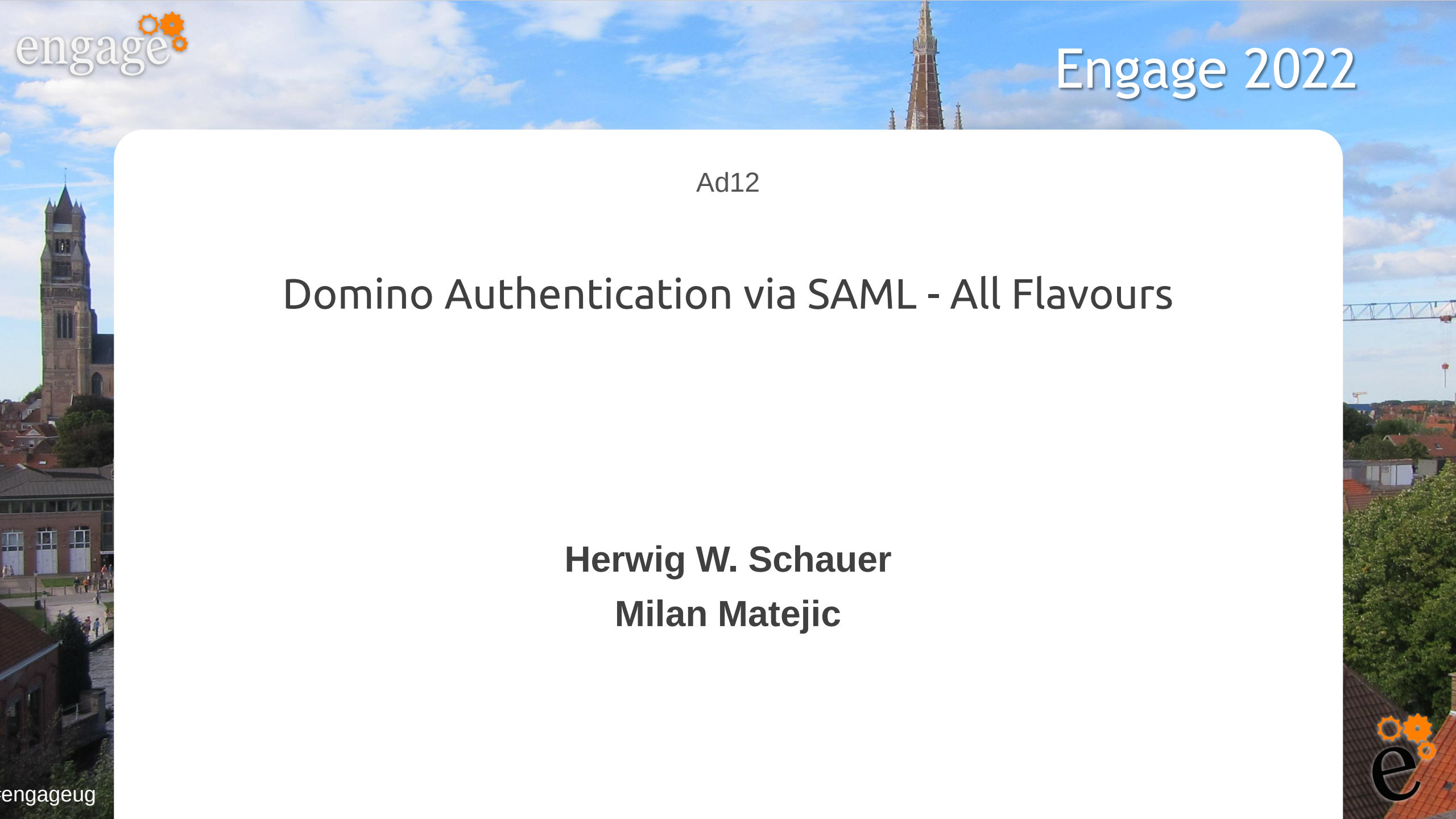


Ad12

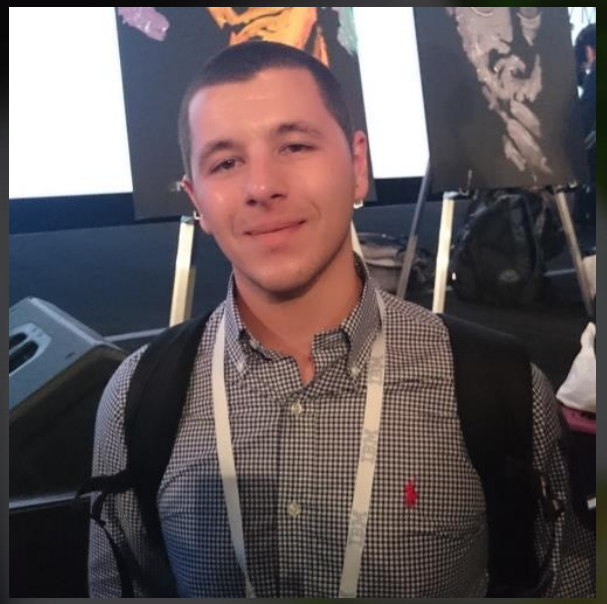
Domino Authentication via SAML - All Flavours

Herwig W. Schauer

Milan Matejic

About us

Milan Matejic



HCL SOFTWARE

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

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

SAML & SSO

Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

SAML & SSO

Web Federated Login

Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

SAML & SSO

Web Federated Login

Notes Federated Login

Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

SAML & SSO

Web Federated Login

Notes Federated Login

Traveler & SAML

Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

SAML & SSO

Web Federated Login

Notes Federated Login

Traveler & SAML

Bonus – Nomad!

Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

SAML & SSO

Web Federated Login

Notes Federated Login

Traveler & SAML

Bonus – Nomad!

Troubleshooting

Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

SAML & SSO

Web Federated Login

Notes Federated Login

Traveler & SAML

Bonus – Nomad!

Troubleshooting

Issues

Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

SAML & SSO

Web Federated Login

Notes Federated Login

Traveler & SAML

Bonus – Nomad!

Troubleshooting

Issues

Q & A

Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

SAML & SSO

Web Federated Login

Notes Federated Login

Traveler & SAML

Bonus – Nomad!

Troubleshooting

Issues

Q & A

Shibboleth

Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

SAML & SSO

Web Federated Login

Notes Federated Login

Traveler & SAML

Bonus – Nomad!

Troubleshooting

Issues

Q & A

Shibboleth

References

Motivation

Password fatigue

Motivation

Motivation

Motivation

Ease of maintenance

Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

SAML & SSO

Web Federated Login

Notes Federated Login

Traveler & SAML

Bonus – Nomad!

Troubleshooting

Issues

Q & A

Shibboleth

References

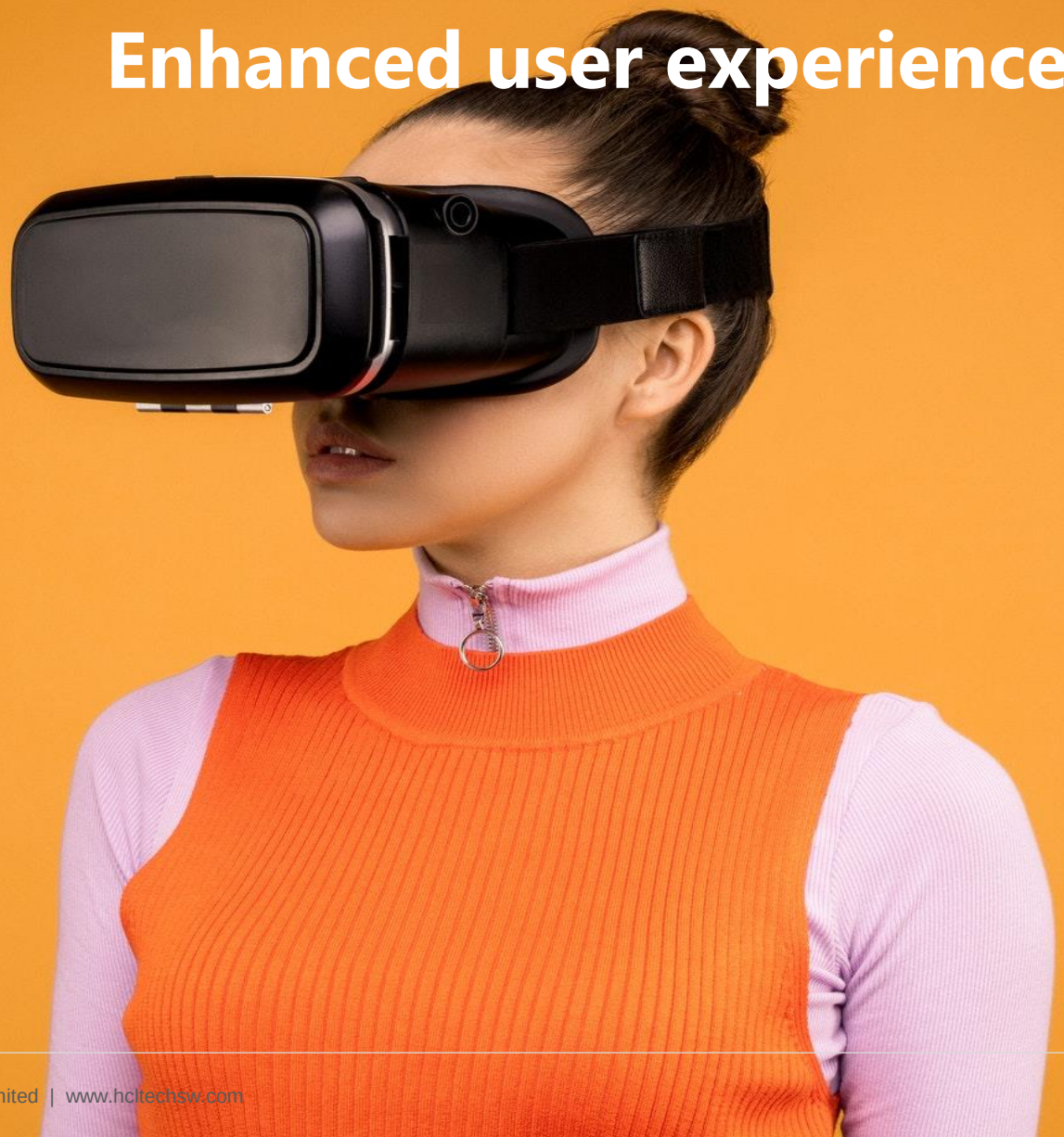
Why SAML!?

Open standard

HCL SOFTWARE

Why SAML!?

Enhanced user experience



Why SAML!?

HCL Digital Solutions portfolio

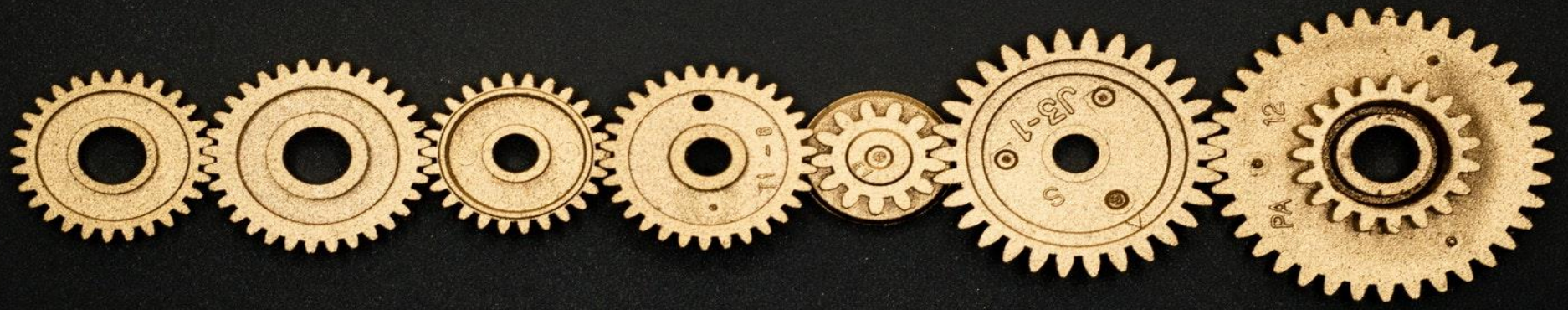


Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

SAML & SSO

Web Federated Login

Notes Federated Login

Traveler & SAML

Bonus – Nomad!

Troubleshooting

Issues

Q & A

Shibboleth

References

Security Assertion Markup Language

Authentication Mechanism

SAML

Open Standard

Current Implementation SAML 2.0

Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

SAML & SSO

Web Federated Login

Notes Federated Login

Traveler & SAML

Bonus – Nomad!

Troubleshooting

Issues

Q & A

Shibboleth

References

Wording

Authentication vs. authorization

Wording

Basic SAML

Wording

Web Federated Login

WFL

Wording

Notes Federated Login

NFL

HCL SOFTWARE

Wording

Nomad Federated Login

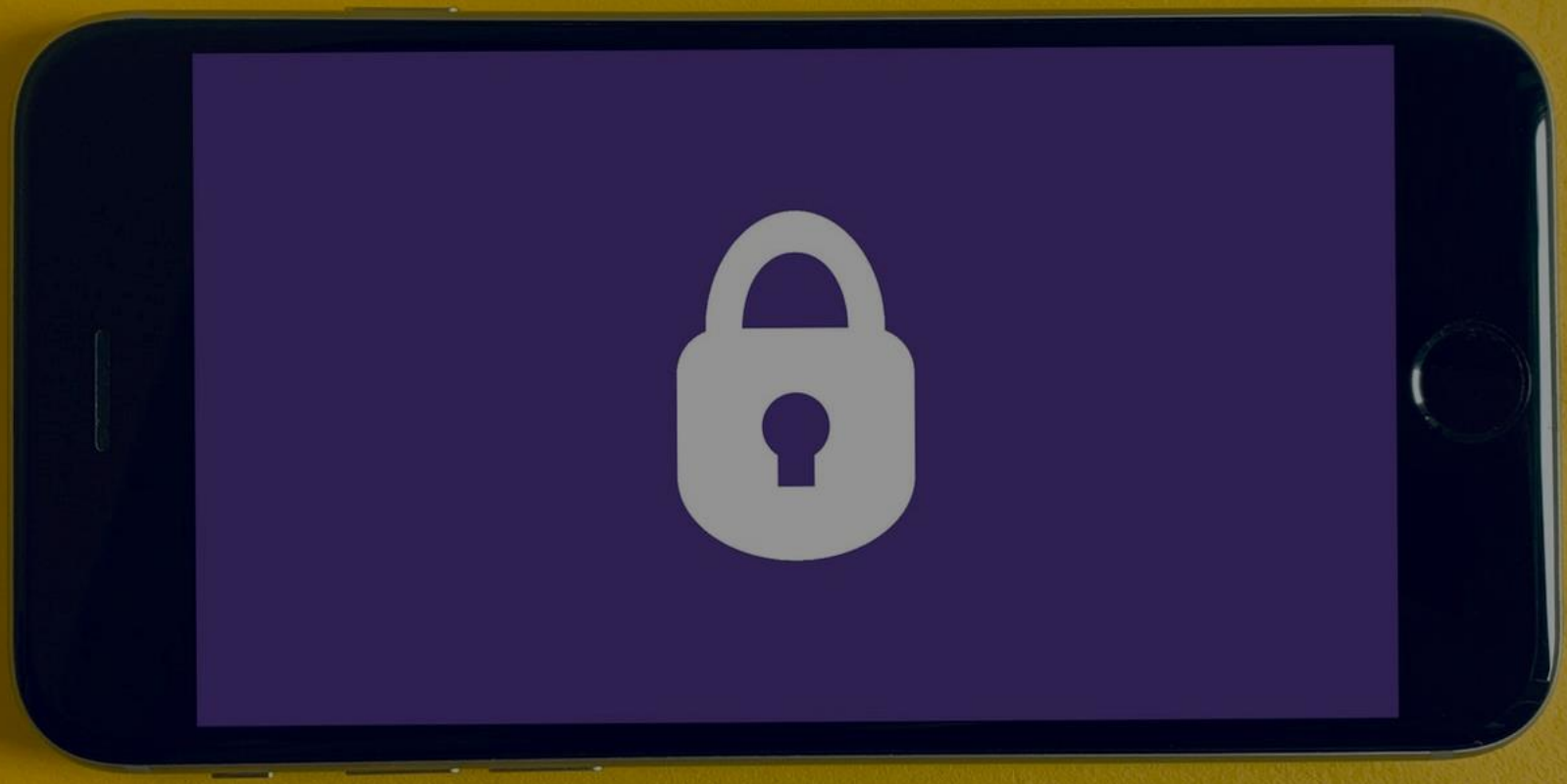


Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

SAML & SSO

Web Federated Login

Notes Federated Login

Traveler & SAML

Bonus – Nomad!

Troubleshooting

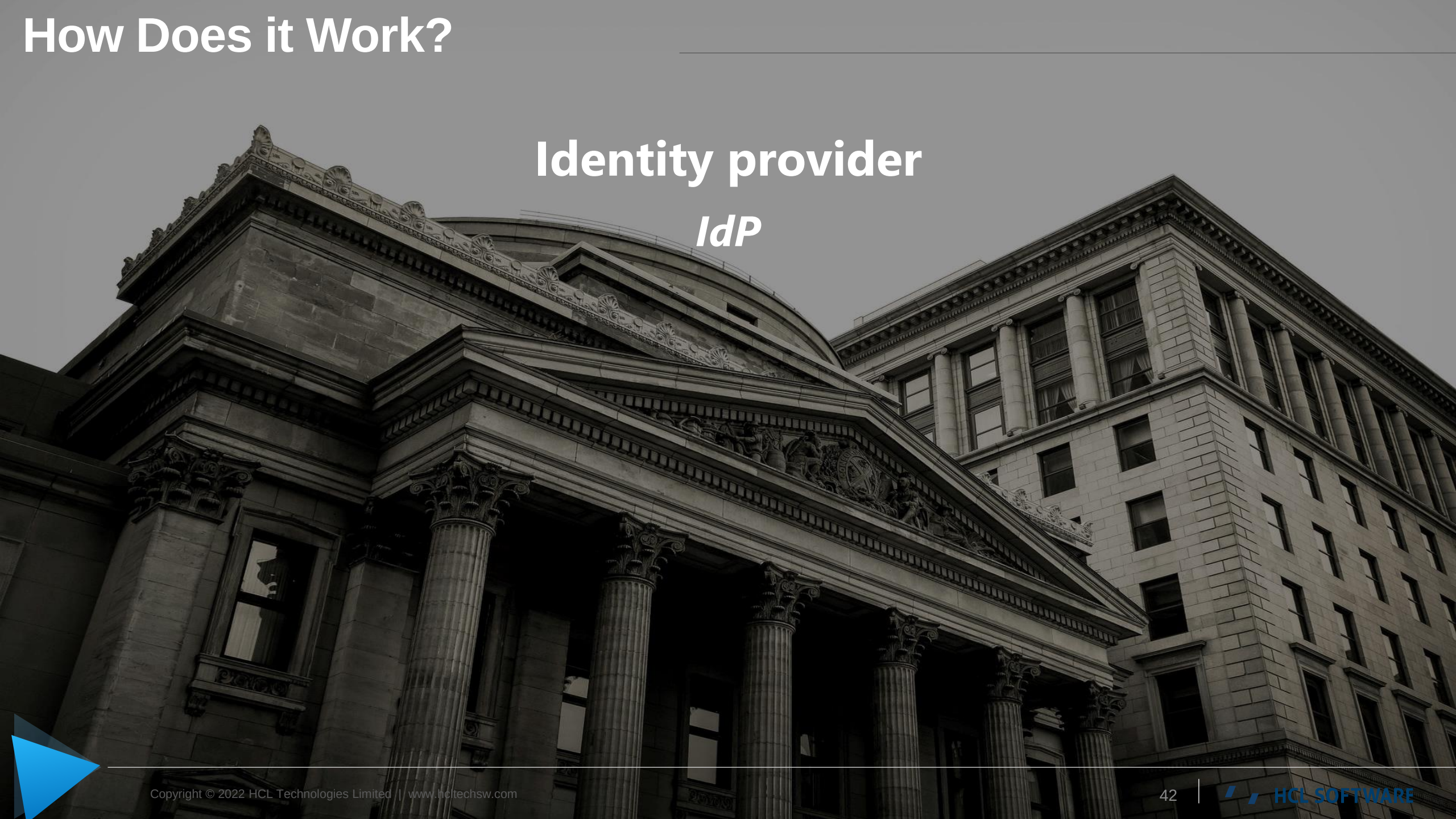
Issues

Q & A

Shibboleth

References

How Does it Work?



How Does it Work?

Service Provider (SP)

Relaying Party

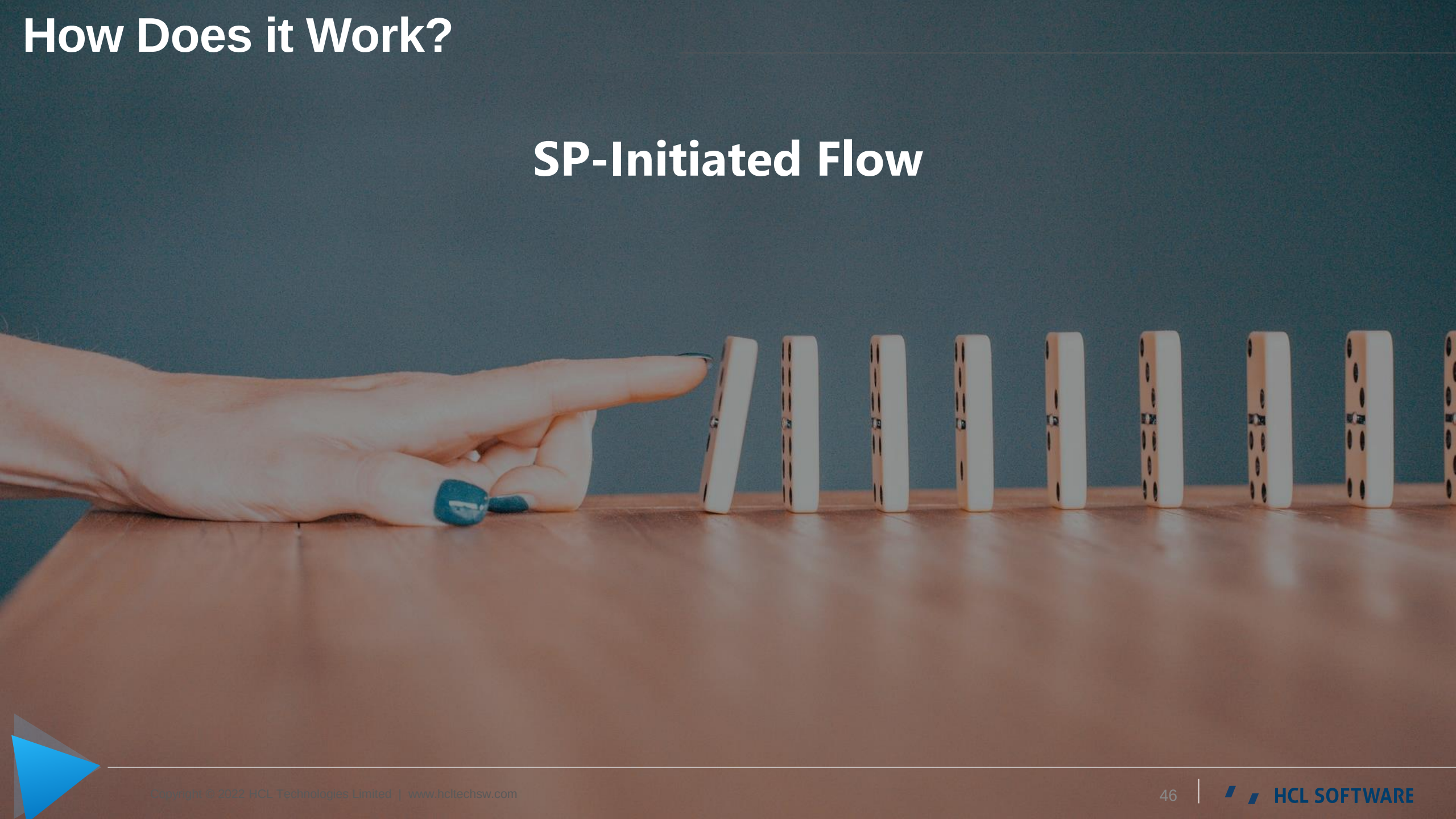
How Does it Work?

SAML assertion

HCL SOFTWARE

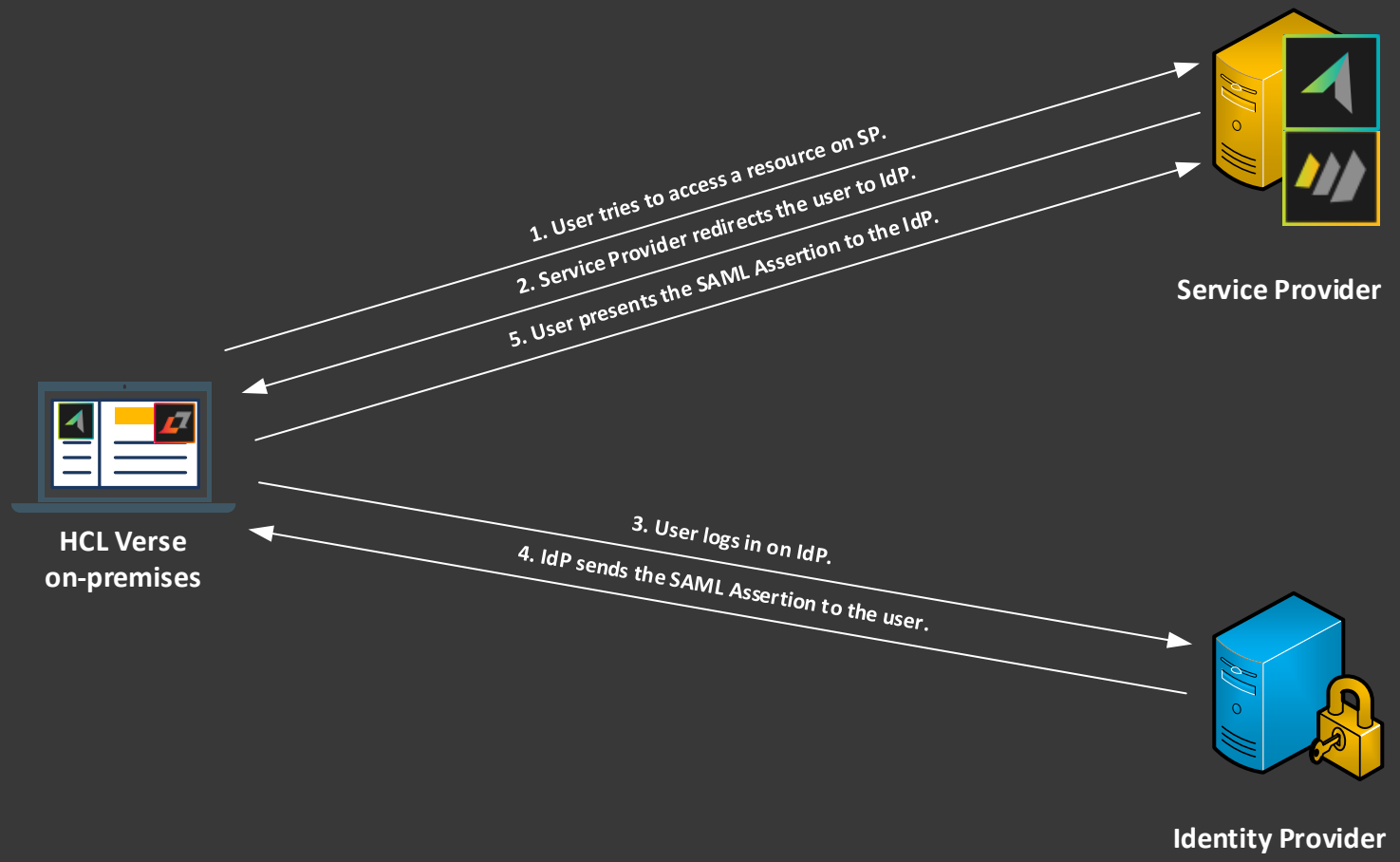
How Does it Work?

SP-Initiated Flow



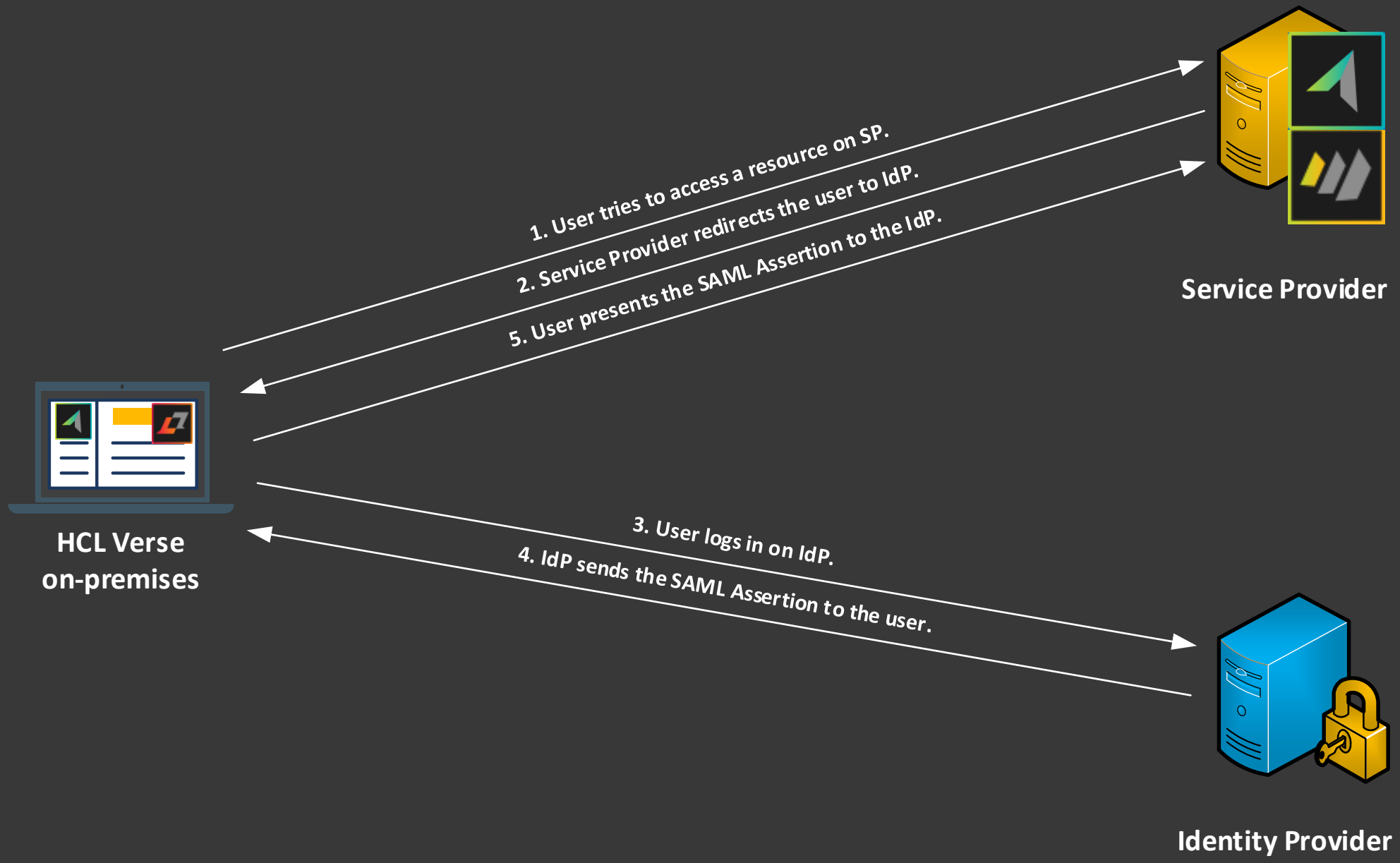
How Does it Work?

SP-Initiated Flow



HCL SOFTWARE

How Does it Work?



HCL SOFTWARE

Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

SAML & SSO

Web Federated Login

Notes Federated Login

Traveler & SAML

Bonus – Nomad!

Troubleshooting

Issues

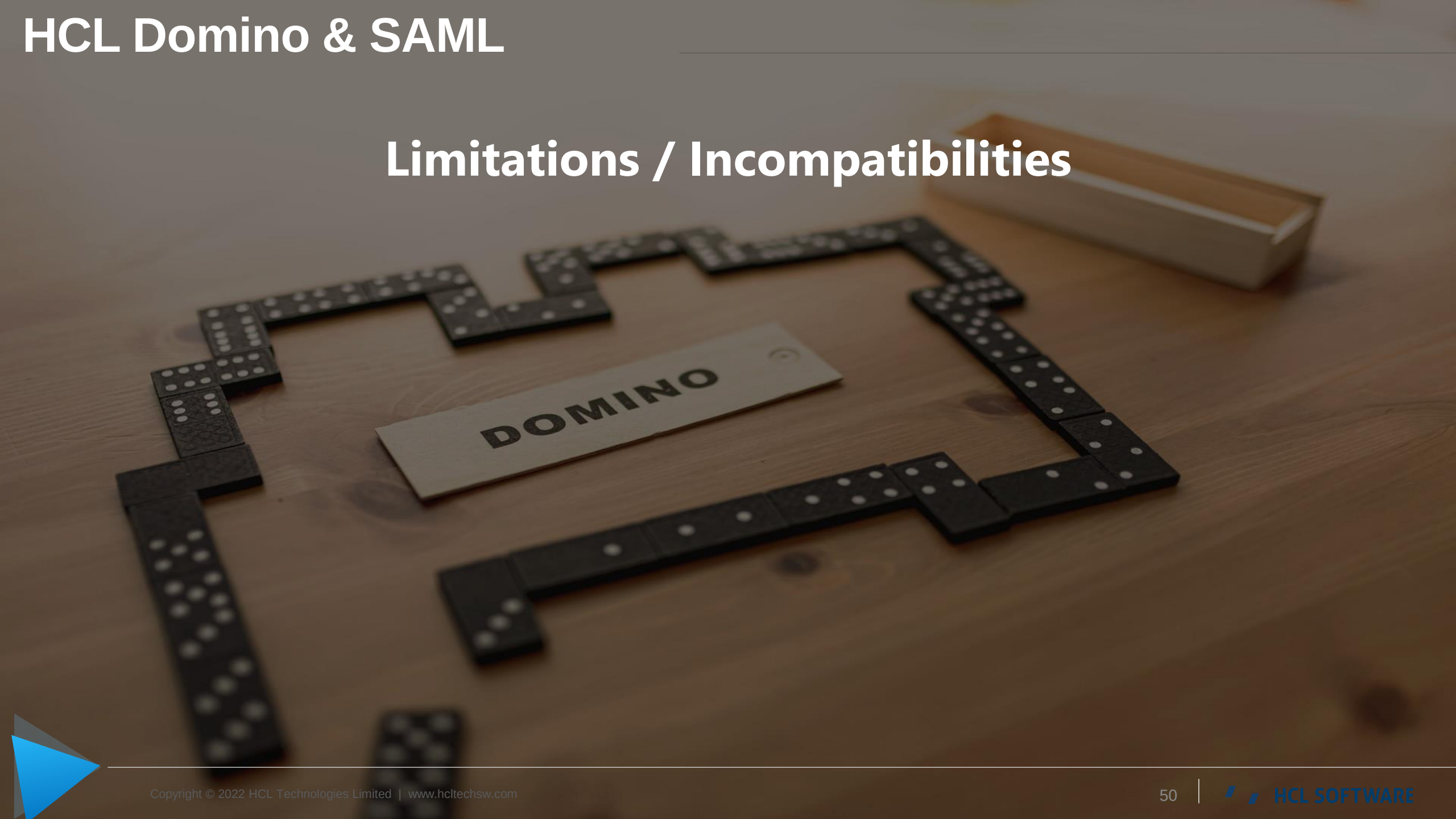
Q & A

Shibboleth

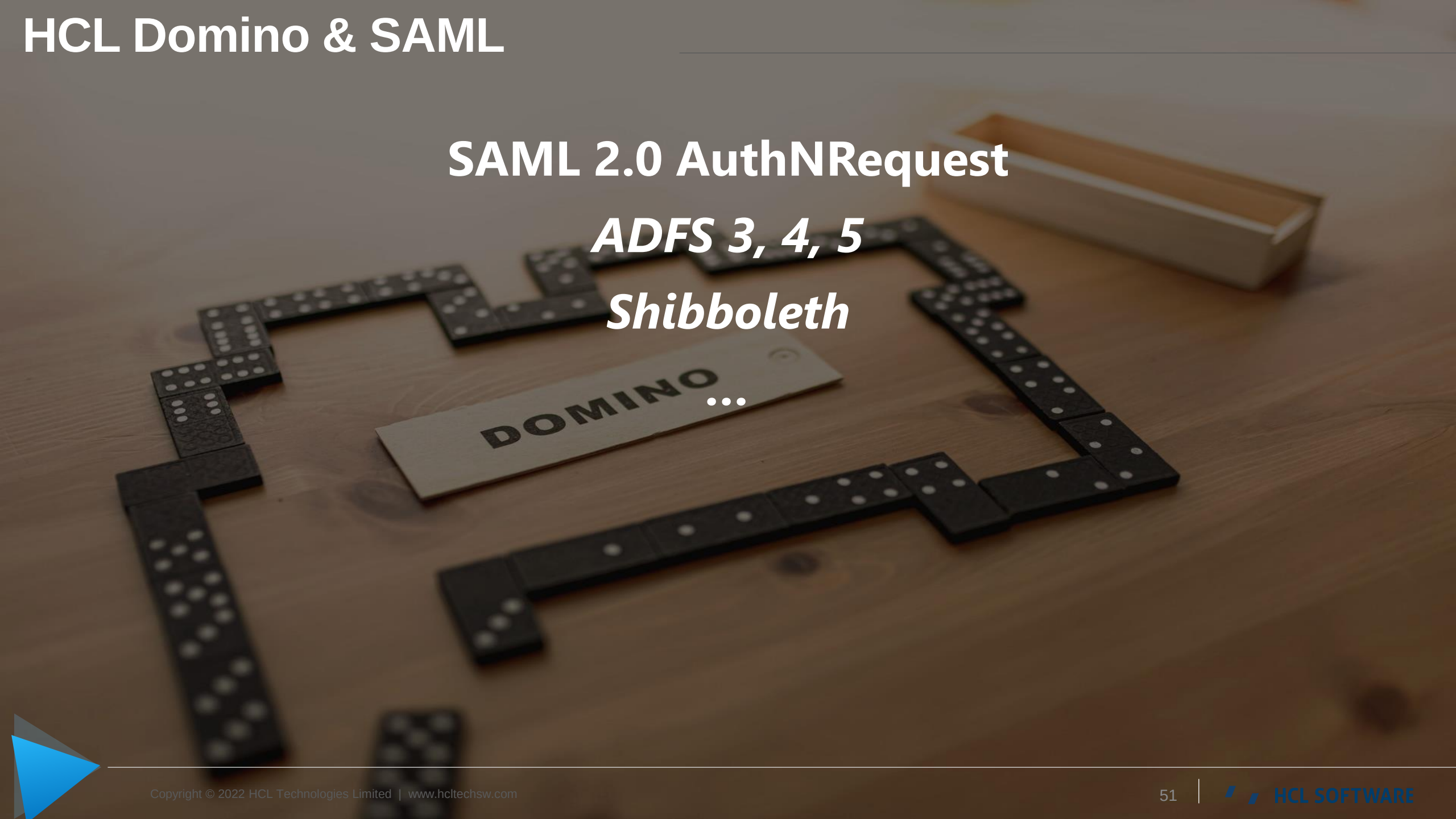
References

HCL Domino & SAML

Limitations / Incompatibilities



HCL Domino & SAML



SAML 2.0 AuthNRequest

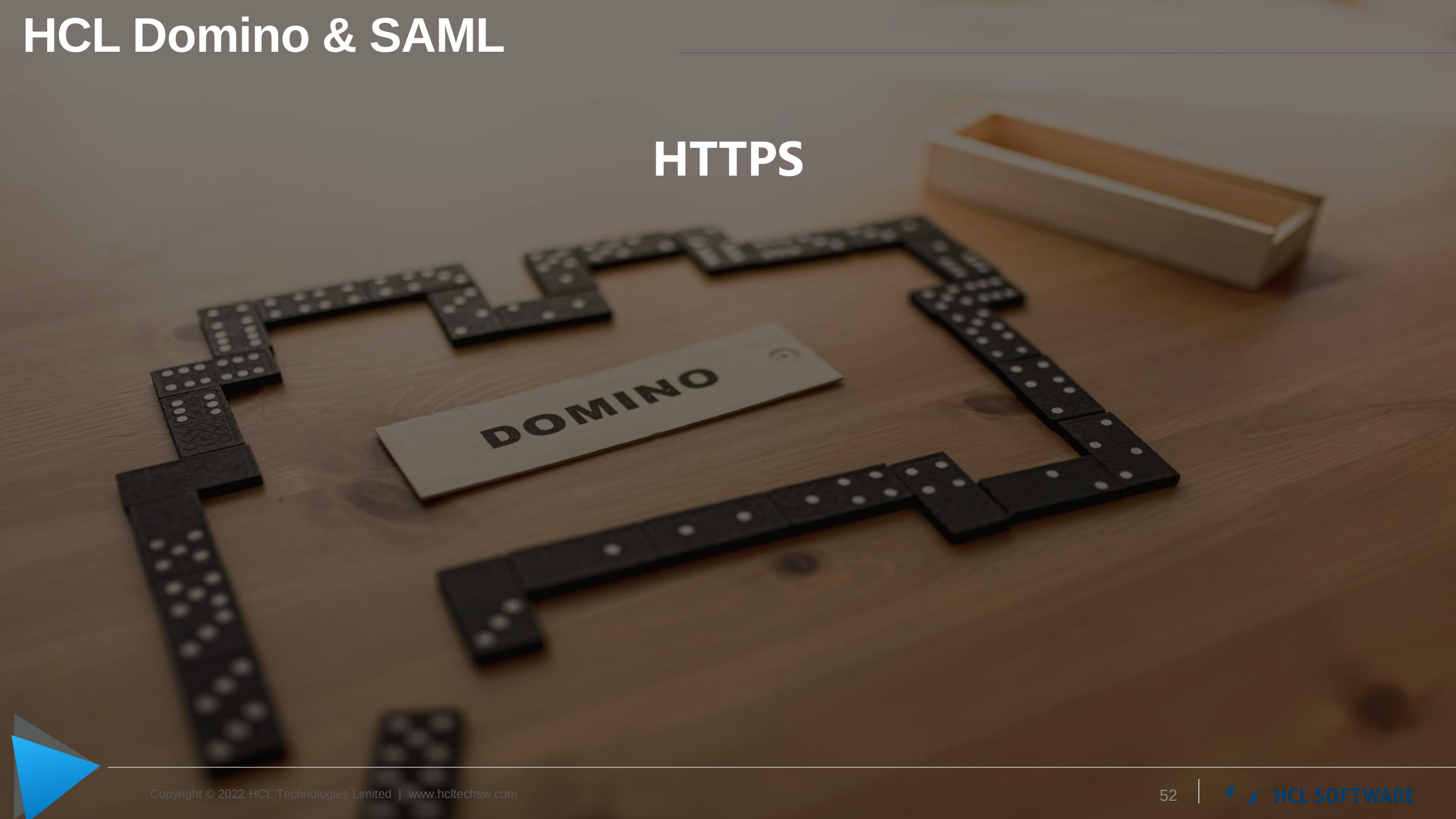
ADFS 3, 4, 5

Shibboleth

…

HCL Domino & SAML

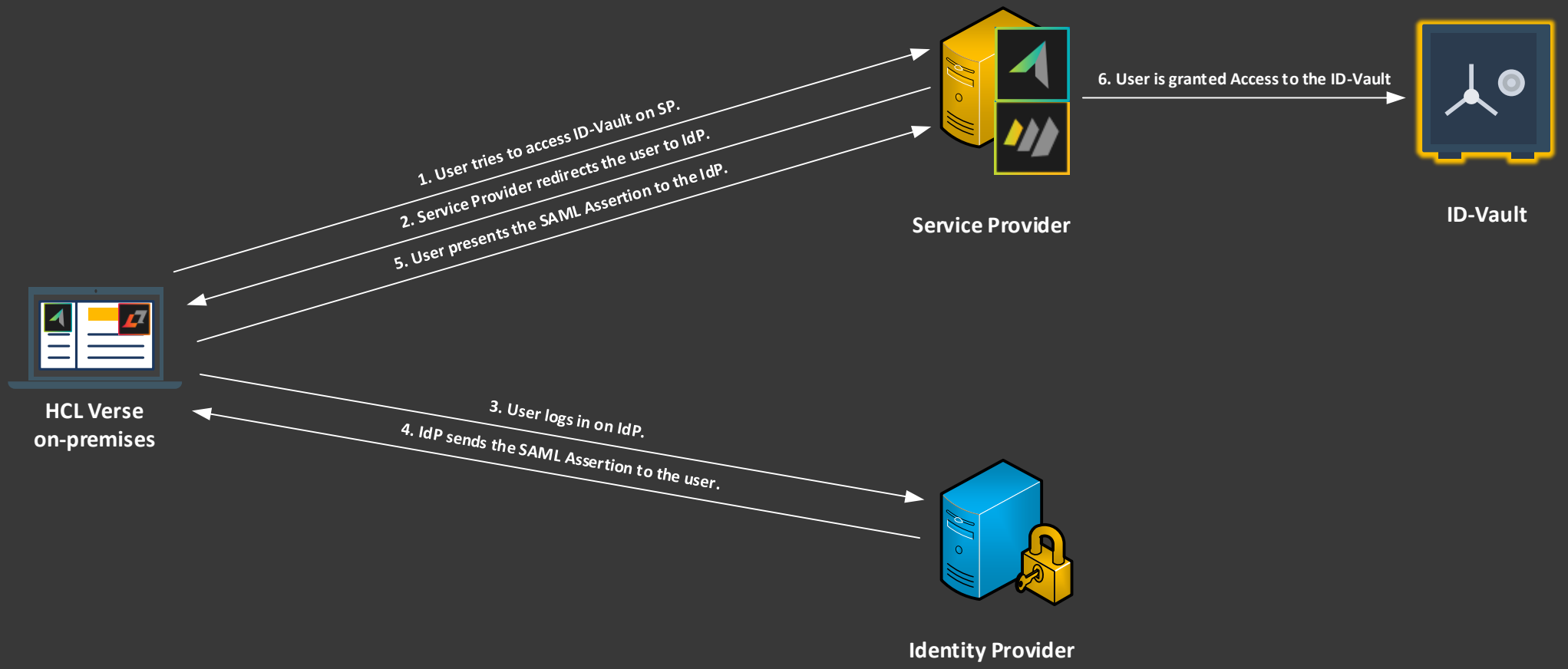
HTTPS



HCL SOFTWARE

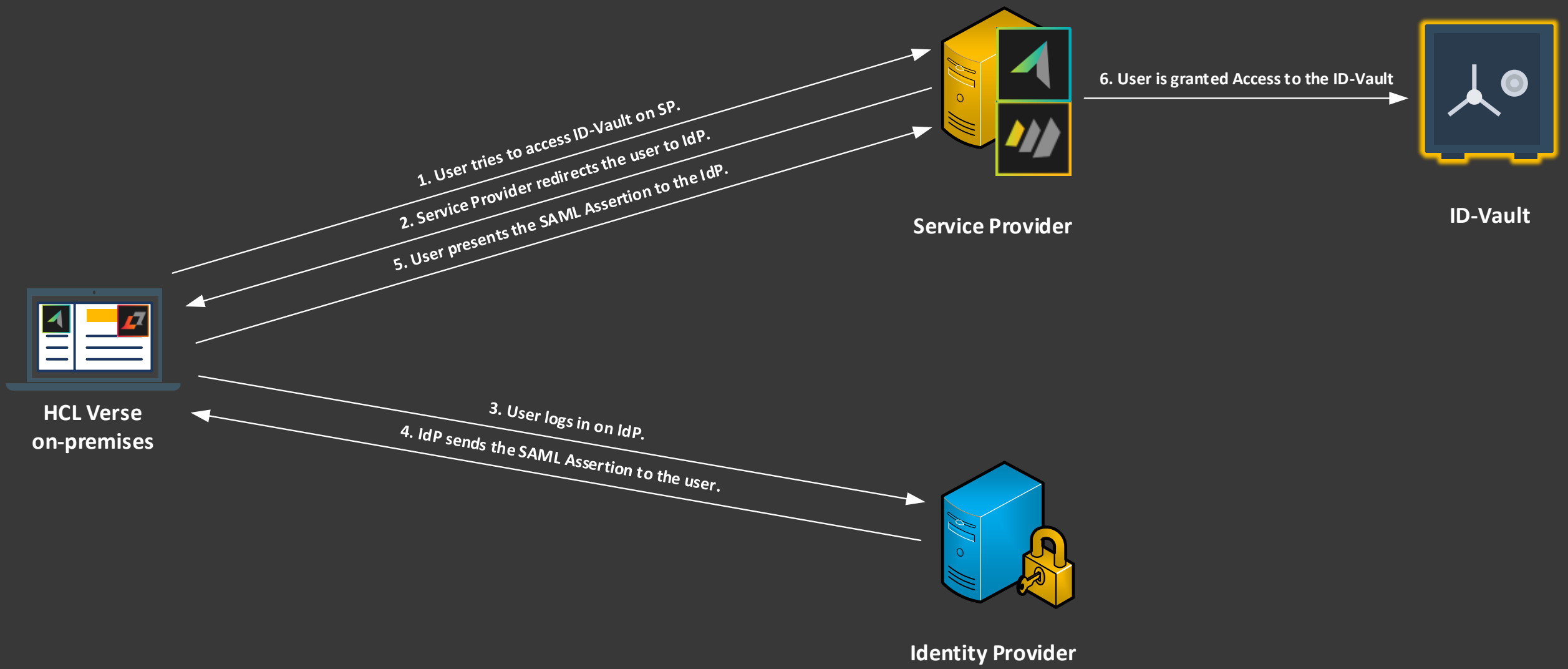
HCL Domino & SAML

Web Federated Login



HCL SOFTWARE

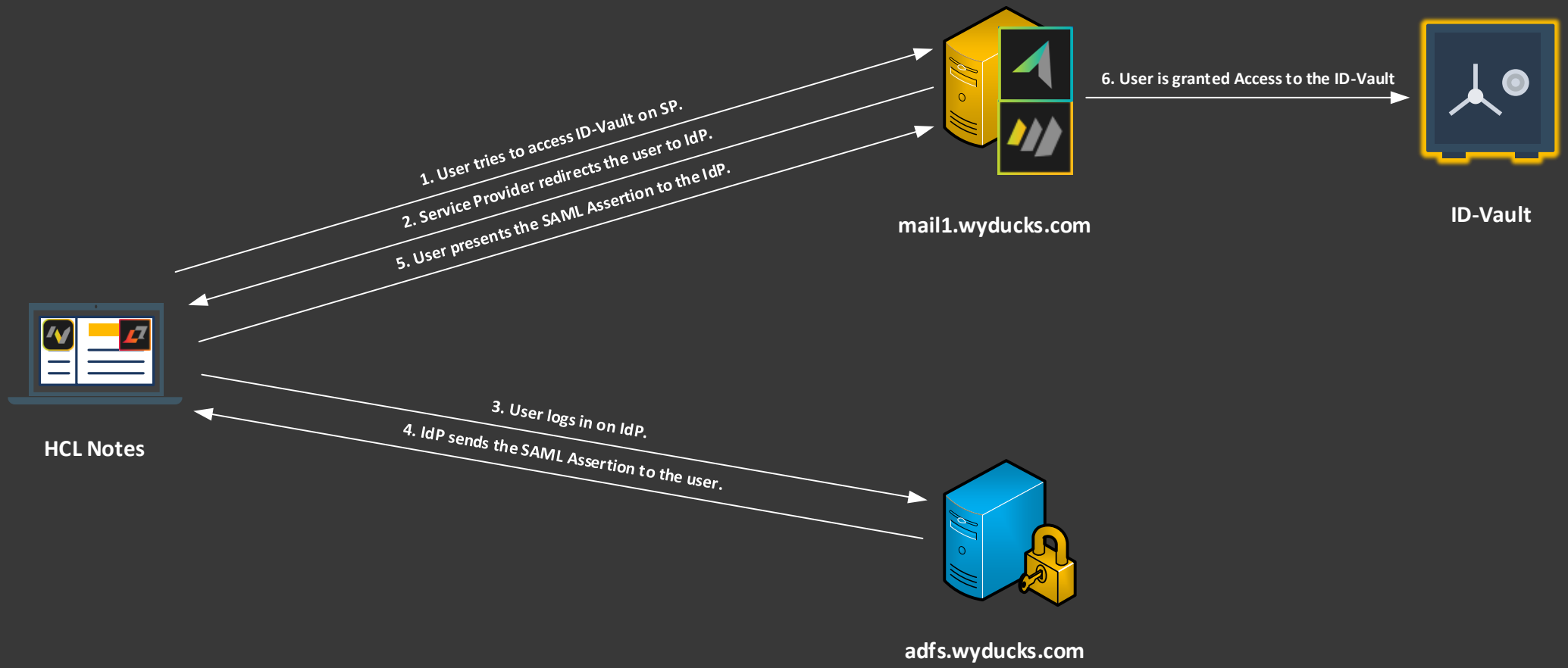
HCL Domino & SAML



HCL SOFTWARE

HCL Domino & SAML

Notes Federated Login



HCL SOFTWARE

HCL Domino & SAML

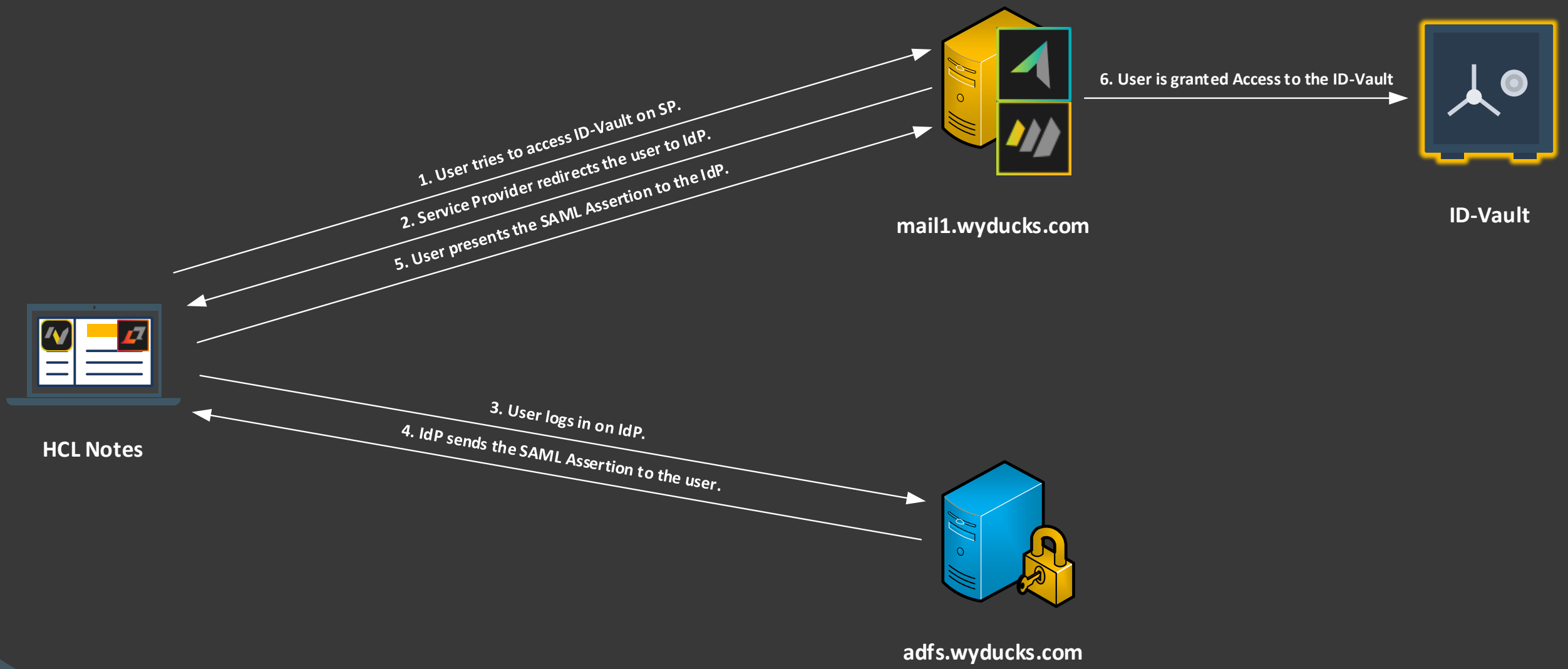


Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

SAML & SSO

Web Federated Login

Notes Federated Login

Traveler & SAML

Bonus – Nomad!

Troubleshooting

Issues

Q & A

Shibboleth

References

Prerequisites

Time Sync

Prerequisites

DNS

HCL SOFTWARE

Prerequisites

HCL Domino 12.0.1 FP1

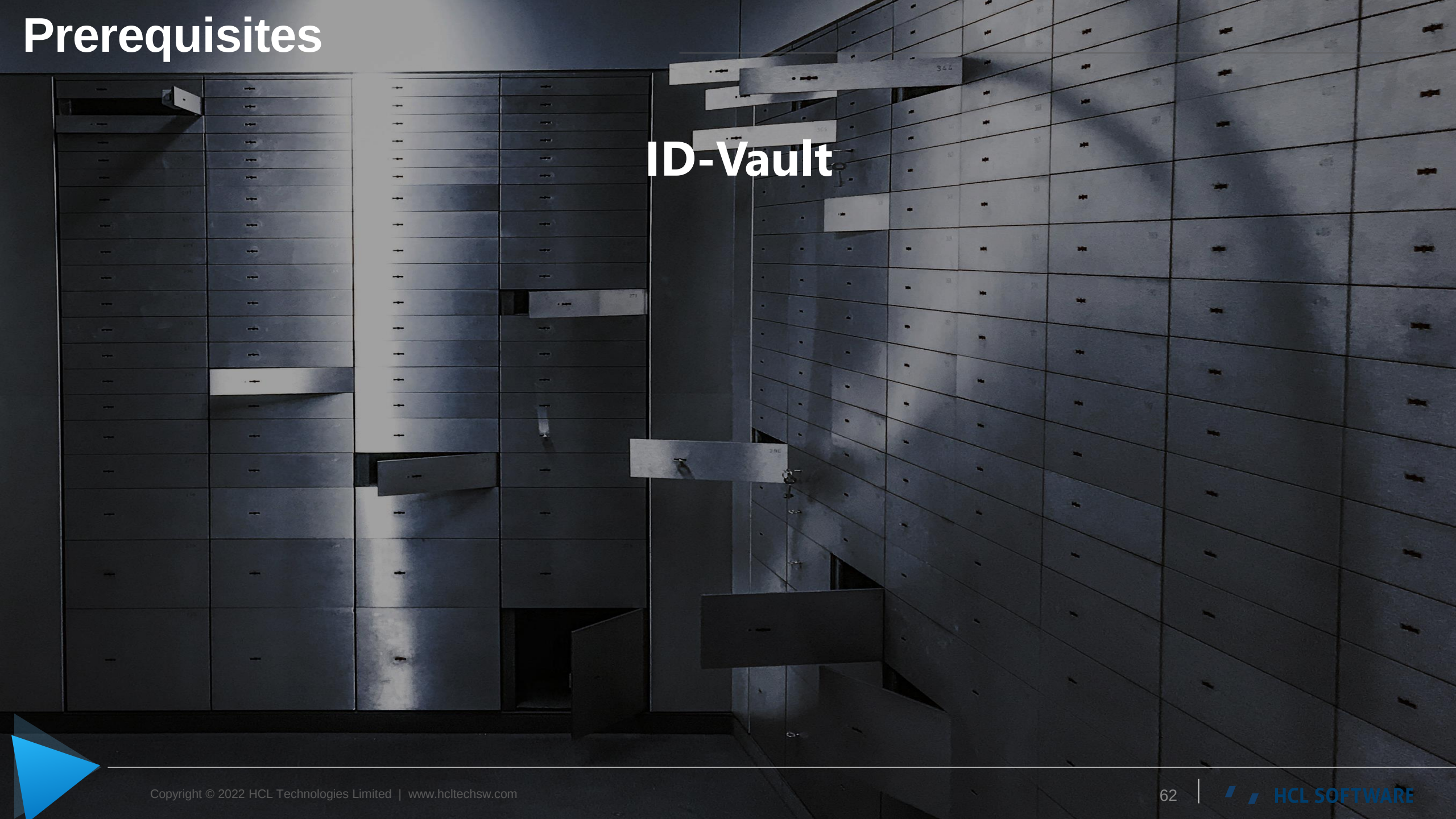
Incl. latest Templates

Prerequisites

Public TLS Certificate

Domino Certificate Manager

Prerequisites



ID-Vault

Prerequisites

Domino / SAML specifics

Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

SAML & SSO

Web Federated Login

Notes Federated Login

Traveler & SAML

Bonus – Nomad!

Troubleshooting

Issues

Q & A

Shibboleth

References

Infrastructure Needed

Three use-cases

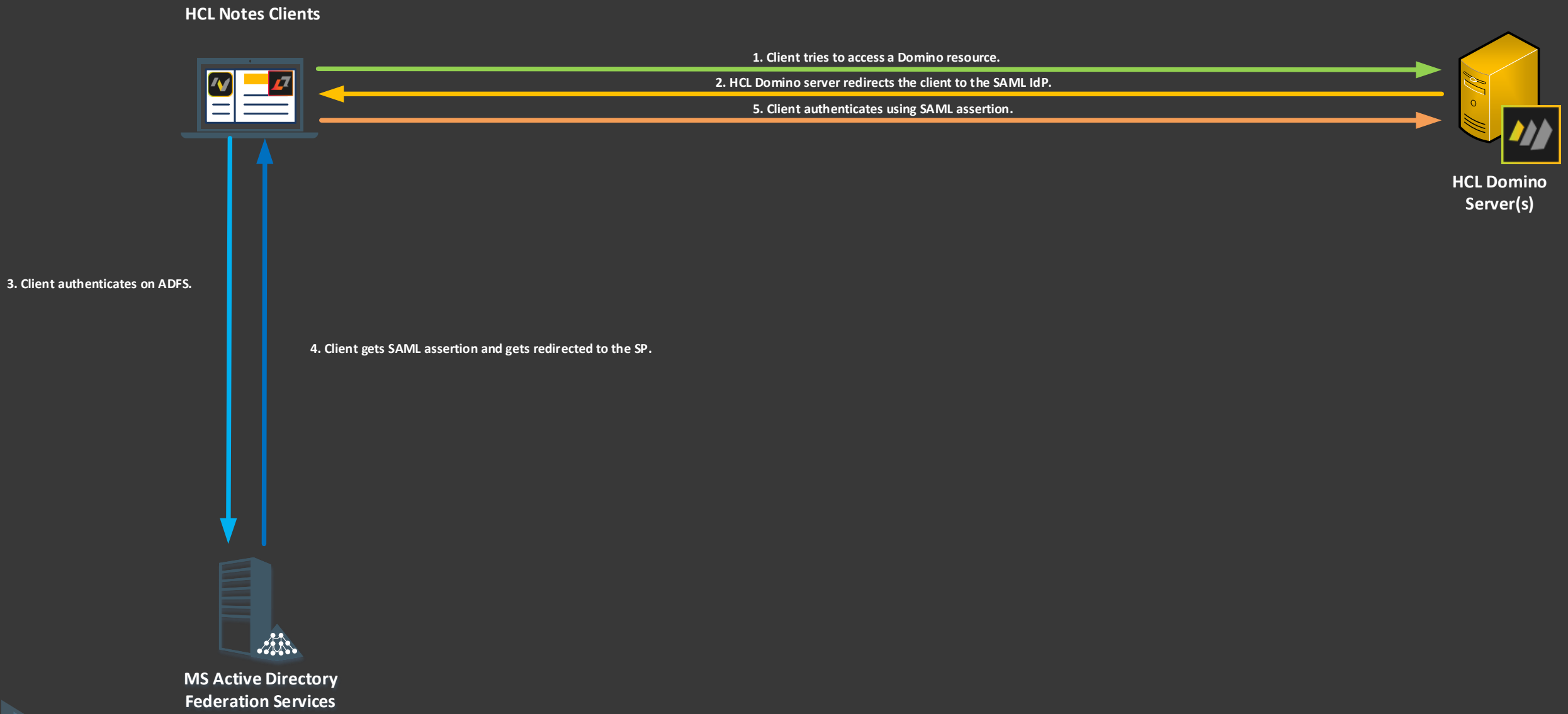
We are using MS ADFS

Infrastructure Needed

Notes clients

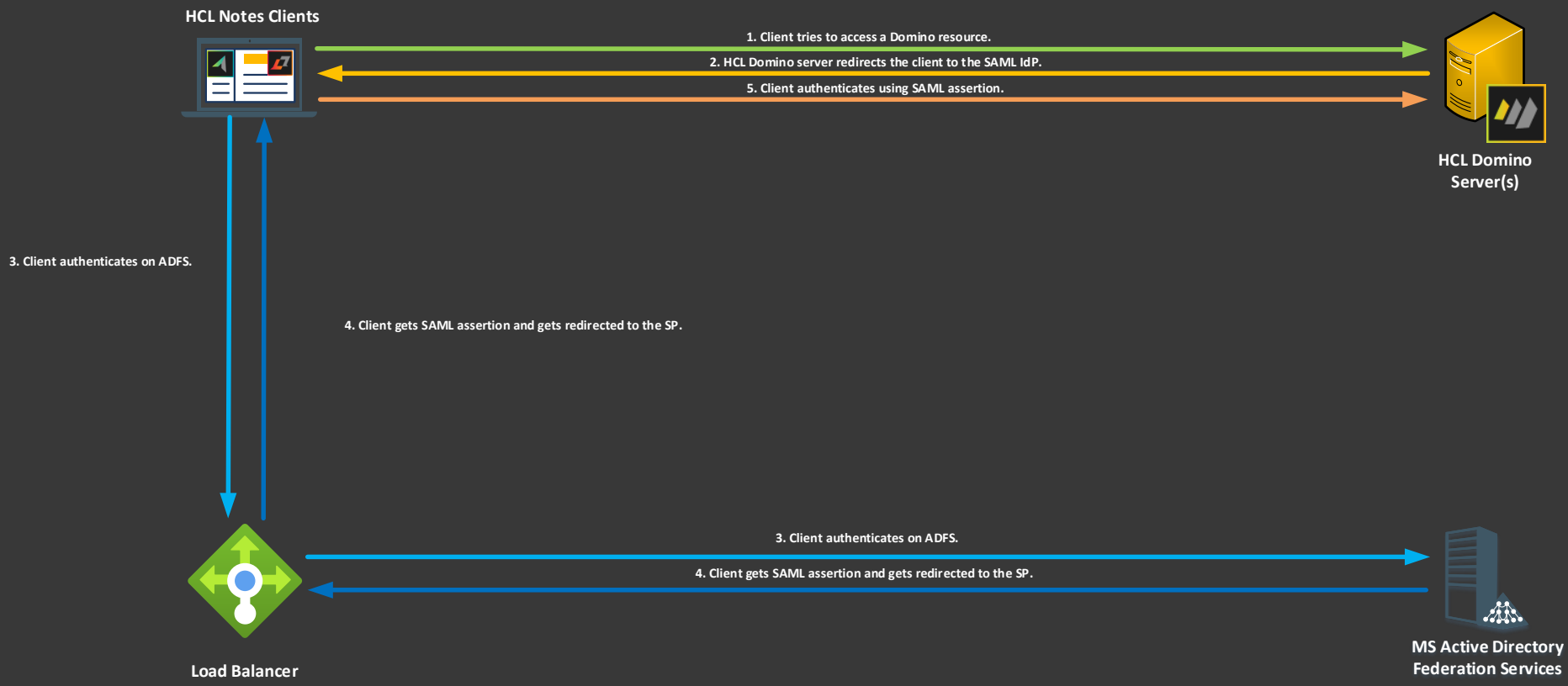
HCL SOFTWARE

Infrastructure Needed



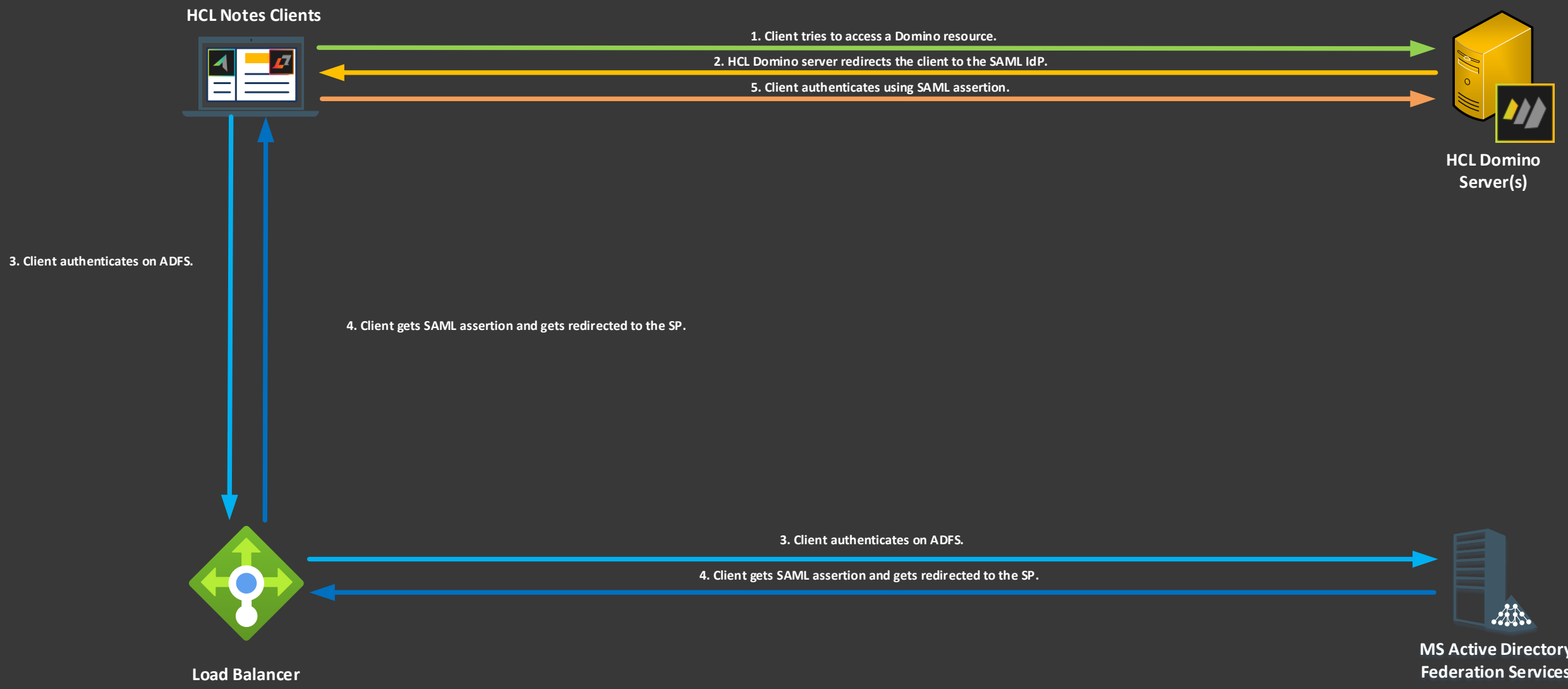
Enterprise Grade Infrastructure

Notes clients



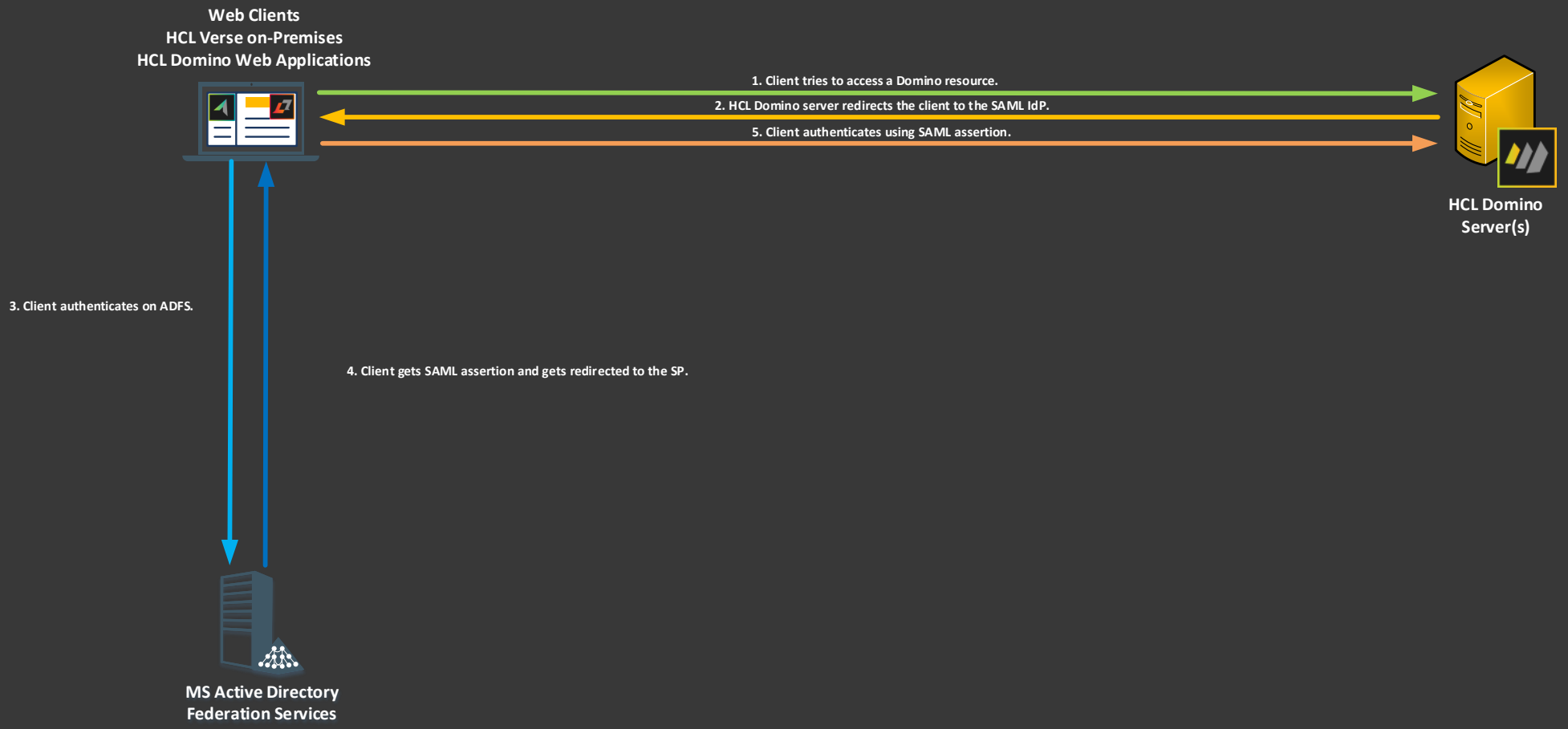
HCL SOFTWARE

Enterprise Grade Infrastructure

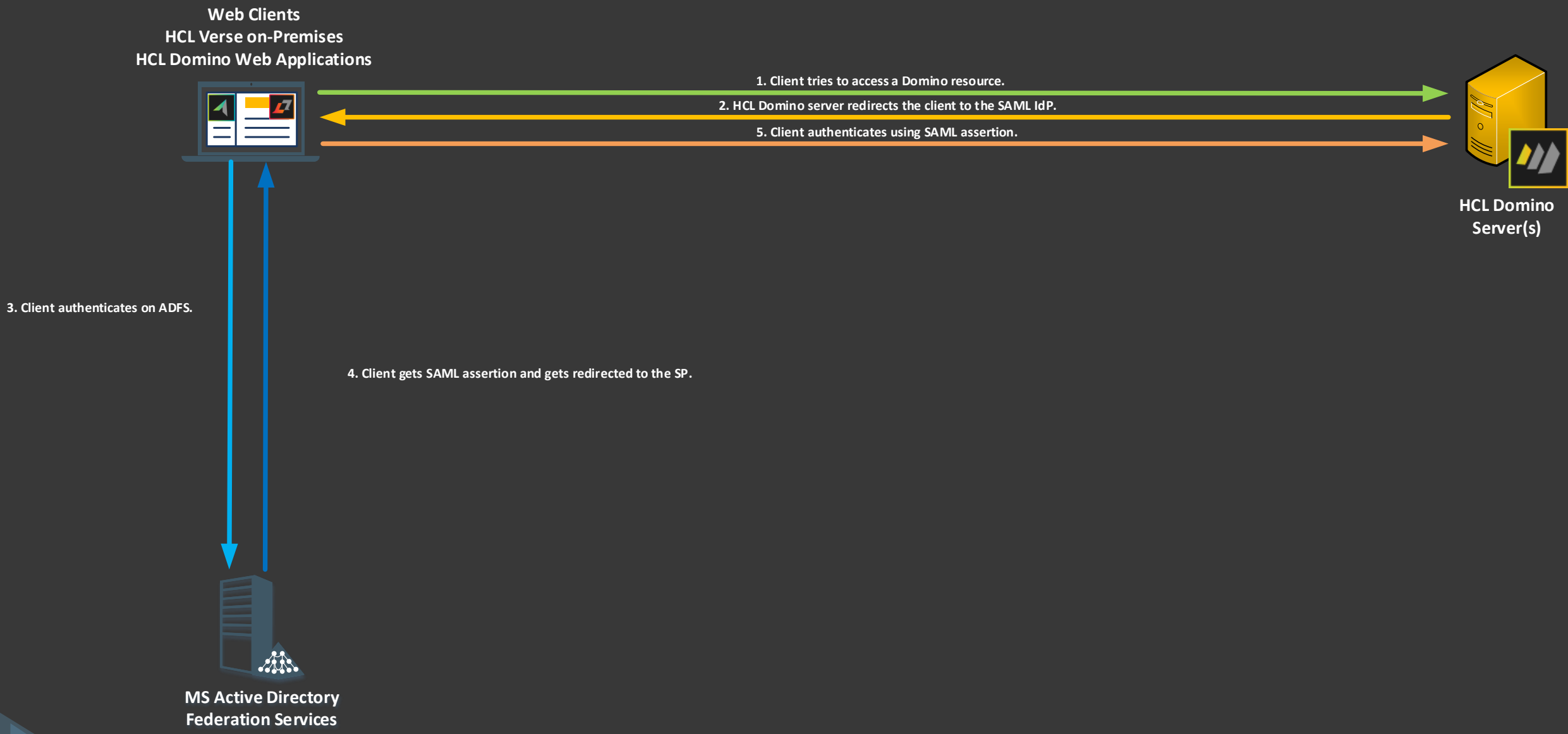


Infrastructure Needed

Internal web clients

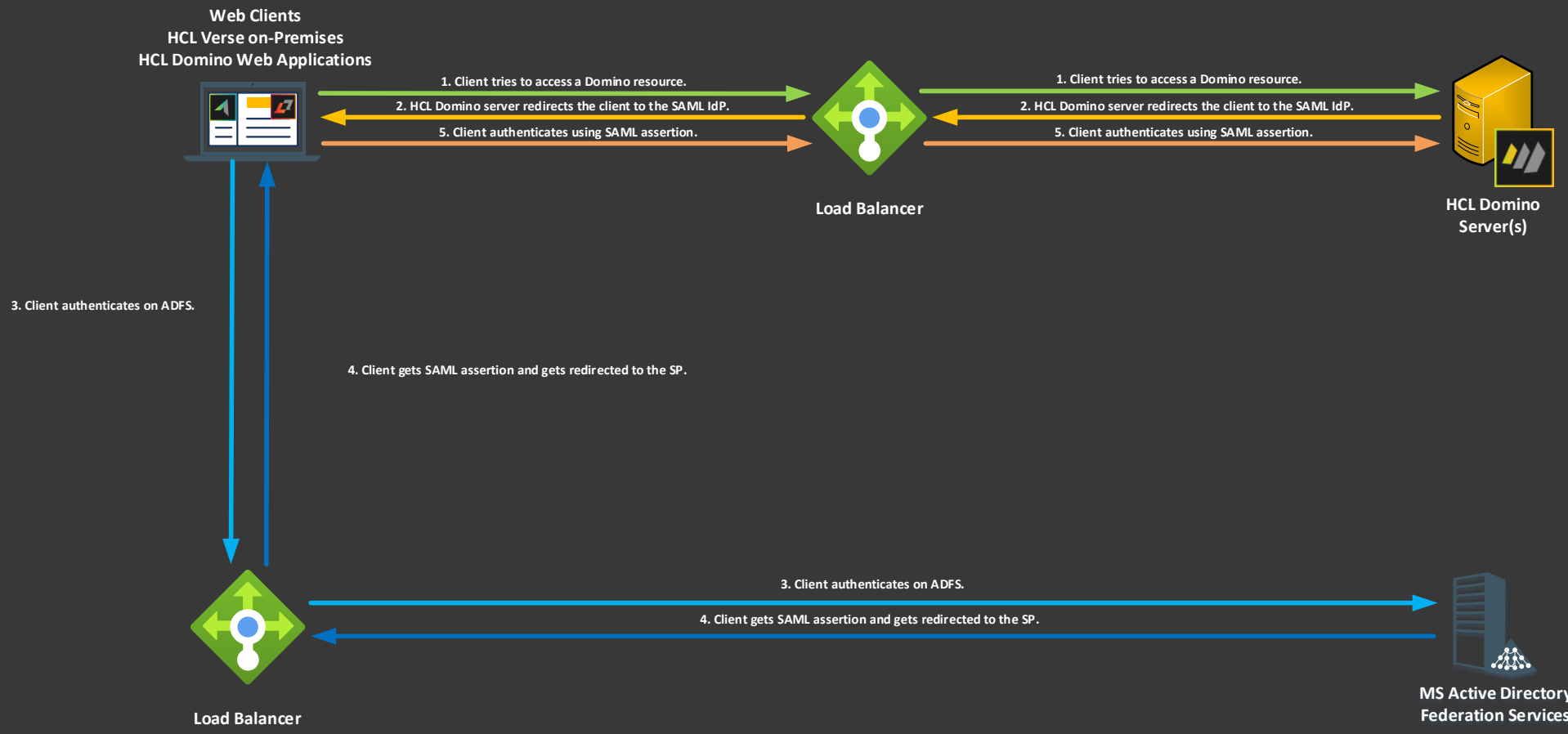


Infrastructure Needed



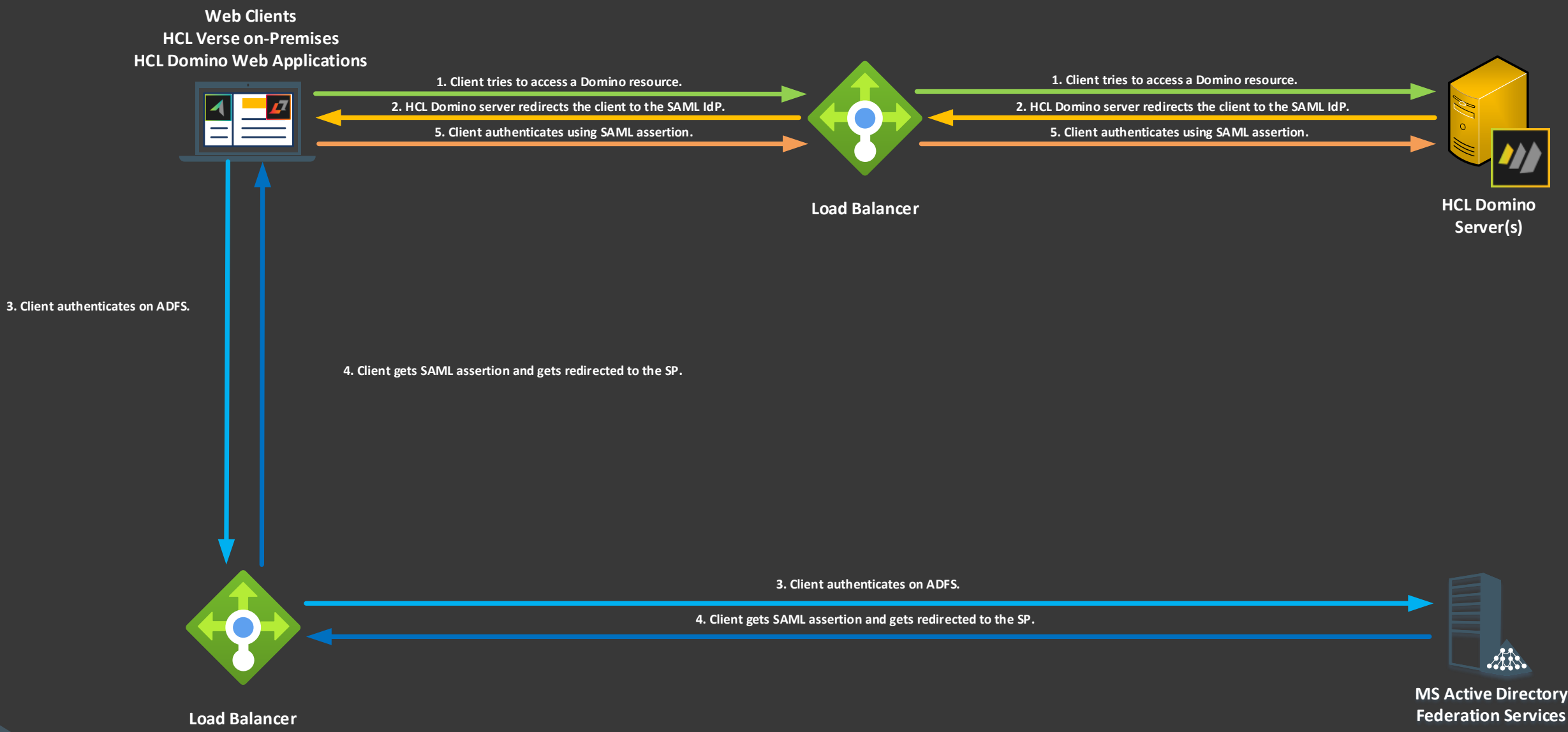
Enterprise Grade Infrastructure

Internal web clients



HCL SOFTWARE

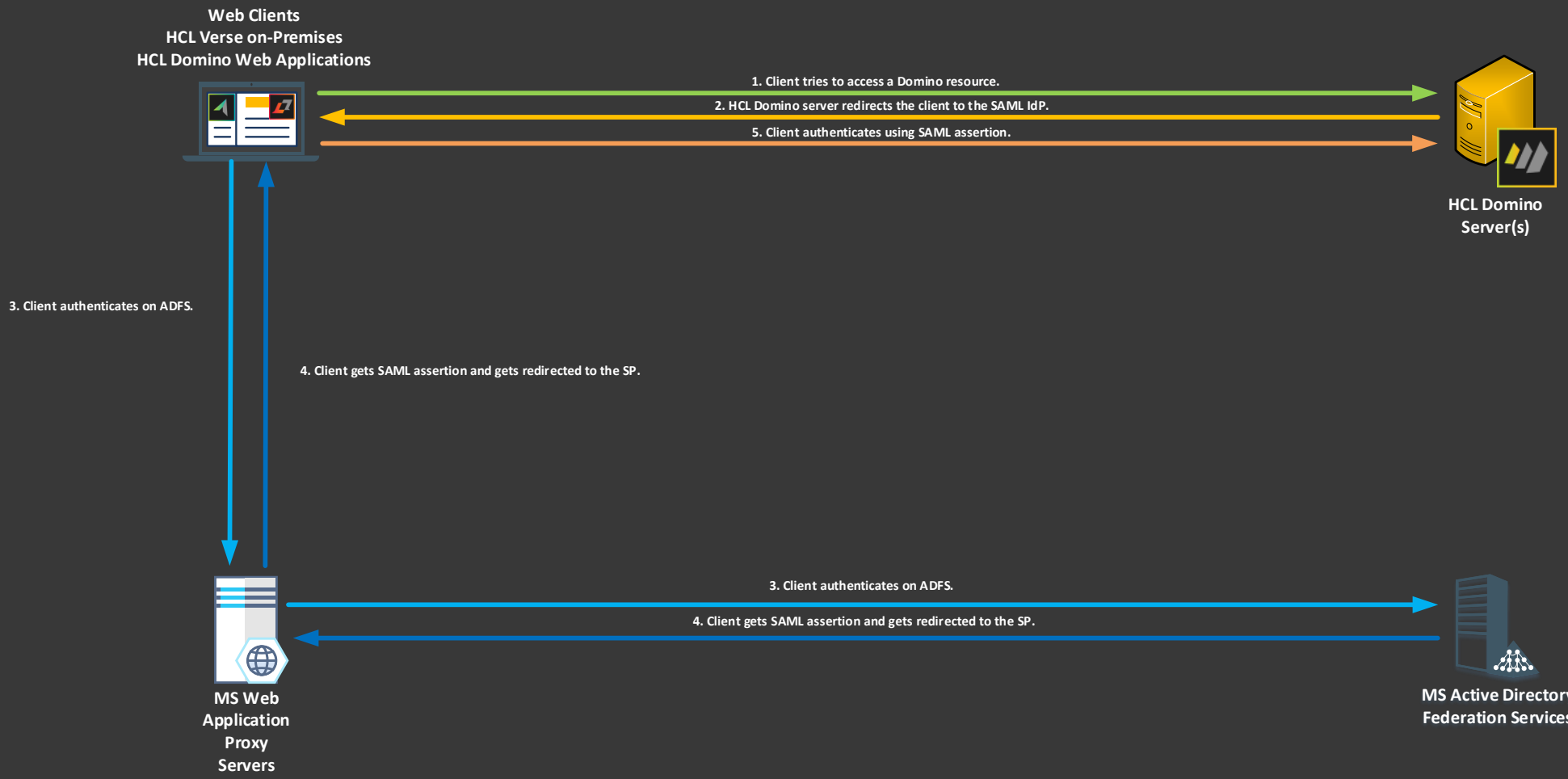
Enterprise Grade Infrastructure



HCL SOFTWARE

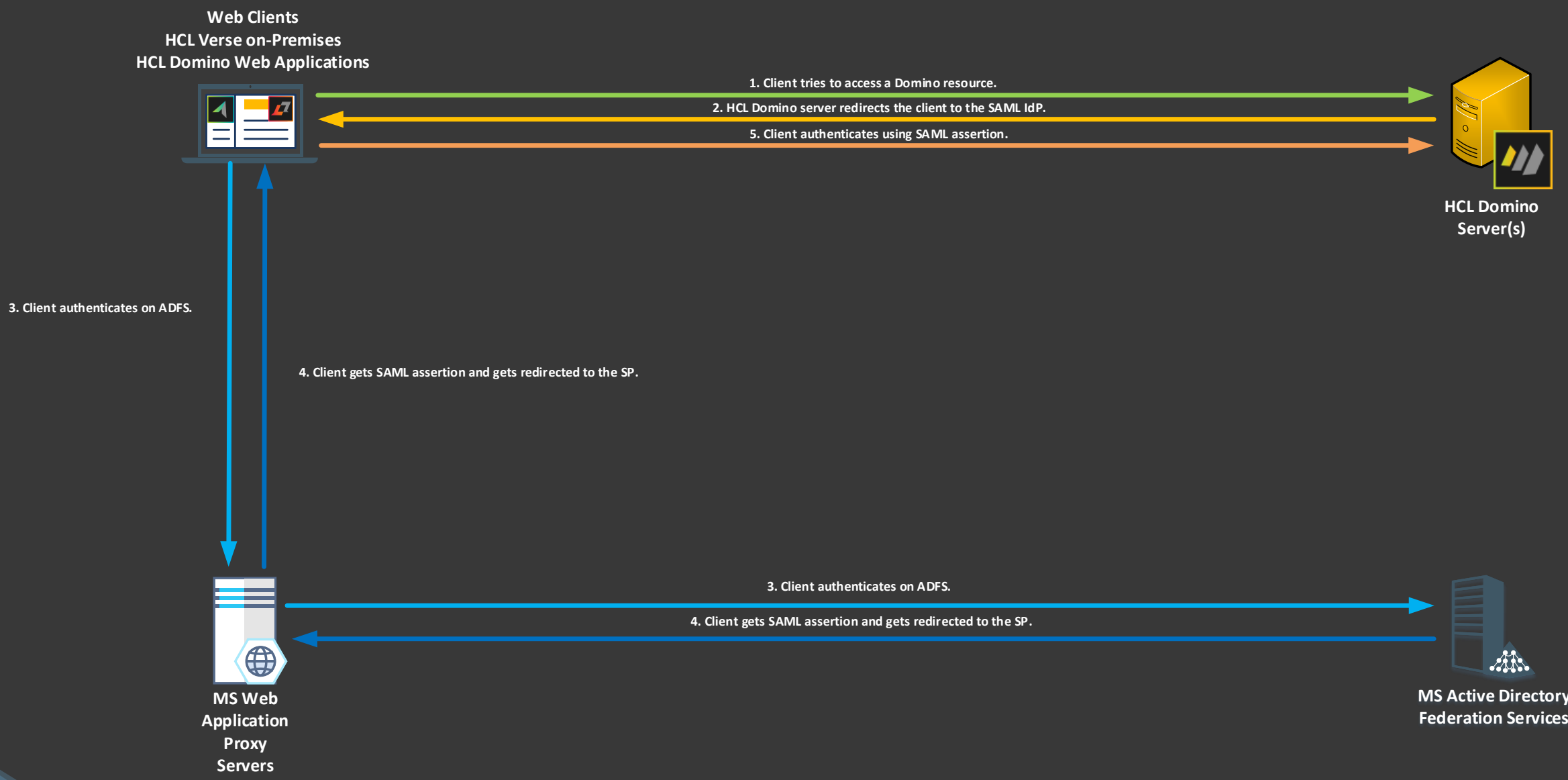
Infrastructure Needed

External web clients



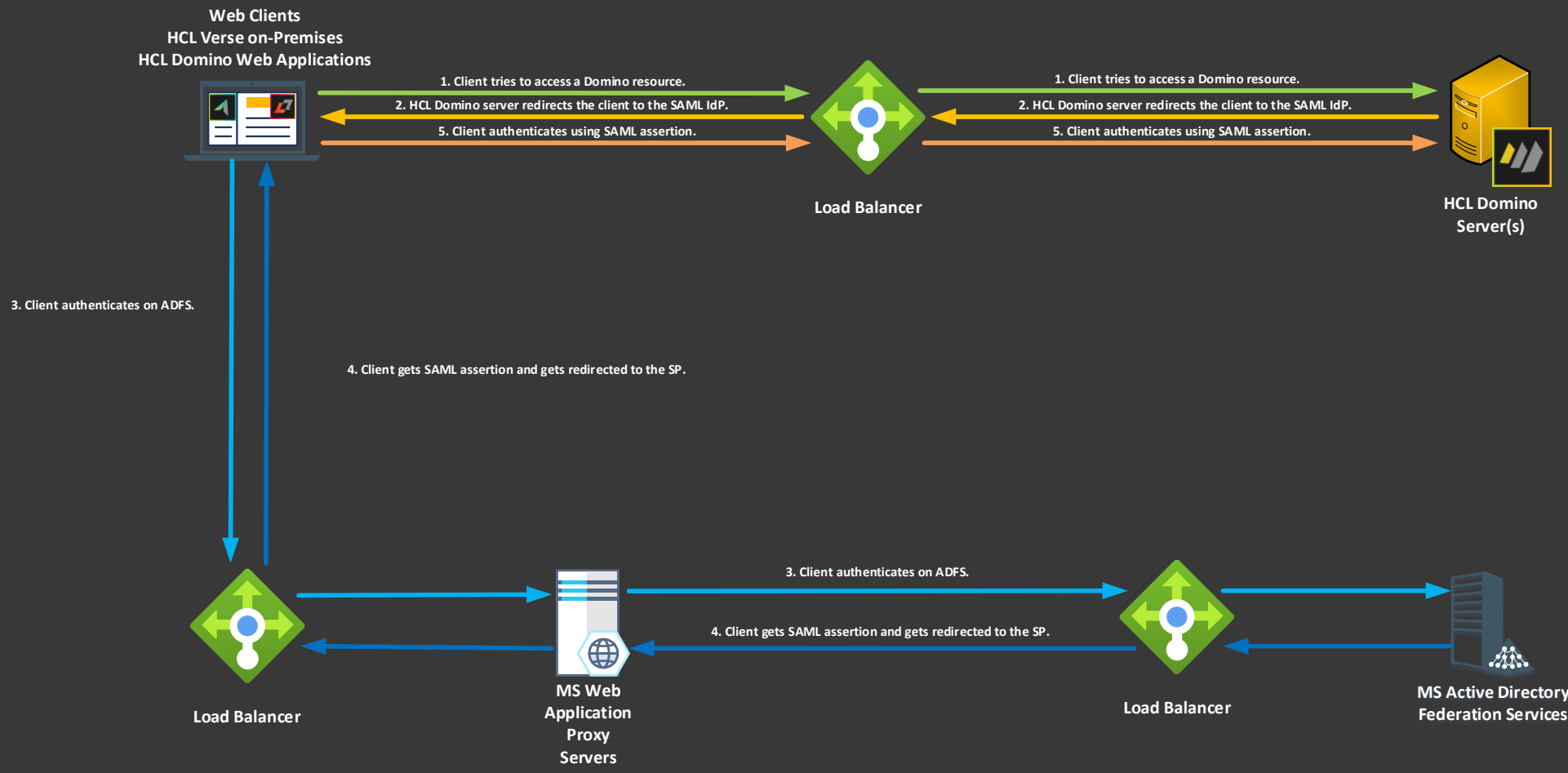
HCL SOFTWARE

Infrastructure Needed



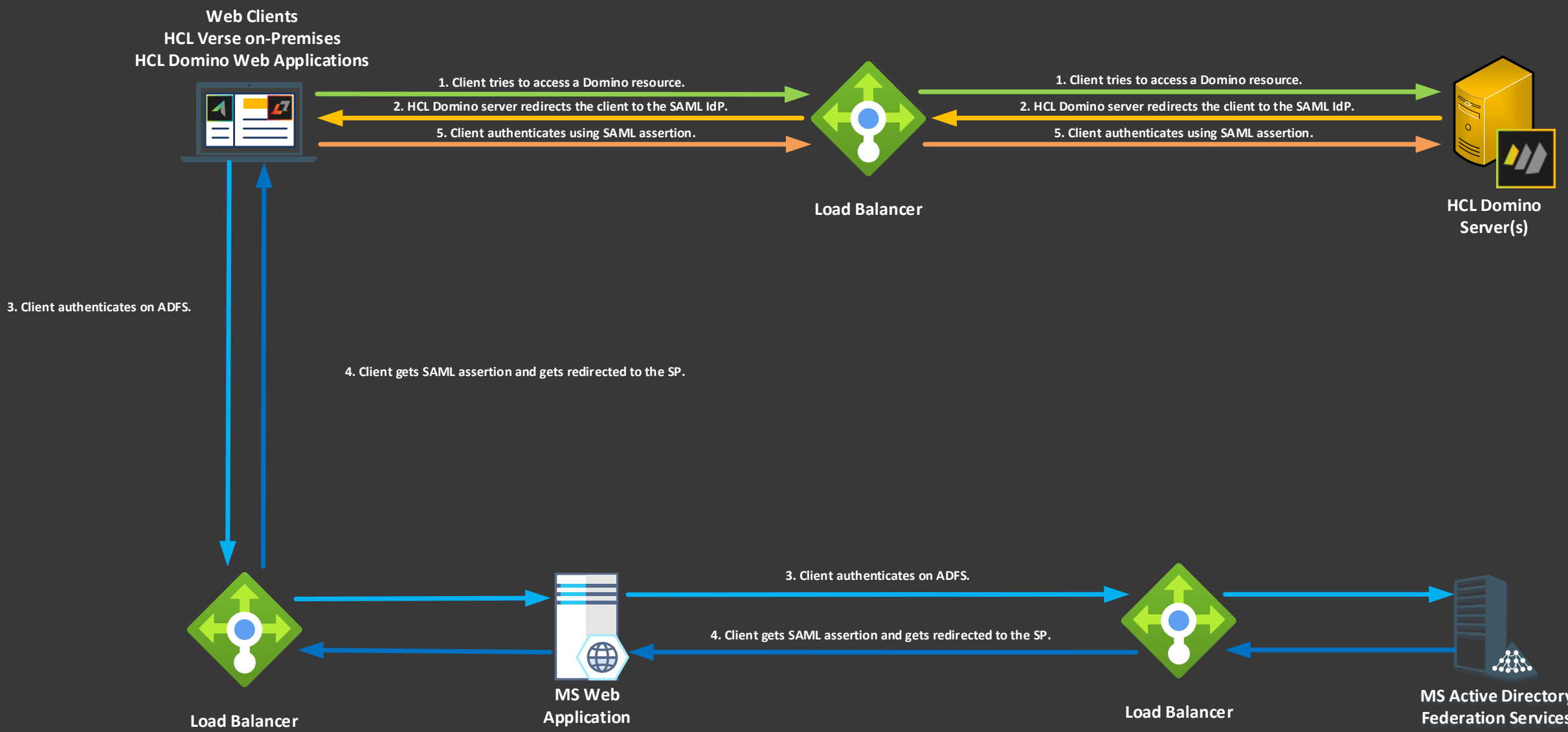
Enterprise Grade Infrastructure

External web clients



HCL SOFTWARE

Enterprise Grade Infrastructure



HCL SOFTWARE

Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

SAML & SSO

Web Federated Login

Notes Federated Login

Traveler & SAML

Bonus – Nomad!

Troubleshooting

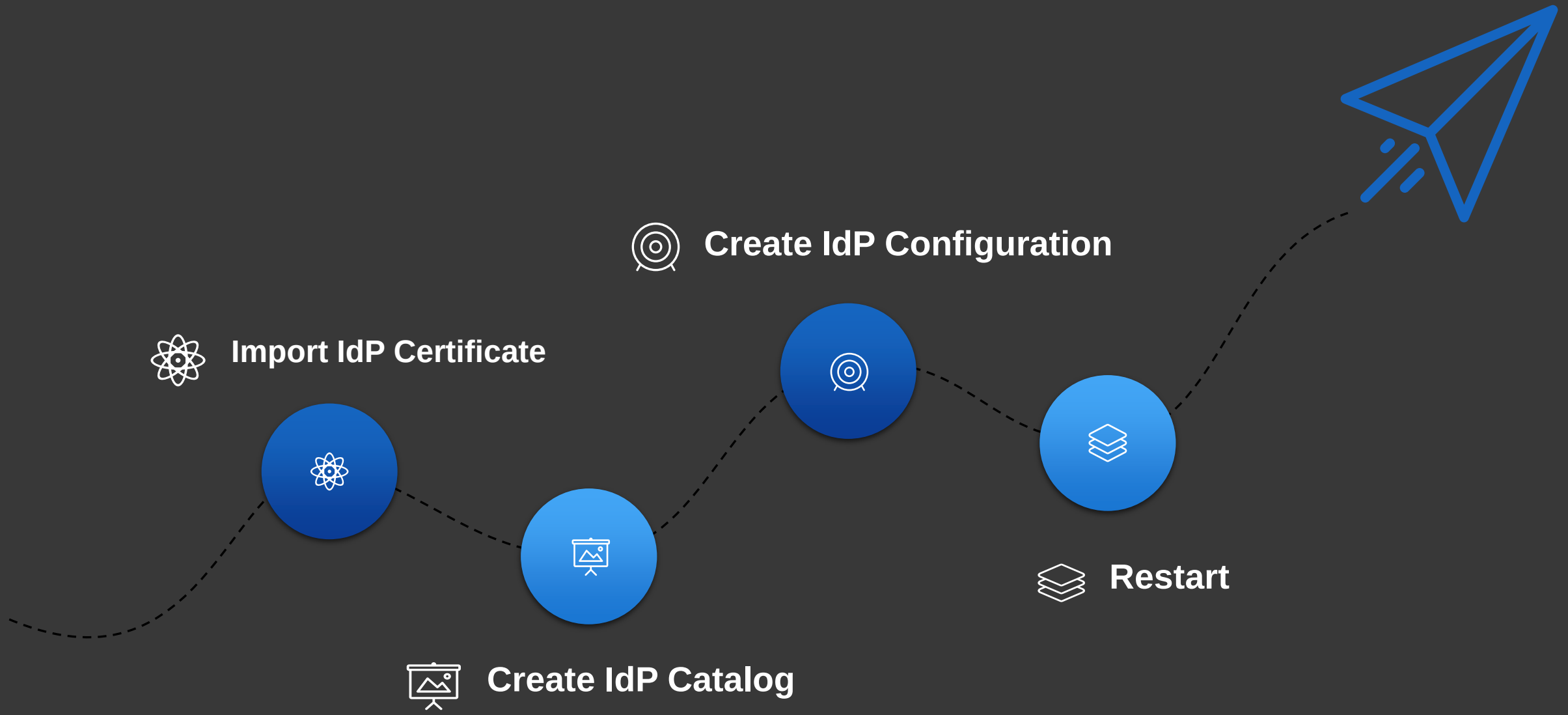
Issues

Q & A

Shibboleth

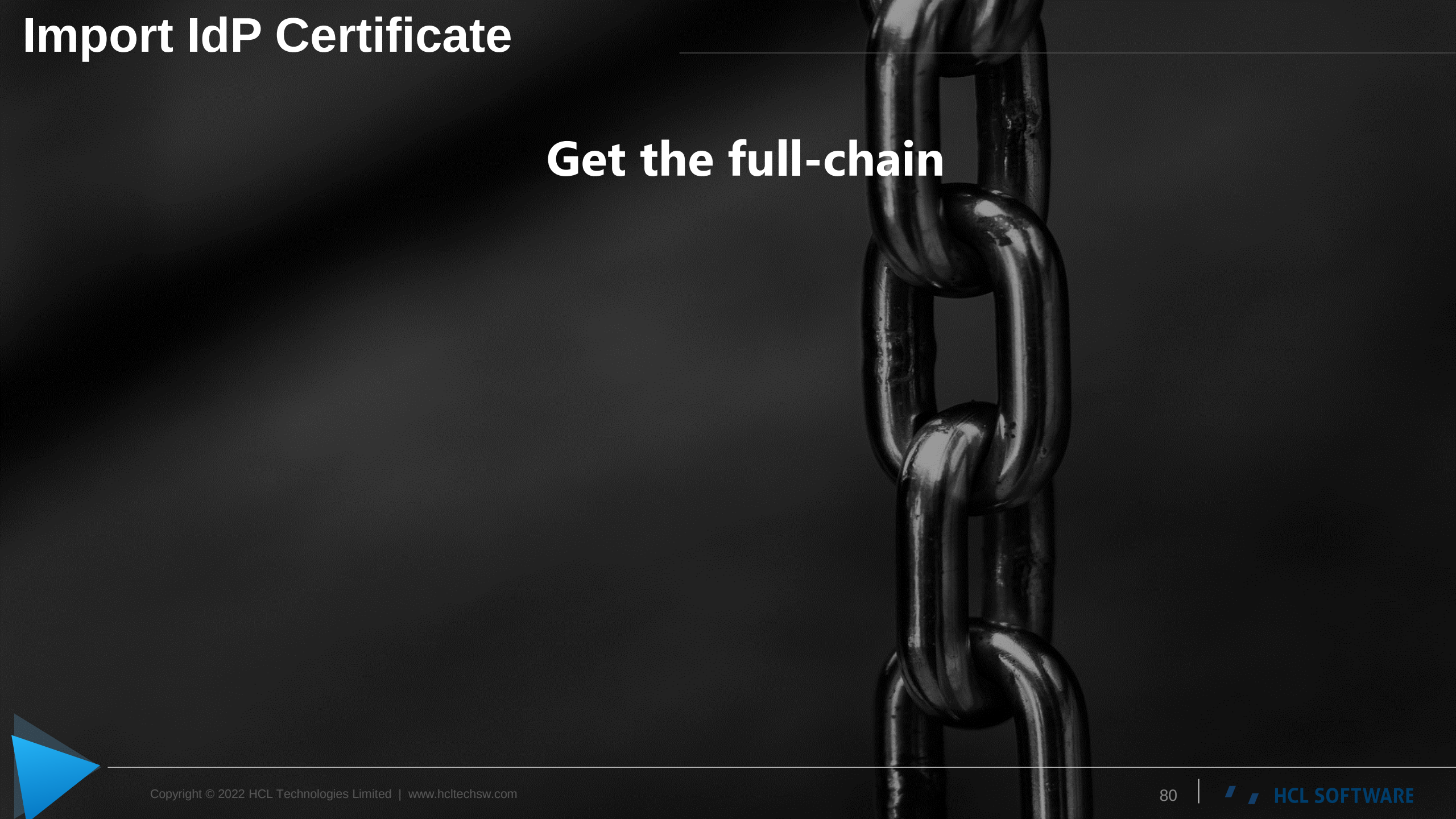
References

Basic SAML Setup

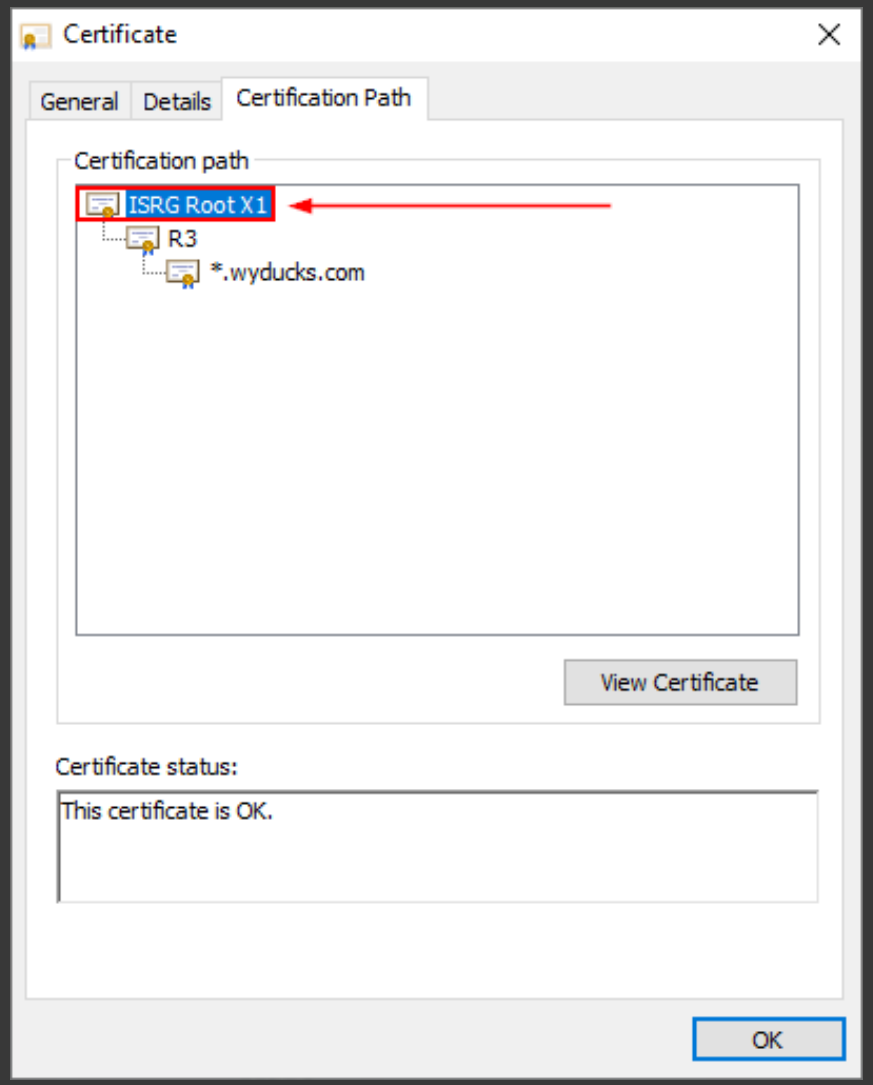


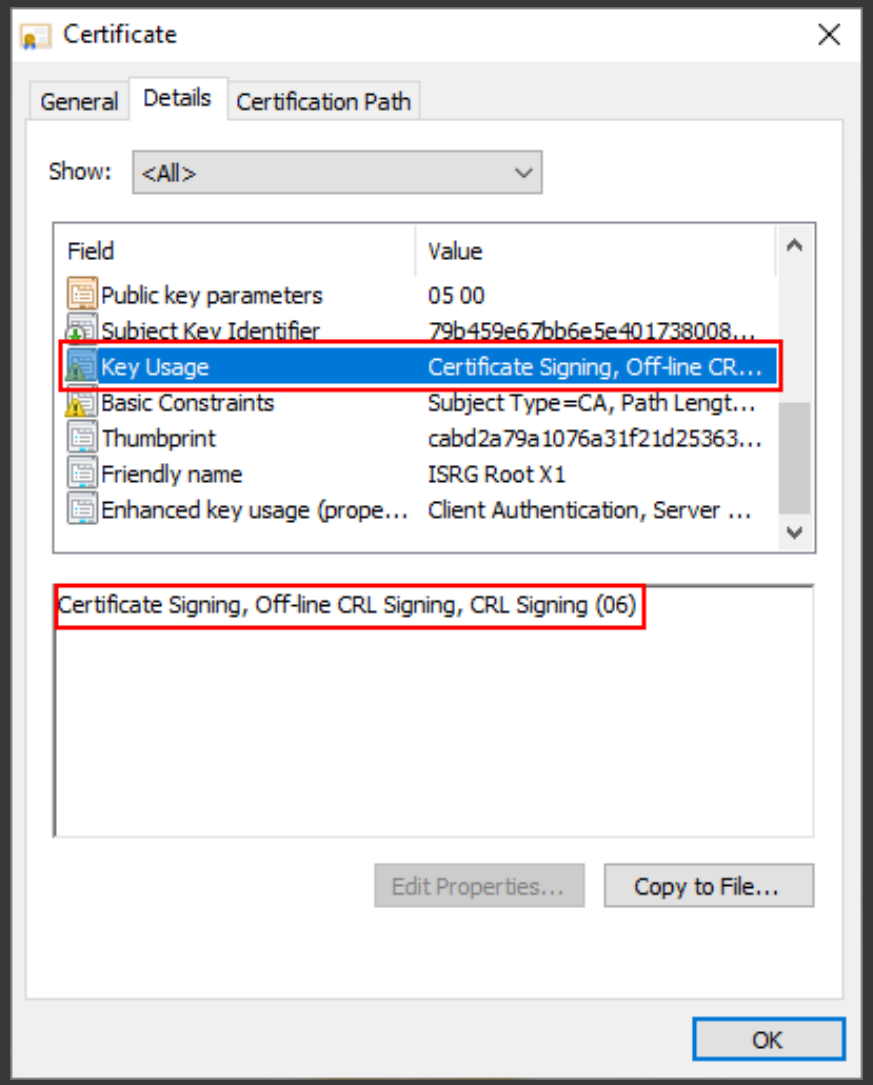
HCL SOFTWARE

Import IdP Certificate



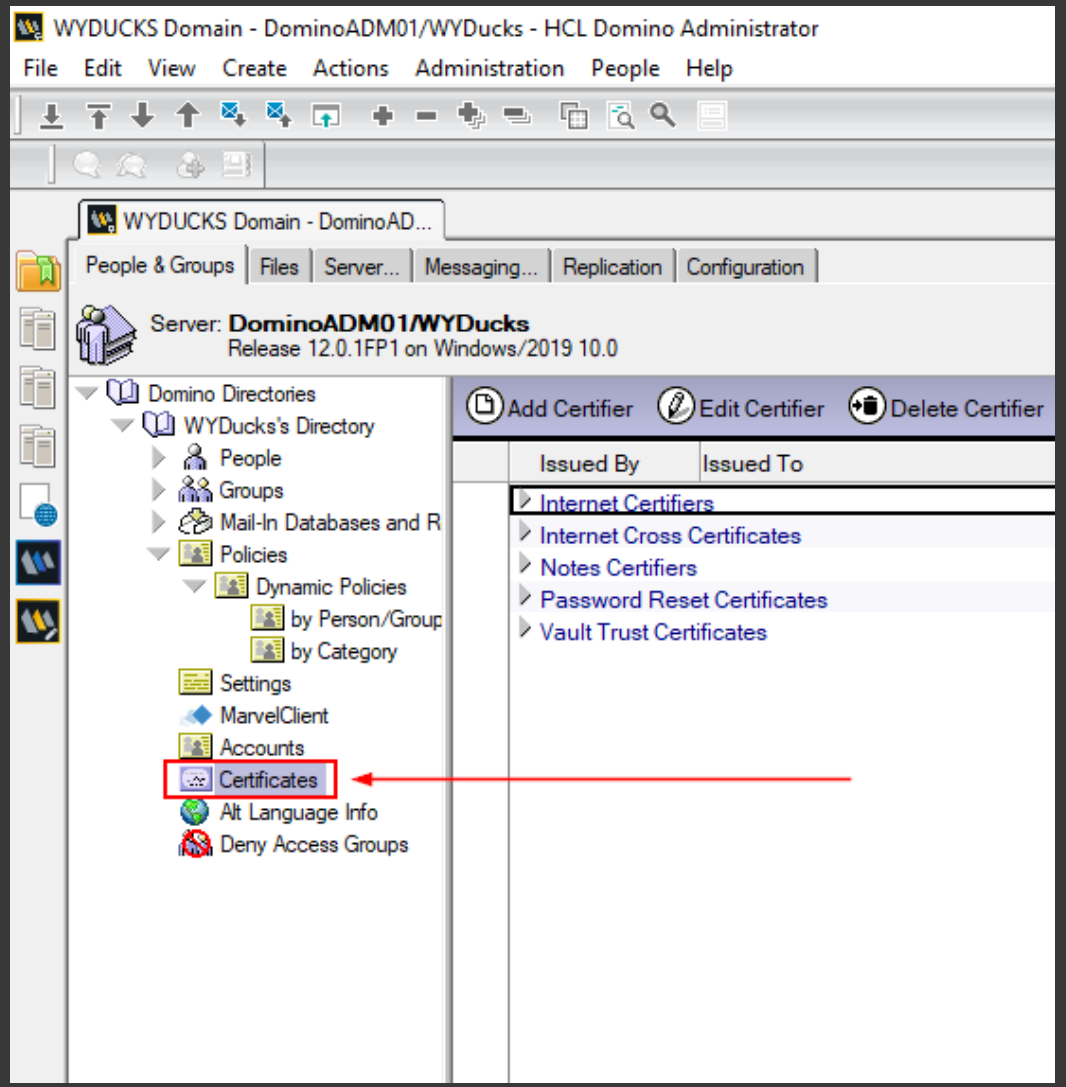
Import IdP Certificate

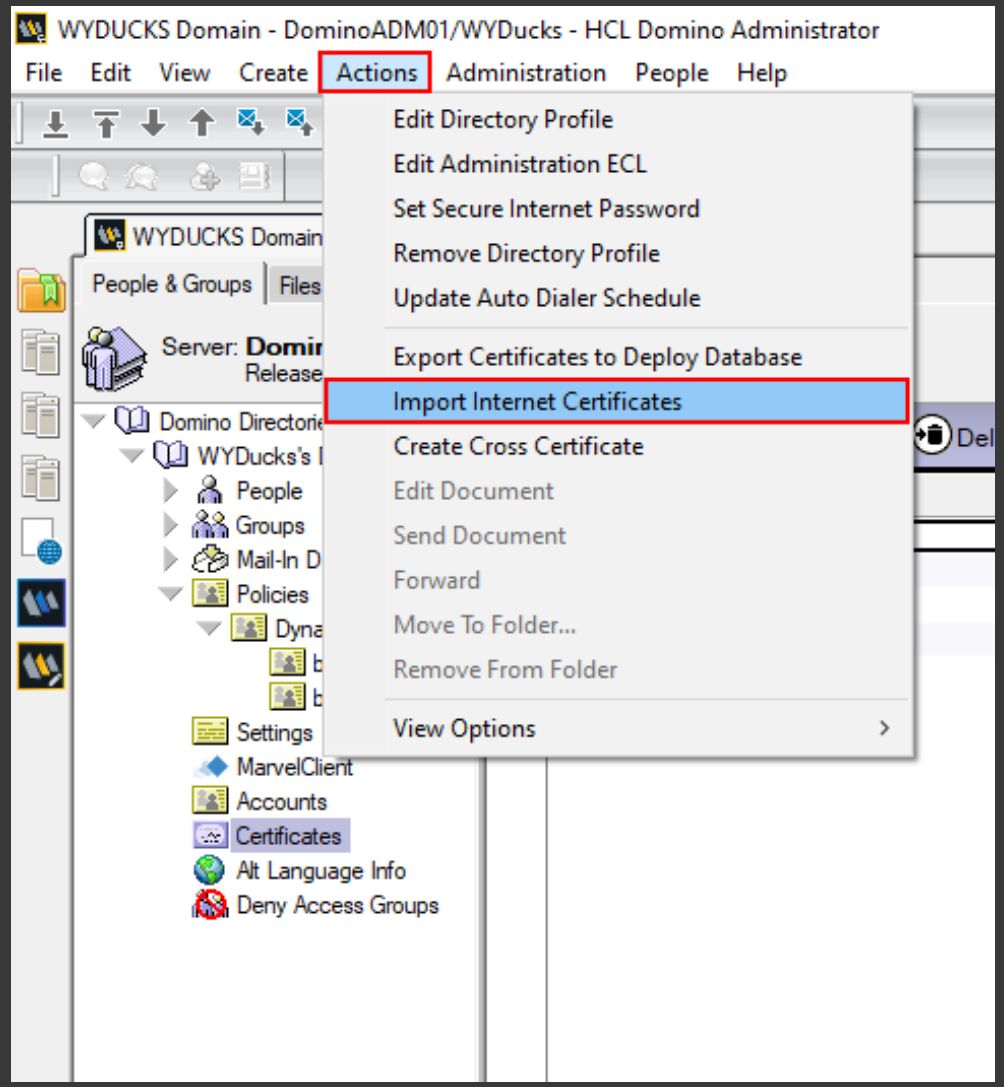




HCL SOFTWARE

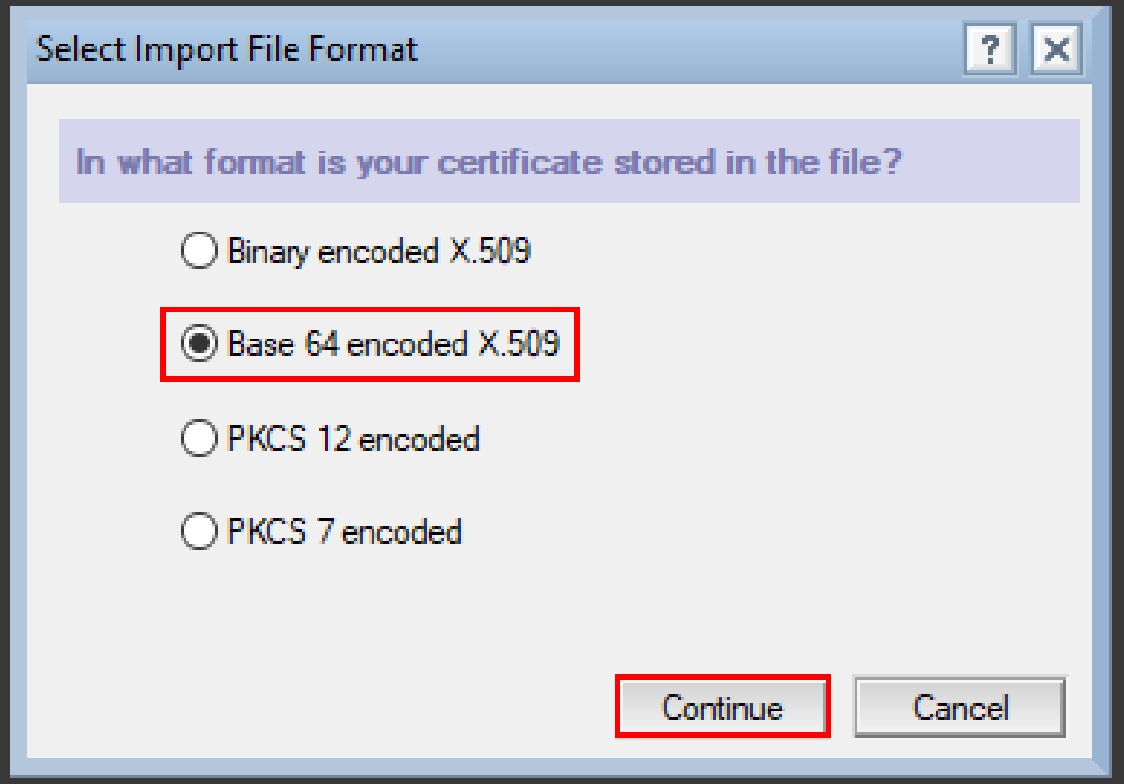
Import IdP Certificate

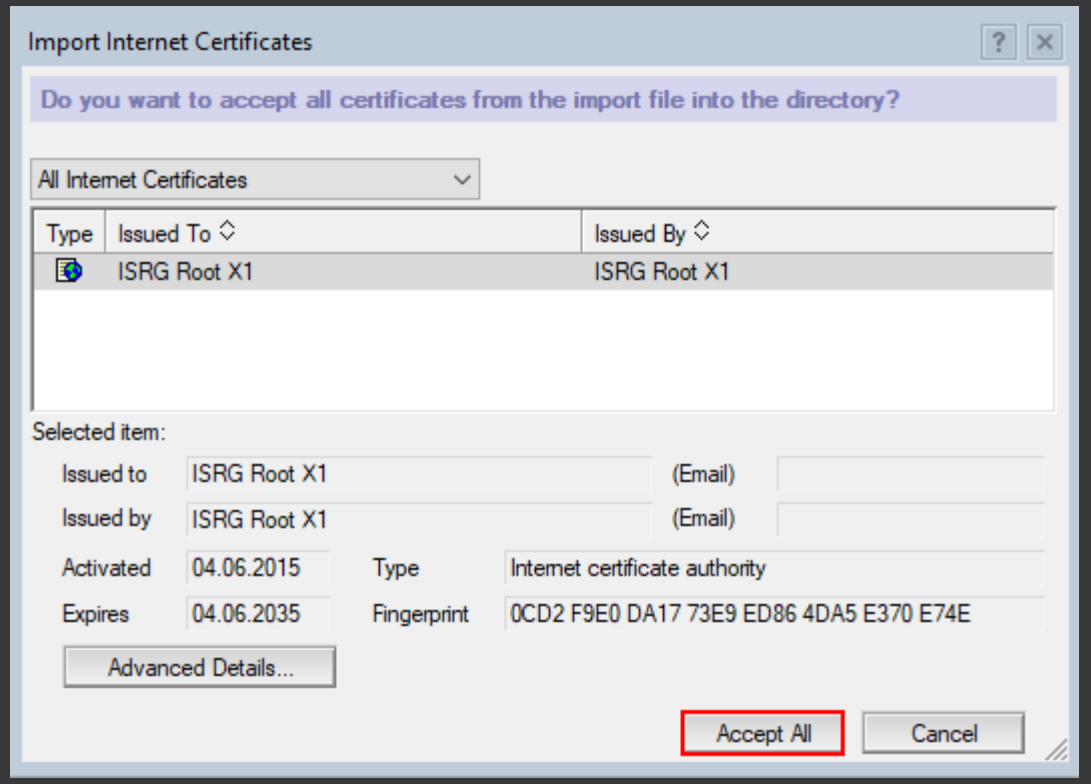




HCL SOFTWARE

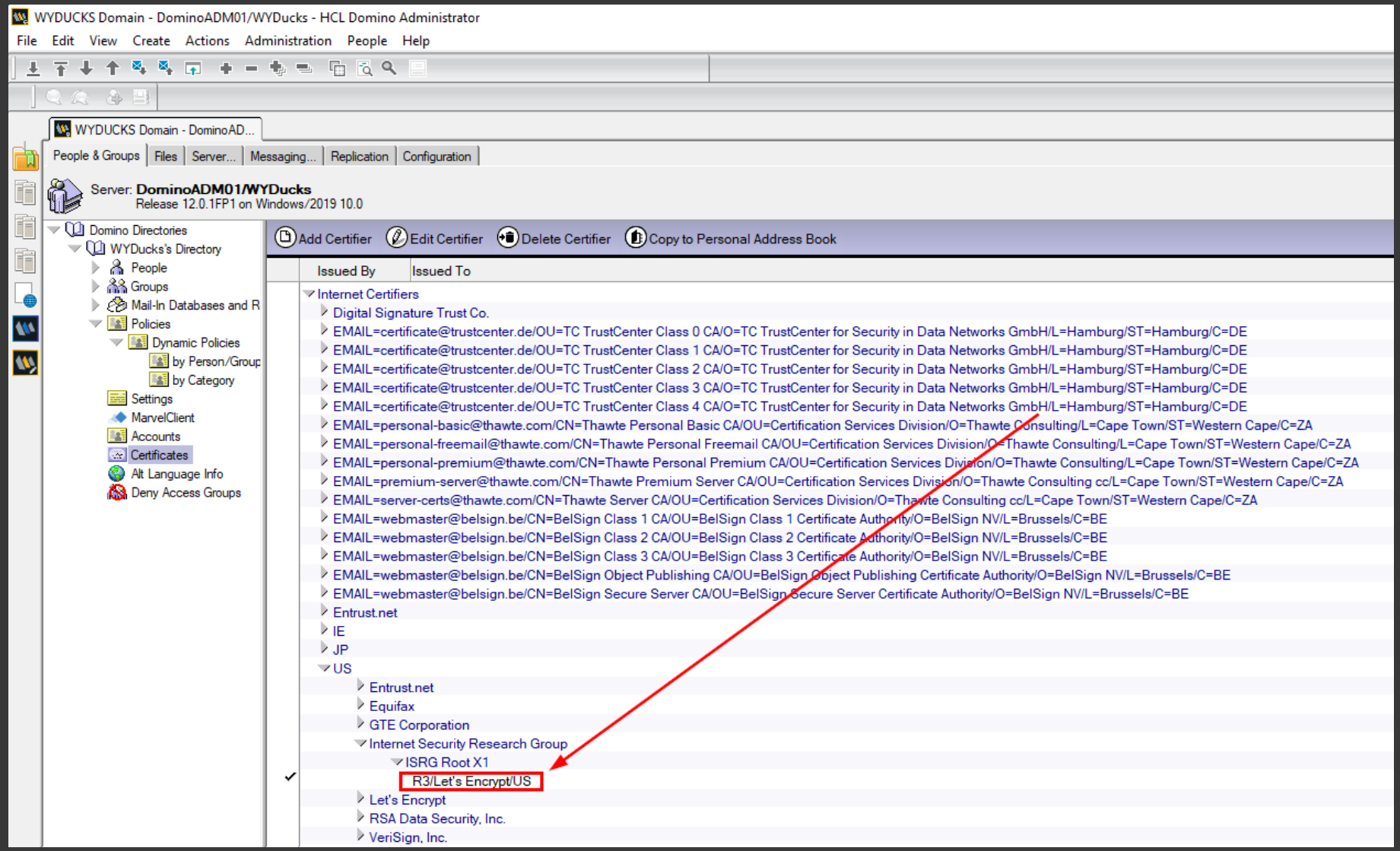
Import IdP Certificate





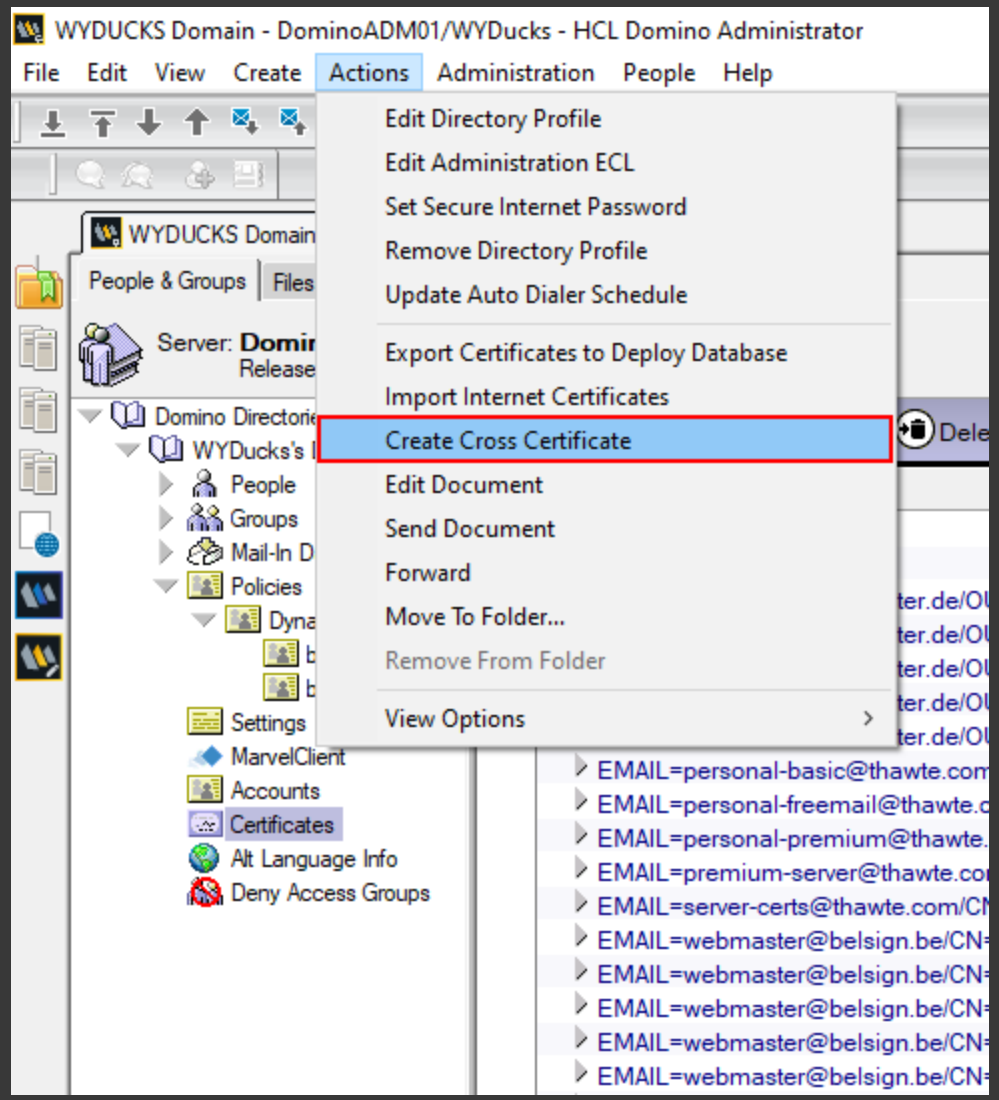
HCL SOFTWARE

Create a Cross Certificate



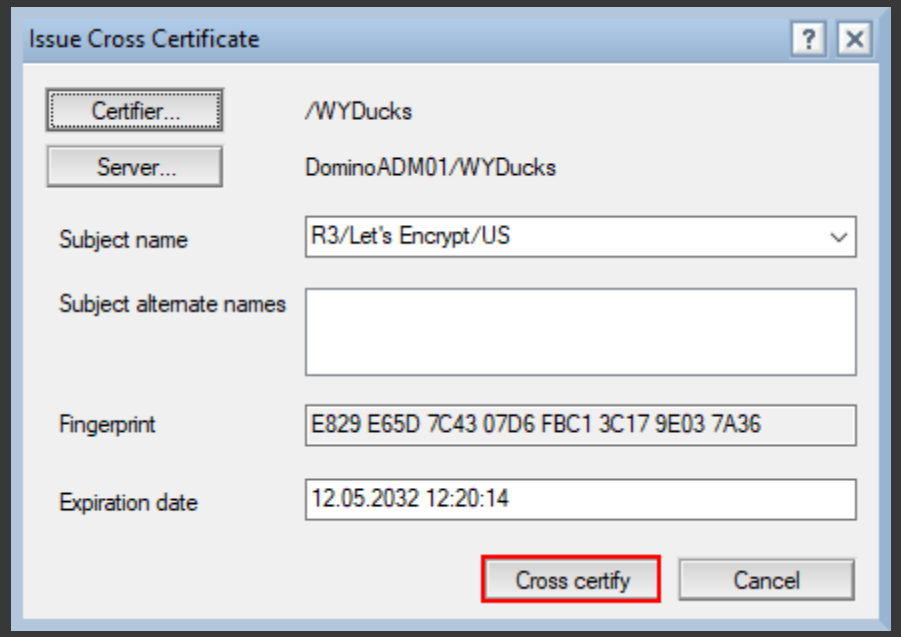
HCL SOFTWARE

Create a Cross Certificate

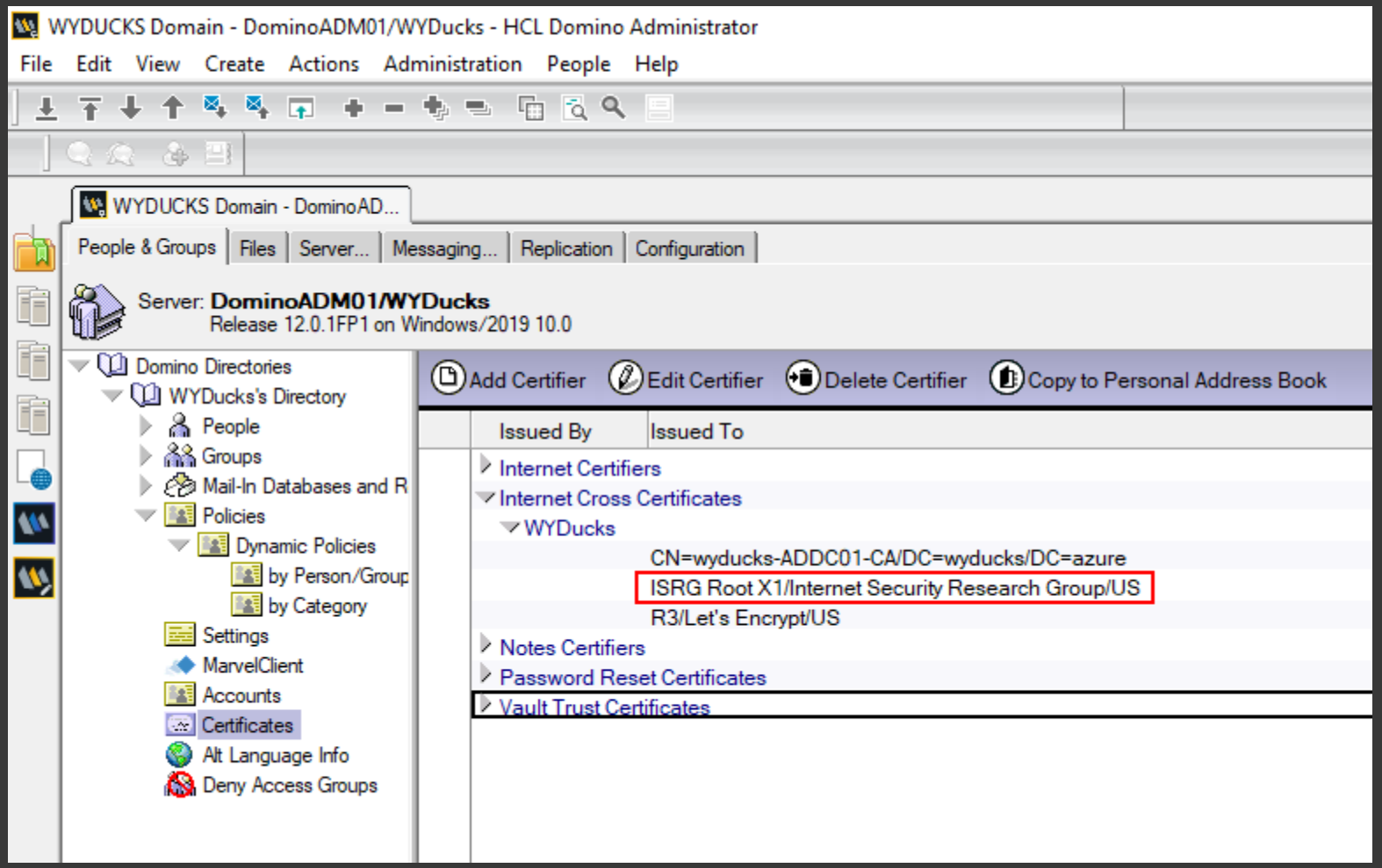


HCL SOFTWARE

Create a Cross Certificate



Create a Cross Certificate



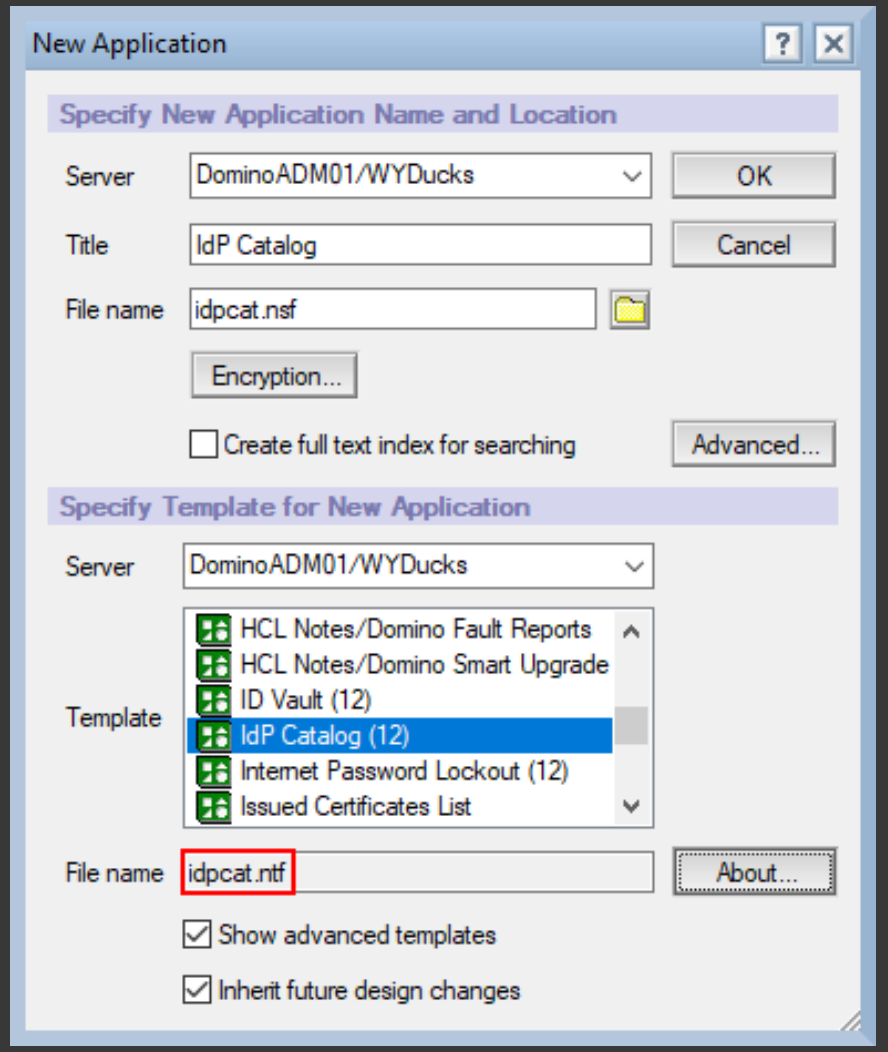
HCL SOFTWARE

Create the IdP Catalog

“idpcat.nsf”

Create and replicate

Create the IdP Catalog



HCL SOFTWARE

Get the IdP Configuration

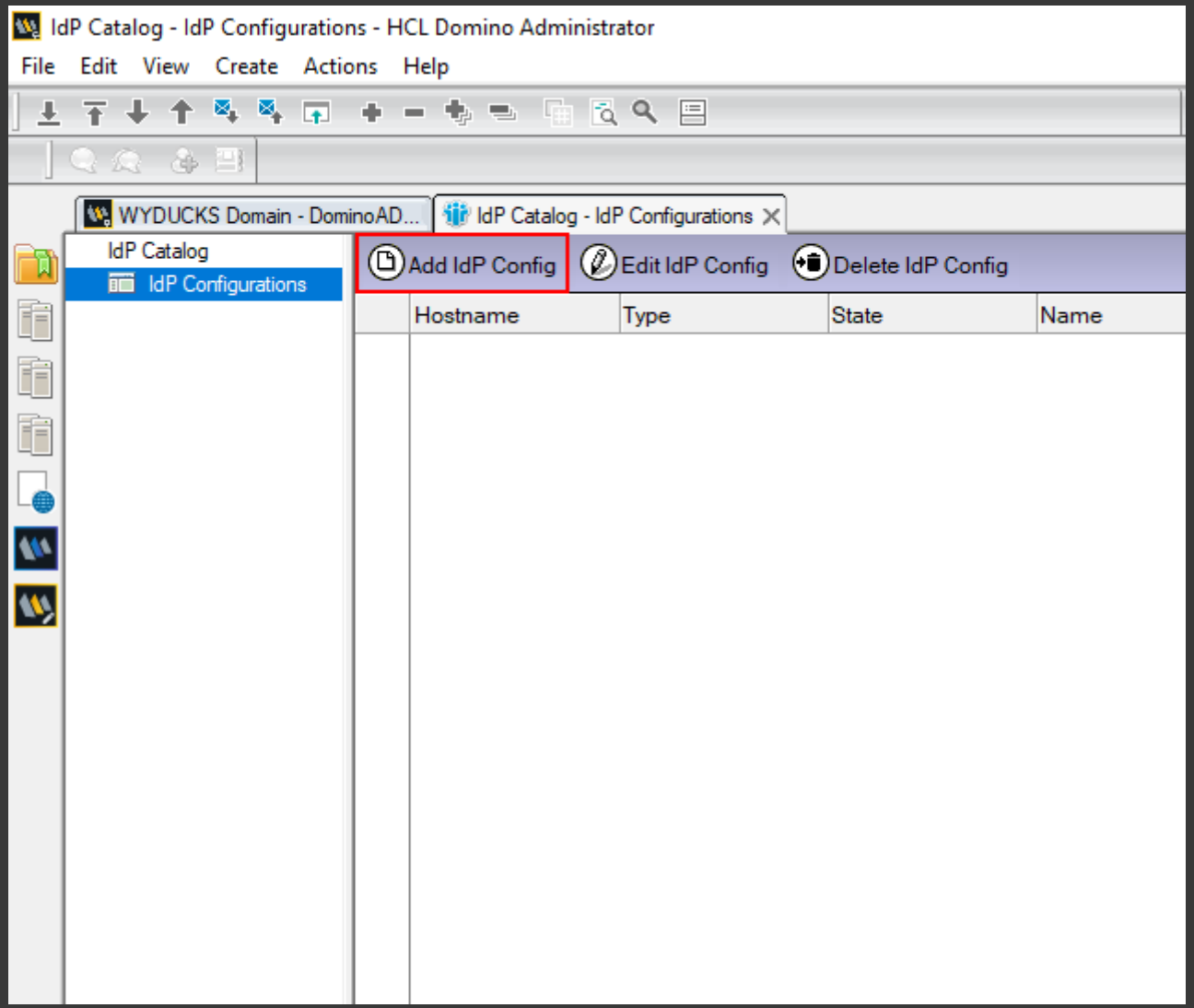
FederationMetadata.xml

Create some backup copies

Create the IdP Configuration Document

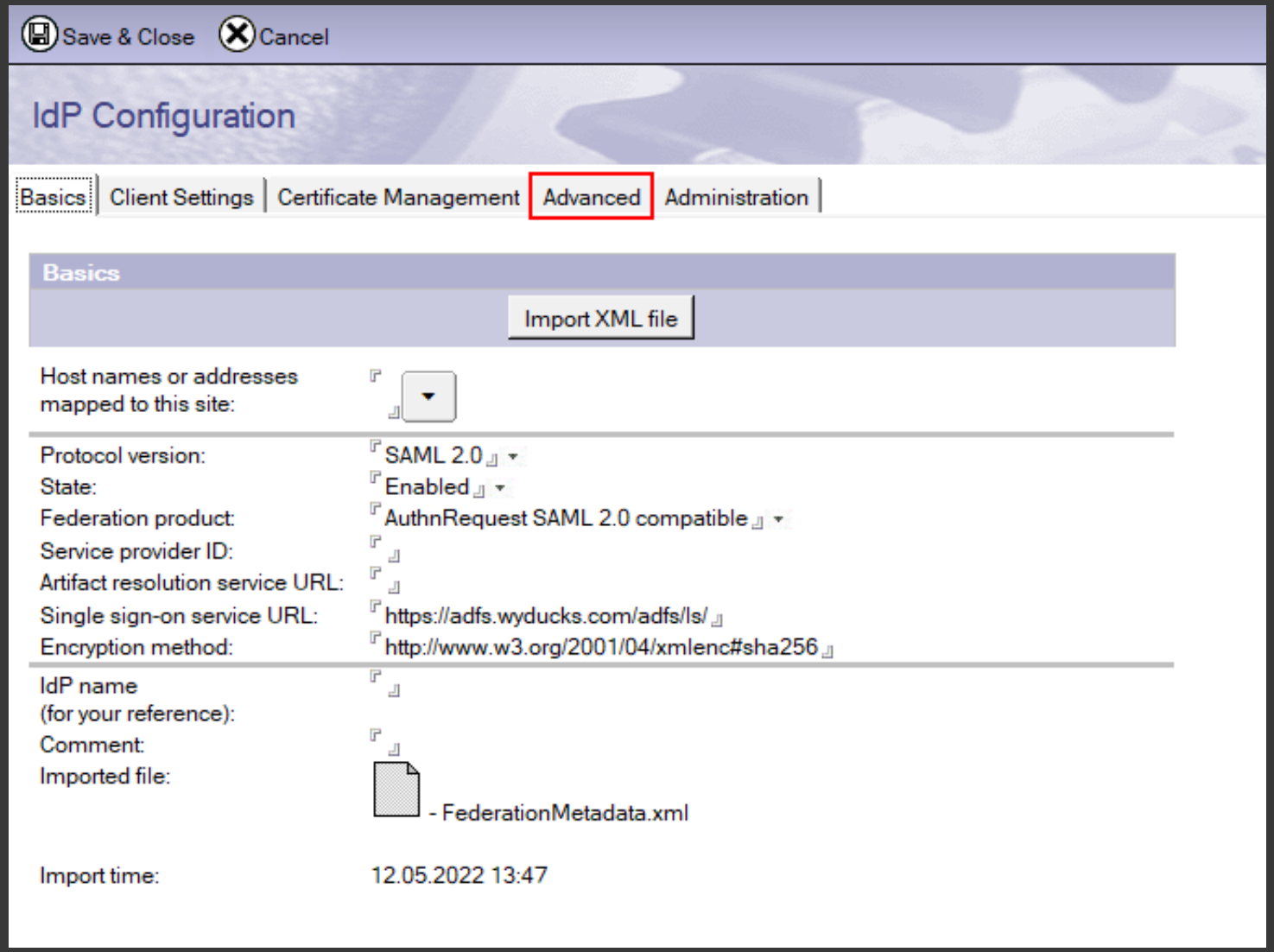
Inside of “idpcat.nsf”

Create the IdP Configuration Document



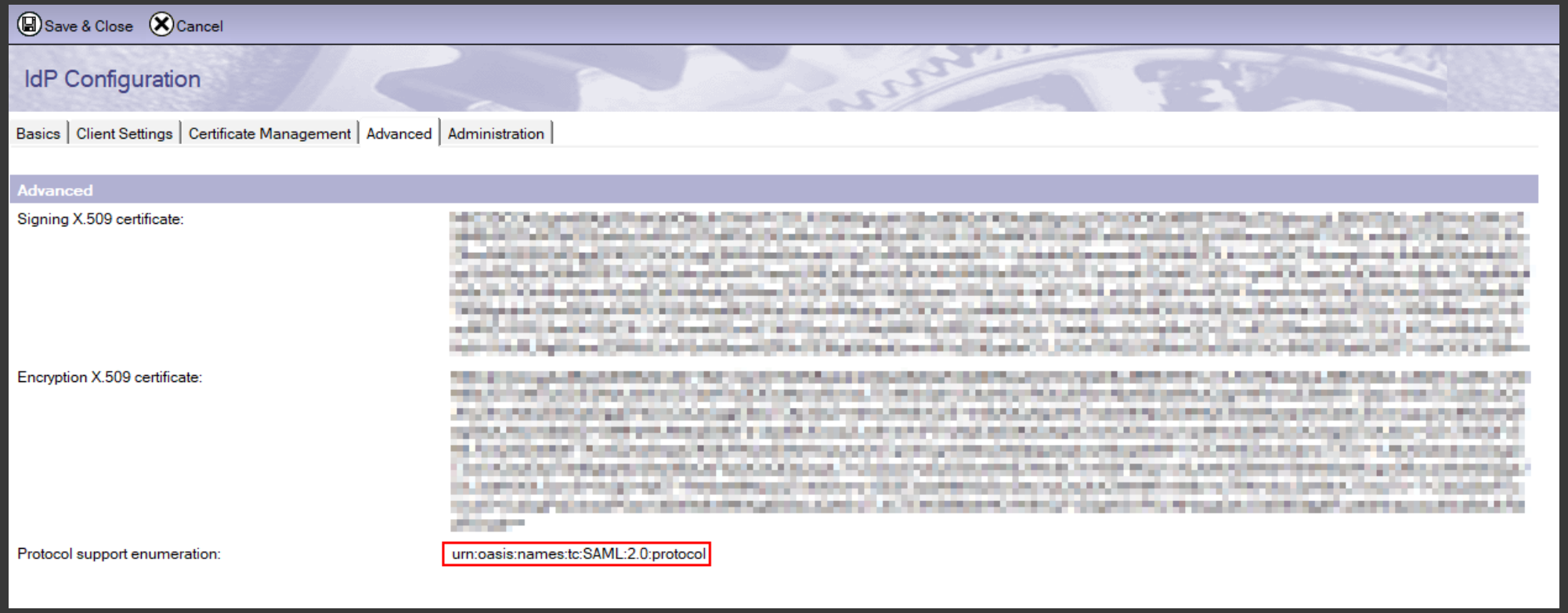
HCL SOFTWARE

Create the IdP Configuration Document



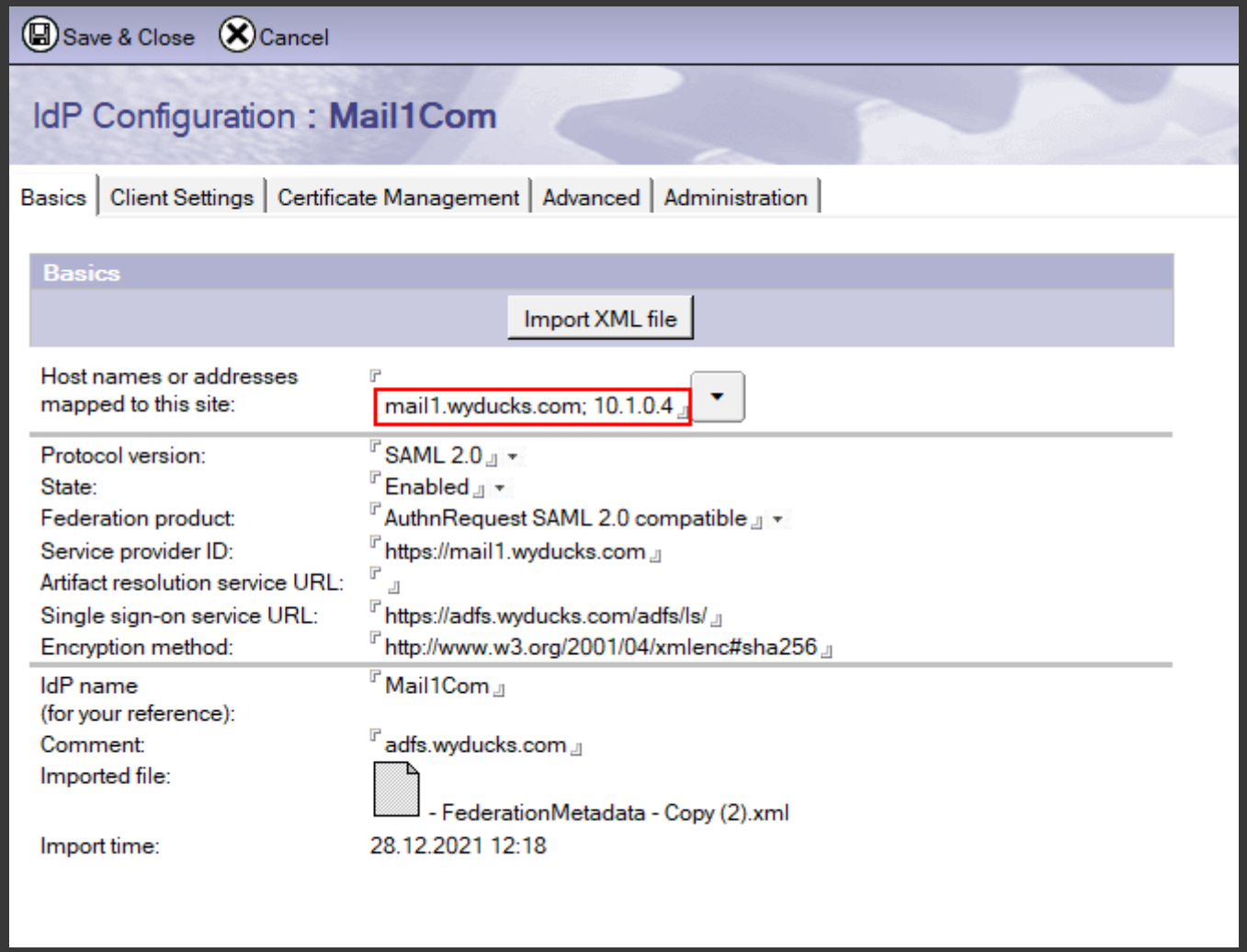
HCL SOFTWARE

Create the IdP Configuration Document



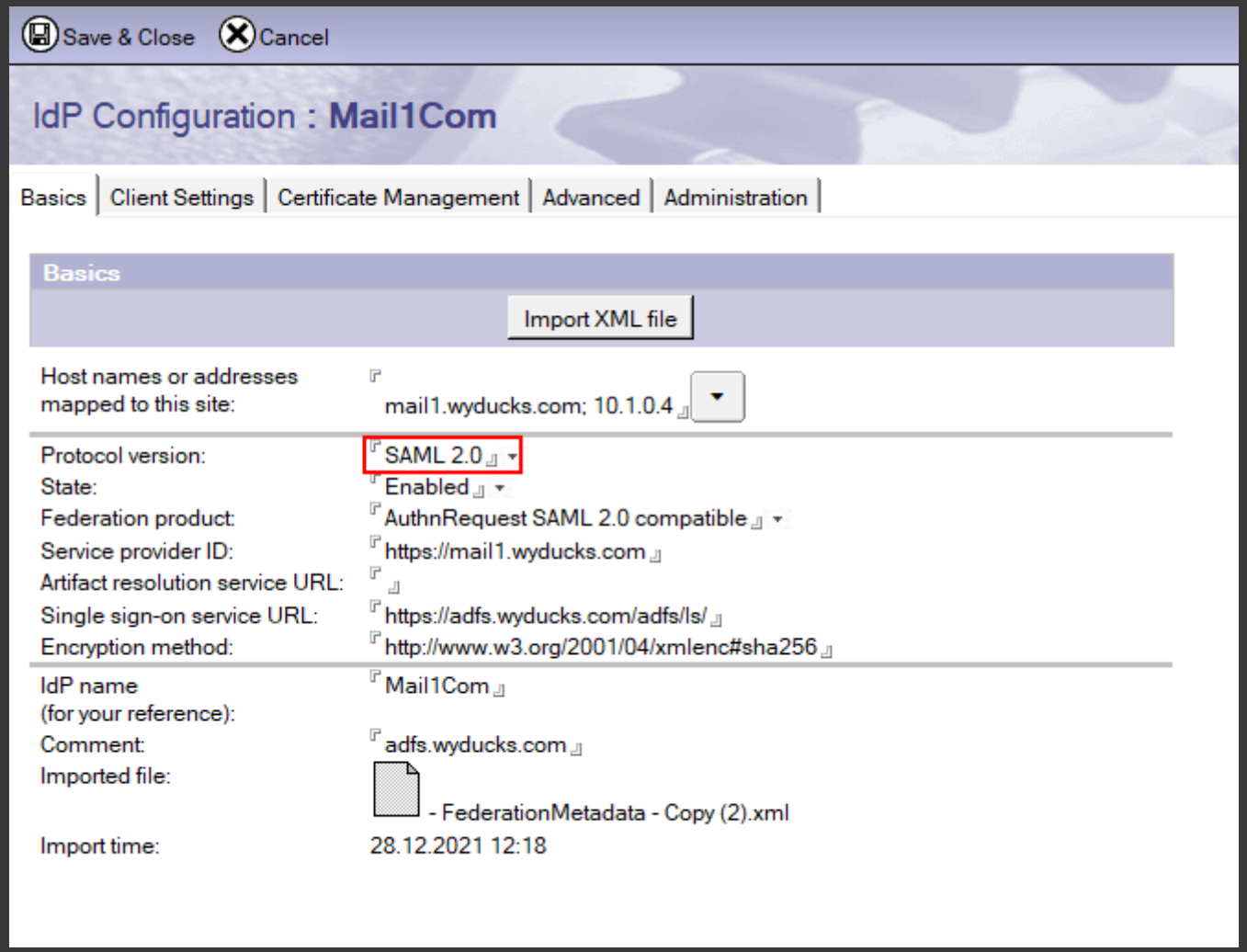
HCL SOFTWARE

Create the IdP Configuration Document

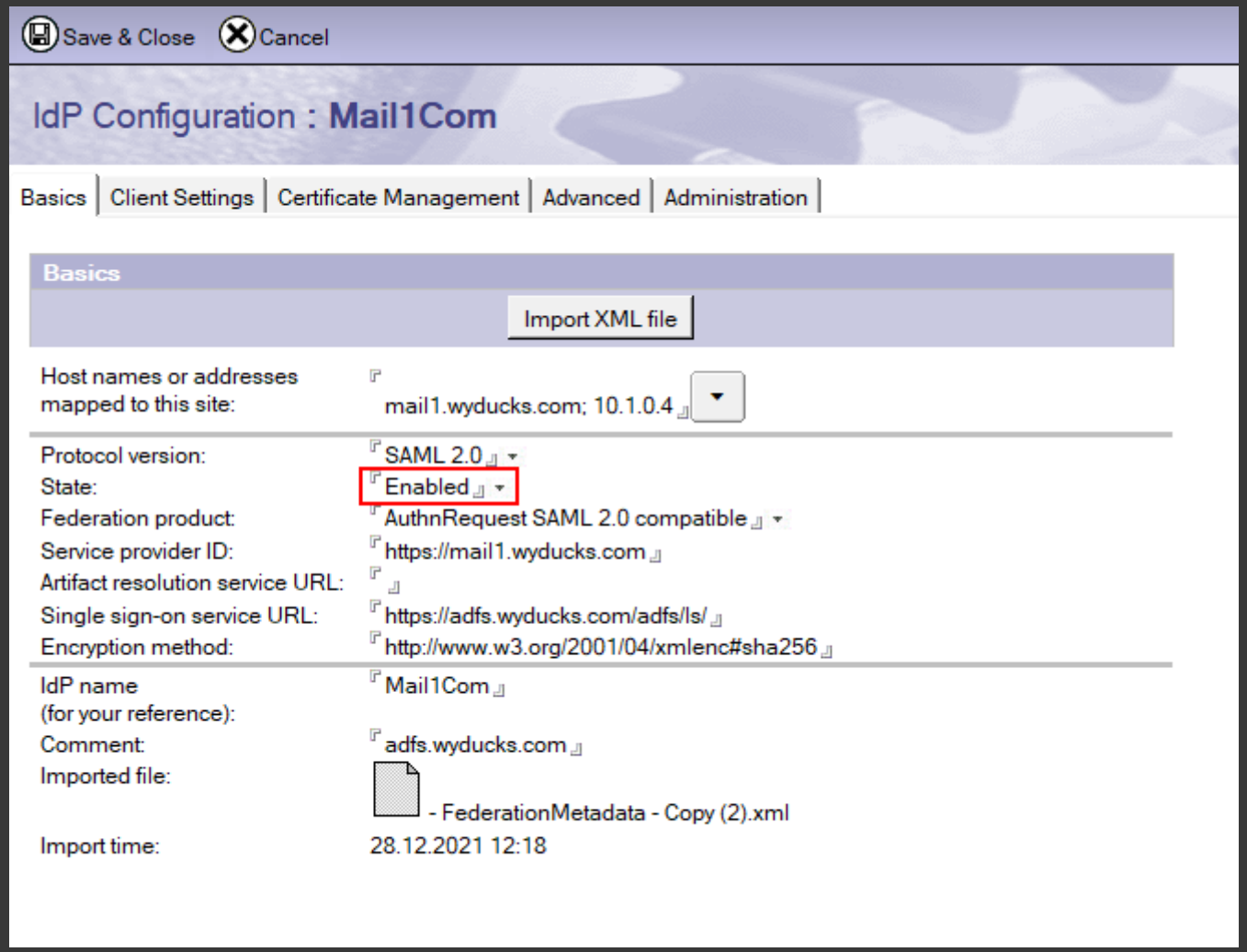


HCL SOFTWARE

Create the IdP Configuration Document

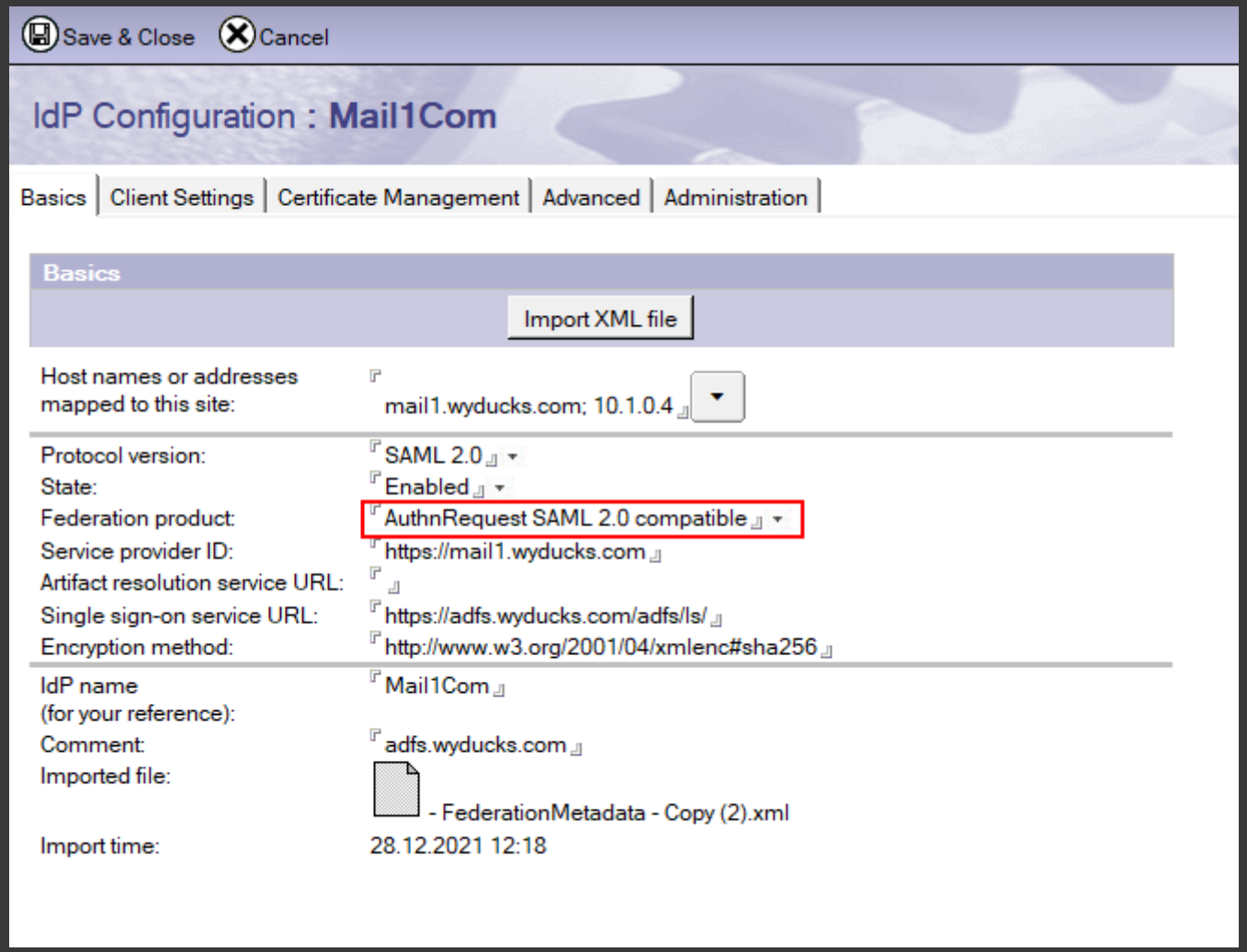


Create the IdP Configuration Document



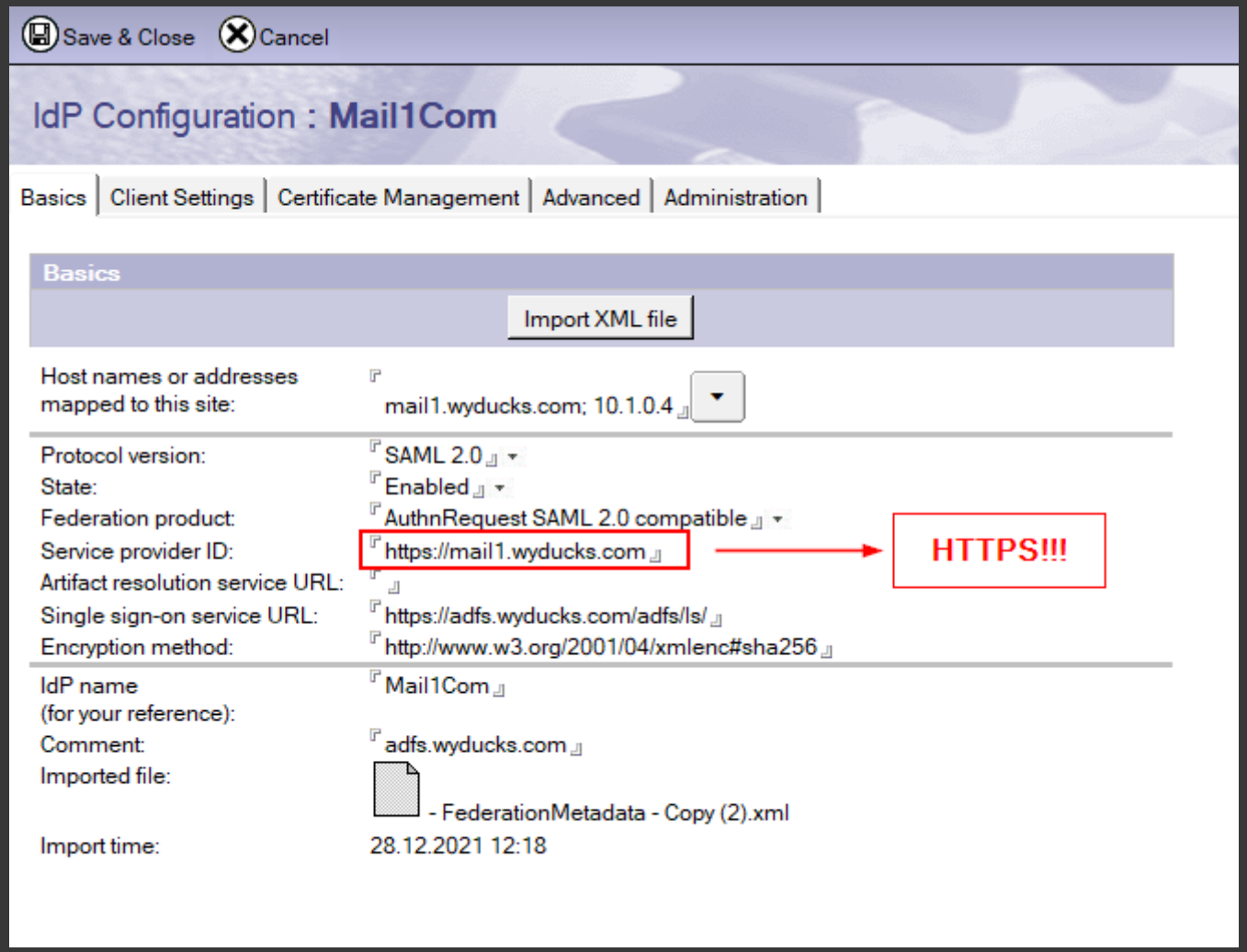
HCL SOFTWARE

Create the IdP Configuration Document

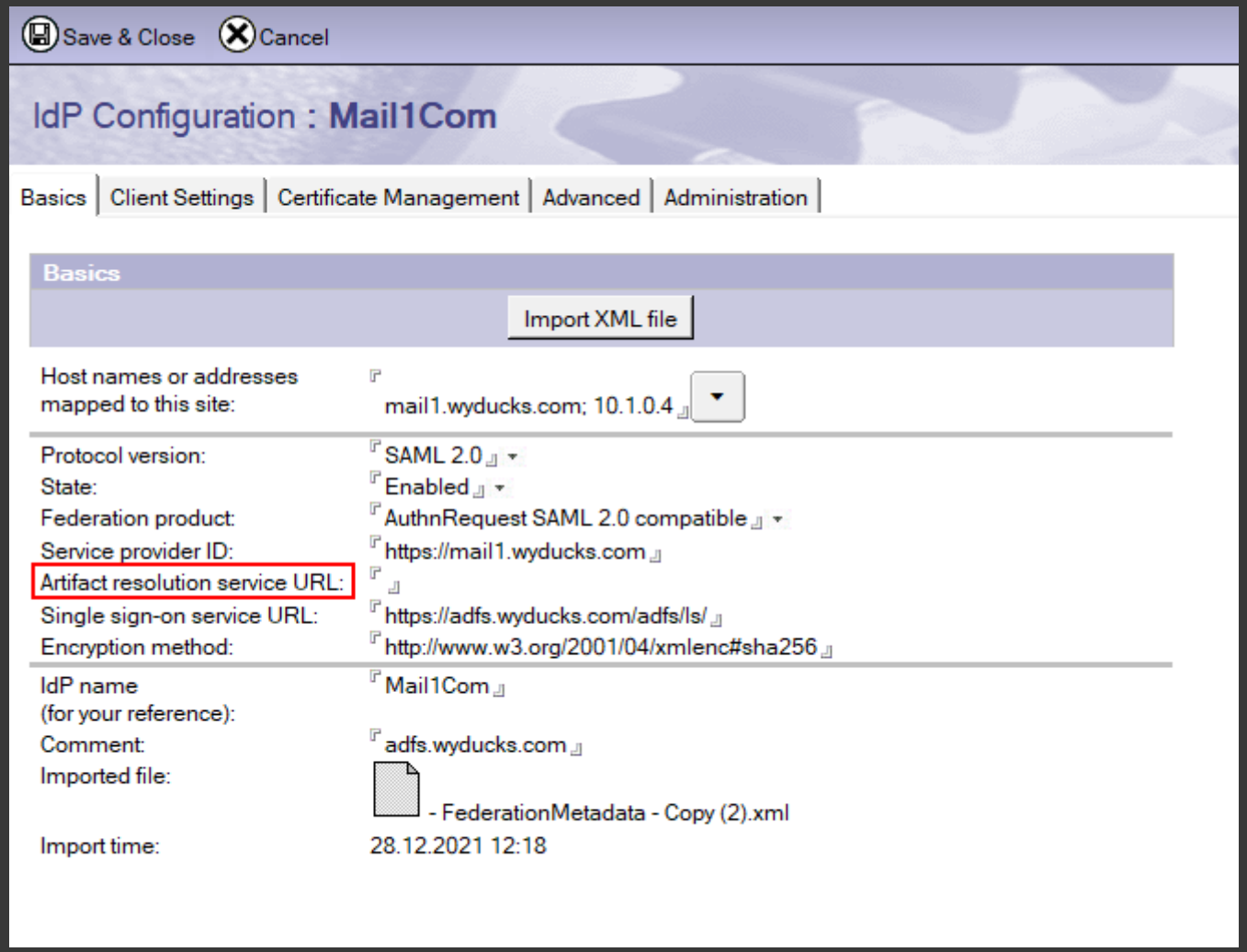


HCL SOFTWARE

Create the IdP Configuration Document

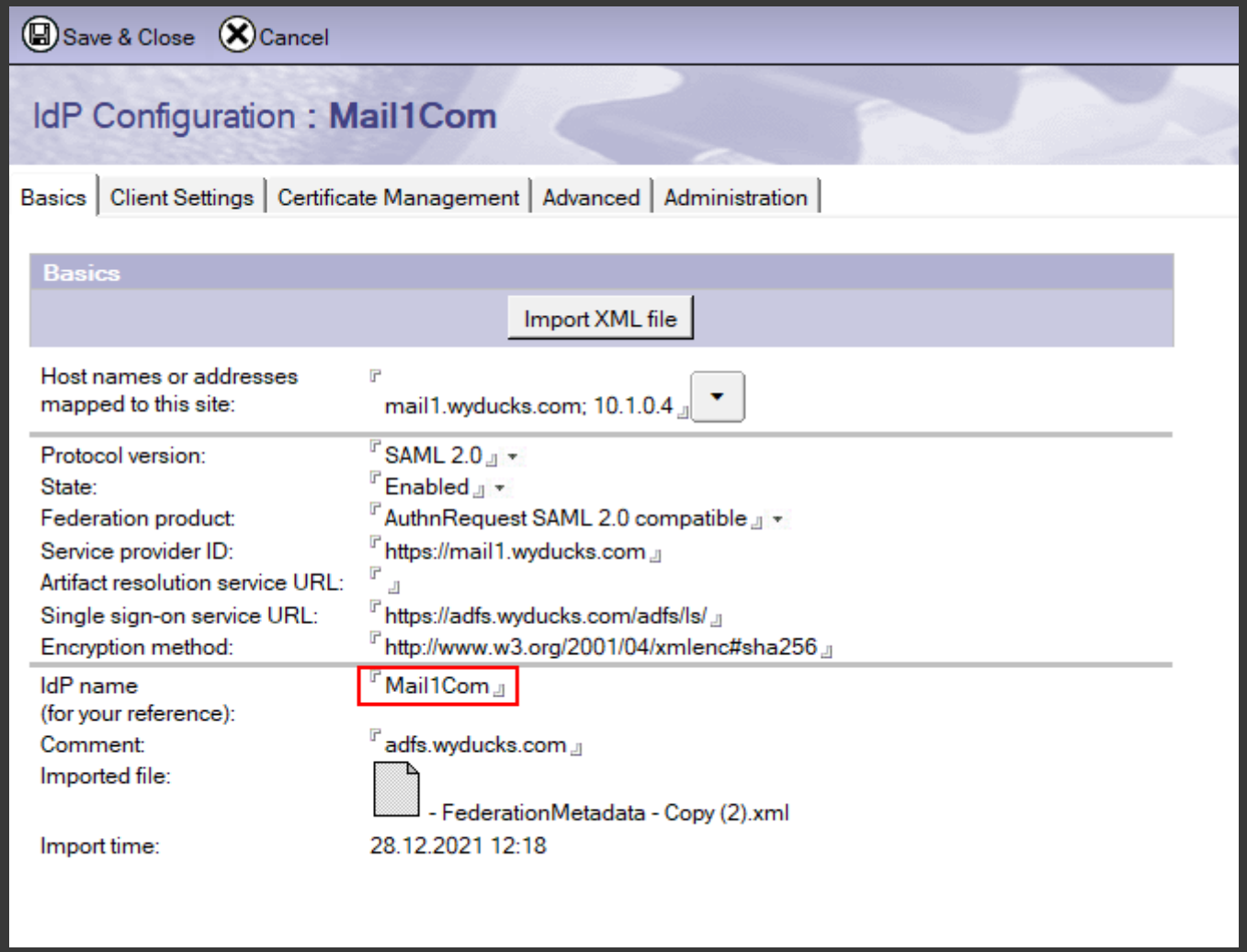


Create the IdP Configuration Document



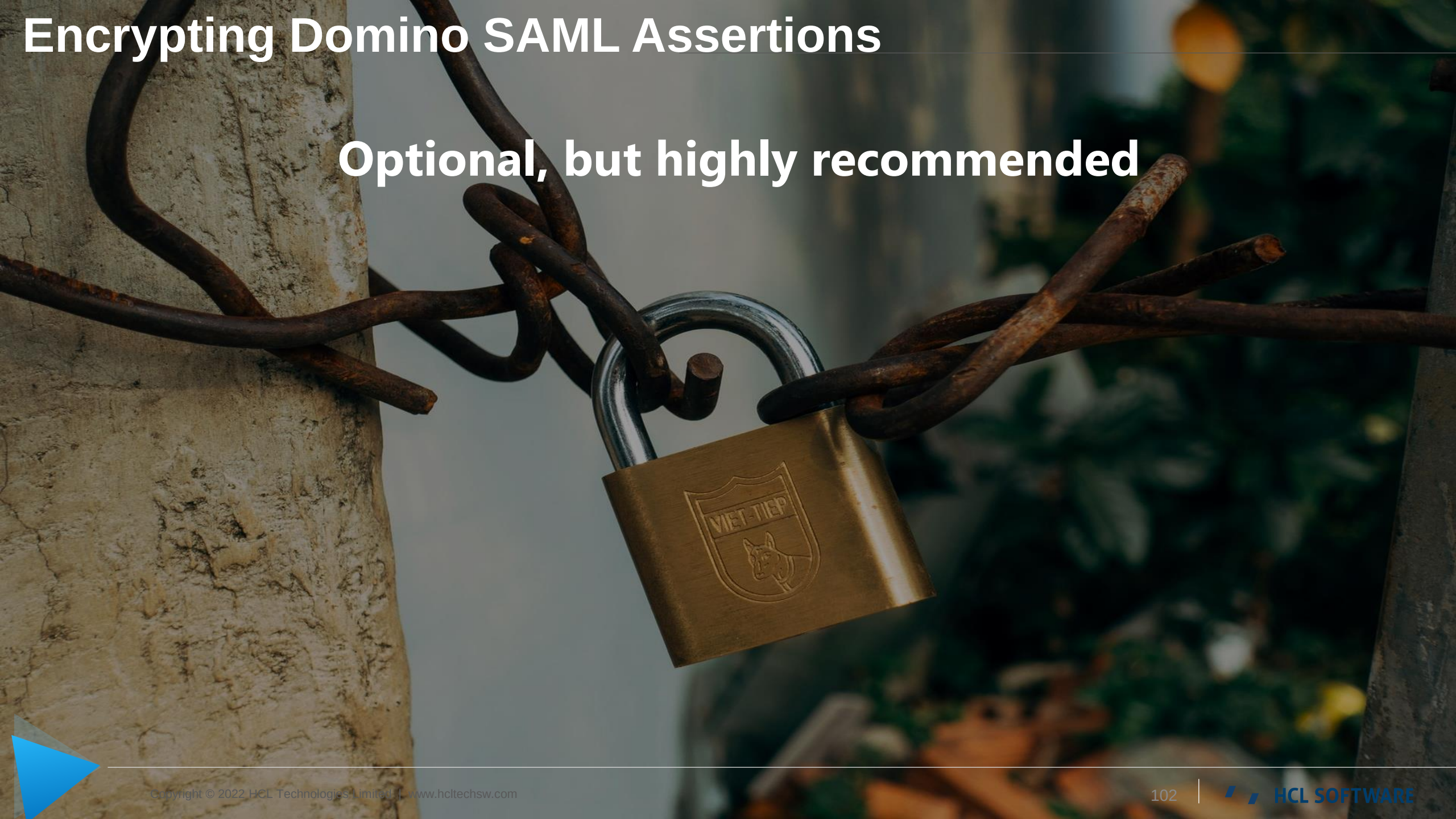
HCL SOFTWARE

Create the IdP Configuration Document



HCL SOFTWARE

Encrypting Domino SAML Assertions

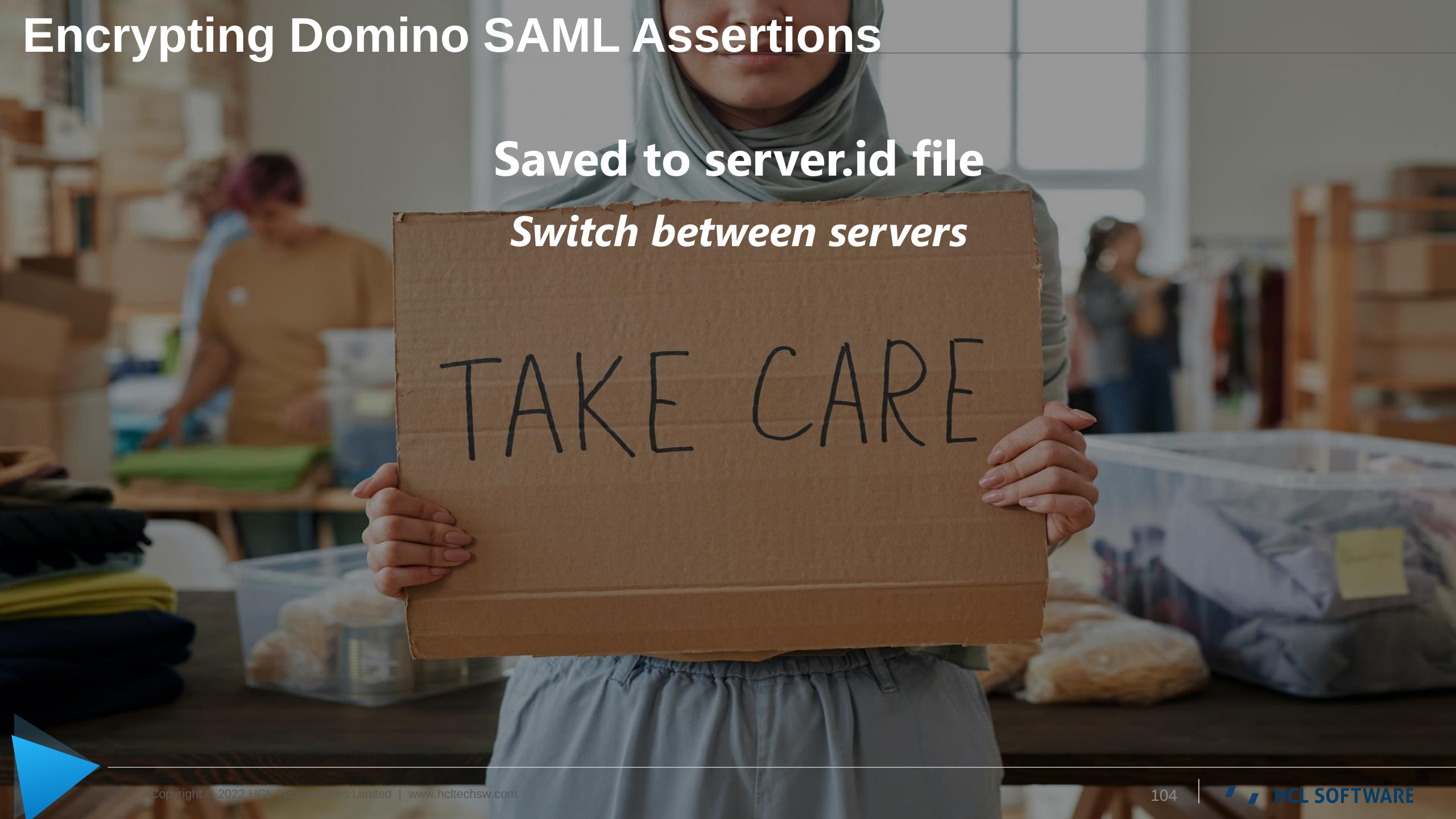


Optional, but highly recommended

Encrypting Domino SAML Assertions

Certificate for encryption

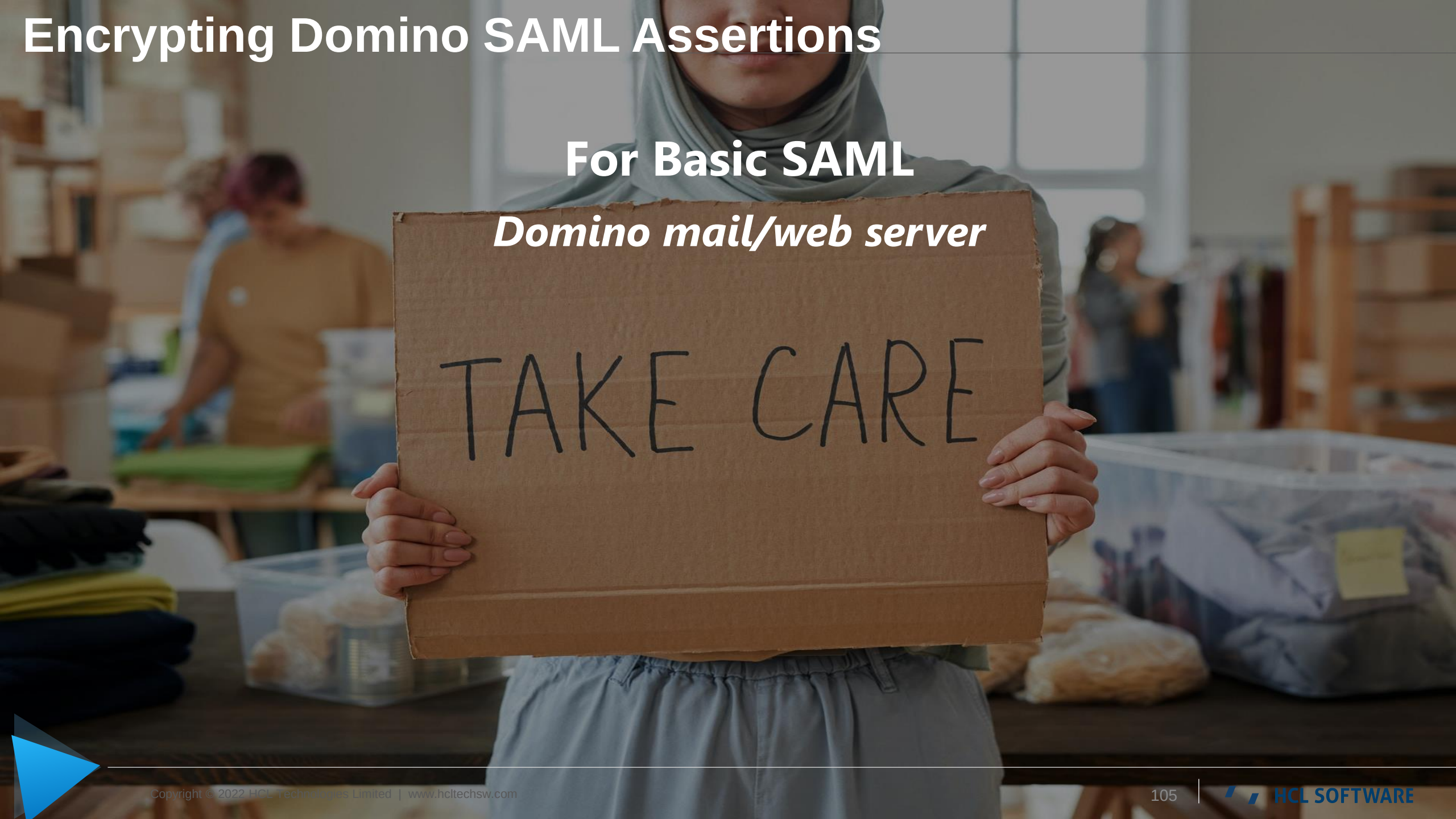
Encrypting Domino SAML Assertions



Saved to server.id file

Switch between servers

Encrypting Domino SAML Assertions



For Basic SAML

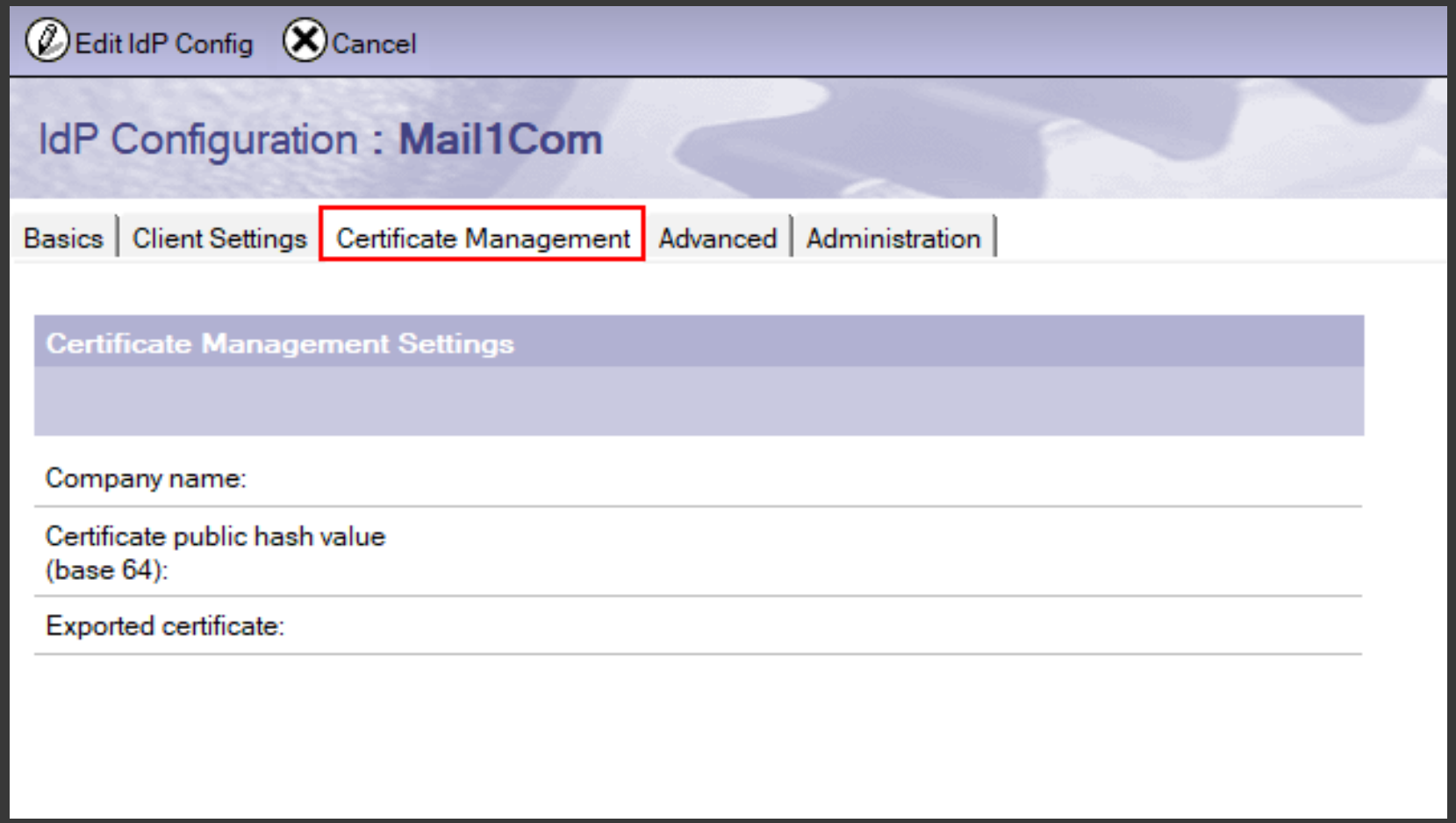
Domino mail/web server

Encrypting Domino SAML Assertions

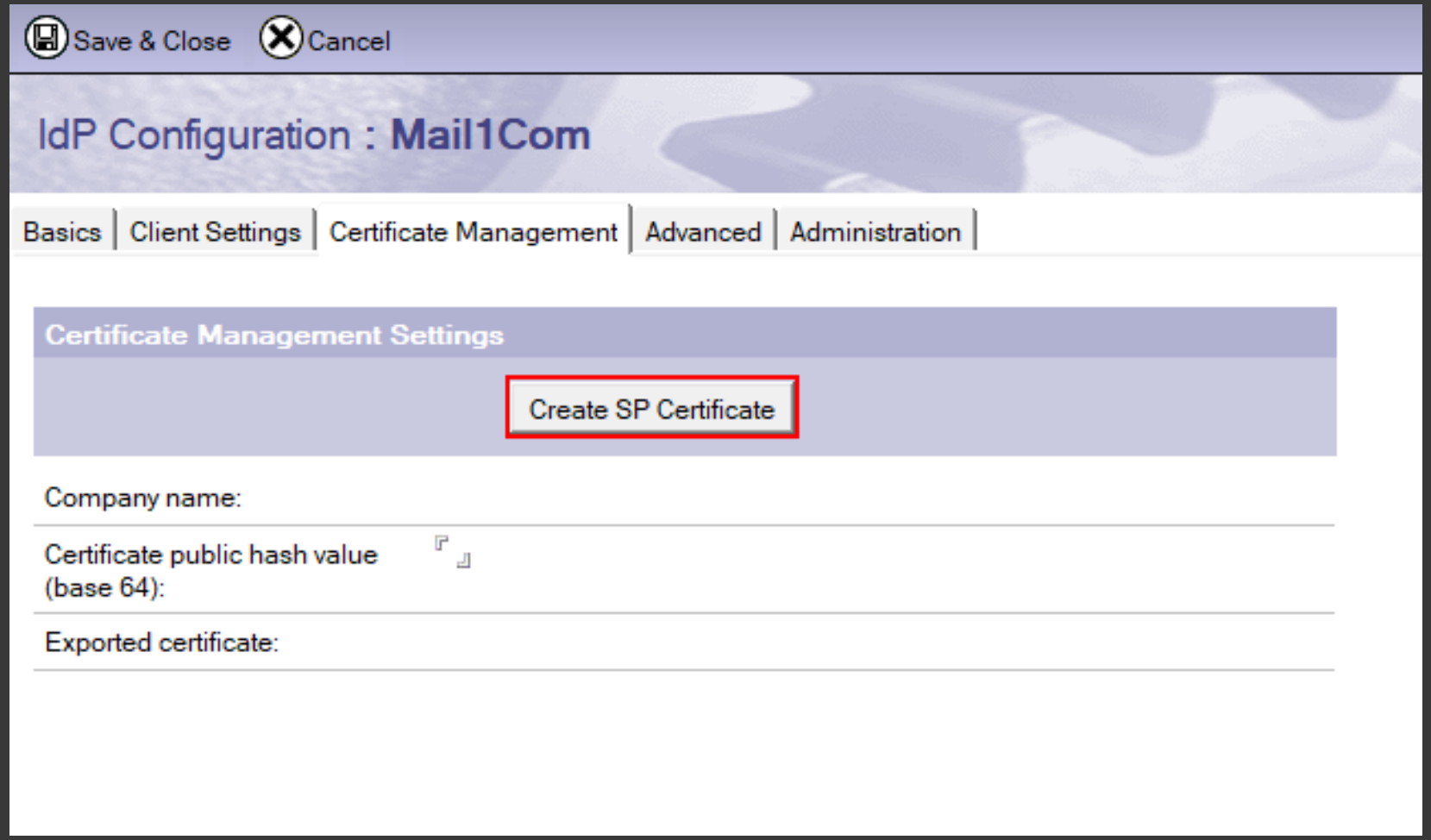
One more thing!

The company name must be unique!

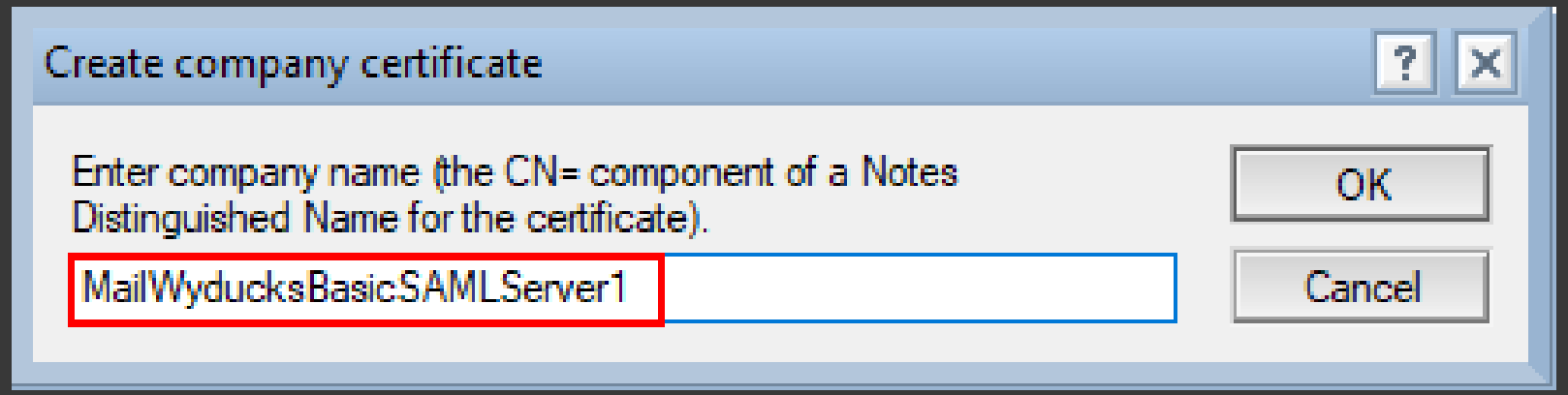
Encrypting Domino SAML Assertions



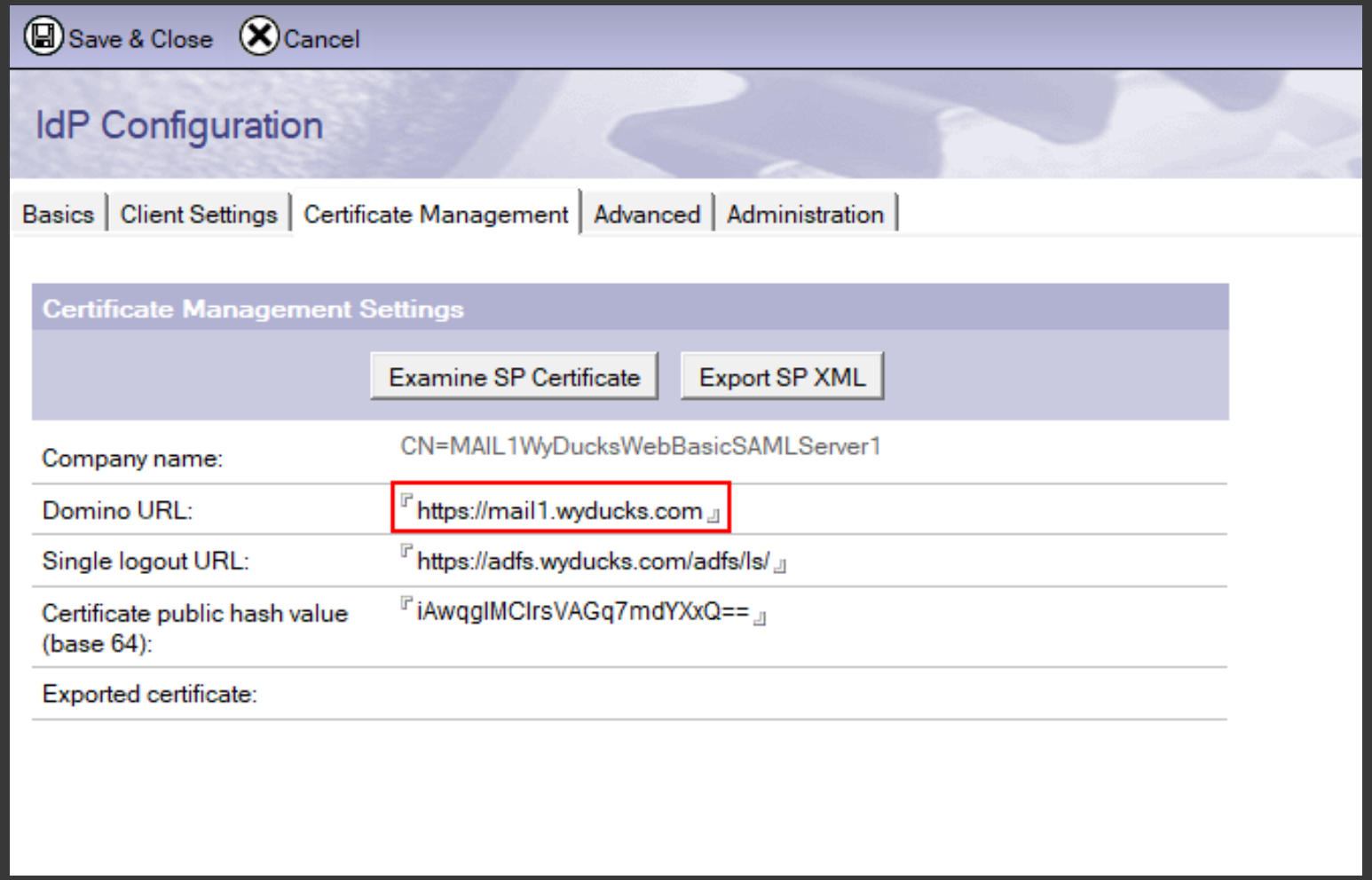
Encrypting Domino SAML Assertions



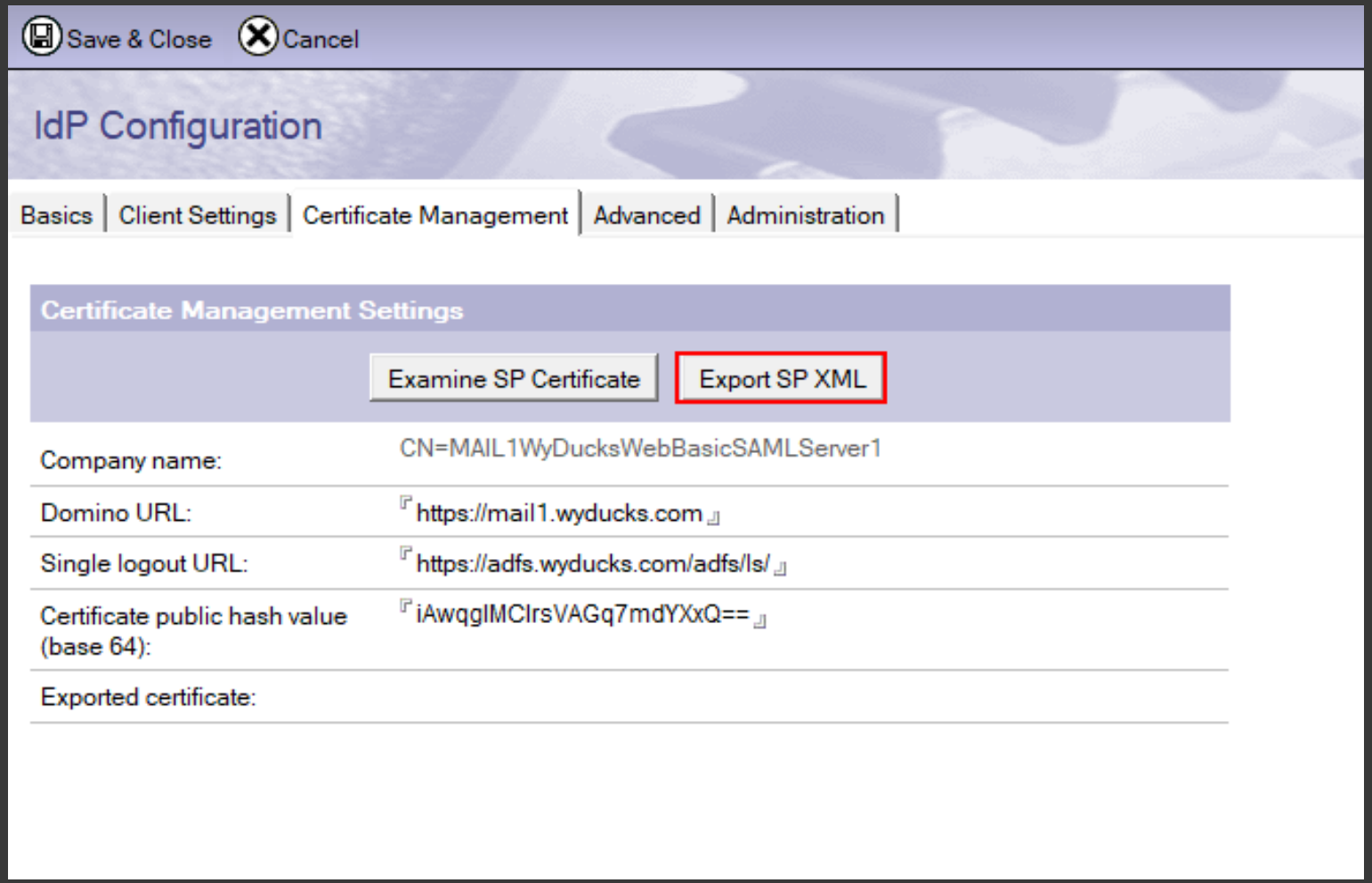
Encrypting Domino SAML Assertions



Encrypting Domino SAML Assertions

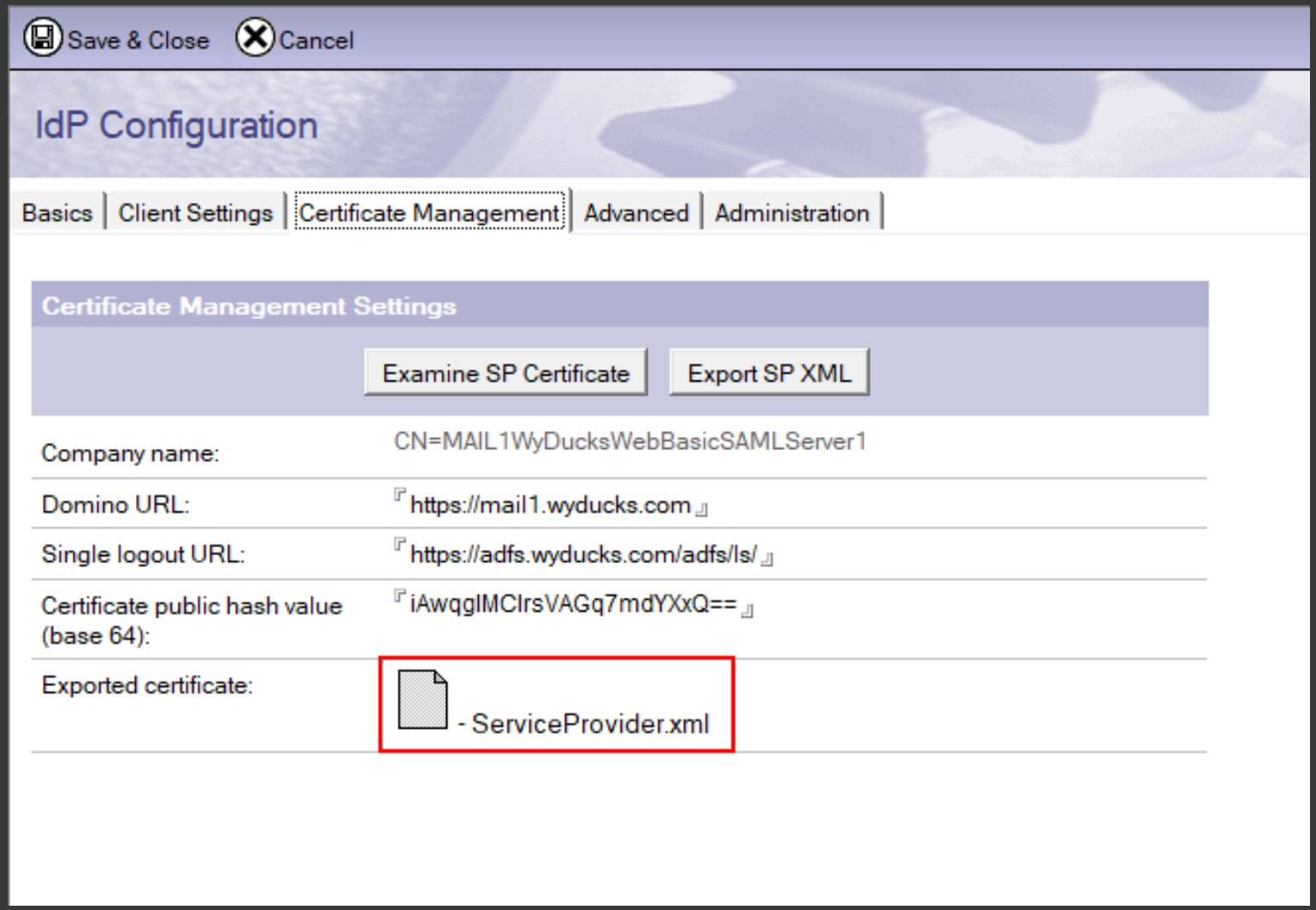


Encrypting Domino SAML Assertions



HCL SOFTWARE

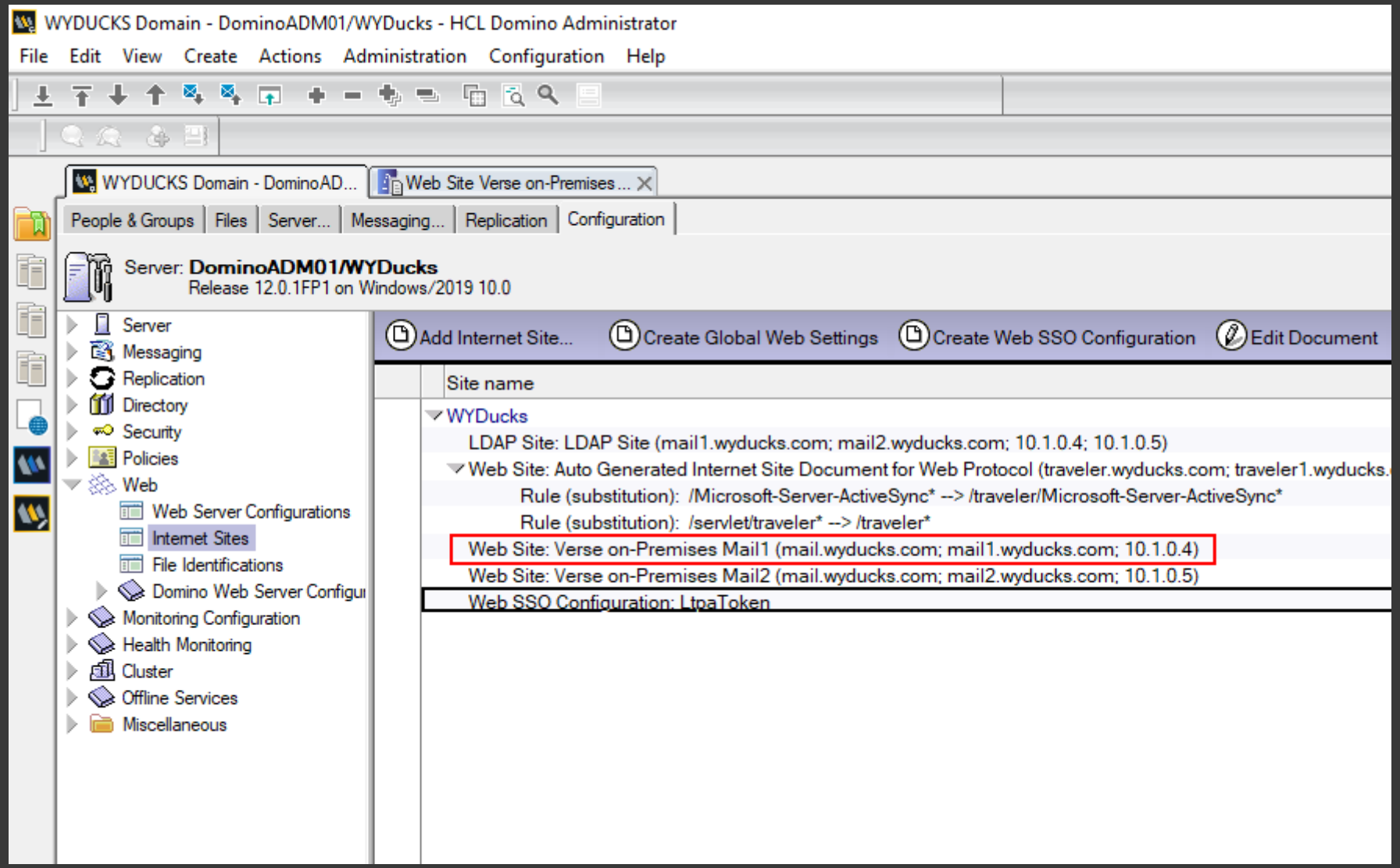
Encrypting Domino SAML Assertions



Enable SAML Authentication in Domino

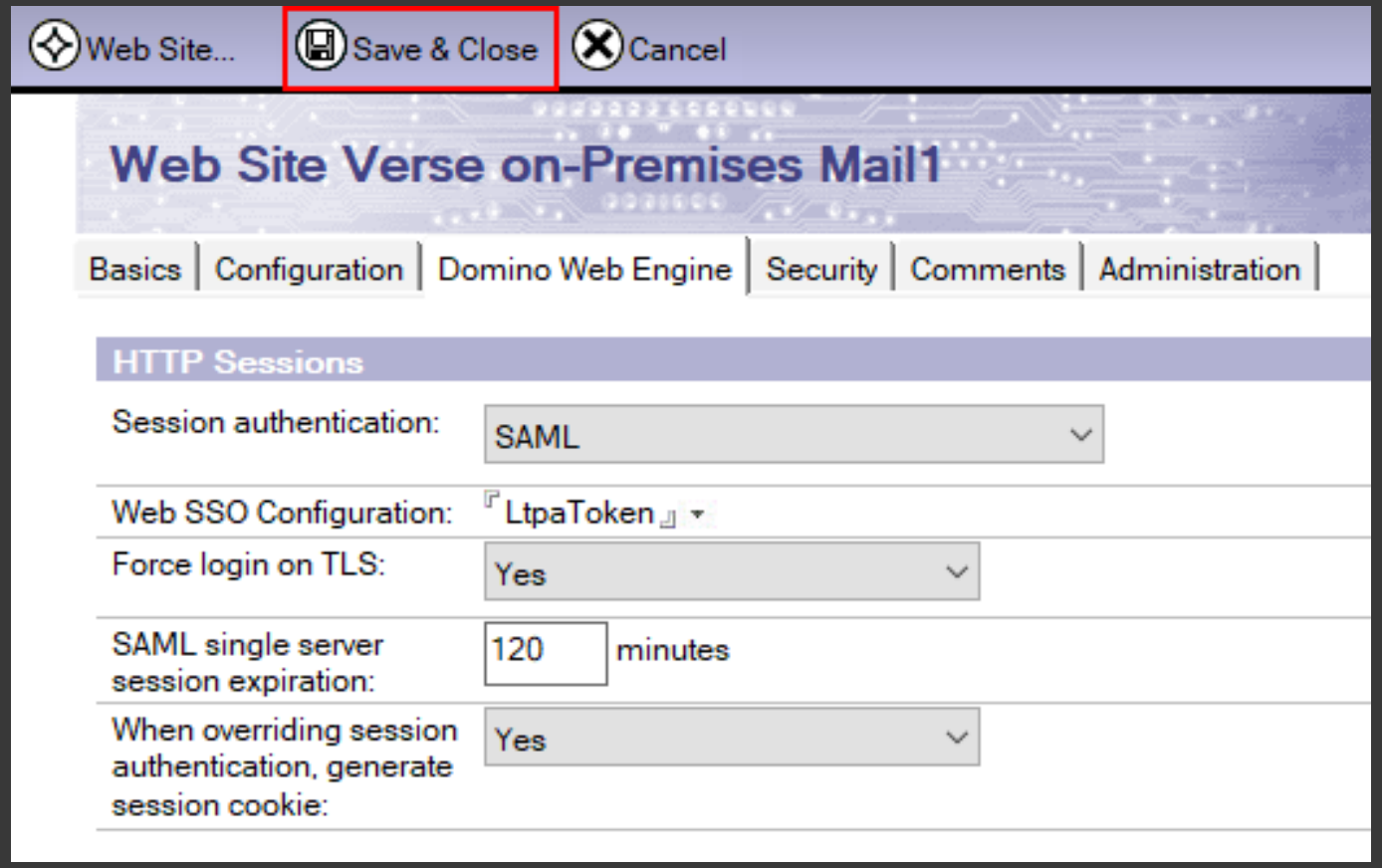
Internet Site documents

Enable SAML Authentication in Domino



HCL SOFTWARE

Enable SAML Authentication in Domino



HCL SOFTWARE

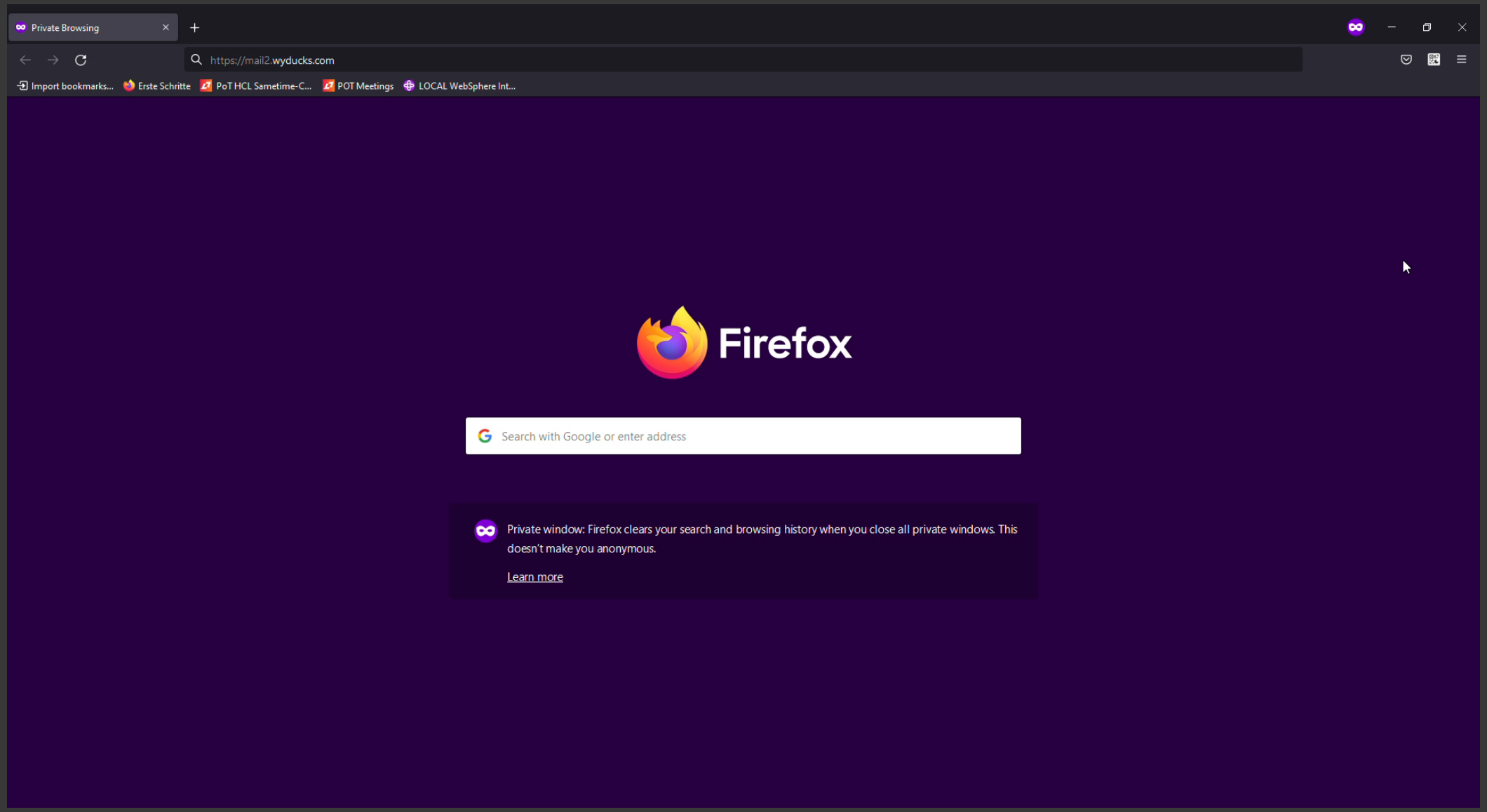
Restart

Domino Server

HTTP Task

Demo

Demo



HCL SOFTWARE

What just happened!?

External access no SSO

PW for secure mail operations

Infrastructure Needed

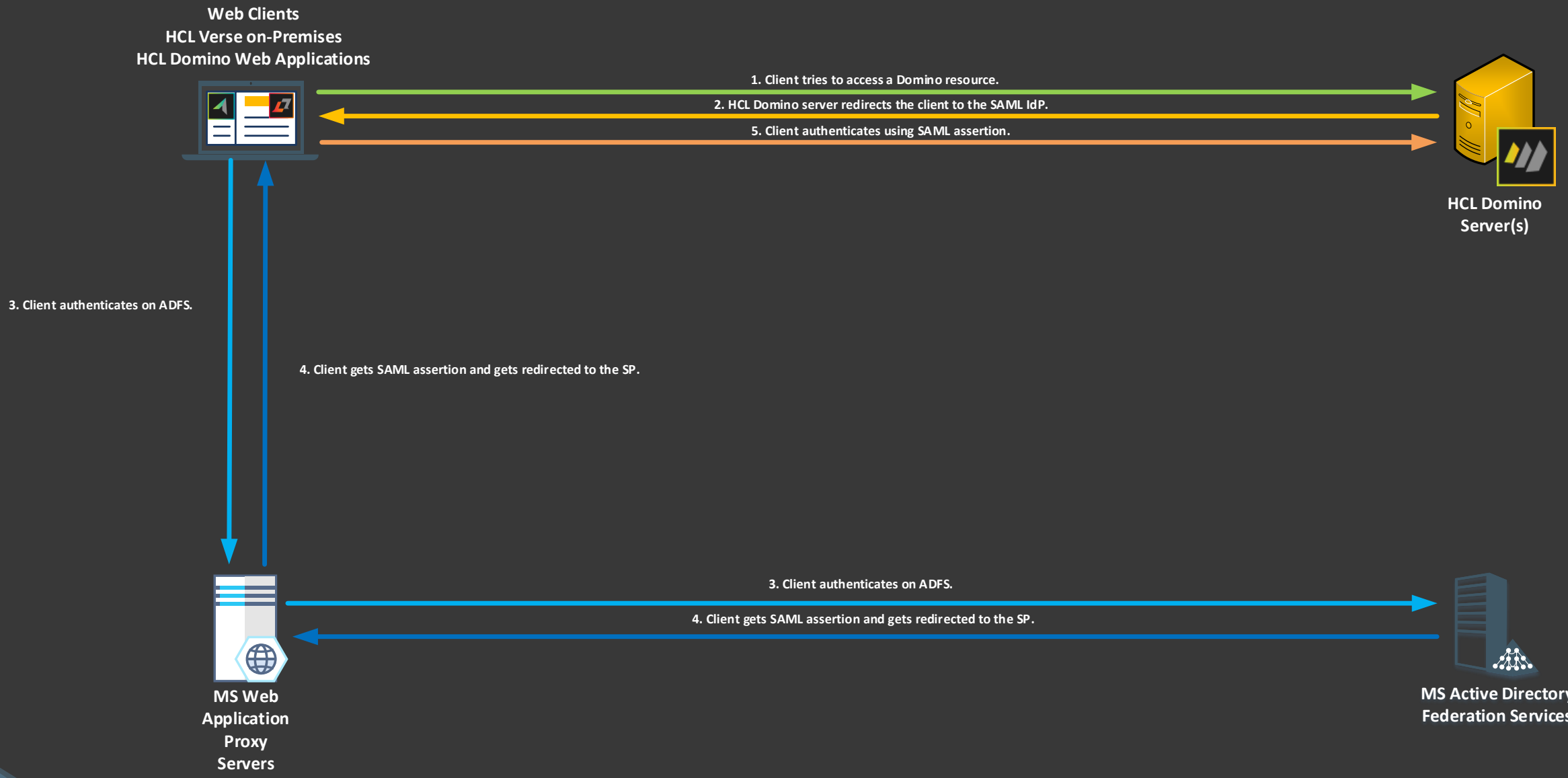


Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

SAML & SSO

Web Federated Login

Notes Federated Login

Traveler & SAML

Bonus – Nomad!

Troubleshooting

Issues

Q & A

Shibboleth

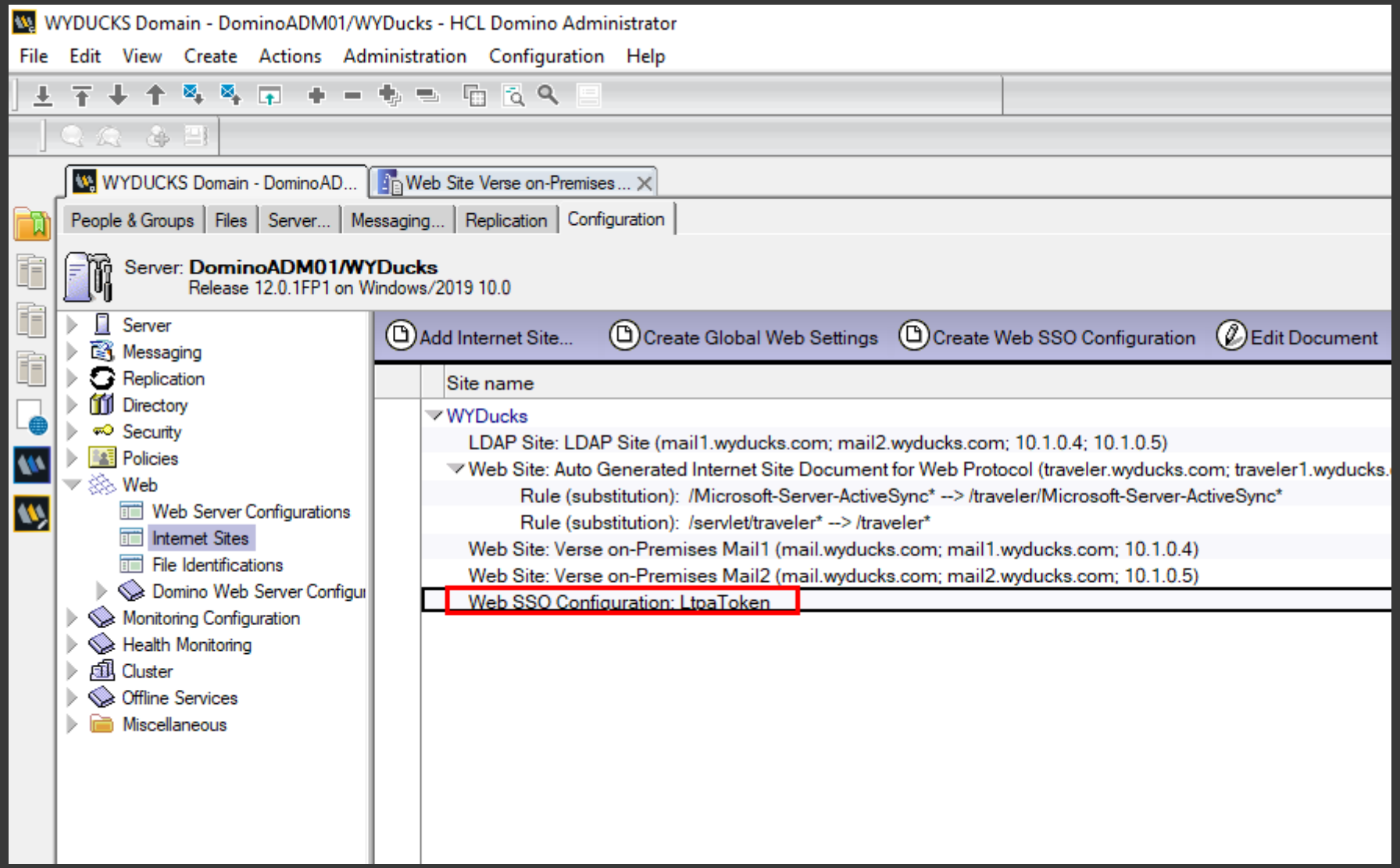
References

IdP offers SSO mechanism

IWA on ADFS

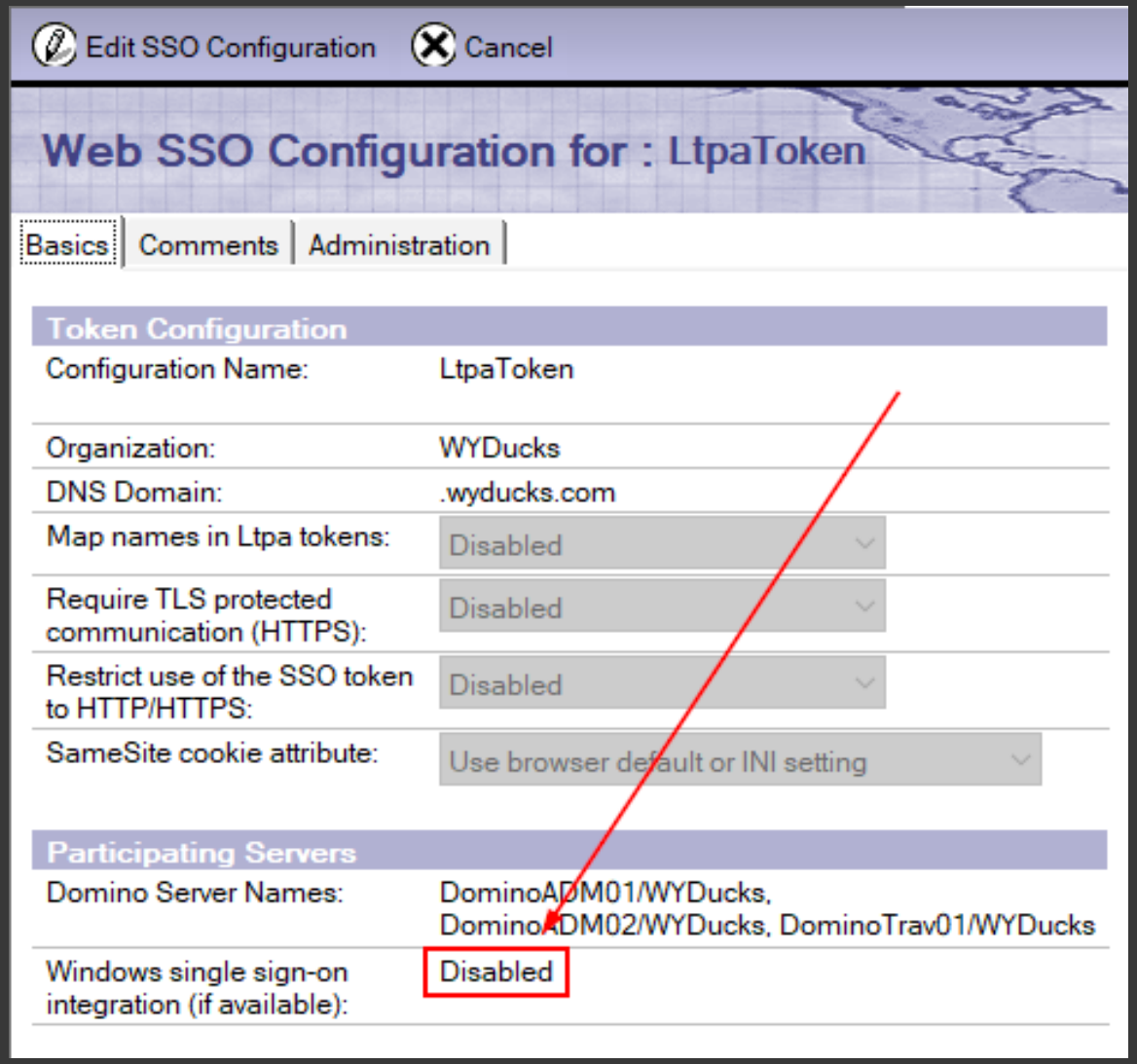
Needed Domino setting

Required Setting for IWA & SAML



HCL SOFTWARE

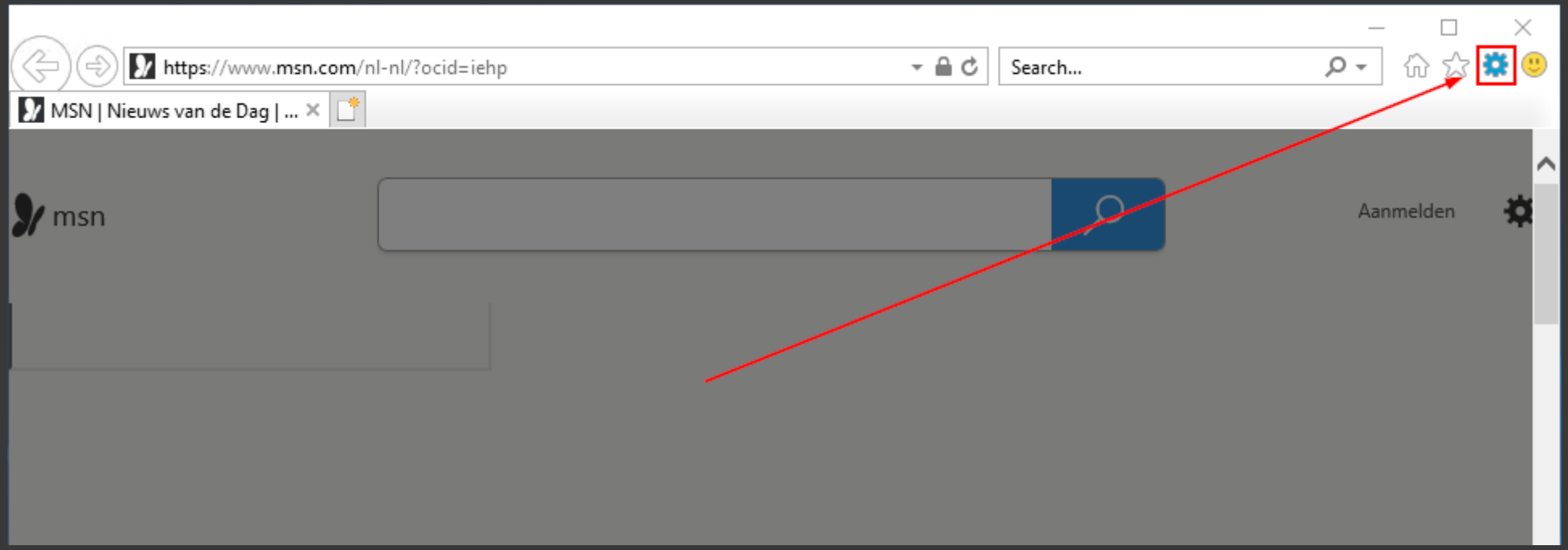
Required Setting for IWA & SAML



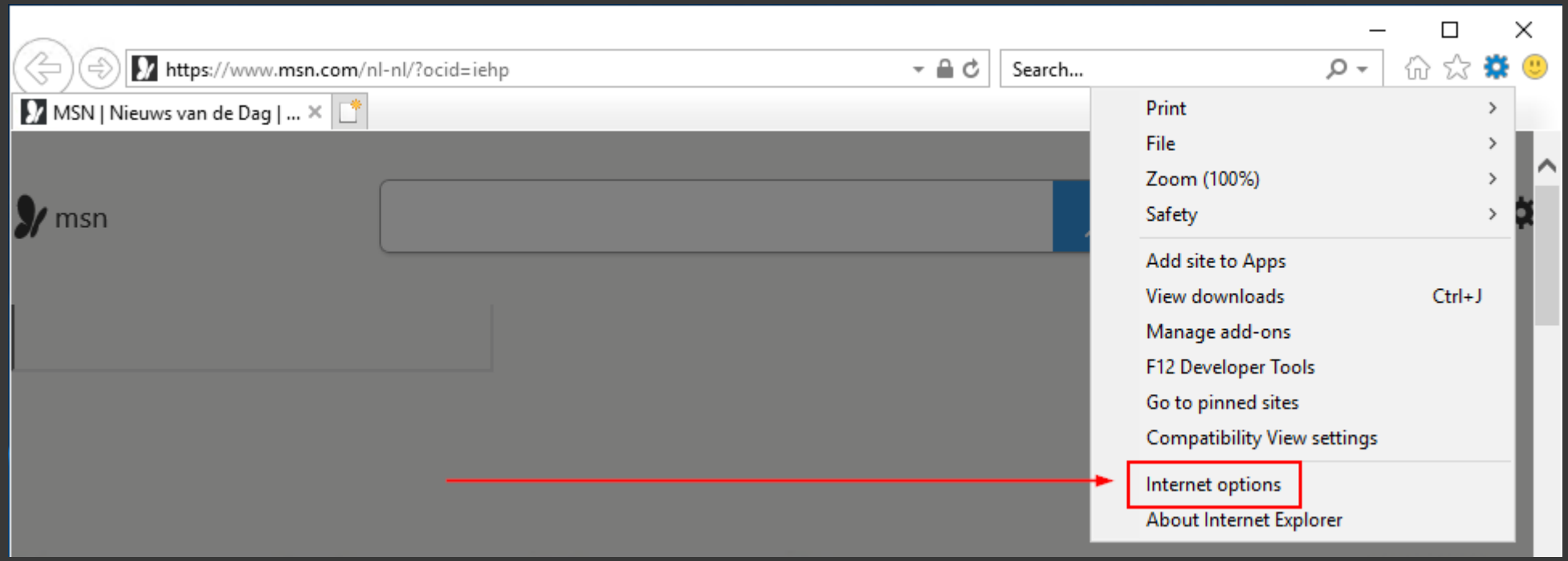
Enable IWA on IdP / ADFS

Browser configuration

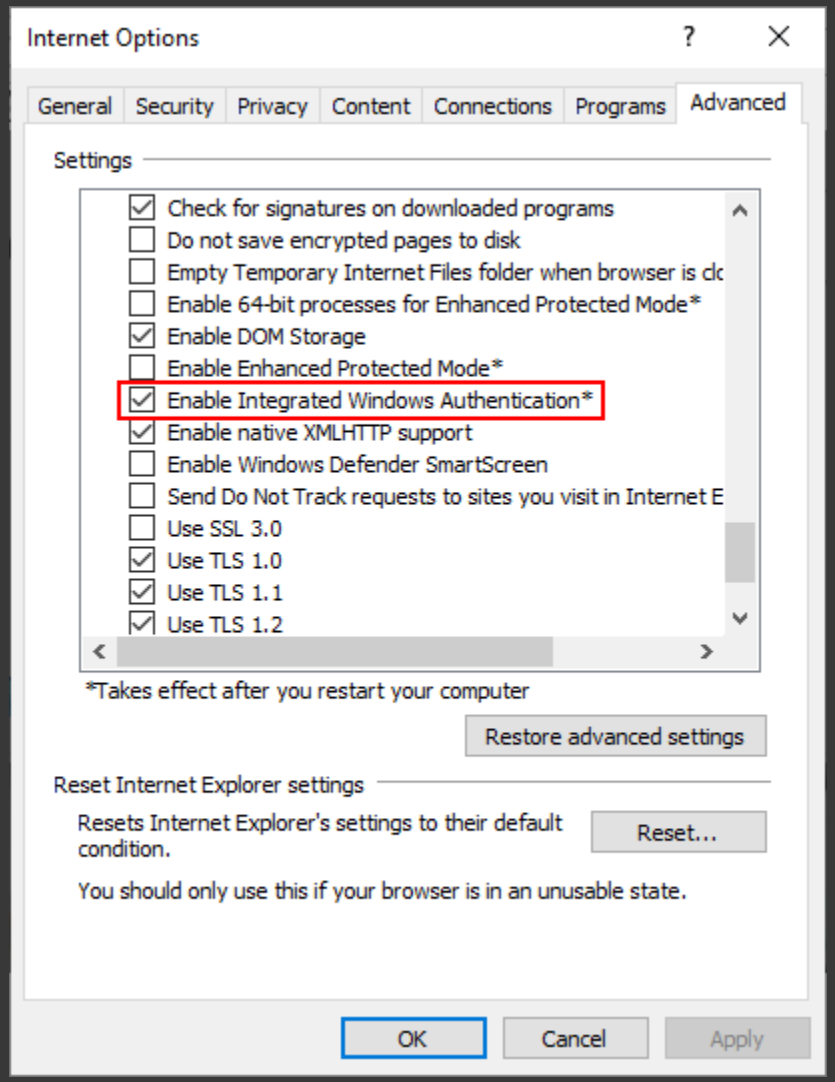
Browser Configuration



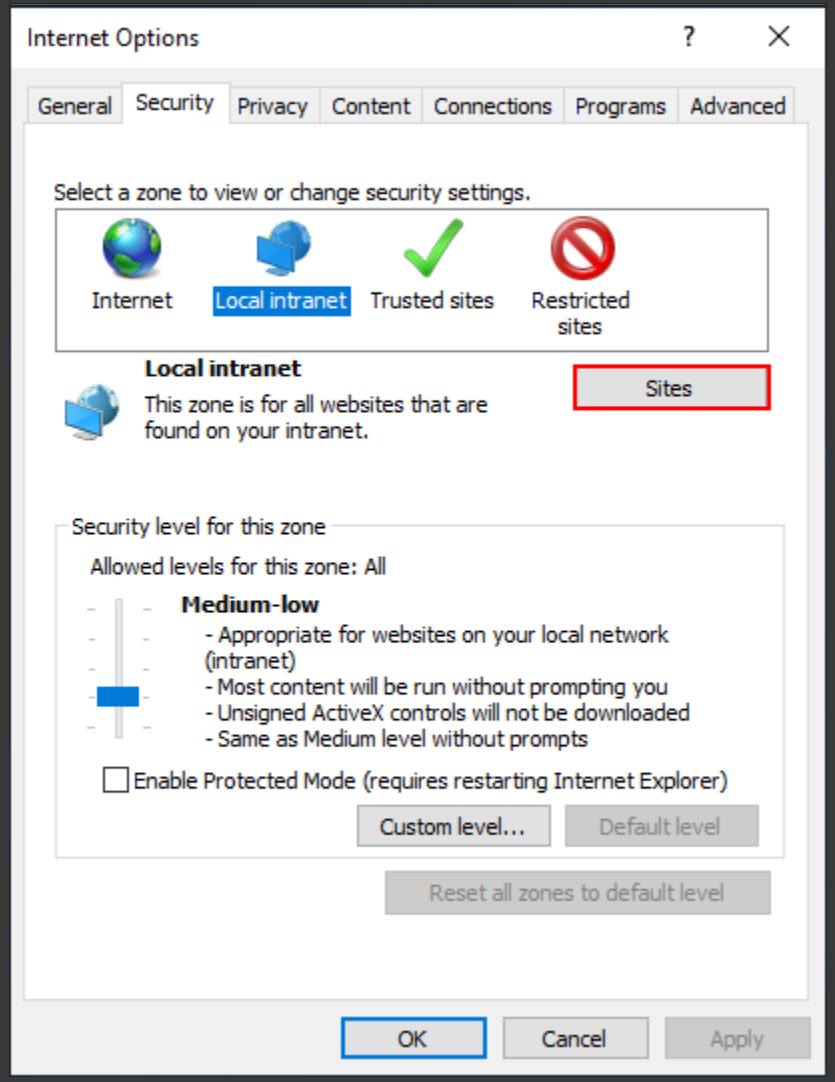
Browser Configuration



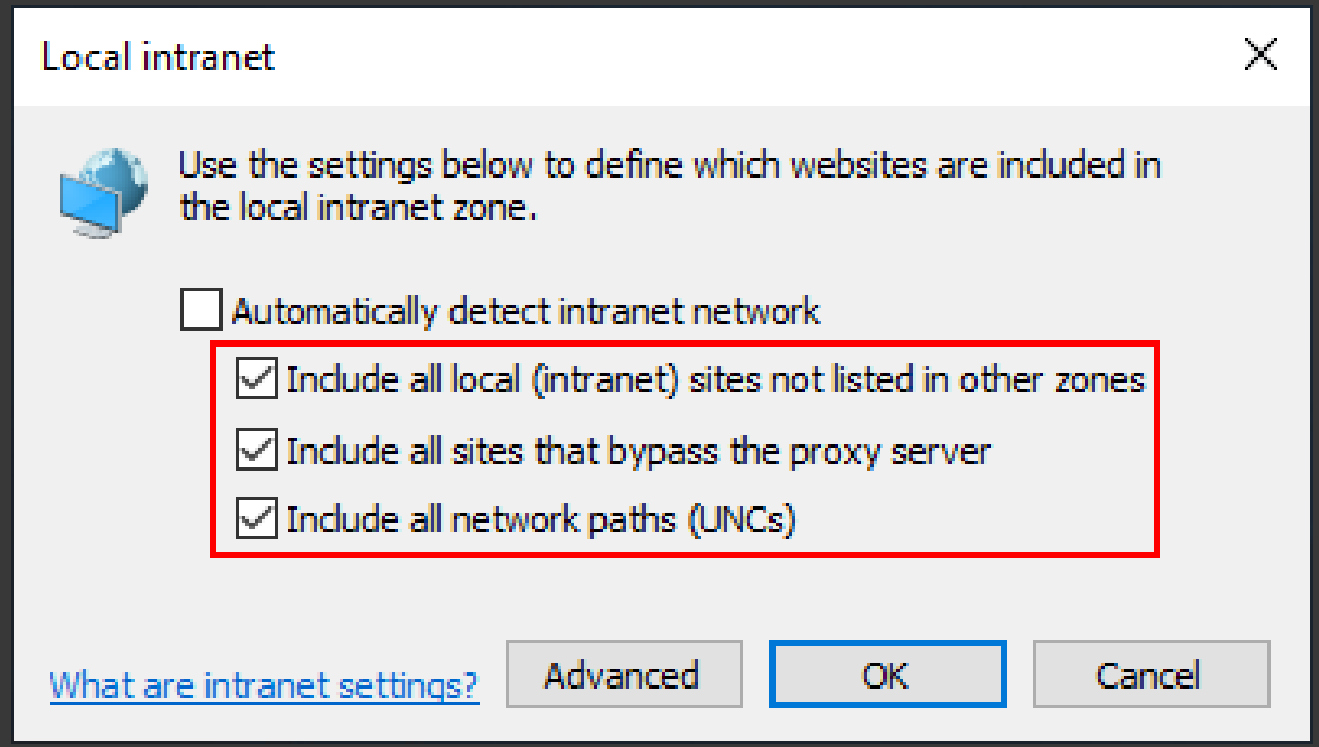
Browser Configuration



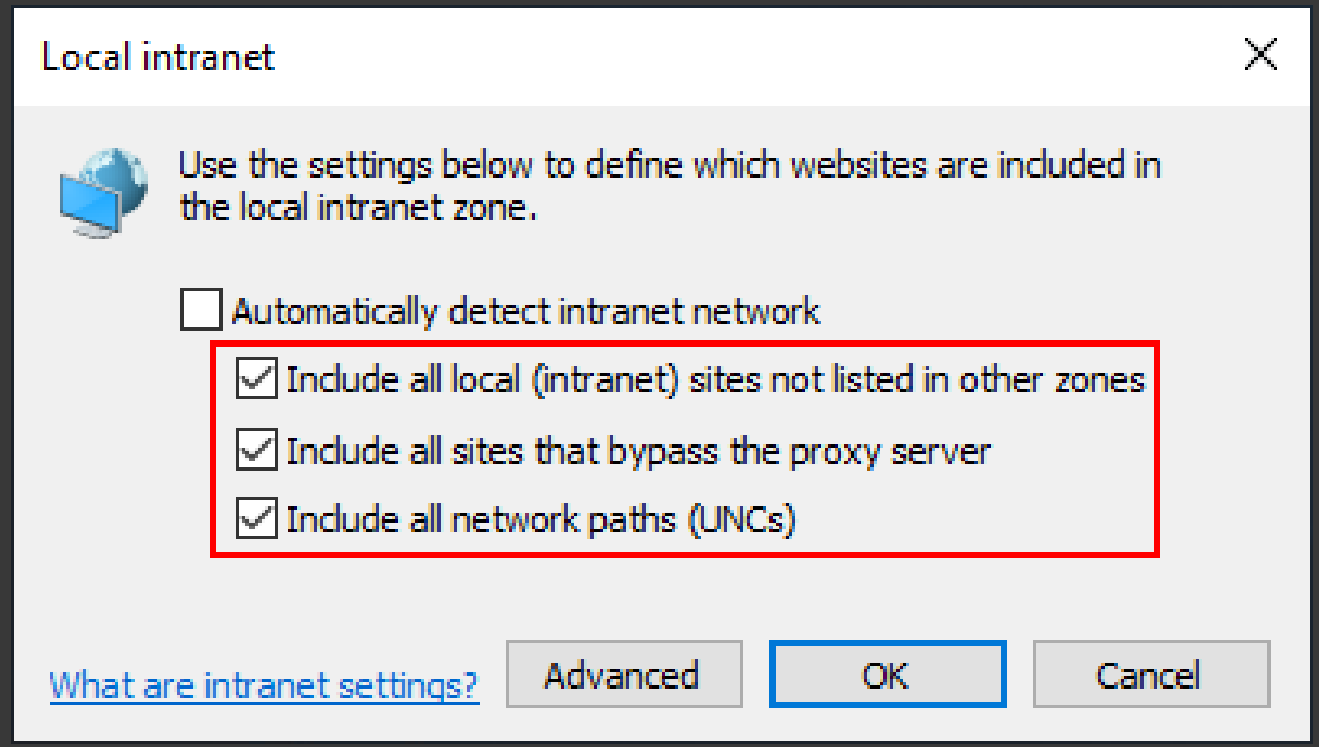
Browser Configuration



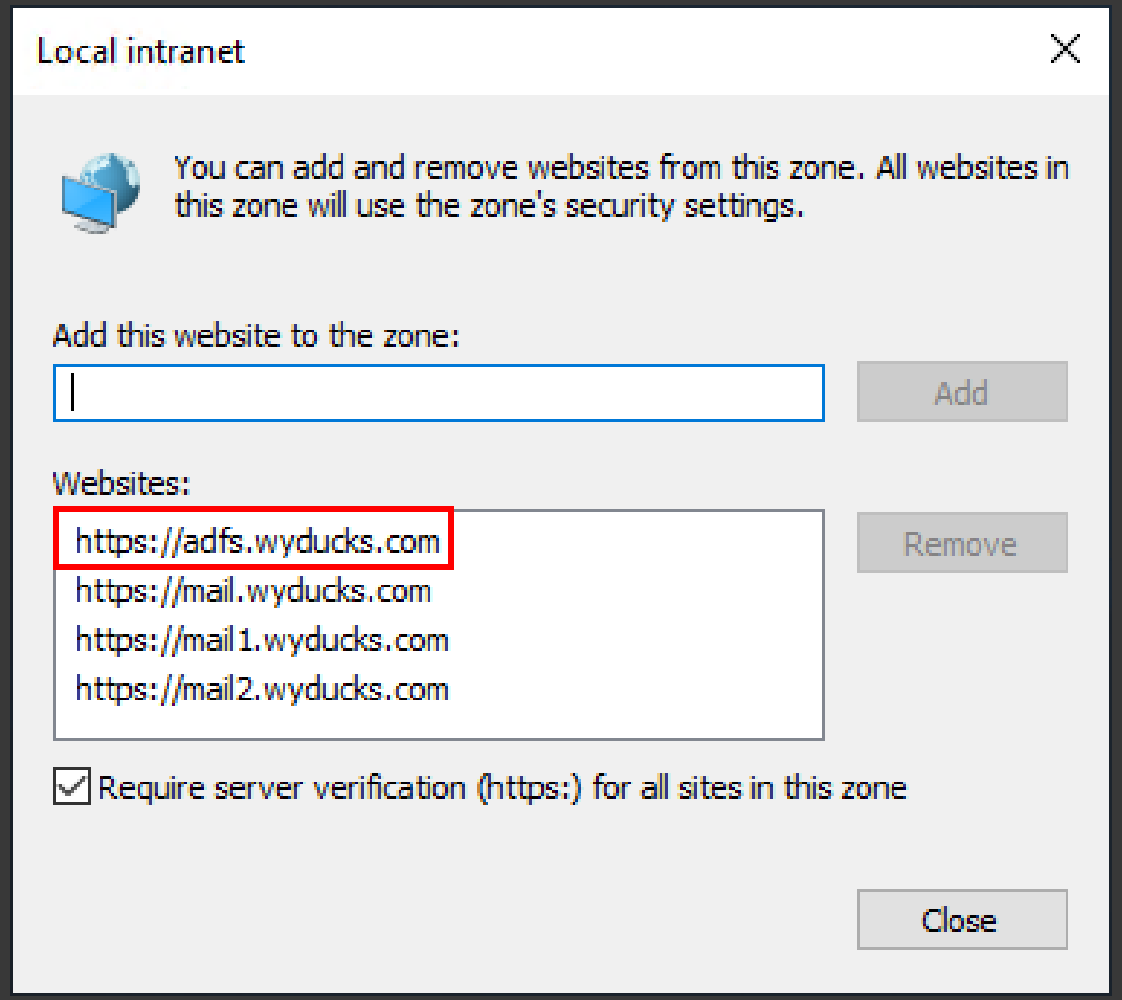
Browser Configuration



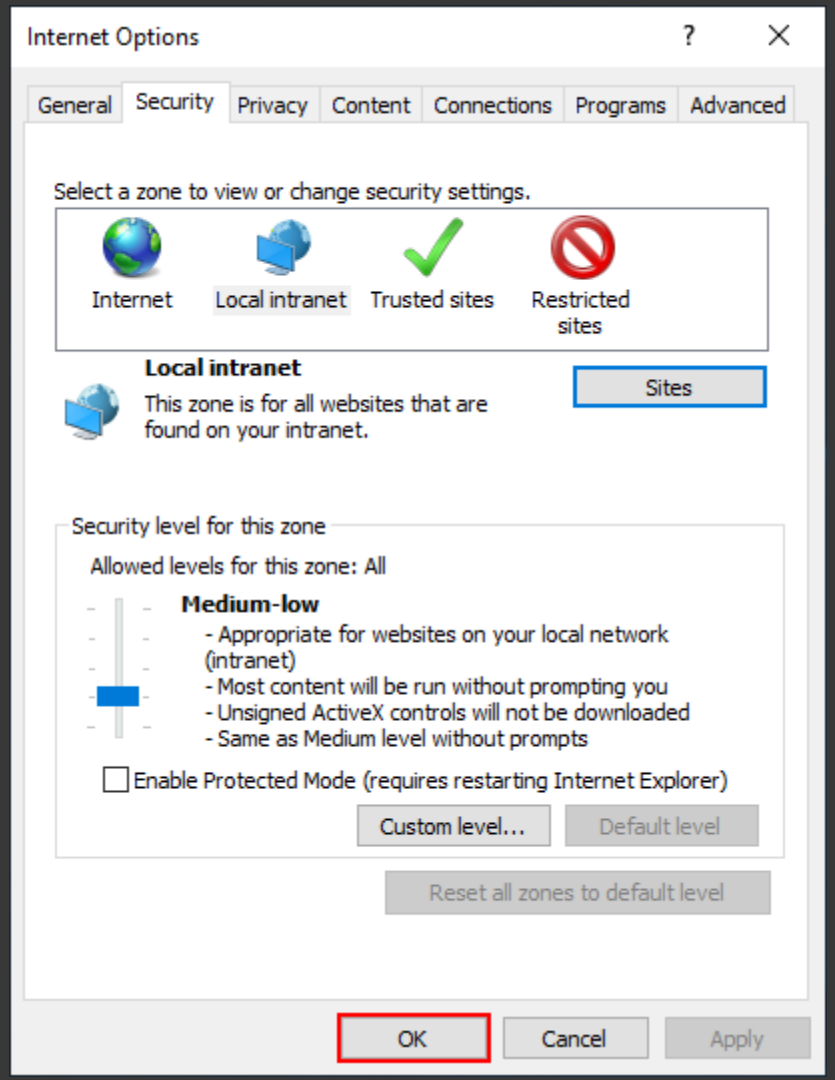
Browser Configuration



Browser Configuration

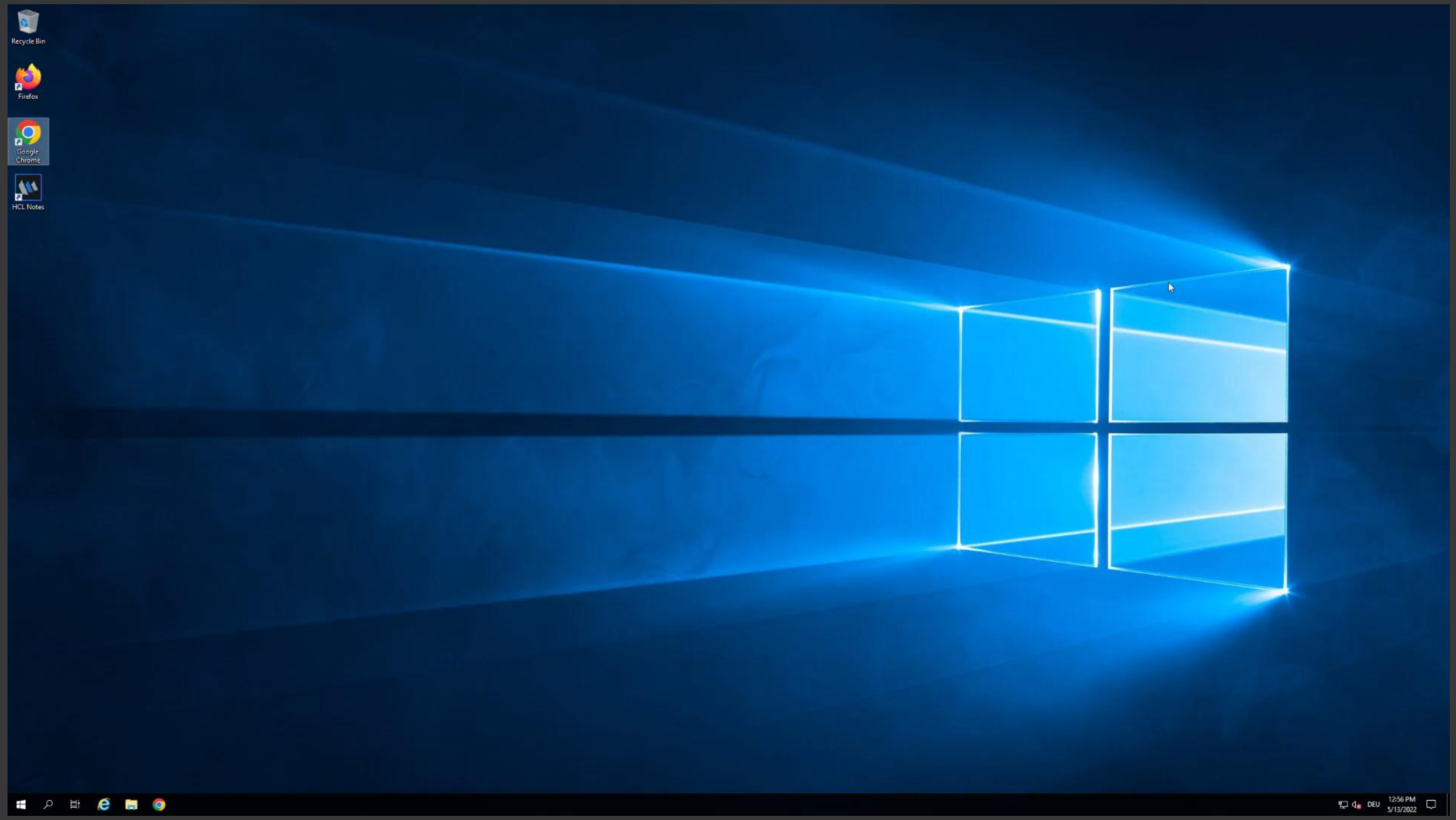


Browser Configuration



Demo

Demo



HCL SOFTWARE

What just happened!?

IdP accepts IWA

From all internal HTTPS connections

Infrastructure Needed

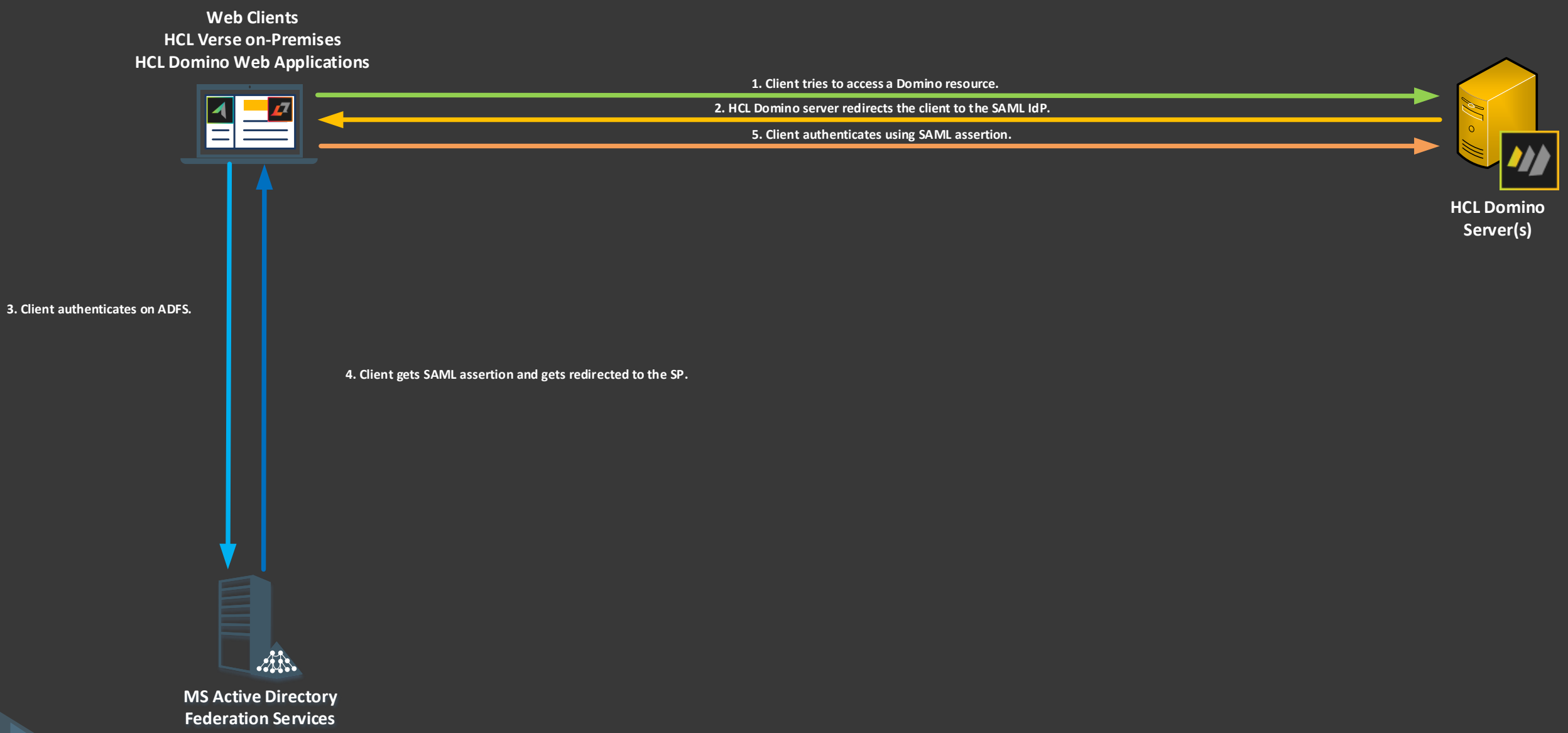


Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

SAML & SSO

Web Federated Login

Notes Federated Login

Traveler & SAML

Bonus – Nomad!

Troubleshooting

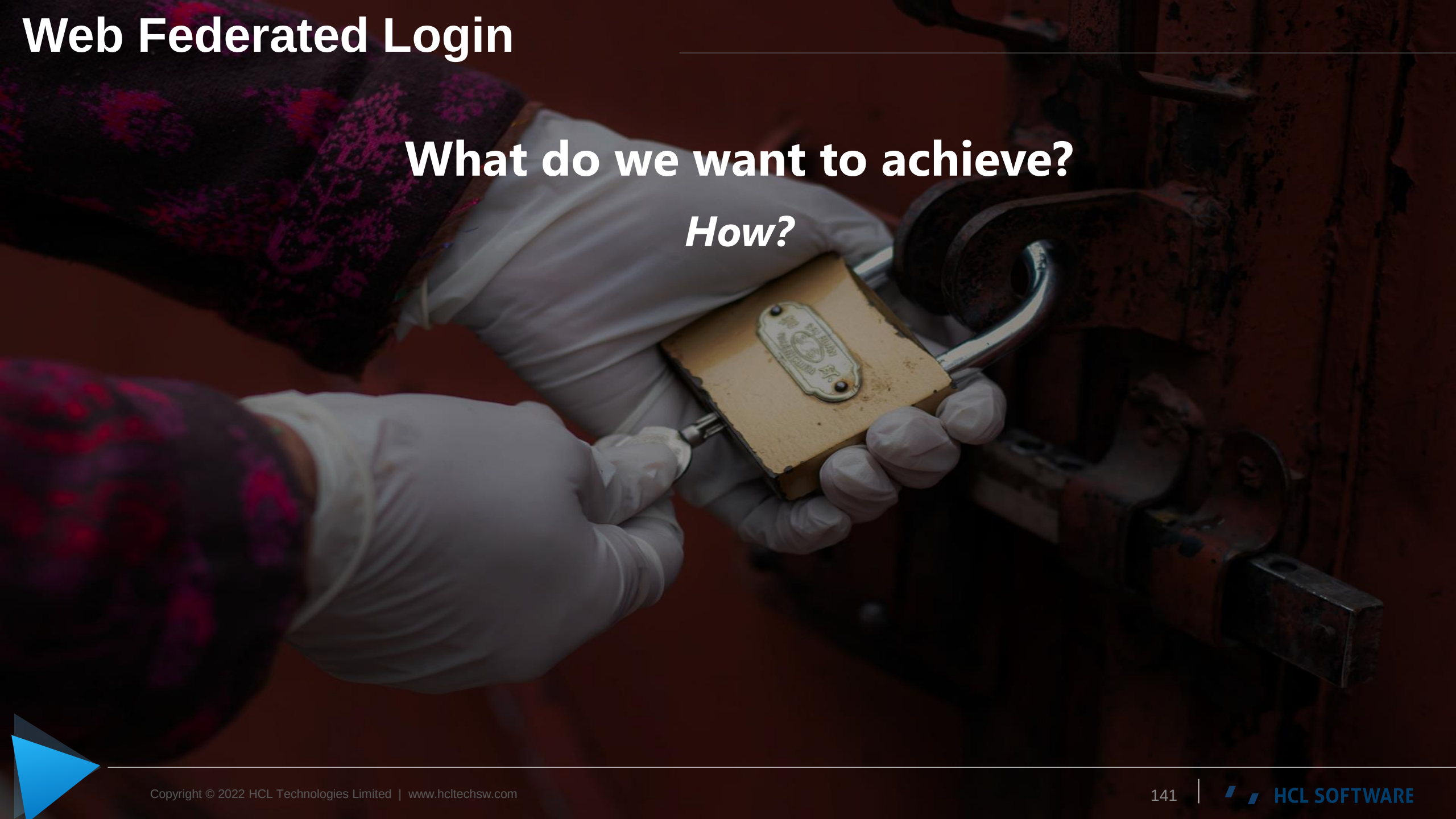
Issues

Q & A

Shibboleth

References

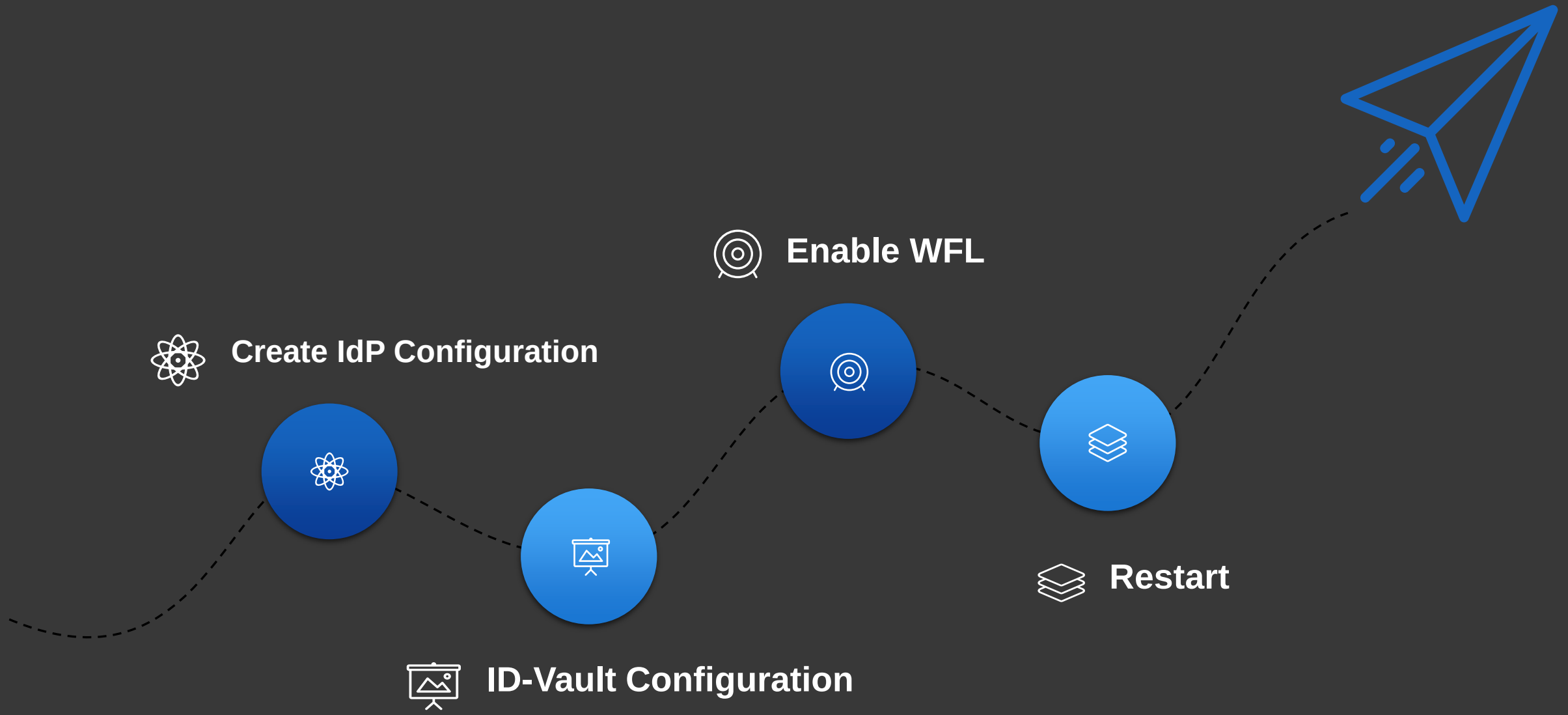
Web Federated Login



What do we want to achieve?

How?

Web Federated Login

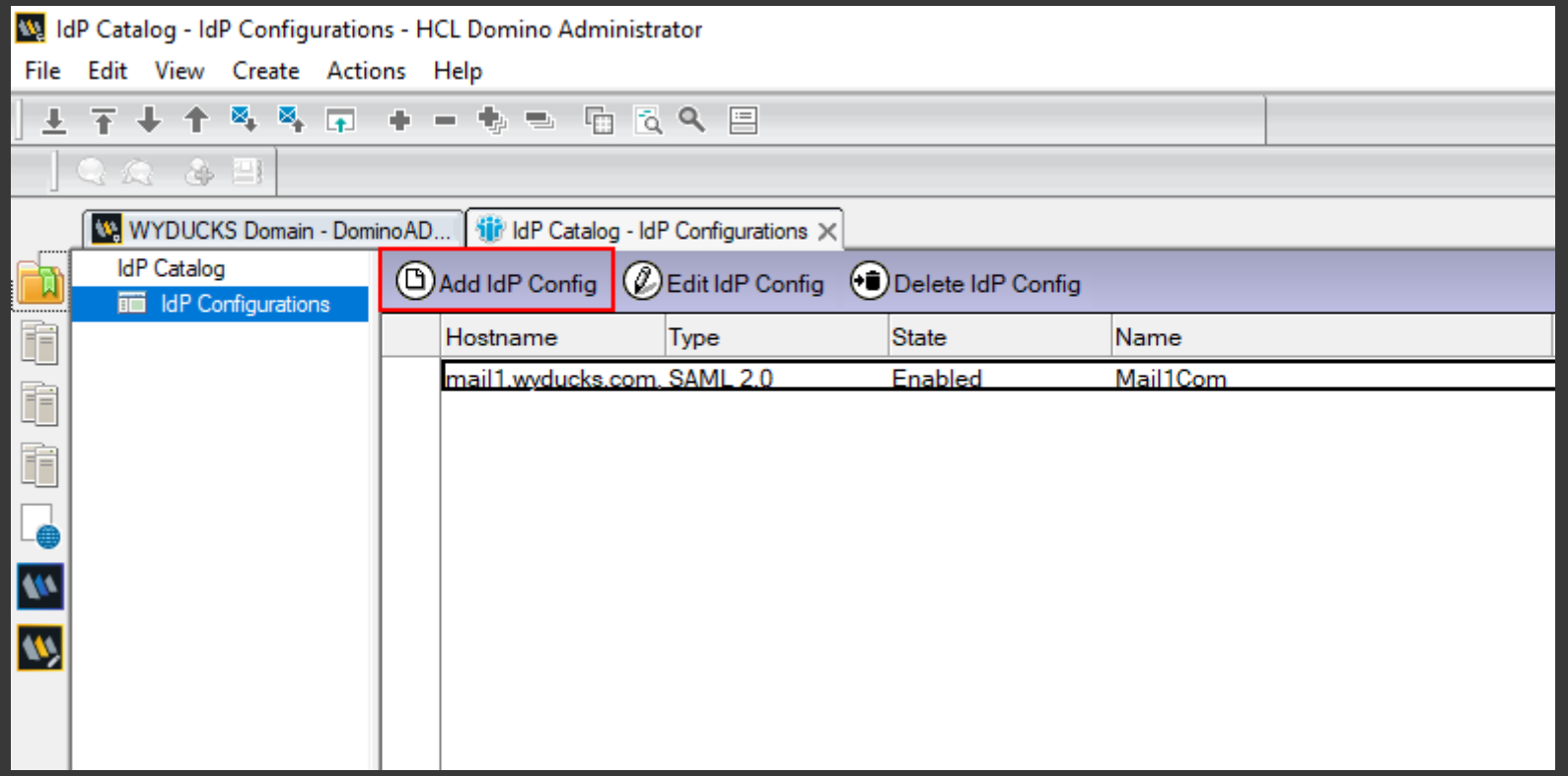


HCL SOFTWARE

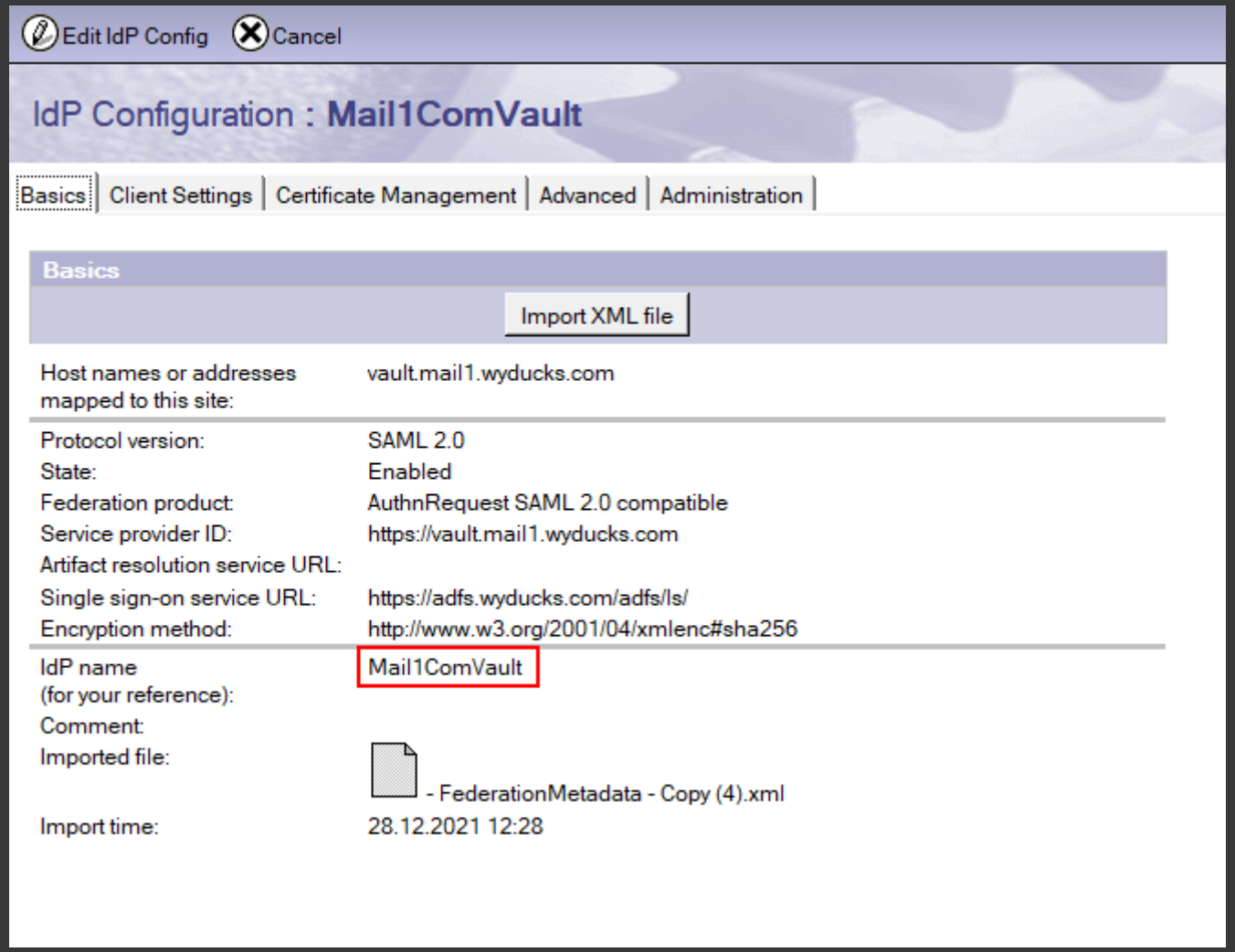
Create the IdP Configuration Document

Inside of “idpcat.nsf”

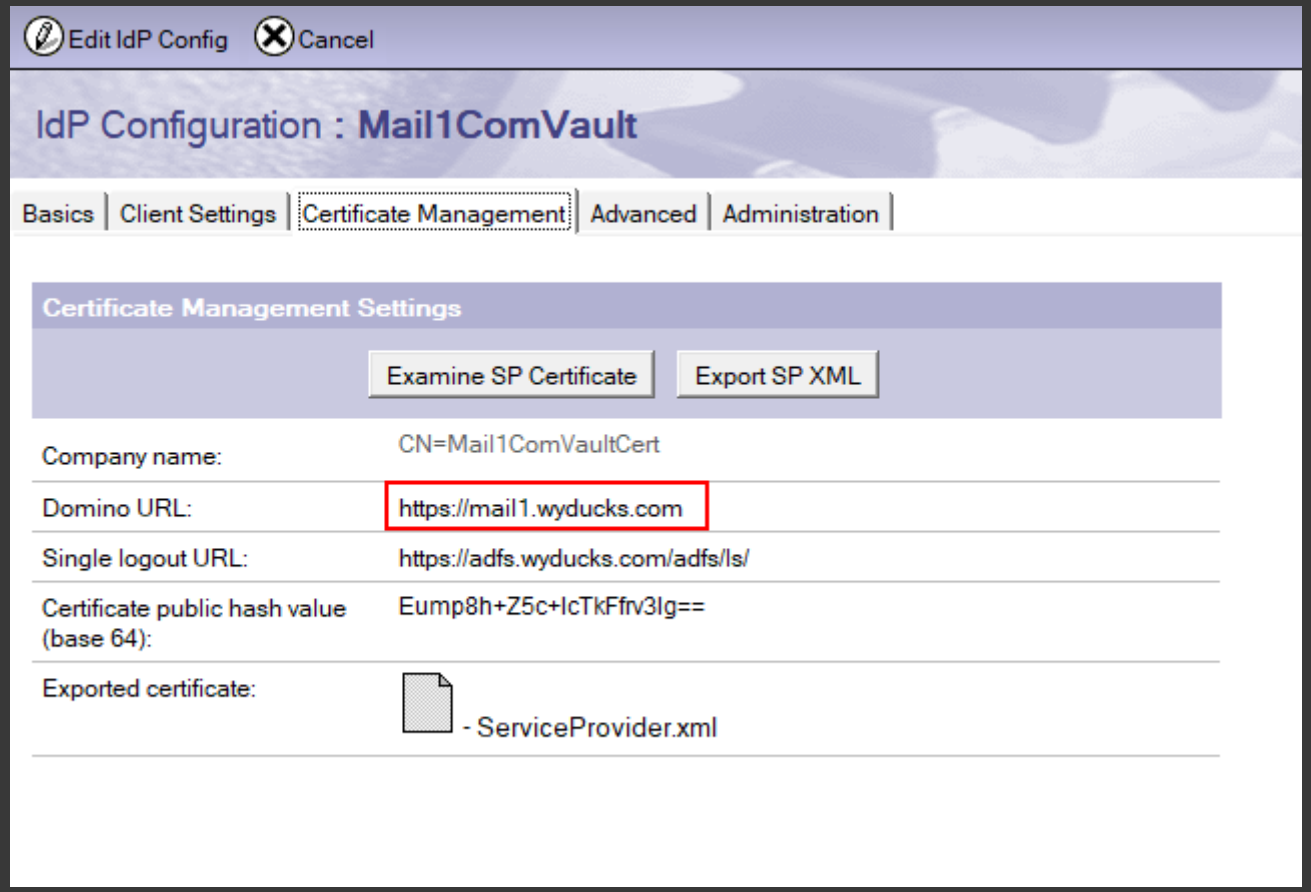
Create the IdP Configuration Document



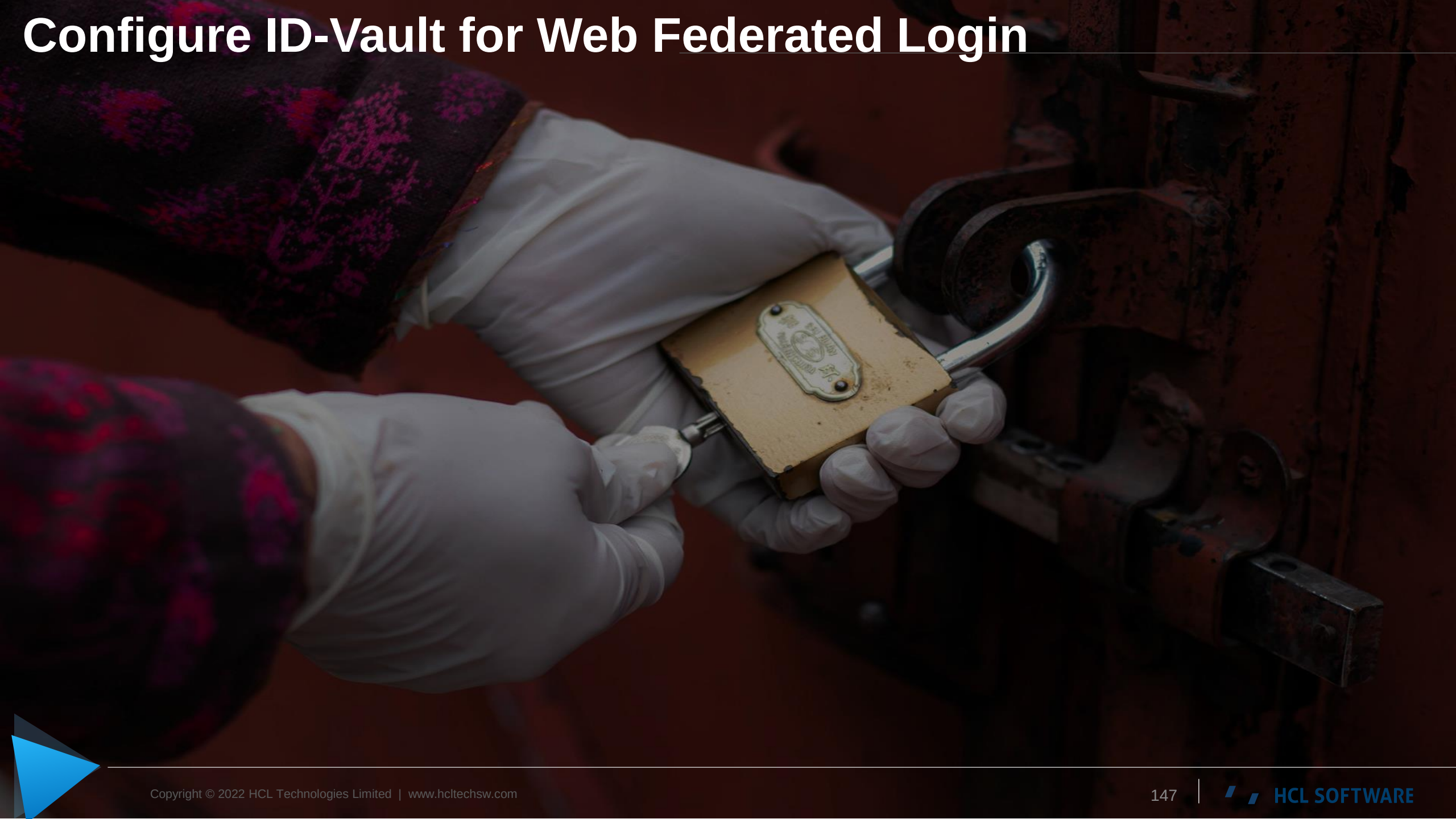
Create the IdP Configuration Document



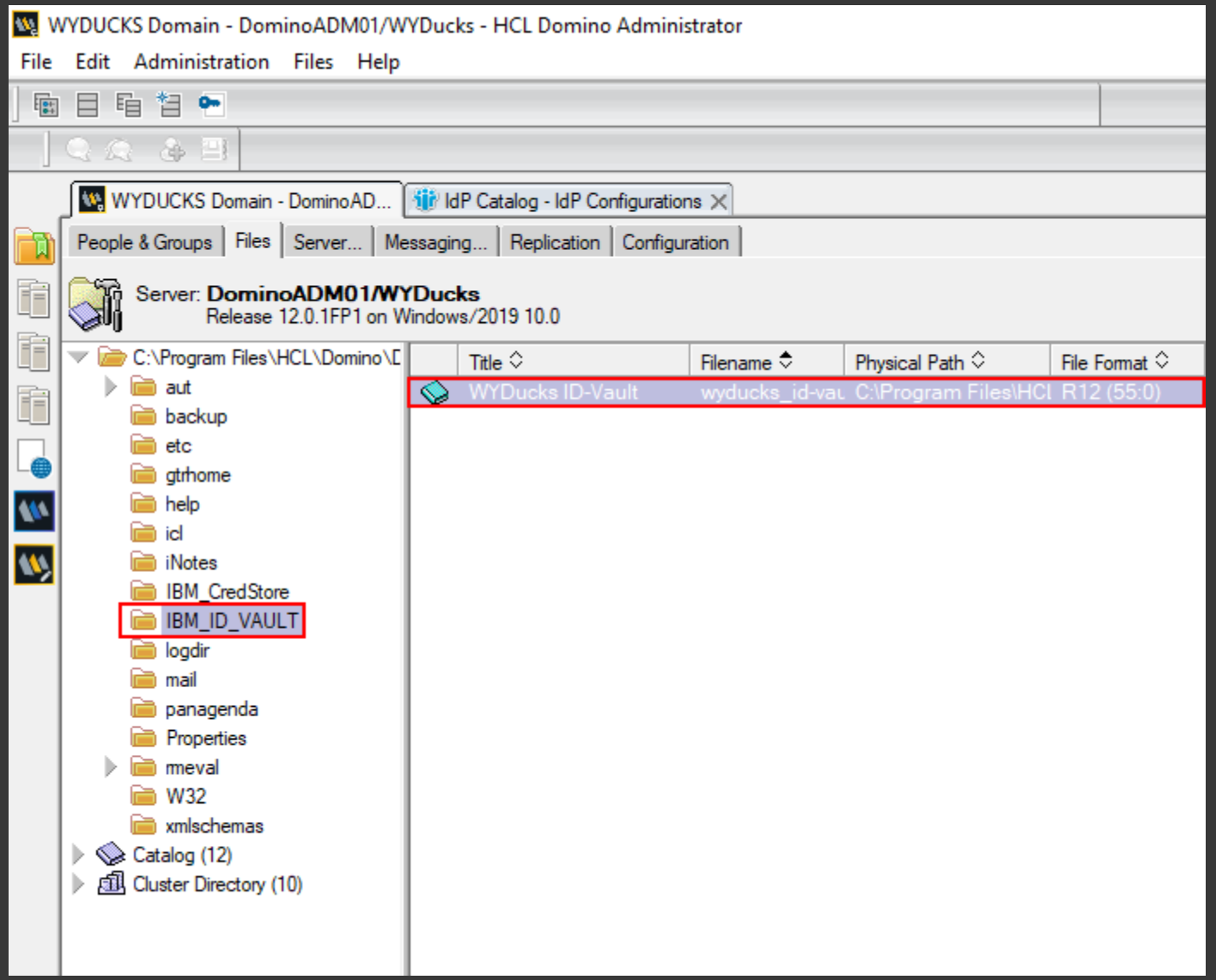
Encrypting Domino SAML Assertions



Configure ID-Vault for Web Federated Login

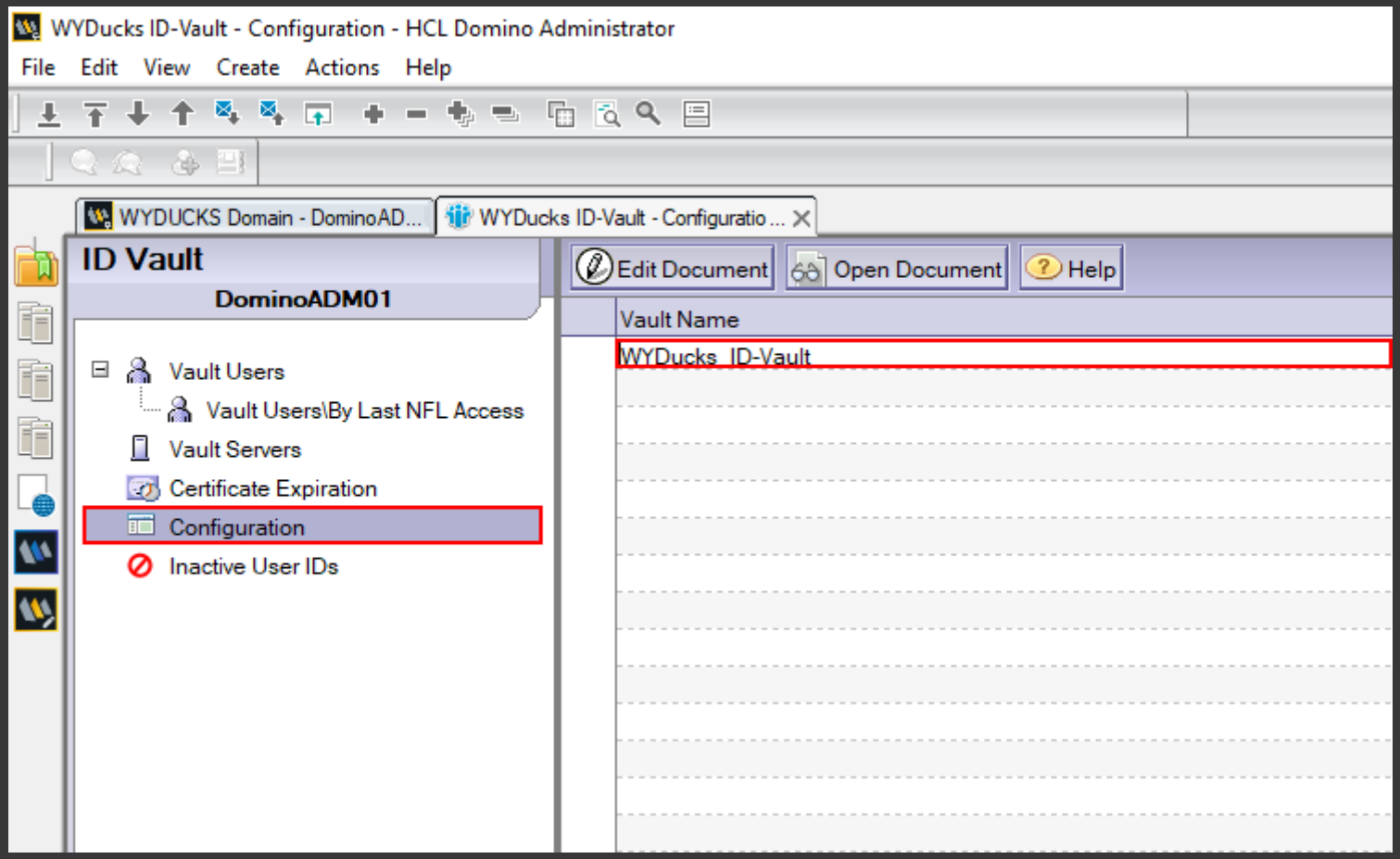


Configure ID-Vault for Web Federated Login



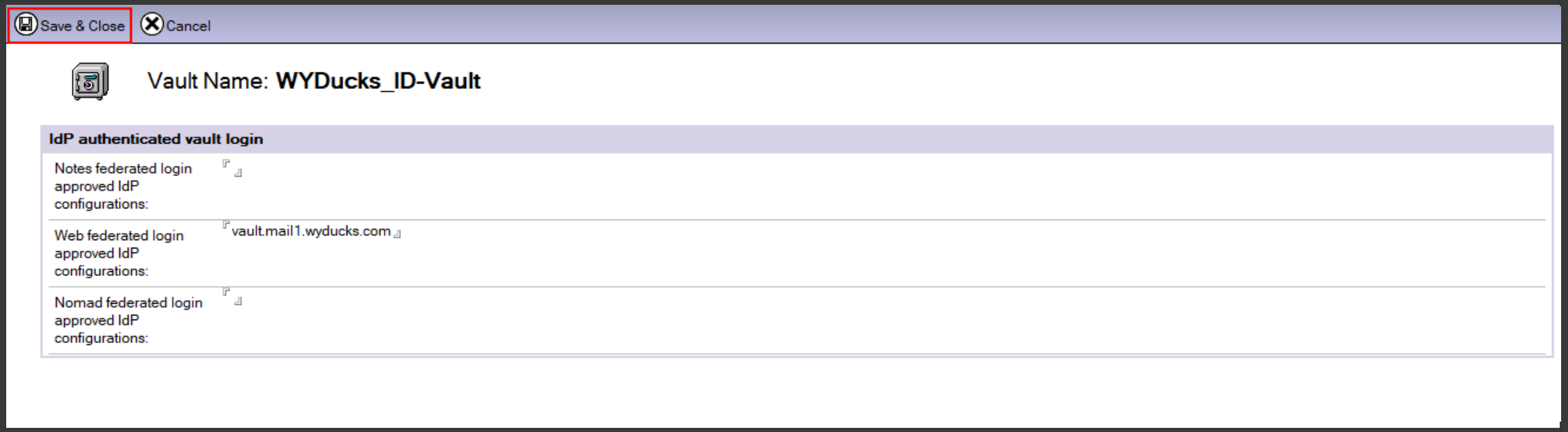
HCL SOFTWARE

Configure ID-Vault for Web Federated Login



HCL SOFTWARE

Configure ID-Vault for Web Federated Login

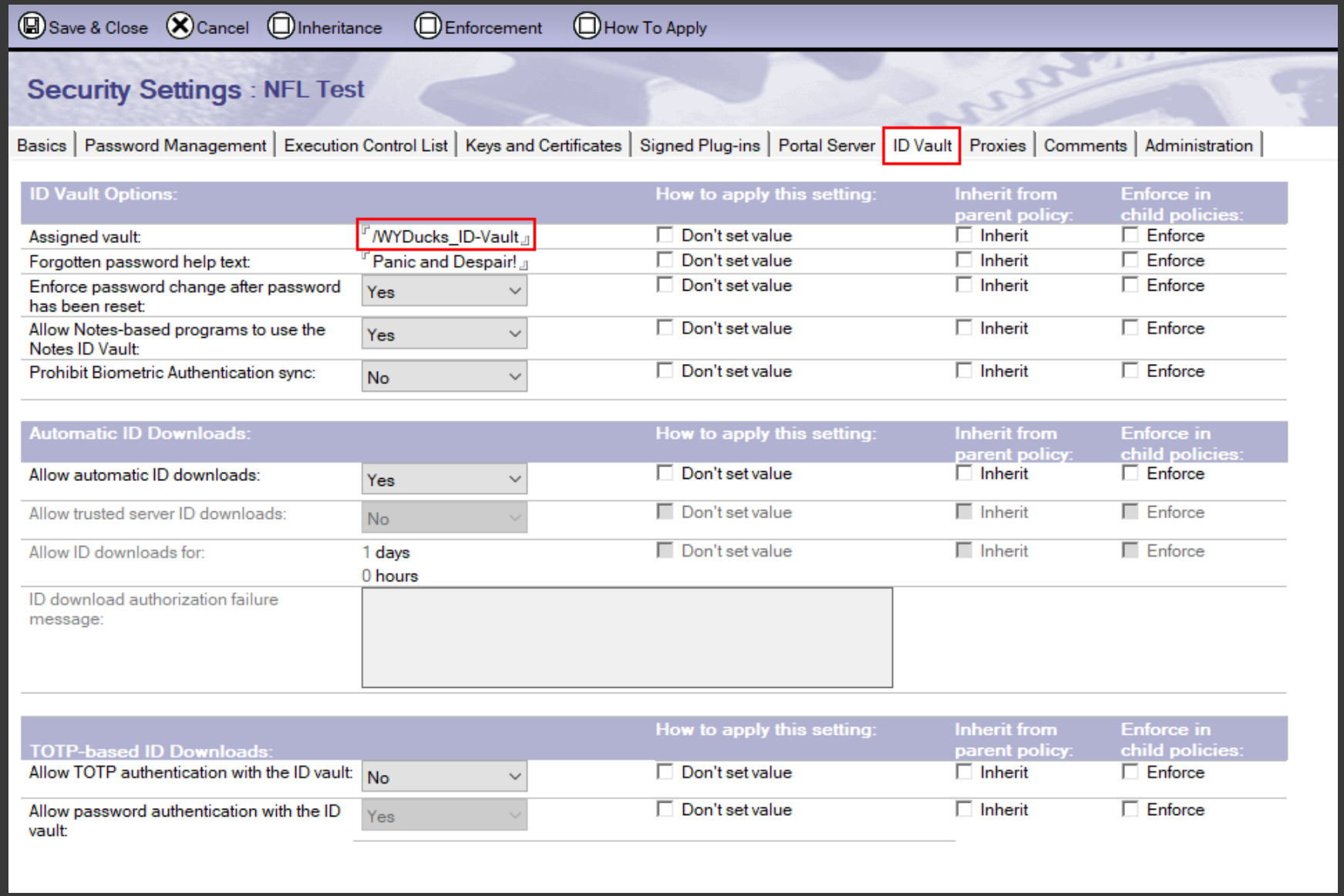


Enable Web Federated Login

How can we do that?

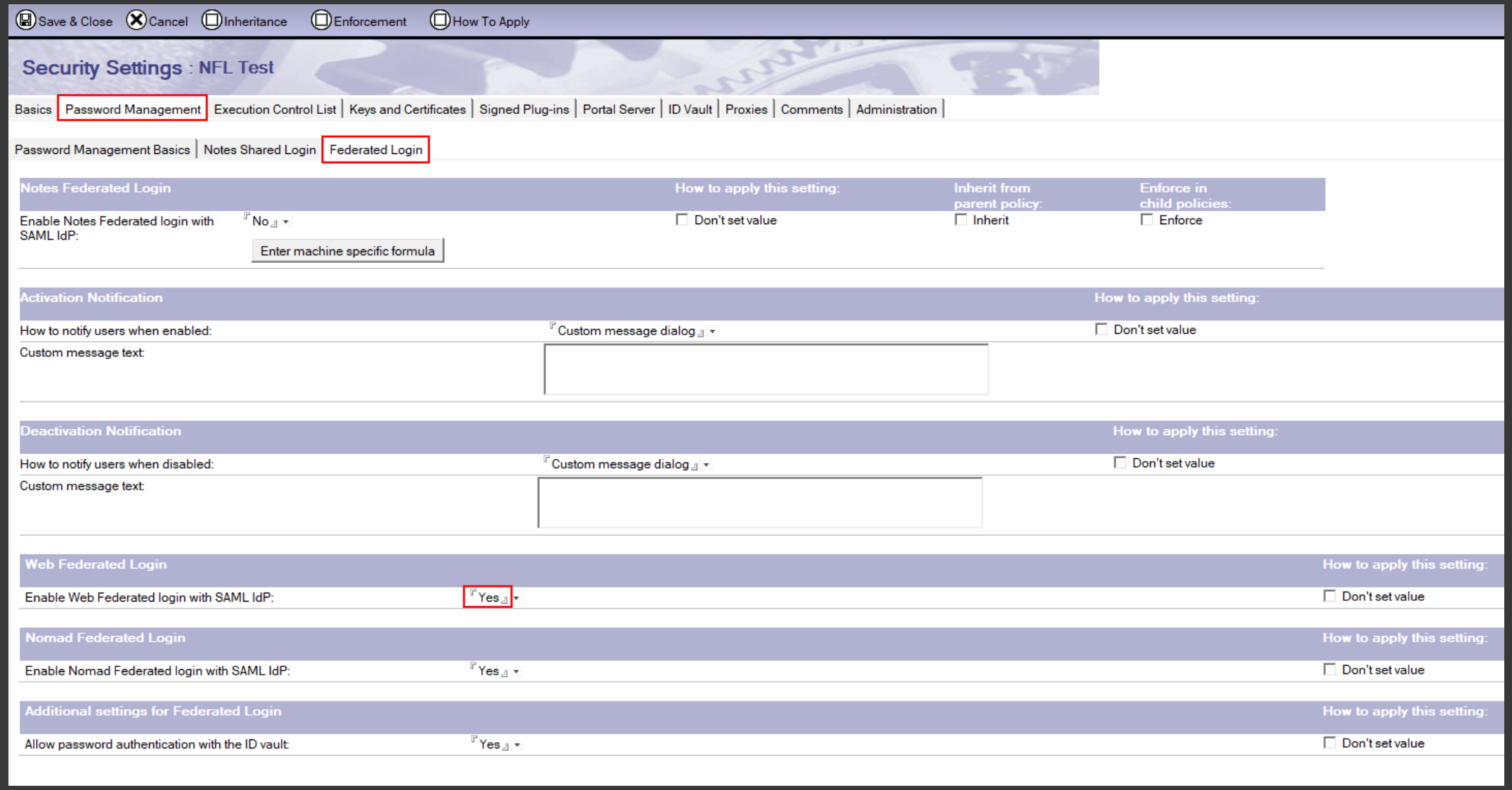
With a Domino Policy!

Enable Web Federated Login



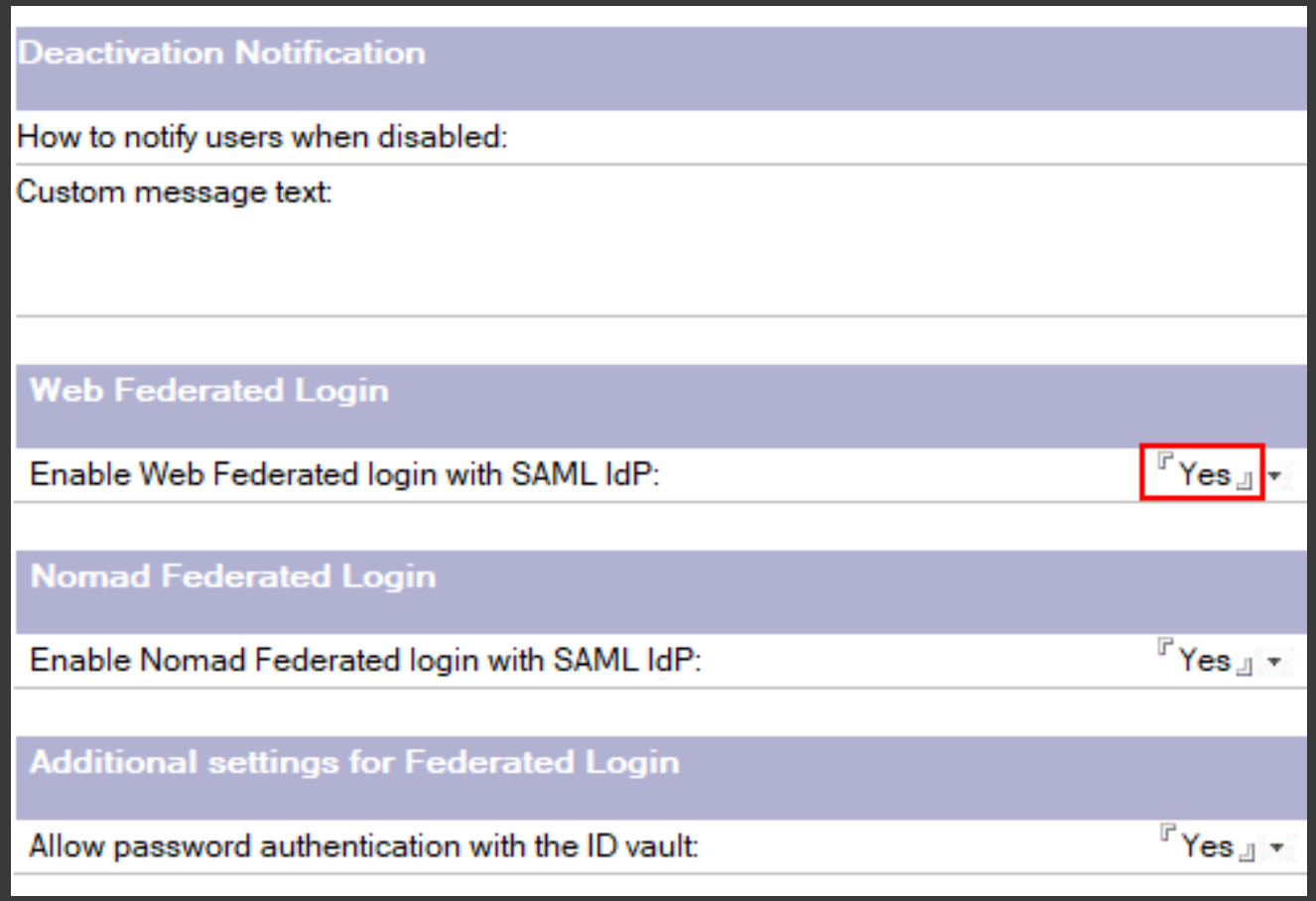
HCL SOFTWARE

Enable Web Federated Login



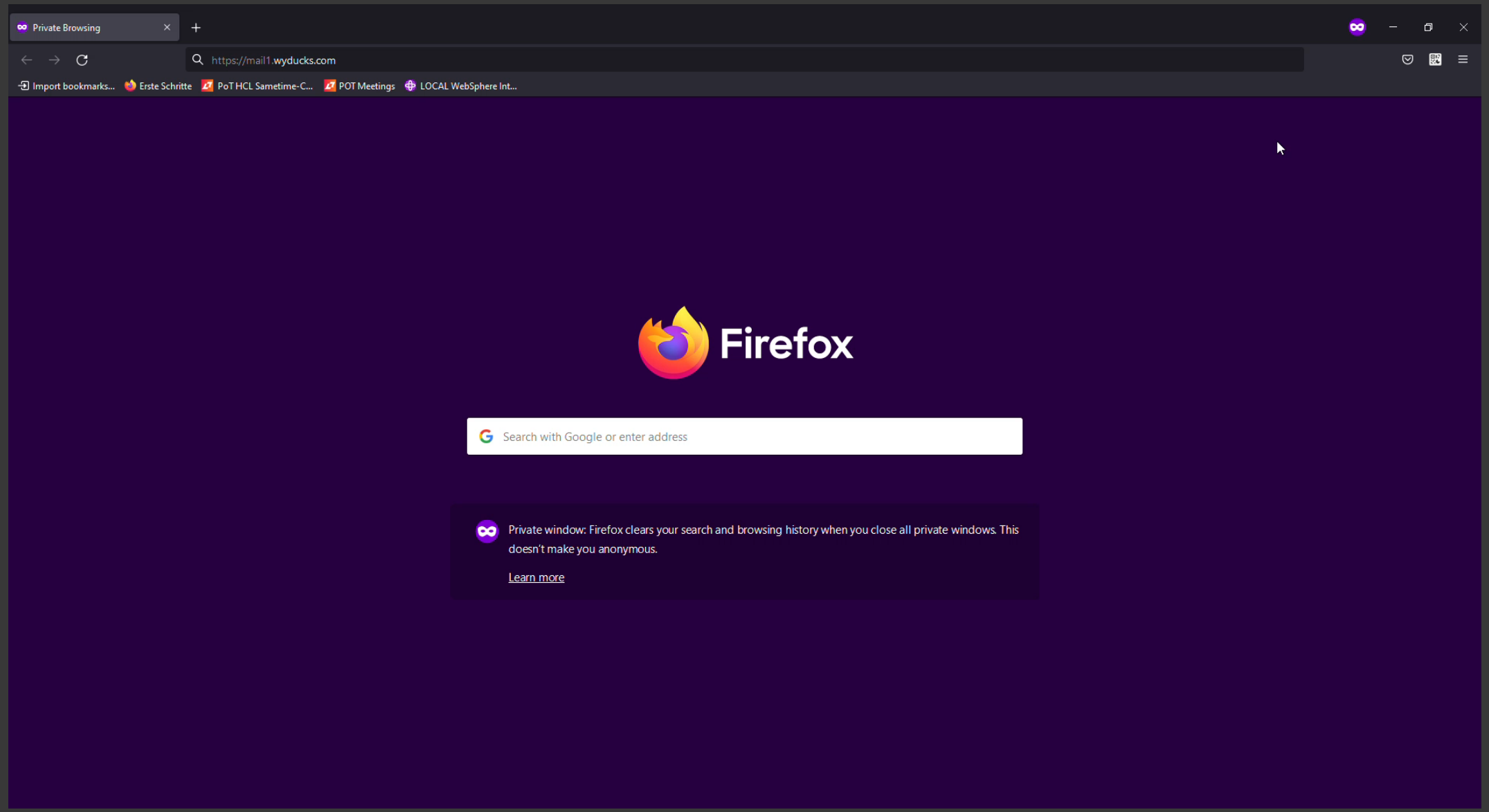
HCL SOFTWARE

Enable Web Federated Login



Demo

Demo



HCL SOFTWARE

What Just Happened!?

Secure Mail Operations

Without entering the ID-Password

Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

SAML & SSO

Web Federated Login

Notes Federated Login

Traveler & SAML

Bonus – Nomad!

Troubleshooting

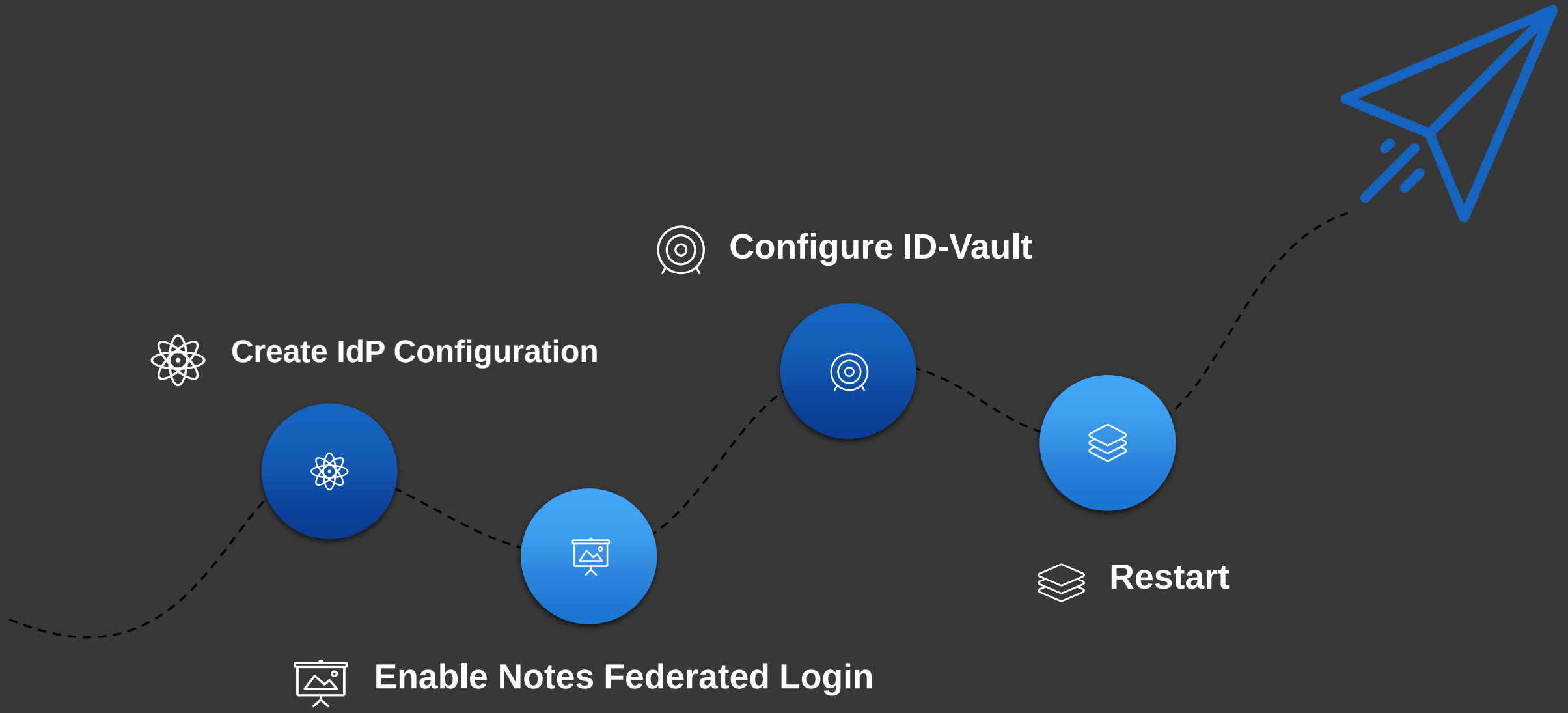
Issues

Q & A

Shibboleth

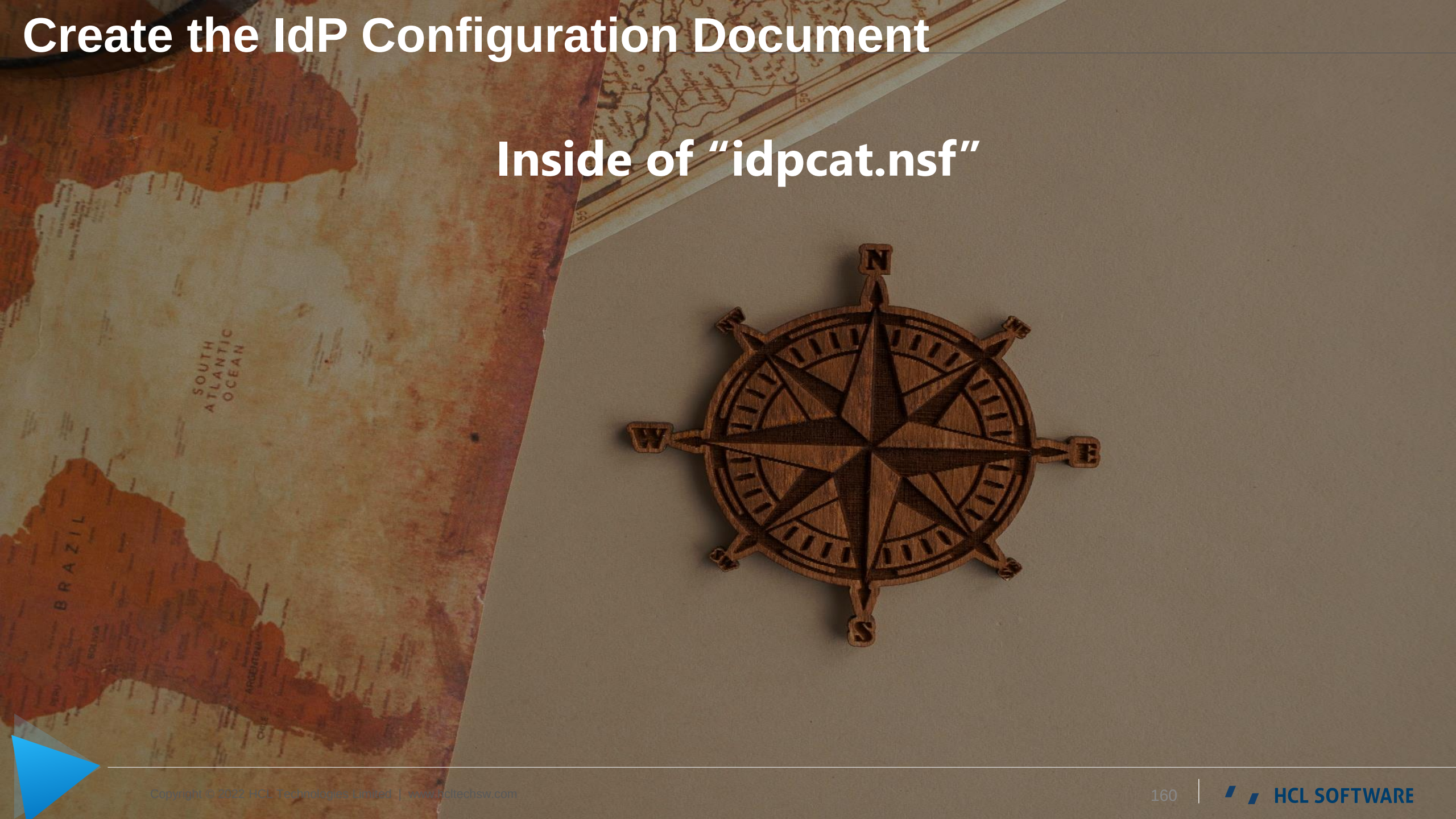
References

Notes Federated Login

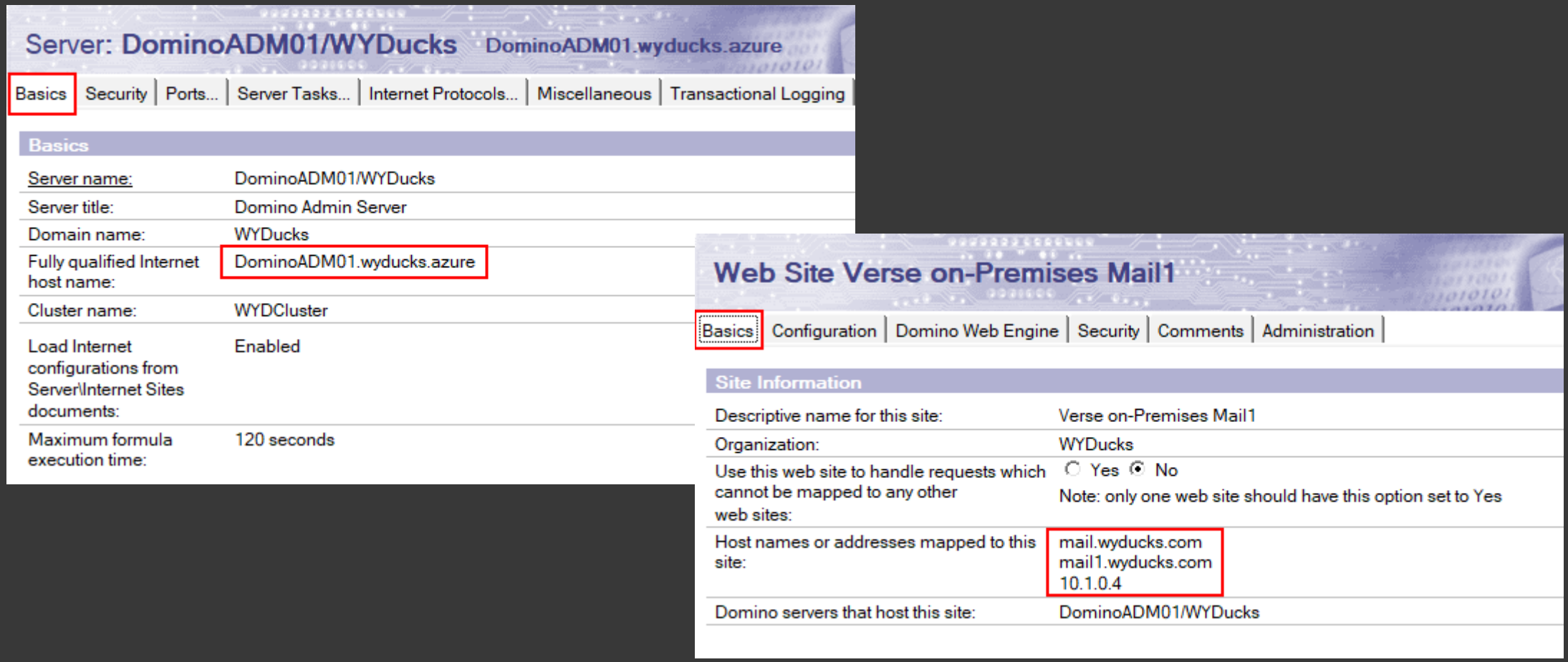


Create the IdP Configuration Document

Inside of “idpcat.nsf”

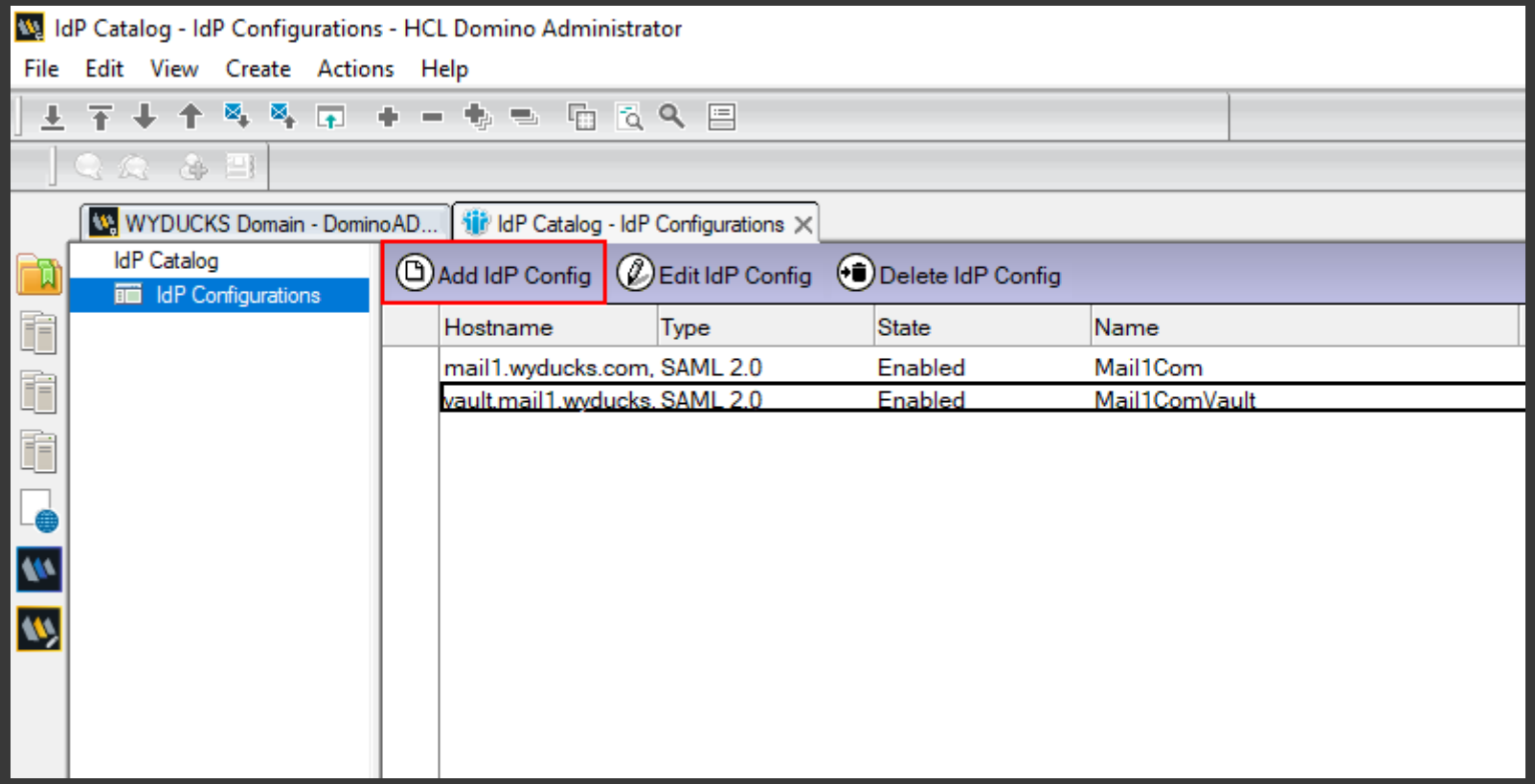


Create the IdP Configuration Document

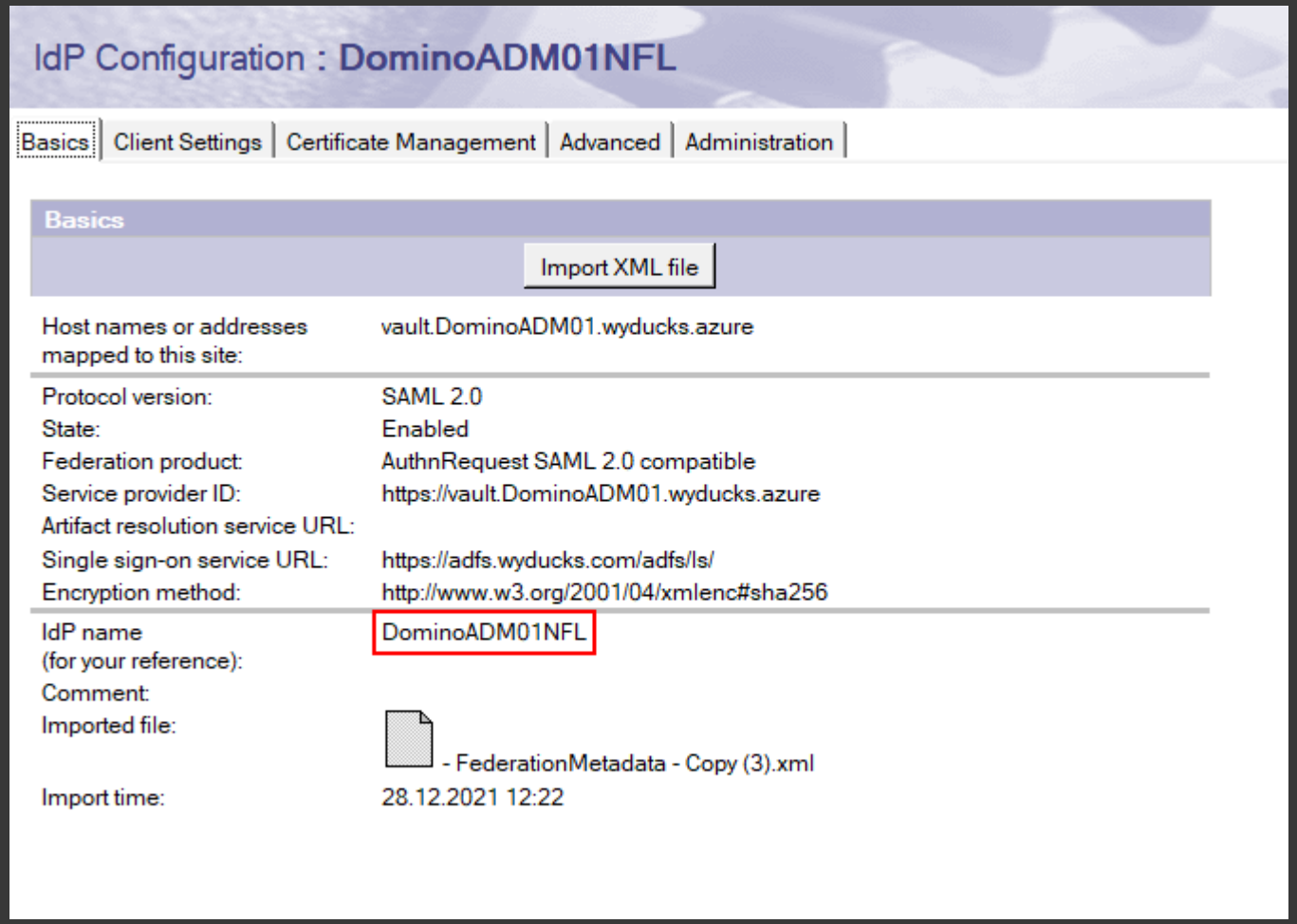


HCL SOFTWARE

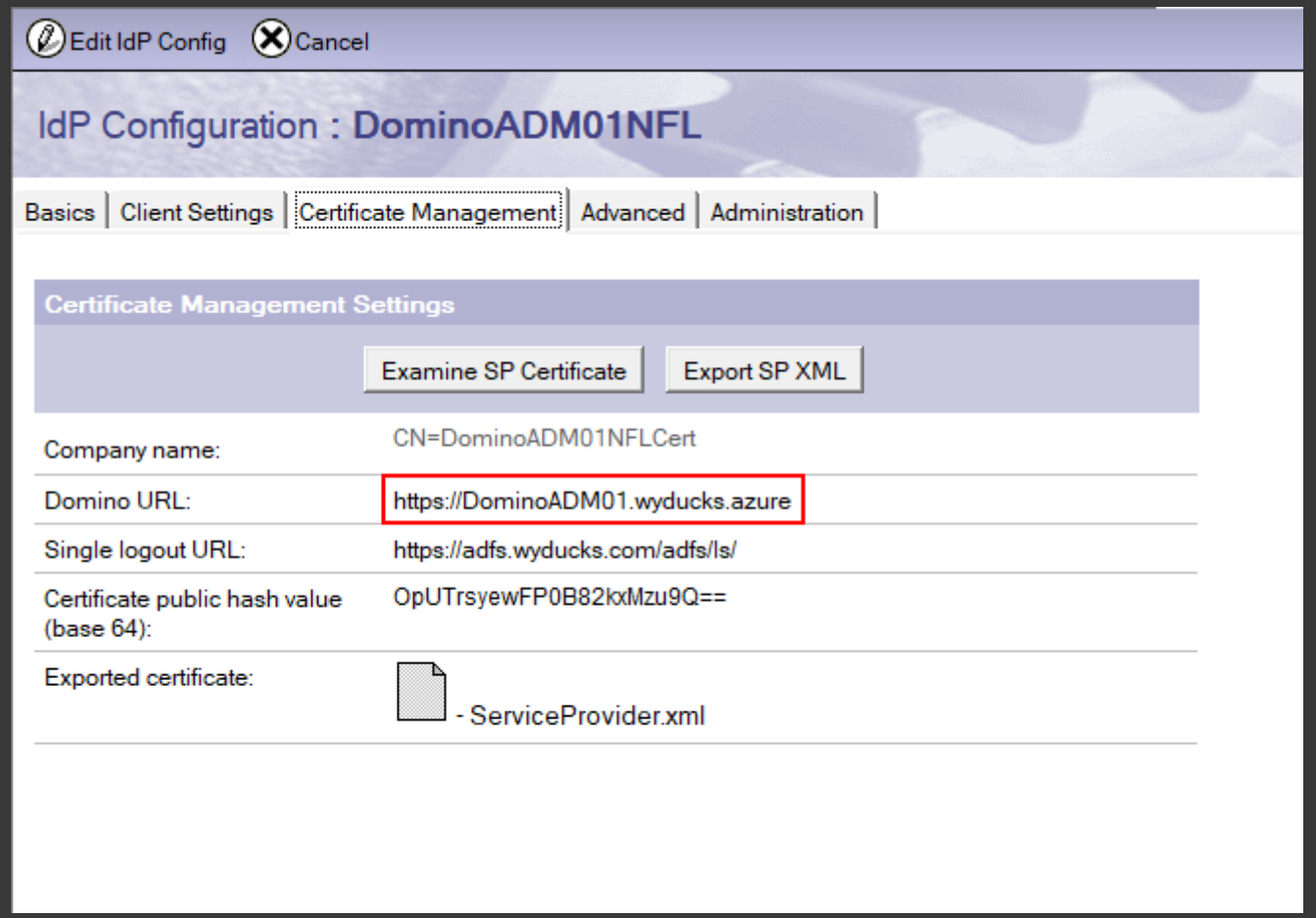
Create the IdP Configuration Document



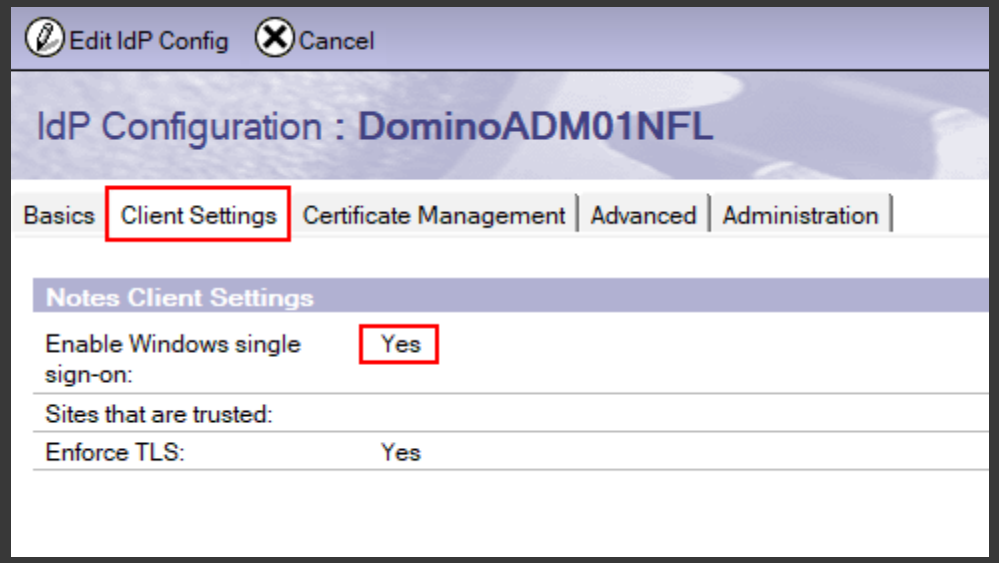
Create the IdP Configuration Document



Encrypting Domino SAML Assertions



Encrypting Domino SAML Assertions



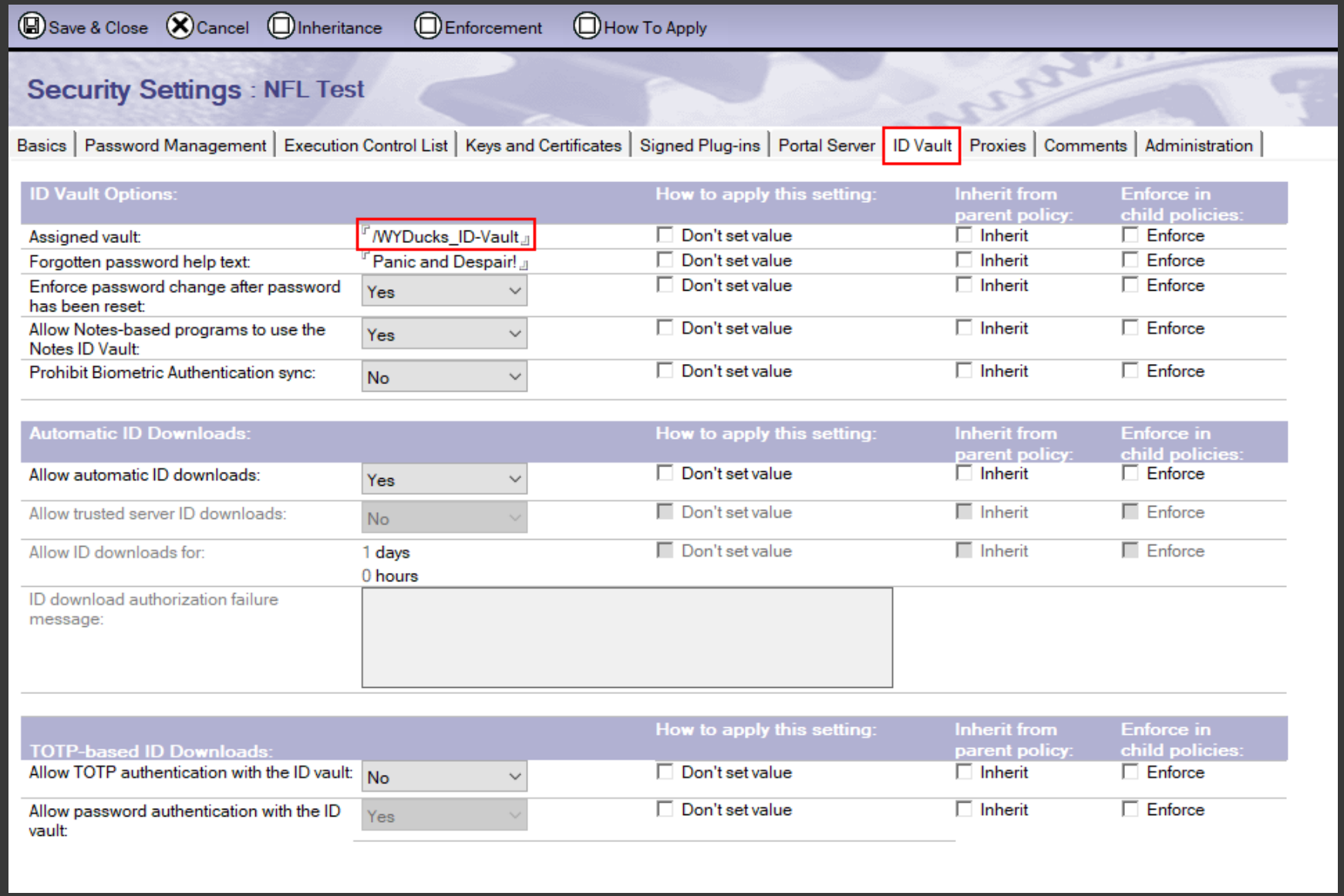
HCL SOFTWARE

Enable Notes Federated Login

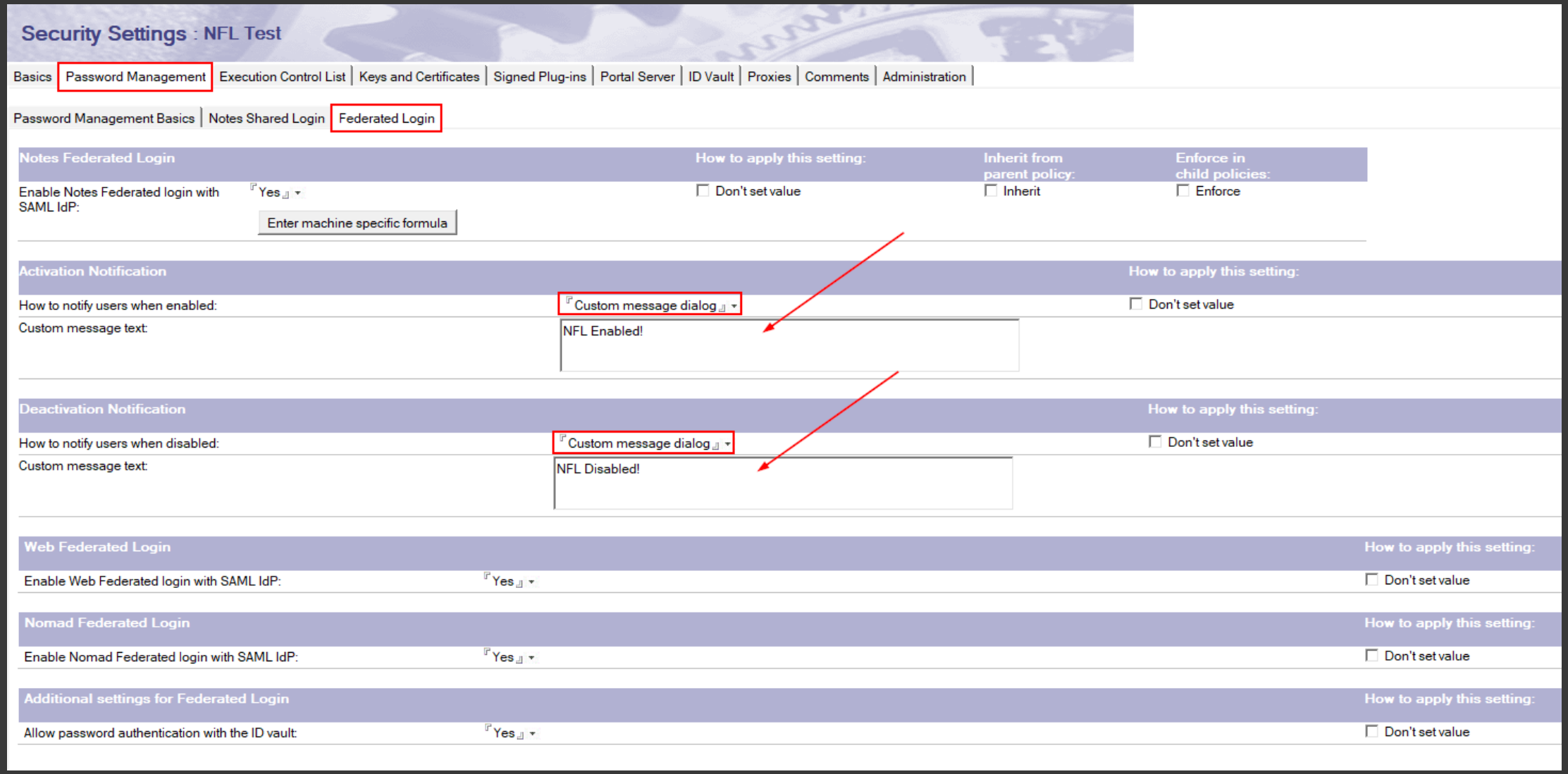
How can we do that?

Again, with a Domino Policy!

Enable Notes Federated Login

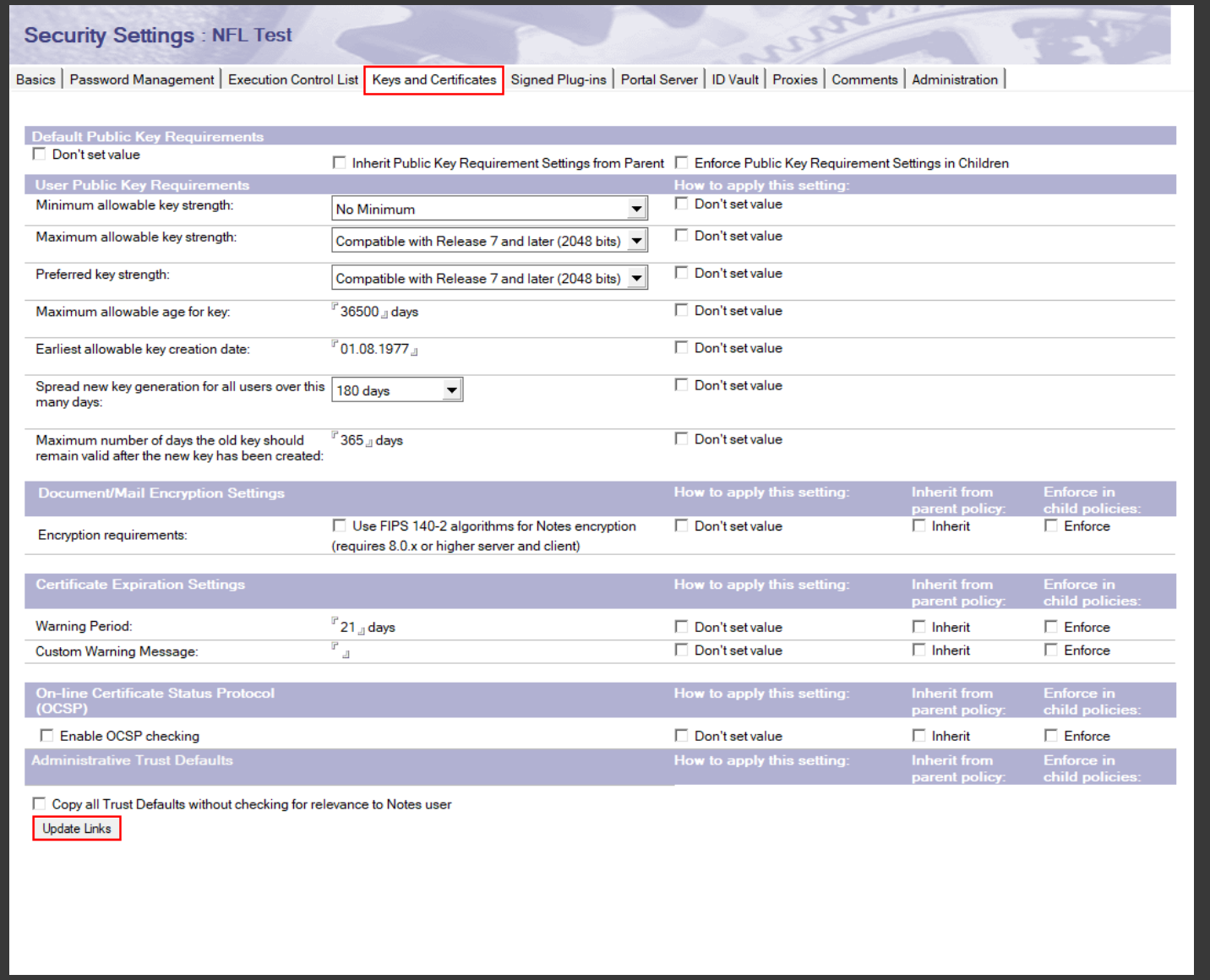


Enable Notes Federated Login



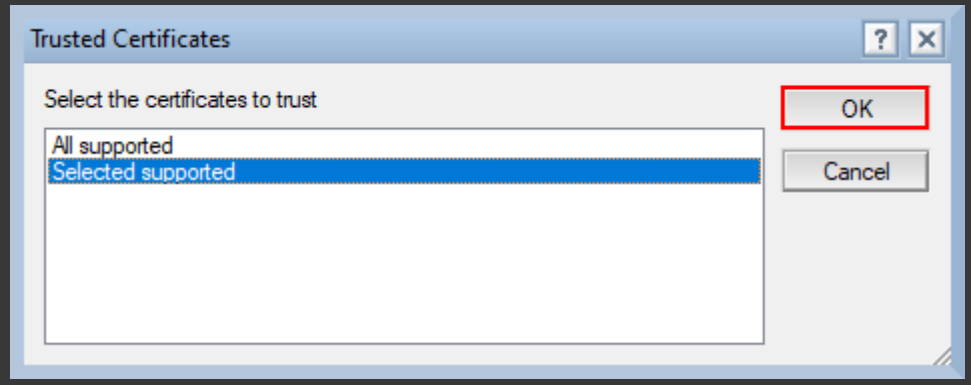
HCL SOFTWARE

Enable NFL – IdP Certificates Rollout

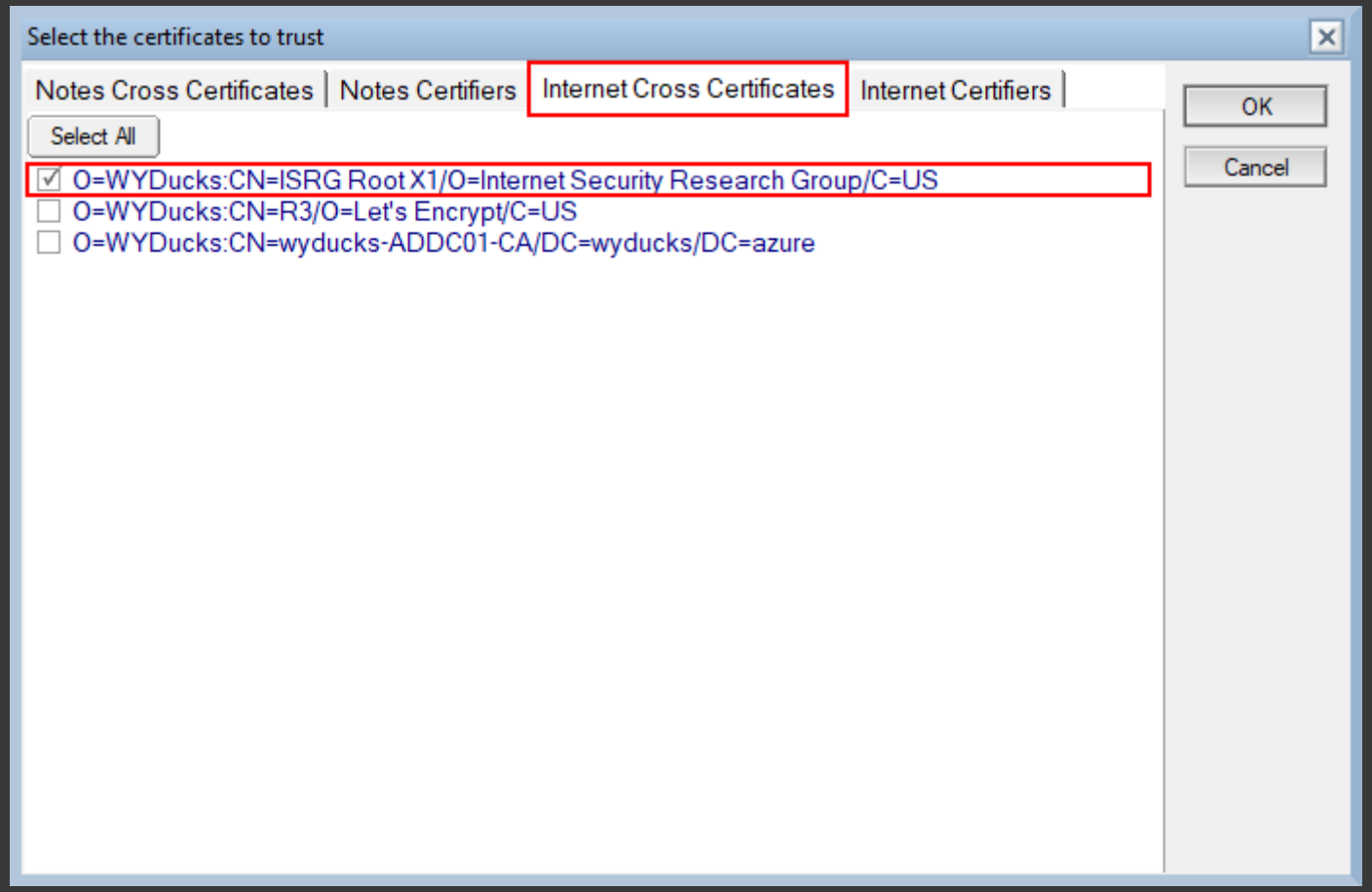


HCL SOFTWARE

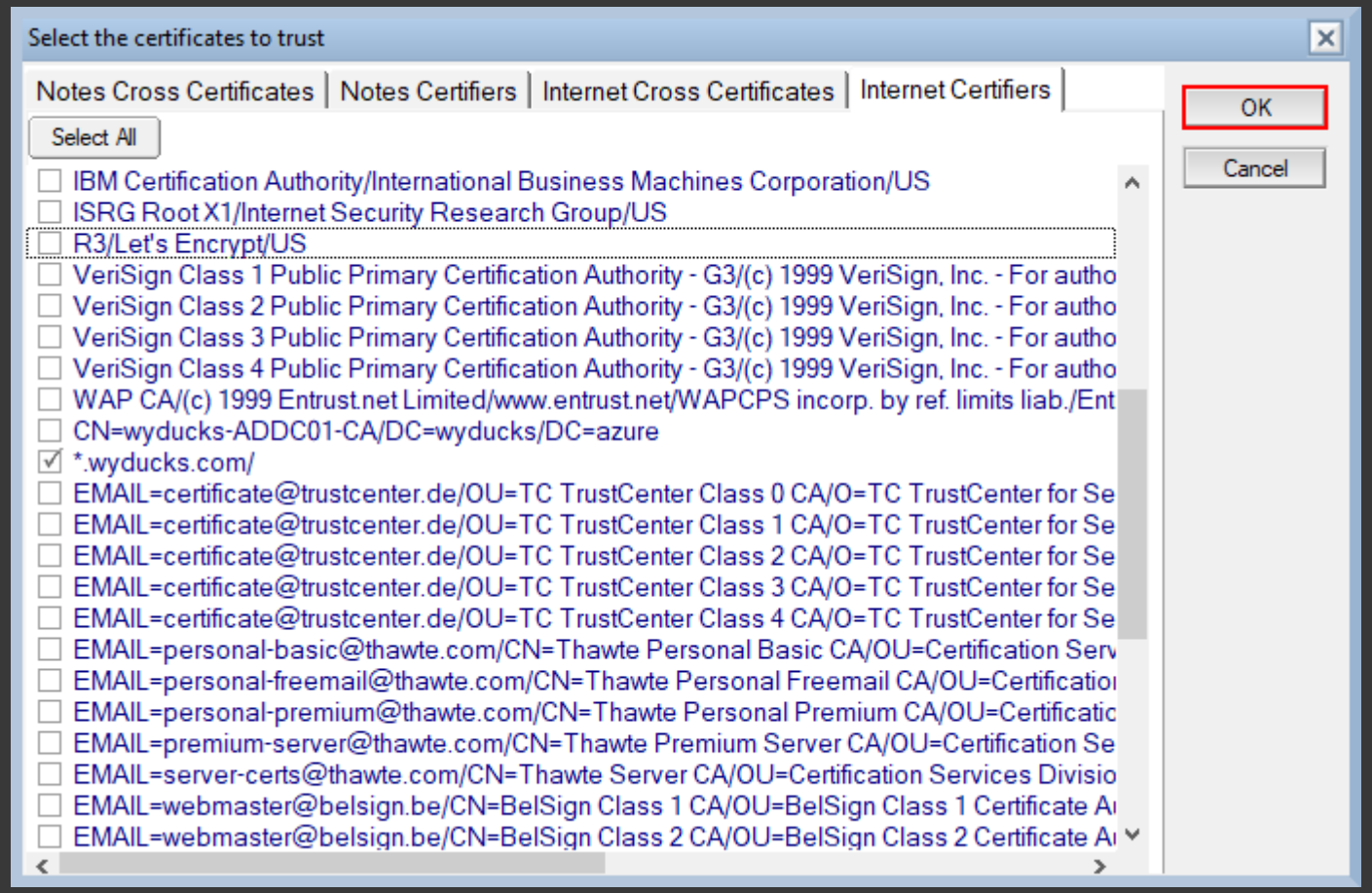
Enable NFL – IdP Certificates Rollout



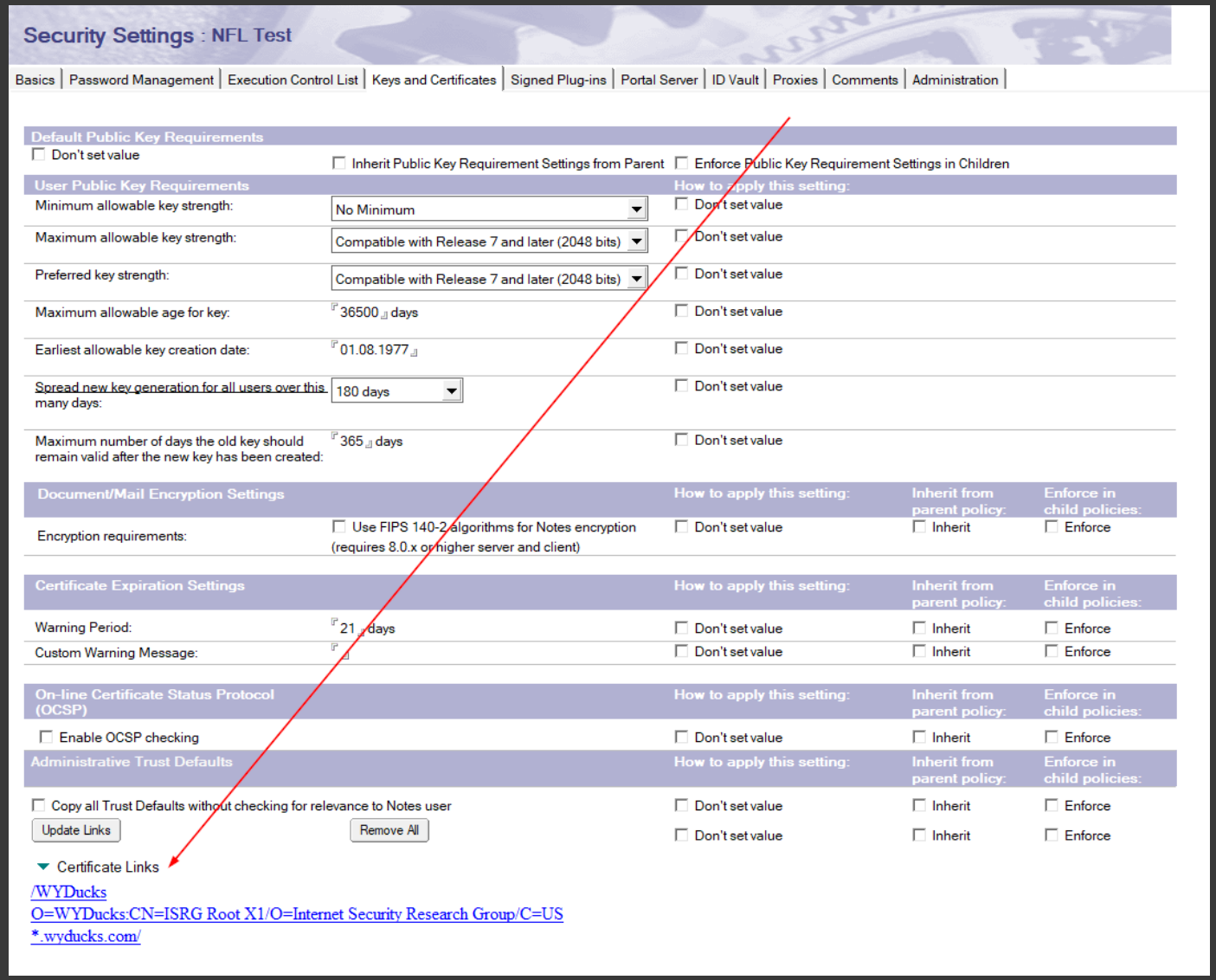
Enable NFL – IdP Certificates Rollout



Enable NFL – IdP Certificates Rollout

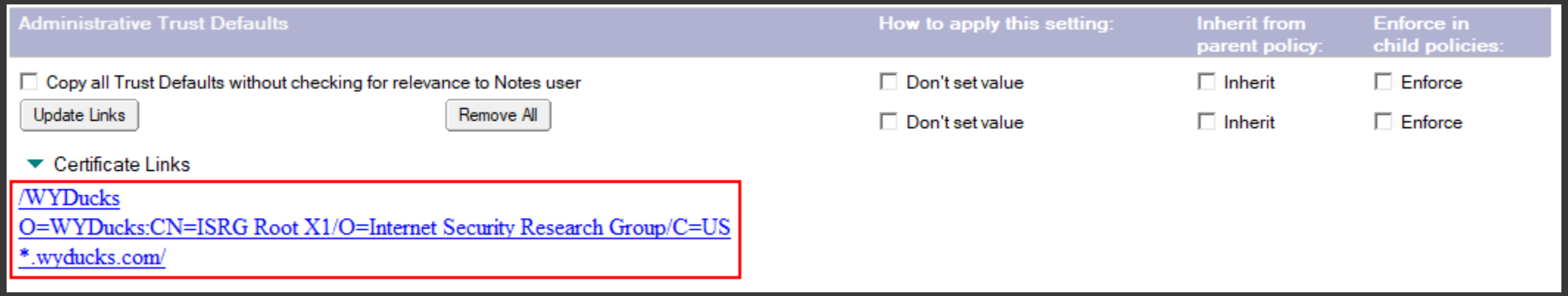


Enable NFL – IdP Certificates Rollout



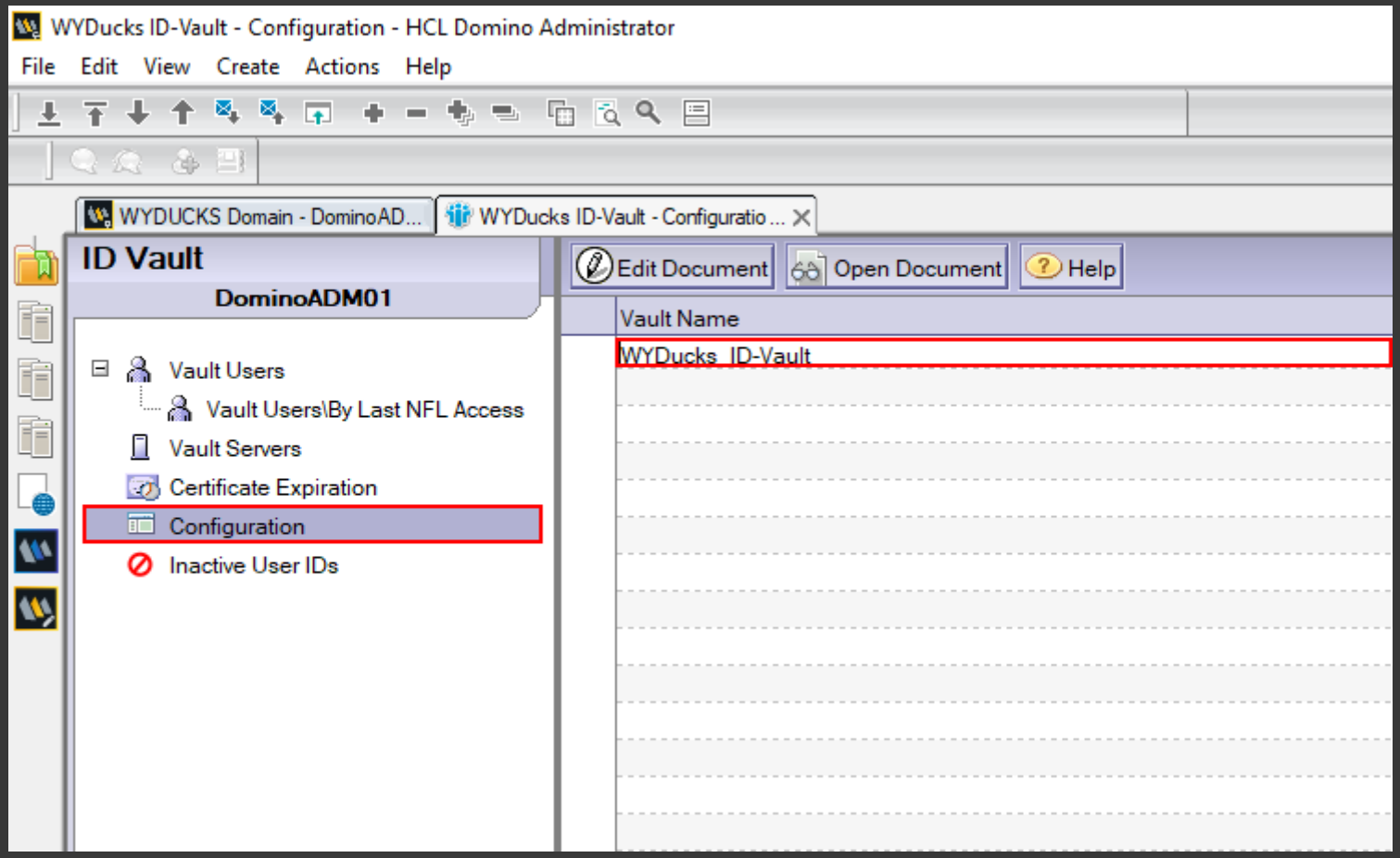
HCL SOFTWARE

Enable NFL – IdP Certificates Rollout



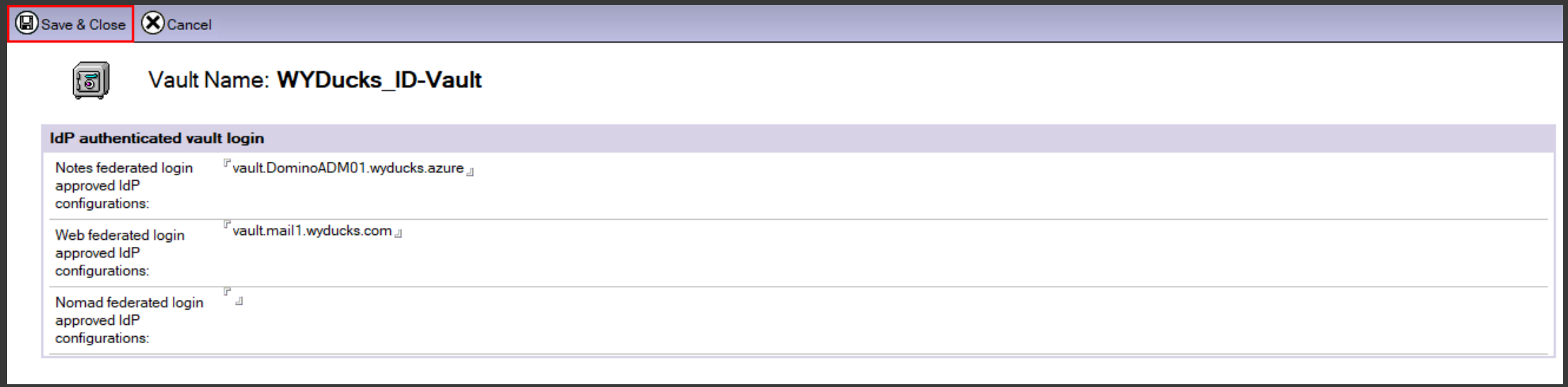
HCL SOFTWARE

Configure ID-Vault for Notes Federated Login



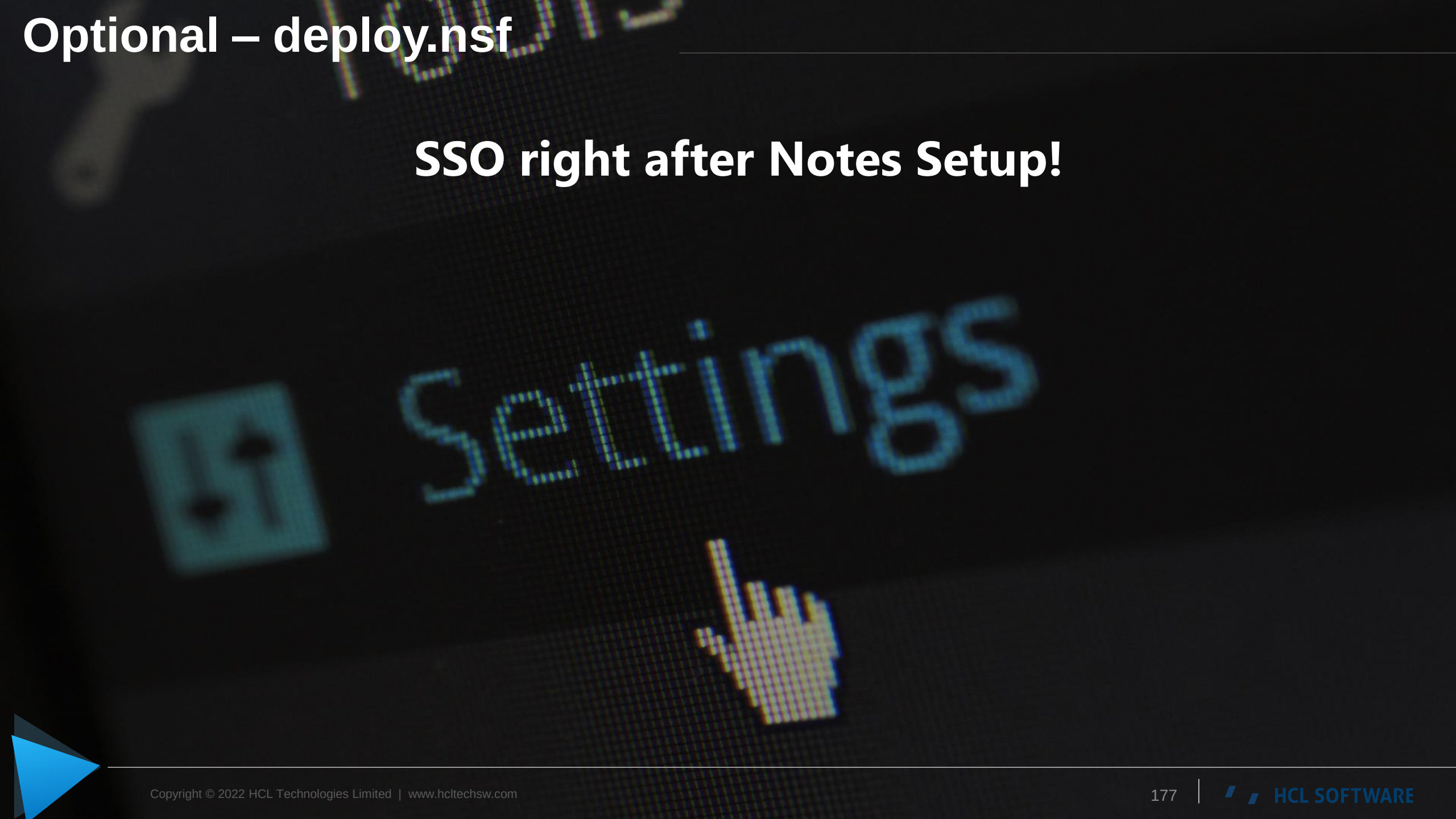
HCL SOFTWARE

Configure ID-Vault for Notes Federated Login

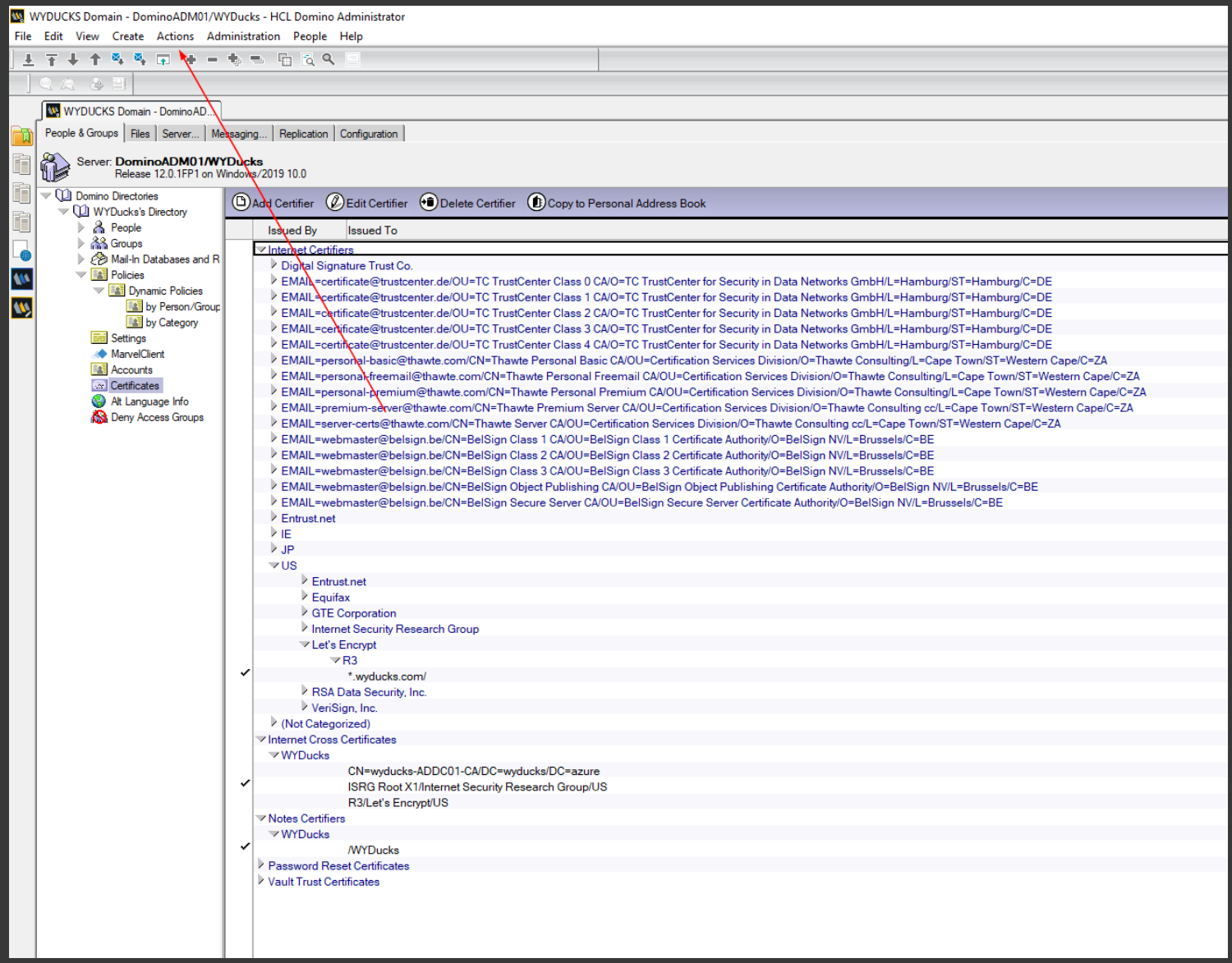


Optional – deploy.nsf

SSO right after Notes Setup!

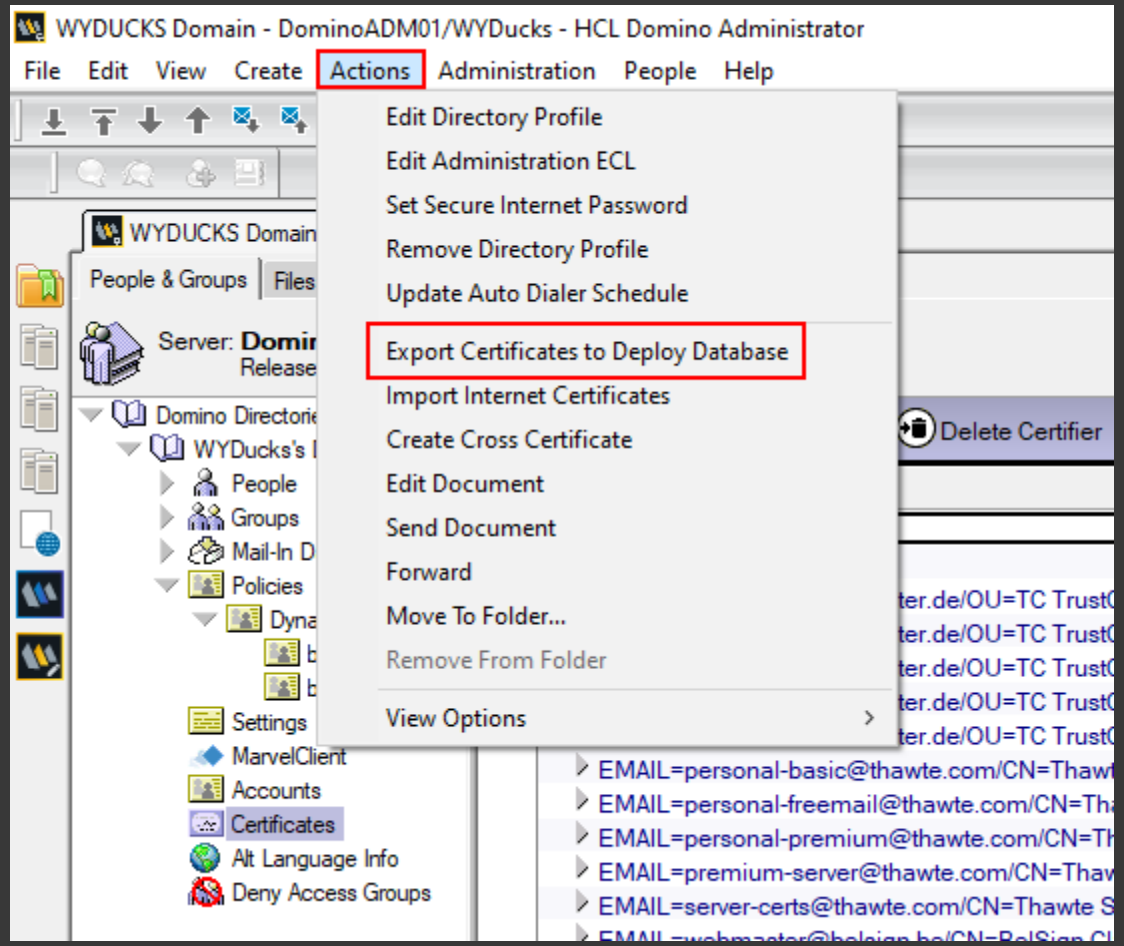


Optional – deploy.nsf



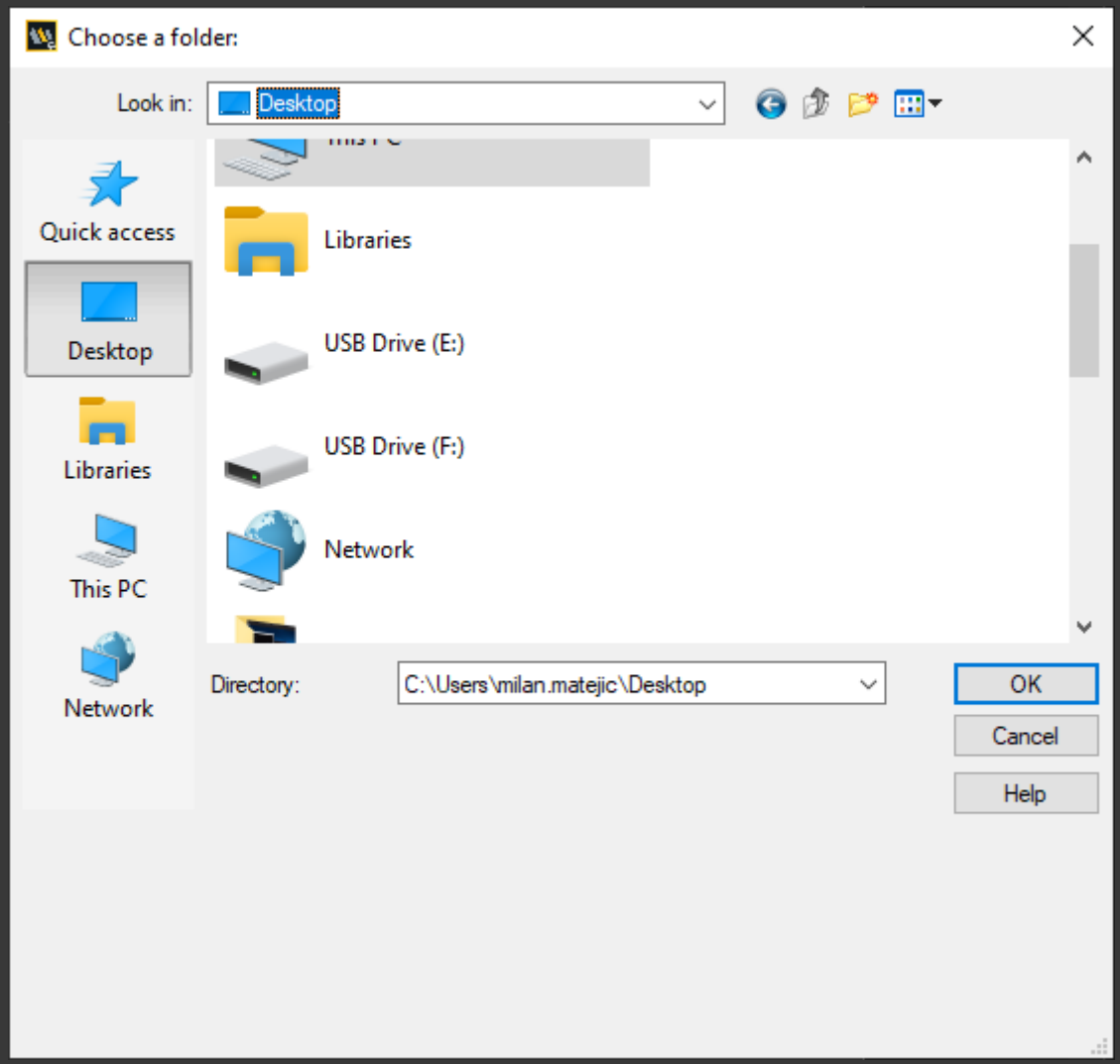
HCL SOFTWARE

Optional – deploy.nsf

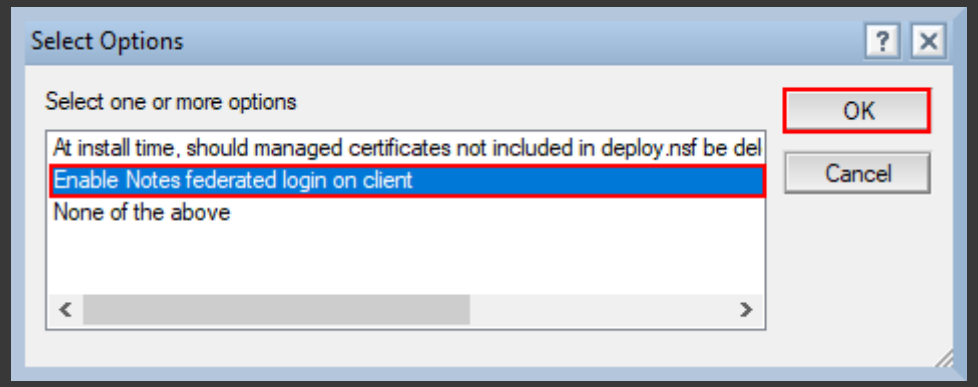


HCL SOFTWARE

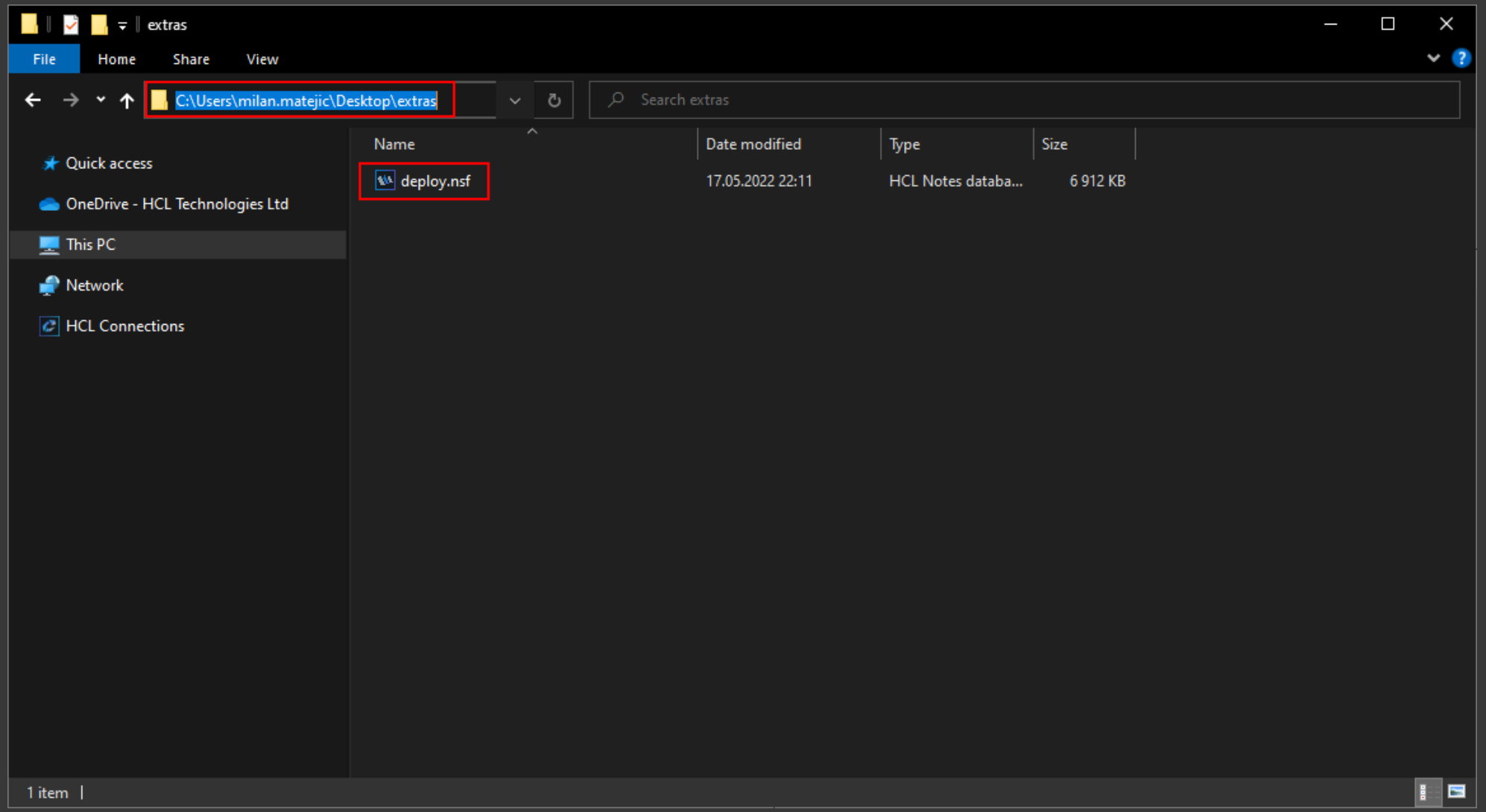
Optional – deploy.nsf



Optional – deploy.nsf



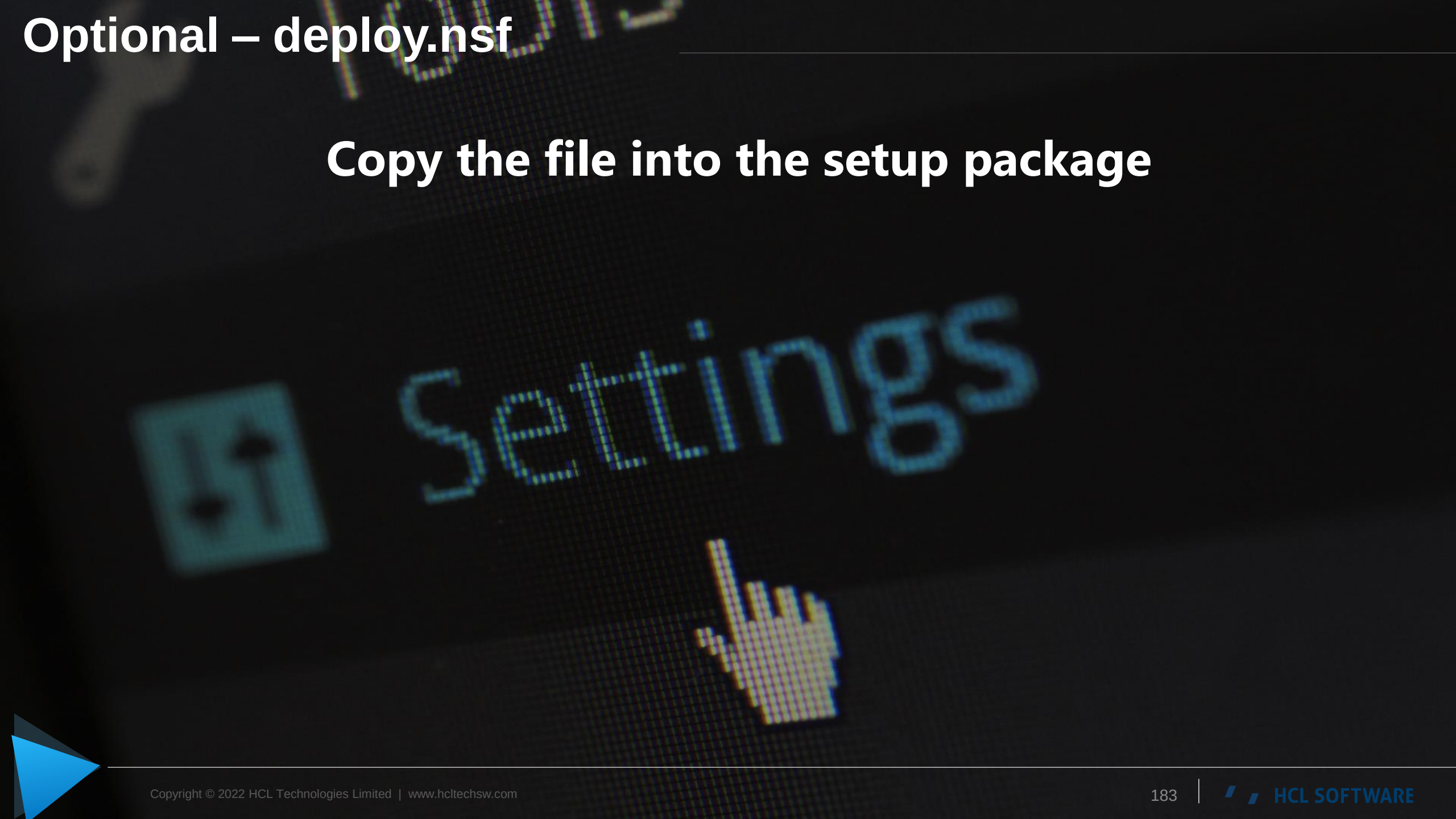
Optional – deploy.nsf



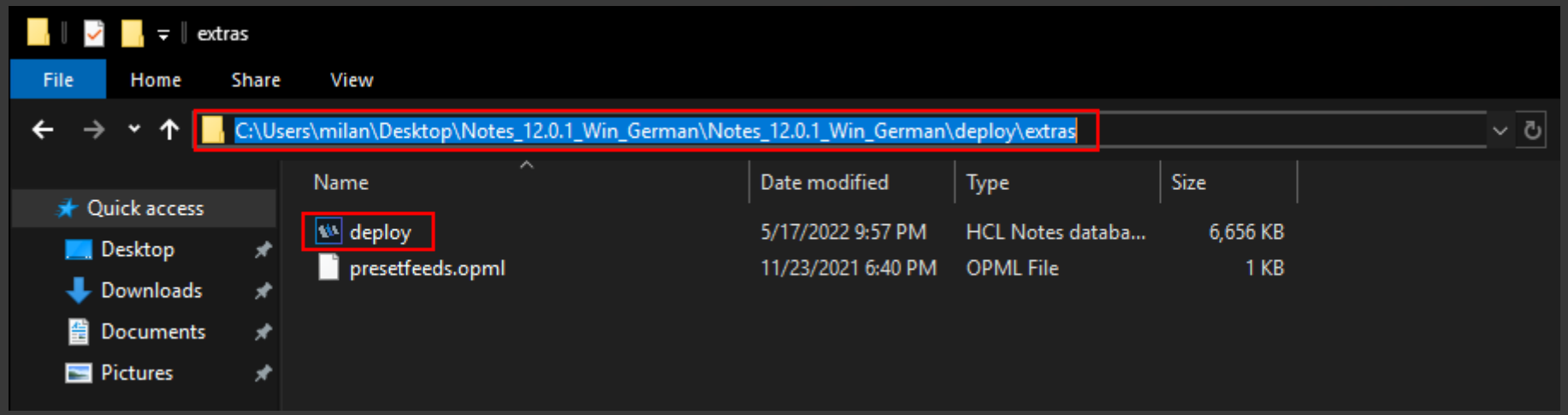
HCL SOFTWARE

Optional – deploy.nsf

Copy the file into the setup package



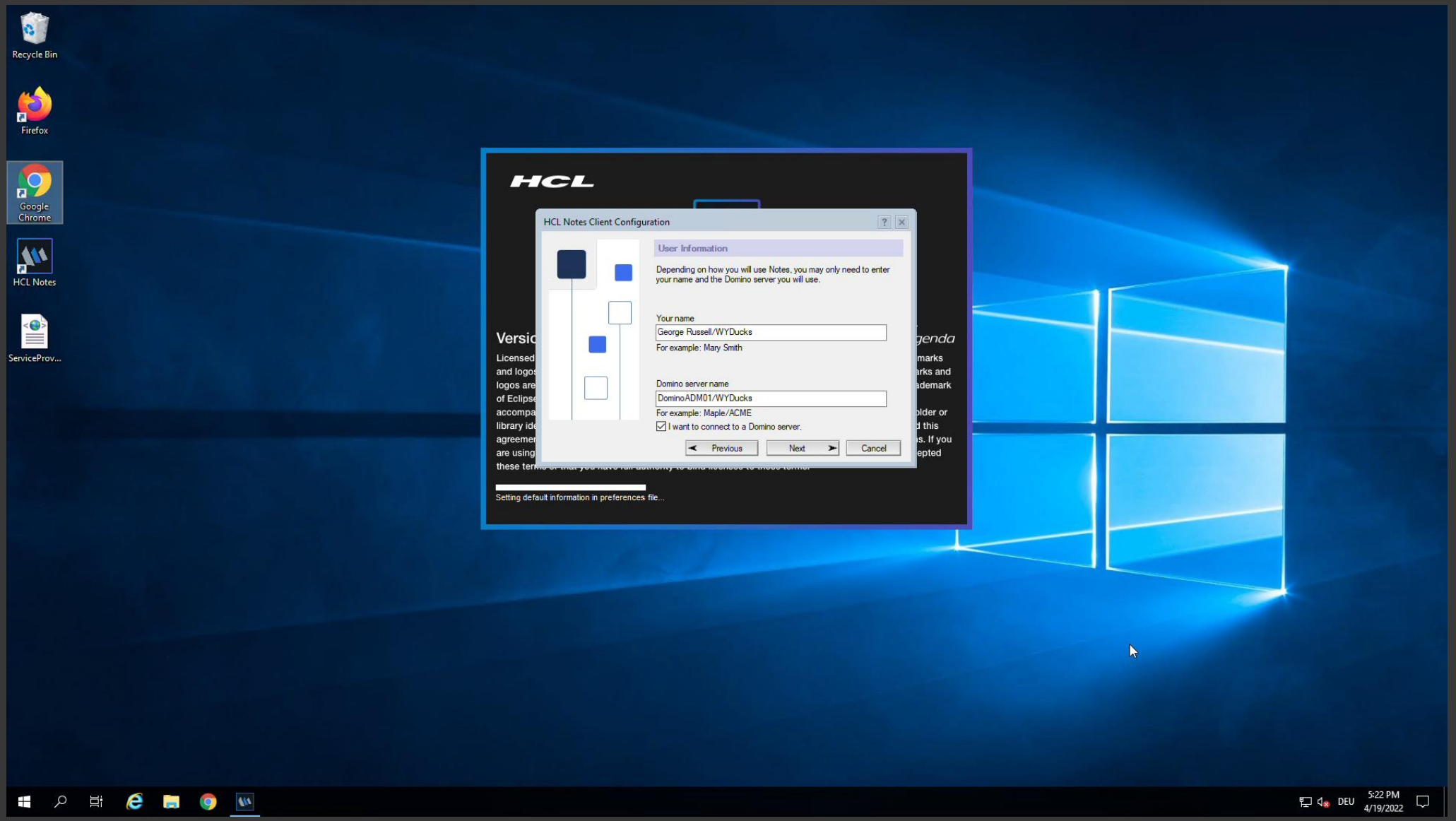
Optional – deploy.nsf



Optional – Notes Shared Login

Demo

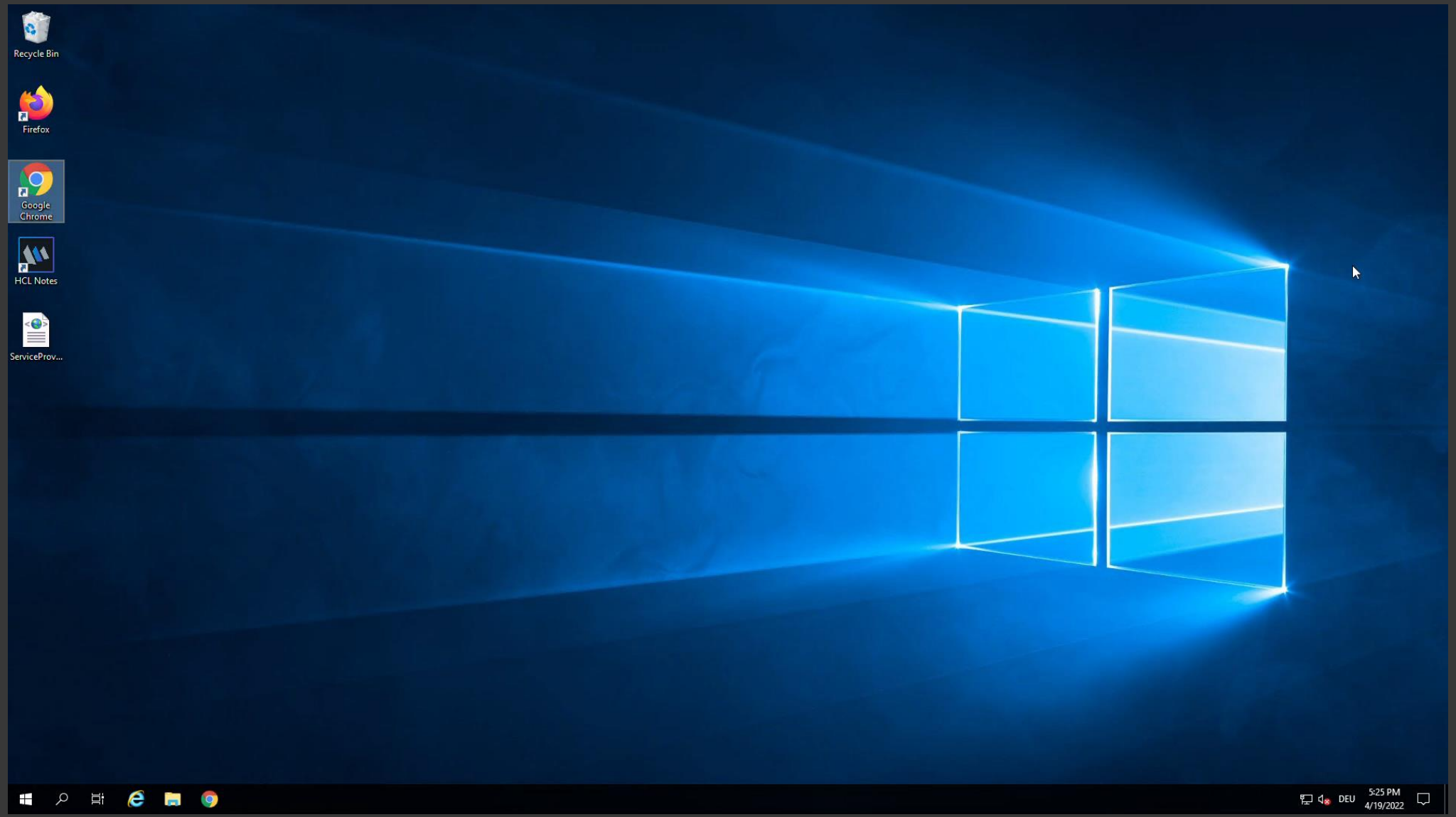
Demo



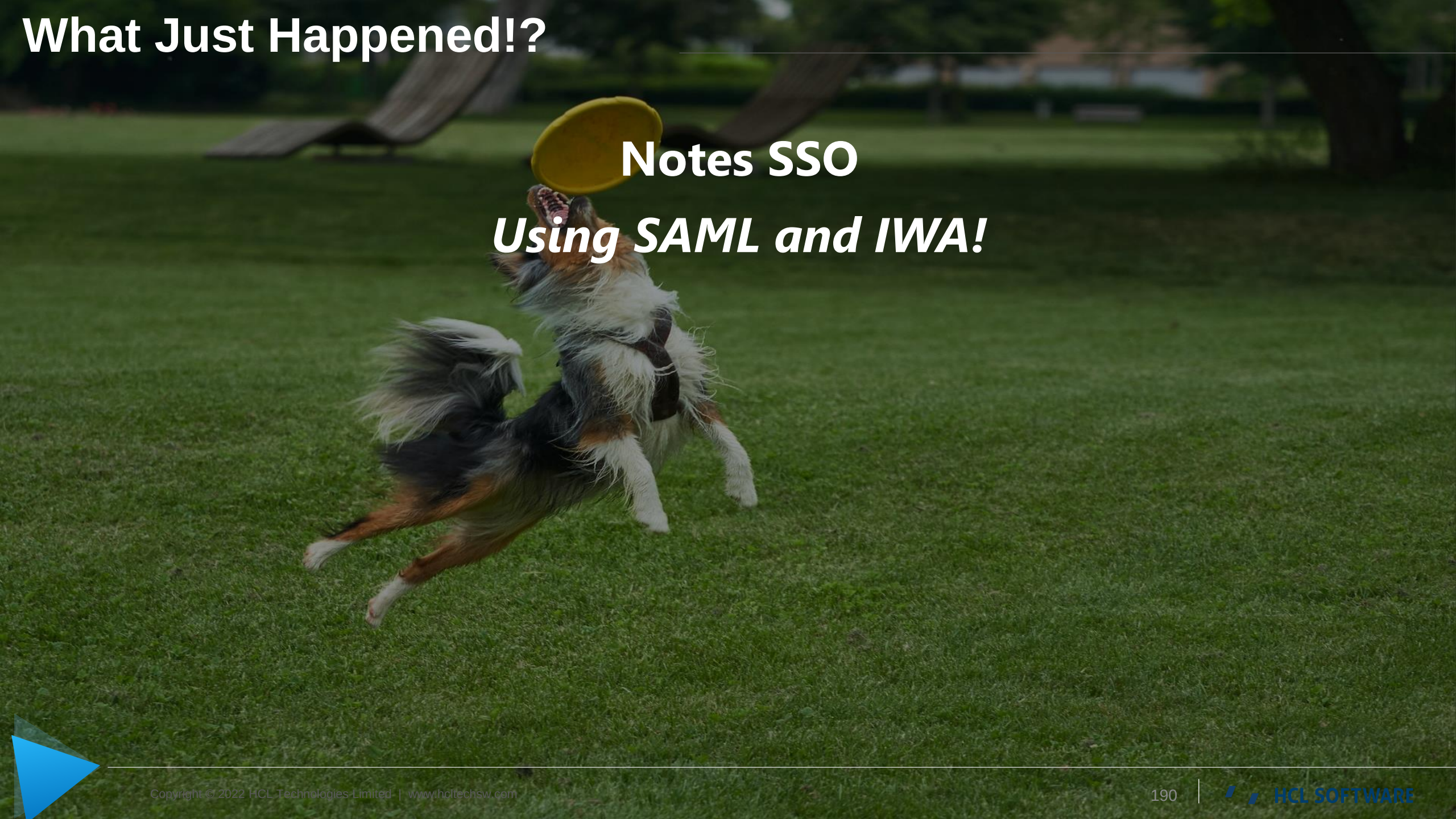
HCL SOFTWARE

Demo

Demo



What Just Happened!?



Infrastructure Needed

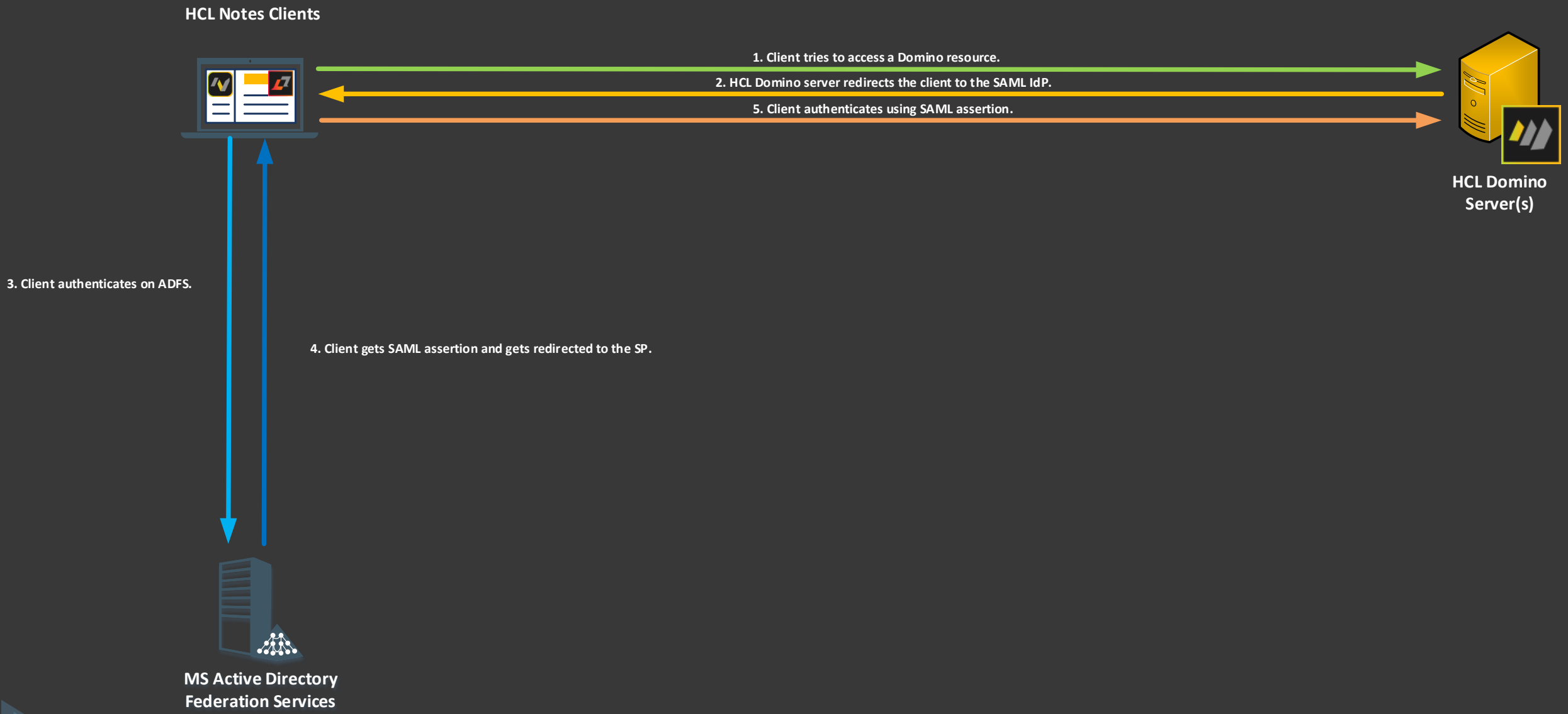


Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

SAML & SSO

Web Federated Login

Notes Federated Login

Traveler & SAML

Bonus – Nomad!

Troubleshooting

Issues

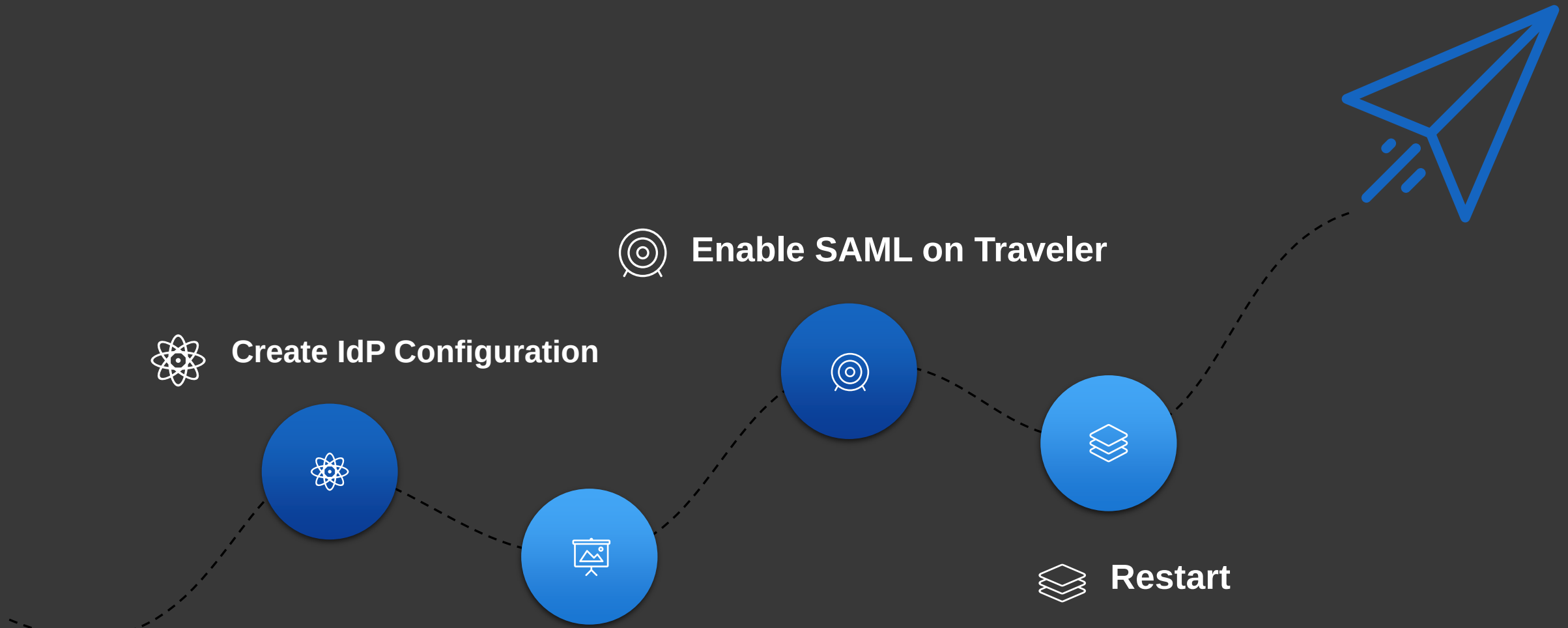
Q & A

Shibboleth

References

Traveler Specific Limitations and Requirements

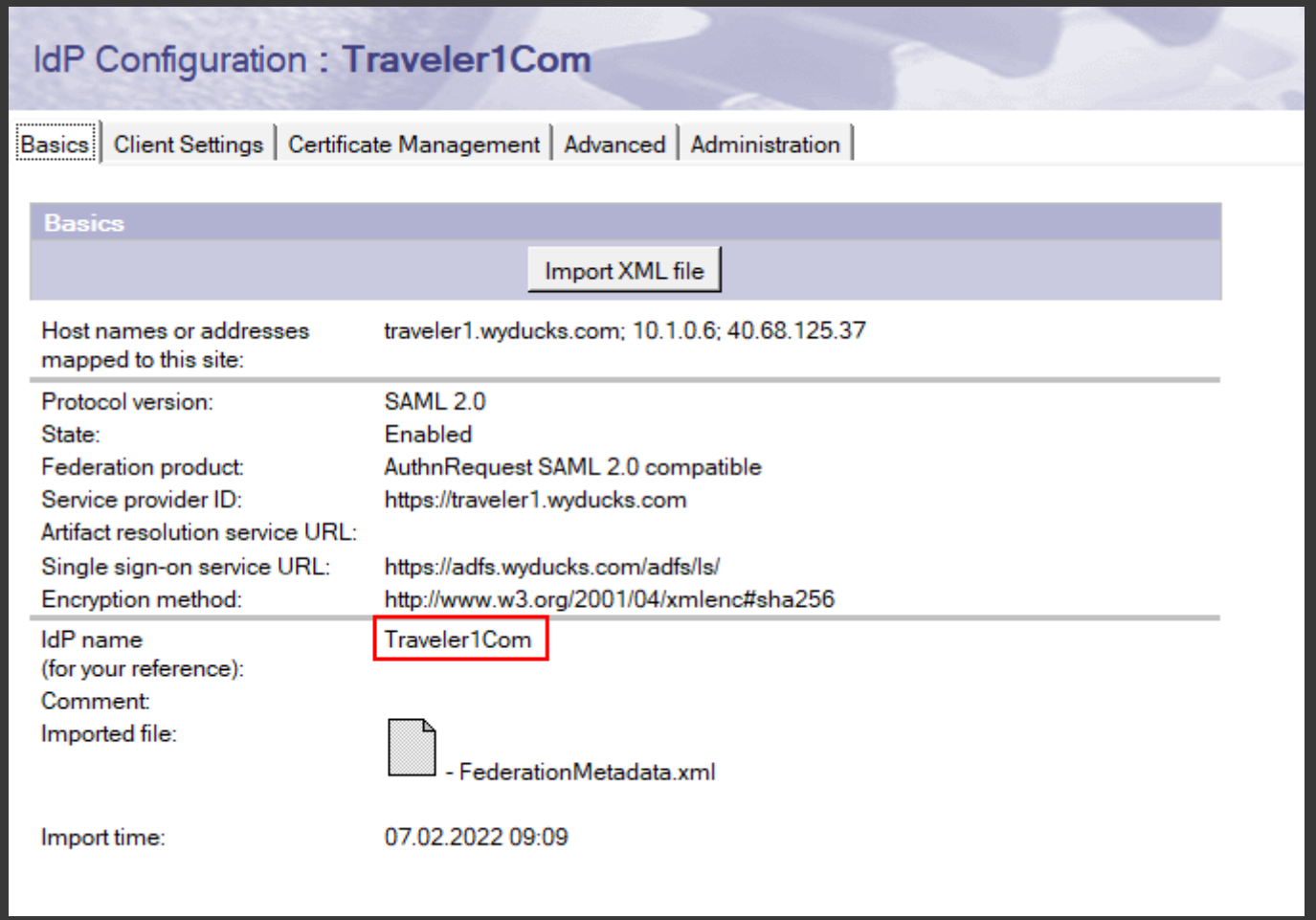
Traveler & SAML



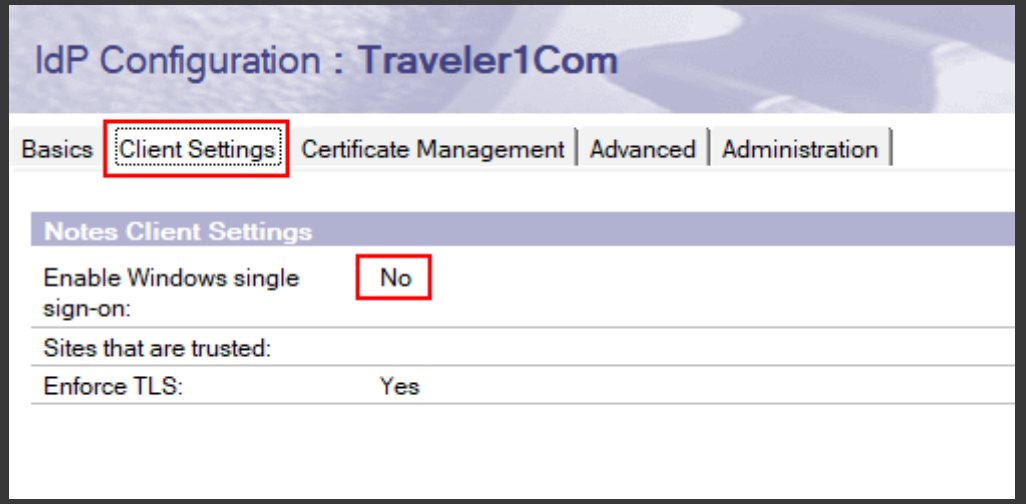
Create the IdP Configuration Document

Inside of “idpcat.nsf”

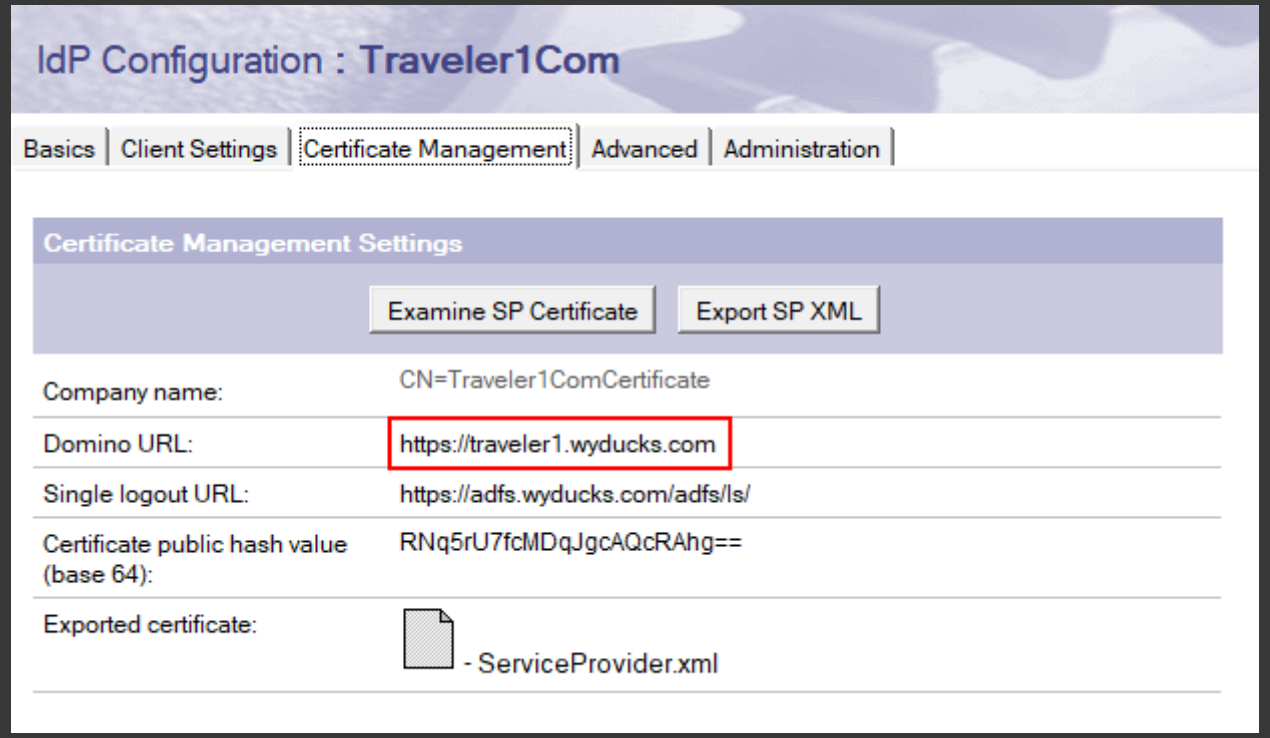
Create the IdP Configuration Document



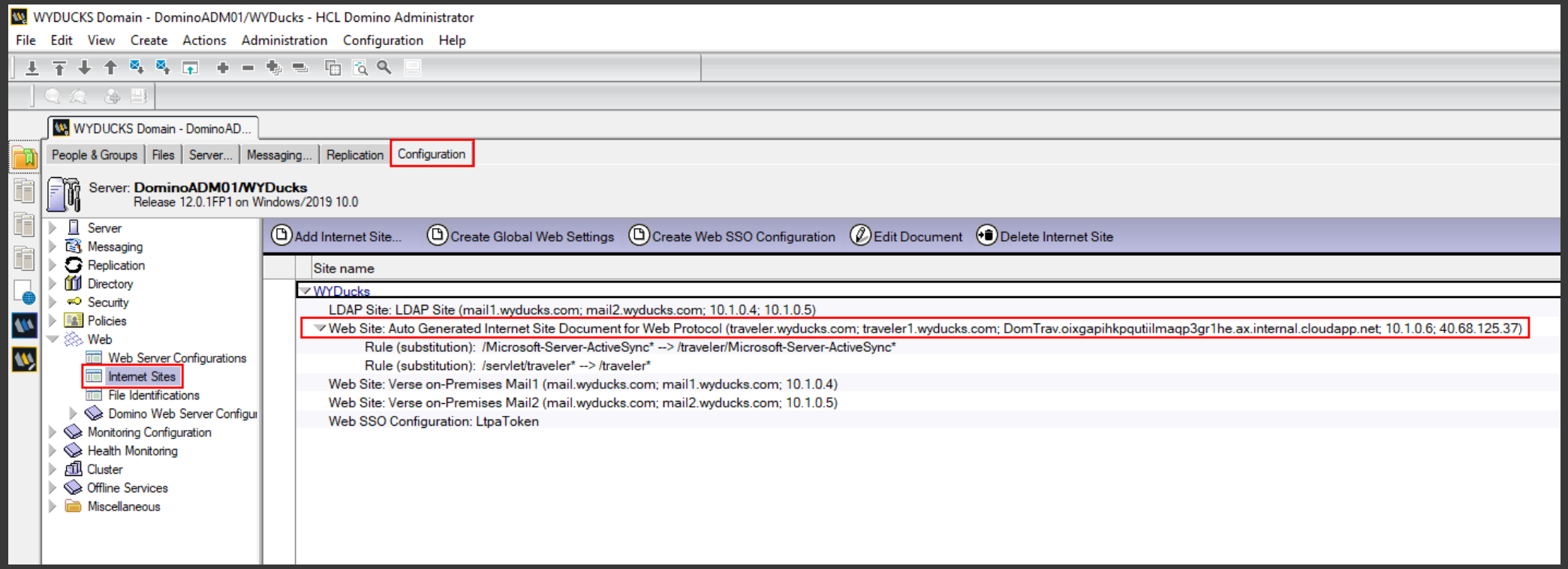
Create the IdP Configuration Document



Encrypting Domino SAML Assertions



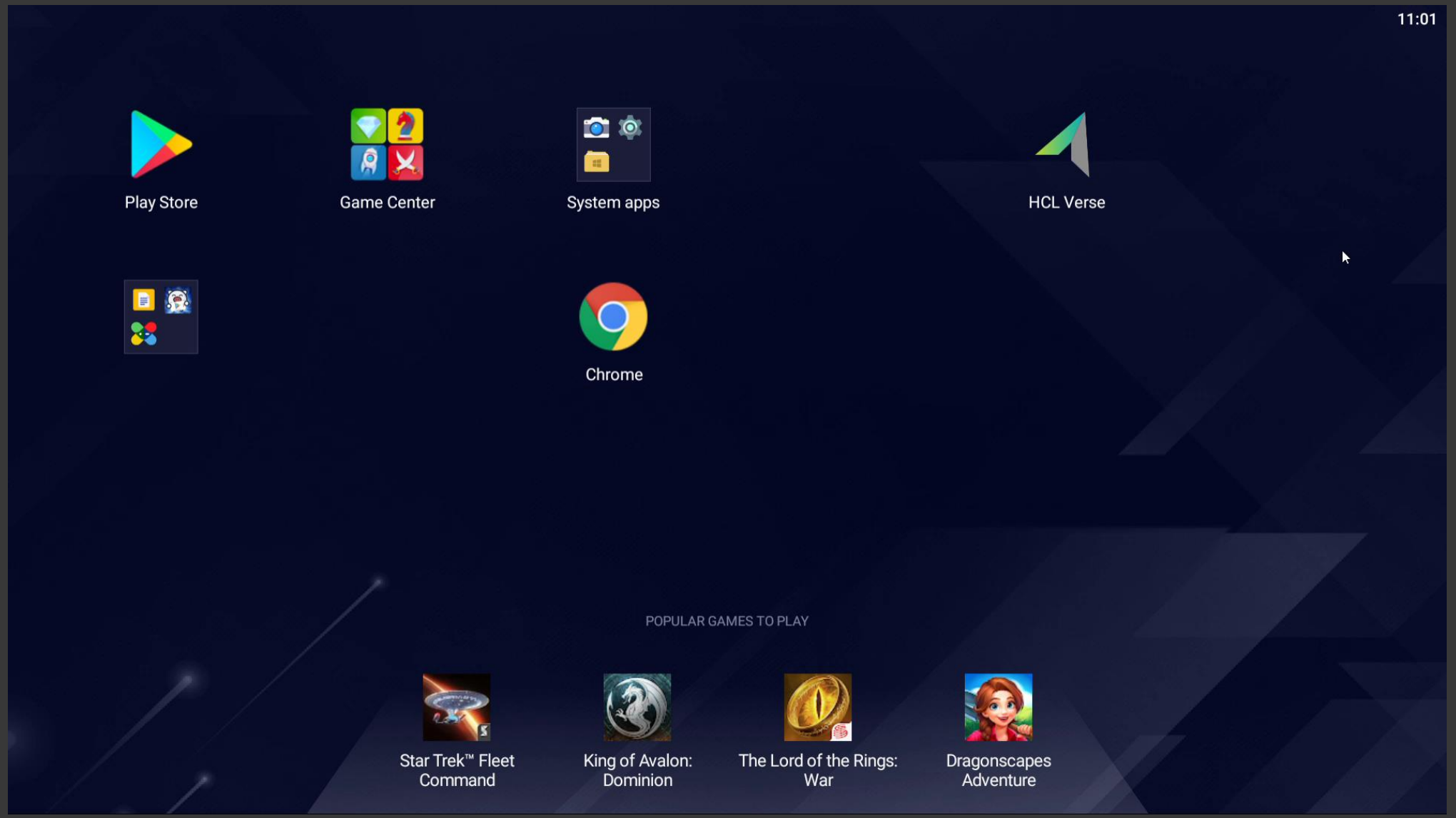
Enable SAML for HCL Verse Mobile Clients



Enable SAML for HCL Verse Mobile Clients

Demo

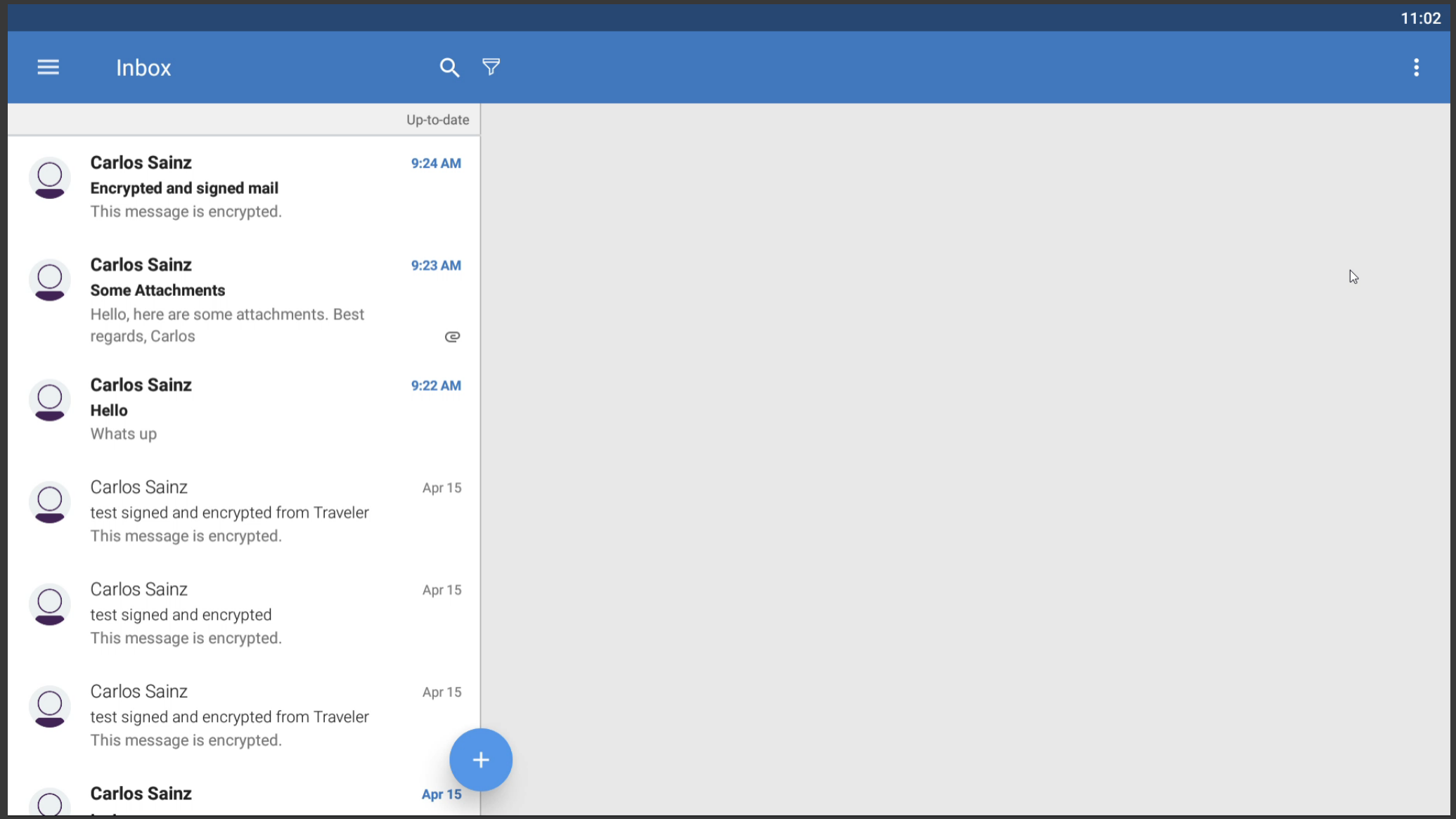
Demo



HCL SOFTWARE

Demo

Demo



HCL SOFTWARE

Optional – Allow PW Authentication with ID-Vault

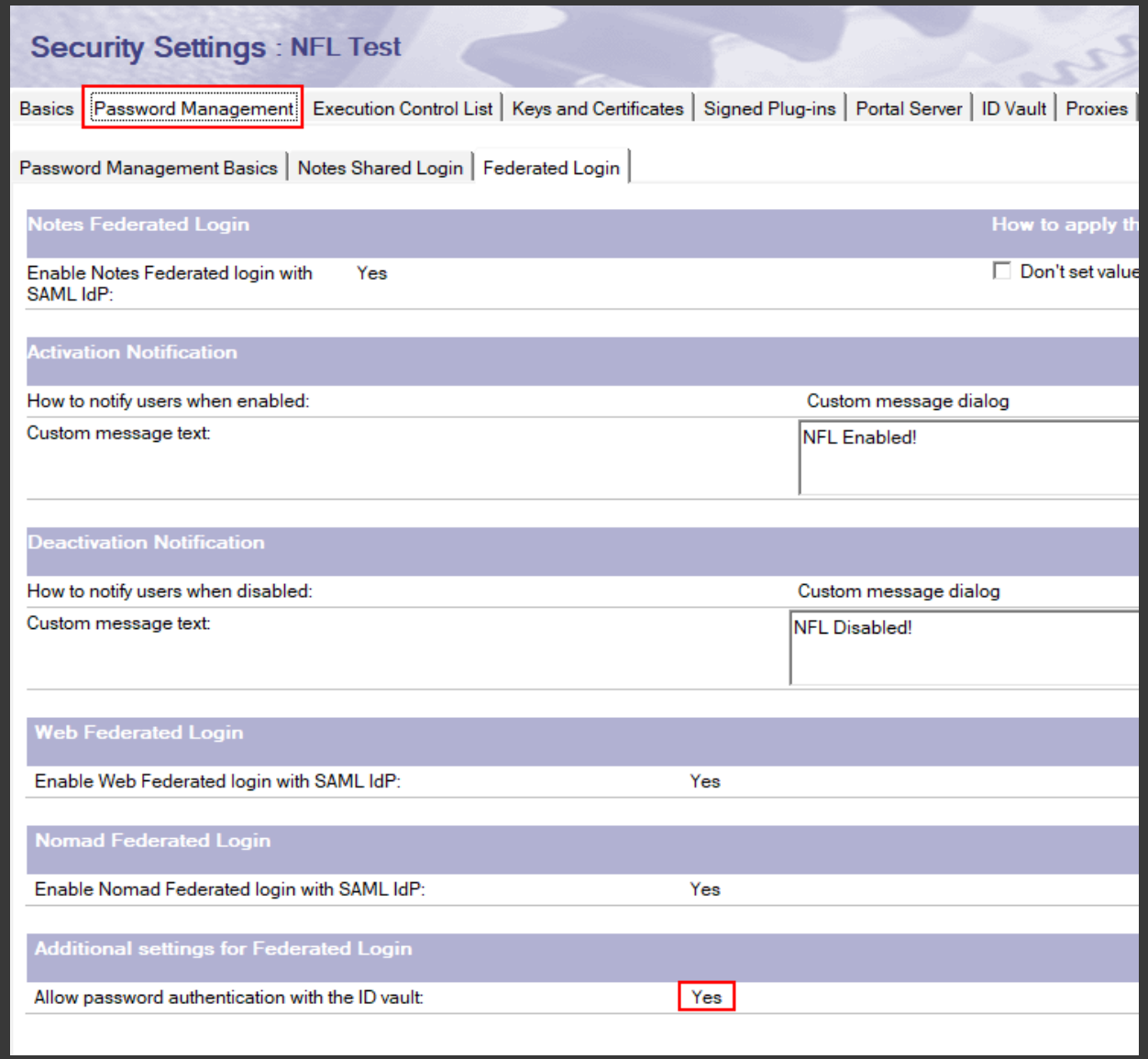


Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

SAML & SSO

Web Federated Login

Notes Federated Login

Traveler & SAML

Bonus – Nomad!

Troubleshooting

Issues

Q & A

Shibboleth

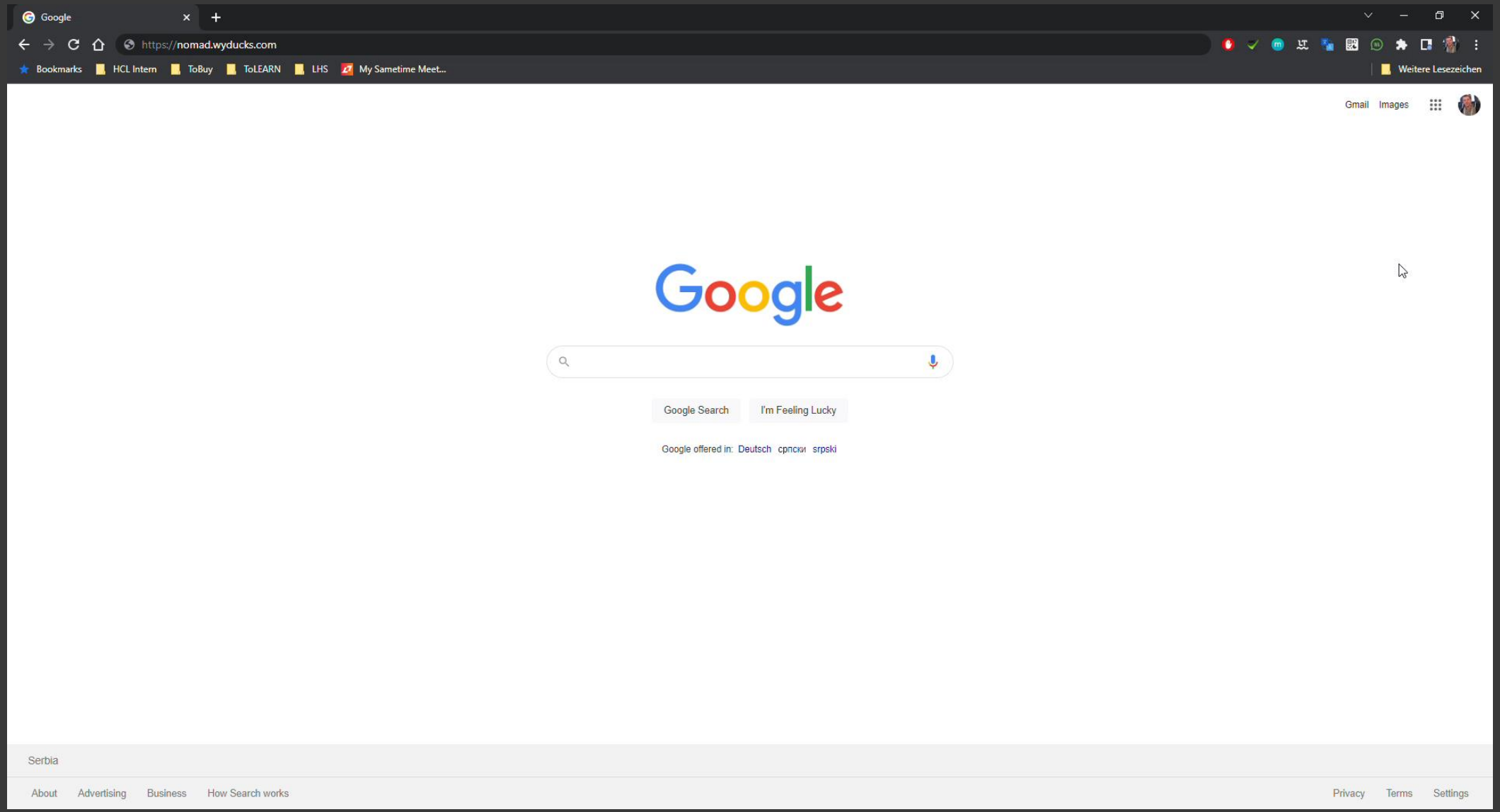
References

Nomad Federated Login

Ad02. Deploying HCL Nomad Web

Demo

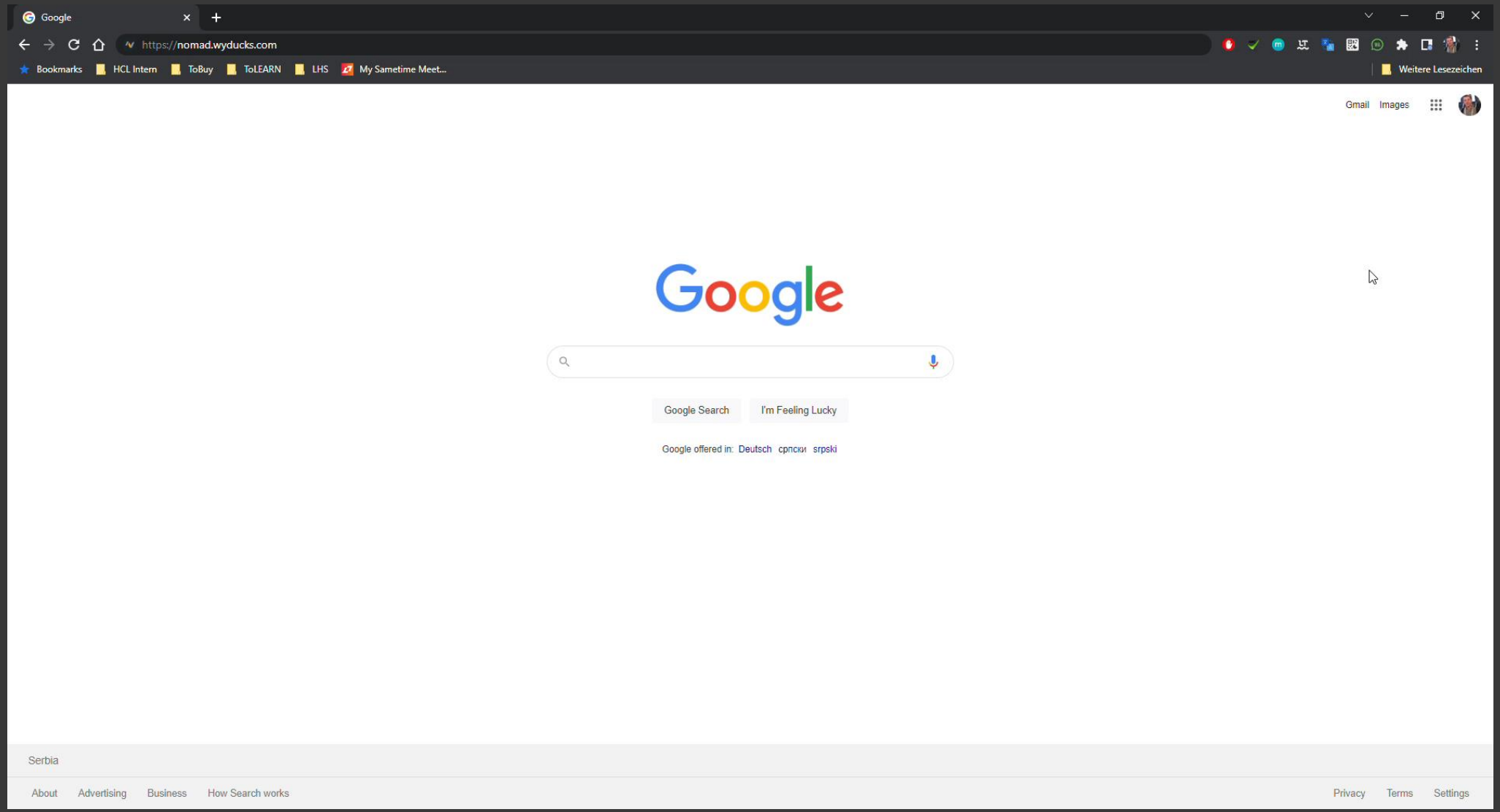
Demo



HCL SOFTWARE

Demo

Demo



HCL SOFTWARE

Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

SAML & SSO

Web Federated Login

Notes Federated Login

Traveler & SAML

Bonus – Nomad!

Troubleshooting

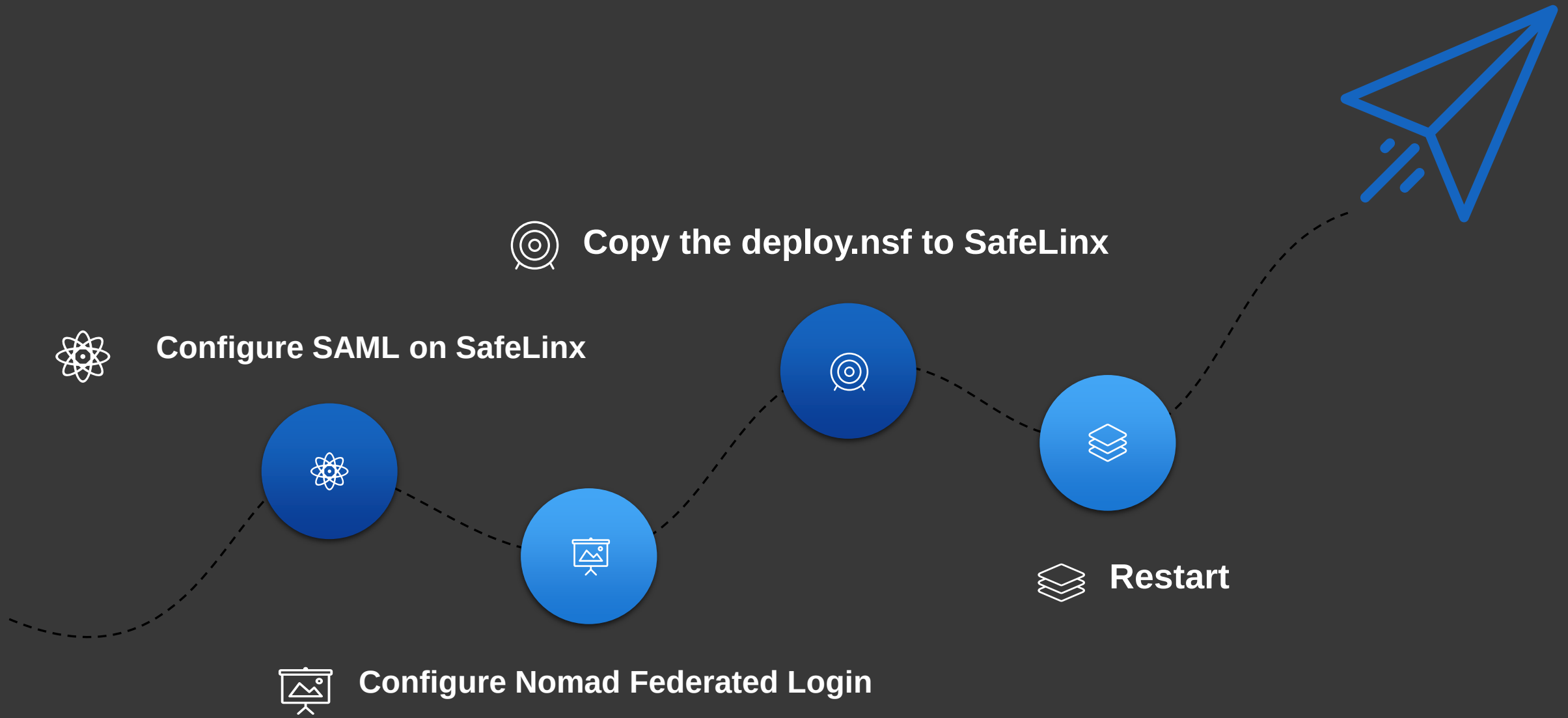
Issues

Q & A

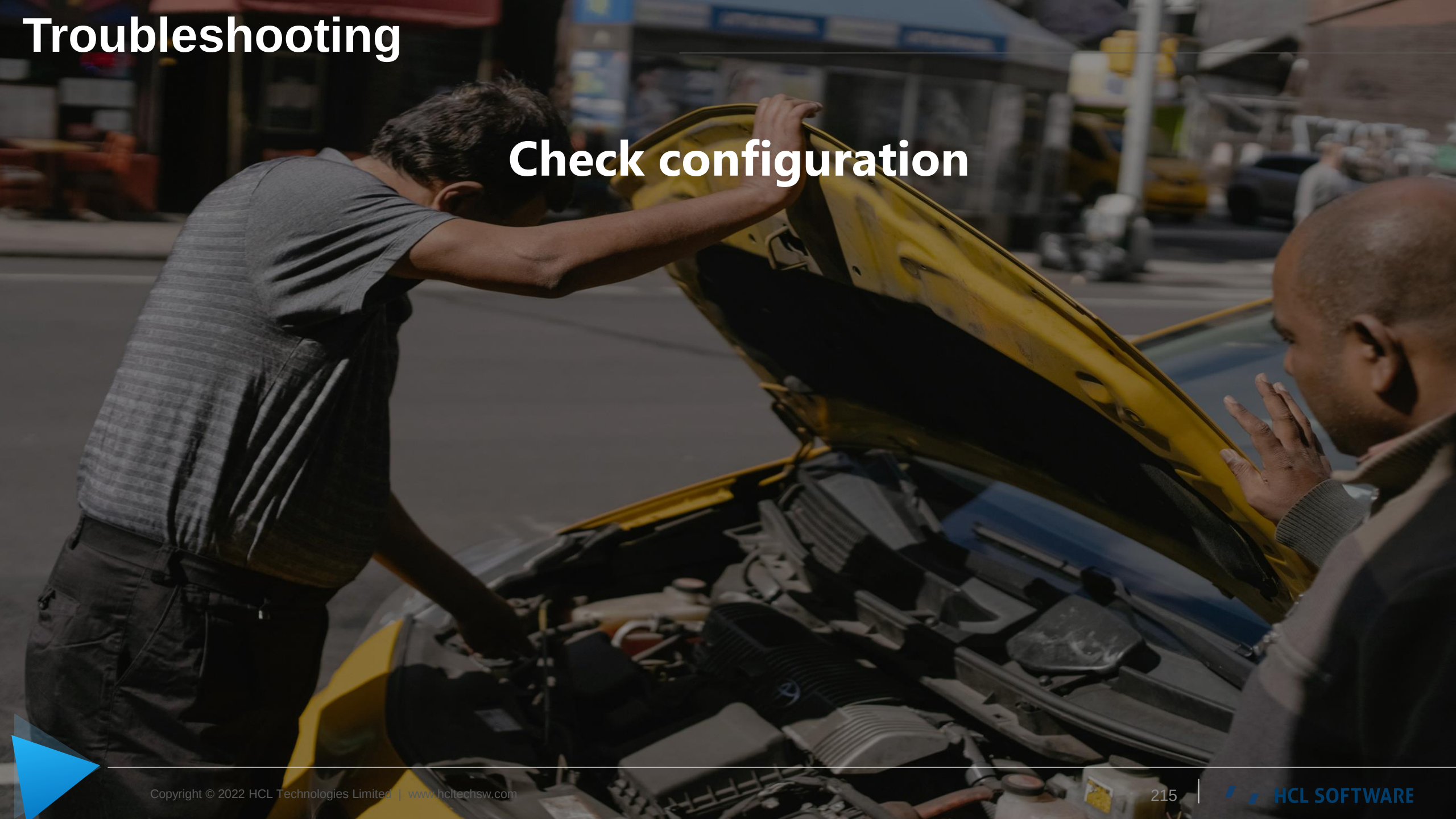
Shibboleth

References

Nomad & SAML



Troubleshooting



Check configuration

Troubleshooting

Set debug in notes.ini

Troubleshooting – Domino Server

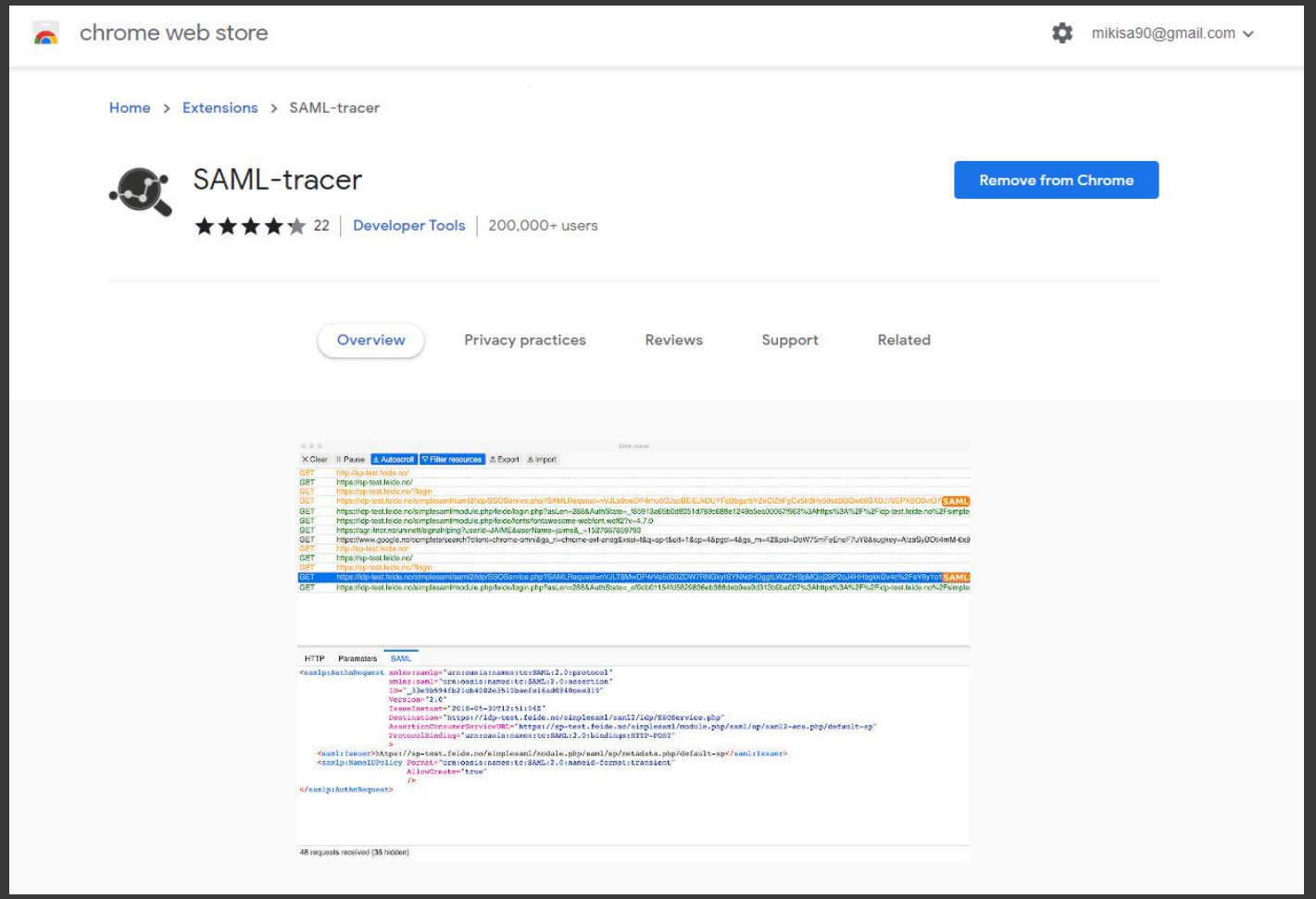
Troubleshooting – Notes Federated Login

Troubleshooting – Useful Tools

SAML-tracer

Chrome extension

Troubleshooting – Useful Tools



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
tell http dump vaulted idcache
[0F00:004F-0618] 04/15/2022 02:07:49 PM  Remote console command issued by Administrator/WYDucks: tell 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

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

SAML & SSO

Web Federated Login

Notes Federated Login

Traveler & SAML

Bonus – Nomad!

Troubleshooting

Issues

Q & A

Shibboleth

References

HCL Traveler

Secure mail operations

HCL SafeLinx

Multiple SAML configurations

Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

SAML & SSO

Web Federated Login

Notes Federated Login

Traveler & SAML

Bonus – Nomad!

Troubleshooting

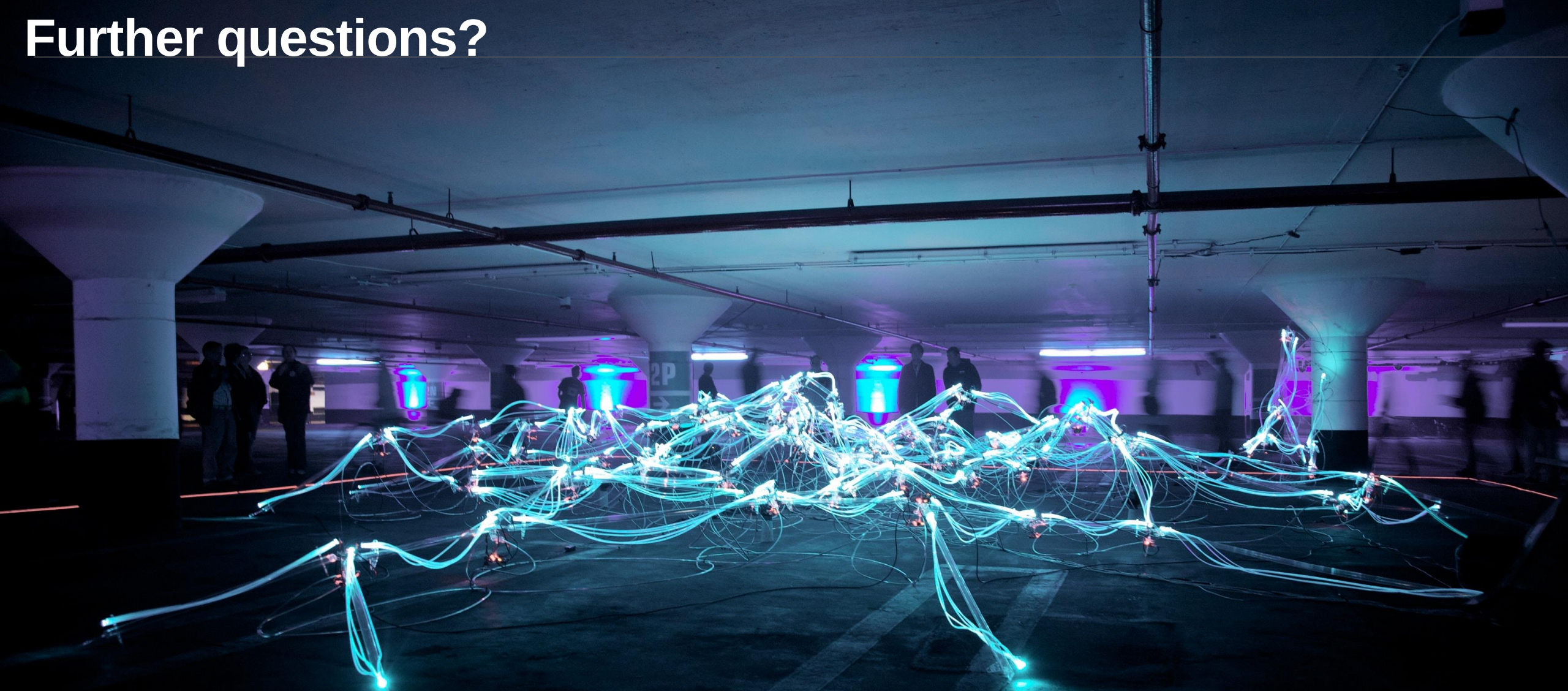
Issues

Q & A

Shibboleth

References

Further questions?



Evolve, disrupt. Together…

Table of Contents

Motivation

Why SAML?

SAML

Wording

How does it work?

HCL Domino & SAML

Prerequisites

Infrastructure Needed

Basic SAML Setup

SAML & SSO

Web Federated Login

Notes Federated Login

Traveler & SAML

Bonus – Nomad!

Troubleshooting

Issues

Q & A

Shibboleth

References

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