

Ad12

Domino Authentication via SAML - All Flavours

Herwig W. Schauer
Milan Matejic

About us

Milan Matejic

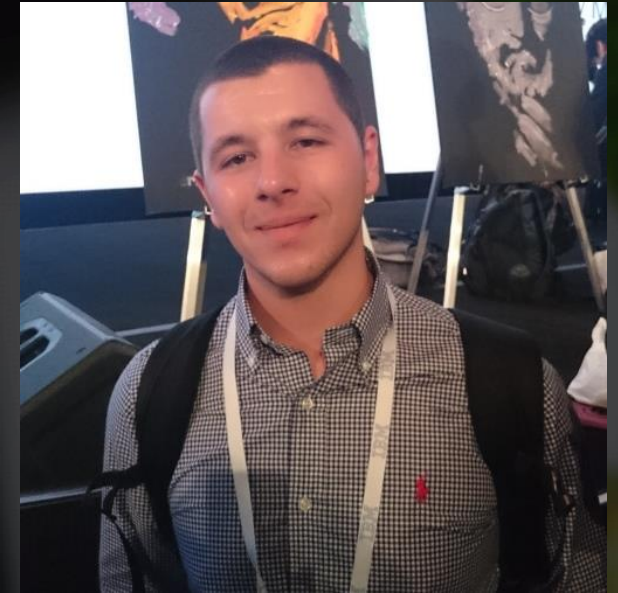


Table of Contents

Table of Contents

Motivation

Table of Contents

Motivation

Why SAML?

Table of Contents

Motivation

Why SAML?

SAML

Table of Contents

Motivation

Why SAML?

SAML

Wording

Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

Table of Contents

Motivation

HCL Domino & SAML

Why SAML?

SAML

Wording

How does it work?

Table of Contents

Motivation

HCL Domino & SAML

Why SAML?

Prerequisites

SAML

Wording

How does it work?

Table of Contents

Motivation

HCL Domino & SAML

Why SAML?

Prerequisites

SAML

Infrastructure Needed

Wording

How does it work?

Table of Contents

Motivation

HCL Domino & SAML

Why SAML?

Prerequisites

SAML

Infrastructure Needed

Wording

Basic SAML Setup

How does it work?

Table of Contents

Motivation

HCL Domino & SAML

Why SAML?

Prerequisites

SAML

Infrastructure Needed

Wording

Basic SAML Setup

How does it work?

SAML & SSO

Table of Contents

Motivation

HCL Domino & SAML

Web Federated Login

Why SAML?

Prerequisites

SAML

Infrastructure Needed

Wording

Basic SAML Setup

How does it work?

SAML & SSO

Table of Contents

Motivation

HCL Domino & SAML

Web Federated Login

Why SAML?

Prerequisites

Notes Federated Login

SAML

Infrastructure Needed

Wording

Basic SAML Setup

How does it work?

SAML & SSO

Table of Contents

Motivation

HCL Domino & SAML

Web Federated Login

Why SAML?

Prerequisites

Notes Federated Login

SAML

Infrastructure Needed

Traveler & SAML

Wording

Basic SAML Setup

How does it work?

SAML & SSO

Table of Contents

Motivation

HCL Domino & SAML

Web Federated Login

Why SAML?

Prerequisites

Notes Federated Login

SAML

Infrastructure Needed

Traveler & SAML

Wording

Basic SAML Setup

Bonus – Nomad!

How does it work?

SAML & SSO

Table of Contents

Motivation

HCL Domino & SAML

Web Federated Login

Why SAML?

Prerequisites

Notes Federated Login

SAML

Infrastructure Needed

Traveler & SAML

Wording

Basic SAML Setup

Bonus – Nomad!

How does it work?

SAML & SSO

Troubleshooting

Table of Contents

Motivation

HCL Domino & SAML

Web Federated Login

Issues

Why SAML?

Prerequisites

Notes Federated Login

SAML

Infrastructure Needed

Traveler & SAML

Wording

Basic SAML Setup

Bonus – Nomad!

How does it work?

SAML & SSO

Troubleshooting

Table of Contents

Motivation

HCL Domino & SAML

Web Federated Login

Issues

Why SAML?

Prerequisites

Notes Federated Login

Q & A

SAML

Infrastructure Needed

Traveler & SAML

Wording

Basic SAML Setup

Bonus – Nomad!

How does it work?

SAML & SSO

Troubleshooting

Table of Contents

Motivation	HCL Domino & SAML	Web Federated Login	Issues
Why SAML?	Prerequisites	Notes Federated Login	Q & A
SAML	Infrastructure Needed	Traveler & SAML	Shibboleth
Wording	Basic SAML Setup	Bonus – Nomad!	
How does it work?	SAML & SSO	Troubleshooting	

Table of Contents

Motivation	HCL Domino & SAML	Web Federated Login	Issues
Why SAML?	Prerequisites	Notes Federated Login	Q & A
SAML	Infrastructure Needed	Traveler & SAML	Shibboleth
Wording	Basic SAML Setup	Bonus – Nomad!	References
How does it work?	SAML & SSO	Troubleshooting	

Password fatigue



Motivation



Motivation

Productivity



Motivation

Ease of maintenance



Table of Contents

Motivation

HCL Domino & SAML

Web Federated Login

Issues

Why SAML?

Prerequisites

Notes Federated Login

Q & A

SAML

Infrastructure Needed

Traveler & SAML

Shibboleth

Wording

Basic SAML Setup

Bonus – Nomad!

References

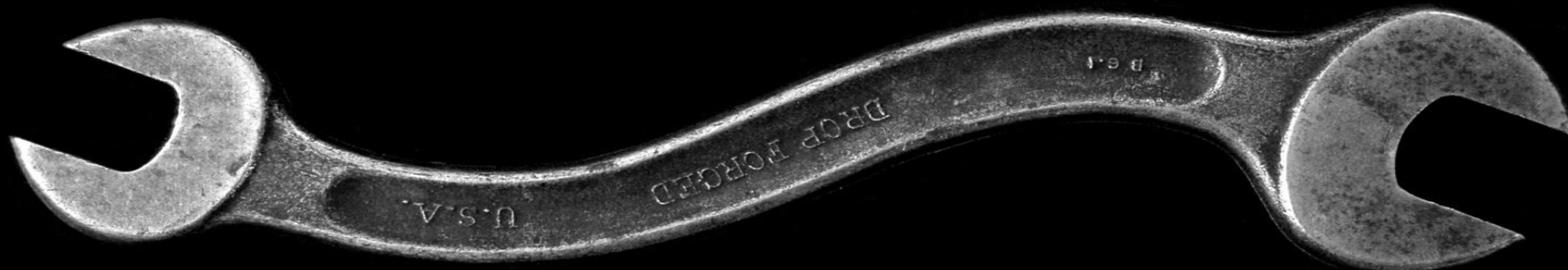
How does it work?

SAML & SSO

Troubleshooting

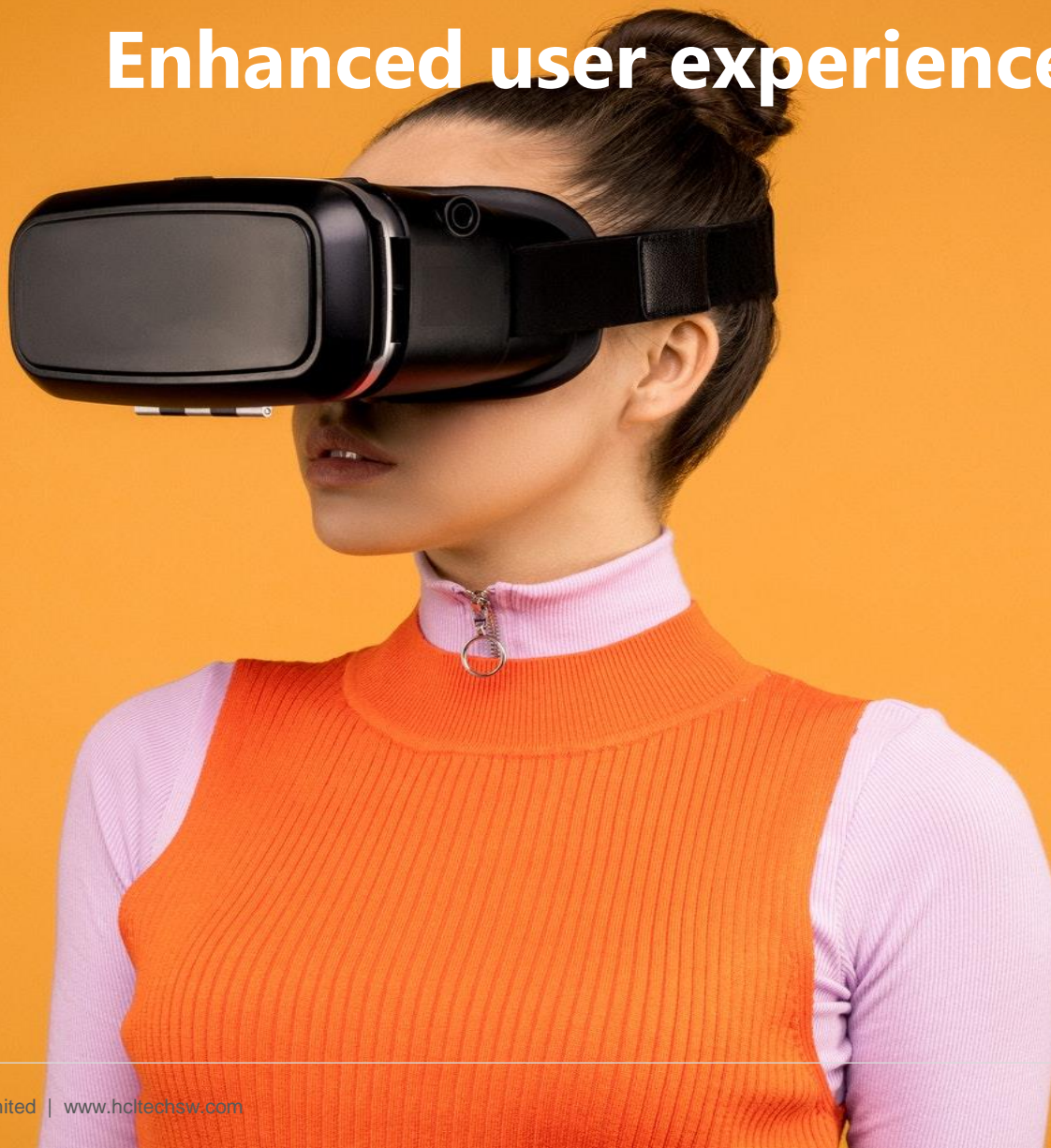
Why SAML!?

Open standard



Why SAML!?

Enhanced user experience



Why SAML!?

HCL Digital Solutions portfolio

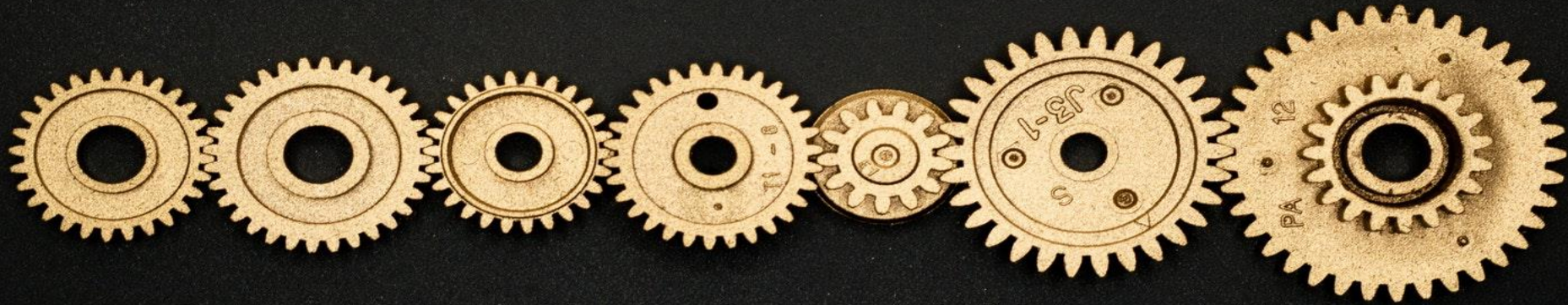


Table of Contents

Motivation	HCL Domino & SAML	Web Federated Login	Issues
Why SAML?	Prerequisites	Notes Federated Login	Q & A
SAML	Infrastructure Needed	Traveler & SAML	Shibboleth
Wording	Basic SAML Setup	Bonus – Nomad!	References
How does it work?	SAML & SSO	Troubleshooting	

Security Assertion Markup Language *Authentication Mechanism*

SAML

Open Standard Current Implementation SAML 2.0

Table of Contents

Motivation	HCL Domino & SAML	Web Federated Login	Issues
Why SAML?	Prerequisites	Notes Federated Login	Q & A
SAML	Infrastructure Needed	Traveler & SAML	Shibboleth
Wording	Basic SAML Setup	Bonus – Nomad!	References
How does it work?	SAML & SSO	Troubleshooting	

Authentication vs. authorization



Basic SAML



Web Federated Login

WFL

Notes Federated Login



Nomad Federated Login

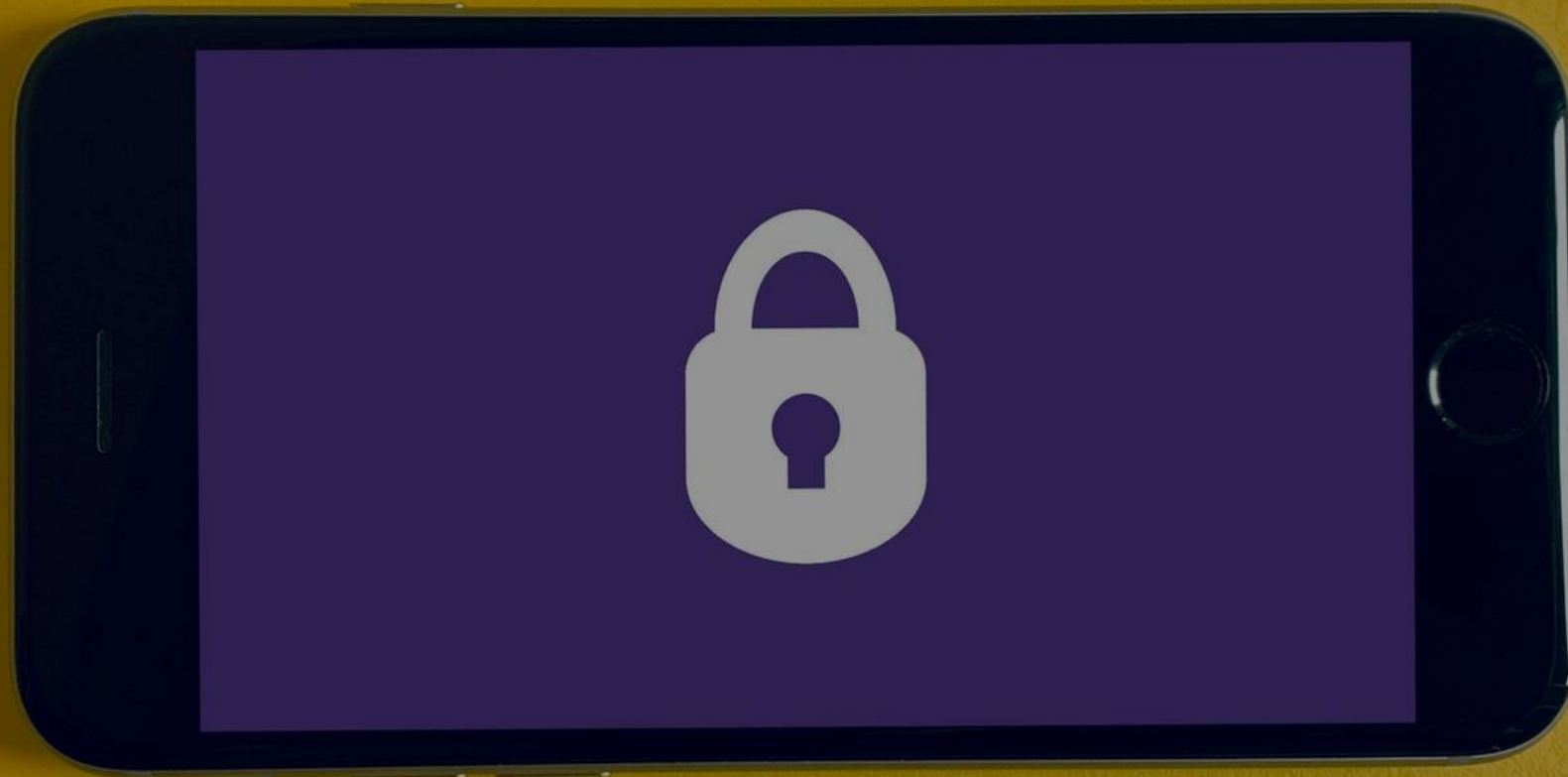


Table of Contents

Motivation

HCL Domino & SAML

Web Federated Login

Issues

Why SAML?

Prerequisites

Notes Federated Login

Q & A

SAML

Infrastructure Needed

Traveler & SAML

Shibboleth

Wording

Basic SAML Setup

Bonus – Nomad!

References

How does it work?

SAML & SSO

Troubleshooting

How Does it Work?

Identity provider

IdP

How Does it Work?

Service Provider (SP) *Relaying Party*



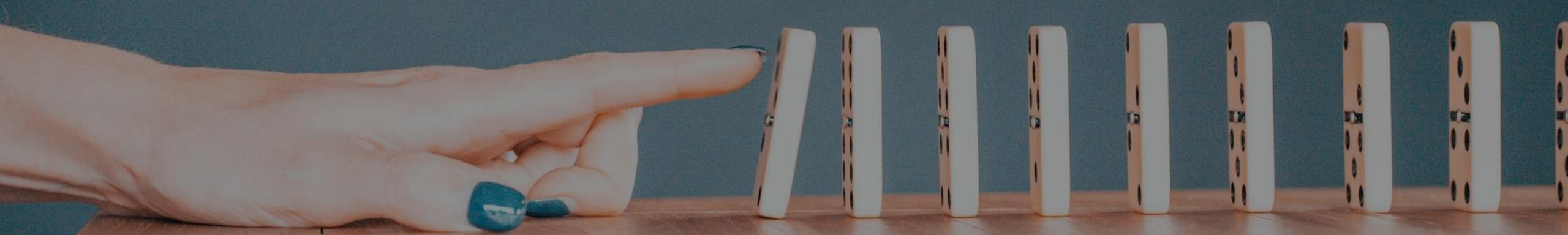
How Does it Work?

SAML assertion



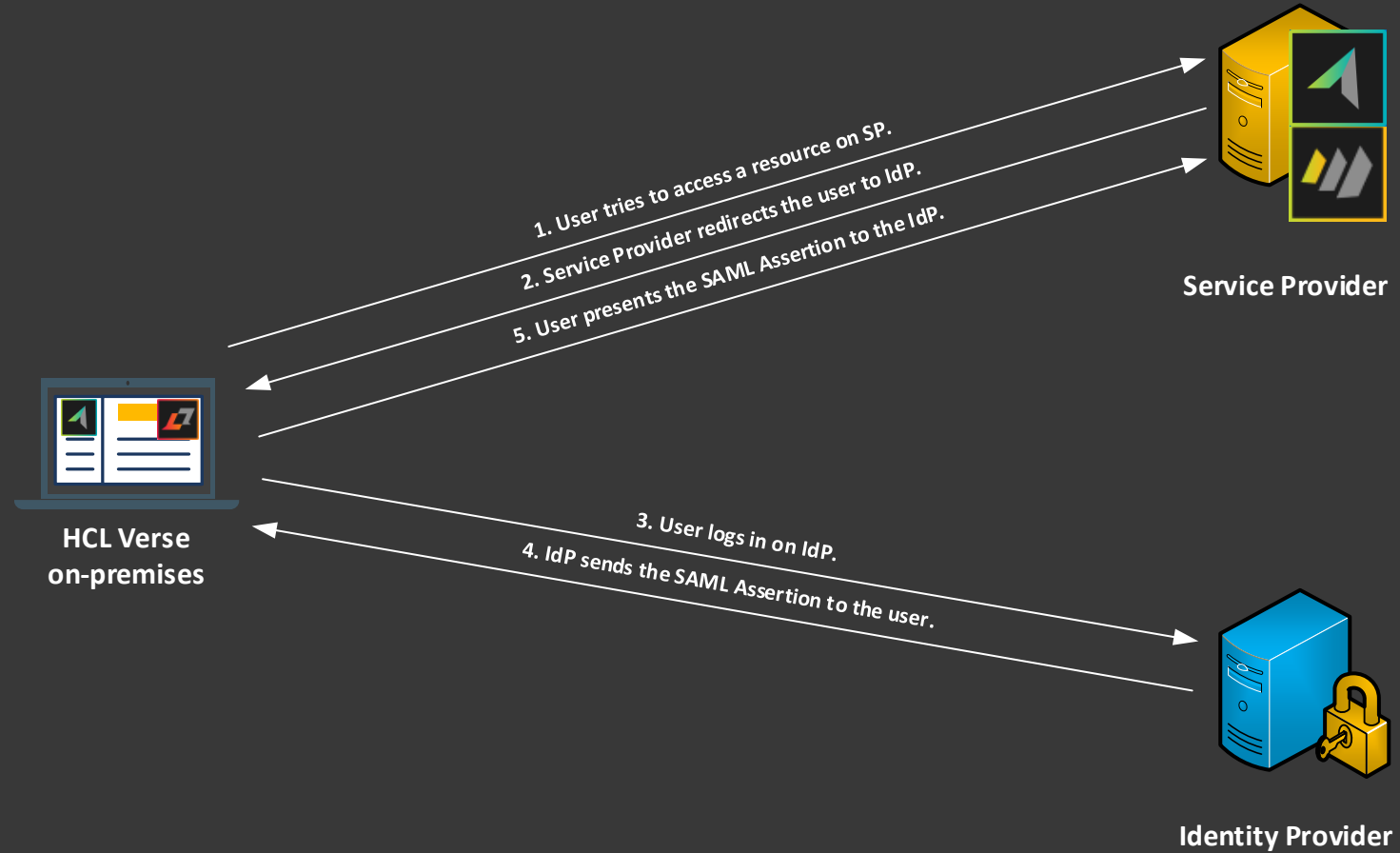
How Does it Work?

SP-Initiated Flow



How Does it Work?

SP-Initiated Flow



How Does it Work?

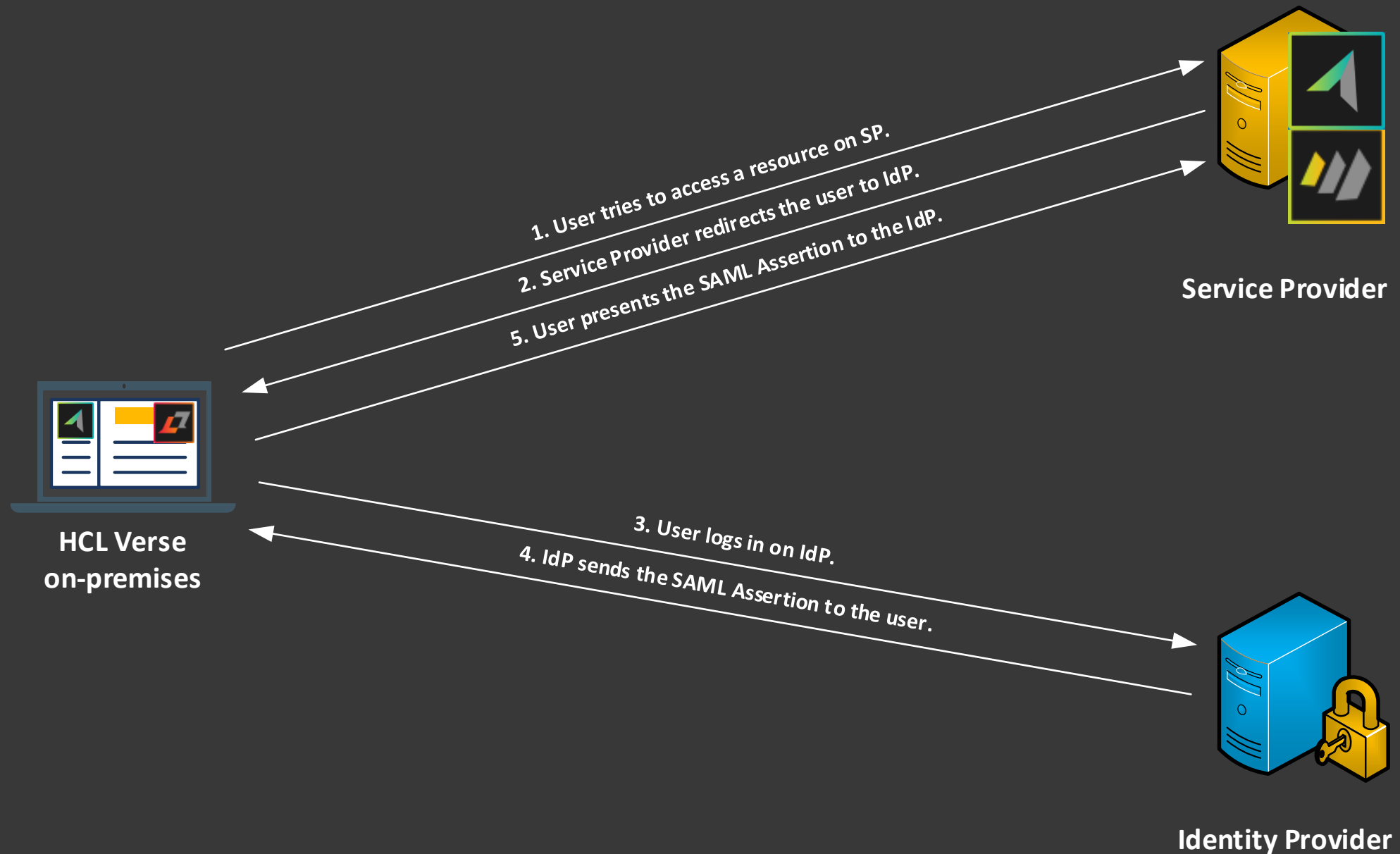


Table of Contents

Motivation	HCL Domino & SAML	Web Federated Login	Issues
Why SAML?	Prerequisites	Notes Federated Login	Q & A
SAML	Infrastructure Needed	Traveler & SAML	Shibboleth
Wording	Basic SAML Setup	Bonus – Nomad!	References
How does it work?	SAML & SSO	Troubleshooting	

Limitations / Incompatibilities



SAML 2.0 AuthNRequest

ADFS 3, 4, 5

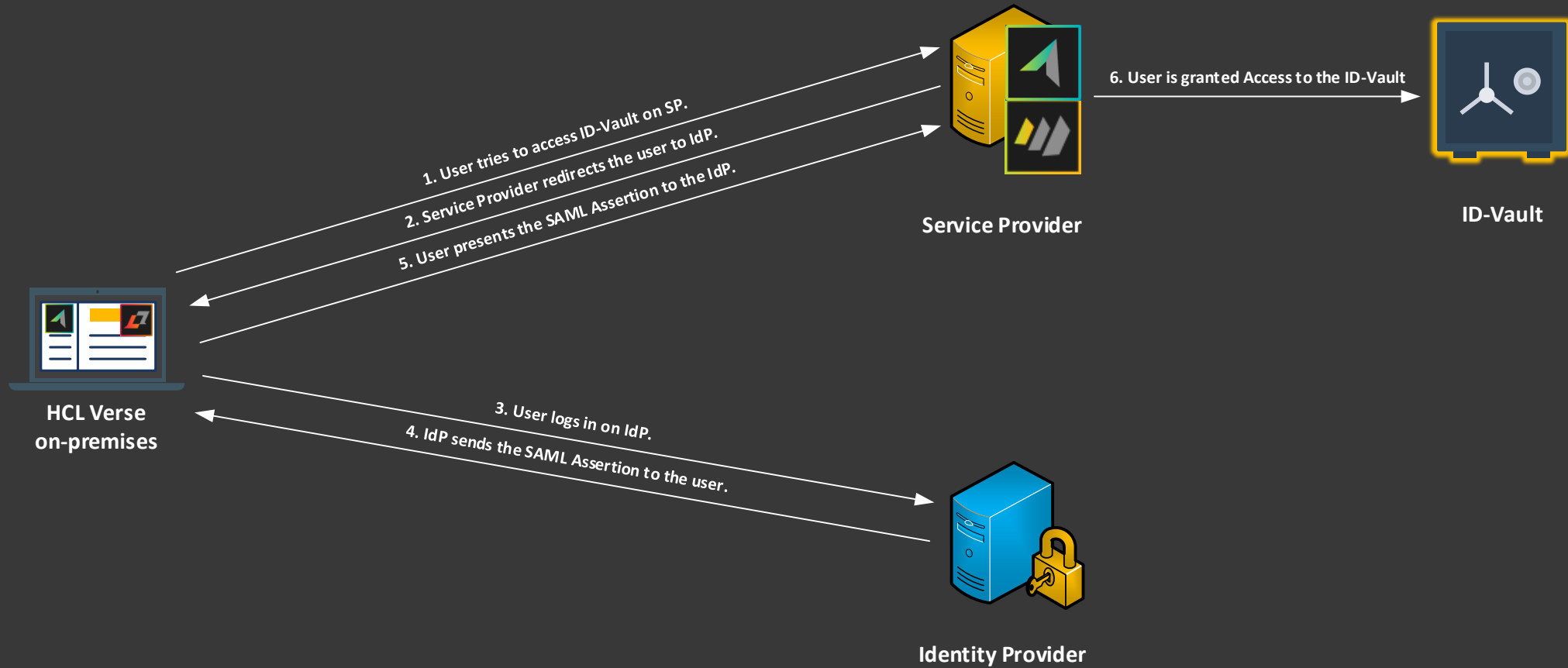
Shibboleth

DOMINO ...

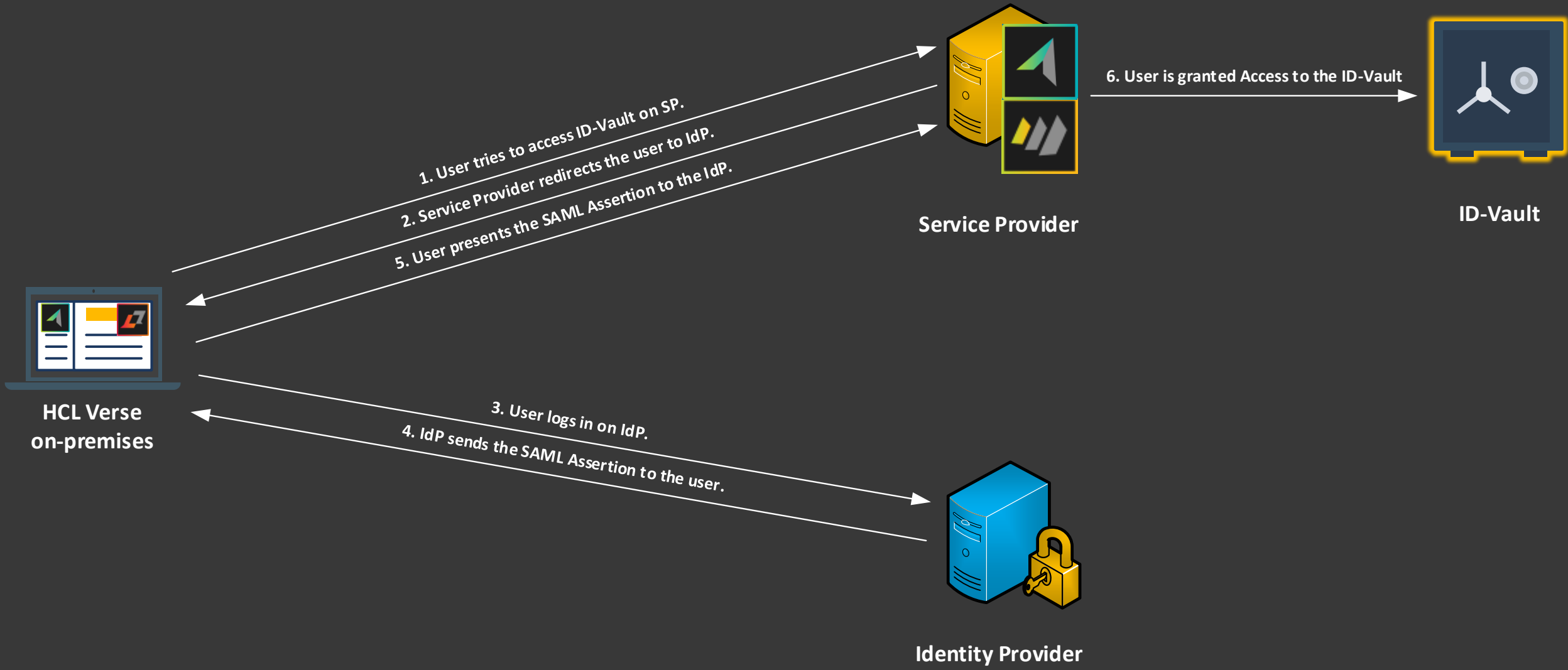
HTTPS



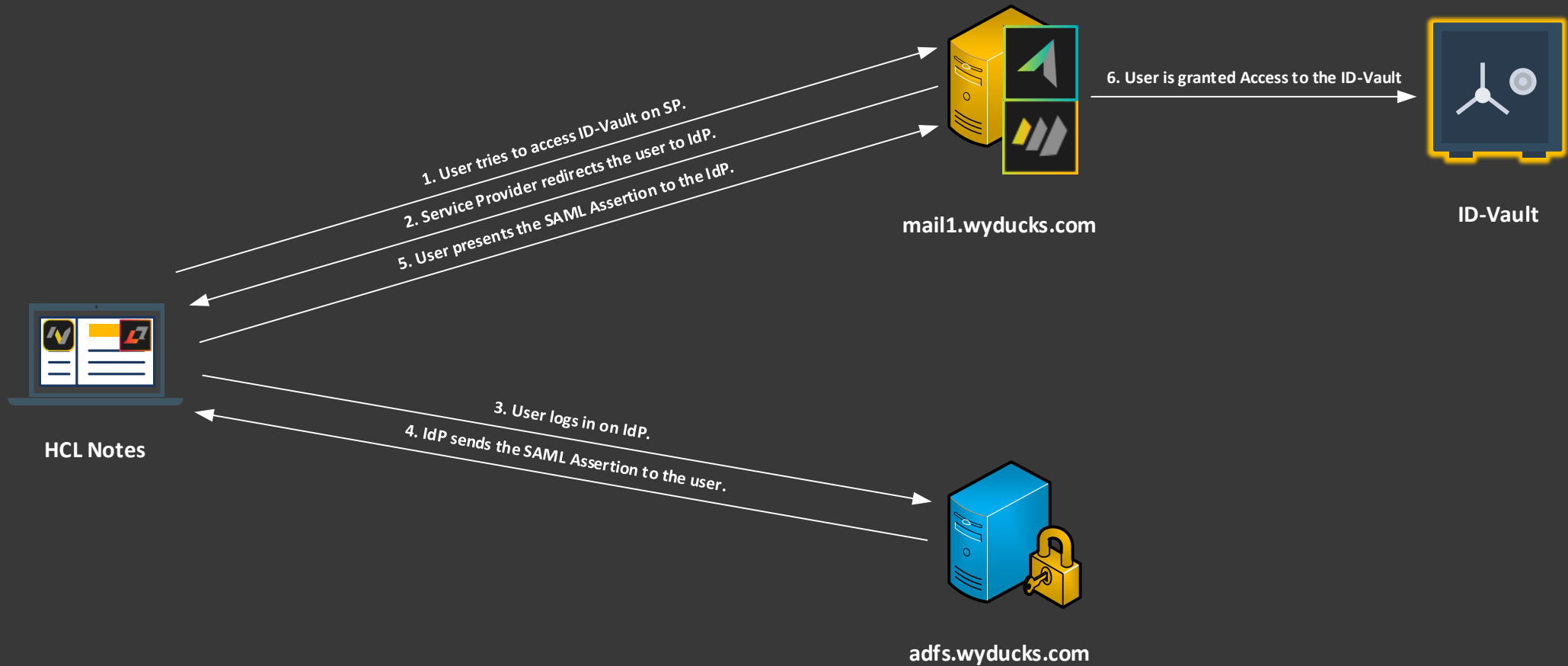
Web Federated Login



HCL Domino & SAML



Notes Federated Login



HCL Domino & SAML

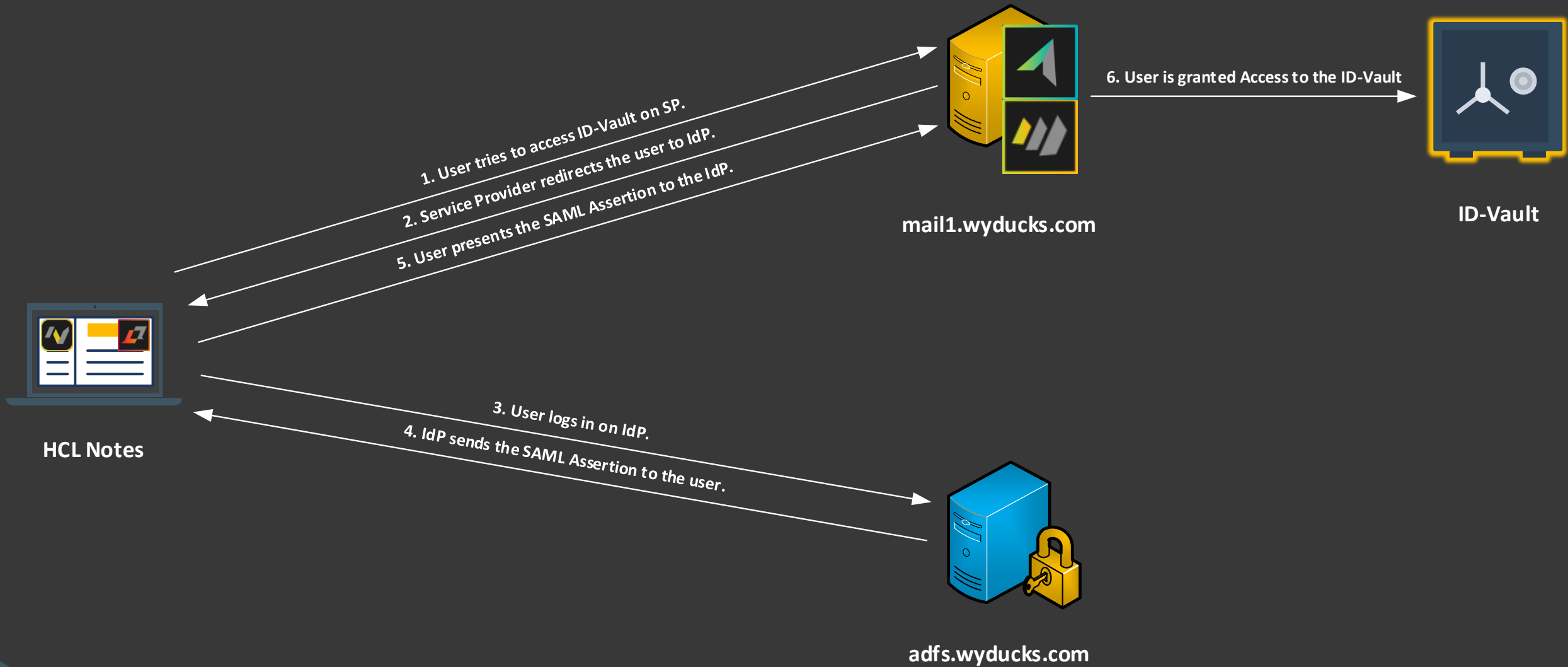


Table of Contents

Motivation

HCL Domino & SAML

Web Federated Login

Issues

Why SAML?

[Prerequisites](#)

Notes Federated Login

Q & A

SAML

Infrastructure Needed

Traveler & SAML

Shibboleth

Wording

Basic SAML Setup

Bonus – Nomad!

References

How does it work?

SAML & SSO

Troubleshooting

Prerequisites

Time Sync

DNS



HCL Domino 12.0.1 FP1 *Incl. latest Templates*

Prerequisites

Public TLS Certificate Domino Certificate Manager

Prerequisites

ID-Vault

Domino / SAML specifics



Table of Contents

Motivation

HCL Domino & SAML

Web Federated Login

Issues

Why SAML?

Prerequisites

Notes Federated Login

Q & A

SAML

Infrastructure Needed

Traveler & SAML

Shibboleth

Wording

Basic SAML Setup

Bonus – Nomad!

References

How does it work?

SAML & SSO

Troubleshooting

Infrastructure Needed

Three use-cases
We are using MS ADFS

Notes clients

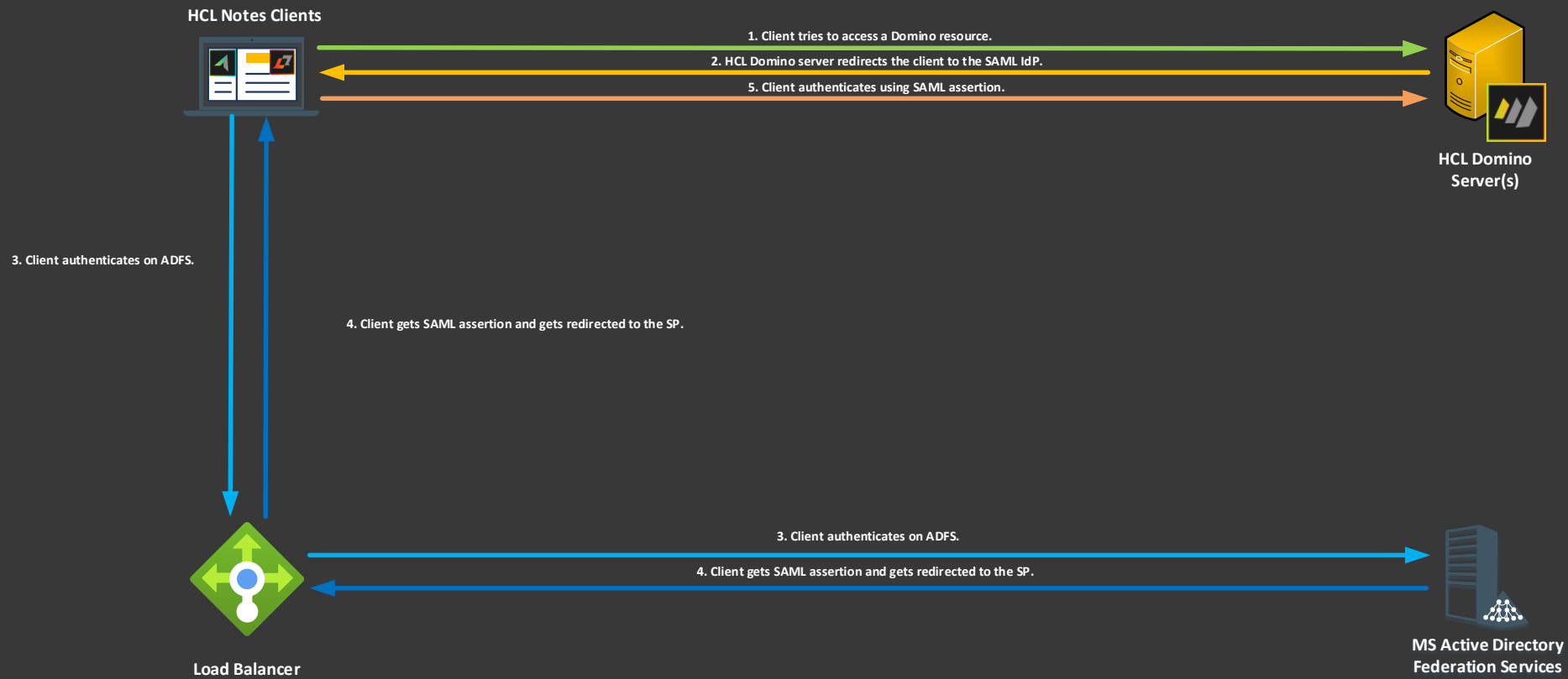


Infrastructure Needed

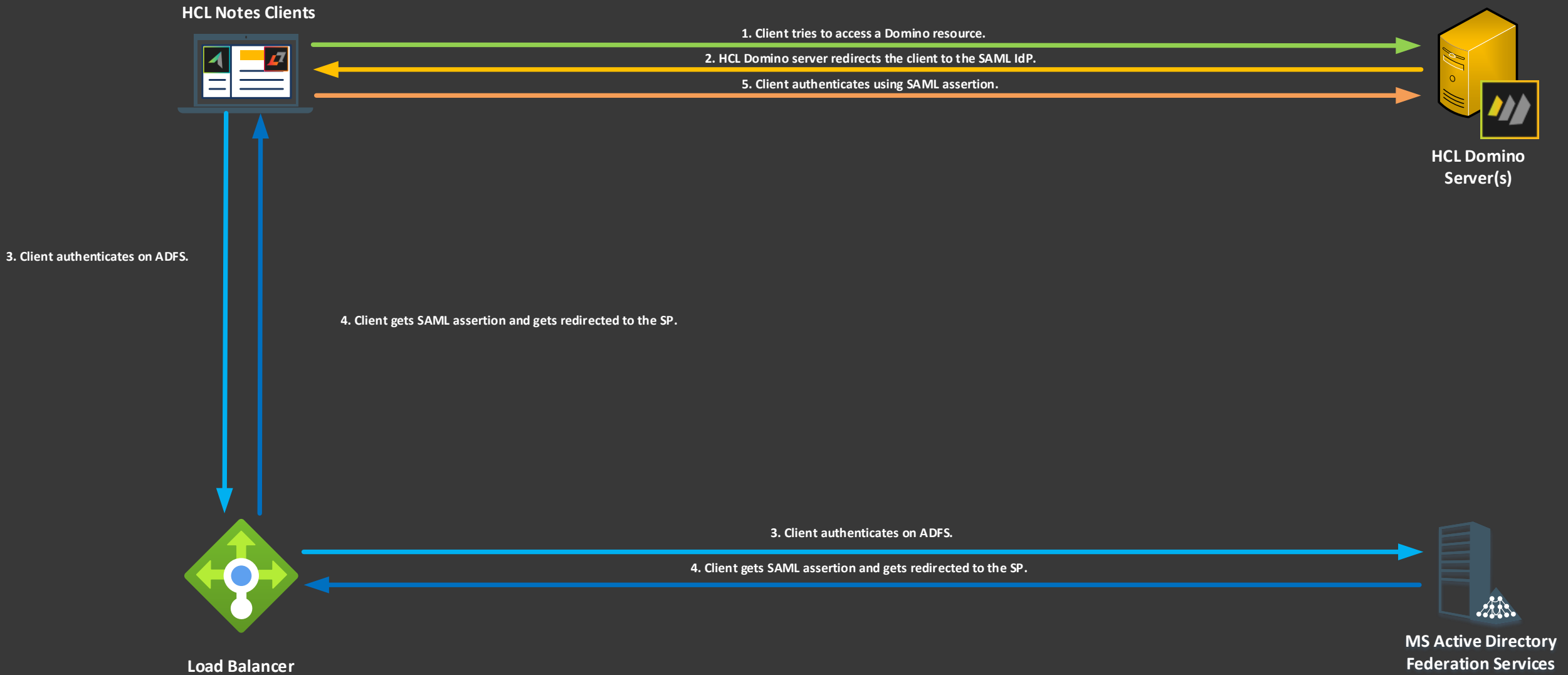


Enterprise Grade Infrastructure

Notes clients

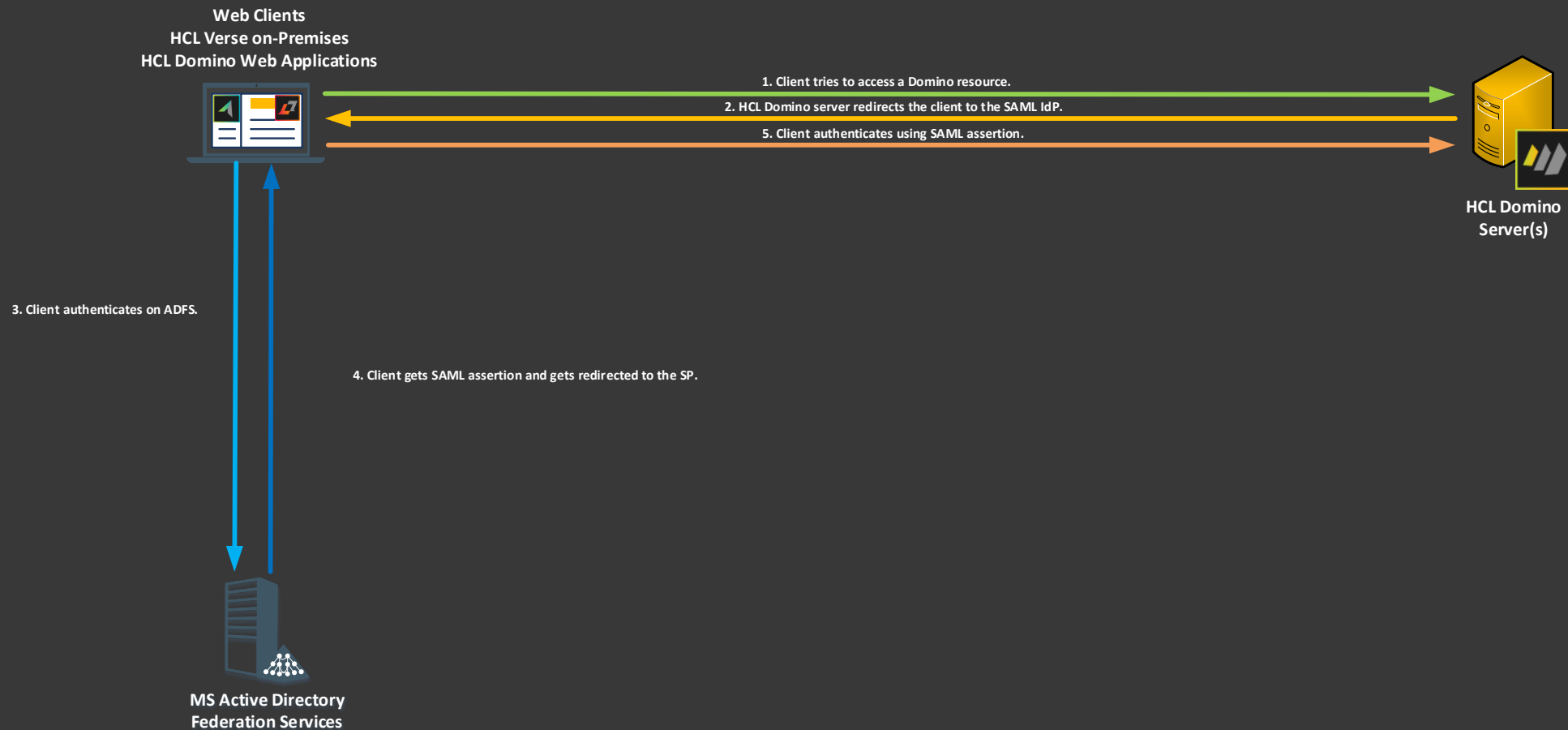


Enterprise Grade Infrastructure



Infrastructure Needed

Internal web clients



Infrastructure Needed

Web Clients
HCL Verse on-Premises
HCL Domino Web Applications



1. Client tries to access a Domino resource.

2. HCL Domino server redirects the client to the SAML IdP.

5. Client authenticates using SAML assertion.



HCL Domino Server(s)

3. Client authenticates on ADFS.

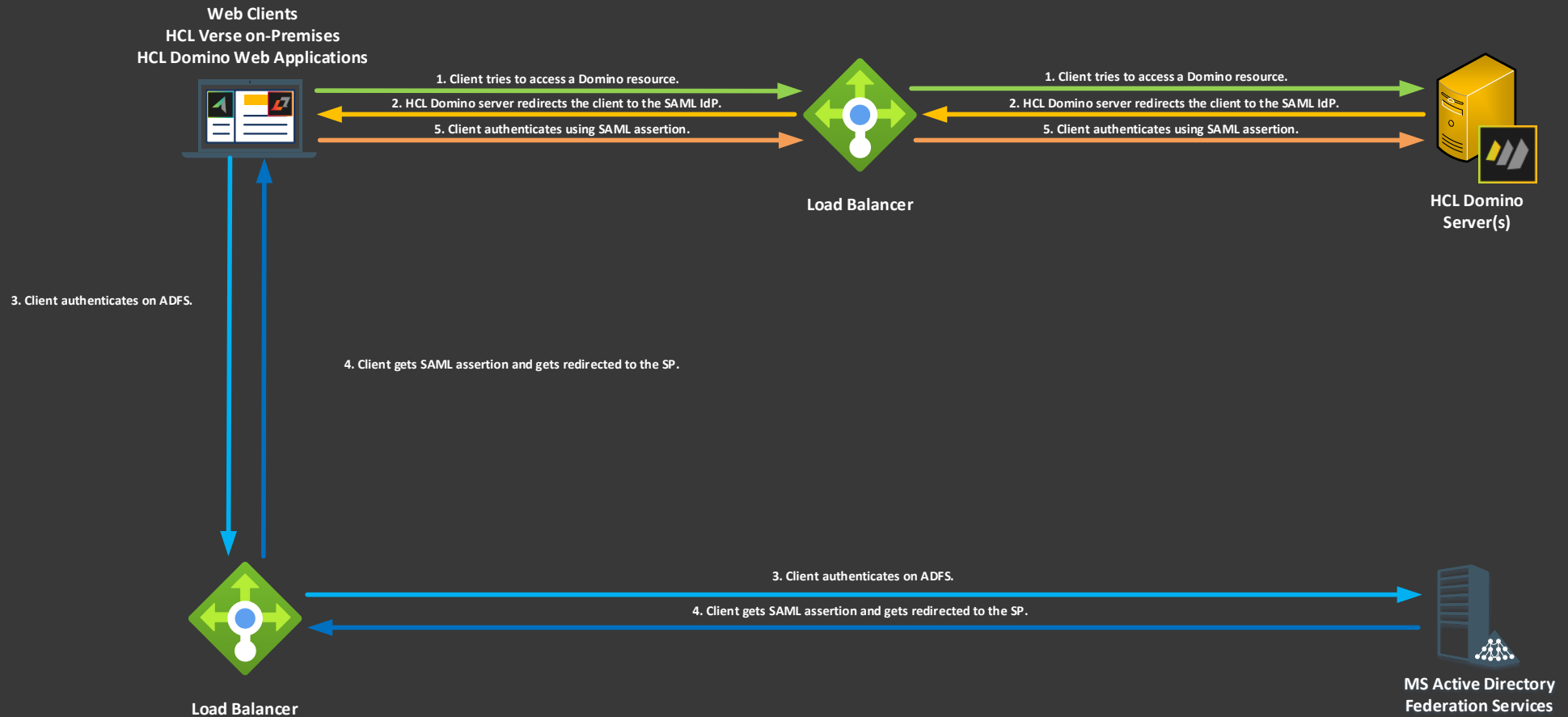
4. Client gets SAML assertion and gets redirected to the SP.



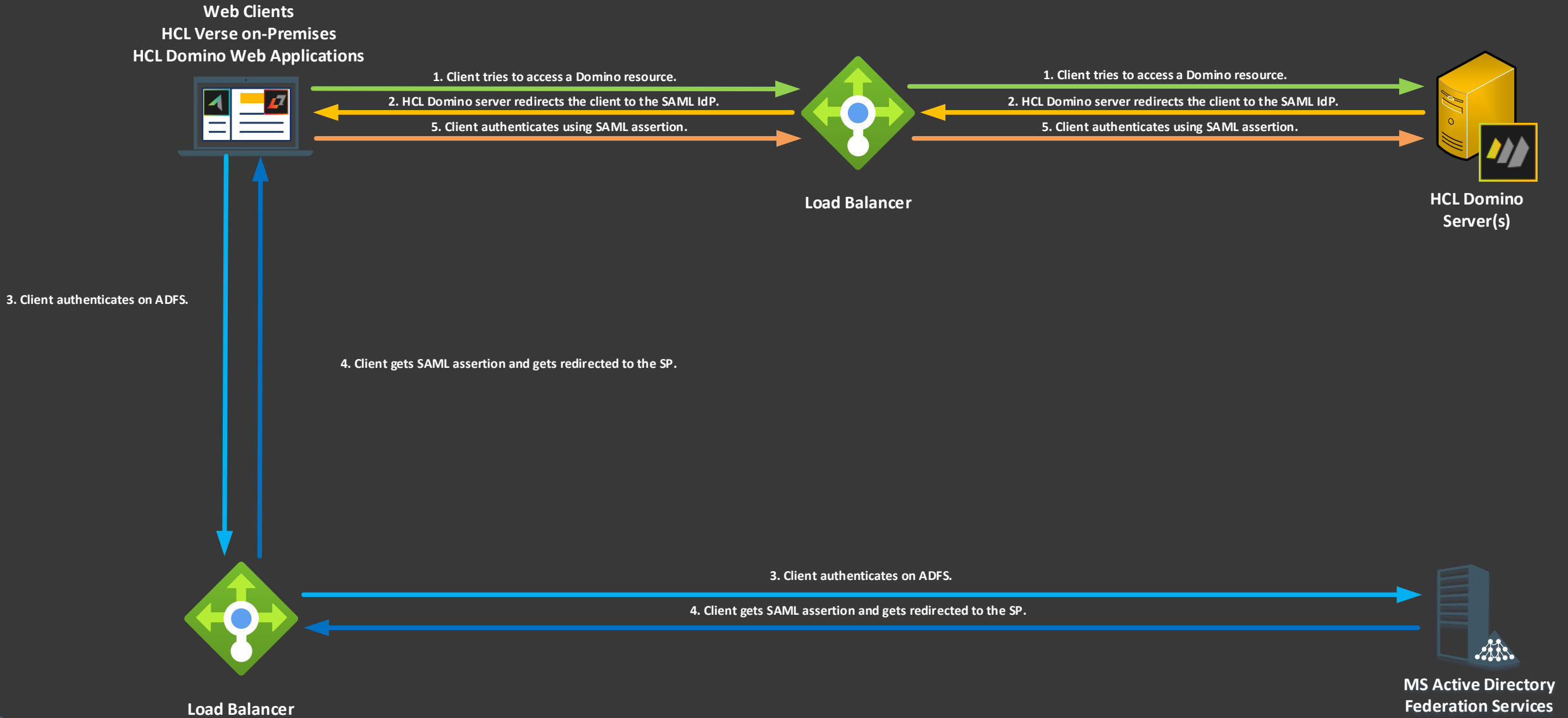
MS Active Directory Federation Services

Enterprise Grade Infrastructure

Internal web clients

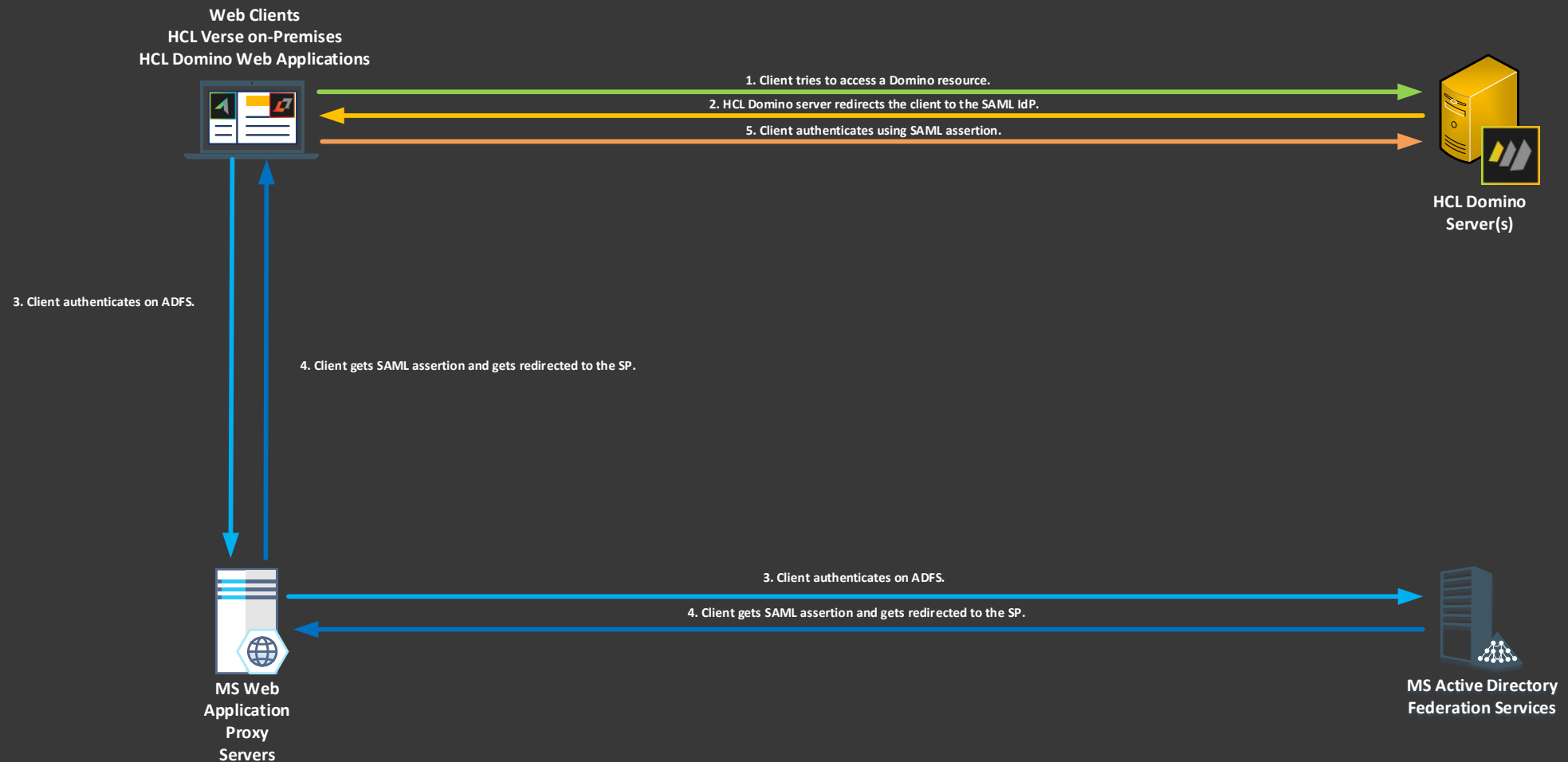


Enterprise Grade Infrastructure

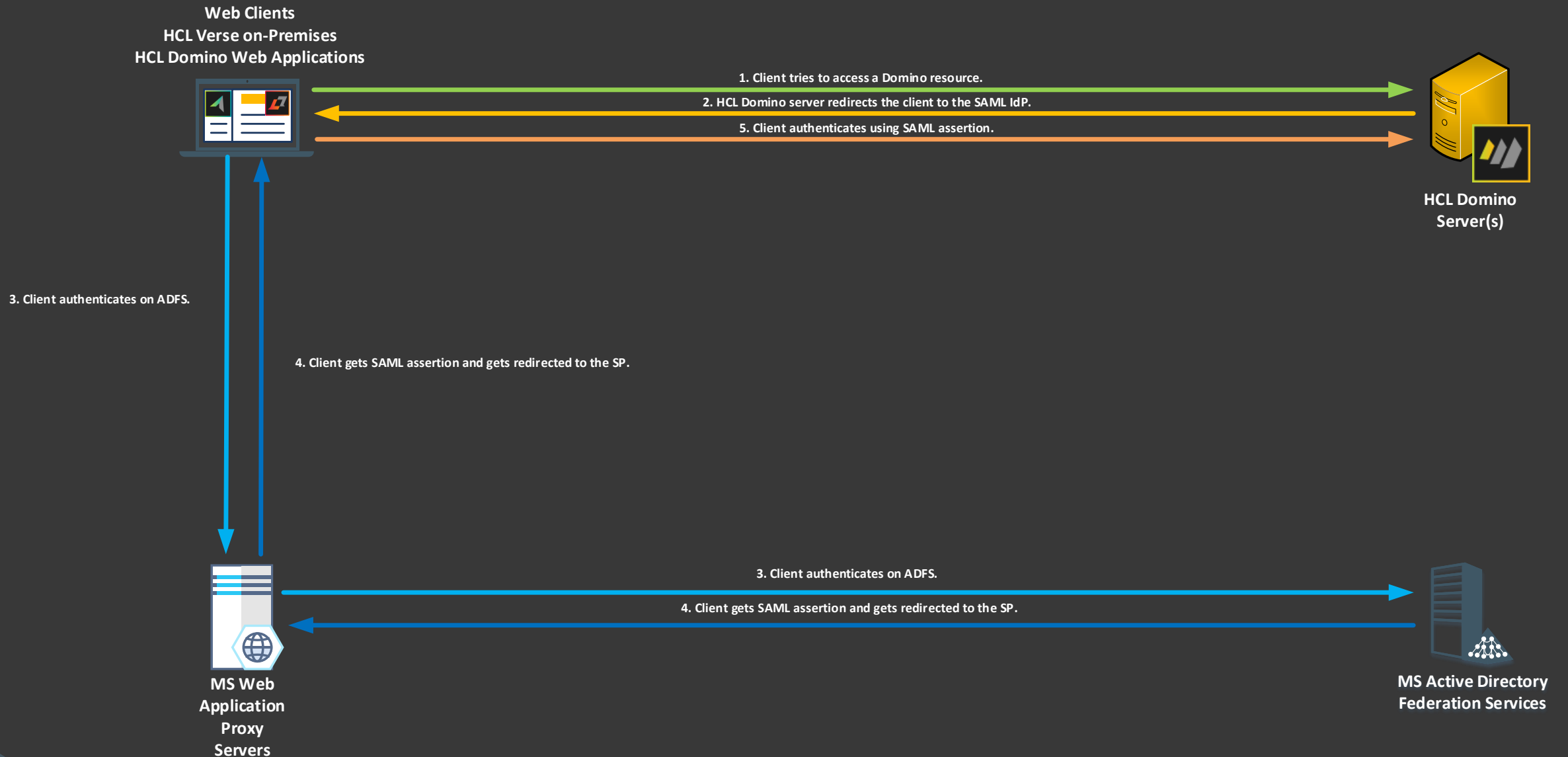


Infrastructure Needed

External web clients

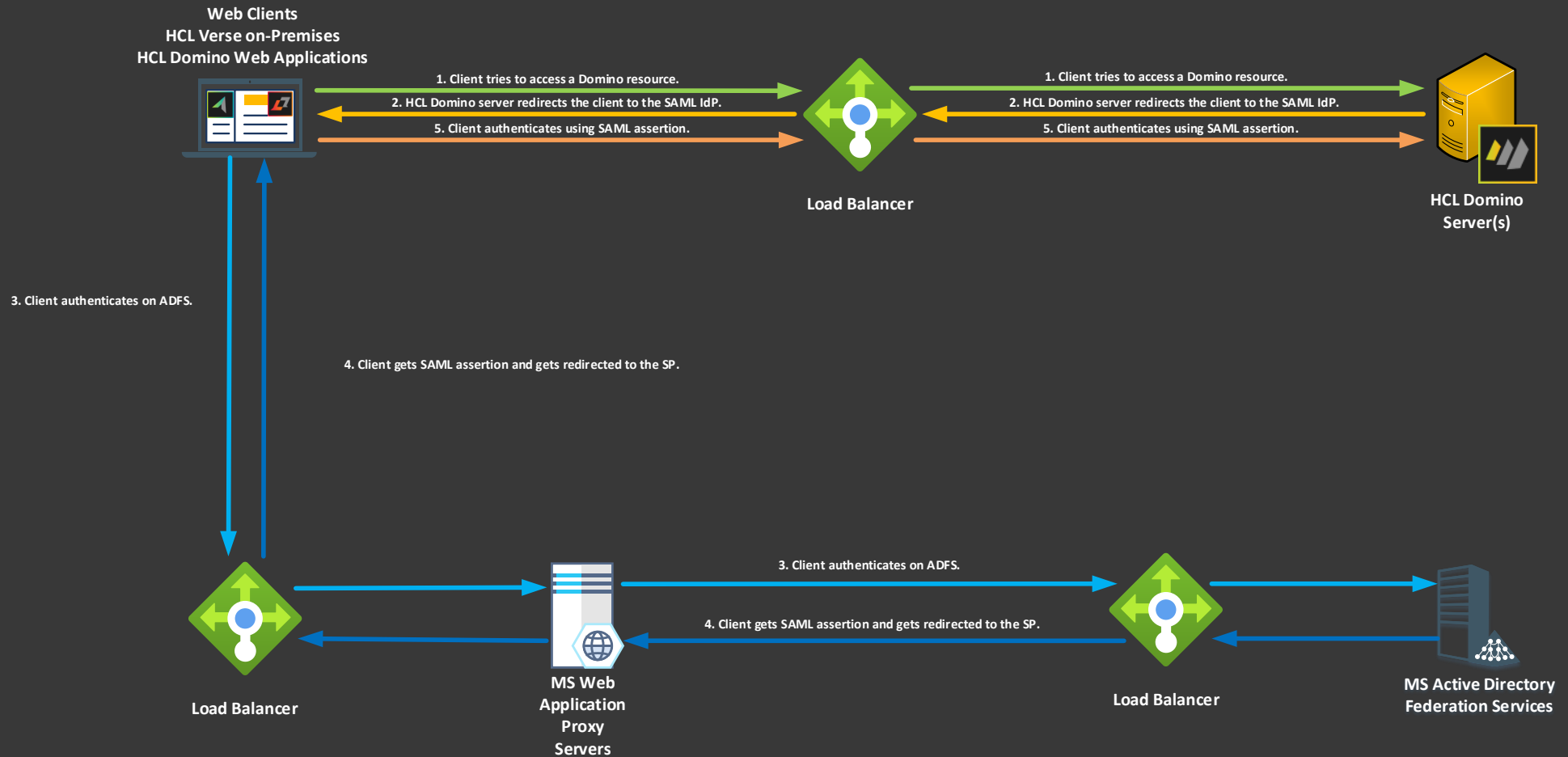


Infrastructure Needed



Enterprise Grade Infrastructure

External web clients



Enterprise Grade Infrastructure

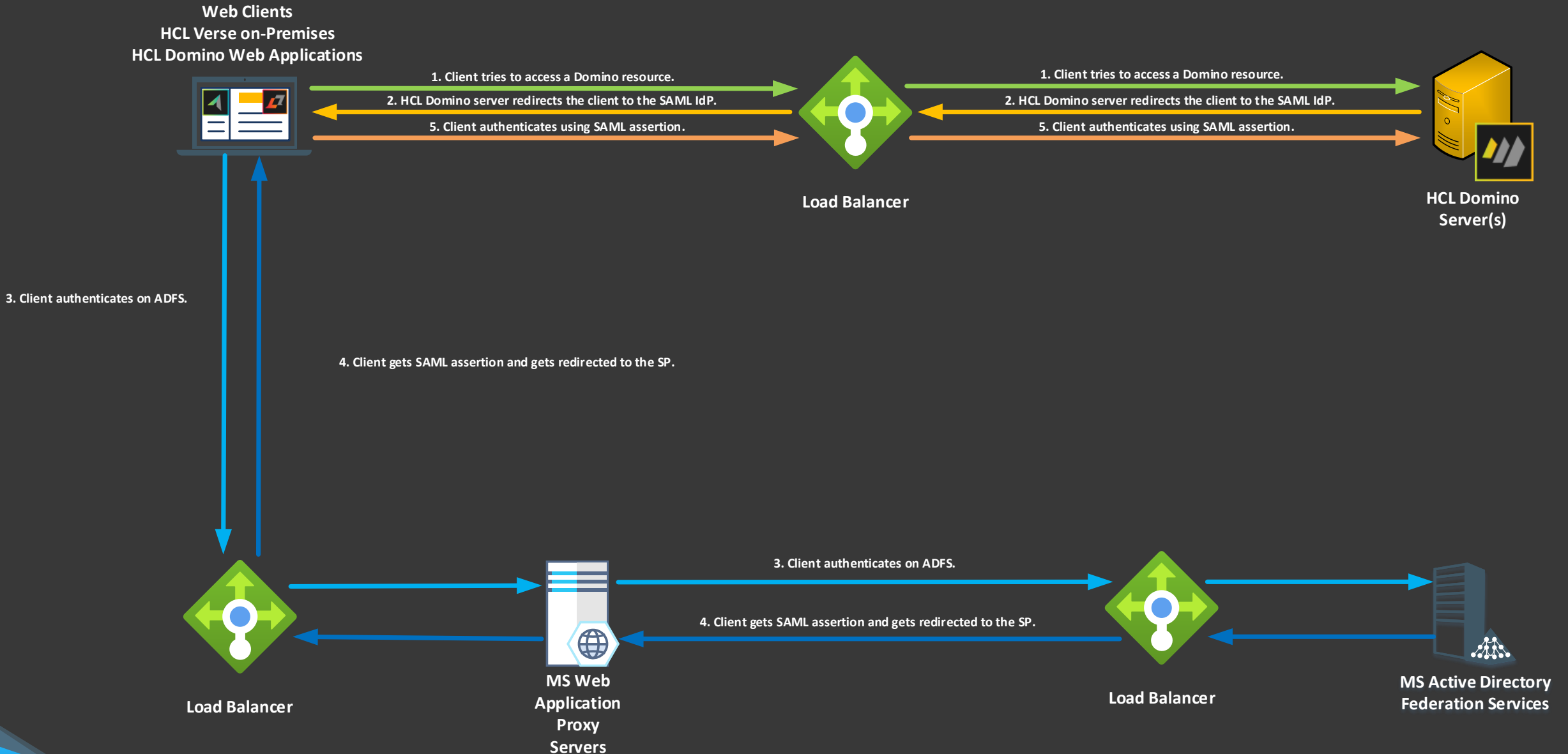
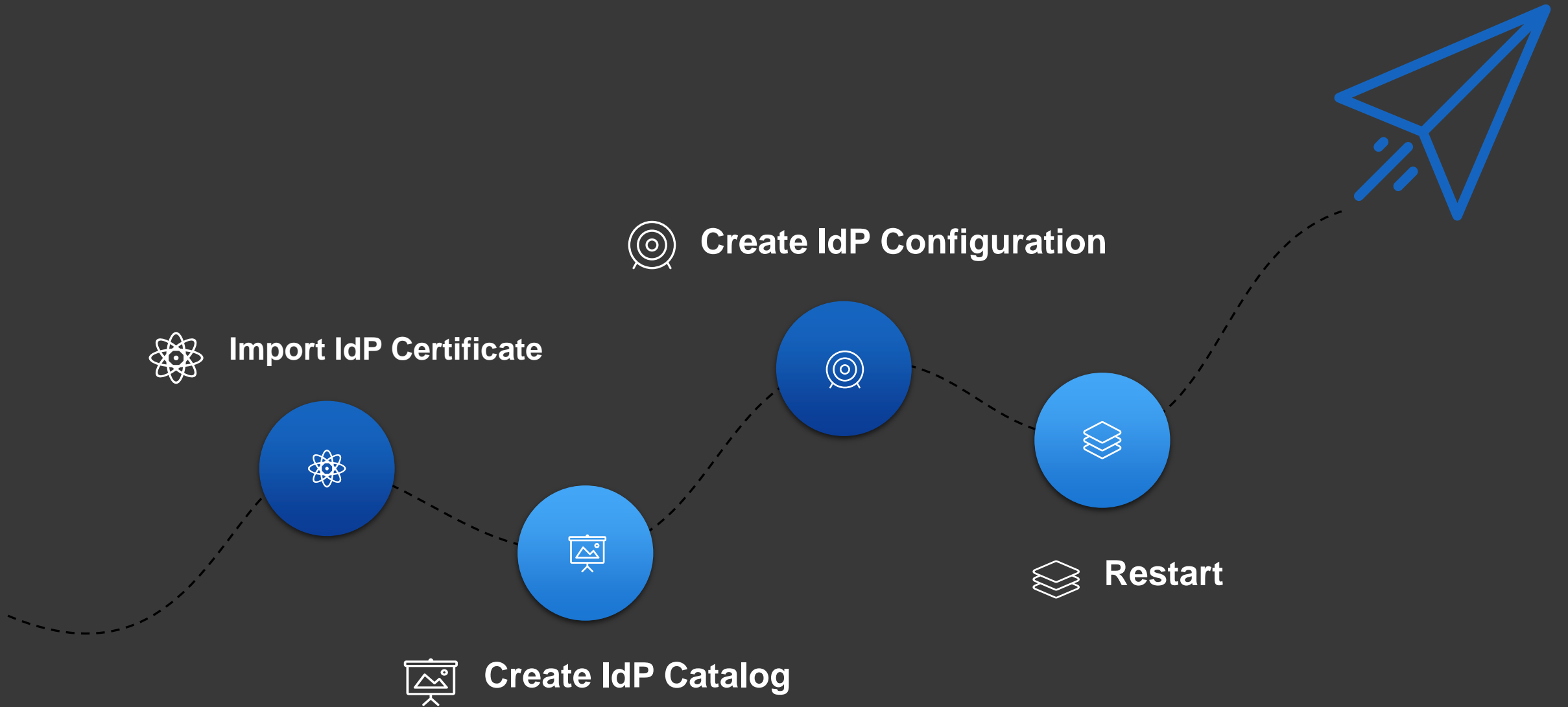


Table of Contents

Motivation	HCL Domino & SAML	Web Federated Login	Issues
Why SAML?	Prerequisites	Notes Federated Login	Q & A
SAML	Infrastructure Needed	Traveler & SAML	Shibboleth
Wording	Basic SAML Setup	Bonus – Nomad!	References
How does it work?	SAML & SSO	Troubleshooting	

Basic SAML Setup

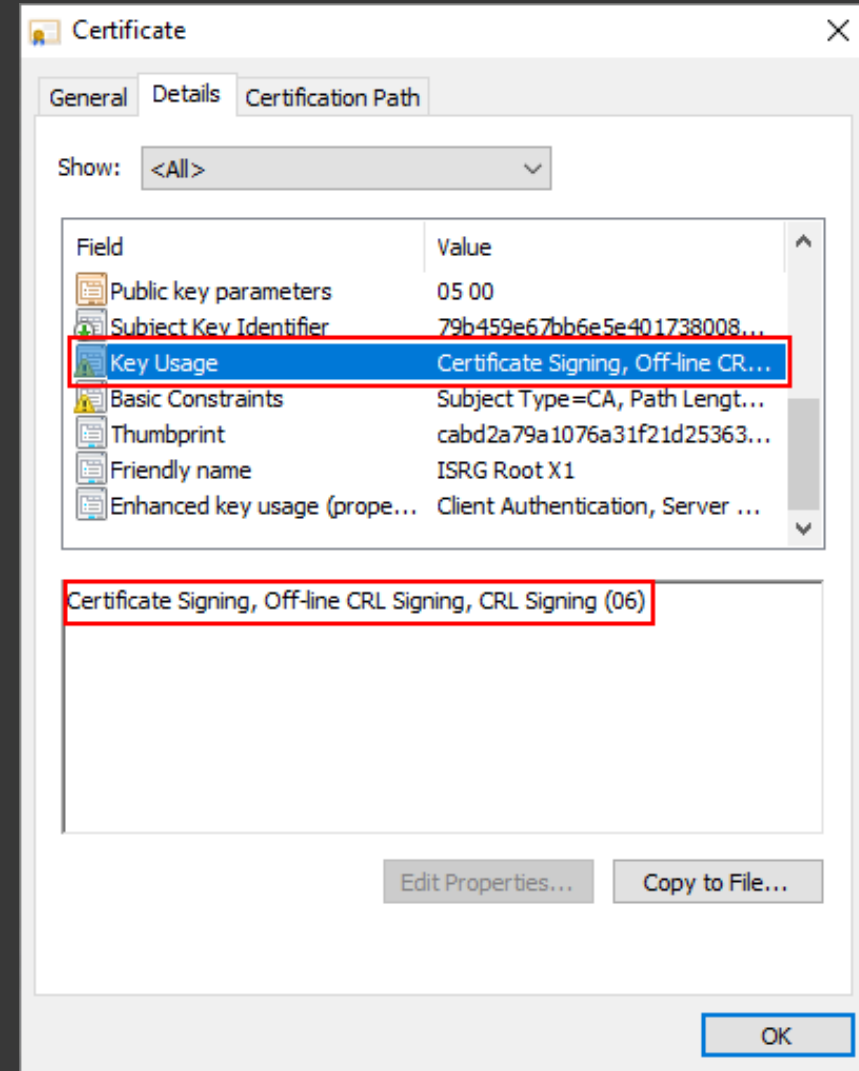
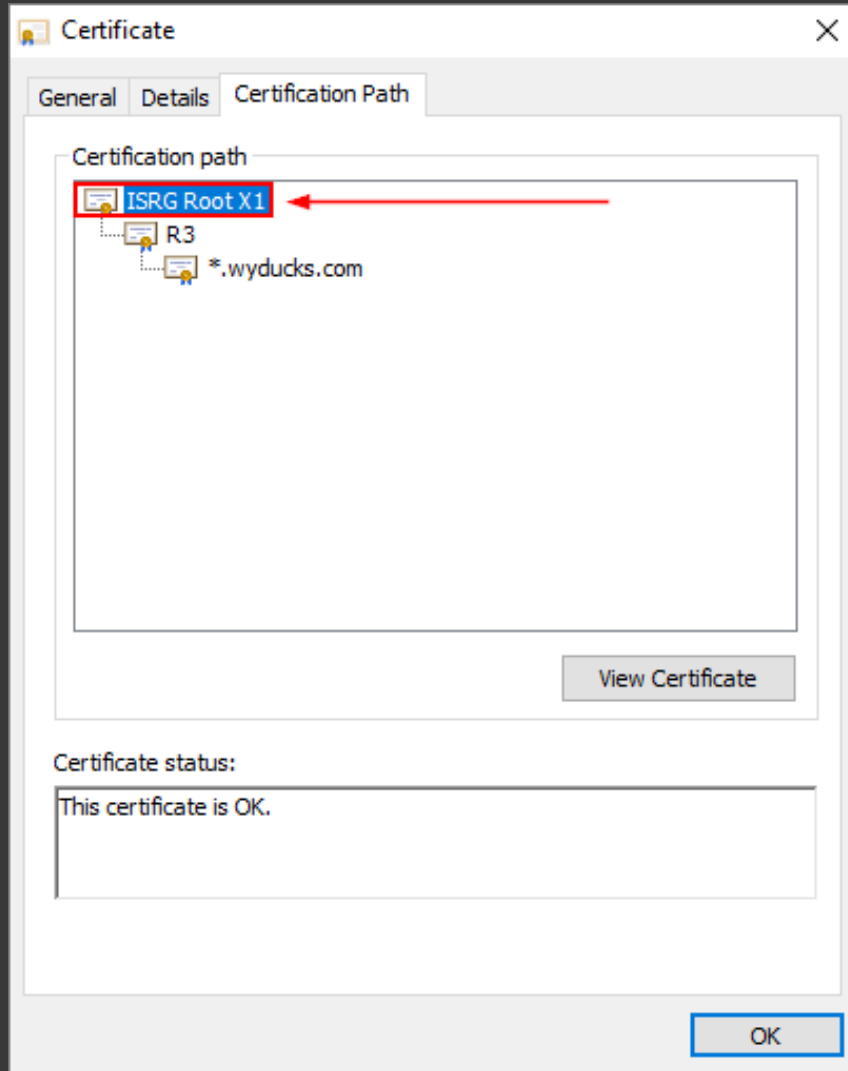


Import IdP Certificate

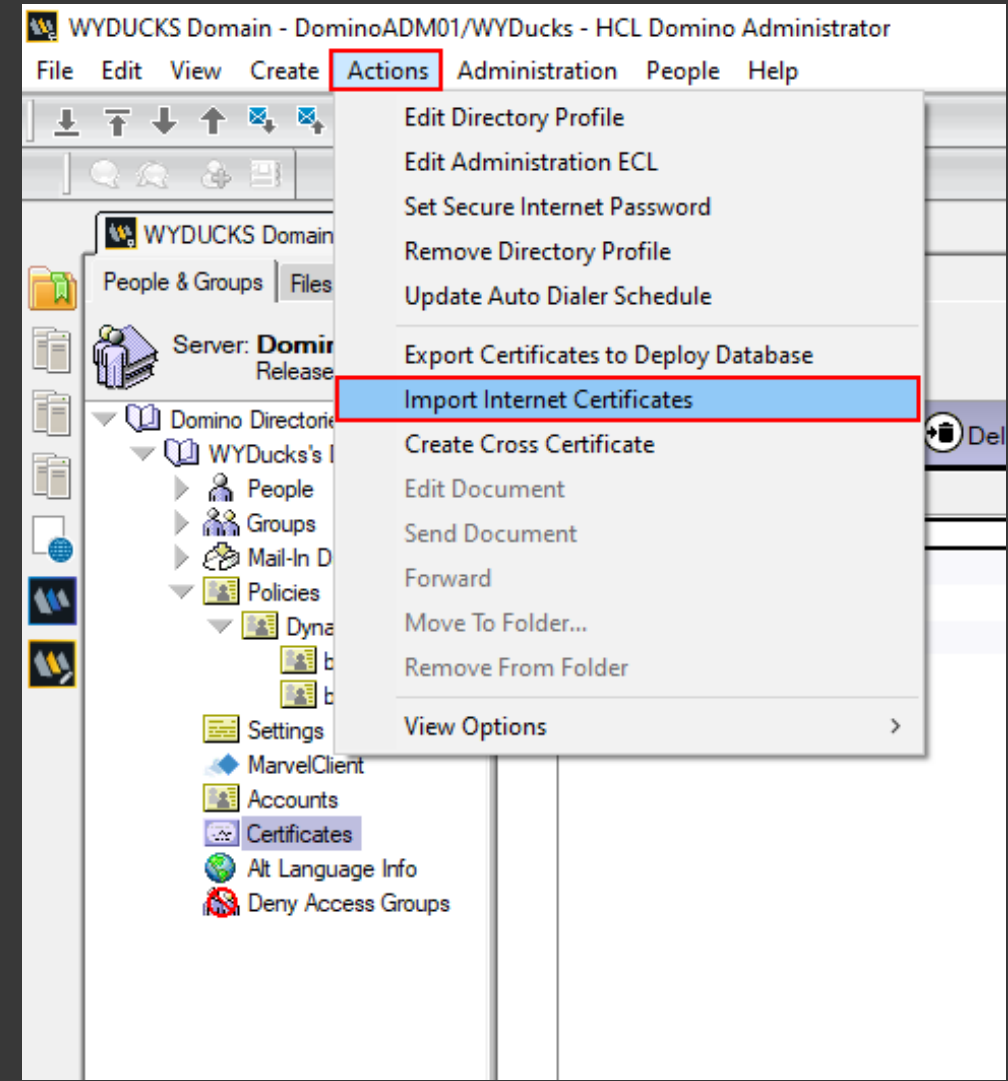
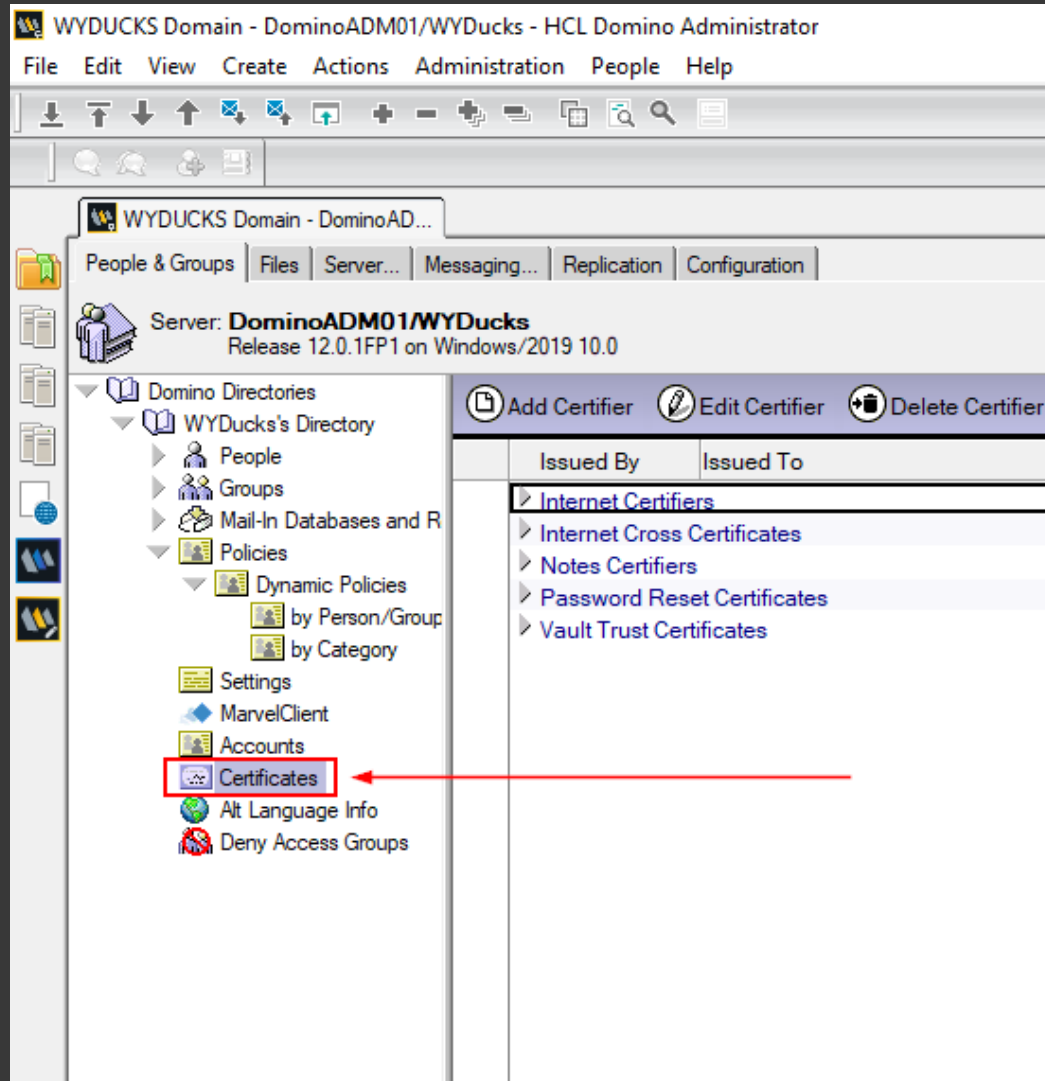
Get the full-chain



Import IdP Certificate



Import IdP Certificate



Import IdP Certificate

Select Import File Format

In what format is your certificate stored in the file?

Binary encoded X.509

Base 64 encoded X.509

PKCS 12 encoded


PKCS 7 encoded

Continue Cancel

Import Internet Certificates

Do you want to accept all certificates from the import file into the directory?

All Internet Certificates

Type	Issued To	Issued By
	ISRG Root X1	ISRG Root X1

Selected item:

Issued to	ISRG Root X1	(Email)	
Issued by	ISRG Root X1	(Email)	
Activated	04.06.2015	Type	Internet certificate authority
Expires	04.06.2035	Fingerprint	0CD2 F9E0 DA17 73E9 ED86 4DA5 E370 E74E

Advanced Details...

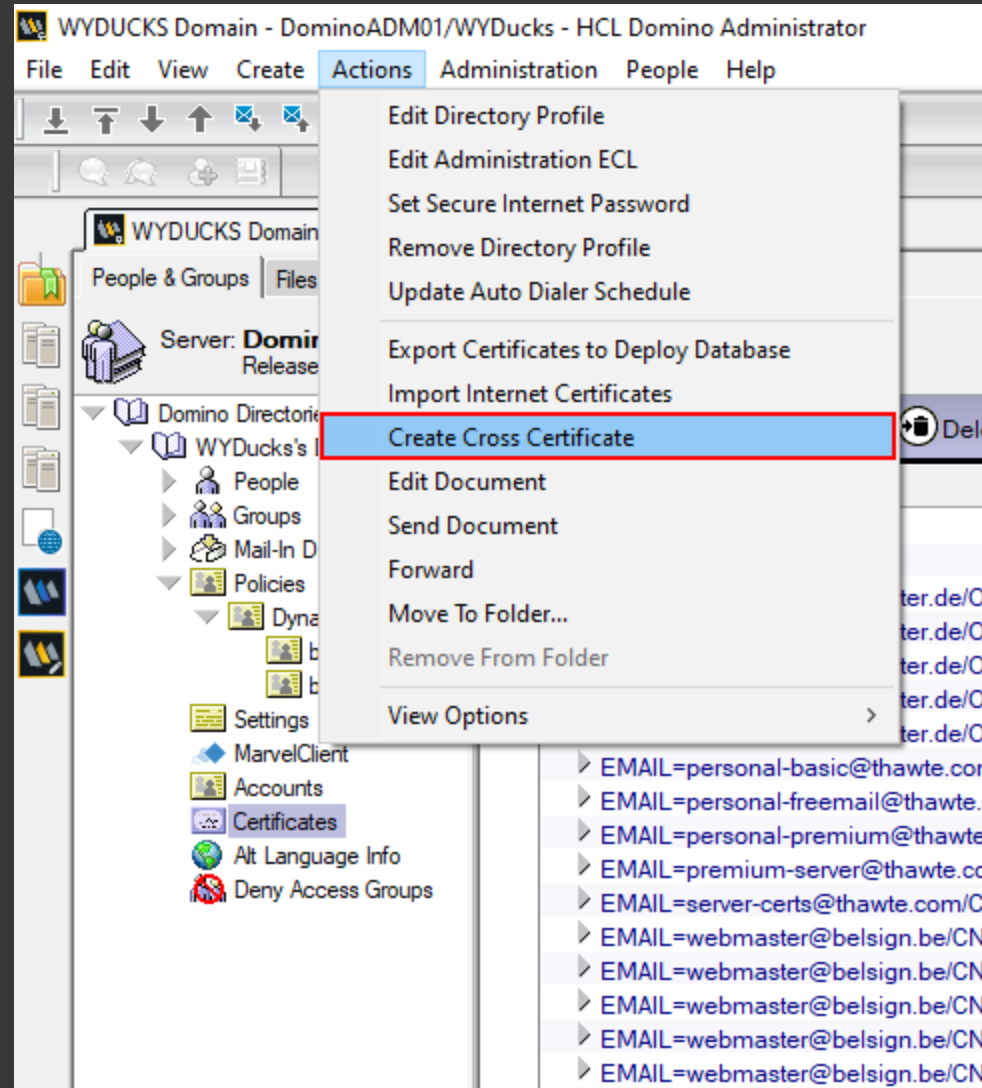
Accept All Cancel

Create a Cross Certificate

The screenshot shows the HCL Domino Administrator interface for the 'WYDUCKS Domain'. The left sidebar displays the 'Domino Directories' tree, with 'Certificates' selected. The main pane shows a list of certificates with columns for 'Issued By' and 'Issued To'. A red arrow points to the entry 'R3/Let's EncryptUS' under the 'Internet Security Research Group' category.

Issued By	Issued To
Internet Certifiers	
Digital Signature Trust Co.	
EMAIL=certificate@trustcenter.de/OU=TC TrustCenter Class 0 CA/O=TC TrustCenter for Security in Data Networks GmbH/L=Hamburg/ST=Hamburg/C=DE	
EMAIL=certificate@trustcenter.de/OU=TC TrustCenter Class 1 CA/O=TC TrustCenter for Security in Data Networks GmbH/L=Hamburg/ST=Hamburg/C=DE	
EMAIL=certificate@trustcenter.de/OU=TC TrustCenter Class 2 CA/O=TC TrustCenter for Security in Data Networks GmbH/L=Hamburg/ST=Hamburg/C=DE	
EMAIL=certificate@trustcenter.de/OU=TC TrustCenter Class 3 CA/O=TC TrustCenter for Security in Data Networks GmbH/L=Hamburg/ST=Hamburg/C=DE	
EMAIL=certificate@trustcenter.de/OU=TC TrustCenter Class 4 CA/O=TC TrustCenter for Security in Data Networks GmbH/L=Hamburg/ST=Hamburg/C=DE	
EMAIL=personal-basic@thawte.com/CN=Thawte Personal Basic CA/OU=Certification Services Division/O=Thawte Consulting/L=Cape Town/ST=Western Cape/C=ZA	
EMAIL=personal-freemail@thawte.com/CN=Thawte Personal Freemail CA/OU=Certification Services Division/O=Thawte Consulting/L=Cape Town/ST=Western Cape/C=ZA	
EMAIL=personal-premium@thawte.com/CN=Thawte Personal Premium CA/OU=Certification Services Division/O=Thawte Consulting/L=Cape Town/ST=Western Cape/C=ZA	
EMAIL=premium-server@thawte.com/CN=Thawte Premium Server CA/OU=Certification Services Division/O=Thawte Consulting/L=Cape Town/ST=Western Cape/C=ZA	
EMAIL=server-certs@thawte.com/CN=Thawte Server CA/OU=Certification Services Division/O=Thawte Consulting/L=Cape Town/ST=Western Cape/C=ZA	
EMAIL=webmaster@belsign.be/CN=BelSign Class 1 CA/OU=BelSign Class 1 Certificate Authority/O=BelSign NV/L=Brussels/C=BE	
EMAIL=webmaster@belsign.be/CN=BelSign Class 2 CA/OU=BelSign Class 2 Certificate Authority/O=BelSign NV/L=Brussels/C=BE	
EMAIL=webmaster@belsign.be/CN=BelSign Class 3 CA/OU=BelSign Class 3 Certificate Authority/O=BelSign NV/L=Brussels/C=BE	
EMAIL=webmaster@belsign.be/CN=BelSign Object Publishing CA/OU=BelSign Object Publishing Certificate Authority/O=BelSign NV/L=Brussels/C=BE	
EMAIL=webmaster@belsign.be/CN=BelSign Secure Server CA/OU=BelSign Secure Server Certificate Authority/O=BelSign NV/L=Brussels/C=BE	
Entrust.net	
IE	
JP	
US	
Entrust.net	
Equifax	
GTE Corporation	
Internet Security Research Group	
ISRG Root X1	
R3/Let's EncryptUS	
Let's Encrypt	
RSA Data Security, Inc.	
VeriSign, Inc.	

Create a Cross Certificate



Create a Cross Certificate

The screenshot shows a Windows-style dialog box titled "Issue Cross Certificate". It contains the following fields and controls:

- Certifier...**: /WYDucks
- Server...**: DominoADM01/WYDucks
- Subject name**: R3/Let's Encrypt/US (dropdown menu)
- Subject alternate names**: (empty text box)
- Fingerprint**: E829 E65D 7C43 07D6 FBC1 3C17 9E03 7A36
- Expiration date**: 12.05.2032 12:20:14
- Buttons**: "Cross certify" (highlighted with a red box) and "Cancel".

Create a Cross Certificate

WYDUCKS Domain - DominoADM01/WYDucks - HCL Domino Administrator

File Edit View Create Actions Administration People Help

WYDUCKS Domain - DominoAD...

People & Groups | Files | Server... | Messaging... | Replication | Configuration

Server: **DominoADM01/WYDucks**
Release 12.0.1FP1 on Windows/2019 10.0

Domino Directories

- WYDucks's Directory
 - People
 - Groups
 - Mail-In Databases and R
 - Policies
 - Dynamic Policies
 - by Person/Group
 - by Category
 - Settings
 - MarvelClient
 - Accounts
 - Certificates**
 - Alt Language Info
 - Deny Access Groups

Add Certifier | Edit Certifier | Delete Certifier | Copy to Personal Address Book

Issued By	Issued To
	Internet Certifiers
	Internet Cross Certificates
	WYDucks
	CN=wyducks-ADDC01-CA/DC=wyducks/DC=azure
	ISRG Root X1/Internet Security Research Group/US
	R3/Let's Encrypt/US
	Notes Certifiers
	Password Reset Certificates
	Vault Trust Certificates

Create the IdP Catalog

“idpcat.nsf”

Create and replicate

Create the IdP Catalog

New Application

Specify New Application Name and Location

Server: DominoADM01/WYDucks

Title: IdP Catalog

File name: idpcat.nsf

Encryption...

Create full text index for searching

Specify Template for New Application

Server: DominoADM01/WYDucks

Template:

- HCL Notes/Domino Fault Reports
- HCL Notes/Domino Smart Upgrade
- ID Vault (12)
- IdP Catalog (12)**
- Internet Password Lockout (12)
- Issued Certificates List

File name: idpcat.ntf

Show advanced templates

Inherit future design changes

Get the IdP Configuration

FederationMetadata.xml

Create some backup copies

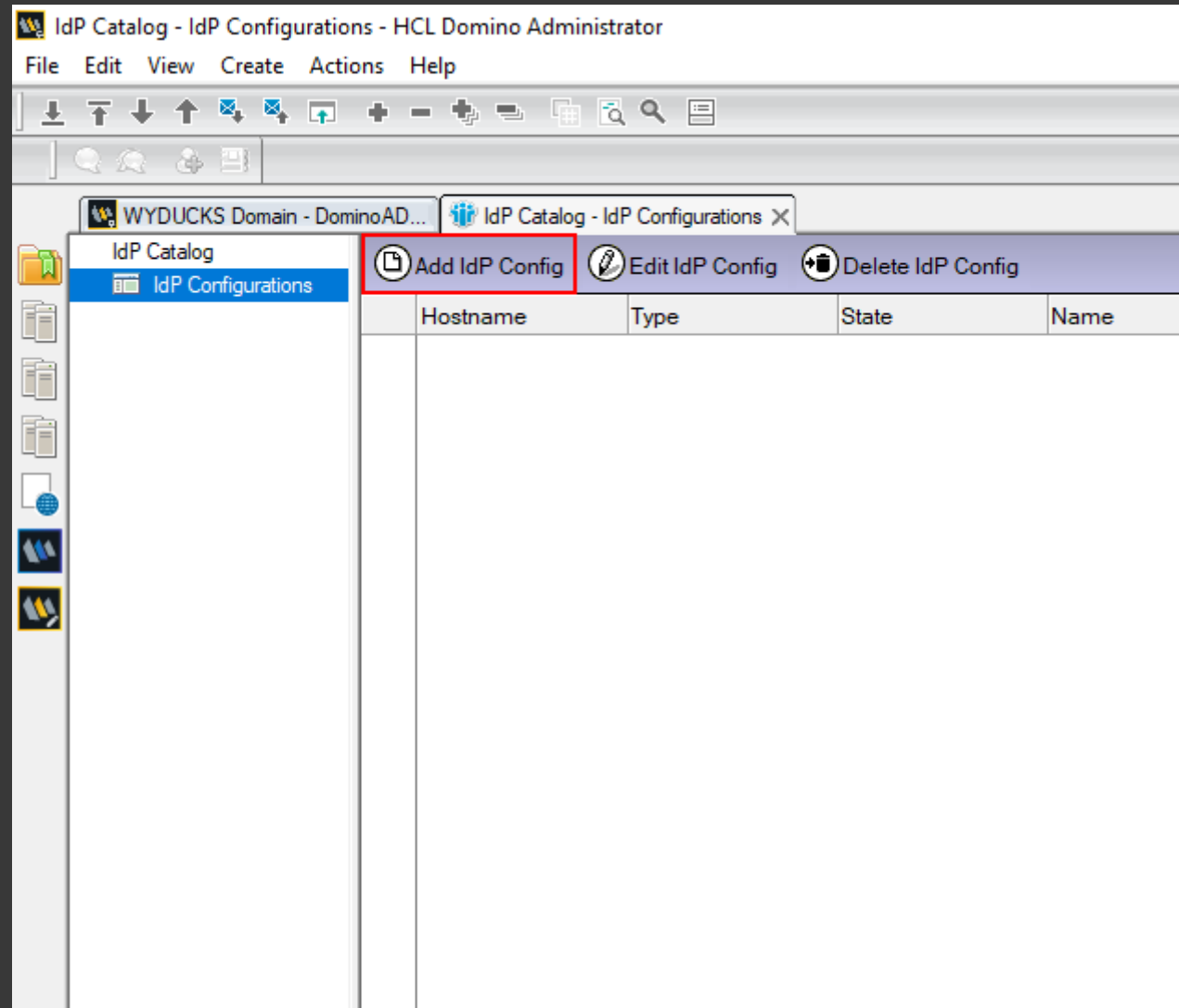
```
function digital_best_reviews_posts  
global $post;  
$orig_post = $post;  
$cat_query1 = new WP_Query(  
    1));  
while ($cat_query1->have_posts()) {  
    $cat_query1->next_post();  
}
```


Create the IdP Configuration Document

Inside of "idpcat.nsf"



Create the IdP Configuration Document



Create the IdP Configuration Document

Save & Close Cancel

IdP Configuration


Basics Client Settings Certificate Management **Advanced** Administration

Basics

Import XML file

Host names or addresses mapped to this site:

Protocol version: SAML 2.0
State: Enabled
Federation product: AuthnRequest SAML 2.0 compatible
Service provider ID:
Artifact resolution service URL:
Single sign-on service URL: https://adfs.wyducks.com/adfs/ls/
Encryption method: http://www.w3.org/2001/04/xmlenc#sha256

IdP name (for your reference):
Comment:
Imported file:  - FederationMetadata.xml

Import time: 12.05.2022 13:47


Create the IdP Configuration Document


Save & Close Cancel

IdP Configuration

Basics | Client Settings | Certificate Management | **Advanced** | Administration

Advanced

Signing X.509 certificate: 

Encryption X.509 certificate: 

Protocol support enumeration: `urn:oasis:names:tc:SAML:2.0:protocol`

Create the IdP Configuration Document


Save & Close Cancel

IdP Configuration : Mail1Com

Basics | Client Settings | Certificate Management | Advanced | Administration

Basics

Import XML file

Host names or addresses mapped to this site:	<input type="text" value="mail1.wyducks.com; 10.1.0.4"/>
Protocol version:	<input type="text" value="SAML 2.0"/>
State:	<input type="text" value="Enabled"/>
Federation product:	<input type="text" value="AuthnRequest SAML 2.0 compatible"/>
Service provider ID:	<input type="text" value="https://mail1.wyducks.com"/>
Artifact resolution service URL:	<input type="text" value=""/>
Single sign-on service URL:	<input type="text" value="https://ads.wyducks.com/ads/ls/"/>
Encryption method:	<input type="text" value="http://www.w3.org/2001/04/xmlenc#sha256"/>
IdP name (for your reference):	<input type="text" value="Mail1Com"/>
Comment:	<input type="text" value="ads.wyducks.com"/>
Imported file:	 - FederationMetadata - Copy (2).xml
Import time:	28.12.2021 12:18

Create the IdP Configuration Document

Save & Close Cancel

IdP Configuration : Mail1Com

Basics | Client Settings | Certificate Management | Advanced | Administration

Basics

Import XML file

Host names or addresses mapped to this site:	mail1.wyducks.com; 10.1.0.4
Protocol version:	SAML 2.0
State:	Enabled
Federation product:	AuthnRequest SAML 2.0 compatible
Service provider ID:	https://mail1.wyducks.com
Artifact resolution service URL:	
Single sign-on service URL:	https://ads.wyducks.com/ads/ls/
Encryption method:	http://www.w3.org/2001/04/xmlenc#sha256
IdP name (for your reference):	Mail1Com
Comment:	ads.wyducks.com
Imported file:	- FederationMetadata - Copy (2).xml
Import time:	28.12.2021 12:18

Create the IdP Configuration Document

Save & Close Cancel

IdP Configuration : Mail1Com

Basics | Client Settings | Certificate Management | Advanced | Administration

Basics

Import XML file

Host names or addresses mapped to this site:	mail1.wyducks.com; 10.1.0.4
Protocol version:	SAML 2.0
State:	Enabled
Federation product:	AuthnRequest SAML 2.0 compatible
Service provider ID:	https://mail1.wyducks.com
Artifact resolution service URL:	
Single sign-on service URL:	https://ads.wyducks.com/ads/ls/
Encryption method:	http://www.w3.org/2001/04/xmlenc#sha256
IdP name (for your reference):	Mail1Com
Comment:	ads.wyducks.com
Imported file:	- FederationMetadata - Copy (2).xml
Import time:	28.12.2021 12:18

Create the IdP Configuration Document

Save & Close Cancel

IdP Configuration : Mail1Com

Basics | Client Settings | Certificate Management | Advanced | Administration

Basics

Import XML file

Host names or addresses mapped to this site:	mail1.wyducks.com; 10.1.0.4
Protocol version:	SAML 2.0
State:	Enabled
Federation product:	AuthnRequest SAML 2.0 compatible
Service provider ID:	https://mail1.wyducks.com
Artifact resolution service URL:	
Single sign-on service URL:	https://ads.wyducks.com/ads/ls/
Encryption method:	http://www.w3.org/2001/04/xmlenc#sha256
IdP name (for your reference):	Mail1Com
Comment:	ads.wyducks.com
Imported file:	- FederationMetadata - Copy (2).xml
Import time:	28.12.2021 12:18

Create the IdP Configuration Document

Save & Close Cancel

IdP Configuration : Mail1Com

Basics | Client Settings | Certificate Management | Advanced | Administration

Basics

Import XML file

Host names or addresses mapped to this site:	mail1.wyducks.com; 10.1.0.4
Protocol version:	SAML 2.0
State:	Enabled
Federation product:	AuthnRequest SAML 2.0 compatible
Service provider ID:	https://mail1.wyducks.com
Artifact resolution service URL:	
Single sign-on service URL:	https://adfs.wyducks.com/adfs/ls/
Encryption method:	http://www.w3.org/2001/04/xmlenc#sha256
IdP name (for your reference):	Mail1Com
Comment:	adfs.wyducks.com
Imported file:	- FederationMetadata - Copy (2).xml
Import time:	28.12.2021 12:18

HTTPS!!!

Create the IdP Configuration Document

Save & Close Cancel

IdP Configuration : Mail1Com

Basics | Client Settings | Certificate Management | Advanced | Administration

Basics

Import XML file

Host names or addresses mapped to this site:	mail1.wyducks.com; 10.1.0.4
Protocol version:	SAML 2.0
State:	Enabled
Federation product:	AuthnRequest SAML 2.0 compatible
Service provider ID:	https://mail1.wyducks.com
Artifact resolution service URL:	
Single sign-on service URL:	https://adfs.wyducks.com/adfs/ls/
Encryption method:	http://www.w3.org/2001/04/xmlenc#sha256
IdP name (for your reference):	Mail1Com
Comment:	adfs.wyducks.com
Imported file:	- FederationMetadata - Copy (2).xml
Import time:	28.12.2021 12:18

Create the IdP Configuration Document

Save & Close Cancel

IdP Configuration : Mail1Com

Basics | Client Settings | Certificate Management | Advanced | Administration

Basics

Import XML file

Host names or addresses mapped to this site:	<input type="text" value="mail1.wyducks.com; 10.1.0.4"/>
Protocol version:	<input type="text" value="SAML 2.0"/>
State:	<input type="text" value="Enabled"/>
Federation product:	<input type="text" value="AuthnRequest SAML 2.0 compatible"/>
Service provider ID:	<input type="text" value="https://mail1.wyducks.com"/>
Artifact resolution service URL:	<input type="text" value=""/>
Single sign-on service URL:	<input type="text" value="https://ads.wyducks.com/ads/ls/"/>
Encryption method:	<input type="text" value="http://www.w3.org/2001/04/xmlenc#sha256"/>
IdP name (for your reference):	<input type="text" value="Mail1Com"/>
Comment:	<input type="text" value="ads.wyducks.com"/>
Imported file:	<input type="text" value="- FederationMetadata - Copy (2).xml"/>
Import time:	<input type="text" value="28.12.2021 12:18"/>

Encrypting Domino SAML Assertions

Optional, but highly recommended



Encrypting Domino SAML Assertions

Certificate for encryption



Encrypting Domino SAML Assertions

Saved to server.id file

Switch between servers

TAKE CARE

Encrypting Domino SAML Assertions

For Basic SAML

Domino mail/web server



TAKE CARE

Encrypting Domino SAML Assertions

One more thing!

The company name must be unique!

Encrypting Domino SAML Assertions

 Edit IdP Config  Cancel

IdP Configuration : Mail1Com

Basics | Client Settings | **Certificate Management** | Advanced | Administration |

Certificate Management Settings

Company name:

Certificate public hash value
(base 64):

Exported certificate:

Encrypting Domino SAML Assertions

Save & Close Cancel

IdP Configuration : Mail1Com

Basics | Client Settings | Certificate Management | **Advanced** | Administration

Certificate Management Settings

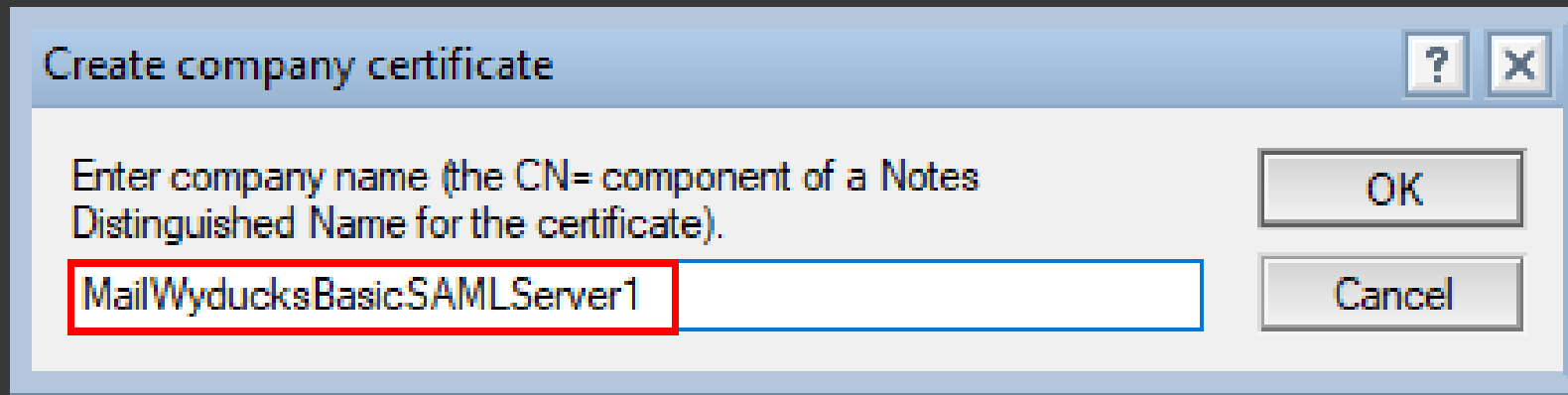
Create SP Certificate

Company name:

Certificate public hash value (base 64):

Exported certificate:

Encrypting Domino SAML Assertions



Create company certificate

Enter company name (the CN= component of a Notes Distinguished Name for the certificate).

MailWyducksBasicSAMLServer1

OK

Cancel

Encrypting Domino SAML Assertions

Save & Close Cancel

IdP Configuration

Basics | Client Settings | Certificate Management | Advanced | Administration

Certificate Management Settings

Examine SP Certificate Export SP XML

Company name: CN=MAIL1WyDucksWebBasicSAMLServer1

Domino URL:

Single logout URL:

Certificate public hash value (base 64):

Exported certificate:

Encrypting Domino SAML Assertions

Save & Close Cancel

IdP Configuration

Basics | Client Settings | Certificate Management | Advanced | Administration

Certificate Management Settings

Examine SP Certificate Export SP XML

Company name: CN=MAIL1WyDucksWebBasicSAMLServer1

Domino URL: https://mail1.wyducks.com

Single logout URL: https://adfs.wyducks.com/adfs/ls/

Certificate public hash value (base 64): iAwqgIMClrsVAGq7mdYXxQ==

Exported certificate:

Encrypting Domino SAML Assertions

Save & Close Cancel

IdP Configuration

Basics | Client Settings | Certificate Management | Advanced | Administration

Certificate Management Settings


Examine SP Certificate Export SP XML

Company name: CN=MAIL1WyDucksWebBasicSAMLServer1

Domino URL:

Single logout URL:

Certificate public hash value (base 64):

Exported certificate:  - ServiceProvider.xml

Enable SAML Authentication in Domino

Internet Site documents



Enable SAML Authentication in Domino

The screenshot shows the HCL Domino Administrator interface for the 'WYDUCKS Domain - DominoADM01/WYDucks'. The left-hand navigation pane is expanded to 'Web' > 'Internet Sites'. The main pane displays a list of Internet Sites under the 'WYDucks' server. The entry 'Web Site: Verse on-Premises Mail1 (mail.wyducks.com; mail1.wyducks.com; 10.1.0.4)' is highlighted with a red rectangular box. Other visible entries include 'LDAP Site: LDAP Site (mail1.wyducks.com; mail2.wyducks.com; 10.1.0.4; 10.1.0.5)', 'Web Site: Auto Generated Internet Site Document for Web Protocol (traveler.wyducks.com; traveler1.wyducks.com)', and 'Web Site: Verse on-Premises Mail2 (mail.wyducks.com; mail2.wyducks.com; 10.1.0.5)'. The 'Web SSO Configuration: LtpaToken' entry is also visible below the list.

Enable SAML Authentication in Domino

Web Site... Save & Close Cancel

Web Site Verse on-Premises Mail1

Basics | Configuration | Domino Web Engine | Security | Comments | Administration

HTTP Sessions

Session authentication: SAML

Web SSO Configuration: LtpaToken

Force login on TLS: Yes

SAML single server session expiration: 120 minutes

When overriding session authentication, generate session cookie: Yes

Restart

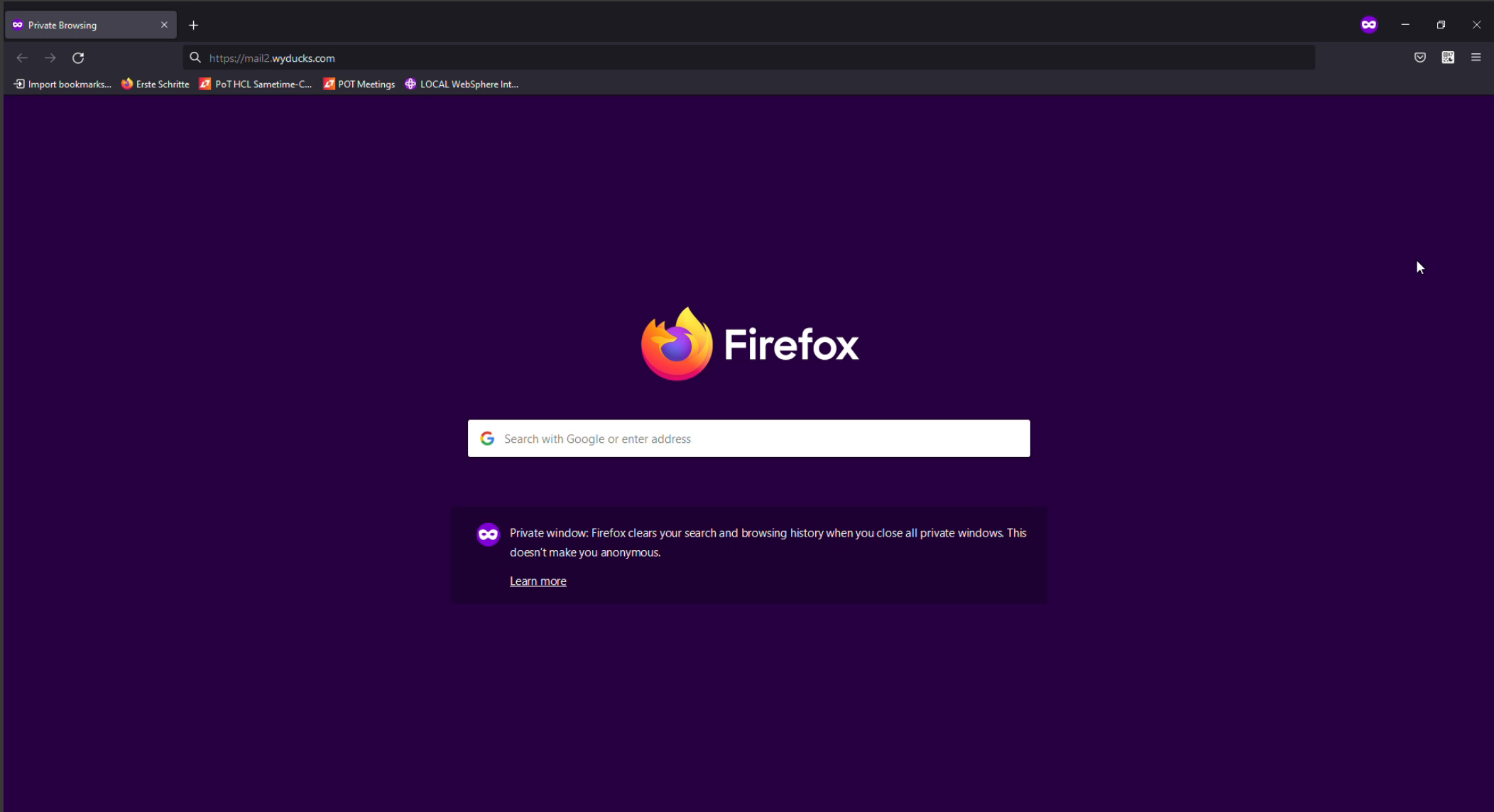
A photograph of a dog jumping in a grassy field to catch a yellow frisbee. The dog is in mid-air, with its mouth open and teeth visible, reaching for the frisbee. The background is a blurred green field with some trees and a building in the distance.

Domino Server

HTTP Task

Demo

Demo



What just happened!?

External access no SSO
PW for secure mail operations



Infrastructure Needed

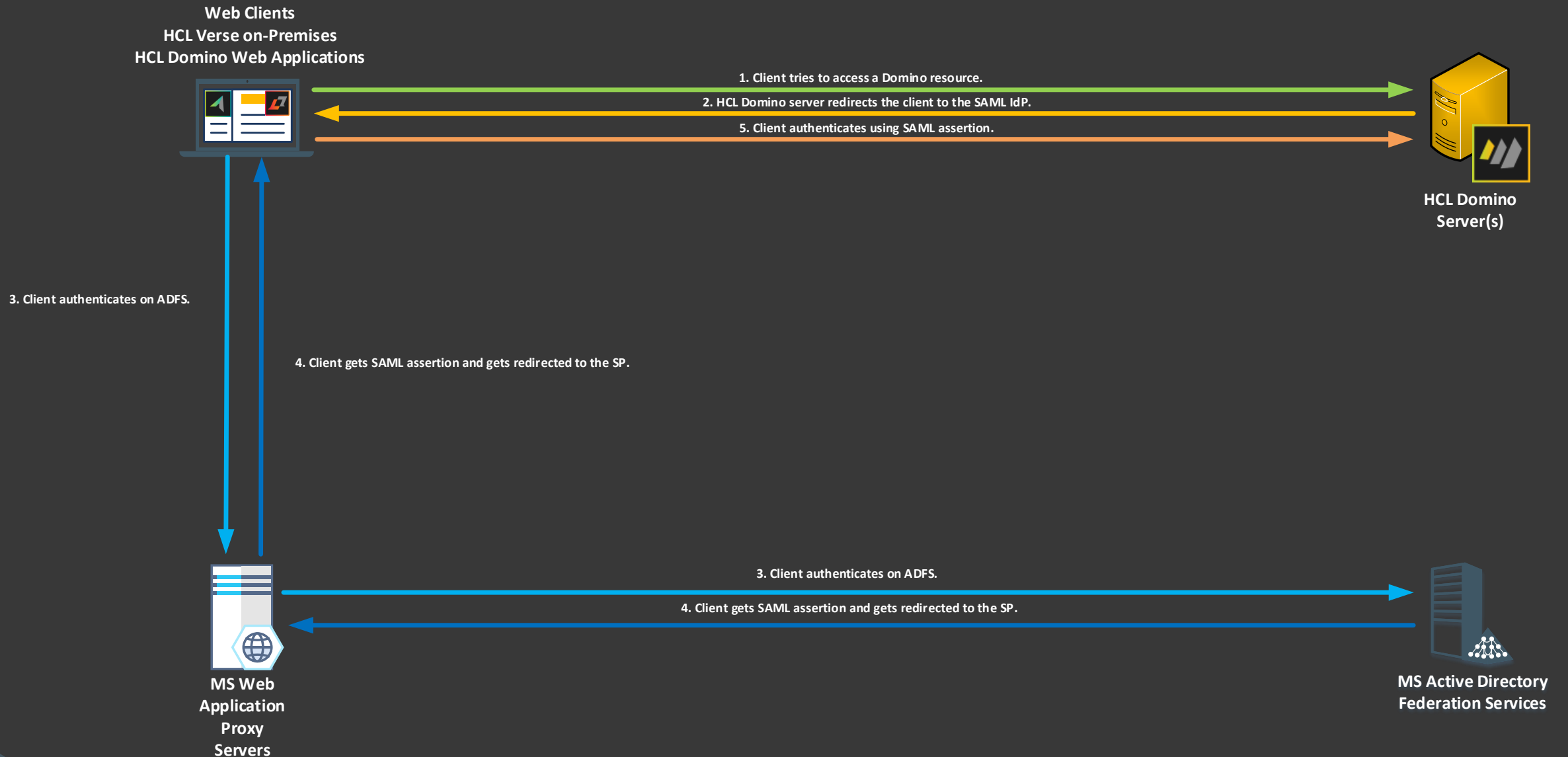


Table of Contents

Motivation

HCL Domino & SAML

Web Federated Login

Issues

Why SAML?

Prerequisites

Notes Federated Login

Q & A

SAML

Infrastructure Needed

Traveler & SAML

Shibboleth

Wording

Basic SAML Setup

Bonus – Nomad!

References

How does it work?

SAML & SSO

Troubleshooting

IdP offers SSO mechanism

IWA on ADFS



Needed Domino setting



Required Setting for IWA & SAML

The screenshot displays the HCL Domino Administrator interface for the 'WYDUCKS Domain - DominoADM01/WYDucks'. The left-hand navigation pane shows a tree view with categories like Server, Messaging, Replication, Directory, Security, Policies, and Web. Under the 'Web' category, 'Internet Sites' is selected. The right-hand pane shows a list of configurations for the 'WYDucks' site, including LDAP Site, Auto Generated Internet Site Document, and two 'Web Site: Verse on-Premises Mail' entries. The 'Web SSO Configuration: LtpaToken' entry is highlighted with a red box. The top of the interface includes a menu bar (File, Edit, View, Create, Actions, Administration, Configuration, Help) and a toolbar with various icons.

Site name
WYDucks
LDAP Site: LDAP Site (mail1.wyducks.com; mail2.wyducks.com; 10.1.0.4; 10.1.0.5)
Web Site: Auto Generated Internet Site Document for Web Protocol (traveler.wyducks.com; traveler1.wyducks.com)
Rule (substitution): /Microsoft-Server-ActiveSync* --> /traveler/Microsoft-Server-ActiveSync*
Rule (substitution): /servlet/traveler* --> /traveler*
Web Site: Verse on-Premises Mail1 (mail.wyducks.com; mail1.wyducks.com; 10.1.0.4)
Web Site: Verse on-Premises Mail2 (mail.wyducks.com; mail2.wyducks.com; 10.1.0.5)
Web SSO Configuration: LtpaToken

Required Setting for IWA & SAML

Edit SSO Configuration Cancel

Web SSO Configuration for : LtpaToken

Basics | Comments | Administration

Token Configuration

Configuration Name:	LtpaToken
Organization:	WYDucks
DNS Domain:	.wyducks.com
Map names in Ltpa tokens:	Disabled
Require TLS protected communication (HTTPS):	Disabled
Restrict use of the SSO token to HTTP/HTTPS:	Disabled
SameSite cookie attribute:	Use browser default or INI setting

Participating Servers

Domino Server Names:	DominoADM01/WYDucks, DominoADM02/WYDucks, DominoTrav01/WYDucks
Windows single sign-on integration (if available):	Disabled

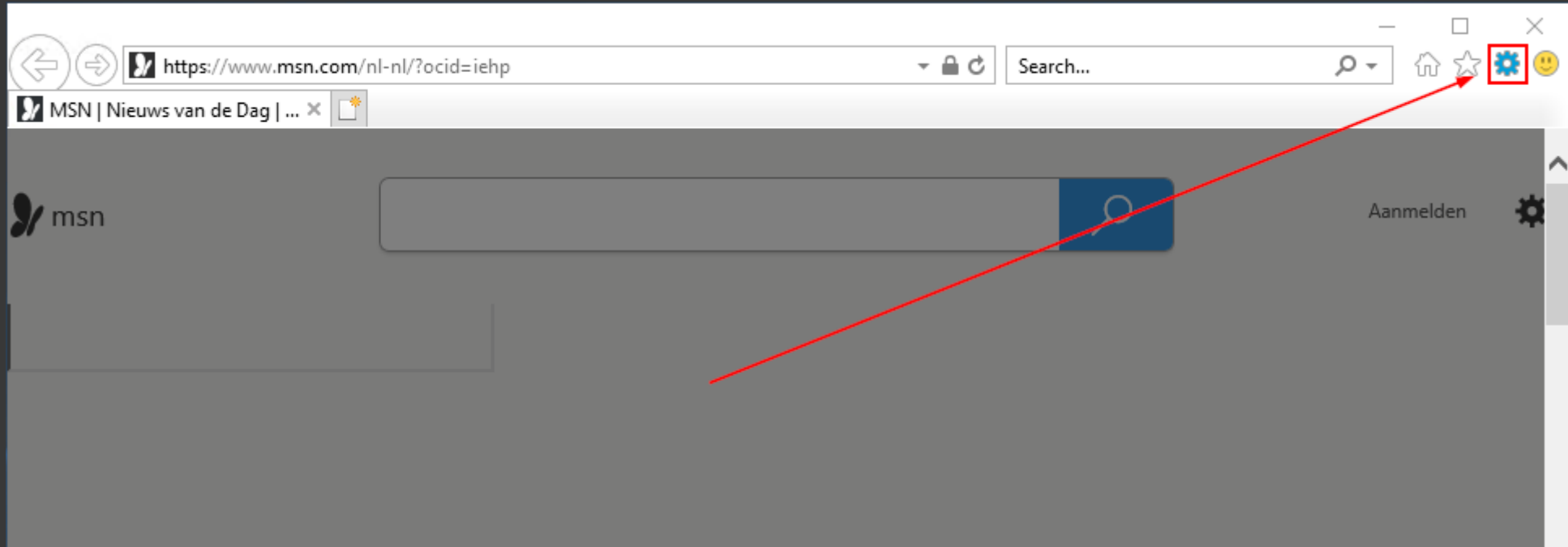
Enable IWA on IdP / ADFS



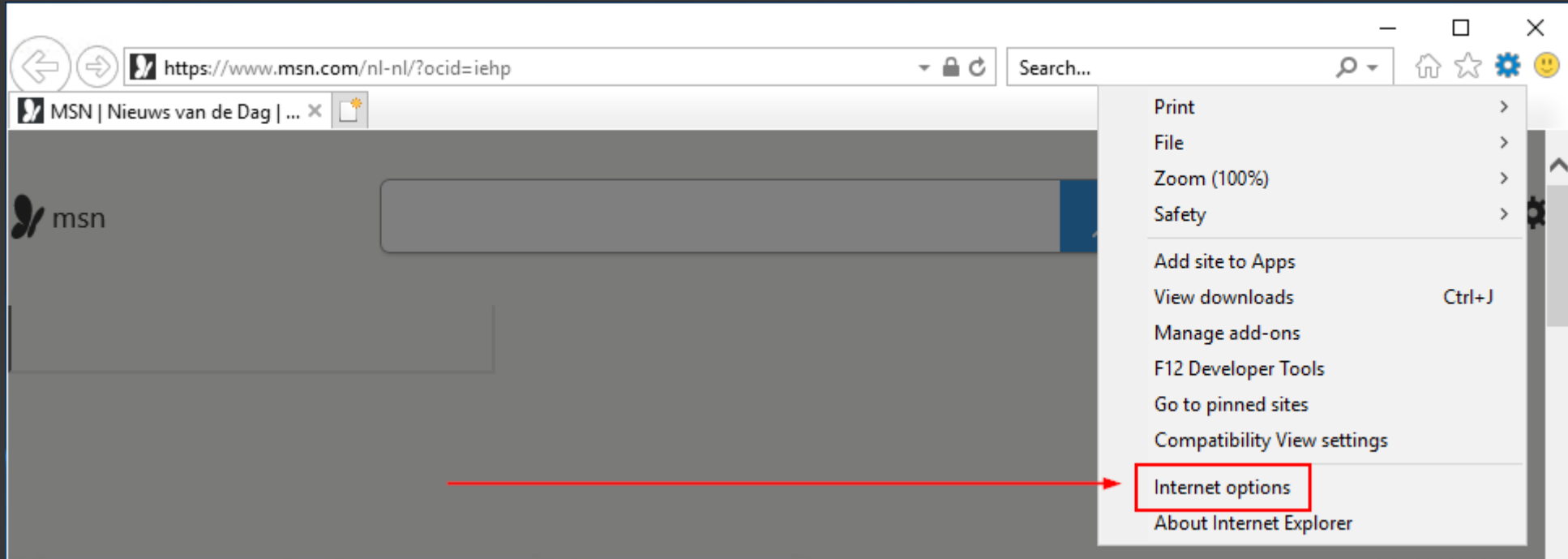
Browser configuration



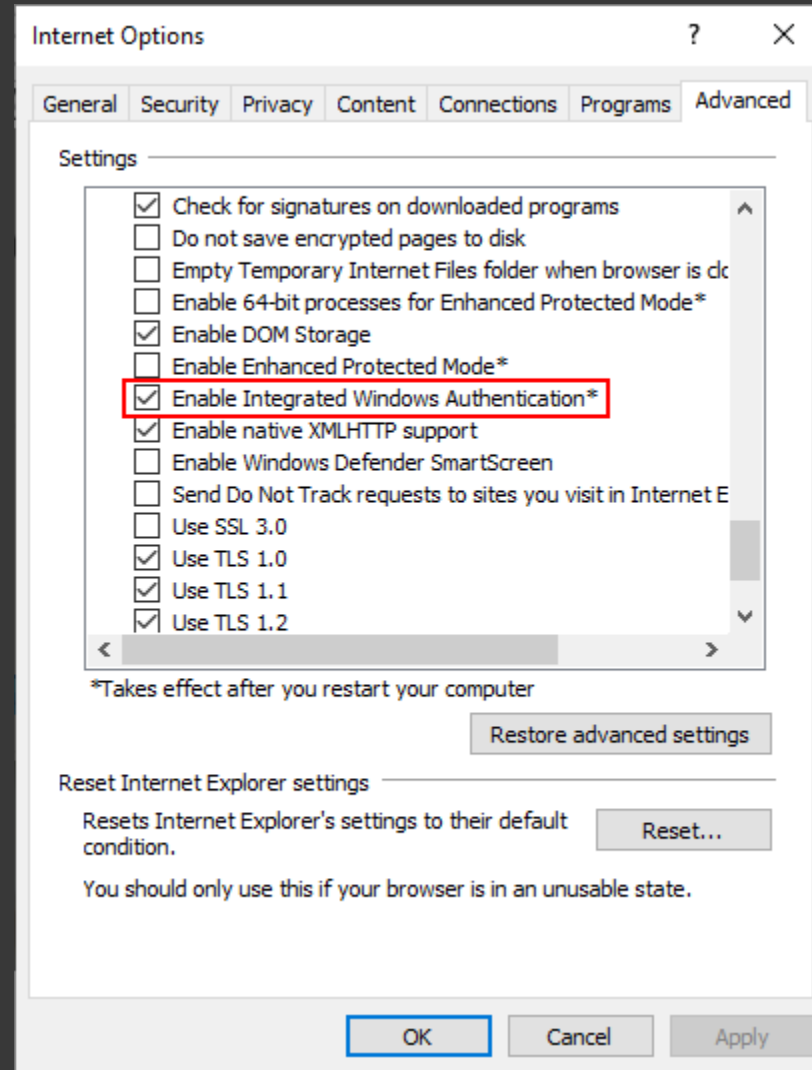
Browser Configuration



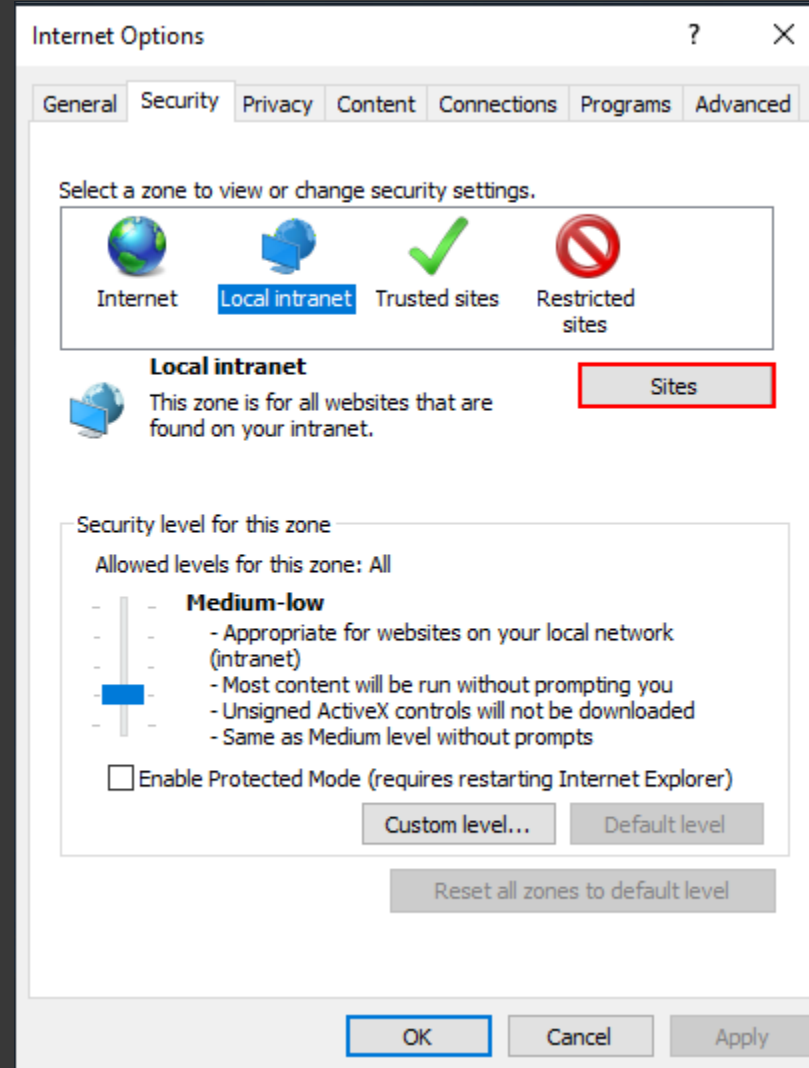
Browser Configuration



Browser Configuration




Browser Configuration



Browser Configuration

Local intranet ✕

 Use the settings below to define which websites are included in the local intranet zone.

Automatically detect intranet network

Include all local (intranet) sites not listed in other zones


Include all sites that bypass the proxy server

Include all network paths (UNCs)

[What are intranet settings?](#)

Browser Configuration

Local intranet ✕

 Use the settings below to define which websites are included in the local intranet zone.

Automatically detect intranet network

Include all local (intranet) sites not listed in other zones


Include all sites that bypass the proxy server

Include all network paths (UNCs)

[What are intranet settings?](#)

Browser Configuration

Local intranet ✕

 You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

Add

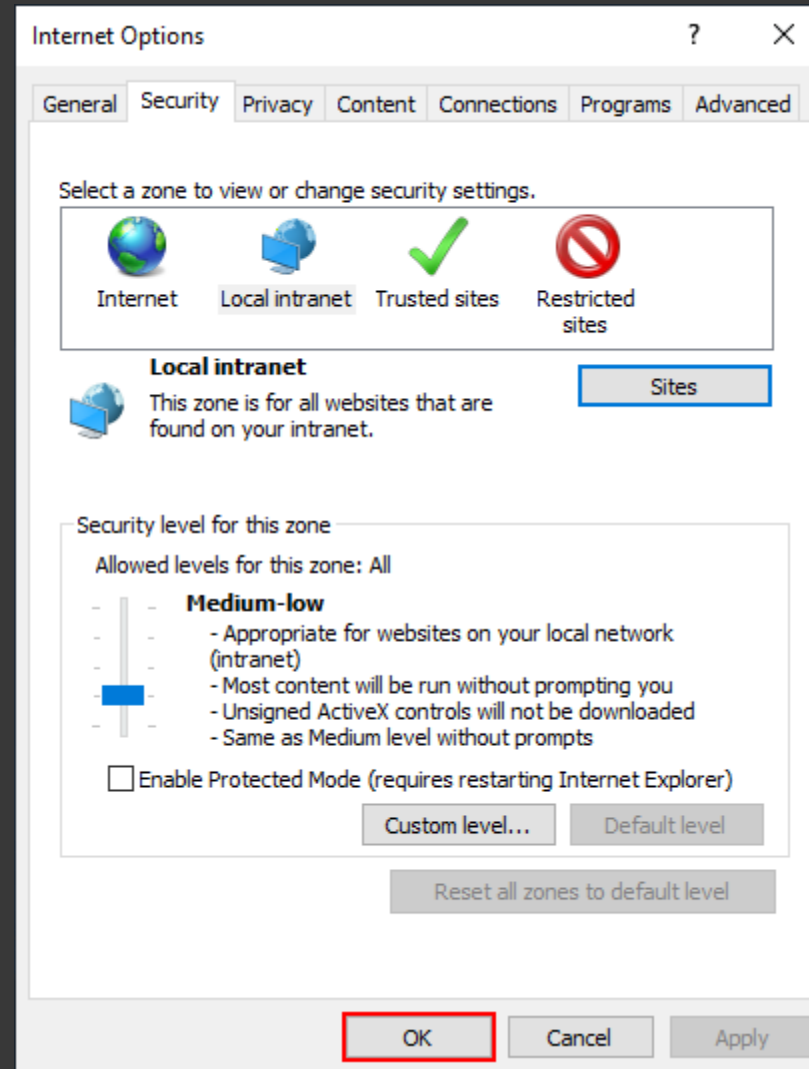
Websites:

Remove

Require server verification (https:) for all sites in this zone

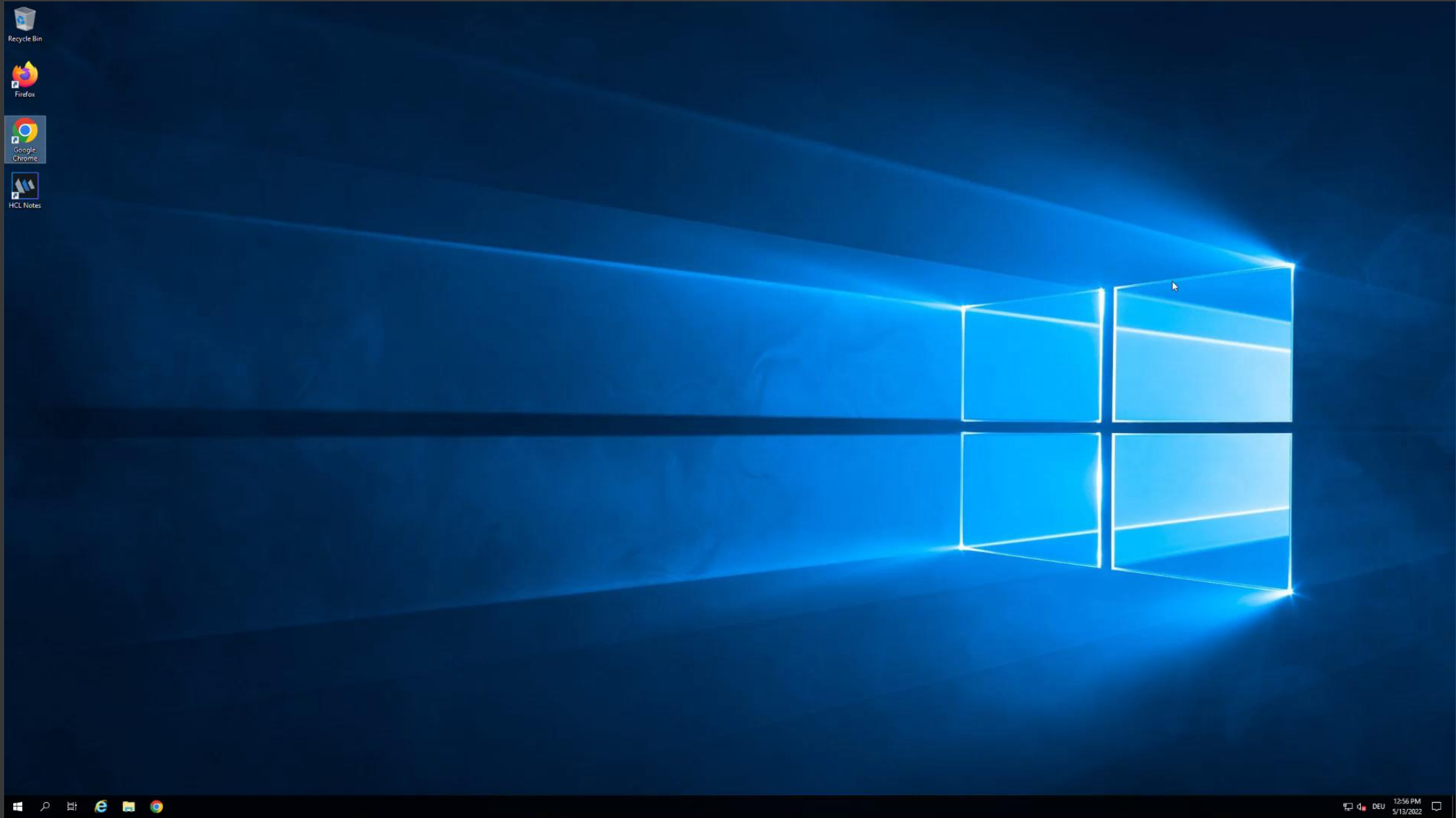
Close

Browser Configuration



Demo

Demo



What just happened!?

IdP accepts IWA

From all internal HTTPS connections



Infrastructure Needed

Web Clients
HCL Verse on-Premises
HCL Domino Web Applications



HCL Domino Server(s)

3. Client authenticates on ADFS.

4. Client gets SAML assertion and gets redirected to the SP.

1. Client tries to access a Domino resource.

2. HCL Domino server redirects the client to the SAML IdP.

5. Client authenticates using SAML assertion.

MS Active Directory
Federation Services

Table of Contents

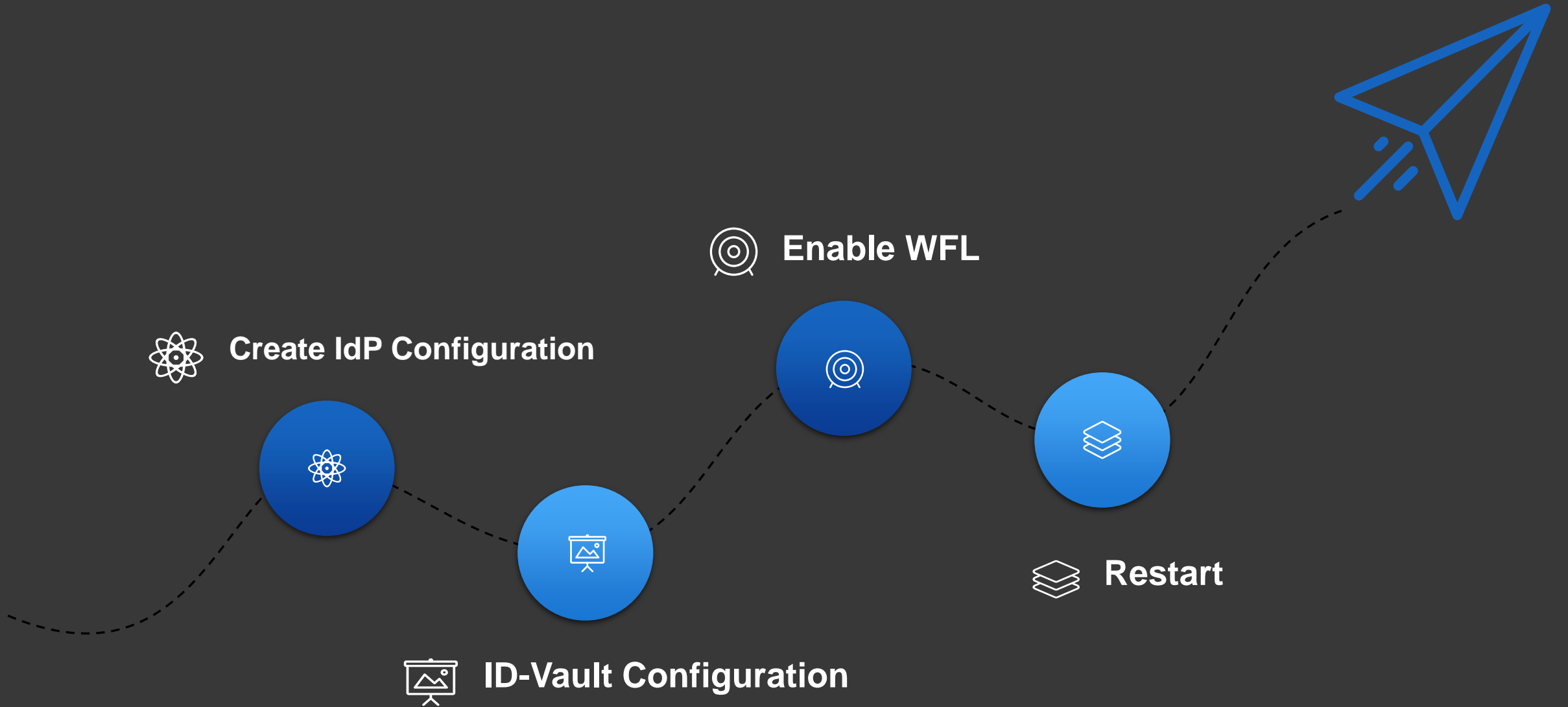
Motivation	HCL Domino & SAML	Web Federated Login	Issues
Why SAML?	Prerequisites	Notes Federated Login	Q & A
SAML	Infrastructure Needed	Traveler & SAML	Shibboleth
Wording	Basic SAML Setup	Bonus – Nomad!	References
How does it work?	SAML & SSO	Troubleshooting	

Web Federated Login

What do we want to achieve?

How?

Web Federated Login



Create the IdP Configuration Document

Inside of "idpcat.nsf"





Create the IdP Configuration Document

The screenshot shows the HCL Domino Administrator interface for the IdP Catalog. The title bar reads "IdP Catalog - IdP Configurations - HCL Domino Administrator". The menu bar includes "File", "Edit", "View", "Create", "Actions", and "Help". A toolbar contains various icons for navigation and actions. The main window has two tabs: "WYDUCKS Domain - DominoAD..." and "IdP Catalog - IdP Configurations". The left sidebar shows a tree view with "IdP Catalog" and "IdP Configurations". The right pane features a toolbar with three buttons: "Add IdP Config" (highlighted with a red box), "Edit IdP Config", and "Delete IdP Config". Below the toolbar is a table with the following data:

Hostname	Type	State	Name
mail1.wyducks.com	SAML 2.0	Enabled	Mail1Com


Create the IdP Configuration Document

 Edit IdP Config  Cancel



IdP Configuration : Mail1ComVault

Basics | Client Settings | Certificate Management | Advanced | Administration

Basics

Host names or addresses mapped to this site:	vault.mail1.wyducks.com
Protocol version:	SAML 2.0
State:	Enabled
Federation product:	AuthnRequest SAML 2.0 compatible
Service provider ID:	https://vault.mail1.wyducks.com
Artifact resolution service URL:	
Single sign-on service URL:	https://ads.wyducks.com/ads/ls/
Encryption method:	http://www.w3.org/2001/04/xmlenc#sha256
IdP name (for your reference):	Mail1ComVault
Comment:	
Imported file:	 - FederationMetadata - Copy (4).xml
Import time:	28.12.2021 12:28


Encrypting Domino SAML Assertions

 Edit IdP Config  Cancel

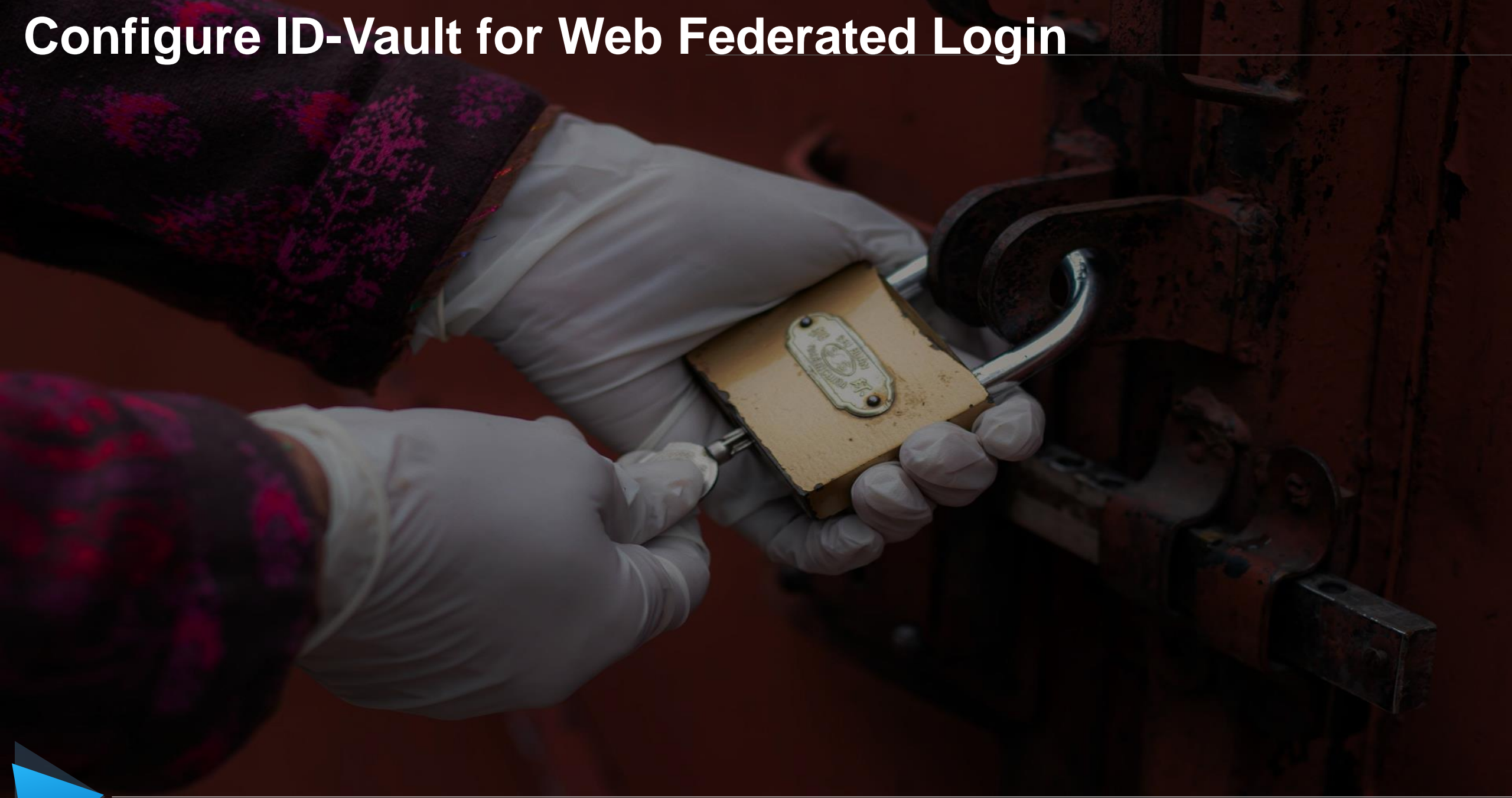
IdP Configuration : Mail1ComVault

Basics | Client Settings | **Certificate Management** | Advanced | Administration

Certificate Management Settings

Company name:	CN=Mail1ComVaultCert
Domino URL:	https://mail1.wyducks.com
Single logout URL:	https://ads.wyducks.com/ads/ls/
Certificate public hash value (base 64):	Eump8h+Z5c+lCtkFfv3lg==
Exported certificate:	 - ServiceProvider.xml

Configure ID-Vault for Web Federated Login



Configure ID-Vault for Web Federated Login

WYDUCKS Domain - DominoADM01/WYDucks - HCL Domino Administrator

File Edit Administration Files Help

WYDUCKS Domain - DominoAD... IdP Catalog - IdP Configurations X

People & Groups Files Server... Messaging... Replication Configuration

Server: **DominoADM01/WYDucks**
Release 12.0.1FP1 on Windows/2019 10.0

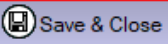
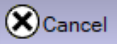
	Title	Filename	Physical Path	File Format
	WYDucks ID-Vault	wyducks_id-val	C:\Program Files\HCL	R12 (55:0)


C:\Program Files\HCL\Domino\

- aut
- backup
- etc
- gtrhome
- help
- icl
- iNotes
- IBM_CredStore
- IBM_ID_VAULT**
- logdir
- mail
- panagenda
- Properties
- meval
- W32
- xmlschemas

Catalog (12)
Cluster Directory (10)

Configure ID-Vault for Web Federated Login

 Save & Close  Cancel

 Vault Name: **WYDucks_ID-Vault**

IdP authenticated vault login

Notes federated login approved IdP configurations:	
Web federated login approved IdP configurations:	<input type="text" value="vault.mail1.wyducks.com"/>
Nomad federated login approved IdP configurations:	

Enable Web Federated Login

How can we do that?
With a Domino Policy!

Enable Web Federated Login

Save & Close Cancel Inheritance Enforcement How To Apply

Security Settings : NFL Test

Basics | Password Management | Execution Control List | Keys and Certificates | Signed Plug-ins | Portal Server | **ID Vault** | Proxies | Comments | Administration

ID Vault Options:		How to apply this setting:	Inherit from parent policy:	Enforce in child policies:
Assigned vault:	<input type="text" value="/WYDucks_ID-Vault"/>	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Forgotten password help text:	<input type="text" value="Panic and Despair!"/>	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Enforce password change after password has been reset:	<input type="text" value="Yes"/>	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Allow Notes-based programs to use the Notes ID Vault:	<input type="text" value="Yes"/>	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Prohibit Biometric Authentication sync:	<input type="text" value="No"/>	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

Automatic ID Downloads:		How to apply this setting:	Inherit from parent policy:	Enforce in child policies:
Allow automatic ID downloads:	<input type="text" value="Yes"/>	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Allow trusted server ID downloads:	<input type="text" value="No"/>	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Allow ID downloads for:	<input type="text" value="1 days"/> <input type="text" value="0 hours"/>	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
ID download authorization failure message:	<input type="text"/>			

TOTP-based ID Downloads:		How to apply this setting:	Inherit from parent policy:	Enforce in child policies:
Allow TOTP authentication with the ID vault:	<input type="text" value="No"/>	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Allow password authentication with the ID vault:	<input type="text" value="Yes"/>	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

Enable Web Federated Login

Save & Close Cancel Inheritance Enforcement How To Apply

Security Settings : NFL Test

Basics Password Management Execution Control List Keys and Certificates Signed Plug-ins Portal Server ID Vault Proxies Comments Administration

Password Management Basics Notes Shared Login Federated Login

Notes Federated Login	How to apply this setting:	Inherit from parent policy:	Enforce in child policies:
Enable Notes Federated login with SAML IdP: <input type="text" value="No"/> <input type="button" value="Enter machine specific formula"/>	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

Activation Notification	How to apply this setting:
How to notify users when enabled: <input type="text" value="Custom message dialog"/>	<input type="checkbox"/> Don't set value
Custom message text: <input type="text"/>	

Deactivation Notification	How to apply this setting:
How to notify users when disabled: <input type="text" value="Custom message dialog"/>	<input type="checkbox"/> Don't set value
Custom message text: <input type="text"/>	

Web Federated Login	How to apply this setting:
Enable Web Federated login with SAML IdP: <input type="text" value="Yes"/>	<input type="checkbox"/> Don't set value

Nomad Federated Login	How to apply this setting:
Enable Nomad Federated login with SAML IdP: <input type="text" value="Yes"/>	<input type="checkbox"/> Don't set value

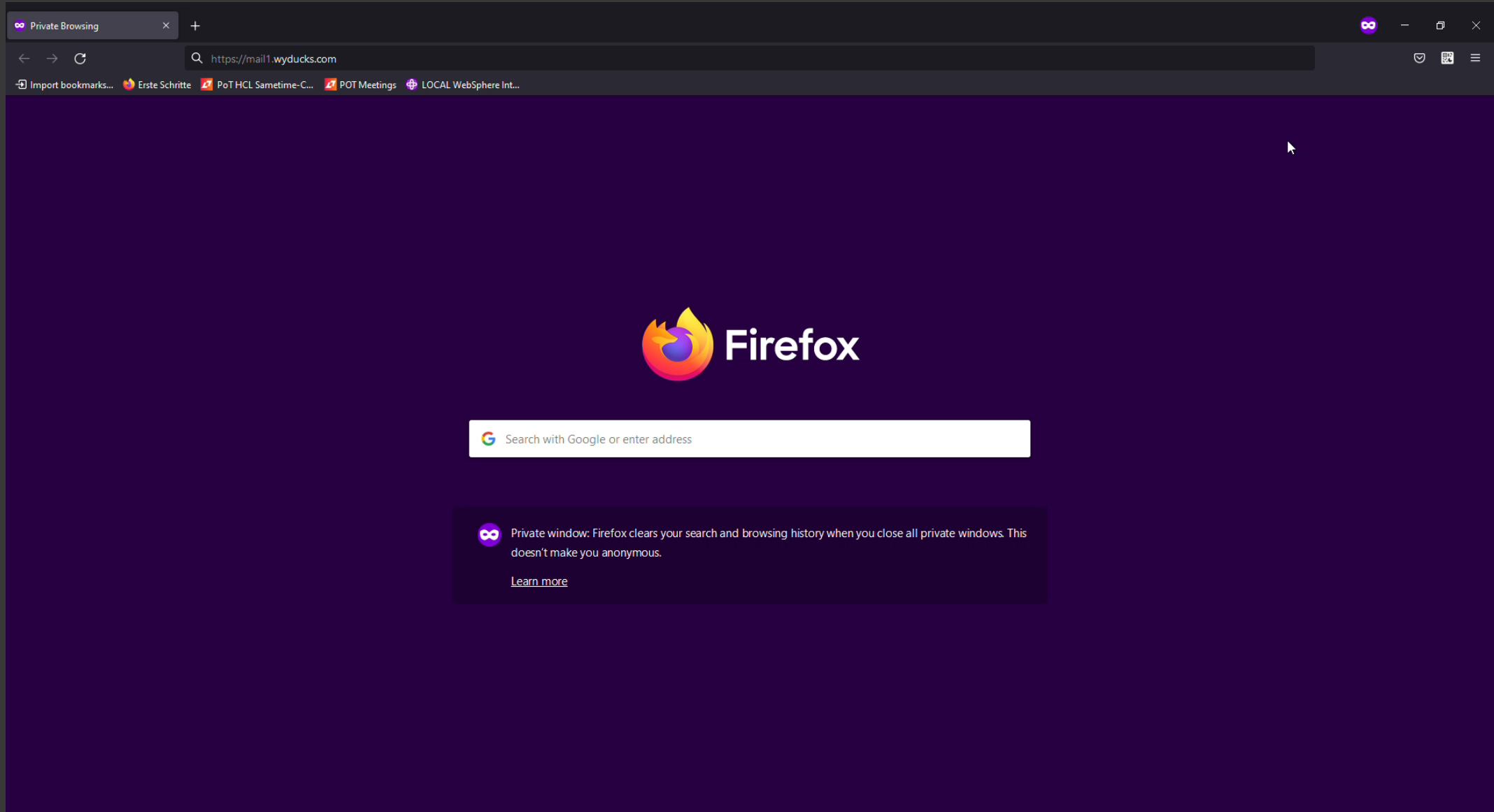
Additional settings for Federated Login	How to apply this setting:
Allow password authentication with the ID vault: <input type="text" value="Yes"/>	<input type="checkbox"/> Don't set value

Enable Web Federated Login

Deactivation Notification	
How to notify users when disabled:	
Custom message text:	
Web Federated Login	
Enable Web Federated login with SAML IdP:	<input type="text" value="Yes"/>
Nomad Federated Login	
Enable Nomad Federated login with SAML IdP:	<input type="text" value="Yes"/>
Additional settings for Federated Login	
Allow password authentication with the ID vault:	<input type="text" value="Yes"/>

Demo

Demo



What Just Happened!?

Secure Mail Operations
Without entering the ID-Password



Table of Contents

Motivation

HCL Domino & SAML

Web Federated Login

Issues

Why SAML?

Prerequisites

[Notes Federated Login](#)

Q & A

SAML

Infrastructure Needed

Traveler & SAML

Shibboleth

Wording

Basic SAML Setup

Bonus – Nomad!

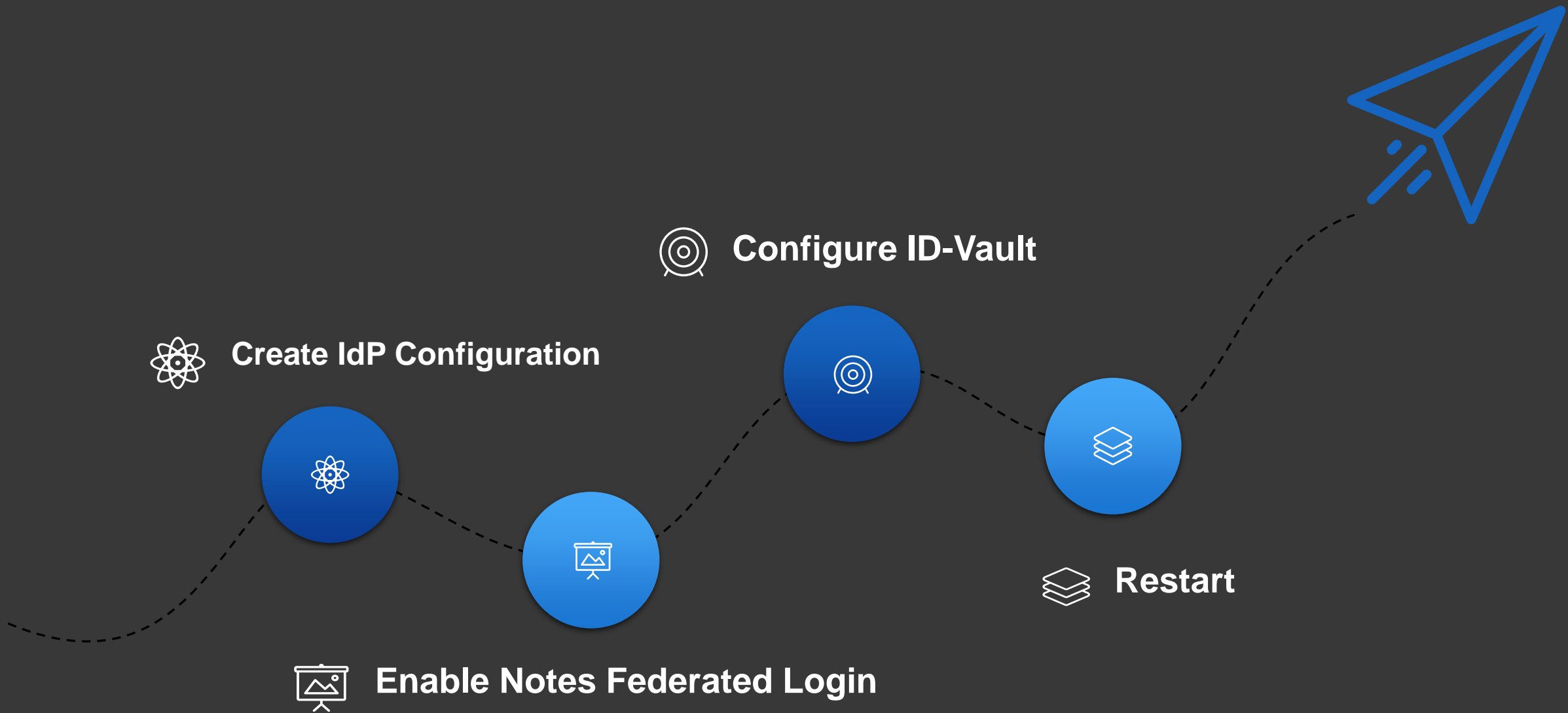
References

How does it work?

SAML & SSO

Troubleshooting

Notes Federated Login



Create the IdP Configuration Document

Inside of "idpcat.nsf"



Create the IdP Configuration Document

Server: **DominoADM01/WYDucks** DominoADM01.wyducks.azure

Basics | Security | Ports... | Server Tasks... | Internet Protocols... | Miscellaneous | Transactional Logging

Basics

Server name:	DominoADM01/WYDucks
Server title:	Domino Admin Server
Domain name:	WYDucks
Fully qualified Internet host name:	DominoADM01.wyducks.azure
Cluster name:	WYDCluster
Load Internet configurations from Server/Internet Sites documents:	Enabled
Maximum formula execution time:	120 seconds

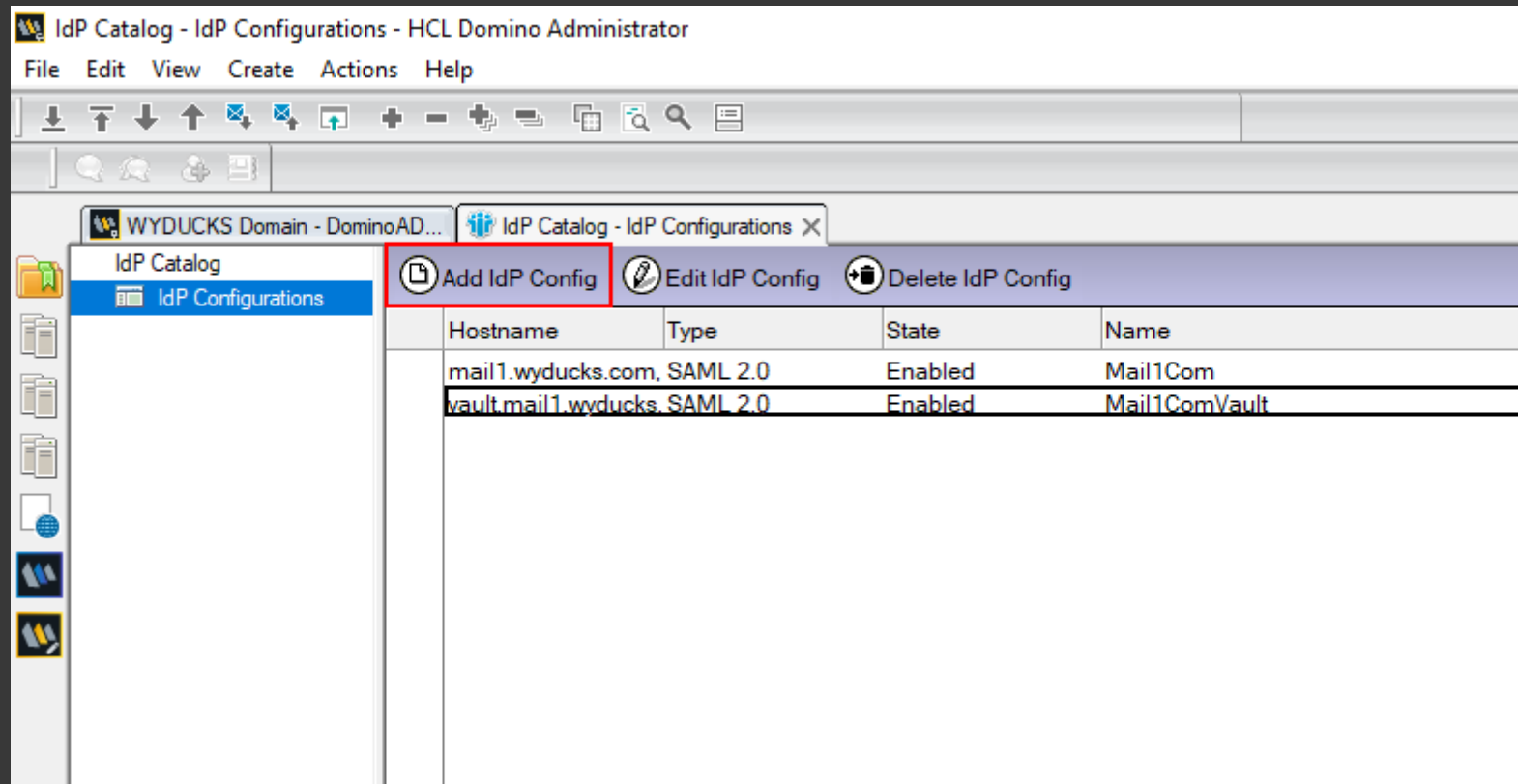
Web Site Verse on-Premises Mail1

Basics | Configuration | Domino Web Engine | Security | Comments | Administration

Site Information

Descriptive name for this site:	Verse on-Premises Mail1
Organization:	WYDucks
Use this web site to handle requests which cannot be mapped to any other web sites:	<input type="radio"/> Yes <input checked="" type="radio"/> No Note: only one web site should have this option set to Yes
Host names or addresses mapped to this site:	mail.wyducks.com mail1.wyducks.com 10.1.0.4
Domino servers that host this site:	DominoADM01/WYDucks

Create the IdP Configuration Document



The screenshot displays the HCL Domino Administrator interface for the 'WYDUCKS Domain - DominoAD...'. The main window is titled 'IdP Catalog - IdP Configurations'. The left sidebar shows the 'IdP Catalog' tree with 'IdP Configurations' selected. The top menu bar includes 'File', 'Edit', 'View', 'Create', 'Actions', and 'Help'. Below the menu bar is a toolbar with various icons. The main content area features a table with the following data:

Hostname	Type	State	Name
mail1.wyducks.com	SAML 2.0	Enabled	Mail1Com
vault.mail1.wyducks.com	SAML 2.0	Enabled	Mail1ComVault


Create the IdP Configuration Document

IdP Configuration : DominoADM01NFL

Basics | Client Settings | Certificate Management | Advanced | Administration

Basics

Import XML file

Host names or addresses mapped to this site:	vault.DominoADM01.wyducks.azure
Protocol version:	SAML 2.0
State:	Enabled
Federation product:	AuthnRequest SAML 2.0 compatible
Service provider ID:	https://vault.DominoADM01.wyducks.azure
Artifact resolution service URL:	
Single sign-on service URL:	https://adfs.wyducks.com/adfs/ls/
Encryption method:	http://www.w3.org/2001/04/xmlenc#sha256
IdP name (for your reference):	DominoADM01NFL
Comment:	
Imported file:	 - FederationMetadata - Copy (3).xml
Import time:	28.12.2021 12:22

Encrypting Domino SAML Assertions

Edit IdP Config Cancel

IdP Configuration : DominoADM01NFL

Basics | Client Settings | Certificate Management | Advanced | Administration

Certificate Management Settings


Examine SP Certificate Export SP XML

Company name: CN=DominoADM01NFLCert



Domino URL: <https://DominoADM01.wyducks.azure>

Single logout URL: <https://adfs.wyducks.com/adfs/ls/>

Certificate public hash value (base 64): OpUTrsyewFP0B82kxMzu9Q==

Exported certificate:  - ServiceProvider.xml

Encrypting Domino SAML Assertions

 Edit IdP Config  Cancel

IdP Configuration : DominoADM01NFL

Basics **Client Settings** Certificate Management | Advanced | Administration |

Notes Client Settings

Enable Windows single sign-on:	<input checked="" type="checkbox"/> Yes
Sites that are trusted:	
Enforce TLS:	Yes

Enable Notes Federated Login

How can we do that?
Again, with a Domino Policy!

Enable Notes Federated Login

Save & Close Cancel Inheritance Enforcement How To Apply

Security Settings : NFL Test

Basics | Password Management | Execution Control List | Keys and Certificates | Signed Plug-ins | Portal Server | **ID Vault** | Proxies | Comments | Administration

ID Vault Options:		How to apply this setting:	Inherit from parent policy:	Enforce in child policies:
Assigned vault:	<input type="text" value="/WYDucks_ID-Vault"/>	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Forgotten password help text:	<input type="text" value="Panic and Despair!"/>	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Enforce password change after password has been reset:	<input type="text" value="Yes"/>	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Allow Notes-based programs to use the Notes ID Vault:	<input type="text" value="Yes"/>	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Prohibit Biometric Authentication sync:	<input type="text" value="No"/>	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

Automatic ID Downloads:		How to apply this setting:	Inherit from parent policy:	Enforce in child policies:
Allow automatic ID downloads:	<input type="text" value="Yes"/>	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Allow trusted server ID downloads:	<input type="text" value="No"/>	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Allow ID downloads for:	<input type="text" value="1 days"/> <input type="text" value="0 hours"/>	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
ID download authorization failure message:	<input type="text"/>			

TOTP-based ID Downloads:		How to apply this setting:	Inherit from parent policy:	Enforce in child policies:
Allow TOTP authentication with the ID vault:	<input type="text" value="No"/>	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Allow password authentication with the ID vault:	<input type="text" value="Yes"/>	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

Enable Notes Federated Login

Security Settings : NFL Test

Basics | **Password Management** | Execution Control List | Keys and Certificates | Signed Plug-ins | Portal Server | ID Vault | Proxies | Comments | Administration

Password Management Basics | Notes Shared Login | **Federated Login**

Notes Federated Login How to apply this setting: Don't set value Inherit from parent policy: Inherit Enforce in child policies: Enforce

Enable Notes Federated login with SAML IdP:

Activation Notification How to apply this setting: Don't set value

How to notify users when enabled:

Custom message text:

Deactivation Notification How to apply this setting: Don't set value

How to notify users when disabled:

Custom message text:

Web Federated Login How to apply this setting: Don't set value

Enable Web Federated login with SAML IdP:

Nomad Federated Login How to apply this setting: Don't set value

Enable Nomad Federated login with SAML IdP:

Additional settings for Federated Login How to apply this setting: Don't set value

Allow password authentication with the ID vault:

Enable NFL – IdP Certificates Rollout

Security Settings : NFL Test

Basics | Password Management | Execution Control List | **Keys and Certificates** | Signed Plug-ins | Portal Server | ID Vault | Proxies | Comments | Administration

Default Public Key Requirements

Don't set value Inherit Public Key Requirement Settings from Parent Enforce Public Key Requirement Settings in Children

User Public Key Requirements How to apply this setting:

Minimum allowable key strength:	No Minimum	<input type="checkbox"/> Don't set value
Maximum allowable key strength:	Compatible with Release 7 and later (2048 bits)	<input type="checkbox"/> Don't set value
Preferred key strength:	Compatible with Release 7 and later (2048 bits)	<input type="checkbox"/> Don't set value
Maximum allowable age for key:	36500 days	<input type="checkbox"/> Don't set value
Earliest allowable key creation date:	01.08.1977	<input type="checkbox"/> Don't set value
Spread new key generation for all users over this many days:	180 days	<input type="checkbox"/> Don't set value
Maximum number of days the old key should remain valid after the new key has been created:	365 days	<input type="checkbox"/> Don't set value

Document/Mail Encryption Settings How to apply this setting: Inherit from parent policy: Enforce in child policies:

Encryption requirements:	<input type="checkbox"/> Use FIPS 140-2 algorithms for Notes encryption (requires 8.0.x or higher server and client)	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
--------------------------	--	--	----------------------------------	----------------------------------

Certificate Expiration Settings How to apply this setting: Inherit from parent policy: Enforce in child policies:

Warning Period:	21 days	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Custom Warning Message:		<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

On-line Certificate Status Protocol (OCSP) How to apply this setting: Inherit from parent policy: Enforce in child policies:

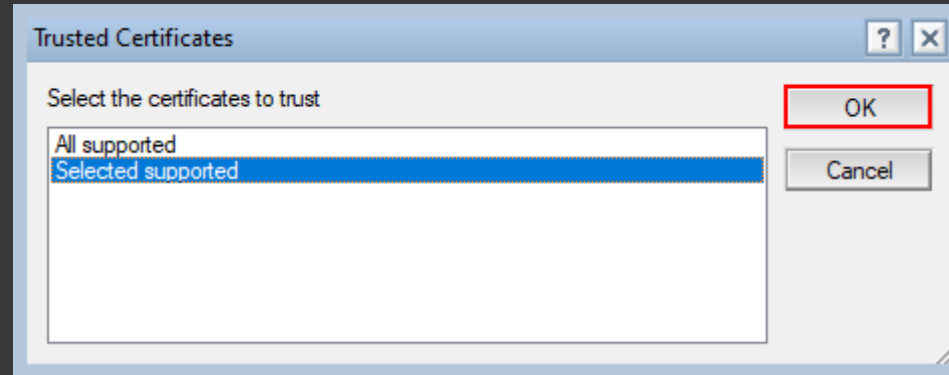
<input type="checkbox"/> Enable OCSP checking	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
---	--	----------------------------------	----------------------------------

Administrative Trust Defaults How to apply this setting: Inherit from parent policy: Enforce in child policies:

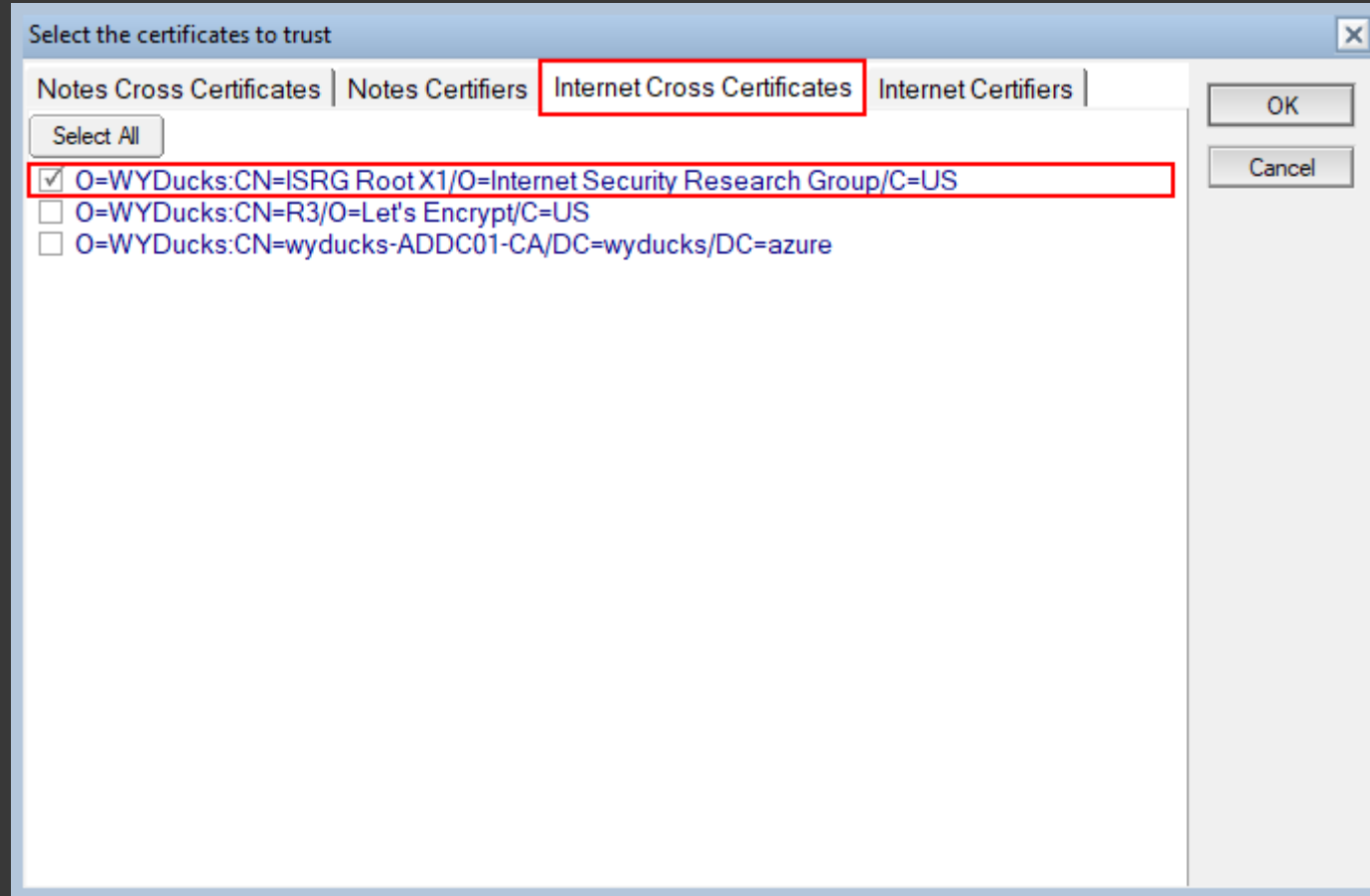
Copy all Trust Defaults without checking for relevance to Notes user

[Update Links](#)

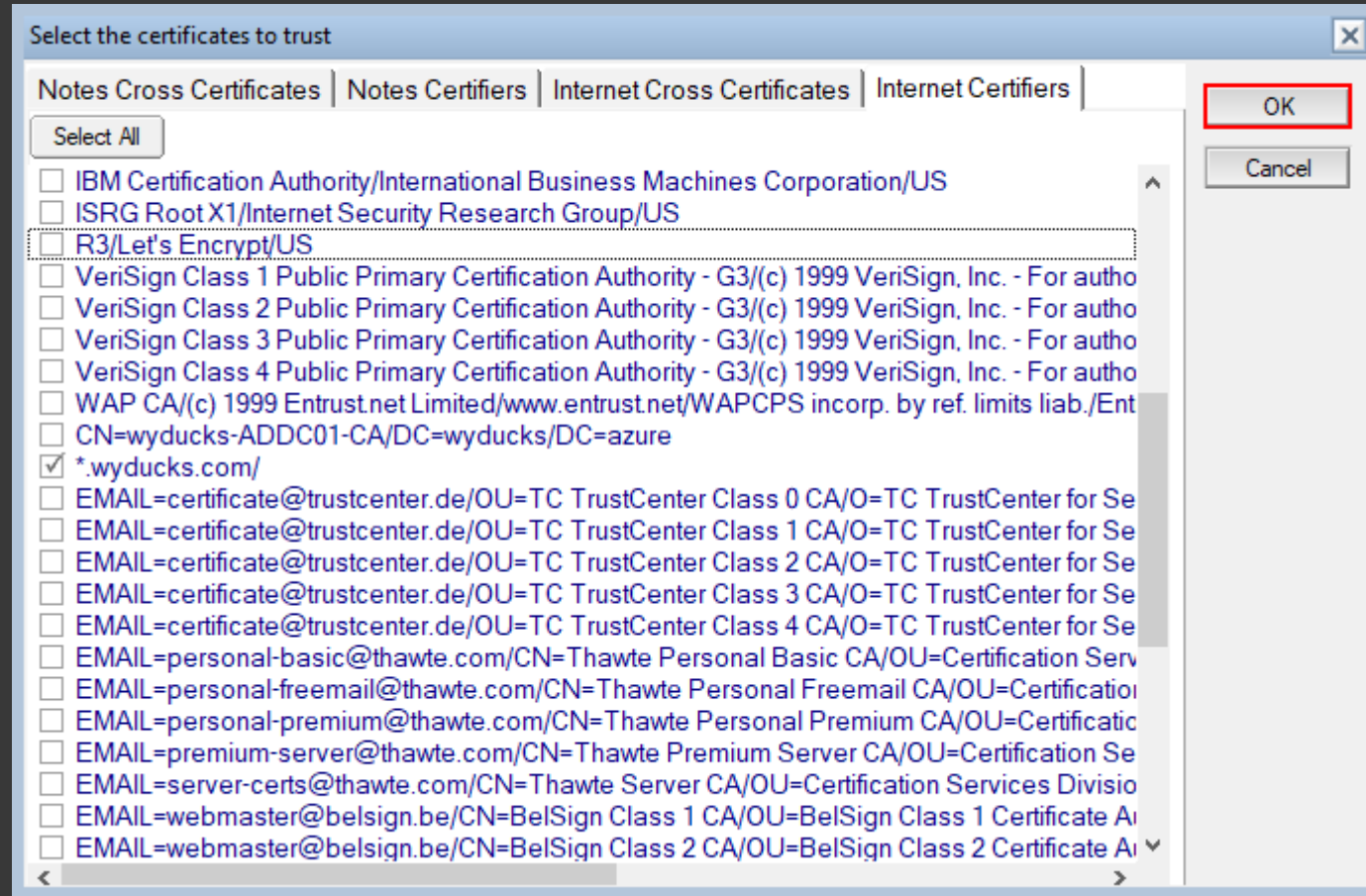
Enable NFL – IdP Certificates Rollout



Enable NFL – IdP Certificates Rollout



Enable NFL – IdP Certificates Rollout



Enable NFL – IdP Certificates Rollout

Security Settings : NFL Test

Basics | Password Management | Execution Control List | Keys and Certificates | Signed Plug-ins | Portal Server | ID Vault | Proxies | Comments | Administration

Default Public Key Requirements

Don't set value Inherit Public Key Requirement Settings from Parent Enforce Public Key Requirement Settings in Children

User Public Key Requirements

Minimum allowable key strength: Don't set value

Maximum allowable key strength: Don't set value

Preferred key strength: Don't set value

Maximum allowable age for key: days Don't set value

Earliest allowable key creation date: Don't set value

Spread new key generation for all users over this many days: Don't set value

Maximum number of days the old key should remain valid after the new key has been created: days Don't set value

Document/Mail Encryption Settings

Encryption requirements: Use FIPS 140-2 algorithms for Notes encryption (requires 8.0.x or higher server and client) Don't set value

How to apply this setting: Inherit Enforce

Certificate Expiration Settings

Warning Period: days Don't set value Inherit Enforce

Custom Warning Message: Don't set value Inherit Enforce

On-line Certificate Status Protocol (OCSP)

Enable OCSP checking Don't set value Inherit Enforce

Administrative Trust Defaults

Copy all Trust Defaults without checking for relevance to Notes user Don't set value Inherit Enforce

Don't set value Inherit Enforce

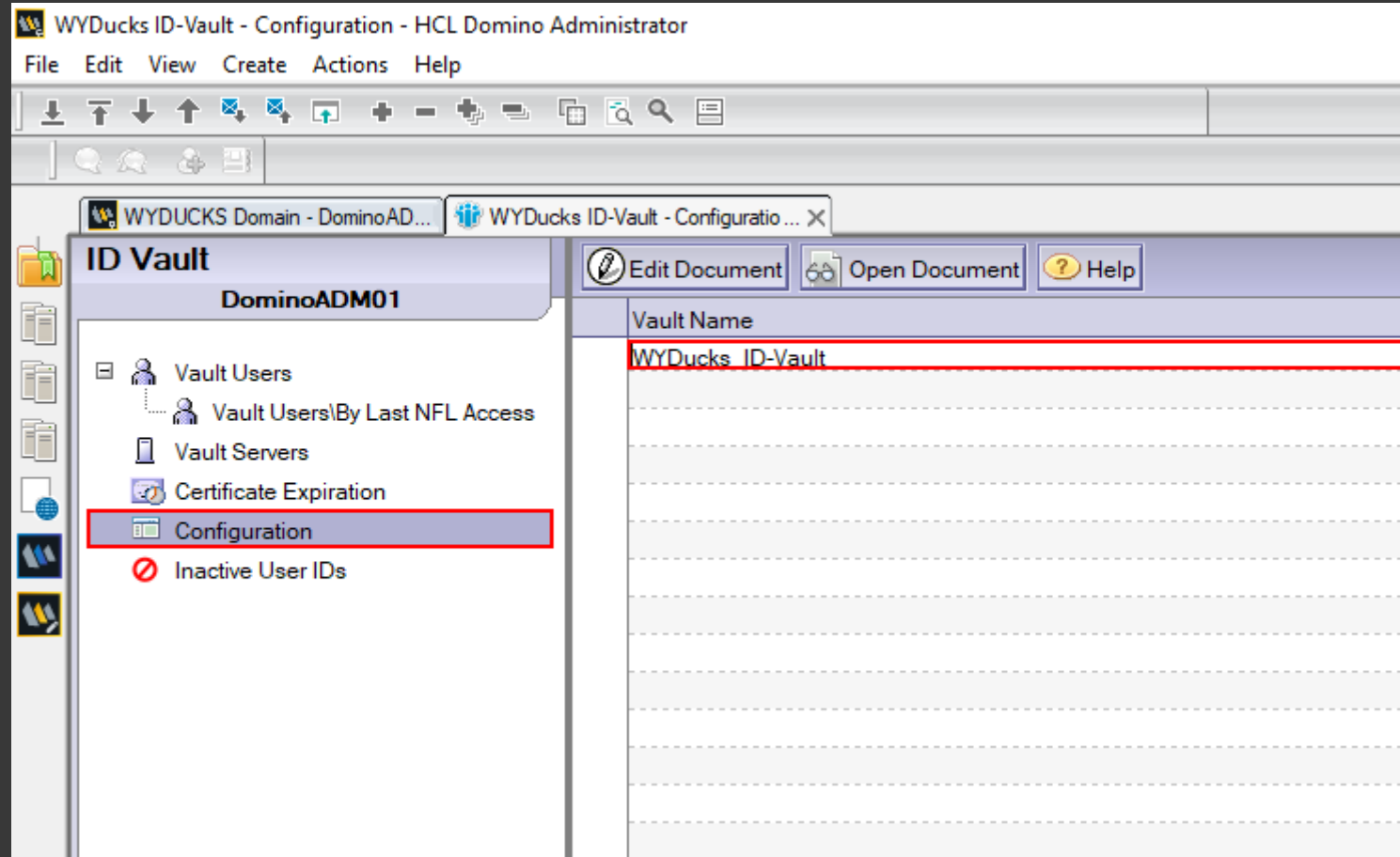
▼ Certificate Links

[/WYDucks](#)
[O=WYDucks:CN=ISRG Root X1/O=Internet Security Research Group/C=US](#)
[*wyducks.com/](#)

Enable NFL – IdP Certificates Rollout

Administrative Trust Defaults	How to apply this setting:	Inherit from parent policy:	Enforce in child policies:
<input type="checkbox"/> Copy all Trust Defaults without checking for relevance to Notes user <input type="button" value="Update Links"/> <input type="button" value="Remove All"/>	<input type="checkbox"/> Don't set value <input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit <input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce <input type="checkbox"/> Enforce
▼ Certificate Links			
<div style="border: 2px solid red; padding: 5px;">/WYDucks O=WYDucks:CN=ISRG Root X1/O=Internet Security Research Group/C=US *.wyducks.com/</div>			

Configure ID-Vault for Notes Federated Login



Configure ID-Vault for Notes Federated Login

 Save & Close  Cancel

 Vault Name: **WYDucks_ID-Vault**

IdP authenticated vault login

Notes federated login approved IdP configurations:	<input type="text" value="vault.DominoADM01.wyducks.azure"/>
Web federated login approved IdP configurations:	<input type="text" value="vault.mail1.wyducks.com"/>
Nomad federated login approved IdP configurations:	<input type="text" value=""/>

SSO right after Notes Setup!

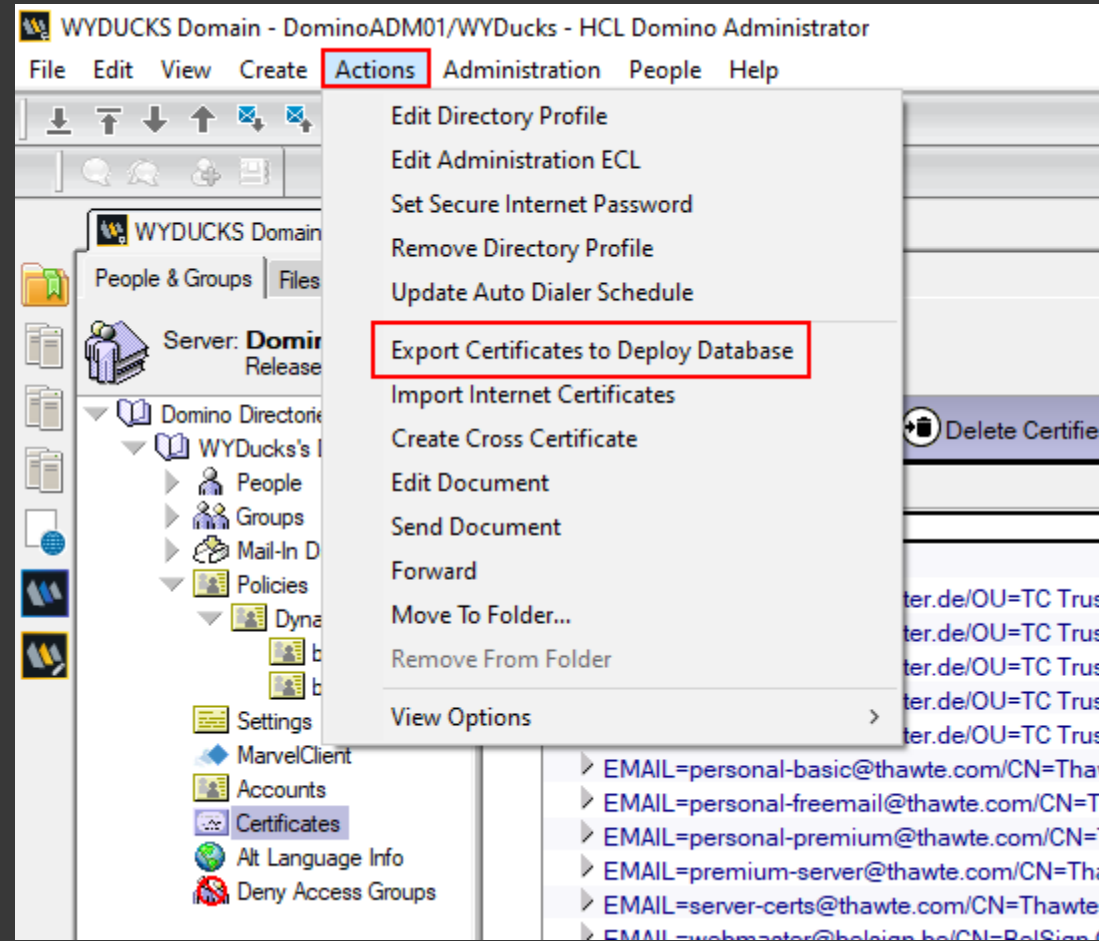


Optional – deploy.nsf

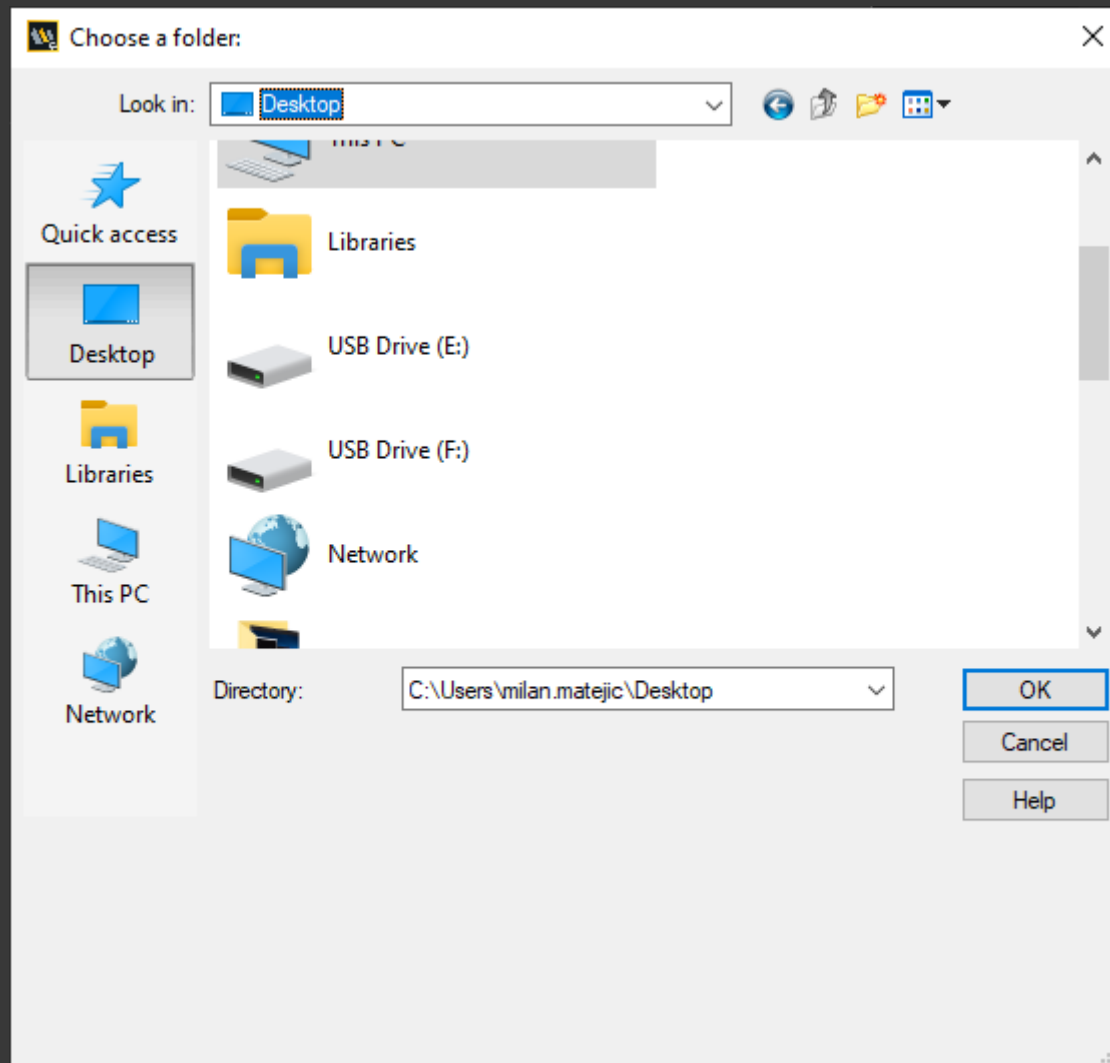
The screenshot displays the HCL Domino Administrator interface for the 'WYDUCKS Domain - DominoADM01/WYDucks'. The left-hand navigation pane shows the 'Domino Directories' tree, with 'Certificates' selected. The main pane shows a list of certifiers under the 'Internet Certifiers' category. A red arrow points to the 'Add Certifier' button in the top toolbar. The list of certifiers includes various issuers such as Digital Signature Trust Co., Thawte, Entrust.net, and VeriSign, Inc., with specific details for each, including email addresses and organizational information.

Issued By	Issued To
Internet Certifiers	
Digital Signature Trust Co.	
EMAIL=certificate@trustcenter.de/OU=TC TrustCenter Class 0 CA/O=TC TrustCenter for Security in Data Networks GmbH/L=Hamburg/ST=Hamburg/C=DE	
EMAIL=certificate@trustcenter.de/OU=TC TrustCenter Class 1 CA/O=TC TrustCenter for Security in Data Networks GmbH/L=Hamburg/ST=Hamburg/C=DE	
EMAIL=certificate@trustcenter.de/OU=TC TrustCenter Class 2 CA/O=TC TrustCenter for Security in Data Networks GmbH/L=Hamburg/ST=Hamburg/C=DE	
EMAIL=certificate@trustcenter.de/OU=TC TrustCenter Class 3 CA/O=TC TrustCenter for Security in Data Networks GmbH/L=Hamburg/ST=Hamburg/C=DE	
EMAIL=certificate@trustcenter.de/OU=TC TrustCenter Class 4 CA/O=TC TrustCenter for Security in Data Networks GmbH/L=Hamburg/ST=Hamburg/C=DE	
EMAIL=personal-basic@thawte.com/CN=Thawte Personal Basic CA/OU=Certification Services Division/O=Thawte Consulting/L=Cape Town/ST=Western Cape/C=ZA	
EMAIL=personal-freemail@thawte.com/CN=Thawte Personal Freemail CA/OU=Certification Services Division/O=Thawte Consulting/L=Cape Town/ST=Western Cape/C=ZA	
EMAIL=personal-premium@thawte.com/CN=Thawte Personal Premium CA/OU=Certification Services Division/O=Thawte Consulting/L=Cape Town/ST=Western Cape/C=ZA	
EMAIL=premium-server@thawte.com/CN=Thawte Premium Server CA/OU=Certification Services Division/O=Thawte Consulting cc/L=Cape Town/ST=Western Cape/C=ZA	
EMAIL=server-certs@thawte.com/CN=Thawte Server CA/OU=Certification Services Division/O=Thawte Consulting cc/L=Cape Town/ST=Western Cape/C=ZA	
EMAIL=webmaster@belsign.be/CN=BelSign Class 1 CA/OU=BelSign Class 1 Certificate Authority/O=BelSign NV/L=Brussels/C=BE	
EMAIL=webmaster@belsign.be/CN=BelSign Class 2 CA/OU=BelSign Class 2 Certificate Authority/O=BelSign NV/L=Brussels/C=BE	
EMAIL=webmaster@belsign.be/CN=BelSign Class 3 CA/OU=BelSign Class 3 Certificate Authority/O=BelSign NV/L=Brussels/C=BE	
EMAIL=webmaster@belsign.be/CN=BelSign Object Publishing CA/OU=BelSign Object Publishing Certificate Authority/O=BelSign NV/L=Brussels/C=BE	
EMAIL=webmaster@belsign.be/CN=BelSign Secure Server CA/OU=BelSign Secure Server Certificate Authority/O=BelSign NV/L=Brussels/C=BE	
Entrust.net	
IE	
JP	
US	
Entrust.net	
Equifax	
GTE Corporation	
Internet Security Research Group	
Let's Encrypt	
R3	
*.wyducks.com/	
RSA Data Security, Inc.	
VeriSign, Inc.	
(Not Categorized)	
Internet Cross Certificates	
WYDucks	
CN=wyducks-ADDC01-CA/DC=wyducks/DC=azure	
ISRG Root X1/Internet Security Research Group/US	
R3/Let's Encrypt/US	
Notes Certifiers	
WYDucks	
WYDucks	
Password Reset Certificates	
Vault Trust Certificates	

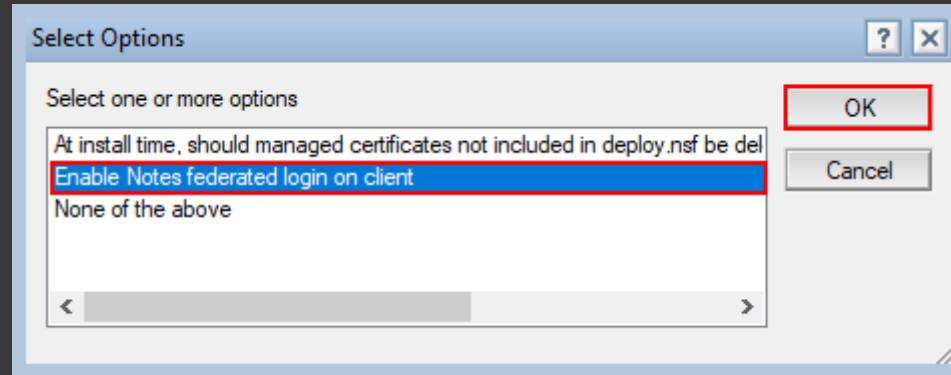
Optional – deploy.nsf



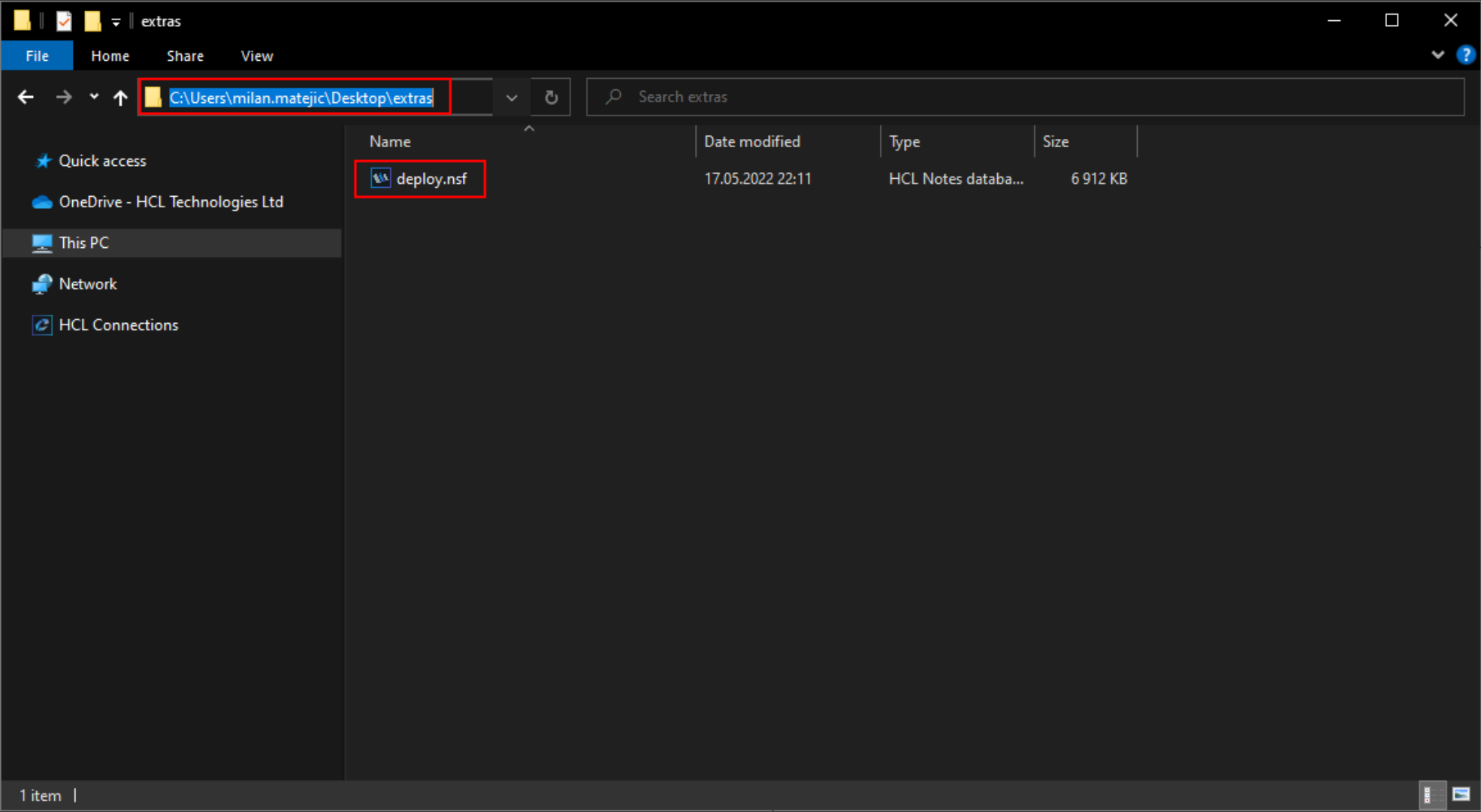
Optional – deploy.nsf



Optional – deploy.nsf



Optional – deploy.nsf

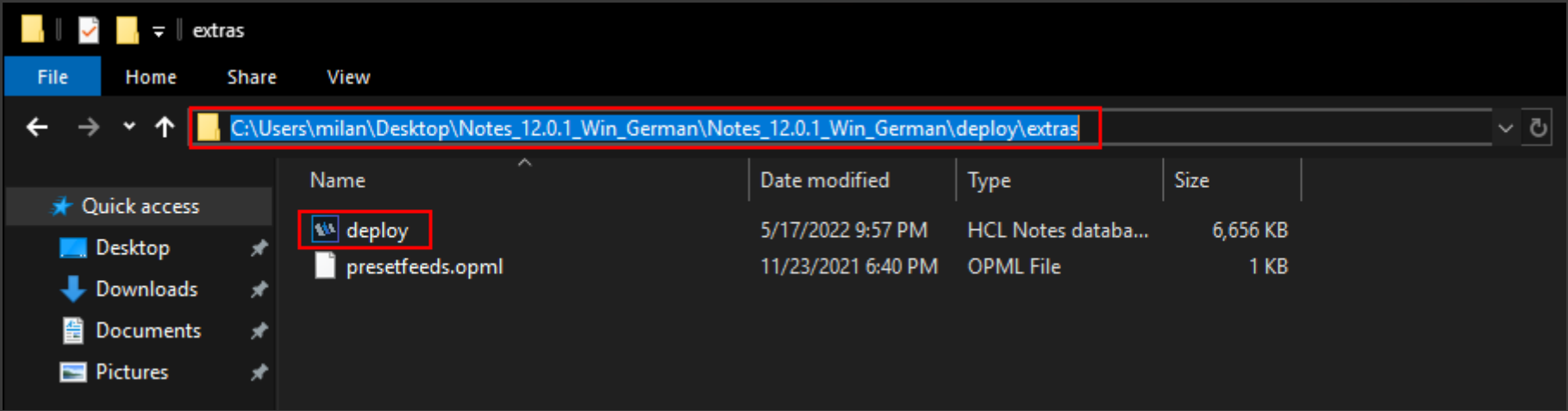


Optional – deploy.nsf

Copy the file into the setup package



Optional – deploy.nsf

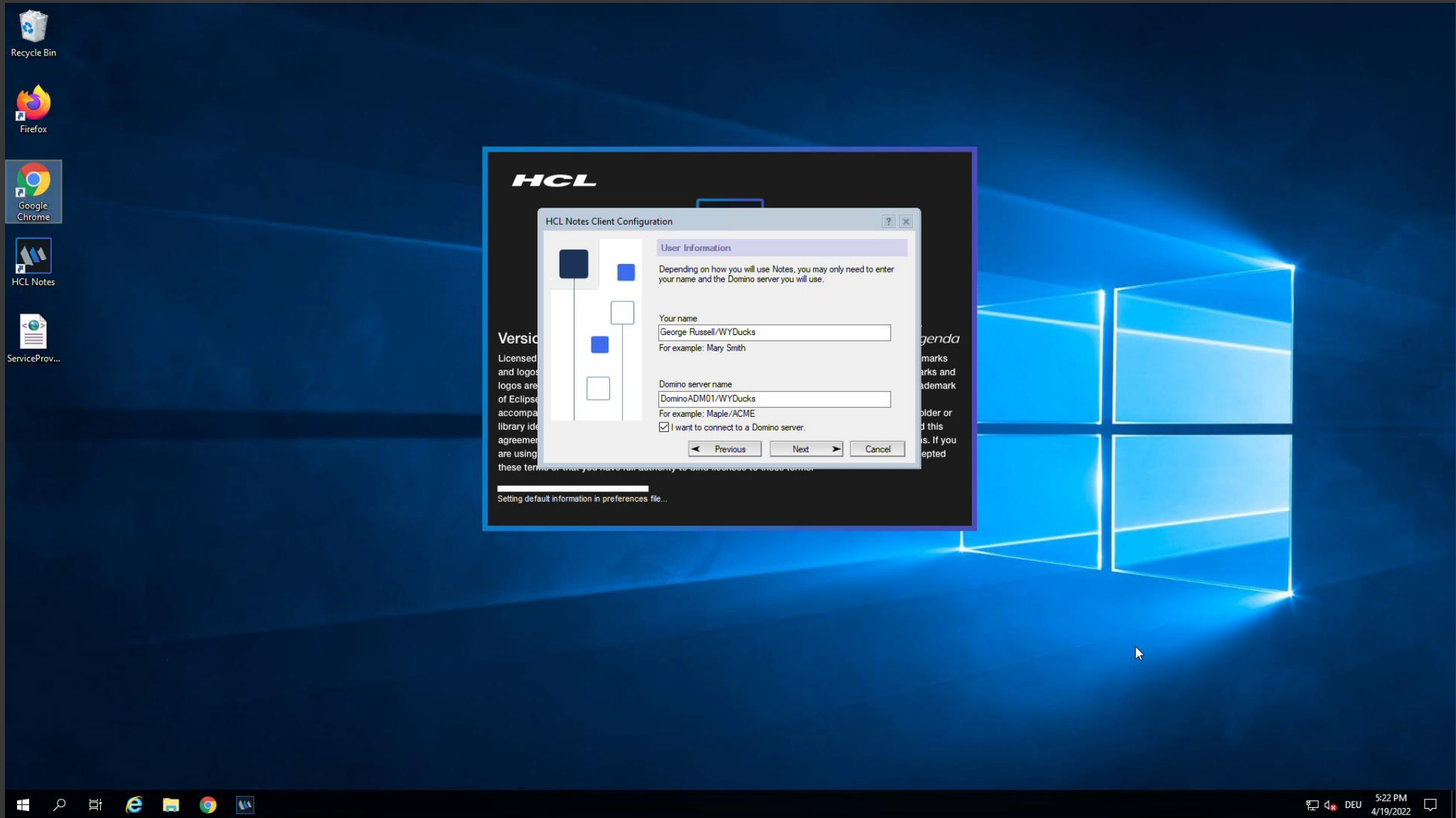


Optional – Notes Shared Login



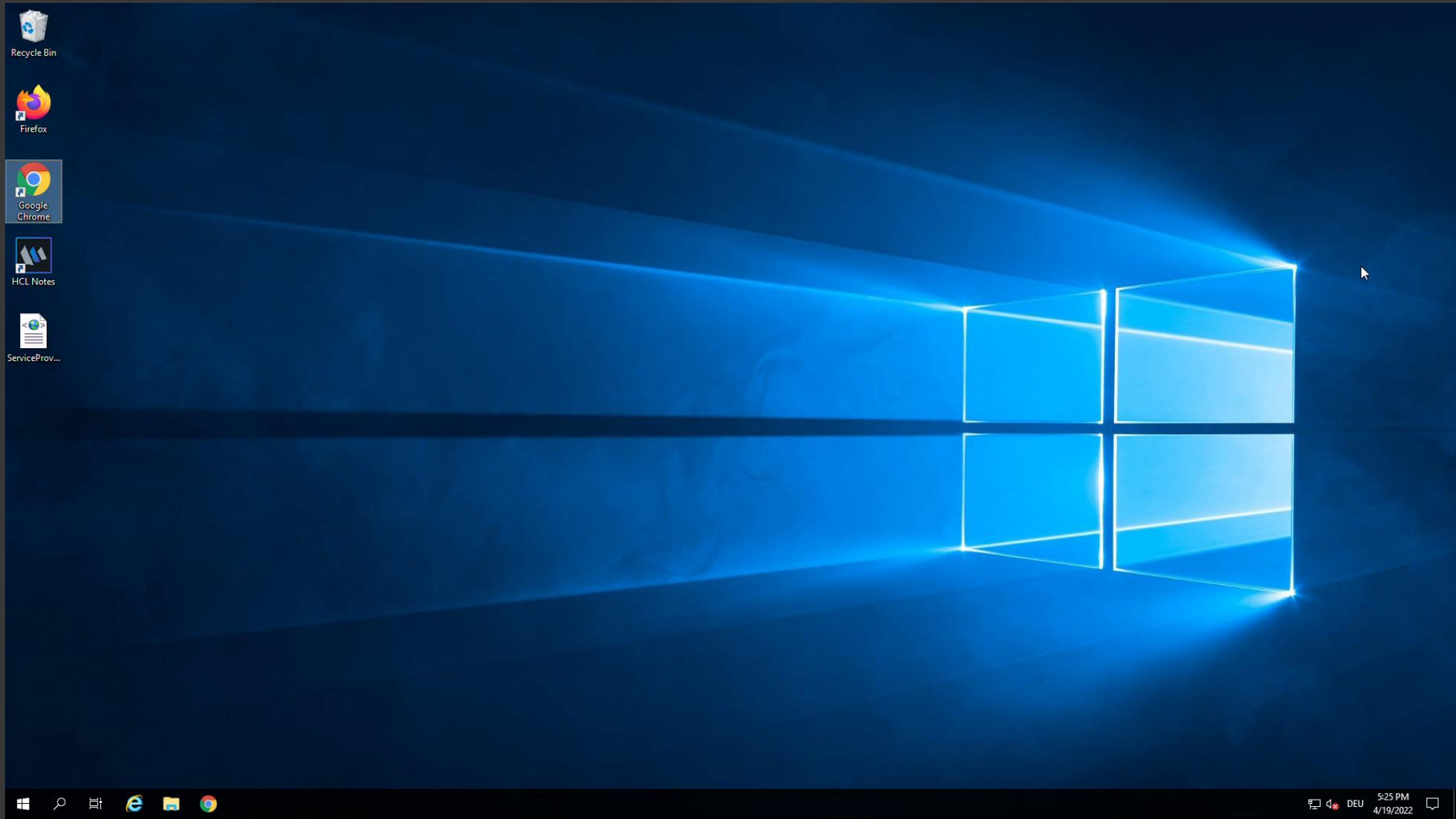
Demo

Demo



Demo

Demo



What Just Happened!?

Notes SSO

Using SAML and IWA!



Infrastructure Needed

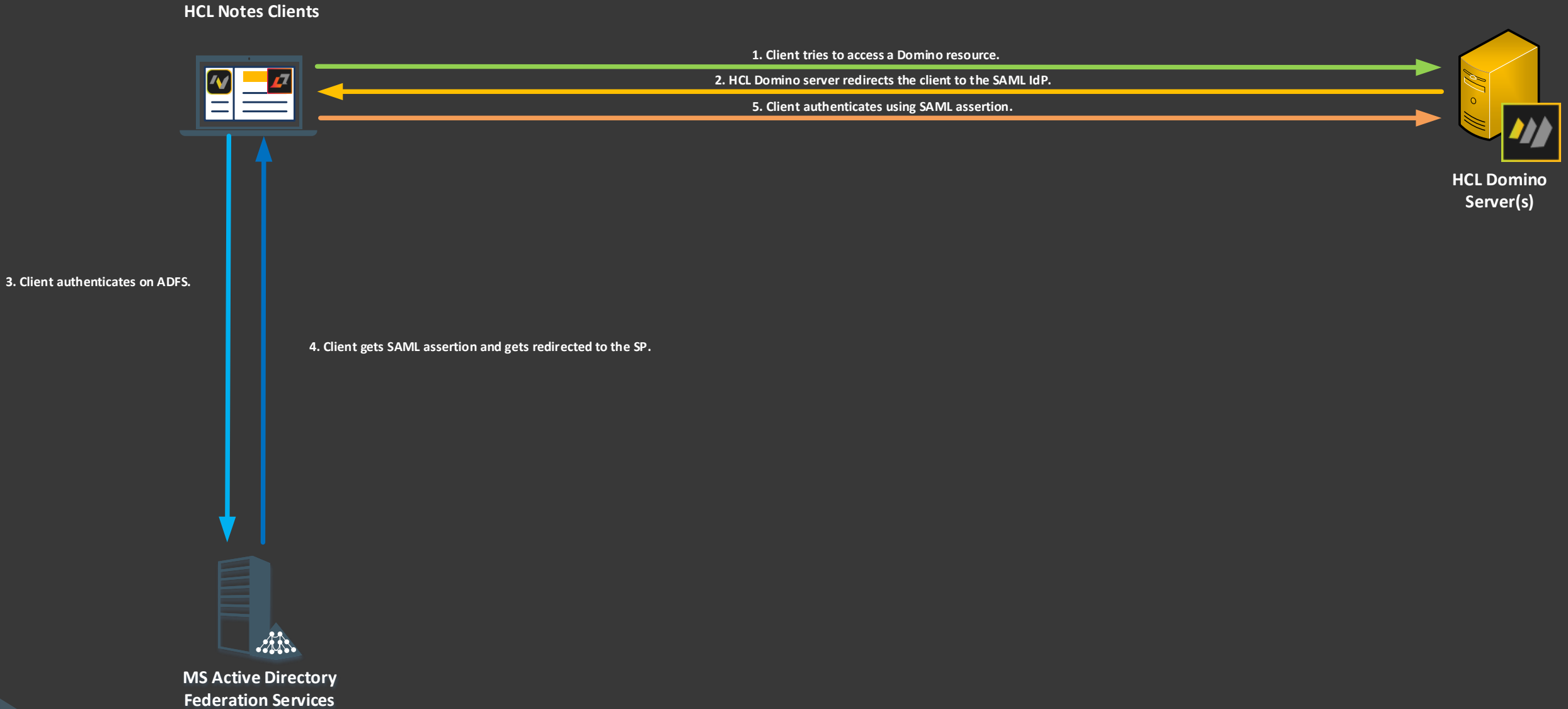


Table of Contents

Motivation	HCL Domino & SAML	Web Federated Login	Issues
Why SAML?	Prerequisites	Notes Federated Login	Q & A
SAML	Infrastructure Needed	Traveler & SAML	Shibboleth
Wording	Basic SAML Setup	Bonus – Nomad!	References
How does it work?	SAML & SSO	Troubleshooting	

Traveler Specific Limitations and Requirements

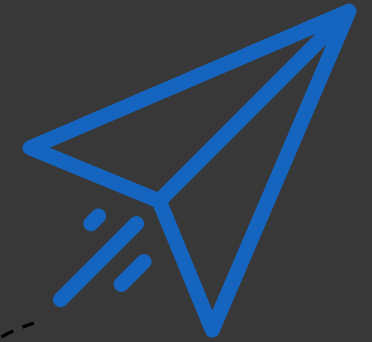


Traveler & SAML

 **Create IdP Configuration**

 **Enable SAML on Traveler**

 **Restart**



Create the IdP Configuration Document

Inside of "idpcat.nsf"




Create the IdP Configuration Document

IdP Configuration : Traveler1Com

Basics | Client Settings | Certificate Management | Advanced | Administration

Basics

Import XML file

Host names or addresses mapped to this site:	traveler1.wyducks.com; 10.1.0.6; 40.68.125.37
Protocol version:	SAML 2.0
State:	Enabled
Federation product:	AuthnRequest SAML 2.0 compatible
Service provider ID:	https://traveler1.wyducks.com
Artifact resolution service URL:	
Single sign-on service URL:	https://adfs.wyducks.com/adfs/ls/
Encryption method:	http://www.w3.org/2001/04/xmlenc#sha256
IdP name (for your reference):	Traveler1Com
Comment:	
Imported file:	 - FederationMetadata.xml
Import time:	07.02.2022 09:09

Create the IdP Configuration Document

IdP Configuration : Traveler1Com

Basics | **Client Settings** | Certificate Management | Advanced | Administration

Notes Client Settings

Enable Windows single sign-on:	<input type="checkbox"/> No
Sites that are trusted:	
Enforce TLS:	<input checked="" type="checkbox"/> Yes

Encrypting Domino SAML Assertions

IdP Configuration : Traveler1Com

Basics | Client Settings | **Certificate Management** | Advanced | Administration

Certificate Management Settings


Examine SP Certificate Export SP XML

Company name: CN=Traveler1ComCertificate

Domino URL: **https://traveler1.wyducks.com**

Single logout URL: https://ads.wyducks.com/ads/ls/

Certificate public hash value (base 64): RNq5rU7fcMDqJgcAQcRAhg==

Exported certificate:  - ServiceProvider.xml

Enable SAML for HCL Verse Mobile Clients

WYDUCKS Domain - DominoADM01/WYDucks - HCL Domino Administrator

File Edit View Create Actions Administration Configuration Help

WYDUCKS Domain - DominoAD...
People & Groups Files Server... Messaging... Replication **Configuration**

Server: **DominoADM01/WYDucks**
Release 12.0.1FP1 on Windows/2019 10.0

Add Internet Site... Create Global Web Settings Create Web SSO Configuration Edit Document Delete Internet Site

Site name
WYDucks
LDAP Site: LDAP Site (mail1.wyducks.com; mail2.wyducks.com; 10.1.0.4; 10.1.0.5)
Web Site: Auto Generated Internet Site Document for Web Protocol (traveler.wyducks.com; traveler1.wyducks.com; DomTrav.oixgapihkpqutiilmaq3gr1he.ax.internal.cloudapp.net; 10.1.0.6; 40.68.125.37)
Rule (substitution): /Microsoft-Server-ActiveSync* --> /traveler/Microsoft-Server-ActiveSync*
Rule (substitution): /servlet/traveler* --> /traveler*
Web Site: Verse on-Premises Mail1 (mail.wyducks.com; mail1.wyducks.com; 10.1.0.4)
Web Site: Verse on-Premises Mail2 (mail.wyducks.com; mail2.wyducks.com; 10.1.0.5)
Web SSO Configuration: LtpaToken

Enable SAML for HCL Verse Mobile Clients

Web Site Auto Generated Internet Site Document for Web Protocol

Basics | Configuration | **Domino Web Engine** | Security | Comments | Administration

HTTP Sessions

Session authentication: SAML [Open IdP Configuration](#)

Web SSO Configuration: LtpaToken

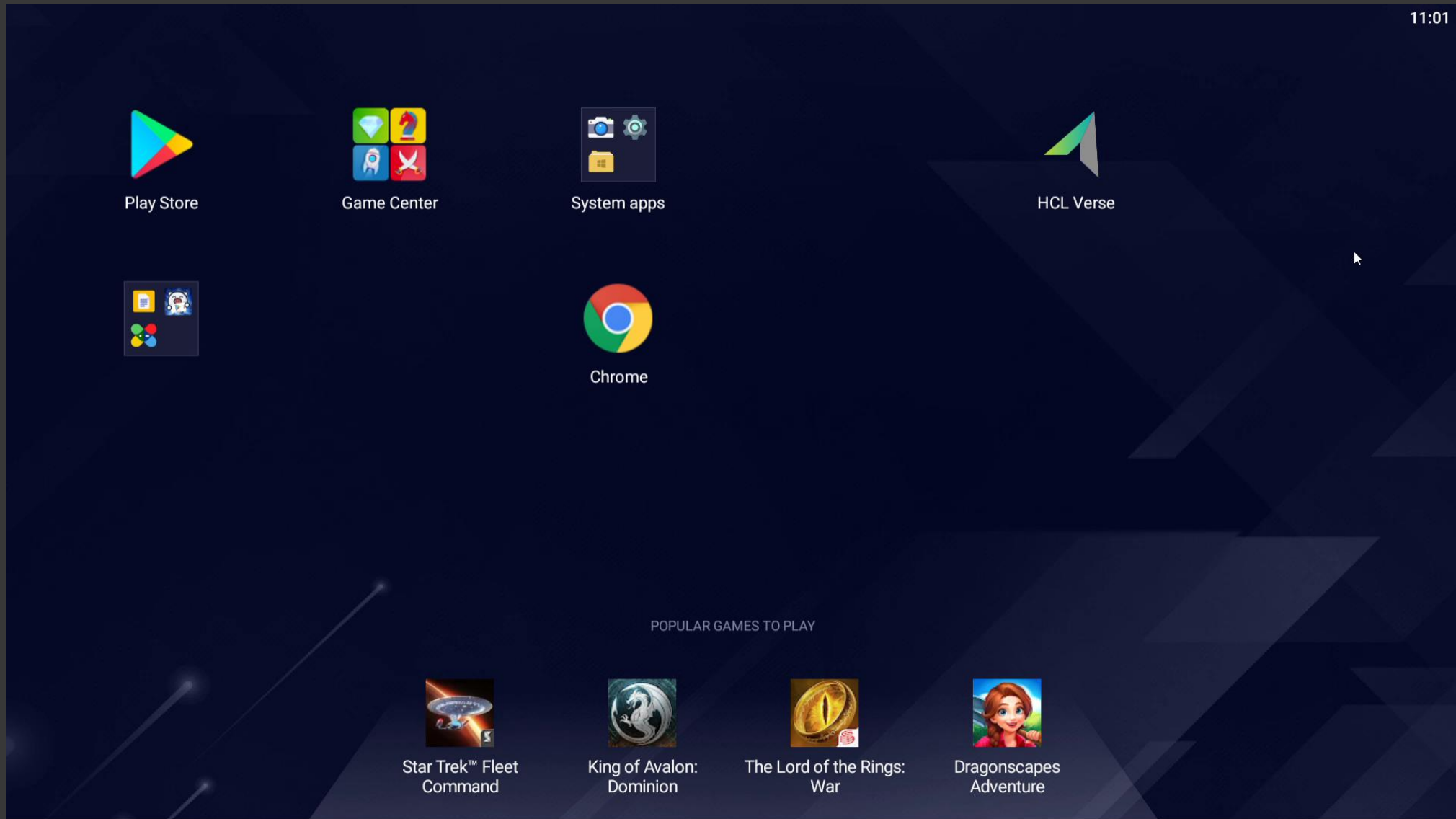
Force login on TLS: Yes

SAML single server session expiration: **600** minutes

When overriding session authentication, generate session cookie: Yes

Demo

Demo



Demo

Demo

The screenshot shows an email inbox interface. At the top right, the time is 11:02. The header bar is blue and contains a menu icon, the word "Inbox", search and filter icons, and a vertical ellipsis. Below the header, a list of email messages is displayed. Each message includes a profile picture of Carlos Sainz, his name, a subject line, and a preview of the message content. The messages are dated from 9:24 AM to Apr 15. A blue circular button with a white plus sign is positioned at the bottom right of the message list. The main content area to the right of the list is currently empty.

Up-to-date	
Carlos Sainz Encrypted and signed mail This message is encrypted.	9:24 AM
Carlos Sainz Some Attachments Hello, here are some attachments. Best regards, Carlos	9:23 AM
Carlos Sainz Hello Whats up	9:22 AM
Carlos Sainz test signed and encrypted from Traveler This message is encrypted.	Apr 15
Carlos Sainz test signed and encrypted This message is encrypted.	Apr 15
Carlos Sainz test signed and encrypted from Traveler This message is encrypted.	Apr 15
Carlos Sainz	Apr 15

Optional – Allow PW Authentication with ID-Vault

Security Settings : NFL Test

Basics | **Password Management** | Execution Control List | Keys and Certificates | Signed Plug-ins | Portal Server | ID Vault | Proxies

Password Management Basics | Notes Shared Login | Federated Login

Notes Federated Login How to apply th

Enable Notes Federated login with SAML IdP: Yes Don't set value

Activation Notification

How to notify users when enabled: Custom message dialog

Custom message text:

Deactivation Notification

How to notify users when disabled: Custom message dialog

Custom message text:

Web Federated Login

Enable Web Federated login with SAML IdP: Yes

Nomad Federated Login

Enable Nomad Federated login with SAML IdP: Yes

Additional settings for Federated Login

Allow password authentication with the ID vault: Yes

Table of Contents

Motivation	HCL Domino & SAML	Web Federated Login	Issues
Why SAML?	Prerequisites	Notes Federated Login	Q & A
SAML	Infrastructure Needed	Traveler & SAML	Shibboleth
Wording	Basic SAML Setup	Bonus – Nomad!	References
How does it work?	SAML & SSO	Troubleshooting	

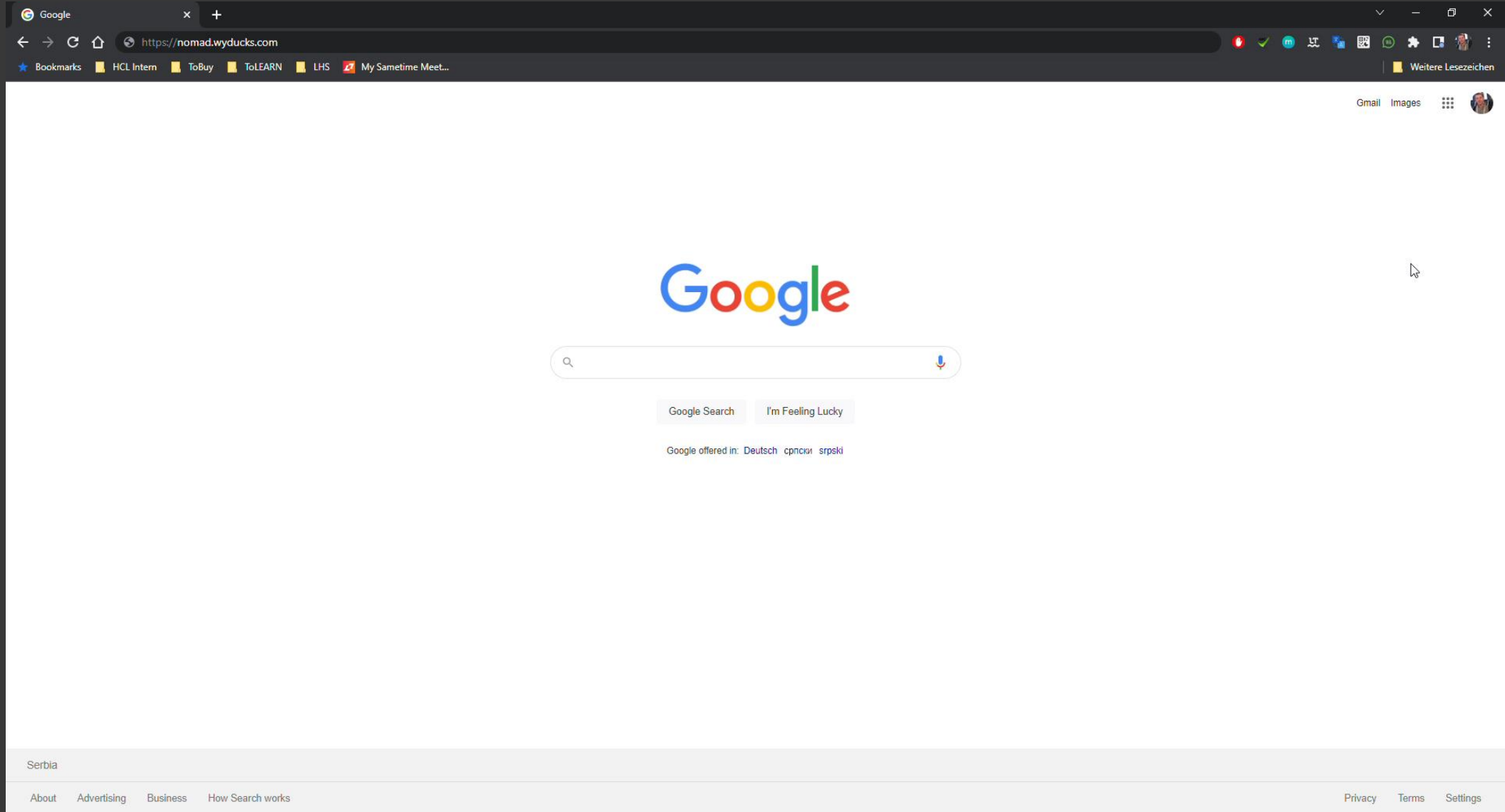
Nomad Federated Login

Ad02. Deploying HCL Nomad Web



Demo

Demo



Demo

Demo

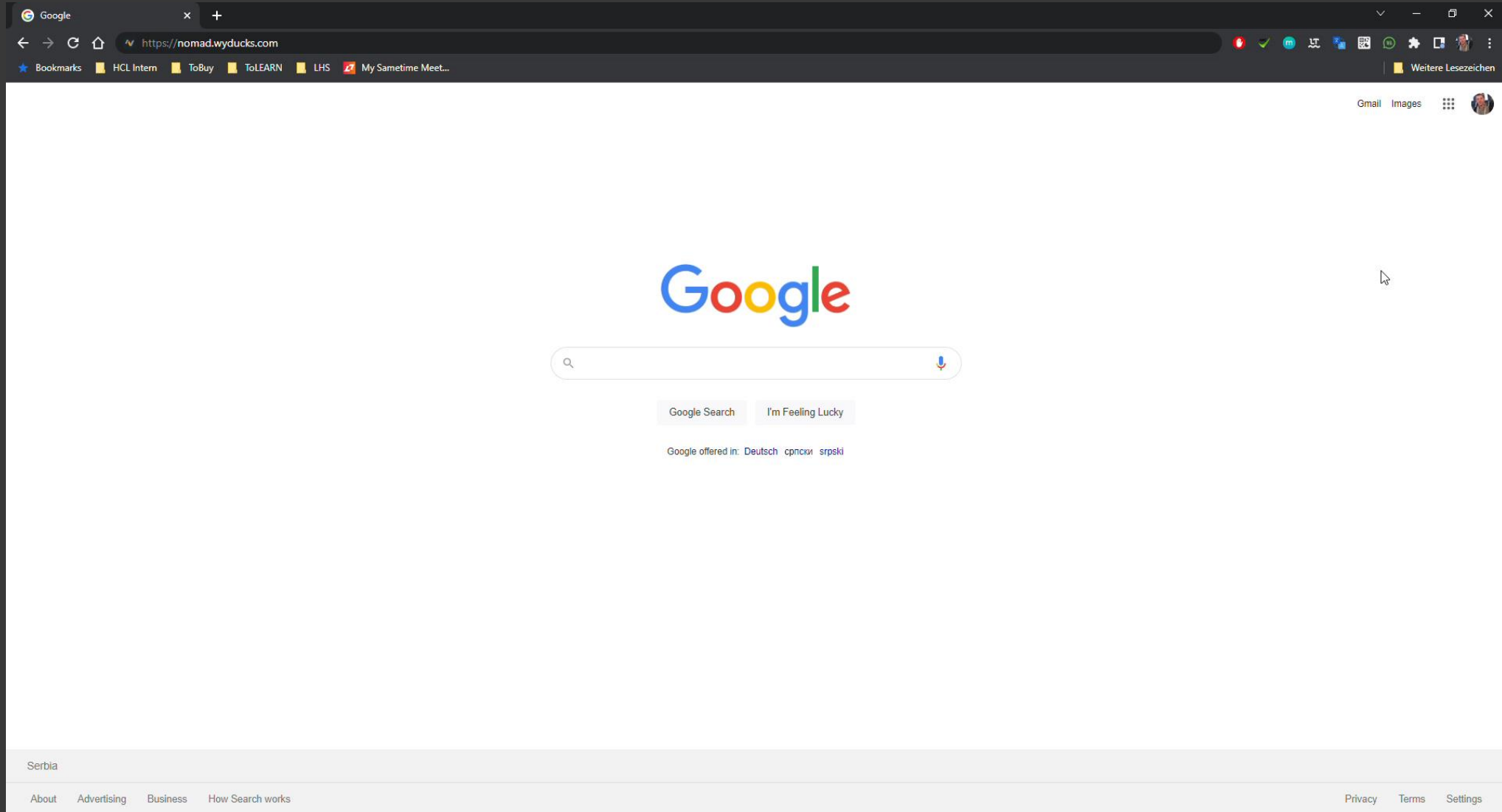
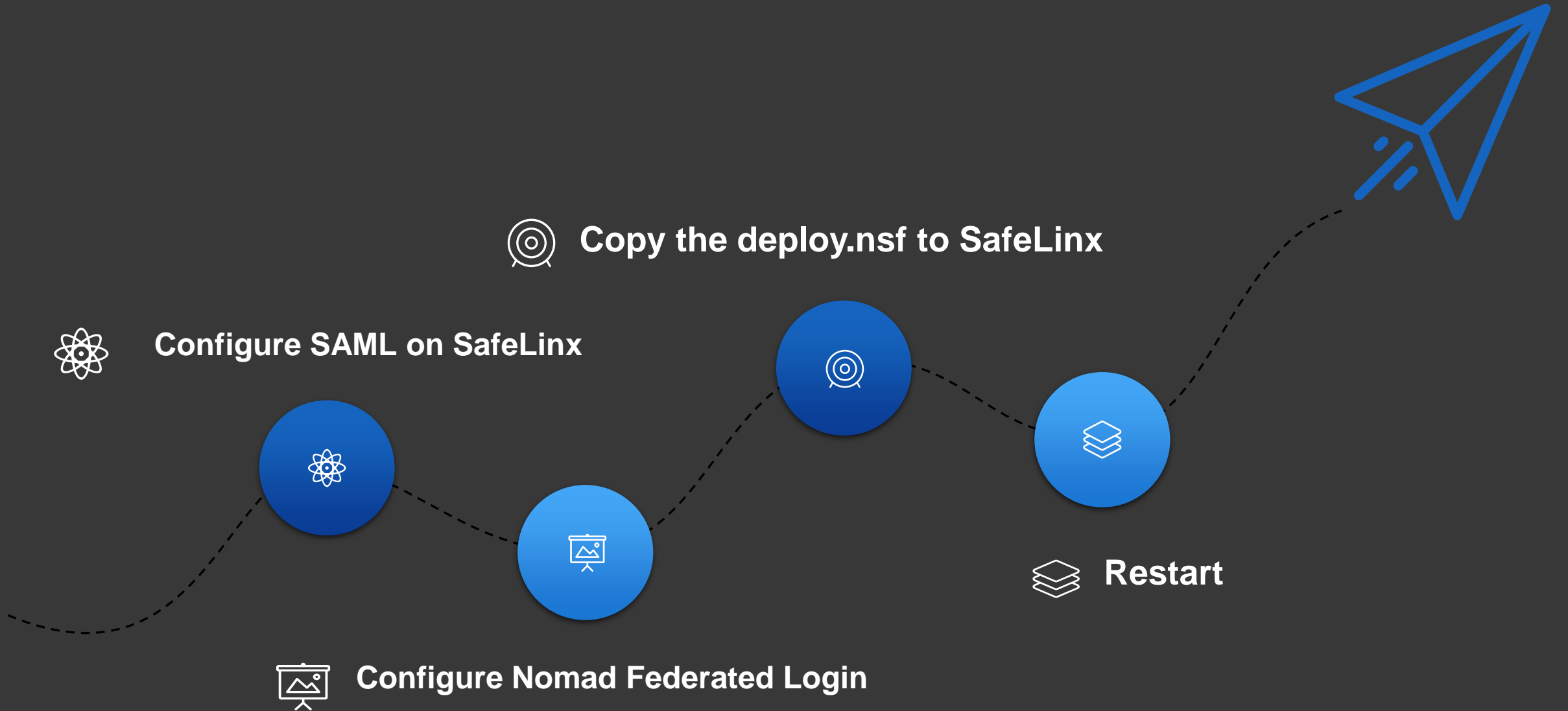


Table of Contents

Motivation	HCL Domino & SAML	Web Federated Login	Issues
Why SAML?	Prerequisites	Notes Federated Login	Q & A
SAML	Infrastructure Needed	Traveler & SAML	Shibboleth
Wording	Basic SAML Setup	Bonus – Nomad!	References
How does it work?	SAML & SSO	Troubleshooting	

Nomad & SAML



Check configuration

Set debug in notes.ini

Troubleshooting – Domino Server



Troubleshooting – Notes Federated Login



Troubleshooting – Useful Tools

SAML-tracer *Chrome extension*

Troubleshooting – Protip

WFL & ID-Cache

tell http dump vaulted idcache

Troubleshooting – Protip

```
* [0C84:0039-0104] 04/15/2022 02:07:36 PM TLS/SSL connection 168.63.129.16(57817) -> 10.1.0.4(443) failed with rejected unknown record type
* [0C84:0039-0104] 04/15/2022 02:07:41 PM TLS/SSL connection 168.63.129.16(57986) -> 10.1.0.4(443) failed with rejected unknown record type
* [0C84:0039-0104] 04/15/2022 02:07:46 PM TLS/SSL connection 168.63.129.16(58121) -> 10.1.0.4(443) failed with rejected unknown record type
tel http dump vaulted idcache
* [0F00:004F-0618] 04/15/2022 02:07:49 PM Remote console command issued by Administrator/WYDucks: tel http dump vaulted idcache
[0C84:0002-05F4] Number of User ID Entries in ID Cache: 2
[0C84:0002-05F4] User Name [CN=George Russell/O=WYDucks], Expire Time Date [04/15 10:07:16 PM]
[0C84:0002-05F4] User Name [CN=Carlos Sainz/O=WYDucks], Expire Time Date [04/15 10:06:04 PM]
* [0C84:0038-0D44] 04/15/2022 02:07:51 PM TLS/SSL connection 168.63.129.16(58252) -> 10.1.0.4(443) failed with rejected unknown record type
* [0C84:0038-0D44] 04/15/2022 02:07:56 PM TLS/SSL connection 168.63.129.16(58408) -> 10.1.0.4(443) failed with rejected unknown record type
* [0C84:0038-0D44] 04/15/2022 02:08:01 PM TLS/SSL connection 168.63.129.16(58559) -> 10.1.0.4(443) failed with rejected unknown record type
* [0C84:0038-0D44] 04/15/2022 02:08:06 PM TLS/SSL connection 168.63.129.16(58710) -> 10.1.0.4(443) failed with rejected unknown record type
* [0C84:0038-0D44] 04/15/2022 02:08:11 PM TLS/SSL connection 168.63.129.16(58882) -> 10.1.0.4(443) failed with rejected unknown record type
```

Table of Contents

Motivation

HCL Domino & SAML

Web Federated Login

Issues

Why SAML?

Prerequisites

Notes Federated Login

Q & A

SAML

Infrastructure Needed

Traveler & SAML

Shibboleth

Wording

Basic SAML Setup

Bonus – Nomad!

References

How does it work?

SAML & SSO

Troubleshooting

HCL Traveler

Secure mail operations

HCL SafeLinx

Multiple SAML configurations

Table of Contents

Motivation

HCL Domino & SAML

Web Federated Login

Issues

Why SAML?

Prerequisites

Notes Federated Login

[Q & A](#)

SAML

Infrastructure Needed

Traveler & SAML

Shibboleth

Wording

Basic SAML Setup

Bonus – Nomad!

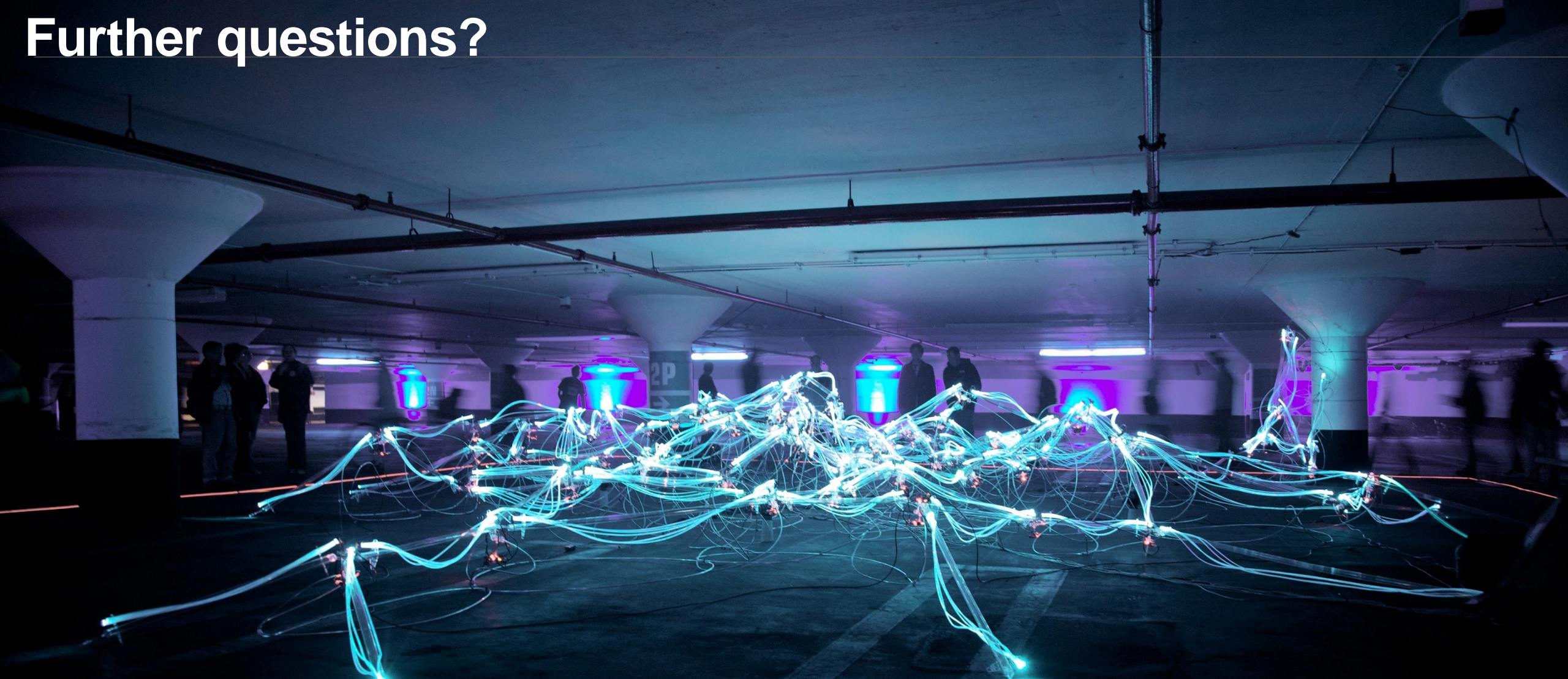
References

How does it work?

SAML & SSO

Troubleshooting

Further questions?



Evolve, disrupt. Together...

Table of Contents

Motivation

HCL Domino & SAML

Web Federated Login

Issues

Why SAML?

Prerequisites

Notes Federated Login

Q & A

SAML

Infrastructure Needed

Traveler & SAML

[Shibboleth](#)

Wording

Basic SAML Setup

Bonus – Nomad!

References

How does it work?

SAML & SSO

Troubleshooting

References

- **SAML 2.0 as defined by OASIS**
 - **<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html>**
- **Domino 12.0.1 SAML Documentation**
 - **https://help.hcltechsw.com/domino/12.0.0/admin/secu_using_security_assertion_markup_language_saml_to_configure_federated_identity_authentication_t.html**
- **Traveler 12.0.1 SAML Documentation**
 - **https://help.hcltechsw.com/traveler/12.0.0/saml_verse_overview.html**
- **imgflip.com**
- **<https://www.qrcode-monkey.com/>**
- **How to configure SAML authentication for Domino HTTP using Microsoft Azure as an Identity Provider**
 - **https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0098580**