# 2.5 Vanguard Product Enhancements



VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# Contents





VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# Vanguard Security Solutions (VSS)

• Modified the VSS Main Menu online process to handle invocation of Vanguard Compliance Manager. If VCM is not installed, an error message will be displayed indicating this fact.

• Added a new member named VSSSPF to the Vanguard Sample Library (VANSAMP). It allows for the concatenation of all Vanguard Security Solutions libraries, VANxxxx and VCMxxxx libraries.

• **Updated the following members in VANSAMP:**

- VRASPF - Removes reference about invoking the VSS procedure.
- VCMSPF - Reflects the VCM data set naming conventions.

## Benefit

Improved functionality with updated VANSAMP members.

# Vanguard Administrator

**Clone User ALIAS Enhancement to Replace CMDEXIT**

## Description

- Added a new ALIAS option to the Clone User command panel, as well as the option to select a User Catalog entry.
- If the new ALIAS methodology is not implemented, the DEFINE ALIAS process will continue to function via CMDEXIT.

## Benefit

Vanguard Administrator now supports the automated ALIAS option to generate the ALIAS command when the Clone User feature is invoked, online and batch. This enhancement eliminates the need to execute the CMDEXIT procedure after a Clone User is performed.

# Vanguard Administrator

**Criteria Name and Value for General Resource Conditional Access Support 'SERVICE' as a New Criteria Name**

## Description

- Vanguard Administrator reporting and command generation now support this new feature, including Security Server Commands option.

## Benefit

Vanguard Administrator facilitates the creation, modification and reporting of Conditional Access Criteria entries and current Criteria Names including SERVICE.

# Vanguard Administrator

**Profile Segment Reports now Support Resource CSDATA Segment**

## Description

- Added CSDATA segment option to the Profile Segment Reports for General Resources. Related information will be displayed as well as generated for applicable commands such as Clone, Rebuild and Delete. These features are available in online and batch modes.

## Benefit

Vanguard Administrator supports the new General Resource CSDATA segment feature and facilitates the administering of profiles and CSDATA segment information. General Resource CSDATA segment is supported across Vanguard Administrator features - online and batch.

# Vanguard Administrator

**DB2 General Resource New Segment Support - CSDATA Segment**

## Description

- Added new General Resource CSDATA segment DB2 table to the Vanguard Administrator DB2 feature.

## Benefit

Same as the above enhancement except added support for General Resource CSDATA segment via DB2 and VRAFLAT Administrator processes.

# Vanguard Administrator

**Added Password and Pass Phrase Encryption Type**

## Description

- Added password encryption support to User Profile Summary and to the LU command.

## Benefit

The Password Encrypt and Pass Phrase Encryption fields have been added to the User Reports panel.

New batch parameters, ENCRYPTPWD and ENCRYPTPHRASE, have been added to the User Profile Report Parameter Descriptions section.

# Vanguard Administrator

**Added a New Column (for ID Status)**

## Description

- Added a new 'IdStatus' column (for ID Status) on the TSO Segment Summary report along with updating its Syntax panel with the following fields: IDSTATUS (Id Status) and SORT(IDSTATUS,A|D).

## Benefit

This allows the security administrator to quickly identify users that have been revoked or inactive and determine any action to be taken in regard to their TSO segment.

# Vanguard Administrator for ACF2

**LIDs in Rules Enhancement**

## Description

Added a new LID in Rules Report section, which allows you to locate ACF2 access rules and/or resource rules that can potentially allow the specified LID access. It also contains an Include input section to help define which rule records to evaluate to see if an input LID gains access via a rule entry. This Include input section can generate reports based on the following:

- Dataset Access Rules
- Resources Rules
- UID(*) Rulelines

**Updated the Vanguard ACF2 Administration menu by adding option L for LID in Rules Report.**

## Benefit

The benefit of this enhancement allows you to locate ACF2 access rules and/or resource rules that can potentially allow the specified LID access. The Vanguard ACF2 LID in Rules window contains an Include input section to help define which rule records to evaluate to see if an input LID gains access via a rule entry.

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# Vanguard Administrator for Top Secret

**Introducing Vanguard Administrator for CA Top Secret**

## Description

- Vanguard Administrator for CA Top Secret is an effective administrative tool that provides a wide range of Top Secret security administration, data mining and reporting. VAX allows you to view reports and perform administrative changes to Top Secret ACIDs, Profiles/Groups, Zones/Divisions/Departments and Resource Ownership.

## Benefit

Vanguard Administrator for CA Top Secret makes it easier to report on Top Secret administration.



VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# Vanguard Advisor

**Added Support to Allow Users to Specify a VSROPT00 Parameter of LSNAME(*)**

## Description

- This enhancement removes the requirement to specify whether SMF log streams or traditional MAN data sets are to be used for online processing in Live mode, creating an Extract File or running a batch report or utility. Customers cannot specify LSNAME(*) to indicated that the SMF log streams on the system where Advisor is running are to be automatically identified and used. They can still specify the two-character suffix of the LSNAMExx VIPOPTS member that contains the log stream names. They can omit the LSNAME parameter in which case Advisor will use the SMF log streams or traditional MAN data sets based on the customer's specification of the SMF Recording Mode in their active SMFPRMxx Parmlib member.

## Benefit

This enhancement allows the customer to use the same VSROPT00 VIPOPTS member on multiple systems. It is no longer necessary to setup multiple LSNAMExx VIPOPTS members for each system. System A can have an SMF Recording Mode of DATASET and System B can have an SMF Recording Mode of LOGSTREAM and share the same VSROPT00 VIPOPTS member.

# Vanguard Advisor

**Updated these Advisor Reports: Sensitive Libraries, TCP/IP and Records Special**

## Descriptions

For Sensitive Libraries Reports:
When running the Sensitive Libraries report (online and batch) and APF Libraries is selected, any library in the Link List will be included if it is not in the APF list when LNKAUTH=LNKLST is in effect. This will allow you to see what libraries are automatically APF authorized.

For TCP/IP Reports:
When running TCP/IP reports (online and batch), the Resource Name will be included if it is in the SMF 119 record.

For Records Special Reports:
The RACF Initialization Records Special Report (online and batch) will now display the following information:

- Password History value
- Inactive User ID revoked value
- Password Warning level

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# Vanguard Advisor cont.

- Password Syntax Rules
- MODEL(GDG) setting
- MODEL(USR) setting
- MODEL(GRP) setting
- List Of Groups checking setting

## Benefit

For Sensitive Libraries Reports:

This allows you to identify all of the libraries that are APF authorized.

For TCP/IP Reports:

This enhancement makes the TCP/IP reports more inclusive.

For Records Special Reports:

More RACF environment controls are displayed.

# Vanguard Active Alerts

**Added Support for Active Alert 18 and Active Alert 19**

## Description

Enhanced Active Alerts to send notifications for specific TCP/IP and zERT Initiation (AA18) and Termination (AA19) activity. All Active Alerts and SIEM notification options are available.

Active Alert 18 will send notifications for these events:

- TCP Connection Initiation
- zERT Connection Initiation
- TN3270E Telnet Server SNA Session Initiation
- TSO Telnet Client Connection Initiation
- FTP Server Logon Failure

# Vanguard Active Alerts cont.

Active Alert 19 will send notification for these events:

- TCP Connection Termination
- FTP Client Transfer Completion
- zERT Connection Termination
- TN3270E Telnet Server SNA Session Termination
- TSO Telnet Client Connection Termination
- FTP Server Transfer Completion

**Note:** All Active Alert and SIEM notification options are available.

## Benefit

Customers can now be alerted when TCP/IP sessions are initiated on their system. By using masking, they can identify which characteristics of the session they are interested. The Termination alert allows them to track how long a session was active.

# Vanguard Active Alerts

**Enhanced the VAARTN Started Task Initialization and Notification Performance**

## Description

- Streamlined the VAARTN Task and Notification Initialization process to allow the alert process to be activated quicker.

## Benefit

The Notification process can begin quicker after the VAARTN Task is started.



VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# Vanguard Active Alerts

**Added Support to Include the Event Code and Event Qualifier Code to Alerts 18 and 19 Events**

## Description

- Added Event Name, Event Name Code, Event Qualifier and Event Qualifier Code to Alerts 18 and 19 SIEM records.

## Benefit

This additional information will help users identify what the type of event data is in the record so they can make a more informed decision on what to do with the event data.



VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# Vanguard Active Alerts

**ACF2 Enhancement to Include New Active Alert 8**

## Description

- This alert will see all Logonid Change Activity, Infostorage Change Activity and Rule Change Activity commands. Active Alerts 1-4 only process a subset of the parameters of these commands and do not support user masking.

## Benefit

This Active Alert 8 allows users to customize the command masking criteria so they can send alert notifications based on criteria important to their installation that is not restricted to the criteria for Active Alerts 1-4.

# Vanguard Active Alerts For Splunk

**Introducing Vanguard Active Alerts for Splunk**

## Description

- Vanguard Active Alerts for Splunk is a web-styled dashboard interface that displays events retrieved via Vanguard Active Alerts from SMF records on these External Security Managers (ESM): ACF2, Top Secret and RACF systems.

## Benefit

With this product, you will be able to monitor, search, analyze and visualize active alerts data in real time. Vanguard Active Alerts for Splunk can capture, index and correlate your data and then present it in graphs and alerts on various dashboards.



VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

# Vanguard Cleanup and Vanguard Offline

**Offload Delay Process is Available**

## Description

- Added 'OFFLOAD DELAY' as a new optional keyword in the VCPOPT00 member.

## Benefit

Specifies the minutes for an offload delay. Default is one (1) minute.

**Forced Abend Detection**

## Description

- Enhanced PC recovery to detect forced abnormal terminations.

## Benefit

Improvements made to product productivity and performance

# Vanguard Cleanup and Vanguard Offline

## Event Spiller Function

### Description

Added the Spiller function to retain uncommitted in-flight events during shutdown of the Vanguard Capture started task.
Also, added the following operator commands:

- 'P xxxxx NOUPDATE' is a new Capture shutdown option. It skips the History Master File (HMF) updates during shutdown and retains the spill file.
- 'P xxxxx KEEPSPILL' is a new Capture shutdown option. It performs the History Master File updates during shutdown and retains the spill file.

Updated the VCPOPT00 member by adding 'VCPSPLL' as a new optional keyword. It specifies the spill file name and activates the event spiller function. Added VCPDEFS as a new Vanguard Sample Library (VANSAMP) member.

### Benefit

Improvements made to product productivity and performance.

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS