# CA Access Control Premium Edition

## Release Notes

r12.5 SP2

Second Edition

This documentation and any related computer software help programs (hereinafter referred to as the "Documentation") are for your informational purposes only and are subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be used or disclosed by you except as may be permitted in a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO THE END USER OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

# Third-Party Notices

# CA Product References

This document references the following CA 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 Manager (formerly Unicenter Service Desk)
- CA Enterprise Log Manager
- CA Identity Manager

# Contact CA

## Contact Technical Support

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

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

## Provide Feedback

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

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

# Documentation Changes

**Second Edition**

The second edition of the documentation was released in the CA Bookshelf format, a HTML interface that provides access to the documentation from the CA Access Control product page on CA Support.

The following topic was updated in this edition:

- Fixed Issues in This Release (see page 32)—Updated topic provides a direct link to the CA Access Control fixlists.

The following UNIX endpoint known issues were added:

- Upgrade Issue from r12.5 SP1 on AIX (see page 74)
- Upgrade Issue from r8 SP1 on AIX (see page 74)

The following UNAB consideration was added:

- Restrictions on Use of Symbols in distinguishedName (see page 78)

The following UNAB known issues were added:

- New Domain User Login May Fail on First Attempt (see page 81)
- Duplicate Audit Records Produced for rlogin by Domain User on Linux SuSE Endpoints (see page 81)
- Incorrect Audit Record Produced for SSH Login by Domain User on Linux SuSE Endpoints (see page 81)
- Issues When root Changes Password of Domain User Who Has Not Logged in to Endpoint (see page 81)
- su from root to Domain User Fails on Linux SuSE Endpoints (see page 82)
- uxconsole -register -s Command Produces Error (see page 82)

The following server component consideration was updated:

- Superuser Account Required for Server Component Installation (see page 91)

**First Edition**

The first edition of the documentation was released with r12.5 SP2.

The following documentation updates have been made since the r12.5 SP1 release of this documentation:

- New and Changed Features (see page 25)—Updated chapter for this release.
- Windows Endpoint Requirements (see page 33)—Updated topic with memory requirements for a Windows endpoint.
- CA Access Control Premium Edition Enterprise Management Server Requirements (see page 35)—Updated topic with support for Microsoft SQL Server 2008.

The following chapter was removed from this release:

- 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.

The following Windows known issue was added:

- "Access Control not found" Message Appears During iRecorder Installation (see page 62)

The following UNIX endpoint considerations were added or updated:

- JRE Prerequisite for SLES 11 Linux s390x Computers (see page 63)
- Change to Default Value of proc_bypass (see page 63)
- Message Queue for Linux 390 Requires J2SE Version 5.0 (see page 64)
- CA Access Control PAM Module on AIX (see page 64)

The following UNAB endpoint considerations were updated:

- HP-UX Feature Support Limitations (see page 78)
- UNAB for Linux 390 Requires J2SE Version 5.0 for Remote Management (see page 79)
- sepass Integration with UNAB Endpoints (see page 79)

The following UNAB known issue was updated:

- Interval between uxconsole -register and -deregister Commands (see page 84)

The following server component considerations were added or updated:

- SAP R3 Connector Restriction (see page 84)
- Cannot Use PUPM to Change Password for the Expert Account (see page 84)
- Login to CA Access Control Enterprise Management Using Active Directory Administrator Account (see page 84)

The following server component known issue was updated:

- Workaround Required to Create PUPM Endpoint After Upgrade (see page 93)
- Do Not Use '$' Character for CA Access Control Enterprise Management Database Password (see page 98)

The following Windows endpoint known issues were removed:

- Cannot Import Windows Native Users and Groups During Installation
- IA64 and x64 Architectures: Cannot Install a Prerequisite in Silent Mode

The following UNIX endpoint known issues were removed:

- Upgrade from CA Access Control r12.5 Using Native Packages Fails on Linux Kernel 2.4
- Report Agent Multi-Threading is Not Supported on Linux Z-series (s390x)
- Issues in Interactive Mode Installation
- Change LOGINFLAGS Value to NONE if UNAB is Installed on a CA Access Control Endpoint
- Native Package Upgrade from r12.0 CR1 Does Not Work
- Cannot Stop CA Access Control on an HP-UX 11.11 Computer

The following UNAB known issues were removed:

- UNAB Not Automatically Restarted After CA Access Control Is Installed on a UNAB Endpoint
- uxconsole -manage -edit Option is Not Supported
- seaudit Reports "Deny" Events on UNAB Agent

The following server component considerations were removed:

- Search Root Parameters Are Case Sensitive
- The PUPM Endpoint and Account Feeder CSV File Fields are Case Sensitive
- CA Identity Manager Provisioning Connector Server Successfully Created in PUPM But Not Validated
- Oracle Database XE Does Not Resolve the Database SID As Required
- Windows Agentless Endpoint Management from CA Access Control Enterprise Management for UNIX Requires a Windows Distribution Server
- Log In to the Windows Endpoint Before You Configure the Endpoint in CA Access Control Enterprise Management
- Do Not Configure More Than a Single Oracle Schema with Reporting Tables
- The CA Access Control Enterprise Management Server Does Not Support CA Identity Manager r12.5 and r12.5 SP1

The following server component known issues were removed:

- Cannot Change Active Directory Account Password using CA Access Control Enterprise Management Windows Connector
- Cannot View or Schedule PUPM Reports Due to a "Page Encapsulation Failed" Error Message on Oracle
- Capture Snapshot Fails When Executed By a Member of an Active Directory Group with More Than 1000 Members
- Report Agent and DMS Fail to Communicate with Message Queue Server on CA Access Control Enterprise Management for Solaris
- Non-English Installation Displays Some English Text

# Contents

## Chapter 1: Welcome 19

## Chapter 2: New and Changed Features 25

## Chapter 3: System Requirements 33

# Chapter 1: Welcome

Welcome to CA Access Control Premium Edition r12.5 SP2. 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.

This section contains the following topics:

## 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 Installation Media

CA Access Control Premium Edition components are available on ten optical discs:

- 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.

  It also contains UNAB installation files.

- 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 Premium Edition Server Components for Solaris

  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 Solaris, 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 Premium Edition Report Portal for Windows (Disc 1)

  CA Business Intelligence Release 2.1 installation files.

- CA Access Control Premium Edition Report Portal for Windows (Disc 2)

  Business Objects Release XIR2 SP5 patch for use by Oracle Database 11g users.

- CA Access Control Premium Edition Report Portal for UNIX (Disc 1)

  CA Business Intelligence Release 2.1 installation files.

- CA Access Control Premium Edition Report Portal for UNIX (Disc 2)

  BusinessObjects XIR2 Release 2.1 SP5 patch for use by Oracle Database 11g users.

- 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.

- CA Access Control Third Party Components for Solaris

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

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

## CA Access Control Installation Media

CA Access Control components are available on six optical discs:

- 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).

  It also contains UNAB installation files for use with CA Access Control Premium Edition.

- CA Access Control Server Components for Windows

  Contains CA Access Control Endpoint Management for Windows.

- CA Access Control Server Components for Solaris

  Contains CA Access Control Endpoint Management for Solaris.

- CA Access Control Third Party Components for Windows

  Contains a prerequisite installer 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.

- CA Access Control Third Party Components for Solaris

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

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

## Complementary CA Enterprise Log Manager License

As the owner of the CA Access Control Premium Edition, you are also entitled to the CA Enterprise Log Manager product for the limited use of collecting, managing and reporting on CA Access Control audit logs. First, you must obtain a license for "CA Enterprise Log Manager 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 Enterprise Log Manager in North America, contact your local account representative. If you are outside of North America, call your local account representative or the local CA office. You can download CA Enterprise Log Manager 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 we supply the same documentation for both editions, 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.

- 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.

- Enterprise Administration Guide

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

- 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 2: New and Changed Features

This section contains the following topics:

## New and Changed Features in r12.5 SP2

The following features were added or enhanced in r12.5 SP2.

### PUPM Enhancements

The following PUPM enhancements were made in r12.5 SP2:

- **su support for SSH endpoints**

  You can use both a connection account and an operation administrator account to administer SSH endpoints. PUPM connects to the endpoint using the connection account credentials and then su's to the operation administrator account to perform administrative tasks, such as password changes.

- **Support for additional endpoint types**

  PUPM now supports additional endpoint types.

  **Note:** For a list of supported endpoint types, see the CA Access Control Compatibility Matrix that is available from the CA Access Control product page on CA Support.

- **Clean up submitted tasks**

  You can automate the removal of submitted tasks from the central database.

**Note:** For more information about PUPM, see the *Enterprise Administration Guide*.

## UNAB Enhancements

The following UNAB enhancements were made in r12.5 SP2:

- **Site support**

  When you register a UNAB endpoint with Active Directory, by default, the uxconsole utility discovers the Active Directory site that is closest to the physical location of the endpoint. The utilty configures the endpoint to communicate with the domain controllers (DCs) in that site.

- **CA Access Control UNIX Attributes plug-in**

  The plug-in lets you manage UNIX Attributes for UNAB users on Active Directory.

- **Enterprise user names resolved in uxconsole output**

  The uxconsole utility now resolves the full user name for enterprise users, for example, user@domain1.

  In previous releases, the utility printed only the user name and not the domain name.

**Note:** For more information about site support and the CA Access Control UNIX Attributes plug-in, see the *Implementation Guide*. For more information about uxconsole, see the *Reference Guide*.

## Other Enhancements

The following enhancements were also made in r12.5 SP2:

- **Microsoft SQL Server 2008 support**

  You can now use Microsoft SQL Server 2008 for the CA Access Control Enterprise Management central database.

- **Enhanced support for Linux s390 and s390x endpoints**

  You can now send report and audit data from Linux s390 and s390x UNAB and CA Access Control endpoints to CA Enterprise Log Manager.

- **fullbypass property**

  The pgmtype(fullbypass) property is added to the SPECIALPGM class. This property lets you define system processes that CA Access Control bypasses completely, such as cluster heartbeats.

# New and Changed Features in r12.5 SP1

The following features were added or enhanced in r12.5 SP1.

## PUPM Target System Feed

The PUPM feeder lets you create or modify many endpoints or privileged accounts in a single step. You list the endpoints or privileged accounts that you want to create in a CSV file, and use the PUPM feeder to upload the file to CA Access Control Enterprise Management for processing.

**Note:** For more information about the PUPM feeder, see the *Enterprise Administration Guide*.

## PUPM Password Extraction Utility

The PUPM password extraction utility, pwextractor, lets you extract privileged account passwords from the central database if PUPM is unavailable.

**Note:** For more information about pwextractor, see the *Enterprise Administration Guide*.

## PUPM Integration with CA Service Desk Manager

You can integrate PUPM with CA Service Desk Manager, so that PUPM validates each privileged account request against an active ticket in CA Service Desk Manager. This lets you integrate your existing CA Service Desk Manager approval process and the PUPM approval process.

**Note:** For more information about PUPM, see the *Enterprise Administration Guide*.

## PUPM Endpoint Support

CA Identity Manager Provisioning Connector supports CA Identity Manager r8.0 and the following endpoint types:

- CA Access Control
- CA ACF2
- CA Top Secret
- Windows NT
- IBM RACF

- Active Directory
- NDS Servers

PUPM support is extended to the following endpoint types:

- CA Access Control (Access Control for PUPM)
- Active Directory (Windows Agentless)

## Solaris Support for CA Access Control Enterprise Management

CA Access Control Enterprise Management now supports Solaris SPARC 10. You can install CA Access Control Enterprise Management for Solaris in console mode only.

## Manual Installation of the Database Schema

The installation media provides scripts to let you customize the central database before you install CA Access Control Enterprise Management. The scripts let you install CA Access Control Enterprise Management with a user account that has the least privileges required to install and manage the database.

**Note:** For more information about manually configuring the database, see the *Implementation Guide*.

## Extended Operating System Support for UNAB

UNAB now supports RHEL 3, 4 AS & ES, RHEL 5 BS & AP and SLES 9, 10 on Z-Series (S390x) and HP-UX 11i V1, V2 and V3 on IA64.

## Active Directory Domain Controllers to Use or Ignore

You can now specify a list of Active Directory Domain Controllers to use or ignore when registering and working with UNAB.

**Note:** For more information about the Active Directory Domain Controllers support option, see the *Implementation Guide*.

## UNAB Supports LDAP Root as Base Search

When you install a UNAB endpoint, you can specify the LDAP root as the base search for LDAP queries. After installation, you can use CA Access Control Enterprise Management to configure this behavior for UNAB hosts and host groups.

In previous releases, you could specify only the user or group container as the base search for LDAP queries.

**Note:** For more information about installing UNAB, see the *Implementation Guide*.

## sepass Integration with UNAB on Solaris

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

**More information:**

sepass Integration with UNAB Endpoints (see page 79)

## Other Enhancements

The following enhancements have also been made to r12.5 SP1:

- **secons -db function**

  This function lets you batch delete XUSER records in the CA Access Control database that no longer exist in the native environment.

  **Note:** For more information about the secons utility, see the *Reference Guide*.

- **Password-protected certificates**

  You can now use password-protected certificates for SSL communication.

  **Note:** For more information about encryption, see the *Implementation Guide*.

- **uxconsole -detail option**

  This option lets you display the user properties in detail. You can use this option with both the -manage and -status arguments.

  **Note:** For more information about the uxconsole utility, see the *Reference Guide*.

# New and Changed Features in r12.5

The following features were added or enhanced in r12.5.

## Privileged User Password Management

Privileged User Password Management (PUPM) is the process through which an organization secures, manages, and tracks all activities associated with the most powerful accounts within the organization.

PUPM in CA Access Control provides role-based access management for privileged accounts on target endpoints from a central location. PUPM also provides secure storage of privileged accounts and application ID passwords, and controls access to privileged accounts and passwords based on policies. Further, PUPM manages privileged accounts and application password lifecycle and let you remove passwords from configuration files and scripts.

PUPM empowers system users to delegate the management of users and access privileged accounts. Users can manage their access to privileged accounts using the PUPM self-service mechanism and request access to privileged accounts as an exception.

CA Access Control integration with CA Enterprise Log Manager provides accountability and tracing of privileged accounts usage.

**Note:** For more information about PUPM, see the *Enterprise Administration Guide*.

## UNIX Authentication Broker

UNIX Authentication Broker (UNAB) lets you log in to UNIX computers using an Active Directory data store. This means you can use a single repository for all your users, letting them log in to all platforms with the same user name and password.

Integrating UNIX accounts with Active Directory enforces strict authentication and password policies, transferring the rudimentary UNIX user and group properties to Active Directory. This lets you manage UNIX users and groups in the same location that you also manage Windows users and groups.

**Note:** For more information about UNAB, see the *Implementation Guide*.

## Unified Data and Resource Protection Console

CA Access Control Enterprise Management is enhanced to provide an integrated console for Data and Resource Protection (DRP) capabilities that CA Access Control provides. DRP capabilities in CA Access Control Enterprise Management include:

- Managing privileged user accounts.
- Managing Active Directory user and group access to UNAB hosts.
- Displaying CA Access Control, PUPM, and UNAB reports that are generated by CA Enterprise Log Manager.

## Variables Support

Variables let you deploy the same policy to endpoints that have different configurations and different operating systems. You can use variables to deploy the same policy to Windows and Solaris endpoints despite the different CA Access Control installation location on each operating system.

**Note:** For more information about variables, see the *Enterprise Administration Guide.*

## Policy Import

Policy import is the process of migrating an existing policy to an advanced policy management environment that lets you deploy and undeploy policies and check the deployment and deviation status of policies.

**Note:** For more information about policy import, see the *Implementation Guide.*

## Streamlined Installation

The installation of CA Access Control r12.5 was simplified to help you to easily deploy CA Access Control in your enterprise. The installation process of CA Access Control r12.5 was streamlined to allow you to quickly deploy CA Access Control Enterprise Management and CA Access Control. The CA Access Control Enterprise Management wizard based installation guides you through the steps and enables you to install CA Access Control Enterprise Management on a single server.

**Note:** For more information, see the *Implementation Guide.*

## CA Enterprise Log Manager Integration

CA Access Control Enterprise Management is enhanced to provide a unified console for CA Access Control, PUPM, and UNAB CA Enterprise Log Manager reports. CA Access Control Enterprise Management displays the CA Enterprise Log Manager reports directly from the console, so you do not need to access CA Enterprise Log Manager to view the reports. CA Enterprise Log Manager contains dozens of  reports that display information from numerous sources of information, including:

- Privileged accounts activity reports
- UNAB activity reports
- CA Access Control usage reports

# 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 3: System Requirements

This section contains the following topics:

## 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.

## 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**—128 MB RAM (256 MB recommended)
- **Available disk space**—100 MB (150 MB for general installations)

The following table details the space required for each installation package:

| Package | Space Required (MB) |
|---|---|
| Client | 60 |
| MFSD | 2 |
| Unicenter | 4 |
| API | 20 |

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*/policies/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

## 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 440MHz
- **Memory**—2 GB RAM
- **Available disk space**—2 GB at installation; 3 GB at %TEMP% (Windows) or /tmp (UNIX)

In addition, the CA Access Control Endpoint Management computer should have the following software installed:

- **JDK**—Java Development Kit (JDK) 1.5.0_18 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's 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

## CA Access Control Premium Edition Enterprise Management Server Requirements

The minimum requirements for the Enterprise Management Server are:

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

In addition, the Enterprise Management Server should have the following software installed:

- **JDK**—Java Development Kit (JDK) 1.5.0_18 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's 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

## CA Access Control Premium Edition 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 this 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*.

  **Important!** If you use Oracle Database 11g, install the BusinessObjects XI Release 2.1 SP5 patch that is available on the CA Access Control Premium Edition Report Portal (Disc 2) DVD under the \boeXIR2_SP5 directory.

- **CA Enterprise Log Manager**—r12.0

  **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 Enterprise Log Manager, see the *CA Enterprise Log Manager Release Notes*.

- **CA Service Desk Manager**—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 Manager, see the *CA Service Desk Manager Release Notes*.

## 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) 1.4.2

## 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, if you have a full integration installation

Further, complete the following before you install UNAB:

- Back up the local user store.
- Synchronize the clocks between the UNIX and Active Directory computers.
- Synchronize the clocks between the Distribution Server and UNAB computers.
- Verify that the UNIX computer name resolves correctly from both the UNIX and Active Directory computers.
- (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.

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

# Chapter 4: Documentation

This section contains the following topics:

## Guides

The PDF guides for CA Access Control Premium Edition r12.5 SP2 are as follows:

- Release Notes
- Implementation Guide
- Endpoint Administration Guide for Windows
- Endpoint Administration Guide for UNIX
- Enterprise Administration 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.

## 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 |

| Format | Meaning |
|---|---|
| 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 |
| 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 both UNAB and CA Access Control for UNIX.
  - UNIX—opt/CA/AccessControlShared
- *ACServerInstallDir*—The default CA Access Control Enterprise Management installation directory.
  - Windows—C:\Program Files\CA\AccessControlServer
  - UNIX—/opt/CA/AccessControlServer
- *DistServerInstallDir*—The default Distribution Server installation directory.
  - Windows—C:\Program Files\CA\DistributionServer
  - UNIX—/opt/CA/DistributionServer
- *JBoss_HOME*—The default JBoss installation directory.
  - Windows—C:\jboss-4.2.3.GA
  - UNIX—/opt/jboss-4.2.3.GA

# Chapter 5: FIPS Compliance

This section contains the following topics:

## 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 4.0 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:
  - 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 ETPKI)—used for signatures of trusted programs, signatures of policies
  - AES (from ETPKI)—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 ETPKI 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 |
| Trusted Programs | CAPKI SHA-1 and MD5 | CAPKI SHA-1 only |

| Feature | Non-FIPS Mode | FIPS Mode |
|---|---|---|
| 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<br>(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 |
| selogrd encryption | Default symmetric key encryption and MD5 | Disabled |
| sechkey key change | Default symmetric key encryption | Disabled |
| iRecorder log file signature | MD5 encryption | Disabled |

**Note:** Where a feature is disabled as a result of the FIPS operational mode, the relevant program prints an error message and exits.

# 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 |

**Note:** Where a feature is disabled as a result of the FIPS operational mode, the relevant program prints an error message and exits.

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 6: Considerations and Known Issues

This section contains the following topics:

## Windows Endpoint Considerations

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

### Versions You Can Upgrade From

You can upgrade to CA Access Control r12.5 SP2 for Windows from r12.5 SP1, r12.5, r12.0, r12.0 SP1, and r8 SP1 (only from a CR release, not from the base version).

### CA Access Control r12.5 SP2 Endpoint Requires a Hot Fix to Manage Policy Models on CA Access Control r12.5 and r12.0 SP1

If you want to use a CA Access Control r12.5 SP2 server or endpoint to manage policy models on r12.5 and r12.0 SP1 endpoints, you must install hot fix T537526 on the r12.5 and r12.0 SP1 endpoints.

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

## Reboot May Be Required When Upgrading

When you upgrade an endpoint to r12.5 SP2 from r12.0 SP1, r12.5, or r12.5 SP1, 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 r12.5 SP2 functionality may not be supported until after the reboot.

When you upgrade an r8.0 SP1 or r12.0 endpoint to r12.5 SP2, you must reboot the computer.

## x64 Feature Support Limitations

The following are known limitations on Windows 2003 x64:

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

  **Important!** Impersonation interception is supported on x64 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*.

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

CA Access Control r12.5 SP2 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")
```

## 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:** 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.

## 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.

## Supported Installation Languages

When you install CA Access Control silently, you can specify the language in which CA Access Control is installed. The following are the supported language IDs you can specify and their respective languages:

- 1033—English
- 1041—Japanese
- 1042—Korean

## CA Access Control Backdoor

During the evaluation phase, rules may be incorrectly defined. Incorrectly defined rules can prevent users from logging in or executing commands. For example, a rule that denies access to the system directory or vital parts of the Windows registry. Because it is difficult to stop CA Access Control and fix these mistakes, CA Access Control comes with a backdoor that lets you fix these types of problem. Because backdoors can be maliciously exploited, CA Access Control also lets you disable this backdoor once your system is set up and stable.

To access this backdoor, select Safe Mode or Safe Mode with Networking from the boot menu. When you select one of these options the system starts without automatically starting the CA Access Control services.

To disable this backdoor, define the registry value 'LockEE' of data type reg_dword under the registry key HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\AccessControl\ and set it to 1.

**Note:** This registry value does not exist by default.

Now when you start the system with LockEE set to 1 in:

- Safe Mode, only CA Access Control Engine and CA Access Control Watchdog load.

  The CA Access Control Agent (and any Policy Models), which rely on network services, do not load.

- Safe Mode with Networking, CA Access Control starts normally.

## CA Access Control Database Size Limitation

The CA Access Control database is limited to one million (1,000,000) objects. This size limitation is only likely to affect your deployment if you use advanced policy management in a large environment.

If the CA Access Control database in your enterprise is expected to hold 1,000,000 objects, you need to remove old DEPLOYMENT objects that are no longer in use.

### Example: Calculating the Number of Objects in the CA Access Control Database

The following example shows you how to calculate the number of objects that you can expect to have in the DMS-the central CA Access Control management database.

In this example, we have an enterprise deployment of CA Access Control on 5000 endpoints, each holding 50 assigned policies. As a result, the DMS contains at least 250,000 objects, as follows:

5,000 endpoints X 50 policies = 250,000 DEPLOYMENT objects

If over time you create four versions of each policy, and assign these policies to each of your 5000 endpoints, the number of objects in the DMS will reach the 1,000,000 objects limit, as follows:

5,000 endpoints X 50 policies X 4 version = 1,000,000 DEPLOYMENT objects

## CA Access Control Generates the Login Session ID

CA Access Control generates at startup the login session ID that it adds to audit log records. This means that a logged on user gets a different session ID within the same terminal session every time CA Access Control restarts. The session ID remains the same only within the same CA Access Control session.

## Conflicts with Other Software in Databases You Create

To avoid conflicts between CA Access Control and other products, CA Access Control provides a coexistence utility that detects and defines special rules for any such software found. When you create a new CA Access Control database using dbmgr, we highly recommended you issue the command with the additional *-k* switch. This switch creates the database with special coexistence rules.

Alternatively, run the coexistence utility separately after you create the database. From the CA Access Control Bin directory, issue the command:

```
eACoexist.exe ACInstallDir\Coexistence
```

## Mainframe Password Synchronization Prerequisite

To work with Mainframe Password Synchronization on the server that has TNG/TND/NSM installed, CA Access Control requires a prerequisite TNG/TND/NSM fix - T129430. Please contact support for getting the fix.

## Firewall Settings

When you install CA Access Control on Windows Server 2003, or Windows Server 2008, CA Access Control opens port 8891 for non-SSL TCP connections and port 5249 for SSL TCP connections. This serves as the default port for CA Access Control agent-client connections.

**Note:** For more information on ports CA Access Control uses on Windows, 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 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*.

## TCP and SURROGATE Class Are Not Active By Default

CA Access Control database classes TCP and SURROGATE are not active by default.

If you upgrade from an earlier release where the TCP class is active but you do not have any TCP records and have not changed the _default TCP resource, CA Access Control deactivates the class during upgrade. The same is true for the SURROGATE class.

If you upgrade from an earlier release where the SURROGATE class is active and you have defined SURROGATE records or have changed the value of any SURROGATE record from its default, CA Access Control retains the SURROGATE class configuration after the upgrade. The class remains active and kernel mode interception remains enabled.

## Enterprise Users Do Not Correspond to the _undefined User

If you use enterprise users (osuser_enabled is set to 1), CA Access Control does not consider any user as undefined.

Rules for the _undefined user are not relevant in this case.

## Policy Model Names Are Case-sensitive

Policy Model names are case-sensitive on Windows for compatibility with UNIX. When specifying PMDB names in commands, make sure you use the correct case.

**Note:** Although PMDB names are case-sensitive, you cannot have two PMDBs on the same computer with only the letter case being different. This is because CA Access Control uses the PMDB name as part of the file path but Windows is case-insensitive and so does not permit this. For example, myPMDB and MYpmdb are two different Policy Model databases but cannot live on the same system.

## seaudit Displays Trace Records by User Name

The seaudit utility displays trace records by user name, not by user ID.

**Note:** You can choose to revert the seaudit utility output to the way it was in a previous release using the -format option. For more information, see the *Reference Guide*.

## Process Creation Trace Limitations

- CA Access Control traces process creation in Windows. However, seosd fetches new process arguments and writes the arguments to the general trace only if the user who started the process is marked to be traced.
- When a new process is created, its arguments may not be available until the process finishes initialization. seosd attempts to trace the process arguments asynchronously; however if the process is very short, the process may terminate before seosd can fetch the process arguments and write them to the trace. In this case the following message appears in the trace:

  ```
  EXECARGS: Not available (87)
  ```
- Process IDs are reused in Windows. If a process is very short, it is theoretically possible that seosd will fetch process arguments for a different process that acquired the same process ID, and write these arguments to the trace.

## PMDB and Host Names Do Not Support Non-English Characters

You cannot use non-English characters in PMDB and host names.

## Password Propagation Requires a Restart When You Change Encryption Modes

When you change the encryption mode (for example, to FIPS-only mode), you must restart CA Access Control services if you need to propagate passwords from a password PMDB.

## 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.

## Non-IPv4 telnet Connections Are Not Secured on Windows Server 2008

On Windows Server 2008, CA Access Control cannot secure a telnet connection unless it uses IPv4.

To protect a localhost telnet connection–telnet from the localhost to the localhost–on Windows Server 2008, you need to modify the /etc/HOSTS file as follows:

```
127.0.0.1       localhost
#      ::1            localhost
127.0.0.1       <your server name without domain suffix>
```

The above configuration works around this issue on an IPv4 domain. If your computer is on an IPv6 domain, you need to add the following line:

```
127.0.0.1    <your server name with domain suffix>
```

## Login Interception is Supported by Sub-authentication Method Only

Login interception on Windows is supported only by CA Access Control sub-authentication method.

You cannot set login interception through the kernel. As a result, you should consider the following:

- Since the sub-authentication component works on the Domain Controller (DC) level, and it is up to the OS to decide which DC authenticates the user's login events (and triggers the CA Access Control sub-authentication module), in a Windows domain environment, CA Access Control needs to be installed on every DC.
- When working in a Windows domain environment, CA Access Control login policy (TERMINAL rules) need to be located on the DCs and not necessarily on the target server.

  For example, if you would like to protect or audit login events made by domain users on a file server, which is part of the Windows domain but is not a DC, the CA Access Control login policy needs to be defined on the DC and not on the target file server. This is because when a domain user accesses the shared file directory, a login authorization occurs on the DC, not the file server.
- When there is more than one DC, CA Access Control login authorization could be processed on any one of the DCs. As a result, we recommended you synchronize CA Access Control login policy between all DCs.

  You can implement this through either the Policy Model mechanism, where all DCs are subscribers to a PMDB, or by adding all DCs into a host group and deploying a common policy using advanced policy management.
- Some user properties, which correspond to login events, are updated at runtime-during event authorization. These properties might be out-of-sync because the login authorization happens only on one of the DCs. These properties are *Gracelogins*, *Last accessed*, and *Last access time*.

  That said, it is possible that, for example, the user's property *Last access time* value will be different between DCs because CA Access Control sub-authentication was triggered on one of the DCs, not on all of them.
- To enforce local users (that is, not domain users) login events, CA Access Control needs to be installed on the local computer that the local user needs access to. This is because the local computer is used as the domain computer (the domain is the local computer).
- Remote Desktop Protocol (RDP)/Terminal Services login events are enforced on the target server as it was in previous CA Access Control versions. However, for RDP login events, CA Access Control login policy should be defined on the target server.

## Policy Manager Interface Discontinued

Policy Manager is not included in r12.0 and later releases. The web-based CA Access Control Endpoint Management replaces this interface. The r8 SP1 Policy Manager is upward compatible with new CA Access Control endpoints. However, it supports pre-r12.0 features only.

## Audit Log Backup Files Are Protected by Default

By default, CA Access Control protects audit log backup files if you configure settings to keep timestamped backups. This is the same default protection that the size-triggered audit backup file receives. To remove these files, you need to set permissive rules in the database.

## Cannot Define Record In SPECIALPGM Class for Incoming Network Interception Events

You cannot define a record in the SPECIALPGM class for incoming network interception events. This is because the incoming network interception event does not have a process name in this context. To bypass writing an audit record for the interception event, set the AUDIT property to NONE for the corresponding record in the TCP class.

## Change to Default Audit Value for Some Users

Before r12.0 SP1 CR1, the default audit mode was None for the following accessors:

- Users that do not have a defined AUDIT value in their corresponding USER class record, and that are not associated with a profile group that has a defined AUDIT value.
- Any user that is not defined in the database (represented by the _undefined user record).

  **Note:** If you use enterprise users, CA Access Control does not consider any users as undefined. Properties of the _undefined user are not relevant in this case.

From r12.0 SP1 CR1, the default audit mode for these accessors is Failure, LoginSuccess, and LoginFailure. To retain earlier behavior, set the value of the AUDIT property to None for these users.

## Change to Value of AUDIT Property for GROUP Records

If you have a GROUP record that has two functions:

- A profile that defines an audit policy for one set of users
- A container for a second set of users

From r12.0 SP1 CR1 onwards, the GROUP record also defines the audit policy for the second set of users. To avoid problems that this behavior change may cause, create a separate GROUP for the second set of users.

## 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.

## 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.

## PUPM Agent Programmable Check Out Requires Case Sensitive Host Name

When using PUPM Agent programmable check-out (Application to Application) command-line interface, verify that you use case-sensitive host name.

## Upgrades from r8 SP1 GA Are Not Supported

Upgrading from eTrust Access Control r8 SP1 GA version is not supported. Upgrade is supported from any r8 SP1 CR, starting with the initial r8 SP1 CR: "September 2006 - QO83379".

Install an r8 SP1 CR before you upgrade.

## Upgrade to CA Access Control r12.5 SP2 from CA Access Control r5.3 and r5.2 Is Not Supported

You cannot upgrade to CA Access Control r12.5 SP2 from CA Access Control for UNIX r5.3 and CA Access Control for Windows r5.2. To upgrade to CA Access Control r12.5 SP2, we recommend that you first install CA Access Control r8.0 SP1 CR1 and then install CA Access Control r12.5 SP2.

## 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).

# Windows Endpoint Known Issues

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

## "Access Control not found" Message Appears During iRecorder Installation

**Valid on 64-bit Windows computers**

If you install iRecorder on a computer on which 64-bit CA Access Control is installed, the iRecorder installation fails and a message informs you that CA Access Control is not installed on the computer. To fix this problem, contact CA Support for a workaround.

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

## "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.

## SPECIALPGM Rule Not Removed from CA Access Control Database After Silent Upgrade

After running a silent upgrade of a CA Access Control endpoint, a SPECIALPGM rule for bypassing msiexec.exe is not removed from the database. To remove the rule, create a selang script or action that removes the rule from the database after the upgrade process is complete.

## PUPM Agent Application to Application Fails to Change Provisioning Account Passwords

Currently, you cannot use the PUPM agent application to application capability to change account passwords that are defined on CA Identity Manager provisioning.

## 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.

## UNIX Endpoint Considerations

This section describes items you should consider when using 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
```

### Versions You Can Upgrade From

You can upgrade to CA Access Control r12.5 SP2 for UNIX from r12.5 SP1, r12.5, r12.0 SP1, r12.0, and r8 SP1.

### JRE Prerequisite for SLES 11 Linux s390x Computers

If you install CA Access Control on a SLES 11 Linux s390x computer, install the J2SE Version 5.0 31-bit System z JRE on the computer before you install CA Access Control. The RPM package name for the JRE is ibm-java2-s390-jre-5.0-10.0.s390.rpm.

### Change to Default Value of proc_bypass

Valid values for the proc_bypass configuration setting in the SEOS_syscall section have changed in r12.5 SP2. The proc_bypass configuration setting specifies if CA Access Control bypasses file access checks when a file belongs to a process file system (/proc).

In earlier releases, the default value was 0 (do not bypass file access checks) and valid values were any sum of access types. In r12.5 SP2 and later, the default value is 1 (bypass file access checks) and valid values are 0 and 1 only. When you upgrade to r12.5 SP2 or later, the upgrade script replaces any nonzero value for this configuration setting with 1.

## 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*.

## CA Access Control Restarts UNAB When Installed and Uninstalled

**Valid on AIX**

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

## CA Access Control PAM Module on AIX

**Valid on AIX**

If you set auth_login=pam in the seos section of the seos.ini file, CA Access Control uses PAM to authenticate users. CA Access Control uses the PAM API library during authentication, but AIX does not provide the PAM library in a shared library format that CA Access Control can easily link to. When CA Access Control attempts to use the PAM API it fails with an error “cannot find /usr/lib/libpam.o”. To avoid this error, you must configure the CA Access Control PAM module.

**To configure the CA Access Control PAM module on AIX**

1. Locate the AIX supplied *libpam.a* archive:

   ```
   cd /usr/lib
   ```

   This archive contains the AIX PAM shared library (shr.o).

2. Extract shr.o from libpam.a to /usr/lib:

   ```
   ar -xv libpam.a
   ```

3. Rename shr.o to libpam.o:

   ```
   mv shr.o libpam.o
   ```

4. Verify that change_pam=yes in the passwd section of the seos.ini file.

   This configuration setting instructs sepass to use the PAM interface to change passwords.

## Linux Kernel Recompilation

On Linux, if you recompile your kernel, you must copy the system.map file to the /boot directory to load the CA Access Control daemons.

## Streams Module Is Not Active by Default

By default, the TCP, CONNECT, and HOST classes are not active and the CA Access Control kernel module is not loaded into streams. Before you activate any of these classes, be sure that the streams module is enabled for network interception.

**Note:** Streams module is only available for systems that support streams.

## 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.

## Some Utilities Require That You Start The Kernel

You must load the CA Access Control kernel module for some utilities to use the CA Access Control kernel interface. These utilities include selogrd and selogrcd on most platforms.

## RENAME Authority Depends on READ Authority on a 2.4 Kernel RHEL

On Red Hat Linux computers with a 2.4 kernel, to deny the RENAME authority you must also deny the READ authority.

## SNMP Extension of selogrd Requires a Variable for a Non-Default Installation Path

If you want to use the SNMP extension of selogrd, and CA Access Control is not installed in the default location (/opt/CA/AccessControl), you must set an environment variable before running selogrd. The environment variables are as follows:

- In AIX, set LIBPATH to *ACInstallDir*/lib
- In Solaris, set LD_LIBRARY_PATH to *ACInstallDir*/lib
- In LINUX, set LD_LIBRARY_PATH to *ACInstallDir*/lib
- In HP, set SHLIB_PATH to *ACInstallDir*/lib

*ACInstallDir* is the directory where you installed CA Access Control.

## Access to SSH Failed Login Attempts Requires PAM Configuration

To obtain failed login events from SSH, the SSH version you are using must be compiled and configured to support PAM.

If your version of SSH does not use PAM, CA Access Control cannot detect whether a user has violated the failed login rules.

## PAM Configuration for CA Access Control Features

CA Access Control PAM features that rely on identifying user login attempts (for example, segrace, serevu, and log audit records) do not work if the line "auth requisite" appears before the CA Access Control line “auth optional *pam_module*” in the operating systems's PAM configuration file.

If you want PAM to write user login attempts, the PAM configuration file should contain the line "auth required *pam_module*" instead of "auth requisite *pam_module*". If you specify the control-flag *required* and the module fails, it continues to next module. If you use the control-flag *requisite* and the module fails, it exits immediately and does not reach the CA Access Control line and so *pam_module* does not run.

**Note:** *pam_module* is the name of the PAM module file on your platform. For example, on Linux, this is pam_unix2.so.

## Lookaside Database Creation from LDAP DIT Requirements

To add information from the LDAP Directory Information Tree (DIT) to the user lookaside database that sebuildla creates (*-n* option), the computer must have LDAP v3 run-time support.

## telnet and rsh Require Specific PAM Configuration

You cannot use telnet or rsh to log in to a computer if your PAM configuration file:

- Is missing the following operating system's line:

  ```
  login account     optional     /usr/lib/security/libpam_unix.1
  ```

- Has the following CA Access Control line:

  ```
  login account     optional     /usr/lib/security/pam_seos.sl
  ```

To fix this, comment out the CA Access Control line if you want PAM to use the "OTHERaccount..." line instead, or uncomment the operating system's line.

## SNMP Configuration

When you set selogrd to route audit records to SNMP listeners, you can use an SNMP community name that is different from the default name (“public”). To do this, use the following format in the selogrd.cfg configuration file:

snmp *gateway@community*

***gateway***

Defines the SNMP gateway host name.

***community***

Defines the SNMP community name that matches the target SNMP environment.

## 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.

## syslog Messages Are Affected by the Product Name Change

syslog messages have been affected by the CA Access Control name change in r12.0.

Where messages contained the "eTrust AC" string before, they now contain the "CA Access Control" string.

## Enterprise Users Do Not Correspond to the _undefined User

If you use enterprise users (osuser_enabled is set to 1), CA Access Control does not consider any user as undefined.

Rules for the _undefined user are not relevant in this case.

## The All Users Mask (*) Applies to Users That Are Not Defined

If you do not use enterprise users (osuser_enabled is set to 0), users that are not defined in the CA Access Control database are included in rules that apply to all users (using the mask *).

If you want to exclude undefined users from rules that apply to all users, create a more specific rule for the _undefined user that defines the required access to users that are not defined in the database.

## serevu Configuration

If you want to work with serevu, and *root* does not have the ADMIN attribute or terminal access to the local database, you should define the following:

```
eu _serevu admin logical
authorize terminal localTerminalName uid(_serevu) access(a)
er specialpgm $ACDIR/bin/serevu seosuid(_serevu ) unixuid(root)
```

## serevu Configuration for Working with a Policy Model

If you want serevu to send commands to the PMD (which, you can configure in serevu.cfg) and *root* is not defined on the PMD with the ADMIN attribute or with terminal access, you should define the following on the PMD and all of its subscribers:

```
eu _serevu logical
authorize admin USER uid(_serevu) access(a)
# The following line can be executed on the master PMD only
authorize terminal localTerminalName uid(_serevu) access(a)
```

## Compiling API Samples

You should use gmake (GNU make) and not make to compile the API samples.

## Compatibility Library Missing on x86_64bit Linux

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

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

## FIPS 140-2 Library Upgrade

This release of CA Access Control uses CAPKI 4.1 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.

CAPKI 4.1 provides a static library (libcapki_stub.lib for Windows, libcapki_stub.a for UNIX) that acts as a stub for the CAPKI interface and removes the need to dynamically load the library.

**More information:**

FIPS Operational Modes (see page 43)

## 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.

## 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.

## CA Access Control Generates the Login Session ID

CA Access Control generates at startup the login session ID that it adds to audit log records. This means that a logged on user gets a different session ID within the same terminal session every time CA Access Control restarts. The session ID remains the same only within the same CA Access Control session.

## Policy Manager Interface Discontinued

Policy Manager is not included in r12.0 and later releases. The web-based CA Access Control Endpoint Management replaces this interface. The r8 SP1 Policy Manager is upward compatible with new CA Access Control endpoints. However, it supports pre-r12.0 features only.

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

When you setup a new Solaris zone, there are several post installation steps you must complete before 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.

## Security Administrator Discontinued

The Security Administrator Motif interface is not included in r12.0 and later releases. The web-based CA Access Control Endpoint Management replaces this interface. The r8 SP1 Security Administrator is upward compatible with new CA Access Control endpoints. However, it supports pre-r12.0 features only.

**Note:** As the Security Administrator is not provided, the CAeACGUI native package is not supplied. Also, the -admin option of the install_base script is no longer available.

## Audit Log Backup Files Are Protected by Default

By default, CA Access Control protects audit log backup files if you configure settings to keep timestamped backups. This is the same default protection that the size-triggered audit backup file receives. To remove these files, you need to set permissive rules in the database.

## Report Agent and PUPM Agent Are Not Supported on Linux IA64

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

## Change Encryption Key After You Patch libcryptscr.so.125.0

The symmetric encryption key is embedded in the libcryptscr.so.125.0 library. If you patch this library, the patch may restore the default CA Access Control encryption key. To avoid communication problems, you must always change the encryption key immediately after you apply a patch to libcryptscr.so.125.0.

To change the key, navigate to /opt/CA/AccessControl/lib/libcryptscr.so.125.0 and run sechkey as follows, where *previous_key* is the encryption key that you used before the patch:

```
sechkey –d previous_key
```

sechkey replaces the default encryption key with the previous key.

## 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.

## Change to Default Audit Value for Some Users

Before r12.0 SP1 CR1, the default audit mode was None for the following accessors:

- Users that do not have a defined AUDIT value in their corresponding USER class record, and that are not associated with a profile group that has a defined AUDIT value.
- Any user that is not defined in the database (represented by the _undefined user record).

  **Note:** If you use enterprise users, CA Access Control does not consider any users as undefined. Properties of the _undefined user are not relevant in this case.

From r12.0 SP1 CR1, the default audit mode for these accessors is Failure, LoginSuccess, and LoginFailure. To retain earlier behavior, set the value of the AUDIT property to None for these users.

## Change to Value of AUDIT Property for GROUP Records

If you have a GROUP record that has two functions:

- A profile that defines an audit policy for one set of users
- A container for a second set of users

From r12.0 SP1 CR1 onwards, the GROUP record also defines the audit policy for the second set of users. To avoid problems that this behavior change may cause, create a separate GROUP for the second set of users.

## 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.

## 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:** 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.

## Upgrade to CA Access Control r12.5 SP2 from CA Access Control r5.3 and r5.2 Is Not Supported

You cannot upgrade to CA Access Control r12.5 SP2 from CA Access Control for UNIX r5.3 and CA Access Control for Windows r5.2. To upgrade to CA Access Control r12.5 SP2, we recommend that you first install CA Access Control r8.0 SP1 CR1 and then install CA Access Control r12.5 SP2.

# UNIX Endpoint Known Issues

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

## Upgrade Issue from r12.5 SP1 on AIX

**Valid on AIX**

If you use AIX native packaging to upgrade an AIX endpoint from r12.5 SP1 to r12.5 SP2, the installation process creates a new CA Access Control database and deletes any records in the existing database. To work around this problem, use the install_base script to upgrade an AIX r12.5 SP1 endpoint to r12.5 SP2.

## Upgrade Issue from r8 SP1 on AIX

**Valid on AIX**

If you use AIX native packaging to upgrade an AIX endpoint from r8 SP1 to r12.5 SP2, selang does not start after the upgrade is complete. To work around this problem, before you start the upgrade, replace all symbolic links named *.o.800.0 in the *ACInstallDir*/lib directory with links to *.o.125.0.

## CA Access Control Fails to Start on SLES 11x86_64

If you use CA Access Control on SELS11 x86_64, you must install a kernel hardware patch. Verify that you use the following kernel patch file or later:

```
kernel-default-base-2.6.27.21-0.1.2.x86_64.rpm
```

To enable CA Access Control to run on SLES11 x86_64, install the kernel patch, restart the system, and start CA Access Control.

## CA Access Control Must Start After ENF on Linux

On Linux, if you load ENF (the Unicenter TNG or NSM kernel for version 3.x and earlier) after the CA Access Control kernel, you cannot unload the CA Access Control kernel.

Start CA Access Control after Unicenter TNG or Unicenter NSM.

## STOP is Not Activated when Native Stack Randomization is Enforced on Linux

The STOP feature on Red Hat Linux and SuSE Linux is not activated when Linux native stack randomization (ExecShield randomize) is enforced.

On Linux s390 RHEL 4, native stack randomization does not work and must be deactivated for STOP to be active. To deactivate native stack randomization, enter the following command:

```
echo 0 > /proc/sys/kernel/exec-shield-randomize
```

## Cannot Use UNIX selang Environment to Create User When passwd_format=NT

If you set the seos.ini file token "passwd_format" ([passwd] section) to "NT", you must use the "native" option (rather than “unix”) when you create a user in selang. For example:

```
nu uSr_1026 native password(uSr_1026)
```

Alternatively, make sure that you work in the native environment (rather than the unix one), as follows:

```
env native
chusr usr_1 password(mypassword)
```

## install_base May Show Errors in a Solaris Zones Installation

If you install CA Access Control using *install_base* in Solaris zones, errors that are caused by attempting to write to read-only files may appear.

Use Solaris native packaging to install CA Access Control on zones.

## Use of uninstall_AC on Global Zone May Prevent Zone Users from Logging In

If you uninstall CA Access Control from the Solaris global zone using *uninstall_AC* before you uninstall from all zones, users may not be able to log in to the zones.

Use Solaris native packaging to install and uninstall CA Access Control on zones.

## Early RPM Package Manager Versions Fail When Building Customized Package

RPM Package Manager versions earlier than rpm-4.2.2-0.8 will fail when building a customized package (customize_eac_rpm script).

**Note:** This is a known issue with the RPM Package Manager. For more information refer to the Red Hat Bugzilla website and look for bug 103867.

## 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.

## 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.

## 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.

## 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.

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

**Valid on Solaris, 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 will not be recognized as a login action by CA Access Control on Solaris, 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.

## 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).

## 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.

## 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—Patch PHSS_35716 or OS QPK Bundle that is dated December 2006 or later.
- 11.23 on PA-RISC—OS QPK Bundle that is dated December 2006 or later.

### Use of selang -d on a Backed Up PMDB Can Lead to Issues

To back up a PMDB, including the advanced policy management server components (DMS and DH), use the sepmd -bd backup option introduced in r12.0.

When backing up any PMDB, avoid using the following command, which can lead to various issues:

```
selang -d . -f file_name
```

You should use the following command instead:

```
selang -p pmd_name -f file_name
```

### 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 Considerations

This section describes items you should consider when using UNAB.

### Restrictions on Use Of Symbols in distinguishedName

When Active Directory creates the distinguishedName (DN) for a user, it masks some symbols in the name with a backslash, for example, a comma or an apostrophe. UNAB does not support distinguishedNames that contain a symbol masked by a backlash.

### 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 (TBC) is not supported.
- seversion utility does not display SHA-1 signature.

## 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*.

## 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*.

## 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 (etc/passwd) to enable Active Directory users to log in.

## License Agreement Acceptance Keyword is Case Insensitive

When customizing the UNAB or CA Access Control installation packages, note that the license agreement acceptance keyword is case insensitive.

## 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.

## 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.

# UNAB Known Issues

This section describes known issues for UNAB.

## New Domain User Login May Fail on First Attempt

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.

## Duplicate Audit Records Produced for rlogin by Domain User on Linux SuSE Endpoints

**Valid on Linux SuSE**

If you implement UNAB in full integration mode on a Linux SuSE endpoint, and a domain user uses rlogin to log in to the endpoint, UNAB creates two audit records for the same login event.

## Incorrect Audit Record Produced for SSH Login by Domain User on Linux SuSE Endpoints

**Valid on Linux SuSE**

If you implement UNAB in full integration mode on a Linux SuSE endpoint, and a domain user uses SSH to log in to the endpoint, the incorrect stage code 59 appears in the login audit record. The correct stage code is 21.

## Issues When root Changes Password of Domain User Who Has Not Logged in to Endpoint

If you implement UNAB in full integration mode, and you log in to the UNAB endpoint as root and use the passwd utility to change the password of a domain user who has never logged in to the UNAB endpoint, the password change succeeds but the process causes a segmentation fault.

## su from root to Domain User Fails on Linux SuSE Endpoints

**Valid on Linux SuSE**

If you implement UNAB in full integration mode on a Linux SuSE endpoint, and you log in to the endpoint as root and su to a domain user, the operation fails and the following message appears:

```
Incorrect Password
```

## uxconsole -register -s Command Produces Error

When you run the uxconsole -register -s *server* command to register a UNIX host in Active Directory, the following error message appears:

```
No Domain Controllers for the registration domain given on lookup_dc_list.
```

To work around this problem, set the value of the lookup_dc_list configuration setting to the names of the Active Directory domain controllers. The lookup_dc_list configuration setting is in the ad section of the uxauth.ini file.

## 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.

## UNAB Not Supported on Linux IA64, Solaris x86 and x64

Currently, you cannot install UNAB on Linux IA64, Solaris x86 and x64 operating systems.

## UNAB Entries Contain Blank Fields in Event Viewer

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

## User Prompted for New Password Twice and Received Incorrect Password Change Failure Message

**Valid on AIX**

When you attempt to change your account password, the new password prompt appears twice and an "incorrect password change" message appears after you enter the new password. To fix this issue, do the following:

1. Open the etc/pam.conf file for editing.
2. Remove the following entry:

   ```
   passwd password optional /user/lib/security/pam_aix
   ```

3. Locate the following entry:

   ```
   password password required /usr/lib/security/pam_aix try_first_pass
   ```

4. Remove the try_first_pass parameter from the end of the line.
5. Save and close the file.

## UNAB is not FIPS140-2 and IPV6 Compliant

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

## Successful Login to Host Generates an Error Message

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 */var/log/message.*

## UNAB Not Started by CA Access Control Watchdog on Linux x64

When running UNAB and CA Access Control 64-bit version on Linux x64, UNAB is not registered as a daemon and as a result, the CA Access Control watchdog daemon (seoswd) cannot start the UNAB daemon if it was not shut down in an orderly fashion.

## 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.

### 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.

## 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).

### SAP R3 Connector Restriction

The SAP R3 connector and the CA Identity Manager provisioning connector cannot coexist on the same Enterprise Management Server.

**Note:** For more information about configuring the SAP R3 connector, see the *Enterprise Administration Guide*.

### 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.

### Login to CA Access Control Enterprise Management Using Active Directory Administrator Account

When Active Directory is the user store for CA Access Control Enterprise Management, you must log in to CA Access Control Enterprise Management with the Active Directory account that you provided during the installation and not with the built-in superadmin account. When using Active Directory for the user store, the superadmin account is not assigned the admin role of SystemManager and you should not use it to administer CA Access Control Enterprise Management.

## Disable Tunneled Clear Text Passwords on SSH Endpoints

**Valid on Linux**

When you configure a PUPM SSH endpoint, disable tunneled clear text passwords on the endpoint before you configure the endpoint settings.

**To disable tunneled clear text password on SSH endpoint**

1. Open the sshd_config file for editing. This file is located in the following directory:

   ```
   etc\ssh
   ```

2. Locate the PasswordAuthentication tag and set the value to **yes**.

   **Example**: PasswordAuthentication yes

## Default JBoss Port

The default JBoss port has changed in r12.5. It is now 18080.

## Maximum Recommended Records in the PUPM Feeder CSV is 500 Endpoints or Accounts

We recommend that you limit the number of endpoints or accounts in a single PUPM feeder CSV file to 500.

## 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.

## 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.

## 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.

## 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.

## Separate List of Identifier Users with a Comma

When you configure a new application and specify more than a single user in the Identifier Users field, separate between the users using a comma.

For example: user1, user2, user3

## Specify the Etaadmin Full Distinguished Name

When you configure an CA Identity Manager provisioning connector server, specify the full distinguished name of the etaadmin.

For example:

eTGlobalUserName=etaadmin,eTGlobalUserContainerName=Global Users,eTNamespaceName=CommonObjects,dc=ProvisioningDomainName,dc=eta

## Supported JDK and JBoss Versions

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

## CA Access Control Database Size Limitation

The CA Access Control database is limited to one million (1,000,000) objects. This size limitation is only likely to affect your deployment if you use advanced policy management in a large environment.

If the CA Access Control database in your enterprise is expected to hold 1,000,000 objects, you need to remove old DEPLOYMENT objects that are no longer in use.

### Example: Calculating the Number of Objects in the CA Access Control Database

The following example shows you how to calculate the number of objects that you can expect to have in the DMS-the central CA Access Control management database.

In this example, we have an enterprise deployment of CA Access Control on 5000 endpoints, each holding 50 assigned policies. As a result, the DMS contains at least 250,000 objects, as follows:

5,000 endpoints X 50 policies = 250,000 DEPLOYMENT objects

If over time you create four versions of each policy, and assign these policies to each of your 5000 endpoints, the number of objects in the DMS will reach the 1,000,000 objects limit, as follows:

5,000 endpoints X 50 policies X 4 version = 1,000,000 DEPLOYMENT objects

## 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.

## 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_r125.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 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.

## Do Not Execute the PUPM Privileged Accounts Discovery Wizard on More Than One Endpoint Type Concurrently

PUPM does not support running the Privileged Accounts Discovery Wizard on more than one endpoint type concurrently. Running the wizard on more than one endpoint type concurrently results in failure to create privileged accounts in the PUPM database or, failure to reset the account passwords on discovery.

Always run the discovery wizard on one endpoint type at a time, verify that the wizard successfully completed the tasks and then run the wizard on another endpoint type.

## CA Enterprise Log Manager Does Not Include PUPM, UNAB Reports

In this version, CA Enterprise Log Manager does not include PUPM nor UNAB reports.

## CA Enterprise Log Manager Supports Only Trusted SSL Connection

When defining the connection settings of the CA Enterprise Log Manager server, define the SSL connection settings. CA Enterprise Log Manager does not support non-SSL connection.

**Note:** For more information about integrating with CA Enterprise Log Manager, see the *Implementation Guide*.

## Special Subscription Needed to View CA Enterprise Log Manager Reports from CA Access Control Enterprise Management

To use view CA Enterprise Log Manager reports from the CA Access Control Enterprise Management interface, apply a special subscription update to your CA Enterprise Log Manager server.

**To apply the subscription update**

1. In CA Enterprise Log Manager, 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 Enterprise Log Manager.

   You can now view CA Enterprise Log Manager reports from CA Access Control Enterprise Management.

## 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.

## 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*).

## 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:

- Report Agent
- DMS
- UNAB
- PUPM Application to Application

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.

## Required Upgrade Sequence

When you upgrade CA Access Control in an enterprise implementation, you should always upgrade the server components before you upgrade endpoints.

## Superuser Account Required for Server Component 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).

## 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.

## 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.

## PUPM Windows Agentless Connector for Active Directory Search Limitations

When using the PUPM Windows Agentless connector to connect to Active Directory the wild card (*) and retrieve all search options do not work. To search for users you must supply the specific account details.

## Do Not Use Administration API Functions Inside a seosd Exit

To avoid deadlocks, do not use any Administration API functions inside a seosd exit.

## 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.

# 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).

## Workaround Required to Create PUPM Endpoint After Upgrade

After you upgrade the Enterprise Management Server to r12.5 SP2, the Create Endpoint screen in CA Access Control Enterprise Management does not display correctly. To work around this problem, delete the following directories on the Enterprise Management Server immediately after you upgrade CA Access Control Enterprise Management:

- *JBoss_HOME*/server/default/tmp
- *JBoss_HOME*/server/default/work

JBoss recreates the directories when you restart it after upgrade. The Create Endpoint screen displays correctly after you perform this step.

## Roles Not Resolved When a Member of a Group with More Than 1000 Members Logs In To the CA Access Control Enterprise Management Server

Members of an Active Directory users group that contains more than 1000 users that attempt to log into the CA Access Control Enterprise Management Server may experience incorrect admin and privileged roles resolution. This behaviour may result users not logging in with their assigned roles.

For example, an Active Directory user that is assigned the System Manager admin role, logs into the CA Access Control Enterprise Management Server and is assigned the User admin role.

To workaround this problem, configure the admin role members using the MemberOf filter option and specify the full distinguished name of the Active Directory group.

For example:

```
CN=GroupName,OU=OrganizationalUnit,DC=DomainName,DC=corp
```

## 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.

## PUPM SSH Device Cannot Set Password if UNAB is Installed on the Endpoint

If UNAB is installed on a CA Access Control for UNIX endpoint that is configured as PUPM SSH device, PUPM cannot set privileged accounts passwords on that endpoint, because PUPM runs the passwd command without specifying an argument.

**To work around this issue**

1. Create an ssh.xml file using the ssh_connector_conf.xml file. By default, this file is located in the following directory:

   ```
   \AccessControlServerDir\Connector Server\conf\override\sshdyn\
   ```

2. Locate the <param name="sCommand" value="passwd [%%user%%]" />tag.
3. Add the value "**-r files**" to the "sCommand" parameter. For example:

   ```
   <param name="sCommand" value="passwd -r files [%%user%%]" />
   ```

4. Save and close the file.

**Important!** Verify that you create an SSH device endpoint in the CA Access Control Enterprise Management Server and specify the file you created in the Configuration File field.

## Japanese and Korean Reports Viewable in InfoView Only

You can view the following CA Access Control Japanese and Korean reports only from InfoView and not from CA Access Control Enterprise Management:

- Baseline Resource Compliance
- Group Privileges

## PUPM Is Not FIPS140-2 and IPV6 Compliant

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

## 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 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.

## Report Portal Installation Fails If C:\temp Does Not Exist

By default, the Report Portal installation creates a log file on C:\temp. If this directory does not exist, the installation will fail without any feedback. Make sure this directory exists or customize the location of the log file.

## Reset Host Does Not Work If GHNODE Name Contains a Space

In CA Access Control Enterprise Management, if a host group (GHNODE) contains a space character in its name and you try to reset a host (HNODE) that is a member of that host group, the reset operation fails. CA Access Control returns the following message:

```
ERROR: Executing command: 'cr GHNODE GHNODE Name mem-("HNODE_Name") noexit' failed with error
code: 10057.
ERROR: Syntax error
ERROR: Invalid token Name
```

To work around this issue, do not include a space character in host group names.

## List of Values Does Not Refresh Automatically When Data Sources Change

On the Report Portal, the List of Values (LOV) in the standard reports CA Access Control provides out-of-the-box does not refresh automatically when data source environments change. This is a known issue with BusinessObjects. You must manually refresh LOVs when you schedule reports.

**To refresh these values manually**

1. Click Start, Programs, BusinessObjects XI Release 2, BusinessObjects Enterprise, BusinessObjects Enterprise Java Administration Launchpad.

   The Business Objects Business Intelligence platform Administration Launchpad opens in a web-browser.

2. Click Central Management Console.

   The Central Management Console Home page appears.

3. Click Folders in the Organize pane on the left.

   The Top Level Folders page appears.

4. Click the CA Reports folder.

   The CA Reports page appears, displaying the list of folders in CA Reports.

5. Click CA Access Control.

   A page displaying all of the reports available in this folder appears.

6. For each of the CA Access Control Crystal Reports displayed in the list, do the following:

   a. Click the report.

      A page displaying the properties of the report appears.

   b. Click Refresh Options in the Properties tab of the page.

      A list of properties you can refresh appears.

   c. Click Select All, click Refresh Report, then click Update.

      The selected Crystal Report refreshes.

## Refresh Mechanism in On-Demand Reports Stops Working After a Manual Refresh

On the Report Portal, if you follow the procedure for manually refreshing reports (see page 96) the refresh mechanism in On-Demand reports stops working. To correct this, change the global refresh setting as follows.

**To change the global refresh setting on Windows**

1. Open the Windows Registry Editor.
2. Navigate to the following registry key:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Business Objects\Suite 11.0\Crystal Reports\
   ```

3. Click Edit, New, Key.

   A new registry key appears.

4. Rename the key to *Database*.
5. In the new key, click Edit, New, String Value.

   A new registry entry of type REG_SZ appears.

6. Rename the entry to *AlwaysRefreshUniverseLOV*.
7. Double-click the entry and edit its Value data to 1.

   The new registry entry is set.

**To change the global refresh setting on Solaris**

1. Open a terminal window.
2. Source the env.sh file in the setup directory of the BusinessObjects installation path as follows:

   ```
   ../bobje/setup/env.sh
   ```

3. Enter **regedit** on the command line.

   The Mainwin registry appears.

4. Navigate to the following entry:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Business Objects\Suite 11.0\Crystal Reports\
   ```

5. Create a new key called Database.
6. In the Database key, create a new string value *AlwaysRefreshUniverseLOV* with the value 1.

**Note:** This is a global setting and has a performance impact on all BusinessObjects reports on this server. Values in input parameter lists are not cached in this configuration.

## Cannot Display r5.3 Audit Records

CA Access Control Endpoint Management cannot display audit records for eTrust Access Control r5.3. Use seaudit to display audit records from endpoints using this version of the product.

## 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.

## 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.

## "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.

## Do Not Use '$' Character for CA Access Control Enterprise Management Database Password

Because InstallAnywhere recognizes the $ character as the start of a variable, do not use the $ character in the CA Access Control Enterprise Management database password. If you use this character in the database password, the installation continues but does not successfully update the database tables.

## 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.

## 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.

## Report Portal Fails to Load a Service

**Valid on Windows**

After you restart a Windows Report Portal, the following message appears:

```
At least one service or driver failed during system startup.
Use Event Viewer to examine the event log for details
```

This message appears because the BusinessObjects Desktop Intelligence service does not load automatically. This does not affect the CA Access Control reporting service as it does not use this service.

To work around this issue, change the startup type of the service to *Manual*.

## 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.

## PUPM Windows Agentless Connector for Active Directory Search Limitations

When using the PUPM Windows Agentless connector to connect to Active Directory with more then 2000 users, the wild card (*) and retrieve all search options do not work. To search for users you must supply the specific account details.

## PUPM Windows Agentless Connector Does Not Support Windows 2000

The PUPM Windows Agentless connector does not support Windows 2000 Server.

## Define a Comma Separated List of Users When Creating a PUPM Application

When defining a PUPM application in CA Access Control Enterprise Management, use a comma (,) to separate the users in the Identifier Users list. Use the following format when adding users:

user1, user2, [..]

**Note:** On Windows, you must provide the fully qualified user name.

# 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.

# Appendix A: Third-Party License Agreements

This section contains the following topics:

# 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
- 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:

# 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.

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

(c) Copyright IBM Corporation 1999, 2002

All Rights Reserved

## AIX JRE 1.5.0

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

(c) Copyright IBM Corporation 1999, 2002

All Rights Reserved

# 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]

Copyright (c) 2005, Terence Parr

All rights reserved.

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

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

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

Neither the name of the 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.

# 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.

* 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

## Hibernate 3.2

Hibernate 3.2

This product is distributed with Hibernate 3.2  (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.

# 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

HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR 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.

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 $

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 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

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,

---- The implementation of the AES encryption algorithm in

src/lib/crypto/aes has the following copyright:

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:

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

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.

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.

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

# 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

This product includes zlib developed by Jean-loup Gailly and Mark Adler.

# 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.