URI.	Have the user follow the new hyperlink.
303 - HTTP see other	This response code lets the output of a POST-activated script redirect the client to a selected resource.	Have the user follow the new hyperlink.
304 - HTTP not modified	The client has performed a conditional GET request and access is allowed, but the document has not been modified.	Have the user quit and restart the browser and then resubmit the request.
305 - HTTP use proxy	The requested resource was not accessed through the proxy given by the Location field.	Have the Probix Trustee Administrator verify the settings for the proxy server are correct.
307 - HTTP temporary redirect	The requested resource resides temporarily under a different URI.	Verify with the Policy Manager or Probix Trustee Administrator that the client is supposed to be redirected to a different URI.
400 - HTTP bad request	The request contains bad syntax or cannot be fulfilled.	Check the URL and try again.
401 - HTTP unauthorized	The request requires user authentication.	Have the user resubmit the request with the proper authentication codes. Note that the user may first have to clear the browser cache, then quit and restart the browser.
402 - HTTP payment required	This code is reserved for future use.	Have the user retry the request. Note that the content server or policy server may need to be restarted.

<b>Error Code</b>	<b>Description</b>	<b>Response</b>
403 - HTTP forbidden	The web page is protected so it cannot be viewed.	Have the Policy Manager verify the content is viewable. If that does not work, have the Probix Trustee Administrator verify permissions on the Apache installation files and directories are correctly set.
404 - HTTP not found	The web page the client was looking for does not exist.	Try another URL. If the URL is correct, protections may need to be changed for the file on the server.
405 - HTTP method not allowed	The method specified in the Request-Line from the client is not allowed for the resource identified by the Request-URI.	Have the Probix Trustee Administrator verify the server response includes an Allow header containing a list of valid methods for the requested resource.
406 - HTTP not acceptable	The resource identified by the request can only generate response entities with content characteristics not acceptable to the client.	Have the user verify the configuration at the client end. If that does not work, have the Policy Manager and Probix Trustee Administrator verify settings.
407 - HTTP proxy authentication required	The client needs to authenticate itself with the proxy server.	Make sure the user is submitting the correct user name and password for the proxy server.
408 - HTTP request time out	The client did not produce a request within the time that the server was prepared to wait. The network may be heavily loaded.	Have the user resubmit the request.
409 - HTTP conflict	The request could not be completed due to a conflict with the current state of the resource, such as trying to access an old version of a file.	The user needs to have the Policy Manager verify the content is available on the specified server.
410 - HTTP gone	The requested resource is no longer available at the server and no forwarding address is known.	The user needs to have the Policy Manager verify the content is available on the specified server.
411 - HTTP length required	The server refused to accept the client request without a defined Content- Length.	Have the client repeat the request adding a valid Content-Length header field containing the length of the message-body in the request message.

<b>Error Code</b>	<b>Description</b>	<b>Response</b>
412 - HTTP precondition failed	A precondition given in one or more of the request-header fields evaluated to false when it was tested on the server.	Have the client place preconditions on the current resource metainformation (header field data) to prevent the requested method from being applied to a resource other than the one intended.
413 - HTTP request entity too large	The request entity from the client is larger than the server is willing or able to process.	Have the user wait a few minutes and then retry the request.
414 - HTTP request uri too large	The client has improperly converted a POST request to a GET request with long query information, or when the server is under attack by a user attempting to exploit security holes present in some servers using fixed-length buffers for reading or manipulating the Request-URI.	Have the user resubmit the request from the client.
415 - HTTP unsupported media type	Probig Trustee does not support the media the user is requesting.	The user can either call Probig Sales and discuss support for that media type, or the user can submit a different request.
416 - HTTP range not satisfiable	The range of bytes requested by the client does not exist in the header.	Have the user verify the code submitting the URL is correct.
417 - HTTP expectation failed	The expectation given in an Expect request-header field could not be met by this server, or, if the server is a proxy, the request could not be met by the next-hop server.	Make sure the URL being submitted by the user is correct, then have the user resubmit the request.
422 - HTTP unprocessable entity	The server could not process the request.	Make sure the URL being submitted by the user is correct, then have the user resubmit the request.
423 - HTTP locked	The server could not process the request.	Make sure the URL being submitted by the user is correct, then have the user resubmit the request.
424 - HTTP failed dependency	The server could not process the request.	Make sure the URL being submitted by the user is correct, then have the user resubmit the request.



Error Code	Description	Response
500 - HTTP internal server error	The problem is at the server end.	Have the user retry the request. Note that the content server or policy server may need to be restarted.
501 - HTTP not implemented	The server does not support the functionality required to fulfill the request.	Make sure the URL being submitted by the user is correct, then have the user resubmit the request.
502 - HTTP bad gateway	The server, while acting as a gateway or proxy, received an invalid response from the upstream server it accessed while trying to fulfill the request.	Have the user retry the request. Note that the content server or policy server may need to be restarted.
503 - HTTP service unavailable	The server is overloaded.	Have the user retry the request.
504 - HTTP gateway time out	The server did not receive a timely response from another server, such as a DNS lookup server.	Have the user verify that the client is pointing towards the right DNS and Probox servers, then retry the request.
505 - HTTP version not supported	There are items in the web page not supported by this version of HTTP.	Make sure the version of IE on the client is at least 5.5 and the version of HTTP supported by the Apache HTTP server is at least 1.1.
507 - HTTP insufficient storage	The content server or policy server has run out of disk space.	Have the user retry the request. Note that the content server or policy server may need to be restarted.



# Appendix A

## Glossary

---

---

The following terms are those you are likely to encounter when administering, managing, or using Probix Trustee.

<b>active</b>	An <i>active</i> entity has access to (such as a user or group) or can be accessed (such as content) by users of the PCPN.
<b>adaptor</b>	An <i>adaptor</i> integrates Probix Trustee™ with an existing user authentication or authorization systems already deployed as part of a web server environment.
<b>Auth Name</b>	An optional username sometimes needed to access a content server to get to protected content.
<b>Content</b>	One or more files or directories to which access is being granted by Probix Trustee.
<b>content server</b>	A <i>content server</i> is a server that contains the customer content. This server is also referred to as a <i>customer server</i> . A content server can be run either by you at your site or by Probix offsite.
<b>customer</b>	A <i>customer</i> is an enterprise or entity using Probix Trustee.
<b>group</b>	A <i>group</i> is a collection of users over which you can simultaneously distribute access permissions. A group is comprised of a group name, a group description, and users.
<b>manager</b>	A <i>manager</i> is a user who can manage a Probix Trustee customer.
<b>members</b>	<i>Members</i> are users who belong to a group.
<b>policy</b>	A <i>policy</i> is a collection or organization of accounts (users and groups), rights to, and schedules of access to your content. A policy lets you define the length of time a content item can be viewed, as well as whether an individual or group can access content and the types of access granted to that content.
<b>policy server</b>	A <i>policy server</i> is a server running the Probix Trustee server software for content protection. This server is also referred to as a <i>Probix server</i> . A policy server can be run either by you at your site or by Probix offsite.
<b>right</b>	A <i>right</i> is a permission given to a user or group to perform a specific action within a policy. Some examples of rights include print, transfer, and watermark.

- schedule*** A *schedule* is a window of time during which a user is granted access to secured content. A schedule can be a length of time, such as three hours, or it can be a specific interval of time with clearly defined start and end dates and times.
- suspended*** A *suspended* entity has had access revoked from (such as a user or group) or can no longer be accessed (such as content) by users of the PCPN.
- user*** A *user* is an individual to whom access to your content is granted. Users can be added to groups.

## A

- access\_log file 42
- accounts
  - adding to policy 95
  - deleting from policy 96
  - removing from policy 96
- activating
  - content 85
  - groups 75
  - members 78
  - policy 93
  - users 71
- active
  - definition 68, 139
- adaptor
  - definition 139
  - See also Probix Adaptor
- adding
  - administrator 61
  - content 83
  - customer 46
  - group 75
  - manager 54
  - policy 88
  - Probix Server 58
  - rights 65
  - rights to policy 96
  - user 71
- administrator
  - adding 61
  - deleting 63
  - editing 63
  - modifying 63
  - removing 63
- Apache server
  - restarting 109
  - starting 107
  - status 110
  - stopping 108

- Auth Name
  - definition 139

## C

- check\_pcpn utility 105
- check\_pcpn\_pkg utility 106
- client requirements
  - supported platforms 11
- content 87
  - activating 85
  - adding 83
  - adding to policy 89, 95
  - definition 68, 139
  - deleting 86
  - editing 85
  - managing 80
  - modifying 85
  - removing 86
  - removing from policy 95
  - restrictions on 87
  - suspending 85
  - types supported by Probix Trustee 68
- Content Server
  - configuration file 27
  - definition 44, 139
  - hardware requirements 10
  - software requirements 10
  - UNIX configuration requirements 10
  - Windows configuration requirements 10
- customer
  - adding 46
  - configuration file 102
  - configuring 102
  - definition 44, 139
  - editing 49
  - exporting to a file 52
  - modifying 49
  - removing 52
  - viewing logs by customer ID 39
- customer server

definition 44, 139  
See also content server

## D

debugging 115  
  Probix Trustee 15, 115

deleting  
  content 86  
  group 76  
  policy 98  
  Probix Server 60  
  rights 66  
  user 73

## E

editing  
  administrator 63  
  content 85  
  customer 49  
  customer configuration file 102  
  group 76  
  manager 55  
  policy 93  
  Probix Server 59  
  rights 66  
  user 72

error messages  
  Java-related 130

error\_log file 42

exporting  
  customer to a file 52

## G

group  
  activating 75  
  adding 75  
  adding to policy 95  
  definition 68, 139  
  deleting 76  
  editing 76  
  managing 74  
  modifying 76  
  removing 76  
  removing from policy 96  
  suspending 75

## H

httpd.conf file 83

## I

IIS Import tool 99

## L

log files

access\_log 42  
and debugging Probix Trustee 42  
error\_log 42  
pcpn\_log 42

## logger

  accessing 33  
  browser 37, 40  
  CID 35, 40  
  customized query 37  
  decoding logs made by 40  
  events 35, 40  
  fields (defined) 34  
  IP address 37, 40  
  query 37, 41  
  session ID 37, 40  
  status 37, 40  
  time 37, 40  
  user 37, 40  
  View All Logs 34  
  View Logs by Customer 39

## M

manager  
  adding 54  
  definition 44, 139  
  deleting 55  
  editing 55  
  modifying 55  
  removing 55

member  
  activating 78  
  suspending 78

members  
  definition 68, 139

Microsoft IIS server 99

modifying  
  administrator 63  
  content 85  
  customer 49  
  group 76  
  manager 55  
  policy 93  
  Probix Server 59  
  rights 66  
  user 72

## MySQL

  starting 111  
  status 113  
  stopping 112

mysqlstart utility 111

mysqlstat utility 113

mysqlstop utility 112

## **N**

notification

add to policy 91

## **O**

operating systems

supported for client 11

## **P**

PCPN

archiving logs 104

check Apache and Tomcat server status 110

check installation 105

check installation of Sun PCPN packages 106

check MySQL server status 113

customer configuration file 102

data flow in 13

data flow in the extended system 14

logger 15

overview 13

Policy Manager 15

Policy Manager tool 67

restart Apache and Tomcat servers 109

start Apache and Tomcat servers 107

starting MySQL server 111

stop Apache and Tomcat servers 108

stopping MySQL server 112

tools 15

pcpn\_log file 42

pcpnCustCfg utility 102

platforms

supported 11

policy

activating 93

add notification user 91

adding 88

adding accounts to 95

adding content 89, 95

adding groups 95

adding rights 91

adding rights to 96

adding schedule 92

adding schedule to 96

adding users 90

adding users to 95

definition 68, 139

deleting 98

deleting accounts from 96

deleting group from 96

deleting rights from 96

deleting schedule from 98

deleting users from 96

displaying 92

editing 93

editing a schedule 97

managing 87

modifying 93

modifying a schedule 97

removing 98

removing accounts from 96

removing content from 95

removing group from 96

removing rights from 96

removing schedule 98

removing users from 96

suspending 93

Policy Manager tool 67

policy server

definition 44, 139

See also Probox Server

Probox Adaptor 15

~CPcpnAdaptor function 24

AdaptorGetPolicy function 26

AdaptorGetUserName function 25

AdaptorIsProtectedResource function 24

architecture 19

ask whether the URL is protected 24

clean up after use 29

content protection 29

content viewing time 32

CPcpnAdaptor class definition 21

CPcpnAdaptor constructor 23

CPcpnAdaptor definition 21

CPcpnAdaptor destructor 24

CPcpnAdaptor function 23

function prototypes (Linux) 21

function prototypes (Solaris) 21

function prototypes (Windows) 28

functions 29

get policy information 26

get user name 25

implementing for Linux 20

implementing for Solaris 20

implementing for Windows 27

initialize 29

overview 18

pcpnmodCanPrint function 31

pcpnmodGetRenderInterval function 32

pcpnmodGetUserName function 30

pcpnmodInitialize function 29

pcpnmodIsContentProtected function 29

- pcpnmodIsWatermark function 31
- pcpnmodUninitialize function 29
- printing content 31
- RegisterAdaptor function 22
- registering 22
- unregister adaptor 23
- UnRegisterAdaptor function 23
- user requesting content 30
- watermarking content 31
- Probix Content Protection Network
  - See PCPN
- Probix Server
  - adding 58
  - administering 57
  - Auth Name 139
  - definition 44, 139
  - editing 59
  - hardware requirements 10
  - modifying 59
  - pcpncust.cfg file 27
  - pcpnpolicy.cfg file 27
  - removing 60
  - software requirements 10
- Probix Trustee 115
  - Administration tool 15
  - archiving logs 104
  - client requirements 11
  - concepts 12
  - debugging 15
  - logger 15
    - See logger
  - Policy Manager tool 67
  - system requirements 10
  - UNIX command-line utilities 15
  - versions of Windows supported 11

## R

- removing
  - administrator 63
  - content 86
  - customer 52
  - group 76
  - manager 55
  - policy 98
  - Probix Server 60
  - rights 66
  - user 73
- right
  - deleting from policy 96
  - removing from policy 96
- rights

- adding 65
- adding to policy 91, 96
- administering 64
- definition 44, 139
- deleting 66
- editing 66
- modifying 66
- print 87
- removing 66

## S

- save\_logs utility 104
- schedule
  - add to policy 92
  - adding to policy 96
  - definition 68, 140
  - deleting from policy 98
  - editing within a policy 97
  - modifying within a policy 97
  - removing from policy 98
- status message
  - text-related 128
- status messages
  - 000 - second create 121
  - 001 - Failed to retrieve IShellBrowser 121
  - 002 - fail to create IStorage object 121
  - 003 - cannot retrieve content from server 121
  - 004 - security update is available; please restart your browser 121
  - 005 - Could not initialize Probix protection 121
  - 007 - Could not start Probix Protection 121
  - 008 - Could not load corresponding \*P2.dll file 122
  - 009 - Could not load Probix01.dll 122
  - 010 - Failed to start corresponding application 122
  - 011 - Failed to get application pointer 122
  - 013 - Could not set protection 122
  - 014 - Could not detect corresponding process 122
  - 015 - Could not load target file 122
  - 016 - Cannot get IDispatch pointer 122
  - 017 - Error to get IPersistStorage interface pointer 122
  - 018 - Error to get IHlink interface pointer 122
  - 019 - PostThreadMessage failed 122
  - 020 - SetClientSite failed 122
  - 021 - Error navigating to target file 122
  - 022 - Detected rogue application 122
  - 023 - probixapp.exe shutdown 123
  - 027 - rogue port 123



029 - Injection into specific failed 123  
030 - attempt screen capture 123  
100 - HTTP continue 133  
1001 - Couldn't get PowerPoint Application Interface 124  
1002 - Failed to get PowerPoint Window HWND 124  
1003 - Failed to get PowerPoint version 124  
1004 - Could not disable menu 124  
1005 - No child window found 124  
101 - HTTP switching protocols 133  
102 - HTTP processing 133  
106 - General Error 116  
119 - General Error 116  
1501 - Unsafe Screen 130  
1502 - Incorrect URL 130  
1503 - General error 130  
1504 - Connection Failed 130  
1505 - Decryption Error 130  
1506 - Action Not Allowed 130  
1507 - Content Type Not Supported 130  
1508 - Character Encoding Error 130  
1509 - Temporarily Unsafe Screen 130  
1510 - Time Expired 130  
1511 - Loading 130  
1512 - Unsupported Browser 130  
1513 - Unsupported OS 130  
1514 - 16-bit Application 130  
1515 - Certificate Denied 131  
200 - HTTP ok 133  
2001 - failed to set Word Document protection 125  
2002 - could not find child window 125  
2003 - failed to remove key binding 125  
2004 - failed to disable menu items 125  
201 - HTTP created 133  
202 - HTTP accepted 133  
203 - HTTP non authoritative 133  
204 - HTTP no content 133  
205 - HTTP reset content 134  
206 - HTTP partial content 134  
300 - HTTP multiple choices 134  
3001 - Query Interface IPersist Memory failed 126  
3001 - QueryInterface IPersistMemory failed 127  
3002 - Couldn't activate object in place 126, 127  
3003 - Invoke "LoadFile" failed 126, 127  
3004 - Failed to get IOleInPlaceObject interface 126, 127  
3005 - Failed to hook authentication server 126, 127  
3006 - ProgIDFromCLSID with CLSID PDF failed 128  
3007 - version of Acrobat is less then 4.0 128  
301 - HTTP moved permanently 134  
302 - HTTP moved temporarily 134  
303 - HTTP see other 134  
304 - HTTP not modified 134

305 - HTTP use proxy 134  
307 - HTTP temporary redirect 134  
400 - HTTP bad request 134  
4001 - Stream for html is not created 128  
4002 - Writing base text into html wasn't succeeded 128  
4003 - Stream for PCPNHTML Reader Info is not created 128  
4004 - Write PCPNHTML Reader Info into stream was not succeeded 128  
4005 - OleLoad Picture in Image wasn't reached 128  
401 - HTTP unauthorized 134  
402 - HTTP payment required 134  
403 - HTTP forbidden 135  
404 - HTTP not found 135  
405 - HTTP method not allowed 135  
406 - HTTP not acceptable 135  
407 - HTTP proxy authentication required 135  
408 - HTTP request time out 135  
409 - HTTP conflict 135  
410 - HTTP gone 135  
411 - HTTP length required 135  
412 - HTTP precondition failed 136  
413 - HTTP request entity too large 136  
414 - HTTP request uri too large 136  
415 - HTTP unsupported media type 136  
416 - HTTP range not satisfiable 136  
417 - HTTP expectation failed 136  
422 - HTTP unprocessable entity 136  
423 - HTTP locked 136  
424 - HTTP failed dependency 136  
441 - PCPN bad request: no parameters 116  
442 - PCPN bad request: parameters count 116  
443 - PCPN bad request: parameters list 116  
444 - PCPN bad request: customer ID 116  
445 - PCPN bad request: nonce length 116  
446 - PCPN bad request: hash length 116  
447 - PCPN bad request: authorized redirect 116  
448 - PCPN bad request: time stamp 117  
449 - PCPN bad request: original URL 117  
450 - PCPN bad request: information 117  
451 - PCPN bad request: SID length 117  
452 - PCPN bad request: public key length 117  
453 - PCPN bad request: authentication test 117  
454 - PCPN bad request: version 117  
455 - PCPN bad request: authentication client 117  
456 - PCPN bad request: key exchange replay 118  
457 - PCPN bad request: redirection replay 118  
500 - HTTP internal server error 118, 137  
5001 - Failed to get application pointer 129  
5002 - Unable to set Excel document Sheets protection 129  
5003 - Unable to remove dangerous hotkeys 129  
5004 - Failed to disable dangerous menu items. 129  
501 - HTTP not implemented 137

502 - HTTP bad gateway 137  
503 - HTTP service unavailable 137  
504 - HTTP gateway time out 137  
505 - HTTP version not supported 137  
507 - HTTP insufficient storage 137  
551 - internal WWW root error 118  
552 - internal configuration error 118  
553 - internal allocation error 118  
554 - internal socket error 118  
555 - internal get state error 118  
556 - internal save state error 119  
557 - internal no policy error 119  
6 - Probix cxa8() function failed 121  
900 - PCPN-specific error 119  
901 - time response error 119  
902 - time authentication content error 119  
951 - customer request URL error 119  
952 - customer request address error 119  
953 - customer connect error 119  
954 - customer read from error 119  
955 - customer no data error 119  
956 - customer HTTP verified error 120  
957 - customer read header error 120  
958 - customer zero header error 120  
959 - customer zero content error 120  
960 - customer content error 120  
961 - customer cont authentication error 120  
Acrobat-related 127  
application errors 124  
Excel-related 129  
Hangul-related 126  
Java-related 130  
JPG-related 128  
PowerPoint-related 124  
Probix Trustee for Outlook  
    -1 - PT4O\_ERR\_PARAM 132  
    -10 - PT4O\_ERR\_MESSAGE 132  
    -11 - PT4O\_ERR\_ENCODING 132  
    -12 - PT4O\_ERR\_DATABASE 132  
    -13 - PT4O\_ERR\_AUTH 132  
    -14 - PT4O\_ERR\_HASH 132  
    -2 - PT4O\_ERR\_NOFILE 132  
    -3 - PT4O\_ERR\_OPEN 132  
    -4 - PT4O\_ERR\_READ 132  
    -5 - PT4O\_ERR\_WRITE 132  
    -6 - PT4O\_ERR\_STAT 132  
    -7 - PT4O\_ERR\_PARSE 132  
    -8 - PT4O\_ERR\_TEMP 132  
    -9 - PT4O\_ERR\_MEMORY 132  
standard HTTP status codes 133  
Windows ActiveX application 121

- Word-related 125
- suspended
  - definition 68, 140
- suspending
  - content 85
  - groups 75
  - members 78
  - policy 93
  - users 71

## **T**

- Tomcat server
  - restarting 109
  - starting 107
  - status 110
  - stopping 108

## **U**

- user
  - activating 71
  - adding 71
  - definition 68, 140
  - deleting 73
  - editing 72
  - modifying 72
  - removing 73
  - suspending 71
- users
  - adding to policy 90, 95
  - deleting from policy 96
  - removing from policy 96
- users.asp file 99

## **W**

- webrestart utility 109
- webstart utility 84, 107
- webstat utility 110
- webstop utility 84, 108