# CA Access Control Premium Edition

## Release Notes

12.6.01

# Third-Party Notices

CONTAINS IBM(R) 32-bit Runtime Environment for AIX(TM), Java(TM) 2 Technology Edition, Version 1.4 Modules



# Sample Scripts and Sample SDK Code

The Sample Scripts and Sample SDK code included with the CA Access Control product are provided "as is", for informational purposes only. They may need to be adjusted in specific environments and should not be used in production without testing and validating them before deploying them on a production system.

CA Technologies does not provide support for these samples and cannot be responsible for any errors that these scripts may cause.

# CA Technologies Product References

This document references the following CA Technologies products:

- CA Access Control Premium Edition
- CA Access Control
- CA Single Sign-On (CA SSO)
- CA Top Secret®
- CA ACF2™
- CA Audit
- CA Network and Systems Management (CA NSM, formerly Unicenter NSM and Unicenter TNG)
- CA Software Delivery (formerly Unicenter Software Delivery)
- CA Service Desk (formerly Unicenter Service Desk)
- CA User Activity Reporting Module (formerly CA Enterprise Log Manager)
- CA Identity Manager

# Documentation Conventions

The CA Access Control documentation uses the following conventions:

| Format | Meaning |
|---|---|
| `Mono-spaced font` | Code or program output |
| *Italic* | Emphasis or a new term |
| **Bold** | Text that you must type exactly as shown |
| A forward slash (/) | Platform independent directory separator used to describe UNIX and Windows paths |

The documentation also uses the following special conventions when explaining command syntax and user input (in a mono-spaced font):

| Format | Meaning |
|---|---|
| *Italic* | Information that you must supply |
| Between square brackets ([]) | Optional operands |

| Format | Meaning |
|---|---|
| Between braces ({}) | Set of mandatory operands |
| Choices separated by pipe (\|). | Separates alternative operands (choose one).<br>For example, the following means *either* a user name *or* a group name:<br>{*username*\|*groupname*} |
| ... | Indicates that the preceding item or group of items can be repeated |
| Underline | Default values |
| A backslash at end of line preceded by a space ( \) | Sometimes a command does not fit on a single line in this guide. In these cases, a space followed by a backslash ( \) at the end of a line indicates that the command continues on the following line.<br>**Note:** Avoid copying the backslash character and omit the line break. These are not part of the actual command syntax. |

### Example: Command Notation Conventions

The following code illustrates how command conventions are used in this guide:

```
ruler className [props({all|{propertyName1[,propertyName2]...})]
```

In this example:

- The command name (ruler) is shown in regular mono-spaced font as it must be typed as shown.
- The *className* option is in italic as it is a placeholder for a class name (for example, USER).
- You can run the command without the second part enclosed in square brackets, which signifies optional operands.
- When using the optional parameter (props), you can choose the keyword *all* or, specify one or more property names separated by a comma.

## File Location Conventions

The CA Access Control documentation uses the following file location conventions:

- *ACInstallDir*—The default CA Access Control installation directory.
  - Windows—C:\Program Files\CA\AccessControl\
  - UNIX—/opt/CA/AccessControl/

- *ACSharedDir*—A default directory used by CA Access Control for UNIX.
  - UNIX—/opt/CA/AccessControlShared
- *ACServerInstallDir*—The default CA Access Control Enterprise Management installation directory.
  - /opt/CA/AccessControlServer
- *DistServerInstallDir*—The default Distribution Server installation directory.
  - /opt/CA/DistributionServer
- *JBoss_HOME*—The default JBoss installation directory.
  - /opt/jboss-4.2.3.GA

# Contact CA Technologies

**Contact CA Support**

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

- 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

**Providing Feedback About Product Documentation**

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

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

# Documentation Changes

The following documentation updates have been made since the last release of this documentation:

-

# Contents


## Chapter 1: Welcome 15

## Chapter 2: CA Access Control Editions 15

CA Access Control Premium Edition Installation Media ..... 15
CA Access Control Installation Media ..... 17
Complementary CA User Activity Reporting Module License ..... 18
A Single Documentation Set for All Editions ..... 19

## Chapter 3: New and Changed Features 21

CA Access Control Enterprise Management and CA Access Control Enhancements ..... 21
UNAB Enhancements ..... 22
PUPM Enhancements ..... 23
Documentation Enhancements ..... 25
Fixed Issues in This Release ..... 25

## Chapter 4: System Requirements 27

Operating System Support ..... 27
Enterprise Management Server Requirements ..... 27
Enterprise Management Server Integration Components ..... 28
CA Access Control Endpoint Management Requirements ..... 29
Enterprise Reporting Requirements ..... 29
Distribution Server Requirements ..... 30
Windows Endpoint Requirements ..... 30
UNIX Endpoint Requirements ..... 30
Policy Model Database Requirements ..... 31
UNAB Requirements ..... 31

## Chapter 5: Documentation 33

Guides ..... 33

## Chapter 6: FIPS Compliance 35

FIPS Operational Modes ..... 35
Unsupported Operating Systems for FIPS-only Mode ..... 35
FIPS Encryption Libraries ..... 35

FIPS Algorithms Used ..... 36
Storage of Keys and Certificates ..... 36
Features Affected (UNIX) ..... 36
Features Affected (Windows) ..... 38

## Chapter 7: Feature Support Limitations 41

IPv6 Support ..... 41
Windows Endpoint Limitations ..... 41
x64 Feature Support Limitations ..... 41
IA64 Feature Support Limitations ..... 42
Windows Server 2008 Feature Support Limitations ..... 42
SAN Support ..... 43
McAfee Entercept Buffer Overflow ..... 43
Short File Name Rules (8.3 Format) Are Not Supported ..... 44
UNIX Endpoint Limitations ..... 44
HP-UX Feature Support Limitations ..... 44
Unicenter Integration is Not Supported on HP-UX Itanium and RHEL Itanium ..... 44
PUPM Agent Are Not Supported on Linux IA64 ..... 44
SAN Support ..... 45
UNAB Limitations ..... 45
Nested Groups Not Supported For One-Way Trust ..... 45
Fully Integrated Active Directory Users Not Supported for One-Way Trust ..... 45
uxconsole Shows Basic Information For One-Way Trust Domains ..... 45
UNAB Not Supported on Linux IA64 ..... 46
UNAB is not FIPS140-2 and IPV6 Compliant ..... 46
PUPM Limitations ..... 46
PUPM Is Not FIPS140-2 and IPV6 Compliant ..... 46

## Chapter 8: Installation Considerations 47

Supported Installation Languages ..... 47
Windows Endpoint Installation Considerations ..... 48
Restart Message Pops Up During Installation, Uninstallation or Upgrade on Windows Server 2008 ..... 48
UNIX Endpoint Installation Considerations ..... 48
AIX 6.1 Requires TL3 or Later for CA Access Control to Start ..... 48
Message Queue for Linux390 Requires J2SE Version 5.0 ..... 48
Compatibility Library Missing on x86_64bit Linux ..... 48
CA Access Control Installation and Uninstallation Restarts UNAB ..... 49
Propagating CA Access Control and UNAB to a New Solaris Zone ..... 49
Installing CA Access Control on Solaris 11 Limitation ..... 49
UNAB Endpoint Installation Considerations ..... 49
UNAB for Linux 390 Requires J2SE Version 5.0 for Remote Management ..... 49

Server Component Installation Considerations ..... 49
Install Primary and Load Balancing Enterprise Management Server on Same Time Zone ..... 50
Installing Endpoint Management on 64-bit Linux ..... 50
Special Characters in Administrator Name ..... 50
Supported JDK and JBoss Versions ..... 50
Prerequisite Kit Installer Considerations ..... 50
Superuser Account Required for Server Components Installations ..... 50
RDBMS Connection Fails During Installation if Java Cannot Be Found ..... 51
Enterprise Management Server Installation Does Not Support Spaces in Installation Path ..... 51
Set Up CA Access Control Enterprise Management to Work with Active Directory on Another Domain ..... 51
CA Access Control Endpoint Management Installation Instructions Refer to Both Editions of CA Access Control ..... 52
CA Access Control Endpoint Management Shortcut Points to Port Number 8080 ..... 52
CA User Activity Reporting Module Supports Only Trusted SSL Connection ..... 53
Special Subscription Needed to View CA User Activity Reporting Module Reports from CA Access Control Enterprise Management ..... 53
Synchronize the System Time of the CA Access Control Enterprise Management and Report Portal Computers ..... 53
Uninstall Fails if You Are Not the Superuser ..... 53

## Chapter 9: Upgrade Considerations 55

Versions You Can Upgrade From ..... 55
Windows Endpoint Upgrade Considerations ..... 56
Reboot May Be Required When Upgrading ..... 56
Change in Default Access to Database ..... 56
UNIX Endpoint Upgrade Considerations ..... 56
Default Installation Location ..... 56
FIPS 140-2 Library Upgrade ..... 56
Systemwide Audit Mode for UNIX Upgrades ..... 57
Authorization Recognizes Resource Group Ownership ..... 57
syslog Messages That Have a Reduced Priority ..... 57
Server Component Upgrade Considerations ..... 57
Upgrading Enterprise Management Server to r12.6.01 Does Not Preserve Roles and Tasks ..... 58
CA Access Control r12.6.01 Requires Hot Fix to Manage Policy Models on CA Access Control r12.5 and r12.0.01 ..... 58
Hot Fix Required Before Upgrade to Use Policies and Host Groups Containing Spaces ..... 58
Software Patch Required to Deploy Policies on Endpoints ..... 58
CA Access Control Enterprise Management Default Encryption Method Set to 256AES ..... 59

## Chapter 10: General Considerations 61

Windows Endpoint Considerations ..... 61

RunAs Administrator to Start CA Access Control on Windows Server 2008 ..... 61
Uninstall Does Not Remove CA License Files ..... 61
UNAB Considerations ..... 61
Disable Local User Account After Migration ..... 61
Do Not Set the unab_refresh_interval Token Value to a Short Interval ..... 62
Do not Set Kerberos dns_lookup_realm to True ..... 62
UNAB Users Cannot Change Account Password According to Specified Password Policy ..... 62
sepass Integration with UNAB Endpoints ..... 62
Log In to UNAB with Active Directory Account ..... 63
You Cannot Log In to CA Access Control for UNIX Using 'Administrator' Account When UNAB Is Installed ..... 63
CA Access Control Installation and Uninstallation Restarts UNAB ..... 63
Server Components Considerations ..... 63
Communication Issues between CA Access Control Components and CA Access Control Message Queue ..... 64
CA Access Control Host Name Limitation ..... 64
Automatic Generation of Policy Undeploy Script ..... 64
Specify the PUPM Endpoint NETBIOS Name and Not the DNS Domain Name ..... 65
You Cannot Configure More Than a Single CA Identity Manager Provisioning Connector Server ..... 65
Cannot Configure CA Identity Manager Provisioning Connector Server Using SSL Port ..... 65
Cannot Use PUPM to Change Password for the Expert Account ..... 65
SQLCMD Utility Does Not Support Blank Passwords ..... 66

## Chapter 11: Known Issues 67

Installation Known Issues ..... 67
Windows Endpoint Installation Known Issues ..... 67
UNIX Endpoint Installation Known Issues ..... 67
UNAB Endpoint Installation Known Issues ..... 69
Upgrade Known Issues ..... 70
Windows Endpoint Upgrade Known Issues ..... 70
UNIX Endpoint Upgrade Known Issues ..... 70
General Known Issues ..... 70
Windows Endpoint Known Issues ..... 71
UNIX Endpoint Known Issues ..... 72
UNAB Known Issues ..... 76
Server Components Known Issues ..... 80
Documentation Known Issues ..... 89

## Appendix A: Third-Party License Agreements 91

Software Under the Apache License ..... 92
Software Under the Daniel Veillard License ..... 99

Software Under the OpenLDAP License ..... 101
Software Under the OpenSSL License ..... 104
AES 2.4 ..... 110
AIX JRE 1.4.2 ..... 111
AIX JRE 1.5.0 ..... 111
ANTLR 2.7.5H3 ..... 112
CentOS 5.6 ..... 113
CPAN Perl 5.8.8 ..... 113
CRC32 ..... 114
Cyrus SASL 2.1.22 ..... 116
dom4j 1.5 ..... 119
Hibernate 3.2 ..... 120
ICU4C 3.4 ..... 121
JBoss 4.0.1 SP1 ..... 122
JBoss Application Server v.4.2.3 ..... 123
JBoss Native v.2.0.6 ..... 124
JDOM 1.0 ..... 125
MD5 Message Digest Algorithm ..... 128
MIT Kerberos v5 r1.5 ..... 130
nss_ldap 2.62 ..... 153
Oracle JDBC Driver 10g Release 2 (10.2.0.1.0) ..... 160
PCRE 6.3 ..... 165
Rhino 1.6r4 ..... 167
SAXPath 1 ..... 168
SHA-1 ..... 171
Sun JDK 1.4.2_13 ..... 172
Sun JDK 1.6.0 ..... 182
Sun JRE 1.5.0_18 ..... 197
XNTP v.3-5.93 ..... 211
XScreenSaver ..... 212
Zlib 1.2.3 ..... 212
ZThread 2.3.2 ..... 213

# Chapter 1: Welcome

Welcome to CA Access Control Premium Edition r12.6.01. This guide describes new enhancements, changes to existing features, operating system support, system requirements, documentation information, installation and general considerations, published solutions, and known issues for CA Access Control Premium Edition.

CA Access Control Premium Edition offers the same functionality and components as CA Access Control. In addition, it offers enterprise management and reporting capabilities, and advanced policy management features.

To simplify terminology, we refer to the product as CA Access Control throughout this guide.

# Chapter 2: CA Access Control Editions

CA Access Control is available in two editions and features vary by product edition:

**CA Access Control**

Contains the core functionality that provides a total security solution for open systems.

**CA Access Control Premium Edition**

Offers the same functionality and components as CA Access Control. In addition, it offers enterprise management and reporting capabilities, advanced policy management features, and CA Enterprise Log Manager for collecting and managing CA Access Control audit logs.

CA Access Control Premium Edition contains Privileged User Password Management (PUPM) to help you manage and audit the tasks performed by privileged accounts. The UNIX Authentication Broker (UNAB) feature lets you manage UNIX users in Active Directory and consolidate your users into a single repository.

## CA Access Control Premium Edition Installation Media

CA Access Control Premium Edition components are available on the following optical discs.

**Note:** CA Access Control Premium Edition installation media is different from that of CA Access Control.

The following optical discs contain endpoint components:

- CA Access Control Endpoint Components for Windows

  Contains CA Access Control for Windows installation files for endpoint components. These include the core CA Access Control functionality required for a standalone Windows computer, additional executables and libraries to extend core functionality (for example, Policy Model support), runtime SDK files and libraries and API samples, mainframe password synchronization, Stack Overflow Protection (STOP), and the PUPM Agent.

- CA Access Control Endpoint Components for UNIX

  Contains CA Access Control for UNIX installation files for endpoint components. These include the core CA Access Control functionality required for a standalone UNIX computer, additional binaries and scripts to extend core functionality (for example, Policy Model support), runtime SDK files and libraries and API samples, mainframe password synchronization, Stack Overflow Protection (STOP), and the PUPM Agent.

  This optical disc also contains UNAB installation files.

The following optical discs contain Enterprise Management Server and Report Portal components for Windows:

- CA Access Control Premium Edition Server Components for Windows

  Contains installation files for CA Access Control Endpoint Management, CA Access Control Distribution Server, and CA Access Control Enterprise Management.

  CA Access Control Enterprise Management includes CA Access Control Endpoint Management, CA Access Control endpoint components for Windows, CA Access Control Distribution Server components, and the Deployment Map Server (DMS).

  This optical disc also includes report packages for import in to CA Business Intelligence.

- CA Access Control Third Party Components for Windows

  Contains a prerequisite installer that installs prerequisite third-party software (JDK and JBoss) on Windows. These software applications are required before you can install CA Access Control Premium Edition Server Components.

The following optical discs contain Enterprise Management Server and Report Portal components for Linux:

- CA Access Control Premium Edition Server Components for Linux

  Contains installation files for CA Access Control Endpoint Management, CA Access Control Distribution Server, and CA Access Control Enterprise Management.

  CA Access Control Enterprise Management includes CA Access Control Endpoint Management, CA Access Control endpoint components for Linux, CA Access Control Distribution Server components, and the Deployment Map Server (DMS).

  This optical disc also includes report packages for import in to CA Business Intelligence.

- CA Access Control Third Party Components for Linux

  Contains prerequisite third-party software (JDK and JBoss) for Linux. These software applications are required before you can install CA Access Control Premium Edition Server Components.

# CA Access Control Installation Media

CA Access Control components are available on the following optical discs.

**Note:** CA Access Control Premium Edition installation media is different from that of CA Access Control.

The following optical discs contain endpoint components:

- CA Access Control Endpoint Components for Windows

  Contains CA Access Control for Windows installation files for endpoint components. These include the core CA Access Control functionality required for a standalone Windows computer, additional executables and libraries to extend core functionality (for example, Policy Model support), runtime SDK files and libraries and API samples, mainframe password synchronization, and Stack Overflow Protection (STOP).

- CA Access Control Endpoint Components for UNIX

  Contains CA Access Control for UNIX installation files for endpoint components. These include the core CA Access Control functionality required for a standalone UNIX computer, additional binaries and scripts to extend core functionality (for example, Policy Model support), API libraries and samples, mainframe password synchronization, and Stack Overflow Protection (STOP).

  This optical disc also contains UNAB installation files for use with CA Access Control Premium Edition.

The following optical discs contain server components for Windows:

- CA Access Control Server Components for Windows

  Contains CA Access Control Endpoint Management for Windows.

- CA Access Control Third Party Components for Windows

  Contains an installer that installs prerequisite third-party software (JDK and JBoss) on Windows. These software applications are required before you can install CA Access Control Endpoint Management.

The following optical discs contain server components for Linux:

- CA Access Control Server Components for Linux

  Contains CA Access Control Endpoint Management for Linux.

- CA Access Control Third Party Components for Linux

  Contains prerequisite third-party software (JDK and JBoss) for Linux. These software applications are required before you can install CA Access Control Endpoint Management.

# Complementary CA User Activity Reporting Module License

As the owner of the CA Access Control Premium Edition, you are also entitled to the CA User Activity Reporting Module product for the limited use of collecting, managing and reporting on CA Access Control audit logs. First, you must obtain a license for “CA User Activity Reporting Module Server for CA Access Control” (Codes ELMSAC99100/ELMSAC991), which is offered to CA Access Control Premium Edition customers for a symbolic price.

To obtain your license for CA User Activity Reporting Module in North America, contact your local account representative. If you are outside of North America, call your local account representative or the local CA Technologies office. You can download CA User Activity Reporting Module online through the Download Center on the CA Support Online web site at http://ca.com/support under your CA Access Control Premium Edition download links.

# A Single Documentation Set for All Editions

We supply the same documentation for both editions. Because of that, some sections of some guides apply only to CA Access Control Premium Edition. The following describes how the documentation applies to CA Access Control:

- Release Notes

  Some information in this guide applies only to CA Access Control Premium Edition features.

- Implementation Guide

  Some information in this guide applies only to CA Access Control Premium Edition features.

- Enterprise Administration Guide

  The entire guide applies only to CA Access Control Premium Edition.

- Upgrade Guide

  Some information in this guide applies only to CA Access Control Premium Edition features.

- Implementation Guide

  This entire guide applies to CA Access Control Premium Edition.

- Endpoint Administration Guide for Windows

  The entire guide applies to CA Access Control.

- Endpoint Administration Guide for UNIX

  The entire guide applies to CA Access Control.

- Reference Guide

  Some information in this guide applies only to CA Access Control Premium Edition features.

- selang Reference Guide

  Some information in this guide applies only to CA Access Control Premium Edition features.

- Troubleshooting Guide

  Some information in this guide applies only to CA Access Control Premium Edition features.

To simplify terminology, we refer to the product as CA Access Control throughout the documentation.

# Chapter 3: New and Changed Features

This section contains the following topics:

CA Access Control Enterprise Management and CA Access Control Enhancements (see page 21)
UNAB Enhancements (see page 22)
PUPM Enhancements (see page 23)
Documentation Enhancements (see page 25)
Fixed Issues in This Release (see page 25)

## CA Access Control Enterprise Management and CA Access Control Enhancements

The following CA Access Control Enterprise Management and CA Access Control enhancements and fixes were made since the last release:

- **Load Balancing Enterprise Management Server**

  Load Balancing Enterprise Management Server has been added to CA Access Control to manage environments where heavy transactions take place. The Load Balancing Enterprise Management Servers enable CA Access Control customers to use a common user and policy stores to distribute workload among the Enterprise Management Servers.

- **LDAP Network Groups Support**

  Added support for netgroup over LDAP to enable CA Access Control policy to allow using netgroups for policy evaluation.

  **Note**: User netgroups are mapped into the user XGROUPS. CA Access Control does not connect to the users directory, rather CA Access Control uses the native OS LDAP to retrieve netgroups information.

- **Policy Management over Message Queue**

  An alternative JMS (Java Messaging Service) protocol is now available which enables better policy distribution for large CA Access Control end point environments.

- **Memory Monitoring**

  Added memory monitoring capability to monitor the daemons memory consumption. Use the command secons -i to display the current memory use.

- **Crash Guard**

  Added a process on CA Access Control for Windows to collect support-related files after a system malfunction occurred.

# UNAB Enhancements

The following UNAB enhancements and fixes were made since the last release:

- **One-Way Trust**

  Added one-way trust support to enable users to log in from domains that have established a one-way trust only.

- **Agent Process Monitoring**

  Added memory size and number of open files monitoring capability. You can view the current memory consumption by running the command uxconsole -status -detail.

- **Agent Self-Healing Option**

  UNAB agent self-healing is now available. The self-healing controls the UNAB agent process and restarts, diagnoses process memory, number of open files, Active Directory connectivity, and process parameters. The daemon automatically initiates auto-restart to restore normal agent functionality.

- **View Enterprise Policy Deployed to Endpoint**

  View enterprise policy that is deployed to the endpoint by running the command uxconsole –manage –show –policy.

- **Restrict Partial User to Use Active Directory Password**

  Added ability to restrict a partial user to log in using an Active Directory password.

- **Change Active Directory Password Using uxconsole**

  You can now change an Active Directory user password using the command uxconsole –krb –passwd.

- **Mapping UNIX Users**

  You can map UNIX users easily using the command uxconsole –map. This command enables you to add, delete, show users map, and to define users as local exceptions.

- **Flexible Debug Capability**

  Debugging is flexible as UNAB PAM and NSS debug data are collected in the syslog and the UNAB debug files. Enable debugging for the UNAB agent by running the command uxconsole –debug.

# PUPM Enhancements

The following PUPM enhancements and fixes were made since the last release:

- **Manage Open Sessions for Privileged Accounts**

  PUPM has been enhanced to deny checking out or checking in privileged accounts if the account is logged in (open session) a target end point. A PUPM administrator can configure open sessions for every PUPM account. The following endpoint types support the open sessions feature:

  - Windows Agentless
  - SSH Device
  - Oracle Server
  - Microsoft SQL
  - Sybase Server
  - Network Devices

- **RACF Connector Enhancement**

  The RACF connector has been enhanced to run through the JCS. The RACF connector is supported through SSL.

  The administrator who creates the endpoint now requires permission to modify a user and use the NOEXPIRED operand (with PASSWORD or PHRASE). Such users do not have the SPECIAL, OPERATIONS, AUDITOR, or PROTECTED attributes.

- **ACF2 Endpoint Supported**

  PUPM has been enhanced to support an ACF2 endpoint type.

- **Windows Agentless PUPM Connector**

  The Windows agentless PUPM connector has been enhanced to enable better management of Windows endpoints. The enhanced Windows agentless PUPM connector has the following features:

  - Search and filter Active Directory accounts
  - Handle service accounts robustly

  **Note**: You can deploy the Windows Agentless PUPM connector on Windows Distribution Servers only. Install an additional Windows Distribution Server, or use the legacy connector when UNIX Distribution Servers are installed.

- **CA Access Control for PUPM Connector**

  The CA Access Control for the PUPM connector has been enhanced with the following features:

  - The connector does not require a username and password.
  - The configuration procedures have been automated.
  - The connector is less affected by operating system changes and requirements.

- The connector handles service accounts.

- **PUPM Network Device Endpoint**

  PUPM now has a Network Device endpoint to manage network devices.

  **Note**: Currently, the PUPM Network Device connector is certified to work with Cisco 2600 network device only.

- **Privileged Account Request**

  The privileged account request feature has been enhanced to allow a PUPM user to request access for other PUPM users.

- **Multiple Account Request and Approval**

  The privileged account request feature has been enhanced to allow multiple requests to be placed at once. Similarly, a PUPM Approver can approve multiple requests at once.

- **Break Glass Feature Enhancement**

  The break glass feature has been enhanced to prevent access to exclusive accounts who are in operation using break glass.

- **Login Applications Enhancement**

  PUPM now prepopulates the Login Applications screen in CA Access Control Enterprise Management. The following login application types are prepopulated:

  - ORACLE_10G_WEB
  - ORACLE_10XE_WEB
  - ORACLE_11G_WEB
  - PUTTY
  - PUTTY_TELNET
  - RDP
  - RDP_AD

- **Disable Advanced Login While Creating Endpoint**

  An option has been added which disables the Advanced Login option for the specified endpoint.

# Documentation Enhancements

The following documentation enhancements were made since the last release:

- **End-to-End Bookshelf**

  Added an enhanced and expanded CA Access Control bookshelf to enable easy access to documentation and reference materials. Use the End-to-End bookshelf to read the latest scenarios, knowledge base articles, white papers, videos, demos and more.

- **Integration Guide**

  Added a new guide that explains how to integrate CA Access Control with CA and third-party products.

- **Upgrade Guide**

  Added a new guide to help you upgrade from previous versions of CA Access Control and CA Access Control Enterprise Management.

# Fixed Issues in This Release

Fixes included in this release are documented in the Release FIXLIST. You can access the FIXLIST from the CA Access Control Latest Maintenance Release page on CA Support.

# Chapter 4: System Requirements

This section contains the following topics:

Operating System Support (see page 27)
Enterprise Management Server Requirements (see page 27)
Enterprise Management Server Integration Components (see page 28)
CA Access Control Endpoint Management Requirements (see page 29)
Enterprise Reporting Requirements (see page 29)
Distribution Server Requirements (see page 30)
Windows Endpoint Requirements (see page 30)
UNIX Endpoint Requirements (see page 30)
Policy Model Database Requirements (see page 31)
UNAB Requirements (see page 31)

## Operating System Support

For a list of supported operating systems, see the CA Access Control Compatibility Matrix that is available from the CA Access Control product page on CA Support.

## Enterprise Management Server Requirements

The minimum requirements for the Enterprise Server are:

- **Processor**—(Windows) Pentium PC 2.66 GHz; (UNIX) SPARC Workstation 440 MHz
- **Memory**—2-GB RAM
- **Available disk space**—2 GB at an installation directory; 3 GB at %TEMP% (Windows) or /tmp (UNIX); 3-GB swap file; 1.5 GB at the JBoss directory

In addition, install the following software in the Enterprise Server:

- **JDK**—Java Development Kit (JDK) 1.6.30 or higher
- **Application server**—JBoss Application Server version 4.2.3.GA
- **A central database (RDBMS)**—Oracle Database 10g, Oracle Database 11g, Microsoft SQL Server 2005, or Microsoft SQL Server 2008

  **Note:** This central database does not need to be installed on the same computer. For information about system requirements for your RDBMS, see the documentation for your product.

On the end-user computer, you need a minimum screen resolution of 1024 x 768 and the following settings as your web browser:

- **Windows**—Microsoft Internet Explorer 6.x or 7.x or 8.x; or Mozilla Firefox 2.x or 3.0 or 3.5
- **Linux**—Mozilla Firefox 2.x or 3.0 or 3.5

# Enterprise Management Server Integration Components

The Enterprise Management Server supports integration with the following products:

- **Active Directory**—(Optional) An enterprise user store.

  **Note:** You do not need to install the user store on the same computer as the Enterprise Management Server.

- **CA Directory**—(Optional) A CA proprietary user store.
- **Sun ONE**—(Optional) An enterprise user store.

  **Note:** You do not need to install the user store on the same computer as the Enterprise Management Server.

- **Report Portal**—CA Business Intelligence.

  **Note:** You do not need to install this software on the same computer as the Enterprise Management Server. For information about system requirements for the Report Portal, see the *CA Business Intelligence Installation Guide*.

  **Note:** For more information about CA Business Intelligence, see the *CA Business Intelligence Installation Guide*, which is available from CA Technologies Support.

- **CA Enterprise Log Manager**—r12.0

  **Note:** Do not install this software on the same computer as the Enterprise Management Server. For information about system requirements for CA Enterprise Log Manager, see the *CA Enterprise Log Manager Release Notes*.

- **CA Service Desk**—r12.1

  **Note:** You do not need to install this software on the same computer as the Enterprise Management Server. For information about system requirements for CA Service Desk, see the *CA Service Desk Release Notes*.

# CA Access Control Endpoint Management Requirements

The minimum requirements for the CA Access Control Endpoint Management computer are:

- **Processor**—(Windows) Pentium PC 2.66 GHz, (UNIX) SPARC Workstation 440 MHz
- **Memory**—2-GB RAM
- **Available disk space**—2-GB at an installation directory; 3 GB at %TEMP% (Windows) or /tmp (UNIX)

In addition, install the following software in the CA Access Control Endpoint Management computer:

- **JDK**—Java Development Kit (JDK) 1.6.30 or higher
- **Application server**—JBoss Application Server version 4.2.3.GA
- **CA Access Control**—Latest version of endpoint installation

  **Note:** The version of CA Access Control endpoint you install must be the same as the version of CA Access Control Endpoint Management that you plan to install.

On the end-user computer, you need a minimum screen resolution of 1024 x 768 and the following as your web browser:

- **Windows**—Microsoft Internet Explorer 6.x or 7.x or 8.x; or Mozilla Firefox 2.x or 3.0 or 3.5
- **Linux**—Mozilla Firefox 2.x or 3.0 or 3.5

# Enterprise Reporting Requirements

If you use Oracle Database 10g or Oracle Database 11g as your central database (RDBMS), do the following before you install the CA Access Control Enterprise Management:

- Verify that the Oracle host and the CA Business Intelligence host can communicate.
- Install Oracle Client software on the CA Business Intelligence host.
- Verify that the Oracle TNS definition on the CA Business Intelligence host points to the central database.

If you use Microsoft SQL Server 2005 or Microsoft SQL Server 2008 as your central database (RDMBS), do the following before you install the Report Server:

- Verify that the MS SQL host and the CA Business Intelligence host can communicate.

**Important!** If you use Microsoft SQL Server as the reporting database, install the Report Portal on a supported Windows operating system.

# Distribution Server Requirements

The minimum requirements for the Distribution Server computer are:

- **Processor**—Pentium PC 266 MHz
- **Memory**—2 GB RAM
- **Available disk space**—2 GB at installation; 1 GB at %TEMP% (Windows) or /tmp (UNIX)

In addition, the Distribution Server computer must have the following software installed:

- **JRE**—Java Runtime Environment (JRE) 1.5.0_18 or higher

# Windows Endpoint Requirements

The minimum requirements for a CA Access Control Windows endpoint are:

- **Processor**—Intel-based Pentium 4 PC 1.6 GHz
- **Memory**—128 MB RAM
- **Available disk space**—100 MB

In addition, you need disk space for your CA Access Control database, which is the repository of records describing your users and user groups, your protected files and other resources, and the authorizations that permit controlled access to the resources. For example, a database for one thousand users, with one thousand files, and five hundred access rules, occupies approximately 2 MB of disk space.

# UNIX Endpoint Requirements

The minimum requirements for a CA Access Control UNIX endpoint are:

- **Memory**—1 GB RAM (2 GB recommended)
- **Available disk space**—250 MB (300 MB for general installations)

In addition, you need disk space for your CA Access Control database, which is the repository of records describing your users and user groups, your protected files and other resources, and the authorizations that permit controlled access to the resources. For example, a database for one thousand users, one thousand files, and five hundred access rules, occupies approximately 2 MB of disk space.

# Policy Model Database Requirements

In addition to endpoint space requirements, you also need additional disk space for each Policy Model you plan to create on the host. Each Policy Model contains a database so you need to calculate the space requirements in the same manner as you did for your CA Access Control database.

If you are upgrading and have all your Policy Models databases (PMDBs) in place already, record the space each of the PMDBs uses in the *ACInstallDir*/*policy_model_path*/pmdb_name directory before you upgrade. Use the following calculations to estimate the additional disk space you will need for upgrading each PMDB:

- *ACInstallDir*/policies/pmdb_name/subscribers.dat (size) x 2
- *ACInstallDir*/policies/pmdb_name/updates.dat (size) x 5 + 1000 KB

# UNAB Requirements

The minimum requirements for UNAB are:

- **Memory**—128-MB RAM (256 MB recommended)
- **Available disk space**—100 MB

Also, you must have an Active Directory server configured, depending on the installation type:

- Windows Server 2000 SP4, if you have a partial integration installation
- Windows Server 2003 SP2 R2, Windows Server 2008 R2, if you have a full integration installation

Further, complete the following before you install UNAB:

- Verify that the clocks synchronization between the UNIX and Active Directory computers.
- Synchronize the clocks between the Distribution Server and UNAB computers.
- Verify forward and reverse name resolution for UNIX endpoints and domain controllers from both UNIX and Active Directory servers.
- (Optional) Check for UNAB system compliance.

  This check runs automatically when you install UNAB.
- (Optional) If you want to implement full integration mode, install a tool that lets you view and modify the UNIX attributes of Active Directory users and groups.

**Note:** For more information about these prerequisite tasks, see the *Implementation Guide*.

# Chapter 5: Documentation

This section contains the following topics:

Guides (see page 33)

## Guides

The guides for CA Access Control Premium Edition r12.6.01 are as follows:

- Release Notes
- Implementation Guide
- Endpoint Administration Guide for Windows
- Endpoint Administration Guide for UNIX
- Enterprise Administration Guide
- Integration Guide
- Upgrade Guide
- Reference Guide
- selang Reference Guide
- Troubleshooting Guide

**Note:** To view PDF files, you must download and install a Portable Document Format (PDF) reader. The CA Access Control documentation requires Adobe Reader 7.0.7 or later. You can download Adobe Reader from the Adobe website if it is not already installed on your computer.

In addition to the PDF guides, the CA Access Control guides are also available in HTML format and Online Help is accessible from the various web-based interfaces.

# Chapter 6: FIPS Compliance

This section contains the following topics:

FIPS Operational Modes (see page 35)
Unsupported Operating Systems for FIPS-only Mode (see page 35)
FIPS Encryption Libraries (see page 35)
FIPS Algorithms Used (see page 36)
Storage of Keys and Certificates (see page 36)
Features Affected (UNIX) (see page 36)
Features Affected (Windows) (see page 38)

## FIPS Operational Modes

CA Access Control has two FIPS operational modes: FIPS-only and regular. In FIPS-only mode, CA Access Control uses only those cryptographic functions that are FIPS 140-2 compliant. This means that some CA Access Control features are disabled in FIPS-only mode. In regular mode CA Access Control uses both FIPS 140-2 cryptographic functions and non-FIPS compliant functions.

**Note:** To switch between FIPS-only mode and regular, use the *fips_only* configuration setting in the crypto section.

## Unsupported Operating Systems for FIPS-only Mode

FIPS-only mode is not supported on the following CA Access Control supported operating system architectures:

- Linux s390
- Linux Itanium (IA64)
- Solaris x64
- Windows Itanium (IA64)

## FIPS Encryption Libraries

In FIPS-only mode CA Access Control uses the CAPKI encryption library. On UNIX systems it uses the OS encryption library for password encryption (“crypt” method). In regular mode, CA Access Control uses the CAPKI 4.1.2 encryption library in addition to the non-FIPS encryption libraries.

# FIPS Algorithms Used

CA Access Control components use the following cryptographic algorithms. Different components use different algorithms.

- In FIPS-only mode:
  - SSL (TLS 1.0)—client/server communication
  - AES in CBC mode—encryption of PMD update file (Windows), bidirectional password history (Windows)
  - SHA-1—Unidirectional password encryption (Windows), Trusted Programs, policy signatures (advanced policy management)
- In regular mode:
  - CA Access Control r8 SP1 encryption libraries (DES, Triple DES, AES, MD5, and so on)
  - SSL (SSL V2, SSL V3 and TLS 1.0)—client/server communication
  - SHA-1 (from CAPKI)—used for signatures of trusted programs, signatures of policies
  - AES (from CAPKI)—used for password validation when working with bidirectional password history

# Storage of Keys and Certificates

CA Access Control stores keys and certificates as follows.

- Symmetric keys are stored as in eTrust Access Control r8 SP1.
- Certificates (subject certificate, private key, and root certificate) are stored on the file system and protected by CA Access Control.

  **Note:** CA Access Control encrypts the private key using AES symmetric encryption (from the CAPKI libraries) using CA Access Control symmetric key.

# Features Affected (UNIX)

The FIPS operational mode can have an effect on the following CA Access Control UNIX features:

| Feature | Non-FIPS Mode | FIPS Mode |
|---|---|---|
| PMD update file encryption | Default symmetric key encryption (two-way) | Disabled |

| Feature | Non-FIPS Mode | FIPS Mode |
|---|---|---|
| Trusted Programs | CAPKI SHA-1 and MD5 | CAPKI SHA-1 only |
| Bidirectional password encryption | Default symmetric key encryption | Disabled |
| Unidirectional password encryption | Operating system's crypt/bigcrypt method | Operating system's crypt/bigcrypt method |
| PMD TNG command | Default symmetric key encryption | Disabled |
| CA Access Control TNG daemon | Default symmetric key encryption | Disabled |
| LDAP password encryption usage (sebuildla -u -n) | Default symmetric key encryption | Disabled |
| LDAP password encryption generation (seldapcred) | Default symmetric key encryption | Disabled |
| TCP communication | Default symmetric key encryption (two-way) or CAPKI sockets over SSL V2, SSL V3, or TLS V1 | CAPKI sockets over TLS V1 |
| seversion utility | CAPKI SHA-1 | CAPKI SHA-1 |
| Trusted Programs (watchdog and seretrust) | CAPKI SHA-1 | CAPKI SHA-1 |
| Advanced policy management policy distribution | CAPKI SHA-1 signature, and for backwards compatibility, CA Access Control internal SHA-1 signature | CAPKI SHA-1 signature only |
| selogrd encryption | Default symmetric key encryption and MD5 | Disabled |
| sechkey key change | Default symmetric key encryption | Disabled |
| iRecorder log file signature | MD5 encryption | Disabled |
| Report Agent | Enabled | Disabled |
| PUPM Agent | Enabled | Disabled |
| DMS | Enabled | UNAB endpoints management disabled |

**Note:** Where a feature is disabled as a result of the FIPS operational mode, the relevant program prints an error message and exits, or writes the error message to the system log if a non interactive process occurred. For example: Report Agent or PUPM Agent.

# Features Affected (Windows)

The FIPS operational mode can have an effect on the following CA Access Control Windows features:

| Feature | Non-FIPS Mode | FIPS Mode |
|---|---|---|
| PMD update file encryption | Default symmetric key encryption (two-way) | CAPKI AES symmetric key encryption |
| Password history (non-bidirectional) | Saved as CAPKI SHA-1.<br>Password validation with CAPKI SHA-1 and fall through to crypt | Saved as CAPKI SHA-1.<br>Password validation with CAPKI SHA-1 only |
| Password history (bidirectional) | Default symmetric key encryption.<br>Password validation with default symmetric key encryption | CAPKI AES symmetric key encryption.<br>Password validation with CAPKI AES only. |
| sechkey key change, password history | Default symmetric key encryption to decrypt and encrypt password history | CAPKI AES symmetric key encryption to decrypt and encrypt password history |
| sechkey key change, policy model | Default symmetric key encryption to decrypt and encrypt policy model update files | CAPKI AES symmetric key encryption to decrypt and encrypt policy model update files |
| Trusted Programs | CAPKI SHA-1 and MD5 | CAPKI SHA-1 only |
| Mainframe password synchronization | Enabled | Disabled |
| iRecorder | Enabled | Disabled |
| TNG integartion | Enabled | Disabled |
| Advanced policy management policy distribution | CAPKI SHA-1 signature, and for backwards compatibility, CA Access Control internal SHA-1 signature | CAPKI SHA-1 signature only |
| Report Agent | Enabled | Disabled |
| PUPM Agent | Enabled | Disabled |

| Feature | Non-FIPS Mode | FIPS Mode |
|---|---|---|
| DMS | Enabled | UNAB endpoint management disabled |

**Note:** Where a feature is disabled as a result of the FIPS operational mode, the relevant program prints an error message and exits, or writes the error message to the system log if a non interactive process occurred. For example: Report Agent or PUPM Agent.

You should also consider the following:

- When moving from non-FIPS to FIPS, the policy model *cannot* read old commands.
- When moving from FIPS to non-FIPS, the policy model *can* read old commands.
- For non-bidirectional password history, there is no impact when not using crypt in FIPS mode. Crypt is only for backwards compatibility.
- For bidirectional password history, moving from non-FIPS to FIPS, CA Access Control cannot decrypt old passwords.

# Chapter 7: Feature Support Limitations

This section contains the following topics:

IPv6 Support (see page 41)
Windows Endpoint Limitations (see page 41)
UNIX Endpoint Limitations (see page 44)
UNAB Limitations (see page 45)
PUPM Limitations (see page 46)

## IPv6 Support

CA Access Control runs in an IPv4-only environment, an IPv6-only environment, or a mixed environment of both IPv4 and IPv6.

**Note:** (UNIX) selogrd and selogrcd will not work in IPv6-only environments.

CA Access Control does not currently support network access controls on IPv6 networks. This affects the HOST, CONNECT and TCP classes.

You can specify IP addresses to CA Access Control in IPv6 format, except that the mask and match feature of HOSTNET class records requires IPv4 format addresses.

## Windows Endpoint Limitations

This section describes feature support limitations for Windows endpoints.

### x64 Feature Support Limitations

The following are known limitations on Windows 2003 x64:

- Unicenter TNG migration and integration
- Mainframe password synchronization
- Impersonation interception (class SURROGATE functionality), if SurrogateInterceptionMode is set to 1

  **Important!** Impersonation interception is supported on x64, IA64 and x86 platforms by default via the RunAs plug-in (SurrogateInterceptionMode is set to 0).

  **Note:** For more information about the SurrogateInterceptionMode registry setting, see the *Reference Guide*.

## IA64 Feature Support Limitations

The following features are not supported on IA64 platforms:

- Unicenter TNG migration and integration
- Mainframe password synchronization
- STOP
- Report Agent
- PUPM Agent
- SSL
- FIPS 140-2 compliance

## Windows Server 2008 Feature Support Limitations

The following are known limitations on Windows Server 2008:

- Impersonation interception (class SURROGATE functionality), if SurrogateInterceptionMode is set to 1

  **Important!** Impersonation interception is supported on x64, IA64 and x86 platforms by default via the RunAs plug-in (SurrogateInterceptionMode is set to 0).

  **Note:** For more information about the SurrogateInterceptionMode registry setting, see the *Reference Guide*.

## SAN Support

CA Access Control supports a SAN (storage area network) environment when you install CA Access Control on:

- A local file system and use it to protect files on a SAN, when the SAN is accessible from a single host.

  **Note:** If the SAN is accessible from multiple hosts, install CA Access Control on each host that can access the SAN and use each installation to protect files on the SAN.

- A SAN disk, subject to the following limitations:
  - CA Access Control drivers must be installed on the local file system.
  - You must manually start CA Access Control on the SAN disk each time you start or restart the computer. Do not start CA Access Control automatically when you start or restart the computer.

    **Note:** The previous condition only applies when you install CA Access Control on a SAN disk. If you install CA Access Control on a local file system and use it to protect files on a SAN, you do *not* need to manually start CA Access Control each time you restart the computer.

If the SAN is accessible from multiple hosts and CA Access Control is installed on the SAN, and you want to install CA Access Control from a different host to the same location on the SAN, consider the following before you begin:

- The new installation of CA Access Control replaces the existing installation of CA Access Control and overwrites the existing CA Access Control configuration files and database.
- You must stop the existing installation of CA Access Control before you begin the new installation.

## McAfee Entercept Buffer Overflow

The CA Access Control STOP feature is incompatible with the McAfee Entercept buffer overflow technology.

Turn off the CA Access Control STOP feature or the McAfee Entercept buffer overflow protection feature.

## Short File Name Rules (8.3 Format) Are Not Supported

CA Access Control does not support rules created as short file names (8.3 format). When you define any of the following classes, you must enter the full path name of the file or directory:

FILE, PROGRAM, PROCESS, SECFILE, SPECIALPGM

The following is an example of a rule using a full path name:

```
nr file ("C:\program files\text.txt")
```

The following is an example of a rule using a short path name that is *not* supported:

```
nr file ("C:\progra~1\test.txt")
```

# UNIX Endpoint Limitations

This section describes feature support limitations for UNIX endpoints.

## HP-UX Feature Support Limitations

The following are known UNAB and CA Access Control limitations on HP-UX operating systems:

- HP-UX Trusted Computing Base (TCB) is not supported.
- seversion utility does not display SHA-1 signature.

## Unicenter Integration is Not Supported on HP-UX Itanium and RHEL Itanium

Unicenter integration is not supported on HP-UX Itanium (IA64) and Red Hat Linux Itanium IA64.

## PUPM Agent Are Not Supported on Linux IA64

The PUPM Agent is not supported on Linux Itanium (IA64). CA Access Control does not install the PUPM Agent on these operating systems regardless of the selections you make during installation.

**Note:** UNAB is also not supported on Linux IA64.

## SAN Support

CA Access Control supports a SAN (storage area network) environment when you install CA Access Control on a local file system and use it to protect files on a SAN, when the SAN is accessible from the single host where CA Access Control is installed.

**Note:** If the SAN is accessible from multiple hosts, install CA Access Control on each host that can access the SAN and use each installation to protect files on the SAN.

If the SAN is accessible from multiple hosts and CA Access Control is installed on the SAN, and you want to install CA Access Control from a different host to the same location on the SAN, consider the following before you begin:

- The new installation of CA Access Control replaces the existing installation of CA Access Control and overwrites the existing CA Access Control configuration files and database.
- You must stop the existing installation of CA Access Control before you begin the new installation.

**Note:** CA Access Control behavior is unspecified when you install it on a SAN and it is executed from multiple connected hosts.

# UNAB Limitations

This section describes feature support limitations for UNAB endpoints.

## Nested Groups Not Supported For One-Way Trust

The one-way trust feature does not support nested groups.

## Fully Integrated Active Directory Users Not Supported for One-Way Trust

**Valid on HP-UX**

The one-way trust feature does not support fully integrated Active Directory users.

## uxconsole Shows Basic Information For One-Way Trust Domains

The uxconsole shows only basic information for users and groups in the one-way trust domains.

### UNAB Not Supported on Linux IA64

Currently, you cannot install UNAB on Linux IA64 operating system.

### UNAB is not FIPS140-2 and IPV6 Compliant

Currently, UNAB is not FIPS140-2 and IPV6 compliant.

## PUPM Limitations

This section describes feature support limitations for PUPM endpoints and server components.

### PUPM Is Not FIPS140-2 and IPV6 Compliant

Currently, PUPM is not FIPS140-2 and IPV6 compliant.

# Chapter 8: Installation Considerations

This section contains the following topics:

Supported Installation Languages (see page 47)
Windows Endpoint Installation Considerations (see page 48)
UNIX Endpoint Installation Considerations (see page 48)
UNAB Endpoint Installation Considerations (see page 49)
Server Component Installation Considerations (see page 49)

## Supported Installation Languages

You can specify the language in which the Enterprise Management Server and CA Access Control are installed. The following language IDs are supported, you can specify and their respective languages:

The Enterprise Management Server supports the following languages:

- 1033—English
- 1041—Japanese
- 1042—Korean
- 2052—Chinese(Simplified)
- 1031—German
- 1040—Italian
- 1036—French
- 1046—Portuguese(Brazilian)
- 1034—Spanish

  **Note**: You can generate CA Access Control reports in English, Japanese and Korean only.

CA Access Control for Windows, CA Access Control for UNIX and UNAB support the following languages:

- 1033—English
- 1041—Japanese
- 1042—Korean
- 2052—Chinese(Simplified)

# Windows Endpoint Installation Considerations

This section describes items you should consider when installing CA Access Control on Windows endpoints.

## Restart Message Pops Up During Installation, Uninstallation or Upgrade on Windows Server 2008

When you install, uninstall or upgrade CA Access Control on Windows Server 2008, a dialog box may appear informing you that a restart is required after the process is complete. To continue, close the dialog box by selecting OK.

# UNIX Endpoint Installation Considerations

This section describes items you should consider when installing CA Access Control on UNIX endpoints.

## AIX 6.1 Requires TL3 or Later for CA Access Control to Start

**Valid on AIX 6.1**

To load CA Access Control on AIX 6.1, verify that TL3 or later is installed.

## Message Queue for Linux390 Requires J2SE Version 5.0

To use Message Queue functionality on Linux s390 and s390x endpoints, verify that J2SE version 5.0 or later is installed on the endpoint. Message Queue functionality lets you send report data to the Report Portal and audit data to CA Enterprise Log Manager.

**Note:** You may need to configure the java_home configuration setting in the accommon.ini file. For more information, see the *Implementation Guide*.

## Compatibility Library Missing on x86_64bit Linux

By default x86_64 Linux operating systems should not include 32bit compatibility libraries when installed. CA Access Control endpoint requires that the library libstdc++.so.6 exists under the usr/lib directory from rpm libstdc++.

Verify that this library exists on the endpoint before you install CA Access Control.

### CA Access Control Installation and Uninstallation Restarts UNAB

When CA Access Control is installed or uninstalled from an endpoint that UNAB is running on, the UNAB agent, uxauthd, is stopped and started.

### Propagating CA Access Control and UNAB to a New Solaris Zone

When you setup a new Solaris zone, you must complete several post installation steps before the native operating system completely propagate and run the post installation part of the package and you can propagate CA Access Control and UNAB to the new zone.

**Note:** For more information on setting up a new zone correctly, see Sun's System Administration Guide: Solaris Containers--Resource Management and Solaris Zones, which is available at the Sun Microsystems Documentation website.

### Installing CA Access Control on Solaris 11 Limitation

Due to a Solaris 11 limitation, CA Access Control package is not propagated into nonglobal zones during installation. We recommend you to install CA Access Control in each zone individually using the Solaris native packaging tool (pkgadd).

## UNAB Endpoint Installation Considerations

This section describes items you should consider when installing UNAB endpoints.

### UNAB for Linux 390 Requires J2SE Version 5.0 for Remote Management

To remotely manage Linux s390 and s390x endpoints, verify that J2SE version 5.0 or later is installed on the endpoint. Remote management lets you use CA Access Control Enterprise Management to manage UNAB endpoints.

**Note:** You may need to configure the java_home configuration setting in the accommon.ini file. For more information, see the *Implementation Guide*.

## Server Component Installation Considerations

This section describes items you should consider when installing server components (the Enterprise Management Server, CA Access Control Endpoint Management, and Enterprise Reporting).

## Install Primary and Load Balancing Enterprise Management Server on Same Time Zone

When configuring Enterprise Management Server for high availability, verify that both the primary and the load balancing servers are installed on the same time zone.

## Installing Endpoint Management on 64-bit Linux

To install Endpoint Management on a 64-bit Linux server, install CA Access Control Endpoint Management 32-bit version. The 32-bit version is required as Endpoint Management installs a 32-bit web service.

## Special Characters in Administrator Name

**Valid on Windows**

The administrative account user name must not include any special characters. For example: '-' character.

## Supported JDK and JBoss Versions

You can find supported JDK and JBoss versions on the CA Access Control Premium Edition Third Party Components DVDs.

## Prerequisite Kit Installer Considerations

When using the Prerequisite Kit installer utility to install CA Access Control Enterprise Management from the media, after you are prompted to insert the CA Access Control Enterprise Management DVD, you must select Done to continue. You may also need to close the ProductExplorer window that appears when you insert the DVD.

## Superuser Account Required for Server Components Installations

To install any of the CA Access Control server components (such as Endpoint Management and Enterprise Management), you must log in as the superuser (root on UNIX or a member of the Administrators group on Windows).

## RDBMS Connection Fails During Installation if Java Cannot Be Found

During CA Access Control Enterprise Management installation, when it tries to connect to the RDBMS, a connection failure may suggest that java.exe cannot be located.

Make sure that the full pathname to java.exe is in the system's PATH environment variable.

## Enterprise Management Server Installation Does Not Support Spaces in Installation Path

**Valid on UNIX**

Do not enter spaces in the installation path when you install the Enterprise Management Server.

## Set Up CA Access Control Enterprise Management to Work with Active Directory on Another Domain

If you want to work with an Active Directory that is located outside of the domain that you installed CA Access Control Enterprise Management on, you must change the host TCP/IP settings.

**To set up CA Access Control Enterprise Management to work with Active Directory on another domain**

**On Windows**

1. Click Start, Control Panel, Network Connections.

   The Network Connections window appears.

2. Right-click the active network connection and click Properties.

   The Connection Properties dialog appears with the General tab open.

3. Select Internet Protocol (TCP/IP) and click Properties

   The Internet Protocol (TCP/IP) Properties General tab appears.

4. Click Advanced and click the DNS tab in the open dialog.

   The Advanced TCP/IP Settings DNS tab appears.

5. Click Add and enter the IP address of the DNS server of the domain that Active Directory is located on.

6. Select Append these DNS suffices (in order) and click Add to add a suffix.

   The TCP/IP Domain Suffix dialog appears.

7. Enter the domain suffix.

   **Example**: *company.com*

8. Click OK on all open dialogs to confirm your changes and exit.

**On UNIX**

Verify that the DNS server name of the domain that Active Directory is located on is set to the correct value.

To verify that the DNS domain name, open the file /etc/resolv.conf and verify that the domain is set to the correct value.

## CA Access Control Endpoint Management Installation Instructions Refer to Both Editions of CA Access Control

The CA Access Control Endpoint Management installation instructions that are documented in the Installing CA Access Control Endpoint Management chapter of the Implementation Guide apply to both CA Access Control Premium Edition and CA Access Control. Non-CA Access Control Premium Edition users that want to install CA Access Control Endpoint Management should follow these instructions and use the non-Premium Server DVD.

## CA Access Control Endpoint Management Shortcut Points to Port Number 8080

By default, the CA Access Control Endpoint Management installer sets the shortcut to port number 8080. To change the default settings, you must run the CA Access Control Endpoint Management installer directly from the CA Access Control Premium Edition DVD and not from the ProductExplorer.

Use the following command line to define the port to use when installing CA Access Control Endpoint Management:

```
install_EM.exe -DJBOSS_PORT=<18080>
```

Alternatively, you can edit the CA Access Control Endpoint Management shortcut to point to a different port after the installation.

## CA User Activity Reporting Module Supports Only Trusted SSL Connection

When defining the connection settings of the CA User Activity Reporting Module server, define the SSL connection settings. CA User Activity Reporting Module does not support non-SSL connection.

**Note:** For more information about integrating with CA User Activity Reporting Module, see the *Implementation Guide*.

## Special Subscription Needed to View CA User Activity Reporting Module Reports from CA Access Control Enterprise Management

To use view CA User Activity Reporting Module reports from the CA Access Control Enterprise Management interface, apply a special subscription update to your CA User Activity Reporting Module server.

**To apply the subscription update**

1. In CA User Activity Reporting Module, click the Administration tab, the Services subtab, and select the Subscription Module.
2. Provide the following RSS feed URL:

   `http://securityupdates.ca.com/CA-ELM/r12/OpenAPI/RSSFeed.xml`
3. Download and apply all of the modules to CA User Activity Reporting Module.

   You can now view CA User Activity Reporting Module reports from CA Access Control Enterprise Management.

## Synchronize the System Time of the CA Access Control Enterprise Management and Report Portal Computers

If you install the Report Portal on a separate computer to CA Access Control Enterprise Management, you must synchronize the system time of the computers. If you do not synchronize the system times, reports that CA Access Control Enterprise Management generates will remain in a pending or recurring status.

## Uninstall Fails if You Are Not the Superuser

To uninstall any of the CA Access Control server components (such as Endpoint Management and Enterprise Management), you must log in as the superuser (root on UNIX or Administrator on Windows). If you are not logged in as the superuser, the uninstall fails.

# Chapter 9: Upgrade Considerations

This section contains the following topics:

Versions You Can Upgrade From (see page 55)
Windows Endpoint Upgrade Considerations (see page 56)
UNIX Endpoint Upgrade Considerations (see page 56)
Server Component Upgrade Considerations (see page 57)

## Versions You Can Upgrade From

You can upgrade your CA Access Control endpoints to r12.6.01 from the following versions:

- r12.6
- r12.5.5
- r12.5 SP4
- r12.5 SP3
- r12.5 SP2
- r12.5 SP1
- r12.5
- r12.0 SP1
- r12.0
- Any r8 SP1 CR

You cannot upgrade your CA Access Control endpoints to r12.6.01 from the following versions:

- r8 SP1 GA

  To upgrade an r8 SP1 GA endpoint, install the latest CR for r8 SP1 before you upgrade to r12.6.01.

- r5.2 and r5.3

  To upgrade an r5.2 or r5.3 endpoint, install the latest CR for r8 SP1 before you upgrade to r12.6.01.

# Windows Endpoint Upgrade Considerations

This section describes items you should consider when upgrading CA Access Control on Windows endpoints.

## Reboot May Be Required When Upgrading

When you upgrade an endpoint to this release from r12.0 SP1 or later, it is not mandatory that you reboot the computer. After the upgrade, CA Access Control preserves backwards compatibility. However, the upgrade is not complete until you reboot the computer, and all new functionality may not be supported until after the reboot.

When you upgrade an r8.0 SP1 or r12.0 endpoint to this release, you must reboot the computer.

## Change in Default Access to Database

The default access to seosdb, the CA Access Control database, is now none. In r12.5 SP2 and earlier, the default access to the database was read.

**Note:** CA Access Control internal processes have full access to the database and the NT AUTHORITY\System user has read access to the database.

# UNIX Endpoint Upgrade Considerations

This section describes items you should consider when upgrading CA Access Control on UNIX endpoints.

## Default Installation Location

The default installation location has changed in r12.0 and is as follows:

```
/opt/CA/AccessControl
```

## FIPS 140-2 Library Upgrade

This release of CA Access Control uses CAPKI 4.1.2 instead of ETPKI 3.2. The upgrade is automatic and keeps the ETPKI 3.2 libraries on your computer if they are used by other components. To determine whether other components are using ETPKI 3.2, CAPKI uses an internal reference count. When this count equals 0, ETPKI 3.2 uninstalls on upgrade.

## Systemwide Audit Mode for UNIX Upgrades

The SYSTEM_AAUDIT_MODE property in the SEOS class specifies the default audit mode for users and enterprise users (systemwide audit mode). When you upgrade to CA Access Control r12.5 SP1 or later, CA Access Control sets the value of the SYSTEM_AAUDIT_MODE property to the value of the DefaultAudit configuration setting in the [newusr] section of the lang.ini file.

**Note:** The default value of both the SYSTEM_AAUDIT_MODE property and the DefaultAudit configuration setting is Failure LoginSuccess LoginFailure.

## Authorization Recognizes Resource Group Ownership

CA Access Control takes into account resource group ownership when checking user authorization to a resource. This behavior was introduced in r12.0. In earlier releases, the authorization process considered only the resource's owner.

For example, you define a FILE resource with a default access of none and no owner that is a member to a GFILE resource with a named owner. In CA Access Control r12.0 and later, the named group owner has full access to the file. In earlier releases, nobody has access to the file.

## syslog Messages That Have a Reduced Priority

The following syslog messages have been reduced to informational priority (INFO rather than ERROR):

- CA Access Control daemon going down.
- START-UP: CA Access Control PID=%d
- SEOS_load: use_streams=$use_streams unload_enable=$unload_enable
- Loading CA Access Control kernel extension.
- $prodname kernel extension is already loaded.
- Starting $SeosBinDir/seosd daemon. (CA Access Control)
- Watchdog started.
- Watchdog initialized Watchdog extensions.

# Server Component Upgrade Considerations

This section describes items you should consider when upgrading server components (the Enterprise Management Server, CA Access Control Endpoint Management, and Enterprise Reporting).

## Upgrading Enterprise Management Server to r12.6.01 Does Not Preserve Roles and Tasks

**Symptom:**

When I upgrade Enterprise Management Server to r12.6.01, the roles and tasks that I created before upgrading do not appear.

**Solution:**

When upgrading to r12.6.01, the Enterprise Management Server does not preserve roles and tasks. The Enterprise Management Server preserves only membership policies.

## CA Access Control r12.6.01 Requires Hot Fix to Manage Policy Models on CA Access Control r12.5 and r12.0.01

If you are using CA Access Control r12.6.01 Server to manage policy models on CA Access Control r12.5 or r12.0.01 endpoints, then install the following hot fixes:

- For r12.5 endpoint, install hot fix T537526
- For r12.0.01 endpoint, install hot fix T537569

**Note**: For more information, contact CA Support at http://ca.com/support.

## Hot Fix Required Before Upgrade to Use Policies and Host Groups Containing Spaces

**Valid on Linux**

To use policies and host groups with space characters, install the hot fix for the operating system you use, before you upgrade to CA Access Control r12.6.

## Software Patch Required to Deploy Policies on Endpoints

To deploy policies on CA Access Control r12.5 endpoints from CA Access Control Enterprise Management r12.6, you must install patch T537526 on the Enterprise Management Server.

Download the software patch from the CA Support website.

## CA Access Control Enterprise Management Default Encryption Method Set to 256AES

The CA Access Control Enterprise Management default encryption method is set to 256AES and not scramble.

# Chapter 10: General Considerations

This section contains the following topics:

Windows Endpoint Considerations (see page 61)
UNAB Considerations (see page 61)
Server Components Considerations (see page 63)

## Windows Endpoint Considerations

This section describes items you should consider when using CA Access Control on Windows endpoints.

### RunAs Administrator to Start CA Access Control on Windows Server 2008

**Valid on Windows Server 2008**

To start CA Access Control using the command line options (seosd -start), you must have administrator privileges if the User Account Control (UAC) option is enabled. Run the command prompt using the RunAs option and specify a user account with administrative privileges.

### Uninstall Does Not Remove CA License Files

When you uninstall CA Access Control, the CA License files are not deleted. By default, the CA License files are in the CA_license directory (for example, C:\Program Files\CA\SharedComponents\CA_LIC).

## UNAB Considerations

This section describes items you should consider when using UNAB.

### Disable Local User Account After Migration

After fully migrating user accounts to Active Directory, you can disable the local UNIX account by adding an asterisk (*) at the beginning of the account entry in the etc/passwd file.

## Do Not Set the unab_refresh_interval Token Value to a Short Interval

To avoid performance issues in UNAB, do not set the value of the unab_refresh_interval token value to a short interval.

## Do not Set Kerberos dns_lookup_realm to True

**Valid for SSO mode**

We recommend that unless required, do not set the Kerberos dns_lookup_realm value to true. When set to true, Kerberos initiates unnecessary DNS searches that can result in a substantial slowdown of UNAB login processing.

## UNAB Users Cannot Change Account Password According to Specified Password Policy

If UNAB users cannot change their account passwords, verify that the Domain Controller security policy you use does not prohibit users from changing their account passwords.

## sepass Integration with UNAB Endpoints

The sepass utility is integrated with UNAB. The integration lets users change their Active Directory passwords on endpoints on which both CA Access Control and UNAB are installed.

To integrate sepass with UNAB:

- Verify that you set the "change_pam" token value, in the seos.ini file, to **yes.** Configure this token to instruct sepass to change passwords using the PAM interface.
- Verify that you set the "auth_login" token value, in the seos.ini file, to **pam.** Configure this token to instruct sepass to validate existing passwords using the PAM interface.

**Note:** For more information about seos.ini initialization file tokens, see the *Reference Guide*.

## Log In to UNAB with Active Directory Account

If you want to log in to UNAB with an Active Directory account that did not previously exist on the local host, follow these steps:

1. Register the UNAB host with Active Directory as follows:

   ```
   uxconsole -register
   ```

2. Activate UNAB as follows:

   ```
   uxconsole -activate
   ```

3. Create a UNAB login authorization (login policy) or local login policy (users.allow, users.deny, groups.allow, groups.deny) to enable Active Directory users to log in.

## You Cannot Log In to CA Access Control for UNIX Using 'Administrator' Account When UNAB Is Installed

You cannot log in to a CA Access Control endpoint for UNIX with the 'Administrator' Active Directory user account if UNAB is installed on the endpoint. To work around this problem, you can create userPrincipleName for this account.

## CA Access Control Installation and Uninstallation Restarts UNAB

When CA Access Control is installed or uninstalled from an endpoint that UNAB is running on, the UNAB agent, uxauthd, is stopped and started.

# Server Components Considerations

This section describes items you should consider when using CA Access Control server components (CA Access Control Endpoint Management, CA Access Control Enterprise Management, and Enterprise Reporting).

## Communication Issues between CA Access Control Components and CA Access Control Message Queue

The following CA Access Control components rely on communications with the CA Access Control Message Queue for some functionality:

- Enterprise Management Server
- Report Agent
- DMS
- DH
- UNAB
- PUPM Password Consumers
- Agent Manager

These components may not be able to communicate with the Message Queue if it is not running, the configuration options are not set correctly for the Message Queue host or queue, or a generic network error is present.

If communication between any of these components and the Message Queue cannot be established or breaks down, the communication does not resume automatically when the problem is fixed. To work around this issue you must fix the communication issue and then restart the CA Access Control component.

## CA Access Control Host Name Limitation

The host name of the CA Access Control endpoint must be 15 characters or less. If the host name of the CA Access Control computer exceeds 15 characters, you cannot use CA Access Control Endpoint Management to log into the endpoint.

## Automatic Generation of Policy Undeploy Script

When you undeploy a policy that does not have an associated undeploy script, CA Access Control automatically generates the required script to remove the policy. This script is based on the deployment script.

If you want to remove the policy but *keep* the policy rules (from the deployment script), provide an undeployment script with a rule that does not modify anything (for example, er GPOLICY *policyName*).

## Specify the PUPM Endpoint NETBIOS Name and Not the DNS Domain Name

When you create a PUPM endpoint in CA Access Control Enterprise Management, the host name that you specify in the Name field must match the host name that appears in World View.

If the endpoint is an Active Directory endpoint, specify the NETBIOS domain name in the Host Domain field. If the endpoint is not an Active Directory endpoint, specify the NETBIOS host name in the Host Domain field, not the DNS domain name. For example, if an endpoint is not an Active Directory endpoint, specify the NETBIOS host name (ACSERVER) in the Host Domain field and not the endpoint DNS domain name (acserver.company.com).

If you specify the DNS domain name, advanced features, such as PUPM Automatic Login, fail.

## You Cannot Configure More Than a Single CA Identity Manager Provisioning Connector Server

Do not configure more than a single CA Identity Manager provisioning connector server in CA Access Control Enterprise Management.

## Cannot Configure CA Identity Manager Provisioning Connector Server Using SSL Port

When you configure an CA Identity Manager provisioning connector server, do not specify the CA Identity Manager provisioning server SSL port (20390). If you specify the connector server SSL port, the connection to the connector server fails.

## Cannot Use PUPM to Change Password for the Expert Account

If you use a Check Point firewall on an SSH endpoint, you cannot use PUPM to change the password for the expert account on the endpoint. This restriction means that the expert account must be a disconnected account in PUPM.

## SQLCMD Utility Does Not Support Blank Passwords

**Valid on SQL Server**

The SQL Server command utility sqlcmd does not support blank passwords. If you defined the SQL Server endpoint as a password consumer in CA Access Control Enterprise Management and check out a password from PUPM, do not leave the password field empty. You can specify the account password or any other string as the password.

# Chapter 11: Known Issues

This section contains the following topics:

Installation Known Issues (see page 67)
Upgrade Known Issues (see page 70)
General Known Issues (see page 70)

## Installation Known Issues

This section describes installation known issues for CA Access Control components.

### Windows Endpoint Installation Known Issues

This section describes installation known issues for Windows endpoints.

#### "No Valid Source Could Be Found" Message When Installing From MSI File

A "no valid source could be found" message appears when you upgrade CA Access Control. The message appears if the media that you currently use and the media that was originally used to install CA Access Control have the MSI file at different paths.

To work around this issue, add a registry string named "MediaPackage" and specify the relative path to the CA Access Control msi package. Add the registry string in the following path:

```
HKLM\Software\Classes\Installer\Products\
CDAFB228040EC5F40AA08B5E852A6D61\SourceList\Media
```

For example, if you install CA Access Control on a 32-bit Windows operating system, the full path to the msi file is: E:\x86\, where E: is the removable media drive. In the MediaPackage value you specify the value: \x86\

### UNIX Endpoint Installation Known Issues

This section describes installation known issues for UNIX endpoints.

## Uninstalling Fails When Native Installation Is Customized to Install CA Access Control and UNAB in The Same Non-Default Location

**Valid on AIX, and HP-UX**

**Symptom:**

Uninstalling CA Access Control fails after I installed CA Access Control and UNAB using native installation and customized the installation directory to the same path on a nondefault location.

**Solution:**

Uninstalling CA Access Control corrupts and fails the UNAB installation. Uninstalling fails as both CA Access Control and UNAB have been installed on the same directory. While customizing native installation to a nondefault destination folder, we recommend that you concatenate the product name (AccessControl or AC) to the destination path CA Access Control installation.

## RPM Package Verification May Return Errors

When verifying RPM package installations you may receive some verification errors.

These errors do not indicate that there are issues with the functionality of the installed product and you can safely ignore them.

## Client-Server Communication Mode Incompatibility

A client set up with non_ssl or all_modes cannot communicate with a server set up with fips_only communication mode.

## API Libraries for Linux Z-series Are 32-bit

The API libraries that CA Access Control supplies for Linux Z-series (s390x) are 32-bit.

CA Access Control does not supply 64-bit libraries for Linux Z-series (s390x).

## HP-UX requires an Updated Patch Level

On HP-UX, CA Access Control requires an updated patch level to install properly. We recommend the following OS patches:

- 11.23 on IA64—Patch PHSS_37492 or OS QPK1123 Bundle that is dated September 2006 or later.
- 11.11 on PA-RISC—OS Path with support for "dld_getenv" or OS QPR Bundle dates December 2006 or later.
- 11.23 on PA-RISC—OS QPK Bundle that is dated December 2006 or later.

### PAM Does Not Work on Linux s390x with Older /lib64/libc.so.6 Library

PAM on Linux s390 and s390x does not work if the /lib64/libc.so.6 library on the host is older than the version CA Access Control PAM library was compiled with.

The library version should be 2.3.2 or later.

## UNAB Endpoint Installation Known Issues

This section describes installation known issues for UNAB endpoints.

### UNAB Restarts Twice When Installing CA Access Control

**Valid on IBM AIX**

When installing CA Access Control on IBM AIX and UNAB is already running, UNAB restarts twice. This behavior is because AIX performs additional Kernel checks.

### Uninstalling Fails When Native Installation Is Customized to Install CA Access Control and UNAB in The Same Non-Default Location [UNAB]

**Valid on AIX, and HP-UX**

**Symptom:**

Uninstalling UNAB fails after I installed CA Access Control and UNAB using native installation and customized the installation directory to the same path on a nondefault location.

**Solution:**

Uninstalling CA Access Control corrupts and fails the UNAB installation. Uninstalling fails as both CA Access Control and UNAB are installed on the same directory. While customizing native installation to a nondefault destination folder, we recommend that you concatenate the product name (uxauth or UNAB) to the destination path.

### Installing SElinux Extensive Policy Twice Shows An Incorrect Message

**Symptom:**

If you install the SElinux extensive policy over an existing SElinux extensive policy on UNAB, then the following message appears:

```
Policy successfully installed
```

**Solution:**

The message is incorrect as UNAB has already installed the SElinux extensive policy.

### UNAB Does Not Support CA Access Control r8.0 SP1 and r12.0 SP1

Currently, you cannot install UNAB on CA Access Control r8.0 SP1 and r12.0 SP1 endpoints. Also, UNAB and CA Access Control must be of identical version or service pack.

# Upgrade Known Issues

This section describes upgrade known issues for CA Access Control components.

## Windows Endpoint Upgrade Known Issues

This section describes upgrade known issues for Windows endpoints.

### "Insufficient Privileges to Modify File" Message Appears During Upgrade

If you upgrade a CA Access Control endpoint and a message appears that informs you that the installer has insufficient privileges to modify a file, acknowledge the message and continue with the upgrade.

## UNIX Endpoint Upgrade Known Issues

This section describes upgrade known issues for UNIX endpoints.

### seaudit, sebuildla Permission Denied Messages After Upgrade

**Valid on AIX**

After you upgrade using the native package, you may receive permission denied error messages when using the seaudit and sebuildla utilities.

To work around this problem, re-trust the utilities after the upgrade completes.

### Pre-r12.0 Versions Must Use a Maximum of 54 Characters for the Encryption Key

If your environment includes versions of CA Access Control earlier than r12.0, you must use a maximum of 54 characters for the encryption key.

# General Known Issues

This section describes general known issues for CA Access Control components.

# Windows Endpoint Known Issues

This section describes known issues for CA Access Control for Windows.

## Audit Filter in CA Access Control Endpoint Management Causes Performance Degradation

Applying a filter on the audit records in CA Access Control Endpoint Management may lead to performance degradation if CA Access Control Endpoint Management cannot find the specified records. This performance degradation applies to very large audit files and is limited to the client who requested the audit records.

For example, if you defined the audit records filter to display the last 100 related records of a specific FILE resource and the audit file contains less than 100 records, CA Access Control Endpoint Management will repeat the request indefinitely.

## Microsoft Internet Explorer 7.0 Compatibility Issues with CA Access Control

Due to compatibility issues of Microsoft Internet Explorer 7.0 with CA Access Control, the browser may stop responding. To work around the issue, Install Microsoft Internet Explorer 8.0 or do the following:

**Important!** Apply Microsoft software patch KB957388 before you begin this procedure. You can download the software patch from the Microsoft web site.

1. Stop all CA Access Control services.
2. Open a command line window and run the following command:

   ```
   net stop cainstrm
   ```

3. Open the regedit utility from the Run command line window.
4. Navigate to the following path:

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSset\Services\cainstrm\parameters
   ```

5. Modify the ExcludeProcess registry entry value to include the iexplorer.exe file.
6. From the command line window, run the following command:

   ```
   net start cainstrm
   ```

7. Start the CA Access Control services.

## Privileged Processes Can Save and Restore a Registry Tree Without Authorization

On Window Server 2003 and later, when a process obtains the special privileges SE_BACKUP_NAME and SE_RESTORE_NAME, it can save and restore a registry tree without CA Access Control authorization.

### FIPS Only Mode on Windows x64

CAPKI 4.1.2 is now supported on x64 CA Access Control endpoint for Windows. However, due to a known issue with RSA, when running the CAPKI 4.1.2 in FIPS enabled mode, communication is significantly delayed.

### Rename HOST Event in selang Marked as Unknown Event in CA Enterprise Log Manager Reports

A rename HOST event performed in selang is displayed as an unknown event in CA Enterprise Log Manager reports.

### Uninstall Does Not Remove Data and Log Directories

When you uninstall CA Access Control, the Data and Log directories are not removed. By default, the Data and Log directories are in the following location:

```
\Program Files\CA\AccessControl\
```

## UNIX Endpoint Known Issues

This section describes known issues for CA Access Control for UNIX.

### CAWIN Installation Requires Ncurses

**Valid on Linux 64-bit Server**

Install Ncurses 32-bit before installing CAWIN on Linux 64-bit servers.

### Define Fully Qualified Name For CA Access Control Administrator

**Valid on Linux**

When creating an *AC for PUPM* endpoint type on Linux, verify that the CA Access Control Administrator user name is defined as a fully qualified name. For example, computer-name\user-name, or entmcomputer\root.

## CAWIN Installation Fails on a Minimal Linux x64 Installation

**Valid on Linux x64**

The CAWIN installation fails when installed on a minimal Linux x64 installation. The installation fails because of a missing 32 bit library.

**Note**: CAWIN is part of CA Access Control installation. CAWIN related error messages are logged in the CA Access Control installation log file.

To workaround this issue, install the 32 bit ncurses RPM package with the libncurses.co file. Verify that the package version is not below version 5.0. For example:

```
ncurses-devel-5.7-3.20090208.el6.i686.rpm
```

## Failed Login Events Not Audited When serevu Daemon Running

**Valid on VMware vCenter 4.0 u2**

When CA Access Control is installed on VMware vCenter version 4.0 u2, the following occurs when the serevu daemon is running:

- A LOGIN records for failed login events do not appear in audit file
- The pam_seos_failed_login.log file size is 0

To work around this issue, do the following:

1. Stop all CA Access Control daemons.
2. Navigate to the following directory:

   ```
   /etc/pam.d/
   ```

3. Edit the system-auth file to remove all references to pam_seos.so. For example:

   ```
   account required pam_per_user.so /etc/pam.d/login.map
   auth required pam_per_user.so /etc/pam.d/login.map
   password required pam_per_user.so /etc/pam.d/login.map
   session required pam_per_user.so /etc/pam.d/login.map
   ```

4. Edit the system-auth-generic file to add reference to pam_seos.so. For example:

   ```
   password  sufficient  pam_seos.so
   auth       optional     pam_seos.so
   account    optional     pam_seos.so
   session    optional     pam_seos.so
   ```

5. Edit the system-auth-local file to add references to pam_seos.so. For example:

   ```
   password  sufficient  pam_seos.so
   auth       optional     pam_seos.so
   account    optional     pam_seos.so
   session    optional     pam_seos.so
   ```

6. Save and close the files.
7. Start CA Access Control daemons.

## SSH Login Not Audited by CA Access Control or by Audit Log if SElinux Enabled

**Valid on RedHat Linux Advanced Server 6**

On RedHat Linux Advanced Server 6, SSH user log ins are not audited by CA Access Control because the SElinux default policy does not allow SSHD to access the /proc file system.

To workaround this issue, run the /opt/CA/AccessControl//lbin/sshd_policy.sh script to load a SElinux policy module to allow access to /proc.

## Cannot Configure JBoss JDBC Password Consumer on Linux

**Valid on Linux**

Currently, you cannot configure a JBoss JDBC password consumer on LInux.

## Log in to CA Access Control Requires PAM_Login Flag Enabled

**Valid on AIX**

If the PAM_login flag is not enabled, CA Access Control cannot detect the Active Directory user account correctly.

To work around this problem, enable the PAM_login flag in the log in program (LOGINAPPL) you set. Verify that seosd daemon accepts log in requests from PAM modules by setting the PamPassUserInfo token to 1 in seos.ini under the [pam_seos] section.

## User Sessions Are Not Logged when Default Shell Is Not Defined in /etc/shells

**Valid for Keyboard Logger**

CA Access Control does not record user sessions when a user logs in with a shell that is not defined in /etc/shells.

## When PAM is Active segrace Is Not Called for FTP and SSH Grace Login

When PAM is activated, segrace is not called automatically for a grace login to FTP and SSH services.

To work around this issue on FTP, change the value of the LOGINFLAGS property to nograce in the LOGINAPPL record for the FTP service.

To work around this issue on SSH, do not call segrace from PAM. Instead, call segrace from the user or operating system startup script.

## CA Access Control Does Not Reset Passwords Once the Grace Period Expires

**Valid on HPUX, and AIX**

If UNAB is installed on the CA Access Control endpoint, CA Access Control PAM does not invoke the 'sepass' utility to reset the account password when the user password grace period expires.

This problem affects login applications that use loginflags(pamlogin), for example, SSH login, rlogin, FTP, and Telnet. SSH login is not recognized as a login action by CA Access Control on HPUX and AIX. To work around this problem, use loginflags(none) for SSH login applications.

### Solaris Network Event Bypass Does Not Work for Some Processes

CA Access Control on Solaris does not bypass network events (bypass type PBN of SPECIALPGM records) for processes that start before CA Access Control starts.

### Stat Interception Calls Not Supported on AIX Systems

File access check on a stat system call with the STAT_intercept token set to “1” is not supported on AIX systems.

## UNAB Known Issues

This section describes known issues for UNAB.

### Unable to remove UNAB policy using CA Access Control Enterprise Management

Fixed an issue with UNAB that prevented removing a deployed policy from a Red Hat Linux endpoint from CA Access Control Enterprise Management.

### Trusted User SSH Login Failed on AIX

**Symptom:**

I tried to log in to an AIX 5.3 endpoint using SSH, however the login attempt failed.

**Solution:**

This error is a known IBM issue with several combinations of AIX and SSH versions. The issue has been logged with IBM development as APAR (Authorized Program Analysis Report) number IV10231.

### uxauth Starts Even When watchdog_enabled Token is Set to No

**Symptom:**

When I set the token watchdog_enabled to no and restart UNAB, uxauth starts.

**Solution:**

The watchdog script ignores changes made to the watchdog_enabled token after starting uxauth for the first time. We recommend you to specify *-n* during the registration process, make changes to the token, and start uxauthd.sh script separately.

## Audit Log Records Login With Local Account Password As Attempt Login

**Symptom:**

When I log in to UNAB and my user account is present in the local password file and the Active Directory, the audit log shows the following record:

`<audit_record_date_and_time> A LOGIN map3`

**Solution:**

This is a known issue with UNAB. The audit log records A LOGIN instead of P LOGIN.

## Rlogin Entries Logged Twice

**Valid on Linux**

If you log in to a host that has UNAB installed using rlogin, the login attempt appears in the audit twice.

## Hot Fix for Microsoft Windows Server 2003 to Improve Performace

**Valid on Windows Server 2003 SP1, Windows Server 2003 64 Bit**

LDAP queries fails to return Active Directory queries results for extended search using LDAP_MATCHING_RULE_IN_CHAIN.

To workaround this issue, install the latest service pack for MIcrosoft Windows 2003 Server or disable the UNAB group update during log in by setting the wingrp_update_login token to no.

**Note**: For more information, see Microsoft Knowledge Base article 914828.

## Uxpreinstall Utility Fails to Verify Host Name Resolution

The uxpreinstall utility fails to verify the host name resolution after you install UNAB and before you register with Active Directory.

To work around this problem, use the -d argument to specify the Active Directory domain name. For example:

`./uxpreinstall -d domain_name`

## Telnet and rlogin Programs Not Displayed in Audit Records

**Valid on Linux, HP-UX**

The UNAB audit records do not display the telnet and rlogin login programs. In LInux, the UNAB audit records show "remote" instead of telnet or rlogin. On HP-UX the UNAB audit records show "login" instead of telnet or rlogin.

## Interval between uxconsole -register and -deregister Commands

If you register then deregister a UNAB host in Active Directory, after you register the host, we recommend that you wait the time necessary for domain controller replication before you deregister the host.

**Note**: If you deregister a UNAB host, policies that were not distributed are deleted.

## New Domain User Login May Fail on First Attempt

**Valid for SSH**

If you create a user in Active Directory and the new user immediately tries to log in to a UNAB endpoint, the first login attempt fails but subsequent login attempts succeed. The first login attempt fails because the user is not known to the endpoint. However, during the failed login process, uxauthd updates the local NSS storage with the user information. Subsequent login attempts succeed because the user is now known to the endpoint.

By default, uxauthd updates the user information in the NSS storage every hour. If the new user tries to log in to the endpoint after uxauthd updates the NSS storage, the login succeeds.

## Login Services Bypass PAM on SSO Login

Several login services bypass PAM on SSO login. The login policy is not applied and audit events are not generated.

## Successful Login to Host Generates an Error Message

**Valid for Linux, AIX, HP-UX**

A limitation in the UNIX PAM flow results in logging a successful login to a UNAB host as an error message, indicating that account authentication failed in the syslog file.

## "Given password does not match OS Password" Message When Issuing Check Login Command

**Valid on Linux, HP-UX**

The "Given password does not match OS password" error message appears when you issue the checklogin command for the Active Directory user who is not authorized to log in. This message is displayed instead of the actual login deny message.

## Password Mismatch Message When Changing Password Using sepass

**Valid on AIX 5.3**

A password mismatch error message appears when a mapped user attempts to change an account password using sepass. Regardless of the error message, the account password is changed on Active Directory.

## Active Directory User Cannot Change Password on Solaris

Due to Sun Solaris password limitations, users that are logging in to the UNIX host with Active Directory account, cannot change their account password using Solaris passwd tool. If the user must change the account password on the first login, the user must login from a system other than Solaris.

If UNAB is running on the UNIX host, use the following command to change the local account password:

```
passwd -r files username
```

If CA Access Control is running on the UNIX host, use the sepass utility to change the local account password.

## Impersonating an Active Directory User Does Not Create Audit Record

If you impersonate an Active Directory user using su, the impersonation attempt is not audited.

## sshd Program Name Appears in Audit Records of SFTP Sessions

The audit records of login sessions done using sftp program can display the sshd daemon in the program field and not the sftp program.

## UNAB Entries Contain Blank Fields in Event Viewer

UNAB events are displayed in the Windows Event Viewer with blank fields.

## FTP SSO Login of Enterprise Users Not Audited

**Valid for Solaris**

Kerberized FTP and telnet programs bypass the PAM stack and therefore, UNAB does not audit FTP and telnet SSO logins of enterprise users.

### Deregistering SSO Enabled UNAB Does Not Delete Records from Keytab File

When you deregister a UNAB host that was previously registered with SSO enabled, the computer object is removed from Active Directory, but the corresponding records are not deleted from the keytab file. If you attempt to register the UNAB host again, the Kerberos ticket is not created.

To overcome this problem, we recommend that you do not deregister UNAB hosts, or remove the keytab file if it is used by UNAB hosts only.

### HP-UX Does Not Support @ Symbol in Passwords

**Valid on HP-UX**

Due to an HP-UX limitation, do not use the @ symbol in passwords on HP-UX endpoints.

### HP-UX Does Not Support Fully Qualified Domain Name Login

**Valid on HP-UX**

You cannot log into a HP-UX host with a fully qualified domain name, for example: user@domain.

## Server Components Known Issues

This section describes known issues for CA Access Control server components (CA Access Control Endpoint Management, CA Access Control Enterprise Management, and Enterprise Reporting).

### Incomplete Privilege Account Discovery Process Due to Time Synchronization

**Symptom:**

I ran the account discovery wizard and I the list of privileged accounts is incomplete.

**Solution:**

The issue can occur if there is a time difference between the Enterprise Management Server, the Distribution Server or the CA Access Control endpoint. To resolve this issue, download the publish fix number RO47404 from the Support website.

## PUPM Report Missing Approved Requests History After Upgrade

**Symptom:**

After I upgraded the Enterprise Management Server to r12.6.01, the following reports are missing approved requests history: Privileged Account Requests by Approver, Privileged Account Requests by Endpoint and Privileged Account Requests by Requester.

**Solution:**

To solve this issue download published fix RO47416. To deploy the publish fix, follow the instructions in the readme file included in the hot fix.

## Hot Fix Required to Manage CA Access Control Endpoint Using CA Access Control for PUPM Endpoint Type

**Valid on Linux**

**Symptom:**

I installed the Enterprise Management Server on Linux and I try to discover privileged account on CA Access Control endpoint suing the CA Access Control for PUPM endpoint type. The discovery process fails to detect the administrator account.

**Solution:**

To solve this issue, install publish fix RO47411 on the Enterprise Management Server. To deploy the hot fix, follow the instructions in the readme file included in the hot fix.

## Telnet Session is Not Supported by Open Sessions

**Valid on Windows**

Open session does not detect and recognize the Telnet session as a login. The Telnet session is not supported by open sessions on Windows.

## Login Integration with PUPM Supported on Windows Agentless Endpoint Type Only

**Valid on Windows Agentless Endpoint**

CA Access Control login integration with PUPM is supported on Windows Agentless endpoint only and when class Regval is disabled on the target endpoint.

## Unapproved Privileged Account Requests Not Preserved After Upgrade

**Symptom:**

When I perform a privileged account request and upgrade CA Access Control before approving the request, I receive a null pointer exception after upgrade.

**Solution:**

Perform the upgrade after approving the privileged account request.

## Out of Memory Error:GC Overhead Limit Exceeded

**Valid on UNIX**

The following error message appear in the JBoss server log if the system or garbage collection settings are not properly configured:

```
"java.lang.OutOfMemoryError: GC overhead limit exceeded"
```

To solve this issue, do the following:

1. Stop the JBoss application server.
2. Navigate to the following directory, where JBOSS_HOME indicates the location where you installed JBoss:

   *JBOSS_HOME*\bin
3. Edit the run_idm.bat file.
4. Locate the JAVA_OPTS variable and add the following arguments:

   ```
   " -XX:+UseParNewGC -XX:+CMSParallelRemarkEnabled -XX:+UseConcMarkSweepGC
   %JAVA_OPTS%"
   ```
5. Save the file and exit.
6. Start the JBoss application server.

### Example: the JAVA_OPTS variable

The following example shows the JAVA_OPTS variable after you added the new arguments:

```
set JAVA_OPTS=-Djava.security.policy=.\workpoint_client.policy -Xms512m -Xmx1024m
-XX:MaxPermSize=256m -XX:+UseParNewGC -XX:+CMSParallelRemarkEnabled
-XX:+UseConcMarkSweepGC %JAVA_OPTS%
```

## Default Request Approver Not Configured

**Valid on SunOne**

If you use SunOne user directory, you need to configure the default request approver. You define the default request approver that all privileged account passwords requests are submitted to.

To configure the default request approver, do the following:

1. Log in to CA Access Control Enterprise Management as a System Manager.
2. Select Users and Groups, Tasks, Modify Admin Task.

   The Modify Admin Task: Search Admin Task window opens.
3. Enter Privileged Account Request in the Name field, then click Search.

   CA Access Control Enterprise Management displays the results that match the search criteria.
4. Select the Privileged Account Request and click Select.

   The Modify Admin Task: Privileged Account Request window opens.
5. Navigate to the Events tab and select the workflow process

   The Workflow Process screen opens.
6. In the Default Approver section, select Add Users.

   The Select User screen opens.
7. Enter the name of the user you want to assign as a default approver and select Search.

   CA Access Control Enterprise Management displays the results according to the search criteria.
8. Click Select.

   The user you selected is added as a default request approver.
9. Click OK to exit.

**Note**: The default request approver you defined does not apply to users that you created before you installed the Enterprise Management Server. The default request approver for users that previously existed in the user directory is superamdin.

## "No Managed Connections Available Within Configured Blocking Timeout" Error Message When Running Batch Operations

"Managed Connections Available Within Configured Blocking Timeout" error message received when you run batch tasks. For example, you attempt to run the automatic reset password task on a large group or accounts. The error message indicates that the JBoss application server has exhausted the available connections and cannot complete the task.

To work around this problem you need to increase the number of available connections in the pool:

1. Stop the JBoss application server.
2. Navigate to the following directory, where *JBoss_HOME* indicates the directory where you installed JBoss:

   *JBoss_HOME*/server/default/deploy/
3. Open the file imtaskpersistencedb-ds.xml for editing.
4. Locate the <max-pool-size> tag and set the value to 40.
5. Locate the <idle-timeout-minutes> tag and set the value to 1.
6. Comment out (<!--) the <blocking-timout-millis> tag as follows:

   ```
   <!--blocking-timeout-millis>5000</blocking-timeout-millis-->
   ```
7. Save and close the file.
8. Start the JBoss application server.

   You have increased the number of available connections in the pool. You can now run the task.

## JBoss for Windows Sample Policy Failed to Deploy

The JBoss for Windows sample policy fails to deploy on an endpoint. The policy deployment process terminates with an internal error message indicating that a PROGRAM resource already exists.

To work around the problem, use the JBoss sample policy and modify the policy before you deploy it to create PROGRAM resources explicitly.

## Error Message Displayed When Viewing Policy Management Reports in CA Access Control Enterprise Management

CA Access Control Enterprise Management displays a message that the task failed when attempting to view policy management reports.

To work around this problem, restart the JBoss application server and the CA Business Intelligence server (Report Portal).

## A CA Access Control User Not Defined a Password Cannot Log Into the CA Access Control Enterprise Management Server

An CA Access Control user account without a password cannot log into the CA Access Control Enterprise Management Server.

## Access Roles Are Not Supported in CA Access Control Enterprise Management

When you define admin role rules, select users that are members of admin roles. CA Access Control Enterprise Management does not support access roles. The access roles option should not appear in the interface.

## "No Operation Required" Message When Modifying UNAB Host or Host Group

When modifying UNAB host or host group settings and submitting the changes, CA Access Control Enterprise Management displays the following message: "No operation required". Although this message indicates that no action was taken, the modifications you made to the UNAB host or host group were applied.

## Control Characters May Cause an Application Exception

Control characters in the CA Access Control database may cause an application exception or render incorrectly in CA Access Control Endpoint Management and CA Access Control Enterprise Management.

## Incomprehensible Characters In the User Interface

**Symptom:**

When I log into the CA Access Control Enterprise Management user interface, I see incomprehensible characters.

**Solution:**

The problem is that the database instance you are using does not fully support UTF8 international characters set. To correct this problem, you must reinstall CA Access Control Enterprise Management on a fully internationalized database instance.

## Cannot Change the Trust Property of a Monitored File

In CA Access Control Endpoint Management, clearing the Trust check box on the Audit tab of a monitored file (SECFILE) resource fails when you try to save the changes.

To work around this issue and change this resource attribute, use selang.

## CA Access Control Enterprise Management Time-Out When Creating Large Policies

The CA Access Control Enterprise Management user interface times out when you create a policy that contains more than 6000 commands. You cannot continue working in the user interface until CA Access Control Enterprise Management creates the policy. To work around this problem, open a new session by logging in to CA Access Control Enterprise Management from a new browser.

## Cannot Deploy Policies That Contain a Trailing Backslash

Conventions for selang let you use a backslash character (\) as the last character of a line to indicate that the command continues on the following line. This is not supported by advanced policy management. Make sure that policy commands do not span multiple lines.

**Note:** The following sample policies CA Access Control provides contain a trailing backslash: _AC_WEBSERVICE, _APACHE, _JBOSS, _MS_SQL_SERVER, and _ORACLE.

## Policy Script Validation Error Messages Are in a Different Language

**Valid in CA Access Control Enterprise Management**

If a policy deploys with errors, the selang result messages you see in CA Access Control Enterprise Management are in the installation language of the CA Access Control endpoint on the Enterprise Management server and not that of the CA Access Control Enterprise Management installation.

To see these messages in a localized language, you must install the CA Access Control endpoint on the Enterprise Management computer in the desired localized language before you install CA Access Control Enterprise Management.

## Cannot View Audit Records for Terminals with Names Longer than 30 Characters

You cannot view audit records if the terminal name has more than 30 characters. This happens when CA Access Control Endpoint Management running on a Windows computer manages a UNIX endpoint.

## PMDB Audit Records Are Not Visible When Managing the PMDB

When you manage a PMDB using CA Access Control Endpoint Management, you cannot see the PMDB's audit records.

To work around this issue and view the audit records for the PMDB, connect to host where the PMDB resides.

## Open Session For Network Devices Fails

If the privileged account name contains more than ten characters, open session for Network Devices fails.

## "No Such Method" or "Failed to Reset Password" Error Message for Access Control for PUPM Endpoint Types

**Valid on Linux**

When you install the Enterprise Management Server on a Linux computer, you receive the following error message when you define Access Control for PUPM endpoints: "No Such Method".

If you specify that CA Access Control Enterprise Management resets a privileged account password on check in, when a user checks in a privileged account on an Access Control for PUPM endpoint they receive the following error message: "Failed to Reset Password".

**Follow these steps:**

1. Stop the Java Connector Server. Do the following:
   a. Navigate to the following directory, where *ACServerInstallDir* refers to the directory where the Enterprise Management Server is installed:

      *ACServerInstallDir*/Connector_Server/bin

   b. Run the following command:

      ```
      ./im_jcs stop
      ```

      The Java Connector Server stops.
2. Open the im_jcs script for editing.
3. Locate and remove the following line from the script:

   ```
   PREJAR="$FULLBASEPATH/bin/jcs-bootstrap.jar:$FULLBASEPATH/
   conf:$FULLBASEPATH/lib/jcs.jar:"`echo $FULLBASEPATH/
   lib/apacheds-server-main-*-app.jar`
   ```
4. Copy the following line and paste it into the script:

   ```
   PREJAR="$FULLBASEPATH/bin/jcs-bootstrap.jar:$FULLBASEPATH/
   conf:$FULLBASEPATH/lib/jcs.jar:$FULLBASEPATH/
   lib/nlog4j__V1.2.25.jar:"`echo
   $FULLBASEPATH/lib/apacheds-server-main-*-app.jar`
   ```

   **Important!** Delete the carriage returns in the line after you paste it into the script.

5. Save the file.
6. Start the Java Connector Server.

   ```
   ./im_jcs start
   ```

   The Java Connector Server starts. You can now configure the Access Control for PUPM endpoint type.

## Telnet Automatic Login Not Supported on Solaris After Upgarde

**Valid on Solaris**

Currently, Telnet automatic login is not supported on Solaris after you upgarde to CA Access Control r12.6.

## Custom Participant Resolvers Removed After Upgrade

Custom participant resolvers that you configured are removed after you upgraded to CA Access Control r12.6.

We recommend that you make a note of the custom participant resolvers before you upgrade to CA Access Control r12.6 and recreate them once you completed the upgrade.

## Changes to Windows Services and Scheduled Tasks Are Not Discovered

**Valid on Windows Server 2003**

**Symptom:**

When you change a Windows Service or Windows Scheduled Task, the changes cannot be discovered.

**Solution:**

This is a known Microsoft issue. After you change the service or task on the endpoint, delete the existing password consumer. Use the Service Account Discovery Wizard to create a password consumer.

## Approval of Service Account Password Request Fails

After you submit a request for a service account password, the request is not sent to the request approver and you cannot check out the service account password.

## No Audit Record for Password Retrieval by JDBC Password Consumer

The Enterprise Management Server does not write an audit record when a JDBC password consumer gets a password from CA Access Control Enterprise Management.

### Error Message When You Use Automatic Login to Log in to Oracle Enterprise Manager

**Valid on Oracle**

An error message appears when you use the automatic login option to log into the Oracle Enterprise Manager after you checked out an administrator account password. The error message appears if you terminated the last session by closing the browser window without logging off.

### Remote Desktop Connection Fails When Endpoint Prompts for Password

**Valid on Windows**

The Windows Remote Desktop automatic login script fails to log into the endpoint if the endpoint Terminal Services settings are configured to always prompt for password on login.

### PUPM Accepts Ticket Numbers for Closed CA Service Desk Tickets

**Valid for integration with CA Service Desk**

If you specify the number for a closed CA Service Desk issue or request ticket (ticket type=iss or cr) when you request access to a privileged account, CA Access Control Enterprise Management forwards the request to the approver.

### Cannot Specify CA Service Desk Change Order Ticket Number

**Valid for integration with CA Service Desk**

If you specify the number for a CA Service Desk change order ticket (ticket type=ch) when you request access to a privileged account, CA Access Control Enterprise Management does not forward the request to the approver.

## Documentation Known Issues

This section describes known issues for the CA Access Control documentation set.

### No Alternate Text for Graphics In the SDK Guide

There is no alternate text for graphics in the SDK Guide. The SDK Guide was first published with a previous release of CA Access Control and is provided as a courtesy with the CA Access Control r12.5 documentation.

## PDF Documentation Requires Adobe Reader 7.0.7

To read the documentation for CA Access Control in print format (PDF files), you must install Adobe Reader 7.0.7 or later. You can download Adobe Reader from the Adobe website if it is not already installed on your computer.

**Note:** Adobe Reader is not available on HP-UX Itanium (IA64) and Red Hat Linux Itanium IA64.

# Appendix A: Third-Party License Agreements

This section contains the following topics:


Software Under the Apache License (see page 92)
Software Under the Daniel Veillard License (see page 99)
Software Under the OpenLDAP License (see page 101)
Software Under the OpenSSL License (see page 104)
AES 2.4 (see page 110)
AIX JRE 1.4.2 (see page 111)
AIX JRE 1.5.0 (see page 111)
ANTLR 2.7.5H3 (see page 112)
CentOS 5.6 (see page 113)
CPAN Perl 5.8.8 (see page 113)
CRC32 (see page 114)
Cyrus SASL 2.1.22 (see page 116)
dom4j 1.5 (see page 119)
Hibernate 3.2 (see page 120)
ICU4C 3.4 (see page 121)
JBoss 4.0.1 SP1 (see page 122)
JBoss Application Server v.4.2.3 (see page 123)
JBoss Native v.2.0.6 (see page 124)
JDOM 1.0 (see page 125)
MD5 Message Digest Algorithm (see page 128)
MIT Kerberos v5 r1.5 (see page 130)
nss_ldap 2.62 (see page 153)
Oracle JDBC Driver 10g Release 2 (10.2.0.1.0) (see page 160)
PCRE 6.3 (see page 165)
Rhino 1.6r4 (see page 167)
SAXPath 1 (see page 168)
SHA-1 (see page 171)
Sun JDK 1.4.2_13 (see page 172)
Sun JDK 1.6.0 (see page 182)
Sun JRE 1.5.0_18 (see page 197)
XNTP v.3-5.93 (see page 211)
XScreenSaver (see page 212)
Zlib 1.2.3 (see page 212)
ZThread 2.3.2 (see page 213)

# Software Under the Apache License

Portions of this product include software developed by the Apache Software Foundation (http://www.apache.org/).

- Ant 1.6.5
- Axis 1.2.1
- Axis 1.4
- Axis2 1.1.1
- Blowfish encryption N/A
- Commons BeanUtils 1.6.1
- Commons BeanUtils 1.7
- Commons Codec 1.3
- Commons Collection 3.1
- commons dbcp 1.2.1
- Commons Digester 1.7
- commons discovery 0.2
- commons el 1.0
- Commons FileUpload 1.2
- Commons httpclient 2.0.2

  This product includes Jakarta Commons HttpClient 2.0.2 which is distributed in accordance with the following license agreement.
- Commons httpclient 3.0.1
- Commons Lang 2.1
- Commons Logging 1.0.4
- Commons Logging 1.04
- Commons Pool 1.3
- Commons Validator 1.2
- HTTP Web Server 2.0.54
- HTTP Web Server 2.2.3
- JSTL 1.0.6
- Log4j 1.2.8
- myfaces 1.1.4
- ORO 2.0.8
- Slide 2.1

- Struts 1.2.9
- Tofigurator v.1.0

  This product includes Tofigurator v.1.0, which is distributed in accordance with the following license agreement.
- tomahawk 1.1.5
- Tomcat 5.0.28
- Tomcat 5.5.12
- Tomcat 5.5.20

  This product includes Apache Tomcat 5.5.20 which is distributed in accordance with the following license agreement.
- Velocity 1.4
- Xalan-C 1.10.0
- Xalan-C 1.9.0
- Xalan-J 2.6.0
- Xalan-J 2.7.0

  This product includes Apache Xalan-J v.2.7.0, which is distributed in accordance with the following license agreement(s):
- Xerces-C++ 2.6.0
- Xerces-C++ 2.7.0
- Xerces-C++ 2.8.0

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 versions 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

# Software Under the Daniel Veillard License

Portions of this product include software developed by the Daniel Veillard.

- Libxml2 2.6.27
- Libxml2 2.6.7

The libxml2 software is distributed in accordance with the following license agreement:

Except as contained in this notice, the name of Daniel Veillard shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from him.

# Software Under the OpenLDAP License

This product includes software developed by The OpenLDAP Foundation:

- OpenLDAP 2.1
- OpenLDAP 2.3.39 (20071118)

  This product includes software distributed in accordance with the following license agreement:

The software is distributed in accordance with the following license agreement:

The OpenLDAP Public License

Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation

("Software"), with or without modification, are permitted provided

that the following conditions are met:

1. Redistributions in source form must retain copyright statements

   and notices,

2. Redistributions in binary form must reproduce applicable copyright

   statements and notices, this list of conditions, and the following

   disclaimer in the documentation and/or other materials provided

   with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time.

Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS "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 OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE 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 names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

# Software Under the OpenSSL License

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

- OpenSSL 0.9.8.d

  This product also includes libraries from an SSL implementation written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

- OpenSSL 0.9.8h

  This product also includes libraries from an SSL implementation written by Eric Young (eay@cryptsoft.com). This product includes OpenSSL Toolkit v0.9.8h, which is distributed in accordance with the following terms:

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 Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission 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 aheared 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 rouines from the library

*    being used are not cryptographic related :-).

* 4. If you include any Windows specific code (or a derivative thereof) from

*    the 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.]

 */
```

# AES 2.4

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

This software is Copyright 1999,2000 Enhanced Software Technologies Inc.

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 acknowledgement:

   This product includes software developed by Enhanced Software Technologies Inc. and its contributors.

4. Neither the name of the Company 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 COMPANY 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 COMPANY 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.

## AIX JRE 1.4.2

CONTAINS IBM(R) 32-bit Runtime Environment for AIX(TM), Java(TM) 2 Technology Edition, Version 1.4 Modules



## AIX JRE 1.5.0

CONTAINS IBM(R) 32-bit Runtime Environment for AIX(TM), Java(TM) 2 Technology Edition, Version 1.5 Modules

# ANTLR 2.7.5H3

Portions of this product include software developed by the ANTLR.org. The ANTLR software is distributed in accordance with the following license agreement.

ANTLR 3 License

[The BSD License]



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 author 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 OWNER 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.

# CentOS 5.6

CentOS 5.6

This CA product is distributed with CentOS 5.6 (the “GPL Software”), the use of which is governed by the following terms:

The GPL Software is open source software that is used with this CA software program (the “CA Product”). The GPL Software is not owned by CA, Inc. (“CA”). Use, copying, distribution and modification of the GPL Software are governed by the GNU General Public License version 2 (the “GPL”). A copy of the GPL license can be found in the same directory where the Third Party Product is located. Additionally, a copy of the GPL license can be found at http://www.opensource.org/licenses/gpl-2.0.html or write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA. CA makes the source code for the GPL Software available at http://opensrcd.ca.com/ips/09001_1/, and includes a copy of the source code on the same media as the executable code. Use of the CA Product is governed solely by the CA end user license agreement (“EULA”), not by the GPL license. You cannot use, copy, modify or redistribute any CA Product code except as may be expressly set forth in the EULA. The GPL Software is provided “AS IS” WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Further details of the disclaimer of warranty with respect to the GPL Software can be found in the GPL license itself. To the full extent permitted under applicable law, CA disclaims all warranties and liability arising from or related to any use of the GPL Software.

# CPAN Perl 5.8.8

Portions of this product include software copyrighted by Larry Wall. The Standard Version of Perl 5.8.3 can be downloaded from http://www.perl.org/.

# CRC32

Portions of this product include software developed by Markus Friedl and are distributed in accordance with the following copyright and permission notices.

```
/*          $OpenBSD: crc32.c,v 1.9 2003/02/12 21:39:50 markus Exp $    */


/*
 * Copyright (c) 2003 Markus Friedl.  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 ``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 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.

*/

# Cyrus SASL 2.1.22

Cyrus SASL Library

This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/). The Cyrus SASL Library was obtained under the following license:

```
/* CMU libsasl
 * Tim Martin
 * Rob Earhart
 * Rob Siemborski
 */
/*
 * Copyright (c) 1998-2003 Carnegie Mellon University.  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 name "Carnegie Mellon University" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For permission or any other legal
*    details, please contact
*      Office of Technology Transfer
*      Carnegie Mellon University
*      5000 Forbes Avenue
*      Pittsburgh, PA  15213-3890
*      (412) 268-4387, fax: (412) 268-7395
*      tech-transfer@andrew.cmu.edu
*
* 4. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by Computing Services
*     at Carnegie Mellon University (http://www.cmu.edu/computing/)."
*
* CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO
* THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
* AND FITNESS, IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE
* FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
* WHATSOEVER RESULTING FROM 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.
```

```
*/
```

# dom4j 1.5

Portions of this product include software developed by the DOM4J Project (http://dom4j.org/) and is distributed in accordance with the following license agreement.

BSD style license

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain copyright statements and notices. Redistributions must also contain a copy of this document.

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 "DOM4J" must not be used to endorse or promote products derived from this Software without prior written permission of MetaStuff, Ltd. For written permission, please contact dom4j-info@metastuff.com.

Products derived from this Software may not be called "DOM4J" nor may "DOM4J" appear in their names without prior written permission of MetaStuff, Ltd. DOM4J is a registered trademark of MetaStuff, Ltd.

Due credit should be given to the DOM4J Project - http://www.dom4j.org

THIS SOFTWARE IS PROVIDED BY METASTUFF, LTD. AND CONTRIBUTORS "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 METASTUFF, LTD. 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.



# Hibernate 3.2

CA Access Control Enterprise Management

This product is shipped with Hibernate v.3.2, the use of which is governed by the following terms:

Hibernate v.3.2 is open source software that is used with this CA software program (the CA Product). Hibernate v.3.2 is not owned by CA, Inc. ("CA"). Use, copying, distribution and modification of Hibernate v.3.2 are governed by the GNU Lesser General Public License ("LGPL") version 2.1. A copy of the LGPL license in its entirety can be found in the same directory on the installation disk on which Hibernate v.3.2 is distributed. CA makes the source code for Hibernate v.3.2 available at http://opensrcd.ca.com/ips/06519_8/, and includes a copy of the source code on the same disk as the executable code. Use of the CA Product is governed solely by the CA end user license agreement ("EULA"), not by the LGPL license. You cannot use, copy, modify or redistribute any CA Product code except as may be expressly set forth in the EULA. Hibernate v.3.2 is provided "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Further details of the disclaimer of warranty with respect to Hibernate v.3.2 can be found in the LGPL license itself. To the full extent permitted under applicable law, CA disclaims all warranties and liability arising from or related to any use of Hibernate v.3.2.

# ICU4C 3.4

Portions of this product include software developed by the International Business Machines Corporation. The IBM software is distributed in accordance with the following license agreement.

ICU License - ICU 1.8.1 and later

COPYRIGHT AND PERMISSION NOTICE

INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM 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.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

# JBoss 4.0.1 SP1

JBoss software is an open source library that is used with the  software. The JBoss software is not owned by Computer Associates International, Inc. ( CA ).  Use, copying, distribution and modification of the JBoss software are governed by the GNU Lesser General Public License ( LGPL ) version 2.1.  A copy of the LGPL license can be found in the  directory on the installation disk on which the JBoss software is distributed. Additionally, a copy of the LGPL license can be found at http://opensource.org/licenses/lgpl-license.php or write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.  CA makes the source code for the JBoss software available at , and includes a copy of the source code on the same disk as the executable code. Use of the  software is governed solely by the  end user license agreement ( EULA ), not by the LGPL license.  You cannot use, copy, modify or redistribute any  code except as may be expressly set forth in the EULA.  The JBoss software is provided  AS IS  WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Further details of the disclaimer of warranty with respect to the JBoss software can be found in the LGPL license itself.  To the full extent permitted under applicable law, CA disclaims all warranties and liability arising from or related to any use of the JBoss software.

# JBoss Application Server v.4.2.3

This product is distributed with JBoss Application Server v.4.2.3 (the LGPL Software), the use of which is governed by the following terms:

The LGPL Software is open source software that is used with this CA software program (the CA Product). The LGPL Software is not owned by CA, Inc. (CA). Use, copying, distribution and modification of the LGPL Software are governed by the GNU Lesser General Public License (LGPL) version 2.1. A copy of the LGPL license can be found in the same directory on the installation disk on which the LGPL Software is distributed. Additionally, a copy of the LGPL license can be found at http://www.opensource.org/licenses/lgpl-2.1.php or write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA. CA makes the source code for the LGPL Software available at http://opensrcd.ca.com, and includes a copy of the source code on the same disk as the executable code. Use of the CA Product is governed solely by the CA end user license agreement (EULA), not by the LGPL license. You cannot use, copy, modify or redistribute any CA Product code except as may be expressly set forth in the EULA. The LGPL Software is provided AS IS WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Further details of the disclaimer of warranty with respect to the LGPL Software can be found in the LGPL license itself. To the full extent permitted under applicable law, CA disclaims all warranties and liability arising from or related to any use of the LGPL Software.

# JBoss Native v.2.0.6

This product is distributed with JBoss Native v.2.0.6 (the LGPL Software), the use of which is governed by the following terms:

The LGPL Software is open source software that is used with this CA software program (the CA Product). The LGPL Software is not owned by CA, Inc. (CA). Use, copying, distribution and modification of the LGPL Software are governed by the GNU Lesser General Public License (LGPL) version 2.1. A copy of the LGPL license can be found in the same directory on the installation disk on which the LGPL Software is distributed. Additionally, a copy of the LGPL license can be found at http://www.opensource.org/licenses/lgpl-2.1.php or write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA. CA makes the source code for the LGPL Software available at http://opensrcd.ca.com, and includes a copy of the source code on the same disk as the executable code. Use of the CA Product is governed solely by the CA end user license agreement (EULA), not by the LGPL license. You cannot use, copy, modify or redistribute any CA Product code except as may be expressly set forth in the EULA. The LGPL Software is provided AS IS WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Further details of the disclaimer of warranty with respect to the LGPL Software can be found in the LGPL license itself. To the full extent permitted under applicable law, CA disclaims all warranties and liability arising from or related to any use of the LGPL Software.

# JDOM 1.0

This product includes software developed by the JDOM Project (http://www.jdom.org/). The JDOM software is distributed in accordance with the following license agreement.

$Id: LICENSE.txt,v 1.11 2004/02/06 09:32:57 jhunter Exp $



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 disclaimer that follows these conditions in the documentation and/or other materials provided with the distribution.

3. The name "JDOM" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact .

4. Products derived from this software may not be called "JDOM", nor

may "JDOM" appear in their name, without prior written permission
from the JDOM Project Management .

In addition, we request (but do not require) that you include in the
end-user documentation provided with the redistribution and/or in the
software itself an acknowledgement equivalent to the following:
"This product includes software developed by the
JDOM Project (http://www.jdom.org/)."
Alternatively, the acknowledgment may be graphical using the logos
available at http://www.jdom.org/images/logos.

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 JDOM AUTHORS OR THE PROJECT
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 JDOM Project and was originally

created by Jason Hunter  and

Brett McLaughlin .  For more information

on the JDOM Project, please see .

# MD5 Message Digest Algorithm

Portions of this product include the RSA Data Security, Inc. MD5 Message-Digest Algorithm. The RSA Data Security software is distributed in accordance with the following license agreement.

/* MD5.H - header file for MD5C.C

*/

/* Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

Rivest [Page 8]

RFC 1321 MD5 Message-Digest Algorithm April 1992

These notices must be retained in any copies of any part of this documentation and/or software.

*/

# MIT Kerberos v5 r1.5

This product includes MIT Kerberos v5 r1.5, excluding the OpenVision Kerberos Administration System donated by Kerberos to MIT for inclusion in the standard Kerberos 5 distribution.

Kerberos Version 5, Release 1.5.3

Release Notes

The MIT Kerberos Team

Unpacking the Source Distribution

---

The source distribution of Kerberos 5 comes in a gzipped tarfile,

krb5-1.5.3.tar.gz.  Instructions on how to extract the entire

distribution follow.

If you have the GNU tar program and gzip installed, you can simply do:

```
gtar zxpf krb5-1.5.3.tar.gz
```

If you don't have GNU tar, you will need to get the FSF gzip

distribution and use gzcat:

```
gzcat krb5-1.5.3.tar.gz | tar xpf -
```

Both of these methods will extract the sources into krb5-1.5.3/src and the documentation into krb5-1.5.3/doc.

Building and Installing Kerberos 5

---

The first file you should look at is doc/install-guide.ps; it contains the notes for building and installing Kerberos 5. The info file krb5-install.info has the same information in info file format. You can view this using the GNU emacs info-mode, or by using the standalone info file viewer from the Free Software Foundation. This is also available as an HTML file, install.html.

Other good files to look at are admin-guide.ps and user-guide.ps, which contain the system administrator's guide, and the user's guide, respectively. They are also available as info files kerberos-admin.info and krb5-user.info, respectively. These files are also available as HTML files.

If you are attempting to build under Windows, please see the src/windows/README file. Note that this release might not build under Windows currently.

Reporting Bugs

---

Please report any problems/bugs/comments using the krb5-send-pr program. The krb5-send-pr program will be installed in the sbin directory once you have successfully compiled and installed Kerberos V5 (or if you have installed one of our binary distributions).

If you are not able to use krb5-send-pr because you haven't been able compile and install Kerberos V5 on any platform, you may send mail to krb5-bugs@mit.edu.

You may view bug reports by visiting

http://krbdev.mit.edu/rt/

and logging in as "guest" with password "guest".

Major changes in krb5-1.5.3

---

[5512] Fix MITKRB5-SA-2007-001: telnetd allows login as arbitrary user
[CVE-2007-0956, VU#220816]

[5513] Fix MITKRB5-SA-2007-002: buffer overflow in krb5_klog_syslog
[CVE-2007-0957, VU#704024]

[5520] Fix MITKRB5-SA-2007-003: double-free in kadmind - the RPC
library could perform a double-free due to a GSS-API library
bug [CVE-2007-1216, VU#419344]

krb5-1.5.3 changes by ticket ID

---

5512 (krb5-1.5.x) MITKRB5-SA-2007-001: telnetd allows login as
arbitrary user
5513 (krb5-1.5.x) MITKRB5-SA-2007-002: buffer overflow in
krb5_klog_syslog
5520 (krb5-1.5.x) MITKRB5-SA-2007-003: double-free in kadmind

Major changes in krb5-1.5.2

---

* Fix for MITKRB5-SA-2006-002: the RPC library could call an
uninitialized function pointer, which created a security
vulnerability for kadmind.

* Fix for MITKRB5-SA-2006-003: the GSS-API mechglue layer could fail
to initialize some output pointers, causing callers to attempt to
free uninitialized pointers. This caused a security vulnerability
in kadmind.

Major known bugs in krb5-1.5.2

---

5293 crash creating db2 database in non-existent directory

Attempting to create a KDB in a non-existent directory using the Berkeley DB back end may cause a crash resulting from a null pointer dereference. If a core dump occurs, this may cause a local exposure of sensitive information such a master key password. This will be fixed in an upcoming patch release.

krb5-1.5.2 changes by ticket ID

---

Listed below are the RT tickets of bugs fixed in krb5-1.5.2. Please see

http://krbdev.mit.edu/rt/NoAuth/krb5-1.5/fixed-1.5.2.html

for a current listing with links to the complete tickets.

3965 Autoconf 2.60 datarootdir issue

4237 windows ccache and keytab file paths without a prefix

4305 windows thread support frees thread local storage after TlsSetValue

4309 wix installer - win2k compatibility for netidmgr

4310 NSIS installer - update for Win2K NetIDMgr

4312 KFW 3.1 Beta 2 NetIDMgr Changes

4354 db2 policy database loading broken

4355 test policy dump/load in make check

4368 kdc: make_toolong_error does not initialize all fields for krb5_mk_error

4407 final commits for KFW 3.1 Beta 2

4499 Document prerequisites for make check

4500 Initialize buffer before calling res_ninit

5307 fix MITKRB5-SA-2006-002 for 1.5-branch

5308 fix MITKRB5-SA-2006-003 for 1.5-branch

Major changes in 1.5.1

---

The only significant change in krb5-1.5.1 is to fix the security vulnerabilities described in MITKRB5-SA-2006-001, which are local privilege escalation vulnerabilities in applications running on Linux and AIX.

krb5-1.5.1 changes by ticket ID

---

Listed below are the RT tickets of bugs fixed in krb5-1.5.1. Please see

http://krbdev.mit.edu/rt/NoAuth/krb5-1.5/fixed-1.5.1.html

for a current listing with links to the complete tickets.

3904 fix uninitialized vars

3956 gssapi compilation errors on Windows

3971 broken configure test for dlopen

3998 Document add_entry in ktutil man page

4012 reverse test for copy_oid_set in lib/gssapi/krb5/indicate_mechs.c

4036 reject configure option for static libraries

4037 respect LDFLAGS in NetBSD build

4063 gss mech glue implementation should validate opaque pointer types

4088 gss_import_name can fail to call gssint_initialize_library()

4125 fix MITKRB5-SA-2006-001: multiple local privilege escalation
vulnerabilities

4137 ksu spuriously fails when exiting shell when ksu-ing to non-root

4168 clean up mkrel patchlevel.h editing etc.

Major changes in 1.5

---

Kerberos 5 Release 1.5 includes many significant changes to the
Kerberos build system, to GSS-API, and to the Kerberos KDC and
administration system. These changes build up infrastructure as part
of our efforts to make Kerberos more extensible and flexible. While

we are confident that these changes will improve Kerberos in the long run, significant code restructuring may introduce portability problems or change behavior in ways that break applications. It is always important to test a new version of critical security software like Kerberos before deploying it in your environment to confirm that the new version meets your environment's requirements. Because of the significant restructuring, it is more important than usual to perform this testing and to report problems you find.

Highlights of major changes include:

* KDB abstraction layer, donated by Novell.

* plug-in architecture, allowing for extension modules to be loaded at run-time.

* multi-mechanism GSS-API implementation ("mechglue"), donated by Sun Microsystems

* Simple and Protected GSS-API negotiation mechanism ("SPNEGO") implementation, donated by Sun Microsystems

* Per-directory ChangeLog files have been deleted. Releases now include auto-generated revision history logs in the combined file doc/CHANGES.

Changes by ticket ID

---

Listed below are the RT tickets of bugs fixed in krb5-1.5. Please see

http://krbdev.mit.edu/rt/NoAuth/krb5-1.5/fixed-1.5.html

for a current listing with links to the complete tickets.

581 verify_krb_v4_tgt is not 64-bit clean

856 patch to add shared library support for BSD/OS 4

1245 source tree not 64-bit clean

1288 v4 ticket file format incompatibilities

1431 fix errno.h references for cygwin

1434 use win32 rename solution in rcache for cygwin

1988 profile library fails to handle space in front of comments

2577 [Russ Allbery] Bug#250966: /usr/sbin/klogind: Authorization behavior not fully documented

2615 Fwd: Patch for telnet / telnetd to avoid crashes when used with MS kdc and PAC field

2628 Cygwin build patches

2648 [Russ Allbery] Bug#262192: libkrb53: krb_get_pw_in_tkt problems with AFS keys

2712 whitespace patch for src/kdc/kerberos_v4.c

2759 fake-getaddrinfo.h incorrectly checks for gethostbyname_r errors

2761 move getaddrinfo hacks into support lib for easier maintenance

2763 file ccache should be held open while scanning for credentials

2786 dead code in init_common() causes malloc(0)

2791 hooks for recording statistics on locking behavior

2807 Add VERSIONRC branding to krb5 support dll

2855 Possible thread safety issue in lib/krb5/os/def_realm.c

2856 Need a function to clone krb5_context structs for thread safe apps

2863 windows klist won't link

2880 fix calling convention for thread support fns

2882 Windows 2003 SP1 ktpass.exe generate keytab files fail to load with 1.4

2886 krb5_do_preauth could attempt to free NULL pointer

2931 implement SPNEGO

2932 implement multi-mech GSSAPI

2933 plug-in architecture

2936 supplementary error strings

2959 profile library should check high-resolution timestamps if available

2979 threaded test program built even with thread support disabled

3008 Incorrect cross-references in man pages

3010 Minor path and service man page fixes

3011 krb5-config should never return -I/usr/include

3013 Man pages for fakeka and krb524init

3014 texinfo variable fixes, info dir entries

3030 Bug report: Kinit has no suport for addresses in

credentials. Kinit -a is not enabled.

3065 Implement RFC 3961 PRF

3086 [Sergio Gelato] Bug#311977: libkrb53: gss_init_sec_context sometimes fails to initialise output_token

3088 don't always require support library when building with sun cc

3122 fixes for AIX 5.2 select() and IPv4/IPv6 issues

3129 shlib build problems on HP-UX 10.20 with gcc-3.4.3

3233 kuserok needs to check for uid 99 on Mac OS X

3252 Tru64 compilation fails after k5-int.h/krb5.h changes

3266 Include errno.h in kdc/kerberos_v4.c

3268 kprop should fall back on port 754 rather than failing

3269 telnet help should connect to a host named help

3308 kadmin.local is killed due to segmentation fault when principal name argument is missing.

3332 don't destroy uninitialized rcache mutex in error cases

3358 krb5 doesn't build when pthread_mutexattr_setrobust_np is defined but not declared

3364 plugins should be thread-safe

3415 Windows 64-bit support

3416 tweak kdb interface for thread safety

3417 move/add thread support to support lib

3423 Add support for utmps interface on HPUX 11.23

3426 trunk builds without thread support are not working

3434 sizeof type should be checked at compile time, not configure time

3438 enhancement: report errno when generic I/O errors happen in kinit

3445 args to ctype.h macros should be cast to unsigned char, not int

3466 ioctl header portability fixes for telnet on GNU/kFreeBSD

3467 Allow GSS_C_NO_OID in krb5_gss_canon_name

3468 udp_preference_limit typo in krb5.conf man page

3490 getpwnam_r status checked incorrectly

3502 Cannot acquire initiator cred using gss_acquire_cred with explicit name on Windows

3512 updates to NSIS installer for KFW

3521 Add configurable Build value to File and Product versions for Windows

3549 library double-free with an empty keytab

3607 clients/ksu/setenv.c doesn't build on Solaris

3620 use strerror_r

3668 Prototype for krb5_c_prf missing const

3671 shsUpdate should take an unsigned int for length

3675 unsigned/signed int warnings in krb5_context variables.

3687 initialize cc_version to 0 not NULL

3688 Added CoreFoundation bundle plugin support

3689 build kadm5 headers in generate-files-mac target

3690 build rpc includes in generate-files-mac target.

3697 kadmin hangs indefinitely when admin princ has escaped chars

3706 ipv4+ipv6 messages can trip up KDC replay detection

3714 fix incorrect padata memory allocation in send_tgs.c

3716 Plugin search algorithm should take lists of name and directories

3719 fix bug in flag checking in libdb2 mpool code

3724 need to export kadm5_set_use_password_server

3736 Cleanup a number of cast away from const warnings in gssapi

3739 vsnprintf not present on windows

3746 krb5_cc_gen_new memory implementation doesn't create a new ccache

3761 combine kdc.conf, krb5.conf data in KDC programs

3783 install headers into include/krb5

3790 memory leak in GSSAPI credential releasing code

3791 memory leak in gss_krb5_set_allowable_enctypes error path

3825 krb5int_get_plugin_dir_data() uses + instead of * in realloc

3826 memory leaks in krb5kdc due to not freeing error messages

3854 CCAPI krb4int_save_credentials_addr should match prototype

3866 gld --as-needed not portable enough

3879 Update texinfo.tex

3888 ftpd's getline conflicts with current glibc headers

3898 Export gss_inquire_mechs_for_name for KFW

3899 Export krb5_gss_register_acceptor_identity in KFW

3900 update config.guess and config.sub

3902 g_userok.c has implicit declaration of strlen

3903 various kadm5 files need string.h

3905 warning fixes for spnego

3909 Plugins need to use RTLD_GROUP when available, but definitely not RTLD_GLOBAL

3910 fix parallel builds for libgss

3911 getaddrinfo code uses vars outside of storage duration

3918 fix warnings for lib/gssapi/mechglue/g_initialize.c

3920 cease export of krb5_gss_*

3921 remove unimplemented/unused mechglue functions

3922 mkrel should update patchlevel.h prior to reconf

3923 implement RFC4120 behavior on TCP requests with high bit set in length

3924 the krb5_get_server_rcache routine frees already freed memory
in error path

3925 krb5_get_profile should reflect profile in the supplied context

3927 fix signedness warnings in spnego_mech.c

3928 fix typo in MS_BUG_TEST case in krb5_gss_glue.c

3940 Disable MSLSA: ccache in WOW64 on pre-Vista Beta 2 systems

3942 make gssint_get_mechanism match prototype

3944 write svn log output when building release

3945 mkrel should only generate doc/CHANGES for checkouts

3948 Windows: fix krb5.h generation

3949 fix plugin.c to compile on Windows

3950 autoconf 2.60 compatibility

3951 remove unused dlopen code in lib/gssapi/mechglue/g_initialize.c

3952 fix calling convention for krb5 error-message routines,
document usage of krb5_get_error_message

3953 t_std_conf references private function due to explicit linking
of init_os_ctx.o

3954 remove mechglue gss_config's gssint_userok and pname_to_uid

3957 remove unused lib/gssapi/mechglue/g_utils.c

3959 re-order inclusions in spnego_mech.c to avoid breaking system headers

3962 krb5_get_server_rcache double free

3964 "kdb5_util load" to existing db doesn't work, needed for kpropd

3968 fix memory leak in mechglue/g_init_sec_ctx.c

3970 test kdb5_util dump/load functionality in dejagnu

3972 make gss_unwrap match prototype

3974 work around failure to load into nonexistent db

Known bugs by ticket ID:

---

Listed below are the RT tickets for known bugs in krb5-1.5. Please

see

http://krbdev.mit.edu/rt/NoAuth/krb5-1.5/bugs-1.5.html

for an up-to-date list, including links to the complete tickets.

3947 allow multiple calls to krb5_get_error_message to retrieve message

3956 gssapi compilation errors on Windows

3973 kdb5_util load now fails if db doesn't exist [workaround]

Copyright Notice and Legal Administrivia

---

Export of this software from the United States of America may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.

WITHIN THAT CONSTRAINT, 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 appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Furthermore if you modify this software you must label your software as modified software and not distribute it in such a fashion that it might be confused with the original MIT software. M.I.T. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

THIS SOFTWARE IS PROVIDED ``AS IS|&"&| AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Individual source code files are copyright MIT, Cygnus Support, OpenVision, Oracle, Sun Soft, FundsXpress, and others.

Project Athena, Athena, Athena MUSE, Discuss, Hesiod, Kerberos, Moira, and Zephyr are trademarks of the Massachusetts Institute of Technology (MIT). No commercial use of these trademarks may be made without prior written permission of MIT.

"Commercial use" means use of a name in a product or other for-profit manner. It does NOT prevent a commercial firm from referring to the MIT trademarks in order to convey information (although in doing so, recognition of their trademark status should be given).

---

Portions contributed by Matt Crawford were
work performed at Fermi National Accelerator Laboratory, which is
operated by Universities Research Association, Inc., under
contract DE-AC02-76CHO3000 with the U.S. Department of Energy.

---- The implementation of the Yarrow pseudo-random number generator in src/lib/crypto/yarrow has the following copyright:

Copyright 2000 by Zero-Knowledge Systems, Inc.

Permission to use, copy, modify, distribute, and sell this software
and its documentation for any purpose is hereby granted without fee,

provided that the above copyright notice appear in all copies and that
both that copyright notice and this permission notice appear in
supporting documentation, and that the name of Zero-Knowledge Systems,
Inc. not be used in advertising or publicity pertaining to
distribution of the software without specific, written prior
permission. Zero-Knowledge Systems, Inc. makes no representations
about the suitability of this software for any purpose. It is
provided "as is" without express or implied warranty.

ZERO-KNOWLEDGE SYSTEMS, INC. DISCLAIMS ALL WARRANTIES WITH REGARD TO
THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND
FITNESS, IN NO EVENT SHALL ZERO-KNOWLEDGE SYSTEMS, INC. BE LIABLE FOR
ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTUOUS ACTION, ARISING OUT
OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- The implementation of the AES encryption algorithm in
src/lib/crypto/aes has the following copyright:

Copyright (c) 2001, Dr Brian Gladman , Worcester, UK.
All rights reserved.

LICENSE TERMS

The free distribution and use of this software in both source and binary form is allowed (with or without changes) provided that:

1. distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer;

2. distributions in binary form include the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other associated materials;

3. the copyright holder's name is not used to endorse products built using this software without specific written permission.

DISCLAIMER

This software is provided 'as is' with no explcit or implied warranties in respect of any properties, including, but not limited to, correctness and fitness for purpose.

--- The implementations of GSSAPI mechglue in GSSAPI-SPNEGO in src/lib/gssapi, including the following files:

lib/gssapi/generic/gssapi_err_generic.et

lib/gssapi/mechglue/g_accept_sec_context.c

lib/gssapi/mechglue/g_acquire_cred.c

lib/gssapi/mechglue/g_canon_name.c

lib/gssapi/mechglue/g_compare_name.c

lib/gssapi/mechglue/g_context_time.c

lib/gssapi/mechglue/g_delete_sec_context.c

lib/gssapi/mechglue/g_dsp_name.c

lib/gssapi/mechglue/g_dsp_status.c

lib/gssapi/mechglue/g_dup_name.c

lib/gssapi/mechglue/g_exp_sec_context.c

lib/gssapi/mechglue/g_export_name.c

lib/gssapi/mechglue/g_glue.c

lib/gssapi/mechglue/g_imp_name.c

lib/gssapi/mechglue/g_imp_sec_context.c

lib/gssapi/mechglue/g_init_sec_context.c

lib/gssapi/mechglue/g_initialize.c

lib/gssapi/mechglue/g_inq_context.c

lib/gssapi/mechglue/g_inq_cred.c

lib/gssapi/mechglue/g_inq_names.c

lib/gssapi/mechglue/g_process_context.c

lib/gssapi/mechglue/g_rel_buffer.c

lib/gssapi/mechglue/g_rel_cred.c

lib/gssapi/mechglue/g_rel_name.c

lib/gssapi/mechglue/g_rel_oid_set.c

lib/gssapi/mechglue/g_seal.c

lib/gssapi/mechglue/g_sign.c

lib/gssapi/mechglue/g_store_cred.c

lib/gssapi/mechglue/g_unseal.c

lib/gssapi/mechglue/g_verify.c

lib/gssapi/mechglue/mglueP.h

lib/gssapi/mechglue/oid_ops.c

lib/gssapi/spnego/gssapiP_spnego.h

lib/gssapi/spnego/spnego_mech.c

are subject to the following license:

IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Acknowledgments

---

Thanks to Russ Allbery for contributing and integrating patches from Debian and other places.

Thanks to Michael Calmer for contributing patches for code clean-up.

Thanks to Novell for donating the KDB abstraction layer.

Thanks to Sun Microsystems for donating their implementations of mechglue and SPNEGO.

Thanks to the numerous others who reported bugs and/or contributed patches.

Thanks to iDefense for notifying us about the vulnerability in MITKRB5-SA-2007-002.

Thanks to the members of the Kerberos V5 development team at MIT, both

past and present: Danilo Almeida, Jeffrey Altman, Justin Anderson, Richard Basch, Jay Berkenbilt, Mitch Berger, Andrew Boardman, Joe Calzaretta, John Carr, Don Davis, Alexandra Ellwood, Nancy Gilman, Matt Hancher, Sam Hartman, Paul Hill, Marc Horowitz, Eva Jacobus, Miroslav Jurisic, Barry Jaspan, Geoffrey King, Kevin Koch, John Kohl, Peter Litwack, Scott McGuire, Kevin Mitchell, Cliff Neuman, Paul Park, Ezra Peisach, Chris Provenzano, Ken Raeburn, Jon Rochlis, Jeff Schiller, Jen Selby, Brad Thompson, Harry Tsai, Ted Ts'o, Marshall Vale, Tom Yu.

# nss_ldap 2.62

This product includes Heimdal software distributed pursuant to the following terms:

GNU LESSER GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc.

Everyone is permitted to copy and distribute verbatim copies

of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates

the terms and conditions of version 3 of the GNU General Public

License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser

General Public License, and the "GNU GPL" refers to version 3 of the GNU

General Public License.

"The Library" refers to a covered work governed by this License,

other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided

by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the

Library is used in it and that the Library and its use are
covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license
document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that,
taken together, effectively do not restrict modification of the
portions of the Library contained in the Combined Work and reverse
engineering for debugging such modifications, if you also do each of
the following:

a) Give prominent notice with each copy of the Combined Work that
the Library is used in it and that the Library and its use are
covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license
document.

c) For a Combined Work that displays copyright notices during
execution, include the copyright notice for the Library among
these notices, as well as a reference directing the user to the
copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany

the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new

versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

# Oracle JDBC Driver 10g Release 2 (10.2.0.1.0)

ORACLE TECHNOLOGY NETWORK

DEVELOPMENT AND DISTRIBUTION LICENSE AGREEMENT

"We," "us," and "our" refers to Oracle USA, Inc., for and on behalf of itself and its subsidiaries and affiliates under common control. "You" and "your" refers to the individual or entity that wishes to use the programs from Oracle. "Programs" refers to the software product you wish to download and use and program documentation. "License" refers to your right to use the programs under the terms of this agreement. This agreement is governed by the substantive and procedural laws of California. You and Oracle agree to submit to the exclusive jurisdiction of, and venue in, the courts of San Francisco, San Mateo, or Santa Clara counties in California in any dispute arising out of or relating to this agreement.

We are willing to license the programs to you only upon the condition that you accept all of the terms contained in this agreement. Read the terms carefully and select the "Accept" button at the bottom of the page to confirm your acceptance. If you are not willing to be bound by these terms, select the "Do Not Accept" button and the registration process will not continue.

License Rights

We grant you a nonexclusive, nontransferable limited license to use the programs for purposes of developing your applications. You may also distribute the programs with your applications to your customers. If you want to use the programs for any purpose other than as expressly permitted under this agreement you must contact us, or an Oracle reseller, to obtain the appropriate license. We may audit your use of the programs. Program documentation is either shipped with the programs, or documentation may accessed online at http://otn.oracle.com/docs.

Ownership and Restrictions

We retain all ownership and intellectual property rights in the programs. You may make a sufficient number of copies of the programs for the licensed use and one copy of the programs for backup purposes.

You may not:

- use the programs for any purpose other than as provided above;

- distribute the programs unless accompanied with your applications;

- charge your end users for use of the programs;

- remove or modify any program markings or any notice of our proprietary rights;

- use the programs to provide third party training on the content and/or functionality of the programs, except for training your licensed users;

- assign this agreement or give the programs, program access or an interest in the programs to any individual or entity except as provided under this agreement;

- cause or permit reverse engineering (unless required by law for interoperability), disassembly or decompilation of the programs;

- disclose results of any program benchmark tests without our prior consent; or,

- use any Oracle name, trademark or logo.

Program Distribution

We grant you a nonexclusive, nontransferable right to copy and distribute the programs to your end users provided that you do not charge your end users for use of the programs and provided your end users may only use the programs to run your applications for their business operations. Prior to distributing the programs you shall require your end users to execute an agreement binding them to terms consistent with those contained in this section and the sections of this agreement entitled "License Rights," "Ownership and Restrictions," "Export," "Disclaimer of Warranties and Exclusive Remedies," "No Technical Support," "End of Agreement," "Relationship Between the Parties," and "Open Source." You must also include a provision stating that your end users shall have no right to distribute the programs, and a provision specifying us as a third party beneficiary of the agreement. You are responsible for obtaining these agreements with your end users.

You agree to: (a) defend and indemnify us against all claims and damages caused by your distribution of the programs in breach of this agreements and/or failure to include the required contractual provisions in your end user agreement as stated above; (b) keep executed end user agreements and records of end user information including name, address, date of distribution and identity of programs distributed; (c) allow us to inspect your end user agreements and records upon request; and, (d) enforce the terms of your end user agreements so as to effect a timely cure of any end user breach, and to notify us of any breach of the terms.

Export

You agree that U.S. export control laws and other applicable export and import laws govern your use of the programs, including technical data; additional information can be found on Oracle's Global Trade Compliance web site located at http://www.oracle.com/products/export/index.html?content.html. You agree that neither the programs nor any direct product thereof will be exported, directly, or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

Disclaimer of Warranty and Exclusive Remedies

THE PROGRAMS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. WE FURTHER DISCLAIM ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT.

IN NO EVENT SHALL WE BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR DATA USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR ENTIRE LIABILITY FOR DAMAGES HEREUNDER SHALL IN NO EVENT EXCEED ONE THOUSAND DOLLARS (U.S. $1,000).

No Technical Support

Our technical support organization will not provide technical support, phone support, or updates to you for the programs licensed under this agreement.

Restricted Rights

If you distribute a license to the United States government, the programs, including documentation, shall be considered commercial computer software and you will place a legend, in addition to applicable copyright notices, on the documentation, and on the media label, substantially similar to the following:

NOTICE OF RESTRICTED RIGHTS

"Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065."

End of Agreement

You may terminate this agreement by destroying all copies of the programs. We have the right to terminate your right to use the programs if you fail to comply with any of the terms of this agreement, in which case you shall destroy all copies of the programs.

Relationship Between the Parties

The relationship between you and us is that of licensee/licensor. Neither party will represent that it has any authority to assume or create any obligation, express or implied, on behalf of the other party, nor to represent the other party as agent, employee, franchisee, or in any other capacity. Nothing in this agreement shall be construed to limit either party's right to independently develop or distribute software that is functionally similar to the other party's products, so long as proprietary information of the other party is not included in such software.

Open Source

"Open Source" software - software available without charge for use, modification and distribution - is often licensed under terms that require the user to make the user's modifications to the Open Source software or any software that the user 'combines' with the Open Source software freely available in source code form. If you use Open Source software in conjunction with the programs, you must ensure that your use does not: (i) create, or purport to create, obligations of us with respect to the Oracle programs; or (ii) grant, or purport to grant, to any third party any rights to or immunities under our intellectual property or proprietary rights in the Oracle programs. For example, you may not develop a software program using an Oracle program and an Open Source program where such use results in a program file(s) that contains code from both the Oracle program and the Open Source program (including without limitation libraries) if the Open Source program is licensed under a license that requires any "modifications" be made freely available. You also may not combine the Oracle program with programs licensed under the GNU General Public License ("GPL") in any manner that could cause, or could be interpreted or asserted to cause, the Oracle program or any modifications thereto to become subject to the terms of the GPL.

Entire Agreement

You agree that this agreement is the complete agreement for the programs and licenses, and this agreement supersedes all prior or contemporaneous agreements or representations. If any term of this agreement is found to be invalid or unenforceable, the remaining provisions will remain effective.

Last updated: 03/09/05

# PCRE 6.3

Portions of this product include software developed by Philip Hazel. The University of Cambridge Computing Service software is distributed in accordance with the following license agreement.

THE BASIC LIBRARY FUNCTIONS

---

Written by: Philip Hazel

Email local part: ph10

Email domain: cam.ac.uk

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.



THE C++ WRAPPER FUNCTIONS

---

Contributed by: Google Inc.

THE "BSD" LICENCE

---

ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER 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.

End

## Rhino 1.6r4

The source code version of Rhino 1.6 Release 4 is licensed under the Mozilla Public License Version 1.1 which can be found at http://www.mozilla.org/MPL/ and is made available for download from http://opensrcd.ca.com/ips/P02056_4/.

# SAXPath 1

This product includes software developed by the SAXPath Project (http://www.saxpath.org/). The SAXPath software is distributed in accordance with the following license agreement.

/*--

$Id: LICENSE,v 1.1 2002/04/26 17:43:56 jstrachan Exp $



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 disclaimer that follows these conditions in the documentation and/or other materials provided with the distribution.

3. The name "SAXPath" must not be used to endorse or promote products

derived from this software without prior written permission. For written permission, please contact license@saxpath.org.

4. Products derived from this software may not be called "SAXPath", nor may "SAXPath" appear in their name, without prior written permission from the SAXPath Project Management (pm@saxpath.org).

In addition, we request (but do not require) that you include in the end-user documentation provided with the redistribution and/or in the software itself an acknowledgement equivalent to the following:

"This product includes software developed by the SAXPath Project (http://www.saxpath.org/)."

Alternatively, the acknowledgment may be graphical using the logos available at http://www.saxpath.org/

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 SAXPath AUTHORS OR THE PROJECT 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 SAXPath Project and was originally created by bob mcwhirter and James Strachan . For more information on the SAXPath Project, please see .

*/

# SHA-1

This product includes software developed by Internet Society. The software is distributed in accordance with the following license agreement.

# Sun JDK 1.4.2_13

This Product is distributed with Sun JRE 1.4.2_13 (JAVATM2 RUNTIME ENVIRONMENT (J2RE), VERSION 1.4.2_13) (Sun JRE). The Sun JRE is distributed in accordance with the Sun Microsystems, Inc. (Sun) Binary Code License Agreement set forth below. As noted in Section F of the Supplemental License Terms of this license, Sun has provided additional copyright notices and license terms that may be applicable to portions of the Sun JRE in the THIRDPARTYLICENSEREADME.txt file that accompanies the Sun JRE.

LICENSE:

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)

# Sun JDK 1.6.0

This Product is distributed with Sun JDK 1.6.0 (JAVA SE DEVELOPMENT KIT (JDK), VERSION 6) (Sun JDK). The Sun JDK is distributed in accordance with the Sun Microsystems, Inc. (Sun) Binary Code License Agreement set forth below. As noted in Section G of the Supplemental License Terms of this license, Sun has provided additional copyright notices and license terms that may be applicable to portions of the Sun JDK in the THIRDPARTYLICENSEREADME.txt file that accompanies the Sun JDK.

Sun Microsystems, Inc. Binary Code License Agreement

for the JAVA SE DEVELOPMENT KIT (JDK), VERSION 6

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 Platform, Standard Edition (Java SE) 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. 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.

8. 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.

9. 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.

10. 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).

11. 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.

12. 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.

13. 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 and restrictions and exceptions set forth in the Software "README" file incorporated herein by reference, 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 for the purpose of designing, developing, and testing your Programs.

B. License to Distribute Software. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software README file, 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 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, (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 and restrictions and exceptions set forth in the Software README file, 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, and only bundled as part of Programs, (ii) the Programs add significant and primary functionality to the Redistributables, (iii) you do not distribute additional software intended to supersede any component(s) of the Redistributables (unless otherwise specified in the applicable README file), (iv) you do not remove or alter any proprietary legends or notices contained in or on the Redistributables, (v) you only distribute the Redistributables pursuant to a license agreement that protects Sun's interests consistent with the terms contained in the Agreement, (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.

D. Java Technology Restrictions. You may not create,

modify, or change the behavior of, or authorize your licensees to create, modify, or change the behavior of, 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. Distribution by Publishers. This section pertains to your distribution of the Software with your printed book or magazine (as those terms are commonly used in the industry) relating to Java technology ("Publication"). Subject to and conditioned upon your compliance with the restrictions and obligations contained in the Agreement, in addition to the license granted in Paragraph 1 above, Sun hereby grants to you a non-exclusive, nontransferable limited right to reproduce complete and unmodified copies of the Software on electronic media (the "Media") for the sole purpose of inclusion and distribution with your Publication(s), subject to the following terms: (i) You may not distribute the Software on a stand-alone basis; it must be distributed with your Publication(s); (ii) You are responsible for downloading the Software from the applicable Sun web site; (iii) You must refer to the Software as JavaTM

SE Development Kit 6; (iv) The Software must be reproduced in its entirety and without any modification whatsoever (including, without limitation, the Binary Code License and Supplemental License Terms accompanying the Software and proprietary rights notices contained in the Software); (v) The Media label shall include the following information: Copyright 2006, Sun Microsystems, Inc. All rights reserved. Use is subject to license terms. Sun, Sun Microsystems, the Sun logo, Solaris, Java, the Java Coffee Cup logo, J2SE, and all trademarks and logos based on Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. This information must be placed on the Media label in such a manner as to only apply to the Sun Software; (vi) You must clearly identify the Software as Sun's product on the Media holder or Media label, and you may not state or imply that Sun is responsible for any third-party software contained on the Media; (vii) You may not include any third party software on the Media which is intended to be a replacement or substitute for the Software; (viii) You shall indemnify Sun for all damages arising from your failure to comply with the requirements of this Agreement. In addition, you shall defend, at your

expense, any and all claims brought against Sun by third parties, and shall pay all damages awarded by a court of competent jurisdiction, or such settlement amount negotiated by you, arising out of or in connection with your use, reproduction or distribution of the Software and/or the Publication. Your obligation to provide indemnification under this section shall arise provided that Sun: (a) provides you prompt notice of the claim; (b) gives you sole control of the defense and settlement of the claim; (c) provides you, at your expense, with all available information, assistance and authority to defend; and (d) has not compromised or settled such claim without your prior written consent; and (ix) You shall provide Sun with a written notice for each Publication; such notice shall include the following information: (1) title of Publication, (2) author(s), (3) date of Publication, and (4) ISBN or ISSN numbers. Such notice shall be sent to Sun Microsystems, Inc., 4150 Network Circle, M/S USCA12-110, Santa Clara, California 95054, U.S.A , Attention: Contracts Administration.

F. 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.

G. 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.

H. Termination for Infringement. 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.

I. Installation and Auto-Update. The Software's installation and auto-update processes transmit a limited amount of data to Sun (or its service provider) about those specific processes to help Sun

understand and optimize them. Sun does not associate the data with personally identifiable information.

You can find more information about the data Sun collects at http://java.com/data/.

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

# Sun JRE 1.5.0_18

This Product is distributed with Sun JRE 1.5.0_18 (JAVA 2 PLATFORM STANDARD EDITION DEVELOPMENT KIT 5.0) ("Sun JDK"). The Sun JDK is distributed in accordance with the Sun Microsystems, Inc. ("Sun") Binary Code License Agreement set forth below. As noted in Section G of the Supplemental License Terms of this license, Sun has provided additional copyright notices and license terms that may be applicable to portions of the Sun JDK in the THIRDPARTYLICENSEREADME.txt file.

Sun Microsystems, Inc. Binary Code License Agreement

for the JAVA 2 PLATFORM STANDARD EDITION DEVELOPMENT KIT 5.0

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. "General Purpose Desktop Computers and Servers" means computers, including desktop and laptop computers, or servers, used for general computing functions under end user control (such as but not specifically limited to email, general purpose Internet browsing, and office suite productivity tools). The use of Software in systems and solutions that provide dedicated functionality (other than as mentioned above) or designed for use in embedded or function-specific software applications, for example but not limited to: Software embedded in or bundled with industrial control systems, wireless mobile telephones, wireless handheld devices, netbooks, kiosks, TV/STB, Blu -ray Disc devices, telematics and network control switching equipment, printers and storage management systems, and other related systems is excluded from this definition and not licensed under this Agreement. "Programs" means Java technology applets and applications intended to run on the Java 2 Platform Standard Edition (J2SE) 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. 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.

8. 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.

9. 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.

10. 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).

11. 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.

12. 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.

13. 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 and restrictions and exceptions set forth in the Software "README" file incorporated herein by reference, 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 for the purpose of designing, developing, and testing your Programs.

B. License to Distribute Software. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software README file, 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 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, (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 and restrictions and exceptions set forth in the Software README file, 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, and only bundled as part of Programs, (ii) the Programs add significant and primary functionality to the Redistributables, (iii) you do not distribute additional software intended to supersede any component(s) of the Redistributables (unless otherwise specified in the applicable README file), (iv) you do not remove or alter any proprietary legends or notices contained in or on the Redistributables, (v) you only distribute the Redistributables pursuant to a license agr eement that protects Sun's interests consistent with the terms contained in the Agreement, (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.

D. Java Technology Restrictions. You may not create, modify, or change the behavior of, or authorize your licensees to create, modify, or change the behavior of,

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. Distribution by Publishers. This section pertains to your distribution of the Software with your printed book or magazine (as those terms are commonly used in the industry) relating to Java technology ("Publication"). Subject to and conditioned upon your compliance with the restrictions and obligations contained in the Agreement, in addition to the license granted in Paragraph 1 above, Sun hereby grants to you a non-exclusive, nontransferable limited right to reproduce complete and unmodified copies of the Software on electronic media (the "Media") for the sole purpose of inclusion and distribution with your Publication(s), subject to the following terms: (i) You may not distribute the Software on a stand-alone basis; it must be distributed with your Publication(s); (ii) You are responsible for downloading the Software from the applicable Sun web site; (iii) You must refer to the Software as JavaTM 2 Platform Standard Edition Development Kit 5.0; (iv) The Software must be reproduced in its entirety and wit hout any modification whatsoever (including, without limitation, the Binary Code License and Supplemental License Terms accompanying the Software and proprietary rights notices contained in the

Software); (v) The Media label shall include the following information: Copyright 2006, Sun Microsystems, Inc. All rights reserved. Use is subject to license terms. Sun, Sun Microsystems, the Sun logo, Solaris, Java, the Java Coffee Cup logo, J2SE, and all trademarks and logos based on Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. This information must be placed on the Media label in such a manner as to only apply to the Sun Software; (vi) You must clearly identify the Software as Sun's product on the Media holder or Media label, and you may not state or imply that Sun is responsible for any third-party software contained on the Media; (vii) You may not include any third party software on the Media which is intended to be a replacement or substitute for the Soft ware; (viii) You shall indemnify Sun for all damages arising from your failure to comply with the requirements of this Agreement. In addition, you shall defend, at your expense, any and all claims brought against Sun by third parties, and shall pay all damages awarded by a court of competent jurisdiction, or such settlement amount negotiated by you, arising out of or in connection with your use, reproduction or distribution of the Software and/or the Publication. Your obligation to provide indemnification under this section shall arise provided that Sun: (a) provides you prompt notice of the claim; (b) gives you sole

control of the defense and settlement of the claim; (c) provides you, at your expense, with all available information, assistance and authority to defend; and (d) has not compromised or settled such claim without your prior written consent; and (ix) You shall provide Sun with a written notice for each Publication; such notice shall include the following information: (1) title of Publication, (2) author(s), (3) date of Publication, and (4) ISBN or ISSN numbers. Such notice shall be sent to Sun Microsystems, Inc., 4150 Network Circle, M/S USCA12-110, Santa Clara, California 95054, U.S.A , Attention: Contracts Administration.

F. 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.

G. 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.

H. Termination for Infringement. 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.

I. Installation and Auto-Update. The Software's installation and auto-update processes transmit a limited amount of data to Sun (or its service provider) about those specific processes to help Sun understand and optimize them. Sun does not associate the data with personally identifiable information. You can find more information about the data Sun collects at http://java.com/data/.

For inquiries please contact: Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. (LFI#143333/Form ID#011801)

# XNTP v.3-5.93

This product includes XNTP v.3-5.93. XNTP v.3-5.93 is distributed in accordance with the following notice and permission:

```
/***********************************************************************
 *                                                                     *
 * Copyright (c) David L. Mills 1992, 1993, 1994, 1995, 1996           *
 *                                                                     *
 * 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 the copyright notice and this permission       *
 * notice appear in supporting documentation, and that the name        *
 * University of Delaware not be used in advertising or publicity      *
 * pertaining to distribution of the software without specific,        *
 * written prior permission. The University of Delaware makes no       *
 * representations about the suitability this software for any         *
 * purpose. It is provided "as is" without express or implied          *
 * warranty.                                                           *
 ***********************************************************************/
```

# XScreenSaver



# Zlib 1.2.3

# ZThread 2.3.2

Portions of this product include software developed by Eric Crahen. The ZThread software is distributed in accordance with the following license agreement.