

CA Cleanup r12

CA Cleanup reduces the effort and pressure associated with maintaining current regulatory, statutory and audit requirements. It does this by removing obsolete, unused, redundant and excessive access rights through easily automated, virtually unattended and continuous cleanup of mainframe security databases CA ACF2™, CA Top Secret® and IBM RACF.

Business Value

CA Cleanup automates two labor-intensive tasks that plague security administrators: creating security commands to remove obsolete IDs or access, and creating commands to restore what was removed. When using CA Cleanup, you can easily identify active and inactive user IDs, profiles and permissions, as well as user-defined resource classes. When the standard monitoring report is executed from the tracking file, the commands can automatically be produced, but you choose when to execute the cleanup – and what is actually cleaned up.

Product Overview

Information security and personal information privacy are at the core of many federal regulations and consumer privacy requirements. Organizations face potentially significant security exposures when unused and obsolete user IDs — and entitlement definitions that may be valid, but are inappropriate for individuals' roles — accumulate in mainframe security databases. This build-up also hampers operating and security system performance, administrator productivity and audit effectiveness. CA Cleanup independently and passively monitors the security system for these problems.

Delivery Approach

CA Services provides a portfolio of mainframe services delivered through CA internal staff and a network of established partners chosen to help you achieve a successful deployment and get the desired business results as quickly as possible. Our standard service offerings are designed to speed deployment and accelerate the learning curve for your staff. CA's field-proven mainframe best practices and training lower risk, improve use/adoption and ultimately align the product configuration to your business requirements.

What's New, What's Compelling?

Mainframe 2.0

CA Cleanup has adopted key Mainframe 2.0 features that are designed to simplify your use of CA Cleanup and enable your staff to install, configure and maintain it more effectively and quickly.

- **CA Mainframe Software Manager:** The CA Mainframe Software Manager automates CA Cleanup installation and maintenance and removes SMP/E complexities.
 - › The Software Acquisition Service enables you to easily move product installation packages and maintenance from CA Support Online directly to your mainframe environment and prepare them for installation.
 - › The Software Installation Service standardizes CA Cleanup installation, which includes a new, streamlined Electronic Software Delivery (ESD) method that allows CA Cleanup to be installed using standard utilities. This service also provides standardized SMP/E product installation and maintenance via APARs and PTFs, and simplifies SMP/E processing through an intuitive graphical user interface and an intelligent Installation Wizard.
- **Best Practices Guide:** This guide provides information on CA Cleanup installation, initial configuration and deployment to shorten the learning curve for staff that is responsible for the installation and management of this product.
- **Interoperability Certification:** CA Cleanup has been tested in an environment with many other CA products as part of a dedicated effort to find and resolve interoperability problems prior to release.

Features

CA Cleanup provides:

- **Continuous 24x7 Monitoring:** CA Cleanup executes continuously, monitoring your security system activity 24x7 to record the actual security definitions that the system is or is not using. It is important to remember that manual cleanup costs and efforts recur on each review for each security definition. An individual cannot be expected to perform such reviews full-time and nonstop. CA Cleanup runs all the time, largely unattended and can be deployed for monitoring in less than a day.
- **Enhanced Security Recertification:** CA Cleanup monitors security activity and can identify used and unused access for any user or application. With the cleanup process, procedures can be shifted in their focus from “flag what to remove” to “flag what to keep.” Recertification procedures can now state that unused access will be removed unless claimed as valid.
- **Non-employee/Non-human (Process) IDs:** Such system process IDs as vendors, partners, contractors/consultants that are used for batch jobs, started tasks, CICS, terminal, FTP and others are rarely cleaned up. These IDs often pose the greatest threat because they can be highly authorized, privileged with bypass security options, require no password and are commonly known (for example, IBMUSER, OMVS, JES and others). While this area is often judged as too sensitive and difficult for manual cleanup, these IDs pose no challenge for CA Cleanup and require no special handling. It will detect and remove these IDs with an option to initially suspend. By generating contingency commands for everything flagged for deletion, IDs that may need to be restored can be recreated on demand.

- **System and Administrative Overhead Reduction:** When security files contain unused user IDs and access rights, the need and cost of overhead for both the system and the administrator increase. CA Cleanup removes unused access rights and IDs from the security system, improving performance and productivity.
- **Report Generator:** CA Cleanup provides a batch utility program that enables you to produce reports for specific purposes. You can specify what criteria are to be used from the tracking file to produce reports, with the values indicating the number of days since an item was referenced in the tracking file. For example, you can specify values to produce a report on resources that have not been referenced in 170 days.
- **Command Generation to Perform or Restore Cleanup:** Creating security commands to remove obsolete IDs or access is a labor-intensive cleanup task – as is creating commands to restore what was removed. CA Cleanup automates both of these tasks for you.
- **Efficient Cleanup:** When using CA Cleanup, you can identify active and inactive logon IDs, rule sets and rules, including user-defined resource classes and NEXTKEY source and target rules. When the standard monitoring report is executed from the tracking file, the commands can be automatically produced. However, even though CA Cleanup creates the command to perform cleanup automatically, it remains your choice as to when cleanup occurs and what is actually cleaned up.
- **Built-in Contingency and Back Out:** In many cases, manually performing cleanup will not include creating commands to rebuild IDs or restore access to its state before deletion. When CA Cleanup creates the commands to enact cleanup, it also recreates the original ID or access.
- **Remote Synchronized Environment:** CA Cleanup supports the processing of multiple concurrent databases to maintain synchronization.
- **Multiple Remote Security Database Capability:** CA Cleanup performs a correlation and produces a collective composite report based on usage across all of your security databases. This means that a user ID or user access right in one location will not be targeted for cleanup unless it is unused across all locations.
- **Role-based Reorganization and Process Support:** CA Cleanup can reorganize and restructure your security file to a role-based structure, identifying both obsolete and active access rights. Active rights can be moved to newer, smaller, reorganized rule sets or groups that match your role-based structure. You can continue to monitor these user IDs and the access rights to help ensure proper setup.

Benefits

CA Cleanup (CA Cleanup for ACF2™, CA Cleanup for Top Secret® and CA Cleanup for RACF) helps you comply with many regulations and laws requiring due diligence to information security, protection and privacy. Additionally, you can use it to:

- Improve security control
- Manage administration costs
- Increase risk mitigation
- Enhance privacy control
- Improve ease of audit
- Increase system performance

Why CA

A key component of both CA's Mainframe 2.0 initiative and Enterprise IT Management (EITM) strategy, CA Cleanup is just one of many CA products and solutions that can help you unify and simplify the management of complex computing environments across the entire enterprise. CA Cleanup provides continuous controls to help you meet your business and compliance requirements and – when combined with CA's mainframe and distributed security solutions – enables end-to-end system security and peace of mind.

Copyright © 2009 CA. All rights reserved. z/OS, RACF and CICS are trademarks of International Business Machines Corporation in the United States, other countries, or both. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. This document is for your informational purposes only. CA assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, CA provides this document "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 for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, goodwill or lost data, even if CA is expressly advised in advance of the possibility of such damages.

315250509