HAUMOUN
IT PIONEERS

PRODUCT BRIEF

Symantec
by Broadcom Software

Identity Governance and Administration

AT A GLANCE

Identity Governance and Administration automates and streamlines user provisioning and access governance to improve user productivity and enforce least privileged access.

KEY BENEFITS

- Increase productivity by giving users the access they need when they need it
- Adopt zero-trust least-privileged access by removing unnecessary privileges
- Prevent security vulnerabilities through real-time policy enforcement
- Improve audit and compliance efficiencies by streamlining the certification process
- Reduce operating costs through virtual appliance and Xpress technologies

KEY FEATURES

- User provisioning
- Self-service
- Identity governance
- Rapid deployment

Overview

Managing the identities and entitlements of users to key applications, critical infrastructure, and sensitive data is a critical process for IT organizations seeking to ensure least privileged access to achieve a zero-trust posture. Users have an expectation of instantaneous and streamlined access to data and services. However, in today's environment, the IT infrastructure has not only grown exponentially, but is also highly distributed across hybrid-cloud structures. This environment poses a challenge. Though it is daunting to ensure you are providing the appropriate level of access to users, Symantec® Identity Governance and Administration (IGA) delivers comprehensive access governance and management capabilities to help customers address the following challenges:

- **User provisioning:** IGA grants and revokes access entitlements automatically as the user joins, moves throughout, and leaves the organization.
- **Self-service:** IGA enables your users to request additional access, manage their own profile attributes, and reset or change their passwords to reduce help desk costs.
- **Identity governance:** IGA streamlines processes for businesses to periodically review and certify access, and automatically revoke inappropriate access.
- **Rapid deployment:** IGA is delivered as a virtual appliance and ships with Xpress technologies, both of which reduce implementation time to deliver faster time to value.

With these core features, IGA automates and streamlines provisioning and certifying user access to applications, systems, and data across the hybrid environment.

User Provisioning

As the number of systems, accounts, and privileges explodes, the IT organization is under increasing pressure to ensure that users have the appropriate access entitlements to applications, systems, and data. At the same time, these organizations are also asked to demonstrate continuous compliance to an ever-increasing set of security and compliance mandates, which require least privileged access.

IGA helps to address these challenges through a provisioning engine that automates the creation, modification, inactivation, and deletion of user accounts and their profiles across business applications and IT systems. This automation includes assigning roles and permissions during new employee onboarding, changing access when users transition to new positions, and removing access and accounts when users leave the organization. These changes can be initiated by an authoritative source, a delegated administrator, or an end user through self-service.

User Provisioning (cont.)

The provisioning engine also enables organizations to establish and enforce a consistent set of identity compliance policies and separation of duties rules to minimize their security risk.

Self-service

The fastest way to improve user satisfaction and minimize IT help desk costs is to enable the user as much as possible. One of the competitive differentiators for IGA is the identity portal, which is an intuitive interface that business users will access for all of their identity and access tasks. Users have the ability to manage profile attributes, reset passwords, request access, and even navigate directly to endpoint applications through the Application Launchpad. The portal's access module translates application-based roles, permissions, and terminology into a common business language; and it provides a shopping cart experience, making it intuitive for even new users to request access to new systems. The solution also incorporates real-time risk analysis, evaluating risks associated with users' entitlements, so potential violations can be remediated in real-time and before new access is granted to a user. Finally, all of this functionality is provided in a single, mobile-optimized web application, so users may perform these activities on the go.

THE SOLUTION OFFERS A VIRTUAL APPLIANCE DELIVERY APPROACH, DESIGNED TO HELP YOU DEPLOY IGA IN MINUTES

Identity Governance

The second principle of Zero Trust is to ensure least privileged access. However, many organizations still struggle with over-privileged users, increasing their risks if these accounts were compromised. User provisioning can help with this, but unfortunately, routine review and certification of user access entitlements is still required. IGA addresses this challenge with a governance engine. Identity governance streamlines the processes associated with user, role, and resource certifications. It also automates the removal of unnecessary access through integration with the provisioning engine. Existing access privileges across a wide variety of IT systems and applications can be gathered and correlated automatically, and then presented to business owners through the identity portal for review and approval. Additionally, these processes can be scheduled to run periodically or run on demand. Certifications can easily be filtered to run against a subset of the users, platforms, and entitlements; and certifications can be based on the current entitlements, a historical snapshot, or differences since the last certification.

Rapid Deployment

One of the biggest deterrents for an organization to successfully deploy an identity management system has been the time required to do so. Most systems present initial use cases that are quick to deploy and show savings, but then require increasingly more time, effort, and cost to integrate more endpoints, handle complex use cases, or enforce unique business logic. IGA addresses these challenges with a few differentiating features. To begin with, the solution offers a virtual appliance delivery approach, designed to help you deploy IGA in minutes. After you have successfully deployed IGA, the next hurdle is configuration. Deployment Xpress represents a radical improvement on how the identity management software is deployed.

IGA ENABLES ORGANIZATIONS TO BE UP AND RUNNING IN MINUTES WITH A FULLY INTEGRATED IDENTITY MANAGEMENT AND GOVERNANCE SOLUTION

Rapid Deployment (cont.)

Deployment Xpress consists of a collection of preconfigured user scenarios for common use cases that most organizations would typically require. The user scenarios include user onboarding, password reset, access certifications, partner onboarding, and so on. You pick the scenarios you need, add them to the shopping cart, and then check out. The key elements needed to implement these scenarios are automatically loaded into IGA.

IGA also includes the following utilities and tools:

- **Connector Xpress:** A wizard-driven utility that enables you to generate custom connectors to homegrown and cloud-based apps through a graphical user interface without coding.
- **Config Xpress:** A utility that provides system administrators the ability to easily move components between staging environments for simplified configuration management.
- **Policy Xpress:** A wizard-based tool that lets you configure policies that execute unique and complex business processes without any custom coding.

Summary

Today's organizations are presented with a seemingly counterintuitive dilemma; they need to enable their users who expect to be able to access everything they need precisely when they need it, and they need to ensure least-privileged access to comply with their zero-trust posture. IGA automatically provisions access as users join and move throughout the organization, and provides these users with an intuitive, mobile-friendly UI where they can manage their identity, request access, complete approvals and certify access, and get one-click access to connected applications. Behind the scenes, IGA is synchronizing user information and passwords with endpoint systems, revoking access when no longer appropriate, creating and executing reviews of users' access, comparing and presenting any violations of risk or other defined policies, and re-evaluating access to refine the role model, further automating the whole process. Combined with the Xpress technologies and a virtual appliance form factor, IGA enables organizations to be up and running in minutes with a fully integrated identity management and governance solution. IGA is a solution capable of running standard business use cases and customization without code, and it is one of the most comprehensive solutions on the market.

For more information, please visit: broadcom.com/symantec-iga

Symantec by Broadcom Software

About Broadcom® Software

Broadcom Software is a world leader in business-critical software that modernizes, optimizes, and protects the world's most complex hybrid environments. With its engineering-centered culture, Broadcom Software is building a comprehensive portfolio of industry-leading infrastructure and security software, including AIOps, Cyber Security, Value Stream Management, DevOps, Mainframe, and Payment Security. Our software portfolio enables scalability, agility, and security for the largest global companies in the world.

For more information, visit our website at: software.broadcom.com

SED-IS-PB102 January 24, 2023