Probix Trustee

Troubleshooting Guide

Release 2.1

July 9, 2003

Probix, Inc.

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

Chapter 1

Introduction

This book explains how to diagnose problems you may encounter while running Probix Trustee™. The topics covered in this chapter are:

- "Probix Trustee Concepts" on page 6
- "Supported Platforms for Probix Trustee" on page 7
- "Probix Content Protection Network Overview" on page 9
- "PCPN Tools" on page 11

PROBIX TRUSTEE CONCEPTS

Probix allows content owners 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 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*. The content can be organized as 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.

- **Revoke Access Rights**

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

- **Review Audit Trail**

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

SUPPORTED PLATFORMS FOR PROBIX TRUSTEE

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 runs on a Sun Microsystems SPARC ULTRA 10 or higher, using:

- 256 MB 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.

Customer (Content) Server Requirements

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

UNIX Configuration

- Sun Microsystems SPARC ULTRA 10 or higher
- 256 MB 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.

Windows Configuration

- Windows 2000
- Microsoft Internet Information Services 6.0
- Tomcat
- Apache web server
- MySQL Database Server version 3.23 or higher

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

Linux Configuration

- Red Hat Linux version 7.3

- Apache web server version 1.3.x
- ModSSL for Apache

Client Requirements

The Probix Trustee client must be running one of the following operating systems:

- Windows 98 SE
- Windows ME
- Windows 2000
- Windows XP
- Windows NT 4.0 SP6 or greater

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.

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.
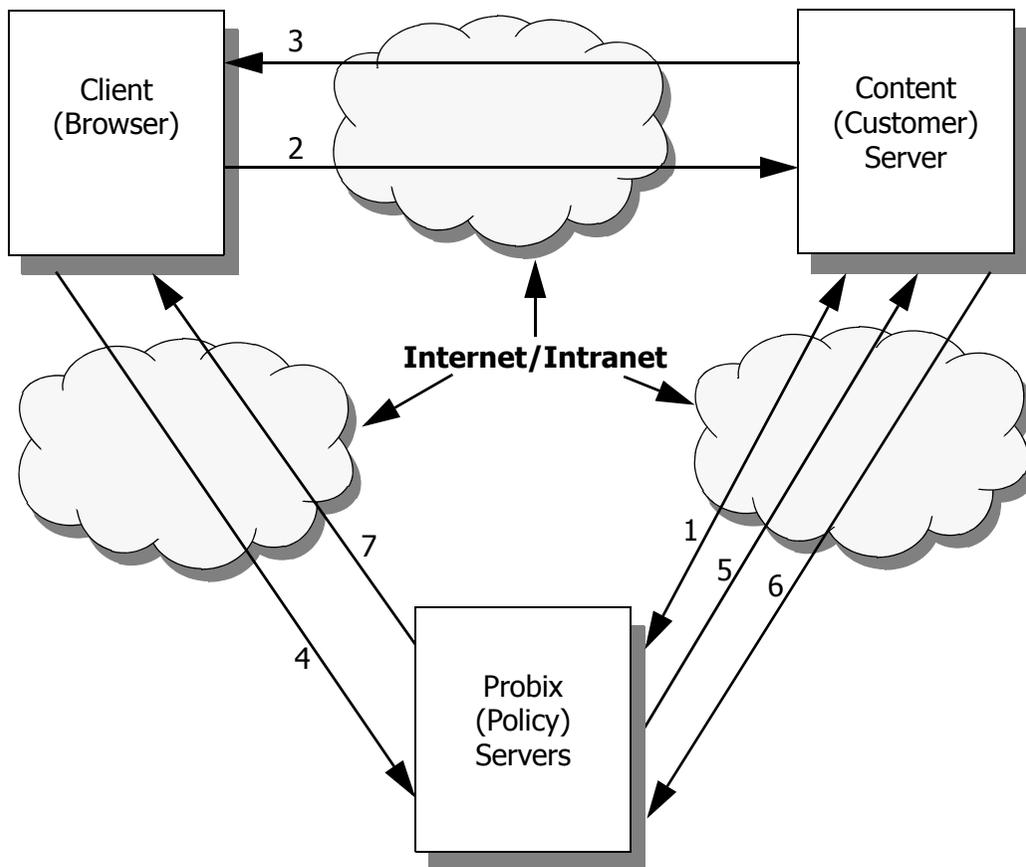
The steps are:

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.
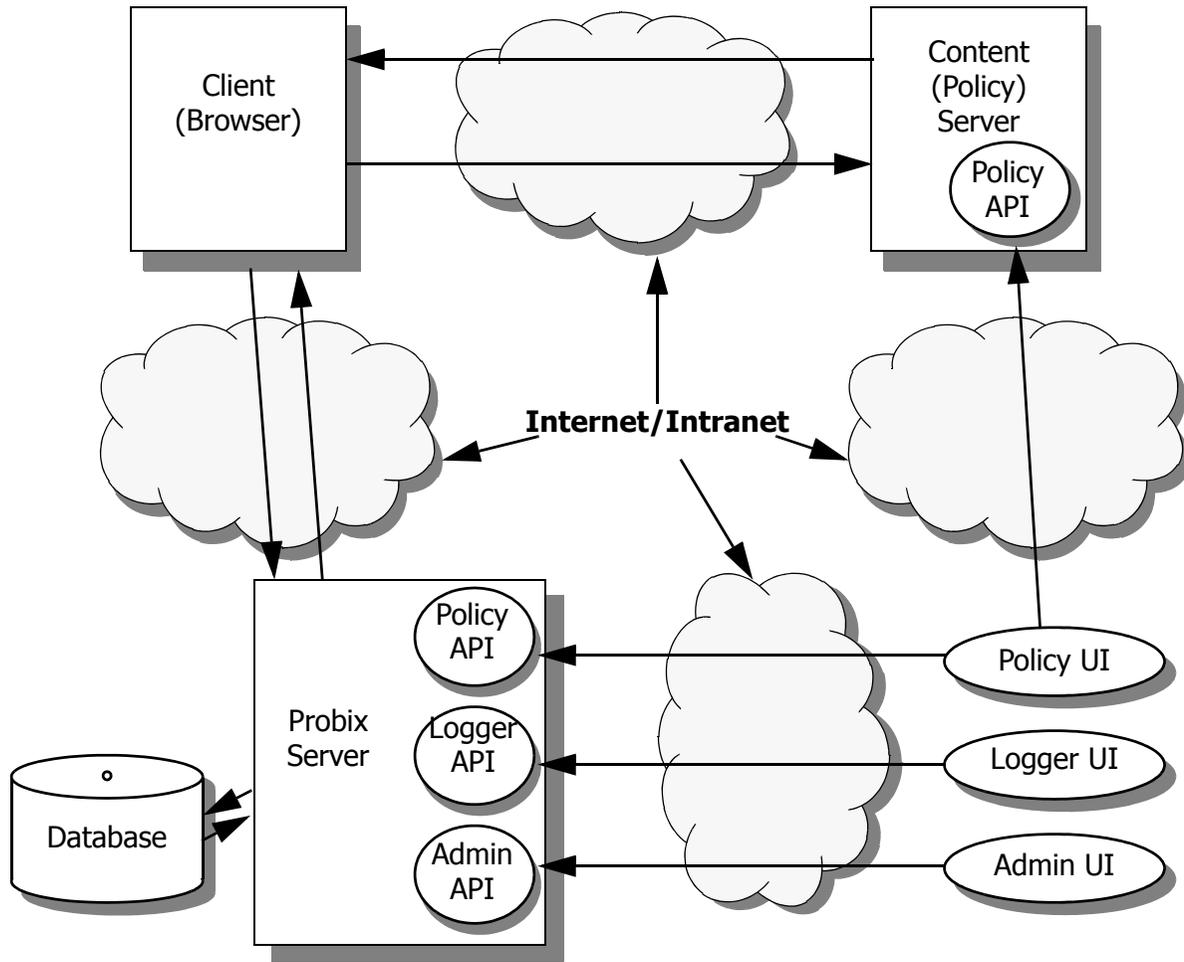
PCPN TOOLS

Problems that occur when running Probix Trustee can be debugged using tools discussed in this document. The tools most appropriate for a given task depend upon where in the PCPN the problem is occurring.

Probix provides two HTML-based tools that allow you to diagnose and clear up client-side problems:

- The `probix_diag.htm` utility creates a log file containing information about the client system and the host running Probix Trustee.

- The `probix_cleanup.htm` utility cleans up extraneous files on the client system.

These utilities are discussed in Chapter 4, "Probix Tools" on page 25.

Client-side diagnostic tools are also available at:

- http://www.probix.com/support/support.htm

- http://gl.probix.net/probix_diag.htm

- http://gl.probix.net/probix_cleanup.htm

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 15.

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 Chapter 6, "Troubleshooting Messages" on page 39.

Some third-party applications may also prove useful in debugging problems encountered while running Probix Trustee. These can be found in Chapter 5, "Third-Party Tools" on page 33.

Chapter 2

Installation Problems

This chapter describes the problems that can occur during installation of Probix Trustee™ and how to troubleshoot them.

Chapter 3

Using the Probix Trustee Logger

The Probix Trustee^{TM} 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 19.

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:

Probix Server Log Record (In typical order)	Description
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.

Probix Server Log Record (In typical order)	Description
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 *not* 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:

Typical WRONGREQ requests	Description
400	A malformed HTTP request, compare with records for the same time in the `access_log` and `error_log` files in the `$APACHE_DIR/logs` directory.
403	This is usually a result of an attempt to transfer protected content via RealDownload.
443	A malformed HTTP request; compare with records for the same time in the `access_log` and `error_log` files in the `$APACHE_DIR/logs` 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 `access_log` and `error_log` files in the `$APACHE_DIR/logs` 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 sssion. 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

Probix Tools

This chapter describes the use of both parts of the ProbixUtil.exe utility to troubleshoot problems with Probix Trustee™:

- "Running the Diagnostic Utility" on page 27
- "Running the Cleanup Utility" on page 29

These diagnostics diagnose the client system. They confirm the necessary support for the PCPN is present and the local security settings are sufficient to support PCPN operation.

To use the utility, select the link `myhost/probix/ProbixUtil.exe` where *myhost* is the name of the server running Probix Trustee.
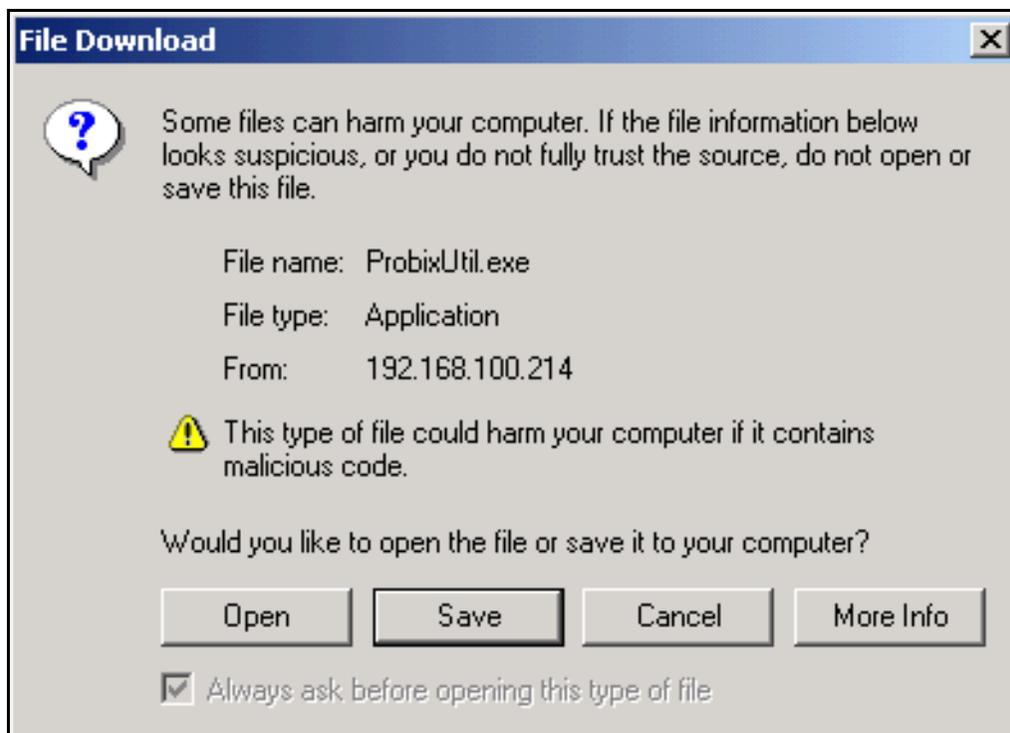
You are asked whether you want to save or open this. Select **Open**.
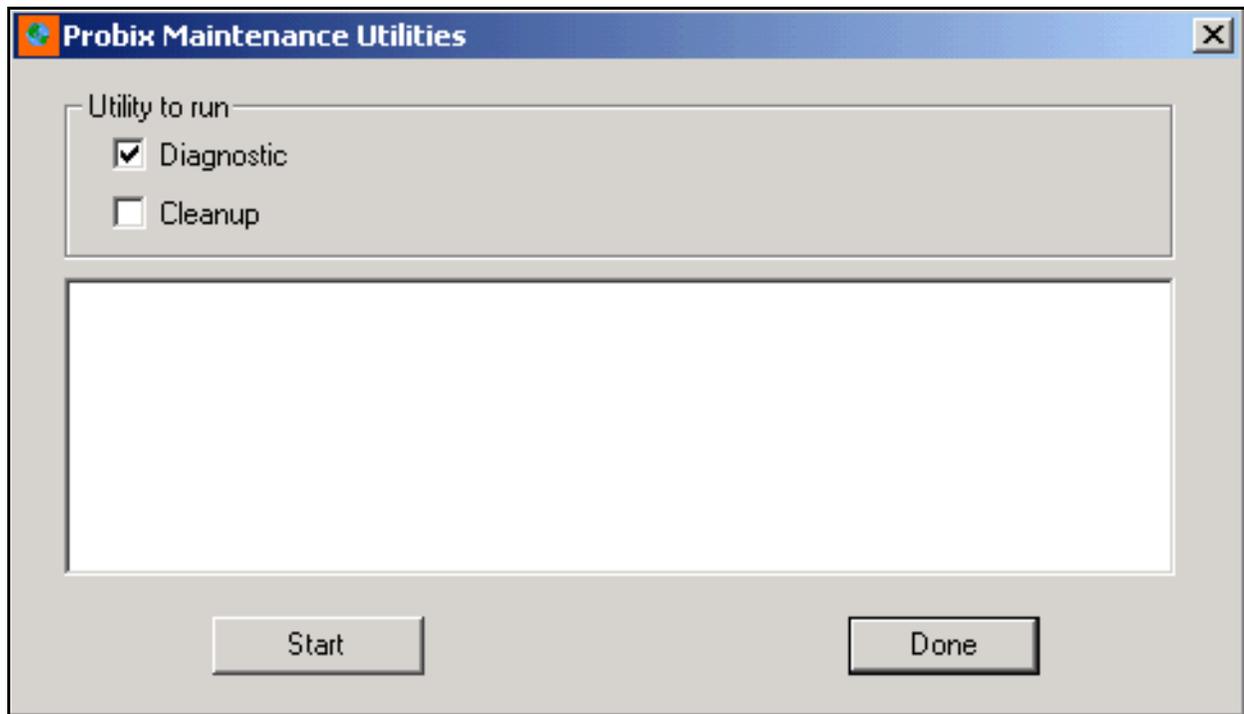
From here you can select one or both of the following:

- **Diagnostic** - perform diagnostic tests on the client environment to make sure it is suitable for running Probix Trustee
- **Cleanup** - remove any files left behind by previously running Probix Trustee that may interfere with accessing protected content

Once you have made your selection, click **Start**.

RUNNING THE DIAGNOSTIC UTILITY

When you select the **Diagnostic** utility and click **Start**, the following appears showing you the diagnostic is running:
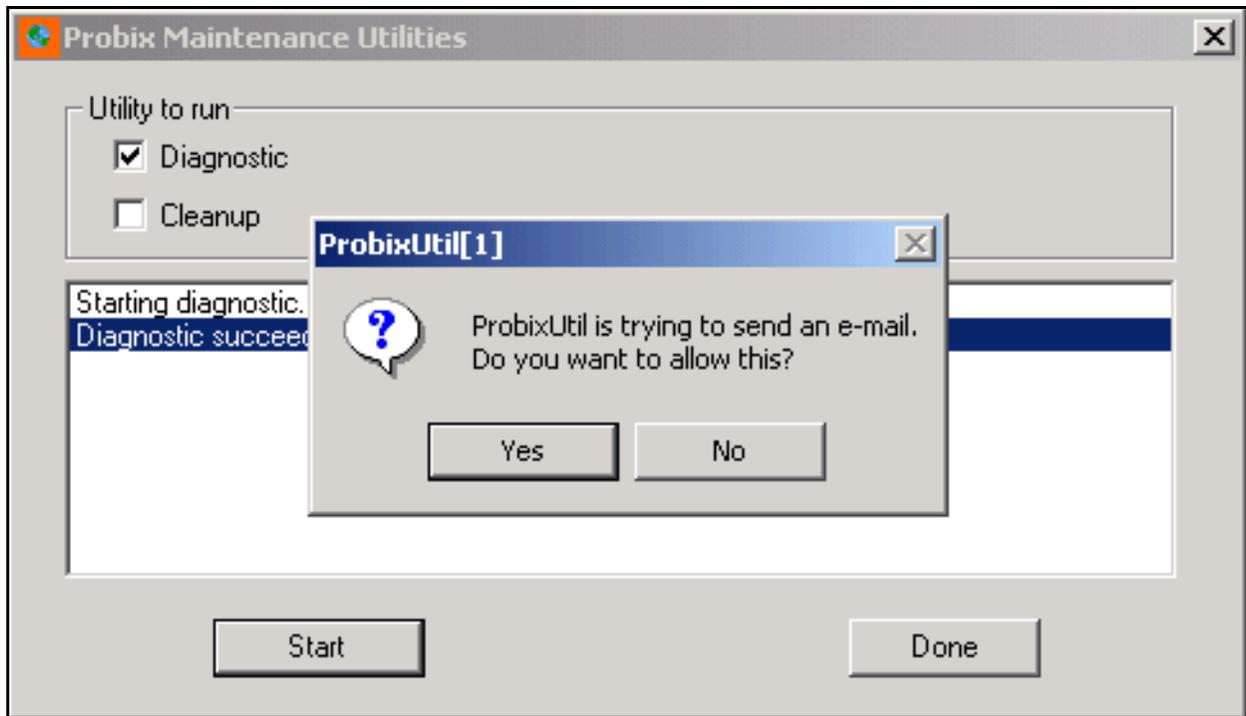

When prompted to send e-mail, click Yes to e-mail a report to Probix support.
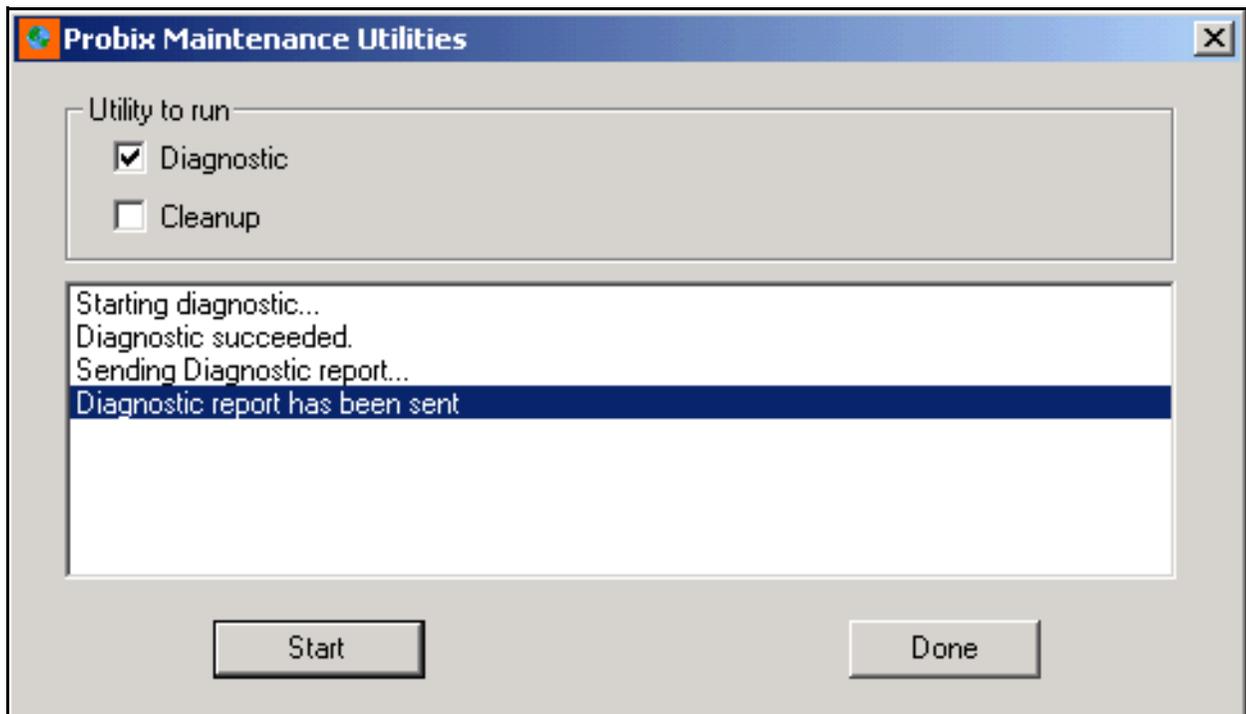
When the Diagnostic is finished running the phrase **Diagnostic report has been sent** appears in the message window. Click **Done** to exit the utility.

RUNNING THE CLEANUP UTILITY

When you select the **Cleanup** utility and click **Start**, the following appears showing you the cleanup utility is running:
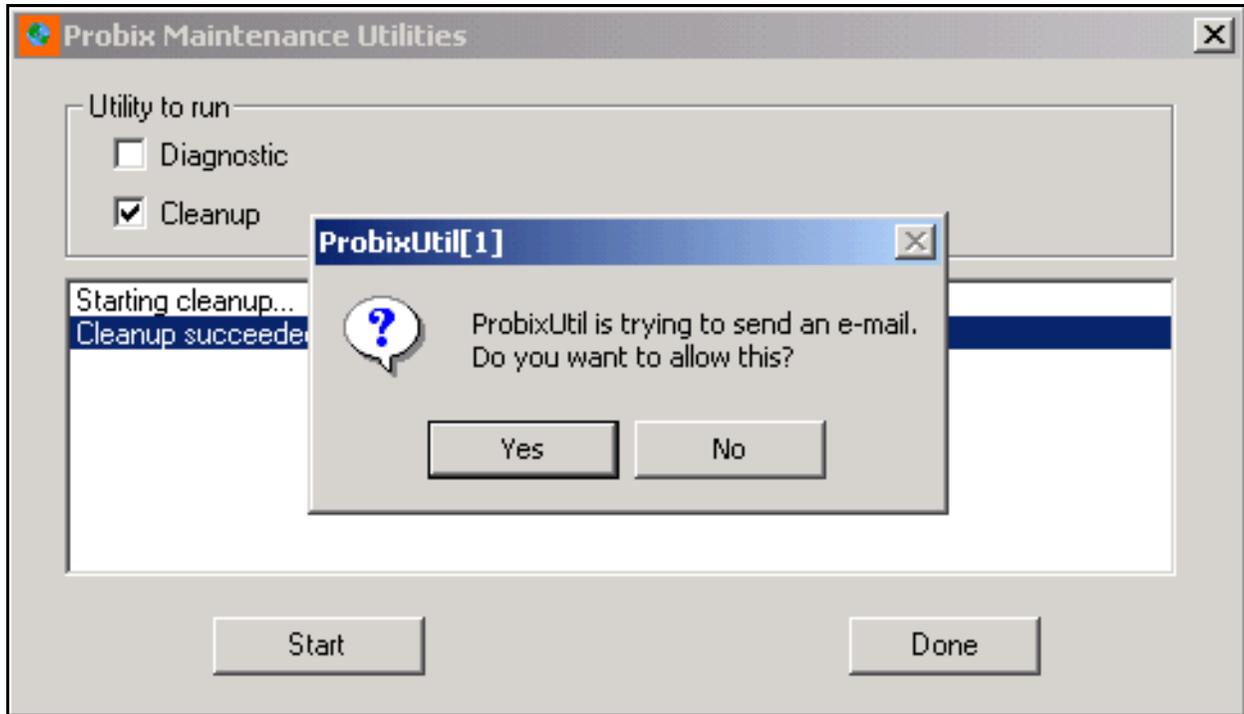
When prompted to send e-mail, click **Yes** to e-mail a report to Probix support.
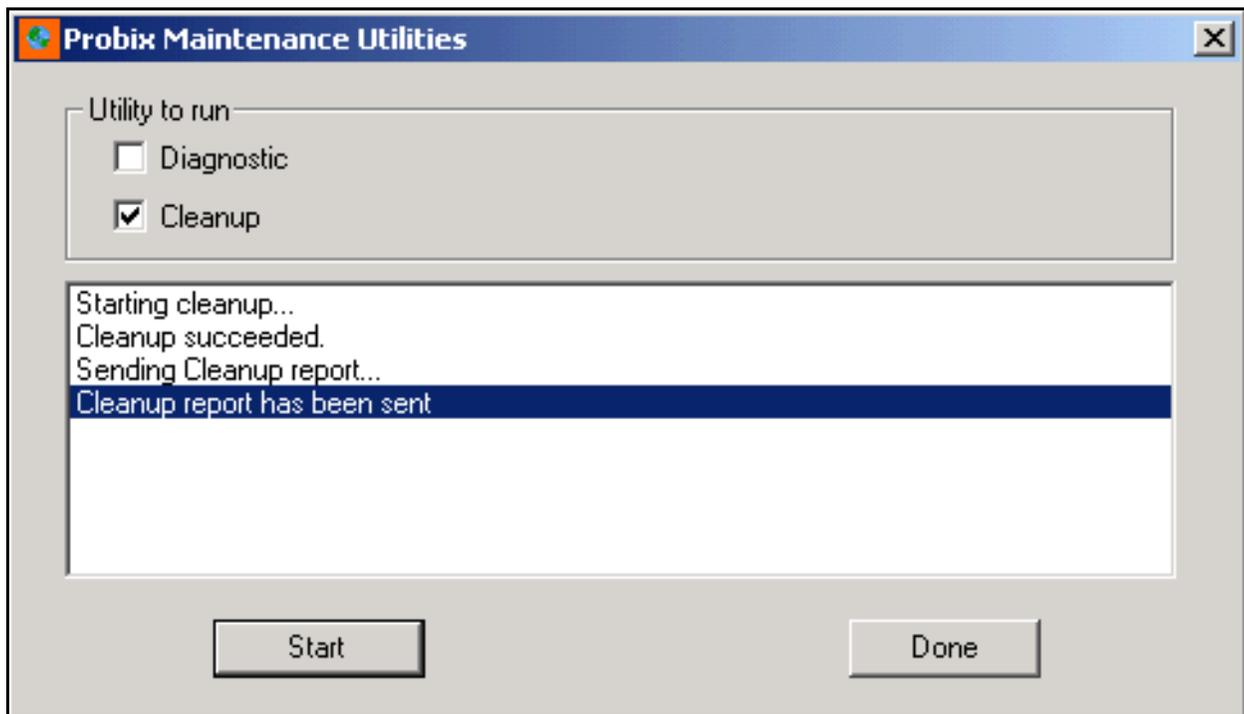
When the Cleanup is finished running the phrase **Cleanup report has been sent** appears in the message window. Click **Done** to exit the utility.

Note: The Cleanup utility cannot run with certain utilities running, such as Microsoft Office applications and Adobe Acrobat. If you do not quit these utilities before running the Cleanup utility, a message similar to the following appears:
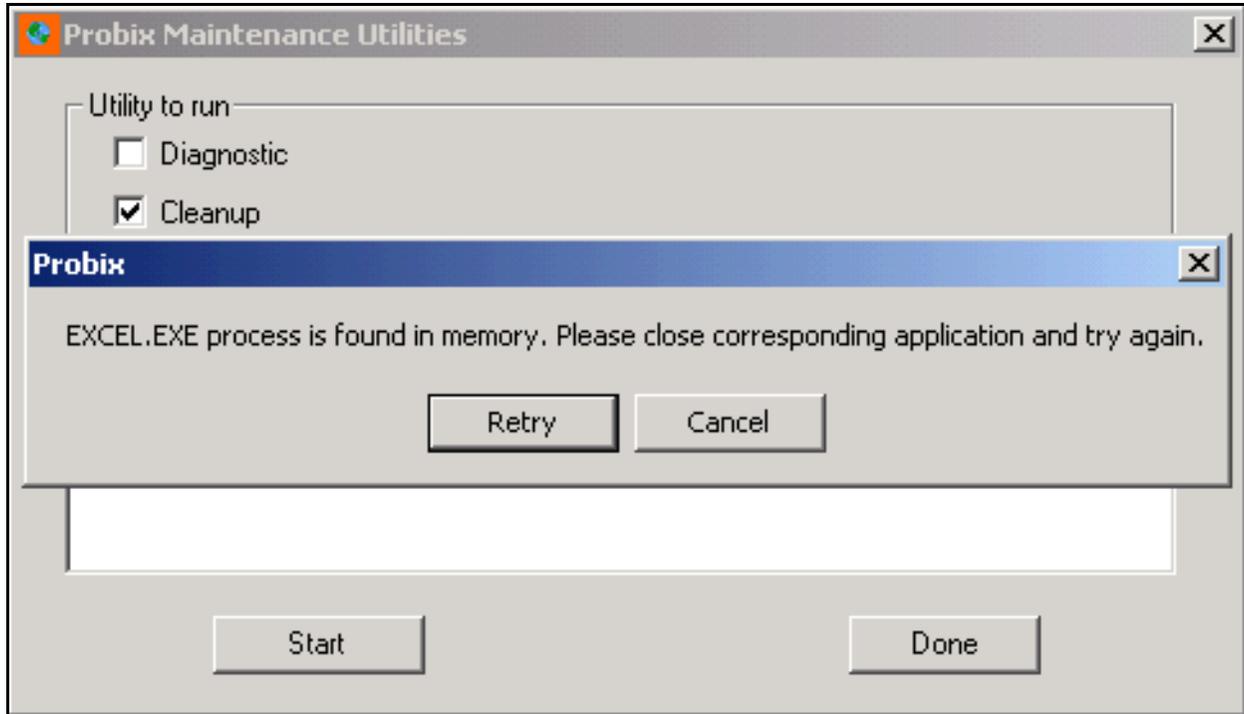
To run the Cleanup utility, you must quit the named application (in this case, EXCEL.EXE) and then click **Retry**, then click **Yes** to send a report.

If you want to exit the Cleanup utility, click **Cancel**.
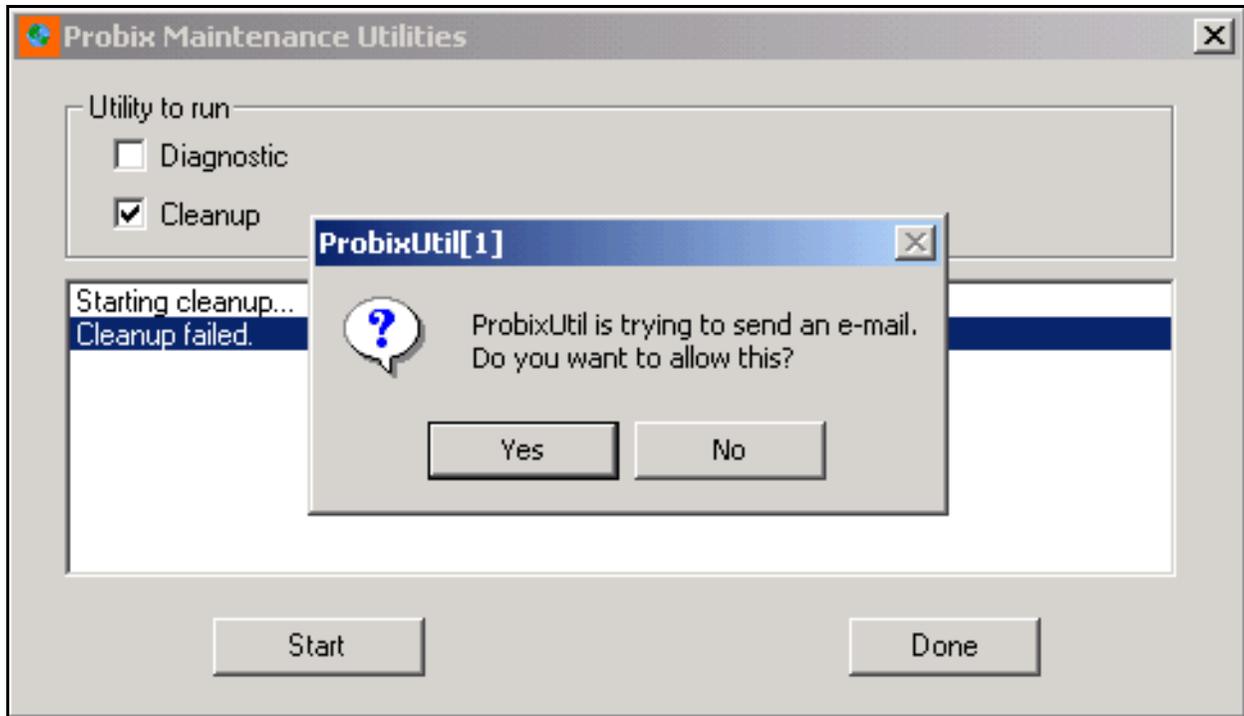
When asked if you want to send e-mail, click **No**.
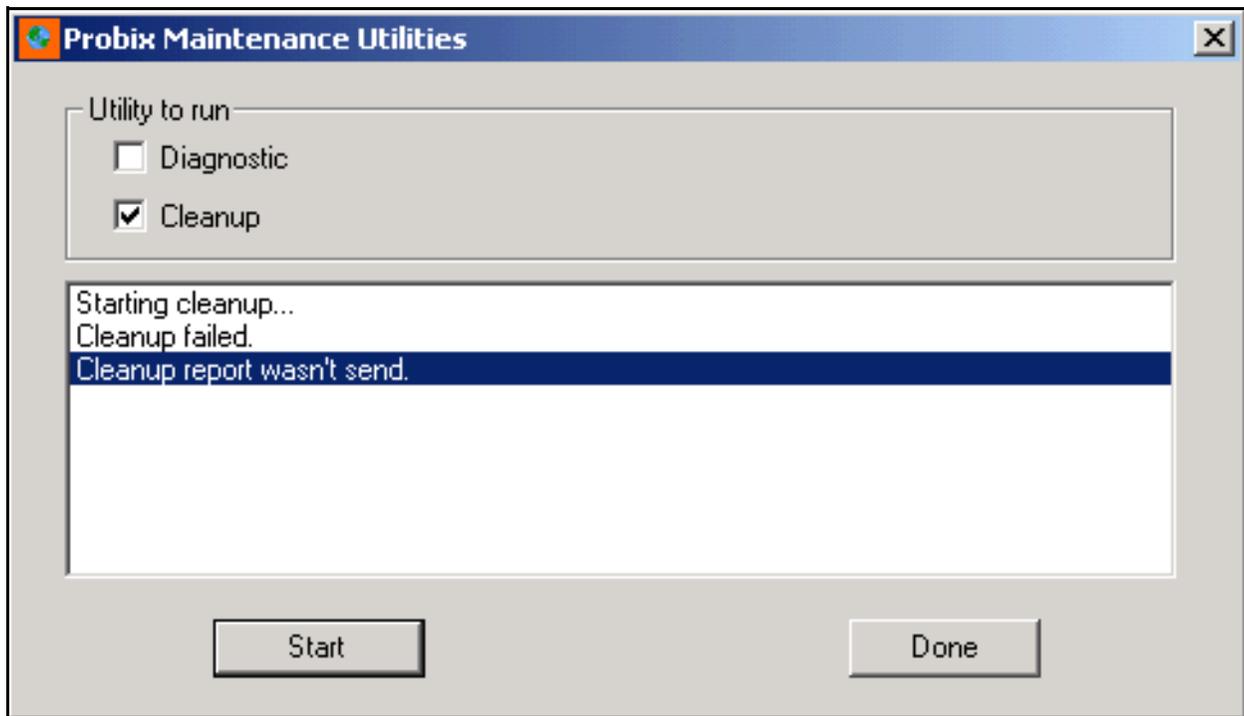
When the Cleanup is finished running the phrase **Cleanup report wasn't send** appears in the message window. Click **Done** to exit the utility.

Chapter 5

Third-Party Tools

This chapter describes third-party tools you can use to troubleshoot problems with Probix Trustee™:

- Tools Sold by Outside Vendors
- Free Tools

TOOLS SOLD BY OUTSIDE VENDORS

The following tools sold by outside vendors have proven useful in troubleshooting problems that occur when running Probix Trustee:

- Cisco Works
- HP OpenView

Cisco Works

Cisco Works is useful for LAN management. It comes with a GUI configuration tool. You can use Cisco Works to perform:

- configuration and software image management
- inventory tracking and syslog analysis

Cisco Works can be purchased from Cisco Systems (http://www.cisco.com).

HP OpenView

The HP OpenView Network Node Manager application is part of the HP OpenView suite. Use this for:

- network topology and availability
- fault management (SNMP traps and syslog)
- notification (e-mail)
- web-based reporting

Through HP OpenView you can access the following tools:

- Network Presenter- lets you view an IP network map on a management station or management console from any machine with a supporting web browser
- Unused IP Addresses - shows addresses in managed networks which NNM has not heard from and are possibly unused.
- Node Filter - lets you view a set of network nodes defined by a filter.
- CDP View - provides a CDP (Cisco Discovery Protocol) view of network nodes.
- Event Correlation Configuration - modifies the flow of events by recognizing patterns of events and replacing them with a single event.
- NNM Alarm Browser - browses incoming alarms and alarms contained in the event database.
- Report Presenter - lets you view reports using a presentation interface.
- Report Configuration - the interface for creating, modifying, and scheduling reports.
- SNMP Data Presenter - lets you view reports and information on configuration and performance
- SNMP MIB Browser - lets you use the HP OpenView Web SNMP MIB Browser to retrieve SNMP data.
- Reporting and Analysis tool - this web-based version of Open View NNM's reporting and analysis tool. This tool tracks availability and performance data for both network and server devices. It uses trend data from Open View based on ICMP ping response times and interface utilization based on collected SNMP data.

HP OpenView can be purchased HP; the home page is http://openview.hp.com.

FREE TOOLS

The following tools useful for debugging Probix Trustee problems are available from various sites on the Internet:

- Centralized Web-Based Management Server
- MRTG
- Netsaint
- ntop
- Snort
- traceroute

All of these tools have web-based interfaces, making them easily accessible via a centralized web-based management server such as Apache.

Centralized Web-Based Management Server

Probix recommends you set up a centralized web-based management server, such as Apache (http://www.apache.org) for your troubleshooting tools. This kind of server makes all information one click away from access.

Applications can monitor data centers via secure virtual private network (VPN) connections using PIX firewalls at each end. Static data, such as configuration and image files, can be stored on the web server. Web-based network management applications can be quickly accessed from any web browser-equipped client on the network.

MRTG

The Multi Router Traffic Grapher (MRTG) performs network performance analysis via SNMP and graphing, and uses custom scripts to monitor system utilization.

MRTG monitors the traffic load on network-links. MRTG generates HTML pages containing graphical images which provide a live visual representation of this traffic; the page http://mrtg.yeehaw.net contains an example. MRTG is based on Perl and C and runs under UNIX and Windows NT.

More information on MRTG can be found at http://www.mrtg.org.

Netsaint

Netsaint is a server and service monitoring tool; it lets you monitor system availability and network services. NetSaint monitors hosts and services, alerting you when things go wrong.

NetSaint's features include:

- Monitoring of network services (SMTP, POP3, HTTP, NNTP, PING)
- Monitoring of host resources (processor load, disk usage)
- A plugin design that allows you to develop your own service checks
- Parallelized service checks
- Ability to define network host hierarchy using "parent" hosts, allowing detection of and distinction between hosts that are down and those that are unreachable

- Contact notifications when service or host problems occur and get resolved (via e-mail, pager, or a user-defined method)

- Ability to define event handlers to be run during service or host events for proactive problem resolution

- Automatic log file rotation

- Support for implementing redundant monitoring hosts

- Optional web interface for viewing current network status, notification and problem history, log file, and so forth.

For more information about Netsaint, visit http://www.netsaint.org.

ntop

The ntop utility a UNIX tool that shows network usage similar to what the UNIX command `top` does. The ntop utility runs under UNIX and on Win32.

The ntop utility comes with two applications:

- the web-based `ntop` that sports an embedded web server

- `intop` (interactive ntop), a command line-based interface to the ntop packet sniffer.

For more information on ntop and intop, visit http://www.ntop.org/ntop.html.

Snort

Snort is a lightweight network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching and matching, and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts.

Snort has three primary uses:

- a straight packet sniffer like tcpdump(1)

- a packet logger (useful for network traffic debugging)

- a full blown network intrusion detection system

Snort uses a flexible rules language to describe traffic it should collect or pass, and a detection engine that utilizes a modular plugin architecture. Snort also has a real-time alerting capability, incorporating alerting mechanisms for syslog, a specified file, a UNIX socket, or WinPopup messages to Windows clients using Samba's smbclient.

Snort comes with the SnortSnarf utility, which is the web front-end for viewing security log data that Snort produces.

SnortSnarf is a Perl program that takes files of alerts generated by Snort and produces HTML output intended for diagnostic inspection and tracking down problems. The model is that one is using a cron job or similar to produce a daily/hourly/whatever file of snort alerts. This script can be run on each such file to produce a convenient HTML breakout of all the alerts.

For more information on Snort, visit http://www.snort.org.

traceroute

The traceroute utility lets you trace the path between your client and another host. The site http://www.traceroute.org lets you trace routes from anywhere in the world to destinations of interest.

Chapter 6

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.

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 *without* 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 con firm 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 con firm 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 con firm 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.	1. Make sure the Content Server and Probix Server have compatible software versions. 2. Use network monitoring tools to con firm the URL the user requested arrives at the Content Server unaltered.
453 - PCPN bad request: authentication test	The user was testing the code.	1. Make sure the Content Server and Probix Server have compatible software versions. 2. Use network monitoring tools to con firm the URL the user requested arrives at the Content Server unaltered.
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.	1. Make sure the Content Server and Probix Server have compatible software versions. 2. Use network monitoring tools to con firm the URL the user requested arrives at the Content Server unaltered.

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.	1. Make sure the Content Server and Probix Server have compatible software versions. 2. Use network monitoring tools to con firm the URL the user requested arrives at the Content Server unaltered.
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.	The redirected URL can be used only once. If the user has not tried to reuse a redirected URL: 1. Make sure the user's broswer is not cacheing the redirected URL. 2. Use network monitoring tools to identify the source using the redirected URL.
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.	1. Make sure the Content Server and Probix Server have compatible software versions. 2. Use network monitoring tools to con firm the URL the user requested arrives at the Content Server unaltered.
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 con firm 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.	1. Use network monitoring tools to identify the source of the communication problem from the Probix Server to the Content Server. 2. Use network monitoring tools to con firm the URL the user requested arrives at the Content Server unaltered.

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.	1. Quit and restart the browser. 2. Run the `probix_cleanup.htm` utility. At the end of the utility you are prompted to close the browser. 3. Quit and restart the browser.
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.

Error Code	Description	Response
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: 1. Quit PowerPoint. 2. Quit and restart the browser. 3. Try requesting the document again.
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: 1. Quit PowerPoint. 2. Quit and restart the browser. 3. Try requesting the document again.
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: 1. Quit PowerPoint. 2. Quit and restart the browser. 3. Try requesting the document again.
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: 1. Quit PowerPoint. 2. Quit and restart the browser. 3. Try requesting the document again.
1005 - No child window found	Microsoft PowerPoint is not operating properly.	If Microsoft PowerPoint is already installed on the client system: 1. Quit PowerPoint. 2. Quit and restart the browser. 3. Try requesting the document again.

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: 1. Quit Word. 2. Quit and restart the browser. 3. Try requesting the document again.
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: 1. Quit Word. 2. Quit and restart the browser. 3. Try requesting the document again.
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: 1. Quit Word. 2. Quit and restart the browser. 3. Try requesting the document again.
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: 1. Quit Word. 2. Quit and restart the browser. 3. Try requesting the document again.

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.

Probix 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.	If the user is already running Adobe Acrobat 4.0 or higher on the client: 1. Quit Acrobat. 2. Quit and restart the browser. 3. Try requesting the document again.
3002 - Couldn't activate object in place	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: 1. Quit Acrobat. 2. Quit and restart the browser. 3. Try requesting the document again.
3003 - Invoke "LoadFile" 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: 1. Quit Acrobat. 2. Quit and restart the browser. 3. Try requesting the document again.
3004 - Failed to get IOleInPlaceObject interface	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: 1. Quit Acrobat. 2. Quit and restart the browser. 3. Try requesting the document again.
3005 - Failed to hook authentication server	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: 1. Quit Acrobat. 2. Quit and restart the browser. 3. Try requesting the document again.

Error Code	Description	Response
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: 1. Quit Acrobat. 2. Quit and restart the browser. 3. Try requesting the document again.
3007 - version of Acrobat is less then 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: 1. Quit Acrobat. 2. Quit and restart the browser. 3. Try requesting the document again.

Probix JPG and Text Viewer Plugin Errors

Error Code	Description	Response
4001 - Stream for html is not created		1. Quit and restart the browser. 2. Try requesting the document again.
4002 - Writing base text into html wasn't succeeded		1. Quit and restart the browser. 2. Try requesting the document again.
4003 - Stream for PCPNHTML Reader Info is not created		1. Quit and restart the browser. 2. Try requesting the document again.
4004 - Write PCPNHTML Reader Info into stream was not succeeded		1. Quit and restart the browser. 2. Try requesting the document again.
4005 - OleLoad Picture in Image wasn't reached		1. Quit and restart the browser. 2. Try requesting the document again.

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.	If the user is already running MS Excel on the client: 1. Quit Excel. 2. Quit and restart the browser. 3. Try requesting the document again.
5002 - Unable to set Excel document Sheets protection	The client is either running an unsupported or improperly installed version of MS Excel.	If the user is already running MS Excel on the client: 1. Quit Excel. 2. Quit and restart the browser. 3. Try requesting the document again.
5003 - Unable to remove dangerous hotkeys	The client is either running an unsupported or improperly installed version of MS Excel.	If the user is already running MS Excel on the client: 1. Quit Excel. 2. Quit and restart the browser. 3. Try requesting the document again.
5004 - Failed to dsiable dangerous menu items.	The client is either running an unsupported or improperly installed version of MS Excel.	If the user is already running MS Excel on the client: 1. Quit Excel. 2. Quit and restart the browser. 3. Try requesting the document again.

JAVA STATUS MESSAGES

Error Code	Description	Response
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.

Error Code	Description	Response
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.

Error Code	Description	Response
-1 - PT4O_ERR_PARAM	Internal error.	Have the user retry sending the message.
-2 - PT4O_ERR_NOFILE	Internal error.	Have the user retry sending the message.
-3 - PT4O_ERR_OPEN	Internal error.	Have the user retry sending the message.
-4 - PT4O_ERR_READ	Internal error.	Have the user retry sending the message.
-5 - PT4O_ERR_WRITE	Internal error.	Have the user retry sending the message.
-6 - PT4O_ERR_STAT	Internal error.	Have the user retry sending the message.
-7 - PT4O_ERR_PARSE	The message has been corrupted into an unrecognized format.	Have the user retry sending the message.
-8 - PT4O_ERR_TEMP	Internal error.	Have the user retry sending the message.
-9 - PT4O_ERR_MEMORY	Internal error.	Have the user retry sending the message.
-10 - PT4O_ERR_MESSAGE	The message has been corrupted into an unrecognized format.	Have the user retry sending the message.
-11 - PT4O_ERR_ENCODING	An attachment uses an unsupported coding algorithm.	Have the user retry sending the message.
-12 - PT4O_ERR_DATABASE	Internal error.	Have the user retry sending the message.
-13 - PT4O_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 - PT4O_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.

Error Code	Description	Response
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.

Error Code	Description	Response
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.

Error Code	Description	Response
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	Probix Trustee does not support the media the user is requesting.	The user can either call Probix 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 Probix 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.

Index