eTrust Audit

Release Notes

r8 SP2 CR1

CA Product References

This document references the following CA products:

- eTrust Security Command Center (SCC)
-

Contact CA

Contact Technical Support

For your convenience, CA provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA products. At http://ca.com/support, you can access the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Provide Feedback

If you have comments or questions about CA product documentation, you can send a message to techpubs@ca.com.

If you would like to provide feedback about CA product documentation, complete our short customer survey, which is also available on the CA Support website, found at http://ca.com/docs.

Contents

Chapter 1: Welcome

Welcome to eTrust Audit r8 SP2 CR1. This document contains information about product installation considerations, operating system support, new features, known and fixed issues, and information about contacting CA Technical Support.

Chapter 2: Operating System Support

This section contains the following topics:

eTrust Audit Client

The following are the supported operating systems for eTrust Audit Client:

Note: If you are installing the Client on a Windows system, and plan to install on a partition other than the system partition, you must have at least 200 MB free space on the system partition, and at least 200 MB free space on the target partition.

Platform	Platform Version	Processor	Patch Level	Prerequisites and Notes
Windows	XP Professional XP Home	x86	Service Pack 2	
	Server 2003, Standard Edition	x86	Service Pack 1, Release 2	
	Server 2003, Enterprise Edition	x64 (AMD64, EM64T)	Service Pack 1, Release 2	
	Server 2008, Standard Edition	x86	Service Pack 1	
	Server 2008, Enterprise Edition	x86	Service Pack 1	
Solaris	8	SPARC	Patches 108434 and 109147, or cluster pack	
	9	SPARC		
	10 Including running in a Solaris Logical Domain (LDOM) and Solaris whole root zone	SPARC		

Platform	Platform Version	Processor	Patch Level	Prerequisites and Notes
Red Hat Linux	EL 3.0	x86	Kernel 2.4.21-4 EL	The following rpm packages need to be installed: compat-libstdc++-33-3.2.3-47.3.i386.rpm compat-gcc-32-3.2.3-47.3.i386.rpm compat-gcc-32-c++-3.2.3-47.3.i386.rpm glibc-devel-2.3.4-2.i386.rpm glibc-headers-2.3.4-2.i386.rpm glibc-kernheaders-2.4-9.1.87.i386.rpm
	EL 4.0	x86	Kernel 2.6.9-5.ELsmp	The following rpm packages need to be installed: compat-libstdc++-33-3.2.3-47.3.i386.rpm compat-gcc-32-3.2.3-47.3.i386.rpm compat-gcc-32-c++-3.2.3-47.3.i386.rpm glibc-devel-2.3.4-2.i386.rpm glibc-headers-2.3.4-2.i386.rpm glibc-kernheaders-2.4-9.1.87.i386.rpm
	EL 4.0 U3	x64 (AMD64 / EM64T)	Kernel 2.6.9-34.0.1.ELsmp	32-bit libstdc++.so.5
	EL 5.0	x86		
	EL 5.0	x64 (AMD64 / EM64T)		
	EL 5.1	x86	Kernel 2.6.18-53.el5	The following rpm packages need to be installed: compat-libstdc++-33-3.2.3-47.3.i386.rpm compat-gcc-32-3.2.3-47.3.i386.rpm compat-gcc-32-c++-3.2.3-

Platform	Platform Version	Processor	Patch Level	Prerequisites and Notes
				47.3.i386.rpm glibc-devel-2.3.4-2.i386.rpm glibc-headers-2.3.4-2.i386.rpm glibc-kernheaders-2.4-9.1.87.i386.rpm
	EL 5.1	x64 (AMD64 / EM64T)	Kernel 2.6.18-53.el5	
SuSe Linux	ES 8	x86	Kernel 2.4.21-138	Same binaries as for Red Hat Linux.
	ES 9	x86	Kernel 2.6.5-7.97 Kernel 2.6.5-7.282	
	ES 8	OS/390 - 31 bit	Kernel 2.4.19-3-S390	No iRouter support - Event Routing from remote iRecorders is not possible.
	ES 9	OS/390 - 31 bit	Kernel 2.6.5-7.97-S390	
	ES 8	z/OS - 64 bit	Kernel 2.4.19-3-S390x	
	ES 9	z/OS - 64 bit	Kernel 2.6.5-7.97	No iRouter support - Event Routing from remote iRecorders is not possible.
	ES 10	z/OS - 64 bit	Kernel 2.6.16.46-0.12	No iRouter support - Event Routing from remote iRecorders is not possible.
	ES 10 SP1	x86	Kernel 2.6.16.46-0.12	
HP-UX	11.11	PA-RISC	PHSS_26263 PHCO_31903 PHCO_31923	No iRouter support on 11iv2 (11.23) on Intel Itanium IA-64 (64-bit native mode) - Event Routing from remote iRecorders is not possible iGateway and eTrust Audit Recorders for iPlanet and Netscape Web Servers are

Platform	Platform Version	Processor	Patch Level	Prerequisites and Notes
				not supported eTrust Audit Client distribution through Unicenter Software Delivery (USA 4.0 SP1) on HPUX 11iv2 (IA-64) is not supported
	11iv2 (11.23)	PA-RISC		(same)
	11iv3 (11.31)	PA-RISC		(same)
	11iv2 (11.23)	Intel Itanium IA-64, 64-bit native mode		(same)
	11iv3 (11.31)	Intel Itanium IA-64, 32-bit emulation mode		(same)
AIX	5.2	POWER		
	5.3	POWER with LPAR support	5300-05	The recommended Technology Level is 5 (5300-05).
	6.1	POWER with LPAR support		
VMware ESX Server	3.0.2 3.5.0	3.0, 3.0.1	Kernel 2.4.21-37.0.2EL	

eTrust Audit Administrator (Policy Manager)

The following are the supported operating systems for eTrust Audit Administrator (Policy Manager):

Important! eTrust Audit Administrator (Policy Manager) requires Microsoft Internet Explorer 6.0 with Service Pack 1 or Internet Explorer 7.

The Policy Manager for Windows computers also requires the Microsoft SQL Server JDBC driver v1.1 regardless of the version of Microsoft SQL Server you are using. This driver is installed automatically as part of the Policy Manager installation.

Note: If you are installing the Policy Manager on a Windows system, and plan to install on a partition other than the system partition, you must have at least 800 MB free space on the system partition, and at least 1 GB (1000 MB) free space on the target partition.

Platform	Platform Version	Patch Level	Prerequisites and Notes
Solaris	10 (SPARC) Includes running in a Solaris Logical Domain (LDOM) and Solaris whole root zone.		Requires Oracle 10g (10.2.0.2 or later). Supports Oracle 11g. Supports Microsoft Internet Explorer 6.0 SP1 or 7. Use the Sun JDK 1.6 during the Policy Manager installation.
Windows	2003 Server Standard Edition	Service Pack 1 Service Pack 2, R2	Requires the Windows Installer 3.1 v2 (msi.dll version 3.1.4000.2435). The installation package is located in the Winnt\Shared directory. Use the WindowsServer2003-KB898715-x86-enu.exe package for this Windows version. Supports Microsoft Internet Explorer 6.0 SP1 or 7. Microsoft SQL Server 2000 SP4, or SQL Server 2005 with TCP/IP protocol support enabled.
Windows	2003 Enterprise Edition (x86)	Service Pack 1 Service Pack 2, R2	Requires the Windows Installer 3.1 v2 (msi.dll version 3.1.4000.2435). The installation package is located in the Winnt\Shared directory. Use the WindowsServer2003-KB898715-x86-e

Platform	Platform Version	Patch Level	Prerequisites and Notes
			nu.exe package for this Windows version. Supports Microsoft Internet Explorer 6.0 SP1 or 7. Microsoft SQL Server 2000 SP4, or SQL Server 2005 with TCP/IP protocol support enabled.

eTrust Audit Data Tools

The following are the supported operating environments for the eTrust Audit Data Tools:

Note: If you are installing the Data Tools on a Windows system, and plan to install on a partition other than the system partition, you must have at least 700 MB free space on the system partition, and at least 1 GB (1000 MB) free space on the target partition.

Platform	Platform Version	Processor	Patch Level	Prerequisites and Notes
Windows	2003 Server Standard Edition	x86	Service Pack 1 Service Pack 2, R2	Security Monitor runs only on Windows platforms. Supports only Microsoft SQL Server 2000 SP4 or Microsoft SQL Server 2005 databases. MIcrosoft SQL Server agent must be running to use Health Monitor. Supports only Oracle 9i Release 2 and 10g databases.

Platform	Platform Version	Processor	Patch Level	Prerequisites and Notes
	2003 Enterprise Edition	x86	Service Pack 1 Service Pack 2, R2	Security Monitor runs only on Windows platforms. Supports only Microsoft SQL Server 2000 SP4 or Microsoft SQL Server 2005 databases. Microsoft SQL Server agent must be running to use Health Monitor. Supports only Oracle 9i Release 2 and 10g databases.
Solaris	8	SPARC	Patches 108434 and 109147, or cluster pack	Audit Reporter and Viewer use IBM WebSphere Application Server 6.0 or Tomcat 5.0.28. If you plan to use WebSphere, install it before running the Data Tools installation. Tomcat is installed automatically if selected during the Data Tools installation. Solaris 8 supports only Oracle 9i Release 2 databases.
	9	SPARC		Oracle 9i Release 2 or 10g databases. Java 1.6 runtime location must be in path.
	10 Including running in a Solaris Logical Domain (LDOM) and Solaris whole root	SPARC		Oracle 9i Release, 10g, or 11g databases Java 1.6 runtime location must be in path.

Platform	Platform Version	Processor	Patch Level	Prerequisites and Notes
	zone.			
HP-UX	11.11	PA-RISC	PHSS_26263 PHCO_31903 PHCO_31923	Oracle 9i Release 2 or 10g Health Monitor is supported only on PA-RISC systems. Do not install on the same system as the eTrust Audit Client. Oracle 11g is not supported on 32 bit emulation mode for IA-64.
	11iv2 (11.23)	PA-RISC		(same)
	11iv2 (11.31)	PA-RISC		(same)
	11iv2 (11.23)	Intel Itanium IA-64		(same)
	11iv2 (11.23)	Intel Itanium IA-64 (32-bit emulation mode)		(same)
	11iv3 (11.31)	Intel Itanium IA-64: 64-bit Native Mode		(same)
	11iv3 (11.31)	Intel Itanium IA-64: 32-bit Emulation Mode	Oracle 11g is not supported for 32-bit emulation mode.	(same)
AIX	5.2	POWER		AIX 5.2 supports only Oracle 9i. For Oracle 9i Release 2

Platform	Platform Version	Processor	Patch Level	Prerequisites and Notes
				or 10g, enable 64-bit operation in the AIX kernel using AIX *smit* system administration tool.
	5.3	POWER	5300-05	The recommended Technology Level is 5 (5300-05). AIX 5.2 supports only Oracle 9i.
	6.1	POWER		Supports Oracle 11g.

eTrust Audit Reporter and Viewer

The following are the supported operating systems for eTrust Audit Reporter and Viewer:

Note: The Reporter and Viewer for Windows systems requires the Microsoft SQL Server JDBC driver v1.1 regardless of the version of Microsoft SQL Server you are using. This driver is installed automatically as part of the Reporter and Viewer installation.

Note: If you are installing the Reporter and Viewer on a Windows system, and plan to install on a partition other than the system partition, you must have at least 700 MB free space on the system partition, and at least 1 GB (1000 MB) free space on the target partition.

Platform	Platform Version	Processor	Patch Level	Prerequisites and Notes
Windows	2003 Server Standard Edition	x86	Service Pack 1	Supports only Microsoft SQL Server 2000 SP4 or SQL Server 2005 databases. Supports only Oracle 9i Release 2 or 10g databases. Audit Reporter uses Tomcat 5.0.28 which is installed automatically.

Platform	Platform Version	Processor	Patch Level	Prerequisites and Notes
	2003 Enterprise Edition	x86	Service Pack 2, R2	Supports only Microsoft SQL Server 2000 SP4 or SQL Server 2005 databases. Supports only Oracle 9i Release 2 or 10g databases. Audit Reporter uses Tomcat 5.0.28 which is installed automatically.
Solaris	8	SPARC	Patches 108434 and 109147, or cluster pack	Reporter and Viewer require Java 1.4.2_13. The Java runtime location must also be in the path. Audit Reporter and Viewer use IBM WebSphere Application Server 6.0 or Tomcat 5.0.28. If you plan to use WebSphere, install it before running the Reporter and Viewer installation. Tomcat is installed automatically if selected during the Reporter and Viewer installation. On Solaris 8, Reporter and Viewer supports only an Oracle 9i Release 2 database.

Platform	Platform Version	Processor	Patch Level	Prerequisites and Notes
	9	SPARC		Reporter and Viewer require Java 1.4.2_13. The Java runtime location must also be in the path. Audit Viewer and Reporter use IBM WebSphere Application Server 6.0 or Tomcat 5.0.28. If you plan to use WebSphere, install it before running the Reporter and Viewer installation. Tomcat is installed automatically if selected during the Reporter and Viewer installation. Supports Oracle 9i Release 2 or 10g databases.
	10	SPARC		Reporter and Viewer require Java 1.4.2_13. The Java runtime location must also be in the path. Audit Viewer and Reporter use IBM WebSphere Application Server 6.0 or Tomcat 5.0.28. If you plan to use WebSphere, install it before running the Reporter and Viewer installation. Tomcat is installed automatically if selected during the Reporter and Viewer installation. Supports Oracle 9i Release 2, 10g, or 11g databases.

Chapter 3: System Requirements

This section contains the following topics:

System Requirements

The following are the minimum hardware requirements to run eTrust Audit:

Note: You can install the Data Tools components on a server with the DBMS and database on the same system (Data Tools with DBMS), or you can install the Data Tools on a dedicated database server and point to a remote database (Data Tools without DBMS).

Product	Operating Environment	CPU	CPU Speed	RAM (MB)	Disk Space (MB)	System Class
Client	Windows 2000 SP4 Windows XP SP2 Windows Server 2003 SP1	1 x Pentium	1 GHz	128	200 (see note at end of table)	
	AIX 5.2, 5.3	POWER	1 GHz	512	100	Workstation-class computer
	HP-UX 11.11, 11iv2 (11.23)	PA-RISC	1 GHz	512	100	Workstation-class computer
	HP –UX 11iv2 (11.23)	Intel Itanium IA-64	1 GHz	512	100	
	Red Hat Linux AS 3.0, AS 4.0	Pentium IV	1 GHz	512	100	Workstation-class computer
	SuSe Linux ES 8, ES 9	Pentium IV	1 GHz	512	100	Workstation-class computer
	Solaris 8, 9, 10	UltraSPARC	1 GHz	512	100	Workstation-class computer
	Tru64 5.1a, 5.1b	Alpha	1 GHz	512	100	Workstation-class computer

Product	Operating Environment	CPU	CPU Speed	RAM (MB)	Disk Space (MB)	System Class
	UnixWare 7.1, 7.1.3	Pentium IV	1 GHz	512	100	Workstation-class computer
Policy Manager or Reporter and Viewer	Windows 2000 SP4 Windows 2003 SP1	1 x Pentium	1 GHz	1000	1000 (see note at end of table)	Requires Microsoft Data Access Components (MDAC) 2.8.
	Solaris 10	UltraSPARC	1 GHz	1000	100	
Data Tools with Microsoft Data Access Components (MDAC) 2.8	Windows 2000 Server SP4 Windows 2003 SP1	1xPentium	1 GHz	1000	1000 (see note at end of table)	
Data Tools without DBMS	AIX 5.2, 5.3	POWER	1 GHz	1000	100	Workstation-class computer
	HP-UX 11.11, 11iv2 (11.23)	PA-RISC	1 GHz	1000	100	Workstation-class computer
	HP –UX 11iv2 (11.23)	Intel Itanium IA-64	1 GHz	1000	100	Workstation-class computer
	Solaris 8, 9, 10	UltraSPARC	1 GHz	1000	100	Workstation-class computer
Data Tools with DBMS	AIX 5.2, 5.3	2 x POWER	1 GHz	1000	1000	Server-class computer
	HP-UX 11.11, 11iv2 (11.23)	2 x PA-RISC	1 GHz	1000	1000	Server-class computer
	HP –UX 11iv2 (11.23)	Intel Itanium IA-64	1 GHz	1000	1000	Server-class computer
	Solaris 8, 9, 10	2 x UltraSPARC	1 GHz	1000	1000	Server-class computer

Note: For Windows systems, when you plan to install on a partition other than the system partition, you must have at least a certain amount of free space on the system partition, in addition to the listed free space on the target partition. The additional space requirements on the system partition or disk are as follows:

- Client - 200 MB
- Data Tools - 700 MB
- Reporter and Viewer - 700 MB
- Policy Manager - 800 MB

Chapter 4: Prerequisites

The following known issues function as prerequisites you should be aware of, or whose solutions you may need to implement, prior to using the related eTrust Audit components.

This section contains the following topics:

Health Monitor Requires SQL Server Agent

Symptom:

The Health Monitor is installed and running, but alerts do not display even though threshold settings have been exceeded.

Solution:

The Health Monitor makes use of stored database procedures. To use the stored procedures, the SQL Server agent must be running. Start the SQL Server agent on the Microsoft SQL Server database before attempting to use the Health Monitor.

Solaris Policy Manager Utilities Require DBA Privilege for Oracle Databases

Symptom:

When the Policy Manager is installed with database privileges other than those of a database administrator in Solaris with Oracle database the Policy Manager utilities acpmdb2xml and acxml2pmdb will not work.

Solution:

Use an account with database administrator privileges to access the acpmdb2xml and acxml2pmdb utilities, or install the Policy Manager with a database account that has database administrator privileges.

Distribution Server Service Does Not Start after System Start or Restart

Symptom:

The eTrust Audit Distribution Server does not start automatically when the system starts or restarts. If the Distribution Server service attempts to connect to the Policy Manager database prior to the start-up of the Microsoft SQL Server database service, the connection cannot be made, and the Distribution Server times out. On Windows systems, the event log shows messages similar to the following:

Event Management.Server.Diagnostic.F.W
eTrust Audit Distribution Server failed to connect to the distribution log : SqlState:(S1T00) NativeError:(0) Microsoft˙ ODBC SQL Server Driver˙Timeout expired; .

Event Management.Server.Diagnostic.F.W
Can't connect to Database eTAuditPMDB. Error: SqlState:(S1T00) NativeError:(0) Microsoft˙ODBC SQL Server Driver˙Timeout expired;

Solution:

Ensure that the eTrust Audit Distribution Server service starts after the Microsoft SQL Server database service. To do this, add a dependency on the Distribution Server service for the MSSQLSERVER service.

Policy Manager Database Connection Fails

Symptom:

When the Policy Manager database is located on a different workstation from the Policy Manager program and Distribution Server service, the connection sometimes fails.

Solution:

If the Policy Manager program and Distribution Server service cannot connect to the computer where the Policy Manager database resides, restoring the connection may not solve the problem.

After the connection is restored, restart the Distribution Server service and reopen the Policy Manager.

Supported Report Formats

Symptom:

Report jobs scheduled in eTrust Audit releases prior to r8 SP2 support the following report formats:

- Text
- Crystal Reports (RPT)
- Word for Windows Document
- HTML 4.0

Attempts to generate reports in the Text, Word for Windows, and HTML formats are not successful.

Solution

The r8 SP2 release of eTrust Audit supports only the following report formats:

- Crystal Reports (RPT)
- PDF
- Rich Text Format (RTF)
- Comma Separated Value

During r8 SP2 upgrade from previous releases, report jobs with unsupported report formats are set to use the Crystal Reports (RPT) format.

Error Message during AuditShared Installation on Solaris Systems

Symptom:

An error message, "sanity Test failed error code 3," displays during the AuditShared installation on Solaris systems.

Solution:

This problem occurs when there are traces of IPv6 enabled on the Solaris computer, and IPv6 has not been configured completely. To resolve this error, do one of the following and then re-install eTrust Audit:

- Edit the /etc/inet/ipnodes file to comment out the line containing "::1 locahost"
- Configure either IPv4 or IPv6 completely on this Solaris computer

Chapter 5: Installation Considerations

This section contains the following topics:

Data Tools and Client May Not Install iGateway Package from DVD Media

Symptom:

The installations for the Data Tools and eTrust Audit Client on AIX and HP-UX platforms may not install the iGateway package when you install using DVD media.

Solution:

Copy the Audit and Shared folders from the DVD media to the computer where you are performing the installation.

Examples:

[DVD]\Aix

[DVD]\Hpux

Manually Register the Audit Components with an Embedded IAM Server

Occasionally, it is necessary to register the Audit application with an embedded Identity and Access Management (eIAM) server manually. The process contains the following two basic steps:

- Register the Audit application and obtain the AuditAdminCert.p12 digital certificate file.
- Deploy the AuditAdminCert.p12 certificate.

You can perform these steps on both Windows and Solaris systems.

To register the Audit application on Windows

1. Change directory to %AUDIT_HOME%\IAMT.
2. Run the following registration command:

   Safex –f Audit_win32.xml –h <IAMThost> -u EiamAdmin –p <EiamAdminPassword>

   The registration process produces the digital certificate file, %AUDIT_HOME%\IAMT\AuditAdminCert.p12.

To deploy the digital certificate on Windows

1. Stop the iGateway service with the command:

   net stop igateway

2. Navigate to the iGateway folder.

   The default folder is <drive>:\Program Files\CA\SharedComponents\iTechnology.

3. Remove the old AuditAdminCert.p12 file from the iGateway folder with the command:

   del AuditAdminCert.p12

4. Navigate to the eIAM directory.

   The default eIAM directory is <drive>:\Program Files\CA\eTrust Audit\IAMT.

5. Copy the new AuditAdminCert.p12 into the iGateway location with the command:

   copy AuditAdminCert.p12 "<drive>:\Program Files\CA\SharedComponents\iTechnology\AuditAdminCert.p12"

6. Restart the iGateway service with the command:

   net start igateway

To register the Audit application on Solaris

1. Change directory to $AUDIT_HOME/IAMT.
2. Execute the commands:

   LD_LIBRARY_PATH=.;$LD_LIBRARY_PATH; export LD_LIBRARY_PATH
3. Run the following registration command:

   Safex –f Audit.xml –h <IAMThost> -u EiamAdmin –p <EiamAdminPassword>

   The registration process produces the digital certificate file, /tmp/AuditAdminCert.p12.

To deploy the digital certificate on Solaris

1. Stop the iGateway service with the command:

   /opt/CA/SharedComponents/iTechnology/S99igateway stop
2. Remove the old AuditAdminCert.p12 file from the iGateway folder with the command:

   rm /opt/CA/SharedComponents/iTechnology/AuditAdminCert.p12
3. Copy the new AuditAdminCert.p12 file into the iGateway location with the command:

   cp /tmp/AuditAdminCert.p12 /opt/CA/SharedComponents/iTechnology/AuditAdminCert.p12
4. Restart the iGateway service with the command:

   /opt/CA/SharedComponents/iTechnology/S99igateway start

Memory Leak May Occur When eIAM and Policy Manager Share a Server

Symptom:

A memory leak may occur when the Policy Manager and the embedded Identity and Access Management (eIAM) components are installed on the same server. Eventually, the iGateway service will slow down noticeably and may eventually hang.

Solution:

Stop and restart the iGateway service or daemon and monitor for memory usage.

To restart the iGateway daemon on Solaris systems

1. Stop the iGateway service (Windows) or iGateway daemon (Solaris) with the command:

   $IGW_LOC > S99igateway stop

2. Restart the iGateway service or daemon with the command:

   S99igateway start

To restart the iGateway service on Windows systems

1. Stop the iGateway service with the command:

   net stop igateway

2. Restart the iGateway service or daemon with the command:

   net start igateway

If Policy Manager and eIAM server are installed on the same physical server, manually monitor the memory available to ensure that iGateway is still running efficiently. When the remaining memory gets low, stop and restart the iGateway service. Your time between restarts will vary depending on the amount of real memory on your server, your level of Policy Manager usage, and the number of users logged in to Policy Manager.

Separating the eIAM and Policy Manager installations to discrete servers helps to alleviate this problem. CA eIAM is a commonly embedded component in many CA products. If you plan to install several CA products, you may want to dedicate a server for eIAM use. If you already have other CA products installed, you may already have a separate eIAM server.

Policy Manager Installation Requires Web Server Domain Name

The Policy Manager installation requires a fully-qualified domain name for the Web Server to be able to connect to Reporter and Viewer URL. The name you enter should follow the format, *server_name.domain_name*. For example, your fully-qualified Web Server domain name might be, WebServer1.MyCompany.com.

Cannot Connect to Remote Policy Manager Database with Custom Port during Installation

Symptom:

Unable to connect to a Policy Manager database during installation on Windows systems when the database is remote and configured to use a custom port.

Solution:

Configure the ODBC data source credentials so that remote connection is correct.

To configure the ODBC data source for a remote database with a custom port

1. Launch the Policy Manager installation.

   The installer creates a System DSN in ODBC connection with name "eTAuditPMDBTemp".

2. Access the Administrative Tools from the Windows Control Panel and double-click Data Sources (ODBC).
3. Select the System DSN tab, select the eTAuditPMDBTemp data source, and then click Configure.
4. Click Next to accept the data source name, description, and server name.
5. Click the Client Configuration... button in the Edit Network Library Configuration dialog.
6. Remove the selection check mark from the check box, Dynamically determine port.
7. Enter the custom port number of the database server in the Port Number field and click OK.
8. Click Cancel to close the MS SQL Server DSN Configuration window.
9. Restart the Policy Manager installation and enter the remote database system details when prompted.

Cannot Connect to Remote Collector Database with Custom Port during Installation

Symptom:

Unable to connect to a Collector (Data Tools) database during installation on Windows when the database is remote and configured to use a custom port.

Solution:

Configure the ODBC data source credentials so that remote connection is correct.

To configure the ODBC data source for a remote database with custom port.

1. Launch the Policy Manager installation.

   The installer creates a System DSN in ODBC connection with name "eTAuditDTNTTemp".

2. Access the Administrative Tools from the Windows Control Panel and double-click Data Sources (ODBC).
3. Select the System DSN tab, select the eTAuditDTNTTemp data source, and then click Configure.
4. Click Next to accept the data source name, description, and server name.
5. Click the Client Configuration... button in the Edit Network Library Configuration dialog.
6. Remove the selection check mark from the check box, Dynamically determine port.
7. Enter the custom port number of the database server in the Port Number field and click OK.
8. Click Cancel to close the MS SQL Server DSN Configuration window.
9. Restart the Policy Manager installation and enter the remote database system details when prompted.

Migrated User Policies Do Not Display in Legacy Policies Folder

Symptom:

After migration to the r8 SP2 Policy Manager, the folder containing legacy policies may not display some policies.

Solution:

Policies that contain actions are migrated into the r8 SP2 release. User policies that do not contain selected rules are not shown in the eTrust Audit Administrator after migration.

Unable to Start eTrust Directory Router Due to Port Conflicts with CA License Service

Symptom:

Not able to start the iTechPoz-<*hostname*> or iTechPoz-<*hostname*>-Router services because the port is being used by the CA Licensing (lic98fds) service.

Solution:

Upgrade the CA Licensing software to version 1.63.03 on the Solaris system running the eTrust Audit r8 SP2 Policy Manager. You can download the latest CA Licensing software from the CA SupportConnect web site.

Reporter and Viewer Job, Log, and Filter Migration

The upgrade to eTrust Audit r8 SP2 migrates the following kinds of information from older Reporter/Viewer releases into the r8 SP2 Reporter/Viewer:

- Report jobs
- Report job logs
- User-specific Viewer filters

The following information is not migrated:

- Generated reports

Migrated user-specific information is available only to users who have the same user name in the new eTrust Audit release. It is the administrator's responsibility to define these users after the upgrade process.

For example, suppose a user named William_North created some personal filters for the Viewer in Audit v1.5 SP3. After an upgrade to r8 SP2, these filters are only available to a user called William_North and defined in the new release. The eTrust Audit administrator would have to define this user after the upgrade is complete.

In addition to this, an administrator must assign all migrated report jobs to an owner. After upgrading, the migrated jobs and their corresponding logs are available only to the specified user or a superuser.

Important! Some migrated jobs make use of report templates that are no longer supported. You should remove MS Proxy report jobs prior to upgrading the Data Tools. If they are not removed, a warning message displays during installation.

Job Scheduling Changes

Job scheduling information may appear differently in eTrust Audit r8 SP2. The following is a description of each of the old scheduling types, and their corresponding settings:

Previous Schedule	r8 SP2 Schedule	Comments
Today	Next (today's date)	
Tomorrow	Next (tomorrow's date)	
Next day1, day2, ...	Next day1, day2, ...	
Every day1, day2, ...	Next day 1, day2, ...	

Jobs whose scheduling information doesn't migrate properly can generally be updated through the user interface.

Filters based on job time may appear differently in eTrust Auditr8 SP2. The following is a description of each of the previous time-based filtering options, and their corresponding settings:

Previous Filter	r8 SP2 Filter	Comments
Today Only	Today Only	
Yesterday Only	Yesterday Only	
Last 2 Days	Past 2 Days	
Last 3 Days	Past 3 Days	
Current Week	Not supported.	Converted to new filter, Week to date.
Last Week	from: 14 days ago to: most recent event	
Week to date	from: 7 days ago to: most recent event	
Current Month	Current Month	
Last Month	Past Month	
Earliest to date	Any time	
Custom Dates	Custom-defined filter	

Note: Since eTrust Audit r8 SP2 is sensitive to jobs from multiple time zones, all migrated jobs are scheduled according to time zone of the Reporter and Viewer server.

Changing the Reporter and Viewer's Web Servers (Solaris)

Valid for Solaris systems

During the Reporter and Viewer's first installation, you can choose a desired Web Server. The application is registered with the Web Server as part of the installation.

If you install the Reporter and Viewer *again*, you receive a warning that the Reporter and Viewer are already installed. If you confirm that you want to continue the installation, you can reconfigure the install parameters. This includes choosing another database server, a different eIAM Server, or a new Web Server. During the installation, the Reporter and Viewer are registered to the selected Web Server.

Important! The existing registration to the previous Web Server is not automatically removed. You must remove it manually.

Health Monitor Requires Initialization Parameter - Oracle

Symptom:

The Health Monitor jobs do not run after installing for use with an Oracle database.

Solution:

When the job_queue_processes initialization parameter is set to 0 for an Oracle database, the Health Monitor jobs will not run.

That value needs to be set to a value greater than 0 in order for the Health Monitor system to function correctly. We recommend setting that value to 10 or greater. Please notify your database administrator or consult the Oracle database documentation for instructions on how to make this change.

Silent Modify Option for Windows 2003 Is Not Supported

The Silent Modify option is not supported for systems running Windows 2003.

Cannot Install Client as "su root" on SuSe Linux

Symptom:

The eTrust Audit Client cannot be installed on SuSe Linux if a user uses the command 'su root' from a normal user's login session.

Solution:

To install Audit Client on SuSe Linux, login as a root user prior to running the installation.

Unable to See Events after Upgrade of Oracle SAPI Recorder

Symptom:

After installation of the Oracle SAPI Recorder, no events are sent to the Collector database or Security Monitor, even though connection to the database was successful, and shared libraries loaded successfully.

For direct installation of eTrust Audit r8 SP2, this problem occurs on the following platforms:

- RHEL4 with Oracle 10g
- SuSe 9 with Oracle 10g
- HP-UX 11.23 (PA-RISC) with Oracle 9i

For upgrades from eTrust Audit r8 SP1 CR2 to r8 SP2, the problem occurs on all platforms.

Solution:

During upgrade from r8 SP1 CR2 to r8 SP2, use the same level of encryption during the upgrade processing. As an alternative, you can follow the instructions for generating a new encryption value below.

For direct installation of r8 SP2, (or to update the encryption after upgrade from r8 SP1 CR2), edit the recorder.ini file to replace the existing encrypted user ID and password with new encryption values. You do not need to change the underlying database access credentials.

You can use the encup utility to create these new values. More information on using the encup utility is available in the *eTrust Audit Reference Guide*.

Unable to Upgrade Certain SAPI Recorders

Symptom:

Attempts to upgrade the FW-1 and Netscape SAPI Recorders are not successful. During the installation, a warning message appears as follows:

If any of the eTrust Audit SAPI recorders is detected on the machine, these recorders and their configuration will be preserved. You must upgrade to version r8 SP2 of these SAPI recorders to ensure proper functionality.
NOTE. Upgrade is not available for CheckPoint FW-1 and Netscape SAPI recorders. You should use Check Point iRecorder and SunONE iPlanet iRecorder instead.
Do you want to continue?

Solution:

The FW-1 and Netscape SAPI Recorders are discontinued in eTrust Audit r8 SP2 and can no longer be upgraded. They are replaced with the CheckPoint and SunONE iPlanet SAPI Recorders, respectively.

Removing Obsolete SAPI Recorders on UNIX Systems

Some SAPI recorders are no longer supported in eTrust Audit r8 SP2, and are thus obsolete. The list of obsolete SAPI Recorders includes the following:

- Check Point FW-1 4.1
- Cisco PIX
- Netscape
- iPlanet
- Solaris BSM
- Microsoft ISA
- Microsoft IIS

You should remove these recorders by following these steps.

To un-install obsolete SAPI Recorders

1. Navigate to the Shared folder on the CD image.
2. Run the provided script, uninstall_obsolete_recorders.

Chapter 6: General Considerations

For installation planning and information about the distributed components of eTrust Audit, see the *eTrust Audit Implementation Guide*.

You can access the documentation for the latest release on the CA Support web site. For assistance, contact Technical Support at http://ca.com/support.

This section contains the following topics:

Minimum Database Permissions to Run eTrust Audit

The r8 SP2 CR1 Implementation Guide lists required database permissions for working with the Collector and Policy Manager databases. While those permissions represent the recommended levels, a lower level of access is possible.

For Oracle databases, you only need to be the owner of the relevant tablespace and have the following permissions:

- roles
  - CONNECT
  - RESOURCE
- privileges
  - CREATE ANY DIRECTORY
  - EXECUTE ANY PROCEDURE
  - SELECT ANY DICTIONARY
  - UNLIMITED TABLESPACE

For Microsoft SQL Server databases, you can be the owner of the database and have the following permissions on the database:

- db_public
- db_owner

The Data Tools on Windows systems using Microsoft SQL Server 2005 require the following permissions:

- db_public
- db_owner
- sysadmin (Server Role)

  Note: The sysadmin Server role is required for Health Monitor installation.

Configuration File and Registry File Backups

eTrust Audit uses a variety of configuration files to store information for startup and operations of your Security Information Management (SIM) system.

For some platforms, you must edit registry entries to make configuration changes. Configuration entries are also saved in digitally signed files that can be modified through policies you create using the Policy Manager.

Best practice for handling configuration files is to make a backup copy of the current registry files before you make your changes. It is also highly recommended that you make backup copies of all configuration files on a regular basis.

Using Static Ports with eTrust Audit

Normally, eTrust Audit is configured to use dynamic ports, which are found using the RPC portmapper service. When you configure eTrust Audit to use static ports, as for operations with a firewall, the same static ports need to be configured on *all* Audit components. This includes the Router, Security Monitor, and Collector. Failure to configure the static ports correctly results in disruptions of proper operation.

For example, if you configure a Router to use MonitorSapiPort 1 and the Security Monitor to use MonitorSapiPort 2, no events from that Router can display on the Security Monitor. The same type of configuration problem can occur with traffic between Routers. For example, if two Routers are configured with different RouterSapiPorts, they cannot communicate with each other and cannot execute any remote actions.

Connection to eIAM Fails When Using Non-English Collector or Policy Manager Database Name

Valid on Windows

Symptom:

A "Server not present in trusted servers list" error appears when trying to log on to the Audit Administrator or Reporter or Viewer web interfaces, and the Collector database or Policy Manager database were set up with a non-English database name during Reporter and Viewer installation.

Solution:

Ensure that an English database name is used for the Policy Manager and Data Tools Collector database during installation.

Allowing Non-Administrator Access

To allow members of groups other than "Administrators" to manage the eTrust Audit Administrator and the eTrust Audit Post-Collection Utility, place the name of your group in the <AdminGroupName> tag of the iControl.conf file.

How to Create and Use Custom Report Templates

You can create custom report templates using the Crystal Reports package. After you create your custom template, you can import that template, and use it with the eTrust Audit Reporter.

Creating custom reports involves the following basic steps:

- Creating a valid report template
- Copying your custom templates to a new folder accessible to eTrust Audit
- Generating or scheduling a report from the Reporter user interface, as usual

iGateway Service on eIAM Server Uses Too Much Memory

Symptom:

The iGateway service can use over 100 MB of memory on a Windows eIAM server, and over 200 MB of memory on a Solaris eIAM server in some cases.

Solution:

Reduce the size of the runtime buffer that the iGateway service uses to cache events.

To reduce event storage

1. Stop the iGateway service.
2. Edit the iControl.conf file.
3. Change the <EventsToCache> value from 5000 to 10.
4. Change the <StoreEventHost max= xxxxx> value from 10000 to 100.
5. Save and exit the file.
6. Start the iGateway service.

Chapter 7: New Features

This section contains the following topics:

Web-based User Interface

The eTrust Audit user interface has been updated and reorganized to reflect new functionality and improve work flow. Entirely new web-based features include:

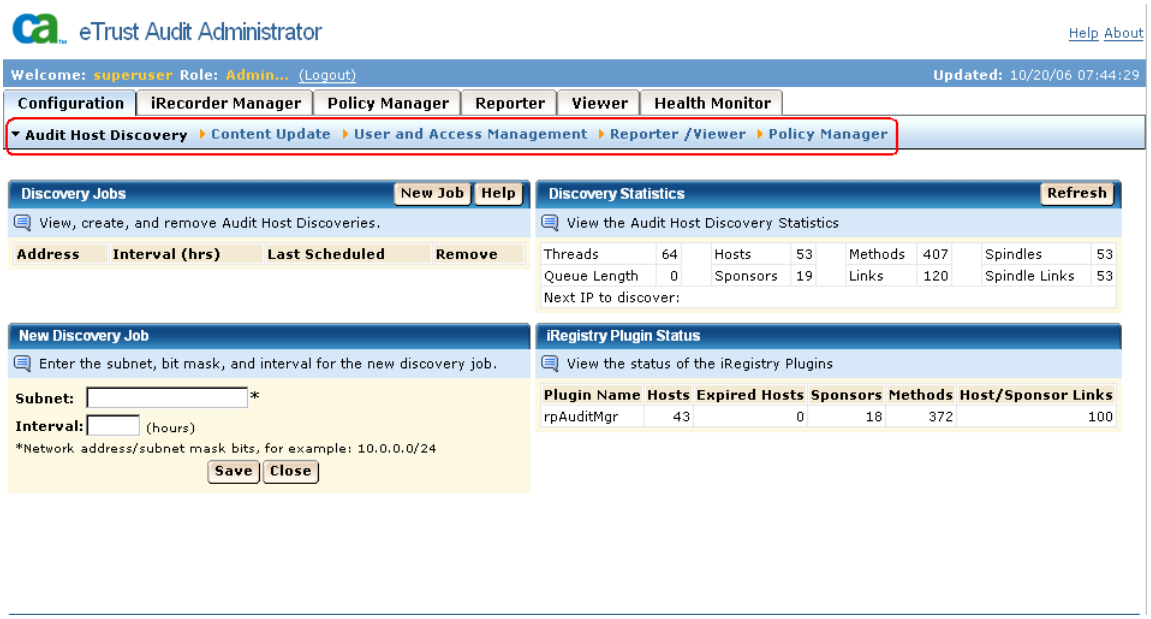
- Audit Policy Manager
- Audit Reporter
- Audit Viewer

These features replace the Win32 interfaces for all eTrust Audit components except Security Monitor, which remains a Win32 interface. The following topics illustrate some of the new interface features.

Note: The new web-based interface introduces significant changes to the Policy Manager and other administrative tasks. Before you upgrade or use the new interface, it is important to review the *eTrust Audit and eTrust Security Command Center Administration Guide*. Additional information is also available in the online help for the Audit Administrator interface and the *eTrust Audit and eTrust Security Command Center Implementation Guide*.

Updated Configuration Interface

The updated Audit Administrator configuration interface lets you complete various types of management and configuration tasks using the UI subtabs as shown in the following illustration.



Audit Host Discovery

Lets you set up and view discovery job status for eTrust Audit Hosts.

Content Update

Lets you update Audit Administrator content by downloading template information and Message Parsing (MP) files from a CA website.

User and Access Management

Lets you configure user role assignments and access to the interface for your Audit Administrator environment.

Reporter/Viewer

Lets you configure eTrust Audit Data Sources for use by the Reporter and Viewer utilities.

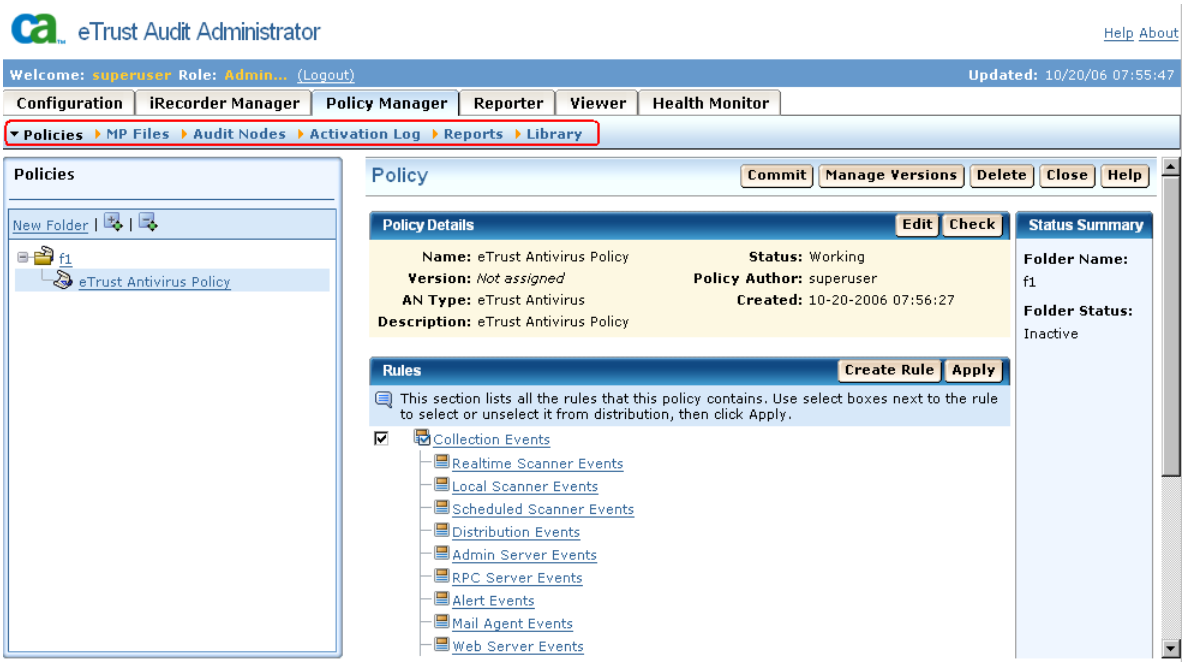
Policy Manager

Lets you perform Policy Manager administration tasks, configuring the Distribution Server and managing locked Policy Manager objects.

See the "Managing Audit Administrator" chapter of the *eTrust Audit and eTrust Security Command Center Administration Guide* for more information on the new Configuration interface. Task-based information for each of the UI subtabs illustrated here is contained in its own sub-chapter.

New Policy Manager Interface

The new Policy Manager interface lets you perform tasks related to creation and distribution of policies and MP files using the UI subtabs as shown in the following illustration.



All the main Maker and Checker tasks are completed in the Policy Manager interface.

Policies

Lets you create policy folders and policies, and review and distribute them.

MP Files

Lets you create MP folders and files, and review and distribute them.

Audit Nodes

Lets you create and search for eTrust Audit host nodes in your environment and attach them to policy or MP folders.

Activation Log

Lets you view policy and MP file activation history for your eTrust Audit environment.

Reports

Lets you access the Reporter utility from the Policy Manager window.

Library

Lets you view and create audit node types, and view rule templates.

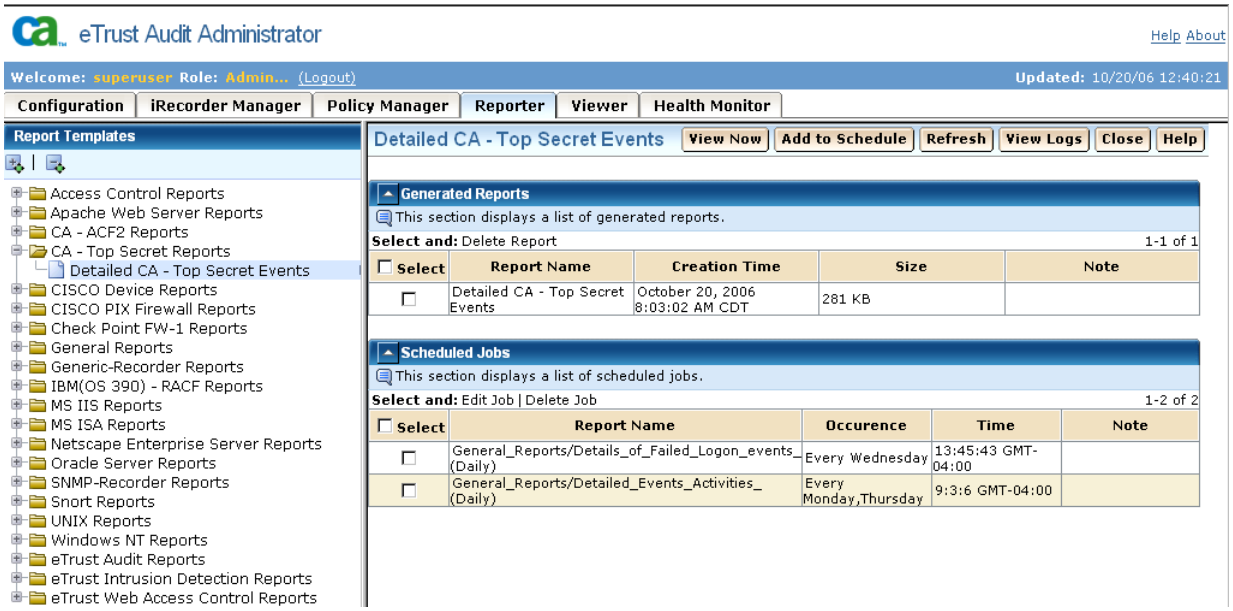
See the "Policy Manager Tasks" chapter of the *eTrust Audit and eTrust Security Command Center Administration Guide*, for more information on the new Policy Manager interface. Task-based information for each of the user interface subtabs illustrated here is contained in its own sub-chapter, along with related user role information.

More information

Policy Manager Change Control Support (see page 57)

New Reporter Interface

The new Reporter utility interface lets you view selected data from eTrust Audit event databases in the form of graphic or detailed reports. It displays available report template types in a folder tree, which you can expand to view specific report templates, as shown in the following illustration.



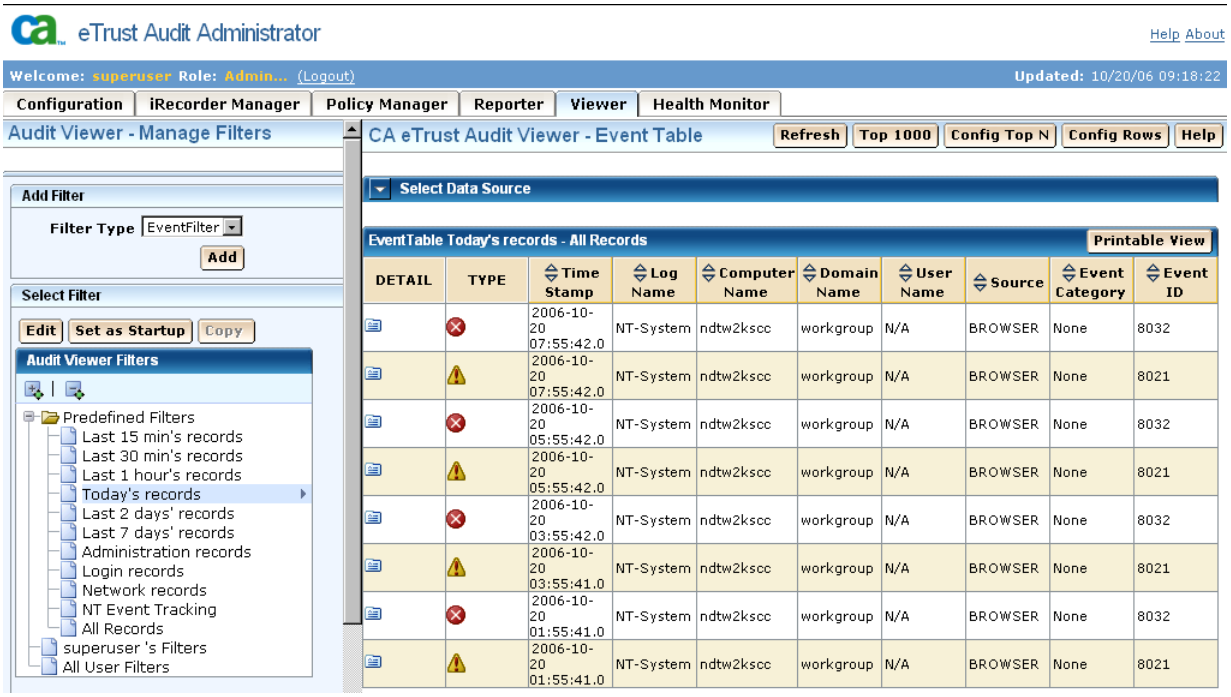
When you select a report template, it appears in the right pane, displaying any previously generated reports of that type. You can create an immediate report, schedule a new report, or view report job logs.

The Scheduled Jobs area displays all scheduled reports for your environment, regardless of their type.

See the "Using Reporter" chapter of the *eTrust Audit and eTrust Security Command Center Administration Guide* for more information on the new Reporter interface, including instructions for viewing, scheduling, and generating reports.

New Viewer Interface

The new Viewer utility interface lets you view, sort, and filter the eTrust Audit event database. It displays available filters in a folder tree, which you can expand to view specific filter details, as shown in the following illustration.



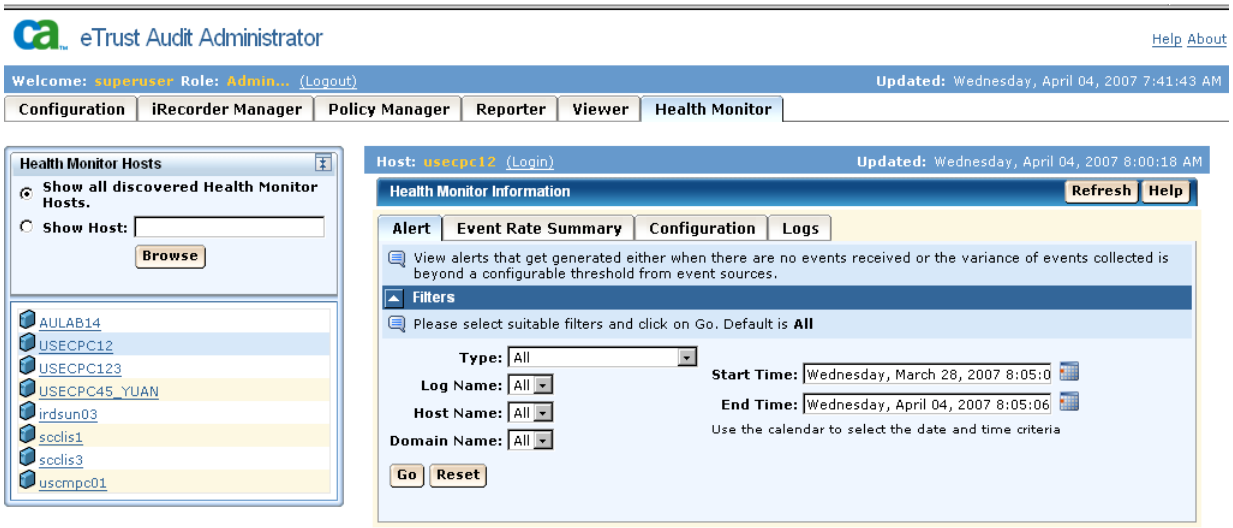
You can add new filters of your design or edit existing filters.

Events matching the qualifications of the filter you select appear in the Event Table pane. You can configure how many rows or events you want the table to display, and sort the events by any attribute other than Detail or Type. You can click the detail icon for any event to open an expanded view in a new window.

See the "Using Viewer" chapter of the *eTrust Audit and eTrust Security Command Center Administration Guide* for more information on the new Viewer interface, including instructions for viewing and filtering events.

New Health Monitor Interface

The new Health Monitor Utility lets you search and display Health Monitor hosts in your environment, as shown in the following illustration.



You can select any of the available hosts displayed in the left pane to view Alert, Event Rate Summary, or Log information from the appropriate tab. You can also control the settings of the selected Health Monitor using the Configuration tab.

See the "Using Health Monitor" chapter of the *eTrust Audit and eTrust Security Command Center Administration Guide* for more information on the new Health Monitor interface, including instructions for viewing and filtering alerts, log records, and setting configuration parameters.

Policy Manager Change Control Support

eTrust Audit Policy Manager supports change control features through the Maker and Checker roles, which are pre-defined in the Embedded Identity and Access Manager (EIAM) Tool Kit.

These roles divide responsibility for the creation of polices, rules and Message Parsing files from responsibility for their review and distribution to the clients. Users with the Maker role are able to create new policies and users with the Checker role to reject or approve them. This distribution of duties is called segregation of duty.

The Maker and Checker roles can be assumed by different users, or the same user, depending on your chosen configuration. In addition, there are two levels of segregation of duty. Segregation fo duty is turned off by default. The default level for segregation of duty on is strict, where no Maker can also be a Checker for a given policy, MP file, or folder. You can also enable a transactional level of duty segregation, where a given Maker cannot check a policy, MP file, or folder if he was the last person to make a change.

See the Managing Users and Access section of the "Managing Audit Administrator" chapter in the*eTrust Audit and eTrust Security Command Center Administration Guide* for more information on change control support through user roles. Additional information is available in the "Policy Manager Tasks" chapter of the *eTrust Audit and eTrust Security Command Center Administration Guide*.

Note: Policy Manager's internal user management is not available in this release. It is replaced by the EIAM Tool Kit.

Centralized Management of Message Parsing (MP) Files

Message Parsing (MP) files are used by several generic Audit Recorders or iRecorders to read text-format log event data. MP Files are managed in the same way as policies; both have the same level of acknowledgement, logging, version control and reporting support.

MP files are attached to Audit Node (AN) groups for distribution by Policy Manager, using the same improved distribution system as policies.

See the MP Files section of the "Policy Manager Tasks" chapter in the *eTrust Audit and eTrust Security Command Center Administration Guide* for more information on MP files.

Note: MP files are created or modified manually and then imported into Policy Manager for version control and distribution.

More information

Improved Policy Distribution (see page 58)

Improved Policy Distribution

SP2 release includes broad improvements to policy distribution protocols. The following list summarizes these enhancements:

1. Policies and MP files are both distributed by the policy distribution protocol.
2. The maximum number of distribution threads can be configured in the user interface. The default number of threads is 10, and can be increased to a maximum setting of 64.
3. When policy files whose names include spaces are distributed to clients running on UNIX, the spaces are converted to underscores, automatically complying with UNIX naming standards.
4. eTrust Audit clients store policy version information in the Policy Manager database.
5. The Disable Node Retry feature allows a Maker to select a node or multiple nodes and exempt these nodes from all automatic policy/MP redistribution.
6. Automatic activation and enforcement is supported for policy/MP files delivered by the Policy Manager without any service restart requirements.

See the Distribution Server section of the "Managing Audit Administrator" chapter in the *eTrust Audit and eTrust Security Command Center Administration Guide* for more information on policy distribution. More information on the Policy Manager database can be found in the Installing Databases chapter of the *eTrust Audit and eTrust Security Command Center Implementation Guide*.

More information

Centralized Management of Message Parsing (MP) Files (see page 57)

Audit Client Status Polling

This feature adds policy and MP file version control, enabling automatic validation of deployed policies or MP files. This allows you to recover from any changes to those policies or MP files.

Policy Manager periodically tests for any difference in status or version between active policies or MP files on the distribution server and those distributed to clients. If a difference is detected, Policy Manager generates an event, and gives you the option to redistribute the correct policy or MP file version.

See the Distribution Server section of the "Managing Audit Administrator" chapter in the *eTrust Audit and eTrust Security Command Center Administration Guide* for more information on client polling. Additional information on policy and MP file version control is available in the Polices and MP Files sections of the "Policy Manager Tasks" chapter.

Additional Client Platform Support

The eTrust Audit client is now supported on additional platforms, including Solaris. For a full list of supported platforms, see the eTrust Audit *Readme.*

Enhanced Policy Manager Support

eTrust Audit Policy Manager now supports MS SQL Server 2000 and 2005 on Windows and Oracle 10g on Solaris 10. For a full list of supported databases, see the eTrust Audit *Readme.*

Migration scripts are provided to upgrade MS Access Policy Manager databases to Oracle 10g or MS SQL Server Policy Manager databases. See the Introduction to the "Installing Databases" chapter of the *eTrust Audit and eTrust Security Command Center Implementation Guide* for more information on databases.

Native Packaging for Solaris, and Red Hat and SUSE Linux

All install packages on Solaris and Linux are now in native packaging format:

- pkg on Solaris
- RPM on Linux

See the *eTrust Audit and eTrust Security Command Center Implementation Guide* for additional installation information. You can consult the chapters on installing various components including Databases, Data Tools, and the Policy Manager.

New Policy Conversion, Import, and Export Utilities

During administration of your r8 SP2 Policy Manager database, you may from time-to-time need to import or export policies. You may also need to convert Windows system PTF files to XML for use with older iRecorders and SAPI Recorders.

For example, if you download an iRecorder and you want to import its default policies to the r8 SP2 Policy Manager database, it may not have an XML policy file supplied with it. In that case, you would need to convert the supplied .ptf file to XML using this utility, and then import the new XML file to the Policy Manager database.

You can use the following utilities to convert policy files to XML, and to import and export policy files:

acptf2xml

Converts Windows PTF policy files to XML format.

acxml2pmdb

Imports XML policy files to the r8 SP2 Policy Manager database.

acpmdb2xml

Exports policy files from the r8 SP2 Policy Manager database to XML files.

See the "Importing, Exporting, and Converting Policies" chapter in the *eTrust Audit and eTrust Security Command Center Reference Guide* for more information.

Chapter 8: Changes to Existing Features

This section contains the following topics:

A main feature of this eTrust Audit release is a new web-based interface (see page 49), so there are significant changes to the Policy Manager and other administrative tasks. Before you upgrade or use the new interface, it is important to review the *eTrust Audit and eTrust Security Command Center Administration Guide*. Additional information is also available in the online help for the Audit Administrator interface and the *eTrust Audit and eTrust Security Command Center Implementation Guide*.

Advanced Encryption Standard (AES) Support

The eTrust Audit Policy Manager distribution server is in frequent contact with eTrust Audit client computers in order to distribute new or changed policies or MP files, receive alerts, or generate reports. You can also configure the distribution server to poll the client computers and automatically redistribute policy or MP files to any node where the software detects version or status changes.

eTrust Audit supports AES 256 for Policy Manager server/client communication, replacing AES 128 as the default encryption method and providing more secure communication for your environment.

See the Distribution Server section of the "Managing Audit Administrator" chapter in the *eTrust Audit and eTrust Security Command Center Administration Guide* for more information on file distribution and client/server contact.

UNIX SAPI Recorders Available Separately

UNIX Supplementary SAPI Recorders, including Oracle, Sybase, DB2, and Apache recorders, are not included in the basic eTrust Audit package for UNIX. These recorders are now available separately as standalone installation packages.

See http://ca.com/support for a full list of available UNIX SAPI recorders.

Visualizer Supported Only on Windows

The Audit Administrator Visualizer utility allows you to run standard queries on data processed by the Post-Collection Utility or drawn from eTrust Security Command Center table collectors. The Visualizer is available only to Windows users.

See the "Using Visualizer" chapter of the *eTrust Audit and eTrust Security Command Center Administration Guide* for more information on the Visualizer interface, including instructions for generating and displaying Visualizer queries.

Client Support Changes

For the eTrust Audit client r8 SP2 release, certain platforms are no longer supported. For a full list of supported platforms, see the eTrust Audit *Readme.*

Microsoft Access Not Supported

With the eTrust Audit enhancement to database support, MS Access is no longer supported for the Collector and Policy Manager databases. Migration scripts are provided to upgrade MS Access Policy Manager databases to Oracle 10g or MS SQL Server Policy Manager databases.

More information

Enhanced Policy Manager Support (see page 59)

Post-Collection Utility Supported Only on Windows

The Post-Collection Utility (PCU) provides a set of tools for defining policies, managing the collector database, and detecting event tampering. The Post-Collection Utility is available only to Windows users.

See the "Post-Collection Utility (PCU) Tasks" chapter of the *eTrust Audit and eTrust Security Command Center Administration Guide* for more information on the Visualizer interface, including instructions for generating and displaying Visualizer queries.

Chapter 9: Known Issues

This section contains the following topics:

eTrust Audit Client

The topics that follow describe the known issues, workarounds, and solutions for eTrust Audit Client.

Received "Failed to Find Local Router" Error Using Generic Recorder

Symptom:

When installing the eTrust Audit Client, if the router is set to localhost, the Generic Recorder fails with the following error:

Failed to find local router

Solution:

Do one of the following:

- Instead of using localhost, use a specific host name or IP address.
- Edit the hosts file and add the line 127.0.0.1 localhost.

  The hosts file is in the /etc directory for UNIX systems.

  The hosts file is in the \system32\drivers\etc directory for Windows systems.

Router Fails to Start on VMware ESX Server

Valid on VMware ESX Server 3.0 and 3.5

Symptom:

Router service does not start after installation. The installer displays the following errors while starting the service:

```
starting iGateway
WARNING: Could not remove rpc info from system file.
.
.
.
Starting eTrust Audit Router
eTrust Audit Log Router (aclogrd) - ok
Message from syslogd@mansr02-sl-v9-udp0565657uds at Tue Oct 31 22:25:24 2006
<servername> eTAudit Router:"Event Management.Agent.Start.F.W¨
eTrust Audit Log Router failed to start, error=0X40023004
```

The same error occurs when starting the Router from "bin" folder.

Solution:

VMWareESX3.0 does not support the Portmapper service. By default the Router will not start until eTrust Audit is configured to run with fixed ports, and *without* the portmapper (RegisterPort=0). Port values can be set in the eaudit.ini file. More information on configuring this file is available in the *eTrust Audit Reference Guide*.

Received "Could Not Stop iTechnology iGateway 4.5 Service" Error

Valid on Windows

Symptom:

When stopping the iTechnology iGateway 4.5 service on Windows, the following error message sometimes appears:

```
Could not stop the iTechnology iGateway 4.5 Service on Local computer. Error 1067: The process terminated unexpectedly.
```

Despite the error message, the iGateway service stops.

Solution:

Restart the iGateway service.

Note: There is no impact on iRecorders and or other eTrust Audit components that use the iGateway service when the iGateway service restarts.

Received "No Version Information" Message from iGateway

Valid on Linux

Symptom:

When the eTrust Audit Client or iRecorder such as the Syslog iRecorder is installed on Linux, the following message appears:

./igateway: ./libetpki2.so: no version information (required by./igateway)

Solution:

This message causes no problems in the operations of iGateway, iRecorder, or iRouter.

Unable to Stop Recorder Installation

Symptom:

During installation of a Recorder, answering "q" to quit after responding to the license agreement, does not appear to stop the installation. Some files are still created even though the install was stopped.

Solution:

Remove the files by running the supplied recorder uninstall script.

eTrust Audit SNMP Recorder Cannot Fetch Events

Symptom:

When using the eTrust Audit SNMP Recorder, the Recorder has problems fetching SNMP events.

Solution:

The SNMP Recorder is an SNMP agent that uses common ports to capture SNMP events. You must disable any other SNMP agent running on the same host as the eTrust Audit SNMP Recorder to ensure proper operation of the Recorder.

Using eTrust Access Control as Logname for Viewer Does Not Display Events

Symptom:

When using the eTrust Audit Viewer with eTrust Access Control specified as the Logname in the filter for Access Control events, the Viewer does not display Access Control events.

Solution:

The Logname field for the eTrust Access Control events is stored as eTrust AC in the collector database. Use eTrust AC as the Logname in the filter in the eTrust Audit Viewer.

eTrust Access Control events sent to the eTrust Audit Router use eTrust Access Control as the Logname. Policy rules to process eTrust Access Control events that are sent to the eTrust Audit Router must use eTrust Access Control as the Logname.

Custom Silent Install Fails When the iRecorder Option Is Not Selected

Symptom:

When the iRecorder option is not selected on the Optional Components dialog when recording the custom silent response file for eTrust Audit Client, the installation fails when the silent installation runs.

Solution:

When creating a custom silent response file for the eTrust Audit Client, select the iRecorder option. This lets you successfully install the Client silently.

Cannot Modify eTrust Audit Client During Silent Installation

Valid on Windows

Symptom:

When using the modify option in the eTrust Audit Client silent installation, the installation fails.

Solution:

The eTrust Audit Client r8 SP2 installation process does not support the modify option in silent mode, and the installation will fail if you attempt to use this option.

acrecorderd Service Does Not Start after Client Install

Valid on SuSE 10 ES SP1

Symptom:

The acrecorderd service will not start after the installation of the eTrust Audit Client on SuSE 10 ES SP1 systems. SuSE 10 ES SP1 supplies syslog-ng daemon as a default.

Solution:

The eTrust Audit Client does not support syslog-ng. To resolve this situation, install the syslog service on the system. The r8 SP2 CR1 eTrust Audit Client is certified with syslog.

eTrust Audit Administrator

The topics that follow describe the known issues, workarounds, and solutions for eTrust Audit Administrator.

Audit Administrator Interface May Become Inoperative While Viewing Reports or Graphs

Symptom:

When using the eTrust Audit Administrator to configure a report, you select a query from the list of Queries. This configures a report or a visual analyzer. The Audit Administrator may become inoperative if you click the View Report or View Graph buttons multiple times.

Solution:

In order to view graphs, you must install the Visualizer on the same computer as the Audit Administrator.

Note: The Visualizer is included in the Policy Manager Windows install package and is installed by default.

The View Report and View Graph buttons initiate a long-running database query. If you click these buttons multiple times, ODBC may experience a fatal error and render the Audit Administrator interface inoperative.

To avoid this situation, click View Report or View Graph button only once, and wait until the results are returned to the Audit Administrator interface.

Computer Becomes Unresponsive When Running Visualizer Queries

Symptom:

When a query is run to extract a large volume of data in an eTrust Audit database of about a million rows, the computer stops responding.

Solution:

When executing a query the computer allocates all resources to processing data and may stop responding. To free up system resources, stop the query manually from the database management interface, or restart the iGateway service.

To prevent slowdowns, limit the queries to a small set of rows.

Example:

Specify a limited date range in the query to return a smaller set of data.

pkgadd Cannot Access Oracle Home

Valid on Solaris

Symptom:

When installing the Policy Manager, the pkgadd utility cannot access Oracle Home as if Oracle is not installed.

Solution

The Solaris 10 pkgadd utility runs internally as a non-root user with limited permissions. To change this default behavior, set the environment variable NONABI_SCRIPTS to TRUE before using the pkgadd command as follows:

Bourne shell, Korn shell or GNU bash

```
NONABI_SCRIPTS=TRUE; export NONABI_SCRIPTS
pkgadd -G -d <Audit package name>
```

csh

```
setenv NONABI_SCRIPTS TRUE
pkgadd -G -d <Audit package name>
```

Error Setting Up Connection to eTrust Audit Database

Valid on Solaris

Symptom:

During the installation of the Policy Manager, Data Tools, or Reporter-Viewer, the following error appears when attempting to establish the connection to the Policy Manager or Collector database when using Oracle:

Bad Oracle service name

Solution:

Ensure that the Oracle System Identifier (SID) consists of four to eight characters. eTrust Audit requires a SID of at least four characters. A SID with fewer than four characters may cause remote connection errors on some platforms.

For more information about the Oracle SID, see the *Oracle Database Installation Guide 10g Release 1 (10.1) for UNIX Systems* and *Oracle Installation Guide 10g Release 2 for UNIX Systems*.

Configuring Data Sources Runs Slowly

Symptom:

It may more than one minute to display and configure the eTrust Audit Data Sources, using the Configuration tab's Reporter / Viewer sub-tab. Access is faster after the first display, unless the browser is closed. In some cases, a blank page is displayed instead of the Audit Data Sources window.

Solution:

If a blank screen displays, click the Reporter / Viewer sub-tab again to display the Data Sources window.

Web Browser Times Out When Accessing Oracle

Symptom:

When using Oracle 10.2.0.1, the web browser displaying the eTrust Audit Administrator times out during routine operations.

Solution:

There is a known issue in Oracle 10.2.0.1 that causes frequent iGateway crashes. This causes the web browser to time out.

Download and install Oracle 10.2.0.2 to avoid this issue.

eTrust Audit Data Tools

The topics that follow describe the known issues, workarounds, and solutions for eTrust Audit Data Tools.

Scheduled Reports Do Not Show Scheduled Jobs

Symptom:

When using a version of Microsoft Internet Explorer lower than 5.0023, the list of scheduled jobs is not shown in the Scheduled Reports.

Solution:

Upgrade to Microsoft Internet Explorer 6.0 to meet minimum requirements.

Post-Collection Utility Cannot Be Installed

Symptom:

Errors appear when trying to install the Post-Collection Utility (PCU) using the eTrust Audit Post-Collection Utility package.

Solution:

Do not use the eTrust Audit Post-Collection Utility package to install the PCU. By design, the PCU is automatically installed as part of the Data Tools installation. This ensures proper configuration and functionality.

Collector Service Fails to Start

Valid on Windows

Symptom:

When running the eTrust Audit Collector service on Windows for the first time after installation, an error message appears indicating that the Data Source failed to open, and the Collector service fails to start.

Solution:

Do the following:

1. Review the following registry keys for the value, eAudit_DSN:

   HKEY_USERS\DEFAULT\Software\ODBC\ODBC.INI
   HKEY_CURRENT_USER\Software\ODBC\ODBC.INI

2. Delete the value, if it appears.

Cannot Insert Events in the Collector Database

Valid on AIX

Symptom:

Events cannot be inserted in bulk to an Oracle 9i Release 2 Collector database when running on an AIX system.

Solution:

A limit of 500 rows for a single bulk insert operation exists for Oracle 9i Release 2 databases running on AIX. The Collector database configuration parameter, MaxBulkInsertRows, is limited to a maximum of 500 rows for this database and operating system combination.

Health Monitor Audit Node and Policy Are Obsolete

The Health Monitor audit node (AN) and the HealthMonitor policies are obsolete and can be safely ignored. You can collect Health Monitor events with a policy that filters on Logname = 'eTrust Audit' and Src = 'Health Monitor'.

Health Monitor Event Source May Not Display in Security Monitor or Collector Database

Symptom:

Health Monitor generates events with Logname = "eTrust Audit" and Source = "Health Monitor" that may not appear in the Security Monitor or Collector database when an eTrust Audit Policy is deployed. But they do appear in the syslog (log file configured in syslog.conf) on AIX systems.

Solution:

1. Manually modify the recorder.ini file to update the location of the messages file to the directory, var/adm/messages, or any log filename configured in syslog.conf.

   The section to be modified is shown in boldface type in the following example:

   ```
   Syslog
   {
     LogName = Unix
     DWORD:StartOver = 0
     DWORD:ReloadLogs = 0
     DWORD:SendUnmatched = 0
     DWORD:SkipCurrentLogs = 1
     MPFile = cfg/syslog.mp
     ConfigFile = /etc/syslog.conf
     DWORD:Source = 1
     LogFiles
     {
        Log1 = /var/adm/messages
     }
   ```

2. Restart the acrecorderd service using the following command:

   ```
   /opt/CA/eTrustAudit/bin/acrecorderd -start
   ```

eTrust Audit Policy Manager

The topics that follow describe the known issues, workarounds, and solutions for eTrust Audit Policy Manager.

Cannot Access Policy Manager Database after Upgrade

Symptom:

The upgraded Policy Manager does not connect to the Policy Manager database in Microsoft SQL Server. The DSN exists and connection through the ODBC administrator is successful. Attempts to connect using the Audit Administrator interface return the error message:

Error: Can not read policies
Decrypt failed with internal error 376882
Failed to connect to the database

Solution:

Change the Policy Manager database user ID and password after upgrading to r8 SP2 in order to gain access to the database.

To change the Policy Manager database access credentials

1. Back up the current registry file.
2. Export HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrust Audit\Policy Manager\Database Key to a .reg file.
3. Run the encup utility with the command:

   encup –ic

   or

   encup –hc

   Note: If you not want the screen to display what you type, use the –hc parameter.
4. Enter and confirm the user ID and password.

   This returns an encrypted value in comma-separated, hexadecimal format.
5. Edit the .reg file and paste in the entire encrypted value returned by the encup utility.
6. Run the .reg file so that the new values are saved to the registry.
7. Restart the Distribution Server and iGateway services.

Policy Manager Logs Display Reporter Log Entries

Symptom:

When you access the Policy Manager logs from user credentials with the Maker role, log entries from the Reporter are displayed in addition to the Policy Manager log entries.

Solution:

This is a known issue with the r8 SP2 Policy Manager. There is no workaround.

Default Policies Folder Not Visible in Policy Manager

Symptom:

Rules created under the Default Policies folder in eTrust Audit Policy Manager are not visible.

Solution:

The Default Policies folder is a repository of template policies and should not be used for policy deployment. The Policy Manager screen of Audit Administrator shows the template policies on the Policy Library tab.

To create new policies and rules, we recommend that you create your own policy folder and copy the rules from the Default Policies folder to your policy folder.

iGateway Service May Stop during MP File Import

Symptom:

The iGateway service may stop when an MP file is created using the Browse option (import), when it is committed, or when it is checked.

This problem occurs more frequently when the embedded Identity and Access Management (eIAM) server and the Policy Manager reside on the same physical server.

Solution:

Stop and restart the iGateway service and then try to import the file again.

Installing the eIAM server on a separate physical server helps to prevent this problem.

To restart the iGateway daemon on Solaris systems

1. Stop the iGateway service (Windows) or iGateway daemon (Solaris) with the command:

   $IGW_LOC > S99igateway stop

2. Restart the iGateway service or daemon with the command:

   S99igateway start

To restart the iGateway service on Windows systems

1. Stop the iGateway service with the command:

   net stop igateway

2. Restart the iGateway service or daemon with the command:

   net start igateway

Import of Custom AN Type Appears Unsuccessful

Symptom:

After the following procedure, a custom AN type created in an earlier Policy Manager version and migrated to r8 SP2 does not display correctly:

1. Create a custom AN type.
2. Create a folder that contains the custom AN type.
3. Generate a .ptf file using the utility, pmu_template_exchange, supplied with the r8 SP1 CR2 Policy Manager.
4. Copy the .ptf file to the r8SP2 Policy Manager server.
5. Generate an .xml file using the utility, acptf2xml, supplied with the r8 SP2 Policy Manager.
6. Run the utility, acxml2pmdb, to import the .xml file to the SQL database.
7. Log in to the Audit Administrator interface page.
8. Create a policy folder.
9. Click Create Policy and select the option, Create a policy from an existing policy.
10. Observe the AN node created.

    The existing policy template is created with the name, policyname..version, for example:

    policy1..1

    No policy folder name is displayed.

Solution:

Log off from the Audit Administrator interface and then log in again. This causes display of the imported AN type as expected.

Policy Distribution to Disabled Node May Require Manual Reactivation

Symptom:

Distribution of a policy or MP File to a node that is physically inactive during the distribution processing may not be successful, even if the active polling feature is enabled. The message "Policy Failed to Distribute" appears in the Policy Manager interface.

Solution:

Re-activate the specific audit node manually from within the Policy Manager and then redistribute the policy or MP file to it.

Distribution Server is not Automatically Started on System Restart

Valid on Windows systems

Symptom:

After the Policy Manager is installed and the server machine is restarted, the Distribution Server service intermittently does not start automatically. The Distribution Server Service is not started as it tries to connect to Microsoft SQL Server which was not up with all of the databases mounted after reboot.

Solution:

To resolve this problem, start the Distribution Server service manually.

iTechPoz Services Set to Manual After Upgrade

Valid on Windows systems

Symptom:

After upgrading the Policy Manager from eTrust Audit Build 125 to r8 SP2 CR1 and you restart the server, both the *iTechPoz%SERVERNAME* and *iTechPoz%SERVERNAME-Router* services are in Manual startup mode. This causes an iPoz error in CA EEM as well as the eTrust Audit Admin user interface.

Solution:

Both of the iTechPoz services are set to manual start-up during the upgrade. Before restarting the Policy Manager server, set both of the services to Automatic.

If you have rebooted the Policy Manager server *before* setting these services to Automatic start-up, do the following:

1. Manually both iTechPoz services manually.
2. Restart the iGateway service.

eTrust Audit Reporter and Viewer

The topics that follow describe the known issues, workarounds, and solutions for eTrust Audit Reporter and Viewer.

Reporter and Viewer Cannot Connect to eTrust Audit Databases

Symptom:

After a successful installation, the eTrust Audit Reporter and Viewer are unable to connect to a Microsoft SQL Server or Oracle database.

Solution

When you install a database system, it uses a standard default port number. For example, Microsoft SQL Server uses default port 1433 and Oracle uses port 1521. The Reporter and Viewer are set out-of-the-box to use default port 1433 for SQL Server or 1521 for Oracle when connecting to the Collector and Policy Manager databases.

If the database server is not using the default port value, you must configure the Reporter and Viewer by inserting the correct port number for each data source. If you chose to use a different default port value during the installation of your DBMS, the Reporter and Viewer will not be able to connect until you change the port assignments.

To change the Reporter and Viewer port assignments

1. Navigate to the *Audit install*/etc directory.
2. Edit the RVConfiguration.xml file.
3. Locate the data source nodes for both the Collector and Policy Manager databases by finding the following lines:

   For the Collector database:

   ```
   <dataType>event</dataType>
   ```

   For the Policy Manager database:

   ```
   <dataType>policy</dataType>
   ```

4. Insert the following line just before the closing </datasource> tag for each data source which does not use a default port:

   ```
   <port>portnumber</port>
   ```

5. Save the XML file.
6. Restart the Web Server to re-initialize the Reporter and Viewer applications.

Insufficient Privilege to Access Reporter and Viewer on Windows 2003

Symptom:

Receive an insufficient privileges error message when accessing the Reporter and Viewer from a Microsoft Internet Explorer browser in Windows 2003.

Solution:

A new feature in Windows 2003 called Internet Explorer Enhanced Security Configuration is blocking the Reporter and Viewer pages. Add both the Reporter and Viewer URLs to the Local Internet list in the browser security settings.

To enable Reporter and Viewer display

1. Access the Microsoft Internet Explorer web browser.
2. Select the Tools menu, then select the Internet Options menu item.
3. Select the Security tab.
4. Select the Local Intranet web zone.
5. Click the Sites button.
6. Click the Advanced button to add the URLs.

Unable to Start Reporter or Viewer with service.sh Script

Symptom

Unable to start or stop the Tomcat Web Service for the Reporter and Viewer using the provided service.sh script. The Reporter and Viewer were installed with a custom path, for example /opt/eTrust.

An attempt to start or stop the service from the custom installation directory displays the following error message:

```
bash-2.05# pwd
 /opt/eTrust/jakarta-tomcat-5.0.28/bin
bash-2.05# ./service.sh stop "$JAVA_HOMERV" "$CATALINA_HOMERV" "root"
 cat: cannot open /opt/CA/eTrustAudit/jakarta-tomcat-5.0.28/jsvc.pid
 ./service.sh: usage: kill [ [ -sig ] id ... | -l ]
 /opt/CA/eTrustAudit/jakarta-tomcat-5.0.28/jsvc.pid: No such file or directory
```

Solution:

You must start and stop the Reporter and Viewer from the /bin directory of the eTrust Audit installation for proper functioning.

To use the service.sh script after installing with a custom installation path

1. Navigate to the /<install Audit path>/bin directory
2. Run the service.sh script from that directory using one of the following commands:

   ```
   ./service.sh start "$JAVA_HOMERV" "$CATALINA_HOMERV" "root"
   ```

   ```
   ./service.sh stop "$JAVA_HOMERV" "$CATALINA_HOMERV" "root"
   ```

Cannot Display Desired Maximum Rows in Viewer

Symptom:

When configuring the number of rows for display in the Viewer, cannot set the value to more than 1000.

Solution:

There is a maximum limit of 1000 rows set in the Viewer to maintain operational efficiency.

Authentication Fails for Reporter or Viewer

Symptom:

When using a Microsoft SQL Server 2000 or 2005 database with Credential type Windows Authentication, you may experience a failure to authenticate when accessing the eTrust Audit Reporter and Viewer. This error can occur immediately after installation, or when you are creating a new DSN name for use with a remote database.

Solution:

Configure the service to use the account credentials at startup.

To configure the service with account credentials

1. Click Start, Settings, Control Panel, Administrative Services, and then access the Services tab.
2. Right-click the eTrust Audit Web Server service and select Properties....
3. Click the Log On tab.
4. Select the This account radio button and enter the domain user name and password in the fields to the right.
5. Save the changes and restart the service.

Improper Results When Using Viewer Filters

Symptom:

When using a Microsoft SQL Server or Oracle database for the Collector database, the eTrust Audit Viewer filter does not give proper results.

Solution:

The eTrust Audit Viewer filters are case-sensitive for Microsoft SQL Server or Oracle Collector databases. You must use the correct character type when defining the filters.

Viewer Slows Down When Using "Show all events" Filter

Symptom:

When using the *Show all events* filter in the eTrust Audit Viewer, the Viewer becomes slow or stops responding.

Solution:

With the *Show all events* (as opposed to *Show top records*) option selected, the Viewer can be slow and unresponsive when processing large amount of data from the Collector database. It also waits for the query to return data from the database, so if the data is difficult to locate, the Viewer can appear unresponsive. This happens when the query is searching matched rows using non-indexed fields of the Collector database. Either wait for the results to return, or exit the application.

You can use more specific selection criteria to reduce the result set size and prevent slowdowns. Generally, you should use a report when you want to look at a set of data that would span more than a couple of screens in the Viewer.

Example:

Limit the range of dates in the query, or select *Show top records* and specify a smaller number of records to view (no more than 1000).

Generated RTF Reports Do Not Open Directly

Symptom:

When opening a scheduled and generated a Rich Text Format (RTF) report, a dialog appears that requires you to select whether to open or save the report. The report should open by default, without having to respond to the dialog or save it first.

Solution:

By default, Microsoft Office plugins for Internet Explorer do not open embedded documents for security reasons. Check the "always open files of this type" check box to cause the reports to open without prompting.

Report Templates Not Localized in eTrust Audit Reporter

Symptom:

When a localized version of the Reporter is installed on a computer with localized Windows, some dialogs in the Reporter are displayed in English and the report templates are not localized.

Solution:

The Reporter uses a non-localized version of Crystal Reporter XI R2 (Business Objects). Because of this, some dialogs remain in English and the report templates cannot be localized. The report data is localized if the data is in a supported language.

Export a Report

You can export a report created in Crystal Reports format to another format, or to a new location.

To export a report

1. Generate a new report in Crystal Reports, or select a report previously generated in Crystal Reports.

   The report opens in a new window.

2. Click the Export button at the top left of the window.

   The Export Report dialog appears.

3. Select the format you want from the File Format drop-down menu. You can select Crystal Reports to save the report to your computer.

4. (Optional) Specify a page range for the export.

5. Click OK.

   A dialog appears, prompting you to open or save the report in the format you want.

Viewer Report Displays Improper Page Numbers

Symptom:

When using Microsoft Word 2003 SP2 to import a report that is exported using Crystal Reports Viewer to Microsoft Word-Editable RTF format, all the page numbers appear either as page 1, or the number specified in the field, From page number.

Solution:

To import the report into Microsoft Word, you must export to RTF.

Reports Not Generated at Scheduled Time

Valid on Solaris

Symptom:

The Reporter is configured to generate recurrent reports at a particular time. During the seasonal switch to daylight savings time, the scheduled report is generated either one hour earlier or one hour later than the scheduled time.

Solution:

Ensure that the Reporter computer's time is correctly maintained between Daylight Saving Time periods.

Ensure the system time is synchronized with the real local time for that time zone.

General

The topics that follow describe the general known issues, workarounds, and solutions for eTrust Audit.

Unable to Set Up Services after eTrust Audit Install or Upgrade

Symptom:

While installing, upgrading, or uninstalling eTrust Audit, an attempt to start, stop, add, or remove an eTrust Audit or iGateway service causes the installation, upgrade, or uninstall to fail.

Solution:

The Service Applet Window sometimes locks the service table. If the eTrust Audit install, upgrade, or uninstall process attempts to start, stop, add, or remove a service while the table is locked, the task will fail causing the install, upgrade, or uninstall to fail. The Service Applet window must be closed when installing, upgrading, or uninstalling eTrust Audit.

Removal of Third-Party Software Disables Portmapper Service

Symptom:

During eTrust Audit installation, if a third-party compatible portmapper service is detected on the computer, eTrust Audit uses that service. The eTrust Audit Portmap service is still installed by default, but it is automatically disabled to allow use of the third-party portmapper service. This prevents problems with other software packages, but allows Audit to run normally.

If the third-party portmapper is removed from the computer where Audit is running, you must manually reconfigure Audit to use the default eTrust Audit Portmap service.

Solution:

You can use the following procedure to reconfigure the eTrust Audit Portmap service.

To reconfigure the Portmap service

1. Access the Windows Registry Editor.
2. Locate the key:

   My Computer, HKEY_LOCAL_MACHINE, SYSTEM, ControlSet001, Services, eTrust Audit Log Router
3. Select the DependOnService key in the right pane.
4. Modify the current value ”portmap LanmanWorkstation LanmanServer” with the new value as “eTrust Audit portmap LanmanWorkstation LanmanServer”.
5. Restart the computer.

   The eTrust Audit Log Router service starts and Audit should operate normally.

iGateway Service Does Not Start Successfully on Solaris

Symptom:

The Security Monitor shows frequent attempts to restart the iGateway daemon, but it is not able to start successfully. The watchdog daemons continue to try to restart iGateway generating a self-monitoring message each time.

Solution:

The Distribution Server is preventing the iGateway daemon from starting properly. To resolve this situation, do the following:

1. Stop the Distribution Server.
2. Start iGateway.
3. Restart the Distribution Server after iGateway has started up completely.

Watchdog Service Does Not Start Properly

Valid on HP-UX PA-RISC and Itanium platforms

Symptom:

After a system restart, the watchdog service that ensures that the iGateway daemon is running does not start. Only the iGateway daemon is running.

Solution:

Manually stop and then restart the iGateway daemon. This automatically restarts the watchdog service.

eTrust Audit Services Fail to Stop

Symptom:

Attempts to stop eTrust Audit services sometimes fail.

Solution:

If the eTrust Audit services cannot be stopped, use the *kill.exe* utility from the eTrust Audit installation directory to kill the service executables.

Mixed Versions of eTrust Audit Components Do Not Function Properly after Upgrading

Symptom:

When different versions of eTrust Audit components are installed on the same computer, they do not function properly.

Solution:

You must upgrade all eTrust Audit components on the same system to the same release for the product to function properly.

acstat Utility Returns "Cannot find file (filename)" Error Message

Valid on all UNIX platforms

Symptom:

After completing an eTrust Audit install, running the acstat utility in the same console window may produce output containing an error message similar to the following in the iTechnology section:

"Cannot find file: (filename)"

Solution:

Verify that the required environment variables (like LIBPATH) are exported. If they are not exported, do the following:

1. Access a command prompt.
2. Navigate to the directory, Audit_install_dir/bin
3. Execute the following script:

   ./ac_set_env.sh

ac_set_env.sh Command Fails

Valid on HP-UX

Symptom:

When running ". ./ac_set_env.sh within a POSIX shell session, the command fails with the following error:

sh: SHLIB_PATH: Parameter not set

Solution:

Run a Korn shell session (/usr/bin/ksh), and then run the following command again:

. . /ac_set_env.sh

Knowledge Base

The topics that follow describe the known facts, workarounds, and solutions for eTrust Audit.

Changes to iRecorder Not Reflected in List of iRecorder Hosts

Symptom:

When changing the host name of an iRecorder host or installing a new iRecorder, the changes are not immediately reflected in the list of discovered iRecorders in the Audit Administrator's iRecorder Manager.

Solution:

The list of discovered iRecorders in the iRecorder Manager is not refreshed automatically whenever you change the host name of a discovered iRecorder host, add or remove iRecorders on a discovered host, or install new iRecorders on a new host.

The iRecorders are discovered by Host Discovery jobs. The next time you execute the discovery job, changes on a discovered host are reflected in the list. The host with newly installed iRecorders is discovered if it is in the subnet of an existing job, or if you define a new job for the new host's subnet.

Use the Show Host option to directly browse a host from which you want to retrieve information on the installed iRecorders or to manage the iRecorders.

Microsoft SQL Server Connection Fails

Symptom:

When trying to connect to a Microsoft SQL Server 2000 database from a client with an ODBC driver older than 2000, the connection fails.

Solution:

Do the following:

- Verify the SQL Server 2000 Network Library configuration for the connection type by invoking the Client Configuration dialog.
- When you select Named Pipes as the Network Library, ensure that the Pipe name is the same as the server to which it is pointing.

  Note: If you are not sure of the server pipe name, select TCP/IP as Network Library.
- Verify the ODBC services to determine whether an upgrade to the latest MDAC is necessary.

Newly Generated Events Not Displayed

Symptom:

A Collector database query for newly generated events does not display the events.

Solution:

If new events are generated, the queries do not show these events until the AuditExtendString table created by the Post-Collection Utility is populated.

Harvesting Events Fails with eTrust VPN or eTrust Access Control Installed

Symptom:

When eTrust VPN and eTrust Access Control are installed on the same network, eTrust Audit experiences problems harvesting the events.

Solution:

When eTrust VPN or eTrust Access Control is installed on the network, either product can block access for eTrust Audit messages or other information in need of delivery.

Stop eTrust VPN or eTrust Access Control to determine whether the problem persists.

Data Tools Uninstall Removes eAudit_DSN ODBC Data Source

Symptom:

When Data Tools are uninstalled, the data source named eAudit_DSN is removed.

Solution:

The Data Tools access the Collector database using an ODBC data source. The data source eAudit_DSN is created automatically during installation. When you uninstall the Data Tools, this data source name is also removed.

Do not use eAudit_DSN as the name of the ODBC data source for other programs you install. This name is reserved for the Data Tools.

Mail Delivery Problems Using SMTP

Symptom:

SMTP mail delivery is not functioning properly.

Solution:

If you have problems with mail delivery using SMTP, you might need to change the name for the mail sender. Certain SMTP servers require the mail sender to have a valid mail account.

The name of the mail sender is stored in the value entry *Sender* under the registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrust Audit\Mail

Chapter 10: Fixed Issues

This section contains the following topics:

Test Fixes

eTrust Audit r8 SP2 CR1 contains the following test fixes:

RO04803	QO94353	T5HU004	T35E121	T35E116
RO02694	QO94057	T5H9009	T35E120	T35E117
RO01054	QO93909	T5HU003	T5IU001	T35E115
RO00546	QO90315	T35E123	T5G4014	T35E114
QO95511	T5G4027	T35E122	T35E118	T4A5020
QO95260	T5FS011	T5FS010	T35E119	T4A5018
QO94490	T35E124	T4A5043	T5HL005	

Fixed Issues List

The following issues are fixed in the r8 SP2 CR1 release:

15018433	15882826	16974228 / 01	17190350	17658920
15108944	15886509 / 01	16986832	17198245	17658925
15112543	15957937	16987582	17216923 / 2	17658937
15186099 / 01	15963917	17055397	17236203	17658958
15205754	16097345	17055397	17238157	17658977
15216636	16097807	17055446	17477693 / 01	17659066
15266211	16179405 / 01	17068469	17482584	17675671 / 1
15279620	16179499	17068469	17482667	17675671 / 2
15337411	16179499 / 2	17068495	17483088	17683059
15417746	16179499 / 3	17068495	17483095	17683059 / 02
15470600	16179499 / 4	17137083	17483135	17733748

15472775	16299173 / 01	17146458 / 2	17483163	17733748 / 01
15494094	16299173 / 02	17160756	17486963 / 01	17733776 / 01
15583389	16299173 / 2	17160793	17563213 / 01	17935041
15644898	16497183 / 05	17160835	17656613 / 01	
15732559	16569229 / 2	17161024	17658596	
15733432	16569229 / 3	17161029	17658651	
15819249	16712926	17161048	17658695	
15841505	16969169	17168836	17658717	
15882810 / 01	16969169 / 01	17168931	17658881	

Chapter 11: Documentation

This section contains the following topics:

Bookshelf

The Bookshelf provides access to all eTrust Audit documentation from a central location. The Bookshelf includes the following:

- Single expandable list of contents for all guides in HTML format
- Full text search across all guides with search terms highlighted in the content and ranked search results
- Breadcrumbs that link you to higher level topics
- Single index across all guides
- Links to PDF versions of guides for printing

The Audit_bookshelf_enu.zip is available for download from the following location:

- CA Support Site

Viewing the Bookshelf requires Internet Explorer 6 or 7 or Mozilla Firefox 2 or 3. For bookshelf links to PDF guides that you can print, Adobe Reader 7 or above is required. You can download the latest version of Adobe Reader at www.adobe.com.

How to Use the Bookshelf

To use the Bookshelf

1. Extract the contents of the ZIP file.
2. Choose one of the following methods:
   - Open the Bookshelf.hta file if the bookshelf is on the local system and you are using Internet Explorer.
   - Open the Bookshelf.html file if the bookshelf is on a remote system or if you are using Mozilla Firefox.

The Bookshelf opens.

Chapter 12: Third-Party Acknowledgements

This section contains the following topics:

Apache Licenses

The following Apache products are used by eTrust Audit r8 SP2 CR1:

- Apache Ant 1.6.5
- Apache Tomcat 5.0.28
- Apache Xalan-C 1.9.0
- Apache Xerces-C 2.6.0

Portions of this product include software developed by the Apache Software Foundation. The Apache software is distributed in accordance with the following license agreement.

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

NET-SNMP 5.1.2

Various copyrights apply to this package, listed in 3 separate parts below. Please make sure that you read all the parts. Up until 2001, the project was based at UC Davis, and the first part covers all code written during this time. From 2001 onwards, the project has been based at SourceForge, and Networks Associates Technology, Inc hold the copyright on behalf of the wider Net-SNMP community, covering all derivative work done since then. An additional copyright section has been added as Part 3 below also under a BSD license for the work contributed by Cambridge Broadband Ltd. to the project since 2001.

Code has been contributed to this project by many people over the years it has been in development, and a full list of contributors can be found in the README file under the THANKS section.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2002, Networks Associates Technology, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2002, Cambridge Broadband Ltd. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

OpenSSL Toolkit 0.9.8.d

LICENSE ISSUES

==========

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Copyright (c) 1998-2003 The OpenSSL Project.All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

> "This product includes software developed by the OpenSSL Projectfor use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used toendorse or promote products derived from this software withoutprior written permission. For written permission, please contactopenssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior writtenpermission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

> "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS|&"&| AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

/

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to.The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

> "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from he apps directory (application code) you must include an acknowledgement:

> "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS|&"&| AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

/

Sun JDK 1.4.2_13

Sun Microsystems, Inc.

Binary Code License Agreement

for the

JAVATM 2 RUNTIME ENVIRONMENT (J2RE), STANDARD EDITION, VERSION 1.4.2_X

SUN MICROSYSTEMS, INC. ("SUN") IS WILLING TO LICENSE THE SOFTWARE IDENTIFIED BELOW TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS BINARY CODE LICENSE AGREEMENT AND SUPPLEMENTAL LICENSE TERMS (COLLECTIVELY "AGREEMENT"). PLEASE READ THE AGREEMENT CAREFULLY. BY DOWNLOADING OR INSTALLING THIS SOFTWARE, YOU ACCEPT THE TERMS OF THE AGREEMENT. INDICATE ACCEPTANCE BY SELECTING THE "ACCEPT" BUTTON AT THE BOTTOM OF THE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY ALL THE TERMS, SELECT THE "DECLINE" BUTTON AT THE BOTTOM OF THE AGREEMENT AND THE DOWNLOAD OR INSTALL PROCESS WILL NOT CONTINUE.

1.DEFINITIONS. "Software" means the identified above in binary form, any other machine readable materials (including, but not limited to, libraries, source files, header files, and data files), any updates or error corrections provided by Sun, and any user manuals, programming guides and other documentation provided to you by Sun under this Agreement. "Programs" mean Java applets and applications intended to run on the Java 2 Platform, Standard Edition (J2SETM platform) platform on Java-enabled general purpose desktop computers and servers.

2.LICENSE TO USE. Subject to the terms and conditions of this Agreement, including, but not limited to the Java Technology Restrictions of the Supplemental License Terms, Sun grants you a non-exclusive, non-transferable, limited license without license fees to reproduce and use internally Software complete and unmodified for the sole purpose of running Programs. Additional licenses for developers and/or publishers are granted in the Supplemental License Terms.

3.RESTRICTIONS. Software is confidential and copyrighted. Title to Software and all associated intellectual property rights is retained by Sun and/or its licensors. Unless enforcement is prohibited by applicable law, you may not modify, decompile, or reverse engineer Software. You acknowledge that Licensed Software is not designed or intended for use in the design, construction, operation or maintenance of any nuclear facility. Sun Microsystems, Inc. disclaims any express or implied warranty of fitness for such uses. No right, title or interest in or to any trademark, service mark, logo or trade name of Sun or its licensors is granted under this Agreement. Additional restrictions for developers and/or publishers licenses are set forth in the Supplemental License Terms.

4.LIMITED WARRANTY. Sun warrants to you that for a period of ninety (90) days from the date of purchase, as evidenced by a copy of the receipt, the media on which Software is furnished (if any) will be free of defects in materials and workmanship under normal use. Except for the foregoing, Software is provided "AS IS". Your exclusive remedy and Sun's entire liability under this limited warranty will be at Sun's option to replace Software media or refund the fee paid for Software. Any implied warranties on the Software are limited to 90 days. Some states do not allow limitations on duration of an implied warranty, so the above may not apply to you. This limited warranty gives you specific legal rights. You may have others, which vary from state to state.

5.DISCLAIMER OF WARRANTY. UNLESS SPECIFIED IN THIS AGREEMENT, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT THESE DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

6.LIMITATION OF LIABILITY. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event will Sun's liability to you, whether in contract, tort (including negligence), or otherwise, exceed the amount paid by you for Software under this Agreement. The foregoing limitations will apply even if the above stated warranty fails of its essential purpose. Some states do not allow the exclusion of incidental or consequential damages, so some of the terms above may not be applicable to you.

7.SOFTWARE UPDATES FROM SUN. You acknowledge that at your request or consent optional features of the Software may download, install, and execute applets, applications, software extensions, and updated versions of the Software from Sun ("Software Updates"), which may require you to accept updated terms and conditions for installation. If additional terms and conditions are not presented on installation, the Software Updates will be considered part of the Software and subject to the terms and conditions of the Agreement.

8.SOFTWARE FROM SOURCES OTHER THAN SUN. You acknowledge that, by your use of optional features of the Software and/or by requesting services that require use of the optional features of the Software, the Software may automatically download, install, and execute software applications from sources other than Sun ("Other Software"). Sun makes no representations of a relationship of any kind to licensors of Other Software. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE OTHER SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Some states do not allow the exclusion of incidental or consequential damages, so some of the terms above may not be applicable to you.

9.TERMINATION. This Agreement is effective until terminated. You may terminate this Agreement at any time by destroying all copies of Software. This Agreement will terminate immediately without notice from Sun if you fail to comply with any provision of this Agreement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right. Upon Termination, you must destroy all copies of Software.

10.EXPORT REGULATIONS. All Software and technical data delivered under this Agreement are subject to US export control laws and may be subject to export or import regulations in other countries. You agree to comply strictly with all such laws and regulations and acknowledge that you have the responsibility to obtain such licenses to export, re-export, or import as may be required after delivery to you.

11.TRADEMARKS AND LOGOS. You acknowledge and agree as between you and Sun that Sun owns the SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET trademarks and all SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET-related trademarks, service marks, logos and other brand designations ("Sun Marks"), and you agree to comply with the Sun Trademark and Logo Usage Requirements currently located at http://www.sun.com/policies/trademarks. Any use you make of the Sun Marks inures to Sun's benefit.

12.U.S. GOVERNMENT RESTRICTED RIGHTS. If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation will be only as set forth in this Agreement; this is in accordance with 48 CFR 227.7201 through 227.7202-4 (for Department of Defense (DOD) acquisitions) and with 48 CFR 2.101 and 12.212 (for non-DOD acquisitions).

13.GOVERNING LAW. Any action related to this Agreement will be governed by California law and controlling U.S. federal law. No choice of law rules of any jurisdiction will apply.

14.SEVERABILITY. If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate.

15.INTEGRATION. This Agreement is the entire agreement between you and Sun relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party.

SUPPLEMENTAL LICENSE TERMS

These Supplemental License Terms add to or modify the terms of the Binary Code License Agreement. Capitalized terms not defined in these Supplemental Terms shall have the same meanings ascribed to them in the Binary Code License Agreement . These Supplemental Terms shall supersede any inconsistent or conflicting terms in the Binary Code License Agreement, or in any license contained within the Software.

A.Software Internal Use and Development License Grant. Subject to the terms and conditions of this Agreement, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce internally and use internally the Software complete and unmodified (unless otherwise specified in the applicable README file) for the purpose of designing, developing, and testing your Programs.

B.License to Distribute Software. Subject to the terms and conditions of this Agreement, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute the Software, provided that (i) you distribute the Software complete and unmodified (unless otherwise specified in the applicable README file) and only bundled as part of, and for the sole purpose of running, your Programs, (ii) the Programs add significant and primary functionality to the Software, (iii) you do not distribute additional software intended to replace any component(s) of the Software (unless otherwise specified in the applicable README file), (iv) you do not remove or alter any proprietary legends or notices contained in the Software, (v) you only distribute the Software subject to a license agreement that protects Sun's interests consistent with the terms contained in this Agreement, and (vi) you agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software.

C.License to Distribute Redistributables. Subject to the terms and conditions of this Agreement, including but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute those files specifically identified as redistributable in the Software "README" file ("Redistributables") provided that: (i) you distribute the Redistributables complete and unmodified (unless otherwise specified in the applicable README file), and only bundled as part of Programs, (ii) you do not distribute additional software intended to supersede any component(s) of the Redistributables (unless otherwise specified in the applicable README file), (iii) you do not remove or alter any proprietary legends or notices contained in or on the Redistributables, (iv) you only distribute the Redistributables pursuant to a license agreement that protects Sun's interests consistent with the terms contained in the Agreement, (v) you agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software.

D.Java Technology Restrictions. You may not modify the Java Platform Interface ("JPI", identified as classes contained within the "java" package or any subpackages of the "java" package), by creating additional classes within the JPI or otherwise causing the addition to or modification of the classes in the JPI. In the event that you create an additional class and associated API(s) which (i) extends the functionality of the Java platform, and (ii) is exposed to third party software developers for the purpose of developing additional software which invokes such additional API, you must promptly publish broadly an accurate specification for such API for free use by all developers. You may not create, or authorize your licensees to create, additional classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun" or similar convention as specified by Sun in any naming convention designation.

E.Source Code. Software may contain source code that, unless expressly licensed for other purposes, is provided solely for reference purposes pursuant to the terms of this Agreement. Source code may not be redistributed unless expressly provided for in this Agreement.

F.Third Party Code. Additional copyright notices and license terms applicable to portions of the Software are set forth in the THIRDPARTYLICENSEREADME.txt file. In addition to any terms and conditions of any third party opensource/freeware license identified in the THIRDPARTYLICENSEREADME.txt file, the disclaimer of warranty and limitation of liability provisions in paragraphs 5 and 6 of the Binary Code License Agreement shall apply to all Software in this distribution.

For inquiries please contact: Sun Microsystems, Inc., 4150 Network Circle,

Santa Clara, California 95054, U.S.A.

(LFI#135955/Form ID#011801)

THIRDPARTYLICENSEREADME.txt:

DO NOT TRANSLATE OR LOCALIZE.

A) The following software may be included in this product: CS CodeViewer v1.0; Use of any of this software is governed by the terms of the license below:

Copyright 1999 by CoolServlets.com.

Any errors or suggested improvements to this class can be reported as instructed on CoolServlets.com. We hope you enjoy this program... your comments will encourage further development! This software is distributed under the terms of the BSD License. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither name of CoolServlets.com nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY COOLSERVLETS.COM AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE."

B) The following software may be included in this product: DES and 3xDES ; Use of any of this software is governed by the terms of the license below:

"Copyright 2000 by Jef Poskanzer . All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE."

C) The following software may be included in this product: Crimson v1.1.1 ; Use of any of this software is governed by the terms of the license below:

/*

* The Apache Software License, Version 1.1

*

```
*
* Copyright (c) 1999-2000 The Apache Software Foundation. All rights
* reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
* notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in
* the documentation and/or other materials provided with the
* distribution.
*
* 3. The end-user documentation included with the redistribution,
* if any, must include the following acknowledgment:
* "This product includes software developed by the
* Apache Software Foundation (http://www.apache.org/)."
* Alternately, this acknowledgment may appear in the software itself,
* if and wherever such third-party acknowledgments normally appear.
*
* 4. The names "Crimson" and "Apache Software Foundation" must
* not be used to endorse or promote products derived from this
```

```
* software without prior written permission. For written

* permission, please contact apache@apache.org.

*

* 5. Products derived from this software may not be called "Apache",

* nor may "Apache" appear in their name, without prior written

* permission of the Apache Software Foundation.

*

* THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED

* WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES

* OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE

* DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION
OR

* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,

* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
NOT

* LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS
OF

* USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED
AND

* ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,

* OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT

* OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF

* SUCH DAMAGE.

*
================================================

*

* This software consists of voluntary contributions made by many
```

* individuals on behalf of the Apache Software Foundation and was

* originally based on software copyright (c) 1999, International

* Business Machines, Inc., http://www.ibm.com. For more

* information on the Apache Software Foundation, please see

* .

*/

D) The following software may be included in this product:

Xalan J2; Use of any of this software is governed by the

terms of the license below:

/*

* The Apache Software License, Version 1.1

*

*

* Copyright (c) 1999-2000 The Apache Software Foundation. All rights

* reserved.

*

* Redistribution and use in source and binary forms, with or without

* modification, are permitted provided that the following conditions

* are met:

*

* 1. Redistributions of source code must retain the above copyright

* notice, this list of conditions and the following disclaimer.

*

* 2. Redistributions in binary form must reproduce the above copyright

* notice, this list of conditions and the following disclaimer in

* the documentation and/or other materials provided with the

* distribution.

*

* 3. The end-user documentation included with the redistribution,

* if any, must include the following acknowledgment:

* "This product includes software developed by the

* Apache Software Foundation (http://www.apache.org/)."

* Alternately, this acknowledgment may appear in the software itself,

* if and wherever such third-party acknowledgments normally appear.

*

* 4. The names "Xalan" and "Apache Software Foundation" must

* not be used to endorse or promote products derived from this

* software without prior written permission. For written

* permission, please contact apache@apache.org.

*

* 5. Products derived from this software may not be called "Apache",

* nor may "Apache" appear in their name, without prior written

* permission of the Apache Software Foundation.

*

* THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED

* WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES

* OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE

* DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR

* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,

* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT

* LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF

* USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND

* ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,

* OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT

* OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF

* SUCH DAMAGE.

* ==

*

* This software consists of voluntary contributions made by many

* individuals on behalf of the Apache Software Foundation and was

* originally based on software copyright (c) 1999, International

* Business Machines, Inc., http://www.ibm.com. For more

* information on the Apache Software Foundation, please see

* .

*/

E) The following software may be included in this product: NSIS 1.0j; Use of any of this software is governed by the terms of the license below:

Copyright (C) 1999-2000 Nullsoft, Inc.

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution. Justin Frankel justin@nullsoft.com"

F) Some Portions licensed from IBM are available at:

http://oss.software.ibm.com/icu4j/

G) Portions Copyright Eastman Kodak Company 1992

H) Lucida is a registered trademark or trademark of Bigelow & Holmes in the U.S. and other countries.

I) Portions licensed from Taligent, Inc.

Sun JDK 1.6.0

ADDITIONAL TERMS AND CONDITIONS FOR THE USE OF

Sun JDK 1.6

(JAVA 2 PLATFORM STANDARD EDITION RUNTIME ENVIRONMENT 6.0)

Licensee agrees that the following terms (in addition to the applicable provisions above) shall apply with respect to any open source code provided by Sun Microsystems, Inc. contained within the Product. Notwithstanding anything contained in the CA End User License Agreement, solely with respect to such open source, these terms are not superseded by any written agreement between CA and Licensee:
"Software" means Java' 2 Platform Standard Edition Version 1.6_X and any user manuals, programming guides and other documentation provided to Licensee.

Title to Software and all associated intellectual property rights is retained by Sun Microsystems, Inc. ('Sun') and/or its licensors. Licensee acknowledges that Software is not designed or intended for use in the design, construction, operation or maintenance of any nuclear facility. Sun disclaims any express or implied warranty of fitness for such uses. No right, title or interest in or to any trademark, service mark, logo or trade name of Sun or its licensors is granted under this agreement.

The Software is provided "AS IS". As to any claim made by Licensee against Sun respecting Software, Licensee's exclusive remedy and Sun's entire liability under this limited warranty will be at Sun's option to replace Software media or refund the fee paid for Software by Licensee to Sun which Licensee acknowledges is $0.

UNLESS SPECIFIED IN THIS AGREEMENT, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT THESE DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. The foregoing limitations shall not affect any warranties provided in any other applicable agreement between Licensee and CA.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event will Sun's liability to you, whether in contract, tort (including negligence), or otherwise, exceed the amount paid for Software by Licensee to Sun which Licensee acknowledges is $0. The foregoing limitations will apply even if the above stated warranty fails of its essential purpose.

Licensee acknowledges that Licensee's use of the Software will terminate immediately without notice if Licensee fails to comply with any provision of this agreement. Licensee acknowledges that Sun may terminate this agreement immediately should the Software become, or in Sun's opinion be likely to become, the subject of a claim of infringement of any intellectual property right. Upon termination, Licensee must destroy all copies of Software.

Licensee acknowledges and agrees as between Licensee and Sun that Sun owns the SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET trademarks and all SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET-related trademarks, service marks, logos and other brand designations ("Sun Marks"), and Licensee agrees to comply with the Sun Trademark and Logo Usage Requirements currently located at http://www.sun.com/policies/trademarks. Any use Licensee makes of the Sun Marks inures to Sun's benefit.
Notwithstanding anything to the contrary contained in any agreement between Licensee and CA, any action related to this agreement in which Sun is a party will be governed by California law and controlling U.S. federal law. No choice of law rules of any jurisdiction will apply.

Licensee acknowledges that additional copyright notices and license terms applicable to portions of the Software are set forth in the THIRDPARTYLICENSEREADME.txt file.

For inquiries please contact: Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A.