



NS

18

**NIAGARA
SUMMIT**

**CONNECTING
THE WORLD**



Active Directory and SAML Integration

Ross Schwalm

Important Terms

Why

Getting Started

High Level Architecture

Configuration Examples

Live Demos

Important Terms

- Attribute
- Identity Provider (IdP)
- Service Provider (SP)
- Assertion
- Single Login vs. Single Sign On (SSO)
- Niagara User Prototype
- Binding

Why? For System Integrators...

- Cyber Security is an enabler
- To offer a better occupant experience, more people need to log in
- You are installing a mission critical server
- More collaboration with the IT department
- Stop implementing complex password policies and setting up user accounts
- Confidently bid on larger projects
- Enable multi-factor authentication

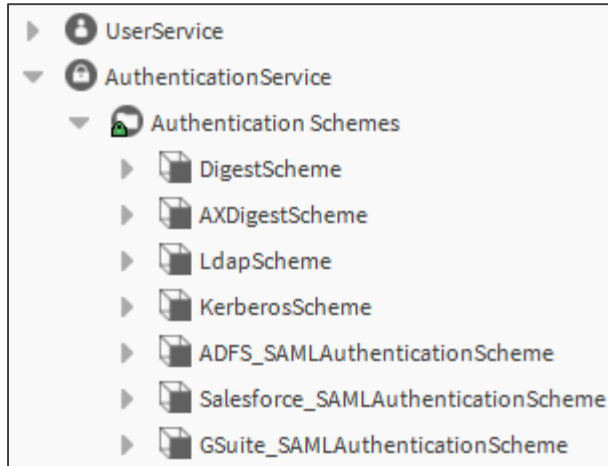
Why? For End Customers...

- The user experience begins at the login screen
- I forgot my password...don't have to remember another password
- Self service
- Centralize Auditing
- Easier to assess impact of large data breaches

Getting Started

- Create a user prototype
- Assign one or more Roles
- Ensure you manage SSL/TLS Certificates
- Setup additional debugging as needed
- Configure your authentication scheme

Niagara Authentication Schemes



- Ldap Palette
 - Lightweight Directory Access Protocol (LDAP)
 - Kerberos
- Saml Palette
 - Security Assertion Markup Language (SAML)

Workbench help: module://docSecurity/doc/auth_AuthenticationSchemes.html

User Prototype

ADFS (User Prototype)	
▶ Full Name	User Prototype Property
▶ Enabled	User Prototype Property
▶ Expiration	User Prototype Property
▶ Language	User Prototype Property
▶ Email	User Prototype Property
▶ Facets	User Prototype Property
▶ Nav File	User Prototype Property
▶ Cell Phone Number	User Prototype Property
▼ Roles	User Prototype Property
Overridable	<input type="radio"/> false
value	<input checked="" type="checkbox"/> admin >>
▶ Allow Concurrent Sessions	User Prototype Property
▶ Auto Logoff Settings	User Prototype Property
▶ web_WebProfileConfig	User Prototype Property
▶ web_MobileWebProfileConfig	User Prototype Property

- The name of the Attribute used to identify the Prototype in the IdP must **exactly** match the name of a user prototype in the station
- At a minimum you need to assign a Role to the User Prototype
- Baja Palette or Ldap Palette

Workbench help: <local:|module://docSecurity/doc/aUserPrototypes.html>

Niagara Certificate Manager

Certificate Management

Certificate Management for "localhost"

User Key Store System Trust Store User Trust Store Allowed Hosts

You have user certificates that identify these certificate authorities:

User Trust Store 3 objects

Alias	Subject	Not After	Key Algorithm	Key Size	Valid	
✓ adfs signing - idp.schwalm.mobi	ADFS Signing - idp.schwalm.mobi	Thu Mar 21 18:15:32 EDT 2019	RSA	2048	true	
✓ salesforce_selfsignedcert_20feb2018_204116	SelfSignedCert_20Feb2018_204116	Wed Feb 20 07:00:00 EST 2019	RSA	2048	true	
✓ google idp	Google	Tue Dec 20 17:36:12 EST 2022	RSA	2048	true	

Workbench help: <local:|module://docSecurity/doc/SSLStoresLocations.html>

Debug Service

Add Log Category

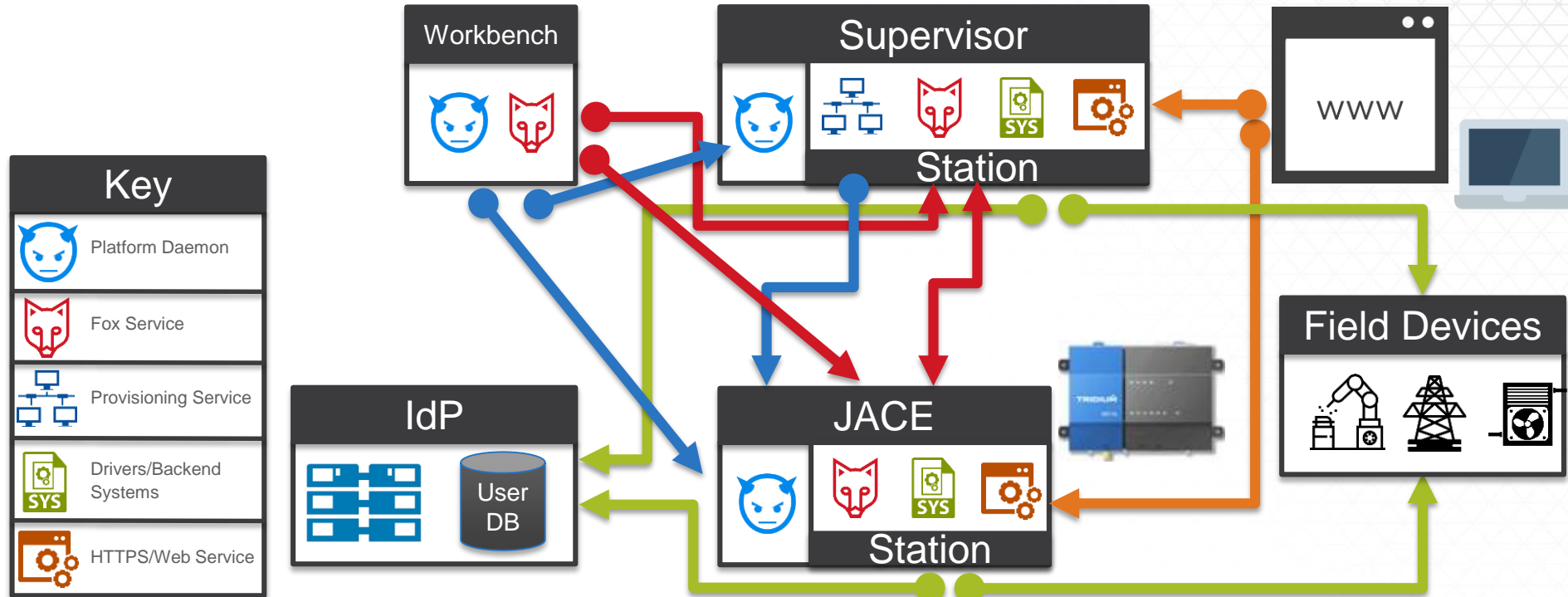
Log Category | INFO

Configured Log Categories

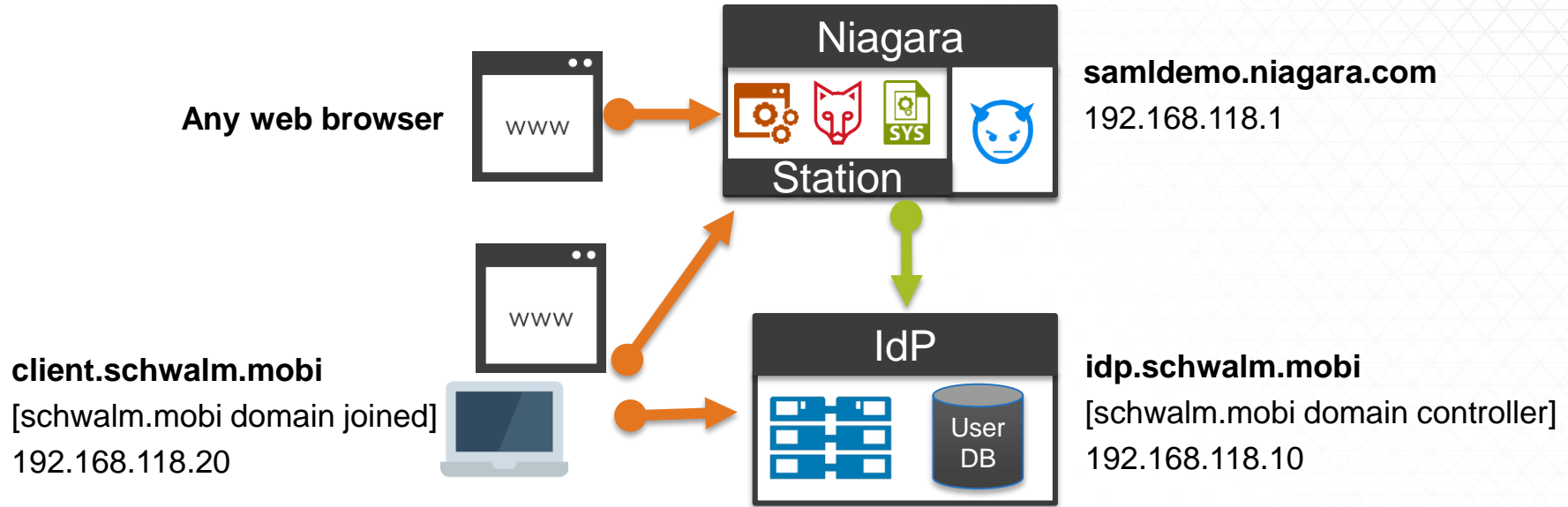
(ROOT)	INFO
java.awt	SEVERE
ldap	ALL
saml	ALL
sun.awt	SEVERE
web.jetty	SEVERE

- Useful information printed to the Application Director
- Don't leave on 'All' after initial setup
- An entry must be generated before autocomplete will find the log category (e.g. attempt an LDAP or SAML login)
- Kerberos logs displayed with ldap log category

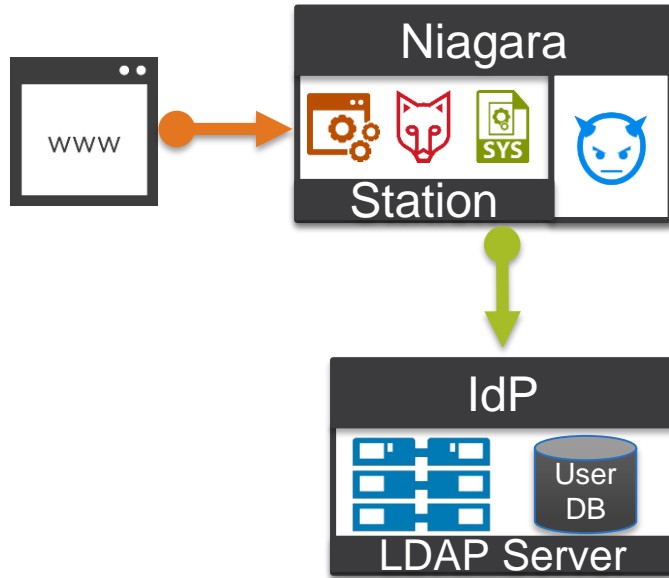
High Level Authentication Architecture



This is our focus



LDAP



- Good place to start
- Niagara AX 3.8+
- Single Login not Single Sign On
- ADSI edit can be a helpful tool

Ldap Authentication Scheme

LdapScheme (Ldap Authentication Scheme)

Type **Ldap V3 Config**

Config

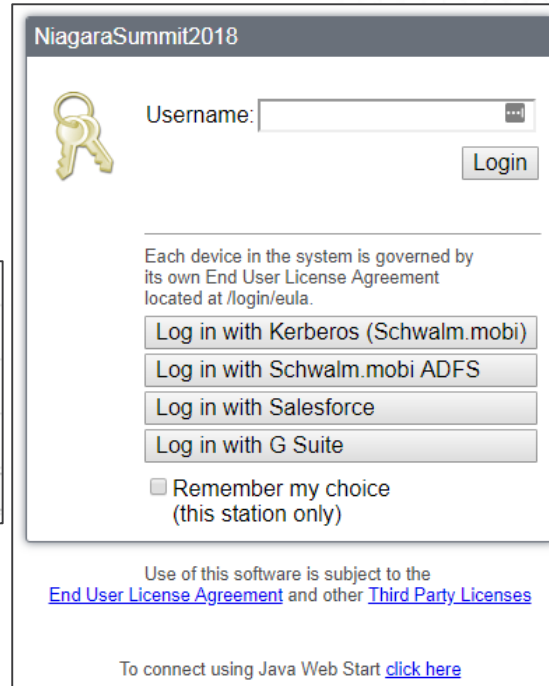
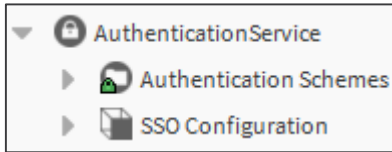
enableConnectionPooling	<input checked="" type="radio"/> true
connectionUrl	ldap://idp.schwalm.mobi
SSL	<input checked="" type="radio"/> true
userLoginAttr	sAMAccountName
userBase	CN=Users, DC=schwalm, DC=mobi
attrEmail	mail
attrFullName	name
attrLanguage	
attrCellPhoneNumber	
attrPrototype	memberOf
cacheExpiration	+00168h 00m 00s
connectionTimeout	15 s[0-60]
bindFormat	%userName% ?
connectionUser	
connectionPassword	••••••••
authenticationMechanism	DIGEST-MD5

- Deploy with SSL
- Start with Ldap V3 for Type and DIGEST-MD5 for authMechanism
- Be as **precise** as possible for userBase

Workbench help:
local:|module://docLdap/
doc/Ldap-Ldap-
LdapSchemeN4.html

LDAP Demo

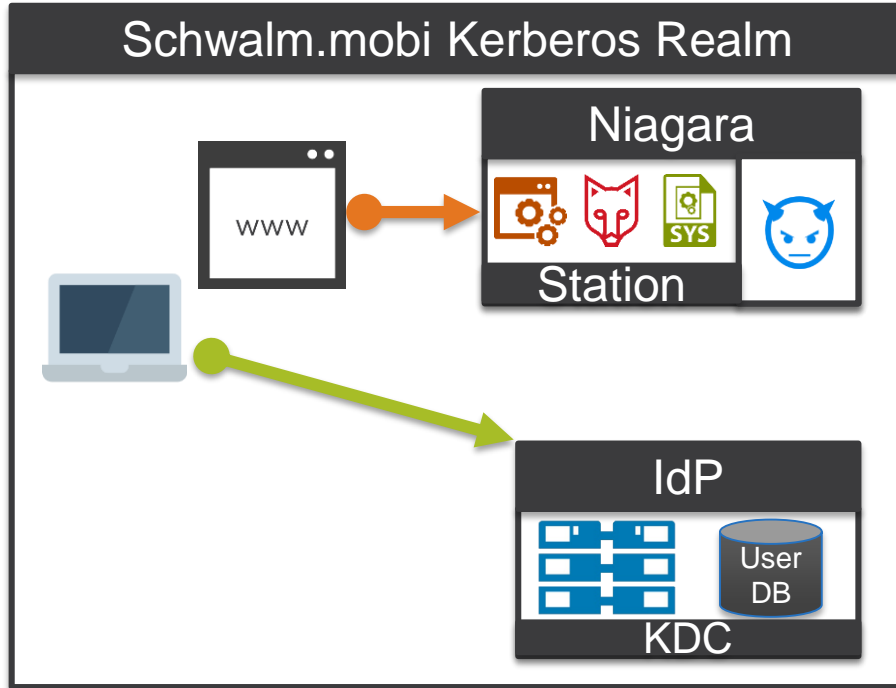
SSO Configuration



- Control SSO functionality
- SSO authentication options appear as buttons on the Niagara login screen

Workbench help: local:|module://docUser/doc/baja-SSOConfiguration.html

Kerberos

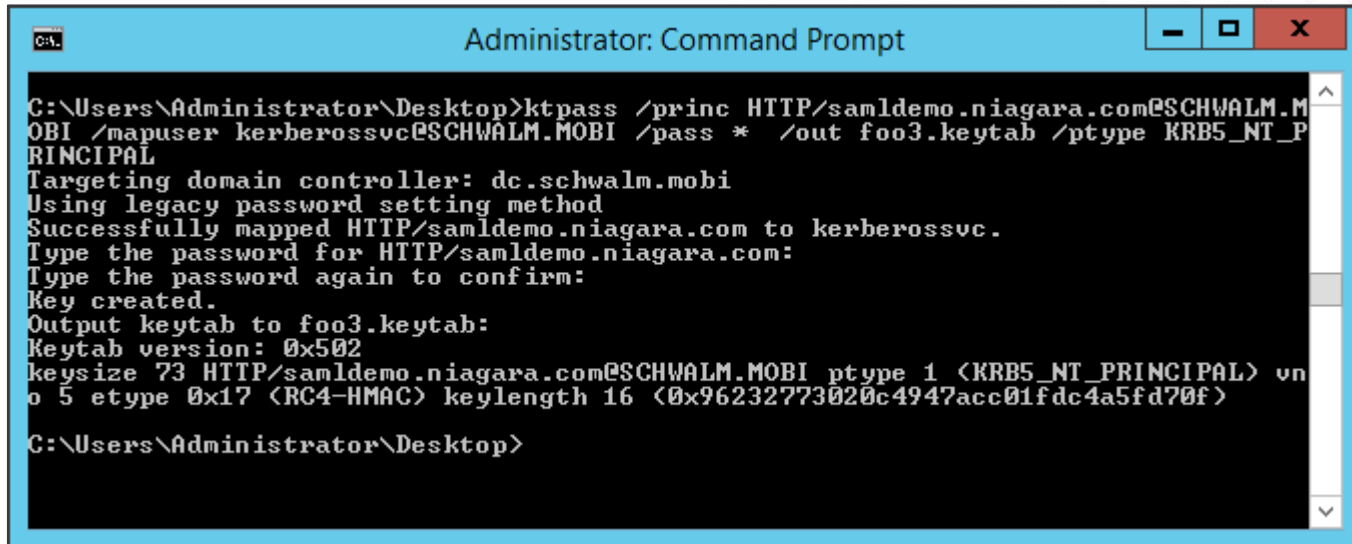


- Single sign on with LDAP attributes
- Niagara AX 3.8U3+
- Key Distribution Center (KDC)
- Client and Server part of the same trusted domain environment (Kerberos Realm)
- Requires browser configuration

Workbench help:

<module://docLdap/doc/MakingSureYouCanConnectUsingABrowse.html#MakingSureYouCanConnectUsingABrowse>

Example Creation of Key Tab File



```
Administrator: Command Prompt
C:\Users\Administrator\Desktop>ktpass /princ HTTP/samldemo.niagara.com@SCHWALM.MOBI /mapuser kerberossvc@SCHWALM.MOBI /pass * /out foo3.keytab /ptype KRB5_NT_PRINCIPAL
Targeting domain controller: dc.schwalm.mobi
Using legacy password setting method
Successfully mapped HTTP/samldemo.niagara.com to kerberossvc.
Type the password for HTTP/samldemo.niagara.com:
Type the password again to confirm:
Key created.
Output keytab to foo3.keytab:
Keytab version: 0x502
keysize 73 HTTP/samldemo.niagara.com@SCHWALM.MOBI ptype 1 (KRB5_NT_PRINCIPAL) vno 5 etype 0x17 (RC4-HMAC) keylength 16 (0x96232773020c4947acc01fdc4a5fd70f)

C:\Users\Administrator\Desktop>
```

Command: ktpass /princ HTTP/samldemo.niagara.com@SCHWALM.MOBI /mapuser kerberossvc@SCHWALM.MOBI /pass * /out foo3.keytab /ptype KRB5_NT_PRINCIPAL

Kerberos Authentication Scheme

KerberosScheme (Kerberos Authentication Scheme)	
Login Button Text	Log in with Kerberos (Schwalm.mobi)
▼ Config Kerberos Config	
Enable Connection Pooling	<input checked="" type="checkbox"/> true
Connection Url	ldap://idp.schwalm.mobi
SSL	<input checked="" type="checkbox"/> true
User Login Attr	sAMAccountName
User Base	CN=Users, DC=schwalm, DC=mobi
Attr Email	mail
Attr Full Name	displayName
Attr Language	
Attr Cell Phone Number	
Attr Prototype	memberOf
Cache Expiration	+00168h 00m 00s
Connection Timeout	15 s [0-60]
Realm	SCHWALM.MOBI
Key Distribution Center	idp.schwalm.mobi
Station Kerberos Name	HTTP/samldemo.niagara.com
Station Kerberos Password	••••••••
Key Tab File	file:^^ldap/kerberossvc.keytab

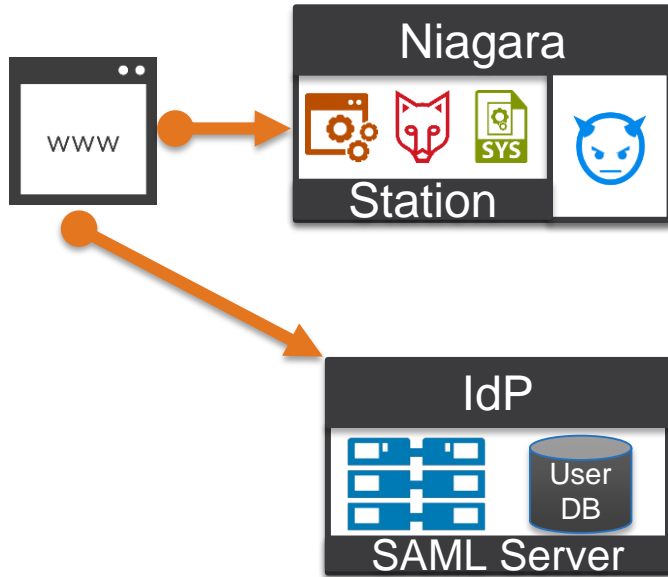
- Follow LDAP guidance
- Get Realm from IT
- Station Kerberos name is the specific Kerberos service name used to create the Key Tab File
- Key Tab file placed in ldap directory in station

Workbench help:

local:|module://docLdap/doc/ldap-KerberosAuthenticationScheme.html

Kerberos Demo

SAML



- Single Sign On with just your browser
- No client browser configuration required
- Niagara 4.4+
- SAML browser plugins are very useful for troubleshooting
- Niagara SAML Service Provider:
 - Issuer/ID=<https://samldemo.niagara.com:443/saml/>
 - AssertionConsumerServiceURL="<https://samldemo.niagara.com:443/saml/assertionConsumerService>"> (HTTP-POST Endpoint)
 - **Replace** samldemo.niagara.com with your URL

What IdPs can I use?

- What Tridium tested with:
 - Salesforce
 - OpenAM
- What I tested and was successful using:
 - Salesforce
 - Active Directory Federation Services (ADFS)
 - G Suite
- “This might not work”
 - Samlidp.io
 - SSOCircle

SAML Authentication Scheme (Salesforce)

SalesforceRedirect (SAML Authentication Scheme)	
Login Button Text	Log in with Salesforce HttpRedirect
IdP Host URL	https://ross-dev-ed.my.salesforce.com
IdP Host Port	443 [1-65535]
IdP Login Path	/idp/endpoint/HttpRedirect
IdP Cert	salesforce_ross_dev_s
SAML Server Cert	samldemo
	email Email
SAMLAttributeMapper	NiagaraPrototype Prototype Name

- Enter the HTTP-Redirect Binding URL
- Select the IdP signing certificate loaded in User Trust Store
- SAML Attribute Mapper from the saml palette

Workbench help: local:|module://docSecurity/doc/Saml-SAMLAuthenticationSchemeStatio-0B798B3F.html

SAML Authentication Scheme (ADFS)

ADFS (SAML Authentication Scheme)	
Login Button Text	Log in with schwalm.mobi ADFS
IdP Host URL	https://idp.schwalm.mobi
IdP Host Port	443 [1-65535]
IdP Login Path	/adfs/ls/
IdP Cert	adfs signing - idp.sc
SAML Server Cert	samldemo
	email Email
SAMLAttributeMapper	prototype Prototype Name

⊕ ✕

SAML Authentication Scheme (G Suite)

GSuite_SAMLAuthenticationScheme (SAML Authentication Scheme)	
Login Button Text	Log in with G Suite
IdP Host URL	https://accounts.google.com
IdP Host Port	443 [1-65535]
IdP Login Path	/o/saml2/initssso?idpid=C01hiysjl&spid=18:
IdP Cert	google idp
SAML Server Cert	samldemo
SAMLAttributeMapper	email Email
	NiagaraPrototype Prototype Name
	fullName Full Name

⊕ ✕

SAML Demo

Resources

- Niagara 4.4 Patch -> saml-rt-4.4.73.50.1.jar
- Designing an Authentication System: A Dialogue in Four Scenes - <https://web.mit.edu/kerberos/dialogue.html>
- The Beer Drinker's Guide to SAML - <https://duo.com/blog/the-beer-drinkers-guide-to-saml>

Thank You

Backup

Example IdP Configurations

- These high level steps are provided as an example for testing with the IdPs discussed during the presentation.
- Actual configuration of the IdP may vary and require different configuration of the Niagara SAML Service Provider.

Salesforce Configuration (1 of 3)


- Sign up for a free developer account (<https://developer.salesforce.com>)
- Company Settings -> My Domain
 - Create a public URL for testing (e.g. ross-dev-ed.my.salesforce.com)
- Identity -> Single Sign-On Settings
 - Enable SAML
- Identity -> Identity Provider
 - Setup Identity Provider
 - Download the public certificate, add it to the User Trust Store in the Niagara station and select that in the SAML Authentication Scheme as the IdP Cert

Salesforce Configuration (2 of 3)


- Service Providers are configured as Connected Apps
 - Entity Id: <https://samldemo.niagara.com:443/saml>
 - ACS URL: <https://samldemo.niagara.com/saml/assertionConsumerService>
 - Upload the public certificate that you selected as the SAML Server Cert in Niagara
 - Assign the connected app to a profile (e.g. Force.com – Free User)
 - Add a Custom Attribute giving it a key name (e.g. NiagaraPrototype) and select the value you will use to identify the user prototype (e.g. \$User.Department)
- Create a user with the profile the connected app is assigned to and enter a value for whatever field will supply the Custom Attribute


Salesforce Configuration (3 of 3)


▼ Web App Settings


Start URL 


Enable SAML


Entity Id 


ACS URL 


Enable Single Logout 


Subject Type 

Name ID Format 

Issuer 

IdP Certificate 

Verify Request Signatures 
C=US, O=Niagara, CN=samldemo.niagara.com 17 Oct 2018 20:25:42 GMT
Upload a certificate: No file selected.

Encrypt SAML Response 

ADFS Configuration (1 of 3)

- Add the ADFS Role to a Windows Server
- You will need to provide a P12 file with an SSL certificate and private key during the Role installation, which will be used by the ADFS Web Service SAML bindings
- During the Role installation you will also need to select the SAML 2.0 option
- After installation, open ADFS Management and navigate to Service -> Certificates, then download the Token-Signing Certificate (View Certificate... -> Details -> Copy to File)
- Add this Token Signing Certificate to the Niagara User Trust Store and select this certificate as the IdP Certificate

ADFS Configuration (2 of 3)

- Select Authentication Policies and under Primary Authentication -> Global Settings -> Authentication Methods, enable Forms Authentication for Intranet.
- Under Trust Relationships -> Relying Party Trusts, edit the Niagara SAML SP configured during the initial Role Installation/Configuration.
 - On the Advanced Tab, specify SHA-1 as the hash algorithm
 - On the Signature Tab, upload the certificate you are using from the Niagara User Key Store
 - On the Endpoints Tab, verify the Assertion Consumer Service URL matches slide 22
 - On the Identifiers Tab, verify the identifier matches slide 22

ADFS Configuration (3 of 3)

The image shows two overlapping windows from the ADFS management console. The background window is titled "Edit Claim Rules for Niagara SAML Service Provider" and shows a list of transform rules. The foreground window is titled "Edit Rule - Send sAMAccountName as Name ID" and provides configuration options for a specific rule.

Edit Claim Rules for Niagara SAML Service Provider

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	Send sAMAccountName as Nam...	Name ID,prototype,email,...

Buttons: Add Rule..., Edit Rule..., Remove Rule...

Buttons: OK, Cancel

Edit Rule - Send sAMAccountName as Name ID

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: Send sAMAccountName as Name ID

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	SAM-Account-Name	Name ID
	Department	prototype
	E-Mail-Addresses	email
	Display-Name	displayName
*		

Buttons: View Rule Language..., OK, Cancel

Under Trust Relationships -> Relying Party Trusts, edit the Claim Rules for the Niagara SAML SP and here is an example:

G Suite Configuration

- In the Google Admin Console, navigate to Security -> Set up Single Sign On (SSO)
- This guide describes the process to setup a custom SAML application: <https://support.google.com/a/answer/6087519?hl=en>
- After you configure the custom application, find the application in your organizations Apps Marketplace, right click the icon, and copy its link location. This URL is what you will need to use for the IdP URL, which adds additional details to the URL listed in the IdP metadata XML file.