

A Miracle Pill for Enterprise SAML

David Brossard | Sam Rosen | Pranesh Radhakrishnan



**David
Brossard**



**Pranesh
Radhakrishnan**

Senior Software Engineer
Salesforce



**Sam
Rosen**

Director Product Mgmt
Salesforce

tried to kill How we ~~killed~~ SAML ... 1.1

but we really had to first help customers first
move to SAML 2.0 and that takes a lot of time
so SAML 1.1 is still around but this makes for
a really poor clickbait title

Mission... possible?

Mission Statement

General upkeep and maintenance of internal libraries

Keep up-to-date with latest innovations

Stay on top of any known vulnerabilities in third-party libraries

Offer latest SAML features (if any)





SAML as the SP
(Service Provider)

SAML as the IdP
(Identity Provider)

Where is SAML even used?

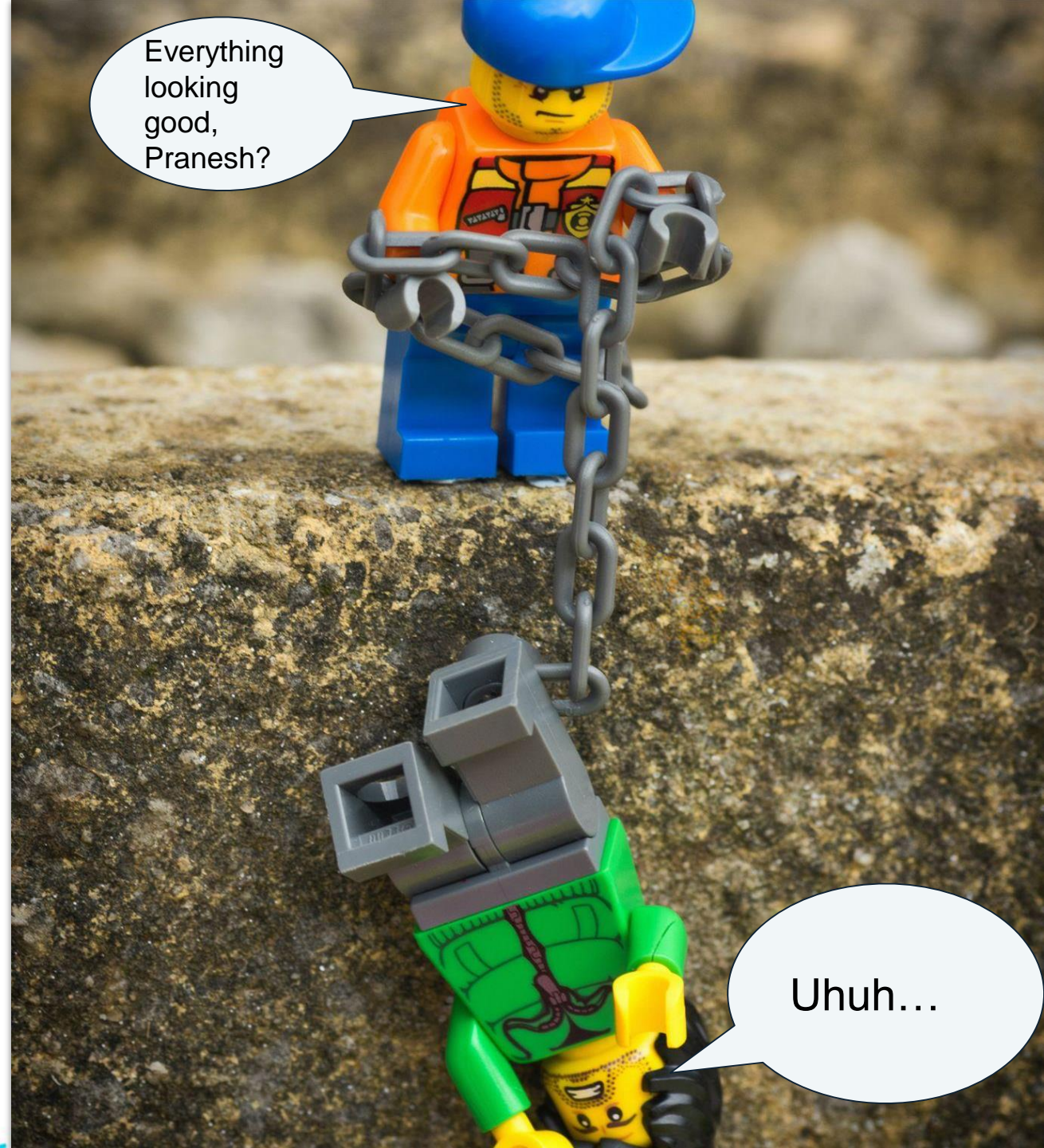
Easy, right?



Mission i(a)mpossible?

The Challenge

- Support for SAML 1.1 very different
- Library contents & structure overhauled
- Functional changes in some methods
- Feature gaps in old version fixed in new one
 - Need to remove custom code



**How we
suddenly felt**



The Opportunity



Reduce feature set we offer

Migrate away from SAML 1.1

Deprecate 'single-config SAML'

Focus features customers want

- *Customize a SAML request*



***It's not like
anyone
uses SAML
1.1
anymore,
right?***

***So
what?***

Right?

Even so, standards be standards?

Yes but...

Migrating from SAML 1.1 to SAML 2.0 does require updating configuration on both sides of the fence:

- the SP
- the IdP



Single-config SAML vs. Multi-config SAML

Prior to 2013, a single SAML config is allowed:

- IdP-initiated only
- Support for SAML 1.1 and SAML 2.0

After 2013, multiple SAML configs allowed:

- SAML 2.0 only
- SP-init and IdP-init
- Connect to multiple IdPs
e.g. Azure AD and Okta
- Let a user choose or apply login discovery

Single Sign-On Settings

[Help f](#)

Configure single sign-on in order to authenticate users in salesforce.com and related environments. Your organization has the following options available for single sign-on:

- Delegated authentication is a single sign-on method that uses a Web Services call sent from salesforce.com to an endpoint.
- Federated authentication, a single sign-on method that uses SAML assertions sent to a Salesforce endpoint.

Edit

Enable Multiple Configs

SAML Assertion Validator

Download Metadata

Delegated Authentication

Disable login with Salesforce
credentials



Delegated Gateway URL

Force Delegated Authentication
Callout



Federated Single Sign-On Using SAML

SAML Enabled



User Provisioning Enabled



SAML Identity Type

Username

SAML Version

2.0

SAML Identity Location

Subject

Issuer

https://login.salesforce.com/

Identity Provider Certificate

CN=Axiom Demo Certificate, OU=FOR DEMONSTRATION
PURPOSES ONLY. DO NOT USE FOR PRODUCTION
ENVIRONMENTS., O=Axiom SSO, L=San Francisco, ST=CA,
C=US
Expiration: 5 Nov 2041 04:30:27 GMT

Make Federation ID case-
insensitive



Identity Provider Login URL

Custom Logout URL

Custom Error URL

Salesforce Login URL

https://login.stmfa.stm.salesforce.com

OAuth 2.0 Token Endpoint

https://login.stmfa.stm.salesforce.com/services/oauth2/token

Entity ID

https://saml.salesforce.com 

Service Provider Initiated Request
Binding

HTTP POST

Edit

Enable Multiple Configs

SAML Assertion Validator

Download Metadata

Getting started

Battle Plan (PM - Eng - Arch initiative)

1. Onboard the third-party library
 - a. Get it approved for internal use
 - b. Add to our own internal repository
2. Plan & execute the engineering work
 - a. Identity areas we can upgrade without impacting a customer
 - b. Draw the line between 'inbound' and 'outbound'
 - c. Identify customers that use SAML 1.1 and/or Single-config
3. Plan the customer communications plan
 - a. For all customers
 - b. For customers we know will be impacted
4. Deploy
 - a. Roll out code updates
 - b. Clean up (rinse & repeat)

Inbound vs. Outbound?

Inbound SAML

Salesforce consumes SAML from the outside world

We can write code paths that adapt

No customer involvement required

Examples:

- Salesforce (SP) receives a SAML response from the IdP
- Salesforce (IdP) receives a SAML request from an SP
- SAML 2.0 Single Logout Protocol (SP/IdP)



Outbound SAML

Salesforce sends SAML to the outside world

We hope the recipient can handle the updated content

Customer communications required

Examples:

- Salesforce (SP) sends a SAML request to the IdP
- Salesforce (IdP) sends a SAML response to an SP
- SAML metadata config downloads

We need to talk

Fortunately, we're good at talking

Dedicated communications team

Well-oiled comms & release
processes

- Release updates
- Release notes
- Help site
- Dedicated communications
- Follow-up emails and reminders
- In-app upgrade process & guide



IDENTITY

THE 5 BEST IAM
STANDARDS THIS YEAR

MAGAZINE

Is OAuth the
SAML killer?
How I changed
my SAML request
@lovesaml

SAML 1.1
END OF
AN ERA

NO.123456

The Release Update

Full [notes here](#).

[SALESFORCE HELP](#) > [DOCS](#) > [SALESFORCE RELEASE NOTES](#)

Upgrade SAML Single Sign-On Framework (Release Update)

Salesforce is upgrading its SAML framework as part of regular ongoing maintenance. This update can impact integrations with third-party systems, such as integrations with SAML identity providers and SAML-enabled applications. This update applies to all SAML-based integrations, even when you're using Identity for Employees or Salesforce Customer Identity, including Experience Cloud.

Where: This change applies to Lightning Experience and Salesforce Classic in all editions.



When: Salesforce enforces this update in **Spring '23**. To get the major release upgrade date for your instance, go to [Trust Status](#), search for your instance, and click the maintenance tab.

Why: This maintenance update improves your org's security posture and potentially increases the platform's performance. Some SSO URLs are now encoded. For service provider-initiated SSO, the Identity Provider URL and Assertion Consumer Service (ACS) URL are encoded. For all single logout configurations, the Single Logout Endpoint and relay state parameter are encoded. All existing SAML-based integrations are potentially impacted.

How: Because Salesforce uses SAML to integrate with third-party systems, this upgrade can break integrations on the third party's side. To avoid disruptions, apply this release update and test your SAML integrations.

To review this update, from Setup, in the Quick Find box, enter Release Updates, and then select **Release Updates**. For **Upgrade SAML Single Sign-On Framework**, follow the testing and activation steps.

Upgrade SAML Single Sign-On Framework

 **COMPLETE STEPS BY: SEP 10, 2022**  TEST RUN SUPPORTED 

Salesforce is upgrading its SAML framework as part of regular ongoing maintenance. This update can impact integrations with third-party systems. For example, this update can impact integrations with SAML identity providers or SAML-enabled applications. This update applies to every SAML-based integration, whether you're using Identity for Employees or Salesforce Customer Identity, including Experience Cloud.

▼ [What's changing?](#)

With this update, Salesforce now uses `saml2p` and `saml2` as namespace prefixes in XML-based SAML artifacts generated such as a request or a response. Also, some SSO URLs are now encoded. For service provider-initiated SSO, the Identity Provider URL and Assertion Consumer Service (ACS) URL are encoded. For all single logout configurations, the Single Logout Endpoint and relay state parameter are encoded. Any existing SAML-based integrations are potentially impacted.

➤ What improvements can I see?

➤ How is my org impacted?



Get all the help you need

Prepare your org

- Before enabling this update, verify that your SAML-based third-party integrations work as expected.
- If you use Salesforce with a third-party identity provider, such as Okta, test your ability to log in using SSO.
- If you use Salesforce as a SAML identity provider, test all the applications that use it for SSO.

Upgrade SAML Single Sign-On Framework

 COMPLETE STEPS BY: SEP 10, 2022  TEST RUN SUPPORTED 

Salesforce is upgrading its SAML framework as part of regular ongoing maintenance. This update can impact integrations with third-party systems. For example, this update can impact integrations with SAML identity providers or SAML-enabled applications. This update applies to every SAML-based integration, whether you're using Identity for Employees or Salesforce Customer Identity, including Experience Cloud.

> What's changing?

> What improvements can I see?

✓ [How is my org impacted?](#)

Because SAML is used to integrate Salesforce with third-party systems, this upgrade can break integrations on the third party's side. To avoid disruptions, use this release update and test these SAML integrations:

- SSO with a third-party identity provider
- SSO using Salesforce as an identity provider
- SSO metadata downloads with Salesforce acting as the service provider or identity provider
- All single logout configurations



Get all the help you need

Prepare your org

- Before enabling this update, verify that your SAML-based third-party integrations work as expected.
- If you use Salesforce with a third-party identity provider, such as Okta, test your ability to log in using SSO.
- If you use Salesforce as a SAML identity provider, test all the applications that use it for SSO.

Quick Find / Search...

Expand All | Collapse All



Lightning Experience Transition Assistant

Move to the new, more
productive Salesforce.

Get Started

Salesforce Mobile Quick Start

Home

Administer

Release Updates

- ▶ Manage Users
- ▶ Manage Apps
- ▶ Manage Territories
- ▶ Company Profile
- ▶ Data Classification
- ▶ Privacy Center
- ▶ Security Controls
- ▶ Domain Management
- ▶ Communication Templates
- ▶ Translation Workbench
- ▶ Data Management
- ▶ Mobile Administration
- ▶ Desktop Administration
- ▶ Outlook Integration and Sync
- ▶ Gmail Integration and Sync
- ▶ Email Administration



SETUP > [RELEASE UPDATES](#)

Upgrade SAML Single Sign-On Framework

Salesforce is upgrading its SAML framework as part of regular ongoing maintenance. This update can impact integrations with third-party systems. For example, this update can impact integrations with SAML identity providers or SAML-enabled applications. This update applies to every SAML-based integration, whether you're using Identity for Employees or Salesforce Customer Identity, including Experience Cloud.



COMPLETE STEPS BY: SEP 10, 2022



ENFORCEMENT SCHEDULED: WINTER '23

SECURITY

TEST RUN SUPPORTED



What's changing?

With this update, Salesforce now uses saml2p and saml2 as namespace prefixes in XML-based SAML artifacts generated such as a request or a response. Also, some SSO URLs are now encoded. For service provider-initiated SSO, the Identity Provider URL and Assertion Consumer Service (ACS) URL are encoded. For all single logout configurations, the Single Logout Endpoint and relay state parameter are encoded. Any existing SAML-based integrations are potentially impacted.

> What improvements can I see?

> How is my org impacted?

Understand and minimize the impact of these changes with our step-by-step guide



You can enable and disable the update during the test period, which ends on the "Complete steps by" date. For a sandbox org, the test period can end early with a release upgrade.

Enable Test Run

Complete the steps and get your org ready for the update.

0% Complete

> 1 Assess the impact of this release update



HELP & TRAINING



SAML Single Sign-On with Salesforce as the Service Provider



Salesforce as a SAML Identity Provider



Configure SAML SSO Between Salesforce Orgs or Experience Cloud Sites



Single Logout

Update History

Rogue Nation

aka those using SAML
1.1

Identify customers that use SAML 1.1 and/or Single-config SAML

1. Look at customer metadata configuration
2. Look at login data
3. Engage with the customers and plan their migration path
 - a. Good news: there are only a handful of customers
 - b. Bad news: not high priority (if it ain't broke...)

Fallout

Technical Hurdles

- Library packaging & dependencies
 - Things moved around
- Library cohabitation
 - Migration strategy
 - Running 2 versions of the library at the same time
- XML handling
 - XML is XML, not string
 - Canonicalization
- SAML features
 - Encoding, RelayState
- Customer Custom Code



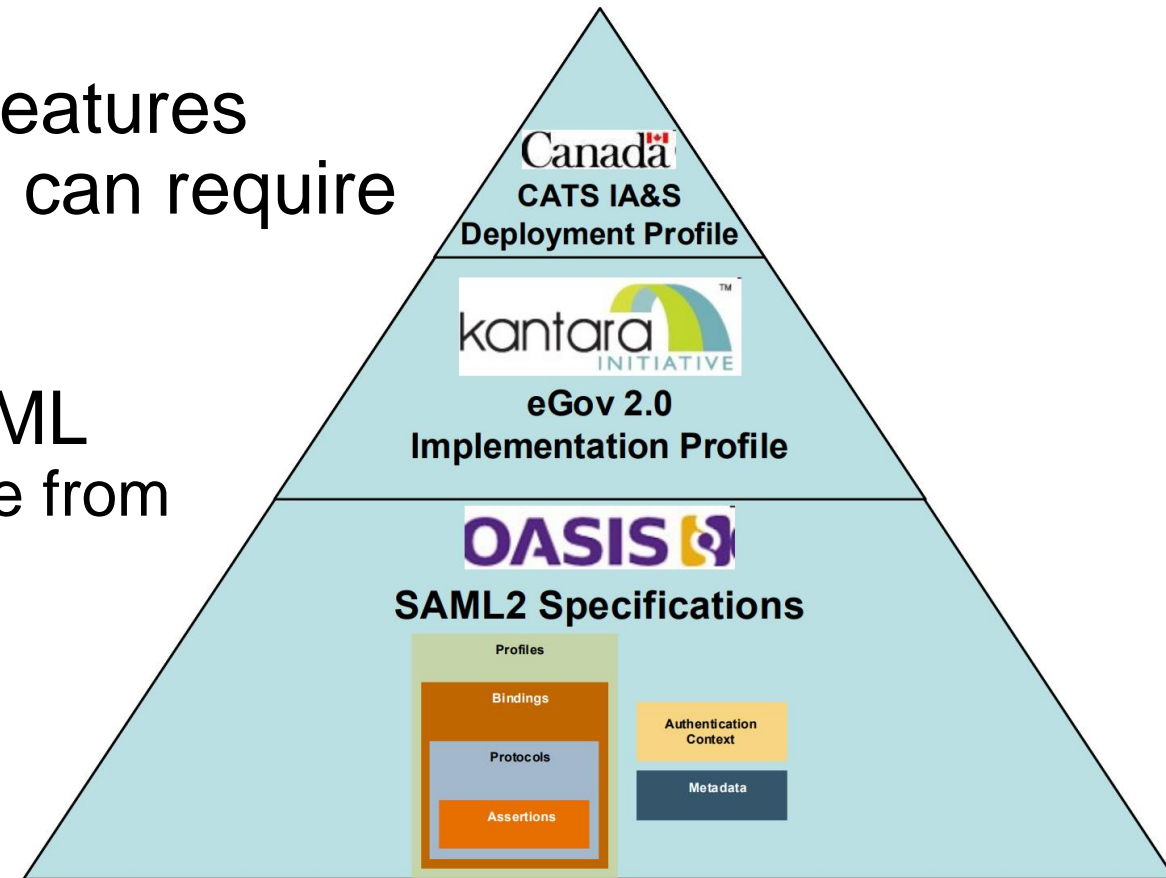


Human Hurdles:
Broad customer comms → questions #identiverse

Dead Reckoning Part One

Is SAML dead?

- TL;DR; no
- Customers keep asking for new features
- Integration with government IdPs can require SAML
 - Example: Canada's GCKey 🍁
- Uptake in 'advanced' uses of SAML
 - Example: signal levels of assurance from the SP to the IdP
- More work for the SP to adapt



Dead Reckoning Part Two

Lessons Learned

1. Although standard-based, SAML integrations can still be brittle
2. Be wary of custom code you didn't know existed
3. Plan communications well ahead of time
4. Educate, educate, educate
5. Be more upfront and aggressive in feature upgrades and tech debt reduction
6. SAML isn't dead (yet) and that's entirely ok

SAM ~~Groundhog~~ Day



THANK YOU!