CA Access Control Premium Edition

Release Notes

r12.0 SP1

Third Edition

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 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/support.

Documentation Changes

The following documentation updates have been made since the r12.0 release of this documentation:

Third Edition

The third edition of this documentation was released with CA Access Control r12.0 SP1 CR1.

The following topics were added or updated in this edition:

- Set Audit Mode by Group (see page 28)—New topic summarizes the audit by groups functionality.
- SQL Server 2005 Support (see page 29)—New topic introduces support for SQL Server 2005.
- Operating System Support for Endpoints (see page 31)—Updated topic adds Linux x64 support.
- CA Access Control Endpoint Management Requirements (see page 38)—Updated the supported endpoint browser versions and RDBMS types.
- CA Access Control Enterprise Management Requirements (see page 39)—Updated the supported endpoint browser versions and RDBMS types.

The following Windows endpoint, UNIX endpoint, and server component considerations were added to this edition:

- Change to Default Audit Value for Some Users (see page 58)
- Change to Default Value of AUDIT Property for GROUP Records (see page 58)
- install_base May Show Errors in a Linux 2.6 Installation (see page 69)
- Do Not Use Administration API Functions Inside a seosd Exit (see page 75)
- SAN Support (see page 69) (UNIX)
- SAN Support (see page 59) (Windows)

The following Windows endpoint known issues were added in this edition:

- Upgrades from r8 SP1 GA Are Not Supported (see page 60)
- Uninstall Does Not Remove CA License Files (see page 60)

Second Edition

The second edition of the documentation was released to coincide with the GA announcement of r12.0 SP1.

The following topics were added or updated in this edition:

- Complementary CA Enterprise Log Manager License (see page 18)—New topic replaced previous Complementary CA Audit License topic.
- CA Enterprise Log Manager Integration (see page 21)—New topic summarizes CA Enterprise Log Manager integration with CA Access Control.
- CA Access Control Endpoint Management Requirements (see page 38)—Updated the minimum available disk space required to install CA Access Control Endpoint Management on a Solaris computer.
- CA Access Control Enterprise Management Requirements (see page 39)—Updated the minimum available disk space required to install CA Access Control Enterprise Management on a Solaris computer.
- Features Affected (Windows) (see page 46)—Updated how non-FIPS mode affects the Password history (non-bidirectional) and Password history (bidirectional) features.

The following Windows endpoint, UNIX endpoint, and server component considerations were added to this edition:

- Audit Log Backup Files Are Protected by Default (see page 57)
- Cannot Define Record in SPECIALPGM Class for Incoming Network Interception Events (see page 57)
- Report Agent Is Not Supported on Linux IA64 and s390x (see page 68)
- Superuser Account Required for Server Components Installations (see page 75)

The following Windows endpoint, UNIX endpoint, and server component known issues were added to this edition:

- IA64 and x64 Architectures: Cannot Install a Prerequisite in Silent Mode (see page 59)
- HP-UX Requires an Updated Patch Level (see page 72)

  Note: This updated topic provides more detail about the recommended patches.
- Stat Interception Calls Not Supported on AIX Systems (see page 73)
- Uninstall or Unload Fails on Solaris 10 (see page 73)
- Control Characters May Cause an Application Exception (see page 75)

  Note: Non-English characters no longer cause an application exception.

- Uninstall Fails if You Are Not the Superuser (see page 80)
- Cannot Deploy Policies That Contain a Trailing Backslash (see page 80)
- Access Roles Are Not Supported in CA Access Control Enterprise Management (see page 80)
- Report Portal Fails to Load a Service (see page 81)
- Policy Script Validation Error Messages Are in a Different Language (see page 81)

The following server component known issues were removed from this edition:

- The Report Server Does Not Receive Endpoint Snapshots After Reinstallation
- Web Service Does Not Start After Installation
- Message "error connecting to web service" Appears After Installation

First Edition

The first edition of this documentation was released on the CA Access Control r12.0 SP1 media.

This guide was rewritten for the r12.0 SP1 release.

Contents

Chapter 1: Welcome

Welcome to the CA Access Control Premium Edition r12.0 SP1. 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 (see page 15)

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 Audit 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 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, Stack Overflow Protection (STOP), and the documentation.

  It also contains the advanced policy management server components.

- 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 documentation.

  It also contains the advanced policy management server components.

- CA Access Control Premium Edition Server Components for Windows

  Contains CA Access Control Endpoint Management, CA Access Control Enterprise Management, CA Access Control reporting service, and the BusinessObjects XI Release 2.1 installation files for Windows.

- CA Access Control Premium Edition Server Components for Solaris

  Contains CA Access Control Endpoint Management, CA Access Control Enterprise Management, CA Access Control reporting service, and the BusinessObjects XI Release 2.1 installation files for Solaris.

- CA Access Control Third Party Components for Windows

  Contains the JDK and JBoss installation files. These software installations are required before you can install CA Access Control Premium Edition Server Components on Windows.

- CA Access Control Third Party Components for Solaris

  Contains the JDK and JBoss installation files. These software installations are required before you can install CA Access Control Premium Edition Server Components on Solaris.

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 disks:

- 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 documentation.

  It also contains the advanced policy management server components for use with CA Access Control Premium Edition.

- 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, Stack Overflow Protection (STOP), and the documentation.

  It also contains the advanced policy management server components 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 the JDK and JBoss installation files. These software installations are required before you can install CA Access Control Server Components on Windows.

- CA Access Control Third Party Components for Solaris

  Contains the JDK and JBoss installation files. These software installations are required before you can install CA Access Control Server Components on Solaris.

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

  The following chapters apply only to CA Access Control Premium Edition:

  - Chapter 6: Installing Enterprise Management
  - Chapter 7: Installing Enterprise Reporting
  - Chapter 8: Integrating with CA Enterprise Log Manager
  - Chapter 9: Installing a Disaster Recovery Deployment
  - Chapter 10: Migrating PMDs to an Advanced Policy Management Environment

  Other chapters also describe or make references to features that only apply to CA Access Control Premium Edition. For example, the Report Agent and advanced policy management server components, which are part of the endpoint installation, are only relevant for CA Access Control Premium Edition.

- Endpoint Administration Guide for Windows

  The entire guide applies to CA Access Control.

- Endpoint Administration Guide for UNIX

  The entire guide applies to CA Access Control.

- Reference Guide

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

- selang Reference Guide

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

- Enterprise Administration Guide

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

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:

CA Enterprise Log Manager Integration

Integration with CA Enterprise Log Manager lets you send CA Access Control audit events from each of your endpoints for collection and reporting by CA Enterprise Log Manager.

You can set CA Access Control to send audit events from the local endpoint's audit file to a remote audit queue on the Report Server. You can then set a CA Enterprise Log Manager connector to connect with the audit queue and pull events (messages) from it. CA Enterprise Log Manager processes these events and sends them to the CA Enterprise Log Manager Server.

CA Enterprise Log Manager integration is supported by the CA Access Control installation.

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

Remote and Enhanced Audit Configuration Management

CA Access Control offers remote audit configuration for the audit.cfg and auditrouteflt.cfg files through the selang configuration environment. This means you can use a unified, cross-platform mechanism to remotely manage your endpoints' audit configuration settings.

Note: For more information about remote audit configuration, see the *Endpoint Administration Guide* for your platform.

The audit.cfg file filters audit records on a host by defining audit records that should not be sent to the audit file. The audit.cfg file offers enhanced syntax to let you accurately filter a wider range of audit records. You can filter the following events:

- General resource access
- Service connection events
- (New) Login and logout events

  Note: Logout events are only supported on UNIX.
- (New) Administrator events
- (New) User trace records

Note: For more information about the audit log filter, see the *Reference Guide*.

Session ID Tracking

Audit records that include the name of an accessor, also include the user login session ID. These are audit records of the following type:

- Login
- General resource
- CA Access Control Shutdown
- CA Access Control Remote Shutdown
- User trace
- TCP connect

If you use CA Enterprise Log Manager to collect and report on CA Access Control audit logs, you can filter by a user session and time to tie the activity to a specific session.

Event Routing to Windows Event Log

CA Access Control can route events to the Windows application log (in addition to sending the events to the CA Access Control audit log). This lets you use native event management tools to view and interrogate CA Access Control events. You can route both Policy Model audit events and CA Access Control audit events to the Windows application log.

On Windows Server 2008, CA Access Control can also send audit events to a specific audit files channel. You can send audit events to both the audit files channel and the Windows application log. The CA Access Control audit file channels are named "CA\AccessControl\AuthorizationEngine\Audit" and "CA\AccessControl\PolicyModels\Audit".

Note: For more information about routing audit events to the Windows event log, see the *Endpoint Administration Guide for Windows*.

Event Routing to the UNIX syslog

CA Access Control can route events to the UNIX syslog (in addition to sending the events to the CA Access Control audit log). This lets you use native event management tools to view and interrogate CA Access Control events. Use the selogrd.cfg file to specify that you want to send audit events to the syslog.

Note: For more information about selogrd.cfg, see the *Reference Guide*.

User Trace for Windows

The existing user trace functionality for Windows has been enhanced to provide the same functionality that is available on UNIX endpoints. You can set a user to be traceable and trace user activity. Each time CA Access Control writes a trace message, a corresponding audit record is written to the audit log. Also, the audit filtering file offers new filtering syntax to let you filter these audit trace records.

Note: For more information about user trace for Windows, see the *Endpoint Administration Guide for Windows*.

User Trace Filtering on UNIX

The audit filter configuration file (audit.cfg) also filters user trace records. CA Access Control only uses the trace filter file trcfilter.init to filter trace records that are written to the seosd.trace file.

Note: For more information about how to migrate your user trace filtering from trcfilter.init to audit.cfg, see the *Endpoint Administration Guide for UNIX*.

Password Verification Audit

A new audit type lets CA Access Control add audit records for failed password verifications. If the PASSWORD class is active, CA Access Control writes failed password verification attempts and the reason for failure (how the password did not match the password policy) to the audit log file.

Advanced Policy Management Enhancements

CA Access Control offers increased support for using advanced policy management. This includes improvements to the CA Access Control Enterprise Management interface, disaster recovery tools and documentation, and additional functionality.

Administrative Scoping

Predefined roles in CA Access Control Enterprise Management provide a basic set of roles that you can assign to administrators in your enterprise according to your requirements. Out-of-the-box, CA Access Control Enterprise Management comes with the following roles:

- **System Manager**—The role of the CA Access Control Enterprise Management superuser.
- **CA Access Control User Manager**—Responsible for user management in CA Access Control Enterprise Management: creating and managing users and groups, and assigning CA Access Control Enterprise Management roles to users.
- **CA Access Control Policy Manager**—Responsible for creating policies.
- **CA Access Control Policy Deployer**—Responsible for the deployment of policies across the environment.
- **CA Access Control Host Manager**—Responsible for the definition of hosts and logical host groups.

Note: For more information about CA Access Control Enterprise Management roles, see the *Enterprise Administration Guide*.

Disaster Recovery

Changes to existing utilities and scripts and new selang commands support disaster recovery procedures more comprehensively:

- The sepmd utility lets you restore a Policy Model from a backup.

  A backup option was already included in r12.0.
- selang support lets you remotely back up and restore a Policy Model.
- The dmsmgr utility lets you restore advanced policy management server components.

Also, the documentation provides complete information on setting up a disaster recovery solution for your advanced policy management implementation.

Note: For more information on disaster recovery for advanced policy management, see the *Implementation Guide*. For more information on utilities, see the *Reference Guide*. For more information on selang commands, see the *selang Reference Guide*.

Policy Verification

When CA Access Control deploys a policy on a host, by default, it first checks to see whether the deployment script can execute on the host before it actually runs the deployment script on the endpoint's database. If the verification of the policy deployment script fails, the policy does not deploy. This lets you avoid situations where you have to resolve the deployment of a policy that deployed with errors.

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

Policy Deletion

Advanced policy management tools (CA Access Control Enterprise Management and policydeploy utility) let you delete policies and policy versions.

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

Deviation Calculator Use

The deviation calculator (devcalc) is now routinely triggered after each heartbeat (a configurable setting of policyfetcher). This means that you do not need to manually schedule the deviation calculator to run using a cron job on UNIX or a scheduled task on Windows. This improved solution provides a better integration of the deviation calculator with the advanced policy management solution.

Note: The Report Agent no longer triggers the deviation calculator. For more information, see the *Enterprise Administration Guide*.

Policy Script Comments

You can add comments to your policy deployment and undeployment scripts (selang commands) in the same way you add comments to any other selang script file. Preface any comment line with the hash character (#).

Sample Policies Out-Of-The-Box

Sample policies that come with CA Access Control provide you with segregation of duties and best practices that we recommend for the protection of operating system (OS) and application resources. Each policy includes comments that explain the policy's purpose and the rules it contains.

Sample policies are available for the following common applications and operating systems:

- Applications:
  - Apache
  - JBoss application server
  - CA Access Control Web Service
  - Microsoft SQL Server
  - Oracle Database 10g
- Operating systems:
  - AIX
  - HP-UX
  - Red Hat Enterprise Linux
  - SuSe Linux Enterprise Server
  - Sun Solaris
  - Windows 2003
- Virtualization systems:
  - VMware ESX Server
  - Hyper-V
  - Solaris 10 Zones

Note: For more information about sample policies, see the *Endpoint Administration Guide* for your platform.

UNIX Unload Readiness Reports

New reports let you view a prediction of whether you could unload CA Access Control on each of your UNIX endpoints. The reports also detail what was holding back each host from being ready to unload when this information was received from the endpoint. These reports can help you manage upgrading CA Access Control for UNIX across your enterprise.

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

Bypass Propagation on UNIX

A new program type for specified programs (PGMTYPE property of the SPECIALPGM class) lets you propagate the program type of the parent program to all the child programs it executes. For example, if you provide the parent program with a network event bypass (pbn program type), you can also add the propagate program type to make sure that any programs the parent program calls also receive the network event bypass.

Note: Security privilege propagation works with PBF, PBN, DCM, and SURROGATE privileges only.

Console Install for Server Components

A console install lets you install CA Access Control Server Components from a text-only terminal. For example, you can install on UNIX without needing to use graphical libraries.

Note: For more information on how to use the console install for each of the server components, see the *Implementation Guide*.

Set Audit Mode by Group

You can use the AUDIT_MODE property for a group or enterprise group to specify which events CA Access Control audits for group members.

Note: When CA Access Control determines the audit mode for a user, it checks the audit mode of the USER or XUSER record and any profile groups the user is assigned to before it checks the audit mode of the group or enterprise group.

Linux x64 Support

CA Access Control support Linux x64 architecture platforms.

Note: For detailed information and supported versions, see OS support for endpoints (see page 31).

SQL Server 2005 Support

RDBMS support for CA Access Control Enterprise Management and the CA Access Control Report Server was extended to include Microsoft SQL Server 2005.

Localization

In addition to the English release of this product, CA Access Control r12.0 SP1 is translated into three languages-Japanese, Korean, and Simplified Chinese-for both UNIX and Windows platforms. The localized versions are available on the CA Access Control media with the English version. You can select the language of your installation during setup.

Chapter 3: Operating System Support

This section contains the following topics:

Operating System Support for Endpoints

The following table lists the supported operating systems for CA Access Control endpoints:

Platform	Architecture	Version	Update Level	Notes
Windows	x86	2000	SP4 with Update Rollup 1	With or without Active Directory Services
		XP Professional	SP2	
		Server 2003	SP1, SP2, and R2 with SP2	Standard or Enterprise editions With or without Active Directory Services
		Cluster Server 2003	SP1	Compute Cluster Edition
		Server 2008	SP1	Standard or Enterprise editions
	x64	Server 2003	SP1, SP2, and R2 with SP2	Standard or Enterprise editions
		Cluster Server 2003	SP1	Compute Cluster Edition
		Server 2008	SP1	Standard or Enterprise editions With or without Hyper-V
	Itanium (IA64)	Server 2003	SP1 and SP2	Enterprise Edition
Microsoft Virtual Server	x86	2005	R2	

Platform	Architecture	Version	Update Level	Notes
AIX	IBM POWER	5.2		32- and 64-bit
		5.3		32- and 64-bit
	IBM POWER	6.1		32- and 64-bit
HP-UX	PA-RISC	11i v1 (11.11)		32- and 64-bit
		11i v1 (11.11) TCB		32- and 64-bit running Trusted Computing Base
		11i v2 (11.23)		
		11i v2 (11.23) TCB		Running Trusted Computing Base
		11i v3 (11.31)		
		11i v3 (11.31) TCB		Running Trusted Computing Base
	Itanium (IA64)	11i v2 (11.23)		
		11i v2 (11.23) TCB		Running Trusted Computing Base
		11i v3 (11.31)		
		11i v3 (11.31) TCB		Running Trusted Computing Base
Sun Solaris	SPARC	8		32- and 64-bit
		9		32- and 64-bit
		10	Base, Update 1 to 6	64-bit
	x64	10	Base, Update 1 to 6	
Linux	x86	RHEL 3 (AS & ES)	Base and Update 1 to 9	RHEL is Red Hat Enterprise Linux
		RHEL 4 (AS & ES)	Base and Update 1 to 7	
		RHEL 5 (BS & AP)	Base and Update 1, 2	
		SLES 9	Base, SP1, SP2, and SP4	SLES is SuSe Linux Enterprise Server
		SLES 10	Base, SP1 and	Without XEN

Platform	Architecture	Version	Update Level	Notes
			SP2	support
	x64	RHES 4 (AS & ES)	Base and Update 1 to 7	
		RHEL 5 (BS & AP)	Base and Update 1, 2	
		SLES 9	Base, SP1, SP2, and SP4	SLES is SuSe Linux Enterprise Server
		SLES 10	Base, SP1 and SP2	Without XEN support
	AMD64/EM64T	RHEL 3 (AS & ES)	Update 4 to 9	
		RHEL 4 (AS & ES)	Base and Update 1 to 7	
		RHEL 5 (BS & AP)	Base and Update 1, 2	
		SLES 9	Base, SP1, SP2 and SP4	
		SLES 10	Base, SP1 and SP2	
	Itanium (IA64)	RHEL 3 (AS & ES)	Base, Update 3, 7, 8, and 9	
		RHEL 4 (AS & ES)	Base and Update 2 to 7	
		RHEL 5 (BS & AP)	Base and Update 1, 2	
		SLES 9	SP3, SP4	
		SLES 10	Base, SP1 and SP2	
	Z-series (s390x)	RHEL 3 (AS & ES)	Base, Update 4, 7, 8, and 9	
		RHEL 4 (AS & ES)	Base and Update 1 to 7	
		RHEL 5 (BS & AP)	Base and Update 1, 2	
		SLES 9	SP2 to SP4	
		SLES 10	Base, SP1 and SP2	Without XEN support

Platform	Architecture	Version	Update Level	Notes
VMware	x86	ESX Server 3		Base functionality
		ESX Server 3.0.1		Base functionality
		ESX Server 3.02		Base functionality
		ESX Server 3.5	Base, SP1 and SP2	Base functionality

Note: This list of supported operating systems *does not* apply to the advanced policy management server components (DMS and DH), which are only supported on CA Access Control Enterprise Management supported platforms.

Note: For an updated list of supported operating systems, refer to the CA Access Control Compatibility Matrix that is available from the CA Access Control product page on CA Support Online at http://ca.com/support.

Operating System Support for Server Components

The following sections list operating system support for CA Access Control server components.

Note: For an updated list of supported operating systems, refer to the CA Access Control Compatibility Matrix that is available from the CA Access Control product page on CA Support Online at http://ca.com/support.

CA Access Control Endpoint Management

The following table lists the supported operating systems for CA Access Control Endpoint Management:

Platform	Architecture	Version	Update Level	Notes
Windows	x86	Server 2003	SP1, SP2, and R2 with SP2	Enterprise, Standard, or Web editions
Sun Solaris	SPARC	9		32- and 64-bit
		10	Base, Update 1 to 5	64-bit

CA Access Control Enterprise Management

The following table lists the supported operating systems for CA Access Control Enterprise Management:

Platform	Architecture	Version	Update Level	Notes
Windows	x86	Server 2003	SP1, SP2, and R2 with SP2	Enterprise Edition
Sun Solaris	SPARC	9		32- and 64-bit
		10	Base, Update 1 to 5	64-bit

Note: This list of supported operating systems also applies to the advanced policy management server components (DMS and DH), which are not officially supported on endpoint supported operating systems.

CA Access Control Enterprise Reporting

Enterprise reporting requires you set up the following server components:

- **A central database**—A supported third-party RDBMS (relational database management system).

  Note: For information about operating system support for your RDBMS, see the product's documentation.

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

  Note: For information about operating system support for the Report Portal, see the *CA Business Intelligence Installation Guide*.

- **Report Server**—CA Access Control Premium Edition software that processes all of your endpoint data and sends it to the central database for storage.

  The Report Server is supported on the following operating systems:

Platform	Architecture	Version	Update Level	Notes
Windows	x86	Server 2003	SP1, SP2, and R2 with SP2	Enterprise Edition
Sun Solaris	SPARC	9		32- and 64-bit
		10	Base, Update 1 to 5	64-bit

Note: You can install all of the enterprise reporting server components on the same computer. If you do this, you have to make sure that your operating system supports all three components, and that the combined system requirements are met.

Operating System Support for CA DSM Delivery

CA Access Control supports endpoint installations using CA Desktop and Server Management (CA DSM) r11.2 C3.

CA Access Control supports CA DSM delivery on all Linux and Windows operating systems that both CA Access Control endpoints *and* the CA DSM Software Delivery Agent support.

Note: For a list of operating systems CA DSM Software Delivery Agent supports, see CA Support Online at http://ca.com/support.

Chapter 4: System Requirements

This section contains the following topics:

Windows Endpoint Requirements

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

- **Processor**—Intel-based Pentium 4 PC 1.6 GHz
- **Memory**—1 GB 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:

	Windows	**Solaris**
Processor	Pentium PC 266 MHz	SPARC Workstation 440MHz
Memory	1 GB RAM	1 GB RAM
Available disk space	200 MB	200 MB

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

- **JDK**—Java Development Kit (JDK) 1.4.2_12 or higher
- **Application server**—JBoss Application Server version 4.0.5.GA
- **CA Access Control**—Latest version of endpoint installation

On the end user's computer you need to have the following as your web browser:

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

CA Access Control Enterprise Management Requirements

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

	Windows	Solaris
Processor	Pentium PC 266 MHz	SPARC Workstation 440MHz
Memory	2 GB RAM	2 GB RAM
Available disk space	2 GB	2 GB

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

- **JDK**—Java Development Kit (JDK) 1.4.2_12 or higher
- **Application server**—JBoss Application Server version 4.0.5.GA
- **RDBMS**—Oracle Database 10g or Microsoft SQL Server 2005

  Note: This central database does not need to be installed on the same computer.
- **CA Access Control**—Latest version of endpoint installation

On the end user's computer you need to have the following as your web browser:

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

CA Access Control Enterprise Reporting Requirements

Enterprise reporting requires you set up the following server components:

- **A central database**—A supported third-party RDBMS (relational database management system).

  Note: For information about system requirements for your RDBMS, see the product's documentation.

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

  Note: For information about minimum system requirements for the Report Portal, see the *CA Business Intelligence Installation Guide*.

- **Report Server**—CA Access Control Premium Edition software that processes all of your endpoint data and sends it to the central database for storage.

Note: You can install all of the enterprise reporting server components on the same computer. If you do this, you have to make sure that your operating system supports all three components, and that the combined system requirements are met.

The minimum requirements for the Report Server computer are:

	Windows (recommended)	**Solaris**
Processor	Pentium PC 2 GHz (4-core Intel- or AMD-based chip)	SPARC Workstation 440MHz
Memory	2 GB RAM (4 GB RAM)	2 GB RAM
Available disk space	30 GB	10 GB

In addition, the Report Server computer should have the following software installed:

- **JDK**—Java Development Kit (JDK) 1.4.2_12 or higher
- **Application server**—JBoss Application Server version 4.0.5.GA
- **RDBMS**—Oracle Database 10g or Microsoft SQL Server 2005

  Note: This central database does not need to be installed on the same computer.

- **CA Access Control**—Latest version of endpoint installation

Chapter 5: Documentation

This section contains the following topics:

Guides

The PDF guides for CA Access Control Premium Edition r12.0 SP1 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

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 documentation is also available in HTML format that 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
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). For example, the following means *either* a user name *or* a group name: {*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. **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.

Chapter 6: 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 (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. Password validation with CAPKI SHA-1 and fall through to crypt	Saved as CAPKI SHA-1. Password validation with CAPKI SHA-1 only
Password history (bidirectional)	Default symmetric key encryption. Password validation with default symmetric key encryption	CAPKI AES symmetric key encryption. 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 7: 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.

Default Installation Location

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

C:\Program Files\CA\AccessControl

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.

Versions You Can Upgrade From

You can upgrade to CA Access Control r12.0 SP1 for Windows from r12.0, r8 SP1, and r5.2.

Dictionary for Password Checks

CA Access Control installs a dictionary file for password quality checking. This file is taken from the standard UNIX installation and is generally available and widely known.

We strongly recommend that you extend or replace this file with a more sophisticated dictionary file.

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 now 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.

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 XP SP2, 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*.

Recommended Microsoft Hotfix

We strongly recommend you apply Microsoft Hotfix KB912143 on Windows XP Professional SP2 and on Windows 2003 Server SP1 (Standard, Enterprise, Web editions).

IA64 Feature Support Limitations

The following features are not supported on IA64 platforms:

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

x64 Feature Support Limitations

The following features are not supported on x64 platforms:

- Unicenter TNG migration and integration
- Mainframe password synchronization
- Process interception (class PROCESS functionality)
- Impersonation interception (class SURROGATE functionality)

Registry Value Protection Is Not Supported on All Windows Platforms

Registry value protection (REGVAL class) is not supported on Windows 2000 and Windows XP. You should continue to use the REGKEY class on these operating systems. To protect a registry value, you need to protect its parent key using a REGKEY database object.

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.

Default for TERMINAL Resource Resolution Has Changed

The default value for the TerminalSearchOrder configuration setting, which is stored in HKLM\SOFTWARE\ComputerAssociates\AccessControl\SeOSD, has changed in r12.0 SP1 to *nameonly*.

If you upgrade from an earlier release where there are no TERMINAL resources named using an IP address, CA Access Control changes the TerminalSearchOrder configuration setting during upgrade to *nameonly*.

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.

FIPS 140-2 Library Upgrade

CA Access Control r12.0 SP1 uses CAPKI 4.0 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 4.0 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)
FIPS Encryption Libraries (see page 43)
FIPS Algorithms Used (see page 44)
Storage of Keys and Certificates (see page 44)

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.

Encryption Mode Communication Limitations

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

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.

System Accounts Do Not Have a Unique Login Session ID

The system account always has the same login session ID. These login session IDs are identical on all Windows computers.

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.

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.

Windows Endpoint Known Issues

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

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.

IA64 and x64 Architectures: Cannot Install a Prerequisite in Silent Mode

CA Access Control installation cannot install the prerequisite Microsoft Visual C++ 2005 Redistributable Package in silent mode on x64 and Itanium (IA64) architectures. To work around this issue, install the Microsoft Visual C++ 2005 Redistributable Package before you start a silent installation of CA Access Control on these architectures.

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.

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).

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

CA Anti-Virus r7 on Linux x86

If you plan to run CA Access Control and CA Anti-Virus r7 together on a Linux x86 machine, you must contact CA Technical Support for a compatibility patch. You must install this compatibility patch before installing CA Access Control on the host.

Versions You Can Upgrade From

You can upgrade to CA Access Control r12.0 SP1 for UNIX from r12.0, r8 SP1, and r5.3.

RPM Package Upgrade from r12.0 CR1

If you are upgrading from a CA Access Control r12.0 CR1 RPM package to r12.0 SP1, you must use the --oldpackage rpm command option as follows:

```
rpm -U CAeAC*rpm –oldpackage
```

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 kernel 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 ([set the alternate Installation Path variable]), 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.

Linux pam_tally Setup

CA Access Control no longer sets up Linux during install time to use the Linux pam_tally option to write failed logins to /var/log/faillog. CA Access Control serevu option works with pam_seos module by default and does not need this option. If you plan to use the native serevu system option with pam_tally (and not CA Access Control pam_seos module), and the Linux OS does not write by default to /var/log/faillog, you need to setup pam_tally manually.

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.

Configure PAM to Work on AIX

When you use PAM to authenticate users for CA Access Control purposes (auth_login = pam), CA Access Control needs to use the PAM API library.

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 configure PAM to work on AIX

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

   cd /usr/lib

2. This archive contains the AIX PAM shared library (shr.o).
3. Extract shr.o from libpam.a to /usr/lib:

   ar -xv libpam.a

4. Rename shr.o to libpam.o:

   mv shr.o libpam.o

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)
```

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*.

Compiling API Samples

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

FIPS 140-2 Library Upgrade

CA Access Control r12.0 SP1 uses CAPKI 4.0 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 4.0 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)
FIPS Encryption Libraries (see page 43)
FIPS Algorithms Used (see page 44)
Storage of Keys and Certificates (see page 44)

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

On UNIX, 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.

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 Is Not Supported on Linux IA64 and s390x

The Report Agent daemon is not supported on Linux Itanium (IA64) and Z-series (s390x). CA Access Control does not install the Report Agent on these operating systems regardless of the selections you make during installation.

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.

install_base May Show Errors in a Linux 2.6 Installation

Valid on Linux

When you use the install_base script with the -all or -uni packages to install CA Access Control, by default the installation script sets the enf_register token in the seos.ini file to yes.

If you use the install_base script with the -all or -uni packages on a Linux 2.6 kernel and you do not want to register seosd to Unicenter NSM Event Notification Facility (ENF), set the enf_register token in the seos.ini file to no. If you do not set the enf_register token to no, the installation script uses the currently installed version of the libenf.so library; if this version is for the Linux 2.4 kernel and the current kernel is of version 2.6, libenf.so might display the following error message:

ERROR: Can't open /proc/ksyms 2 (No such file or directory)

This errors does not indicate that there are issues with the functionality of the installed product and you can safely ignore it.

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 that SAN is accessible from only a single host.
- A SAN, and that SAN is accessible from only the single host where CA Access Control is running.

CA Access Control does *not* support a SAN which multiple hosts access, as follows:

- CA Access Control executes on one host connected to the SAN does not protect files on that SAN from access by other hosts that are connected to the SAN.
- CA Access Control behavior is unspecified when you install it on a SAN and it is executed from multiple connected hosts.

UNIX Endpoint Known Issues

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

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.

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.

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*

Native Package Upgrade from r12.0 CR1 Does Not Work

You cannot use native packages to upgrade from r12.0 CR1 to r12.0 SP1 on Linux.

Use regular script installation to upgrade from r12.0 CR1. On Linux, you can also use the --oldpackage option when you upgrade using RPM packaging to work around this issue.

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.

Uninstall or Unload Fails on Solaris 10

Before you unload or uninstall CA Access Control, you should make sure that CA Access Control can unload. Check for any blocking system calls and, if they exist, stop the related services before you unload or uninstall CA Access Control.

On Solaris 10, if you have Solaris Management Console installed, a related service called wbem spawns a Java process that keeps an open system call, waiting for events. If the wbem service starts after CA Access Control, CA Access Control will fail to unload. When you check for blocking system calls you will see the Java process. To unload CA Access Control in this case, enter the following commands to restart the wbem service:

```
/etc/init.d/init.wbem stop
/etc/init.d/init.wbem start
```

You should then check for blocking system calls again to make sure that there are no other blocking system calls. If there are none, you can now unload or uninstall CA Access Control.

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).

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.

Supported JDK and JBoss Versions

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

Automatic Generation of Policy Undelopy 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*).

Oracle Database XE Does Not Resolve the database SID as Required

Oracle Database XE does not resolve the Oracle database SID to service name in JDBC database URLs as required by CA Access Control Enterprise Management. This means that you may need to ensure that the Oracle database SID matches the Oracle database service name (SID=SERVICE_NAME) to work around this issue.

To set this, you need to modify the Oracle listener configuration file (listener.ora).

Required Upgrade Sequence

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

To upgrade CA Access Control server components

1. Upgrade the Report Server.
2. Upgrade advanced policy management server components.

   This includes the DMS, all of the attached DHs, and the disaster recovery components.
3. Upgrade the computer serving CA Access Control web-based interfaces (Enterprise Management or Endpoint Management).

   Upgrade CA Access Control on this computer before you upgrade CA Access Control Endpoint Management or CA Access Control Enterprise Management.

You can now upgrade your endpoints.

Superuser Account Required for Server Components Installations

To install any of the CA Access Control server components (Report Server, Endpoint Management, Enterprise Management), you must log in as the superuser (root on UNIX or Administrator on Windows).

Do Not Use Administration API Functions Inside a seosd Exit

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

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).

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.

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 77) 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.

Tibco Directory Requires Manual Uninstall

Valid on Windows

On Windows, when you uninstall the CA Access Control Report Server, you must also remove the Tibco directory manually.

If you do not remove this directory, when you reinstall the Report Server, the Tibco service does not start.

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.

Non-English Installation Displays Some English Text

CA Access Control Enterprise Management installation in non-English mode displays some English text.

Uninstall Displays CA Identity Manager Uninstall Screen

When you uninstall CA Access Control Enterprise Management, the wizard displays an CA Identity Manager uninstall screen.

Start Menu Shortcuts Are Incorrect When You Install to Custom Ports

Valid on Windows

When you install CA Access Control Enterprise Management or CA Access Control Endpoint Management on Windows with a JBoss Application Server using a non-default HTTP port, you need to manually modify the Start menu shortcuts after installation for the URL to include the correct JBoss port.

You need to do this regardless of whether you specified the correct JBoss port during installation.

Uninstall Fails if You Are Not the Superuser

To uninstall any of the CA Access Control server components (Report Server, Endpoint Management, 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.

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.

Appendix A: Third-Party License Agreements

This section contains the following topics:

AEScrypt 0.7.0

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

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

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

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

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

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

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

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

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

Axis 1.4

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

Apache License

Version 2.0, January 2004

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

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions.

Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

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

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

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

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

END OF TERMS AND CONDITIONS

CRC32

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

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


/*

 * Copyright (c) 2003 Markus Friedl.   All rights reserved.

 *

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

 * modification, are permitted provided that the following conditions

 * are met:

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

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

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

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

 *      documentation and/or other materials provided with the distribution.

 *

 * THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS|&"&| AND ANY EXPRESS OR

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

 * OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.

 * IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,

 * INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT

 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
```

```
 * DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED
AND ON ANY

 * THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR
TORT

 * (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF
THE USE OF

 * THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH
DAMAGE.

 */
```

Perl2Exe

A separate registered copy of Perl2Exe must be obtained for each workstation on which Perl2Exe will be used even if such use is only temporary.

Exe files created by Perl2Exe are shipped with Run-time portions of Perl2Exe. No registered user, nor anyone else, may alter or modify the generated Exe files. You cannot give anyone else permission to modify the Exe files.

Exe files generated by the registered version of Perl2exe may be freely distributed.

If you use this software after the 30 day evaluation period a registration fee is required. You may not distribute Exe files created by the shareware evaluation version of Perl2Exe. Unregistered use of Perl2Exe after the 30 day evaluation period is in violation of copyright laws.

You can make as many copies of the shareware evaluation version of this software and documentation as you wish; give exact copies of the original shareware version to anyone; and distribute the shareware version of the software and documentation in its unmodified form via electronic means. There is no charge for any of the above.

You are specifically prohibited from charging, or requesting donations, for any such copies, however made; and from distributing the software and/or documentation with other products (commercial or otherwise) without prior written permission.

POSIX Threads for Win32 2.8.0

Pthreads-win 32 v2.8.0 is an open source library that is used with the CA software. The Pthreads library is not owned by CA, Inc. Use, copying, distribution and modification of the Pthreads library is governed by the GNU Lesser General Public License v. 2.1. A copy of the LGPL license can be found in the http://opensrcd.ca.com/ips/777_1/ directory from which the Pthreads library 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 Pthreads library available at http://opensrcd.ca.com/ips/777_1/. Use of the CA software 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 code except as may be expressly set forth in the CA EULA. The Pthreads library 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 Pthreads library 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 Pthreads library.

Click on the 'I agree' button below to indicate your agreement to the foregoing and continue with the installation of the Pthreads library. Clicking on the 'I disagree' button will cause the installation of the CA software to cease.

SHA-1

This product includes software developed by Internet Society. The software is distributed in accordance with the following license agreement.

Xerces-C++ Version 2.8.0

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

Apache License

Version 2.0, January 2004

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

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions.

Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

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

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

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

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

END OF TERMS AND CONDITIONS

XScreenSaver