CA Single Sign-On
Vision and Roadmap

June 2018

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 June 1, 2018 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 n**o 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.

Agenda

1 PRODUCT OVERVIEW

2 VISION AND STRATEGIC THEMES

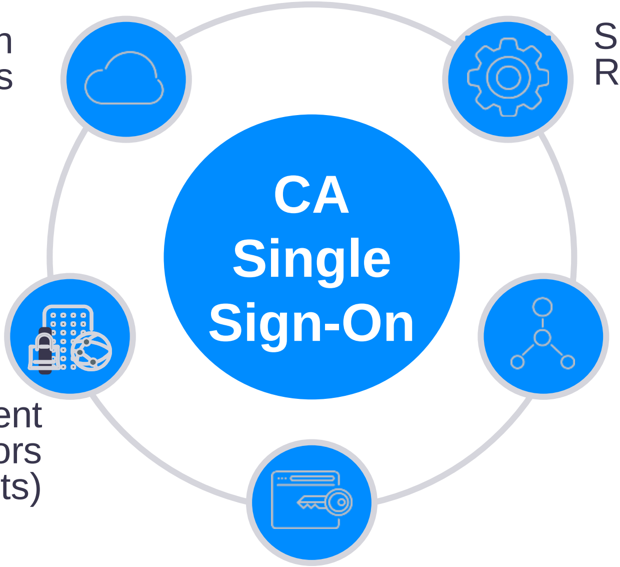
3 ROADMAP: DELIVERED & UNDER CONSIDERATION

4 BUILDING THE MODERN SOFTWARE FACTORY

5 SUMMARY AND QUESTIONS

Flexibility to Meet Evolving Needs

Application Integration Options



CA Single Sign-On

Open Standards

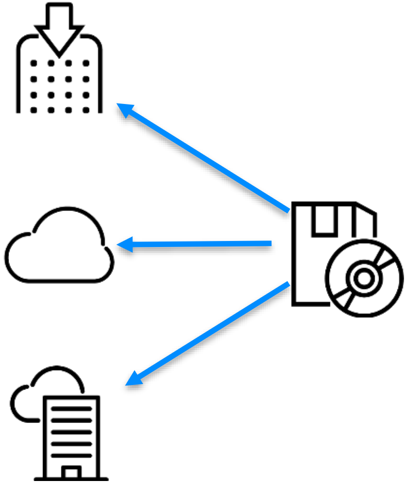
SOAP and REST APIs

Policy Enforcement Gateway (Access Gateway)

Open Format Token

Policy Enforcement Connectors (Agents)

Deployment Options



On-premises

In the cloud

Hybrid

Vision Statement

CA Single Sign-On

A market-leading access management solution, within a broader CA IAM solution, that is designed for easy adoption, rapid time-to-value, modern security standards, cloud-native deployment and DevOps practices to enable the Modern Software Factory.

Strategic Themes

Securely Enable Business

Comprehensive Access Mgmt.

Flexible Deployment

Cloud Ready & On-Premises

Improve ROI

App Experience with Lower TCO

VALUE DRIVERS

Broad Authn & Federation
Social Auth, Bio, Multi-factor, OIDC, SAML

Common Access Enforcement Layer
Efficient access control across app infrastructure

Comprehensive App Support
SaaS App, Web Svr, App Svr, ERP, Collaboration

Partner Eco System
Robust partner system to extend the solution

Scalability
Performance to meet service demand

Flexible Deployment Options
IaaS, SaaS,On-Premises

Please note that this presentation is for your informational purposes only does not serve as any technical user guides or documentation. There is no direct or indirect warranty provided pertaining the products and actual use may vary from the illustrations provided.

12.7 (May 2017)

Feature	Benefit	Feature Detail
REST interface for Policy Objects	▪ Accelerated method for access policy creation & update ▪ Easier to incorporate into a Dev Ops process	▪ REST interface for Policy Objects ▪ Complete Swagger documentation with examples
OpenID Connect OP	▪ Lightweight federation protocol to achieve single sign on to COTS and Custom applications	▪ Authorization Code flow ▪ Simple management in Admin UI
IWA Fall back to forms	▪ Simplify configuration and authentication for users that are frequently off the corporate network	▪ Offered as an out of the box authentication chaining method ▪ Top voted customer item from the community site
Improved authorization for JavaScript client apps	▪ Extending and simplifying the access policy administration for JavaScript clients	▪ Configuration of the response format for requests from Web 2.0 resources at global level ▪ Response in XML or JSON format

See the 12.7 Release Notes for information about other features in 12.7

Improved Security – IP Whitelisting

CA SSO 12.8

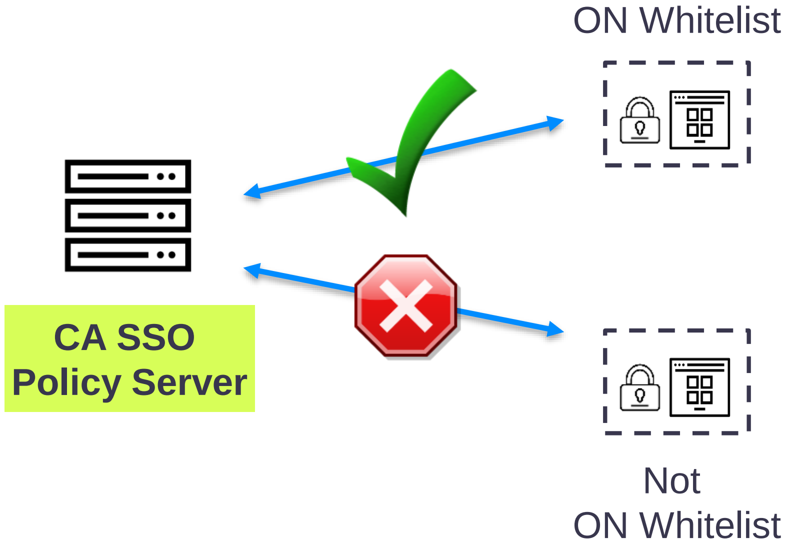
WHAT

Ability to define an IP whitelist for a trust-based authentication scheme

Supported Authentication Schemes:
- X.509 schemes
- Windows
- Custom

WHY

Improve Security – ensures user authentication only accepted from whitelisted CA SSO agents



ON Whitelist

CA SSO
Policy Server

Not
ON Whitelist

Improved Authentication – JWT Authentication

CA SSO 12.8

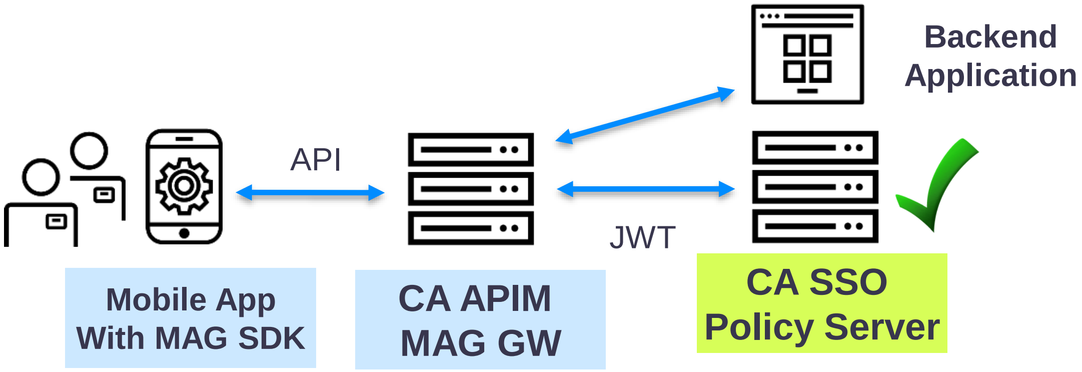
WHAT

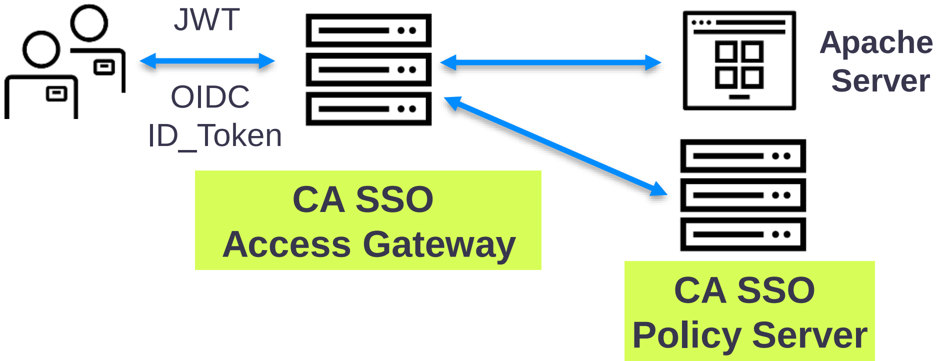
JSON Web Token (JWT) authentication scheme

WHY

Enables CA SSO to:

- Better integrate with CA APIM
- Accept OIDC Tokens generated by an OIDC provider for user authentication





Additional Application Support – JSON/REST

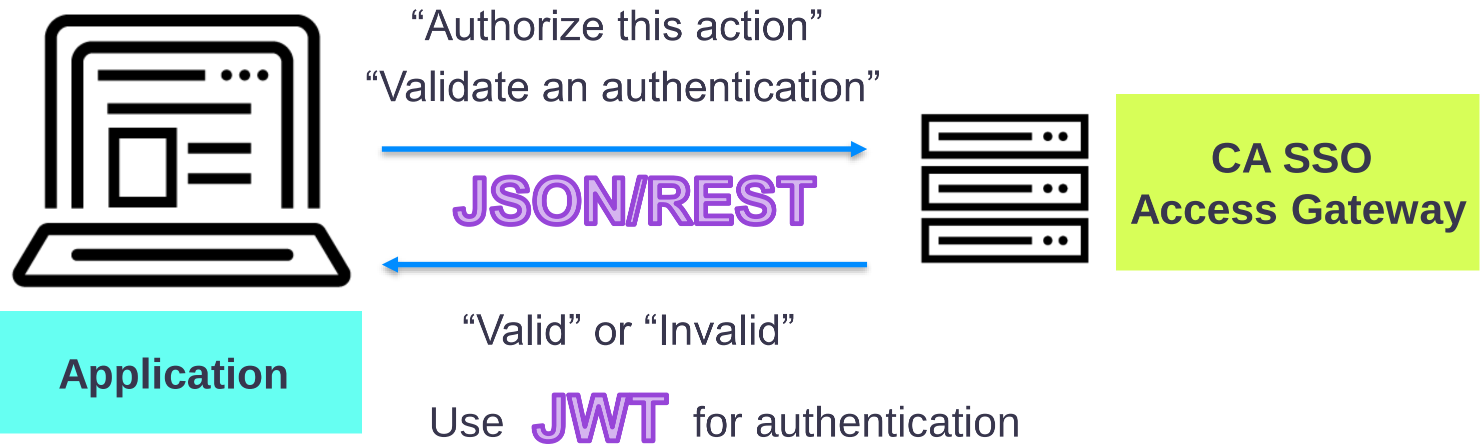
CA SSO 12.8

WHAT

JSON Request & Response for CA SSO to AuthN & AuthZ service interface

WHY

- Expands application types CA SSO can support
- Dynamic applications can directly call CA SSO for authentication and authorization via JSON (preferred data format for dynamic applications)



Use JWT for authentication

OIDC - Refresh Token

CA SSO 12.8

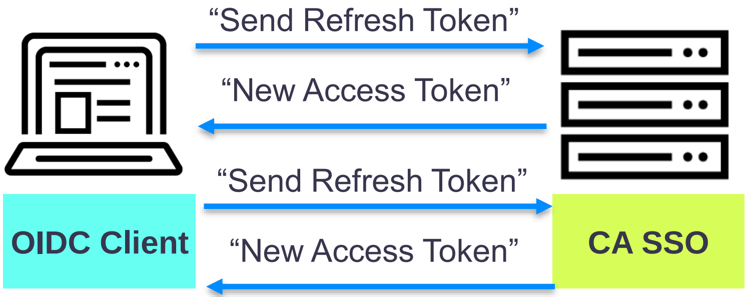
WHAT

Generate and support use of Refresh Token

WHY

- Simplifies end user experience
- Able to refresh access token with no additional authentications for the duration of the Refresh token

Situation: Access Token Times Out



OIDC - Proof Key Code Exchange

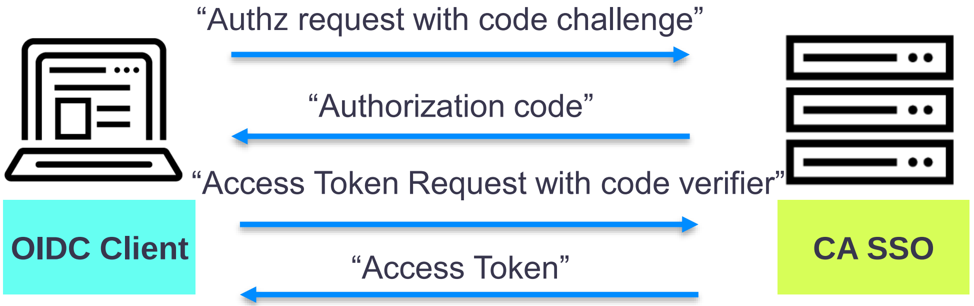
CA SSO 12.8

WHAT

In line method to securely identify public OIDC clients

WHY

- Blocks possible intercept of authorization code
- Used with Authorization code flow



“Authz request with code challenge”
“Authorization code”
“Access Token Request with code verifier”
“Access Token”
OIDC Client
CA SSO

OIDC - Implicit Flow

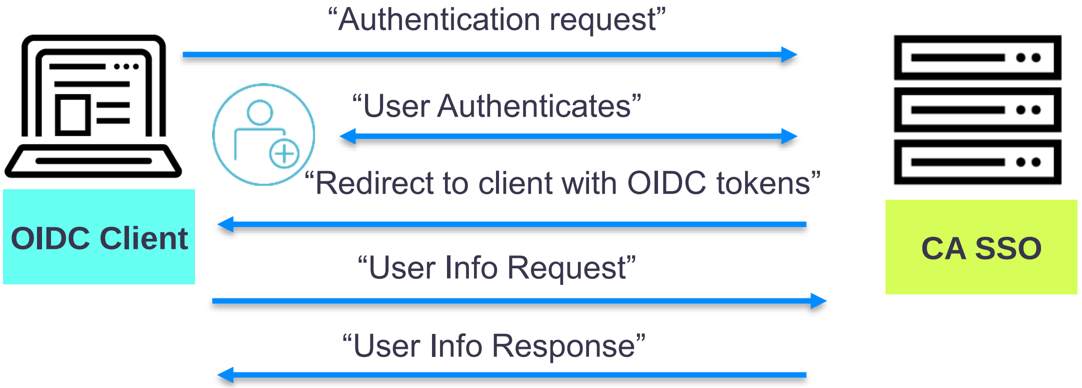
CA SSO 12.8

WHAT

A lighter OIDC flow

WHY

- Fewer redirects, which can be important for performance with **single page apps**
- Single page apps can store Access and ID token in browser



OIDC Client

CA SSO

“Authentication request”

“User Authenticates”

“Redirect to client with OIDC tokens”

“User Info Request”

“User Info Response”

OIDC - Step Up Authentication with ACR

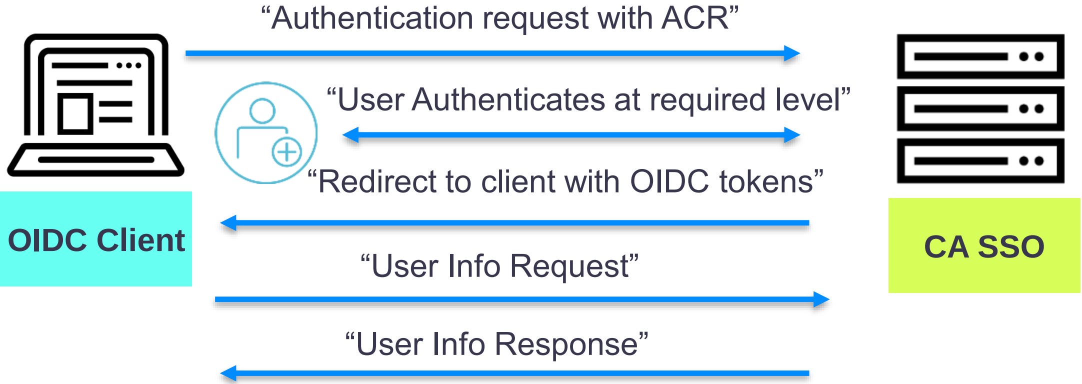
CA SSO 12.8

WHAT

Support for both step up authentication and authentication context request (ACR)

WHY

- Improved security controls
- Dynamic ability to respond to RP’s authentication requirement


“Authentication request with ACR”
“User Authenticates at required level”
“Redirect to client with OIDC tokens”
“User Info Request”
“User Info Response”
OIDC Client
CA SSO

Additional OIDC Support

CA SSO 12.8

WHAT

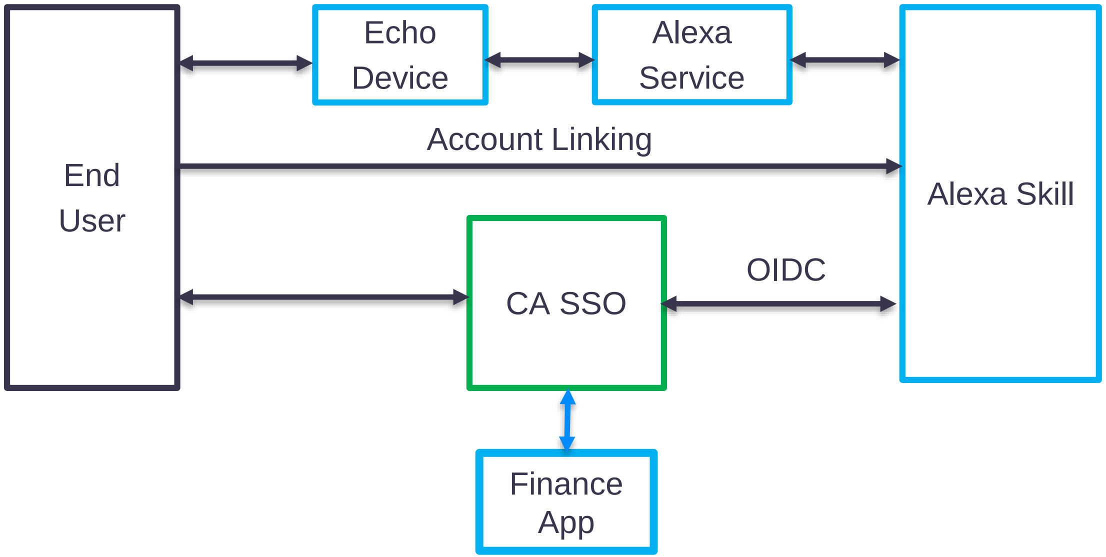
Additional OIDC enhancements

WHY

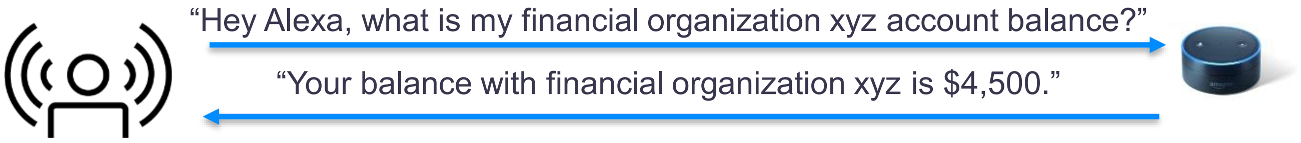
Enable CA SSO to support more of the applications and use cases for applications using OIDC

Feature	Value
User Attribute Mapping	Adds flexibility for integration and access mgmt.
Custom URI as Redirect URI	Adds flexibility for integration and access mgmt.
Custom OIDC Client IDs	Simplify administration
User Info Request in Query Format	Adds flexibility for integration and access mgmt.
Response to redirect_URI in encoded HTML form values	Adds flexibility for integration and access mgmt.
SSO as OIDC Resource Server	Adds flexibility for integration and access mgmt.

OIDC Use Case – Amazon Alexa

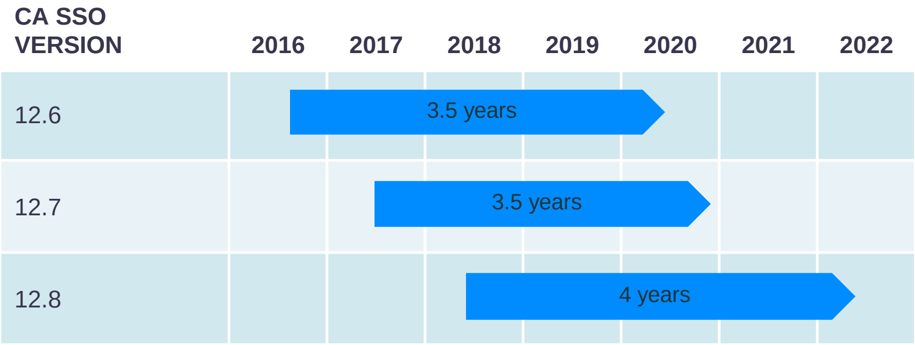


Integration instructions posted in the “Documents” section of the CA SSO Community site


“Hey Alexa, what is my financial organization xyz account balance?”

“Your balance with financial organization xyz is $4,500.”

Important Reminder



- Approaching EOS dates
  - CA SSO 12.52’s EOS date ***Feb. 28, 2019***
  - EOS does NOT include agents
- Please plan your path to upgrade to 12.8
  - 4 year mainstream life – longest of all GA’d versions
  - Defect fixes in all previously released CR’s & SP’s of all previous versions are in 12.8
  - CA is ready to assist you
- For more specific information about available help please
  - See the EOS announcements on CA SSO’ s “Release and Support Lifecycle” page

    Or
  - Contact CA Support

Roadmap: CA Single Sign-On

Timeline as of June 2018

	DELIVERED	UNDER CONSIDERATION
Product/ Releases	CA SSO 12.8	CA SSO

Marquee Features/ Business Value

DELIVERED – CA SSO 12.8

- **Enhanced OIDC federated single sign-on** improving user experience, security, and single page application support.
- **Agentless access control** for JSON-based applications.
- **JWT Authentication scheme** supports lightweight token and simplified integration for API gateway solutions
- **Improved security** for trust-based authentication methods via IP Whitelisting
- **Platform updates** including Windows 2016 support and internal library updates

UNDER CONSIDERATION – CA SSO

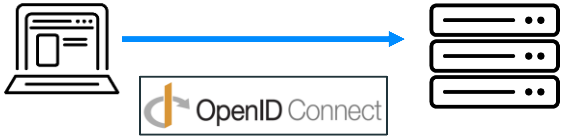
- **Authentication and Authorization Improvements**
  - **Enhanced standards-based SSO** through expanded support of federation standards and adjacent regulatory guidelines/requirements
  - **Improved advanced authentication support** with out of the box support for CA MFA as a Service
  - **Behavioral Access Control,** ranging from insight to dynamic control based on user behavior, with out of the box support for CA Threat Analytics as a Service
- **Architecture and Componentry**
  - **Simplify installation and deployment** via embedded installation of administration application and policy store
  - **Improved fit for Cloud deployment and auto-scaling** by delivering a Docker Container formatted CA SSO components
- **Improved security** via HSM support
- **Platform Updates**

Under Consideration

Authentication and Authorization

GOAL: Address additional use cases, improve ROI

- **Expanding OIDC Support**
  - Discovery - How clients discover information about OpenID Providers
  - Dynamic - How clients dynamically register with OpenID Providers
  - Session Management
  - Certified RP support
- **Authentication Improvements**
  - Additional authentication chaining options
  - Out of the box support for multi-factor authentication via CA IDaaS
- **Enhanced support for identity regulations**
  - GDPR – expanding flexibility of user consent for their attributes
  - eIDAS - ensuring support for federation specification requirements
  - NIST 800-63C – Federation and Assertions



NGINX

NIST National Institute of Standards and Technology U.S. Department of Commerce

OIDC Provider: Discovery Profile

FEATURE

- CA SSO OpenID Provider publishes its metadata at a well-known URL
- Well-known URL returns a JSON listing of OpenID endpoints, supported scopes and claims, public keys used to sign the tokens, and other details

VALUE

✓ **Simplifies application integration to CA SSO** - Client or Relying Party can use this information to construct a request dynamically to the OpenID Provider

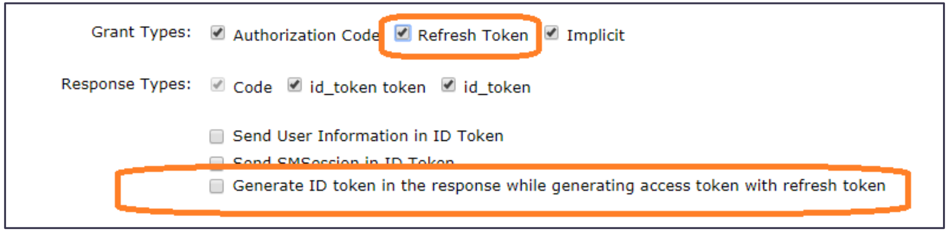
OIDC Provider: Generate ID Token in Refresh Token Flow

FEATURE

- Refresh token flow generates new ID token along with Access token
- New ID token will be generated with modified value for ‘iat’ i.e current time
- Generation of ID token is optional configuration in the Refresh token flow

VALUE

✓ **Expands integration use cases:** If any Relying Party validates the ID token, then client expects the ID token to be generated in the refresh token flow along with the access token



Grant Types:	☑ Authorization Code ☑ Refresh Token ☑ Implicit
Response Types:	☑ Code ☑ id_token token ☑ id_token
	□ Send User Information in ID Token
	□ Send SMSession in ID Token
	□ Generate ID token in the response while generating access token with refresh token

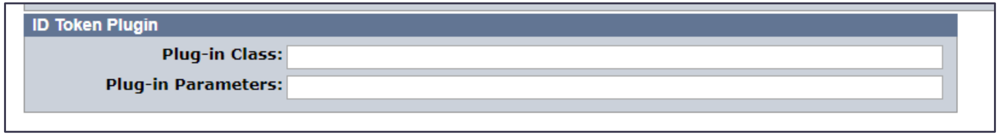
OIDC Provider: Custom ID Token Generator Plugin

FEATURE

- Allows to generate custom claims in both ID Token and User Info response using ID Token Generate Plugin
- Provide an option in **Authorization Provider** to configure fully qualified **class name and parameter** for ID Token Plugin

VALUE

✓ **Simplifies and enables more application integration** - If Relying Party expects the claims in a format or specific values for the claims in the ID Token, in such cases CA SSO OIDC Provider allows to customize the id token before generating to RP



ID Token Plugin

Plug-in Class:

Plug-in Parameters:

SAML 2.0 IDP – Identity Mapping

TARGET FEATURE

- **Identity Mapping** capability in SAML 2.0 allows to authenticate user from one directory and use another directory for authorization

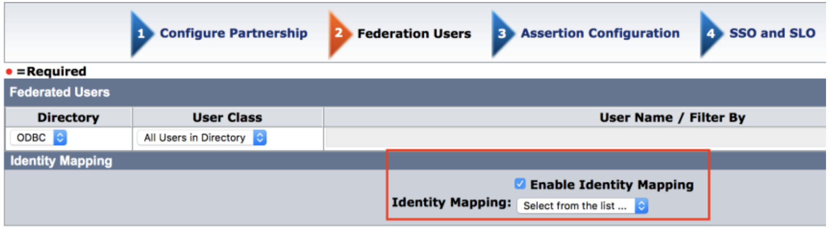
VALUE

- ✓ **Simplifies cost of managing federation** - It allows to keep the separate directories, one for authentication and other for authorization for external applications (Federations) to avoid the replication user details into a single directory.
- ✓ **Highly voted item in the Community site**

SAML 2.0 IDP – Identity Mapping

FEATURE BEHAVIOR

- Configurable option to enable/disable ‘Identity Mapping’
- In Runtime, validation of user happens with one directory and authorization of user happens with other user directory, assertion attributes are retrieved from authorization user store i.e., second user store



● =Required

Federated Users

Directory	User Class	User Name / Filter By
ODBC	All Users in Directory	

Identity Mapping

☑ Enable Identity Mapping

Identity Mapping: Select from the list ...

eIDAS (electronic IDentification, Authentication and trust Services)

TARGET FEATURE

- **eIDAS** is an EU regulation on / a set of standards for electronic identification and trust services for electronic transactions in the European Single Market.
- **CA SSO SAML 2.0 federation partnerships** supports exchange messages including personal and technical attributes to support cross-border identification and authentication processes in compatible with eIDAS framework

VALUE

✓ **Make cross-border electronic transactions more secure and trustworthy** - Clients will be allowed to use CA SSO SAML 2.0 Federation partnerships to authenticate the users across borders as defined by eIDAS framework

eIDAS (electronic IDentification, Authentication and trust Services)

TARGETED CAPABILITIES

Capabilities targeted for SAML 2.0 IDP to support eIDAS framework

- Support for ECDSA certificates and private keys
- New Signing Algorithms.
- Support Organization and Contact tags in IDP Metadata
- Support Friendlyname in the attributes
- Honor requested claims in Authentication Request
- Support for Extensions tag in IDP Metadata

Note: SAML 2.0 Service Provider specific capabilities for eIDAS conformance not covered in this document

Recording User Consent

FEATURE

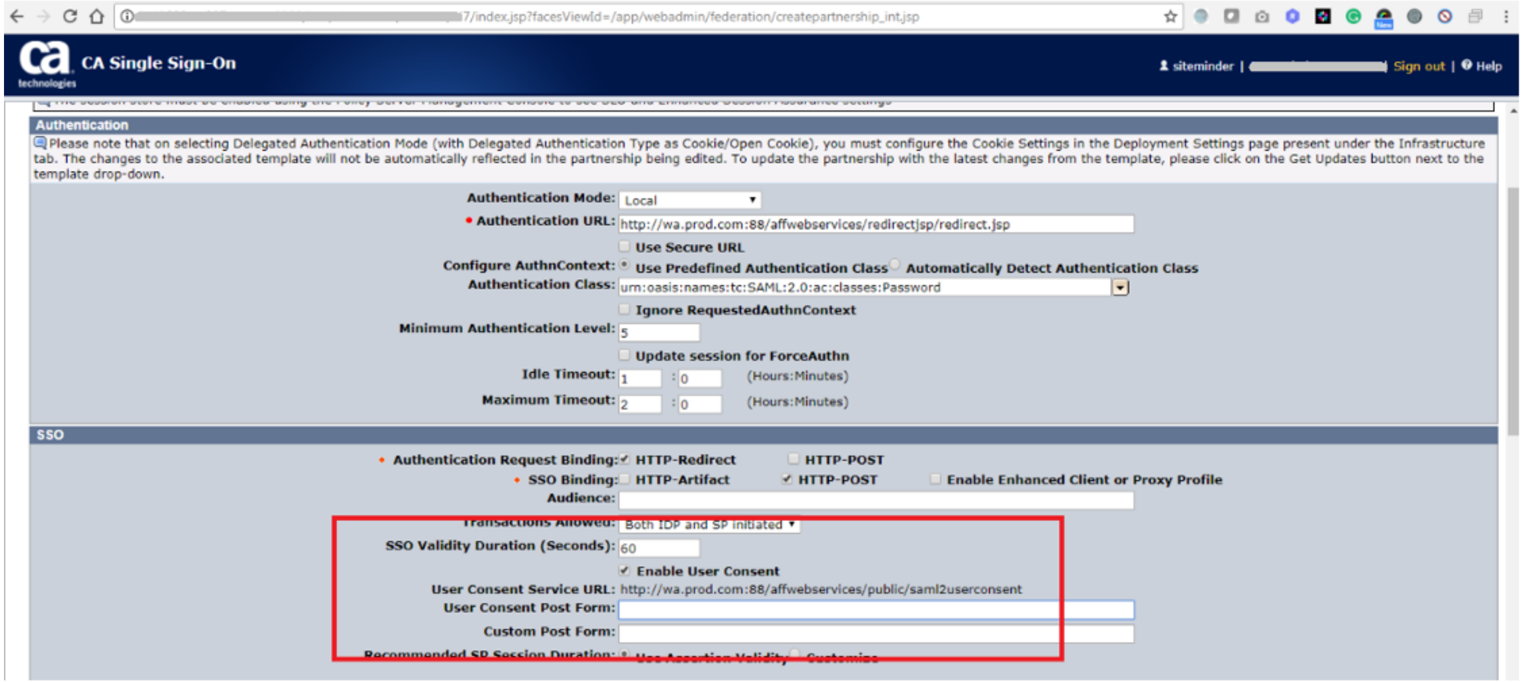
- Ability to record user consent in audit logs, in the case of OIDC and SAML2 flows, when user consent is configured

VALUE

✓ **Improve compliance with GDPR Article 7**

SAML2 Consent Form Snapshot

SAML2 CONSENT CONFIGURATION (**AS IT EXISTS TODAY**)



[redacted]7/index.jsp?facesViewId=/app/webadmin/federation/createpartnership_int.jsp

CA Single Sign-On

siteminder | [redacted] Sign out | Help

The session store must be enabled using the Policy Server Management Console to use SLO and Enhanced Session Assurance settings

Authentication

Please note that on selecting Delegated Authentication Mode (with Delegated Authentication Type as Cookie/Open Cookie), you must configure the Cookie Settings in the Deployment Settings page present under the Infrastructure tab. The changes to the associated template will not be automatically reflected in the partnership being edited. To update the partnership with the latest changes from the template, please click on the Get Updates button next to the template drop-down.

Authentication Mode: Local ▾

• **Authentication URL:** http://wa.prod.com:88/affwebservices/redirectjsp/redirect.jsp

□ **Use Secure URL**

Configure AuthnContext: ● **Use Predefined Authentication Class** ○ **Automatically Detect Authentication Class**

Authentication Class: urn:oasis:names:tc:SAML:2.0:ac:classes:Password

□ **Ignore RequestedAuthnContext**

Minimum Authentication Level: 5

□ **Update session for ForceAuthn**

Idle Timeout: 1 : 0 (Hours:Minutes)

Maximum Timeout: 2 : 0 (Hours:Minutes)

SSO

• **Authentication Request Binding:** ☑ **HTTP-Redirect** □ **HTTP-POST**

• **SSO Binding:** □ **HTTP-Artifact** ☑ **HTTP-POST** □ **Enable Enhanced Client or Proxy Profile**

Audience:

Transactions Allowed: Both IDP and SP initiated ▾

SSO Validity Duration (Seconds): 60

☑ **Enable User Consent**

User Consent Service URL: http://wa.prod.com:88/affwebservices/public/saml2userconsent

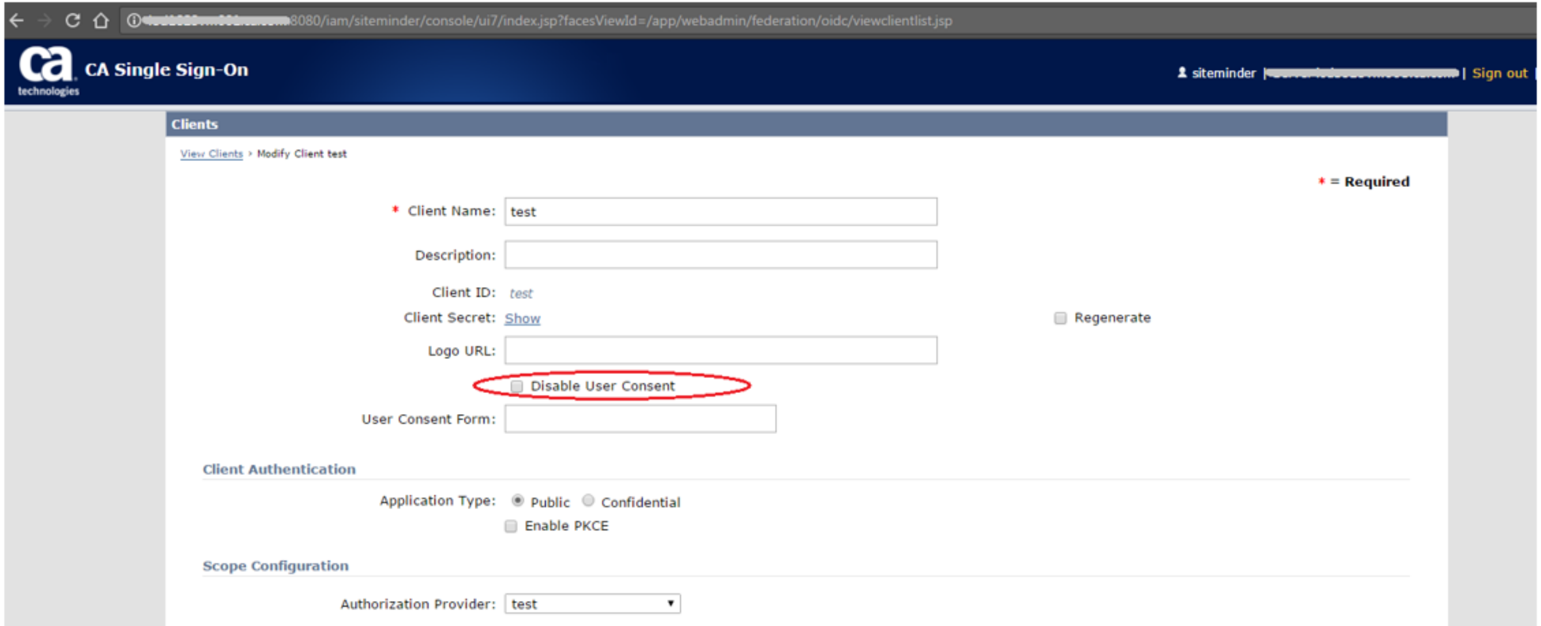
User Consent Post Form:

Custom Post Form:

Recommended SP Session Duration: ● **Use Assertion Validity** ○ **Customize**

OIDC Consent Form Snapshot

OIDC CLIENT CONFIGURATION PAGE (**AS IT EXISTS TODAY**)



[redacted]8080/iam/siteminder/console/ui7/index.jsp?facesViewId=/app/webadmin/federation/oidc/viewclientlist.jsp

CA Single Sign-On

siteminder | [redacted] | Sign out

Clients

View Clients > Modify Client test

* = **Required**

* Client Name:	test
Description:	
Client ID:	*test*
Client Secret:	Show □ Regenerate
Logo URL:	
	□ Disable User Consent
User Consent Form:	

Client Authentication

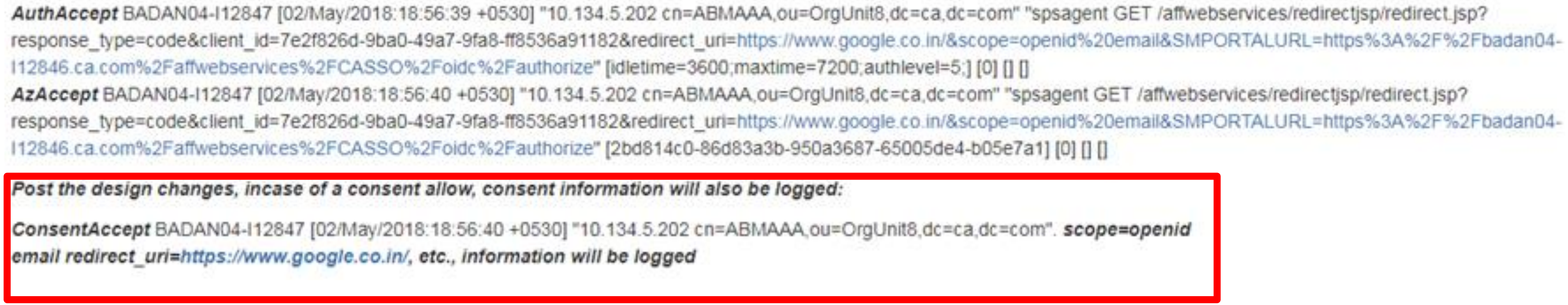
Application Type:	● Public ○ Confidential
	□ Enable PKCE

Scope Configuration

Authorization Provider:	test ▾

SAMPLE LOG FORMAT ENHANCEMENT

AUDIT LOG ENHANCEMENT (OIDC EXAMPLE REFERRED HERE)



```
AuthAccept BADAN04-I12847 [02/May/2018:18:56:39 +0530] "10.134.5.202 cn=ABMAAA,ou=OrgUnit8,dc=ca,dc=com" "spsagent GET /affwebservices/redirectjsp/redirect.jsp?
response_type=code&client_id=7e2f826d-9ba0-49a7-9fa8-ff8536a91182&redirect_uri=https://www.google.co.in/&scope=openid%20email&SMPORTALURL=https%3A%2F%2Fbadan04-
I12846.ca.com%2Faffwebservices%2FCASSO%2Foidc%2Fauthorize" [idletime=3600;maxtime=7200;authlevel=5;] [0] [] []
AzAccept BADAN04-I12847 [02/May/2018:18:56:40 +0530] "10.134.5.202 cn=ABMAAA,ou=OrgUnit8,dc=ca,dc=com" "spsagent GET /affwebservices/redirectjsp/redirect.jsp?
response_type=code&client_id=7e2f826d-9ba0-49a7-9fa8-ff8536a91182&redirect_uri=https://www.google.co.in/&scope=openid%20email&SMPORTALURL=https%3A%2F%2Fbadan04-
I12846.ca.com%2Faffwebservices%2FCASSO%2Foidc%2Fauthorize" [2bd814c0-86d83a3b-950a3687-65005de4-b05e7a1] [0] [] []
```

Post the design changes, incase of a consent allow, consent information will also be logged:

ConsentAccept BADAN04-I12847 [02/May/2018:18:56:40 +0530] "10.134.5.202 cn=ABMAAA,ou=OrgUnit8,dc=ca,dc=com". ***scope=openid email redirect_uri=https://www.google.co.in/, etc., information will be logged***

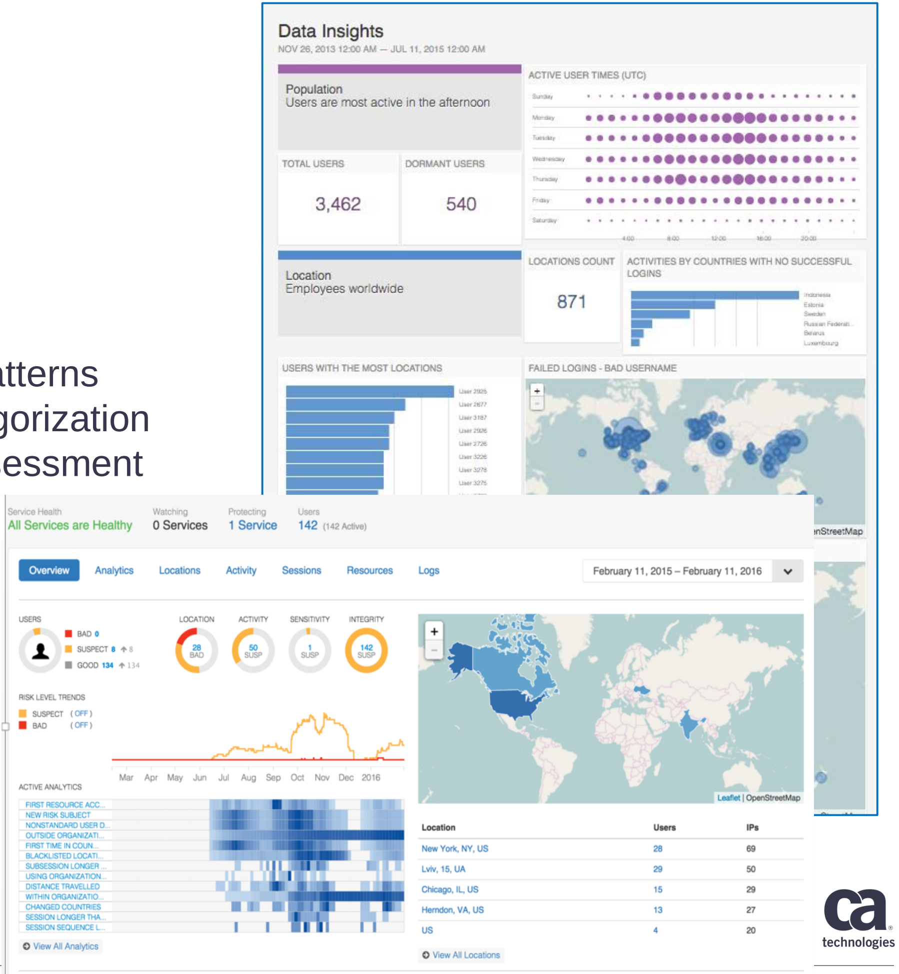
What other support for GDPR do you need or expect from CA SSO?

Under Consideration

Authentication and Authorization

GOAL: Address additional use cases, improve ROI

- **Threat Analytics for CA SSO**
  - Identify threats
    - based on authentication and access patterns
    - enhanced via resource sensitivity categorization
  - Enforcement options driven by the threat assessment
    - Log the risk assessment
    - Force a reauthentication
    - Force a step up authentication
    - Revoke a session
    - Turn on session monitoring (via CA PAM)



Data Insights

NOV 26, 2013 12:00 AM — JUL 11, 2015 12:00 AM

Population
Users are most active in the afternoon

TOTAL USERS: 3,462

DORMANT USERS: 540

Location
Employees worldwide

LOCATIONS COUNT: 871

Service Health: All Services are Healthy

Watching: 0 Services

Protecting: 1 Service

Users: 142 (142 Active)

February 11, 2015 – February 11, 2016

USERS: BAD 0; SUSPECT 8 ↑ 8; GOOD 134 ↑ 134

LOCATION: 28 BAD

ACTIVITY: 50 SUSP

SENSITIVITY: 1 SUSP

INTEGRITY: 142 SUSP

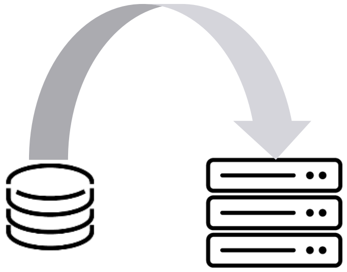
RISK LEVEL TRENDS: SUSPECT (OFF); BAD (OFF)

Location	Users	IPs
New York, NY, US	28	69
Lviv, 15, UA	29	50
Chicago, IL, US	15	29
Herndon, VA, US	13	27
US	4	20

ca technologies

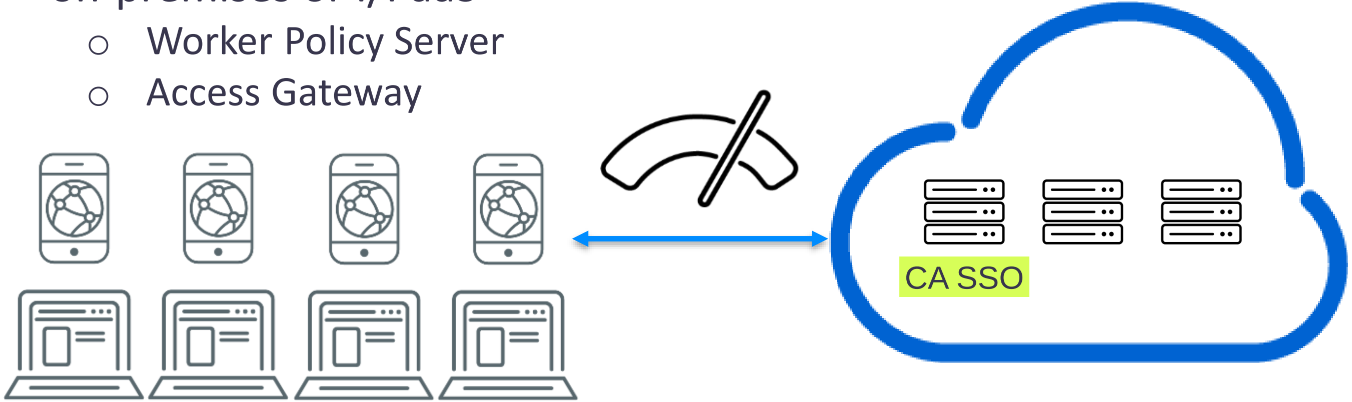
Under Consideration

Architecture and Componentry



GOAL: Cloud Ready, Lower Cost of Ownership

- Embedded policy store for simpler deployment and upgrade
- Improving fit of CA SSO in auto-scaling environments
- Docker container form factor with support for Kubernetes orchestration for on-premises or I/PaaS
  - ○ Worker Policy Server
  - ○ Access Gateway



Container Form Factor For Policy Server

FEATURE

- Provide the below Docker Images
  - ➢ Separate Docker Image consisting of WAM UI & Policy Server Functions Combined
  - ➢ Separate Docker Image for Policy Server Functions
- Provide **Kubernetes Manifest files for a Sample Deployment.

**Knowledge of Dockers and Kubernetes will be essential to setup these container images in the Kubernetes environment

VALUE

✓ **Improved TCO** by supporting the deployment of policy servers and WAM UI in the container ecosystem and therefore leverage the inherent abilities of container ecosystem

- Auto-scaling
- Accelerated Upgrades
- Portability

Other Capabilites Under Consideration

FUTURE WORK – OTHER TARGETED CAPABILITIES

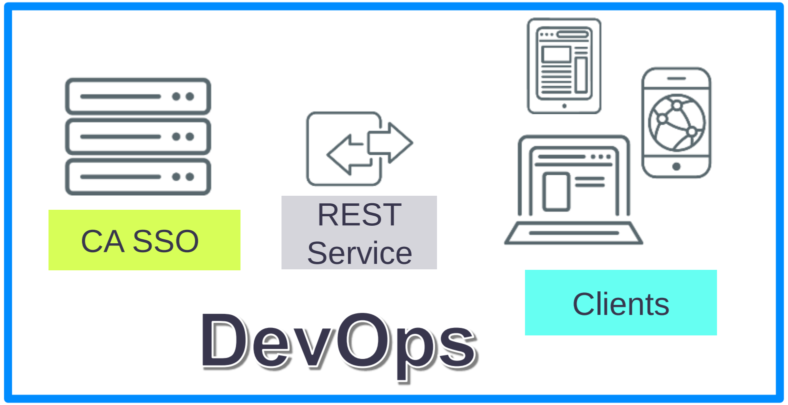
- Support for Deployment Using HELM.
- Sample Configurations for Rolling Upgrades
- Sample Configurations for Patch Management
- Sidecar Container Implementation to Support Custom Add-ons and Integrations
- Certification on RedHat OpenShift and AWS EKS platforms

Under Consideration

Architecture and Componentry

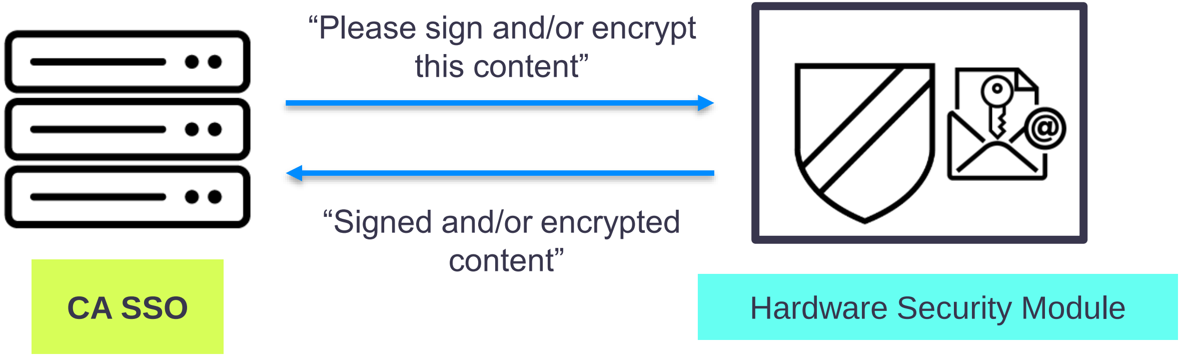
GOAL: Cloud Ready, Lower Cost of Ownership

- Install of Admin App & UI in base Policy Server install process
- Expansion of REST interface to additional administrative functions
  - Console
  - Registry Settings



Under Consideration

Enhance Security



“Please sign and/or encrypt this content”

“Signed and/or encrypted content”

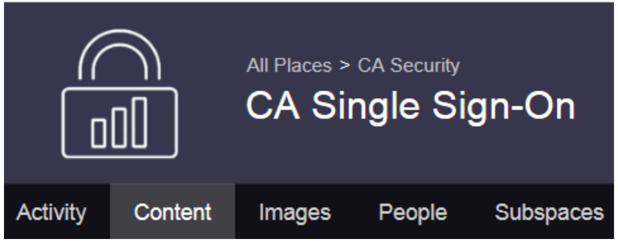
CA SSO

Hardware Security Module

Influencing our Roadmap

CA Communities Ideation

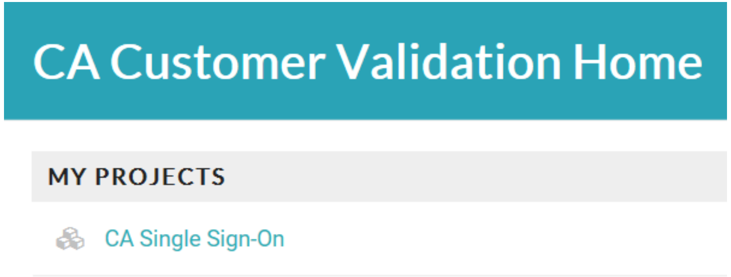
- Submit your ideas on communities.ca.com
- Vote and comment on ideas that are important to you
- CA Product Management reviews ideas and updates status
- “Currently Planned” idea status indicates inclusion in Agile Backlog or Product Roadmap


All Places > CA Security

CA Single Sign-On

Customer Validation

- Register to participate in private:
  - Use case forums
  - Design review webinars
  - Pre-Release versions with development team support for download and testing (Beta)
- Enroll at: validate.ca.com


CA Customer Validation Home

MY PROJECTS

CA Single Sign-On

Questions

Thank You.

Herb Mehlhorn
Sr. Director, Product Management
Herbert.Mehlhorn@ca.com

@cainc

slideshare.net/CAinc

linkedin.com/company/ca-technologies

ca.com