CA Single Sign-On (CA SSO)

Customer Validation Program
April 2016

Disclaimer

Certain information in this presentation may outline CA's general product direction. This presentation shall not serve to (i) affect the rights and/or obligations of CA or its licensees under any existing or future license agreement or services agreement relating to any CA software product; or (ii) amend any product documentation or specifications for any CA software product. This presentation is based on current information and resource allocations as of **April 15, 2016** and **is subject to change or withdrawal by CA at any time without notice**. **The development, release and timing of any features or functionality described in this presentation remain at CA's sole discretion**.

Notwithstanding anything in this presentation to the contrary, upon the general availability of any future CA product release referenced in this presentation, CA may make such release available to new licensees in the form of a regularly scheduled major product release. Such release may be made available to licensees of the product who are active subscribers to CA maintenance and support, on a when and if-available basis. The information in this presentation is not deemed to be incorporated into any contract.

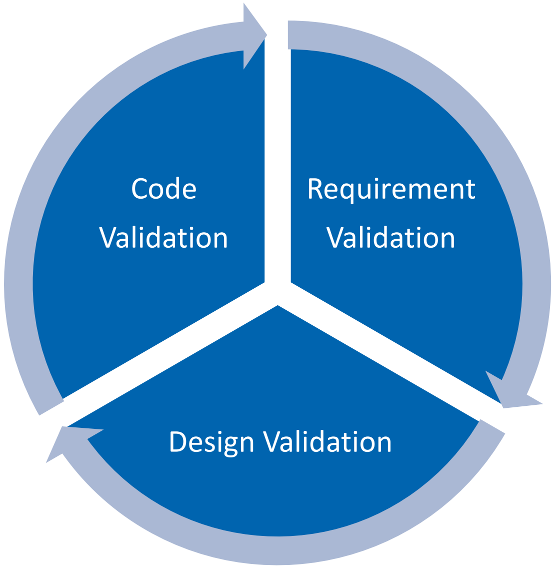
THIS PRESENTATION IS FOR YOUR INFORMATIONAL PURPOSES ONLY. CA assumes no responsibility for the accuracy or completeness of the information. TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. **In no** event will CA be liable for any loss or damage, direct or indirect, in connection with this presentation, including, without limitation, lost profits, lost investment, business interruption, goodwill, or lost data, even if CA is expressly advised in advance of the possibility of such damages.

CA’s Customer Validation Model

Better together – Engage with CA SSO product team in an Agile fashion

Multi-phased engagement model

1. Requirement validation – are we building right things, in right order?
2. Design validation – will this solve your problem?
3. Code validation – did we build it right?



CA SSO Customer Validation Program

Code Validation – CA SSO 12.6

- Early access to pre-GA builds of CA SSO 12.6 and beta support
  - Limited to first 20 participants
  - Try the release in your own test environment with your specific use cases
  - Help us deliver a real world tested release
  - Validation builds available starting May 10, 2016
  - Active validation (beta) support* provided by CA through June 20, 2016
  - Support provided by a combination of CA SSO Product Management, Engineering, Support and SWAT teams

Requirements and Design Validation – for features beyond CA SSO 12.6

- Weigh-in on future features, use case definitions, design and user experience
  - Limited to first 2-3 participants per feature
  - Provide specific feedback regarding features planned for future CA SSO releases
  - Engage directly with CA SSO Product Management and Engineering teams to help shape the future of CA SSO
  - Always ongoing – depending on where a particular feature is in the grooming and product development cycle (e.g. Use case definition, design, or implementation)

* More details in next slides

CA SSO 12.6 Code Validation

- Get access to pre-GA builds of CA SSO 12.6 for testing and validation purposes only (non-production)
- Some clarifications:
  - By including a certain feature or platform support in this customer validation program, no explicit or implicit commitment is being made regarding whether CA will GA these features, in which release and when?
  - There will likely be multiple validation builds made available to the participants through the course of the validation program, and all validation features or platform support may not be available in all builds
  - Any CA or third party custom components (such as CA Global Delivery Packaged Work Products) are currently not certified with the validation builds

CA SSO 12.6 Code Validation – Features for Validation*

- 64 bit Policy Server for RHEL 6, RHEL 7 and Windows 2012 R2
  - Upgraded Policy Server to 64 bit architecture
  - Updated third party libraries to 64 bit and newer versions
- 64 bit Access Gateway for RHEL 6, RHEL 7, Windows 2012 R2 and Solaris 11
  - Upgraded Access Gateway to 64 bit architecture
  - Updated third party libraries to 64 bit and newer versions
- Enhanced and simplified Session Assurance
  - Eliminates the need for full deployment of CA Advanced Authentication server on the Policy Server machine
  - Added support for SSL Accelerator on the Access Gateway (previously SPS)
  - POST preservation added to Session Assurance

* Refer slide 5, exact composition of a release and interim builds is not guaranteed until the release is GA

CA SSO 12.6 Code Validation – Features for Validation*

- ACO search and usability improvements
  - The Admin UI ACO task page was enhanced to include a filter control
  - Additional filters added to separate active vs. inactive settings
  - Removed pagination in favor of a scrollable list
- Added key rollover for certificate verification
  - Added support for secondary verification certificates in both SP and IdP partnership
  - Now displays expiry details of the certificate
- Added support for certificate update without partnership deactivation
- Added Connect.Gov support
  - Federation was enhanced to add several capabilities needed to align with the Connect.Gov specification

* Refer slide 5, exact composition of a release and interim builds is not guaranteed until the release is GA

CA SSO 12.6 Code Validation – Features for Validation*

- Dynamic authentication flows
  - Federation was enhanced to trigger dynamic authentication flows depending on requested authentication context
- IWA added to O365 thick-client support
  - Support for IWA was added to our O365 capability for thick clients.
  - Added in 12.52 SP1 Cr4 and brought forward into 12.6
- Italian Governance Project for Digital Identity (SPID) Compliance
  - Support for <NameIDPolicy> in AuthnRequests even when allowcreate is set to ‘false’
  - Support for Destination attribute in POST-binding AuthnRequest

* Refer slide 5, exact composition of a release and interim builds is not guaranteed until the release is GA

CA SSO 12.6 Code Validation – Features for Validation*

New to RHEL (already available on Windows as of 12.52 SP2)

- PostgresSQL as a Policy Server Data Store
- Updated JBoss version embedded with the Admin UI
- In-Memory Tracing capability added to Policy Server
- Remote Engineer – data collection tool for simplifying collection and forwarding of log information to CA Support team
- Policy Store Integrity Tool – for checking and repairing store integrity

* Refer slide 5, exact composition of a release and interim builds is not guaranteed until the release is GA

CA SSO 12.6 Code Validation – Features for Validation*

New to RHEL (already available on Windows as of 12.52 SP2)

- Policy Server support for two multi-byte databases
  - SQL SVR 2K12 multi-byte
  - Active Directory 2K12 multi-byte
- OCSP Configuration for CDS available in Admin UI
- Microsoft Azure integration added to Federation
- OneView Monitor converted to use Apache Tomcat
- Secure URL's support added to Federation Partnership

* Refer slide 5, exact composition of a release and interim builds is not guaranteed until the release is GA

CA SSO 12.6 Code Validation – Known Issues*

- In-place upgrades are currently not available with the validation builds
- RHEL 7 support for Policy Server and Access Gateway will likely be available for validation only towards the middle of the validation program
- RSA SecureID authentication scheme is currently not available for with RHEL 7 due to lack of SDK support

* Refer slide 5, exact composition of a release and interim builds is not guaranteed until the release is GA

CA SSO 12.6 Code Validation – Expectation from Participants

- Install this version in your specific test environment
- Conduct an overall validation and run through your key use cases
- Test any specific features that are of particular interest to you
- Observe and report any functional, regression, performance or documentation issues

CA SSO 12.6 Code Validation – Suggested Time and Resource Needs

- Expected time commitment: 12 to 16 hours total
  - Installation and setup: 4 hours
  - Run through existing use cases: 2 hours
  - Exercise new features: 1-2 hours per feature
  - Provide feedback (check-in calls, emails): 2-4 hours total

- Hardware and software needed
  - At least one Windows Server 2012 R2 or RHEL 6, 7 server or virtual image (recommended – 4 GB memory and 100 GB disk)
  - A directory (LDAP or RDBMS) to use a policy store and/or user store (new or existing test environment)
  - Endpoints as needed based on features tested

CA SSO 12.6 Code Validation – Defect Response Timelines

- Timelines* regarding defects submitted as part of code validation
  - Initial response – within two business days
  - Defect resolution
    - P1 – highly likely to be fixed prior to and in the GA release of CA SSO 12.6
    - P2 – likely to be fixed prior to GA, but may be deferred to a future release
    - P3 – will be triaged and added to the CA SSO defect backlog for future consideration
- Active support for code validation will end on June 20, 2016
  - Defects submitted after this date will be addressed on a best effort basis and the timelines above will not apply

* Note

1. These timelines are targeted but not guaranteed
2. These timelines apply only to this code validation program and not to any other existing or future version or program of CA SSO and other CA products and services

Requirement, Design and User Experience Validation

- We are currently conducting requirement, design and/or UX validation for following features for consideration in future releases*
  - JWT authentication scheme
  - FSS UI deprecation and replacement by Admin UI
  - OpenID Connect Authorization and Token Server support
  - REST APIs for policy management
  - IWA fallback to forms
  - Latest CA SSO news delivered directly to the SSO UI
- We welcome you to engage with us and help shape these features

* Note

1. These features are not planned to be delivered with CA SSO 12.6. Currently, customers can engage in requirement, design and/or UX validation, but not code validation.
2. By including these features in customer validation, no explicit or implicit commitment is being made regarding whether CA will GA these features, in which release and when?

Next Steps

- This program is available to a limited number of CA SSO customers and partners on a first come first served basis and based on fit
  - CA SSO 12.6 Code Validation – first 20 participants
  - Requirement, Design and User Experience Validation – first 2-3 participants per feature
- Selected participants will be invited to join the program via CA's central validation portal
- Please confirm you interest within next 2-3 days to secure your place in the program