FERMILAB-SLIDES-19-033-CD

Migrating Office 365 From ADFS to Ping Federate

NLIT 2019

Kevin Conway

May 31, 2019

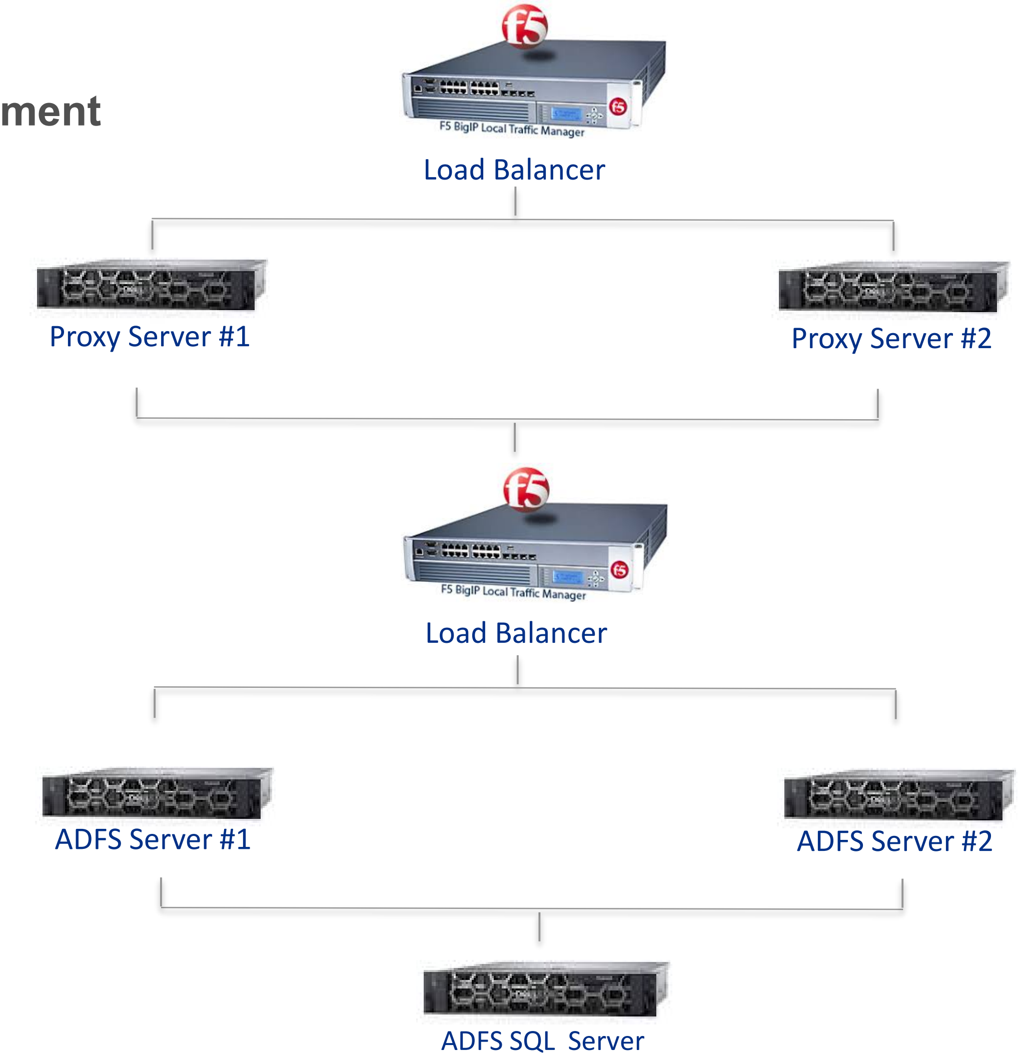
This manuscript has been authored by Fermi Research Alliance, LLC under Contract No. DE-AC02-07CH11359 with the U.S. Department of Energy, Office of Science, Office of High Energy Physics.

Agenda

- Why migrate?
- Pre-Requisites for Migration
- Create the O365 Connection
- Federated Trust Maintenance
- Testing
- Lessons Learned
- Questions

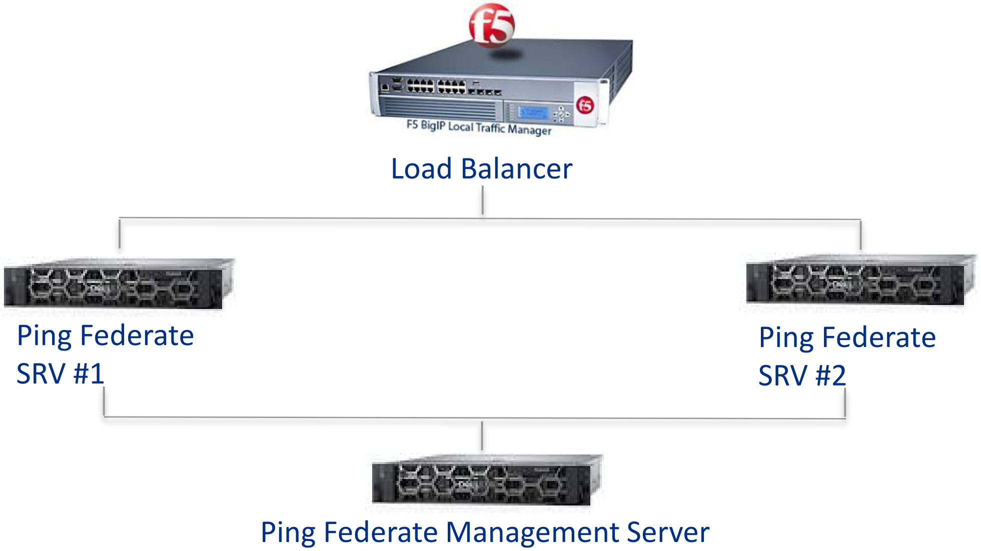
Why migrate?

ADFS Deployment



Why migrate?

Ping Federate Deployment


F5 BigIP Local Traffic Manager
Load Balancer
Ping Federate
SRV #1
Ping Federate
SRV #2
Ping Federate Management Server

- Simple
- Easier to scale
- Cost-effective

Why migrate?

PingFederate®

176 Added Service Providers!

Recently added…

SharePoint

Microsoft

Active Directory

Federation Services

The last remaining SP…

↓

Office 365

Pre-Requisites for Migration

Office 365 Tenant (Test Tenant makes life easier!)

- Global Admin Account

Ping Federate version 8.4 (Recommend version 9.X)

- Admin Account – Full Rights to Management Console

Azure Ad Connect version 1.1.880.0 08

PingFederate Integration with Azure Active Directory and Office 365

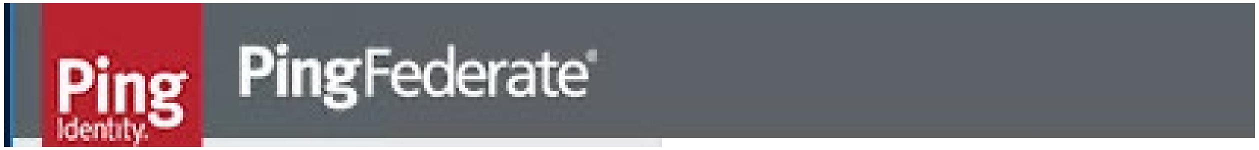
Updated June 18, 2018

https://docs.pingidentity.com

Create the O365 Connection

High Level Steps

- Preparing your Ping Federate Environment
- Create an O365 Connection in Ping Federate Development
- Copy the Connection Settings into Ping Federate Production – API Interface
- Break the ADFS Trust -PowerShell
- Federate Domain with Ping Federate – Use Azure Ad Connect
- Test your O365 Connection – Browsers, Mobile, & Client Applications



Existing Settings Used

Adapter

Data Stores

Signing Certificate

Items needed to Add/Configure

WS-Trust Protocol

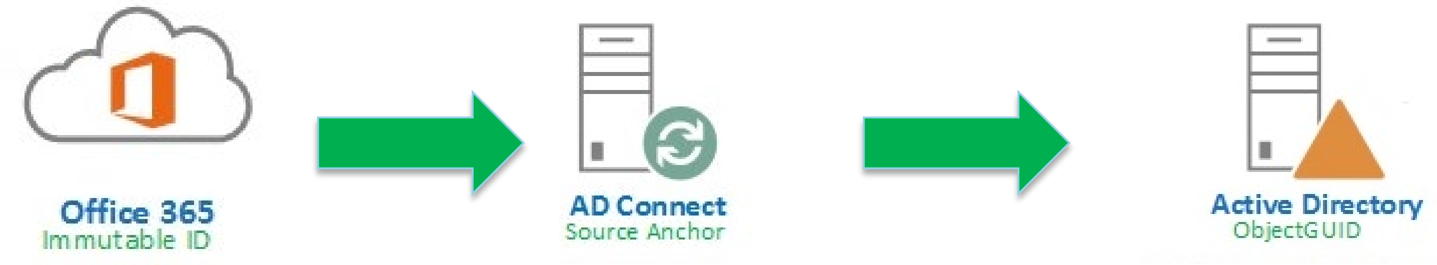
Token Processor

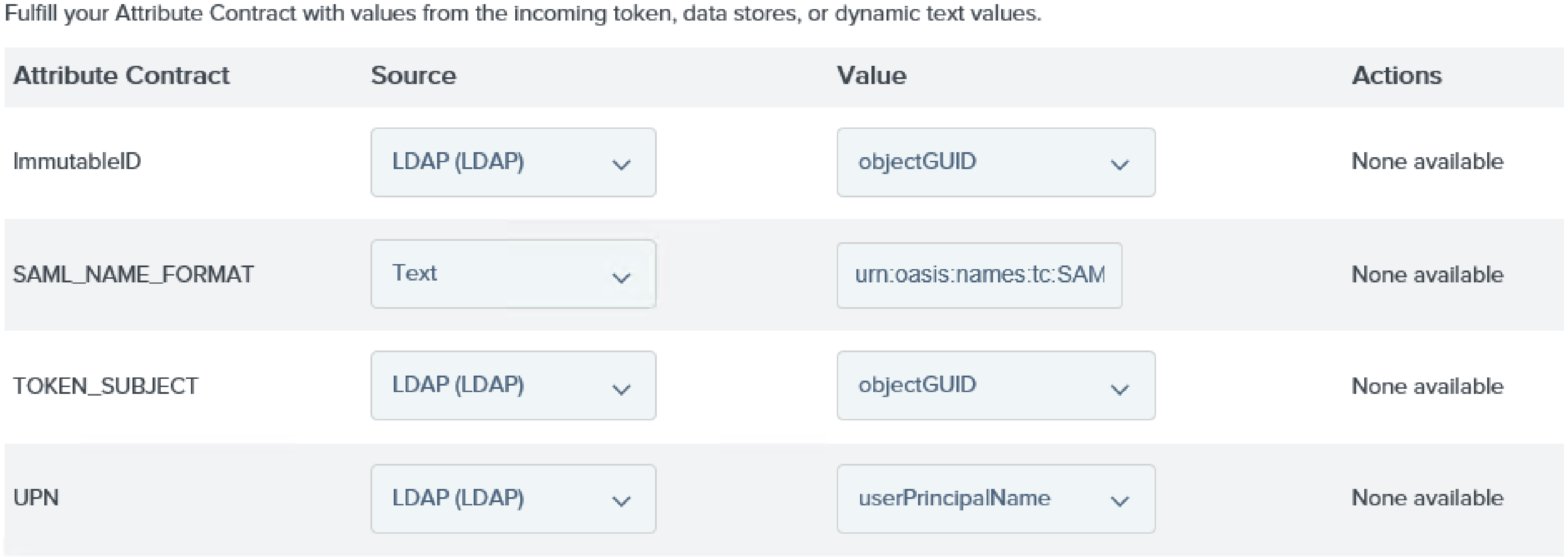
Create Credential Validator for upn

Enable objectGUID as binary attribute in datastore

LDAP Identity Attribute Mapping

Attribute Contract Fulfillment



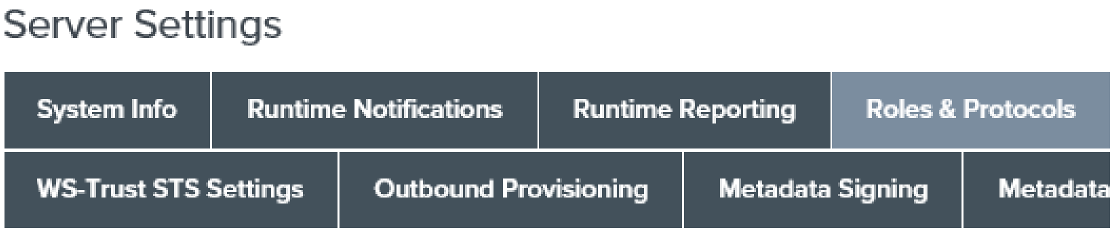


Fulfill your Attribute Contract with values from the incoming token, data stores, or dynamic text values.

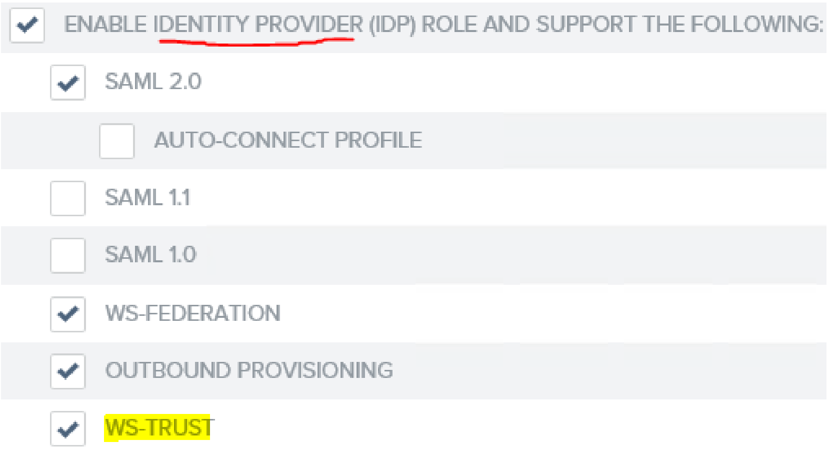
Attribute Contract	Source	Value	Actions
ImmutableID	LDAP (LDAP)	objectGUID	None available
SAML_NAME_FORMAT	Text	urn:oasis:names:tc:SAM	None available
TOKEN_SUBJECT	LDAP (LDAP)	objectGUID	None available
UPN	LDAP (LDAP)	userPrincipalName	None available

Enable the WS-Trust Protocol

Enable the WS-Trust Protocol in *Server Settings* on The Ping Management Server Interface



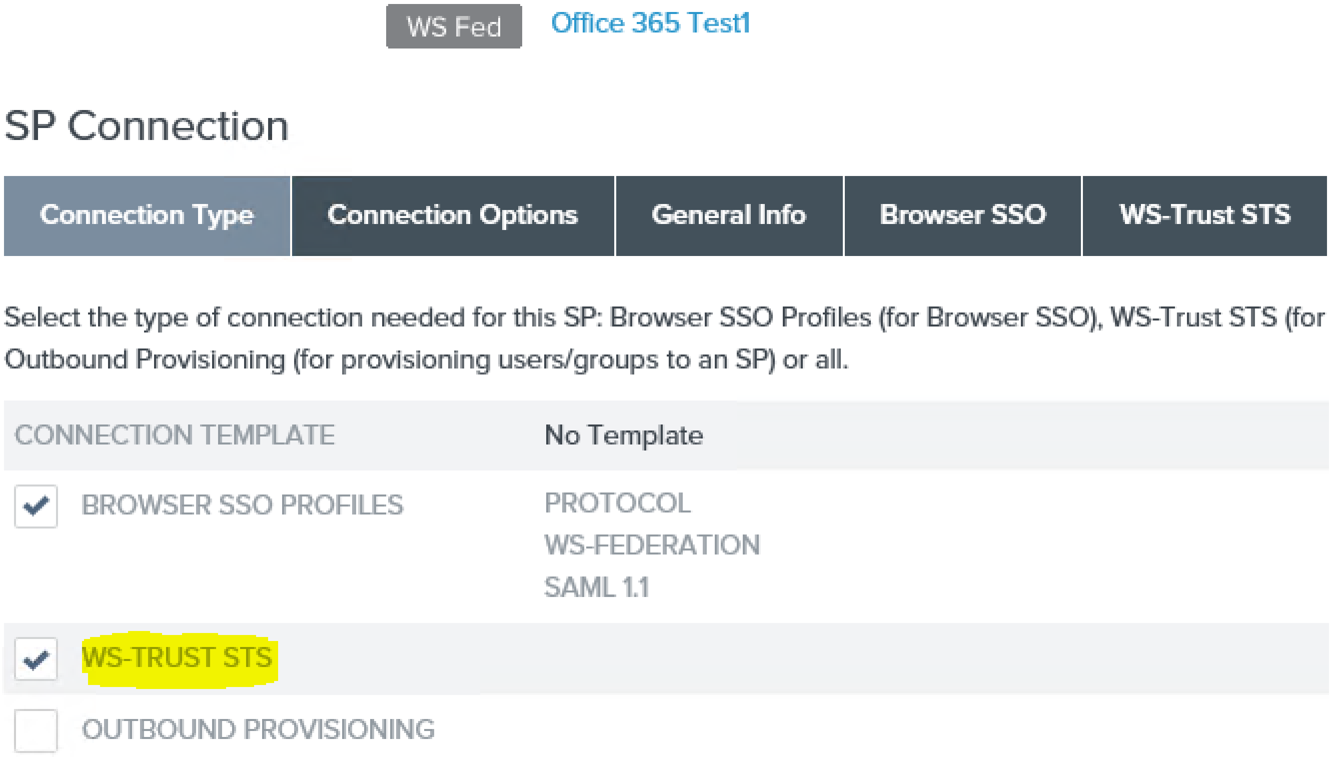
Enable for Identity Providers



- ☑ ENABLE IDENTITY PROVIDER (IDP) ROLE AND SUPPORT THE FOLLOWING:
  - ☑ SAML 2.0
    - □ AUTO-CONNECT PROFILE
  - □ SAML 1.1
  - □ SAML 1.0
  - ☑ WS-FEDERATION
  - ☑ OUTBOUND PROVISIONING
  - ☑ WS-TRUST

Enable the WS-Trust Protocol

Enable WS-Trust Protocol in *Server Settings → Connection Type* for the Office 365 Connection



WS Fed Office 365 Test1

SP Connection

Select the type of connection needed for this SP: Browser SSO Profiles (for Browser SSO), WS-Trust STS (for Outbound Provisioning (for provisioning users/groups to an SP) or all.

CONNECTION TEMPLATE No Template

☑ BROWSER SSO PROFILES

PROTOCOL
WS-FEDERATION
SAML 1.1

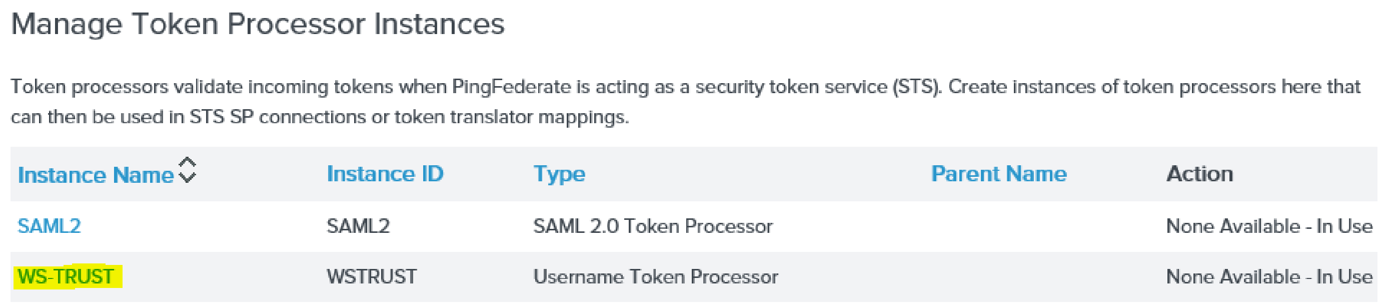
☑ WS-TRUST STS

☐ OUTBOUND PROVISIONING

Note! You may receive an error when running through The Azure AD Connect Wizard that it requires WS-TRUST Protocol and will not proceed until its selected In the Management Console. **Ping Documentation seemed incorrect here. WS-Trust Protocol was required to complete the Federated Trust with Ping Federate**.

Create Token Processor instance for WS-TRUST

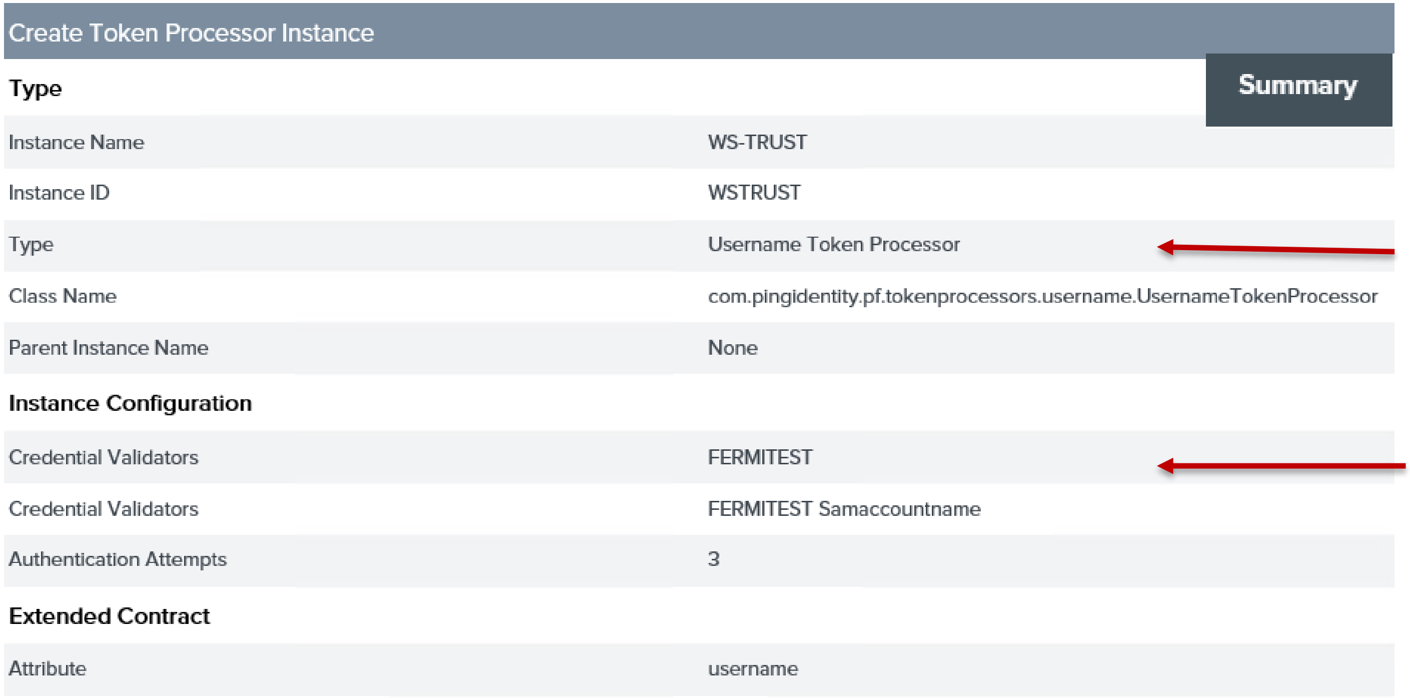
From the Identity Provider Page select *Token Processors*



Manage Token Processor Instances

Token processors validate incoming tokens when PingFederate is acting as a security token service (STS). Create instances of token processors here that can then be used in STS SP connections or token translator mappings.

Instance Name	Instance ID	Type	Parent Name	Action
SAML2	SAML2	SAML 2.0 Token Processor		None Available - In Use
WS-TRUST	WSTRUST	Username Token Processor		None Available - In Use



Create Token Processor Instance

Type

Instance Name	WS-TRUST
Instance ID	WSTRUST
Type	Username Token Processor
Class Name	com.pingidentity.pf.tokenprocessors.username.UsernameTokenProcessor
Parent Instance Name	None

Instance Configuration

Credential Validators	FERMITEST
Credential Validators	FERMITEST Samaccountname
Authentication Attempts	3

Extended Contract

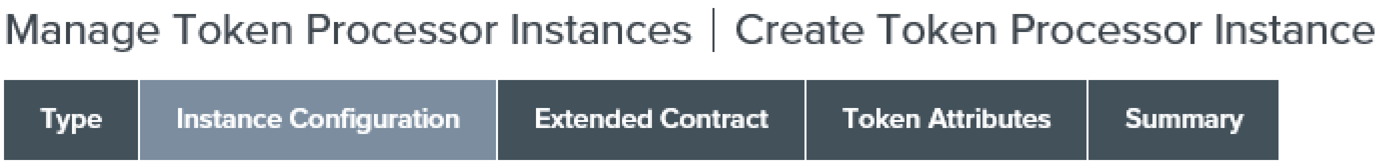
Attribute	username

Type - Username

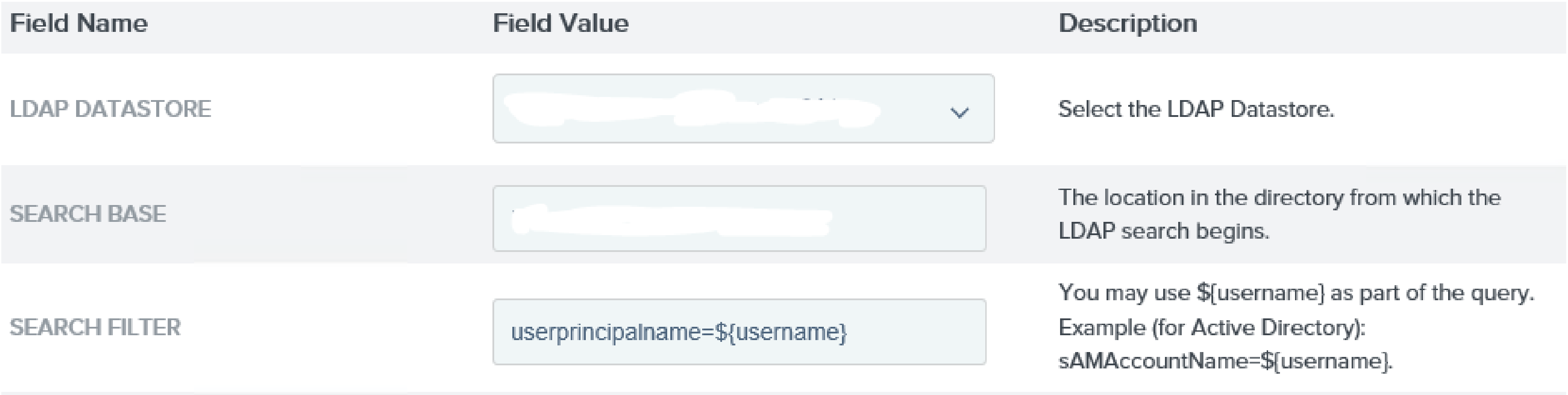
Credential Validators Are configured here

Create the Credential Validator for UPN

Configure a Password Credential Validator that uses UPN


Manage Token Processor Instances | Create Token Processor Instance

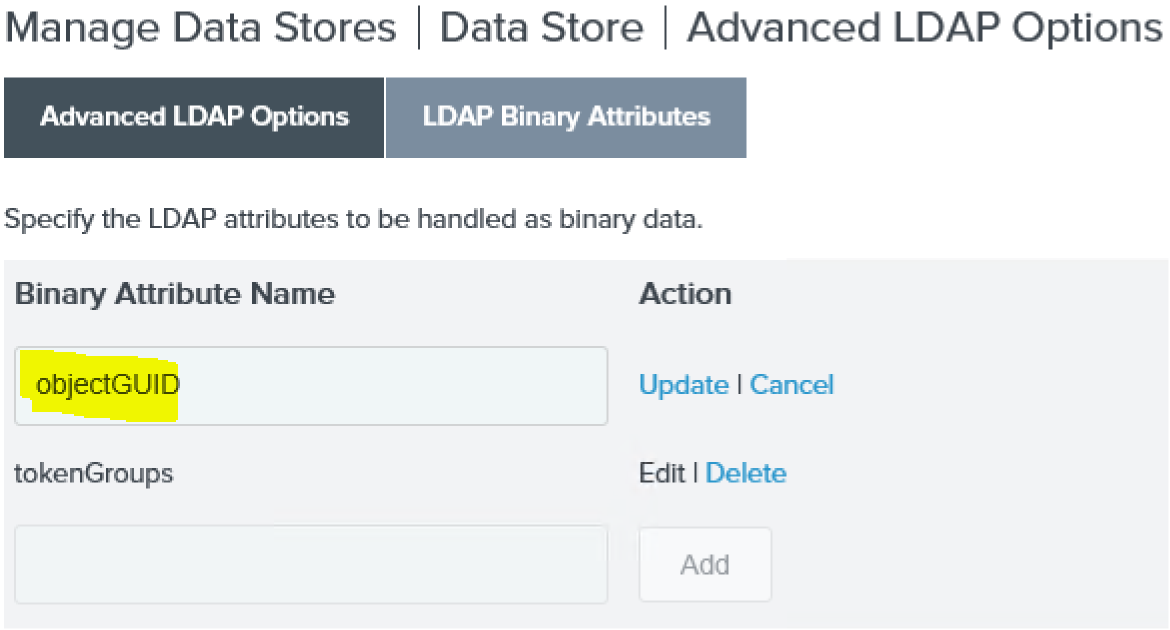
- Used to verify username/password pairs in various contexts
- We had one instance created for sAMAccountName=${username}
- We needed to add an instance for UserPrincipalName=${username}



Field Name	Field Value	Description
LDAP DATASTORE	[redacted]	Select the LDAP Datastore.
SEARCH BASE	[redacted]	The location in the directory from which the LDAP search begins.
SEARCH FILTER	userprincipalname=${username}	You may use ${username} as part of the query. Example (for Active Directory): sAMAccountName=${username}.

Enable objectGUID as binary attribute

From *Server Configuration* navigate to your Data Store Configurations, choose your Data Store and choose the *Advanced LDAP Options → LDAP Binary Types*



Manage Data Stores | Data Store | Advanced LDAP Options

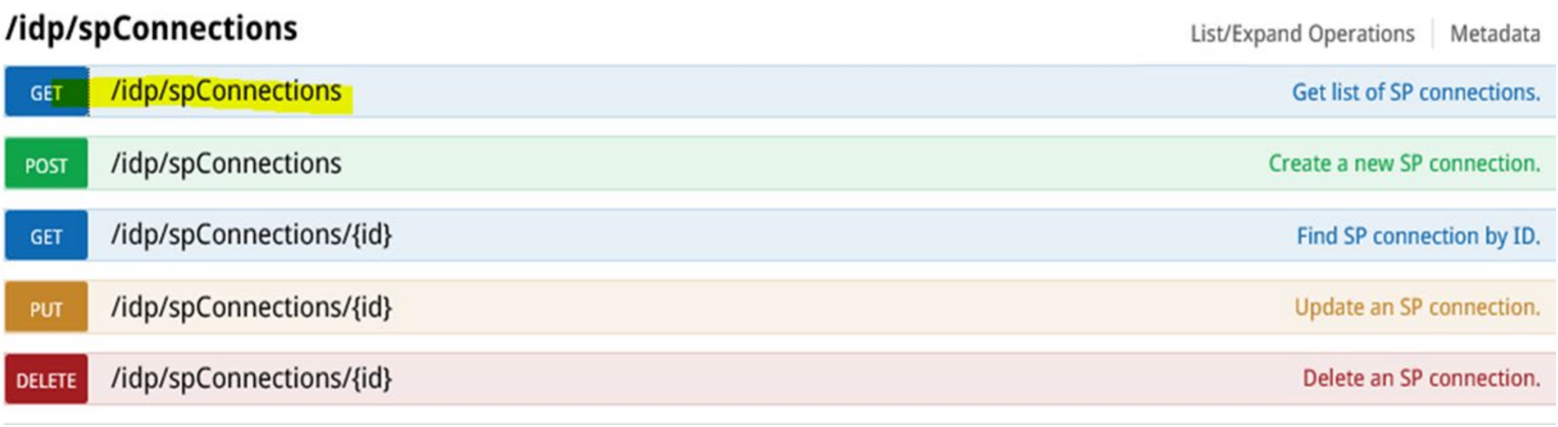
Specify the LDAP attributes to be handled as binary data.

Binary Attribute Name	Action
objectGUID	Update | Cancel
tokenGroups	Edit | Delete
	Add

Add *objectGUID* in the Binary Attribute Name filed and select *update*

Create the O365 Connection using API Interface

Select /idp/spConnections → *Get*

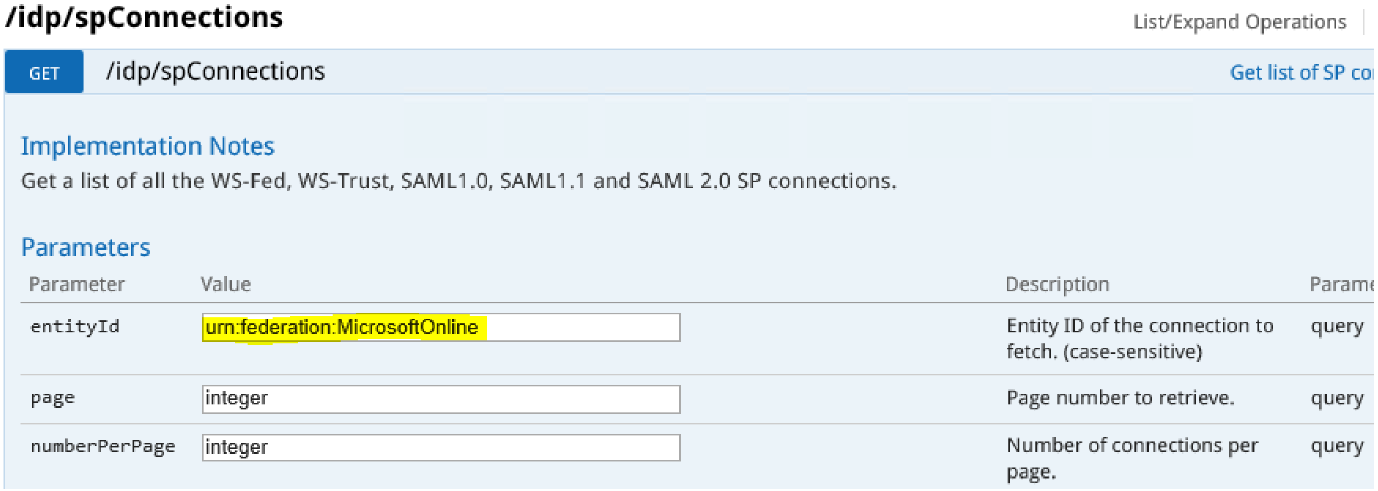


/idp/spConnections

List/Expand Operations | Metadata

GET	/idp/spConnections	Get list of SP connections.
POST	/idp/spConnections	Create a new SP connection.
GET	/idp/spConnections/{id}	Find SP connection by ID.
PUT	/idp/spConnections/{id}	Update an SP connection.
DELETE	/idp/spConnections/{id}	Delete an SP connection.

Search by *entityid* found in Ping Management Interface



/idp/spConnections

List/Expand Operations

GET /idp/spConnections Get list of SP co

Implementation Notes

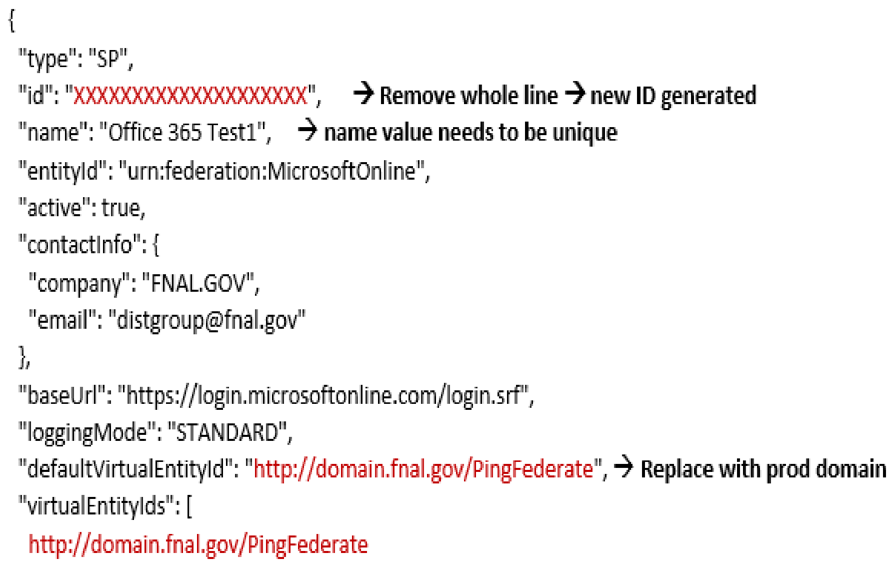
Get a list of all the WS-Fed, WS-Trust, SAML1.0, SAML1.1 and SAML 2.0 SP connections.

Parameters

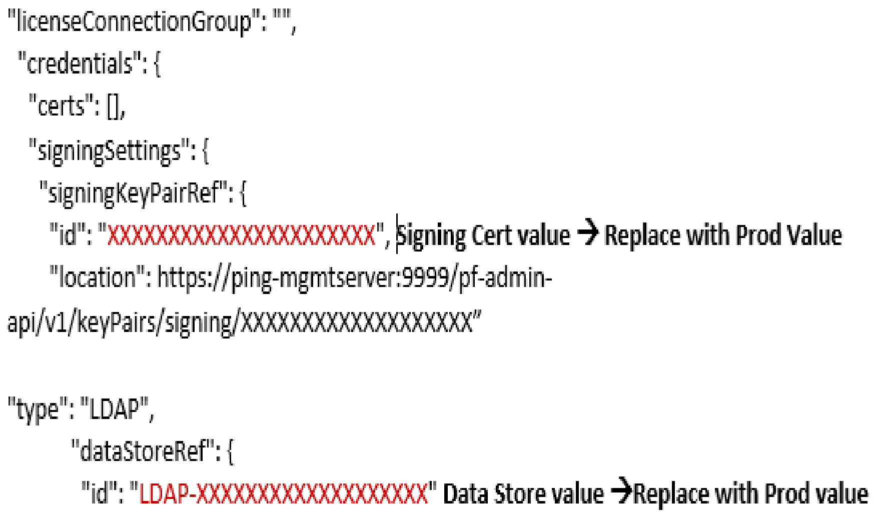
Parameter	Value	Description	Parame
entityId	urn:federation:MicrosoftOnline	Entity ID of the connection to fetch. (case-sensitive)	query
page	integer	Page number to retrieve.	query
numberPerPage	integer	Number of connections per page.	query

Selecting *Try it Out* will return only that connection and not all sp connections in the Management Console

Create the O365 Connection using the API Interface



```
{
 "type": "SP",
 "id": "XXXXXXXXXXXXXXXXXXXX",    → Remove whole line → new ID generated
 "name": "Office 365 Test1",    → name value needs to be unique
 "entityId": "urn:federation:MicrosoftOnline",
 "active": true,
 "contactInfo": {
  "company": "FNAL.GOV",
  "email": "distgroup@fnal.gov"
 },
 "baseUrl": "https://login.microsoftonline.com/login.srf",
 "loggingMode": "STANDARD",
 "defaultVirtualEntityId": "http://domain.fnal.gov/PingFederate", → Replace with prod domain
 "virtualEntityIds": [
  http://domain.fnal.gov/PingFederate
```



```
"licenseConnectionGroup": "",
 "credentials": {
  "certs": [],
  "signingSettings": {
   "signingKeyPairRef": {
    "id": "XXXXXXXXXXXXXXXXXXXXXXX", Signing Cert value → Replace with Prod Value
    "location": https://ping-mgmtserver:9999/pf-admin-
api/v1/keyPairs/signing/XXXXXXXXXXXXXXXXXXX"

"type": "LDAP",
      "dataStoreRef": {
       "id": "LDAP-XXXXXXXXXXXXXXXXXXX" Data Store value →Replace with Prod value
```

Connection ID and Name ID Values
In Text Editor you can Edit/Replace values

- "id" value gets generated when connection is created
- "name" value must be unique among SP's
- "virtualEntityID" values refers to Federated Domain

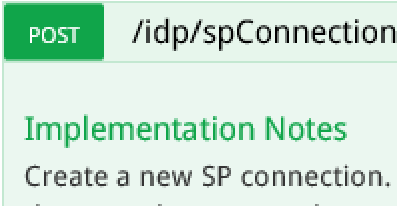
Certificate and Data Store Values
In a Text Editor you can Find/Replace All

- "id" refers to Signing Certificate value
- "location" refers to Ping Management Server
- "id" LDAP –xxxxxxx refers to Data Store

Create the O365 Connection using the API Interface

Back to the API Interface to paste updated values into the body of new connection field

Select → *POST*

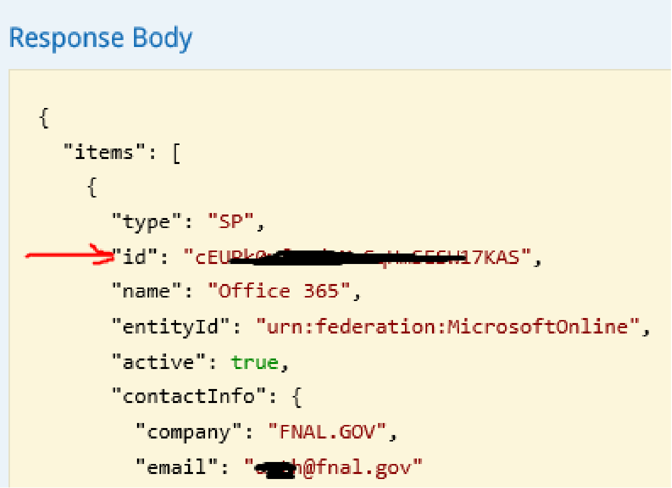


POST /idp/spConnection

Implementation Notes

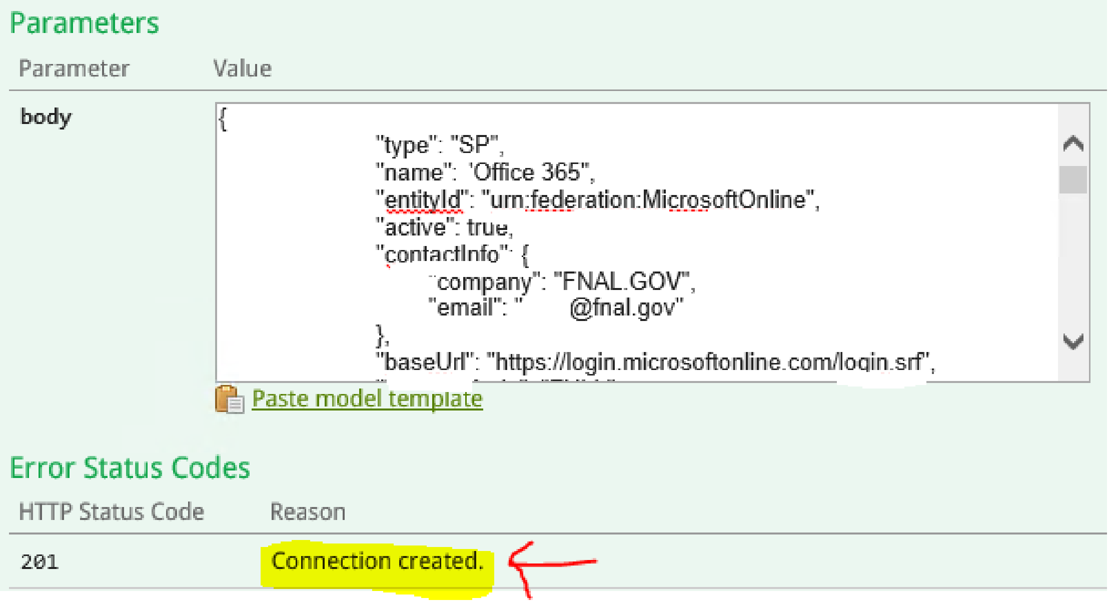
Create a new SP connection.

Once Connection is Created, you will find A value for SP “id”



Response Body

```
{
  "items": [
    {
      "type": "SP",
      "id": "cEU[redacted]7KAS",
      "name": "Office 365",
      "entityId": "urn:federation:MicrosoftOnline",
      "active": true,
      "contactInfo": {
        "company": "FNAL.GOV",
        "email": "[redacted]h@fnal.gov"
```



Parameters

Parameter	Value
body	see below

```
{
        "type": "SP",
        "name": 'Office 365",
        "entityId": "urn:federation:MicrosoftOnline",
        "active": true,
        "contactInfo": {
                "company": "FNAL.GOV",
                "email": "       @fnal.gov"
        },
        "baseUrl": "https://login.microsoftonline.com/login.srf",
```

Error Status Codes

HTTP Status Code	Reason
201	Connection created.

The Connection should now appear in the Ping Management Interface

Check current Federated Domain Settings from LDAP Maintenance Server containing Azure AD Connect Software

$msolcred = Get-Credential

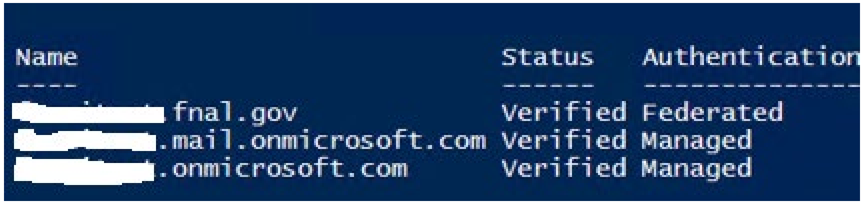
#provide credentials cloud service account@domain.onmicrosoft.com

Connect-msolservice -credential $msolcred

#At this point, you are authenticated in the cloud tenant

#Check the current state of the target domain “domain.fnal.gov”

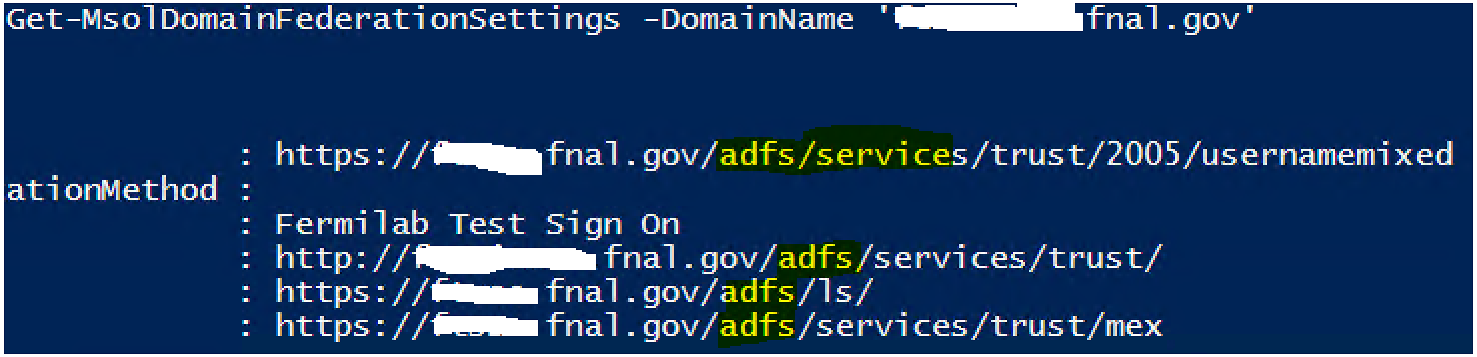
Get-MsolDomain



```
Name                              Status   Authentication
----                              ------   --------------
[redacted]fnal.gov                Verified Federated
[redacted].mail.onmicrosoft.com   Verified Managed
[redacted].onmicrosoft.com        Verified Managed
```

#Check Federated Domain settings to determine identity Provider

Get-MsolDomainFederationSettings -DomainName ‘domain.fnal.gov'



```
Get-MsolDomainFederationSettings -DomainName '[redacted]fnal.gov'



            : https://[redacted]fnal.gov/adfs/services/trust/2005/usernamemixed
ationMethod :
            : Fermilab Test Sign On
            : http://[redacted]fnal.gov/adfs/services/trust/
            : https://[redacted]fnal.gov/adfs/ls/
            : https://[redacted]fnal.gov/adfs/services/trust/mex
```

Break the Federated Trust with ADFS

#Break the Federated Trust with current identity provider (ADFS)

Set-MsolDomainAuthentication -DomainName domain.fnal.gov -Authentication Managed

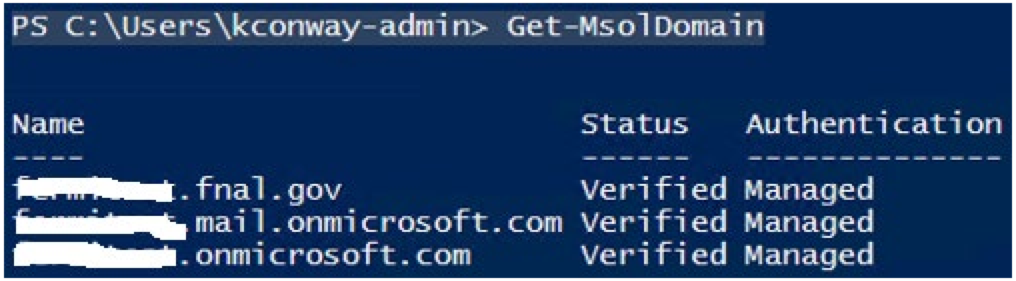
If successful, No output just prompt below. Trust Broken!!

PS C:\Users\kconway-admin> *Get-MsolDomain*

Verify Settings after change

#verify Federated Domain Status is now "managed" and NOT federated

Get-MsolDomain



```
PS C:\Users\kconway-admin> Get-MsolDomain


Name                              Status   Authentication
----                              ------   --------------
[redacted].fnal.gov               Verified Managed
[redacted]mail.onmicrosoft.com    Verified Managed
[redacted].onmicrosoft.com        Verified Managed
```

#check status that there is no listed provider

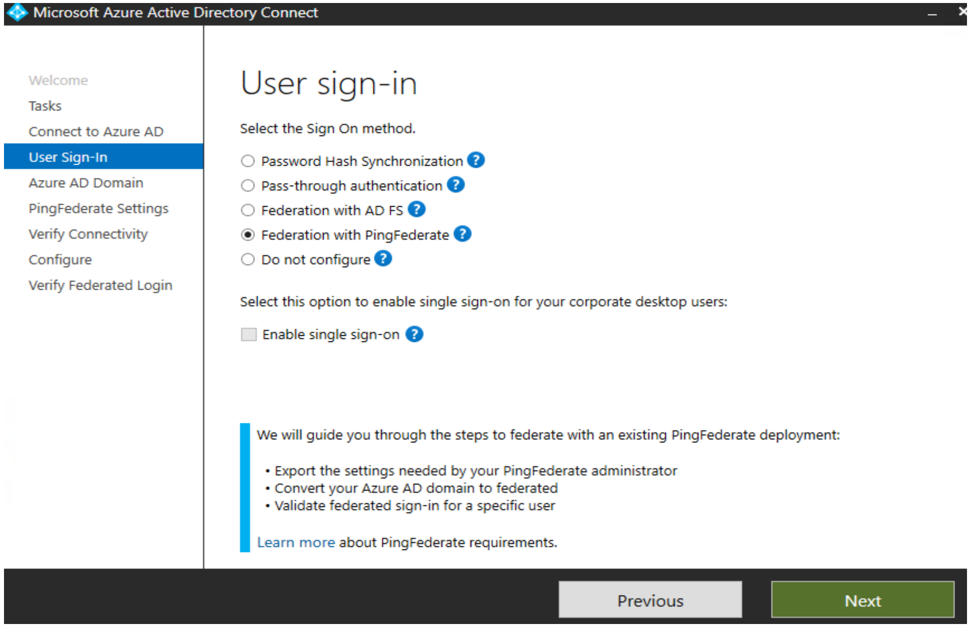
Get-MsolDomainFederationSettings -DomainName ‘domain.fnal.gov’

#No output means no listed provider – This is expected

Proceed to LDAP Server and run Azure Ad Connect to federate with Ping Federate

Federate Domain with Ping Federate

Log into LDAP Management Server containing Azure AD Connect Software and run *Azure AD Connect.exe*



User sign-in

Select the Sign On method.

○ Password Hash Synchronization

○ Pass-through authentication

○ Federation with AD FS

● Federation with PingFederate

○ Do not configure

Select this option to enable single sign-on for your corporate desktop users:

□ Enable single sign-on

We will guide you through the steps to federate with an existing PingFederate deployment:

- Export the settings needed by your PingFederate administrator
- Convert your Azure AD domain to federated
- Validate federated sign-in for a specific user

Learn more about PingFederate requirements.

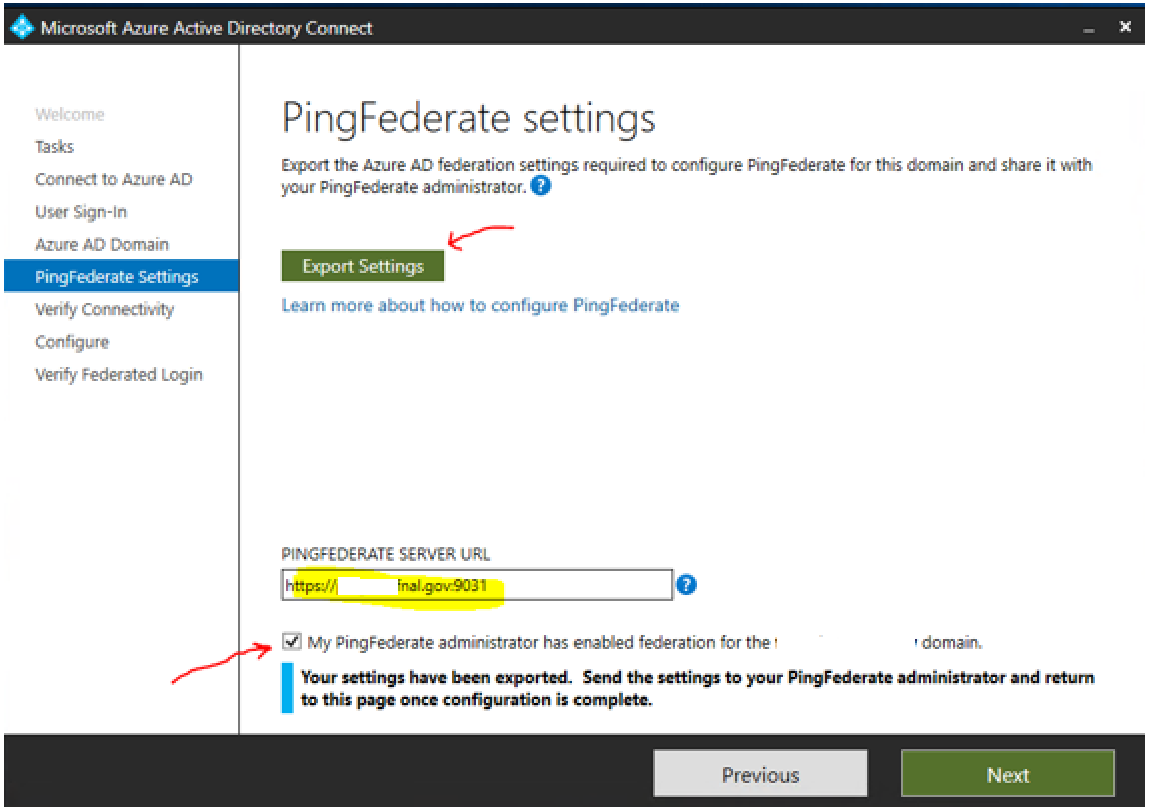
Next →

Select your Target domain (domain.gov)

displays message indicating domain is *managed* and will be converted to a *federated* domain

Federate the Domain with Ping Federate & export Settings for Ping Management Console

Ping Federate Settings Screen



PingFederate settings

Export the Azure AD federation settings required to configure PingFederate for this domain and share it with your PingFederate administrator.

PINGFEDERATE SERVER URL

https://[redacted]fnal.gov:9031

☑ My PingFederate administrator has enabled federation for the [redacted] domain.

Your settings have been exported. Send the settings to your PingFederate administrator and return to this page once configuration is complete.

File contents containing Federated Domain Settings for Ping Federate Management Console

Configuration Parameters from exported Configuration file

Connection types: WS-Federation and WS-Trust

EntityID (Connection ID): "urn:federation:MicrosoftOnline“

Virtual Server ID: "http://domain.com/PingFederate"

Attribute Contract:

ImmutableID - http://schemas.microsoft.com/LiveID/Federation/2008/05

UPN - http://schemas.xmlsoap.org/claims

Directory attribute source for ImmutableID: "objectGUID" (Binary, Base64)

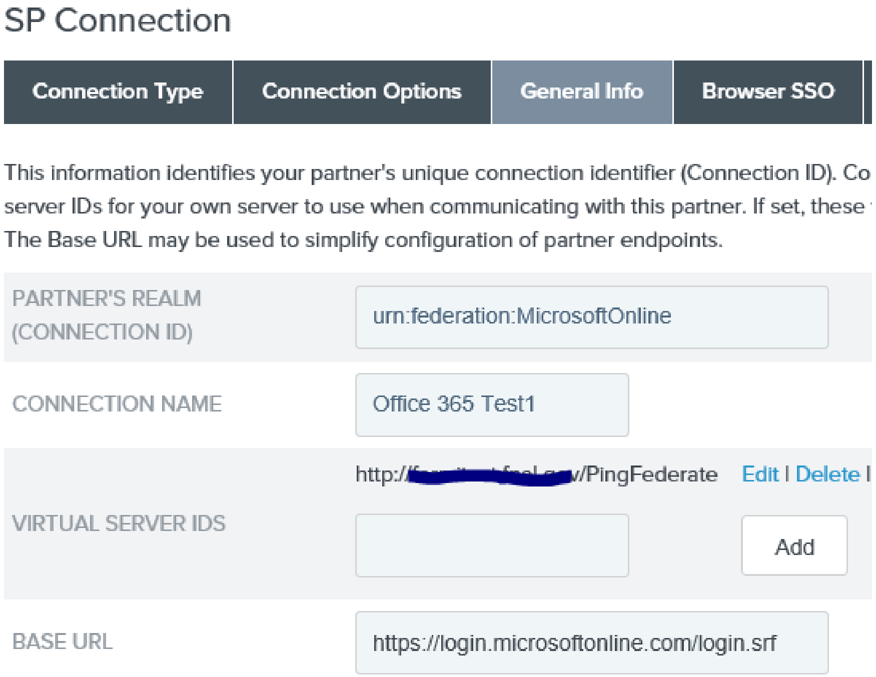
Directory attribute source for UPN: "userPrincipalName" (String)

Endpoint URL: https://login.microsoftonline.com/login.srf

WS-Trust default token type (PingFederate 8.4 and above): SAML 1.1 for Office 365

WS-Trust token processor type: Username Token Processor

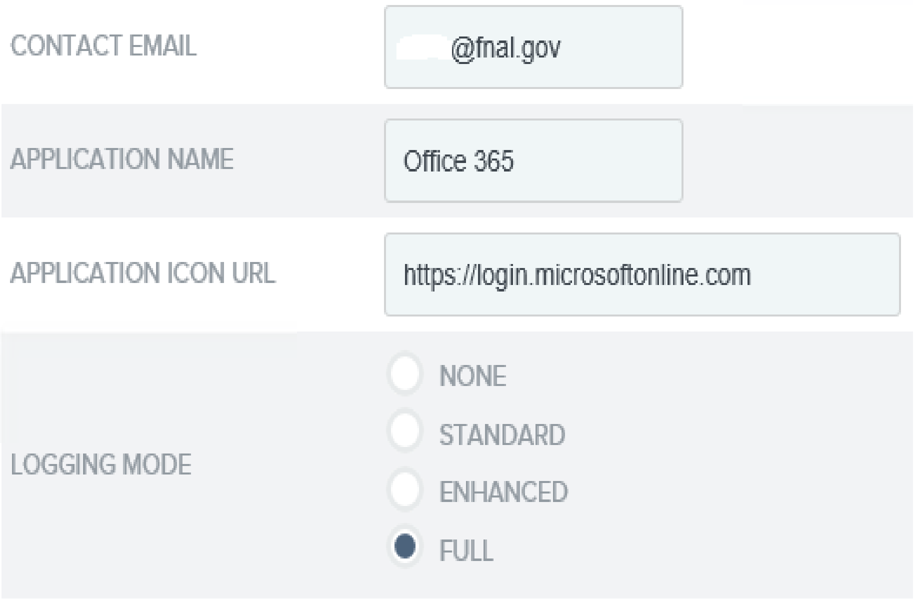
Populate values from exported File into Ping Federate Management Console



SP Connection

This information identifies your partner's unique connection identifier (Connection ID). Co
server IDs for your own server to use when communicating with this partner. If set, these
The Base URL may be used to simplify configuration of partner endpoints.

PARTNER'S REALM (CONNECTION ID)	urn:federation:MicrosoftOnline
CONNECTION NAME	Office 365 Test1
VIRTUAL SERVER IDS	http://[redacted]/PingFederate Edit | Delete | Add
BASE URL	https://login.microsoftonline.com/login.srf



CONTACT EMAIL	@fnal.gov
APPLICATION NAME	Office 365
APPLICATION ICON URL	https://login.microsoftonline.com
LOGGING MODE	○ NONE ○ STANDARD ○ ENHANCED ● FULL

EntityID (Connection ID): "urn:federation:MicrosoftOnline“

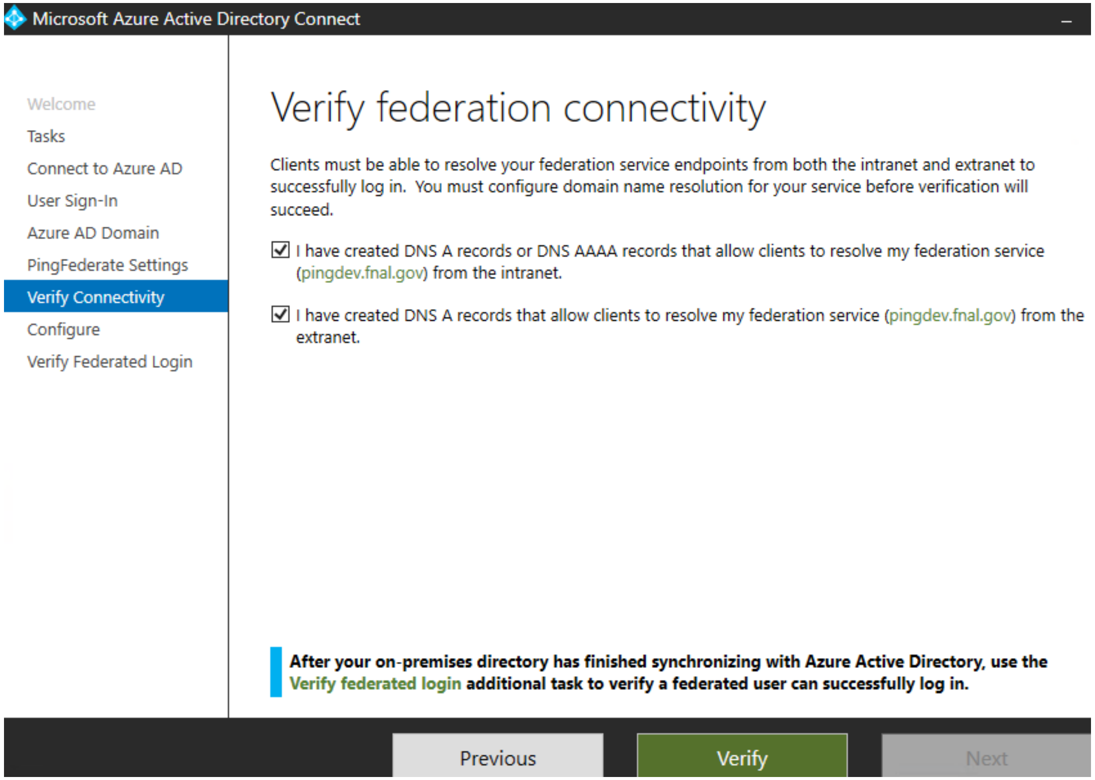
Endpoint URL: https://login.microsoftonline.com/login.srf

Informational items here

- *Contact info*
- *Application Name*
- *Application ICON URL*
- *Logging*

Federate Domain with Ping Federate

Verify Connectivity



Verify federation connectivity

Clients must be able to resolve your federation service endpoints from both the intranet and extranet to successfully log in. You must configure domain name resolution for your service before verification will succeed.

☑ I have created DNS A records or DNS AAAA records that allow clients to resolve my federation service (pingdev.fnal.gov) from the intranet.

☑ I have created DNS A records that allow clients to resolve my federation service (pingdev.fnal.gov) from the extranet.

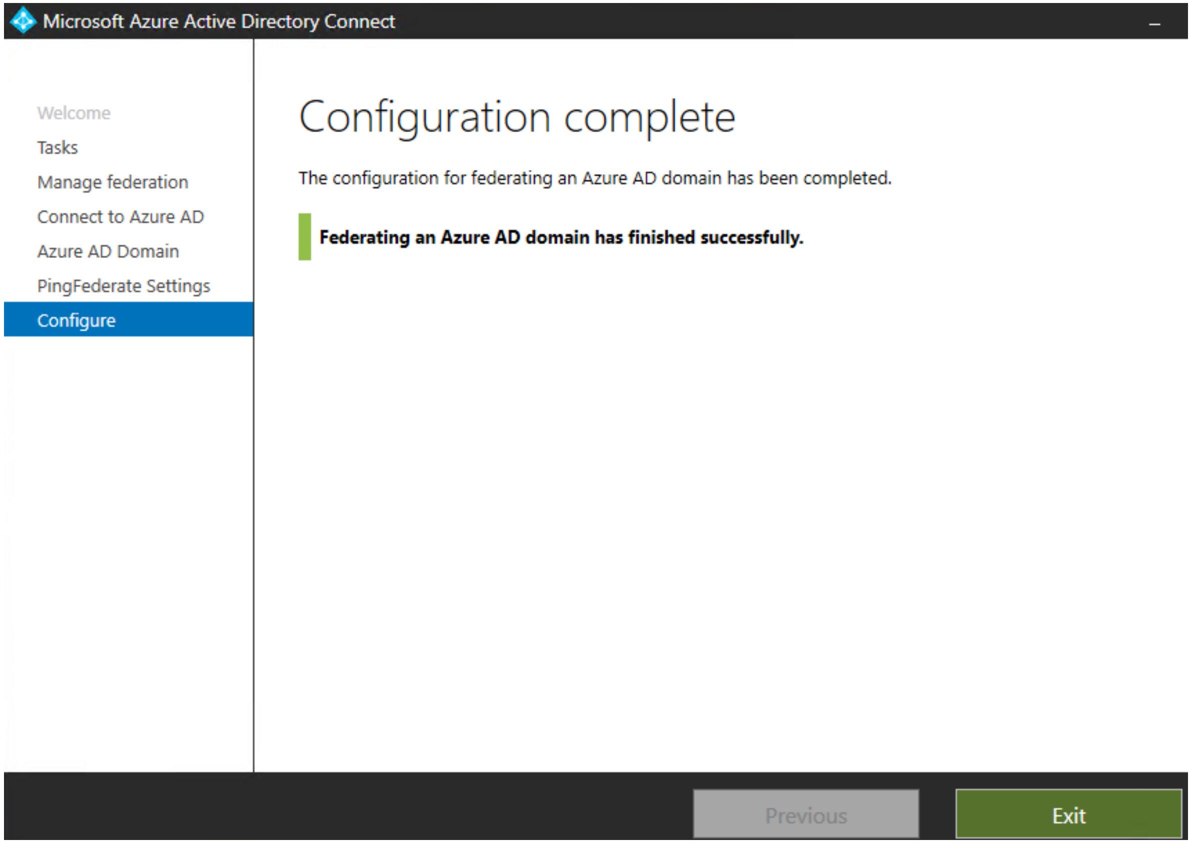
After your on-premises directory has finished synchronizing with Azure Active Directory, use the Verify federated login additional task to verify a federated user can successfully log in.

Next →

Configure Screen just tells what domain you will configure the trust with

Federate Domain with Ping Federate

Configuration Complete! You have now Federated with Ping



Configuration complete

The configuration for federating an Azure AD domain has been completed.

Federating an Azure AD domain has finished successfully.

Time to test sign-in!

Testing

Operating Systems

Windows

Mac OS

Linux

Browsers on Windows

INTERNET EXPLORER

MICROSOFT EDGE

chrome

mozilla Firefox

Browsers on MAC

Safari

chrome

mozilla Firefox

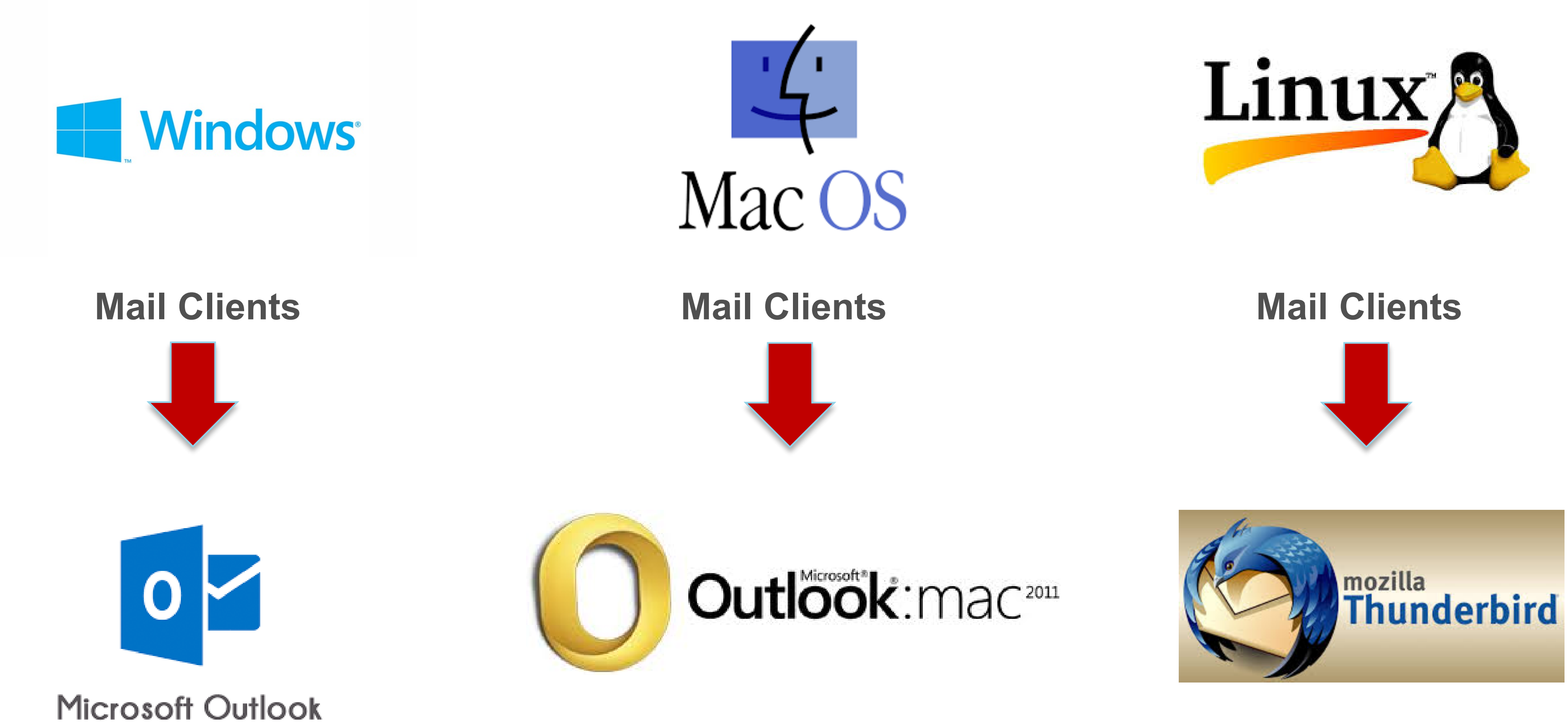
Browsers on Linux

mozilla Firefox

chrome

Testing

Operating Systems



Mail Clients

Mail Clients

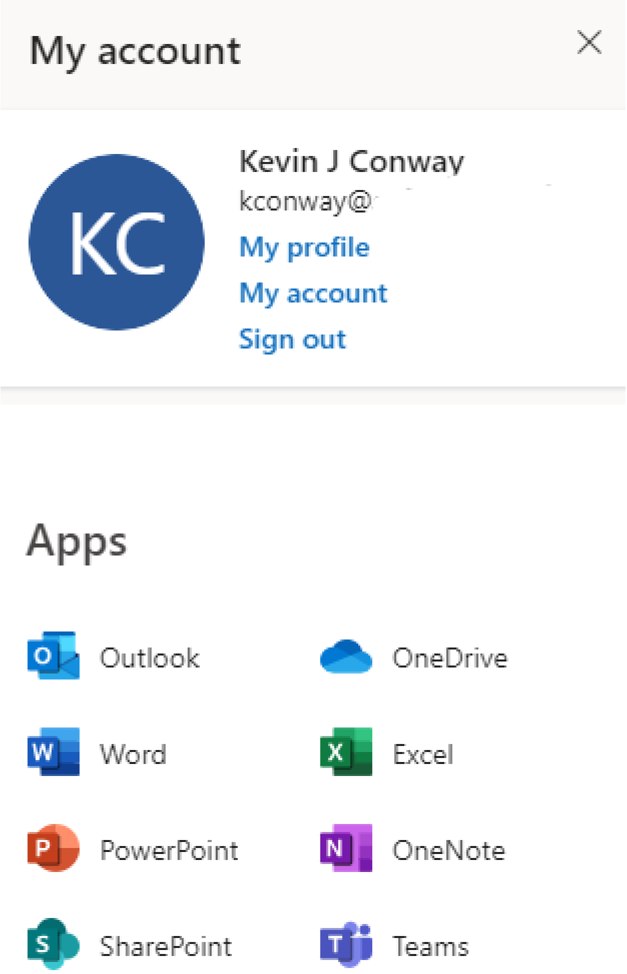
Mail Clients

Testing

Android & IOS Mobile

Don’t forget Outlook App on both platforms

Sign into Office Applications



My account

KC

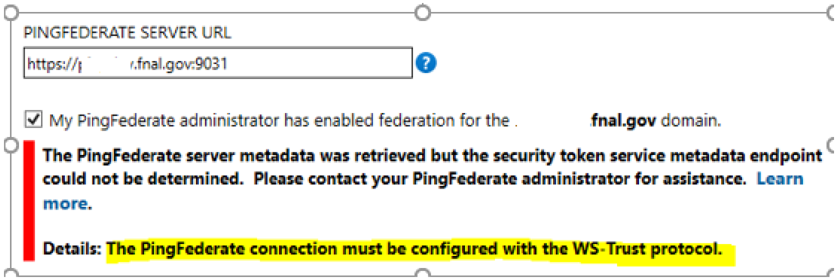
Kevin J Conway
kconway@
My profile
My account
Sign out

Apps

Outlook
OneDrive
Word
Excel
PowerPoint
OneNote
SharePoint
Teams

Lessons Learned

Make sure the WS-TRUST protocol is selected in the Management Console before federating with Ping.



PINGFEDERATE SERVER URL

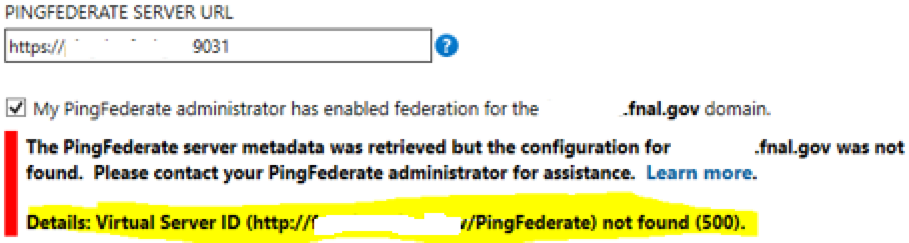
https:// .fnal.gov:9031

☑ My PingFederate administrator has enabled federation for the fnal.gov domain.

The PingFederate server metadata was retrieved but the security token service metadata endpoint could not be determined. Please contact your PingFederate administrator for assistance. Learn more.

Details: The PingFederate connection must be configured with the WS-Trust protocol.

Virtual Server ID value is *http://domain/Ping Federate* and it is required in the Connection Settings.



PINGFEDERATE SERVER URL

https:// 9031

☑ My PingFederate administrator has enabled federation for the .fnal.gov domain.

The PingFederate server metadata was retrieved but the configuration for .fnal.gov was not found. Please contact your PingFederate administrator for assistance. Learn more.

Details: Virtual Server ID (http:// /PingFederate) not found (500).

You need **2** password Credential Validators for mail clients, mobile phones, & other active clients

- sAMAccountName=${username}
- userprincipalname=${username}

Questions