



NS2024

POWER OF PARTNERSHIP

LDAP and Oauth and SAML, Oh My!

James Johnson

Sales Engineer - Tridium, Inc.

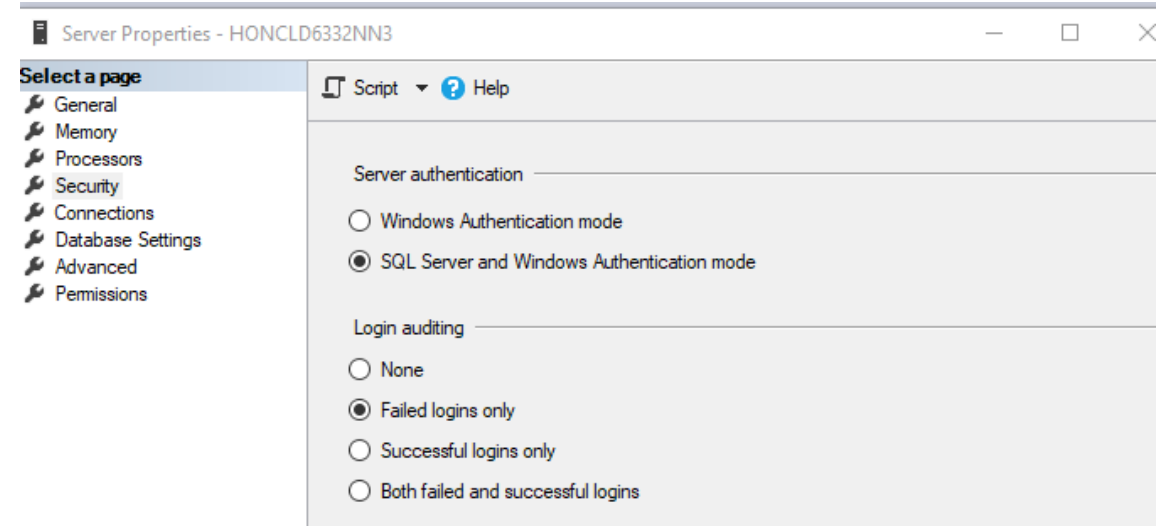
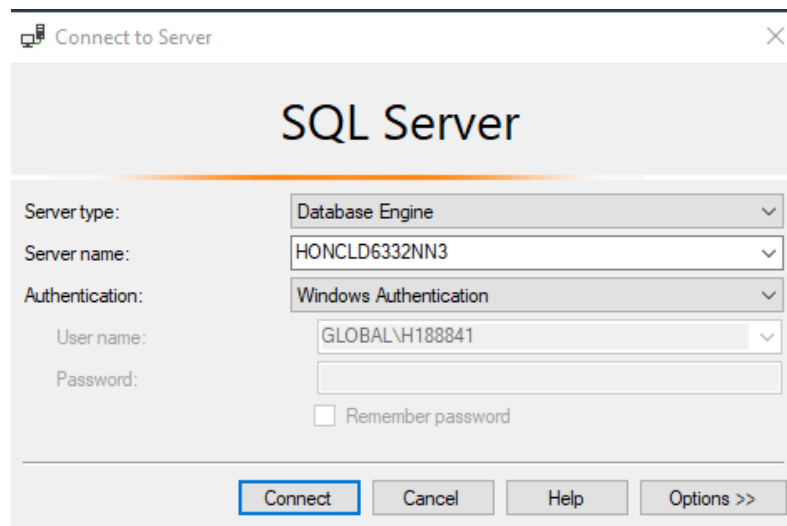
NS2024
POWER OF PARTNERSHIP

Agenda

- Windows authentication for MS SQL
- OAuth2 email authentication
- Google authentication workflow improvements
- LDAP
- SAML authentication updates
- Client certificate authentication

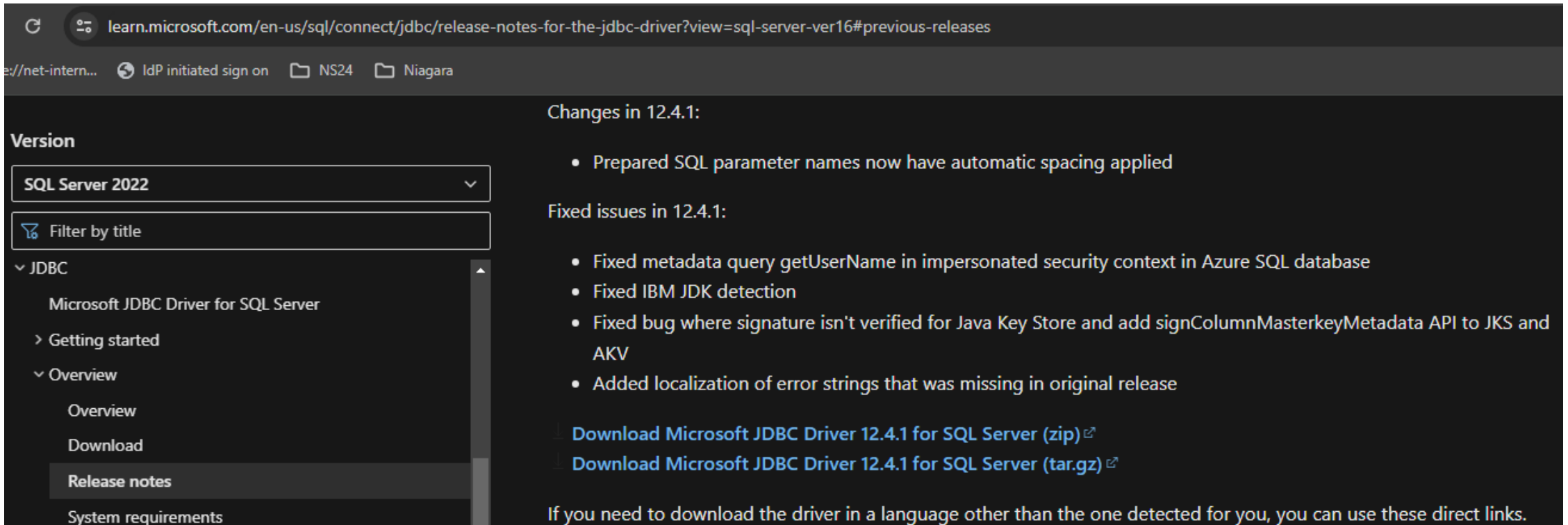
Windows Authentication for MS SQL (4.14)

- Prior Niagara versions require mixed mode authentication to be enabled and a service account configured using SQL Server Authentication.
- Windows Authentication is the default authentication mode for SQL Server and is much more secure than SQL Server Authentication.
- Users can be authenticated via standard Windows domain accounts.



Download - JDBC Driver for SQL Server

- Need to match the JDBC driver version packaged with the rdbSqlServer-rt.jar
- Niagara 4.14 version includes SQL Server JDBC driver 12.4.1 version.



The screenshot shows a web browser window displaying the Microsoft JDBC Driver for SQL Server release notes for version 12.4.1. The browser address bar shows the URL: learn.microsoft.com/en-us/sql/connect/jdbc/release-notes-for-the-jdbc-driver?view=sql-server-ver16#previous-releases. The page content includes a navigation menu on the left with options like 'Version', 'Getting started', 'Overview', 'Download', 'Release notes', and 'System requirements'. The main content area is titled 'Changes in 12.4.1:' and lists several updates and fixed issues. Below the list, there are two download links for the driver in zip and tar.gz formats. At the bottom, a note states: 'If you need to download the driver in a language other than the one detected for you, you can use these direct links.'

Version

SQL Server 2022

Filter by title

▼ JDBC

- Microsoft JDBC Driver for SQL Server
- > Getting started
- ▼ Overview
 - Overview
 - Download
 - Release notes
 - System requirements

Changes in 12.4.1:

- Prepared SQL parameter names now have automatic spacing applied

Fixed issues in 12.4.1:

- Fixed metadata query getUsername in impersonated security context in Azure SQL database
- Fixed IBM JDK detection
- Fixed bug where signature isn't verified for Java Key Store and add signColumnMasterkeyMetadata API to JKS and AKV
- Added localization of error strings that was missing in original release

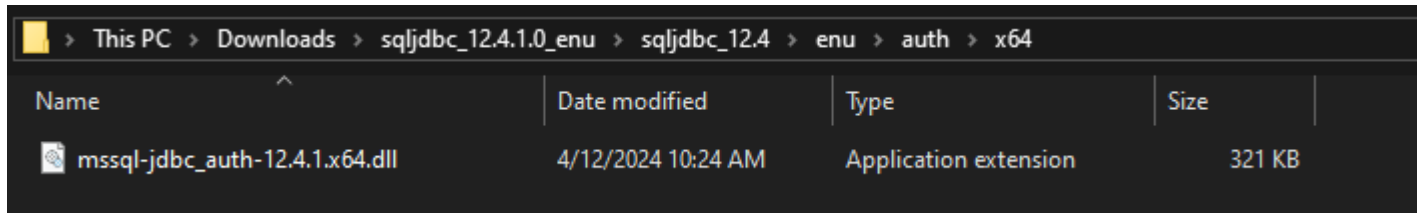
[Download Microsoft JDBC Driver 12.4.1 for SQL Server \(zip\)](#)

[Download Microsoft JDBC Driver 12.4.1 for SQL Server \(tar.gz\)](#)

If you need to download the driver in a language other than the one detected for you, you can use these direct links.

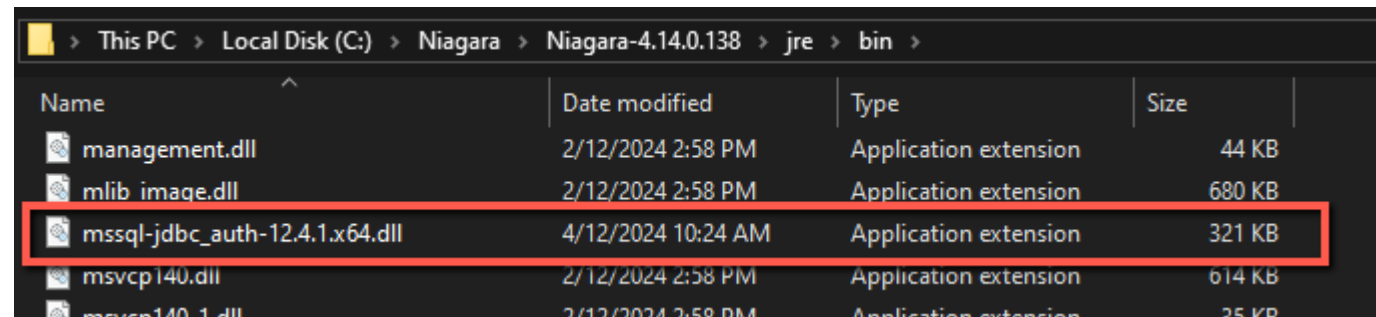
Move JDBC dll file

- Extract the downloaded zip and move the dll file to the /jre/bin directory under the Niagara system home.



This screenshot shows a Windows File Explorer window with the address bar set to 'This PC > Downloads > sqljdbc_12.4.1.0_enu > sqljdbc_12.4 > enu > auth > x64'. The main pane displays a table with the following data:

Name	Date modified	Type	Size
mssql-jdbc_auth-12.4.1.x64.dll	4/12/2024 10:24 AM	Application extension	321 KB



This screenshot shows a Windows File Explorer window with the address bar set to 'This PC > Local Disk (C:) > Niagara > Niagara-4.14.0.138 > jre > bin'. The main pane displays a table with the following data:

Name	Date modified	Type	Size
management.dll	2/12/2024 2:58 PM	Application extension	44 KB
mllib_image.dll	2/12/2024 2:58 PM	Application extension	680 KB
mssql-jdbc_auth-12.4.1.x64.dll	4/12/2024 10:24 AM	Application extension	321 KB
msvcp140.dll	2/12/2024 2:58 PM	Application extension	614 KB
msvcp140_1.dll	2/12/2024 2:58 PM	Application extension	35 KB

The file 'mssql-jdbc_auth-12.4.1.x64.dll' is highlighted with a red rectangular box.

Windows Authentication

- Requires valid Windows credentials entered in User Name and Password properties
- Database name needs to be specified using Instance Name property
- Extra Connection Properties needs to include:

`integratedSecurity=true;authenticationScheme=NTLM`

SqlServerWindowsAuth		Sql Server Database	
Status	{ok}		
Enabled	<input checked="" type="checkbox"/> true		
Fault Cause			
Health	Ok [12-Apr-24 1:04 PM EDT]		
Alarm Source Info	Alarm Source Info		
Host Address	IP sql.training.lan		
Use Encrypted Connection	<input checked="" type="checkbox"/> true		
User Name	James		
Password	••••••		
Worker	Rdbms Worker		
Export Mode	By History Type		
Use Unicode Encoding Scheme	<input type="checkbox"/> false		
Timestamp Storage	Dialect Default		
Points	Rdbms Point Device Ext		
Sql Scheme Enabled	<input type="checkbox"/> false		
Rdb Security Settings	Rdb Security Settings		
Tls Min Protocol	TLSv1.2+		
Verify Subject In Certificate	<input checked="" type="checkbox"/> true		
Instance Name	NiagaraDb		
Port	1433		
Histories	Sql Server History Device Ext		
Extra Connection Properties	integratedSecurity=true;authenticationScheme=NTLM		

Integrated Security

- Uses the account associated with the station.exe process
- Default Niagara daemon behavior uses the Local SYSTEM account to start the station
- User Name and Password fields should be blank
- Database name needs to be specified using Instance Name property
- Extra Connection Properties needs to include:

`integratedSecurity=true;`

SqlServerIntegrated	Sql Server Database
Status	{unackedAlarm}
Enabled	<input checked="" type="checkbox"/> true
Fault Cause	
Health	Ok [13-Apr-24 9:55 AM EDT]
Alarm Source Info	Alarm Source Info
Host Address	IP 192.168.5.217
Use Encrypted Connection	<input checked="" type="checkbox"/> true
User Name	
Password
Worker	Rdbms Worker
Export Mode	By History Type
Use Unicode Encoding Scheme	<input type="checkbox"/> false
Timestamp Storage	Dialect Default
Points	Rdbms Point Device Ext
Sql Scheme Enabled	<input type="checkbox"/> false
Rdb Security Settings	Rdb Security Settings
Tls Min Protocol	TLSv1.2+
Verify Subject In Certificate	<input checked="" type="checkbox"/> true
Instance Name	NiagaraDb
Port	1433
Histories	Sql Server History Device Ext
Extra Connection Properties	integratedSecurity=true

OAuth 2.0 – Authorization Framework

- Does not provide a mechanism to say who a user is or by what mechanism they authenticated.
- Allows a user to delegate an application to act on their behalf.
- Applications provide their application credentials via an authorization request to an authorization server and receive an authorization token.
- Applications present their authorization token to access resources from other servers or application.
- Application credentials typically include a client ID and client secret or certificate.

Email Authenticator (4.13+)

- Maintain security posture using preferred authentication by major email providers: Microsoft (365/Exchange) and Gmail (Workspace)
- Basic Email Client Authenticator – basic authentication with username and password
- OAuth Client Credentials Flow – only supported for incoming accounts
 - Email Client Secret Authenticator – uses client ID and client secret
 - Email Client Certificate Authenticator – uses client ID and client certificate

Auth Server Metadata Endpoint

- The URL that the OAuth client uses to discover the URLs to use for authentication and the server's public signing keys
- Expected to be at the 'well-known' configuration document path which is `/.well-known/openid-configuration`
- Do not include the `/.well-known/openid-configuration`
- Gmail – <https://accounts.google.com>
- Outlook 365 – <https://login.microsoftonline.com/<tenenatID>/v2.0>

Scope

Defines permissions granted to application

Scopes	
https://mail.google.com/	Read, compose, send, and permanently delete all your email from Gmail
https://www.googleapis.com/auth/gmail.addons.current.action.compose	Manage drafts and send emails when you interact with the add-on
https://www.googleapis.com/auth/gmail.addons.current.message.action	View your email messages when you interact with the add-on
https://www.googleapis.com/auth/gmail.addons.current.message.metadata	View your email message metadata when the add-on is running
https://www.googleapis.com/auth/gmail.addons.current.message.readonly	View your email messages when the add-on is running
https://www.googleapis.com/auth/gmail.compose	Manage drafts and send emails
https://www.googleapis.com/auth/gmail.insert	Add emails into your Gmail mailbox
https://www.googleapis.com/auth/gmail.labels	See and edit your email labels
https://www.googleapis.com/auth/gmail.metadata	View your email message metadata such as labels and headers, but not the email body
https://www.googleapis.com/auth/gmail.modify	Read, compose, and send emails from your Gmail account
https://www.googleapis.com/auth/gmail.readonly	View your email messages and settings
https://www.googleapis.com/auth/gmail.send	Send email on your behalf
https://www.googleapis.com/auth/gmail.settings.basic	See, edit, create, or change your email settings and filters in Gmail
https://www.googleapis.com/auth/gmail.settings.sharing	Manage your sensitive mail settings, including who can manage your mail

<https://developers.google.com/identity/protocols/oauth2/scopes>

Office 365 Exchange

Property Sheet

IncomingAccount (Incoming Account)

Hostname	outlook.office365.com										
Port	993 [-1 - max]										
Type	O Auth Email Client Secret Authenticator										
Email Authenticator	<table><tr><td>authServerMetadataEndpoint</td><td>https://login.microsoftonline.com/82308c...</td></tr><tr><td>account</td><td>KyleSardinia@TridiumSE805.onmicrosoft.co...</td></tr><tr><td>clientId</td><td>ec647154-0db2-40cc-8a7b-f5dcc24b2b83</td></tr><tr><td>scope</td><td>https://outlook.office365.com/.default</td></tr><tr><td>clientSecret</td><td>.....</td></tr></table>	authServerMetadataEndpoint	https://login.microsoftonline.com/82308c...	account	KyleSardinia@TridiumSE805.onmicrosoft.co...	clientId	ec647154-0db2-40cc-8a7b-f5dcc24b2b83	scope	https://outlook.office365.com/.default	clientSecret
authServerMetadataEndpoint	https://login.microsoftonline.com/82308c...										
account	KyleSardinia@TridiumSE805.onmicrosoft.co...										
clientId	ec647154-0db2-40cc-8a7b-f5dcc24b2b83										
scope	https://outlook.office365.com/.default										
clientSecret										
Pollrate	00000h 01m 05s [1 second - +inf]										
Enabled	<input checked="" type="checkbox"/> true										
Status	{ok}										
Last Poll Success	10-Apr-2024 11:42 PM EDT										
Last Poll Failure	10-Apr-2024 10:02 PM EDT										
Last Poll Failure Cause	javax.mail.MessagingException: Unable to										
Debug	<input checked="" type="checkbox"/> true										
Use Ssl	<input checked="" type="checkbox"/> true										
Use Start Tls	<input type="checkbox"/> false										
Tls Min Protocol	TLSv1.2+										
Store	Imap										
Delivery Policy	Mark As Read										
Email To Read	All Email										
Incoming Email Size Limit	25000 KB [1 - max]										
Size Limit Per Poll	25000 KB [1 - max]										
Ignore Attachments	<input type="checkbox"/> false										

EmailTesting - Microsoft Azure

https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenu...

Search resources, services, and docs (G+)

Home > App registrations >

EmailTesting

Search

Delete Endpoints Preview features

✖ A certificate or secret has expired. Create a new one →

Essentials

Display name	: EmailTesting
Application (client) ID	: ec647154-0db2-40cc-8a7b-f5dcc24b2b...
Object ID	: 83dcdc6b-1bf4-4518-83d9-db4600054...
Directory (tenant) ID	: 82308c1c-8f27-4a56-8d5c-58a77948cb92
Supported account types	: My organization only
Client credentials	: 0 certificate, 3 secret
Redirect URIs	: Add a Redirect URI
Application ID URI	: Add an Application ID URI
Managed application in local directory	: EmailTesting

Manage

- Overview
- Quickstart
- Integration assistant
- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles

Flexible Authentication Schemes

- Lightweight Directory Access Protocol (LDAP)/ Active Directory (AD)
 - Integrates to existing directory information services
 - Supports using Kerberos for SSO
- Security Assertion Markup Language (SAML)
 - Provides SSO functionality
 - Works with popular on premise and cloud based SAML Identity Providers (IdP) such as OpenAM, Salesforce, Active Directory, etc
- Client Certificate
 - Utilizes PKI certificate authentication
- Google
 - Provides two factor authentication using Google Authenticator app
 - Available for Android, BlackBerry and iOS devices

Google Authenticator Enrollment

- Use two-factor authentication to keep Niagara user accounts secure
- Improved Workflow Enrolling Users With GAuth (4.14)

Authentication Scheme Name GoogleAuthenticationScheme

Password: [masked]

Confirm: [masked]

Force Reset At Next Login true

Never Expires Expires On 12-Apr-2024 11:59 PM EDT

Secret Key

Force Secret Key Reset At Next Login true



AcmeCorp


Password Reset
You are required to reset your password before continuing. Please enter your new password and confirm.


Your password must contain:

- at least 10 character(s)
- at least 1 digit(s)
- at least 1 lower case character(s)
- at least 1 upper case character(s)
- at least 0 special character(s)
- at most 64 character(s)

Set Up Authenticator
Download the Google Authenticator app, then scan the QR code below or enter the key. Finally, enter the 6-digit token displayed in the app into the "Token" field.

 New Password: [input] 

Retype Password: [input] 

QR Code: 

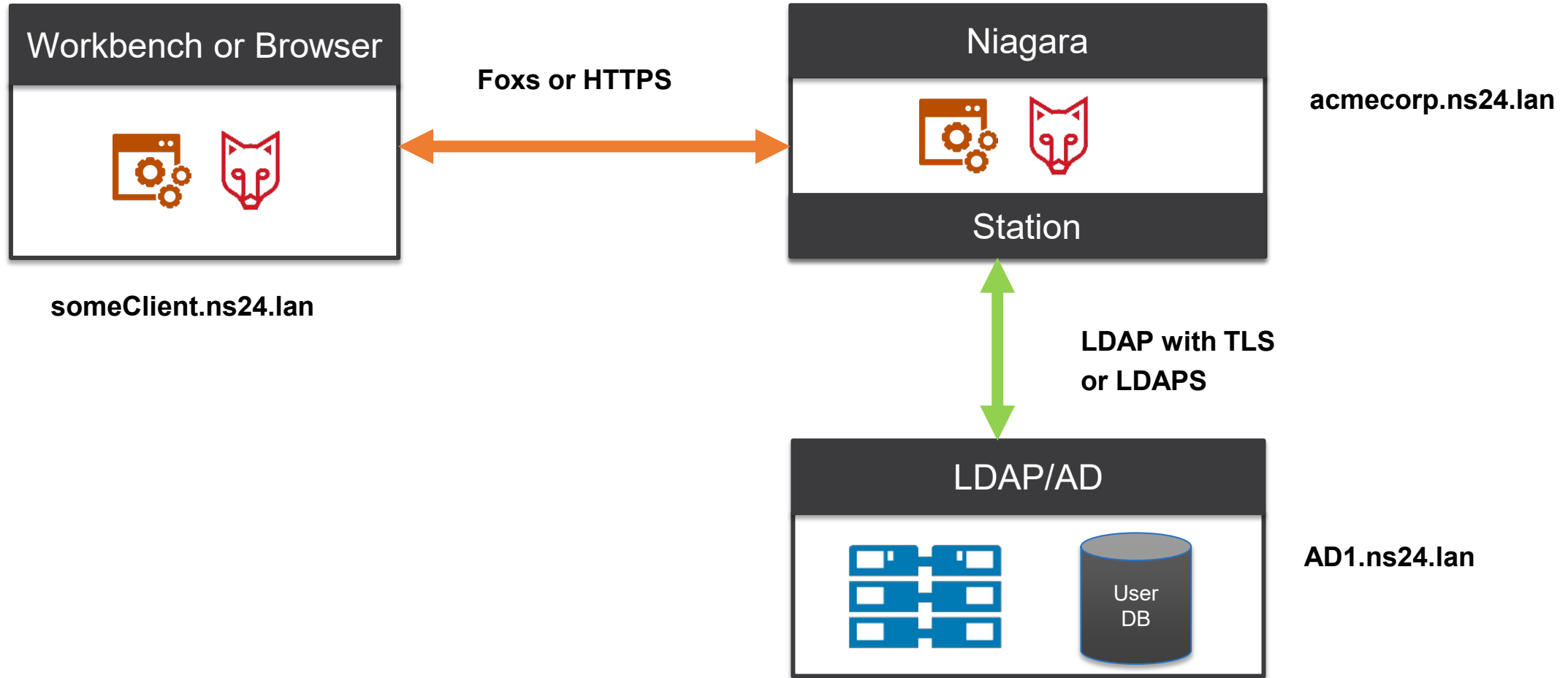
IXOVNFLPNXWBKROP
James@AcmeCorp

Token: [input]

LDAP and AD Authentication

- Lightweight Directory Access Protocol (LDAP) is an application protocol for accessing and maintaining distributed directory information services over an IP network
- Active Directory (AD) is a Microsoft specific implementation of an LDAP server
- LDAP is commonly used in corporate networks for managing domain user accounts and the user's access to applications and network resources
- Allows the customer's IT group to manage access to the Niagara station using their standard tools

LDAP/AD Architecture



LDAP/AD Architecture

- When a user logs into a Niagara station using LDAP authentication, the station creates a Niagara user account based on information from the LDAP server.
- Niagara specific properties such as roles, web profile and nav file are applied using a prototype.
- The authentication scheme's attrPrototype property configures which property of the user account in the LDAP server to use when determining the user prototype to apply.
- The prototype is typically resolved based on group membership, department or other property which relates to the user's functional role in the organization.
- Provides a single login credential for users managed by the end user without requiring Niagara application knowledge.

LDAP Scheme Versions

- Supports Active Directory, LDAP V2 and LDAP V3 specifications.
- LDAP V2 and V3 may require configuring a service account connection username and password.

Type	Active Directory Config
enableConnectionPooling	<input checked="" type="checkbox"/> true
connectionUrl	ldap://ad1.training.lan
SSL	<input checked="" type="checkbox"/> true
userLoginAttr	sAMAccountName
userBase	CN=Users,DC=training,DC=lan
attrEmail	mail
attrFullName	name
attrLanguage	
attrCellPhoneNumber	mobile
attrPrototype	memberOf
cacheExpiration	+00168h 00m 00s
connectionTimeout	15 s [0 - 60]
domain	training.lan

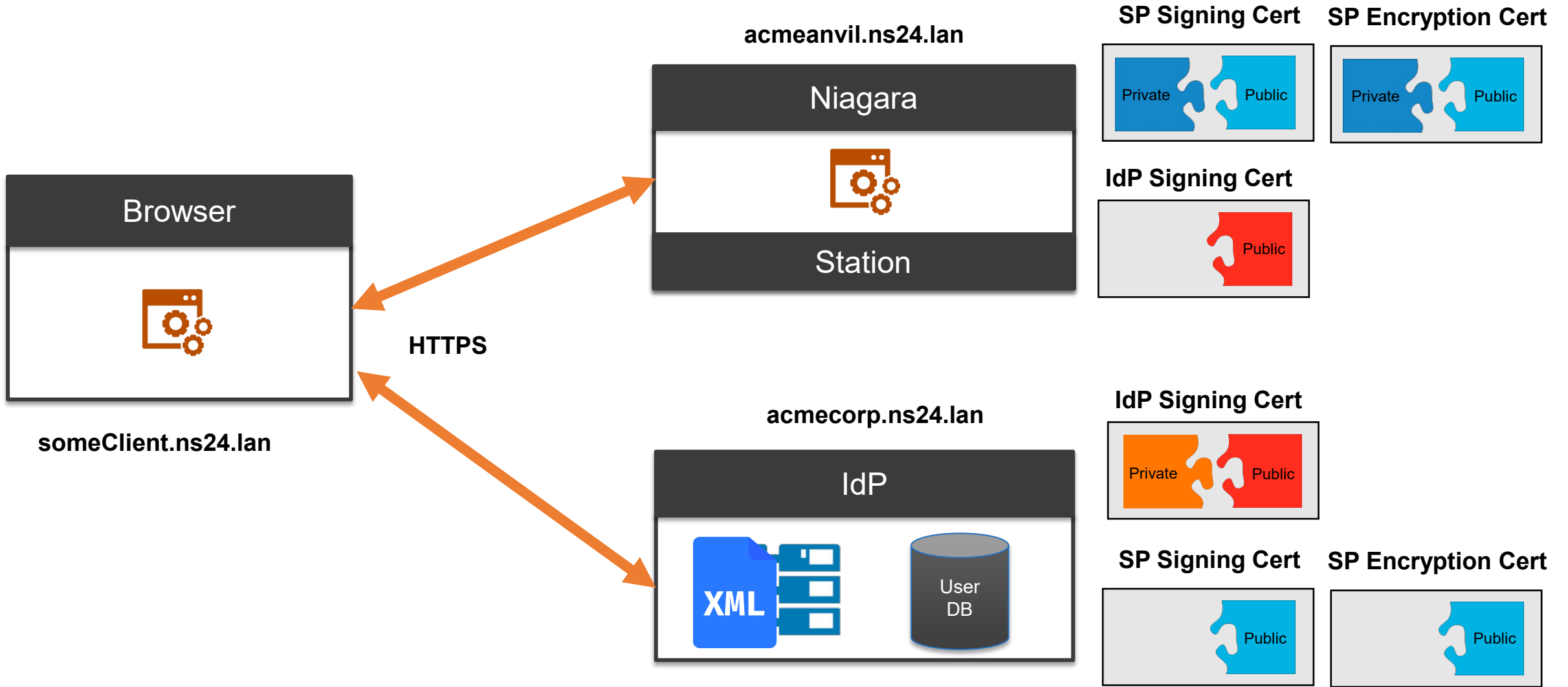
Security Assertion Markup Language (SAML)

- An open standard for exchanging authentication and authorization data in the form of messages passed between security domains.
- Messages may be encrypted and are typically signed using a PKI certificate.
- Since Niagara 4.4 version SAML 2.0 is supported.
- Works with popular third party on premise and cloud based SAML IdPs such as OpenAM, Salesforce, Active Directory, etc.
- Since Niagara 4.9 version, a Niagara based SAML Idp Service is supported in place of third party IdP.

Important Terms

- **Assertion** – a package of information that supplies statements made by a SAML authority.
- **Attribute** – a piece of information which determines the properties of a field or tag in a database.
- **Identity Provider (IdP)** – a system entity that issues authentication assertions in conjunction with SSO.
- **Service Provider (SP)** – a system entity that receives and accepts authentication assertions in conjunction with SSO.

SAML Architecture



SAML User Prototypes

- The **defaultPrototype** is a **baja:User** component used with Niagara user synchronization and legacy LDAP/AD authentication.
- **LDAP, AD and SAML** authentication utilize newer **baja:UserPrototype** component found in baja and Idap palettes.
- **Alternate Default Prototype** should be configured to select a **baja:UserPrototype** and is used if no matching prototype is detected.

User Prototypes (User Prototypes)	
▶ Default Prototype	defaultPrototype
Alternate Default Prototype	<input type="text" value="NoAccess"/>
▶ NiagaraManagers	User Prototype
▶ NiagaraOperators	User Prototype
▶ NoAccess	User Prototype

Slot	#	Name	Display Name	Definition	Flags	Type
<input type="radio"/> Property	0	defaultPrototype	Default Prototype	Frozen		baja:User
<input type="radio"/> Property	1	alternateDefaultPrototype	Alternate Default Prototype	Frozen		baja:String
<input checked="" type="radio"/> Topic	2	userEvent	User Event	Frozen		baja:UserEvent
<input type="radio"/> Property	3	NiagaraManagers	NiagaraManagers	Dynamic		baja:UserPrototype
<input type="radio"/> Property	4	NiagaraOperators	NiagaraOperators	Dynamic		baja:UserPrototype
<input type="radio"/> Property	5	NoAccess	NoAccess	Dynamic		baja:UserPrototype

SAML Authentication Scheme

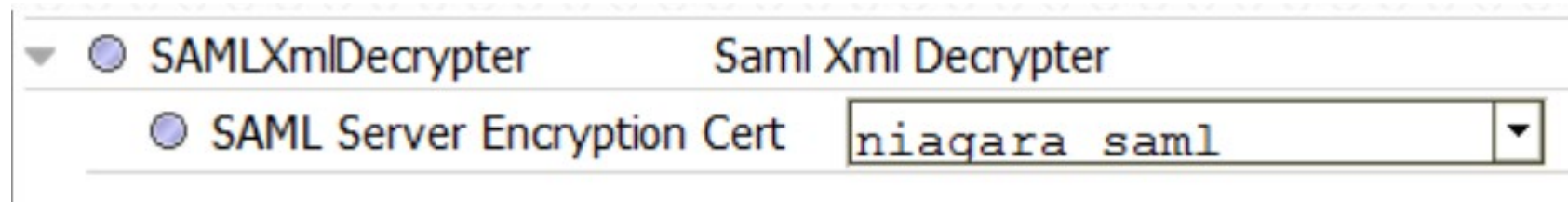
- Entity ID – URL to identify the station (SP) SAML services.
- IdP Host URL – redirect URL to the IdP server.
- IdP Login Path – appended to the IdP Host URL to specify the IdP login page URL.
- IdP Cert – certificate provided by the IdP administrator which must be in the station's trust store. Used to validate messages signed by the IdP.
- SAML Server Cert – certificate in the station's key store which must be provided to the IdP administrator. Used to sign messages sent to the IdP.

SAML Authentication Scheme

NiagaraIdP_ns24 SAML Authentication Scheme	
Login Button Text	Log in with ns24 COT
Entity ID	https://acmeanvil.ns24.lan:444/saml/
IdP Host URL	https://acmecorp.ns24.lan
IdP Host Port	443 [1 - 65535]
IdP Login Path	/saml/idp/auth/httpredirect/cot/44658fc7
Include Query Params In Destination	<input checked="" type="radio"/> false
IdP Cert	saml_idp
▶ SAML Server Cert	samlSigningcert
Time Skew	+00000h 03m 00s
Requested Authentication Type	PasswordProtectedTransport (e.g. Digest or LDAP over TLS) >>
▶ Prototype Merge Policy	User Prototype Merge Policy
▶ samlDecrypter	Saml Xml Decrypter

SAML Encrypted Assertions

- Optional for IdP to encrypt assertions sent to SP
- Must add SAML Xml Decrypter to SAML Authentication Scheme.
- IdP requires public key from specified certificate to encrypt assertions.
- Station (SP) requires the private key from specified certificate in its key store to decrypt received assertions.



The screenshot shows a configuration interface with two rows of settings. The first row has a dropdown arrow on the left, a radio button selected next to the text 'SAMLXmlDecrypter', and the text 'Saml Xml Decrypter' to its right. The second row has a radio button selected next to the text 'SAML Server Encryption Cert', followed by a text box containing 'niagara saml' and a dropdown arrow on the right.

SAML Assertions

- Browser extensions or saml log are useful to debug assertion.
- View attribute key names and values in assertion.

```
Request  Response  SAML
```

```
<samlp:Response
  ID="_06044e98-e293-471c-a904-3a3f727a3ee9"
  Version="2.0"
  IssueInstant="2019-08-01T19:54:46.456Z"
  Destination="https://jace25.training.lan/saml/assertionConsumerService"
  Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"
  InResponseTo="_ae150362-f9d2-4981-be55-cdf7c9e679f1"
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <Issuer
    xmlns="urn:oasis:names:tc:SAML:2.0:assertion">http://idp.training.lan/adfs/services
  </Issuer>
  <samlp:Status>
    <samlp:StatusCode
      Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
  </samlp:Status>
  <Assertion
    ID="_acccf060-40f6-4fd8-8504-13ef076c6559"
    IssueInstant="2019-08-01T19:54:46.425Z"
    Version="2.0"
    xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    <Issuer>http://idp.training.lan/adfs/services/trust</Issuer>
    <ds:Signature
```

```
<AttributeStatement>
  <Attribute
    Name="department">
    <AttributeValue>NiagaraOperators</AttributeValue>
  </Attribute>
  <Attribute
    Name="email">
    <AttributeValue>pjfry@planetexpress.com</AttributeValue>
  </Attribute>
  <Attribute
    Name="fullName">
    <AttributeValue>Phillip J. Fry</AttributeValue>
  </Attribute>
  <Attribute
    Name="telephone">
    <AttributeValue>804-555-1212</AttributeValue>
  </Attribute>
</AttributeStatement>
```

SAML Attribute Mapper

- Defines attributes by name from the SAML claim sent by IdP and maps the attribute values to properties on the Niagara user account.
- SAML DevTools extension in Chrome may be used to view claims response

Claim rule name:
Niagara4SAML

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	department
	E-Mail-Addresses	email
	Display-Name	fullName
	Telephone-Number	telephone

department Prototype Name

CN Only

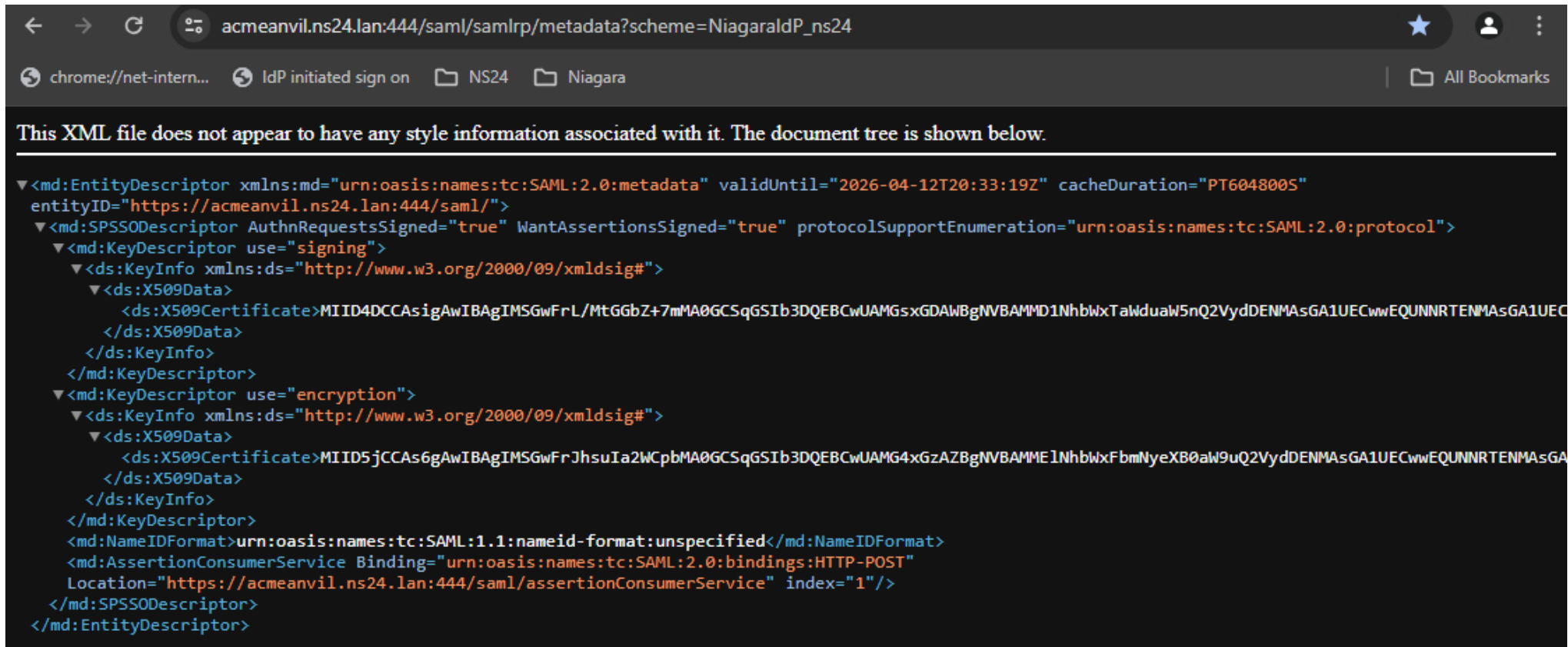
telephone Cell Phone Number

● SAMLAttributeMapper

SAML Metadata URL

- Simplifies IdP configuration by providing metadata via XML

<https://<host>/saml/samlrp/metadata?scheme=<schemeName>>



The screenshot shows a web browser window with the address bar containing the URL: `acmeanvil.ns24.lan:444/saml/samlrp/metadata?scheme=NiagaraIdP_ns24`. The browser's address bar also shows tabs for "chrome://net-intern...", "IdP initiated sign on", "NS24", and "Niagara". The main content area displays a message: "This XML file does not appear to have any style information associated with it. The document tree is shown below." Below this message is a tree view of the XML document. The root element is `<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" validUntil="2026-04-12T20:33:19Z" cacheDuration="PT604800S" entityID="https://acmeanvil.ns24.lan:444/saml/">`. It contains a `<md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">` element, which includes two `<md:KeyDescriptor use="signing">` and `<md:KeyDescriptor use="encryption">` elements. Each key descriptor contains a `<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">` element, which in turn contains a `<ds:X509Data>` element with a `<ds:X509Certificate>` element. The certificate data is truncated in the screenshot. The XML also includes `<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>`, `<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://acmeanvil.ns24.lan:444/saml/assertionConsumerService" index="1"/>`, and closing tags for the `</md:SPSSODescriptor>` and `</md:EntityDescriptor>` elements.

SAML Requested Authentication Type (4.14)

- Allows the SP to specify to the IdP what types of authentication it allows
- Niagara 4.4 – 4.13 version was hard coded

```
</samlp:NameIDPriority>  
<samlp:RequestedAuthnContext  
  Comparison="exact">  
  <saml:AuthnContextClassRef  
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport  
  </saml:AuthnContextClassRef>  
</samlp:RequestedAuthnContext>
```

- Niagara 4.14 is now configurable

```
<samlp:RequestedAuthnContext  
  Comparison="minimum">  
  <saml:AuthnContextClassRef  
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:oasis:names:tc:SAML:2.0:ac:classes:TLSCClient  
  </saml:AuthnContextClassRef>  
  <saml:AuthnContextClassRef  
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport  
  </saml:AuthnContextClassRef>  
  <saml:AuthnContextClassRef  
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken  
  </saml:AuthnContextClassRef>  
</samlp:RequestedAuthnContext>
```

Configure Niagara IdP and SAML Scheme

- Manually add/configure SAML IdP Service including COT and user's SAML prototypes.
- Either manually or using set property job step, setup user prototypes in remote stations.
- Use the provisioning job step to:
 - Add and configure the SAML Authentication Scheme to remote stations.
 - Import the public signing certificate from the supervisor to the trust store of each remote station.
 - Generate a unique SAML signing certificate in the remote station's user key store to be used for signing SAML messages.
 - A copy of the remote stations SAML signing certificate's public key is assigned to the station Service Provider (SP) under the COT in the supervisor.

SAML IdP Service

- Native Niagara based Identity Provider (IdP).
- Typically setup in supervisor station.
- Requires samIDP feature in license.

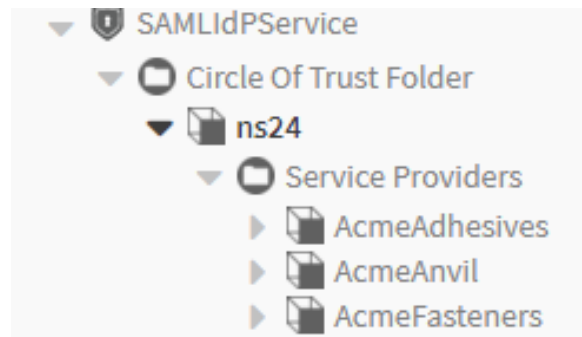
Property Sheet

SAMLIdPService (S A M L Id P Service)

Status	{ok}
Fault Cause	
Enabled	<input checked="" type="checkbox"/> true
Idp Signing Cert Alias And Password	saml_idp
Entity ID	https://acmecorp.ns24.1an:443/saml/
Time Skew	+00000h 03m 00s
Apply Time Skew To Response	<input type="checkbox"/> false
Circle Of Trust Folder	Circle Of Trust Folder
xmlEncrypter	Saml Xml Encrypter

Circle Of Trust (COT)

- Component which defines a group of stations to which designated users have access via SAML authentication.
- Each COT has its own HTTP Redirect Endpoint URL.
- Can define multiple COT components under the SAML IdP Service.



Circle Of Trust (COT)

ns24

Circle Of Trust Editor

Display Name	Value	Commands
Description	<input type="text"/>	
Http Redirect Endpoint	<input type="text" value="https://acmecorp.ns24.lan:443/saml/idp/auth/l"/>	
Enabled	<input checked="" type="checkbox"/>	

- Stations
- Users
- Auth Schemes
- Prototypes

filter list

Name
<input checked="" type="checkbox"/> AcmeAdhesives
<input checked="" type="checkbox"/> AcmeAnvil
<input checked="" type="checkbox"/> AcmeFasteners

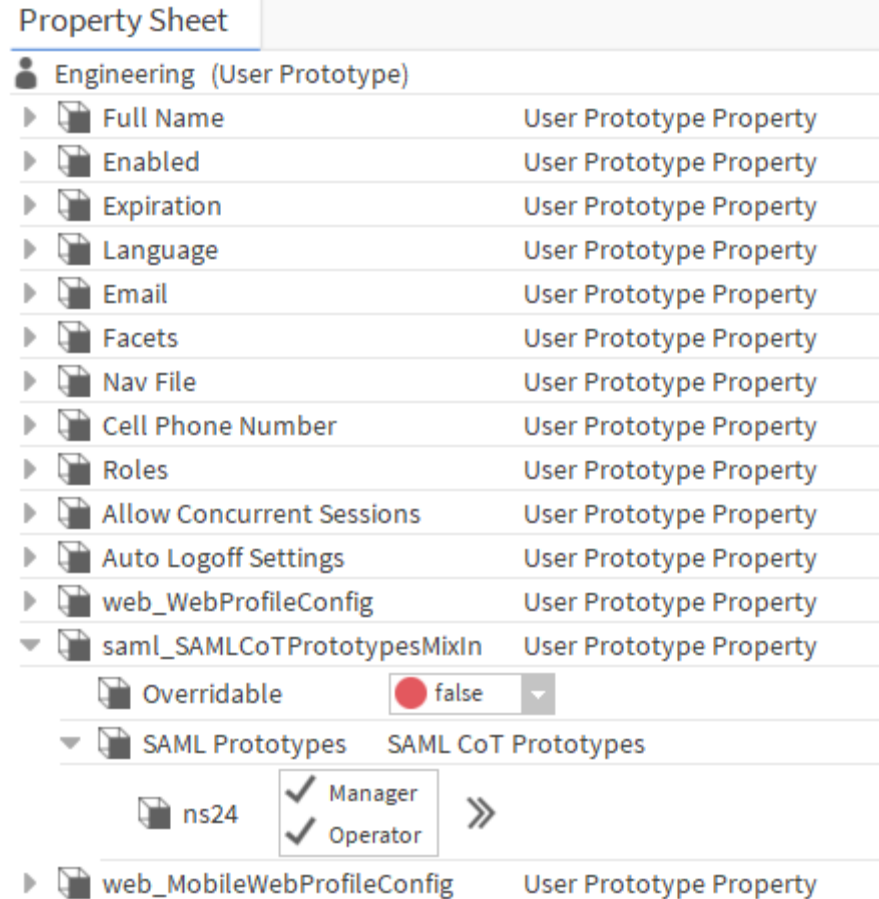
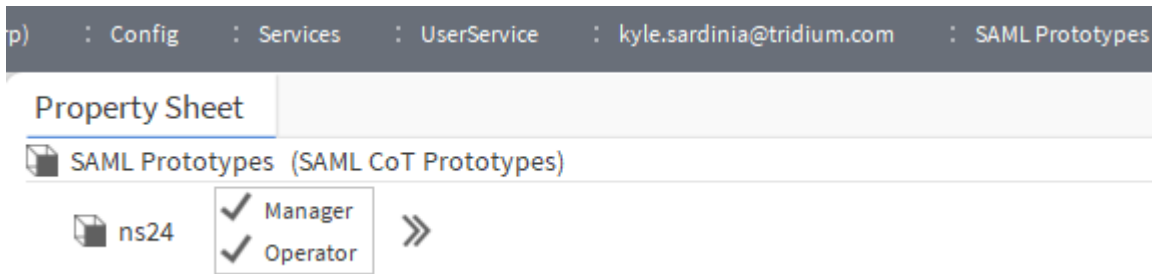
- New Station
- Edit Station
- Delete Station

COT Editor

- Stations – configures which stations are included.
- User – configures which station users are included.
- Auth Schemes – configures authentication schemes such as LDAP where a local user may not exist to be assigned. Enabling an authentication scheme allows all users who log in with that scheme to utilize SAML SSO.
- Prototypes – defines place holder names for user prototypes used in the remote station to assign role, nav file and other properties to a user created via SAML authentication.

COT – SAML Prototypes

- Configures the user prototype for each COT.
- Only lists COT components which have the user enabled.
- Configured on user prototype for other authentication schemes such as LDAP.



SAML Debugging

← → ↺ 🏠 📄 https://chromewebstore.google.com/detail/saml-devtools-extension/jndllhgbinhiiddkbeoepbpdhhdho

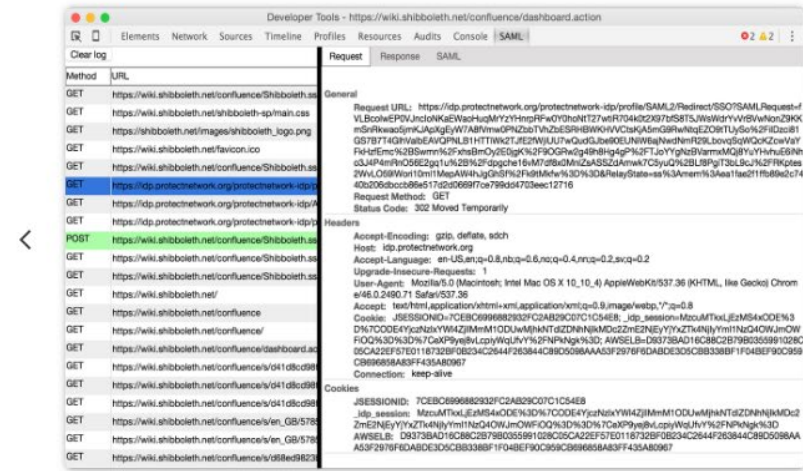
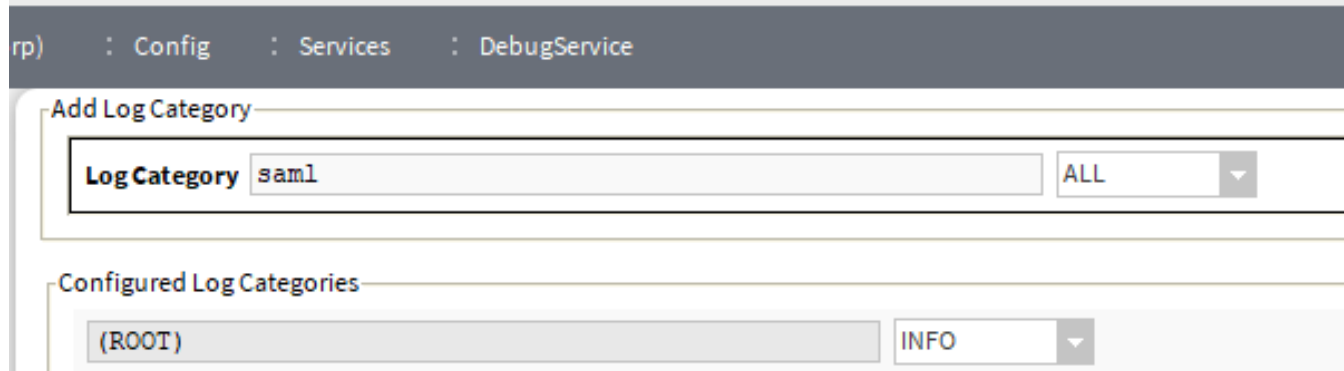
 chrome web store Discover **Extensions** Themes

SAML SAML DevTools extension

Remove from Chrome

4.3 ★ (28 ratings)

Extension Developer Tools 40,000 users



Prototype Merge Policy (4.12+)

- Disabled by default, must opt into new behavior on upgrade
 - Default behavior varies by property when enabled
 - Roles are merged from all matching user prototypes
 - Expiration uses earliest expiration from any matching user prototype
 - Allow Concurrent Sessions false if any matching user prototype has false value
 - Auto Logoff Settings uses shortest value from any matching user prototype

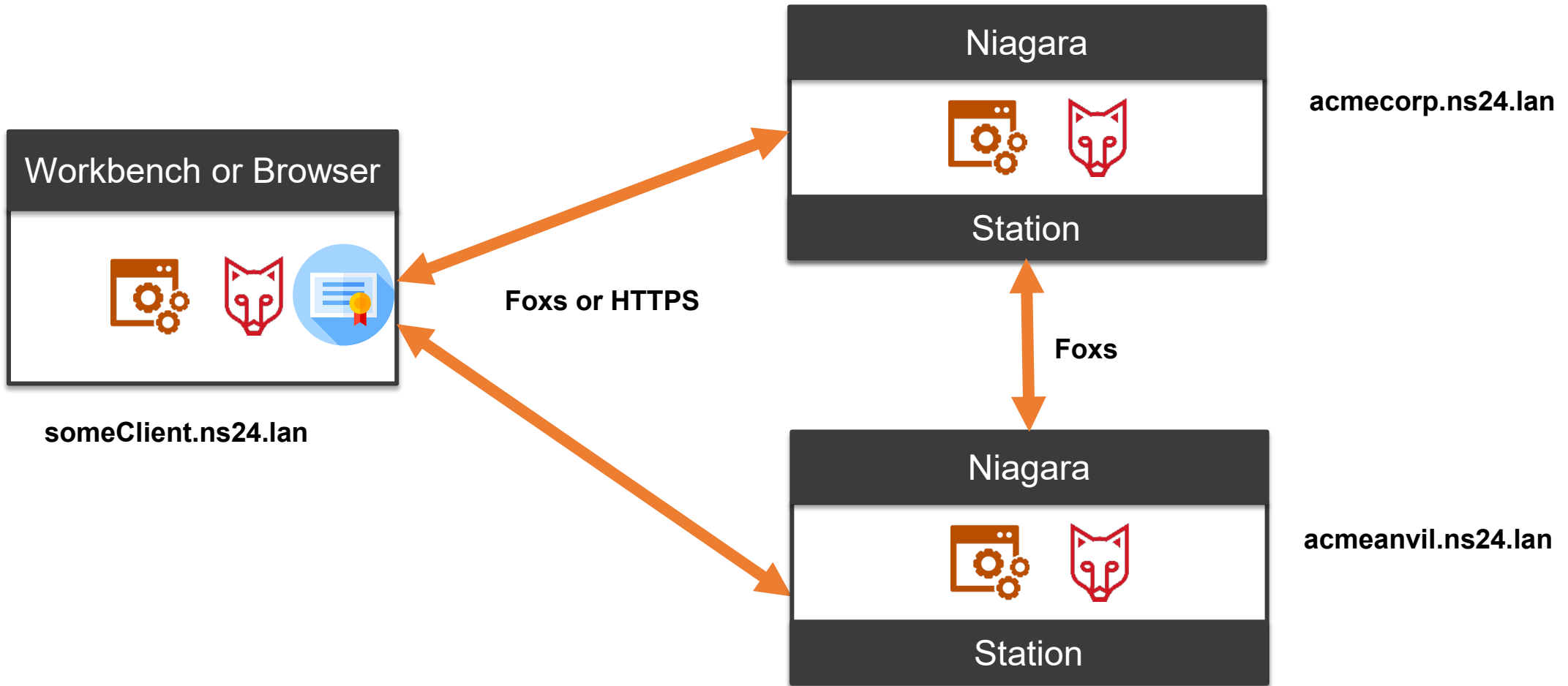
<input checked="" type="radio"/> Prototype Merge Policy	User Prototype Merge Policy
<input checked="" type="radio"/> Enabled	<input checked="" type="radio"/> true
<input type="radio"/> Roles Merge Mode	Union
<input type="radio"/> Expiration Merge Mode	Prefer Earliest
<input type="radio"/> Allow Concurrent Sessions Merge Mode	Prefer False
<input type="radio"/> Auto Logoff Settings Merge Mode	Prefer Shortest

Client Certificate Authentication

- Provides authentication using PKI certificate instead of traditional username and password.
- Extended key usage must be TLS Web Client Authentication.
- User must export public key from their certificate and share with the Niagara system administrator.

<input type="radio"/> ClientCertAuthScheme (Client Cert Auth Scheme)
<input type="radio"/> Login Button Text <input type="text" value="Log in with Client Certificate"/>

Client Certificate Architecture



Kiosk Support – Client Cert Auth (4.8)

- Browser based kiosks can utilize certificates in the client's key store for station authentication.
- Station SSO configuration or client browser cookie may allow the browser client to automatically attempt certificate authentication.
- Browser client may be configured to automatically select a specific certificate for a given station URL.

Questions

