Access Control 5.3
Pre-Implementation Checklists for Implementation Consultants

Applies to:

Access Control 5.3

Summary

GRC Access Control identifies and prevents access and authorization risks in cross-enterprise IT systems to prevent fraud and reduce the cost of continuous compliance and control. This document discusses key pre- and post-technical implementation considerations for each of the Access Control capabilities. It also provides checklists to assist project teams in completing key steps for a basic installation of Access Control.

Author: Erin Hughes
Customer Advisory Office
Governance, Risk and Compliance

Company: SAP

Created on: 12 January 2009

Version 1.0

Typographic Conventions

Type Style	Description
Example Text	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation
Example text	Emphasized words or phrases in body text, graphic titles, and table titles
`Example text`	File and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
`Example text`	User entry texts. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example text>`	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE TEXT`	Keys on the keyboard, for example, F2 or ENTER.

Icons

Icon	Description
	Caution
	Note or Important
	Example
	Recommendation or Tip

Table of Contents

1. Management Overview

SAP GRC Access Control delivers a comprehensive, cross-enterprise set of access control tools that enable all corporate compliance stakeholders, including business managers, auditors, and IT security personnel, to collaboratively define and oversee proper access risks, enterprise role management, compliant provisioning, and superuser privilege management. Bundling the functionality formerly provided by the Virsa Access Control products, SAP GRC Access Control addresses a complete range of control over access related risks.

SAP solutions for governance, risk and compliance are powered by the SAP NetWeaver® platform. SAP NetWeaver unifies technology components into a single platform, allowing organizations to reduce IT complexity and obtain more business value from their IT investments. It provides the best way to integrate all systems running SAP or non-SAP software. SAP NetWeaver also helps organizations align IT with their business. With SAP NetWeaver, organizations can compose and enhance business applications rapidly using enterprise services. As the foundation for enterprise service-oriented architecture (enterprise SOA), SAP NetWeaver allows organizations to evolve their current IT landscapes into a strategic environment that drives business change.

This guide provides guidelines and GRC best practices for the pre-implementation of SAP GRC Access Control (AC). Pre-implementation is the process of understanding customer requirements and helps lay a firm groundwork for successful implementation of AC.

This guide describes the different steps of the process and describes some of the factors that influence performance and hardware requirements.

2. Key Features and Benefits

The SAP GRC Access Control product includes Risk Analysis and Remediation (RAR), Compliant User Provisioning (CUP), Enterprise Role Management (ERM), and Superuser Privilege Management (SPM) capabilities. When deployed together, they provide an end-to-end access control solution that addresses the following areas:

Risk detection

- SAP Access Control detects even the most obscure access and authorization risks across SAP and non-SAP applications, providing protection against every potential source of risk, including segregation of duties and transaction monitoring.

Risk remediation and mitigation

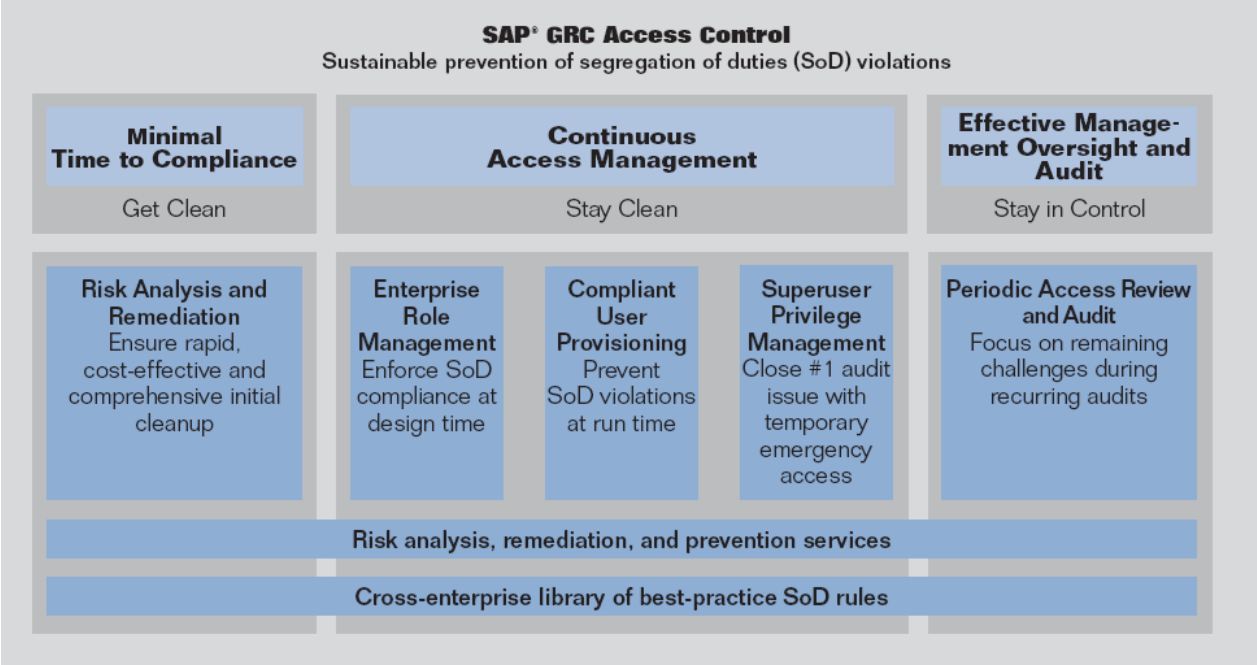
- This application for access and authorization control enables fast, efficient remediation and mitigation of access and authorization risks by automating workflows and enabling collaboration among business and technical users.

Reporting

- The application delivers the reports and role-based dashboards businesses need to monitor the performance of compliance initiatives and to take action as needed.

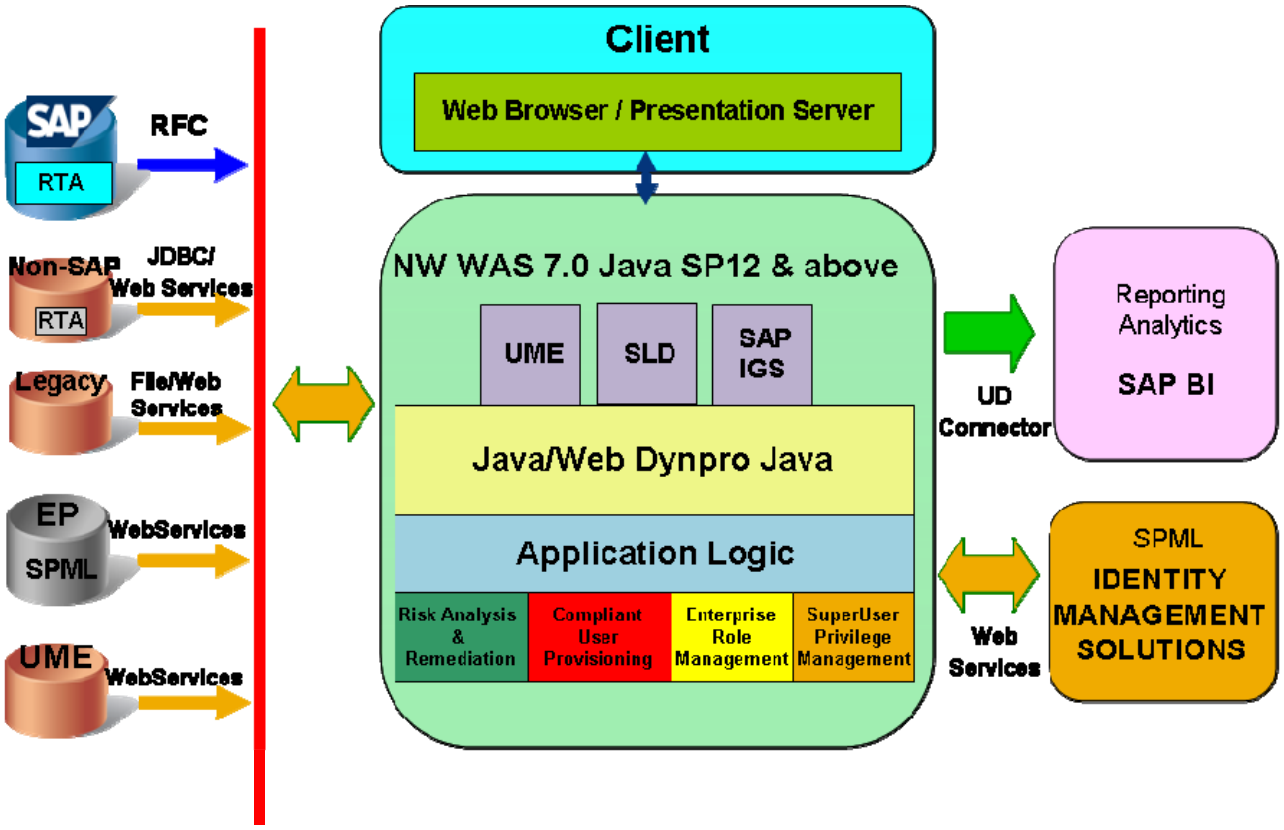
Risk prevention

- Once access and authorization risks have been remediate, only SAP's application for Access Control can prevent new risks from entering a production system. By empowering business users to check for risks in real time and automating user administration, the application makes risk prevention a continuous, proactive process.



3. Technical Pre-requisites

SAP GRC Access Control resides on the SAP NetWeaver Platform.



AC5.3 has the following technical requirements:

- Web Application Server (WAS) 700 SP 12 or higher with Internet Graphics Server (IGS) version 700 or higher.
- Target System Minimum Basis Requirements:

Basis Version	Original SP	Revised SP
4.6c	55	44
620	63	26
640	21	9
700	13	6

- AC 5.3 Real-Time Agents (RTAs) can be installed on lower Basis SP levels on if the corresponding Attribute Change Package (ACP) is uploaded to the SAP system. The following notes contain information to download the ACP.
  - 1246567 - AC 5.3 - VIRSANH & VIRSAHR Lower Import Conditions for 4.6C
  - 1247785 - AC 5.3 - VIRSANH & VIRSAHR Lower Import Conditions for 620
  - 1252111 - AC 5.3 - VIRSANH & VIRSAHR Lower Import Conditions for 640
  - 1247361 - AC 5.3 - VIRSANH & VIRSAHR Lower Import Conditions for 700

A full description of the hardware and software requirements can be accessed through the SAP Help Portal by going to http://help.sap.com/bu/ and clicking on SAP GRC Access Control on the left side of the page.

4. Pre-Implementation Preparation

Prior to the technical installation of Access Control, the following items should be discussed and decided:

1. How will the GRC system landscape look?

    a. SAP GRC recommends a three-tier landscape. A sample landscape diagram can be found by selecting this link.

    b. SAP GRC recommends a dedicated server for the Access Control components. Please refer to the installation guide for recommended minimum hardware and software requirements by selecting this link and selecting *SAP BusinessObjects > SAP Solutions for GRC > SAP GRC Access Control* and choosing the appropriate version.

    c. Please refer to the Sizing Guide for Access Control for recommendations and important factors in determining sizing for your Access Control environment. The sizing guide can be found at https://service.sap.com/sizing and then selecting *Solution Life-Cycle Management > Hardware Sizing > Sizing Guidelines > Solutions & Platform > Sizing SAP GRC Access Control.*

2. What should the User Management Engine (UME) use as its user data source?

    a. The UME provides central user administration for the Access Control capabilities. It administers users and can leverage various data sources as repositories for user data. Additional information on UME data sources can be found in *Application Help* by selecting this link.

    b. During the technical installation of the Access Control products, the Basis/Java administrator must choose whether to pull the UME user ID and password information from an existing data source, or use the local UME database as its source for user ID and password information.

    c. Once this decision is made, there are limited data source changes that are supported by SAP. Please see SAP Note 718383 for supported changes to the UME data source.

3. Which target back-end systems will be analyzed by Access Control?

    a. In Access Control 5.3, Real Time Agents (RTAs) are available for SAP, SAP Enterprise Portal (EP), Oracle Applications, PeopleSoft, and JD Edwards.

    b. Each back-end system in scope will require RTAs to be installed to facilitate communication between the target back-end systems and front-end Access Control components.

5. Post-Installation Steps and Checks

The items in this section should be confirmed prior to completing the post-installation steps for each of the Access Control capabilities. After the Basis team completes the technical installation of Access Control, it is imperative to make sure that all of the items in this section are satisfied before beginning the post-installation process.

5.1 Support Package Application

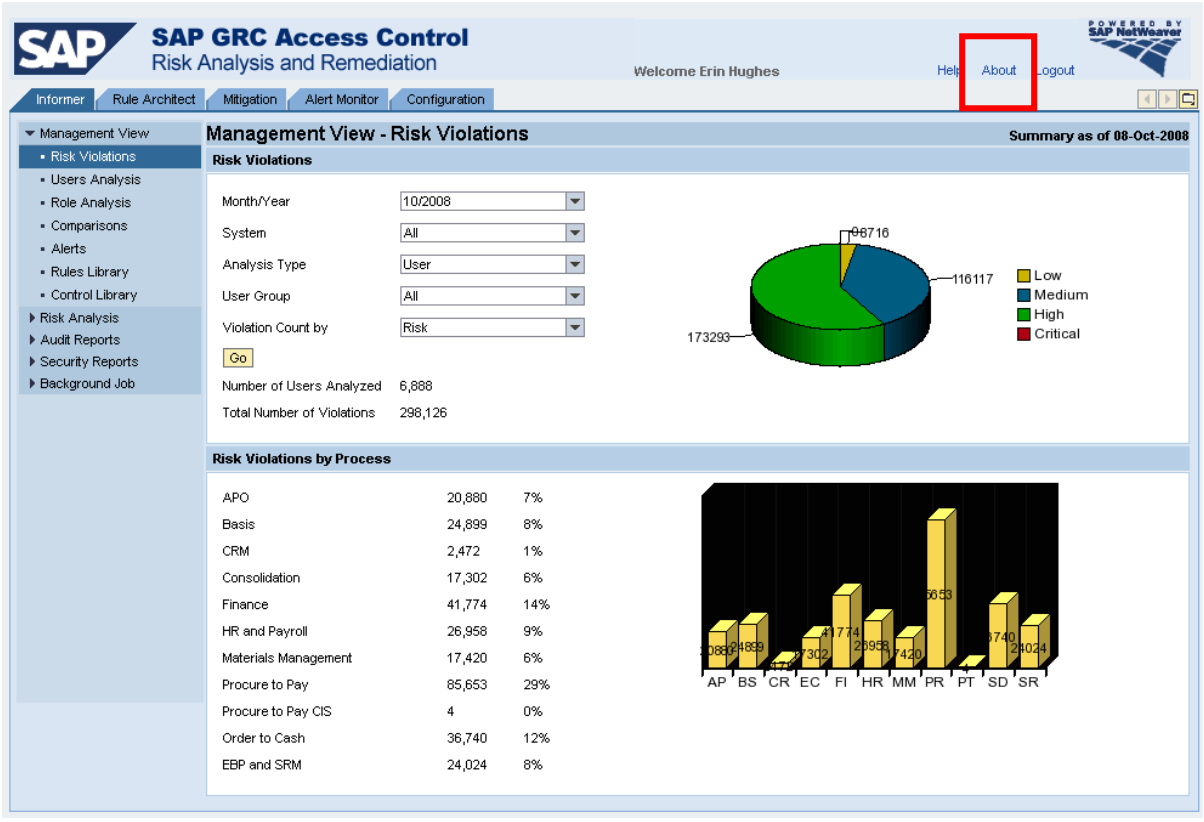
The SAP GRC Access Control installation contains two parts:

1. Java Front-End Package.
2. Access Control Real Time Agents.

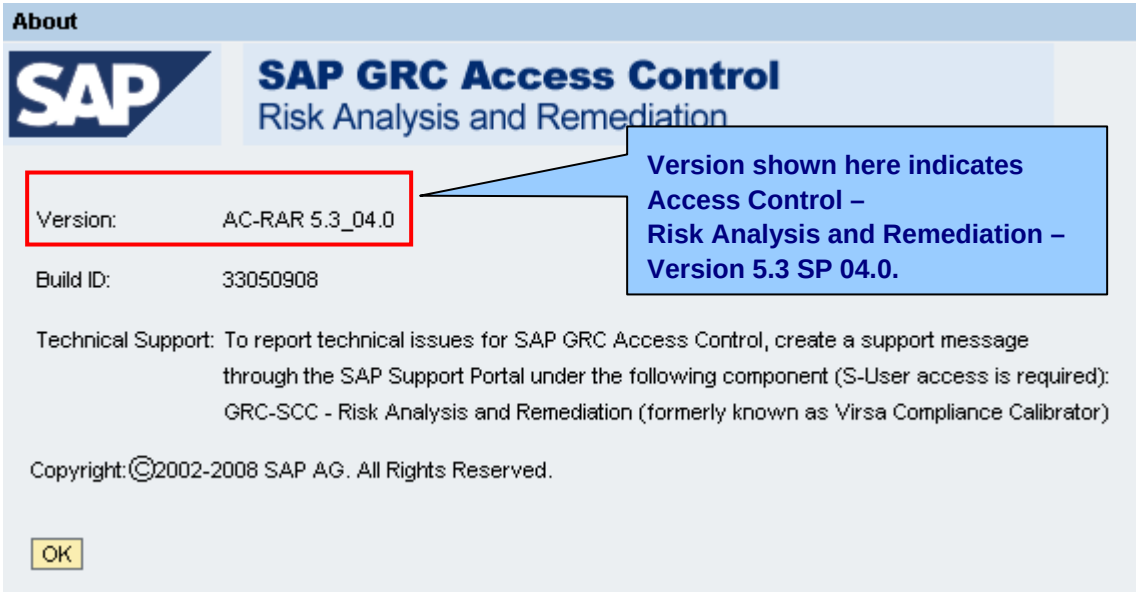
Confirm the installation of the latest Support Packages (SP) on both the front-end Access Control capabilities as well as the RTAs on each of the target back-end systems;

5.1.1 Java Front-End Support Packages

The SP level of each front-end Access Control capability can be displayed by logging in and selecting the *About* link in the top right corner of your window.



Choose *About* in any capability and a new screen will be displayed to show the Support Pack (SP) level of the capability in which you are currently working.



Note: The screenshot above is from Risk Analysis and Remediation. Each Access Control capability has its own SP, so this step should be performed in each capability to ensure all front-end SPs have been applied. The process for checking the SP is the same for each capability.

Use the chart in section 6.2, *Post-Installation Checklist for Basis/Installation Team,* below to document the SP levels of your system to compare to the current SP release levels, which can be checked in the following SAP Notes:

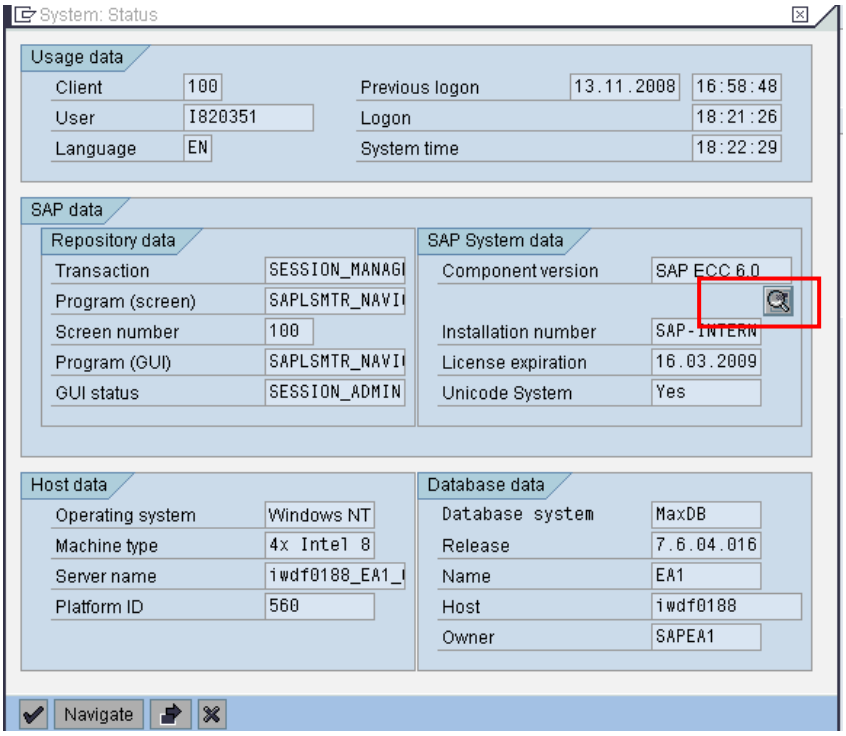
- 1168691 Access Control Launch Pad
- 1168120 Risk Analysis and Remediation
- 168508 Compliant User Provisioning
- 1168121 Superuser Privilege Management
- 1168120 Enterprise Role Management

SAP Notes can be found on the SAP Service Marketplace at https://websmp106.sap-ag.de/support > *Help & Support* > *Search for SAP Notes* with the *Application Area* GRC-SAC.

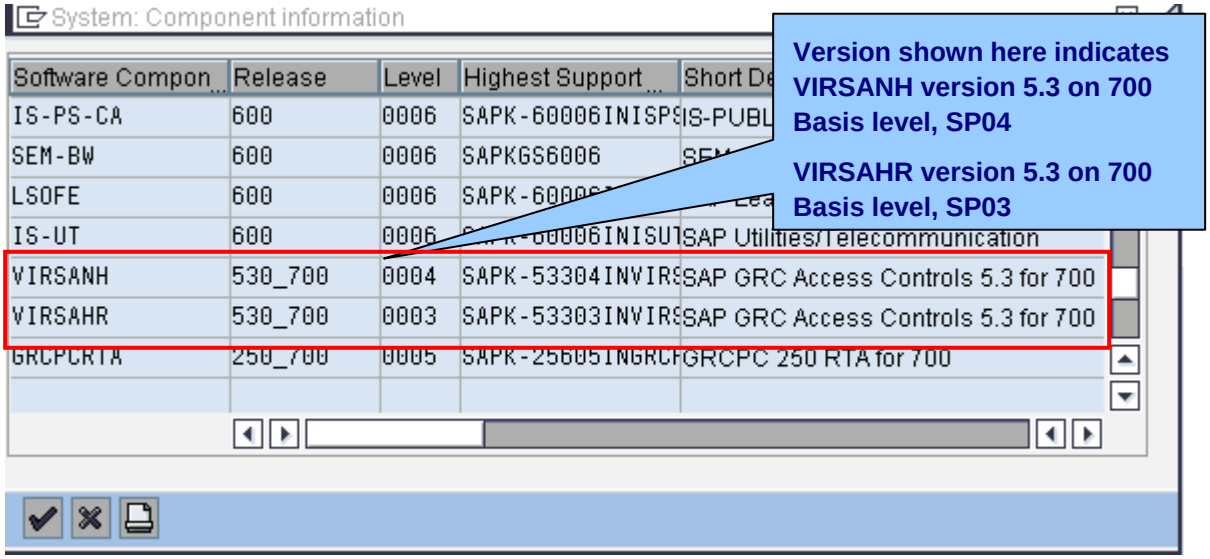
5.1.2 Access Control Real Time Agent (RTA) Support Packages

Access Control SAP RTAs are delivered for SAP ERP (HR and non-HR), CRM, SRM and other SAP ABAP systems, as well as SAP Enterprise Portal (EP). If an HR component is installed in the target back-end system, regardless of whether SAP HR is being used, then both HR and non-HR RTAs should be installed. SAP Note 1086823 provides additional information on when to install the Access Control HR or non-HR (NH) RTAs.

The SP level of the ABAP RTAs can be displayed by logging in to the target back-end system and selecting *System* > *Status*. Select the *Search* button to search for the component versions installed.



Scroll to find the Access Control RTAs and the SP level of each RTA.



Access Control RTAs are also available for non-SAP systems. See SAP Note 1076755 for more details.

Note: an RTA is required on each back-end system that you wish to connect to or analyze with Access Control.

Use the chart in section 6.2, *Post-Installation Checklist for Basis/Installation Team,* below to document the SP levels of your systems to compare to the current SP release levels. RTAs for SAP ABAP systems are dependent on the Basis Level, and can be checked in the following SAP Notes:

- 1138015 VIRSANH 530_46C Support Packages for 46C.
- 1138109 VIRSAHR 530_46C Support Packages for 46C.
- 1138016 VIRSANH 530_620 Support Packages for 620.
- 1138020 VIRSAHR 530_620 Support Packages for 620.

- 1138017 VIRSANH 530_640 Support Packages for 640 (ECC 500).
- 1138041 VIRSAHR 530_640 Support Packages for 640 (ECC 500).
- 1138018 VIRSANH 530_700 Support Packages for 700 (ECC 600).
- 1138042 VIRSAHR 530_700 Support Packages for 700 (ECC 600).
- 1076755 GreenLight Adapters- Versions of ORA, JDE and PS Supported.

5.2 User Accounts and Roles for Connectors

5.2.1 Load UME Roles and Assign to Communication User

The UME provides central user administration for the Access Control components. It administers users and can leverage various data sources as repositories for user data. SAP GRC Access Control is delivered with the following UME roles:

- VIRSA_CC_ADMINISTRATOR
- VIRSA_CC_REPORT
- VIRSA_CC_SECURITY_ADMIN
- VIRSA_CC_BUSINESS_OWNER
- AEADMIN
- AESecurity
- AEApprover
- READMIN
- REBusinessUser
- RERoleDesigner
- RESecurity
- RESuperUser
- REConfigurator
- FF_ADMIN

Confirm with the UME administrator that the delivered Access Control roles have been loaded into the UME.

In order for the Access Control capabilities to communicate with each other to perform risk analysis for CUP access requests, modifying roles and other tasks, a user ID, password, and AC administrator rights are required. The following roles should be assigned to a user ID in the GRC UME to allow for communication between the AC front-ends:

- VIRSA_CC_ADMINISTRATOR
- AEADMIN
- READMIN
- FF_ADMIN

Note: The Access Control *Security Guide* also provides a list of authorization requirements in the event that a customer wishes to build a custom role instead of using the default roles delivered with the product.

Note: If new features are delivered within a support package, the delivered roles may be updated with additional security. Therefore, the UME roles should be reloaded after the SP has been applied.

5.2.2 ABAP Role Generation and Assignment to Communication User(s)

Each of the Access Control capabilities uses a connector to communicate with the target back-end system(s). Each connector requires a user ID, password, and RFC authorizations to facilitate communication. The following roles should be generated and assigned to a user ID in each target back-end system to allow for communication to Access Control front-ends:

- /VIRSA/CC_DEFAULT_ROLE
- /VIRSA/AE_DEFAULT_ROLE
- /VIRSA/RE_DEFAULT_ROLE
- /VIRSA/FF_DEFAULT_ROLE

Note: The Access Control *Security Guide* also provides a list of authorization requirements in the event that a customer wishes to build a custom role instead of using the default roles delivered with the product.

5.2.3 LDAP User ID Creation and Assignment of Rights to Read Directory

Compliant User Provisioning can integrate with LDAP systems to pull user details from an LDAP data source, to allow for auto-population of certain fields on a CUP access request. In order to do so, a connector must be created within CUP to facilitate the transfer of data between CUP and the LDAP system(s).

A user ID must be created on the LDAP with rights to read the directory structure to pull information into Compliant User Provisioning.

5.3 Performance Tuning

The SAP GRC Regional Implementation Group (RIG) recently published a document titled "*How to Performance Optimize GRC Access Control*" which can be found by selecting this link. Included in this document are important SAP Notes specifically related to Access Control performance, memory and database recommendations, as well as rule set options and recommendations for Risk Analysis and Remediation.

This document should be reviewed by the Java Administrator for optimized Access Control performance. This document should also be reviewed by the Access Control implementation team for suggestions on optimizing the setup of the rule set in Risk Analysis and Remediation.

6. Checklists

6.1 Pre-Installation Considerations Checklist

AC 5.3 System Landscape				
	Verify/Identify	**Details/Decision**		
☐	AC Landscape has been identified	Environment	Yes	No
		Sandbox		
		Development		
		Quality		
		Production		
☐	Sizing guide for AC has been reviewed			
☐	Hardware for the AC environment has been procured	Processor Speed: RAM: Hard Disk Space:		
User Management Engine				
	Verify/Identify	**Details/Decision**		
☐	UME Data Source has been discussed	What will the UME use as its data source?		
Target Back-End Systems				
	Verify/Identify	**Details/Decision**		
☐	Target back-end systems have been identified for the AC 5.3 sandbox environment	System ID	HR Installed?	CUA System?
☐	Target back-end systems have been identified for the AC 5.3 development environment	System ID	HR Installed?	CUA System?
☐	Target back-end systems have been identified for the AC 5.3 quality assurance environment	System ID	HR Installed?	CUA System?
☐	Target back-end systems have been identified for the AC5.3 production environment	System ID	HR Installed?	CUA System?

6.2 Post-Installation Checklist for Basis/Installation Team

AC5.3 Deployment			
	Verify/Identify	**Description**	
☐	AC 5.3 files have been deployed and reflect the latest Support Package	**AC Component**	**Current SP**
		AC Launch Pad	
		RAR	
		CUP	
		ERM	
		SPM	
☐	RTAs have been installed on all target back-end systems and agree with the front-end SP level	**RTA**	**Current SP**
		VIRSANH	
		VIRSAHR	
		Enterprise Portal	
		Oracle Applications	
		PeopleSoft	
		JD Edwards	
☐	Internet Graphics Server (IGS) is running		
☐	NetWeaver J2EE Server is running		
☐	Data Supplier Bridge is running		
☐	SLD Connection (if applicable) has tested successfully		
☐	JCo Connections (if applicable) have been tested and pinged successfully		
☐	Background Daemon is Running		
☐	Analysis Daemon is Running		
☐	Delivered AC 5.3 UME Roles have been uploaded into the UME; AC Communication User has been created and assigned Admin roles for each AC capability.	User ID: Password:	
☐	Delivered AC 5.3 Default ABAP roles have been generated in each target back-end system; AC Communication User has been created and assigned Default Roles for each AC capability.	User ID: Password:	

☐	LDAP user ID has been created with rights to read the directory (if LDAP will be used as a data source for Compliant User Provisioning).	User ID: Password:
☐	CC5.3 Messages.txt file has been uploaded into Risk Analysis and Remediation.	
☐	The following files have been uploaded into Compliant User Provisioning: AE_init_append_data.xml AE_init_append_data_ForSODUARReview.xml AE_init_clean_and_insert_data.xml AE_init_append_data_CC.xml AE_init_append_data_RE.xml	
☐	The following files have been uploaded into Enterprise Role Management: RE_init_append_data.xml RE_init_clean_insert_data.xml RE_init_methodology_data.xml	
☐	"*How to Performance Optimize GRC Access Control*" guide has been reviewed and suggested performance optimization settings applied	SAP Notes applied after reviewing the "*How to Performance Optimize GRC Access Control*" guide (List all for change control purposes):

6.3 Post-Installation Checklist for Implementation Consultants

<table>
<tr><th colspan="4">AC5.3 Deployment</th></tr>
<tr><td></td><td>Verify/Identify</td><td colspan="2">Description</td></tr>
<tr><td rowspan="6">☐</td><td rowspan="6">AC 5.3 files have been deployed and reflect the latest Support Package</td><td>AC Component</td><td>Current SP</td></tr>
<tr><td>AC Launch Pad</td><td></td></tr>
<tr><td>RAR</td><td></td></tr>
<tr><td>CUP</td><td></td></tr>
<tr><td>ERM</td><td></td></tr>
<tr><td>SPM</td><td></td></tr>
<tr><td rowspan="7">☐</td><td rowspan="7">RTAs have been installed on all target back-end systems and agree with the front-end SP level</td><td>RTA</td><td>Current SP</td></tr>
<tr><td>VIRSANH</td><td></td></tr>
<tr><td>VIRSAHR</td><td></td></tr>
<tr><td>Enterprise Portal</td><td></td></tr>
<tr><td>Oracle Applications</td><td></td></tr>
<tr><td>PeopleSoft</td><td></td></tr>
<tr><td>JD Edwards</td><td></td></tr>
<tr><td>☐</td><td>Initial Data Load Files have been imported into the relevant capabilities</td><td colspan="2">Verify that Basis has loaded the following data files into the relevant capability:
Compliant User Provisioning:
AE_init_append_data.xml
AE_init_append_data_ForSODUARReview.xml
AE_init_clean_and_insert_data.xml
AE_init_append_data_CC.xml
AE_init_append_data_RE.xml
Enterprise Role Management:
RE_init_append_data.xml
RE_init_clean_insert_data.xml
RE_init_methodology_data.xml</td></tr>
</table>

7. Post-Installation Steps by Capability

Note: The post-installation steps below for each capability are intended to provide an overview of key steps to for a basic installation. These steps are not all-inclusive and implementation consultants should refer to the AC 5.3 *Configuration Guide* for additional information and features.

7.1.1 Risk Analysis and Remediation

Risk Analysis and Remediation Configuration Settings		
	Step	**Description**
☐	Define target back-end systems	Define the target back-end systems for each instance of Risk Analysis and Remediation. Keep in mind that the Connector names must be consistent across the AC capabilities to allow for communication between the products. If CUA is being targeted for provisioning in CUP, the Connector name must be the same as the Logical System ID of each system. For more information on Connector requirements, see the AC 5.3 *Configuration Guide*.
☐	Consider use of Logical System	A Logical System is grouping of two or more physical systems to allow you to maintain rules against one system grouping instead of each physical system. Logical systems reduce the time and system resources required to maintain rule sets by avoiding identical rule sets for multiple systems.
☐	Define Master User Source	The Master User Source specifies the primary system where Risk Analysis and Remediation obtains user data. Not all users must be defined in the Master User Source; it is just the initial source for retrieving basic user information, such as name and user group.
☐	Upload Static Text	The system uses descriptive text to complete the report output and provide the text descriptions for technical objects, such as actions and permissions.
☐	Upload Authorization Objects	The system uses authorization object data to provide default objects for the rule architect when building functions.
☐	Create Rules using Rule Upload (Consider Logical Systems)	Risk Analysis and Remediation is delivered with rules for SAP ERP, APO, CRM, and SRM systems; Oracle Applications; PeopleSoft; and JD Edwards. These rules are intended to be used as a starting point, and should be customized for each individual customer. Note: When upgrading AC, do not reload the rule set. Doing so may overwrite any customization of the rule set.
☐	Schedule Initial Background Jobs	After generating the rule set, schedule synchronization with back-end systems, run batch risk analysis, and update management reports.

Risk Analysis and Remediation Additional Features		
☐	Supplementary Rules	Supplementary Rules can be used to eliminate 'false positives' by adding an additional check when running Segregation of Duties risk analysis. If the system reports conflicts for actions the user is already restricted from performing due to an additional check performed against an SAP table, you can define supplemental rules to include or exclude this user.
	Organizational Rules	Organizational Rules can be used to eliminate 'false positives' by adding an additional check when executing Segregation of Duties risk analysis. If the system reports conflicts for actions the user is already restricted from performing due to an additional check performed against an SAP organizational value, you can identify and remove that violation.
	Mitigating Controls	Mitigating controls can be defined and assigned to users, roles, profiles, or HR objects within Risk Analysis and Remediation to mitigate risks that cannot be removed by modifying access.
	Alerts	Alerts can be defined and generated to report on usage of critical actions, conflicting actions, and execution of mitigating controls associated with SAP transactions within Risk Analysis and Remediation.

7.1.2 Compliant User Provisioning

Compliant User Provisioning Application Configuration Settings		
	Step	**Description**
☐	Define target back-end systems	Define the target back-end systems for each instance of Compliant User Provisioning. Keep in mind that the Connector names must be consistent across the AC capabilities to allow for communication between the products. If CUA is being targeted, the Connector name must be the same as the Logical System ID of each system. For more information on Connector Requirements see the AC 5.3 *Configuration Guide*.
☐	Field Mapping	Field mapping should be completed if using LDAP connectors for user data and user details data sources, or for provisioning from Access Request fields to User Master Record fields.
☐	Define system to be used as authentication source	When users sign on to CUP to create or submit requests on behalf of others, this system will be used to authenticate their user ID and password.
☐	Define system to be used as User Data Source	Define the User Search Data Source, which is where Compliant User Provisioning searches for existing user IDs.

☐	Define system to be used as User Details Data Source	Define the User Details Data Source, which is where Compliant User Provisioning searches for additional user data such as phone number, e-mail address, manager, etc. The User Details Data Source does not have to be the same as the User Search Data Source. In CUP 5.3, you can configure multiple User Details Data Sources.
☐	Define Number Ranges	Requests in Compliant User Provisioning are identified through a unique number range. You use the Number Ranges configuration option to define this range.
☐	Define SMTP Server	Compliant User Provisioning interacts with approvers and, if configured to do so, other interested parties via email. For this reason, you must identify the SMTP server to be used to send email notifications.
☐	Define Change Log Requirements	In Compliant User Provisioning 5.3, you can configure a change log to capture any changes users make to configuration parameters.
Compliant User Provisioning Workflow Configuration Settings		
	Step	**Description**
☐	Request Types	You configure the request type(s) that are available for selection during request creation. The Request Type configuration specifies what actions are performed on the processing of that request type.
☐	Priorities	You define a priority for each request type to indicate priority for the reviewers of the request. The priority can also be used as a workflow attribute.
☐	Employee Type	You configure the employee types available for selection during request creation. The Employee Type can also be used as a workflow attribute.
☐	Service Levels	You configure expected service levels for workflow types dependent on the attributes of the request. Service level reporting is available to generate performance reports.
☐	Initiator/Approver Determinator/Stage/Path	Initiators, Approver Determinators, Stages, and Paths are all components of workflow in Compliant User Provisioning. They must be defined in order for requests to flow through the system.
☐	Detour/Fork Escape Route Paths	Detour Paths, Fork Paths, and Escape Routes allow a request to take an alternate approval route when conditions are satisfied for a request.
☐	Email Reminder/Escalations	Emails can be configured to communicate with users, requestors, managers, and approvers to inform them of request progress, in addition to letting them know when a request requires their attention. Configuration for whether an initial password is to be sent in emails for new access is also found in the Email Reminder section.
☐	User Defaults	User defaults allow you to link data fields that are automatically set for newly created users based upon information on requests or roles.

Compliant User Provisioning Role Mapping		
	Step	**Description**
☐	Role Attribute Mapping	Role Attributes can be assigned to roles to help a requestor find the desired roles, as well as to facilitate the workflow functionality. When role attributes are assigned to roles, they help a user select roles during request creation by filtering on these attributes. Note: Role Attributes in Compliant User Provisioning should be consistent with common Role Attributes in Enterprise Role Management.
☐	Role Approver Assignment	You can define approvers in a variety of places based on the workflow approver choices.
☐	Default Roles	Default Roles allows for the automatic assignment of roles to a request based upon the attributes selected by the requestor.
☐	Role Mapping	Role Mapping allows for the assignment of additional roles to specific systems depending on the selected role in the request.
Compliant User Provisioning Additional Features		
☐	User Access Review	User Access Review is an automated feature that allows designated approvers (Manager or Role Approver) to review access on a periodic basis and take corrective actions.
☐	Segregation of Duties Review	Segregation of Duties Review is an automated feature that allows designated approvers (Manager or Risk Owner) to review risk violations on a periodic basis and take corrective actions.
☐	Mitigation Reaffirm Review	Mitigation Reaffirm Review is an automated feature that allows designated mitigating control owners to review mitigating controls on a periodic basis for pertinence.
☐	Role Reaffirm	Role Reaffirmation is an automated feature that allows designated Role Approvers to review access to the roles they are responsible for on a periodic basis and approve or reject that access. The Role Reaffirmation option is similar to User Access Review with Role Approver with the exception that Role Reaffirmation entails configuring the reaffirm date on roles.
☐	HR Triggers	HR Triggers is a configuration option that allows for the creation of rules in Compliant User Provisioning based upon actions taken in a back-end SAP system which, when satisfied, create requests automatically in Compliant User Provisioning.

7.1.3 Enterprise Role Management

Enterprise Role Management Application Configuration Settings		
	Step	**Description**
☐	Define miscellaneous system configuration	Miscellaneous Configuration includes definitions for overall Enterprise Role Management system parameters.
☐	Define target back-end systems	Define the target back-end systems for each instance of Enterprise Role Management. Keep in mind that the Connector names must be consistent across the AC capabilities to allow for communication between the products. If CUA is being targeted for provisioning in CUP, the Connector name must be the same as the Logical System ID of each system. For more information on Connector Requirements see the AC5.3 Configuration Guide.
☐	Define System Landscape	The system landscape includes configuration of systems where role definition, creation, testing, and risk analysis are performed.
☐	Schedule Initial Background Jobs	Schedule the initial transaction/object/field sync, activity value sync, and org value sync.
☐	Define Methodology	The methodology is the overall role creation process, which guides you through the process of defining, generating, and testing a role during role creation.
☐	Define Naming Convention	Naming conventions can be created to enforce role and profile naming standards during the role creation process. Naming conventions are specific to a system landscape and role type.
☐	Define Role Attributes	Role Attributes are categories that can be assigned to roles to help a requestor find the desired roles, as well as to facilitate the workflow functionality. When role attributes are assigned to roles, they help a user select roles during request creation by filtering on these attributes in Compliant User Provisioning. Note: Role Attributes in Enterprise Role Management should be consistent with common Role Attributes in Compliant User Provisioning.

7.1.4

7.1.5 Superuser Privilege Management

Superuser Privilege Management ABAP Configuration Settings		
	Step	**Description**
☐	Create Remote Function Call	Configure a remote function call (RFC) destination to call an RFC-enabled function module. Superuser Privilege Management uses this RFC each time a Firefighter ID logs on and creates a new session.
☐	Define Background Jobs	Define the Firefighter background job, which monitors the use of Firefighter IDs and records logon events and transaction use.
☐	Define Configuration Parameters	Configuration parameters define role-based and ID-based activities, mail preferences, and report preferences.
☐	Configure Email Parameters	Define email configuration parameters for when notifications should be sent for activities performed in Firefighting sessions.
☐	Define Reason Codes	Reason codes describe each task that a Firefighter expects to perform.
☐	Create and define Firefighter IDs, Owners, Controllers, and Firefighters	Create and define Firefighter IDs, Owners, Controllers, and Firefighters, which are the key users of the Superuser Privilege Management capability.
Superuser Privilege Management NetWeaver Configuration Settings		
☐	Define target back-end systems	Define the target back-end systems for each instance of Superuser Privilege Management. Keep in mind that the Connector names must be consistent across the AC capabilities to allow for communication between the products. If CUA is being targeted for provisioning in CUP, the Connector name must be the same as the Logical System ID of each system. For more information on Connector Requirements see the AC5.3 Configuration Guide.

8. Related Content

Access Control Installation and Configuration Guides

Access Control Application Help

Preferred Practices for GRC Access Control

How to Performance Optimize Access Control 5.3

GRC Forum

9. Copyright