CA Access Control

Troubleshooting Guide

r12.5

Second Edition

Third-Party Notices

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

CA Product References

This document references the following CA products:

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

Documentation Conventions

The CA Access Control documentation uses the following conventions:

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

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

Format	Meaning
Italic	Information that you must supply
Between square brackets ([])	Optional operands
Between braces ({})	Set of mandatory operands

Format	Meaning
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.

Contact CA

Contact Technical Support

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

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

Provide Feedback

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

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

Documentation Changes

Second Edition

The second edition of the documentation was released to coincide with the GA announcement of r12.5.

The following topic was updated in this edition:

- Troubleshooting Policy Deployment (see page 43)—Updated topic with changes to the Restore option.

First Edition

The first edition of the documentation was released with r12.5. This deliverable was added to this release of the documentation.

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 Premium Edition.

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:

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 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.xml

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
   ```

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.

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.

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.

Note: The RemoveAC.exe utility is not included in the CA Access Control installation package. For assistance, contact Technical Support at http://ca.com/support.

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

Chapter 3: Creating Policies and Access Authorities

This section contains the following topics:

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 60).

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 75) 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 Technical 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.

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. This problem may occur when I:

- Create a new Active Directory user.
- Create or move a user to a container that is not specified in the user_container configuration setting.

  Note: The user_container configuration setting is located in the AD section of the uxauth.ini file.
- Create or move a user directly under the Active Directory domain, that is, the user is not in a container.

Solution:

Use the following procedure to troubleshoot the problem.

1. Verify that the user has a UID and a GID in Active Directory.
2. Verify that the user is not suspended.
3. Verify that UNAB is started on the endpoint:
   a. Open a command prompt window on the endpoint.
   b. Run the following command:

      ```
      ./uxauthd -status
      ```

      A message informs you of the current status of UNAB.
4. 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.

5. Stop the name or password caching daemon for your OS on the endpoint, as follows:

   a. Stop uxauthd, the UNAB daemon:

      ```
      ./uxauthd -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 uxauthd:

      ```
      ./uxauthd -start
      ```

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

Backup Operations on the CA Access Control Database Generate UTimes and Denied Records in the Audit Log

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/Access Control.

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/Access Control/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 77).

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 Technical 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 60).

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\AccessControl

   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 Technical 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 advanced policy management objects.

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

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

  Use this option when you manually reset an endpoint (re-install CA Access Control or the operating system) to redeploy all the policies that the DMS indicates are effective on that endpoint.

  Note: If the host has some policies already applied, the restore will fail because it does not reset the host status before executing.

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.

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.

Chapter 9: Tuning Performance

This section contains the following topics:

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 61).

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, change the proc_bypass configuration setting to 0 in the [SEOS_syscall] section of the seos.ini file.

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

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 75) 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 Technical 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 Technical 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 75) 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 78)

How to Troubleshoot Performance Problems

The following process helps you identify the cause of performance problems.

Note: For assistance, contact Technical 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 76).
   d. Rebuild the database (see page 77).
   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\AccessControl

   c. Restart CA Access Control and check if the problem still exists.
5. Run a trace (see page 75) 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*.

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 63)
   - Troubleshoot the Report Agent on a Windows computer (see page 67)
2. Troubleshoot the Distribution Server (see page 70).
3. Troubleshoot JBoss (see page 72).
4. Troubleshoot the Report Portal (see page 74).

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.

To troubleshoot the Report Agent on a UNIX computer

1. 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.

2. 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 7443. You should verify that the Distribution Server URL specifies the correct port number for the communication type.

   Default: none

   Example: tcp://130.119.176.145:7222. This URL configures the Report Agent to communicate with the Distribution Server at the IP address 130.119.176.145 on port 7222, using the TCP protocol.

3. 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.

4. Navigate to the following directory:

   ACSharedDir/lbin

5. Stop the Report Agent daemon:

   report_agent stop

6. Navigate to the following directory:

   ACSharedDir/bin

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

   reportagent -debug 0 -task 1 -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 1

   Specifies that the Report Agent collects and sends information about the CA Access Control database that 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. Navigate to the following directory:

   ACSharedDir/lbin

10. Restart the Report Agent daemon:

report_agent start

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.

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\communication

   Distribution_Server

   Defines the Distribution Server URL.

   Note: The default port for TCP communication is 7222 and the default port for SSL communication is 7443. You should verify that the Distribution Server URL specifies the correct port number for the communication type.

   Default: none

   Example: tcp://130.119.176.145:7222. This URL configures the Report Agent to communicate with the Distribution Server at the IP address 130.119.176.145 on port 7222, using the TCP protocol.

3. Verify that the CA Access Control Report Agent service is started.
4. Open a command prompt window and stop CA Access Control:

   ```
   secons -s
   ```

5. Disable the CA Access Control Report Agent service in Windows Services Manager.
6. Start CA Access Control:

   ```
   seosd -start
   ```

   CA Access Control starts but the Report Agent service is stopped.
7. Run the Report Agent in debug mode, using the following command:

   ```
   reportagent -debug 0 -task 1 -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 1

   Specifies that the Report Agent collects and sends information about the CA Access Control database that 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. Stop CA Access Control:

   ```
   secons -s
   ```

10. Start the CA Access Control Report Agent service in Windows Services Manager.

    Note: You must select Automatic startup type.
11. Start CA Access Control:

    ```
    seosd -start
    ```

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

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/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\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 the password is what you specified when you installed CA Access Control.
   You are connected to the local Tibco environment.
5. Enter the following command:
   show queues
   A list of the Tibco queues on the Distribution Server appears.
6. (UNIX) Open a command prompt window on an endpoint and navigate to the following directory:
   ACSharedDir/bin
   Note: By default, the *ACSharedDir* directory is located at /opt/CA/AccessControlShared.

7. (Windows) Do the following:
   a. Open a command prompt window on an endpoint and stop CA Access Control:

      ```
      secons -s
      ```

   b. Disable the CA Access Control Report Agent service in Windows Services Manager.
   c. Start CA Access Control:

      ```
      seosd -start
      ```

      CA Access Control starts but the Report Agent service is stopped.
8. Run the Report Agent on the endpoint:

   ```
   reportagent -debug 0 -task 1 -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.

   -task 1

   Specifies that the Report Agent collects and sends information about the CA Access Control database that is used to generate CA Access Control reports.

   -now

   Specifies to run the Report Agent now.
9. 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.
   - If the queue grows and shrinks, the Message Queue appears to be working as expected.

     You must troubleshoot the Report Portal.

     Note: The queue may grow and shrink very quickly.
   - If the queue does not grow, the snapshots that the Report Agent sent have not reached the Message Queue.

     You must troubleshoot the Report Agent.

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

10. (Windows) Do the following on the endpoint:
    a. Stop CA Access Control:

       secons -s

    b. Start the CA Access Control Report Agent service in Windows Services Manager.

       Note: You must select Automatic startup type.

    c. Start CA Access Control:

       seosd -start

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

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 reporting database.

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 test the connection to the CA Access Control Universe and deploy the report package, see the *Implementation Guide*.

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*.

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 77) 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 76) 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:

   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 -f *exported_filename*
   dbmgr -migrate -w *migrated_filename*
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.

Diagnostic Information

The CA Access Control Support utility collects information about your CA Access Control installation. The information that the utility collects helps Support to identify the cause of problems with your installation.

The CA Access Control Support utility is not included in the CA Access Control installation package. For assistance, contact Technical Support at http://ca.com/support.