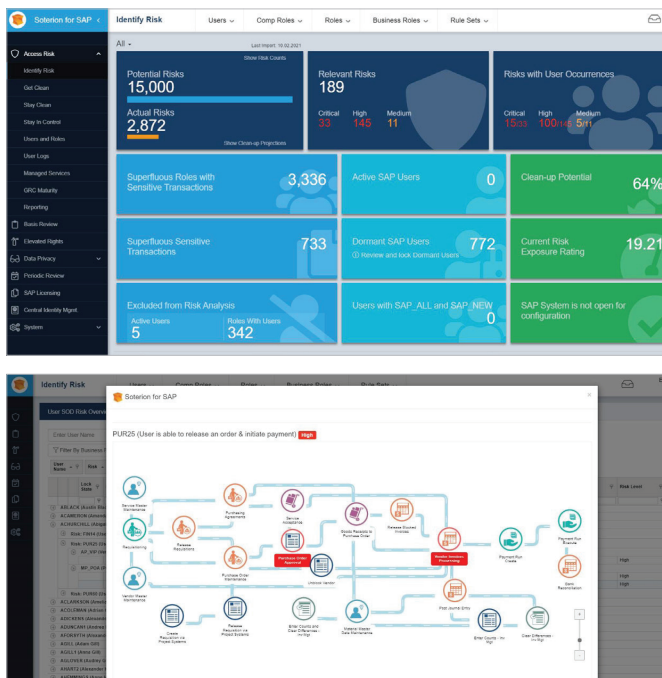


ACCESS RISK MANAGER

Access Risk Manager: Identify Risk



Gain insight into your SAP access risks with business-friendly reporting.

SAP Access Risk Analysis — Incorporating Transactional Usage

Soterion for SAP analyses users' authorizations and incorporates the user's historical transactional usage data to differentiate between the potential and the actual access risks. This allows business to focus on the real access risk in the SAP environment.

Business-friendly SAP Access Risk Reporting

Soterion for SAP allows the organisation to view data from every angle by using drag and drop functionality for grouping and filtering. Graphical overviews show the organisation's access risk landscape, including high-risk areas, in relation to risk tolerance and appetite levels. Reporting on SAP access risks at department level makes it easy to define the responsibility of ownership.

Business-Process Flows Reporting

Supporting business process flow diagrams provide more context to the access risk, converting the technical GRC language into a business-friendly language to ensure better decision-making.

Access Risk Manager: Get Clean

Remediate SAP access risks with minimal business interruption using powerful data analytics.

Resolution-driven Gap Analysis Reporting

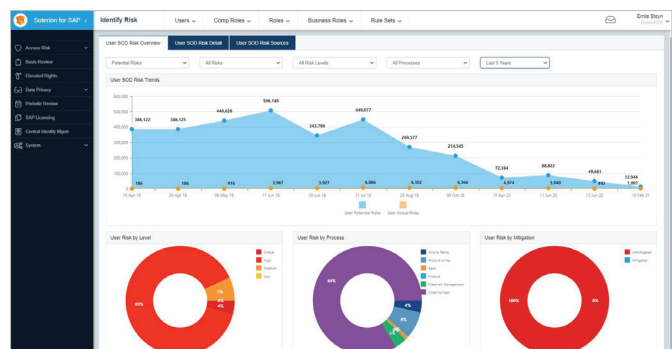
Soterion for SAP performs a Gap Analysis between potential SAP access risk and the actual SAP access risk in your authorization environment. Identifying and resolving this superfluous access is the first step in taking control of your SAP authorization landscape. Any redundant user access can then be remediated without business interruption and allows business to focus on the real access risk. Redundant user access typically contributes to 80% of the access risks in an SAP environment.

SAP Access Risk Clean-up Projection

The Risk Clean-up Projection view estimates to which degree your SAP Authorization solution can be cleaned up using Soterion for SAP's methodology. The clean-up actions focus initially on the removal of unused access contributing to risk, ensuring significant risk remediation with minimal impact on business.

Risk Clean-up Wizards

The Risk Clean-up Wizards provide clear, focused, step-by-step suggestions on how to eradicate access risks, from the removal of superfluous allocations to the splitting of roles based on role usage analytics.



Get Clean: User Risk Overview

The majority of access risk in a SAP environment is caused by functionality that is assigned to a user but is not being used. Soterion for SAP's Gap Analysis functionality enables you to align your authorization solution to what the users are actually doing in the system, thus allowing you to focus on the real access risk in your SAP environment.

Access Risk Manager: Stay Clean

Simulates "What-if" scenarios prior to making the changes in SAP - business approval is done using workflow.

Allocation Simulations and "What-If" Analysis

Soterion for SAP allows for the simulation of SAP authorization changes prior to effecting the changes in SAP. By incorporating the user's transactional usage history, business is empowered to make better access risk decisions. Change control ensures business approval of authorization changes, together with the risk impact.

"Out-the-Box" Rule Set that is Fully Customisable

Soterion for SAP comes with an 'out-the-box' access risk rule set based on best practice for all industries. The rule set is easily customisable to cater for an organisation's specific needs.

Mitigating Controls

Soterion for SAP's unique Gap Analysis functionality enables business to focus on mitigating the actual SAP access risks. Business can graphically view the mitigation status of identified risks.

The Control Library is a central repository of mitigating controls, allowing business to easily and effectively mitigate access risk through default controls and workflow functionality.

Simulator

1 Type 2 Simulation Selection 3 Results

Allocate Users To Role

SAP System: All Systems

Select Role: AP_00.PAY_RUN_CRE

Assign Users: ADAVIES (Alexander Davies)

Paste User(s) Clear Values Run Simulation

Simulation

Simulator Administrator

1 Type 2 Simulation Selection 3 Results

Summary

Introduces New Risk

Role	Users	Risk Change
AP_00.PAY_RUN_CRE (AP - Payment Run Create (F110))	ADAVIES (Alexander Davies)	2 High

Create Workflow Item Create Approval PDF

Detail

New risks caused by this change request

ADAVIES (Alexander Davies) Expand All Risks

- FIN34 (User is able create the payment proposal and execute/edit the payment run) High
- CT_F108 (Critical Transactions FINANCE: Edit Payments) High

Simulation Result

Stay Clean: Allocation Simulator

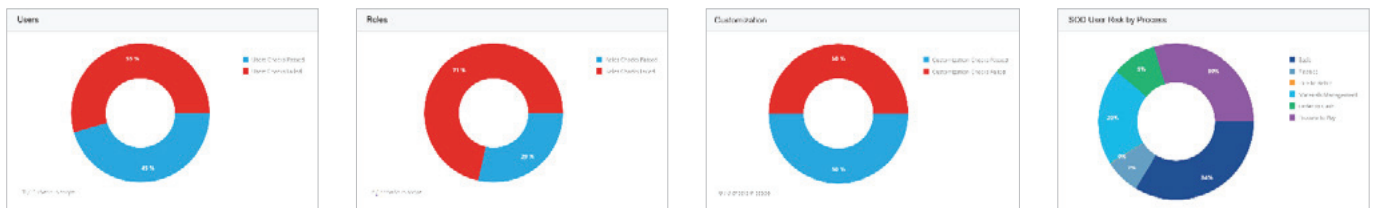
Ensure that the SAP Authorization solution remains clean going forward by simulating allocations prior to affecting these changes in SAP. Soterion for SAP's Allocation Simulator identifies whether these changes will introduce any new SAP access risk violations. These changes can be sent for approval using workflow, thereby ensuring that business accepts the new risk, as well as establishing audit trails for changes and risks.

BASIS REVIEW MANAGER

Inspecting the SAP Basis Configuration to Ensure Compliancy

SAP Basis Configurations provide system-level controls to secure a SAP system. These configuration settings can be set up to be in line with your specific security requirements. The Soterion Basis Review Manager will inspect your SAP Basis Configuration against a set of rules that are based on industry best practices. Since these configurations usually form part of an annual external audit, our Basis Review Manager will allow you to be prepared, and will establish complete compliance to avoid adverse audit findings.

The Basis Review Manager consists of a number of checks that can be executed against your SAP system. The results will be highlighted as either passes or fails, with the option of mitigating failed reports. Examples of typical tests are:



Parameter Settings (RSPARAM)

- ✓ Password lengths, expiry and complexity
- ✓ Restricting multiple logons
- ✓ Examining table logging

Role Checks

- ✓ Roles that are in the Production environment, but not assigned to users
- ✓ Roles that were created or changed in the Production environment
- ✓ Roles with wildcards for transactions

User Checks

- ✓ Users who have developer keys in the Production environment
- ✓ Test users who are working in the Production environment
- ✓ Users who have SAP standard roles in the Production environment

Rule Identifier	Name	Description	Enabled	Result
C.100	Inadequate Parameter (RSPARAM) settings	Identify inadequate parameter (RSPARAM) settings	✓	✗ Failed
C.102	Non productive Company codes	Identify non productive Company Codes	✓	✗ Failed
C.104	Prohibited Passwords	Identify prohibited passwords (from table USR40)	✓	✓ Passed
C.106	SCC4 Client Settings	SCC4 Client Settings	✓	✗ Failed
C.107	List of critical tables being looged (esp T000)	List of tables that should be looged	✓	✗ Failed
C.114	List of locked transaction codes	List of transactions that should be locked	✓	✗ Failed

ELEVATED RIGHTS MANAGER

Granting Sensitive Access in a Safe and Structured Environment

From time to time, users need temporary or emergency access for a limited period - often called **firefighter access**. This module allows you to do this effortlessly, while adhering to audit requirements.

Soterion's Elevated Rights Manager grants sensitive access in an automated workflow-driven process, and enables your management team to perform a structured review of any activities that were performed during the Elevated Rights Access check-out period.

Our Process

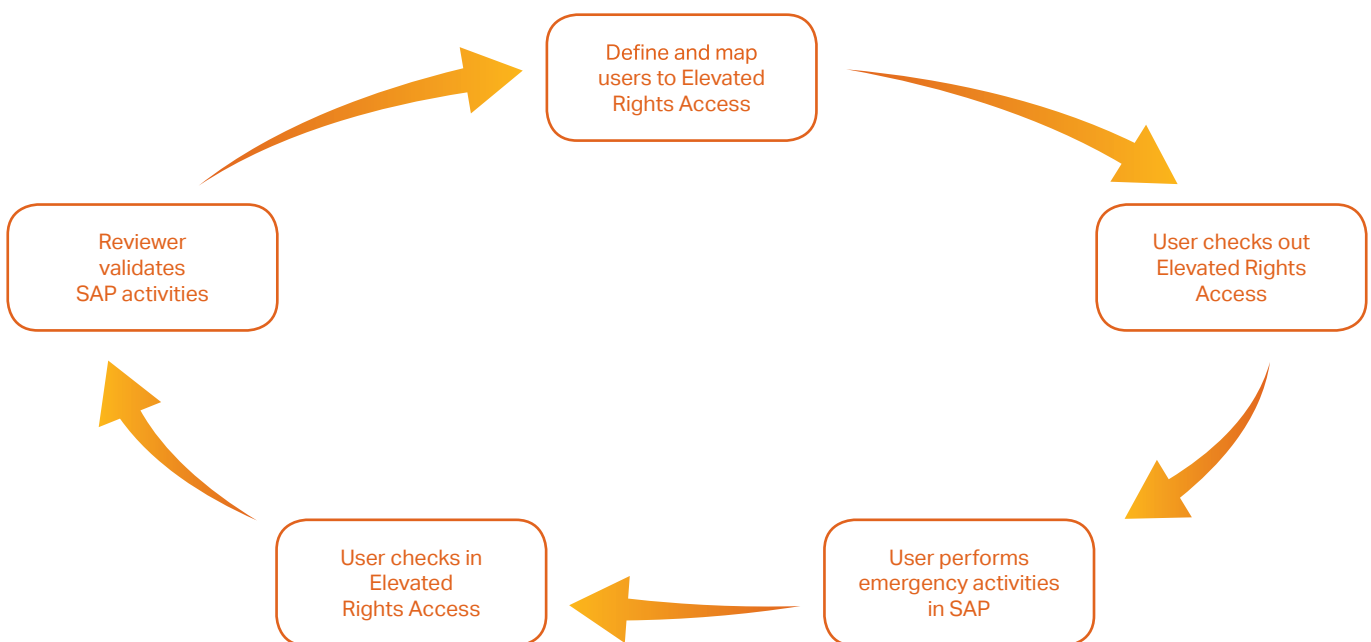
The Elevated Rights Manager can be tailored to your specific business environment. Elevated Rights Access may be granted to either a role or to an SAP user.

Elevated Rights Roles

Wide access roles can be assigned to pre-approved SAP Users when performing a check out. The particular SAP user will use their SAP User ID to perform the required activities in SAP.

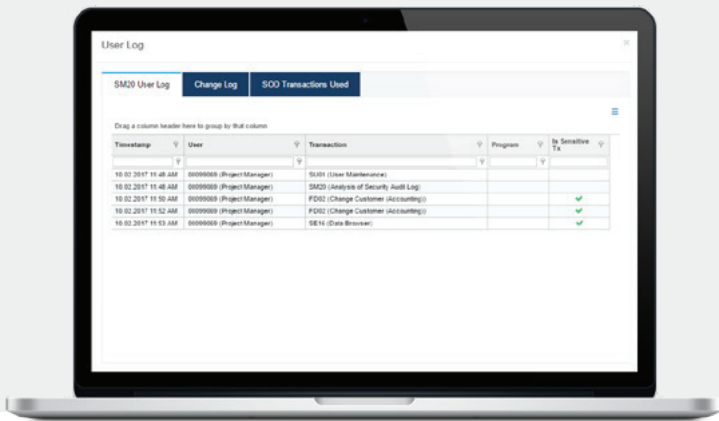
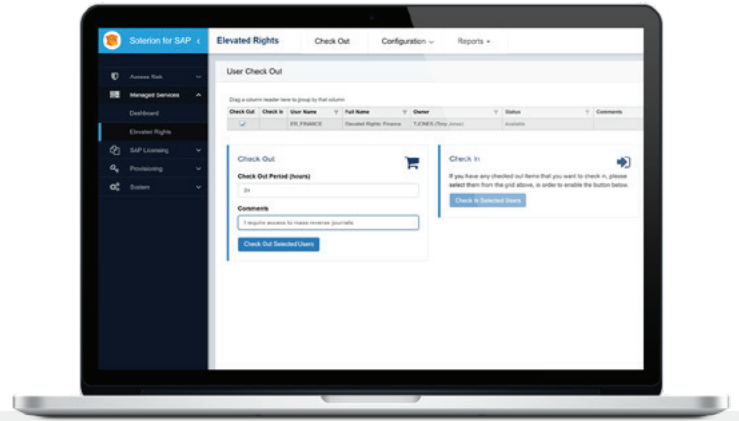
Elevated Rights SAP Users

An SAP user account containing requisite wide access will be unlocked, and the password will be sent to a pre-approved entitled SAP User. The relevant SAP User account will be used to perform the necessary activities in SAP.



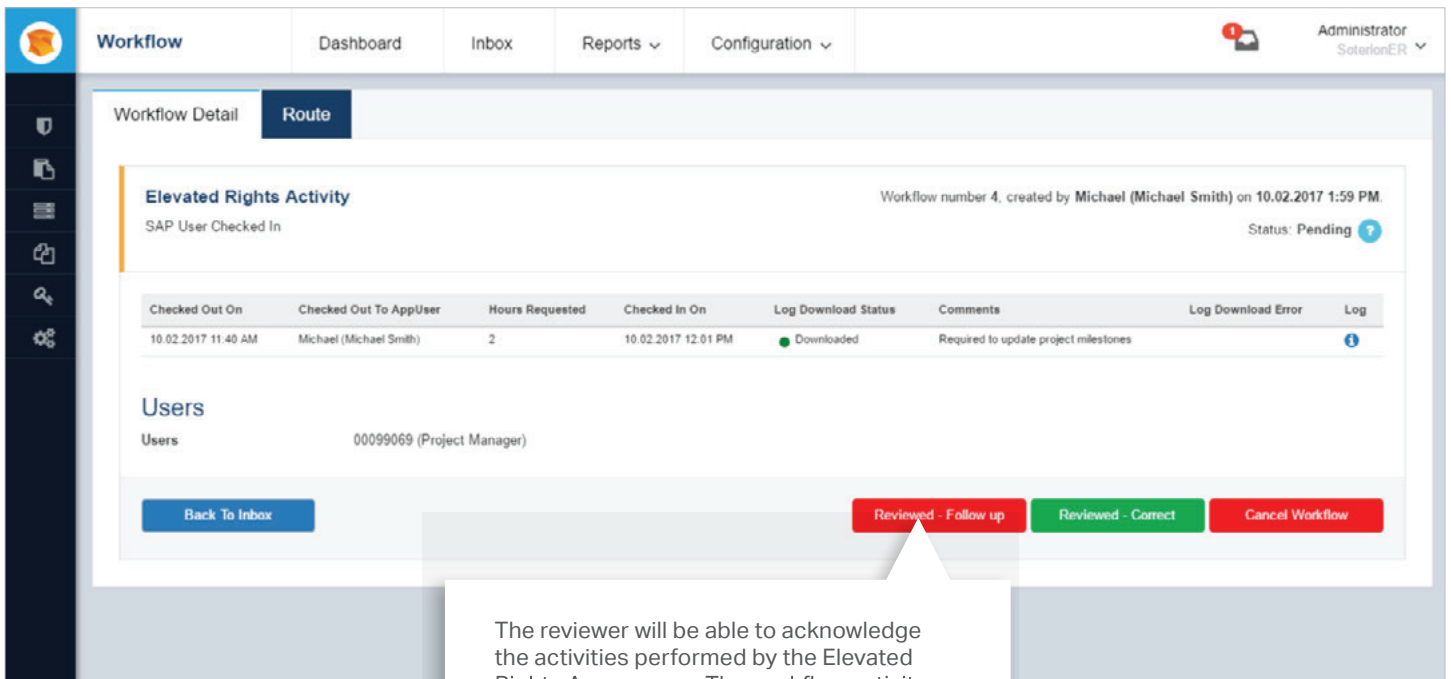
Checking Out Elevated Rights Access

When a user performs a check out, the Elevated Rights Access will be assigned to them for a predefined period to enable them to perform the required emergency activities. Once completed, the user will be able to check the Elevated Rights Access back in. Alternatively, it will automatically be checked in once the allocated period has expired.



Review of Elevated Rights Access Activities

All changes in SAP will be logged and downloaded to the Soterion Elevated Rights Manager for review. All transactions that were executed and any sensitive fields that were changed can be reviewed by the reviewer. Any sensitive transactions that were executed (SOD or Critical Transactions) will also be highlighted for their attention.



The reviewer will be able to acknowledge the activities performed by the Elevated Rights Access user. The workflow activity can be marked for "Review - Follow up" if there are any queries.

PERIODIC REVIEW MANAGER

Aligning Your GRC Capabilities with Your Business Objectives

Periodically reviewing your SAP user access, analysing the associated risks and evaluating the necessary controls will align your GRC capacity with your individual business targets. This process will significantly enhance the insight into your GRC environment, as well as being an audit and statutory requirement in many business environments.

A Mature GRC Capability Includes Periodically Reviewing a User's Access, Risks and Controls

The Periodic Review Manager provides a platform where user access reviews can be performed by business users in a simple, workflow-driven web environment while facilitating external rule set and control reviews.

Soterion's Periodic Access Review Manager ensures central control, but decentralised management throughout the entire user access review process.

Rule Set Review

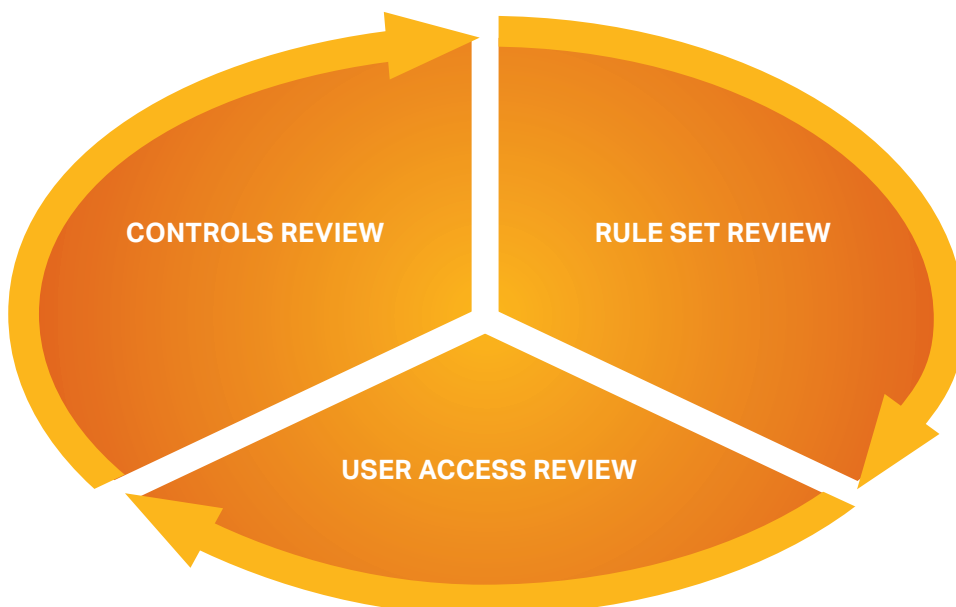
Regularly reviewing and updating your risk rule set will ensure continued relevancy in an evolving business environment.

Controls Review

Periodic reviews will consistently optimise the efficiency of your mitigating controls by identifying any gaps in control effectiveness.

User Access Review

Review your SAP user access allocations to ensure that all assignments are still relevant. Recertify user access by identifying and removing redundant and superfluous access.

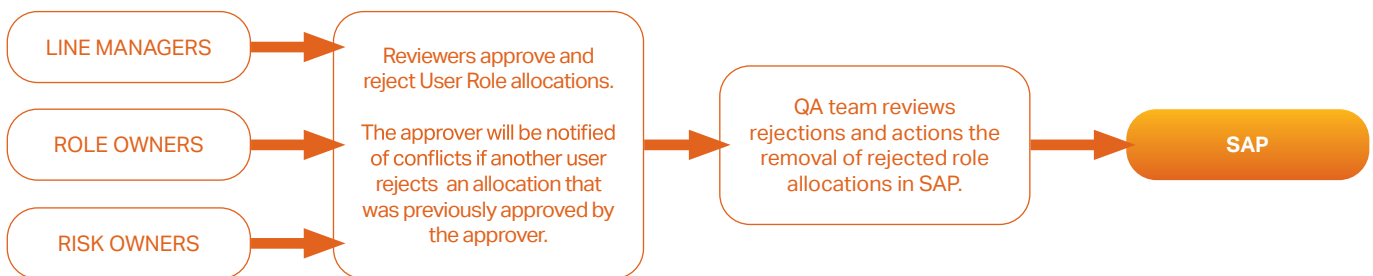


Persons Involved in a Review



Any combination of line managers, risk owners and role owners may accept or reject user role allocations in the context of a particular risk scenario. Business users are able to participate from any web-enabled device. The Administrator has access to an illustrated view of the overall progress of all reviewers. Queries and disputes can be effectively regulated, and business users will be regularly updated via email.

The Review Process



A review set is a snapshot of the user access landscape in SAP at the time of its creation. Each review set also contains a list of owners and approvers for users, risks and roles.

Reviewers can Perform User Role Approvals and Rejections

An automated email from the Administrator prompts all relevant users to participate in the review process by simply logging into their Review Inbox from any web-enabled device and using the URL specified in the email.

When logging in, the user will be presented with an Inbox that will detail the role allocations and associated risks in separate tabs.

The user can approve or reject role allocations and if necessary, will be able to add comments.

The user is able to view (and revert) allocations that were previously approved or rejected by them. The user will have access to view and remediate allocations where conflicts exist that is allocations that were previously approved, but have been rejected by another user.

#	Locked	User Name	User Role	Role	Comp Role	Tasks In Role	Tasks Change	Contributor To Role	
1		GRANDALL, Corinne Marlene	AAB0	ZF_AP_RELEASE_BLOCKED_INVOICE SAP - Release Blocked Invoice		2	18	✓	
2		FOOLEMAN, Paul Coleman	F88C	ZF_HCM_PAYROLL_PA_ADMIN_ALL_HCM Payroll PA Administrator All		14	4,462	✓	
3		COLLARK, Carl Clark	F88C	ZF_HCM_ALL_TIME_APPROVAL_HCM Time Approval All		1	84	✓	
4		COLLARK, Carl Clark	F88C	ZF_HCM_EMPLOYEE_PT_STATUS_ALL_HCM Employee Payroll Status All		2	4,595	✓	
5		COLLARK, Carl Clark	F88C	ZF_HCM_PAYROLL_ADMINIST_ALL_HCM Payroll Administrator All		4	5,937	✓	
6		COLLARK, Carl Clark	F88C	ZF_HCM_ALL_TIME_MAINTENANCE_HCM Time and Attendance Maintenance All		26	105	✓	
7		COLLARK, Carl Clark	F88C	ZF_HCM_ALL_TIME_APPROVAL_HCM Time Approval All		1	0	✓	
8		COLLARK, Carl Clark	F88C	ZF_HCM_PAYROLL_PROCESSING_ALL_HCM Payroll Processing		47	14,329	✓	
9		ZIMMER, Dale David	TT00	ZC_SALE_CO-ORDINATOR (SAP Co-ordinator Job Role)		✓	301	4,940	✓
10		EDWARDS, Glenn Gordon	F88C	ZC_AP_AND_TAX_ALL_HCM AP and Tax User Job Role		✓	198	10,454	✓
11		COCHRAN, Glenn Gordon	F88C	ZF_HCM_PAYROLL_PA_ADMIN_ALL_HCM Payroll PA Administrator All		14	4,120	✓	
12		ROCKENS, Ruth Downes	F88C	ZF_AP_RELEASE_BLOCKED_INVOICE SAP - Release Blocked Invoice		2	603	✓	

Soterion Converts the Technical GRC Language into a Language your Business Users can Understand.

Review Inbox: ESTEYIN (Emile Stizyn) | Review Set: Company User Access Review

Review Items: Approve Functional Access | View Risks

#	Locked	User Name	User Group	Department	Role	Comp Role	Term In Role	Term Usage	Contributed To Risk	Is Super...	Is New	Previously Reviewed
		DOLIVER (Dawn Oliver)	FSSC	OOL - FSSC	ZC_AP_MD_CONTROLLER (AP MD Controller Job Role)			119	10.886			
		JDAVIES1 (Jan Davies)	FSSC	OOL - FSSC	ZC_AP_MD_CONTROLLER (AP MD Controller Job Role)			119	11.612			
		DOLIVER (Dorothy Oliver)	FSSC	OOL - FSSC	ZC_AP_MD_CONTROLLER (AP MD Controller Job Role)			119	15.554			

Soterion's Periodic Review Manager allows the business users (reviewers) the option of performing their review by business process flow. If your organization has SAP roles that either do not have a good naming convention i.e. where the SAP role name is non-descriptive of the function of the role, or where the SAP roles are large and contain many activities, this often leads to reviewers not knowing what access is contained in the SAP roles.

Soterion allows the reviewers to perform their review by business process flow. All highlighted steps in the business process flow indicate access that has been assigned to the reviewer's SAP users.

By selecting the business process step, Soterion will filter which SAP roles provide that access, as well as which SAP users have been assigned those SAP roles.

Soterion's business process flow functionality significantly reduces the effort it takes to carry out a User Access Review, saving the organization time and money.

EMPLOYEE SELF-SERVICE MODULE

SAP User Role Provisioning will be Revolutionised by Soterion's Employee Self-Service (ESS) Module

Soterion's ESS Module will enable you to decentralise the provisioning of SAP user access. This functionality will reduce the time it takes users to obtain their required access, as well as lowering the costs associated with having large SAP Security teams to support the user provisioning process in your business.

Role Provisioning

Roles in SAP can either be assigned directly to a user's SAP User ID or via their SAP HR position. Soterion's Business Role option will provide you with an alternative and more efficient method of provisioning access to users.

A Business Role is a role container in our system that includes all the applicable single and composite roles for a specific job function. It is similar to the SAP Composite role, but has the following benefits for your business:

Standardisation and Flexibility

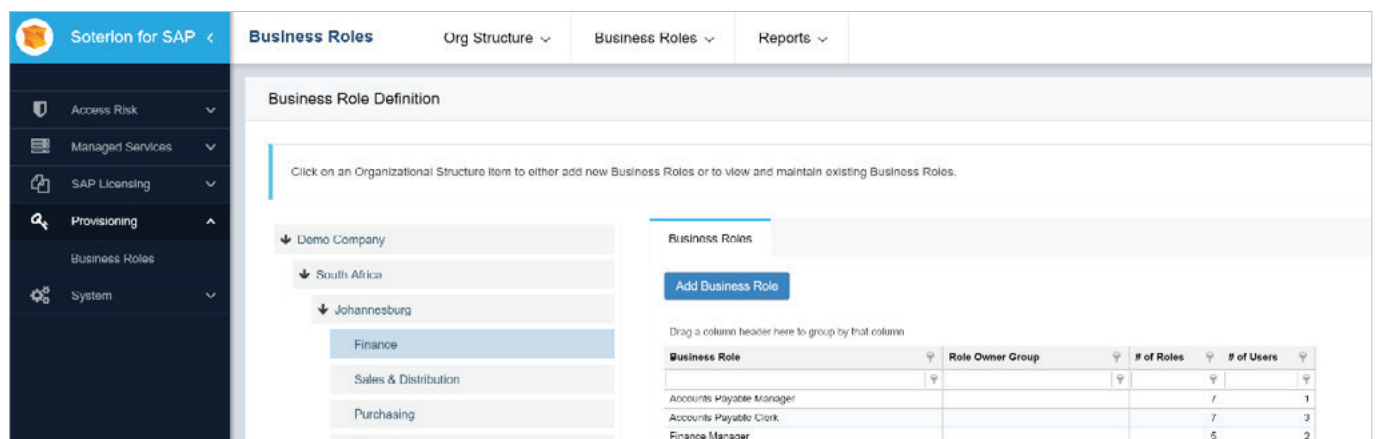
Business Roles will enable the standardisation of job functions, while facilitating the removal of irrelevant access to a specific user's job function.

Effortless Navigation

Soterion's Organisational Structure gives the user easy access to the required results.

Provisioning Using the Business Role Concept

The Business Role concept resides in an organisational structure within the Soterion application. This will enable specific SAP Roles to be assigned to the applicable Business Roles, consequently simplifying the selection process for all relevant users.

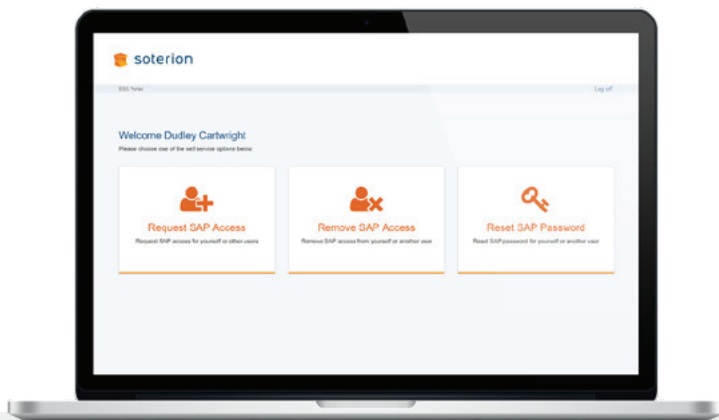
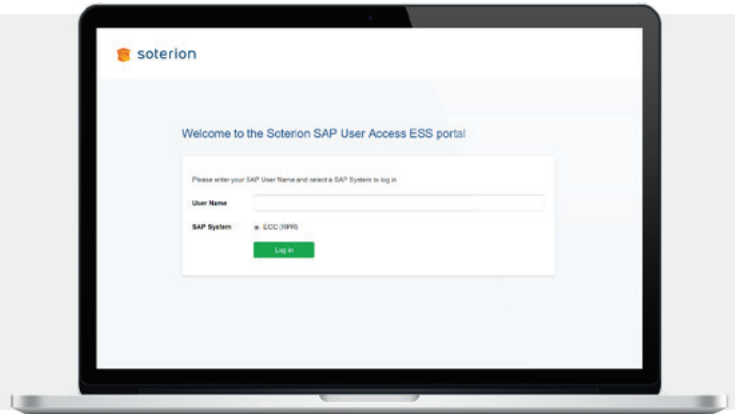


The screenshot displays the 'Business Roles' section of the Soterion application. On the left, a navigation menu includes 'Access Risk', 'Managed Services', 'SAP Licensing', 'Provisioning', 'Business Roles', and 'System'. The main area shows a breadcrumb trail: 'Business Roles > Org Structure > Business Roles > Reports'. Below this, a 'Business Role Definition' section contains a tree view of the organizational structure: 'Demo Company' > 'South Africa' > 'Johannesburg' > 'Finance'. A table titled 'Business Roles' is visible, with columns for 'Business Role', 'Role Owner Group', '# of Roles', and '# of Users'. The table lists three roles: 'Accounts Payable Manager' (7 roles, 1 user), 'Accounts Payable Clerk' (7 roles, 3 users), and 'Finance Manager' (5 roles, 2 users).

Business Role	Role Owner Group	# of Roles	# of Users
Accounts Payable Manager		7	1
Accounts Payable Clerk		7	3
Finance Manager		5	2

Soterion's ESS Module

Users may access the Soterion ESS portal from any web browser in order to provision access to themselves or to other users.

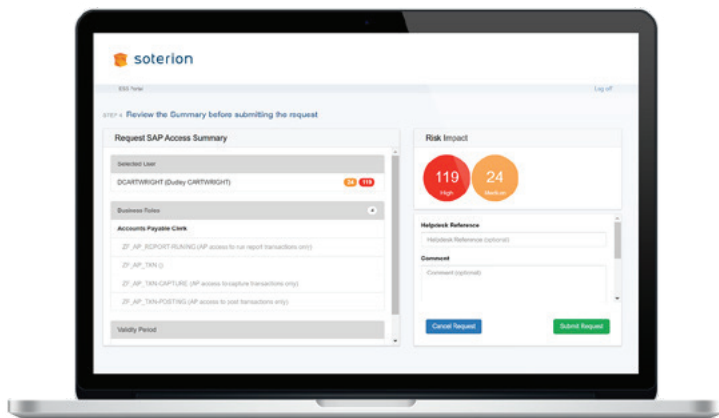
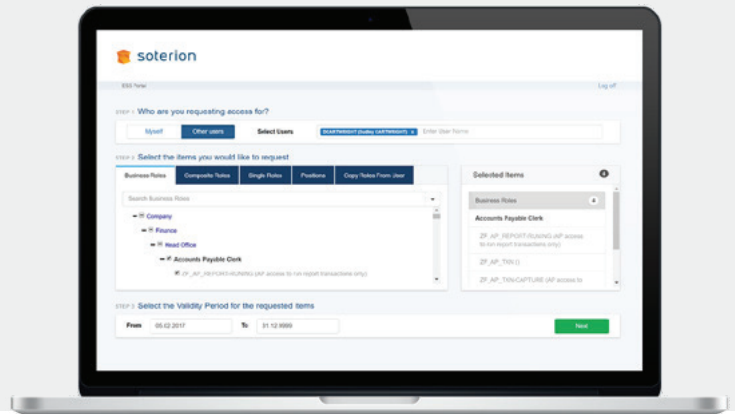


ESS will enable users to:

- ✓ Request additional SAP access
- ✓ Remove existing SAP access
- ✓ Reset SAP passwords

ESS users will be able to provision access to users using the following options:

- ✓ Business Roles
- ✓ SAP Composite Roles
- ✓ SAP Single Roles
- ✓ SAP HR Positions



The ESS module will perform a Risk Impact Analysis on the proposed request.

A workflow task will be created for the change request and will automatically be provisioned in SAP once it is approved.

SOTERION SAP LICENSING MANAGER

Optimise Expenditure and Retain Compliance by Taking Control of Your SAP License Management

SAP License Management is a crucial element in creating an economical and compliant strategy for effective software asset management. Soterion's SAP Licensing Manager can provide you with the insight you need to tailor your SAP license agreement to your organisation's specific requirements, ensuring optimal contract management and complete compliance whilst reducing unplanned and excess costs.

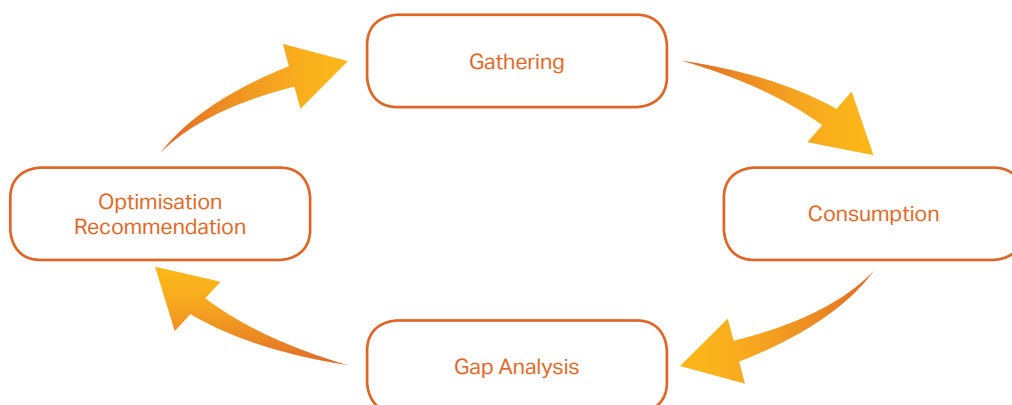
Our Background

Our specialised experience and in-depth comprehension of pre-SAP license audits ensure that our clients can confidently monitor productivity and manage cost, while governing SAP license compliance.

Key Points

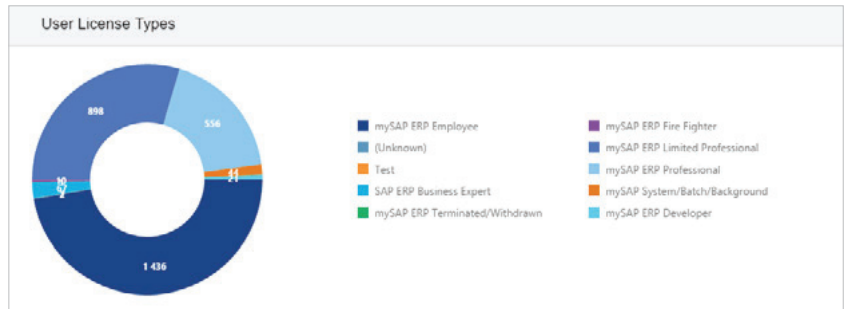
Our Approach

- ✓ **Gathering (Bill of Material)**
 Collate SAP license agreements and compare with SAP License Bill of Material.
- ✓ **Consumption**
 Determine configuration and usage of various licensing categories.
- ✓ **Gap Analysis**
 Compare the consumption figures with the Bill of Material and determine whether it is within licensing thresholds to avoid facing unplanned excess charges.
- ✓ **Optimisation Recommendations**
 Determine optimisation opportunities based on the actual usage of license categories. This will include activities such as locking or expiring dormant user accounts.



SAP Licensing Categories typically fall into the following areas:

- ✓ Named users (including indirect usage)
- ✓ Master records
- ✓ Throughput
- ✓ Hardware



User License Optimisation Recommendations

User Maintenance

- ✓ Dormant users
- ✓ Users locked and not expired
- ✓ Users never logged on

User Classification

- ✓ Users inconsistently classified are deemed to be in the higher license category by SAP. Named SAP user licenses must be aligned across the various SAP systems.
- ✓ Users not classified will be categorised by SAP as a Professional license type (high end category) during the annual license audit.

45

USERS LOCKED, BUT NOT EXPIRED
 These Users are locked, but have not been expired by changing their "Valid To" dates. A User that is locked, but not expired, is considered to be an active SAP Named User.

612

USERS NEVER LOGGED ON
 These Users have never logged on to the SAP System. Consider whether these accounts could be locked and expired.

User Classification

- ✓ **Users inconsistently classified** are deemed to be in a higher license category by SAP. Named SAP user licenses must be aligned across the various SAP systems.
- ✓ **Users not classified** will be categorised by SAP as a Professional license type (high end category) during the annual license audit.

User License Category Adjustment Recommendations

The graph summarises the reclassification recommendations based on usage.

Since it is not possible to include the SAP user usage data in the classification process in the standard version of SAP, most SAP clients follow the SAP license classifications methodology that is based on role allocations. This methodology can be used successfully if the specific SAP roles allocated to users are well aligned with what the users are indeed doing in SAP.

However, research shows that SAP users on average use only 20% of the functionality allocated to them, resulting in the unnecessary allocation of higher SAP license categories access to the majority of users (80%).



Going Forward

Soterion SAP Licensing Manager uses its database as a repository for future SAP license reviews, hence reducing the time and resources you will require to maintain your SAP licenses.

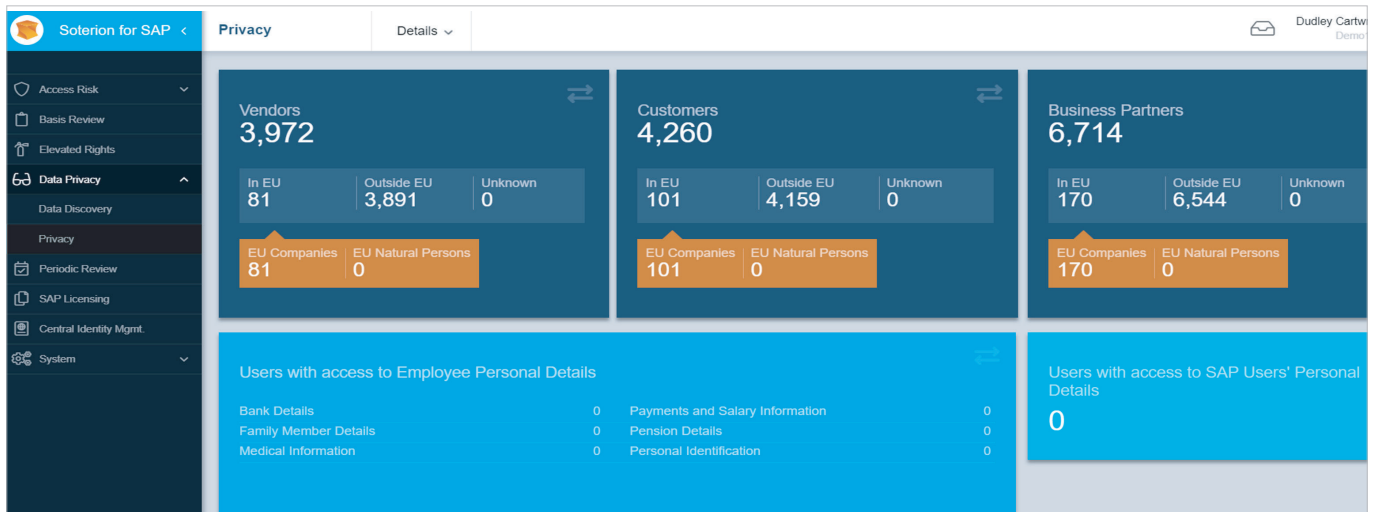
Our solution also allows you to store agreements, documents and notes to demonstrate your SAP license compliance which will minimise the number of consulting days you will need on future SAP licensing audits.

DATA PRIVACY MANAGER

Manage Personal Data in SAP

Monitor which users in SAP have access to sensitive personal information.

Due to the sheer volume of SAP tables and fields, complying with data privacy regulations is a real challenge for many organizations. Only once the organization has identified and classified what personal data resides in their SAP solution can they start to effectively manage it.



Data Discovery | Configuration ▾ | Discover Tables ▾ | Discover Transactions ▾

Data Domains

Data Domains are the categories into which you can group sensitive and/or privacy fields. By clicking on a domain you will be able to mark it as relevant and update the risk level.

Add Data Domain

Domain	Relevant	Remove
Address	✓	🗑️
Age	✓	🗑️
Bank Details	✓	🗑️
Country	✓	🗑️
Date of Birth	✓	🗑️
Education	✓	🗑️
Email	✓	🗑️
Identification Number	✓	🗑️
Medical	✓	🗑️
Other	✓	🗑️
Password	✓	🗑️
Payment Card	✓	🗑️
Pension Contribution	✓	🗑️
Person Name	✓	🗑️
Remuneration	✓	🗑️

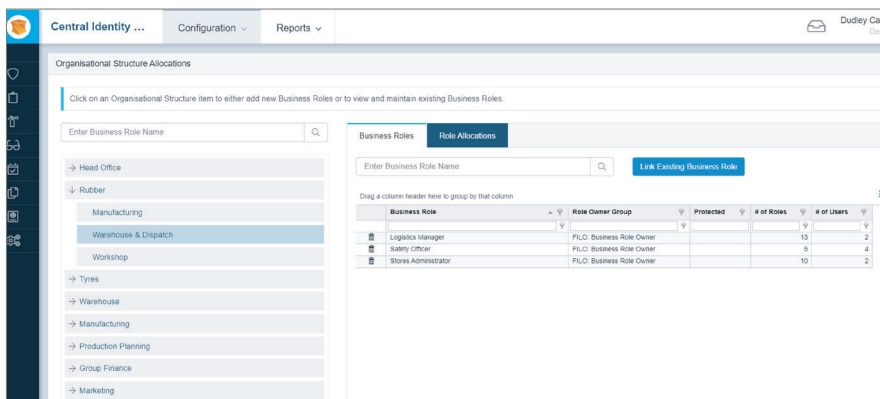
Soterion's Data Privacy Manager analyses all tables in SAP and highlights those that contain fields with personal or sensitive information, categorizing the data by Data Domain (Bank Details, Email Address, ID Number etc) per Data Subject (Business Partner, Vendor, Customer, Employee, SAP User).

Soterion facilitates the creation of a Data Privacy rule set based on the fields defined as sensitive by your organization. Soterion will highlight which SAP users have access to this information either via table display transaction codes (SE16, SE16N etc), or via normal transaction codes (standard or custom) that reference personal / sensitive information.

CENTRAL IDENTITY MANAGER

Business Roles

Address multiple business objectives with the Business Role concept.



A Business Role is a data container for a group of SAP single roles which can be from multiple SAP systems.

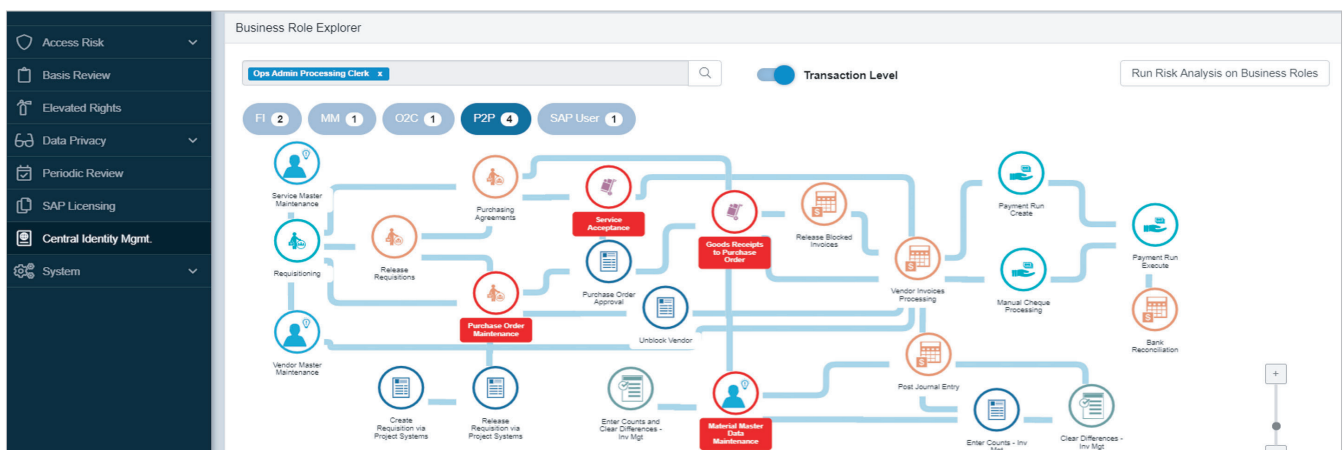
A Business Role is similar to an SAP Composite role with the added benefits:

- A Business Roles is more flexible as users can be assigned partial roles.
- SAP single roles from multiple SAP systems can be included in the Business Role.

The Business Role concept addresses several important GRC business objectives. These include:

- Increased efficiencies of the provisioning (Joiner – Mover – Leaver) process, as well as reducing the effort required to carry out a User Access Review.
- Standardization of job functions across the organization to reduce complexity.
- Enhance business accountability of risk by presenting SAP access in a more business-friendly manner.

Business Roles to linked to Departments on the Organizational Structure to simplify finding the appropriate access for SAP users.



Soterion's Business Role functionality displays the SAP access contained in the Business Role using a visualization technique that converts the technical GRC language into a business-friendly language.

All actions that the Business Role is able to perform are highlighted (in red) in the business process flow, making it easier for Business Role owners to make informed decision.

Central User Administration

Soterion's Central User Administration facilitates user management in non-production SAP systems (DEV, QAS). This reduces the support effort and associated costs required to manage user access in non-production SAP systems.

Central Identity ... Configuration Services Reports

SAP Distribution Configuration

Add Distribution SAP System Test Connections Configuration

Drag a column header here to group by that column

Type	Description	System Identifier	SAP Installation Number	Application Server	Instance Number	Client	Language	Environment
1	Production System	PRD	1234567	123.123.123	0	100	EN	PRD
1	Quality Assurance 100	QA	987654321	321.321.321	0	100	EN	QA
1	Quality Assurance 200	QAS	987654321	213.213.213	1	200	EN	QA
1	Development Golden Client	DEV	987654321	123.123.432	0	100	EN	DEV
1	Development Testing	DEV	987654321	123.321.654	1	120	EN	DEV
2	CRM Quality Assurance	CRQ	987654321	123.321.432	0	100	EN	QA
2	CRM Development	CRD	987654321	543.321.123	0	500	EN	DEV

SAP Distribution Configuration

Creation of new Users

Password Resets

Role Allocation

User Locking

Cancel Save

Soterion provides the administrator with the added flexibility to decide which functions can be performed in the different distribution systems.