Date: **July 23rd, 2020**
To: **Symantec Identity Governance & Administration (Identity Manager, Identity Governance, and Identity Portal) customers**
From: **Symantec Identity Governance & Administration**
Subject: **General Availability Announcement for Symantec Identity Governance & Administration (IGA) 14.3 Cumulative Patch (CP) 2**

On behalf of Broadcom, we appreciate your business and the opportunity to provide you with high quality, innovative software and services. As part of our ongoing commitment to customer success, we regularly release updated versions of our products.

Today, we are pleased to announce the availability of Symantec Identity Governance & Administration (IGA) 14.3 Cumulative Patch (CP) 2 and important updates to the release process and End-Of-Support dates.

Overall program and End-of-Support date changes:
As part of our continued effort to improve our solution delivery, we are announcing the following changes:

- For the foreseeable future, we will no longer release major "dot" versions of IGA (14.4, 14.5, and so on), rather we will focus on cumulative patches (CP) for the 14.3 code branch that will release on a 6 month cadence.
- These new CPs will include both product features and enhancements shipped in a non-installer format to allow for a better upgrade experience. Note that we may still ship some components with installers when we deem it necessary.
- In support of these program changes, we are announcing changes to our End-of-Support (EOS) dates for Symantec Identity Governance & Administration (Formally CA/Layer7 Identity Suite)
    - **14.3 CP2 Cumulative Patch (CP) 2** EOS date is **July 31st, 2023**
    - **14.3 GA and Cumulative Patch (CP) 1** EOS date will remain at **April 20th, 2022**
- As a reminder, the current EOS date for version **14.2** is **5/31/2021**
- For more information on our End-of-Support dates, please visit our support site.

New Features and enhancements:

Identity Manager:

- **Load Balancing with Provisioning Servers**
  Identity Manager can now use round-robin load balancing support, without any restrictions on either types of provisioning operations or existing runtime limitations. This load balancing approach distributes client requests across a group of Provisioning servers.
- **Section 508 compliance support**
  Section 508 requires that the website content is accessible to people with disabilities. This applies to Web applications, Web pages, and all attached files on both the Intranet and the Internet.
  In accordance with Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998, we have introduced a new Identity Manager User Console skin named ui7-508 , to support the law and assist people with disabilities.
- **Link User Information from Your HR Data Source Using HR Feed**
  The HR Feed feature allows you to use a defined Workday™ endpoint instance to link user information from the HR data source to streamline the user provisioning process in Identity Manager**.**
  Note: With this release, we are moving the release and management of this feature out of our validation site. Customers who participated in the validation program are now required to install this CP to gain access to support and new enhancements.

- **RACF v2 and CA Top Secret v2 connectors support IBM Multi-Factor Authentication (MFA) for z/OS systems**
  The most common way for users to access z/OS systems is by using passwords or password phrases. Simplicity of passwords can pose a threat for exploitation, as users tend to choose common passwords, write down their passwords, or unintentionally install malware that can log keystrokes of user passwords. A more secure option is for systems to apply multiple authentication factors to verify the user’s identity. With multiple authentication factors, a user's account cannot be compromised if one of the factors is discovered.
  To amplify logon security, RACF v2 and CA Top Secret v2 connectors are enhanced to support IBM Multi-Factor Authentication (MFA) for z/OS systems. RACF v2 and CA Top Secret v2 users can now be entailed for authentication through IBM MFA. To accomplish user configuration for MFA, a new tab MFA appears in the Modify User Account action of the RACF v2 and CA Top Secret V2 user accounts.
- **RACF v2 connector supports IBM Netview for z/OS systems**
  Unauthorized RACF v2 user access to NetView programs on z/OS systems can lead to either changing or destroying vital system information. To prevent unauthorized system use and ensure that users are responsible for the actions taken by their operator task, RACF v2 connector is enhanced to support the IBM NetView segment of a user profile on z/OS systems. RACF v2 users can now be configured with access authorization to z/OS systems through IBM NetView. Access authorization restricts or enables RACF v2 users to view or change information, issue commands, and perform operator duties on NetView programs.
  To configure access authorization for NetView programs, a new tab NETVIEW appears in the Modify User Account action of the RACF v2 user accounts.
- **RACF v2 connector supports IBM CSDATA for z/OS systems**
  RACF v2 connector now supports the IBM CSDATA segment of a user profile on z/OS systems. Using IBM CSDATA, RACF v2 users can now be assigned RACF custom fields that store security information about a user, as defined by the security administrator on z/OS systems.
  As part of this enhancement, a new container named User Defined Fields in the Explore operation to store the user-defined fields locally. To assign custom fields to RACF v2 users, a new tab User Defined Fields appears in the Modify User Account action of the RACF v2 user accounts.
- **Active Directory Password Synchronization Agent Supports LSASS Protection Mode**
  Password Synchronization Agent is now compatible to work with Local Security Authority Server Service (LSASS) protection mode enabled on Active Directory and WindowsNT endpoints.
- **Manage Active Directory Unix NIS Domain**
  Microsoft has deprecated Identity Management for Unix (IDMU) and NIS Server roles starting from Window Server 2016.
  As a result, starting from Active Directory 2016, the NIS domain is not applicable for managing UNIX attributes. Going forward, you must manually provide the Unique Identification (UID) value in the Active Directory template to create UID for UNIX domain users.
- **Multiple connections supported from C++ Connector Server to the Active Directory Domain Server**
  Identity Manager now supports multiple active connections from C++ Connector Server (CCS) to Active Directory Domain Server. The default maximum connections allowed in a connection pool per endpoint is 10. The extended connection support allows multiple operations to in parallel,improving the overall scalability and stability of the application.
- **Ability to unlock Oracle E-Business Suite (EBS) accounts**
  The Oracle Applications connector can now retrieve the locked state of an Oracle E-Business Suite (EBS) account.
- **Full support for endpoint outages**
  Identity Manager provides full support for endpoint outages. The outages can include both planned outages managed by administrators, and unplanned outages.
- **Get a One Time Password with a Voice Message**
  Users can now request a one-time password from the login screen and receive it as a voice message. Note that you can only recover a One Time Password with a voice message if you are using Twilio.
- **Configure the maxElementsInMemory property to help improve performance**
  You can configure the maxElementsInMemory property in the ehcache.xml file to help improve performance. Ehcache governs the access to cached data with minimal costs of time and system

resources. Editing Ehcache improves performance by reducing the load on the underlying resources. Ehcache primarily concerns itself with Java Objects, but is also used for SOAP and RESTful server caching, application persistence, and distributed caching.

- **Updated SwitchTabWhenInvalid property**
- Identity Manager numbers all validation failures that appear in any Identity Manager screens that display failures. The failures are not sortable. Validation messages shown in a task context are now hyperlinked to the screen pages where the attribute appears.
- **Using Custom Group Membership Tabs**
  You can install and use the following custom group membership tabs:
    - The **Group Membership DN** tab allows you to manage and view all members of a group via their associated DN. To ensure good performance when fetching members in large groups, this tab fetches the member's unique identifier (DN) instead of the member's complete record. This reduces the number of calls that Identity Manager makes to the user directory.
    - The **Group Membership Filter** tab allows you to search for the members of a group that match a certain query filter. Identity Manager then displays members whose unique identifier matches the filter.
- **Additional Worker Attribute Mappings for HR Feed**
  HR Feed has two additional Worker Attribute Mappings that you can edit in the Workday.xml file:
    - **Custom Request Criteria**: For deployments that need to add additional request criteria to fetch data from workday, edit this element to include other request criteria.
    - **Custom Response Group**: If the **CustomHRUserAttributes** defined in the **CustomHRUserAttributes** section of your Workday.xml are not retrieved by the standard set of Response Group, **then** you can use this **CustomHRResponse Groups** section to define the response groups.
- **Schema Extension for Dynamic Connector**
  The custom attributes count for Dynamic endpoint increased from 800 to 1500.
- **User Role Certification**
  The Identity Manager User Role Certification feature allows an administrator to run user roles (Admin, Access, and Provisioning) certification directly from Identity Manager, including the ability to perform close-loop-remediation (de-provisioning) activities based on the certification reviewer decisions.

Identity Governance:

- **Increased the Column Size of User, Resource and Role Description Fields**
  Identity Governance now allows you to store a maximum of 768 characters in the User custom fields, Resource custom fields and Role Description field.

Identity Portal:

- **Forms Support Organization Selector Property**
  Identity Portal now allows an administrator to add the Organization Selector property to a user creation form. During the user creation process, a business user leverages the Organization Selector form property to assign organizations either by specific organization search or by selecting an organization from the available tree view.
- **Manage User Roles Certification from Identity Portal**
  As the solution administrator, you can manage the user roles certification either from Identity Manager or from Identity Portal. However, managing the user roles certification from Identity Portal's intuitive and user-friendly interface allows easier administration and certification of user roles by Portal administrators and business users.
- **Mobile View Enhancements**
    - Mobile View provides the capability to search applications or user permissions in the Access module.
    - The Mobile View of the certification campaigns in Identity Portal now provides additional information about users and resources that help reviewers to make better certification decisions.
    - The Mobile View displays additional information about a user or resource under a new tab called Information. This tab includes the same attributes displayed in the Desktop View of the

certification campaigns. The Information tab displays the default attributes of a user or resource. To view more information, select the **Show more** option.

- **Group Membership Scoping**
  In Identity Manager, a user can assign any groups to any users as defined in the admin scope without being an administrator of those groups. The group membership assignment privilege is given to a user by enabling the **Manage Members** flag in the **Relationship** tab of the admin task.
  The group membership scoping functionality is now extended to Identity Portal, starting from 14.3 CP2. Identity Portal now checks the **Manage Members** flag while checking the user scope for group assignment via Access Catalog.
- **Multi Select Supports Select All Functionality**
  The Multi Select list object of the form property now supports the Select All functionality. This new capability enriches admin user experience and saves time as the users can now be selected in bulk, instead of manually selecting each user from the list.
- **Show or Hide Additional Information About Users in the Tasks Approval Details Page**
  Portal administrators can now either show or hide the additional information about users in the Task Approval Details page of the application.
- **Voice Message Support for One-Time Password**
  Business users can now recover their forgotten username and password with the one-time password received as a voice message on their registered mobile phone.

New Certifications

- RedHat™ JBoss 7.2 and WildFly 15.0.x
- Windows Server 2019 as a server platform and as a managed endpoint
- Oracle Database 18c and 19c
- Microsoft SQL Server Enterprise Edition 2016 and 2017 including SQL Always On Availability Group
- Red Hat Enterprise Server 8.0 (RHEL 8.0) as Server Platform
- SAP S/4 Hana as a managed endpoint
- Oracle Unified Directory Server (OUD) 12.2.x as a managed endpoint
- System for Cross-Domain Identity Manager (SCIM) 2.0 Outbound Connector
- Symantec Privileged Access Manager Server Control 14.1 as a managed endpoint
- Symantec Privileged Access Manager (PAM) 3.3 as a managed endpoint
- CA Business Intelligence JasperReports Server 7.1.1
- CA Directory 14.1

Existing customers should strongly consider updating their deployment for the many benefits that this new release can provide. If you are already an existing customer using the Virtual Appliance platform, you can download an upgrade patch from the virtual appliance upgrade section of the documentation and very easily upgrade to this release using the documented instructions in our documentation.

For more information about this release, including any updates made after this announcement, refer to the release notes section of the documentation.

The release also includes over 100 fixes and enhancements to the current solution. For more information, see our documentation,

You can download your copy of Symantec Identity Governance & Administration (IGA) from Broadcom Support Online https://support.broadcom.com/

If you have any questions or require assistance, please contact Broadcom Customer Care online at https://www.broadcom.com/support/software/contact where you can submit an online request using the Customer Care web form:
https://ca-broadcom.wolkenservicedesk.com/web-form?_ga=2.205828371.1432263889.1590607313-713014253.1588711301

You can also call Broadcom Customer Care at +1-800-225-5224 in North America or see https://www.broadcom.com/support/software/contact for the local number in your country.

Should you need any assistance, our Broadcom Services experts can help. For more information on Broadcom Services and how you can leverage our experience, please visit https://www.broadcom.com/support/ca/services-support/ca-services

Your success is very important to us, and we look forward to continuing our successful partnership with you.

To review Broadcom Support lifecycle policies, please review the Broadcom Support Policy and Terms located at https://support.broadcom.com/

Thank you again for your business.

Itamar Budin

Product Management Lead - Identity Governance & Administration | Symantec Software Division

Symantec, A Broadcom Company