CA Chorus™ for Security and Compliance Management

User Guide

Version 03.0.00, Fifth Edition

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time. This Documentation is proprietary information of CA and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA.

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

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

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

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

The manufacturer of this Documentation is CA.

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

Copyright © 2013 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Technologies Product References

This document references the following CA Technologies products:

- CA ACF2™ (CA ACF2)
- CA Chorus
- CA Chorus for Security and Compliance Management
- CA Chorus Software Manager™ (CA CSM)
- CA Datacom®/AD (CA Datacom/AD)
- CA Datacom Server (CA Datacom Server)
- CA Deliver™
- CA Distributed Security Integration for z/OS (CA DSI Server)
- CA LDAP Server for z/OS (CA LDAP Server)
- CA Scheduler JM®
- CA Top Secret® (CA Top Secret)
- CA View®
- CA Workload Automation CA 7 Edition

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 first edition of this documentation:

- Legal Notices (see page 2)—Updated to reflect public documentation legal disclaimer.

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

- Substantially reorganized and edited this guide to emphasize scenario-based content and functionality specific to CA Chorus for Security and Compliance Management.
- Sample CA Chorus for Security and Compliance Management Workspace (see page 17)—Added this mini-scenario, which describes how a first-time CA Chorus for Security and Compliance Management administrator might organize their workspace.
- Using CA Chorus for Security and Compliance Management to Troubleshoot a System Slowdown (see page 19)—Added this mini-scenario, which describes how a CA Chorus for Security and Compliance Management administrator can use CA Chorus to investigate and resolve a system slowdown.
- CA Chorus and ESM Field Name Comparison (see page 91)—Updated this table to include limits and format details for many fields.

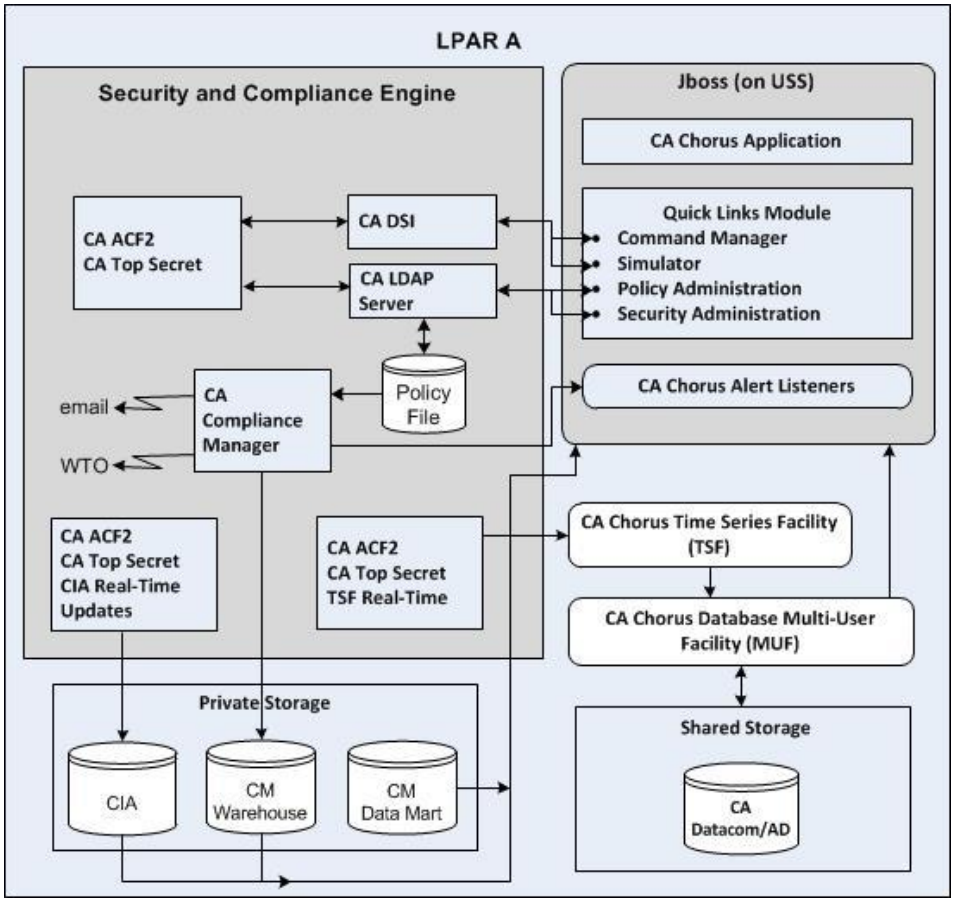
Contents

Chapter 1: Introduction

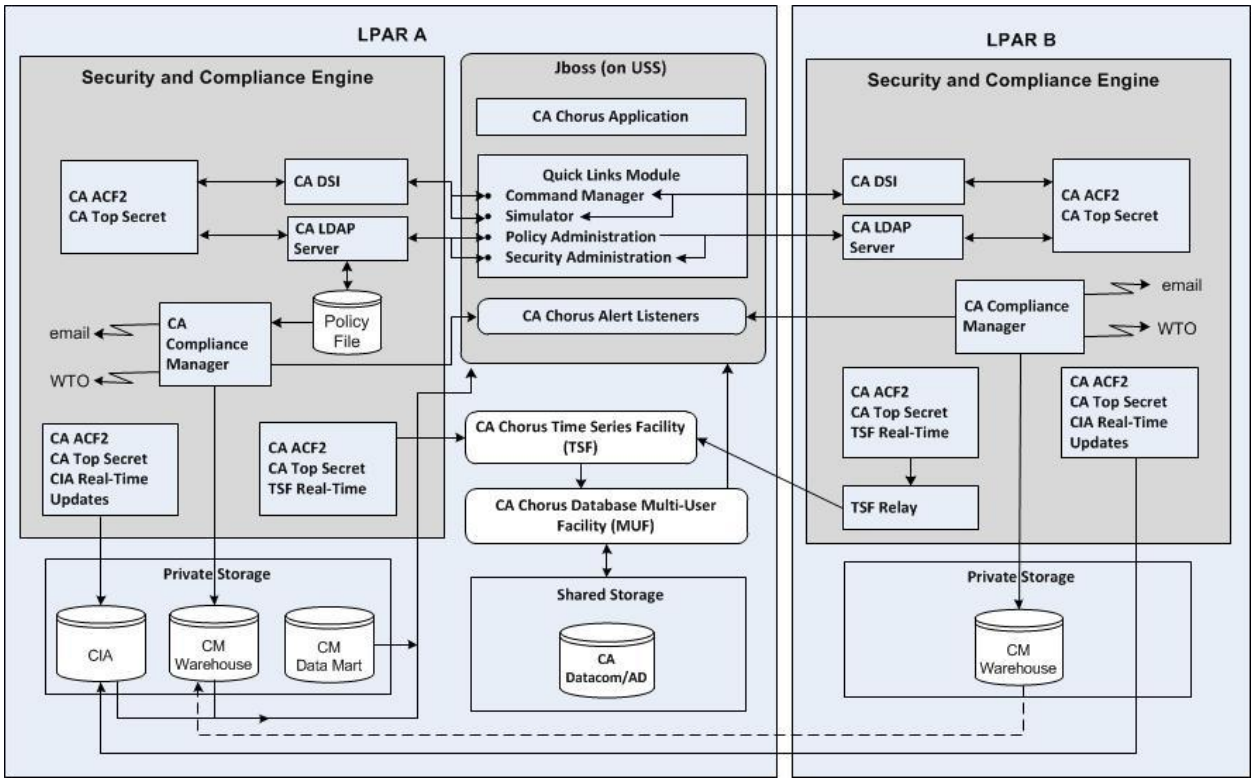
Architecture and Setup Overview

The following diagrams provide an overview of the CA Chorus for Security and Compliance Management discipline architecture. After installation and setup, use it to manage security resources across your z/OS enterprise.

- Single LPAR architecture:



- Multiple LPAR architecture:



Observe the following:

- In the single LPAR architecture it is common to have the security engine and CA Chorus Application Server in the same LPAR, but this setup is not required.
- The multiple LPAR architecture and setup diagram shows two LPARs. You can have more LPARs if needed.

To install and configure this discipline you must:

- Install and configure the security engine components on one or more selected LPARs.
- Install and configure a single CA Chorus instance to communicate with the security engines.

The diagrams illustrate the basic architecture:

LPARs

Identify logical partitions of a mainframe (z/OS system), on which you execute your External Security Manager (ESM) as a back-end engine for this discipline. Multiple LPARs are supported.

CA Chorus Application Server

Contains the CA Chorus system. Includes the following components:

CA Chorus Application

Provides the browser support and components to communicate with the back-end engines for the various disciplines, such as the security engine.

Quick Links Module

For this discipline this module includes the Administer Compliance Policy, Administer Security Definitions, and Simulate Access Attempt interfaces.

Security Command Manager Module

Issues native commands to backend security engines from the CA Chorus interface.

CA Chorus Listeners

Provides the service for receiving Alerts sent by the various backend security engines.

CA Chorus Time Series Facility (TSF)

Provides the facility for receiving, storing, and querying metrics about objects managed by the security backend engines. Because all metrics are date- and time-stamped, a series can be graphed over time to show trends, and to project into the future.

CA Chorus Database Multi-User Facility (MUF)

Provides the infrastructure for storing and retrieving TSF.

Security Engines

Composite of the ESM and compliance products that together provide the input to this discipline. Includes but is not limited to CA ACF2, CA Top Secret, Compliance Policy Administration interface, and CA LDAP Server for z/OS.

Shared Storage

Represents all storage devices that are shared across the CA Chorus disciplines.

Private Storage

Represents storage devices that are shared only across this discipline.

Terminology

The CA Chorus, Security Administration, and Compliance Administration interfaces can use different terminology for the same objects. Security Administration interface and Compliance Policy Administration interface use CA ACF2 and CA Top Secret terminology. These differences are reflected in the documentation. The following table maps commonly used objects between these products.

CA Chorus	Security Administration interface and Compliance Policy Administration for CA ACF2	Security Administration interface and Compliance Policy Administration for CA Top Secret
user ID	logon ID or logonid	user ACID
discipline	group profile record, UID strings used in rules	profile ACID

Example: Adding an ACID

You add a user ACID on the Security Administration interface on a CA Top Secret system. This ACID appears in CA Chorus as a user ID and can be viewed in the Investigator tree under: Security Definitions, Users.

Security Knowledge Center Best Practices

The Knowledge Center is the repository for all CA Chorus documentation. The Knowledge Center includes online help and guides from CA, user-generated documentation, and links to third-party content. Links to relevant topics appear in the Knowledge Center window when you click the online help icon or by searching. When you request online help, the search engine finds topics that are focused on the task you are performing. The engine also searches based on your location in the interface. This information appears in the Knowledge Center window and is updated whenever you refresh the window or click the online help icon.

We recommend that you add security-specific documentation to your Knowledge Center. For example, you could add the documentation that is associated with a specific release of IBM z/OS. This best practice helps ensure that your security administrators have accurate and current security information that is related to the z/OS operating system.

Note: For the steps to index content, see the *CA Chorus Product Guide*.

We recommend that you add the following content to your Knowledge Center:

- CA Customer Value Program reports. For more information, see http://ca.com/support.

- *IBM Introduction and Release Guide* for your supported z/OS versions.
- IBM z/OS glossaries.
- IBM RACF documentation set, if you are using it with this product.
- Security best practices for your site.

We also recommend that you configure your search settings so that only CA back-end product content specific to your role appears in Knowledge Center results. Implementing this recommendation can improve the relevance of search results. For the configuration steps, see the *CA Chorus Product Guide*.

CA Chorus for Security and Compliance Management Functionality

The following functionality is specific to the CA Chorus for Security and Compliance Management discipline. For information about other CA Chorus functionality, see the *Product Guide*.

- Monitor your systems for security events using the *Compliance Policy Administration* interface, including the following events:
  - Security events
  - Changes to security records
  - Changes to security configuration options
  - Changes to system data sets
  - Changes to z/OS configuration controls

  The Compliance Policy Administration interface helps you demonstrate regulatory compliance, mitigate the risk of negative security events, and reduce the total cost of compliance.
- The *Security Administration interface* lets you administer security using CA ACF2 or CA Top Secret. This interface includes many logically grouped native commands and fields, which simplify security administration.
  - For CA ACF2, use th is interface to manage logon IDs, data sets, resources, rule lines, and rules.
  - For CA Top Secret, use this interface to manage ACIDs, departments, divisions, groups, profiles, zones, resources, passwords, and options.

  Note: The Security Administration interface does not support digital certificates or compiled data profile records.

- The *Investigator module* lets you load, edit, and delete complete paths that you have followed while viewing and managing your systems. You can view data in chart and tabular views in the Investigator. For CA Chorus for Security and Compliance Management, use the Investigator module to monitor security definitions (such as systems, users, roles, scopes and rules), and security and compliance events (such as object accesses, account administration, policy administration, and others). The Investigator includes the following functionality:

  Topology Viewer

  Displays a pictorial view of your data. After you select data from an Investigator table, you can launch this tool.

  Time Series Facility

  Displays line charts of time-based performance data. After you select data from an Investigator table, you can launch the Time Series Facility (TSF).

  For more information about the Investigator, see the chapter "View Security Data in the Investigator."

Sample CA Chorus for Security and Compliance Management Workspace

CA Chorus for Security and Compliance Management offers a customizable workspace. You customize your workspace to better suit your role and site, adding dashboards for various tasks, and selecting modules to access different functionality.

The following list details key product touch-points with real-world examples that demonstrate why you would use each component for your discipline. CA Chorus offers an intuitive user interface; however, if you are unsure how to proceed see the Product Guide. Additionally, you can click the question mark icon from within a module for procedures and concept help topics.

Dashboard

A dashboard is a customizable area that contains modules necessary for your tasks and projects. You can create multiple dashboards, and add and remove a dashboard as needed.

For this sample, create three dashboards named **Search**, **Alerts**, and **Security Tools**.

Metrics Panel

The Metrics panel provides a visual display of key system metrics.

Add the following security metrics to the Metrics panel. These metrics provide an overview of your systems' stability and usage levels.

RACROUTE SIGNONs

Monitor the number of signons on each of your systems.

CPF Inbound Requests

Monitor the number of Command Propagation Facility commands.

RACROUTE FASTAUTHs

Monitor the number of access validation requests.

You also add the RACROUTE signons metric to your Alerts dashboard. Use the TextBox module to label this metric with information about the system.

Web Application Module

You want easy access to CA Technologies product news and documentation. To do so, add http://support.ca.com as a Web Application module to your Security Tools dashboard. This integrates this site with your dashboard.

Alerts Module

Add an Alerts module to your Alerts dashboard. Follow the wizard to configure this module to use your site's alerts policy, and to label the module.

Quick Links Module

As a security administrator, you want quick access to key tools. Add the Quick Links module to your Security Tools dashboard. The Quick Links module includes an Access Attempt Simulator, as well as the Security Administration interface. These tools are used to access and administer your external security manager (ESM).

Command Manager

Add the Command Manager module to your Security Tools dashboard so you have quick access to a command interface. Select a system and issue a command to display the status of your ESM. For CA Top Secret, issue TSS MODIFY STATUS. For CA ACF2, issue SHOW ACF2.

Investigator

The Investigator lets you access security definitions, performance statistics, and otherwise monitor your systems. Add the Investigator to your Search dashboard.

Your focus is user administration, so you customize your view for quick access to certain user information. Under Security, select Definitions, then select Users. Select a user from the list. When you do, a tabbed Details pane opens at the bottom of the field. Click the plus symbol to add a new tab, and rename the new tab to **User Administration** (to rename a tab, double-click its title).

You add six fields to this tab. To add a field, right-click in the new tab and select Insert Field. Add these three fields from the Basic Information section: Name, Suspended, and Last Used Date. Add these three fields from the TSO Information section: Account Number, Region Size, and Default Proc.

You have customized this data so you can quickly find key fields in one tab, more efficiently investigating and resolving requests and issues.

Knowledge Center

Configure the Knowledge Center to search only the data sources related to your discipline. Doing so improves the relevance of your search results.

Open the Knowledge Center and click Advanced Search. Under Show Results From, select MVS/Quick Ref, User Documentation, CA Chorus, and either CA ACF2 or CA Top Secret, as appropriate.

Dashboard Sharing

Now that you customized your dashboards, share them with your peers to help them start working quickly. Right-click the dashboard and follow the prompts.

Summary

This sample shows you one of the many ways you can customize your CA Chorus for Security and Compliance Management workspace. This customization can improve productivity and response time for customer issues. Use this sample as a starting point to explore how you can customize the workspace for your user- and site-specific needs.

Example: Troubleshoot a System Slowdown

As a security administrator, you are alerted to an issue. One of your production systems has been experiencing a serious slowdown since 2:00 a.m. last night, disrupting key applications. The following example shows how you can use CA Chorus to troubleshoot and resolve the situation.

Research the Situation in the Knowledge Center

The Knowledge Center contains CA Technologies documentation and much more. It also preserves expertise from other security administrators, by incorporating Notes and Investigator comments. You use the Knowledge Center to see if a colleague has written anything that can help you resolve this problem.

After searching the Knowledge Center for the system ID, you discover another administrator has written instructions to troubleshoot a similar issue. The saved note says to perform the following procedure:

1. Assess the System in the Metrics Panel

You add key metrics to the Metrics panel. Examining the sparklines, you discover a spike in RACROUTE VERIFY and RACROUTE VERIFYX counts, indicating an increase in signon attempts and signon violations. You add this metric to your Dashboard and examine the timeline in more detail. This research confirms that the spike began at 2:00 a.m.

2. Find the Culprit in the Investigator

Because your site policy is to record signon violations to a Warehouse repository, you are able to examine these violations in the Investigator. You see that the violations are coming from a variety of user IDs, many of which do not match your corporate naming standards. From this data point, you deduce that someone is attempting a denial of service attack.

3. Stop the Attack

You note the attacker's application name and TCP/IP addresses, then use your external security manager to block the offending jobname. You also modify your firewall rules to block the addresses that were used in the attack.

Returning to the Metrics Panel, you verify that RACROUTE VERIFY and RACROUTE VERIFYX counts have returned to normal. Using CA Chorus, you have stopped the attack. You contact the appropriate authorities and begin a more detailed investigation.

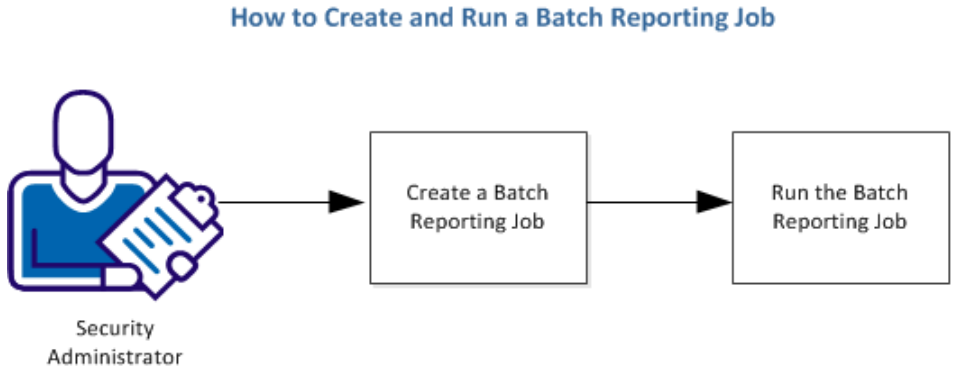
Chapter 2: Manage Data and Objects

How to Create and Run a Batch Reporting Job

As a security administrator, you are often asked to provide information to an auditor. For example, you can be asked to produce a quarterly report of user IDs that have been suspended due to excessive password violations.

The CA Chorus Investigator lets you search for these user IDs and save the search query to a JCL batch job. This batch job, when executed, generates a report. After you create the JCL, you can run the report every quarter. You can also add the batch job to a job scheduler so that it executes at predetermined intervals, providing automated, consistent, and updated reports for the auditors. This scenario explains how you create and run a batch reporting job.

The following illustration shows how a security administrator creates and runs a batch reporting job to list suspended IDs:



Complete the following tasks to create and run a batch reporting job to list suspended IDs:

1. Create a Batch Reporting Job (see page 22)
2. Run the Batch Reporting Job (see page 23)

Create a Batch Reporting Job

The Investigator helps you view and analyze information stored in discipline-specific data repositories by providing multiple work areas (panes) to help you manage your data.

In this example, you use the Investigator to create a list of suspended users, which auditors requested. You then save the search queries behind this list to a z/OS PDS member with the click of an icon. After you save them, the Investigator adds JCL statements to create a batch job that you can submit to generate a report.

Follow these steps:

1. Log in to CA Chorus with security discipline access.
2. Add the Investigator module to your workspace, and click Start New Investigation.
3. Select Security from the discipline drop-down list.
4. Select Definitions, Users.

   The list of users appears in the Investigator.
5. Click the View Filter icon, if the search panel is not loaded.
6. Specify **Suspended (password) =Y** as your filter criteria to identify the suspended users, and click Search.

   Note: Narrow your search by adding criteria.

   A list of users suspended for password violations appears in the Investigator.
7. (Optional) Customize the tabular view:

   a. Add or remove columns from the table by clicking the wrench icon in the Investigator toolbar and editing the All Selected Columns in Select and Reorder Columns dialog. In this example, the security administrator adds the Number of Password Violations column.

   b. Click Save.

   The column settings are saved for this view.
8. Save the search query as a JCL batch job:

   a. Click the Save search queries icon, and select Save JCL from the pop-up menu.

b. Enter the following information:

- (Optional) The name of the data set and member containing the JCL template to apply to the job. Enter this name when only more than one template is available. The default is *your_chorus_runtime*.CETJEZTR(EZTMPL01).
- The name of a data set and member name to save the JCL batch job to.
- A description of the batch job being saved (for example, "Quarterly Suspended ID Report").

c. Click Yes.

d. Click OK in response to the successful save message.

Note: You can also save the search query as an Investigator query by clicking the Save search queries icon and selecting Save Query. This feature saves you from creating the query each time that you want to view the information in the Investigator. Also, you can export the list of suspended users that currently appear in Investigator by clicking the Export icon.

The Investigator saves the batch job to the specified data set. This job consists of search queries and JCL statements. In our example, you now have a list of suspended users for the quarter.

Run the Batch Reporting Job

You can submit the batch reporting job manually, or you can automate the job submission using existing scheduling and output management products at your site. For example, your site may use CA Workload Automation CA 7 Edition or CA Scheduler JM® Job Management to schedule jobs, and CA View® or CA Deliver™ to manage output.

Follow these steps:

1. Open an ISPF session, and display the data set member containing the saved JCL job.
2. Edit the job according to the comments provided in the JCL, and then save the JCL.
3. Add the job to a scheduler, specifying how often to execute the job and where to direct the generated report output. Complete this step using your site-specific practices.

By using the Investigator, you created the batch job. By using ISPF, you edited the job and submitted it to a scheduler. You successfully provided updated and timely reports to the auditors, and you have automated the process for future audits.

Issue a Security Command

The Security Command Manager module supports all CA ACF2, CA Top Secret, and IBM RACF commands. This module works with the CA DSI Server to process the commands and display the results. You can connect to multiple security systems based on the configuration set by your systems programmer.

Note: For more information about security system access from this module, see the *CA Chorus for Security and Compliance Management Site Preparation Guide*.

Follow these steps:

1. Add the Security Command Manager module to your dashboard from the Module Library.

   The Security Command Manager module opens. The previously selected system appears in the System field. Your CA Chorus logged-in user name appears in the User Name field.

   Note: If there is not a previously-selected system, the first system in the System drop-down list is selected.

2. Select a system from the System drop-down list to connect to a different system.
3. Choose *one* of the following options:

   - If the user name for the selected system is the same as the logged-in user name, go to step 6.
   - If the user name for the selected system is different, go to step 4.

   Note: After you select a system, CA Chorus generates a PassTicket to authorize your connection. If the PassTicket authorization fails, enter your password to log in to the system.

4. Enter your user name.
5. (Optional) Enter the password for the selected system. The Password field appears in the following cases:

   - The PassTicket generation fails.
   - The user name that you enter is different from the logged-in user name.
   - If the application ID is not set while configuring the security systems. The application ID is used to generate a PassTicket for a logged-in user.

   Note: For more information about the application ID and identifying systems for the Security Command Manager module, see the *CA Chorus for Security and Compliance Management Site Preparation Guide.*

6. Do *one* of the following:
   - To enter a single command, enter the security command in the input text area.
   - To enter multiple commands at a time, enter each command on a separate line in the input text area.
   - To import security commands from a .txt file or a .sql file, click the Import icon on the toolbar. Browse to select a file, click Import and Submit.

     Note: The Security Command Manager validates the selected file. The file must be a .txt file (UTF-8 or ASCII) or .sql file, less than 100 KB. Binary files are not supported.
7. Click Submit.

   The Command Results area shows the output. The module appends the output for each additional command at the bottom of the results of the previous command.

   Note: You can export security commands output to a text file. Click the Export icon on the toolbar, enter a file name, and click save. If you are using Mozilla Firefox, the file is saved as "chorusdata.txt".
8. Click Clear Input or Clear Output to clear command data area.

Note: If you are unable to access a security system, contact your systems programmer. For command syntax details, see the *CA ACF2 Administration Guide, CA Top Secret Command Functions Guide, CA Top Secret Control Options Guide*, or IBM documentation.

View Security Object Relationships in the Topology Viewer

Use the Topology Viewer in the Investigator to generate pictorial views of the following security data:

- Security definitions
- Security and compliance events

The Topology Viewer provides a pictorial representation of data in your system. This view makes it easier to identify relationships as you manage your data. Viewing data pictorially is useful when modifying users, roles, and rules because you can clearly see the relationships, dependencies, and impact of your changes.

Example: Compare Roles

You want to compare the roles of existing users of the same group to decide which roles the new user needs.

Follow these steps:

1. Add the Investigator module to your dashboard.
2. Click Start New Investigation, and select the Security role from the drop-down list in the Investigator.
3. Select Definitions, Users from the discipline drop-down list.

   The Search Users view appears.
4. Click View Filter (the magnifying glass icon) and filter users, for example by their User ID. Click Search.

   The filtered list of users is displayed.
5. Select the users that you want to compare. Click Navigation, Add to Topology Viewer in the Actions pane.

   Note: If the Actions pane is hidden, click the double arrow in the right column to show it.

   The Topology Viewer opens and displays a pictorial object for each selected user.
6. Right-click an object and click Show Child Objects From Roles.

   A group object appears under the parent object. The group object indicates the number of child elements that satisfy this relationship. In this example, it shows how many roles this user has.
7. Right-click the group object and click Expand.

   The relationships between the roles for each user are displayed.
8. (Optional) Click Save Path to save this view for later use.

You can now compare a subset of users by role:

- Right-click objects to Expand, Collapse, or Remove nodes.
- Click the toolbar icons to switch between a symmetrical or hierarchical view of the relationships.
- Click View in Grid to return to the table view of the filtered results.

More information:

Security Definitions (see page 61)
Security Events (see page 71)

Chapter 3: Viewing Security Object Performance Data in the Investigator

Security Performance Data

CA Chorus for Security and Compliance Management lets you view, monitor, and compare the following security statistics in the Investigator, Metrics Panel, and Time Series Facility:

- Sysplex statistics
- Cache statistics
- Command Propagation Facility (CPF) statistics
- Command statistics (CA Top Secret only)
- Workload statistics (CA Top Secret only)
- I/O statistics (CA Top Secret only)
- RACROUTE request statistics
- SECCACHE facility statistics (CA Top Secret only)

Note: For a list of the fields that appear in each category, see the Details pane in the Investigator. Additionally, see the *CA ACF2 Reports and Utilities Guide* and the *CA Top Secret Report and Tracking Guide*.

View Security Statistics in the Investigator

Reviewing performance statistics for your security data can help you identify trends and set thresholds for acceptable performance.

Note the following prerequisites for viewing security statistics data:

- **CA ACF2** - To view CA ACF2 metrics in CA Chorus, the STATG bit in the GSO record must be turned on and statistics must be enabled with the Start command.

  Note: The Time Series Facility must be active in order for records to appear in the metrics panel.

- **CA Top Secret** - To view CA Top Secret metrics in CA Chorus, the CHORUSSTATG(ON) control option must be set. To automatically activate the CHORUSSTATG option during CA Top Secret initialization set the option in the parameter file.

After configuring your ESM, you must wait for the time interval setting before data displays in the metrics panel. Metrics display only when actions are occurring.

Note: For more information about how to configure your ESM to provide security performance data to the Time Series Facility, see the *CA Chorus for Security and Compliance Management Site Prep Guide*.

Example: Monitor SECCACHE improvements

Your team is about to enable the SECCACHE feature, which is a CA best practice. This option helps to reduce CPU cycles in the user and security address spaces that are required to complete subsequent system entry requests. This option also helps to reduce I/O against the security file when the file is shared between the systems. The best way to see the benefits of SECCACHE is by monitoring I/O statistics. This option helps to reduce CPU cycles that are required to complete subsequent system entry requests in the user and security address spaces.

Follow these steps:

1. Add the Investigator to your dashboard. Launch the Investigator by clicking Start New Investigator.
2. Select Security from the drop-down list, then select Statistics from the folder list. Select the system you want to view, and select Statistics Reporting.
3. Select your system from the table in the center pane.

   The Details pane appears with your data.
4. Perform *one* of the following sequences:
   - To review all of the data in a tabular view:
     a. Select the wrench icon.

b. Add all of the IO fields to the grid, and click Save.

c. The IO statistics appear in the table in the center pane.

d. Click the export icon in the upper-right corner of the center pane.

e. Save the table data to a comma-separated value (CSV) file.

- To review the data using the Time Series Facility (TSF):

  a. Click Add Entity to Time Series.

  b. Select the IO statistics to compare in the TSF, and click Perform Charting.

  c. Click the icon next to the Contributors button to duplicate the chart.

  d. Set the charts so one shows data before SECCACHE was enabled and one after.

After you enable the SECCACHE feature in your back-end security product and let it run for a week, repeat these steps and compare the data in TSF graphs or CSV files. The IO statistics should be lower than when SECCACHE was off.

View Security Object Performance Data in the Time Series Facility

The *Time Series Facility* (TSF) stores data that is collected and provided by CA products. TSF provides a single point for collection, storage, management, and organization of the product data. When you request a Time Series chart from the Investigator, TSF provides the data content for the chart.

Note: For detailed common TSF concepts and procedures, see the *CA Chorus Product Guide*.

For CA Chorus for Security and Compliance Management, use TSF to display and review security statistics. For example, you can add a security system to the TSF and then analyze the cache calls received contributors. By monitoring the ratio between cache calls and cache hits, you can evaluate the performance boost compared to running the same load without the cache feature enabled.

When you add a security object to TSF, it becomes an entity. You can use this entity to create a chart. Doing so lets you determine trends and identify valid anomalies. The TSF charts allow up to four lines.

Follow these steps:

1. Add the Investigator to your dashboard and click Start New Investigation.
2. Select Security from the drop-down list.
3. Select Statistics from the folder list.

4. Select your system.
5. Select Statistics Reporting
6. Highlight a row of statistics and click Add Entity to Time Series in the Actions Pane.

   You can now review these statistics in TSF.

Chapter 4: Manage Users

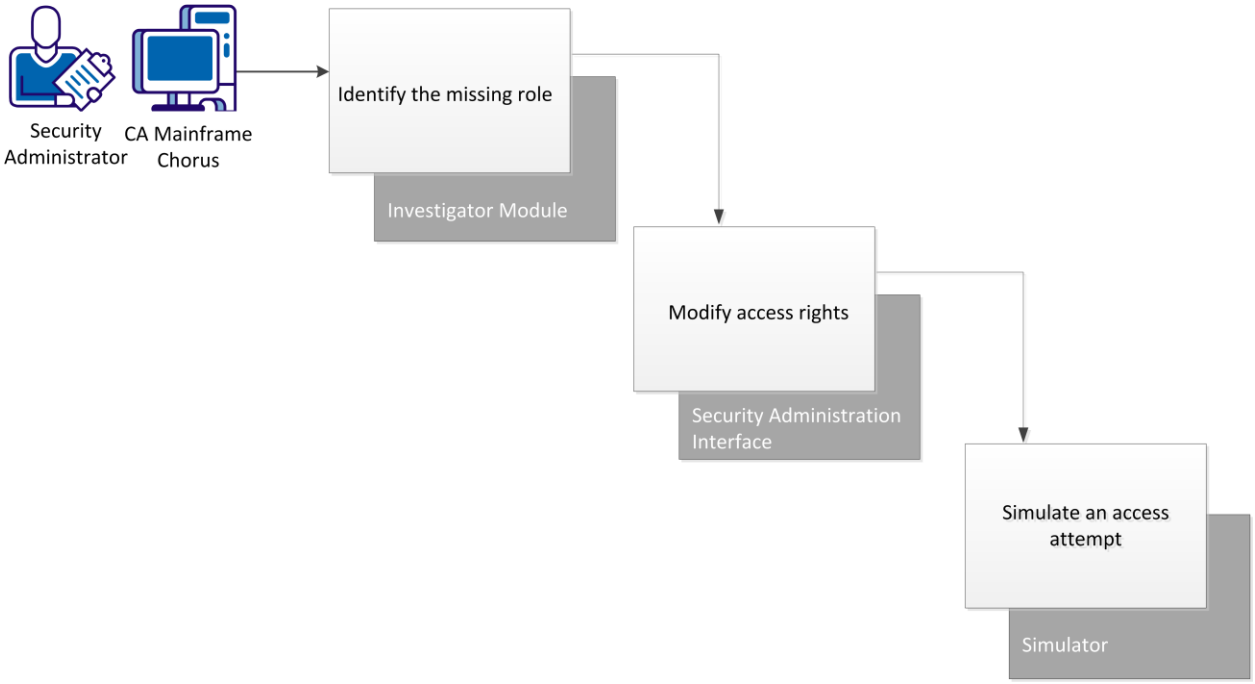
How to Identify and Correct an Access Rights Problem

As a security administrator, modifying access rights for resources within your scope is a task that you regularly perform. This task is important because it:

- Ensures that users have appropriate access to resources.
- Enables users to access the appropriate resources quickly and remain productive.

This example describes how you can use CA Chorus and CA Top Secret to identify and correct an access rights problem, and then verify that you have corrected the problem.

Identify and Correct an Access Rights Problem



In this example, you have just received a service desk ticket with the following information:

- An employee does not have proper access rights to information that is critical for the job.
- The employee has opened a helpdesk ticket to correct the problem.

- The manager confirms that you should give access to the employee.
- The employee has provided the name of a colleague who already has access to this information.

Your research indicates that the employee needs read access to a particular data set.

Perform these tasks to identify and correct the access problem:

1. Identify the missing role (see page 32).
2. Modify access rights (see page 33).
3. Verify the New Access (see page 34).

Identify the Missing Role

Use the Investigator to compare two users to identify which role a user requires to access a particular resource.

In CA Chorus a *role* is a collection of rules that define permissions for access to resources. Adding rules in groups helps you to administer security more efficiently and accurately.

Follow these steps:

1. Add the Investigator module to your dashboard.
2. Click Start New Investigation, and select the Security role from the drop-down list in the Investigator.
3. Select Definitions, Users from the discipline drop-down list.

   The Search Users view appears.
4. Click View Filter (the magnifying glass icon) and filter users, for example by their User ID. Click Search.

   The filtered list of users is displayed.
5. Select the users that you want to compare. Click Navigation, Add to Topology Viewer in the Actions pane.

   Note: If the Actions pane is hidden, click the double arrow in the right column to show it.

   The Topology Viewer opens and displays a pictorial object for each selected user.
6. Right-click an object and click Show Child Objects From Roles.

   A group object appears under the parent object. The group object indicates the number of child elements that satisfy this relationship. In this example, it shows how many roles this user has.

7. Right-click the group object and click Expand.

   The relationships between the roles for each user are displayed.

8. Drill down into any unshared roles by clicking the role icon and selecting Show Child Objects From, Rules for User.

   Rules for that role appear in the bottom pane.

9. Examine the rules until you find the rule that grants access to the resource you are looking for.

   You have identified the access problem.

Modify the Access Rights

Add a profile to a user ACID using the Security Administration Interface. Adding a profile to an ACID adds all the rules contained in the profile to the ACID.

Follow these steps:

1. Add the Quick Links module to your dashboard and click Administer Security Definitions.

   The main Security Administration window opens.

2. Click the applicable Security Administration instance from the Administration pane.

   One of the following occurs:

   - If your CA Chorus credentials are also valid on this instance, Security Administration opens. The Logged In As field displays your user name, and the Administration pane expands to show you your options.
   - If your CA Chorus credentials are not valid on this instance, the Log In page for that Security Administration instance appears. Enter your user ID and password.

   You are logged in to the selected system.

3. Select ACIDs, Modify an Acid on the Administration pane.
4. Enter the user ACID to add the profile to in the ACID field and click Search.
5. Select the ACID.
6. Click the Profile/Group List subheading.
7. Enter the profile name to add in the Profile/Group Name field.
8. Enter the appropriate information in the remaining fields.
9. Click Modify.

   The profile is added to the user ACID. You have corrected the access rights problem.

Verify the New Access

Use the Simulator to test the access of a user to a data set. Simulating access verifies that a user ID has the appropriate access rights to a resource.

Follow these steps:

1. Add the Quick Links module to your dashboard and click Simulate Access Attempt.
2. Select the correct system from the System drop-down list.
3. Choose *one* of the following options:
   - If the user name for the selected system is the same as the logged-in user name, go to step 6.
   - If the user name for the selected system is different, go to step 4.

   Note: After you select a system, CA Chorus generates a PassTicket to authorize your connection. If the PassTicket authorization fails, you can enter your password to access the system.
4. Enter your user name.
5. Enter the password for the selected system. The Password field appears in the following cases:
   - The PassTicket generation fails.
   - The user name that you enter is different from the logged-in user name.
   - If the application ID is not set while configuring the security systems. The application ID is used to generate a PassTicket for a logged-in user
6. Enter the appropriate information in the remaining fields and click Simulate.
7. Review the simulation results to verify that the user now has appropriate access to the data set.

You have corrected the access rights problem. You identified the missing role using the Investigator, modified the ACID using the Security Administration interface, then verified access using the Simulate Access Attempt quick link.

How to Remove a User

As a security administrator, when an employee leaves your company, you must ensure that the user can no longer access your systems. Remove unused user IDs to keep your company resources secure.

In CA Chorus, a backend external security manager (ESM) controls user access rights. The ESM can be CA Top Secret® for z/OS (CA Top Secret) or CA ACF2™ for z/OS (CA ACF2). Use CA Chorus for Security and Compliance Management to manage users on CA Chorus.

You can remove a user in two ways:

Suspend the user

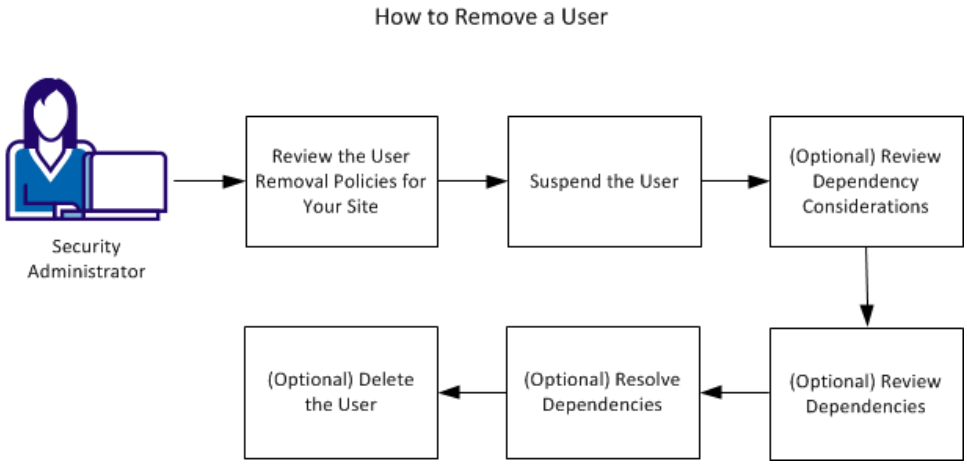
Deactivate but do not delete the user ID from the ESM.

Delete the user

Delete the user ID and all related entitlements from the ESM.

As a best practice, we recommend that you first suspend the user and later optionally delete the user.

Important! Review your site removal policies before you delete a user. Improper deletion can result in security or legal issues.



To remove a user:

1. Review the User Removal Policies for Your Site (see page 36).
2. Suspend the User (see page 37).
3. (Optional) Review Dependency Considerations (see page 38) in one of the following ways:
   - Review Dependencies (CA ACF2)
   - Review Dependencies (CA Top Secret)
4. (Optional) Review Dependencies (see page 39).
5. (Optional) Resolve Dependencies (see page 40).
6. (Optional) Delete the User (see page 41).

Prerequisites

The following access and privileges are required to remove a user:

- Access to the CA Chorus Security and Compliance Management discipline
- In CA ACF2, security administrators must have the ACCOUNT or SECURITY privilege to delete logonids.
- In CA Top Secret:
  - To delete ACIDs, security administrators must have ACID(CREATE|ALL) authority for ACIDs within their scope.
  - To suspend ACIDs, security administrators must have MISC1(SUSPEND) authority. Security administrators who do not have MISC1(SUSPEND) authority can still suspend ACIDs within their scope. To do so, they must have UPDATE access to entity TSSCMD.USER.ADDTO.SUSPEND in the CASECAUT resource class.

Review User Removal Policies for Your Site

Before you suspend a user, review your site policies for user removal.

Improper removal of a user can result in legal or security issues. We recommend that you suspend a user and later optionally delete the user. This recommendation offers the following benefits:

- Helps ensure security continuity
- Enables easier restoration if user definition changes are incorrectly made, or if a user is inappropriately deleted

Note: We assume that your site user removal policy includes the recommendations of auditors and applicable government and industry requirements.

Examples

- Your company terminates an employee due to misconduct. Because your company may need the security definitions and entitlements of this employee for legal purposes, preserve this information by suspending, not deleting, the user.
- A new employee joins your company. You inadvertently assign this employee a user ID that was previously used by a former employee, and then deleted. After several weeks, you are unsure which of these two employees created some of its logging records. Confusion now exists for other forensic records, access entitlement verification, reuse of entitlements and other controls, and possibly other areas that you have not yet identified.

Suspend a User

Suspend a user ID to deactivate but not delete the user ID from an ESM. Suspension preserves the user security definitions and entitlements for future reference. Before you suspend a user, review your site policies for user removal (see page 36).

Follow these steps:

1. Log in to CA Chorus.
2. Add the Security Command Manager module to your dashboard from the Module Library.

   The Security Command Manager module opens. The previously selected system appears in the System field. Your CA Chorus logged-in user name appears in the User Name field.

   Note: If a previously selected system is not present, the first system in the System drop-down list is selected.
3. (Optional) Select a system from the System drop-down list to connect to a different system.
4. Choose *one* of the following options:

   - If the user name for the selected system is the same as the logged-in user name, go to step 6.
   - If the user name for the selected system is different, go to step 4.

   Note: After you select a system, CA Chorus generates a PassTicket to authorize your connection. If the PassTicket authorization fails, enter your password to log in to the system.
5. Enter your user name.
6. (Optional) Enter the password for the selected system. The Password field appears in the following cases:

   - The PassTicket generation fails.
   - The user name that you enter is different from the logged-in user name.
   - If the application ID is not set while configuring the security systems. The application ID is used to generate a PassTicket for a logged-in user.

   Note: For more information about the application ID and identifying systems for the Security Command Manager module, see the *CA Chorus for Security and Compliance Management Site Preparation Guide.*

7. Enter one of the following commands, and click Submit:

   Note: If you are unable to access a security system, contact your systems programmer.

   For CA ACF2:

   `CHANGE logonid SUSPEND`

   For CA Top Secret:

   `TSS ADDTO(acid_name) SUSPEND`

   The Command Results area shows the output.

You have removed the user. The user no longer has access to your system. If you are suspending a user, this scenario is done. If you want to delete the user, go to the next topic.

(Optional) Review Dependency Considerations

Before you delete a user, review dependencies to help ensure that you can delete the user without negatively impacting your system. Do one of the following:

- Review Dependencies (CA ACF2) (see page 38)
- Review Dependencies (CA Top Secret) (see page 39)

(Optional) Review Dependency Considerations (CA ACF2)

To help ensure continuity of security, consider the following points before deleting the user:

- When you delete a logonid, CA ACF2 also deletes the associated User Profile records. Consider the impact of deletion, especially if the logonid is used for production batch jobs, started tasks, or other types of production workloads.

  For example, deleting a logonid deletes all CERTDATA records and KEYRING records associated with that logonid. Deletion can affect processes that use these records (for example, CICS, WebSphere application servers, and others). These transaction processing platforms can use digital certificates and keyrings to support the encryption of IP data flows and user authentication. If necessary CERTDATA and KEYRING definitions are improperly deleted, significant workload disruptions can occur.

- When you delete a logonid, CA ACF2 does not remove specific mention of the explicit logonid in data set access rules, generalized resource rules, or DB2 resource rules. Manually delete these rule lines, or run the CA ACF2 Rule Cleanup Utility (ACFRULCU) to remove them. For information about this utility, see the *CA ACF2 Reports and Utilities Guide*.

- When you delete a logonid, CA ACF2 does not remove specific mention of that logonid in other CA ACF2 records, such as Entry records (for example, scope records), Structured records (for example, GSO, CACHE, DCO records), Cross Reference records, and other record types.
- Physical system resources such as data sets, z/OS UNIX files, directories, or others can belong to the logonid. To determine if you must also delete these resources, review your site policies.
- A logonid can logically own resources (that is, it can have complete or shared administrative authority for a resource or set of resources). Review logical ownership to determine if you must appoint new logical owners to ensure administrative continuity.

(Optional) Review Dependency Considerations (CA Top Secret)

To help ensure continuity of security, consider the following points before deleting the user:

- Physical system resources such as data sets, z/OS UNIX files, directories, or others can belong to the user. Review your site policies to determine if you must also delete these resources.
- Transaction processing platforms can use digital certificates and keyrings to support the encryption of IP data flows and user authentication. When you delete an ACID, CA Top Secret also deletes keyrings or digital certificates that the ACID owns. If the DIGICERT and KEYRING definitions are improperly deleted, significant workload disruptions can occur.
- When you delete an ACID, CA Top Secret also deletes keyrings or digital certificates that the ACID owns. Production batch jobs, started tasks for purposes of enabling secure communications, or certificate-based user authentication can use these resources. Deletion can cause significant workload disruptions.
- You must also resolve dependencies if the ACID:
  - Owns resources
  - Is permitted to other ACIDs
  - Is a divisional, departmental, or profile ACID that has other ACIDs linked to it

(Optional) Review Dependencies

Use the Topology Viewer to review dependencies that you identified before you delete a user.

Follow these steps:

1. Add the Investigator module to your dashboard, and click Start New Investigation.
2. Select Security from the drop-down list.

3. Select Definitions, Users.

   The list of users appears in the Investigator.

4. (Optional) Click the View Filter icon, if the search panel is not loaded.

5. Specify your filter criteria so that you identify the user that you want to remove, and click Search.

6. Highlight the row that includes the applicable user information.

   The Actions pane opens. Detailed information about the selected user appears in the Details pane at the bottom of the Investigator.

7. Select Add to Topology Viewer from the Actions pane.

8. Right-click a node to drill into its dependencies. Explore all relevant dependencies.

   You have identified dependencies to resolve before you delete the user ID.

(Optional) Resolve Dependencies

Use the Security Command Manager to resolve any dependencies that you identified before deleting a user ID. Resolve dependencies to help ensure continuity of security after you delete the user.

Follow these steps:

1. Add the Security Command Manager module to your dashboard from the Module Library and select the appropriate system.

   The Security Command Manager module opens. The previously selected system appears in the System field. Your CA Chorus user name appears in the User Name field.

   Note: If there is no previously selected system, the first system in the System drop-down list is selected.

2. Do *one* of the following:

   - To enter a single command, enter the security command in the input text area.
   - To enter multiple commands at a time, enter each command on a separate line in the input text area.

   Note: For command syntax details, see the CA ACF2 *Administration Guide, CA Top Secret Command Functions Guide,* or *CA Top Secret Control Options Guide*. For information about managing digital certificates, see the *CA Top Secret Cookbook* or *CA ACF2 Cookbook.*

The Command Results area shows the output. The module appends the output for each additional command to the results of the previous command.

You have resolved dependencies and can now delete the user.

Example: Resolve Dependencies

This example transfers dataset sys.01 from existing CA Top Secret ACID to ACID testdep1.

```
TSS ADDTO(testdep1) DSN(sys.01) UNDERCUT
```

This example moves ACID divtest1 to zone zonetst1.

```
TSS MOVE(divtest1) ZONE(zonetst1)
```

This example moves ACID testdep1 to division divtest2.

```
TSS MOVE(testdep1) DIV(divtest2)
```

(Optional) Delete a User

You can delete the suspended user to remove the user ID permanently. Delete the user only if you are sure that deletion does not compromise the security or integrity of your system.

Before you delete a user, consider the following:

- Verify that the user ID has been suspended long enough to accommodate infrequently run workloads, such as jobs that are run quarterly, biannually, or annually.
- CA ACF2 and CA Top Secret permit logical synchronization of user ID definitions. These definitions reside in security databases residing on remote systems using the Command Propagation Facility (CPF). Review your site policies to determine if you must also delete the user ID on remote mainframe systems.
- CA ACF2 and CA Top Secret allow controlled sharing of update information to one or more remote LDAP directories using the LDAP Directory Services (LDS) feature. Review your site policies to determine if you must also delete the user ID on remote user directories.
- CA LDAP Server may share database updates with remote systems.

Important! Deletion of a user is not reversible. Delete a user only if you want to delete that user from the database permanently.

Note: For CA ACF2, administrators must have ACCOUNT and SECURITY privileges to delete logonids. For CA Top Secret, administrators must have ACID(CREATE|ALL) authority for ACIDs within their scope to delete ACIDs.

Follow these steps:

1. Add the Investigator module to your dashboard, and click Start New Investigation.
2. Select Security from the drop-down list.
3. Select Definitions, Users.

   The list of users appears in the Investigator.
4. (Optional) Click the View Filter icon, if the search panel is not loaded.
5. Specify filter criteria to identify the user that you want to delete, and click Search.
6. Highlight the row that includes the user that you want to delete.
7. Highlight the row that includes the applicable user information.

   The Actions pane opens. Detailed information about the selected user appears in the Details pane at the bottom of the Investigator.
8. Click Delete User on the Actions pane. Click yes to confirm deletion.

You have suspended the user, reviewed and resolved dependencies to help ensure continuity of security, and permanently deleted the user from the ESM and CA Chorus.

Modify a User

As a security administrator, you frequently modify data for users within your scope. Use the CA Chorus Investigator to quickly modify user data by typing over existing values.

Note: You can also modify users on the Security Administration interface or by executing commands on the Security Command Manager module.

Follow these steps:

1. Log in to CA Chorus.
2. Add the Investigator module to your dashboard, and click Start New Investigation.
3. Select Security from the drop-down list.
4. Select Definitions, Users.

   The list of users appears in the Investigator.
5. Specify filter criteria to identify the user that you want to modify, and click Search.

6. Highlight the row that includes the applicable user information.

   The Actions pane opens. Detailed information about the selected user appears on the Details pane at the bottom of the Investigator.

7. Click the pencil icon on the Details pane.

   You can edit the fields in the Details pane.

8. Click a field to edit it.

   Fields are grouped logically on tabs. For information about a field, hover over it.

9. Click Save.

   CA Chorus saves your changes to the ESM. You have modified the user.

CA ACF2 Examples:

- To change a user name, enter the new value in the Name field on the Basic User Information tab.
- To change a user telephone number, enter the new number on the ACF2 Information tab.
- To add ACCOUNT privileges to a user, enter Y in the Account field on the ACF2 Information tab.
- To add SECURITY privileges to a user, enter Y in the Security field on the ACF2 Information tab.

CA Top Secret Examples:

- To change a user name, enter the new value in the Name field on the Basic User Information tab.
- To change a user telephone number, enter the new number on the TSS Information tab.
- To suspend a user, enter Y in the Suspended (password): field on the Top Secret Information tab.
- To add MAIL privileges to a user, enter Y in the Mail field on the TSO Information tab.

Simulate an Access Attempt

Use the Simulator to test the access of a subject (such as a user) to a system resource (such as a data set). Simulating access helps ensure that subjects have the correct permissions and decreases unnecessary violations and loggings. For field name definitions, see *CA ACF2 Administration Guide*, *CA Top Secret Command Functions Guide*, or IBM documentation.

Note: You can simulate access attempts only on CA ACF2 and CA Top Secret systems. RACF systems are not available on the Simulator.

Follow these steps:

1. Click Simulate Access Attempt from one of the following locations:
   - The Quick Links module
   - The Investigator tree, Users, Roles, or Rules in the Security Definitions category, the Actions pane

   The Simulate Access Attempt window appears.
2. Select a system from the System drop-down list.
3. Choose *one* of the following options:
   - If the user name for the selected system is the same as the logged-in user name, go to step 6.
   - If the user name for the selected system is different, go to step 4.

   Note: After you select a system, CA Chorus generates a PassTicket to authorize your connection. If the PassTicket authorization fails, enter your password to log in to the system.
4. Enter your user name.
5. (Optional) Enter the password for the selected system. The Password field appears in the following cases:
   - The PassTicket generation fails.
   - The user name that you enter is different from the logged-in user name.
   - If the application ID is not set while configuring the security systems. The application ID is used to generate a PassTicket for a logged-in user.

   Note: For more information about the application ID and identifying systems for the Security Command Manager module, see the *CA Chorus for Security and Compliance Management Site Preparation Guide.*
6. Enter the appropriate information in each field and click Simulate.

   Note: For information about a field, hover over it.

   The results of the simulation appear.

Example: Simulate access for a data set on a CA Top Secret system

You believe that an employee, Joe Smith, is inappropriately changing sensitive Human Resources information. The Simulator lets you research if Joe Smith has write access to HR.BONUSES data set on volume ABC321.

Follow these steps:

1. Open the Quick Links module from the Module Library.
2. Click Simulate Access Attempt.
3. Enter the following information:
   a. Select a CA Top Secret system from the System drop-down list.
   b. Enter your user name and password for the selected system.
   c. Type the user ID of Joe Smith in the User Details field.
   d. Select Data Set from the Resource Type drop-down list.
   e. Type **HR.BONUSES** in the Data set Name field.
   f. Type **TSO** in the Facility Field, TSO is the application that Joe Smith uses.
   g. Type **ABC321** in the Volume field.
   h. Select Write from the Permissions drop-down list.
   i. (Optional) To refine the simulation, enter Environment Details. Click the arrow next to Environmental Details to see available fields.
   j. Click Simulate.

      The results of the simulation appear.
4. Review the simulation results to see if Joe Smith has write access to HR.BONUSES.

   You discover that Joe Smith has access to the HR.BONUSES data set. You revoke his access and escalate the issue.

Example: Simulate access for a resource on an CA ACF2 system

Employees in your human resources are having trouble accessing critical files. The Simulator lets you check if users whose UID string matches HR01CAT have update access to a resource named HR.FILES with resource type code HRF.

Follow these steps:

1. Open the Quick Links module.
2. Click Simulate Access Attempt.
3. Enter the following information:
   a. Select the ACF2 system from the System drop-down list.

b. Select the UID option from User Details.

c. Type **HR01CAT** under User Details.

d. Select Resource Type Code from the Resource Type drop-down list.

e. Select HRF from the Type Code drop-down list.

f. Type **HR.FILES** in the Resource Name field.

g. Select UPDATE from the Permissions drop-down list.

h. (Optional) To refine the simulation, enter information in the DATE, TIME, and SOURCE fields in the Environment Details section. Click the arrow next to Environmental Details to see available fields.

i. Click Simulate.

   The results of the simulation appear.

4. Review the simulation results to see if the users have update access to HR.FILES.

   You discover that the users do not have update access to HR.FILES, and grant them access to the resource.

Chapter 5: Monitor Your System

Configure and Launch the Alerts Module

The Alerts module lets you monitor and investigate alerts from the dashboard as they are generated. The alert provides immediate knowledge about a problem occurring on the system. The Alerts module displays only current information.

As a Security Administrator, it is important to be aware of alerts as they happen. We recommend that you create a dashboard named *Alerts* and add the Alerts module to that dashboard. Use this procedure to create a dashboard and configure the Alerts module.

By keeping an active Alerts module on your dashboard, you can see if the user tries to access the payroll data set.

Follow these steps:

1. Click the plus sign icon on the dashboards tab, enter a name for your dashboard, and click Add Dashboard.

   The dashboard name can be up to 21 characters. Valid characters are numeric (0 through 9), alpha (a to z) and (A to Z), underscores, and blank spaces.

2. Add the Alerts module to your customized dashboard.
3. Click the link to configure alerts.
4. Select Security from the Select Alert Source drop-down list, and click Save.

   The Security Alerts module appears on the customized dashboard.

Note: There must be an alert policy in place before the alerts can be seen. For more information, see how to Create an Alert to Monitor a Dataset (see page 53).

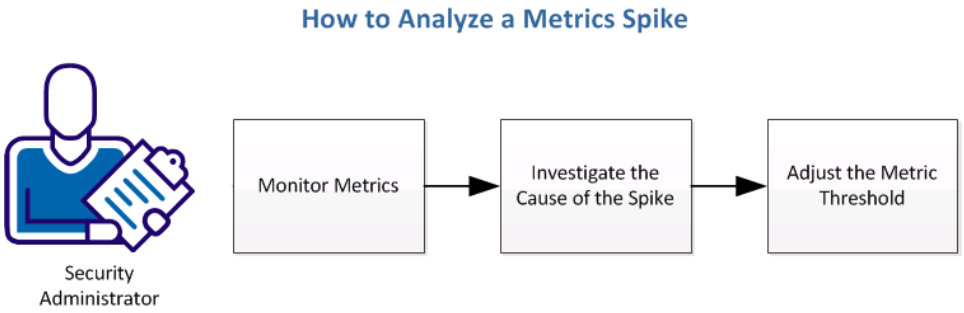
How to Analyze a Metric Spike

Your company invests significant resources to keep your system safe. As a security administrator, you monitor, analyze, and address potential threats. CA Chorus offers several tools to help you complete these tasks. Use the Metrics panel to monitor performance metrics for your systems. Use the Investigator to drill down into the data to discover the reasons for anomalies such as spikes or drops.

Unexpected spikes or drops in metrics may represent a potential problem or threat to your system. You can set thresholds for metrics. When thresholds are met or exceeded, the Metrics panel displays an alert. Adjust threshold values as conditions on your system change.

Example: A spike in user signon validations

Throughout the day, you monitor the Metrics panel. Suddenly, the number of user signon validations (RACROUTE REQUEST=VERIFY) spikes beyond the typical threshold, and the metric color changes. This change alerts you to investigate whether an attacker is attempting to break into the system by guessing passwords. This example explains how you analyze such a spike. Optionally you can adjust the threshold for that metric to avoid unnecessary warnings.



Complete the following tasks to analyze a potential threat:

1. Monitor Metrics (see page 48)
2. Investigate the Cause of Spike (see page 50)
3. (Optional) Adjust the Metric Threshold (see page 52)

Monitor Metrics

As a security administrator, you add metrics to the workspace and monitor them to ensure they do not exceed their thresholds. Use this procedure to configure the Metrics Panel. If you support multiple disciplines in CA Chorus, the Metrics Panel can display data across all disciplines.

In this example, you are monitoring the number of signons (RACROUTE REQUEST=VERIFY).

Follow these steps:

1. Log in to the CA Chorus interface and click the plus sign control (+) on the Metrics panel.

   The Select Metrics Domain view of the Add New Metrics panel opens.

2. Click Security in the *Metric Source* menu.

3. Select Group Metrics by Metric Type.
4. Click Show Tree next to Metric Type and select a metric. Click Next.

   Example: Add 'Statistics Reporting/RACROUTE VERIFY Counts' to monitor the number of signons per minute.
5. Click to select a system from the Available Systems list, or control-click to select multiple systems. Click Add Selected. Click Finish

   The selected metrics appear in the metric panel.

Next, configure threshold values of caution and danger states for each metric.

Follow these steps:

1. Hover the mouse over the metric to monitor the current values.

   Watch the metric over time to determine the typical highs and lows at your site.
2. Click the metric, and click Set Threshold.
3. Set the Caution threshold to *Above*. Enter the highest average number of signons that you encountered.
4. Set the Danger threshold to *Above*. For now, enter an estimated number that is higher than the Caution threshold.
5. Click Set Threshold.

   The thresholds are defined. The cache is highlighted when the value exceeds the caution or danger threshold. A bar appears over the metric to indicate that a threshold is defined.

The threshold bar and the metric color change to yellow when the caution criteria are met. The color changes to red when the danger criteria are met.

Investigate the Cause of the Spike

As a security administrator, you investigate metrics that exceed their thresholds. You can investigate metrics directly from the Metrics panel, or you can add them to your dashboard for further monitoring.

In this example, you are investigating the number of signons, which has exceeded the caution threshold and alerted you. If this spike was caused by a hacker, the most logical cause of failed signon attempts would be a high number of invalid user IDs or invalid passwords. You can use several objects in the Investigator to research this potential threat.

Follow these steps:

1. Stop the Metrics panel scrolling by using the panel controls.

   Note: You can hover over the metric to examine the context of the spike more closely.

2. (Optional) Click the metric and click Add to Dashboard to see a larger view of the metric.

3. Click the metric and then click Investigate.

   The Investigator opens.

4. Choose the Security discipline from the drop-down list.

5. Click the object that you want to investigate. The following example looks at Definitions/Users, Events/Data Warehouse, and Events/Data Marts.

6. Click Customize the Tabular Data View (wrench icon) to add relevant columns, or remove irrelevant columns. Click View Filter (magnifying glass icon) to specify range filters, and click Search to limit the amount of data presented.

   Definitions/Users

   Filter the Users table to display rows with alarmingly high counts for relevant columns.

   Example: A high volume of password violations on one or more accounts in a short time could be an indication of a brute-force hacking attempt. Add the Number of Password Violation, Date of Last Invalid Password, and the Suspended Due to Password columns, to investigate these metrics.

   Events/Data Warehouse and Events/Data Marts

   You can use Compliance Policy Administration interface data to identify System Access Events that occur due to signon violations. Filter the list of events by data and time range, System ID, event category, and event type to narrow down the search.

Example: A large number of signon violations due to invalid passwords for the same user, or violations due to invalid user IDs (IDs that do not exist) could be an indication of a hacking attempt.

Note: The Data Mart contains Compliance Policy Administration interface data with the same type of events as the Warehouse, and supports the same type of research. The difference is that the Warehouse contains real-time data, whereas a current Data Mart must be created first. You create the Data Mart using a batch utility that extracts the appropriate data from the Compliance Policy Administration interface Logger component.

The filtered data appears in the Investigator.

7. (Optional) Click the View Charts icon in the Investigator toolbar. Filter and customize your pie chart using the drop-down lists, and click Add.

   The customized pie chart appears in the center pane of the Investigator. You can dynamically filter the data being displayed, and add more charts using the View Filter and View Charts icons.

   Example: Create a pie chart for System Access Events that includes a count of all detail events within that category and time period. Compare the counts of signon violations and successful signons.

8. Analyze the results to determine if a threat exists. Do *one* of the following:

   - If a threat exists, identify the source of the signon attempt (a terminal or network identifier). Involve the network group to physically locate the source and take it out of service. Consider suspending compromised user IDs to prevent further problems.

     Example: Repeated signon attempts without a valid user ID, or with invalid passwords that cause valid users to be suspended, are a threat to your system.

   - If no threat exists, consider adjusting the thresholds for the metric so the alert does not trigger unnecessarily.

     Example: You know that the number of employees at your company has recently increased because of an acquisition. In this situation, an overall increased number of signons does not represent a threat. Based on your analysis, you adjust the metric threshold to avoid unnecessary warnings in the future.

(Optional) Adjust the Metric Threshold

Color changes visually alert you of metric spikes that could represent a threat to your system. Adjust the threshold for your metrics to ensure that only valid state change warnings appear in the Metrics panel.

Follow these steps:

1. Click the metric in the Metrics panel, and click Edit Threshold.
2. Change the value in Caution State, Danger State, or both. The threshold can be above or below a fixed value.
3. Click Save Threshold.

   The metric now warns you when reaching the updated threshold criteria.

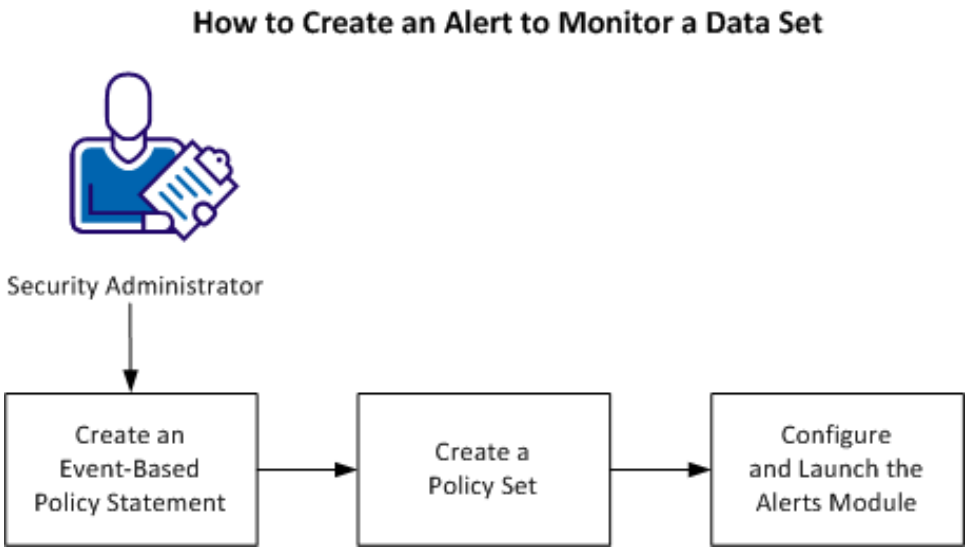
You used the Metrics panel to monitor events and users, and used the Investigator to analyze the cause of an event. You analyzed a metric spike to verify that nothing compromised your system. You then adjusted the threshold setting to avoid unnecessary warnings in the future.

How to Create an Alert to Monitor a Data Set

Management has grown suspicious of an unauthorized employee attempting to access sensitive payroll information. As a clerk in the mail room, the employee does not require access to payroll information. As a security administrator, you plan to monitor the payroll data set and receive an alert when an unauthorized user attempts to gain access.

The Compliance Policy Administration interface logs active security event records, making event history readily available. The interface lets you create policy statements to identify event records to pass to the Compliance Policy Administration interface components.

By using the Compliance Policy Administration interface and the Alerts module, you can identify the event to monitor and receive an alert notification after an unauthorized attempt.



Perform the following tasks to create an alert to monitor a data set:

1. Create an Event-Based Policy Statement (see page 54)
2. Create a Policy Set (see page 55)
3. Configure and Launch the Alerts Module (see page 55)

Create an Event-Based Policy Statement

Use this procedure to create an event-based policy statement. This policy statement monitors the payroll data set and triggers an alert notification if the employee in question tries to gain access.

Follow these steps:

1. Add the Quick Links module to a dashboard and click Administer Compliance Policy.
2. Click the applicable Compliance Policy Administration interface instance from the Administration pane.

   The tree expands to show Compliance Policy Administration interface folders.
3. Click Policy Administration, Policy Statement, Create a Policy Statement.
4. Select Event-Based from the Type drop-down list, click Select, and type a policy statement description.
5. Select Object Access Violation in the events section. This event records violations that occur to a specific object.

   The event appears in the Selected Events portion of the window.
6. Create the following test conditions to identify the employee and payroll data set:
   - Select USERID from the field drop-down list. Select equal sign from the Operator field. Type the user ID in the Value field, and click Add Test Condition.
   - Select CLASS from the field drop-down list. Select equal sign from the Operator field. Type DATASET in the Value field, and click Add Test Condition.
   - Select ENTITY from the field drop-down list, equal sign from the Operator field, type PAYROLL.DSN in the Value field, and click Add Test Condition.
7. Select Chorus Alert under Actions section and click New under Attach Chorus Alert Action. An action can be an email, WTO (write-to-operator), service desk ticket, or a Chorus Alert.

   If the specified user tries to gain access to the payroll data set, an alert is issued to the Alerts module. The Alerts module lets you monitor and investigate alerts as they are generated. This module contains alerts that are based on the Alerts module configuration.
8. Type the description of the alert and select the severity from the drop-down list in the Description field. Click Save Chorus Alert.
9. Click Create Policy Statement.

   The policy statement is now available for use with a policy set.

Create a Policy Set

A policy set is made up of one or more policy statements. Create policy statements before creating a policy set.

Follow these steps:

1. Go to the Quick Links module and click Administer Compliance Policy interface.
2. Click the applicable Compliance Policy Administration interface instance from the Administration pane.
3. Click Policy Administration, Policy Set, Create a Policy Set.

   The Create a Policy Set window opens.
4. Type a policy set name and description.

   The Compliance Policy Administration interface component STC JCL uses this information to associate a component with a policy set. Policy set names are case-sensitive.
5. Specify the Activated setting.

   Yes indicates that the policy set is available for use by a component. No indicates that the policy set is being created and is not yet available.
6. Click Attach Policy Statements in the Policy Statements Attached pane.
7. Select the policy statements that you want to add to the policy set, and click Attach.

   Note: To add all available policy statements on this dialog, click the check box next to Select.
8. Click Create Policy Set.

   The policy set is created.
9. Edit the parameter file that is associated with the Alert component. Add the policy set name in the parameter file.
10. Configure and launch the Alerts module.

By creating this policy statement and policy set, you can monitor each time an unauthorized employee attempts to access sensitive data.

Configure and Launch the Alerts Module

The Alerts module lets you monitor and investigate alerts from the workspace as they are generated. The alert provides immediate knowledge about a problem occurring on the system. The Alerts module displays only current information.

As a security administrator, it is important to be aware of alerts as they happen. You create a dashboard named *Alerts* and add the Alerts module to that dashboard. Use this procedure to create a dashboard and configure the Alerts module.

By keeping an active Alerts module on your dashboard, you can see if the user tries to access the payroll data set.

Follow these steps:

1. Click the dashboard tab that contains the plus sign, click Create a Dashboard, enter a name, and click Add Dashboard.

   The dashboard name can be up to 21 characters. Character types include numerics (0 through 9), alpha (a to z) and (A to Z), underscores, and blank spaces.

2. Add the Alerts module to your customized dashboard.
3. Click the link to configure alerts.
4. Select Security from the Select Alert Source drop-down list, and click Save.

   The Security Alerts module appears on the customized dashboard.

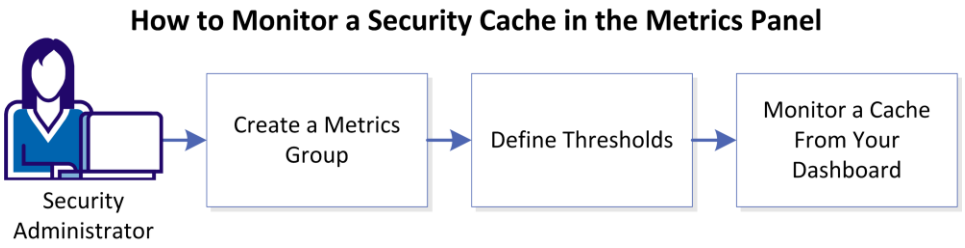
You have created an alert to monitor the payroll data set. If the employee in question tries to gain access to the payroll data set, an alert appears in the Alert module for investigation.

How to Monitor a Security Cache in the Metrics Panel

As a security administrator, you monitor cache size to balance storage needs and performance and to be aware of performance impacts from the cache being emptied too frequently. Your external security manager (ESM) stores recently-accessed security data in the cache to improve performance. The ESM flushes the cache when cache size reaches the defined maximum. After the cache is flushed, performance slows while the cache rebuilds.

Therefore, you monitor cache size to ensure the cache is not flushed too often. You also monitor cache size to ensure that the cache is not too large, thereby wasting critical storage. You configure and maintain proper cache size by monitoring cache size over time.

You can use CA Chorus for Security and Compliance Management to visually monitor cache size in any dashboard from the Metrics panel. You can also perform more detailed monitoring when you configure alert thresholds, and add a cache to your dashboard.



Follow these steps:

1. Create a Metrics Group (see page 57)
2. Define Thresholds (see page 58)
3. Monitor a Cache From Your Dashboard (see page 58)

Create a Metrics Group

To monitor cache size, create a metrics group in the Metrics panel. The Metrics panel is visible above your dashboard. Creating a metrics group lets you view increases and decreases in cache size over time.

Follow these steps:

1. Log in to CA Chorus by entering your mainframe user ID and password at the URL.

   Note: If you do not know the URL, contact your system administrator.

2. Click the plus sign on the Metrics panel.

   The Select Metrics Domain dialog appears.

3. Select Security from the Metric Source drop-down list, and click the group metrics by Metric Type button.

4. Enter **cache** in the Metric Type field, select the metric that you want to monitor, and click Next.

   The Select Systems dialog appears. This dialog lists all systems that use the selected metric.

5. Click the arrows to add individual systems to monitor. Click the multiple arrows control to select all systems.
6. Specify **Cache Size** in the Metrics Group Name field, and click Finish.

   The new metrics group appears in the Metrics panel.

Define Thresholds

Thresholds alert you visually when a cache becomes too large. You define thresholds for a caution state and a danger state. A cache that exceeds the caution state threshold is highlighted in yellow, and a cache that exceeds the danger threshold is highlighted in red. By defining thresholds, you know when a cache will be flushed soon. You are then prepared for any decreases in performance after the cache is flushed.

Follow these steps:

1. In the Metrics panel, click the cache that you want to monitor, and click Set Threshold.
2. Define the caution and danger thresholds by doing the following:
   a. Select Above on the Data Spikes drop-down list, and specify a value in kilobytes for the caution threshold.
   b. Select Above on the Data Spikes drop-down list, and specify a value in kilobytes for the danger threshold.
3. Click Set Threshold.

   The thresholds are defined. The cache is highlighted when the value exceeds the caution or danger threshold.

Monitor a Cache from Your Dashboard

Add a cache metric to your dashboard to investigate it in more detail, or to view changes in its size over a recent time period. Perform this procedure when a cache is being emptied too frequently, or requires other investigation.

The time period for which statistics are available depends on how you configured the STATGINT control in your external security manager. You can then see how often the cache is flushed and use this information to balance storage and performance needs.

Follow these steps:

1. Select the dashboard where you want to view the cache metric.

2. Click the cache metric that you want to add and click Add to Dashboard.

   The cache metric appears in the current dashboard.

3. Click and drag the timeline arrows to view the cache metric over a given time period.

You have configured CA Chorus for Security and Compliance Management to monitor cache size. You are prepared for any slowdown in performance when the cache is flushed. You can also balance storage and performance needs by assessing changes in cache use over time.

Chapter 6: Viewing Security Object Data in the Investigator

View Security Data in the Investigator

The Investigator gives you access to a security repository. The information in the security repository has been designed to service compliance activities. The Investigator simplifies your access to this information. The data in the Investigator is from the external security managers that you have identified to load into CA Chorus.

As you drill down into security compliance data, the Investigator table header includes information to indicate how you arrived at a piece of data. If you filter data, those values appear as header information in your results. As you drill into data, use the Actions pane on the right to identify dependencies and relationships among the records.

Follow these steps:

1. Add the Investigator module to your dashboard, and click Start New Investigation.
2. Select Security from the drop-down list.
3. Drill down to and select an event, definition, or system.
4. Click View Filter (magnifying glass icon).
5. Scroll through the data or filter data using one of the following methods:
   - Leave the filter fields empty and click Filter.
   - Enter specific filter criteria and click Filter.

   Note: To use a wildcard to filter on a string, enter the string and then the percent(%) sign.
6. Select rows of data and the Details pane displays more data.
7. (Optional) Select a row and specify an action to drill further into your data.

   The applicable data appears, with header information that provides the context for the data.

Security Definitions

Security definitions are a grouping that includes all of your security system settings. This folder offers several categories that are based on your security product.

Systems

Security administrators and auditors must know at a glance the origin of their data. The Systems category in the Investigator provides an inventory of all your security systems that are managed through CA Chorus for Security and Compliance Management.

Example: Identify the data loaded in the product

You want to identify the origin of the data that is loaded into CA Chorus as part of the CIA load process. You know that it is from CA ACF2, but you want to identify the specific systems. This information helps you see the breadth of the data available in the Investigator.

1. Add the Investigator module to your dashboard, and click Start New Investigation.
2. Select Security from the drop-down list.
3. Select Definitions, Systems from the folder list.
4. Click View Filter (magnifying glass icon).
5. Filter the data by completing the following steps:
   a. Select Security Application from the Search System drop-down list from the center pane.
   b. Select *contains* from the second drop-down list, and type **ACF.**
6. Click Search.

   The list of CA ACF2 systems that are loaded in CA Chorus appears.

Users

The Users category lets security administrators and auditors view user information across one or more systems. CA ACF2 uses logon IDs and CA Top Secret uses accessor IDs (ACID) to identify users. After you select a row of data, more granular information appears in the Details pane at the bottom of the Investigator.

The following are examples of information that CA Chorus for Security and Compliance Management lets you query at your enterprise:

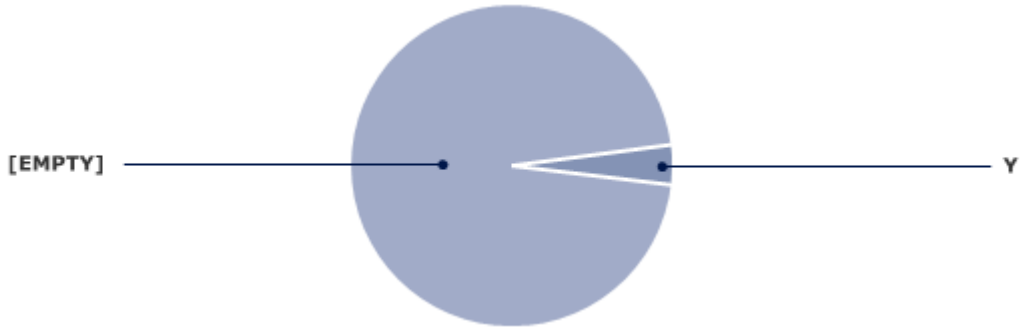
- Identify suspended user IDs. After you identify the ID, drill down to investigate the cause of the suspension.
- Compare user IDs to model permissions and attributes of an existing user to a new one.
- Determine if a user has more than one ID.

Example: Identify and Delete Suspended Users Who Have Left the Company

Your manager has asked you to search for suspended users to identify ones that were suspended instead of permanently removed from the system. In the future, you will perform this internal audit periodically to make certain that your offboarding process is effective. Your manager has given you a list of the users who have left the company in the last year.

1. Add the Investigator module to your dashboard and click New Investigation.
2. Select Security from the drop-down list.
3. Select Definitions, Users from the folder list.
4. Click View Charts (pie chart icon).
5. Select Suspended from the Chart By drop-down list, Select Count from the Aggregate drop-down list, and click Add.

   A pie chart appears that shows you have one suspended user.



6. Sort the Suspended column.

   The suspended user is identified.
7. Compare the data that you gathered with the data provided by your manager to ensure the suspended user left the company.
8. (Optional) Select the suspended user in the Investigator, and select the Delete User action in the Actions pane.

   The selected user is deleted.

Roles

The Roles category lets you view all available roles. A *role* is a basic precept of *role-based security,* a security architecture best practice. A role groups users according to their level of access authorization. Grouping users into roles simplifies administration and security policy.

In a role-based security implementation, access authorization to a resource is not given to the individual users who require access. Instead, roles are identified that have a common set of responsibilities and requirements. For each role, a group of users are identified who share the role. For example, all people in a specific job position can share the same set of responsibilities and have the same authorization requirements. The job position is identified as a role and the people in that job position are identified as sharing the role.

In a role-based security implementation, a security role is defined for a common set of authorization requirements. Access authorization is given once to the role, rather than individually to each user. The users who perform in the role are attached to the role in the security model. By being attached to the role, a user acquires all of the access authorizations that are given to the role. Users typically have a set of roles that they perform in their job function. The roles are attached to the corresponding set of roles in the security model.

When new users are provisioned, they are attached to the roles that correspond to their job requirements.

After you select a row of data, more granular information appears in the Details pane at the bottom of the Investigator.

Example: Identify roles for a new team member

A new security administrator has transferred to your team. Your manager has requested your assigned roles. Your manager wants the new person to have the same roles. You use the Investigator to identify the roles to which you are assigned. You can then export the list of roles to a comma-separated value (CSV) file.

1. Add the Investigator module to your dashboard and click Start New Investigation.
2. Select Security from the drop-down list.
3. Select Definitions, Users from the folder list.
4. Click View Filter (magnifying class icon).
5. Filter the data based on your User ID, which is case-sensitive.
6. Select Show Roles from the Action pane.
7. Select the export icon in the upper-right corner of the Investigator.
8. Specify where to save this file.
9. Email this file to your manager.

CA ACF2 Scope XREF

S*cope records* limit a user's administrative authority over the CA ACF2 Logonid, Rule, and Infostorage databases. The SCPLIST field of the logonid record points to the name of the scope record. You can also see scope records as *scope lists*.

A scope record specifies a list of data set high-level indexes, logonids, UIDs, or infostorage keys. When you assign a scope record for a logonid, you limit its access to the CA ACF2 databases. Scope records grant no special privileges to a user. They provide you with a means to delegate security administration to other logonids and limit the power of those logonids.

CA Chorus for Security and Compliance Management lets you review scope as it relates to the user identification (UID) string. The UID identifies the user and places each user in a CA ACF2-related structure. Whereas CA ACF2 uses the logonid record to verify a user's system access and privileges, CA ACF2 uses the UID to verify a user's access to data and resources. Furthermore, while the logonid identifies a unique user, the UID can identify a user or a group of users in CA ACF2 rules. The logonid record contains the fields that comprise the UID; however, the actual UID does not exist in the logonid record. The UID string is dynamically built at sign-on time.

Example: Adding Scope to a User

Your company has lost a security administrator through retirement. You plan to have an existing employee take over their work. You have identified a strong performer who has the same privileges as the retiree. You would like to increase the existing employee's scope. Before doing so, confirm their present scope.

1. Add the Investigator module to your dashboard.
2. Select Security from the drop-down list.
3. Select Definitions, CA ACF2 Scope XREF from the folder list.
4. Click View Filter (magnifying glass icon).
5. Filter your data to display the user.
6. Review the UID scope as noted in the Details pane.

   You can see their current scope and the changes you need to make to increase their scope. As previously noted, the retiree and the existing employee have the same privileges so no changes are necessary.

CA Top Secret Scopes

CA Chorus for Security and Compliance Management lets you see the scope of authority in the Details pane for each scope list ID. The Top Secret Scopes category lets you view scope records. These records limit the authority a specially privileged user has over ACIDs, access rules, and other security system records. For your security hierarchy, the security administrator is responsible for the scope of authority. CA Top Secret provides several different levels of control ACID scope. Each level corresponds to a level in your corporate structure. By virtue of your security title in the hierarchy of your company, you have scope over one or several areas. In addition to scope authority, you need administrative authority to view and change entities within your scope.

Title	Scope	Example
MSCA	Entire installation	The master SCA (MSCA) can create and modify all entities and CA Top Secret administrators, including SCAs, LSCAs, ZCAs, DCAs, VCAs, and auditors.
SCA	Entire installation	The scope of authority for an SCA depends on the administrative authorities that they were granted. An SCA can create ZCAs, DCAs, VCAs, Profile, and User ACIDs, but not other SCAs.
LSCA	A zone, another LSCA, or both	An LSCA can have all the authority of an SCA, but unlike the SCA, the LSCA must have a scope of authority that is assigned to it. This scope of authority can be one or more LSCAs, zones, or both.
ZCA	A zone	A zone security administrator can perform the following tasks: ■ Permit access to resources owned by the zone, all connected divisions, departments and users within that zone. ■ Define profiles and perform maintenance for ACIDs that are within their scope. ■ Create ACIDs in their zone. ■ Permit ACIDs in other zones to access resources in their zone, but the ZCA cannot perform maintenance for ACIDs in other zones.

Title	Scope	Example
VCA	A division	A divisional security administrator can perform the following tasks: ■ Permit access to resources owned by their division, all departments and users within that division. The VCA can also define profiles and perform maintenance for ACIDs that are within their scope. ■ Create ACIDs in their division. ■ Permit ACIDs in other divisions to access resources in their division, but the VCA cannot perform maintenance for ACIDs in other divisions.
DCA	A department	A department security administrator has the same scope over a department that a VCA has over a division. DCAs can also create ACIDs in their department.

Example: Review Scope of Authority in Your New Department

You have been transferred to a new division that secures sensitive information for your company. As you begin your new role, you want to understand the entities within your scope. Additionally, you want to identify the other security administrators that have scope over your division.

1. Add the Investigator to your dashboard.
2. Select Security from the drop-down list.
3. Select Definitions, CA Top Secret Scopes from the folder list.
4. Click the Filter icon, which resides above the table on the left.
5. Filter your data to display the applicable Scope list ID.
6. Review the scope as noted in the Details pane, including the administrators.

   You now have a better understanding of your division. However, you are concerned about the number of administrators who can potentially change entities in your division. You decide to share your concerns with your manager.

Rules

The Rules category lets you view access, resource rules, and rule lines that are associated with data sets. You can also view resources such as TSO accounts, procedures, commands, facilities, and IMS transactions. The CA Chorus for Security and Compliance Management supports rules and rule lines for CA ACF2 and CA Top Secret.

- CA ACF2 supports rules. Access rules describe the conditions for accessing particular data sets and determine whether access is permitted or prevented for a user or group of users. Resource rules describe conditions for accessing particular resources including TSO accounts, TSO procedures, IMS transactions, commands, and other resources.
- CA Top Secret supports permissions, which give users access to defined resources. Permissions make an owned resource available to other users in a controlled manner. Permissions are by the following:
  - Facility
  - Day and time
  - SYSID
  - Access level

After you select a row of data, more granular information appears in the Details pane at the bottom of the Investigator.

Example: Identify the scope of a change to the CA ACF2 rule

You have received a request to modify a rule. You recognize that this rule can be widely used, but you want to confirm. Doing so lets you determine the impact and decide the best time to implement the change.

1. Add the Investigator module to your dashboard, and click Start New Investigation.
2. Select Security from the drop-down list.
3. Select Definitions, Rules from the folder list.
4. Click View Filter (magnifying glass icon).
5. Filter the data to locate the rule to be changed.
6. Select the rule-line in the table, and select Show All Users from the Action pane.

   The results indicate that this rule is widely used. Based on this information, you plan to suggest to your manager that you implement this change during off hours.

Roles and Users by Resource

Roles and Users By Resource lists the roles and users who have access to a specific resource and the conditions under which access is permitted.

For CA ACF2, this information can help you answer the following compliance questions:

- What UID masks have access to the resource through policy (rule lines)?
- For UID masks that have access to the resource, who are the users that have access because they match the UID mask?

For CA Top Secret, this information can help you answer the following compliance questions:

- What users and profiles have access to the resource through PERMITs, either through the best fit resource entity or through a different masked resource entity?
- For profiles that have access to the resource, who are the users that have access because they are connected to a profile?

The filter parameters for this category use the following default settings. To filter based on different criteria, you must enter a value in the applicable text box to overwrite the default.

- RESOURCE = SYS1.PARMLIB
- TYPE = DATASET
- SYSID = %
- PREFIX = NOPREFIX

Example: Attestation

Your company requires that you show who has access to key resources on a quarterly basis. Use the Roles and Users By Resource category to identify and show this access. After you have done so, click the export icon to save this data to a comma-separated value (CSV) file.

Data Classifications

The Data Classification and Ownership category lists the data class and ownership information of system resources as defined by the Data Class Ownership (DCO) records. This view can help you evaluate data classification and ownership information for resources in a security system environment.

Data classification records help determine which data (files, data sets, resources) pertains to which regulation.

Example

An increasing number of regulations exist that pertain to the secure access of data. The Health Insurance Portability and Accountability Act (HIPAA) dictates the type of data that must be kept confidential for patients. The Family Educational Rights and Privacy Act (FERPA) describes the data that can be accessed from the educational records of a student. Many other regulations (SOX, FISMA, FFIEC, and so on) exist that pertain to secure data. Use this field to track your data to honor these regulations.

Facilities Class XREF

The Facilities Class XREF category lets you view facilities defined in your CA Top Secret systems. A *facility* is a way of grouping options that are associated with a particular service that users login to. To log in to a service, a user must have access to the facility. Only the MSCA can access any facility by default. Everyone else must be authorized to access one or more facilities.

CA Top Secret ships with defined facilities in its Facilities Matrix Table. Examples of such services are BATCH, Started Tasks, CICS, and TSO.

To log in to a service, a user must be given access to the facility. Some services such as BATCH, STC, and TSO are automatically associated with the facility of the same name. Others such as CICS, CA IDMS, and IMS must be associated with an appropriate facility.

After you select a row of data, more granular information appears in the Details pane at the bottom of the Investigator.

Sources

Source Groups control from which terminals (sources) a user can access the system.

- CA ACF2 has Source Groups (ESGP) records that are created and assigned to users.
- In CA Top Secret, sources are added directly to a user and CIA interprets all the terminals for a user as source groups.

The Sources category lets you view different queries for the CIA SRCREC table:

All Records

Displays all records in the SRCREC table: System ID (SYSID), Record ID (SRCRECID), Source Group (SRCGRP), Source Name/Mask (SRCMASK), Record Type (RECTYPE), Include/Exclude Indicator (INCLEXCL), Source Type (SRCTYPE).

Source Groups

Displays distinct System ID, Source Group, Record Type and Source Type records from the SRCREC table: System ID (SYSID), Source Group (SRCGRP), Record Type (RECTYPE), Source Type (SRCTYPE).

ACF2 ESRC Sources

Displays all records in the SRCREC table for ESRC records (Record Type “E”): Displays System ID (SYSID), Source Group (SRCGRP), and Source Name/Mask (SRCMASK). Use this query to map logical source names (for example, "shipping1") to physical source names (for example, "LV396").

Note: After you select a row of data, more granular information appears in the Details pane at the bottom of the Investigator.

Example: Inspect source access restrictions for users

You want to know which users have CA Top Secret source restrictions.

1. Filter Source Groups for the CA Top Secret System ID.

   The grid displays all the users (Source Groups).

2. Click the action “Show Entries” to inspect the sources for a user.

Example: Inspect which source groups exist.

You want to know which CA ACF2 Source Groups exist.

1. Filter Source Groups for the CA ACF2 System ID.

   The grid displays all the Source Groups.

2. Click the action “Show Entries” to inspect the sources in the source group.

Example: Inspect who uses a source

You want to know where a source "abc" is used. Filter All Records for:
“Source Name/Mask” = abc

The grid displays all the groups (CA ACF2) or Users (CA Top Secret) that use this source.

Security Events

The Investigator helps you monitor and evaluate your external security manager systems events by providing multiple work areas to help you manage your data. The Investigator provides the tools to help you locate and review event records to perform the following tasks:

- Demonstrate regulatory compliance
- Mitigate the risk of negative security events
- Reduce the total cost of compliance

Object Accesses

The Investigator displays the following searchable object access event records related to all data set, resource, and database access:

Successful Object Access

Includes a record for each time a user accesses an object.

Event Code: 21

Object Access Audit

Includes a record for each event that is tied to a user whom you are auditing.

Event Code: 22

Object Access Violation

Includes a record for each time a user tries to modify a user account, but is denied.

Event Code: 23

Note: For a comprehensive list of security events and the event triggers, see the security events chapter in your external security manager documentation.

Example: Identify object access audit events for an exiting employee

A finance employee with a significant scope of responsibility at your company has submitted a letter of resignation. This employee plans to work two more weeks and then leave your company. To monitor the actions of this employee, you enable an object access audit. The object access audit produces a record for each user action against objects for your one system. As the two-week period ends, you want to review the records to confirm that no breach has occurred.

1. Add the Investigator module to your dashboard, and click Start New Investigation.
2. Select Security from the drop-down list.
3. Select Events, Object Accesses from the folder list.
4. Click View Filter (magnifying glass icon).
5. Filter the data by completing the following steps:
    a. Select User ID from the first drop-down list from the center pane.
    b. Select = from the second drop-down, and type the *exiting employee user ID*.
    c. Click the plus icon.
    d. Select AND from the first drop-down list.
    e. Select Event Category Description from the second drop-down list from the center pane.
    f. Select = from the second drop-down list, and type *Object Access Audit*.

g. Specify the two-week time period in the Select Time Range pane.

h. Click Search.

The object access events for this employee appear for the last two weeks.

6. Use this information to compare with historical trends or drill into each record, if necessary.

Account Administration

The Investigator displays the following searchable account administration event records:

Successful Account Administration

Includes a record for each time a user account is modified.

Event Code: 31

Account Administration Violation

Includes a record for each time a user tries but is denied when modifying a user account.

Event Code: 32

Note: For a comprehensive list of security events and the event triggers, see the security events chapter in your external security manager documentation.

Example: Identify account administration violations

Your company is looking for efficiencies to maximize productivity. You are tasked with identifying the number of account administration violations in 2012. After you identify them, you can identify the common reasons (poor training, user error, and so on). You can then begin to educate your users about their scope of access. Additionally, you can also identify users attempting to bypass system security.

1. Add the Investigator module to your dashboard, and click Start New Investigation.
2. Select Security from the drop-down list.
3. Select Events, Account Administration from the folder list.
4. Click View Filter (magnifying glass icon).
5. Filter the data by completing the following steps:
   a. Select Event Category Description from the first drop-down list from the center pane.
   b. Select contains from the second drop-down, and type *Violation*.
   c. Click the plus icon.
   d. Select Security Product from the first drop-down list from the center pane.

e. Select contains from the second drop-down list, and type *ACF*.

f. Specify the time range from 1/1/12 to 12/31/12.

g. Click Search.

Your account administration violations for 2012 appear for the specified system.

Policy Administration

The Investigator displays the following searchable policy administration event records to help ensure the integrity of your implemented policy. For CA ACF2, you configure rules to set policy, and for CA Top Secret, you configure permissions to set policy.

Successful Policy Administration

Includes a record for each time a policy is modified.

Event Code: 41

Policy Administration Violation

Includes a record for each time a user tries but is denied when modifying policy.

Event Code: 42

Note: For a comprehensive list of security events and the event triggers, see the security events chapter in your external security manager documentation.

Example: Identify violations to vital data sources

To protect your employees and comply with various government regulations, you monitor activity for vital data sources, such as the personnel file and payroll file. To do so, you review the violations in the Investigator and compare the count with historical data. Additionally, you drill further into some records to investigate questionable activity.

1. Add the Investigator module to your dashboard, and click Start New Investigation.
2. Select Security from the drop-down list.
3. Select Events, Policy Administration from the folder list.
4. Click the Filter icon, which resides above the table on the left.
5. Filter the data by completing the following steps:
   a. Select *Event Category Description* from the first drop-down list from the center pane.
   b. Select = from the second drop-down, and type *Policy Administration Violation*.
   c. Specify a start and end date and time for the last week.

d. Click Search.

Your Policy Administration Violation events appear for the last week.

6. Review the count based on the number in the lower-right corner of the center Investigator pane.
7. Compare this count with historical trends to determine anomalies.
8. Review individual events on an as needed basis. Use the actions to determine event ownership (system and user).

Miscellaneous Administration

The Investigator displays the following searchable miscellaneous administration event records. For example, for CA Top Secret you can see a record based on an ADDTO command for a Field Descriptor Table (FDT) ACID. For CA ACF2, you can see a record for a DELETE command for Infostorage records, except against user profile and resource or database rules.

Successful Other Administration

Includes a record for each time a miscellaneous entity is modified. This record is only generated for entities which are not objects, user accounts, or policies.

Event Code: 51

Other Administration Violation

Includes a record for each time a user tries to modify a miscellaneous entity but is denied. This record is generated only for entities which are not objects, user accounts, or policies.

Event Code: 52

Note: For a comprehensive list of security events and the event triggers, see the security events chapter in your external security manager documentation.

Example: Identify why a new user has access to an RDT in CA Top Secret

All new employees are given limited security system access until they complete mandatory training. One of your new administrators tells you that they were allowed to change the resource descriptor table (RDT). The RDT is a reserved ACID that contains predefined resources classes, such as VOLUME, DATASET, and TERMINAL, and user-defined resource classes. You want to know who gave the new employee this level of access, when, and why. If the company protocol remains the same as you understand, this access must be revoked, but you want to research the details first.

1. Add the Investigator module to your dashboard, and click Start New Investigation.
2. Select Security from the drop-down list.
3. Select Events, Misc Administration from the folder list.

4. Click View Filter (magnifying glass icon).
5. Filter the data:
    a. Select Event Category Description from the first drop-down list from the center pane.
    b. Select contains from the second drop-down, and type *Successful Other Administration*.
    c. Click the plus icon.
    d. Select AND from the first drop-down list.
    e. Select Event System ID from the second drop-down list from the center pane.
    f. Select contains from the third drop-down list, and type the *system ID*.
    g. Specify a start and end date and time from the present until the first day for the employee.
    h. Click Search.

    All successful events appear. Use the actions pane to drill further into each record to determine who granted the access and when.

Control

The Investigator displays the following searchable security control event records:

Security System Start

Includes a record for each time a security system starts.

Event Code: 1

Security System Stop

Includes a record for each time a security system stops.

Event Code: 2

Security System Stop Violation

Includes a record for each time a security system stops abnormally, which appears as an ABEND in the external security manager.

Event Code: 3

Security System Modify

Includes a record for each time a user issues a modify command for the security product.

Event Code: 4

Security System Modify Violation

Includes a record for each time a user tries but is denied when issuing a modify command for the security product.

Event Code: 5

Note: For a comprehensive list of security events and the event triggers, see the security events chapter in your external security manager documentation.

Example: Identify the security system modify owner

You have noticed that your default security system settings have changed in the last 24 hours. You would like to know who issued the modify command that changed these settings. This information helps you contact the individual that issued the modify command.

1. Add the Investigator module to your dashboard, and click Start New Investigation.
2. Select Security from the drop-down list.
3. Select Events, Control from the folder list.
4. Click View Filter (magnifying glass icon).
5. Filter the data by completing the following steps:
   a. Select Event Category Description from the first drop-down list from the center pane.
   b. Select contains from the second drop-down, and type *System Modify*.
   c. Specify a start and end date and time that covers the last 24 hours.
   d. Click Search.

   Your Security System Modify events appear for the last 24 hours.
6. Scroll to the event tied to your system or filter further to narrow the results.
7. Locate the event and click User from the Actions pane.

   Use the contact information in the record to contact the originator to discuss the modifications.
8. Click the notes icon and add the details of your conversation to help ensure that future users understand why the settings changed.

USS File Services

The Investigator lets you review events that are related to calls from applications that are made through UNIX System Services (USS) to the System Authorization Facility (SAF).

CA Chorus for Security and Compliance Management lets you view the following file service events:

USS ck_access

Indicates each instance when this service determines that the current process has requested access to the element.

USS R_chown

Indicates when a user changes the owner of a file.

USS R_chmod

Indicates when a user changes the mode of a file system for file systems and directories.

USS R_chaudit

Indicates when a user changes audit flags for a file.

USS R_audit

Indicates each instance when this service provides an interface for actions that must write a record for a condition where a security check service audit is not sufficient.

USS R_setfacl

Indicates when a user modifies a file access control list.

USS User Services

The Investigator lets you review events that are related to calls made through UNIX System Services (USS) to the System Authorization Facility (SAF).

CA Chorus for Security and Compliance Management lets you view the following user service events:

USS InitUSP

Indicates each instance when this service verifies that a user is authorized to use z/OS UNIX and sets security attributes for the calling process.

USS DeleteUSP

Indicates each instance when this service deletes the calling process security environment.

USS R_setuid

Indicates each instance of a setuid event, which lets a user run an executable based on the executable owner permissions.

USS R_seteuid

Indicates when this service checks if the user has the authorization to modify z/OS UNIX UIDs and changes the effective UID for the current process.

USS R_setgid

Indicates when a user setgid event occurs, which lets a user run an executable based on the permissions of the executable group.

USS R_setegid

Indicates when a user changes the owner of a file.

USS InitACEE

Indicates each instance when a user invokes this callable service. The initACEE service provides the following:

- Interface to create and manage security contexts.
- Interface to register and deregister certificates.
- Interface to query a certificate to determine an association with a user ID.

Chapter 7: Troubleshooting

Identify the CA LDAP Server for z/OS Version

To identify system properties when communicating with CA Support, you can access this information directly in the user interface. System properties that are displayed include the LDAP version and the time limits set in the acf2_config.xml or tss_config.xml files.

Follow these steps:

1. Add the Quick Links module to your dashboard, and click Administer Compliance Policy.

   The Administer Compliance Policy interface opens.

2. Select the system whose properties you want to view.
3. Click LDAP Node Information from the tree.

   The LDAP Node Information window displays. This window identifies the following system properties:

   LDAP Server Configuration

   Identifies target machine name, port, suffix, and time limits. The time limits are set in the acf2_config.xml or tss_config.xml file.

   Miscellaneous

   Identifies the number of rows to display from search results at one time. The values are set in the acf2_config.xml or tss_config.xml file.

   LDAP Module Version Information

   Identifies vendor name, versions of your LDAP installation, and your LDAP installation modules and naming contexts.

Receive LDAP Connect Error in Security and Policy Interfaces

Symptom:

When I click any of the links in the Quick Links module, I see a Connect Error.

Solution:

The LDAP server may be down. Start the LDAP server and try again.

Note: For more information about the LDAP server, see the *CA LDAP Server for z/OS Product Guide*.

Receive HTTP 404 error in Security and Policy Interfaces in the Quick Links Module

Symptom:

When I select the Administer Security Definitions or Administer Compliance Policy in the Quick Links module, I receive an HTTP 404 page not found error.

Solution:

This error occurs when the Security Administration interface or Compliance Policy Administration interface war files are not deployed during JBoss startup.

Follow these steps:

1. Open the SERVER.LOG located in your INSTALL_DIR/logs.
2. Locate the following line
   - deploy, ctxPath=/PolicyAdmin (For Compliance Policy Administration)
   - deploy, ctxPath=/SecAdmin (For Security Administration)
3. The last line in the war file deployment section of the log file must match the following line:

   .ContextLoader. Root WebApplicationContext: initialization completed in 612 ms
4. If you do not see the line as noted in step 3 and instead you see an error message, contact CA Technical Support.

HTTP 400 Error in the Quick Links Module

Symptom:

When I click the Administer Security Definitions link or Administer Compliance Policy link, I receive an HTTP 400 error.

Solution:

The URL is case-sensitive. Check the URL and confirm that the URL is correct.

Receive HTTP 500 error in Security and Policy Interface in the Quick Links Module

Symptom:

When I click the Administer Security Definitions link or Administer Compliance Policy link, I get an HTTP 500 error.

Solution:

This error indicates that the configuration file is in the wrong location or the file does not exist.

Follow these steps:

1. Look out for the following null pointer exceptions in the stack trace:

   ```
   javax.servlet.ServletException: javax.faces.el.EvaluationException: Cannot get value for expression '#{vantageTreeBean.userName}'
   ```

   The presence of this exception indicates a user error.

   Note: If you find any other errors in the HTTP 500 stack trace, such as other null pointer exceptions, contact CA Technical Support.

2. Verify that the following configuration files exist in the specified directories:

   - For Compliance Policy Administration, locate the configuration file in INSTALL_DIR/config:
     - cmgr_config.xml
   - For Security Administration, locate the following configuration files in INSTALL_DIR/config:
     - acf2_config.xml for CA ACF2
     - tss_config.xml for CA Top Secret

   If the configuration file is not present, you have edited and submitted the job E1MI0014 in the CE1MJCL data set during the installation process.

   Run job E1MI0014 now.

   Important! Restart JBoss to apply the changes.

3. Verify whether you see the following message in the root cause in the stack trace.

   ```
   javax.servlet.ServletException: Cannot get value for expression '#{vantageTreeBean.model}'
   ```

   This indicates a syntax error in the config.xml file.

For Compliance Policy Administration, check the configuration file named cmgr_config.xml in INSTALL_DIR/config.

- For Security Administration, check the following configuration files in the INSTALL_DIR/config:
  - acf2_config.xml for CA ACF2
  - tss_config.xml for CA Top Secret

Check the options that you specified in these files. Verify that each option is closed correctly with an end tag. For example, verify that the option <ldapsuffix> is correctly paired with its end tag </ldapsuffix> (notice the backslash).

Cannot see any nodes in the navigation tree

Symptom:

I cannot see nodes in the navigation tree in the Security Administration interface, Compliance Policy Administration interface, or both.

Solution:

You cannot see the nodes when LDAP nodes are not defined in the configuration file. To see the nodes, edit and submit job E1MI0014 in the CE1MJCL data set.

Cannot see any nodes after clicking on the LDAP node

Symptom:

After I click an LDAP node in the Compliance Policy or Security Administration interfaces, I cannot see a navigation tree.

Solution:

This error occurs when the tree location path in the configuration file does not match the default location. Confirm that the path matches the following default values:

- Security Administration:
  - Open the acf2_config.xml file located in INSTALL_DIR/configdir and confirm that the path matches the following line: <xmlfile>conf/esm/acf2/acf2tree.xml</xmlfile>.

- Open the tss_config.xml file located in INSTALL_DIR/configdir and confirm that the path matches the following line:
  <xmlfile>conf/esm/tss/tsstree.xml</xmlfile>

- Compliance Policy Administration:
  - Open the cmgr_config.xml file located in INSTALL_DIR/configdir and confirm that the path matches the following line:
    <xmlfile>conf/cmgr/cmgrtree.xml</xmlfile>.

Policy Administration and Policy Disclosure nodes are missing

Symptom:

In the Compliance Policy Administration interface, I cannot see Policy Administration and Policy Disclosure nodes in the navigation tree.

Solution:

Follow these steps:

1. Verify that LDAP starts with PGM = BPXBATA8 instead of BPXBATCH.

   The following line in the LDAP Proc specifies the PGM value.

   ```
   //LDAPR15 EXEC PGM=BPXBATA8, REGION=0M, TIME=NOLIMIT
   ```

2. Confirm that MAPDB in the DD statement in the LDAP proc matches the MAPDB in the slapd.conf file of LDAP.

   A MAPDB DD statement in the LDAP Proc should appear as follows:

   ```
   //MAPDBXX DD DISP=SHR, DSN=YOUR.DATABASE.MAPDB
   ```

   Open the slapd.conf file found in LDAP_INSTALL_DIRECTORY.

   The line that defines MAPDB in the slapd.conf file is

   ```
   cmgrPolicyDD MAPDB
   ```

3. Change the DD statement in LDAP PROC to the value in the slapd.conf file. The DD statement should appear as follows:

   ```
   //MAPDB DD DISP=SHR,DSN=YOUR.DATABASE.MAPDB
   ```

Event Reports, Summary Reports, Change Approvals are not directories

Symptom:

When I select an LDAP node and the navigation tree expands, Event Reports, Summary Reports, and Change Approvals do not appear as directories and I cannot open them.

Solution:

1. If your site is using a DB2 configuration, start DB2 and Resource Recovery Services (RRS). After you start DB2, recycle LDAP.
2. If your site is using a CA Datacom configuration, start CA Datacom/AD Version 14.0 and CA Datacom Server Version 14.0. After CA Datacom is started, recycle LDAP.

Symptom:

I have restarted DB2 and RRS, LDAP is up, but I still see that Event Reports, Summary Reports, Change Approvals are not directories and I cannot open them.

Solution:

1. Go to the console and issue the following command:
   `F YOUR_LDAP_STC,Backend`
2. Scroll down to see the following PARM:
   `DB Discovered Yes`

   If this output indicates No it means that the LDAP server has not connected to DB2. One reason could be that LDAP was started before DB2, or that RRS was up.
3. Recycle LDAP.

Symptom:

DB2 and RRS are started, LDAP is up and the "F YOUR_LDAP_STC,Backend" command in the console indicates "DB Discovered Yes". However, I still see that Event Reports, Summary Reports, Change Approvals are not directories and I cannot open them.

Solution:

Check the permissions to the Compliance Policy Administration interface Components. If the Compliance Policy Administration interface does not have permission to read the DB2 Tables during startup, it does not show the expandable tree items.

Receive LDAP Timeout Messages in the Interface

Symptom:

I see LDAP timeout messages in my web interface during searches.

Reason:

The time limit set in the configuration XML file is lower than the time taken by the servers to capture and display the results.

Solution:

To change the time limit

1. Go to the CHORUS_HOME/config directory.
2. Find the file cmgr_config.xml.
   - For Compliance Policy Administration, locate the configuration file in INSTALL_DIR/config:
     - cmgr_config.xml
   - For Security Administration, locate the following configuration files in INSTALL_DIR/config:
     - acf2_config.xml for CA ACF2
     - tss_config.xml for CA Top Secret
3. Edit the configuration file. The file is in ASCII format on the Mainframe and you edit it in one of two ways:
   - FTP the file to your PC, edit it, and FTP it back to your LPAR.
   - Use ispfedit:
     - Issue the EA 'FILE_NAME' command to edit the ASCII file.
     - Issue the VA 'FILE_NAME' command to view the ASCII file.
4. Convert the file using one of the following commands:
   ```
   iconv -f iso8859-1 -t ibm-1047 cmgr_config.xml > cmgr_config.xml.e
   iconv -f iso8859-1 -t ibm-1047 acf2_config.xml > acf2_config.xml.e
   iconv -f iso8859-1 -t ibm-1047 tss_config.xml  > tss_config.xml.e
   ```
5. Increase the time limit. Specify the time in seconds. The default is 60 seconds.
   ```
   <searchTimeLimit>60</searchTimeLimit>
   ```

6. Save the file, and then convert it back using one of the following commands:

```
iconv -f ibm-1047 -t iso8859-1 cmgr_config.xml.e > cmgr_config.xml
iconv -f ibm-1047 -t iso8859-1 acf2_config.xml.e > acf2_config.xml
iconv -f ibm-1047 -t iso8859-1 tss_config.xml.e  > tss_config.xml
```

Important! Restart JBOSS to pick up the changes.

Receive SIZELIMIT Exceed Message in the UI search

Symptom:

I see "Size Limit exceeded" messages in my web interface during searches.

Solution:

1. Open the LDAP slapd.conf file.
2. Check the size limit. The default value in the slapd.conf file is 500.

   ```
   Sizelimit 500
   ```

   If your database has results over 500, this could lead to a size limit exceeded message in the UI or in the LDAP log.
3. Change the limit to a higher value, or set it to -1. If you specify -1, the database returns all results that are available.

Symptom:

I specified a size limit option of -1 in the LDAP slapd.conf file, and I still see "Size Limit exceeded" messages in my web interface during searches.

Reason:

This message means that the number of returned results is higher than the default size limit of the interface, which is limited to displaying up to 1000 returned results.

Solution:

To change the size limit

1. Go to the CHORUS_HOME/config directory.
2. Find the file cmgr_config.xml.
   - For Compliance Policy Administration, locate the configuration file in INSTALL_DIR/config:
     - cmgr_config.xml

- For Security Administration, locate the following configuration files in INSTALL_DIR/config:
  - acf2_config.xml for CA ACF2
  - tss_config.xml for CA Top Secret

3. Edit the configuration file. The file is in ASCII format on the mainframe and you edit it in one of two ways:
   - FTP the file to your PC, edit it, and FTP it back to your LPAR.
   - Use ispfedit:
     - Issue the EA 'FILE_NAME' command to edit the ASCII file.
     - Issue the VA 'FILE_NAME' command to view the ASCII file.
4. Convert the file using one of the following commands:

```
iconv -f iso8859-1 -t ibm-1047 cmgr_config.xml > cmgr_config.xml.e
iconv -f iso8859-1 -t ibm-1047 acf2_config.xml > acf2_config.xml.e
iconv -f iso8859-1 -t ibm-1047 tss_config.xml  > tss_config.xml.e
```

5. Increase the size limit to a value equivalent to or higher than the number of entries in your database.

```
<searchRows>2500</searchRows>
```

6. Save the file, and then convert it back using one of the following commands:

```
iconv -f ibm-1047 -t iso8859-1 cmgr_config.xml.e > cmgr_config.xml
iconv -f ibm-1047 -t iso8859-1 acf2_config.xml.e > acf2_config.xml
iconv -f ibm-1047 -t iso8859-1 tss_config.xml.e  > tss_config.xml
```

Important! Restart JBOSS to pick up the changes.

Receive an LDAP Startup Update Access Denied Error

Symptom:

I see the following error when starting up LDAP:

```
CAS2312E LDAPR15  - UPDATE  ACCESS DENIED 270
         /U.USERS.STRRO02.LDAPR15.LDAPR15$STDOUT$LOG
BPXM009I BPXBATCH FAILED BECAUSE OPEN (BPX1OPN) FOR STDOUT  FAILED WITH
      RETURN  CODE 0000006F REASON CODE 5BC80004
IEF404I LDAPR15 - ENDED - TIME=11.15.34
```

Solution:

This error indicates that LDAP received a CA SAF HFS Security violation.

Cannot log on to Policy Administration Interface using Quick Links module

Symptom:

When I select Manage Security Definitions and click the CA ACF2 or CA Top Secret node in the tree, I see the following error:

CA Web Administrator for CA Top Secret/CA ACF2 only supports managing hosts that are r12 or higher.

Solution:

Stop and start the LDAP server and try again.

Appendix A: CA Chorus and ESM Field Name Comparison

The following table provides a list of field names displayed in CA Chorus and the CA ACF2 and CA Top Secret equivalent:

CA Chorus	CA ACF2	CA Top Secret
System ID	Supplied as the input parameter in the CIA UNLOAD job or defaults to the SMCASID (the z/OS SMFID) where the CIA UNLOAD job was executed	SYSID
DCO Record Identifier	RECORD ID of DCO DATA record Limits: Begins with the DATA keyword, followed by a 1 to 28 character qualifier.	Combination of DCLASS + RCLASS + a sequence number
Regulation Class	DCLASS of DCO DATA record Limits: Multi-valued field of up to 32 bytes per character.	DCLASS
Sequence	Identifies the sequence number of the DCLASS value in the DCLASS list of DCO DATA record	A number assigned to differentiate the combination of DCLASS and RCLASS starting with 0001
Data Classification Description	DESC of DCO DATA record Limits: 32 bytes	DESCRIPT Limits: 32 characters. If the description field contains blanks, enclose it in single quotes.
Resource Class Name	RCLASS of DCO DATA record Limits: 8 bytes	RCLASS
Resource Class	TYPE of DCO DATA record Limits: Four characters, beginning with R for a generalized resource and D for a DB2 resource.	RCLASS

CA Chorus	CA ACF2	CA Top Secret
Resource Name/Mask	RESOURCE of DCO DATA record Limits: 255 bytes, using the dash (-) as the masking character.	RESNAME Limits: 1 to 255 characters
First Entitlement Owner ID	OWNER1 of DCO DATA record Limits: This is a logonid value.	OWNER1
Second Entitlement Owner ID	OWNER2 of DCO DATA record Limits: This is a logonid value.	OWNER2
First Entitlement Owner Name	ONAME1 of DCO DATA record Limits: 255 bytes	ONAME1 Limits: 1 to 255 characters. If the data contains blanks, enclose the data in quotation marks.
Second Entitlement Owner Name	ONAME2 of DCO DATA record Limits: 255 bytes	ONAME2 Limits: 1 to 255 characters. If the data contains blanks, enclose the data in quotation marks.
Resource Class	R' + $TYPE for resource, 'D' + $TYPE for DB2 rules, 'DATASET' for access rules	Resclass
Rule Key	$KEY Limits: 8 characters	Owned resource
Authorization ID	UID, ROLE, USER	acid
Rule Sequence Number	Sequence number of this permission in the rule set.	Number used to identify which perm tables go together (permxref/permlibx/etc)
Rule Resource Name/Mask	DSNMASK for access rules, RSRCMASK for resource and DB2 rules Limits: 1 to 22 levels of qualifiers, with each qualifier beginning with: an alphabetic character, @, $, or #. Maximum of 8 characters per level, and 44 characters total.	Resource name
Non-Prefix Resource Mask	n/a	n/a
Rule Set Prefix	$PREFIX Limits: 24 characters	n/a
Next Ruleset for Validation	$NEXTKEY Limits: 8 characters	n/a
Application Indicator	n/a	T = TSS A = ACF2

CA Chorus	CA ACF2	CA Top Secret
Authorization Type	UID, ROLE, USER	U = User type vs R = Profile
TSS Last Change Administrator ID	n/a	ADMINBY acid
TSS Last Change Date	n/a	ADMINBY date
TSS Last Change Time	n/a	ADMINBY time
Activation Date	ACTIVE Format: MM/DD/YY	n/a
Expiration Date	UNTIL, FOR Format: MM/DD/YY	UNTIL
Associated Data	n/a	The list of access levels available to this particular resource
Allow Read Access	READ(ALLOW, LOG, PREVENT), SERVICE(READ)	ACCESS(READ)
Allow Write Access	WRITE(ALLOW, LOG, PREVENT)	ACCESS(WRITE)
Allow Update Access	SERVICE(UPDATE)	ACCESS(UPDATE)
Allow Delete Access	SERVICE(DELETE)	ACCESS(DELETE)
Allow Execute Access	EXECUTE(ALLOW, LOG, PREVENT), SERVICE(EXECUTE)	ACCESS(EXECUTE)
Allow Add Access	SERVICE(ADD)	ACCESS(ADD)
Allow All Access	If SERVICE is not specified, the default is all services	ACCESS(ALL)
Allow Allocate Access	ALLOCATE(ALLOW, LOG, PREVENT)	ACCESS(ALLOCATE)
Allow Alter Access	SERVICE(ALTER)	ACCESS(ALTER)
Allow DB2 Alterin Access	SERVICE(ALTERIN)	ACCESS(ALTERIN)
Allow DB2 Any Access	SERVICE(ALL)	ACCESS(ANY)
Allow TSS APPC Access	n/a	ACCESS(APPCLU)
Allow TSS Autolog Access	n/a	ACCESS(AUTOLOG)
Allow DB2 Bind Access	SERVICE(BIND)	ACCESS(BIND)
Allow TSS BLP Access	n/a	ACCESS(BLP)
Allow TSS Browse Access	n/a	ACCESS(BROWSE)

CA Chorus	CA ACF2	CA Top Secret
Allow TSS Collect Access	n/a	ACCESS(COLLECT)
Allow TSS Control Access	n/a	ACCESS(CONTROL)
Allow Copy Access	SERVICE(COPY)	ACCESS(COPY)
Allow Create Access	SERVICE(CREATE)	ACCESS(Create)
Allow DB2 Create In Access	SERVICE(CREATEIN)	ACCESS(CREATEIN)
Allow DB2 Create Table Access	SERVICE(CRETAB), SERVICE(CREATETAB)	CRETAB privilege
Allow DB2 Create Tablespace Access	SERVICE(CRETS), SERVICE(CREATETS)	CRETS privilege
Allow DB2 Admin Access	SERVICE(DBAM)	DBADM privilege
Allow DB2 DB CNTL Access	SERVICE(DBCTRL)	DBCTRL privilege
Allow DB2 DB MAINT Access	SERVICE(DBMAIN)	DBMAINT privilege
Allow DB2 Display DB Access	SERVICE(DISPDB) SERVICE(DISPLAYDB)	DISPDB privilege
Allow DB2 Drop Access	SERVICE(DROP)	DROP privilege
Allow DB2 Drop in Access	SERVICE(DROPIN)	DROPIN privilege
Allow TSS Eread Access	n/a	ER (Exclusive read)
Allow TSS Ewrite Access	n/a	EW (Exclusive write)
Allow TSS Exec Access	n/a	ACCESS(Execute)
Allow TSS FEOV Access	n/a	FEOV ACCESS
Allow TSS Fetch Access	n/a	ACCESS(FETCH)
Allow TSS Find Access	n/a	ACCESS(FIND)
Allow TSS Grplogon Access	n/a	For VMACH - Group logon
Allow DB2 Image Copy Access	SERVICE(IMAGCOPY)	IMAGCOPY privilege
Allow DB2 Index Access	SERVICE(INDEX)	INDEX
Allow TSS Inquire Access	n/a	INQUIRE

CA Chorus	CA ACF2	CA Top Secret
Allow DB2 Insert Access	SERVICE(INSERT)	TABLE INSERT
Allow TSS Install Access	n/a	INSTALL
Allow DB2 Load Access	SERVICE(LOAD)	LOAD privilege
Allow TSS Logon Access	n/a	LOGON
Allow TSS Mread Access	n/a	VM Minidisks - MULTI READ
Allow TSS Multi Access	n/a	MULTI
Allow TSS Mwrite Access	n/a	MULTI/WRITE MW
Allow TSS Nocreate Access	n/a	NOCREATE
Allow TSS None Access	n/a	NONE
Allow TSS Noshr Access	n/a	LOAD NOSHR
Allow TSS Unknown Access	n/a	OTHER
Allow DB2 Package Admin Access	SERVICE(PACKADM)	DB ADMIN/DB2 Package
Allow TSS Perform Admin Access	n/a	PERFORM
Allow TSS Purge Access	n/a	PURGE
Allow DB2 Recover DB ACCESS	SERVICE(RECOVDB), SERVICE(RECOVERDB)	RECOVER/RECOVDB privilege
Allow DB2 Refer Access	SERVICE(REFER)	REFER
Allow DB2 Reorg Access	SERVICE(REORG)	REORG/REORG privilege
Allow DB2 Repair Access	SERVICE(REPAIR)	REPAIR/REPAIR privilege
Allow TSS Replace Access	n/a	REPLACE
Allow TSS Scratch Access	n/a	SCRATCH
Allow TSS Search Access	n/a	SEARCH
Allow DB2 Select Access	SERVICE(SELECT)	SELECT/TABLE SELECT
Allow TSS Set Access	n/a	SET

CA Chorus	CA ACF2	CA Top Secret
Allow TSS SHR Access	n/a	SHR/LOAD SHR
Allow TSS Smulti Access	n/a	SMULTI/SM (Stable multi)
Allow TSS Sread Access	n/a	SREAD/SR (Stable read)
Allow DB2 Start DB Access	SERVICE(STARTDB)	DB START/STARTDB privilege
Allow DB2 Stats Access	SERVICE(STATS)	STATS/STATS privilege
Allow DB2 Stop DB Access	SERVICE(STOPDB)	STOP DB/STOPDB privilege
Allow TSS Surrogate Access	n/a	SURROGATE
Allow TSS Swrite Access	n/a	SWRITE/SW (Stable write)
Allow DB2 Trigger Access	SERVICE(TRIGGER)	TRIGGER/TRIGGER privilege
Allow DB2 Usage Access	SERVICE(USAGE)	USAGEDB/Usage privilege
Allow TSS Use Access	n/a	USE
Log Access	n/a	ACTION(AUDIT)
Deny Resource	n/a	ACTION(DENY)
Call Exit	n/a	ACTION(EXIT)
Process Fail	n/a	ACTION(FAIL)
Skip Dataset Validation	n/a	ACTION(NODSN)
Notify Console	n/a	ACTION(NOTIFY)
Return Control for Password	n/a	ACTION(PASSWORD)
Reverify Password	VERIFY	ACTION(REVERIFY)
Use VM Privileged Commands	n/a	ACTION(VMPRIVILEGE)
Access Mode in Effect	$MODE(Quiet|Log|Abort)	MODE
DDNAME Required for Permission	DDNAME(*ddnmask*) Limits: 8 characters	n/a
Dataset Volume Required for Permission	VOLUME(*volmask*) Limits: 6 characters	n/a
Day Restriction	Shift record ID	Either CALENDAR record, or DAYS keyword
Time Restriction	Shift record ID	Either TIMEREC record or TIMES keyword

CA Chorus	CA ACF2	CA Top Secret
Source Record ID	SOURCE(sourcemask) masked name of the source group records Limits: 8 characters	SOURCE keyword
APPLDATA Value	n/a	APPLDATA
Owner	$OWNER, for db2 rules $LIDOWNER(logonid), $UIDOWNER(uidmask)	Owner of the resource
Owner Type	$LIDOWNER(logonid), $UIDOWNER(uidmask)	Acid type of the Owner - OR D for Department, V for Division and Z for Zone
ACF2 $RESOWNER Value	$RESOWNER Limits: 8 characters	n/a
ACF2 $OWNER Value	$OWNER Limits: 24 characters	n/a
ACF2 Last Change Administrator ID	ACALLID in ACAREC, ACGLID in ACGREC	n/a
ACF2 Last Change Date	ACATOD in ACAREC, ACGTOD in ACGREC	n/a
ACF2 Last Change Time	ACATOD in ACAREC, ACGTOD in ACGREC	n/a
ACF2 $USERDATA Value	$USERDATA Limits: 64 characters	n/a
Rule Key	$KEY Limits: 8 characters	RESOURCE
RESOURCE Parameter	Supplied as input by user and relates to DSNMASK and RSRCMASK	RESOURCE
SYSID Parameter	Supplied as input by user and relates to the CIA SYSID	SYSID
TYPE Parameter	Supplied as input by user and relates to 'R' + $TYPE for resource, 'D' + $TYPE for DB2 rules, 'DATASET' for access rules	RESCLASS
PREFIX Parameter	Supplied as input by user and relates to $PREFIX	N/A
Allow TSS Discard Access	n/a	DISCARD access
Allow DB2 Drop In Access	SERVICE(DROPIN)	DROPIN privilege

CA Chorus	CA ACF2	CA Top Secret
Rule Key	$KEY Limits: 8 characters	N/A
Rule Sequence Number	Sequence number of this permission in the rule set	N/A
Column Name	COLUMN	N/A
Resource Class	n/a	Resclass
Rule Key	n/a	Resname
Authorization ID	n/a	Acid name
Rule Sequence Number	n/a	Number used to identify which perm tables go together (permxref/permlibx/etc)
Facility Name	n/a	Facility
Rule Key	$KEY Limits: 8 characters	Resname
Library Name	LIBRARY(libmask) Limits: 44 characters	LIBRARY
Program Name	PGM(pgmmask), PROGRAM(pgmmask) Limits: 8 characters	PRIVPGM
Permission System ID	n/a	SYSID of the system where the resource requiring this permission is used
Role ID	ROLENAME part of the Record Id of an X-ROL record Limits: 1 to 8 characters	PROFILE
Record System ID	SYSID part of the Record Id of an X-ROL record Limits: 1 to 8 characters	N/A
Role Type	ROLE or GROUP specified in an X-ROL record	= 'P' if a Top Secret Profile
Expiration Date	n/a	UNTIL Limits: Date format.
Activated	n/a	Date that role is activated for all members Limits: Date format.
Console	n/a	CONSOLE
Trace	n/a	TRACE attribute
Update INSTDATA	n/a	DUFUPD

CA Chorus	CA ACF2	CA Top Secret
TSS RACROUTE	n/a	DUFXTR
INSTDATA	n/a	INSTDATA
MRO	n/a	MRO
RACF bit	n/a	NOADSP
No ATS	n/a	NOATS
No DSN Check	n/a	NODSNCHK
No LCF Check	n/a	NOLCFCHK
No Password Change	n/a	NOPWCHG
No Resource Check	n/a	NORESCHK
No Submit Check	n/a	NOSUBCHK
Do Not Suspend	n/a	NOSUSPEND
No Volume Check	n/a	NOVOLCHK
ID Card	n/a	OIDCARD attribute
Source ID	n/a	SOURCE keyword
Time Zone	n/a	TIME ZONE
Primary Language	n/a	LANGUAGE
Secondary Language	n/a	LANGUAGE - we only allow one language to be specified.
Physical Key	n/a	PHYSKEY
Operator Class	n/a	OPCLASS
CICS Operator ID	n/a	OPIDENT
CICS Operator Priority	n/a	OPPRTY
Time Out	n/a	CICS TIMEOUT value Limits: Defined by the OPTIME keyword.
SYSOUT User Name	n/a	WANAME Limits: Up to 60 characters. If spaces are used, enclose the value in single quotes.
SYSOUT Building	n/a	WABLDG Limits: Up to 60 characters. If spaces are used, enclose the value in single quotes.

CA Chorus	CA ACF2	CA Top Secret
SYSOUT Dept	n/a	WADEPT Limits: Up to 60 characters. If spaces are used, enclose the value in single quotes.
SYSOUT Room	n/a	WAROOM Limits: Up to 60 characters. If spaces are used, enclose the value in single quotes.
SYSOUT Addr 1	n/a	WAADDR1 Limits: Up to 60 characters. If spaces are used, enclose the value in single quotes.
SYSOUT Addr 2	n/a	WAADDR2 Limits: Up to 60 characters. If spaces are used, enclose the value in single quotes.
SYSOUT Addr 3	n/a	WAADDR3 Limits: Up to 60 characters. If spaces are used, enclose the value in single quotes.
SYSOUT Addr 4	n/a	WAADDR4 Limits: Up to 60 characters. If spaces are used, enclose the value in single quotes.
Account Number	n/a	WAACCNT Limits: Up to 255 characters. If spaces are used, enclose the value in single quotes.
Role ID	ROLENAME part of the Record Id of an X-ROL record Limits: 1 to 8 characters	N/A
Role System ID	SYSID part of the Record Id of an X-ROL record Limits: 1 to 8 characters	N/A
Role Type	ROLE or GROUP specified in an X-ROL record	N/A
Role Mask	Single masked value of a user, group of users, role, or group of roles that is specified in the INCLUDE or EXCLUDE field of an X-ROL record	N/A
Include/Exclude	Indicates if this rolemask is an INCLUDE entry or an EXCLUDE entry of an X-ROL record	N/A

CA Chorus	CA ACF2	CA Top Secret
User ID	logonid, %CHANGE, %RCHANGE in the ruleset	N/A
Scope Record ID	SCPLIST in logonid record; if the ruleset, then %CHANGE+RCLASS+$KEY or %RCHANGE+RCLASS+$KEY	n/a
Authorization Type	If the authorization id is a logonid or XREF role, set this value to 'U' If the authorization id is a UID, set this value to 'R'	n/a
Scope Record ID	n/a	Department ACID this group is attached to
TSS Group ACID Name	n/a	Group acid name
Scope Record ID	n/a	Department ACID this profile is attached to
TSS Profile Name	n/a	PROFILE acid name
Parent Scopelist ID	SCPLIST in logonid record; if ruleset, then %CHANGE+RCLASS+$KEY or %RCHANGE+RCLASS+$KEY	The acid that has the scope
Child Scopelist ID	SCPLIST in logonid record; if ruleset, then %CHANGE+RCLASS+$KEY or %RCHANGE+RCLASS+$KEY	The acid that the PARENT_SCOPEID has scope over
Scopelist ID	SCPLIST in logonid record; if ruleset, then %CHANGE+RCLASS+$KEY or %RCHANGE+RCLASS+$KEY	The acid that has the scope
Scope Record ID	SCPLIST in logonid record; if ruleset, then %CHANGE+RCLASS+$KEY or %RCHANGE+RCLASS+$KEY	ACID name
Authorization ID	logonid, %CHANGE, %RCHANGE in ruleset	Acid that has scope over the AUTHID
Authorization Object Type	If the authorization id is a logonid or XREF role, set this value to 'U' If the authorization id is a UID, set this value to 'R'	U/R/V/D/Z for User/Permit/Division/Department/Zone
Scopelist ID	Scope record name Limits: 1 to 8 characters	The acid that has the scope
Next Scopelist ID	NEXTKEY in scope record	The acid that the SCOPEID has scope over

CA Chorus	CA ACF2	CA Top Secret
Scope Record ID	Scope record name Limits: 1 to 8 characters	n/a
UID Mask	UID in scope record	n/a
Scopelist ID	SCPLIST in logonid record; if ruleset, then %CHANGE+RCLASS+$KEY or %RCHANGE+RCLASS+$KEY	DEPARTMENT
User Mask	LID in scope record	User acid residing in the department
Resource Class	If the scope is based on rules, see $TYPE or set to 'DATASET'. If the SCOPE is scope record-based, see the DSN field or INF field	Resource class
Resource Mask	DSN, INF in scope record	Resource name
Resource Mask Type	= ['K' or 'F'] for values specified in $KEY, %CHANGE and %RCHANGE, = ['P', 'K', 'F'] for values specified in DSN, INF in scope record	P = prefix vs F = fully qualified
Scope Type	'S' = SCPLIST in logonid record, 'C' = %CHANGE in ruleset, 'R' = %RCHANGE in the ruleset	n/a
Application Indicator	A for ACF2 Application	T for TSS Application
TSS Facility Name	n/a	FACILITY
TSS Facility Authorization Sequence Number	n/a	Sequence number
TSS Authorization Object Type	n/a	U/R/V/D/Z for User/Permit/Division/Department/Zone
TSS Processing Mode	n/a	MODE (D/W/I/F = Dormant/Warn/Impl/Fail)
TSS Denies Access Indicator	n/a	ACTION DENY
TSS ACID Audit Indicator	n/a	ACTION AUDIT
TSS ACID Notify Indicator	n/a	ACTION NOTIFY
TSS Fail Mode Indicator	n/a	ACTION FAIL
TSS Access Expiration Date	n/a	Expire date Limits: Date field.

CA Chorus	CA ACF2	CA Top Secret
TSS Allow Multi-Signon Indicator	n/a	SIGNMULTI
Day Restriction	n/a	DAY or CALENDAR record
Time Restriction	n/a	TIME or TIMEREC
TSS LINUX System ID	n/a	Linux UID (from LNXENTS keyword)
TSS LINUX Home Directory	n/a	Linux Home (from LNXENTS keyword)
TSS LINUX Shell Program	n/a	Linux shell (from LNXENTS keyword)
TSS LINUX Group	n/a	Group (from LNXENTS keyword)
TSS Number Minutes before Lock	n/a	LOCK TIME
Group ID	n/a	Group acid name
Linux GID	n/a	Linux GID from LNXENTS
TSS Command Restriction	n/a	COMMAND (Displayed as LCF FAC)
TSS Command Allowed	n/a	Command
TSS Command Masked Indicator	n/a	COMMAND Mask
TSS Allow Password Command Access Indicator	n/a	Verify Password if command used
TSS Available Transaction Name	n/a	Transaction
Facility System Sequence	n/a	Sequence number
Facility System ID	n/a	SYSID of the system on which the user can access the facility
Security Application	= 'CA ACF2'	Application name (Security product)
Application Version	ACCREL#, ACCPIDS, ACCPIDL from ACCVT	Version of the product
Operational Mode	ACCMABN, ACCMWRN, ACCMLG, ACCMWRN from ACCMFLG flag bits in ACCVT	MODE (D/W/I/F = Dormant/Warn/Impl/Fail)
Load Date	TOD stamp when the CIA UNLOAD job was executed	Date

CA Chorus	CA ACF2	CA Top Secret
UID String	The Logonid fields that make up the UID string	n/a
User ID	The ACF2 Logonid value	ACID
Create Date	Logonid field name = CRE-TOD - Date and time the Logonid was created Limits: The format varies depending on the DATE field of the GSO OPTS record.	CREATED
Create Time	Logonid field name = CRE-TOD - Date and time the Logonid was created Limits: The format varies depending on the DATE field of the GSO OPTS record.	CREATED
Name	Logonid field name = NAME - The 1 to 20 character name of the user	NAME
Default Group	Logonid field name = GROUP - The default OMVS group name Limits: 1 to 8 characters	DFLTGRP
Last Used Date	Logonid field name = ACC-DATE - The date of the last system access by this user Limits: The format varies depending on the DATE field of the GSO OPTS record.	LAST MOD
Last Used Time	Logonid field name = ACC-TIME - The time of the last system access by this user Limits: Four-byte binary field, displayed in the format *hh.mm.*	LAST MOD
Console	Logonid field name = CONSOLE - Permits access to the TSO/E CONSOLE facility	CONSOLE
Suspended	Logonid field name = SUSPEND - Indicates that a user cannot enter this logonid to access the system	SUSPEND
Trace	Logonid field name = TRACE - Creates SMF loggings for all data set and resource access attempts made by the user	TRACE

CA Chorus	CA ACF2	CA Top Secret
Activated	Logonid field name = ACTIVE - Activates the logonid one minute after midnight on the date contained in this field Limits: The format varies depending on the DATE field of the GSO OPTS record.	n/a
Expiration Date	Logonid field name = EXPIRE - Indicates when the privileges for this logonid will expire Limits: The format varies depending on the DATE field of the GSO OPTS record.	Expiration date that is set from FOR or UNTIL
LDAP Synchronization	Logonid field name = LDS - Administrative logonid changes will be propogated to all active LDAP servers	LDS
EIM Record Identifier	Identifies the LDAPBIND profile record that contains the bind information for the application	EIMPROF
LDS Record Identifier	Logonid field name = LDSNODES - Specifies a GSO NODELIST record ID qualifier Limits: 8 characters	Acid name that has the LDAPDEST node
Proxy Record Identifier	PROXY User Profile Record ID - Specifies information that the z/OS LDAP server will use when acting as a proxy on behalf of a requester	EIMPROF
Source ID	Logonid field name = SOURCE - The logical or physical input source name or source group name (E(SRC), E(SGP), or X(SGP) record name) from which a user must access the system Limits: 1 to 8 characters	SOURCES
Time Zone	Logonid field name = ZONE - The name of the zone record that defines the time zone from which this logonid normally accesses the system Limits: 3 characters	TZONE
Global identifier	n/a	IDMAP
Default Command	n/a	TSOCOMMAND
Default Destination	Logonid field name = TSO-DEST - Specifies the default remote destination for TSO spun SYSOUT data sets	TSODEST

CA Chorus	CA ACF2	CA Top Secret
Hold Class	Logonid field name = DFT-SUBH - The default TSO submit hold class Limits: 1 character	TSOHCLASS
Job Class	Logonid field name = DFT-SUBC - The default TSO submit class Limits: 1 character	TSOJCLASS
Message Class	Logonid field name = DFT-SUBM - The default TSO submit message class Limits: 1 character	TSOMCLASS
Sysout Class	Logonid field name = DFT-SUBM - The default TSO SYSOUT class	TSOSCLASS
Multi password	n/a	TSOMPW
OID Card Required	Logonid field name = OID - An OID card is required	TSOOPT(OIDCARD)
User Data	n/a	TSOUDATA
Account Number	Logonid field name = TSOACCT - Default TSO logon account Limits: 40 characters	TSOLACCT
Mail	Logonid field name = MAIL - User can receive mail messages from TSO at logon time Limits: Bit field	TSOOPT(MAIL)
Notices	Logonid field name = NOTICES - User can receive TSO notices at logon time Limits: Bit field	TSOOPT(NOTICES)
Default Performance group	Logonid field name = TSOPERF - User's default TSO performance group Limits: 1-byte binary field	TSOPRFG
Default Proc	Logonid field name = TSOPROC - User's default TSO procedure name Limits: 8 characters	TSOLPROC
Region Size	Logonid field name = TSORGN - User's default TSO region size Limits: 4-byte binary field	TSOLSIZE
Max Region Size	Logonid field name = TSOSIZE - User's maximum TSO region size Limits: 4-byte binary field	TSOMSIZE

CA Chorus	CA ACF2	CA Top Secret
Unit Name	Logonid field name = TSOUNIT - User's default TSO unit name Limits: 8 characters	TSOUNIT
USS User ID	P(USER) DIV(OMVS) UID field	UID
Home Directory	P(USER) DIV(OMVS) HOME field	HOME
Shell Path	P(USER) DIV(OMVS) OMVSPGM field	OMVSPGM
MAXASSIZE	P(USER) DIV(OMVS) ASSIZE field	ASSIZE
MAXMMAPAREA	P(USER) DIV(OMVS) MMAPAREA field	MMAPAREA
MAX CPU	P(USER) DIV(OMVS) CPUTIME field	OECPUTM
MAXFILEPROC	P(USER) DIV(OMVS) FILEPROC field	OEFILEP
Nonshared MaxMem	P(USER) DIV(OMVS) MEMLIMIT field	MEMLIMIT
Shared Memory MAX	P(USER) DIV(OMVS) SHMEMMAX field	SHMEMMAX
MAXPROCUSER	P(USER) DIV(OMVS) PROCUSER field	PROCUSER
MAXTHREADS	P(USER) DIV(OMVS) THREADS field	THREADS
Lotus Notes ID	P(USER) DIV(LNOTES) record id	SNAME
NDS ID	P(USER) DIV(NDS) UNAME field	UNAME
UUID	P(USER) DIV(DCE) UUID field	UUID
Principal DCE Name	P(USER) DIV(DCE) DCENAME field	DCENAME
Home UUID	P(USER) DIV(DCE) HOMEUUID field	HOMEUUID
HomeCell	P(USER) DIV(DCE) HOMECELL field	HOMECELL
Autolog	P(USER) DIV(DCE) AUTOLOG field	AUTOLOG
Init Cmd	P(USER) DIV(NETVIEW) IC field	NETVIC
Console ID	P(USER) DIV(NETVIEW) CONSNAME field	SYSCONS
Security Check	P(USER) DIV(NETVIEW) SECCTL field	n/a
Receive Messages	P(USER) DIV(NETVIEW) MSGRECVR field	n/a
GMF Admin	P(USER) DIV(NETVIEW) NGMFADMN field	n/a
Autolog All	Logonid field name = AUTOALL Limits: Bit field	n/a
Autolog No PWD	Logonid field name = AUTONOPW Limits: Bit field	n/a

CA Chorus	CA ACF2	CA Top Secret
Autolog Only	Logonid field name = AUTOONLY Limits: Bit field	n/a
Diag 84	Logonid field name = DG84DIR Limits: Bit field	n/a
DIAL Bypass	Logonid field name = DIALBPY Limits: Bit field	n/a
Optional Group ID	Logonid field name = GRP-OPT Limits: Bit field	n/a
Last User	Logonid field name = GRP-USER Limits: 8 characters	n/a
Group Logon	Logonid field name = GRPLOGON Limits: Bit field	n/a
Logical Devices	Logonid field name = LDEV Limits: Bit field	n/a
No Spool	Logonid field name = NOSPOOL Limits: Values listed in PREVENT, LOG, ALLOW, and null.	n/a
CP Syntax Check	Logonid field name = SYNERR Limits: Values listed in PREVENT, LOG, ALLOW, and null.	n/a
TempDisk Rules	Logonid field name = TDISKVLD Limits: Bit field	n/a
VM Account	Logonid field name = VLDVMACT Limits: Bit field	n/a
Default Account Number	Logonid field name = VMACCT Limits: 8-byte logonid field	n/a
Diag D4	Logonid field name = VMD4AUTH Limits: Bit field	n/a
D4 CMS	Logonid field name = VMD4FSEC Limits: Bit field	n/a
Reset	Logonid field name = VMD4RSET Limits: Bit field	n/a
Diag D4 Alternate	Logonid field name = VMD4TARG Limits: Bit field	n/a

CA Chorus	CA ACF2	CA Top Secret
VM Idle Time	Logonid field name = VMIDLEMN Limits: 1 to 240 minutes	n/a
Idle Processing	Logonid field name = VMIDLEOP Limits: Valid values are OFF, DISC, LOGOFF, NOLOGOFF, or REPROMPT	n/a
VM ESM	Logonid field name = VMESM Limits: Bit field	n/a
Diag A0 (SAF)	Logonid field name = VMSAF Limits: Bit field	n/a
VM SFS Server	Logonid field name = VMSFS Limits: Bit field	n/a
VM/ESA Logon	Logonid field name = VMXA Limits: Bit field	n/a
VSE SRF	Logonid field name = VSESRF Limits: Bit field	n/a
Acid Type	n/a	MSCA/SCA/LSCA/ZCA/DCA/VCA/USER
Suspended (admin)	n/a	ASUSPEND
Suspended (password)	n/a	PSUSPEND
Suspended (Resources)	n/a	VSUSPEND
Suspended (Exit)	n/a	XSUSPEND
User Last Accessed Sysid	n/a	CPU on last used
Batch or STC control	n/a	MASTFAC
ID Card	n/a	TSOOPT(OIDCARD)
Telephone	Logonid field name = PHONE Limits: 1 to 12 character telephone number	n/a
Audit	Logonid field name = AUDIT Limits: Bit field	n/a
Account	Logonid field name = ACCOUNT Limits: Bit field	n/a
Consult	Logonid field name = CONSULT Limits: Bit field	n/a

CA Chorus	CA ACF2	CA Top Secret
Leader	Logonid field name = LEADER Limits: Bit field	n/a
REFRESH Command Allowed	Logonid field name = REFRESH Limits: Bit field	n/a
Security	Logonid field name = SECURITY Limits: Bit field	n/a
No Cancel	Logonid field name = NON-CNCL Limits: Bit field	n/a
RX all DSNs	Logonid field name = READALL Limits: Bit field	n/a
Resource Validation Needed	Logonid field name = RSRCVLD Limits: Bit field	n/a
Access Validation Needed	Logonid field name = RULEVLD Limits: Bit field	n/a
Last Accessed Source	Logonid field name = ACC-SRCE Limits: 1 to 8 character source name source name or source group name	n/a
Day Restriction	Logonid field name = SHIFT Limits: 1 to 8 characters	DAYS
Time Restriction	Logonid field name = SHIFT Limits: 1 to 8 characters	TIMES
Number of Accesses	Logonid field name = ACC-CNT Limits 4-byte binary field	n/a
TSO Account Priv	Logonid field name = ACCTPRIV Limits: Bit field	n/a
ACF CICS	Logonid field name = CICS Limits: Bit field	n/a
Bypass Restricted Command	Logonid field name = ALLCMDS Limits: Bit field	n/a
Command Limiting	Logonid field name = ATTR2 Limits: 2-byte hexadecimal field	n/a
Extended Authentication 1	Logonid field name = AUTHSUP1 Limits: Bit field	n/a

CA Chorus	CA ACF2	CA Top Secret
Extended Authentication 2	Logonid field name = AUTHSUP2 Limits: Bit field	n/a
Extended Authentication 3	Logonid field name = AUTHSUP3 Limits: Bit field	n/a
Extended Authentication 4	Logonid field name = AUTHSUP4 Limits: Bit field	n/a
Extended Authentication 5	Logonid field name = AUTHSUP5 Limits: Bit field	n/a
Extended Authentication 6	Logonid field name = AUTHSUP6 Limits: Bit field	n/a
Extended Authentication 7	Logonid field name = AUTHSUP7 Limits: Bit field	n/a
Extended Authentication 8	Logonid field name = AUTHSUP8 Limits: Bit field	n/a
Auto SVC Dump	Logonid field name = AUTODUMP Limits: Bit field	n/a
BDT	Logonid field name = BDT Limits: Bit field	n/a
ACF2 Cancel	Logonid field name = CANCEL Limits: Bit field	n/a
TSO Delete Character	Logonid field name = CHAR Limits: 1-byte binary field, or one of these special strings: BS or NO	n/a
CICS Authority	CICS|NOCICS in logonid record Limits: Bit field	n/a
CICS Operator Class	CICSCL(class) in logonid record Limits: 3-byte hexadecimal field	n/a
CICS Operator ID	CICSID(id) in logonid record Limits: 3 characters	n/a
CICS Operator Priority	CICSPRI(class) in logonid record Limits: 1-byte binary field	n/a
C-CIC Sysid	CICSOPT(cicsopt) in logonid record Limits: 8 characters	n/a

CA Chorus	CA ACF2	CA Top Secret
TSO Command List Bypass	CMD-LONG|NOCMD-LONG in logonid record Limits: Bit field	n/a
SET TARGET	CMD-PROP|NOCMD-PROP in logonid record Limits: Bit field	n/a
Date of CANCEL	CSDATE(date) in logonid record Limits: The format varies depending on the DATE field of the GSO OPTS record.	n/a
CANCEL Logon ID	CSWHO(logonid) in logonid record Limits: 8 characters	n/a
TSO Prefix	DFT-PFX(prefix) in logonid record Limits: 8 characters, but the last character is reserved	n/a
Dump Authorized	DUMPAUTH|NODUMPAUTH in logonid record Limits: Bit field	n/a
Terminal Idle Time	IDLE(time) in logonid record Limits: 1-byte binary field	n/a
IMS	IMS|NOIMS in logonid record Limits: Bit field	n/a
Accept TSO Send	INTERCOM|NOINTERCOM in logonid record Limits: Bit field	n/a
Submit Allow	JCL|NOJCL in logonid record Limits: Bit field	n/a
Batch Logon ID	JOB|NOJOB in logonid record Limits: Bit field	n/a
Use JOBFROM	JOBFROM|NOJOBFROM in logonid record Limits: Bit field	n/a
Kerberos Violations	KERB-VIO in logonid record Limits: 2-byte binary field	n/a
TSO Line delete character	LINE(char) in logonid record Limits: 1 character, or one of these special strings:ATTN, CTLX, or NO	n/a

CA Chorus	CA ACF2	CA Top Secret
MAXDAYS LID	LIDZMAX|NOLIDZMAX in logonid record Limits: Bit field	n/a
MINDAYS LID	LIDZMIN|NOLIDZMIN in logonid record Limits: Bit field	n/a
Account Permission	LGN-ACCT|NOLGN-ACCT in logonid record Limits: Bit field	n/a
Remote DEST Permission	LGN-DEST|NOLGN-DEST in logonid record Limits: Bit field	n/a
Logon Message Class Specify	LGN-MSG|NOLGN-MSG in logonid record Limits: Bit field	n/a
Performance Group Specify	LGN-PERF|NOLGN-PERF in logonid record Limits: Bit field	n/a
TSO PROC Specify	LGN-PROC|NOLGN-PROC in logonid record Limits: Bit field	n/a
Recover option allow	LGN-RCVR|NOLGN-RCVR in logonid record Limits: Bit field	n/a
Override Region Size	LGN-SIZE|NOLGN-SIZE in logonid record Limits: Bit field	n/a
Set Session Limit permission	LGN-TIME|NOLGN-TIME in logonid record Limits: Bit field	n/a
Set TSO Unit Permission	LGN-UNIT|NOLGN-UNIT in logonid record Limits: Bit field	n/a
Access off shift	LOGSHIFT|NOLOGSHIFT in logonid record Limits: Bit field	n/a
Bypass Rules	MAINT|NOMAINT in logonid record Limits: Bit field	n/a

CA Chorus	CA ACF2	CA Top Secret
Max days between Password change	MAXDAYS(days) in logonid record Limits: 1-byte hexadecimal field	n/a
Min days before Password change	MINDAYS(days) in logonid record Limits: 1-byte hexadecimal field	n/a
Modal Messages from TSO	MODE|NOMODE in logonid record Limits: Bit field	n/a
Log SMF Record	MON-LOG|NOMON-LOG in logonid record Limits: Bit field	n/a
Send Logon to Console	MONITOR|NOMONITOR in logonid record Limits: Bit field	n/a
Mount permission	MOUNT|NOMOUNT in logonid record Limits: Bit field	n/a
Prefix message ID	MSGID|NOMSGID in logonid record Limits: Bit field	n/a
Multi signon privs	MULTSIGN|NOMULTSIGN in logonid record Limits: Bit field	n/a
Logon Single AS	MUSASS|NOMUSASS in logonid record Limits: Bit field	n/a
Logon Multi AS	MUSDLID(logonid) in logonid record Limits: 8 characters	n/a
Multi-user ID	MUSID(musid) in logonid record Limits: 1 to 8 characters	n/a
MUSID Required	MUSIDINF|NOMUSIDINF in logonid record Limits: Bit field	n/a
MUSASS Privilege	MUSUPDT|NOMUSUPDT in logonid record Limits: Bit field	n/a
Network Can't Inherit	NO-INH|NONO-INH in logonid record Limits: Bit field	n/a

CA Chorus	CA ACF2	CA Top Secret
No MAXVIO	NOMAXVIO|NONOMAXVIO in logonid record Limits: Bit field	n/a
NO USS	NO-OMVS|NONO-OMVS in logonid record Limits: Bit field	n/a
Bypass SMC	NO-SMC|NONO-SMC in logonid record Limits: Bit field	n/a
MUSASS Statistics Bypassed	NO-STATS|NONO-STATS in logonid record Limits: Bit field	n/a
No Store or Delete Rule Sets	NO-STORE|NONO-STORE in logonid record Limits: Bit field	n/a
TSO Operator	OPERATOR|NOOPERATOR in logonid record Limits: Bit field	n/a
Pause on Multi Clist	PAUSE|NOPAUSE in logonid record Limits: Bit field	n/a
Account Number Required at Logon	PMT-ACCT|NOPMT-ACCT in logonid record Limits: Bit field	n/a
TSOPROC Required At Logon	PMT-PROC|NOPMT-PROC in logonid record Limits: Bit field	n/a
Submit Program	PROGRAM(program) in logonid record Limits: 8 characters	n/a
GSO PPGM Execute	PPGM|NOPPGM in logonid record Limits: Bit field	n/a
Log SMF Active on Attempt	PP-TRC|NOPP-TRC in logonid record Limits: Bit field	n/a
Log SMF Active on Violation	PP-TRCV|NOPP-TRCV in logonid record Limits: Bit field	n/a
Rule Prefix	PREFIX(prefix) in logonid record Limits: 0 to 8 characters	n/a

CA Chorus	CA ACF2	CA Top Secret
Dynamic Logonid Privileges	PRIV-CTL|NOPRIV-CTL in logonid record Limits: Bit field	n/a
Prompt on invalid parms	PROMPT|NOPROMPT in logonid record Limits: Bit field	n/a
Cumulative password violations	PSWDCVIO(nn) in logonid record Limits: 2-byte binary field	n/a
Date of Last Invalid Password	PSWD-DAT(date) in logonid record Limits: 4-byte packed field	n/a
Password Expired Manually	PSWD-EXP|NOPSWD-EXP in logonid record Limits: Bit field	n/a
Number password violations since last logon	PSWD-INV(nn) in logonid record Limits: 2-byte binary field	n/a
Last Input Source Name/Group with Invalid Password	PSWD-SRC(sourceid) in logonid record Limits: 8 characters	n/a
Time of Last Invalid Password	PSWD-TIM(hh:mm) in logonid record Limits: 4-byte binary field	n/a
Max Password Length 8	PSWD-MX8 in logonid record	n/a
Password Change Date	Date section of the PSWD-TOD field in logonid record	n/a
Password Change Time	Time section of the PSWD-TOD field in logonid record	n/a
Password Uppercase	PSWD-UPP|NOPSWD-UPP in logonid record Limits: Bit field	n/a
Number of Password Violations	PSWD-VIO(nn) in logonid record Limits: 2-byte binary field	n/a
APF Decrypt Only	PSWD-XTR|NOPSWD-XTR in logonid record Limits: Bit field	n/a
GSO allow	PWPALLOW|NOPWPALLOW in logonid record Limits: Bit field	n/a

CA Chorus	CA ACF2	CA Top Secret
Last Invalid Password Date	PWP-DATE(date) in logonid record Limits: 4-byte packed field	n/a
Number of Passphrase Violations	PWP-VIO(count) in logonid record Limits: 2-byte binary field	n/a
Passticket RESTRICT	PTICKET|NOPTICKET in logonid record Limits: Bit field	n/a
TSO Recover	RECOVER|NORECOVER in logonid record Limits: Bit field	n/a
RESTRICT Logon	RESTRICT|NORESTRICT in logonid record Limits: Bit field	n/a
Restrict UNIX	RSTDACC|NORSTDACC in logonid record Limits: Bit field	n/a
Scoped	= 'Y' if any of the following fields in the logonid record are nonblank: DSNSCOPE(logonid mask), LIDSCOPE(logonid mask), SCPLIST(scpname), UIDSCOPE(UID mask)	n/a
Cumulative Violations	SEC-VIO(nn) in logonid record Limits: 2-byte binary field	n/a
SRF for VM	SRF|NOSRF in logonid record Limits: Bit field	n/a
Logon for STC	STC|NOSTC in logonid record Limits: Bit field	n/a
Submit APF only	SUBAUTH|NOSUBAUTH in logonid record Limits: Bit field	n/a
Sync Node	SYNCNODE(nodeid) in logonid record Limits: 8 characters	n/a
Sysplex	SYSPEXCL|NOSYSPEXCL in logonid record Limits: Bit field	n/a
Bypass Label	TAPE-BLP|NOTAPE-BLP in logonid record Limits: Bit field	n/a
Limited Bypass Label	TAPE-LBL|NOTAPE-LBL in logonid record Limits: Bit field	n/a

CA Chorus	CA ACF2	CA Top Secret
TSO logon	TSO|NOTSO in logonid record Limits: Bit field	n/a
TSO Trace	TSO-TRC|NOTSO-TRC in logonid record Limits: Bit field	n/a
TSO Command List Module	TSOCMDS(module) in logonid record Limits: 8 characters	n/a
Full Screen Display Logon	TSOFSCRN|NOTSOFSCRN in logonid record Limits: Bit field	n/a
Mail Index Record Pointer	TSORBA(pointer) in logonid record Limits: 3-byte hexadecimal field	n/a
TSO Time	TSOTIME(time) in logonid record Limits: 2-byte binary field	n/a
Common Services	UNICNTR|NOUNICNTR in logonid record Limits: Bit field	n/a
Logon ID Update Date	Date section of the UPD-TOD(date-time) field in logonid record	n/a
Logon ID Update Time	Time section of the UPD-TOD(date-time) field in logonid record	n/a
Validate TSO account number	VLD-ACCT|NOVLD-ACCT in logonid record Limits: Bit field	n/a
Validate TSO Proc Name	VLD-PROC|NOVLD-PROC in logonid record Limits: Bit field	n/a
Validate SUBAUTH/PROGRAM	VLDRSTCT|NOVLDRSTCT in logonid record Limits: Bit field	n/a
VM Logon permit	VM|NOVM in logonid record Limits: Bit field	n/a
ACF uses WTP	WTP|NOWTP in logonid record Limits: Bit field	n/a
System ID	n/a - Supplied as input to the CIA UNLOAD JCL job	SYSID
User ID	n/a	Acid name

CA Chorus	CA ACF2	CA Top Secret
Group Name	n/a	Group name
USS GID	n/a	GID
SMS Application Name	n/a	SMS Application name Limits: 8 characters
SMS Data Class	n/a	SMS Data Class Limits: 8 characters
SMS Management Class	n/a	SMS Management Class Limits: 8 characters
SMS Storage Class	n/a	SMS Storage Class Limits: 8 characters
User ID	logonid	n/a
Hex UID	UID in hex format	n/a
UID	UID	n/a
User ID	logonid	Acid that has the profile
Role ID	ROLENAME part of the X-ROL Record Id if the ROLETYPE is a role group (g) or base role (r), UID mask from rulelines if the ROLETYPE is a UID string (u)	Profile acid name
Record System ID	SYSID part of the X-ROL Record Id if the ROLETYPE is a role group (g) or base role (r)	n/a
Role Type	= 'U' if this is a uid mask is from a ruleline; = 'R' if this is a role from an X-ROL record; = 'G' if this is a role group from an X-ROL record	= 'P' if a Top Secret Profile
ESM System ID	Supplied as input parm in the CIA UNLOAD job or defaults to the SMCASID (the z/OS SMFID) where the CIA UNLOAD job was executed	The CIA SYSID
Expiration Date	n/a	Expiration date of the profile use on the acid Limits: Date field
Role Order	n/a	Which profile it is on the acid
Event System ID	Supplied as input parm in the CIA UNLOAD job or defaults to the SMCASID (the z/OS SMFID) where the CIA UNLOAD job was executed	LPAR

CA Chorus	CA ACF2	CA Top Secret
ACF2 Sysid	Supplied as input parm in the CIA UNLOAD job or defaults to the SMCASID (the z/OS SMFID) where the CIA UNLOAD job was executed	Date database created
Timestamp	n/a	Time at which the database was last updated