EBOOK

Six Critical Capabilities of Saviynt's Application Access Governance

Ease the Burden on Security Teams, Fast-Track the Provisioning Process, and Ensure SoD Compliance With Saviynt AAG

Saviynt

Table of contents

Saviynt

Introduction

As more and more businesses move sensitive finance, accounting, and payroll data to ERP apps, maintaining continuous compliance becomes more and more critical — and complex. If your organization is tripping up in audits or with access-related violations in the past year, you're not alone.

Last year, **one-third** of all application hacks were due to unauthorized access from default, shared, or stolen credentials. Saviynt and Ponemon Institute **State of Enterprise Identity** survey of 1000 IT and IT security practitioners found that 46% failed to comply with regulations due to access-related issues.

Each app that an enterprise relies on correlates to hundreds of functions, potentially to thousands of people. But it only takes one wrong role with the wrong type of access to create a toxic combination. It's essential that companies implement high-quality internal controls to prevent users from executing both sides of a transaction — such as being able to create an invoice and pay an invoice. Regulations like Sarbanes Oxley (SOX) or the Graham-Leach-Bilely Act (GLBA) exact stiff penalties for Separation-of-Duties (SoD) violations. Or, if employees see lax controls with no action taken, companies risk the nightmare of whistleblower lawsuits.

> **Last year, one-third of all application hacks were due to unauthorized access from default, shared, or stolen credentials.**
>
> - 2022 State of Enterprise Identity Report

To preserve your reputation, keep you compliant — and out of court, internal auditors and Boards of Directors must ensure your SoD controls are operating effectively. If your GRC solution lets some SoD violations slip through the cracks or keeps your teams mired in time-consuming processes with poor visibility, it's simply not delivering. Without automated controls and enterprise-wide visibility, you could be leaving the door open to breaches, business disruption, and **significant fines.**

Six Critical Capabilities of Saviynt's Application Access Governance

The challenge for many organizations is knowing which GRC capabilities add the most value to an efficient system. There are six key capabilities that form the nucleus of a solid enterprise-ready solution. Together, they ease the burden on security teams, fast-track the provisioning process, and ensure SoD compliance for the long haul.

They include:

1. Out-of-the-Box Rulesets
2. Fine-Grained SoD Controls
3. Seamless Risk Reporting
4. Automated Certification
5. Fast, Secure Emergency Access
6. Out-of-the-Box Compliance Management

In this eBook, we'll show you how Saviynt AAG converges all of these critical capabilities into one pane of glass, simplifying cross-application monitoring, reducing time spent on certifications, and helping you get audit-ready — and stay there — with continuous compliance.

1 Out-of-the-Box Rulesets

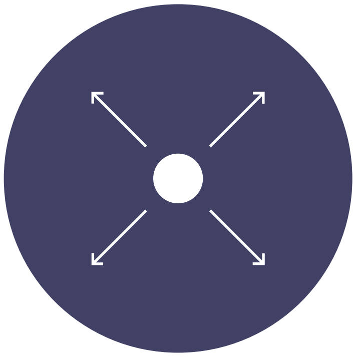
With the rapid adoption of cloud solutions, many organizations are relying on ERP applications for critical business functions.

Each of these business functions includes "rulesets" or entitlements that provide internal checks and balances against inappropriate actions. For example, they might prevent an employee who hires vendors from being able to also pay those vendors. Or they might ensure that employees who fill out timesheets aren't also able to approve those invoices. These types of internal controls are the foundation of SoD controls — and good compliance.

Saviynt's Intuitive workbench comes with built-in-out-of-the-box SoD management controls for a long list of ERP applications.

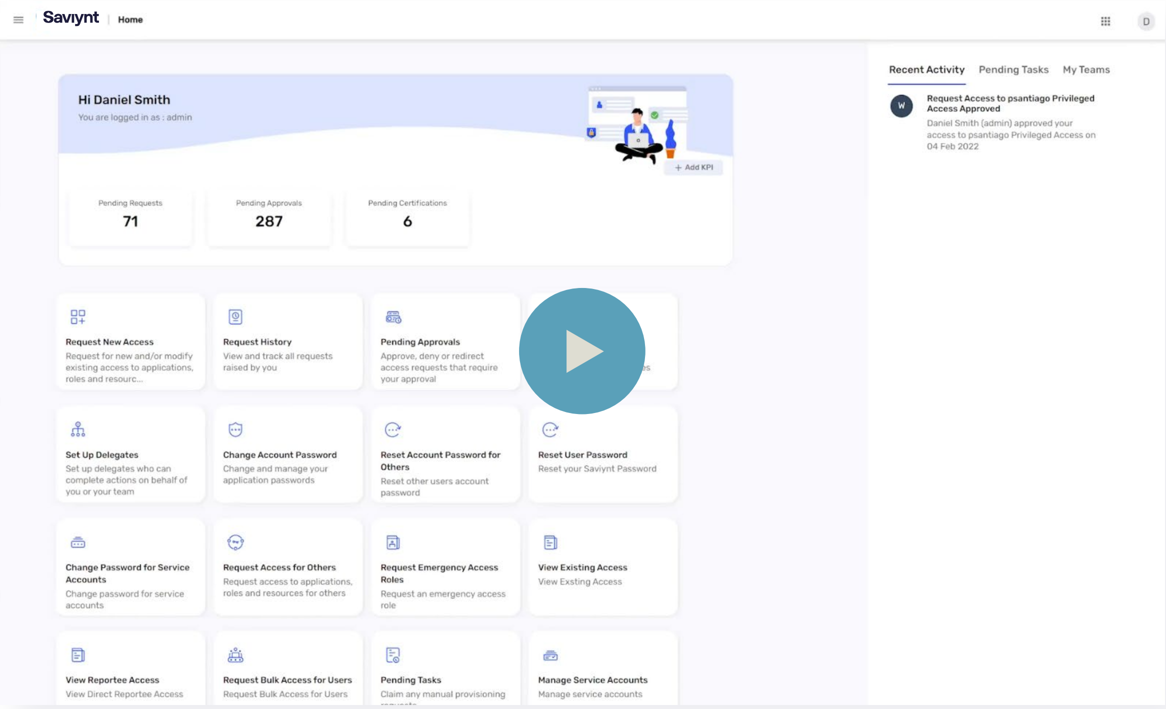
However, when you're dealing with ERP applications designed by different software vendors, each with their own security model, each speaking a different security "language," it becomes very difficult to build rulesets from scratch. When you're provisioning many different functions across different apps with different rulesets, how do you maintain healthy SoD between sales orders in Salesforce and Accounts Receivable in Oracle EBS?

Most organizations rely on point solutions or time-intensive, burdensome spreadsheets for in-scope apps. Admins often have to put new users on hold while they follow outdated or manual procedures to hunt down access approvals from other team members. While other GRC solutions may focus on a single application, like SAP, Saviynt's intuitive workbench comes with built-in out-of-the-box SoD management controls for a long list of ERP applications. Pre-loaded fine-grained rulesets can identify SoD violations across applications deep within the security models of such popular software offerings as SAP, Oracle, Active Directory, Cerner, Epic, and others.



In the SoD module, you can upload and view rulesets for different applications and easily view a description of what the risk entails. You can also bundle hundreds of functions together to define risk. Or, create your own ruleset per your organizational needs, job titles, or other factors, removing risks and entitlements that are not in scope.

Admins can run SoD assessments in real time, detect all violations in the system, and provide priority, description, and the user associated with it — right down to the most fine-grained fields possible. When and if a user makes a problematic access request, preventative SoD analysis detects anomalies and can stop the problem before it starts. Risks can then be auto-rejected, flagged, or escalated for further levels of approval.



Hi Daniel Smith
You are logged in as : admin

Pending Requests	Pending Approvals	Pending Certifications
71	287	6

Request New Access
Request for new and/or modify existing access to applications, roles and resourc...

Request History
View and track all requests raised by you

Pending Approvals
Approve, deny or redirect access requests that require your approval

Set Up Delegates
Set up delegates who can complete actions on behalf of you or your team

Change Account Password
Change and manage your application passwords

Reset Account Password for Others
Reset other users account password

Reset User Password
Reset your Saviynt Password

Change Password for Service Accounts
Change password for service accounts

Request Access for Others
Request access to applications, roles and resources for others

Request Emergency Access Roles
Request an emergency access role

View Existing Access
View Exsting Access

View Reportee Access
View Direct Reportee Access

Request Bulk Access for Users
Request Bulk Access for Users

Pending Tasks
Claim any manual provisioning

Manage Service Accounts
Manage service accounts

Request Access to psantiago Privileged Access Approved
Daniel Smith (admin) approved your access to psantiago Privileged Access on 04 Feb 2022

Demo 1: Import custom rulesets to suit your unique business needs with Saviynt's AAG Out-of-the-box SoD analysis.

2 Fine-Grained SoD Controls

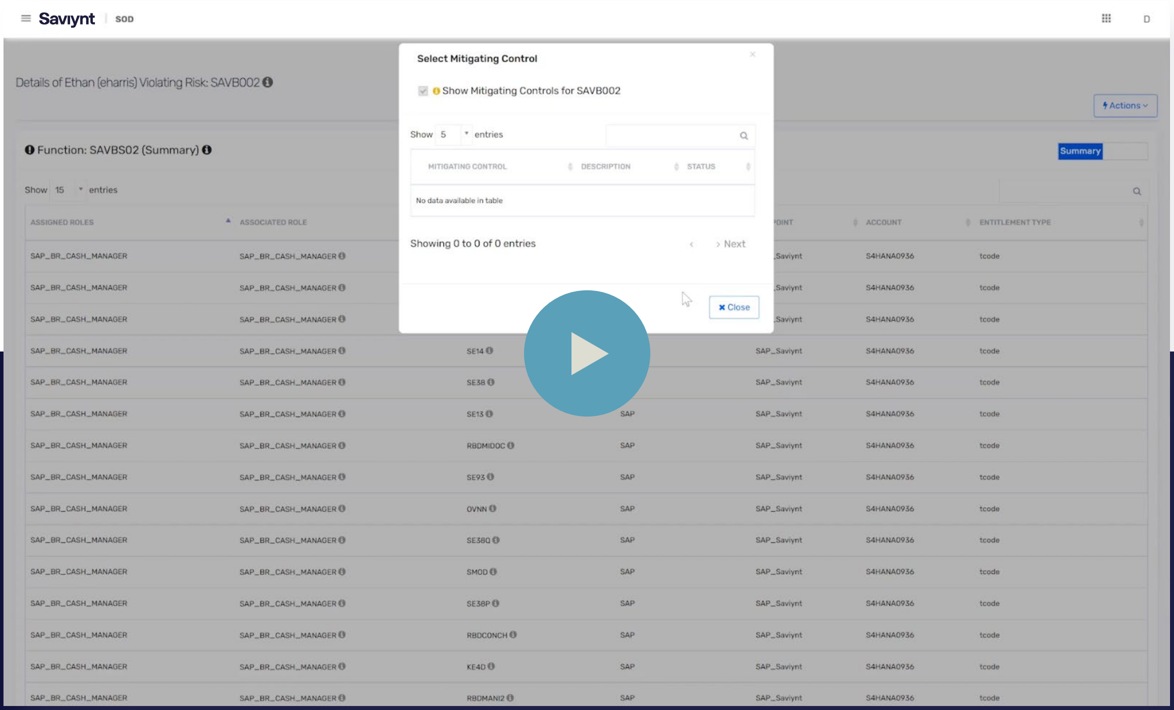
Once you've detected risks, you need a GRC workflow that can show you how many risks are in play, how many are being addressed, which were accepted, and whether they were closed and remediated — both in a single application and across applications.

Historically, this has been a workload-intensive challenge. Some solution providers can get you partly compliant by assessing SoD at the role level, but if your organization is adding custom roles or functionalities, this level of risk analysis won't be enough for auditors. Effective SoD controls must be "fine-grained" — equipped to identify risks where transactions for critical tasks occur: deep in your applications at the page, function, TCode, Auth Object, or privilege level. Coarse-grained Governance Risk and Compliance (GRC) solutions simply can't detect violations at this level.

Some solution providers can get you partly compliant by assessing SoD at the role level, but if your organization is adding custom roles or functionalities, this level of risk analysis won't be enough for auditors.

With AAG, security teams and auditors can detect and confront or accept a wide variety of risks using an extensive built-in library of user-friendly controls. Saviynt's risk scoring tools include not only static and inherent risk scores assigned to an account, but also dynamic risk scores derived from usage, behavior analytics, peer group analytics, and data gathered from external systems.

Whether on the ground, in the cloud, or in a hybrid environment, you'll be equipped to run automatic mitigation to address suspicious activities, prioritize remediation, and prevent breaches — all while preserving the time and productivity of your security teams.



Details of Ethan (eharris) Violating Risk: SAVB002

Select Mitigating Control

☑ Show Mitigating Controls for SAVB002

Show 5 entries

MITIGATING CONTROL	DESCRIPTION	STATUS
No data available in table		

Showing 0 to 0 of 0 entries

‹ › Next

✖ Close

Function: SAVBS02 (Summary)

Show 15 entries

ASSIGNED ROLES	ASSOCIATED ROLE			OINT	ACCOUNT	ENTITLEMENT TYPE
SAP_BR_CASH_MANAGER	SAP_BR_CASH_MANAGER			Saviynt	S4HANA0936	tcode
SAP_BR_CASH_MANAGER	SAP_BR_CASH_MANAGER			Saviynt	S4HANA0936	tcode
SAP_BR_CASH_MANAGER	SAP_BR_CASH_MANAGER			Saviynt	S4HANA0936	tcode
SAP_BR_CASH_MANAGER	SAP_BR_CASH_MANAGER	SE14		SAP_Saviynt	S4HANA0936	tcode
SAP_BR_CASH_MANAGER	SAP_BR_CASH_MANAGER	SE38		SAP_Saviynt	S4HANA0936	tcode
SAP_BR_CASH_MANAGER	SAP_BR_CASH_MANAGER	SE13	SAP	SAP_Saviynt	S4HANA0936	tcode
SAP_BR_CASH_MANAGER	SAP_BR_CASH_MANAGER	RBDMIDOC	SAP	SAP_Saviynt	S4HANA0936	tcode
SAP_BR_CASH_MANAGER	SAP_BR_CASH_MANAGER	SE93	SAP	SAP_Saviynt	S4HANA0936	tcode
SAP_BR_CASH_MANAGER	SAP_BR_CASH_MANAGER	OVNN	SAP	SAP_Saviynt	S4HANA0936	tcode
SAP_BR_CASH_MANAGER	SAP_BR_CASH_MANAGER	SE38Q	SAP	SAP_Saviynt	S4HANA0936	tcode
SAP_BR_CASH_MANAGER	SAP_BR_CASH_MANAGER	SMOD	SAP	SAP_Saviynt	S4HANA0936	tcode
SAP_BR_CASH_MANAGER	SAP_BR_CASH_MANAGER	SE38P	SAP	SAP_Saviynt	S4HANA0936	tcode
SAP_BR_CASH_MANAGER	SAP_BR_CASH_MANAGER	RBDCONCH	SAP	SAP_Saviynt	S4HANA0936	tcode
SAP_BR_CASH_MANAGER	SAP_BR_CASH_MANAGER	KE4D	SAP	SAP_Saviynt	S4HANA0936	tcode
SAP_BR_CASH_MANAGER	SAP_BR_CASH_MANAGER	RBDMANI2	SAP	SAP_Saviynt	S4HANA0936	tcode

Demo 2: AAG's easy-to-use interface helps you detect real and potential risks for rapid mitigation.

3 Seamless Risk Reporting

While visualizing the risks associated with user access across multiple applications is foundational to a good GRC system, the true value is being able to report on risks continually using a predictive model.

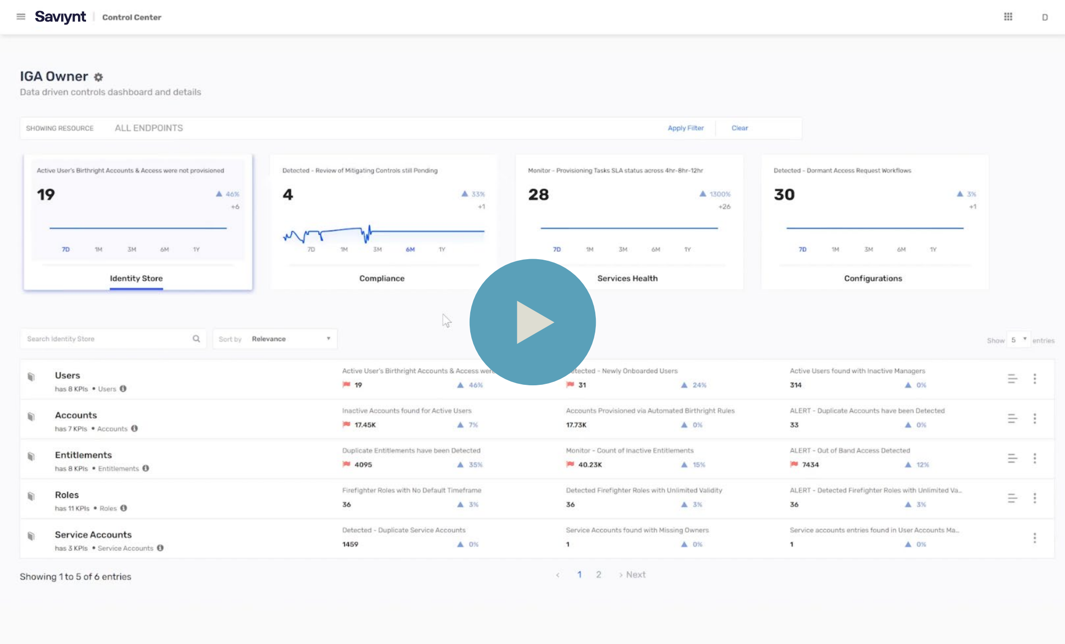
When it comes time to pull the data together for auditors, one of the biggest challenges for risk managers is to establish a clear line of sight into how tasks interact across a wide range of cloud, on-prem, and hybrid applications. How do they run an airtight report for multiple apps with siloed security models? The answer: not very easily.

Ideal reporting covers cross-application rulesets and can identify the risk code, the functions causing the risk, a risk priority, a clear description, and status — whether it's potential or active. You'll also need to know the user's account information and whether a dashboard is open, in-process, closed, remediated — or assessed and accepted without further action needed.

One of the biggest challenges for risk managers is to establish a clear line of sight into how tasks interact across a wide range of cloud, on-prem, and hybrid applications.

Most application GRC solutions can help you with one major ERP application, like SAP or Oracle. But Saviynt's comprehensive cross-application governance can manage your SaaS and on-prem applications.

As risk managers prioritize remediation efforts, AAG logs all changes in the platform, creating an audit trail that you can access with minimal effort. With pre-defined reports, your staff can slash time spent on data interpretation.



Saviynt | Control Center

IGA Owner

Data driven controls dashboard and details

SHOWING RESOURCE ALL ENDPOINTS Apply Filter Clear

Active User's Birthright Accounts & Access were not provisioned
19 ▲ 46% +6
Identity Store

Detected - Review of Mitigating Controls still Pending
4 ▲ 33% +1
Compliance

Monitor - Provisioning Tasks SLA status across 4hr-8hr-12hr
28 ▲ 1300% +26
Services Health

Detected - Dormant Access Request Workflows
30 ▲ 3% +1
Configurations

Search Identity Store | Sort by Relevance | Show 5 entries

Users has 8 KPIs • Users	Active User's Birthright Accounts & Access wer 19 ▲ 46%	etected - Newly Onboarded Users 31 ▲ 24%	Active Users found with Inactive Managers 314 ▲ 0%
Accounts has 7 KPIs • Accounts	Inactive Accounts found for Active Users 17.45K ▲ 7%	Accounts Provisioned via Automated Birthright Rules 17.73K ▲ 0%	ALERT - Duplicate Accounts have been Detected 33 ▲ 0%
Entitlements has 8 KPIs • Entitlements	Duplicate Entitlements have been Detected 4095 ▲ 35%	Monitor - Count of Inactive Entitlements 40.23K ▲ 15%	ALERT - Out of Band Access Detected 7434 ▲ 12%
Roles has 11 KPIs • Roles	Firefighter Roles with No Default Timeframe 36 ▲ 3%	Detected Firefighter Roles with Unlimited Validity 36 ▲ 3%	ALERT - Detected Firefighter Roles with Unlimited Va... 36 ▲ 3%
Service Accounts has 3 KPIs • Service Accounts	Detected - Duplicate Service Accounts 1459 ▲ 0%	Service Accounts found with Missing Owners 1 ▲ 0%	Service accounts entries found in User Accounts Ma... 1 ▲ 0%

Showing 1 to 5 of 6 entries ‹ 1 2 › Next

Demo 3 : Saviynt provides data-driven controls dashboards to identify trends.

4 Automated Certification

Certifications are scheduled access reviews that determine whether a user's access is still valid or should be discontinued.

These controls give organizations the proof needed to make the grade with external auditors.

Effective certification campaigns can certify from various owner types, such as an entitlement owner, organization owner, service account, or user manager.

But there are three predictable stumbling blocks to certifying correct access:

JOINERS, MOVERS, AND LEAVERS.

Security teams are usually very good at providing access as users join or move positions within the company. Unfortunately, "leavers" often take their access with them when they go.

RUBBERSTAMPING.

When admins need to conduct separate access certification campaigns for standard and privileged access, they may end up copying other users' access to prevent a logjam.

LOSS OF PRODUCTIVITY.

During audits, access reviewers often get mired in time-consuming cross-application complexity or multiple SoD risks.

In today's overwhelming threat landscape, your security team needs all hands on deck, not all heads down in outdated processes. It's time to get automated.

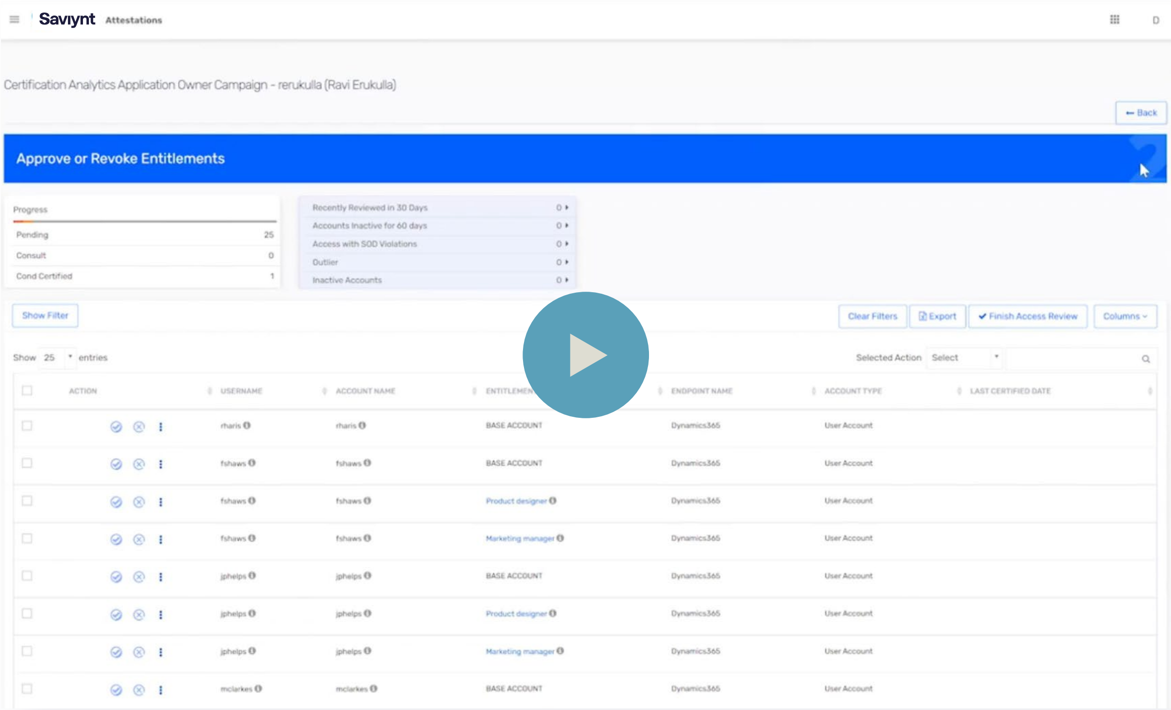
With Saviynt's intelligent access request capabilities and prevent-and-detect risk analysis, your teams can reduce the number of potential violations found during user access reviews and ensure your organization stays focused on the riskiest exposures first.

AAG allows reviewers to quickly see all toxic conflicts, understand the business impact, and track access certification through to completion.

As employees onboard or move between departments, this capability ensures they only have the proper amount of access to do their job. If they leave the organization, their access should be removed in a timely manner.

Most importantly, you stay compliant, reduce the workload on your security team, and speed up user access.

AAG allows reviewers to quickly see all toxic conflicts, understand the business impact, and track access certification through to completion.



Certification Analytics Application Owner Campaign - rerukulla (Ravi Erukulla)

Approve or Revoke Entitlements

Progress	
Pending	25
Consult	0
Cond Certified	1

Recently Reviewed in 30 Days	0
Accounts Inactive for 60 days	0
Access with SOD Violations	0
Outlier	0
Inactive Accounts	0

Show 25 entries

Selected Action Select

□	ACTION	USERNAME	ACCOUNT NAME	ENTITLEMEN	ENDPOINT NAME	ACCOUNT TYPE	LAST CERTIFIED DATE
□	✓ ⊗ ⋮	rharis	rharis	BASE ACCOUNT	Dynamics365	User Account	
□	✓ ⊗ ⋮	fshaws	fshaws	BASE ACCOUNT	Dynamics365	User Account	
□	✓ ⊗ ⋮	fshaws	fshaws	Product designer	Dynamics365	User Account	
□	✓ ⊗ ⋮	fshaws	fshaws	Marketing manager	Dynamics365	User Account	
□	✓ ⊗ ⋮	jphelps	jphelps	BASE ACCOUNT	Dynamics365	User Account	
□	✓ ⊗ ⋮	jphelps	jphelps	Product designer	Dynamics365	User Account	
□	✓ ⊗ ⋮	jphelps	jphelps	Marketing manager	Dynamics365	User Account	
□	✓ ⊗ ⋮	mclarkes	mclarkes	BASE ACCOUNT	Dynamics365	User Account	

Demo 4: Saviynt makes regular access certifications simple and fast.

5 Fast, Secure Emergency Access

The needs of a business can change quickly — and attack surfaces can expand faster than the ability to defend them.

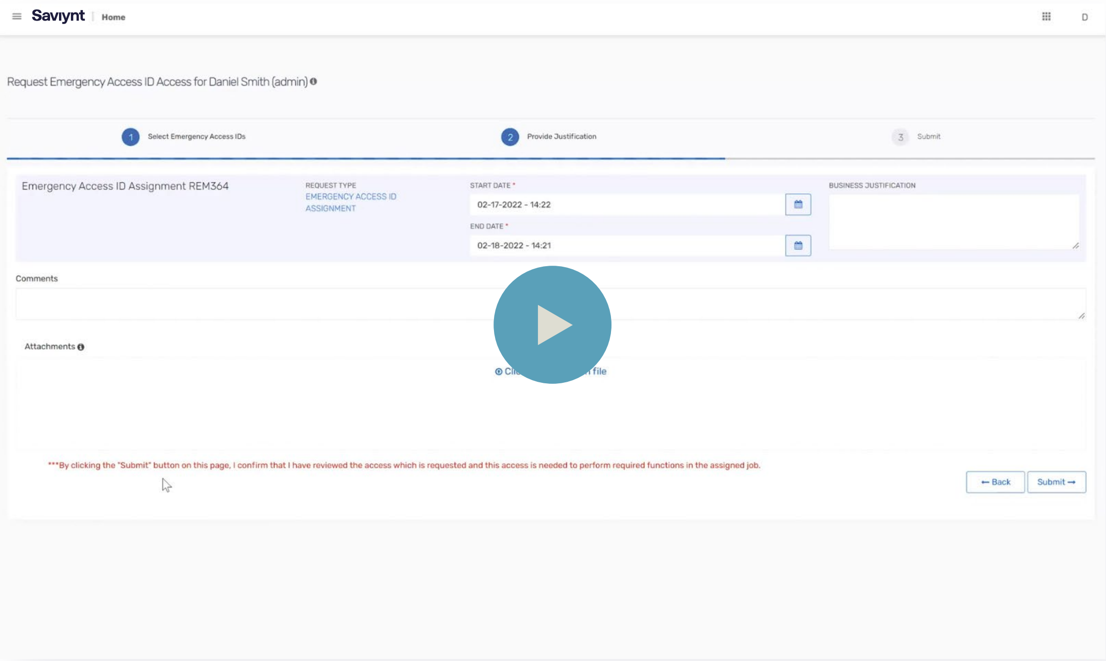
When users request elevated or ‘firefighter’ permissions to critical resources and sensitive data, time is of the essence. How quickly can your security teams gather all the information they need to provide privileged access to an application? How many people are involved in providing the information? When the work is completed, are you immediately de-provisioning privileged sessions?

To avoid chokepoints and ensure smooth audits, admins need a solution that rapidly enables real-time emergency access with a clear line of sight into what users are doing with that access — and the ability to raise the drawbridge fast when users perform unauthorized activities.

With AAG Emergency Access Management and Log Reviews, emergency capabilities can be added as a role with existing credentials or as a customized ID. With an emergency access role, we use existing credentials to grant additional access to that role. With an emergency access ID, the user doesn’t have existing credentials, so organizations set up IDs with an approved set of access.

With either access type, admins need to be able monitor sessions and immediately revoke access to eliminate standing privileges or orphaned identities. With AAG, automated session monitoring gives admins the flexibility they need to implement time-bound and customized access that expires when the session is over.

With AAG, automated session monitoring gives admins the flexibility they need to implement time-bound and customized access that expires when the session is over.



Request Emergency Access ID Access for Daniel Smith (admin)

Emergency Access ID Assignment REM364

REQUEST TYPE: EMERGENCY ACCESS ID ASSIGNMENT

START DATE *: 02-17-2022 - 14:22

END DATE *: 02-18-2022 - 14:21

BUSINESS JUSTIFICATION

Comments

Attachments

***By clicking the "Submit" button on this page, I confirm that I have reviewed the access which is requested and this access is needed to perform required functions in the assigned job.

Demo 5: AAG allows you to provide emergency access, monitor actions, and remove access quickly.

6 Out-of-the-Box Compliance Management

With the rapid adoption of cloud solutions, many organizations are relying on ERP applications for critical business functions.

One of the primary reasons for deploying an application GRC solution is to maintain regulatory compliance and ensure you have strong cybersecurity controls in place. How many times each year do you have to audit the same access controls for different compliance regulations? How many different solutions do you need to make sure those controls work — and how much time and money is that costing you?

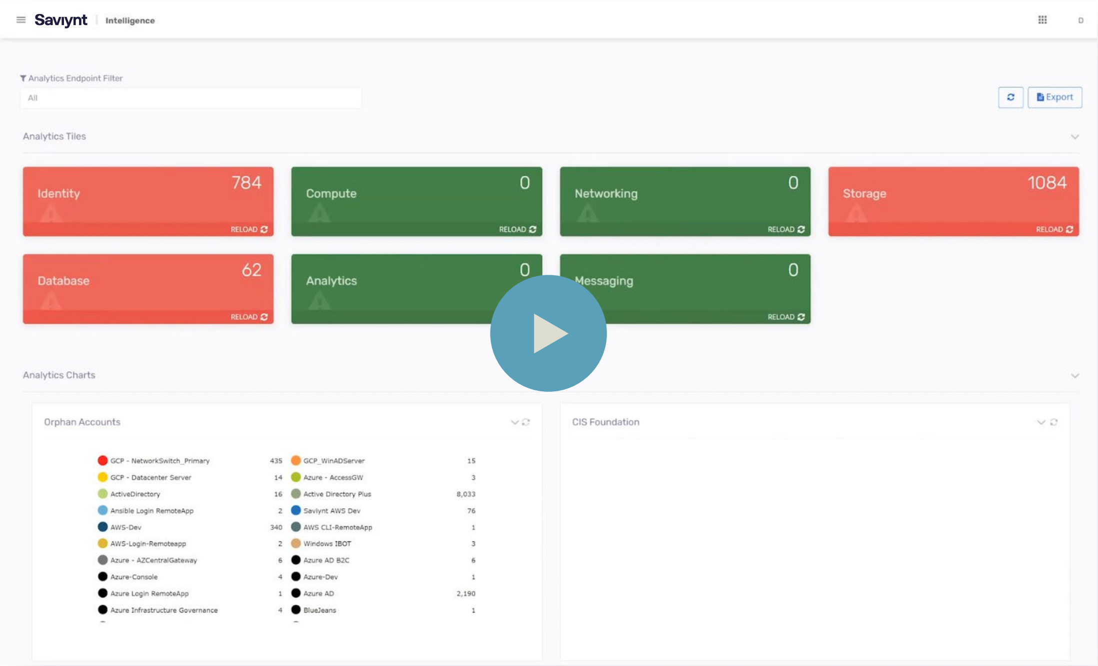
Most GRC technologies can assist with compliance requirements for only certain critical apps. If you have multiple regulations to meet across multiple applications, integrating application governance with an IDM platform becomes complex, burdensome, and time-intensive. With Saviynt's out-of-the-box compliance reporting, your security teams can vastly simplify the compliance review and management process.

Analytics should form the basis of configuring tests that can run on an ad-hoc or scheduled basis — and should be able to be filtered by application or by the specific regulation.

Analytics should form the basis of configuring tests that can run on an ad-hoc or scheduled basis and should be able to be filtered by application or by the specific regulation.

With AAG's Usage Analytics, you can generate compliance reports against a wide range of industry-specific requirements, including SOX, NIST, ITGC, FINRA, PCI-DSS, and many more. Healthcare organizations, for example, can scan user activities for HIPAA violations. Companies that do business in Europe can check risks against GDPR rules. Configuration testing can be run on your schedule and filtered by application or by regulation. Saviynt's built-in, one-click reporting saves resources, streamlines audit preparation, and ensures ongoing compliance.

Saviynt converges all of these security tools into one dashboard, empowering internal auditors and risk managers with a comprehensive, automated, and seamless line of sight.



GCP - NetworkSwitch_Primary	435	GCP_WinADServer	15
GCP - Datacenter Server	14	Azure - AccessGW	3
ActiveDirectory	16	Active Directory Plus	8,033
Ansible Login RemoteApp	2	Saviynt AWS Dev	76
AWS-Dev	340	AWS CLI-RemoteApp	1
AWS-Login-Remoteapp	2	Windows IBOT	3
Azure - AZCentralGateway	6	Azure AD B2C	6
Azure-Console	4	Azure-Dev	1
Azure Login RemoteApp	1	Azure AD	2,190
Azure Infrastructure Governance	4	BlueJeans	1

Demo 6: AAG provides out-of-the-box controls for one-click reporting.

Minimize Threats and Simplify Audits With AAG

IT and security teams face new challenges in implementing consistent, compliant GRC processes across all cloud and on-premises applications. Business processes blur the lines between various types of identities and access — rendering separate product solutions cumbersome and obsolete.

There's a reason Saviynt earned the highest score among all vendors in the **Gartner Solution Scorecard** for IGA platforms. With one easy-to-use interface, you can unite all the capabilities of privileged access management, identity governance and administration, and data access governance — with industry-leading application access governance that:

- ✓ **Makes audit preparation more efficient**
- ✓ **Frees up certification bottlenecks with automated user access reviews**
- ✓ **Detects, mitigates, and remediates risks with just a few clicks**
- ✓ **Identifies potential and real SoD violations down to the most granular level**
- ✓ **Eases cross-application complexity**

No matter how complex your application environment is, or where you are on your GRC journey, AAG can help you automate who gets access and how, keep that access secure, and maintain complete visibility into risks for continuous compliance and peace of mind.

GET STARTED TODAY

See the power & simplicity of Saviynt

REQUEST A DEMO

Saviynt

Headquarters, 1301 E
El Segundo Bl, Suite D, El Segundo, CA
90245, United States

310. 641. 1664 | info@saviynt.com
www.saviynt.com