CA Access Control

Troubleshooting Guide

12.8

technologies

Third-Party Notices

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

Sample Scripts and Sample SDK Code

The Sample Scripts and Sample SDK code included with the CA Access Control product are provided "as is", for informational purposes only. Adjust them to your specific environment and do not use them in production without running tests and validations.

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

CA Technologies Product References

This document references the following CA Technologies products:

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

Documentation Conventions

The CA Access Control documentation uses the following conventions:

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

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

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

Format	Meaning
Between braces ({})	Set of mandatory operands
Choices separated by pipe (|).	Separates alternative operands (choose one). 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.

File Location Conventions

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

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

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

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Documentation Changes

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

- Required packages are Missing for Linux Installation
- MALLOC_ARENA_MAX=1 Not Working on RedHat Linux 6.2
- Cannot Create Endpoints Due to Incorrect Parameter
- PUPM Feeder Polling Inconsistent In a Load Balancing Environment

Contents

Chapter 1: Introduction

This section contains the following topics:

About this Guide

This guide provides solutions and workarounds to some common problems you may have with CA Access Control.

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

Who Should Use this Guide

This guide was written for security and system administrators who encounter problems when they implement, configure, and maintain a CA Access Control-protected environment.

Chapter 2: Installing CA Access Control Endpoints and Server Components

This section contains the following topics:

Configure the Java Connector Server for JDK 1.7

Symptom:

What are the modifications I need to complete to support JDK 1.7 U17 on the Enterprise Management Server.

Solution:

To support JDK 1.7 U17on the Enterprise Management Server you must modify the Java Connector Server (JCS). Do the following:

Windows 2008 Server 32 bit operating system

1. From a command line window, run regedit.

   The Registry Editor opens.

2. Navigate to the following location:

   `HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Identity Manager\Procrun 2.0\im_jcs\Parameters`

3. Select the environment registry key and modify the value as follows:

   `PATH=%PATH%;C:\Program Files\Java\jdk1.7.0_17\jre\bin`

4. Navigate to the following location:

   `HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Identity Manager\Procrun 2.0\im_jcs\Parameters\Java`

5. Select the jvm registry key and modify the value as follows:

   `C:\Program Files\Java\jdk1.7.0_17\jre\client\jvm.dll`

Windows 2008 Server R2 64 bit operating system

1. From a command line window, run regedit.

   The Registry Editor opens.

2. Navigate to the following location:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Computer Associates\Identity Manager\Procrun 2.0\im_jcs\Parameters`

3. Select the environment registry key and modify the value as follows:

   `PATH=%PATH%;C:\Program Files (x86)\Java\jdk1.7.0_17\jre\bin`

4. Navigate to the following location:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Computer Associates\Identity Manager\Procrun 2.0\im_jcs\Parameters\Java`

5. Select the jvm registry key and modify the value as follows:

   `C:\Program Files (x86)\Java\jdk1.7.0_17\jre\bin\client\jvm.dll`

Red Hat Linux x64 operating system

1. Remove all existing links to the JDK.
2. Verify that the Java Connector Server is not running.
3. Change the /usr/bin/java link to point to Java 7. Follow this example:

```
# ln -s /opt/Java/jdk1.7.0_17/bin/java /usr/bin/java
# ln -s /opt/Java/jdk1.7.0_17/bin/java /bin/java

# ls -l /usr/bin/java
lrwxrwxrwx 1 root root 30 Apr  8 12:05 /usr/bin/java ->
/opt/Java/jdk1.7.0_17/bin/java
# which java
/usr/bin/java
```

4. Remove the following directory:
   `/opt/CA/AccessControlServer/Connector_Server/jvm`
5. Start the Java Connector Server.
   `./im_jcs.new start`

Required packages are Missing for Linux Installation

Symptom:

The installation fails because required Linux packages are missing.

Solution:

Use the rpm --requires and the rpm --whatprovides commands to verify package dependencies, and install missing packages.

Note: For more information on required packages, see also Required 32 bit Packages for installing the Enterprise Management Server on Red Hat Linux 6 in the Installation Considerations section of the *CA Access Control Release Notes*.

rpm --requires—Detect Library Dependencies

When installing Enterprise Management on Linux, you want to know on which libraries the CAeAC package depends.

The command uses the following syntax:

```
rpm -qp --requires package
```

The command has the following parameters:

-q

Specifies that you want to query RPM package information.

-p

Query a RPM package file. Also retrieves information on packages that are not installed.

--requires *package*

Retrieves the dependencies that are required by the package.

Example

You want to retrieve dependency information on CA Access Control 12.8 SP0.

```
root> rpm -qp --requires CAeAC-1280-0.0.1275.i386.rpm
rpm >= 4.0
libcrypt.so.1
libc.so.6
libdl.so.2
libgcc_s.so.1
libm.so.6
libnsl.so.1
libpam.so.0
libpthread.so.0
libresolv.so.2
libstdc++.so.6
rpmlib(PayloadFilesHavePrefix) <= 4.0-1
rpmlib(CompressedFileNames) <= 3.0.4-1
```

Continue running the rpm command on the listed packages one by one to retrieve further dependencies.

```
root> rpm -qp --requires libcrypt
```

More information:

rpm --whatprovides—Verify That a Library Exists (see page 19)

rpm --whatprovides—Verify That a Library Exists

Before installing Enterprise Management on Linux, verify that all required libraries are present on the target system.

The command uses the following syntax:

```
rpm -q --whatprovides capability
```

The command has the following parameters:

-q

Specifies that you want to query RPM package information.

--whatprovides *capability*

Specifies that you want to retrieve information which packages provide the capability.

Example: Verify that a library is installed

In this example, you want to verify that libcrypt.so.1 is installed. You receive a positive answer ($? is 0) and you learn that its is the glibc-2.5-42 package that provides libcrypt.so.1.

```
root> rpm -q --whatprovides libcrypt.so.1
glibc-2.5-42
root> echo $?
0
```

Example: Detect that a library is not installed

In this example, you want to find out whether libexample.so.1 is installed. You receive a negative answer ($? is 1), because no package is installed that provides this capability.

```
root> rpm -q --whatprovides libexample.so.1
no package provides libexample.so.1
root> echo $?
1
```

If a required library is missing, install it before proceeding the installation.

More information:

rpm --requires—Detect Library Dependencies (see page 18)

Modify the Oracle Database Host Settings After Installation

Symptom:

After installing the Enterprise Management Server, I need to modify the Oracle database server settings to point to a different server.

Solution:

You can modify the Enterprise Management Server to work with an Oracle database on a different host after installation:

1. Stop the JBoss application server service on the Enterprise Management Server.
2. Backup the Oracle database on the current host.
3. Restore the Oracle database on the new host.
4. Navigate to the following directory, where *JBoss_HOME* indicates the directory where you installed JBoss:

   JBoss_HOME/server/default/deploy
5. Locate and back up the following files:
   - imauditdb-ds.xml
   - imquartzdb-ds.xml
   - imtaskpersistencedb-ds.xml
   - imworkflowdb-ds.xml
   - objectstore-ds.xml
   - reportsnapshot-ds.xml
6. Open each file and locate the <connection-url> entry.
7. Modify the connection settings to specify the new Oracle database host name. For example:

   <connection-url>jdbc:oracle:thin@//*new_host_name*:1521/*sid_or_service_name*</connection-url>
8. Start the JBoss application server service.

   You have modified the Oracle database host settings.

Enterprise Management Server Fails To Register Endpoints Type

Symptom:

I cannot view the endpoint types when I attempt to register the endpoint, after installing the Enterprise Management Server.

Solution:

The componentregistration utility registers the endpoints with the Enterprise Management Server. When the installation fails to register the endpoints, you can manually run the componentregistration utility.

Follow these steps:

1. Log in to the Enterprise Management Server.
2. Open a Command Prompt window and navigate to the following bin directory:

   `\ProgramFiles\CA\AccessControlServer\APMS\AccessControl\bin\`

3. Execute the ComponentRegistration utility by running the following command:

   `ComponentRegistration -comp jcs -register -userDN <user> -serverDN <server> -pwd <communication_password> -port CA Portal -ssl yes`

   For example: ComponentRegistration -comp jcs -register -userDN cn=root,dc=etasa -serverDN dc=im,dc=etasa -pwd password -port 20411 -ssl yes

4. Restart CA Access Control Services.
5. Verify that the endpoint types are registered by logging in to CA Access Control Enterprise Management.
6. Browse to Privileged Accounts, Endpoints, View Endpoints Types and check the listed endpoints types.

You have successfully registered the endpoint types.

"Bad Interpreter" Error Message During CA Access Control Enterprise Management Installation

Valid on UNIX and Linux

Symptom:

When I try to install CA Access Control Enterprise Management, I receive the following error message:

```
/bin/sh: bad interpreter: Permission denied
```

Solution:

In some UNIX or Linux releases, the operating system automounts the optical disc drive with the noexec option. To install CA Access Control Enterprise Management, verify that the optical disc drive is not mounted with the noexec option.

Cannot Use '$' Character for CA Access Control Enterprise Management Database Password

Symptom:

When I install CA Access Control Enterprise Management, I enter the database password and receive the following error message: "Database version could not be detected".

Solution:

CA Access Control Enterprise Management installation displays this error message if you enter a '$' character at the end of the password. If you must place a '$' character at the end of the password, you must change the database password after the installation.

Cannot Open CA Access Control Server Components

Symptom:

I cannot open CA Access Control Enterprise Management, CA Access Control Endpoint Management, or CA Access Control Password Manager in a web browser after I start all prerequisite CA Access Control services. I have installed JBoss and Oracle on the same server.

Solution:

Both Oracle and JBoss use a default port of 8080. To fix this problem, you must resolve the port conflict between Oracle and JBoss. You should consider which change is easiest to implement in your enterprise before you change the Oracle or JBoss port.

Use the following procedures to change the default JBoss and Oracle ports:

To change the default JBoss port

1. Open a command window and navigate to the following directory, where *JBossInstallDir* is the directory in which you installed JBoss:

   *JBossInstallDir/*bin

2. Stop JBoss:

   - (Windows) shutdown.bat -S
   - (UNIX) shutdown.sh -S

3. Open the following file in a text editor:

   *JBossInstallDir/*server/default/deploy/jbossweb-tomcat55.sar/server.xml

4. Change the port number in the following section:

```
<!-- A HTTP/1.1 Connector on port 8080 -->
    <Connector port="8080" address="${jboss.bind.address}"
```

5. Save and close the file.

6. Open the following file in a text editor:

   *JBossInstallDir/*server/default/deploy/httpha-invoker.sar/META-INF/jboss-service.x ml

7. Change the port number in each of the following lines:

```
<attribute
name="InvokerURLSuffix">:8080/invoker/EJBInvokerServlet</attribute>
<attribute
name="InvokerURLSuffix">:8080/invoker/EJBInvokerHAServlet</attribute>
<attribute
name="InvokerURLSuffix">:8080/invoker/JMXInvokerServlet</attribute>
<attribute
name="InvokerURLSuffix">:8080/invoker/readonly/JMXInvokerServlet</attribute>
<attribute
name="InvokerURLSuffix">:8080/invoker/JMXInvokerHAServlet</attribute>
```

8. Save and close the file.

9. Start JBoss.

10. (Windows) Change the CA Access Control Enterprise Management, CA Access Control Endpoint Management, and CA Access Control Password Manager shortcuts, as follows:

    a. Click Start, Programs, CA, Access Control, and right-click the appropriate shortcut.

       For example, to change the CA Access Control Enterprise Management shortcut, click Start, Programs, CA, Access Control, and right-click Enterprise Management.

    b. Click Properties.

    c. Change the port number in the URL field to the new JBoss port number.

To change the default Oracle port

1. Start the SQL command line.
2. Connect to Oracle as sysdba:

   ```
   connect / as sysdba
   ```

3. Check what port is currently used for HTTP communication:

   ```
   select dbms_xdb.gethttpport from dual;
   ```

4. Set the port to the desired port number:

   ```
   exec dbms_xdb.sethttpport('portNumber');
   ```

5. Stop and restart the database.

   ```
   shutdown immediate
   startup
   ```

No Tabs Visible in CA Access Control Enterprise Management

Valid for Active Directory user stores

Symptom:

I successfully install CA Access Control Enterprise Management. When I log in as the system user that I specified during installation, no tabs appear in the interface.

Solution:

When you install CA Access Control Enterprise Management, you provide the following Active Directory parameters:

- Host
- Port
- Search root

- User DN (and the password for this user)
- System User

This problem occurs when the Active Directory search root is in the same node in the directory tree as the DNs (Distinguished Names) for User DN and System User. To fix this problem, specify a search root one or more nodes higher in the directory tree than the DNs for the specified User DN and System User.

Example: The Active Directory Search Root

This example uses the following DNs for User DN and System User:

- User DN: CN=MyQueryUser,OU=ENTERPRISE,OU=NFS, OU=ACCOUNTS,DC=EXAMPLE,DC=LAB
- System User: CN=MySystemManager,OU=ENTERPRISE,OU=NFS, OU=ACCOUNTS,DC=EXAMPLE,DC=LAB

The following search root is one node higher in the directory tree than the DNs for User DN and System User. If you specify the following search root, CA Access Control Enterprise Management successfully installs and tabs appear in the interface:

```
OU=NFS,OU=ACCOUNTS,DC=EXAMPLE,DC=LAB
```

The following search root is in the same node in the directory tree as the DNs for User DN and System User. If you specify the following search root, CA Access Control Enterprise Management successfully installs but no tabs appear in the interface:

```
OU=ENTERPRISE,OU=NFS,OU=ACCOUNTS,DC=EXAMPLE,DC=LAB
```

Example: Set the Active Directory Search Root One Node Higher In the Directory Tree

This example uses the same DNs for User DN and System User as the previous example.

In this example, you specified the following search root when you installed CA Access Control Enterprise Management:

```
OU=ENTERPRISE,OU=NFS,OU=ACCOUNTS,DC=EXAMPLE,DC=LAB
```

Because this search root is in the same node in the directory tree as the DNs for User DN and System User, you need to specify a search root one node higher in the directory tree.

To set the Active Directory search root one node higher in the directory tree

1. Enable the CA Identity Manager Management Console.
2. Open the CA Identity Manager Management Console.
3. Click Directories, and click the ac-dir directory.

   The Directory Properties dialog appears.
4. Click Export at the bottom of the Directory Properties dialog.

5. When prompted, save the XML file and open it for editing.

   Note: The file name is ac-dir.xml.

6. Locate the tag that contains the search root that you specified during installation. For example:

   ```
   <LDAP searchroot="OU=ENTERPRISE,OU=NFS,OU=ACCOUNTS,DC=EXAMPLE,DC=LAB"
   secure="false"/>
   ```

7. Replace the existing search root with the new search root. For example:

   ```
   <LDAP searchroot="OU=NFS,OU=ACCOUNTS,DC=EXAMPLE,DC=LAB" secure="false"/>
   ```

   Note: Because you removed the Enterprise OU (Organizational Unit), this search root is one node higher in the directory tree than the previous search root.

8. Save and close the file.

9. In the CA Identity Manager Management Console, click Update in the Directory Properties dialog.

   The Update Directory page appears.

10. Click Choose File, navigate to the XML file that you edited, click Open, and click Finish.

    The CA Identity Manager Management Console validates the XML file and displays status information in the Directory Configuration Output field.

    Note: If you receive a "Failed to Import" error, see the Cannot Import ac-dir.xml Directory Configuration File topic.

11. Click Continue.

    The Directories page appears.

12. Click ac-dir, and click ac-env in the Environment(s) section.

    The Environment Properties page appears.

13. Click Restart.

    The CA Identity Manager Management Console restarts the environment and applies your changes.

Note: For more information about how to enable and start the CA Identity Manager Management Console, see the *Implementation Guide*.

More information:

Cannot Import ac-dir.xml Directory Configuration File (see page 27)

Cannot Import ac-dir.xml Directory Configuration File

Symptom:

I exported the ac-dir.xml directory configuration file from the CA Identity Manager Management Console. When I try to import the file, the following error message appears in the Directory Configuration Output field:

```
Deploying directory configuration...

Parsing input stream...
Error: (140:67): cvc-complex-type.4: Attribute "value" must appear on element
"Container".
Error: Failed to import

*********
1 error(s), 0 warning(s)
```

Solution:

The ac-dir.xml directory configuration file describes the structure and content of the user store. You use this file to change how CA Access Control Enterprise Management interacts with the user store, for example, to change the user directory password or the Active Directory search root. You also edit the ac-dir.xml file when you configure CA Access Control Enterprise Management for SSL communication and Active Directory for failover.

To fix this problem, do the following:

1. Open the ac-dir.xml file for editing.
2. Locate the following tag:

   ```
   <Container objectclass="top,organizationalUnit" attribute="ou"/>
   ```

3. Replace the previous tag with the following tag:

   ```
   <Container objectclass="top,organizationalUnit" attribute="ou" value=""/>
   ```

4. Save and close the file.

You can now import the directory configuration file in to the CA Identity Manager Management Console. To apply any changes that you made in the directory configuration file, you must restart the environment after you import the file.

CA Access Control Enterprise Management Cannot Connect to DMS

Symptom:

When I log in to CA Access Control Enterprise Management, I receive a message similar to the following:

```
Error: Login procedure failed
Error: Password on target does not match client's password
```

Solution:

The user ac_entm_pers cannot log in to the DMS. This user authenticates communication and data flow between the Enterprise Management Server and the DMS.

Note: The ac_entm_pers user has the following authorization attributes: ADMIN, AUDITOR, IGN_HOL, LOGICAL

To troubleshoot this problem, do the following:

1. Open selang.
2. Connect to the DMS:

   `host DMS__@`*`entM_host_name`*

3. Change the password for ac_entm_pers:

   `eu ac_entm_pers admin auditor nonative password(password) logical nonative grace-`

4. Authorize ac_entm_pers to log in to the host on which the Enterprise Management Server is installed:

   `authorize TERMINAL `*`entM_host_name`*` uid(ac_entm_pers) access(a)`

5. Validate that ac_entm_pers can log in to the Enterprise Management Server:

   `host DMS_@`*`entM_host_name`*` uid(ac_entm_pers) password(`*`password`*`) logical`

6. Update the Enterprise Management Server DMS connection settings with the new password for ac_entm_pers.

   The DMS authenticates ac_entm_pers and CA Access Control Enterprise Management is connected to the DMS.

   Note: For more information about how to configure the connection to the DMS, see the *CA Access Control Enterprise Management Online Help*.

If you receive an error when you update the connection settings, the DMS cannot authenticate ac_entm_pers. To troubleshoot this problem, do the following:

1. Verify that you entered the same password in each step of the previous procedure.
2. Verify that the host name of the Enterprise Management Server (*entM_host_name*) in Step 4 of the previous procedure is correct.

   For example, if you specify the fully qualified host name of the Enterprise Management Server in Step 4, but the TERMINAL record for the Enterprise Management Server uses a short host name, the host names are not resolved and ac_entm_pers cannot log in to the Enterprise Management Server.
3. Review the CA Access Control audit file:

   ```
   seaudit -a
   ```
4. Review the DMS audit file:

   ```
   seaudit -a -fn DMS_log_file
   ```

   Note: The audit records may provide information about the correct host name of the TERMINAL record for the Enterprise Management Server.

Example: Display the DMS Audit File

The following example displays the audit file for a DMS named DMS__:

```
seaudit -a -fn "C:\Program
Files\CA\AccessControlServer\APMS\AccessControl\Data\DMS__\pmd.audit"
```

Question Marks Appear in CA Access Control Enterprise Management Tabs

Symptom:

When I open CA Access Control Enterprise Management, I see question marks in the tabs.

Solution:

To fix this problem, change the default language of your browser to US English.

Received "Null page" Error in InfoView

Symptom:

When I try to access the CA Access Control reports I get the following error in InfoView:

```
Null page: Unable to create page from report source
```

Solution:

On Windows, the CA Access Control Universe may not be defined or installed properly. Test the connection for the CA Access Control Universe. If the connection is not working, edit the connection; if the connection is working, replace the connection.

On Solaris, log in as bouser and edit the script $CASHCOMP/CommonReporting/bobje/setup/env.sh as follows:

1. Append the following LIBRARYPATH:

   ```
   $MWHOME/lib-sunos5_optimized
   ```

2. Restart BusinessObjects services:

   ```
   cd $CASHCOMP/CommonReporting/bobje
   ./stopservers
   ./startservers
   ```

CA Access Control Does Not Start Automatically After a UNIX Installation

Valid on UNIX

Symptom:

CA Access Control does not start automatically after I install it on a UNIX endpoint.

Solution:

By default, CA Access Control does not start automatically on a UNIX endpoint.

To configure the seosd daemon to start automatically upon startup on a UNIX computer, use the *ACInstallDir*/samples/system.init/*sub-dir* directory, where *sub-dir* is the directory for your operating system. Each sub-directory contains a readme file with instructions on how to start CA Access Control automatically on your operating system.

Note: For more information about how to start CA Access Control, see the *Implementation Guide*.

Cannot Start Daemons on Linux s390 Endpoint

Valid on Linux s390 and Linux s390x

Symptom:

I cannot start the seosd or ReportAgent daemon.

Solution:

CA Access Control cannot locate the Java environment on the endpoint. To fix this problem, do the following:

1. Verify that the java_home configuration setting in the global section of the accommon.ini file contains the path to the Java environment.
2. Set the value of the LD_LIBRARY_PATH environment variable to the path to the shared libraries of the Java environment.

Cannot Connect to selang After Installation

Symptom:

After I install CA Access Control, I receive the following error when I try to start selang or connect to the CA Access Control database:

```
ERROR: Initialization failed, EXITING!
(localhost)
ERROR: Login procedure failed
ERROR: You are not allowed to administer this site from terminal example.com
```

Solution:

Terminal rules are not correctly defined. Troubleshoot the terminal rules to determine the problem.

To troubleshoot terminal rules

1. Stop CA Access Control:

   ```
   secons -s
   ```

2. Start selang in local mode:

   ```
   selang -l
   ```

   Note: You must be the root user to run selang in local mode on a UNIX computer.

3. Check that you have created a TERMINAL record for the local terminal (*terminal_name*), and that the terminal access authorities are correctly defined:

   `showres TERMINAL terminal_name`

   - If a record does not exist, create a TERMINAL record for the local terminal:

     `editres TERMINAL terminal_name owner(name) defaccess(accessAuthority)`

     Note: The owner can be either a user or a group. Because the default access for a TERMINAL record is none, we recommend that you specify a default access when you create the record to avoid locking users out of the terminal.

   - If the terminal access authorities are incorrect, define the correct access authorities for the terminal:

     `authorize TERMINAL terminal_name uid(name) access(accessType)`

4. (UNIX) Check the value of the terminal_default_ignore configuration setting in the [seosd] section.

   This configuration setting determines if CA Access Control considers the defaccess value of the _default TERMINAL and of the specific TERMINAL records when authorizing administrative access.

   Note: For more information about the terminal_default_ignore configuration setting, see the *Reference Guide*.

5. (UNIX) Check that the lookaside database reflects the terminal, as follows:

   a. Build a hostname-specific lookaside database:

      `sebuilda -h`

   b. Check that the terminal entry and the hostname are the same in the lookaside database:

      `sebuilda -H | grep hostname`

      The contents of the hosts lookaside database files are listed.

6. Start CA Access Control:

   - (UNIX) seload
   - (Windows) seosd -start

Note: If you still cannot start selang or connect to the CA Access Control database, you may have to modify the hosts file for your OS. Contact your system or network administrator for assistance.

Messages Appear in Solaris 10 Log File

Valid on Solaris 10

Symptom:

When I stop CA Access Control using "secons -s", CA Access Control messages appear in the "/var/adm/messages" log file on my Solaris 10 computer. The SEOS_use_streams configuration setting on my computer is set to yes.

Solution:

These messages are informational only and do not indicate any failure or error. You do not need to do anything. The messages and their interpretation follow:

- "SEOS: Restored tcp wput" "SEOS: Restored strrhead rput"

  These messages indicate that the SEOS_syscall function disabled network hooks.

- "SEOS: Replaced tcp wput" "SEOS: Replaced strrhead rput"

  These messages indicate that the SEOS_syscall function enabled network hooks.

Received Error When Manually Deleting Registry Keys During Uninstall

Valid on Windows

Symptom:

When I try to delete a registry key while uninstalling CA Access Control, I receive the following error message:
`Cannot open Data: Error while opening key.`

Solution:

Run the RemoveAC.exe utility to remove CA Access Control registry keys and directories. The RemoveAC.exe utility does not uninstall the product, but helps ensure that all CA Access Control registry keys and directories are removed from the computer.

ProductExplorer Not Started

Symptom:

When I insert the CA Access Control Server Components DVD for Windows into my optical drive, the ProductExplorer does not start.

Solution:

Do the following:

- Navigate to the optical disc drive directory and double-click the ProductExplorerx86.EXE file.
- Enable autorun to startup the ProductExplorer automatically.

Licensing Error Occurs When Upgrading to CA Licensing 1.9.04

Valid on UNIX

Symptom:

When I upgrade CA Access Control, the new CA Licensing rpm script (1.9.04) first executes. The uninstaller for the previous rpm script then executes and the following error message records in the UNIX syslog:

```
<Error opening lic98.err - /opt/CA/SharedComponents/ca_lic/lic98.err, original
code=5000>2E2U eTrust Access Control for UNIX <Error opening lic98.err -
/opt/CA/SharedComponents/ca_lic/lic98.err, original code=5000>  LRF=2E2U,
000000000000, Linux_x86.64_1_*, ismelx84, 0
```

Solution:

The CA Licensing version 1.9.03 or lower installer removes links and folders resulting in the error. We recommend you not to perform an upgrade, but directly install CA Licensing version 1.9.04.

Follow these steps:

1. If CA Access Control is running, shut it down by logging in as an administrator and entering the following commands:

   ```
   ACInstallDir/bin/secons -sk
   ACInstallDir/bin/SEOS_load -u
   ```

2. Back up the following files to a temporary folder:
   - /etc/profile.
   - /etc/profile.CA.
   - /etc/csh_login.CA.
   - Note all symbolic link information for the following entries:
     - /usr/local/CAlib
     - /opt/CA/CAlib
     - $CASHCOMP/CAlib
     - /ca_lic
     - /opt/CA/ca_lic
     - $CASHCOMP/ca_lic
     - $CASHCOMP/lib
3. Back up all symbolic directories.
4. Download the latest CA Licensing package from the Support web site.
5. Extract the content of the compressed file in to a temporary directory.

6. Navigate to the new lic98_install directory.
7. Enter the following command to install CA Licensing:

   ```
   ./install <install directory>
   ```

8. Enter the following command to source the /etc/profile:

   ```
   ./etc/profile
   ```

9. Perform the following steps to restore the ca.olf file:
   a. Run the following command:

      ```
      rpm -e --nodeps ca-lic
      ```

   b. Restore the directories that are backed up in Step 2 to the following directory:

      ```
      /opt/CA/SharedComponents/ca_lic
      ```

   c. Restore the symbolic links noted down in Step 2(d) to the following directory:

      ```
      /opt/CA/SharedComponents/ca_lic
      ```

   d. Restore backed up /etc/profile, /etc/profile.CA and /etc/csh_login.CA files to the following directory:

      ```
      /opt/CA/SharedComponents/ca_lic
      ```

   CA Licensing 1.9.04 is installed successfully and you can proceed to use all registered CA Products.

Block HTTP Access on the Enterprise Management Server

Symptom:

After installation, HTTP and HTTPS ports are open by default. You need to disable the HTTP port.

Solution:

To disable the HTTP port, comment out the HTTP connector in the JBoss configuration.

Follow these steps:

1. Browse to *JBOSS_HOME*/server/default/deploy/jboss-web.deployer and edit the server.xml file.
2. Search for the following string that defines the default port of the HTTP connector: `port="18080"`

   Note: If you have configured a different port in the installation wizard, the port number may be different.

   This port attribute is part of a <Connector> element.
3. Comment out this <Connector> element by surrounding the element with comment tags (<!-- and -->).

   The HTTP connector is disabled.
4. Restart the JBoss service.

Example

```
<!-- <Connector port="18080" address="${jboss.bind.address}"
         connectionTimeout="20000" /> -->
```

Chapter 3: Creating Policies and Access Authorities

This section contains the following topics:

Block Users Access to Network Drives and Shared Drives

Valid on Windows

Symptom:

I am able to block users access to a system drive, but I cannot stop users access to network and shared drives.

Solution:

To block users access to network and shared drives on Windows 2008, add the following selang command to the policy:

```
newres FILE \Device\Mup\*
```

To block users access to network and shared drives on Windows 2003, add the following selang command to the policy:

```
newres FILE \Device\LanmanRedirector\*
```

User Can Access Protected Resources

Symptom:

I created a default access authority of none for a resource, but the superuser can still access the resource.

Solution:

Troubleshoot the resource access problem (see page 120).

Read Access Checks Bypass /etc/passwd and /etc/group Files

Valid on UNIX

Symptom:

I created a rule that has a default access authority of none for the /etc/passwd and /etc/group files, but I still have read access to these files.

Solution:

By default, the CA Access Control authorization engine bypasses read access checks for the /etc/passwd and /etc/group system files. To stop CA Access Control bypassing read access checks for system files, change the value of bypass_system_files in the [seosd] section of the seos.ini file to no.

Important! If you stop CA Access Control bypassing read access checks for system files, verify that correct authorizations are in place. If you do not set the correct authorizations and bypass read access checks, users including CA Access Control administrations and the root user may not be to access the system, and critical system processes may fail.

An Enterprise User or Group Cannot Access Resources but Correct Access Rules are Set

Valid on Windows

Symptom:

I can see that an enterprise user or group has permissions to access a resource but they cannot access it.

Solution:

It is possible that the enterprise account has been recycled and the permissions in the database apply to the old account, not the new account that has the same name but a different SID. To check for this scenario, resolve recycled enterprise accounts.

Note: For more information about resolving recycled enterprise accounts, see the *Endpoint Administration Guide for Windows*.

Failed Login Does Not Lock Out User

Valid on UNIX

Symptom:

I configure serevu to disable users in the password PMD after a specified number of failed login attempts. When a user fails to log in correctly, CA Access Control does not lock out the user. When I start serevu with the nodaemon option to view the pam_failed_logins.log file, the server does not respond.

Solution:

The value of passwd_pmd in the [seos] section of the seos.ini file is incorrect. Set the value of passwd_pmd to the name of the password PMD to which sepass sends password updates.

Users Can Run Commands Outside Time Restrictions

Symptom:

I set time restrictions on a group, but group members can run CA Access Control commands outside the permitted times.

Solution:

During a restricted time period, CA Access Control prevents users from starting a new login session but cannot force users to disconnect. To prevent users from accessing resources or commands in a restricted time period, change the resource record for the resource or command to include time restrictions.

Note: CA Access Control checks if time restrictions exist in the USER or XUSER record for the user before it checks if time restrictions exist for GROUP or XGROUP to which the user belongs.

CA Access Control Recognizes All Users as root

Valid on UNIX

Symptom:

When I run the sewhoami utility for a non-root user, CA Access Control recognizes the user as root.

Solution:

To troubleshoot this problem, verify the following in the LOGINAPPL record of the login application:

- The name of the LOGINAPPL record is the name of the login application.
- The LOGINPATH parameter in the LOGINAPPL record specifies the correct, full path to the login application.

  To determine the path to the login application, run a trace (see page 123) then use the login application to log in and log out of CA Access Control. Review the trace to obtain the path.
- The LOGINSEQUENCE parameter in the LOGINAPPL record specifies the correct login sequence for the login application. For assistance, contact CA Support at http://ca.com/support.

Note: CA Access Control does not define LOGINAPPL records for third-party login applications. If you use a third-party login application, manually define the LOGINAPPL record for the application.

Cannot Add User as Password Manager to Only One Group

Symptom:

I want to make a user a password manager for a specific group, but when I execute the following command the user becomes a password manager for all groups:

```
editusr userName pwmanager
```

Solution:

Specify the name of the group to which you want to add the user as a password manager, as follows:

```
join userName group(groupName) pwmanager
```

Windows Administrators Can Change CA Access Control Passwords

Valid on Windows

Symptom:

Windows administrators can change CA Access Control passwords in my CA Access Control-protected Windows environment.

Solution:

To help ensure that only users that you specify in CA Access Control can change CA Access Control passwords, set the value of the EnforceViaeTrust registry entry to 1 in the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\passwd
```

This registry entry specifies to enforce that you can update or create user passwords through CA Access Control only. The default value of the registry entry is 0, meaning that you do not have to use CA Access Control to update or change a user password.

Global Password Policies Lock Users Out of Protected Systems

Symptom:

When I implement a global password policy, the password policy locks users out of systems protected by CA Access Control.

Solution:

Create a separate password policy for the users who must access the CA Access Control-protected system. Use a profile group to create a password policy for these users.

The following process describes how to use a profile group to implement a password policy:

1. Create a profile group.
2. Set the password policy for the profile group.
3. Assign the users to the profile group.

   The password policy that you set for the profile group now applies to the users associated with the profile group.

Task Delegation Hangs for Interactive Application

Valid on Windows

Symptom:

I write a task delegation rule that lets a user run an interactive Windows application, for example, notepad.exe. When the user tries to run the application, the task delegation hangs.

Solution:

The interactive flag must be set for the SUDO class record that permits the user to run the application. If you use task delegation to run an interactive Windows application and the interactive flag is not set, the application runs in the background and you cannot interact with it.

To fix this problem, do the following:

1. Set the interactive flag for the SUDO record:

   ```
   er SUDO resourceName interactive
   ```

   resourceName

   Specifies the name of the resource record that lets the user run the application.

   The interactive flag is set for the specified resource.

2. Restart the Task Delegation service, as follows:

   a. Kill the interactive application.

   b. If task delegation still hangs, restart CA Access Control.

Note: For more information about task delegation and defining SUDO records, see the *Endpoint Administration Guide for Windows*.

Chapter 4: Managing the CA Access Control Database

This section contains the following topics:

selang Query Returns Maximum of 100 Records

Symptom:

When I run a selang query that should return more than 100 records, CA Access Control displays the following message:

```
WARNING: Only 100 (query size limit) items are displayed.
```

Solution:

The default value of the query_size configuration setting is 100. To increase the number of records that CA Access Control returns for selang queries, change the value of the query_size configuration setting.

The query_size configuration setting is located in the:

- (UNIX) [lang] section of the seos.ini file
- (Windows) lang subkey, as follows:

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\lang
  ```

UTimes and Denied Records in the Audit Log After Database Backup

Symptom:

When CA Access Control is running and I back up the CA Access Control database with my OS backup tools, CA Access Control sends an entry to the audit log similar to the following message:

```
03 Mar 2008 15:58:01 D FILE            UTimes     69 10
/opt/CA/AccessControl/seosdb/seos_pvf.fre /usr/sbin/fbackup
```

Note: The example above is written using UNIX pathnames, but the solution is also valid for Windows computers.

Solution:

The audit message means that CA Access Control prevented the backup operation from updating the UTimes file date stamp. CA Access Control did not prevent the backup itself.

To prevent this message from appearing in the audit log, do the following:

- If the backup program is executed by a non superuser, verify that the user has the OPERATOR attribute.
- If the backup program is executed by a superuser, verify that the backup program has a SPECIALPGM record that has the pgmtype(backup) property.

To help ensure that the database is correctly backed up, use the dbmgr utility to perform the back up.

The CA Access Control Database Is Corrupt

Valid on UNIX

Symptom:

I notice messages similar to the following messages in the CA Access Control error log:

```
seoswd: [ID 973226 auth.error] Communication time out to seosd. Executing seosd
FATAL!
Inseosrt_InitDatabase (0x270)
WARNING: /Path of Access Control/seosdb/seos_cdf.dat was corrupted
```

Solution:

Use the following procedure to fix the database corruption.

Note: This procedure assumes that the database is installed in the default installation location, /opt/CA/AccessControl/.

To fix the CA Access Control database corruption

1. Stop CA Access Control:

   ```
   secons -s
   ```

2. (Optional) Back up the database to another location so that the database can be provided to Technical Support if required.

3. Verify that the database is marked as closed:

   ```
   cd /opt/CA/AccessControl//seosdb
   ```

   ```
   dbmgr -util -close
   ```

   Note: If CA Access Control is not shut down correctly, the database can be marked as open.

4. Check the database:

   ```
   dbmgr -util -check
   ```

5. Do *one* of the following:

   - If you do not receive an error message when you check the database, go to Step 6.
   - If you receive an error message when you check the database, do not complete Steps 6 and 7; instead, rebuild the database (see page 126).

6. Build the database files:

   ```
   dbmgr -util -build all
   ```

7. Check the database again:

   ```
   dbmgr -util -check
   ```

8. Start CA Access Control:

   ```
   seload
   ```

Note: If the database is still corrupt, further investigation is required. For assistance, contact CA Support at http://ca.com/support.

Chapter 5: Connecting to Remote Computers

This section contains the following topics:

Cannot Connect to Remote Computer

Symptom:

I cannot connect to a remote CA Access Control computer.

Solution:

Troubleshoot the connection problem (see page 120).

Communication Time Out to seosd Appears Continuously in syslog

Valid on Windows

Symptom:

When I run CA Access Control, the computer occasionally slows down and the following messages appear in syslog:

```
seoswd: Communication time out to seosd. Executing seosd
seoswd: Communication problem with seosd returned 5378 [Success]
seoswd: Description: Timeout communication with seosd.
```

Solution:

The antivirus software on the computer causes CA Access Control to time out. Do the following in the antivirus software:

- Exclude the CA Access Control directory from real-time scanning
- Stop the real-time (on access) scan for the CA Access Control directory

Because CA Access Control protects the CA Access Control registry keys, files, and installation directory by default, the previous actions should not increase the virus threat to the computer.

We recommend that you create a SPECIALPGM record for the antivirus software, and set the PGMTYPE property to pbf for the SPECIALPGM record. The pbf program type bypasses database checks for file handling events.

First Incoming ftp Connection Cannot Be Controlled

Valid on UNIX

Symptom:

When I start CA Access Control it does not control the first incoming ftp connection from vsftpd. I have created a TCP rule for ftp and a HOST rule for vsftpd, and CA Access Control controls all subsequent incoming ftp connections from vsftpd according to the TCP or HOST rule that I created.

Solution:

If you start vsftpd before you start CA Access Control, vsftpd places a hook in the accept system call for incoming ftp connections. The hook means that vsftpd processes the first incoming ftp connection before CA Access Control can intercept it.

After vsftpd processes the ftp connection it tries to call the accept system call in preparation for the next ftp connection. However, CA Access Control intercepts this system call and hence controls all subsequent ftp connections.

To intercept the first incoming ftp connection, use one of the following workarounds:

- Start CA Access Control before you start vsftp.
- Use a super-server daemon such as inetd or xinetd to start vsftpd.

  Note: For more information about configuring a super-server daemon, contact your OS vendor.
- Run the tripAccept utility after you start CA Access Control.

  To run the tripAccept utility, you must enable the call_tripAccept_from_seload token in the [SEOS_syscall] section of the seos.ini file. We recommend that you define a SPECIALPGM record for the tripAccept utility before you run it.

Target Pages on Local Host and Target Host Are Different

Valid on UNIX

Symptom:

When I try to connect to a CA Access Control host, I get the following message:

```
WARNING: Local machine's code page is different from target host's.
```

Solution:

Verify that the locale configuration setting in the [seos] section of the seos.ini file has the same value on the local host and the target host.

Cannot Connect to Endpoint Using selang

Symptom:

When I try to connect to an endpoint using selang, I receive an error message similar to the following:

```
Unpacking of data failed
```

Solution:

There is a problem with the encryption used to protect inter-component communication. Check CA Access Control computers for recent changes to the encryption key and the encryption method.

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

Chapter 6: Deploying Rules from a PMD

This section contains the following topics:

Subscriber PMDB Cannot Receive Updates from the Master PMDB

Symptom:

I have a hierarchical PMDB architecture. A subscriber PMDB does not receive updates from the master PMDB. The error log of the master PMDB has the following message:

```
Cannot receive update from non-parent PMDB
```

Solution:

When a subscriber PMDB does not receive updates from the master PMDB, use the following procedure to troubleshoot the problem.

To troubleshoot PMDB update problems

1. List the subscribers of the master PMDB (*master_pmdb_name*) and their status:

   `sepmd -L` *`master_pmdb_name`*

   Note: Run this command on the master PMDB computer.

2. Review the list of subscribers to determine which subscribers are unavailable.

3. Verify that the value of the parent_pmd configuration setting is correct on each unavailable subscriber.

   The parent_pmd configuration setting is located in:

   - (UNIX) The [seos] section of the seos.ini and the pmd.ini files
   - (Windows) The following registry key:

     ```
     HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\AccessContro
     l
     ```

   Note: The hostname that you specify in the parent_pmd token must match the hostname of the master PMDB exactly. Verifying that hostname resolution is correctly configured may help troubleshoot this issue. If you use a UNIX computer, you can use the sehostinf utility to discover the hostname of the master PMDB. For assistance, contact CA Support at http://ca.com/support.

If the problem still exists, do the following:

1. Display the master PMDB error log:

   ```
   sepmd -e master_pmdb_name
   ```

2. Review the error log and note what error codes are reported for the unavailable subscribers.
3. For each unavailable subscriber, use the error code to troubleshoot the problem.

If the problem still exists, do the following:

1. Remove the problematic subscriber from the list of unavailable subscribers that the master PMDB maintains:

   ```
   sepmd -r pmdb_name subscriber_name
   ```

   The parent PMDB tries to send updates to the subscriber.

2. Repeat the previous procedure.
3. If there are any changes to the list of subscribers or to the parent PMDB error log, use the changes to troubleshoot the problem.

Failed Events in Audit Log of Subscriber Endpoint

Symptom:

A subscriber does not receive updates from a master PMDB. I notice *Failed* events in the CA Access Control audit log of the subscriber.

Solution:

The PMDB user does not have the ADMIN attribute. To give the PMDB user the ADMIN attribute, edit the user record using the following selang command:

```
chusr userName admin
```

Note: You must have the ADMIN attribute to run this selang command. CA Access Control bypasses TERMINAL rules when deploying PMDB updates to subscribers.

Chapter 7: Deploying Policies

This section contains the following topics:

Troubleshooting Policy Deployment

When you assign a policy to a host, the policy is not deployed on the assigned endpoint until policyfetcher retrieves the deployment task and runs the policy script. As a result, deployment errors may occur for different reasons when the policy is transferred or deployed at the endpoint.

To resolve policy deployment errors, advanced policy management provides you with troubleshooting actions. You can perform these actions using either CA Access Control Enterprise Management or the policydeploy utility. In CA Access Control Enterprise Management, the troubleshooting actions are located in the Policy sub-tab of the Policy Management tab.

The troubleshooting actions are as follows:

- **Redeploy**—Creates a new deployment task that contains the policy script and deploys the task to the endpoint.

  Use this option when the policy deploys on the endpoint with errors. That is, selang policy script execution failed. You need to manually fix the reason for the script error on the endpoint before you can redeploy the policy.

  Note: This option is only available in CA Access Control Enterprise Management, and is not supported in the policydeploy utility.

- **Undeploy**—Undeploys the policy from the specified endpoint without unassigning the policy from the corresponding host.

  Use this option to remove any policies from the endpoint that are not assigned to the host on the DMS.

- **Reset**—Resets an endpoint. CA Access Control resets host status, undeploys all effective policies, and deletes all GPOLICY, POLICY, and RULESET objects.

  Use this option to clean an endpoint, and its status on the DMS, from all policy deployments.

  Note: This option does not remove DEPLOYMENT or GDEPLOYMENT objects from the endpoint or from the DMS, because you may need these objects for auditing purposes. You can use the dmsmgr -cleanup function to remove the DEPLOYMENT and GDEPLOYMENT objects after you reset the endpoint. After you reset an endpoint, you can assign policies to the endpoint as normal.

- **Restore**—Undeploys any policies on the specified host, then restores all the policies that should be deployed (assigned or directly deployed) on the host by creating new deployment tasks and sending the tasks to the host for execution.

  Use this option when you re-install CA Access Control or the operating system on the endpoint, or when you restore an endpoint from a backup, to redeploy all the policies that the DMS indicates are effective on that endpoint.

Modify the Advanced Policy Management Communication Layer

Starting from CA Access Control 12.6.01, the Advanced Policy Management communication layer between the DMS and the Distribution Hosts modified to use the Message Queue server. You can modify existing endpoints communication method to use the Message Queue Server.

Follow these steps:

1. From the Enterprise Management Server that holds the DMS, verify that all subscribers are synchronized with the DMS.

   Note: Verify the DH subscribers offset matches the global offset.

2. Remove all subscribers from the DMS, for example:

   ```
   sepmd -u DMS__DH__@dhname
   ```

3. Add a Message Queue subscriber to the DMS, as follows:

   ```
   sepmd -smq DMS__ -predefined ServerToServerBroadcast -destination DH
   ```

4. From each Distribution Server, verify that the DMS subscriber is synchronized with the DH__WRITER using the following command:

   ```
   sepmd -L DH__WRITER
   ```

   Note: Verify the DMS subscribers offset matches the global offset.

5. Remove the DMS subscriber from the DH__WRITER, for example:

   ```
   sepmd -u DH__WRITER DMS__@dmsname
   ```

6. Add a Message Queue subscriber, as follows:

   ```
   sepmd -smq DH__WRITER -predefined ServerToServer -destination DMS
   ```

Policy Does Not Successfully Deploy on All Endpoints

Symptom:

I deployed a policy to a host group. The policy successfully deployed on some hosts in the host group, but deployed with errors on other hosts.

Solution:

To fix this problem, do one of the following:

- If the policy failed on few hosts, redeploy the policy on these hosts.

  You need to manually fix the reason for the deployment error on the host before you can redeploy the policy.

- If the policy failed on many hosts, run the policydeploy -fix function on each endpoint.

  The policydeploy -fix function fixes and redeploys the specified deployment task or package. You need the name of the deployment task to use this function.

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

Example: The policydeploy -fix Function

The following example fixes the specified deployment package on the endpoint:

```
policydeploy -fix -task 1266471565#0f6a3cec-a37d-47d9-bde3-0112a49b714a
```

DH or Disaster Recovery DMS Fails to Resubscribe

Symptom:

As part of the disaster recovery process, I resubscribe a DH to a DMS or resubscribe the disaster recovery DMS to the production DMS. The following message appears:

```
Failed to resubscribe subscriber on dms@host.
To complete restore operation please manually resubscribe subscriber@host on dms@host
at offset value.
```

Solution:

The message appears when you resubscribe a DH or a disaster recovery DMS to a parent DMS that is not running. You must use the offset value in the message to manually resubscribe the DH to the DMS, or the disaster recovery DMS to the production DMS. Specifying the offset value ensures that the subscriber is only sent commands that were not present in its database when it was restored.

To resubscribe a DH or disaster recovery DMS to its parent DMS, run the following command on the parent DMS host:

```
sepmd -s parent_name child_name@host offset
```

Example: Subscribe a DH to a DMS

The following example subscribes DH__@test.com to DMS__ with an offset of 18028. Run this command on DMS__:

```
sepmd –s DMS__ DH__@test.com 18028
```

Policy Status is Not Executed

Symptom:

I have enabled policy verification. When I deploy a policy, the policy does not deploy and the policy status is Not Executed.

Solution:

Policy verification found one or more errors in the policy. You must fix the errors before you can successfully deploy the policy.

To successfully deploy the policy, follow these steps:

1. Review the errors.

   You must identify if the errors occur in the policy or in the CA Access Control database before you can fix them.

   a. In CA Access Control Enterprise Management click Policy Management, Policy subtab, expand the Deployment tree in the task menu on the left, and click Deployment Audit.

      The Deployment Audit page appears.

   b. Define a scope for the search, then click Go.

      A list of deployment tasks, that match the scope of the search you defined, appears.

   c. Click the name of the deployment task that did not deploy.

      Information about the deployment appears, including a list of the errors in the policy.

2. (Optional) If the error is in the CA Access Control database, do the following:
    a. Fix the error in the CA Access Control database.
    b. Do *one* of the following:
        - Use the policydeploy utility to fix the deployment task.

          Fixing the deployment task removes the Fail status on the deployment task, and, if the deployment is successful, changes the status of the policy on the endpoint to Deployed.
        - Use CA Access Control Enterprise Management or the policydeploy utility to deploy the policy again.

          Deploying the policy again creates another deployment task. The status of the previous deployment task with errors remains Fail. If the deployment is successful, the policy status on the endpoint is Deployed.
3. (Optional) If the error is in the policy, do the following:
    a. Create a new policy version that does not contain the error.
    b. Use CA Access Control Enterprise Management or the policydeploy utility to upgrade the policy.

Policy Status is Undeployed with Failures

Symptom:

After trying to undeploy a policy from an endpoint, I noticed that the status is set to Undeployed with Failures.

Solution:

Undeployed with Failures status indicates that the policy undeployed with one or more rules from the undeployment script failing to execute on the endpoint. This policy status cannot be removed in CA Access Control Enterprise Management.

To fix this problem, manually remove the status of the policy version.

More information:

Cannot Remove the Status of a Policy Version (see page 63)

Cannot Remove the Status of a Policy Version

Symptom:

A policy version is not effective on a host, but I cannot remove the status of the policy version. This prevents me from deleting the policy version.

Solution:

To fix this problem, you must manually remove the policy status.

To manually remove the policy status, do the following:

1. Remove the status of the policy version on the endpoint.

    a. Execute the following selang command on the endpoint:

        `sr HNODE __local__`

    b. Find the name of the policy in the Policy Status section of the output, and make a note of the Updated by user for the policy.

    c. Execute the following selang command on the endpoint:

        `er HNODE __local__ policy(name(`*`policyName#policyVersion`*`) status(undeployed) updator(`*`userName`*`))`

        policyName#policyVersion

        Defines the name and version number of the policy version that you want to delete.

        userName

        Defines the name of the Updated by user.

    The status of the policy version is removed on the endpoint.

2. Remove the status of the policy version on the DMS.

    a. Execute the following selang command on the DMS:

        `sr HNODE `*`hnodeName`*

        hnodeName

        Defines the name of the host on which the policy version is deployed.

    b. Find the name of the policy in the Policy Status section of the output, and make a note of the Updated by user for the policy.

    c. Execute the following selang command on the DMS:

        `er HNODE `*`hnodeName`*` policy(name(`*`policyName#policyVersion`*`) status(undeployed) updator(`*`userName`*`))`

    The status of the policy version is removed on the DMS.

Example: Remove the Status of a Policy Version on an Endpoint

The following example removes the status of version 01 of a policy named mypolicy on an endpoint:

```
AC> sr HNODE __local__
(localhost)
Data for HNODE '__local__'
-----------------------------------------------------------
Defaccess        : R
Audit mode       : Failure
Owner            : Domain\Administrator (USER)
Create time      : 28-Feb-2010 12:34
Update time      : 04-Mar-2010 05:10
Updated by       : +policyfetcher (USER)
Effective UID    : superadmin
Policy Status    :
    mypolicy#01  : Deployed              Updated by: superadmin  On: 04-Mar-2010
05:10
    Deviation    : Unset                 Updated on: N/A

AC> er HNODE __local__ policy(name(mypolicy#01) status(undeployed)
updator(superadmin))
(localhost)
Successfully updated HNODE __local__
```

Rule with Variable Does Not Deploy On Endpoint

Symptom:

I created a policy that contains a rule with a variable and deployed the policy to an endpoint, but the rule is not implemented on the endpoint.

Solution:

Use the following procedure to troubleshoot the policy deployment:

1. Verify that the value of the policyfetcher_enabled configuration setting in the policyfetcher section on the endpoint is 1.

   A value of 1 for this configuration setting specifies to run policyfetcher. If policyfetcher is not running, it cannot deliver the policy to the endpoint.

2. Check the policyfetcher log for errors.

   Note: The policyfetcher log is in the *ACInstallDir*/Log directory, where *ACInstallDir* is the directory in which you installed CA Access Control.

3. Use CA Access Control Endpoint Management to verify that the variable is defined on the endpoint.

   Note: If the variable is not defined on the endpoint, the policy status is Deploy Pending.

   If the variable is not defined on the endpoint, create a new policy version that contains a selang rule that defines the variable, and deploy the new policy version to the endpoint.

4. Verify that the following are true:

   - The policy is assigned to the endpoint

     If the policy is not assigned to the endpoint, use CA Access Control Enterprise Management to assign the policy.

   - The deployment script for the policy does not contain errors.

     If the deployment script for the policy contains errors, create a new policy version that fixes the errors and deploy the new policy version to the endpoint.

   - The policy status is not Out of Sync.

     If the policy status is Out of Sync, a variable value may have changed in the CA Access Control endpoint. Redeploy the policy to clear the Out of Sync status.

5. Audit deployment information to verify that:

   - The endpoint has correctly compiled the policy
   - The DEPLOYMENT object for the policy does not contain any deployment errors

   If policy did not correctly compile or the DEPLOYMENT object contains errors, fix the errors and redeploy the policy.

6. Restart CA Access Control.

Built-In Variable Is Not Refreshed

Symptom:

I changed the system settings on a CA Access Control endpoint, but the value of a built-in variable has not changed to the value of the new system setting.

Solution:

Use the following procedure to troubleshoot this problem:

1. Verify that the value of the policyfetcher_enabled configuration setting in the policyfetcher section on the endpoint is 1.

   A value of 1 for this configuration setting specifies to run policyfetcher. If policyfetcher is not running, it cannot check the CA Access Control database for updated variables.

2. Verify that policyfetcher has sent a heartbeat after you changed the system setting, as follows:

   a. In CA Access Control Enterprise Management, click World View and click the World View task.

      The Search screen appears.

   b. If required, define the search criteria to locate a particular subset of data, and click Go.

      The results matching the criteria you defined are displayed by category.

   c. Verify that the update time in the Last Status column is later than the time at which you changed the system setting.

      If the update time in the Last Status column for the endpoint is earlier than the time you changed the system setting, policyfetcher has not sent a heartbeat and has not yet checked for updated variable values.

      Note: You can change the interval between heartbeats by changing the endpoint_heartbeat configuration setting.

3. Restart CA Access Control and verify that the system setting has changed.

DNSDOMAINNAME Variable Does Not Have a Value

Symptom:

The built-in <!DNSDOMAINNAME> variable does not have a value.

Solution:

Verify that the endpoint has a DNS domain.

To verify that a Windows endpoint has a DNS domain, do the following:

1. Open a command prompt and run the following command:

   ```
   ipconfig/all
   ```

2. Verify that the Primary DNS Suffix is set to the correct value.

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

DOMAINNAME Variable Does Not Have a Value

Symptom:

The built-in <!DOMAINNAME> variable does not have a value.

Solution:

Verify that the endpoint is connected to a domain.

To verify that a Windows endpoint is connected to a domain, do the following:

1. Right-click My Computer, click Properties, click the Computer Name tab, and click Change.
2. Verify that a domain appears in the Member Of Domain: field.

To verify that a UNIX endpoint is connected to a domain, do the following:

1. Run the following command:

   ```
   ypcats hosts
   ```

2. Verify that the endpoint is connected to a NIS domain.

HOSTNAME Variable Does Not Have a Value

Symptom:

The built-in <!HOSTNAME> variable does not have a value or is not fully qualified.

Solution:

Verify that the endpoint has a fully-qualified host name.

To verify that a Windows endpoint has a fully-qualified host name, do the following:

1. Open a command prompt and run the following command:

   ```
   ipconfig/all
   ```

2. Verify that the Primary DNS Suffix is set to the correct value.

To verify that a UNIX endpoint is connected to a domain, check that the hostname is defined and fully qualified in the following files:

- /etc/hosts
- /etc/resolv.conf

HOSTIP Variable Does Not Have a Value

Symptom:

The built-in <!HOSTIP> variable does not have a value or does not have all IP addresses for the endpoint.

Solution:

Verify that the IP addresses are present on the endpoint.

To verify that IP addresses are present on a Windows endpoint, do the following:

1. Open a command prompt and run the following command:

   ```
   ipconfig/all
   ```

2. Verify that the IP address or addresses are correct.

To verify that that IP addresses are present on a UNIX endpoint, do the following:

1. Run the following command:

   ```
   ifconfig -a
   ```

2. Verify that the IP address or addresses are correct.

An Operating System Variable Does Not Have a Value

Symptom:

I defined a CA Access Control operating system variable to point to a location on an endpoint. When I use this variable in a rule in a policy, CA Access Control does not enforce the rule because the operating system variable does not have a value.

Solution:

Verify that the environment variable exists in the operating system on the endpoint.

To verify that the variable exists in the operating system

1. Verify that the CA Access Control variable is defined as an operating system variable (OSVAR type).
2. Verify that the operating system variable exists in the operating system, as follows:
   - (Windows) Open a command prompt window and run the following command:

     ```
     set
     ```

   - (UNIX) Open a command prompt window and run the following command:

     ```
     env
     ```

     Note: You must be the root user to run this command.

A Registry Variable Does Not Have a Value

Valid on Windows

Symptom:

I defined a CA Access Control registry variable to point to a location on an endpoint. When I try to use this variable in a rule in a policy, CA Access Control does not enforce the rule because the registry variable does not have a value.

Solution:

Registry variables (REGVAL type variables) must point to REG_SZ or REG_EXPAND_SZ registry types. Verify that the registry value specified in the registry variable is REG_SZ or REG_EXPAND_SZ type.

Chapter 8: Collecting Audit Records

This section contains the following topics:

Some Audit Log Messages Are Not Received By the Collection Server

Valid on UNIX

Symptom:

I configured the endpoints in my CA Access Control installation to route their local audit logs to a central log collection server, but the server does not receive all the audit logs. I configured selogrd to emit the audit records and selogrcd to collect the audit records.

Solution:

To troubleshoot selorgd, the emitter daemon for the CA Access Control log routing system, do the following:

- Review the selogrd.cfg file. This file configures which audit messages CA Access Control routes to the central log collector.
- Review the audit log for each endpoint. If an audit event is missing from the audit log, review the audit.cfg file. The audit.cfg file configures which audit events CA Access Control writes to the audit log. If the audit.cfg file prevents CA Access Control from writing an audit event to the audit log, the audit event cannot be routed.
- Configure selogrd, the emitter daemon for the log routing system, to print debug messages then recreate the problem. Use the following command to configure selogrd to print debug messages:

  ```
  selogrd -d
  ```

No Audit Log Messages Are Received By the Collection Server

Valid on UNIX

Symptom:

I configured the endpoints in my CA Access Control installation to route their local audit logs to a central log collection server, but the server does not receive any audit logs. I configured selogrd to emit the audit records and selogrcd to collect the audit records.

Solution:

Verify that selogrcd is running on the log collection server.

Note: If selogrcd does not run for an extended period of time, audit events may be discarded by the endpoints.

SID Resolution Failed (Event Viewer Warning)

Valid on Windows

Symptom:

When I view the Application log of the Windows Event Viewer, I find a Warning event from CA Access Control that says that resolving a specific SID into an account name has failed.

Solution:

A *security identifier (SID)* is a numeric value that identifies a user or group to the operating system. Each entry in the discretionary access control list (DACL) has an SID that identifies the user or group for whom access is allowed, denied, or audited.

This warning appears when the operating system was not able to convert the SID into an account name, for example, if the user or group that the SID refers to no longer exists. Make sure that the problematic system and its corresponding domain controller are configured correctly for SID resolution.

SID Resolution Times Out (Event Viewer Warning)

Valid on Windows

Symptom:

When I view the Application log of the Windows Event Viewer, I find a Warning event from CA Access Control that says that resolving a specific SID into an account name has timed out.

Solution:

A *security identifier (SID)* is a numeric value that identifies a user or group to the operating system. Each entry in the discretionary access control list (DACL) has an SID that identifies the user or group for whom access is allowed, denied, or audited.

This warning appears when the operating system was not able to convert the SID into an account name within the defined timeout. Make sure that the:

- Problematic system and its corresponding domain controller are configured correctly for SID resolution
- Network settings are configured correctly

You can also increase the timeout by changing the DefLookupTimeout configuration setting in the following registry key:

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\SeOSD
```

Note: Increasing the SID resolution timeout may downgrade CA Access Control performance.

Receive Error Code 4631 When Attempting to Start selogrd

Valid on UNIX

Symptom:

I attempt to start selogrd. selogrd does not start and I receive the following error message:

```
ERROR 4631 (0x1217) initializing /opt/CA/AccessControl/bin/selogrd
```

Solution:

Resolve the local host name before you start selogrd. To resolve the host name, add the host name to the operating system hosts file, or define the host name to NIS or DNS.

Audit Logging Stops When Audit File Size Exceeds 2 GB

Symptom:

CA Access Control stops writing audit records to the audit file when the audit file size exceeds 2 GB.

Solution:

CA Access Control cannot write audit records to the audit file when the size of the audit file exceeds 2 GB. The maximum size of the CA Access Control audit file is specified, in KB, by the audit_size configuration setting in the logmgr section.

To set the maximum size of the seos.audit file to 2 GB, set the value of the audit_size configuration setting in the logmgr section to 2097151.

System Slows When CA Access Control Writes to Audit Log

Symptom:

My computer slows when CA Access Control writes to the audit log.

Solution:

Most processes in the system could be blocked while CA Access Control writes audit and trace data. To reduce the time it takes for CA Access Control to write audit data and trace data, do the following:

- Set the audit mode only for resources and accesses you need.
- Open the trace only when you need to.
- Store audit file, trace file, and CA Access Control database files on the fastest available file system.

Filter Not Applied if Host is Assigned Multiple IP Addresses

Symptom

I configured the audit.cfg to filter TCP events on a host that is assigned multiple IP addresses using the host name. After I applied the filter, I cannot see the TCP logs for all the IP addresses.

Solution

When you apply the audit.cfg filter, the audit system resolves the host name to the IP address of the host and the host IP address to the host name. If you configure the host with more than one IP address, the audit.cfg filters the first IP address only.

To apply the audit.cfg filter to all IP addresses, specify all the IP addresses in the filter only and not the host name, for example:

```
TCP;*;192.168.30.138;*;R;P
TCP;*;192.168.30.139;*R;P
```

Chapter 9: Tuning Performance

This section contains the following topics:

MALLOC_ARENA_MAX=1 Not Working on RedHat Linux 6.2

Valid on RedHat Linux 6.2

Symptom:

I noticed that the UNAB uxauthd agent process exceeds the permitted memory threshold and periodically restart.

Solution:

The cause of the unstable behavior is related to the MALOC_ARNEA_MAX variable. To resolve the issue do *one* of the following:

- Upgrade the glibc library.
- Set the memory threshold to 500MB minimum:
  - Modify the agent_vmemory_max token value in uxauth.ini
  - Modify the ProcVSizeHigh token value in seos.ini if CA Access Control is installed
- Decrease the number of used threads:
  - Modify the working_threads token value in the uxauth.ini file to 2

Performance Degrades When CA Access Control Is Running

Symptom:

My computer slows when CA Access Control is running. When I stop CA Access Control, my computer performs as usual.

Solution:

To diagnose and correct the performance problem, troubleshoot the performance problem (see page 121).

System Load on CA Access Control Server Is Too High

Symptom:

I need to reduce system load on the CA Access Control server.

Solution:

To reduce system load, do the following:

- Avoid deep hierarchies in the database.

  Deep hierarchies of users and resources require system loads to obtain and check all dependencies.

- Avoid generic rules for frequently used directories.

  If you define a generic rule for a frequently used directory, CA Access Control checks many system actions. For example, if you write a generic protection rule that protects /usr/lib/*, CA Access Control checks every action in the system.

- (Solaris only) Specify that CA Access Control bypasses file access checks when the file belongs to a process file system (/proc).

  To specify that CA Access Control bypasses file access checks when the file belongs to a process file system, verify that the value of the proc_bypass configuration setting is 1 in the [SEOS_syscall] section of the seos.ini file.

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

Chapter 10: Troubleshooting UNAB

This section contains the following topics:

Failed to Install UNAB

Symptom:

I customized the installation package but when I attempt to install UNAB on the endpoint, the installation fails.

Solution:

Use the following procedure to troubleshoot the problem.

1. Review the UNAB installation log file, uxauth_install.log for errors. By default, the file is located in the following directory:

   `/opt/CA/uxauth`

2. Export the UNAB installation log file and send the file to CA Support.
3. Run the installation process in debug mode:
   - For native package installations, create a file named seos_debug_on in /tmp directory and assign a debug level, between 0-9 to the file.
4. Run the native package in debug mode:
   - AIX— add -e<*log_file_name*> flag to the install command
   - HP-UX—review the installation log file that the swinstall generates for swjob
   - Linux—add -vv flag to the install command
   - Solaris—add -v flag to the install command

Troubleshoot UNAB Registration

The following section contains information that you can use to troubleshoot problems you encounter during UNAB registration with Active Directory.

UNAB Registration Failed Due to Incorrect Password

Symptom:

When I try to register UNAB with Active Directory, registration fails with the following error message:

```
Preauthentication failed while getting initial credentials Kerberos
preauthentication using <Administrator> failed
```

Solution:

UNAB registration failed due to incorrect administrator password. To troubleshoot this issue, verify the administrator password and register UNAB.

UNAB Registration Failed Due to Incorrect Clock Skew

Symptom:

When I try to register UNAB with Active Directory, I receive the following error message:

```
Clock skew too great while getting initial credentials Kerberos preauthentication
using <Administrator> failed
```

Solution:

UNAB registration failed because the clock skew between Active Directory and the UNAB endpoint is larger than configured.

To resolve this issue, do the following:

1. Manually synchronize the UNAB endpoint clock with that of Active Directory.
2. Set use_time_sync token value to yes under the [Agent] section in uxauth.ini to automatically configure time synchronization.

UNAB Registration Failed Due to Incorrect NTP Server Configuration

Symptom:

When I try to register UNAB with Active Directory, I receive the following error message:

```
WARNING: NTP service location is specified incorrectly
```

Solution:

UNAB registration failed because the network time protocol server (NTP) is incorrectly configured.

To troubleshoot this issue, set the ntp_server token under the [Agent] section in uxauth.ini to point to the NTP server.

UNAB Registration Failed Due to Invalid Configuration

Symptom:

When I try to register UNAB in Active Directory, I receive the following error message:

```
Error initializing Kerberos 5 library.Please check '/opt/CA/uxauth/uxauth.ini'
Kerberos preauthentication using <Administrator> failed
```

Symptom:

UNAB registration failed because the uxauth.ini file contains invalid Kerberos values.

To troubleshoot this issue, run the uxpreinstall utility to verify the Kerberos configuration.

UNAB Registration Failed Due to Missing DNS Settings

Symptom:

When I try to register UNAB with Active Directory, I receive the following error message:

```
Cannot find RRs for LDAP services in <domain_name> domain
```

Solution:

UNAB registration failed because the DNS settings are not configured in Active Directory.

To troubleshoot this issue, do the following:

1. Run the uxpreinstall utility to check the DNS settings.
2. Review the output of the uxpreinstall utility to identify the DNS settings.
3. If incorrect, update the DNS settings in the following file:

   /etc/resolv.conf

uxconsole -register Fails

Valid on UNIX

Symptom:

When I run uxconsole -register to register a UNAB endpoint, the following error message appears:

```
No server can be used as a DC for communicating with Active Directory.
Please check the lookup_dc_list and ignore_dc_list tokens in the [ad] section.
```

Solution:

When uxconsole registers the UNAB endpoint in Active Directory, the Active Directory site that is closest to the physical location of the endpoint is discovered. However, the ignore_dc_list configuration setting in the ad section of the uxauth.ini file lists domain controllers that the UNAB endpoint does not communicate with. If all domain controllers from the discovered Active Directory site are listed in the ignore_dc_list configuration setting, registration fails.

To fix this problem, delete the names of any domain controllers in the discovered Active Directory site from the ignore_dc_list configuration setting and rerun the uxconsole utility.

Note: The uxconsole utility writes the name of the discovered Active Directory site to the ad_site configuration setting in the ad section of the uxauth.ini file. For more information about UNAB Active Directory site support, see the *Implementation Guide*.

UNAB Log in Policy Not Distributed

Symptom:

I attempted to deploy a UNAB log in policy to the UNAB endpoints, but the policy is not distributed.

Solution:

To troubleshoot this issue, do the following:

1. Verify that UNAB is started on the endpoint:
   a. Open a command prompt window on the endpoint.
   b. Run the following command:

      ```
      ./uxauthd.sh status
      ```

   A message informs you of the current status of UNAB.
2. Verify that the policy was downloaded to the host:
   a. From a command prompt window on the endpoint, run the following command:

      ```
      ./uxconsole -status -detail
      ```

   The information includes the policy name, if deployed to the endpoint.
3. Review the policy authorization commands that the Enterprise Management Server sent to the UNAB endpoint.
   - From a command prompt window on the endpoint, run the following command:

     ```
     ./uxaudit -a
     18 Jan 2011 11:03:23 S UPDATE       TERMINAL   ac_entm_pers  338 10
     _default             acmanager.forwardinc.com auth terminal _default
     xuid(yaeyu01)access(read) (OS user)
     ```

   Verify that the rules were not modified.
4. Search the syslog file for Message Queue communication errors.
5. Verify the user account for login permissions and status.
6. Run the following command for a command prompt window:

   ```
   uxconsole –manage –show –user <AD_user_account>
   ```

ReportAgent Fails to Send Reports to the Enterprise Management Server

Symptom:

I started UNAB and verified that the ReportAgent daemon is running but I cannot view reports in CA Access Control Enterprise Management.

Solution:

Use the following procedure to troubleshoot this issue:

1. Check the syslog for Message Queue server communication-related error messages in the 'UNAB EP communication problems with ENTM' section.
2. Verify that the audit_enabled token under the [ReportAgent] section in the accommon.ini file is set to 1, If you want to send reports data to CA User Activity Reporting Module.
3. Enable ReportAgent debugging.
4. Set the debug token under the [ReportAgent] section in the accommon.ini file to 1
5. Review the UNAB reports debug file unab2xml.log. The file is located in the following directory:

   ```
   /opt/CA/AccessControlShared/log
   ```

6. Run the ReportAgent manually to generate a UNAB database snapshot:

   ```
   /opt/CA/AccessControlShared/bin/ReportAgent -debug 0 -task 2 –now
   ```

   Note the following:

   - Add the path '/opt/CA/AccessControlShared/lob' to $LD_LIBRARY_PATH before you run the ReportAgent manually.
   - Remove the .dat files from the /opt/CA/AccessControlShared/data/audit2txt/ directory before you manually run the ReportAgent.
   - For more information about ReportAgent utility debug mode, refer to the *Reference Guide*.

Kerberos Preauthentication Fails When Registering a UNAB Host

Valid on UNIX

Symptom:

When I use the uxconsole -register command, I receive the following error message:

```
krb5_set_config_files failed for /opt/CA/uxauth/uxauth.ini: Missing open brace in
profile
Kerberos preauthentication using <Administrator> failed
```

Solution:

There is an unset configuration setting in the uxauth.ini file. To fix this problem, verify that each configuration setting in the uxauth.ini file has a value.

Receive Error Code 2803 When Registering or Starting UNAB

Valid on UNIX

Symptom:

I receive the following error message when I try to register a UNAB host in Active Directory or try to start UNAB:

```
Unable to open nss or create nss cache. Error code 2803.
```

Solution:

There is not enough memory in the /var directory. To fix this problem, verify that less than 95% of /var is used, and retry the command.

Active Directory User Cannot Log In to UNAB Endpoint

Valid on UNIX

Symptom:

An Active Directory user that has UNIX attributes cannot log in to a UNAB endpoint.

Solution:

To troubleshoot the problem, do the following:

1. Verify that the user's container is one of the following:
   - The container specified in the user_container configuration setting.
   - A sub-container under the container specified in the user_container configuration setting.

     Note: The user_container configuration setting is located in the AD section of the uxauth.ini file.
2. Verify that the user has a UID and a GID in Active Directory.
3. Verify that the user is not suspended.
4. Verify that UNAB is started on the endpoint:
   a. Open a command prompt window on the endpoint.
   b. Run the following command:

      ```
      ./uxauthd.sh status
      ```

      A message informs you of the current status of UNAB.
5. Verify that the endpoint is registered in Active Directory.

   Note: If the endpoint is not registered in Active Directory, use the uxconsole -register utility to register the host.
6. Stop the name or password caching daemon for your OS on the endpoint, as follows:
   a. Stop UNAB:

      ```
      ./uxauthd.sh stop
      ```
   b. Delete the NSS cache database:

      ```
      rm -rf /opt/CA/uxauth/etc/nss.db
      ```
   c. Check if the name or password caching daemon for your OS is running on the endpoint.

      For example, for a Linux or Solaris endpoint, check if the nscd daemon is running. For an HP-UX endpoint, check if the pwgrd daemon is running.
   d. If the name or password caching daemon for your OS is running, kill the process.
   e. Start UNAB:

      ```
      ./uxauthd.sh start
      ```

7. Obtain a Ticket Granting Ticket (TGT) using a different Active Directory user account.

   Run the following command to connect to Active Directory using the Administrator account:

   ```
   ./uxconsole -krb -init Administrator
   ```

   Note: You can obtain a TGT using the agent keytab, for example:

   ```
   ./uxconsole -krb -init -k
   ```

8. Resolve the Active Directory user account directly:

   - Run the following search:

     ```
     ./uxconsole -ldap -search "(&(objectClass=user)(sAMAccountName=johndoe))"
     ```

     Check for discrepancies between the expected and actual user account name.

9. Search for the user account in other domains, if applicable.

   - Run the following command:

     ```
     ./uxconsole -ldap -search -b DC=unabca,DC=test,DC=co,DC=il
     "(&(objectClass=user)(objectCategory=person))"
     ```

10. Verify that the user account UNIX attributes are identical on the Active Directory and UNIX.

User Cannot Run Commands on a UNAB Endpoint

Symptom:

I successfully log in to a UNAB endpoint, and UNAB creates a P (permitted) record in uxaudit, the UNAB audit file, that corresponds to my login. However, I cannot run any UNIX commands on the endpoint.

Solution:

The user has previously logged in to the same endpoint with the same username but with a different UID, so the user cannot access their /home directory.

To fix this problem, do the following:

1. Delete the /home directory for the user.

   Note: The /home directory is often located at /home/userName.

2. Ask the user to log in to the endpoint.

   A new /home directory is created for the user. The user can now perform UNIX commands on the UNAB endpoint.

Cannot View UNAB Endpoint in World View

Valid on UNIX

Symptom:

I use CA Access Control Enterprise Management to manage UNAB endpoints, but a UNAB endpoint does not appear in World View.

Solution:

Verify that the UNAB endpoint can communicate with the Distribution Server. Do the following on the UNAB endpoint:

1. Verify that the value of the Distribution_Server configuration setting is set to the name of the Distribution Server computer.

   The Distribution_Server configuration setting is located in the communication section of the accommon.ini file.

   Example: ssl://ds.comp.com:7243

   Note: By default, the Distribution Server is located on the Enterprise Management Server.

2. Verify that the Message Queue password is correct. The endpoint uses this password to communicate with the Distribution Server. Do the following:

   a. Open a command prompt window.

   b. Run the following command:

      ```
      acuxchkey -t pwd "password"
      ```

      password

      Defines the Message Queue password. By default, this password is the communication password that you define when you install CA Access Control Enterprise Management.

3. Restart the UNAB agent, as follows:

   a. Navigate to the UNAB lbin directory.

      By default, this directory is under /opt/CA/uxauth

   b. Restart the UNAB agent:

      ```
      ./uxauthd.sh restart
      ```

4. Verify that the Message Queue server is running, as follows:

   - Windows—verify that the CA Access Control Message Queue service is running.
   - UNIX—verify that the tibemsd process is running

5. Check the syslog or event viewer for Message Queue server communication errors.

6. Set the Message Queue server to log communicated-related messages to a log file. Do the following:
   - UNIX:
     a. Open the pmd.ini
     b. Modify the debug_mode token in the [endpoint_management] section to 1
   - Windows:

   a. Navigate to the following registry key:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Pmd\
   DMS_NAME\endpoint_management
   ```

   b. Modify the debug_mode token value to 1
7. Restart the Enterprise Management Server to apply the changes. Review the endpoint_management.log file located in the DMS directory for communication messages.

   You have verified that the UNAB endpoint can communicate with the Distribution Server.

Cannot Start Daemons on Linux s390 Endpoint

Valid on Linux s390 and Linux s390x

Symptom:

I cannot start the uxauthd or ReportAgent daemon.

Solution:

UNAB cannot locate the Java environment on the endpoint. To fix this problem, do the following:

1. Verify that the java_home configuration setting in the global section of the accommon.ini file contains the path to the Java environment.
2. Set the value of the LD_LIBRARY_PATH environment variable to the path to the shared libraries of the Java environment.

User Cannot Log In or Change Password

Valid on UNIX

Symptom:

When I try to log in or change my password on a UNAB endpoint, the following error message appears:

```
passwd: Authentication token manipulation error
```

Solution:

The PAM module timed out while waiting for uxauthd to respond to the password change request.

To fix this problem, do the following:

1. Increase the value of the pam_receive_timeout configuration setting in the pam section of the uxauth.ini file.

   For example, pam_receive_timeout=100

2. Stop and restart UNAB.

Note: For more information about the uxauth.ini file, see the *Reference Guide*.

Chapter 11: Troubleshooting PUPM

This section contains the following topics:

Break Glass Approval Workflow

Symptom:

I want to configure a single-step break-glass workflow to verify that the PUPM endpoint system administrator that the request applies to is notified and not the user manager.

Solution:

You can configure a single step, break glass workflow to specify that break glass requests are approved by the system administrator and not by the default approver.

Follow these steps:

1. In CA Access Control Enterprise Management, select Users and Group, Tasks, Modify Admin Tasks.

   The modify admin task: select task search window opens.

2. Select Category from the pull-down menu and enter *home* in the text box area. Click Search.

   CA Access Control Enterprise Management displays the tasks that correspond with the search criteria.

3. Select the Break Glass WF task, then click Select.

   The Break Glass WF properties window opens.

4. Navigate to the Events tab and click the right pointing arrow.

   The workflow mapping window opens.

5. Select SingleStepApproval from the Workflow Process pull-down menu.

6. Do the following in the Primary Approver section:

   a. Select Approve Break Glass Privileged Account from the Approval Task pull-down menu.

   b. Select Custom: PrivilegedAccountOwnerResolver from the Participant Resolver pull-down menu.

      A message appears, informing you that participant resolver configuration parameters are not set.

   c. Specify SourceObject in the New Parameter Name text box.

   d. Specify TaskAdmin in the Value text box.

   e. Click Add Parameter.

      CA Access Control Enterprise Management adds the approver task.

   f. Repeat steps c through e, using the following parameter name and values:

      - SourceObjectAttribute—tblUser.manager
      - TargetType—USER

7. Click OK.

   You have configures a single step break glass workflow and defined the system administrator as an approver.

RunAs Password Consumer Request Times Out

Valid on Windows

Symptom:

I configure a Windows RunAs password consumer to let a user execute the RunAs utility to perform a task. When the user executes the RunAs utility, the password request times out and the user cannot execute the utility.

Solution:

To fix this problem, increase the value of the following registry entry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\Plug
ins\RunAsPlg\CommunicationWaitTimeout
```

The registry entry specifies the time, in seconds, that the password consumer waits for a reply from the PUPM Agent.

Example: Change the Value of the CommunicationWaitTimeout Registry Entry

The following example increases the value of the CommunicationWaitTimeout registry entry to 30:

```
AC> env config
AC(config)> editres CONFIG ACROOT section(Instrumentation\PlugIns\RunAsPlg)
token(CommunicationWaitTimeout) value(30)
(localhost)
Successfully set the token.
```

ODBC, OLEDB, or OCI Database Password Consumer Request Times Out

Valid on Windows

Symptom:

I configure an ODBC, OLEDB, or OCI database password consumer on an endpoint. The password consumer requests a password when an application on the endpoint connects to a database. However, when the application tries to connect to the database, the password request times out.

Solution:

To fix this problem, increase the value of the following registry entry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\Plug
ins\plugin\CommunicationWaitTimeout
```

plugin

Specifies the name of the plug-in that intercepts the connection attempt.

Values: OCIPlg, ODBCPlg, OLEDBPlg

The registry entry specifies the time, in seconds, that the password consumer waits for a reply from the PUPM Agent.

Example: Change the Value of the CommunicationWaitTimeout Registry Entry

The following example increases the value of the CommunicationWaitTimeout registry entry to 30 for an OCI database password consumer:

```
AC> env config
AC(config)> editres CONFIG ACROOT section(Instrumentation\PlugIns\OCIPlg)
token(CommunicationWaitTimeout) value(30)
(localhost)
Successfully set the token.
```

PUPM SSH Device Timeout

Valid on Red Hat 5

Symptom

The create endpoint task timed out after I configured a Japanese Red Hat 5 as a PUPM SSH device endpoint and specified to use the operation administrator user login and operation administrator password.

Solution

To fix the problem, do the following:

1. Navigate to the following directory, where *ACServerInstallDir* indicates the directory where you installed the Enterprise Management Server:

   `ACServerInstallDir/Connector Server/conf/override/sshdyn`

2. Open the ssh_connector_conf.xml file for editing.

3. Add the following item under <array name="oChangePassword">

```
<item>
    <param name="sCommand" value="set LANG=C" />
    <param name="iWait" value="500" />
</item>
```

4. Save and close the file.

Requested Password Available For Check Out Without Approval Workflow Triggered

Valid for SunOne

Symptom:

After I enter a request for a privileged account password, the password is available for checkout without my manager first approving the request.

Solution:

By default, when you install the Enterprise Management Server with SunOne user directory, workflow support is disabled. You need to enable workflow support for users to submit requests for privileged account password.

To enable workflow support for SunOne directory, do the following:

1. If you did not do so before, enable the CA Identity Manager Management Console.
2. Open the CA Identity Manager Management Console.
3. Select Environments, ac-env, Advanced Settings, Workflow

   The workflow properties window opens.
4. Select the checkbox next to the Enable field.
5. Select Save, then select Restart to restart the environment.

   You have enabled workflow support for the SunOne directory.

Access Denied Message When Creating Windows Agentless Endpoint

Valid on Windows 7 Enterprise Edition

Symptom:

When I attempt to define a Windows 7 endpoint as a Windows Agentless endpoint type, I receive an "Access Defined" message and the process fails.

Solution:

The endpoint creation process fails because the account you specified is not the Administrator account but a member of the Administrators group.

To work around this problem, do the following:

1. Log in to the endpoint you want to manage as a member of the Administrators group.
2. Select Control Panel, User Accounts, Change User Accounts Control Settings.

   The User Account Control Settings window opens.
3. Set the notification level to Default, then click OK.

   You may need to restart your computer for the changes to take effect.
4. Select Administrative Tools, Computer Management, Services and Applications.
5. Right-click WMI Control, then select Properties.

   The WMI Control properties window opens.
6. Navigate to the Security tab.

   The Namespace navigation window opens.
7. Select Root, then select Security.

   The security dialog opens.
8. Select the Authenticated User from the group or user names section.
9. From the Allow column, clear the Execute Methods check box.
10. Click OK to apply the changes.

Filter CA Access Control Endpoints by Property

Valid on Windows

Symptom:

I installed several Distribution Servers to distribute communication handling with the PUPM endpoints. How can I configure the endpoints to communicate with a specific Distribution Server?

Solution:

You can configure each endpoint to communicate with a specific Distribution Server by using the endpoint details option.

Do the following:

1. In CA Access Control Enterprise Management, select Privileged Accounts, Endpoints, Modify Endpoint.
2. Search for the endpoint that you want to modify and select it.

   The general tab opens.
3. Move to the Information tab and specify a unique name in the Department field.
4. Save the settings.
5. On the Distribution Server, stop all CA Access Control services.
6. Access the Windows registry and locate the ENDPOINT_DEPARTMENT token in the following path:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Common\AgentManager\Plugins\AccountManager\QueryFilter
   ```
7. Set the token value to the department name you specified.
8. Start all CA Access Control services.

Cannot Create Endpoints Due to Incorrect Parameter

Symptom:

When creating an endpoint definition using PUPM, you may receive an error that indicates that "The parameter is incorrect."

```
Error: [General] Endpoint cannot be created in this endpoint type.
Details: Endpoint hostname: The parameter is incorrect.
```

The error is logged in the AgentManager.log as shown:

```
10/05/2013 12:37:54 acctmgr 2712> Using WMI ...
10/05/2013 12:37:54 acctmgr 2712> Connecting to host <HOST> using account CORP
\UserName ...
10/05/2013 12:37:55 acctmgr 2712> Failed IWbemLocator::ConnectServer,
                                  Error = 0x80070005 (Access is denied.)
10/05/2013 12:37:55 acctmgr 2712> Failed ValidateEndpointWMI, Trying
ValidateEndpointLDAP ...
10/05/2013 12:37:55 acctmgr 2712> Using LDAP ...
10/05/2013 12:37:55 acctmgr 2712> Connecting to host <HOST> using account CORP
\UserName ...
10/05/2013 12:37:59 acctmgr 2712> Failed IADsComputer::get_OperatingSystem,
                                  Error = 0x80070057 (The parameter is incorrect.)
10/05/2013 12:37:59 acctmgr 2712> Failed to validate endpoint HOSTNAME -
                                  The parameter is incorrect.
10/05/2013 12:37:59 acctmgr 2712> 'validate ep' ret FAIL
```

Solution:

The error is caused by a malformed username. In the above error log, note the misplaced space between the domain name and the slash in front of the username, “CORP \UserName”.

The correct formatting of the account name is “CORP\UserName”. Make certain to remove trailing spaces from the domain name, and remove leading spaces from the user name.

PUPM Feeder Polling Inconsistent In a Load Balancing Environment

Symptom:

I notice that the PUPM feeder polling demonstrates inconsistent behavior when working in an environment that contains a primary and a load balancing Enterprise Management Servers.

Solution:

When you work in an environment that contains a load balancing Enterprise Management Server you must place the feeder polling directory in a shared location on the network. You map the full pathname to shared directory from both Enterprise Management Servers.

Follow these steps:

1. In CA Access Control Enterprise Management select Users and Groups, Tasks, Modify Admin Task.
2. Search for and select the Import Endpoints Or Accounts task.
3. Expand the Import Endpoints or Accounts task.
4. Specify the PUPM feeder polling folder in the Folder for Polling (absolute path) field. For example: /Z:/Feeder).
5. Click OK and then click Submit.
6. Navigate to the following path where *JBoss_HOME* indicates the directory where you installed JBoss:

   JBoss_HOME`/server/default/deploy\/dentityMinder.ear/custom/ppm/default/feeder.properties`
7. Specify the full pathname to the shared folder as follows:
   FOLDER_FOR_POLLING=Z:/Feeder

   Important! Perform this procedure on each Enterprise Management Server in your environment.

Chapter 12: Troubleshooting the Reporting Service

This section contains the following topics:

How to Troubleshoot the Reporting Service

The CA Access Control reporting service lets you view the security status of each endpoint (users, groups, and resources) in a central location. When you troubleshoot the reporting service, you check each of its components in turn.

The following process helps you troubleshoot the reporting service:

1. Do *one* of the following, as appropriate to the operating system on the endpoint:
   - Troubleshoot the Report Agent on a UNIX computer (see page 101)
   - Troubleshoot the Report Agent on a Windows computer (see page 105)
2. Troubleshoot the Distribution Server (see page 108).
3. Troubleshoot JBoss (see page 110).
4. Troubleshoot the Report Portal (see page 111).

Troubleshoot the Report Agent on a UNIX Computer

Valid on UNIX

The Report Agent collects scheduled snapshots of the local CA Access Control database and any policy model databases (PMDBs) on the endpoint, and sends this snapshot in XML format to the report queue on the Distribution Server.

Note: The Report Agent also performs other tasks. For more information about the Report Agent, see the *Reference Guide*.

To troubleshoot the Report Agent on a UNIX computer

1. Verify that the library path environment variable is set correctly. Do the following:

   a. su to root.

   b. Set the library path environment variable to *ACSharedDir*/lib. Be default, *ACSharedDir* is the following directory:

      `/opt/CA/AccessControlShared`

   c. Export the library path environment variable.

2. Verify that the following configuration settings are correct. The configuration settings are located in the [ReportAgent] section of the accommon.ini file:

   Note: You can use either CA Access Control Endpoint Management or selang commands to verify the value of the configuration settings. However, for this procedure we recommend that you use selang commands in the config environment to change the value of configuration settings. Using selang commands lets you change the configuration settings in this procedure without having to stop and restart CA Access Control.

   reportagent_enabled

   Specifies whether reporting is enabled (1) on the local computer.

   Default: 0

   Important! You must set the value of this configuration setting to 1 to enable the Report Agent to run automatically. If the value of this configuration setting is 0, the Report Agent does not send scheduled snapshots of the database to the Distribution Server. However, if the value of this configuration setting is 0 you can still run the Report Agent in debug mode.

   schedule

   Defines the schedule of when reports are generated and sent to the Distribution Server.

   You specify this setting in the following format: time@day[,day2][...]

   Default: 00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

   Example: "19:22@Sun,Mon" generates reports every Sunday and Monday at 7:22 pm.

   send_queue

   Defines the name of the Message Queue on the Distribution Server to which the Report Agent sends snapshots of the local database.

   Default: queue/snapshots

   Important! Do not change the default value of this configuration setting.

3. Verify that the following configuration setting is correct. The configuration setting is located in the [communication] section of the accommon.ini file:

   Note: You can use either CA Access Control Endpoint Management or selang commands to verify the value of the configuration settings. However, for this procedure we recommend that you use selang commands in the config environment to change the value of configuration settings. Using selang commands lets you change the configuration settings in this procedure without having to stop and restart CA Access Control.

   Distribution_Server

   Defines the Distribution Server URL.

   Note: The default port for TCP communication is 7222 and the default port for SSL communication is 7243. You should verify that the Distribution Server URL specifies the correct port number for the communication type.

   Default: none

   Example: ssl://172.24.176.145:7243. This URL configures the Report Agent to communicate with the Distribution Server at the IP address 172.24.176.145 on port 7243, using the SSL protocol.

4. Verify that the following line exists in the [daemons] section of the seos.ini file:

   ```
   ReportAgent = yes, ACSharedDir/lbin/report_agent.sh start
   ```

   This line enables the Report Agent daemon to execute automatically when CA Access Control starts.

   Note: By default, the *ACSharedDir* directory is located at /opt/CA/AccessControlShared.

5. Stop CA Access Control:

   ```
   secons -s
   ```

   CA Access Control and the Report Agent stops.

6. Navigate to the following directory:

   ```
   ACSharedDir/bin
   ```

7. Run the Report Agent in debug mode, using the following command:

   ```
   ./ReportAgent -debug 0 -task 0 -now
   ```

   ReportAgent

   Runs the Report Agent.

   -debug 0

   Specifies to run the Report Agent in debug mode and to display the output on the console.

   Note: You cannot run the Report Agent in debug mode if the Report Agent daemon is enabled.

   -task 0

   Specifies that the Report Agent collects and sends information about the CA Access Control database, and any local PMDBs, to the Distribution Server. This information is used to generate CA Access Control reports.

   -now

   Specifies to run the Report Agent now.

8. Review the Report Agent output as follows:

   - Review the output for errors
   - Verify that the correct names are specified in the Send Queue and the Report File parameters in the Send report parameters section

9. Start CA Access Control:

   ```
   seload
   ```

   CA Access Control and the Report Agent start.

Example: Report Agent Output

The following Report Agent output shows the Send Queue and Report File parameters:

```
------------------------------------------------------------------------
Send report parameters:
------------------------------------------------------------------------
Send Queue.................. queue/snapshots
Report File.................
/work/opt/CA/AccessControlShared/data/db2xml/ACDB.xml
------------------------------------------------------------------------
start sending report to queue 'queue/snapshots'...
```

Troubleshoot the Report Agent on a Windows Computer

Valid on Windows

The Report Agent collects scheduled snapshots of the local CA Access Control database and any policy model databases (PMDBs) on the endpoint, and sends this snapshot in XML format to the report queue on the Distribution Server.

Note: The Report Agent also performs other tasks. For more information about the Report Agent, see the *Reference Guide*.

To troubleshoot the Report Agent on a Windows computer

1. Verify that the following configuration settings are correct. The configuration settings are located in the following registry key:

   `HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\ReportAgent`

   Note: You can use either CA Access Control Endpoint Management or selang commands to verify the value of the configuration settings. However, for this procedure we recommend that you use selang commands in the config environment to change the value of configuration settings. Using selang commands lets you change the configuration settings in this procedure without having to stop and restart CA Access Control.

   reportagent_enabled

   Specifies whether reporting is enabled (1) on the local computer.

   Default: 0

   Important! You must set the value of this configuration setting to 1 to enable the Report Agent to run automatically. If the value of this configuration setting is 0, the Report Agent does not send scheduled snapshots of the database to the Distribution Server. However, if the value of this configuration setting is 0 you can still run the Report Agent in debug mode.

   schedule

   Defines the schedule of when reports are generated and sent to the Distribution Server.

   You specify this setting in the following format: time@day[,day2][...]

   Default: 00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

   Example: "19:22@Sun,Mon" generates reports every Sunday and Monday at 7:22 pm.

send_queue

Defines the name of the Message Queue on the Distribution Server to which the Report Agent sends snapshots of the local database.

Default: queue/snapshots

Important! Do not change the default value of this configuration setting.

2. Verify that the following configuration setting is correct. The configuration setting is located in the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Common\communica
tion
```

Distribution_Server

Defines the Distribution Server URL.

Note: The default port for TCP communication is 7222 and the default port for SSL communication is 7243. You should verify that the Distribution Server URL specifies the correct port number for the communication type.

Default: none

Example: ssl://172.24.176.145:7243. This URL configures the Report Agent to communicate with the Distribution Server at the IP address 172.24.176.145 on port 7243, using the SSL protocol.

3. Verify that the CA Access Control Report Agent service is started.

   Note: You must set the reportagent_enabled configuration setting to 1 to configure the CA Access Control Report Agent service to start automatically.

4. Open a command prompt window and stop CA Access Control:

```
secons -s
```

CA Access Control stops, including the Report Agent service.

5. Run the Report Agent in debug mode, using the following command:

   ```
   reportagent -debug 0 -task 0 -now
   ```

   reportagent

   Runs the Report Agent.

   -debug 0

   Specifies to run the Report Agent in debug mode and to display the output on the console.

   Note: You cannot run the Report Agent in debug mode if the Report Agent service is started.

   -task 0

   Specifies that the Report Agent collects and sends information about the CA Access Control database, and any local PMDBs, to the Distribution Server. This information is used to generate CA Access Control reports.

   -now

   Specifies to run the Report Agent now.

6. Review the Report Agent output as follows:

   - Review the output for errors
   - Verify that the correct names are specified in the Send Queue and the Report File parameters in the Send report parameters section

7. Start CA Access Control:

   ```
   seosd -start
   ```

   CA Access Control starts and the Report Agent service is started.

Example: Report Agent Output

The following Report Agent output shows the Send Queue and Report File parameters:

```
----------------------------------------------------------------------
Send report parameters:
----------------------------------------------------------------------
Send Queue................... queue/snapshots
Report File.................. C:\Program
Files\CA\AccessControl\data\db2xml\ACDB.xml
----------------------------------------------------------------------
start sending report to queue 'queue/snapshots'...
```

Library Path Environment Variable Example

The following example sets and exports the library path environment variable on a Linux or Solaris computer:

```
LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/opt/CA/AccessControlShared/lib
export LD_LIBRARY_PATH
```

The following example sets and exports the library path environment variable on an AIX computer:

```
export LIBPATH=$LIBPATH:/opt/CA/AccessControlShared/lib
```

The following example sets and exports the library path environment variable on an HP-UX computer:

```
export SHLIB_PATH=$SHLIB_PATH:/opt/CA/AccessControlShared/lib
```

Troubleshoot the Distribution Server

On the Distribution Server, the Message Queue receives information that the Report Agents send from the endpoints. Message-driven Java beans (MDBs) then read the data in the Message Queue and write the data to the central database.

To troubleshoot the Distribution Server

1. (UNIX) Start the Tibco EMS Administration Tool, as follows:
   a. Navigate to the following directory:
      `/opt/CA/AccessControlServer/MessageQueue/tibco/ems/5.1/bin`
   b. Run the following command:
      ```
      ./tibemsadmin
      ```
2. (Windows) Start the Tibco EMS Administration Tool, as follows:
   a. Navigate to the following directory:
      `C:\Program Files\CA\AccessControlServer\MessageQueue\tibco\ems\5.1\bin`
   b. Run the following command:
      ```
      tibemsadmin.exe
      ```

3. Connect to the current environment, using *one* of the following commands:

   ■ If the Distribution Server listens for the Report Agent on port 7222 (the default port), use the following command:

     `connect`

   ■ If the Distribution Server listens for the Report Agent in SSL mode on port 7243, use the following command:

     `connect SSL://7243`

4. Enter your username and password.

   Note: The default username is admin, and by default the password is the communication password that you specified when you installed CA Access Control Enterprise Management or the Distribution Server.

   You are connected to the Message Queue on the Distribution Server.

5. Enter the following command:

   `show queues`

   A list of the queues on the Distribution Server appears.

6. Open a command prompt window on an endpoint.

7. (UNIX) Set the library path environment variable, as follows:

   a. su to root.

   b. Set the library path environment variable to *ACSharedDir*/lib. By default, *ACSharedDir* is the following directory:

      `/opt/CA/AccessControlShared`

   c. Export the library path environment variable.

8. (UNIX) Navigate to the following directory:

   ACSharedDir`/bin`

9. Run the Report Agent on the endpoint. Do *one* of the following:

   ■ (Windows) Run the following command:

     `ReportAgent -report snapshot`

   ■ (UNIX) Run the following command:

     `./ReportAgent -report snapshot`

   The Report Agent sends a snapshot of the CA Access Control database and any local PMDBs to the report queue on the Distribution Server.

10. Observe the queue named queue/snapshots in the tibemsadmin utility as the Report Agent runs.

    If the queue grows and does not shrink, JBoss may not be running. You must troubleshoot JBoss.

Troubleshoot JBoss

The JBoss web application server environment contains the message-driven Java beans (MDBs) that read the data from the Message Queue and write it into the central database. The central database stores reporting data.

To troubleshoot JBoss

1. Verify that JBoss starts correctly, as follows:
   - If you start JBoss from a command prompt, review the initial output when JBoss starts. Verify that the output does not contain any errors.
   - If you start JBoss as a service, use the log files or the tail command to review the initial output when JBoss starts. Verify that the output does not contain any errors.
2. Open the following file and review it for errors, where *JBossInstallDir* is the directory in which you installed JBoss:

   JBossInstallDir/server/default/log/boot.log

   This file lists the steps that JBoss takes each time it boots the microkernel.
3. Verify that the JAVA_HOME variable is set to the correct location.

   Note: If the JAVA_HOME variable is set to the correct location but JBoss does not resolve the variable, set the JAVA_HOME variable to a lower location, for example, the bin directory under the JDK installation path.
4. Open the following file and review it for errors:

   JBossInstallDir/server/default/log/server.log

   This file lists the actions that JBoss performs in the JBoss web application server environment.

   Note: JBoss creates to new server.log file each time you start it.
5. Verify that JBoss ports do not conflict with ports that are used on other services.
6. (Optional) If the JNP port conflicts with another service, change the JNP port on 1099 to another port, as follows:

   a. Open the following file in a text editor:

      JBossInstallDir/server/default/conf/jboss-service.xml

   b. Change the port number in the following section:

```
<!-- The listening port for the bootstrap JNP service. Set this to -1 to run
the NamingService without the JNP invoker listening port.-->
<attribute name="Port">1099</attribute>
```

   c. Save and close the file.

7. (Optional) If the RMI port conflicts with another service, change the RMI port on 1098 to another port, as follows:

   a. Open the following file in a text editor:

      JBossInstallDir/server/default/conf/jboss-service.xml

   b. Change the port number in the following section:

```
<!-- The port of the RMI naming service, 0 == anonymous -->
<!-- attribute name="RmiPort">1098</attribute -->
<attribute name="RmiPort">1098</attribute>
```

   c. Save and close the file.

Troubleshoot the Report Portal

The Report Portal lets you access the endpoint data that the Distribution Server stores in the central database to produce built-in reports, or to interrogate the data and produce custom reports. To do this, it uses CA Business Intelligence.

To troubleshoot the Report Portal

1. Verify that you use the correct URL to access the reporting interface (BusinessObjects InfoView). The correct URL is:

   http://*host*:*port*/businessobjects/enterprise115/desktoplaunch

2. (Windows) Verify that you use the correct menu option to access InfoView.

   To access InfoView, click Start, Programs, BusinessObjects XI Release 2, BusinessObjects Enterprise, BusinessObjects Enterprise Java InfoView.

3. Verify that the following services are started:

   - Apache Tomcat
   - Central Management Server
   - Connection Server
   - Crystal Reports Cache Server
   - Crystal Reports Job Server
   - Crystal Reports Page Server
   - Desktop Intelligence Cache Server
   - Desktop Intelligence Job Server
   - Desktop Intelligence Report Server
   - Destination Job Server
   - Event Server

- Input File Repository Server
- List of Values Job Server
- Output File Repository Server
- Program Job Server
- Report Application Server
- Web Intelligence Job Server
- Web Intelligence Report Server

4. Test the connection to the CA Access Control Universe.

   Note: If the CA Access Control Universe does not appear in BusinessObjects Designer, the report package may not be deployed. For more information about how to deploy the report package, see the *Implementation Guide*.

Test the CA Access Control Universe Connection

The CA Access Control Universe is provided by CA to simplify the creation of reports from the CA Access Control reporting service central database.

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

If after you install the standard CA Access Control reports you experience issues with the reporting service connection, you should test and modify the connection as required.

To test the CA Access Control Universe Connection

1. Select Start, Programs, Business Objects XI Release 2, BusinessObjects Enterprise, Designer.

   The User Identification dialog appears, letting you log in to BusinessObjects Designer.

2. Enter your credentials and click OK.

   The welcome screen of the Quick Design wizard appears.

3. Clear the Run this Wizard at Startup check box, and click Cancel

   An empty Designer session opens. The user name and repository name appear in the title bar.

4. Click File, Import, browse to the directory that contains the CA Access Control Universe, select the CA Access Control universe, then click OK.

   The CA Access Control Universe imports successfully and opens in the current Designer window.

   Note: The CA Access Control Universe is stored under CA Universe\CA Access Control in the directory designated as the default universe file store.

5. Click Tools, Connections

   The Wizard Connection dialog appears.

6. Select the Access_Control1 connection that you want to test, then click Test.

   A message confirms that the connection is responding. If the connection is not responding you receive an error message.

7. If you received an error, click Edit to modify connection settings:

   - Database Middleware Selection—Oracle\Oracle 10\Oracle Client
   - Type—Secured
   - Name—Access_Control1
   - User name—*Oracle_adminUserName*
   - Password—*Oracle_adminUserPass*
   - Service—Oracle_TNS_Name

   Repeat step 6 as required to test the connection.

Report Server is Down or Unreachable

Symptom:

When I try to view a report in CA Business Intelligence or CA Access Control Enterprise Management, I receive the following error message:

```
The Report Server is either down or unreachable.
```

Solution:

To troubleshoot this problem, do the following:

1. Open the JBoss log file. The JBoss log file is located in the following directory, where *JBossInstallDir* is the directory in which you installed JBoss:

   JBossInstallDir/server/default/log/server.log

   This file lists the actions that JBoss performs in the JBoss web application server environment.

   Note: JBoss creates to new server.log file each time you start it.

2. Locate the cause of the error in the log file.
3. Make a note of the case-sensitive name of the computer that appears in the error.

   You must record the name exactly as it appears in the log file.
4. Open the hosts file. The hosts file is located in the following directory by default:
   - (UNIX) /etc/hosts
   - (Windows) C:\WINDOWS\system32\drivers\etc
5. On a new line in the file, enter the IP address and the case-sensitive name of the computer, separated by a space.

   You recorded the computer name in Step 3.
6. Save and close the file.

Example: The Hosts File

The following snippet is an example of the hosts file:

```
127.0.0.1       localhost
```

Cannot View Reports in CA Business Intelligence with an MS SQL Database

Symptom:

I use an MS SQL database as my central database, and I cannot view reports in CA Business Intelligence. When I try to view a report, I receive the following error message:

```
Failed connect
```

Solution:

The following process helps you troubleshoot the problem with CA Business Intelligence:

1. Verify the BusinessObjects version number, as follows:

   a. Open the following URL:

      `http://`*`hostname`*`:8080/businessobjects/enterprise115/adminlaunch/launchpad.html`

      hostname

      Defines the name of the Report Portal host.

      The Central Management Console log on page appears.

   b. Enter your username and password, and click Log On.

      The Central Management Console appears.

   c. Click Servers, *hostname*, Web_IntelligenceReportServer, Metrics.

      The BusinessObjects version number is displayed.

   d. Verify that the BusinessObjects version number is either 11.5.8.1061 or higher, or 11.5.10.1263 or higher.

2. Verify the CA Business Intelligence version number, as follows:

   a. Open the following file on the Report Portal:

      - (Windows) C:\Program Files\CA\SC\CommonReporting\version.txt
      - (UNIX) /opt/CA/SC/CommonReporting/version.txt

   b. Verify that the CA Business Intelligence version is 2.1.13.

3. Verify that the database credentials are correct, as follows:

   a. Click Start, Programs, Microsoft SQL Server 2005, SQL Server Management Studio.

      The SQL Server 2005 login page appears.

   b. Type the username and password for the RDBMS administrative user that you created when you prepared the database for CA Access Control Enterprise Management.

   c. Click Connect.

      You are logged in to the SQL Server Management Studio. If you cannot log in, the database credentials are incorrect.

4. Verify that the *import_biar_config*.xml file has the correct values, as follows:
    a. Open the *import_biar_config*.xml file that you used to deploy the report package on the Report Portal.
    b. Verify that the values for the following properties correspond to the values that you specified in Step 3:
        - <username> is identical to the username that you entered.
        - <password> is identical to the password that you entered.
        - <datasource> is identical to the name of the database that you entered.
        - <server> is identical to the name of the Report Server computer.

Cannot View Reports in CA Business Intelligence with an Oracle Database

Symptom:

I use an Oracle database as my central database, and I cannot view reports in CA Business Intelligence. When I try to view a report, I receive the following error message:

```
Failed connect
```

Solution:

The following process helps you troubleshoot the problem with CA Business Intelligence:

1. Verify the BusinessObjects version number, as follows:
    a. Open the following URL:

        http://*hostname*:8080/businessobjects/enterprise115/adminlaunch/launchpad.html

        hostname

        Defines the name of the Report Portal host.

        The Central Management Console log on page appears.
    b. Enter your username and password, and click Log On.

        The Central Management Console appears.
    c. Click Servers, *hostname*, Web_IntelligenceReportServer, Metrics.

        The BusinessObjects version number is displayed.
    d. Verify that the BusinessObjects version number is either 11.5.8.1061 or higher, or 11.5.10.1263 or higher.

2. Verify the CA Business Intelligence version number, as follows:
   a. Open the following file on the Report Portal:
      - (Windows) C:\Program Files\CA\SC\CommonReporting\version.txt
      - (UNIX) /opt/CA/SC/CommonReporting/version.txt
   b. Verify that the CA Business Intelligence version is 2.1.13.
3. Verify that the Oracle system environment variables are defined as follows, where *Oracle_home* is the directory in which you installed Oracle:
   - ORACLE_HOME points to the *Oracle_home* directory
   - PATH contains the *Oracle_home*/bin directory
   - TNS_ADMIN points to the *Oracle_home*/network/admin directory
4. Verify that TNS is correctly defined, as follows:
   a. Open a command prompt window.
   b. Run the following command:

      ```
      tnsping TNSname
      ```

      TNSname

      Defines the name of the TNS.

      If you receive an error message, TNS is not correctly defined.
5. Verify that you use the correct credentials to access the database, as follows:
   a. Open a command prompt window.
   b. Run the following command:

      ```
      sqlplus user/password@TNSname
      ```

      user

      Defines the name of the RDBMS administrative user that you created when you prepared the database for CA Access Control Enterprise Management.

      password

      Defines the user password.

      If you cannot log on to the SQL Command Line, the database credentials are incorrect.

6. Verify that the *import_biar_config*.xml file has the correct values, as follows:

   a. Open the *import_biar_config*.xml file that you used to deploy the report package on the Report Portal.

   b. Verify that the values for the following properties are identical to the values that you specified in Step 5:

      - <username> is identical to *user*
      - <password> is identical to *password*
      - <datasource> is identical to *TNSname*

7. (UNIX) Run the commands in Step 4 and Step 5 as the user that you specified when you installed CA Business Intelligence.

   You specify this user in the CMS Database Settings page of the CA Business Intelligence installation wizard. This step verifies that the user has read and execute access to the entire *Oracle_home* directory.

Cannot View Reports in CA Access Control Enterprise Management

Symptom:

When I try to view a report in CA Access Control Enterprise Management, a Business Objects log on dialog appears and the Privacy Report icon appears in my browser.

Solution:

Your browser is blocking cookies from the Report Portal. To fix this problem, adjust the cookie settings in your browser to permit cookies from the Report Portal.

Note: The Privacy Report provides more information about the cookies that your browser blocks. To display the Privacy Report, double-click the Privacy Report icon.

Appendix A: Troubleshooting and Maintenance Procedures

This section contains the following topics:

How to Verify That CA Access Control Is Correctly Installed

Valid on Windows

You should verify that CA Access Control is correctly installed immediately after you install the product. The following process helps you verify that CA Access Control is correctly installed.

If you have installed CA Access Control successfully, you will notice the following changes:

- A new key is added to the Windows registry:

  ```
  HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl
  ```

  While CA Access Control is running, the CA Access Control keys and sub-keys are protected and you can modify the keys only through CA Access Control Endpoint Management or by using selang commands. However, you do not need to use CA Access Control Endpoint Management or selang commands to read the keys and values.

- When you restart your computer, several new CA Access Control services start automatically. These services include the Watchdog, Engine, and Agent, which are always installed. Other services, such as Task Delegation, exist depending on the options you chose during installation. The Display name for all CA Access Control services begins with "CA Access Control". You can check what services are installed, and verify that these services are running, using Windows Services Manager.

How to Troubleshoot Resource Access Problems

Incorrect access authorities are the most common cause of resource access problems. An example of a resource access problem is a root user that can still access a protected resource, but the protected resource has a default access authority of none. The following process helps you troubleshoot resource access problems:

1. Change the audit mode for the protected resource to audit all:

   ```
   chres CLASS ResourceName audit(all)
   ```

   Changing the audit mode to audit all makes the audit log easier to read.

2. Run a trace (see page 123) and recreate the problem.

3. Review the trace file and the audit log for occurrences of the protected resource. Try to troubleshoot the cause of the resource access problem from the information in the files.

   Note: SPECIALPGM objects provide bypasses that are not audited, but these bypasses appear in the trace file.

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

How to Troubleshoot Connection Problems

Many factors affect connections between CA Access Control computers. Connection problems include being unable to connect to a remote CA Access Control computer, or the connection to the remote computer timing out. The following process helps you identify the cause of the connection problem.

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

1. Check the CA Access Control computers for recent changes to the following:
   - Encryption key
   - Encryption method
   - TCP and UDP ports

2. Review any new or recently changed rules in the TCP, CONNECT, HOSTNET, or HOST classes.

3. Determine the port that has the connection problem.

4. Run a trace (see page 123) and review the trace file for:
   - Connections that CA Access Control blocked due to TCP rules or other rules
   - A code other than P (permitted) next to the port number that has the connection problem

5. Review the CA Access Control audit log for D (deny) records that refer to the problematic port.
6. Check that firewalls do not block the problematic port.
7. Review the log files for your OS for error messages that are caused by ports that cannot bind.

More information:

Change Port Number for CA Access Control Agent Communication (see page 127)

How to Troubleshoot Performance Problems

The following process helps you identify the cause of performance problems.

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

1. Identify when the performance problem occurs. Does performance degrade:
   - When the OS starts?
   - When CA Access Control starts?
   - When CA Access Control has been running for some time?
   - When CA Access Control or the OS run a scheduled process?
   - (UNIX) When the CA Access Control kernel extension is loaded?
   - When CA Access Control daemons or services are loaded?
2. If you have determined that CA Access Control causes the performance problem, investigate the following questions:
   - What processes are using the most resources when performance degrades?
   - Are the CA Access Control processes keeping the same process ID throughout their lifecycle?
   - Are there any third-party filter drivers installed on the computer?
   - Are there any system monitoring applications installed on the computer?

3. Check the CA Access Control database:

   a. Stop CA Access Control.

   b. Check the database:

      ```
      dbmgr -util -all
      ```

   c. Reindex the database (see page 125).

   d. Rebuild the database (see page 126).

   e. Restart CA Access Control and check if the problem still exists.

4. (Windows) Disable driver interception:

   a. Stop CA Access Control.

   b. Change the value of the UseFsiDrv registry entry to 0. The UseFsiDrv registry entry is in the following registry key:

      ```
      HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\AccessContro
      l
      ```

   c. Restart CA Access Control and check if the problem still exists.

5. Run a trace (see page 123) and recreate the problem. Review the trace file for the following:

   - Repeated events in a small period of time, for example, many file accesses in several seconds.
   - Processes that have been killed.
   - Either of the following values:
     - ACEEH = -1
     - U = a negative value

     These values may specify that CA Access Control cannot resolve a user name or assign a value to a resource.

Note: For more information about improving CA Access Control performance on your UNIX computer, see the *Endpoint Administration Guide for UNIX*.

Run a Trace

Running a trace can help you troubleshoot problems. CA Access Control writes trace records to the seos.trace file, which is located in the *ACInstallDir*/log directory.

To run a trace

1. Remove all records from the trace file:

   ```
   secons -tc
   ```

2. Start the trace:

   ```
   secons -t+
   ```

3. Recreate the problem.
4. Stop the trace:

   ```
   secons -t-
   ```

5. Review the trace file.

Note: The configuration settings in the seosd section configure the trace file. For more information about the seosd section, see the *Reference Guide*.

Run a Trace on CA Access Control Web Service Components

Valid on Windows

Running a trace on the CA Access Control web service components can help you troubleshoot problems. For example, if CA Access Control Enterprise Management cannot connect to the DMS, you can run a trace to review the messages that these two components exchange.

CA Access Control writes trace records for web service components to the file that is defined in the logFileName configuration setting in the WebService section. The default value for this configuration setting is C:\Program Files\CA\AccessControlServer\WebService\log\WebService.log.

To run a trace on CA Access Control web service components

1. Stop CA Access Control and the CA Access Control Web service.
2. Create a registry key in the following location:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\WebService\Trace
   Enabled
   ```

3. Set the value of the key to 1.
4. Start CA Access Control and the CA Access Control Web Service.

   Tracing starts on the CA Access Control web service components.

5. Recreate the problem.
6. Stop CA Access Control and the CA Access Control Web service.

   Tracing stops on the CA Access Control web service components.

7. Set the value of the key to 0.
8. Review the trace file.

Reindex the CA Access Control Database

Because many updates are made to the CA Access Control database, the database files may become fragmented. Reindexing and rebuilding the database (see page 126) helps ensure database optimization for speed and reliability. Reindex the database during your routine maintenance procedures every three to six months, and whenever you have a performance problem.

Note: In this procedure the CA Access Control database is installed in the default location, /opt/CA/AccessControl/seosdb (UNIX) and C:\Program Files\CA\AccessControl\Data\seosdb (Windows). To perform this procedure, you must log in as a root user (UNIX) or as an administrator (Windows).

To reindex the CA Access Control database

1. Stop CA Access Control.
2. Navigate to the following directory:
   - (UNIX) /opt/CA/AccessControl/seosdb
   - (Windows) C:\Program Files\CA\AccessControl\Data\seosdb
3. Back up the database:

   ```
   dbmgr -backup backup_directory
   ```

4. Index the database:

   ```
   dbmgr -util -build seos_cdf.dat
   dbmgr -util -build seos_odf.dat
   dbmgr -util -build seos_pdf.dat
   dbmgr -util -build seos_pvf.dat
   ```

Note: To further reduce the size of the database on UNIX computers, you can use the sepurgdb utility to delete references to undefined records from the database. For more information about the sepurgdb utility, see the *Reference Guide*.

Rebuild the CA Access Control Database

Because many updates are made to the CA Access Control database, the database files become fragmented. Reindexing (see page 125) and rebuilding the database helps ensure database optimization for speed and reliability. Rebuild the database during your routine maintenance procedures every three to six months.

Note: In this procedure the CA Access Control database is installed in the default location, /opt/CA/AccessControl/seosdb (UNIX) and C:\Program Files\CA\AccessControl\Data\seosdb (Windows). To perform this procedure, you must log in as a root user (UNIX) or as an administrator (Windows).

To rebuild the CA Access Control database

1. Stop CA Access Control.
2. Navigate to the following directory:
   - (UNIX) /opt/CA/AccessControl/seosdb
   - (Windows) C:\Program Files\CA\AccessControl\Data\seosdb
3. Back up the database:

   ```
   dbmgr -backup backup_directory
   ```
4. Export the existing rules and the user-related data from the database:

   ```
   dbmgr -export -l -f exported_filename
   dbmgr -migrate -r migrated_filename
   ```
5. Navigate to the following directory and create a directory in it named seosdb_new:
   - (UNIX) /opt/CA/AccessControl
   - (Windows) C:\Program Files\CA\AccessControl\Data
6. Create a database in the seosdb_new directory using the following command:

   ```
   dbmgr -create -cq
   ```
7. Copy the *exported_filename* and *migrated_filename* files to the seosdb_new directory.
8. Import into the new database the existing rules and user-related data that you exported from the old database:

   ```
   selang –l –d “absolute path for seosdb_new” –f exported_filename
   dbmgr -migrate -w migrated_filename
   ```

   Note: Selang does not use -d option. If you run the "selang -l -f exported_filename" command after stopping the CA Access Controlservice and move to seosdb_new directory, the exported rules are stored in $SEOSDIR/seosd.
9. Rename the seosdb directory to seosdb_old.
10. Rename the seosdb_new directory to seosdb.

11. Start CA Access Control.

Change Port Number for CA Access Control Agent Communication

CA Access Control client applications—such as selang, policydeploy, and devcalc—and the CA Access Control Agent communicate on port 8891. We do not recommend that you change this port. If you do need to change this port, use the following procedure.

To change the port number for CA Access Control Agent Communication

1. Open the following file in a text editor:
   - (UNIX) /etc/services
   - (Windows) %SystemRoot%\drivers\etc\services
2. Add the following file to the file:

   `seoslang2 *port-number*/ tcp`
3. Save and close the file.
4. Restart CA Access Control daemons or services.

Configure the Message Queue TCP Port

When you install CA Access Control Enterprise Management, by default you configure the Message Queue to work with the SSL port (7243). You can change this default behavior and configure the Message Queue to use the TCP port (7222).

To connect to the Message Queue TCP port

1. On the Enterprise Management Server, stop the Message Queue and JBoss server.
2. Open the file tibemsd.conf for editing. This file is located in:

   `C:\Program Files\CA\AccessControl\/MessageQueue/tibco/tibco/cfgmgmt/ems/data`
3. Locate the entry listen=, remove the value, then enter the value: tcp://7222.
4. Locate the entry authorization=, remove the value, then enter disabled.
5. Save and close the file.
6. Open the file factories.conf and locate the tag [SSLXAQueueConnectionFactory].
7. Locate the entry url=, remove the value, then enter tcp://7222.
8. Save and close the file.

9. Open the file tibco-jms-ds.xml for editing. The file is located in:

   JBoss_HOME/server/default/deploy/jms

10. Search for and replace all the values displaying the SSL port number (7243) with the TCP port number 7222.

11. Search for and replace all the entries displaying the value SSLXA with XA.

12. Comment (<!--) the following two entries:

```
com.tibco.tibjms.naming.security_protocol=ssl
com.tibco.tibjms.naming.ssl_enable_verify_host=false
```

13. Save and close the file.

14. Start the Message Queue and JBoss server.

Chapter 13: Information to Provide to CA Support

When you contact CA Support, they will ask you to provide information about any changes to the environment to help them diagnose the cause of the problem. For example, host and user name changes and changes to the operating system may affect CA Access Control. CA Support may also ask you to use the CA Access Control Support utility to provide additional diagnostic information.

CA Support will ask you to provide the following information:

- CA Access Control version
- Operating system name, version, architecture, and update level
- Details of any CA Access Control patches installed on the computer
- Number of CPUs

Note: For more information about the operating systems, versions, architectures, and update levels that CA Access Control supports, see the CA Access Control Compatibility Matrix that is available from the CA Access Control product page on CA Support.

CA Support may ask you the following questions:

- What is the impact of the problem?
- When did the problem first occur?
- Is the problem reproducible?
- Was anything added, removed, or changed in the environment before the problem occurred?
- Did you restart the computer before the problem occurred?

- How many times has the problem occurred?
- What happens on the system when the problem occurs? For example, does the problem occur when you execute a particular process or command?
- Does the problem occur consistently or randomly?
- Do any segmentation faults or access violations occur when you execute a CA Access Control command?
- Why do you think CA Access Control caused the problem?
- If the problem is an operating system problem, did you report the problem to the operating system vendor? If yes, can you provide a crash analysis from the operating system vendor?

Generate Diagnostic Information about a Windows Endpoint

The CA Access Control Support utility collects information about your CA Access Control installation to help CA Support diagnose the cause of problems. You specify the information that the CA Access Control Support utility collects in the ACSupport dialog.

You can collect the following system information:

- System information reports
- The event log

You can collect the following CA Access Control information:

- Common information about the CA Access Control version, home directory, and the status of CA Access Control services
- The CA Access Control registry
- Configuration files for auditing, tracing, and the coexistence utility
- Audit and trace logs, including the audit logs for local PMDBs or DMSs and instrumentation traces
- Authorization and cache statistics
- A list of the CA Access Control executable files and DLLs installed on the computer
- A snapshot of the CA Access Control database, including local PMDBs and DMSs

  Note: If you collect a copy of the CA Access Control database, the CA Access Control Support utility stops CA Access Control before it snapshots the database and restarts CA Access Control when the snapshot is complete.

To generate diagnostic information about a Windows endpoint

1. Navigate to the following directory, where *ACInstallDir* is the directory in which you installed CA Access Control:

   `ACInstallDir\bin`

2. Double-click ACSupport.exe.

   The ACSupport dialog opens.

3. Complete the dialog and click Proceed.

   The CA Access Control Support utility snapshots your installation and places the output in the *ACInstallDir*\ACSupport directory.

Generate Diagnostic Information about a UNIX Endpoint

The CA Access Control Support utility collects information about your CA Access Control installation to help CA Support diagnose the cause of problems. If you include the CA Access Control database in the snapshot, the CA Access Control Support utility stops CA Access Control before it snapshots the database and restarts CA Access Control when the snapshot is complete.

The CA Access Control Support utility always collects the following information about UNIX endpoints:

- seos.ini—The CA Access Control initialization file
- tmpetc—The files from the CA Access Control /etc directory, including the following:
  - audit.cfg—The audit filter file
  - auditroute.cfg—The audit route filter file
  - nfsdevs.init—A file that contains the NFS defaults for major device numbers for each operating system
  - osver—The operating system version
  - sereport.cfg—The sereport configuration file
  - serevu.cfg—The serevu configuration file
  - trcfilter.init—The trace filter file
- versions.txt—A file that contains versions of key CA Access Control binaries
- Some operating system files, for example, some variable files

If you specify that the CA Access Control Support utility collects information about the CA Access Control database, it collects the following information:

- seosdb—The CA Access Control database
- seosdb.tar—A compressed file of the CA Access Control database
- The lookaside databases for groups, hosts, services, and users

If you specify that the CA Access Control Support utility collects information about the CA Access Control logs, it collects the following information:

- tmplog—The CA Access Control log files
- log.tar—A compressed file of the CA Access Control log directory

To generate diagnostic information about a UNIX endpoint

1. Navigate to the following directory, where *ACInstallDir* is the directory in which you installed CA Access Control:

   ```
   ACInstallDir/lbin
   ```

2. Execute the following command:

   ```
   ./support.sh [-db] [-log] [-all] [-none]
   ```

   -db

   Collects information about seosdb, the CA Access Control database, but does not collect information about the audit logs.

   -log

   Collects information about the audit logs but does not collect information about seosdb.

   -all

   Collects information about both seosdb and the audit logs.

   -none

   Does not collect information about seosdb and the audit logs.

   Note: If you do not specify an option, the CA Access Control Support utility runs in interactive mode.

   The CA Access Control Support utility snapshots your installation and places the output in the *ACInstallDir* directory.