

# AnyZearch Setup

kt-chan/anysearch at 0.0.1

AnyZearch | Your personal LLM

Not secure https://win10.local

Apps | 百度 Google W3 W3 Meeting iHR 智谱清言 讯飞星火 Kimi.ai Copilot 存储营销装备库 术语库 ChatGPT Pangu-s AnyZearch Work demo Course

KT

+ New Workspace

Welcome to AnyZearch, AnyZearch is an open-source AI tool by iteasoft labs that turns anything into a trained chatbot you can query and chat with.

AnyZearch is the easiest way to put powerful AI products like OpenAi, GPT-4, LangChain, PineconeDB, ChromaDB, and other services together in a neat package with no fuss to increase your productivity by 100x.

AnyZearch can run totally locally on your machine with little overhead you wont even notice it's there! No GPU needed. Cloud and on-premises installation is available as well.  
The AI tooling ecosystem gets more powerful everyday. AnyZearch makes it easy to use.

How do I get started?!

It's simple. All collections are organized into buckets we call "Workspaces". Workspaces are buckets of files, documents, images, PDFs, and other files which will be transformed into something LLM's can understand and use in conversation.  
You can add and remove files at anytime.

+ Create your first workspace

Is this like an AI dropbox or something? What about chatting? It is a chatbot isn't it?

Red arrow pointing to a wrench icon.

Type here to search

4:43 PM 11/8/2024

kt-chan/anysearch at 0.0.1 AnyZearch | Your personal LLM https://win10.local/settings/system-preferences Not secure Apps 百度 Google W3 W3 Meeting iHR 智谱清言 讯飞星火 Kimi.ai Copilot 存储营销装备库 术语库 ChatGPT Pangu-s AnyZearch Work demo Course KT

## System Preferences

These are the overall settings and configurations of your instance.

### Limit messages per user per day

Restrict non-admin users to a number of successful queries or chats within a 24 hour window. Enable this to prevent users from running up OpenAI costs.

### Single Sign-On (SSO) Configuration

Set up Single Sign-On (SSO) with Active Directory Federation Services (ADFS) on SAML 2.0.

You have to complete three steps one by one for ADFS SSO system setup.

Step 1: Generate Configuration File, please provide the endpoint path of ADFS on SAML 2.0, and the system would generate SSO configuration file.  
Step 2: Validate ADFS SSO, your system administrator should upload the file generated and set up the ADFS accordingly.  
Step 3: Convert the system to SSO. Remember that once changed to SSO, it is non reversible.

Contact Support Privacy & Data Save Changes

kt Chan 4:43 PM 11/8/2024 9

kt-chan/anysearch at 0.0.1 AnyZearch | Your personal LLM https://win10.local/settings/system-preferences

Not secure Apps 百度 Google W3 W3 Meeting iHR 智谱清言 讯飞星火 Kimi.ai Copilot 存储营销装备库 术语库 ChatGPT Pangu-s AnyZearch Work demo Course

KT

**Single Sign-On (SSO) Configuration**

Set up Single Sign-On (SSO) with Active Directory Federation Services (ADFS) on SAML 2.0.

You have to complete three steps one by one for ADFS SSO system setup.

Step 1: Generate Configuration File, please provide the endpoint path of ADFS on SAML 2.0, and the system would generate SSO configuration file.  
Step 2: Validate ADFS SSO, your system administrator should upload the file generated and set up the ADFS accordingly.  
Step 3: Convert the generated SSO Configuration File to XML, it is non reversible.

**ADFS SAML Endpoint Path**  
https://anysearch.local/adfs/ls/

**ADFS SAML Issuer**  
(e.g. anysearch.local)  
win10.local

**Callback Host with Port**  
(e.g. https://currentsite.local:3001)  
https://win10.local:3001/

**Download and Config at ADFS**

Pending for Configuration

Generate Config pending for validation... pending for conversion...

INSTANCE SETTINGS

AI Providers Admin

Users Workspaces

ADFS Entry Point Path

Invites General Settings

ADFS Party Trust Name

Customization Tools

ADFS Accessible URL  
ADFS 能链接的网址

Privacy & Data

Click twice to change

Type here to search

4:44 PM 11/8/2024

kt-chan/anysearch at 0.0.1 AnyZearch | Your personal LLM https://win10.local/settings/system-preferences Apps 百度 Google W3 W3 Meeting iHR 智谱清言 讯飞星火 Kimi.ai Copilot 存储营销装备库 术语库 ChatGPT Pangu-s AnyZearch Work demo Course KT

You have to complete three steps one by one for ADFS SSO system setup.

Step 1: Generate Configuration File, please provide the endpoint path of ADFS on SAML 2.0, and the system would generate SSO configuration file.

Step 2: Validate ADFS SSO, your system administrator should upload the file generated and set up the ADFS accordingly.

Step 3: Convert the system to SSO. Remember that once changed to SSO, it is non reversible.

Click twice to change

ADFS SAML Endpoint Path  
https://anysearch.local/adfs/ls/

ADFS SAML Issuer  
(e.g. anysearch.local)  
win10.local

Callback Host with Port  
(e.g. https://currentsite.local:3001)  
https://win10.local:3001/

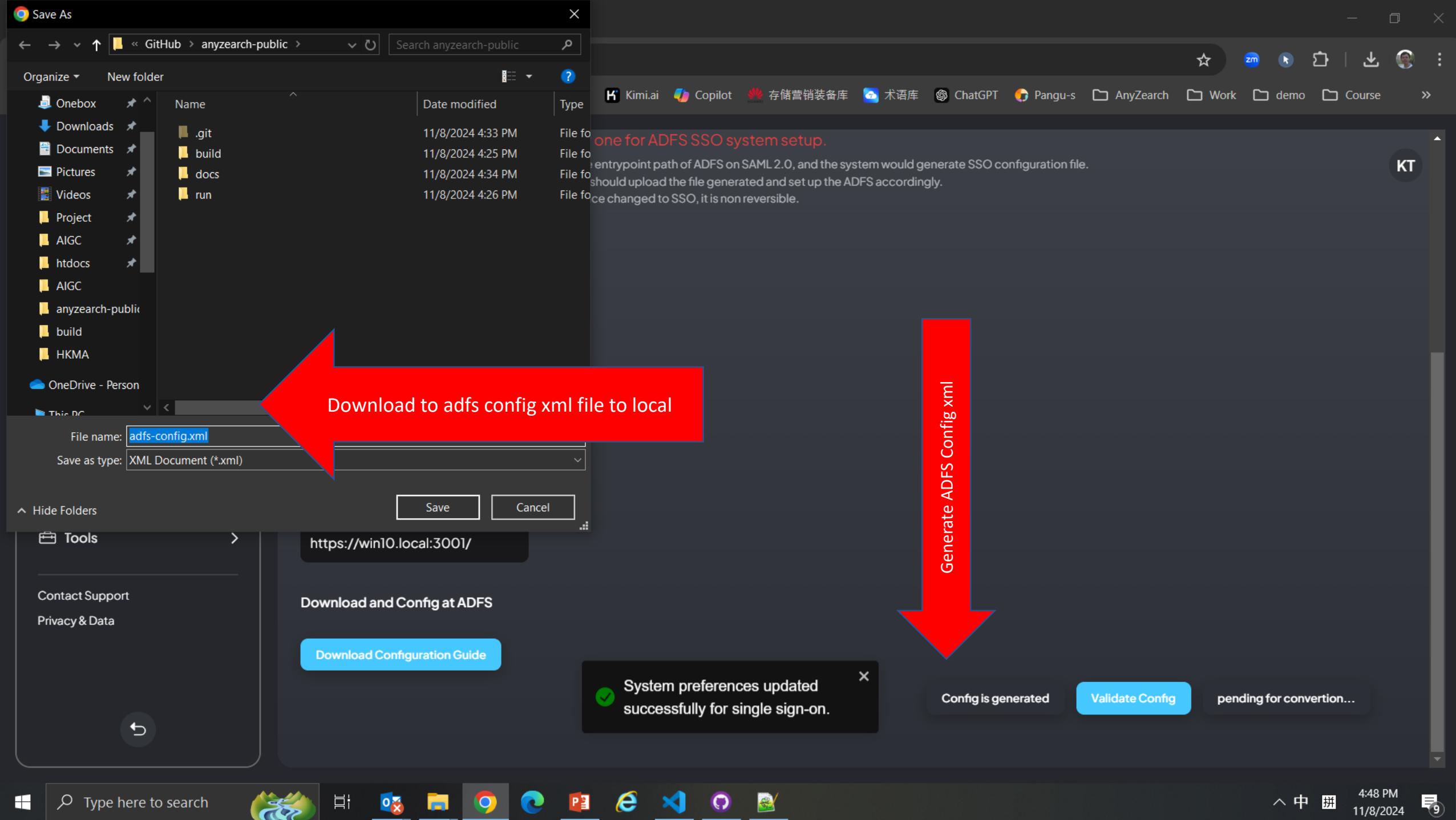
Download and Config at ADFS  
Pending for Configuration

Generate ADFS Config xml

Generate Config pending for validation... pending for conversion...

Type here to search

4:47 PM 11/8/2024



Save As

This PC > Downloads

Organize New folder

Name Date modified

HKMA

OneDrive - Person

This PC

3D Objects

Desktop

Documents

Downloads

Music

Onebox Sync

Pictures

Videos

Windows (C:)

Local Disk (D:)

File name: adfs-setup.pdf

Save as type: Adobe Acrobat Document (\*.pdf)

Save Cancel

https://win10.local:3001/

Download and Config at ADFS

Download Configuration Guide

Config is generated

Validate Config

pending for conversion...

Type here to search

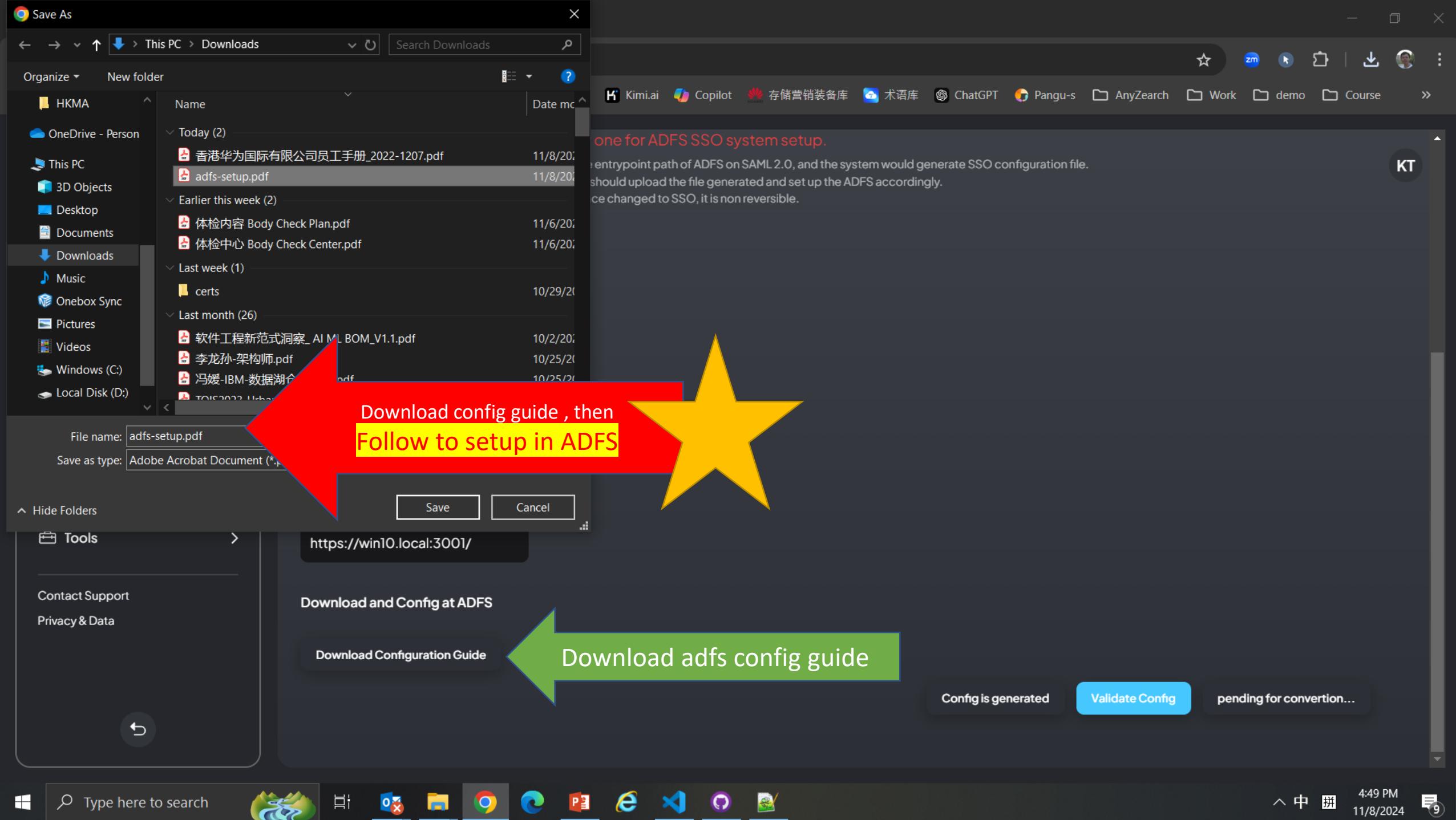
4:49 PM  
11/8/2024

KT

one for ADFS SSO system setup.  
entrypoint path of ADFS on SAML 2.0, and the system would generate SSO configuration file.  
should upload the file generated and set up the ADFS accordingly.  
ce changed to SSO, it is non reversible.

Download config guide , then  
**Follow to setup in ADFS**

**Download adfs config guide**



kt-chan/anysearch at 0.0.1

AnyZearch | Your personal LLM

Not secure https://win10.local/settings/system-preferences

Apps | 百度 Google W3 W3 Meeting iHR 智谱清言 讯飞星火 Kimi.ai Copilot 存储营销装备库 术语库 ChatGPT Pangu-s AnyZearch Work demo Course

AnyZearch

INSTANCE SETTINGS

- AI Providers
- Admin
  - Users
  - Workspaces
  - Workspace Chats
  - Invites
- General Settings
- Agent Skills
- Customization
- Tools
  - Contact Support
  - Privacy & Data

You have to complete three steps one by one for ADFS SSO system setup.

Step 1: Generate Configuration File, please provide the endpoint path of ADFS on SAML 2.0, and the system would generate SSO configuration file.  
Step 2: Validate ADFS SSO, your system administrator should upload the file generated and set up the ADFS accordingly.  
Step 3: Convert the system to SSO. Remember that once changed to SSO, it is non reversible.

ADFS SAML Endpoint Path  
https://anysearch.local/adfs/ls/

ADFS SAML Issuer  
(e.g. anysearch.local)  
win10.local

Callback Host with Port  
(e.g. https://currentsite.local:3001)  
https://win10.local:3001/

Download and Config at ADFS

Download Configuration Guide

After setup done in adfs

Config is generated

Validate Config

pending for conversion...

KT

After setup down, then click this to validate

Type here to search

4:50 PM 11/8/2024

9

# Microsoft ADFS Setup

\*D:\Downloads\adfsConfig.xml - Notepad++ [Administrator]

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

env.example adfsConfig.xml

```
1 <EntityDescriptor entityID="win10.local" xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
2   <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
3     <KeyDescriptor use="signing">
4       <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
5         <ds:X509Data>
6           <ds:X509Certificate>
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22       </ds:X509Certificate>
23     </ds:X509Data>
24   </ds:KeyInfo>
25 </KeyDescriptor>
26 <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://win10.local:3001/adfs/auth/logout"/>
27 <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://win10.local:3001/adfs/auth/postResponse" index="0"/>
28 </SPSSODescriptor>
29 </EntityDescriptor>
30
```

extensible Markup Language file length : 1,788 lines : 30 Ln : 7 Col : 13 Pos : 375 Unix (LF) UTF-8 INS

Type here to search 5:05 PM 10/28/2024



- [Manage](#)
  - [Tools](#)
  - [View](#)
  - [Help](#)
- 
- [Active Directory Administrative Center](#)
  - [Active Directory Domains and Trusts](#)
  - [Active Directory Module for Windows PowerShell](#)
  - [Active Directory Sites and Services](#)
  - [Active Directory Users and Computers](#)
  - [AD FS Management](#)
  - [ADSI Edit](#)
  - [Component Services](#)
  - [Computer Management](#)
  - [Defragment and Optimize Drives](#)
  - [Disk Cleanup](#)
  - [DNS](#)
  - [Event Viewer](#)
  - [Group Policy Management](#)
  - [Internet Information Services \(IIS\) Manager](#)
  - [iSCSI Initiator](#)
  - [Local Security Policy](#)
  - [Microsoft Azure Services](#)
  - [ODBC Data Sources \(32-bit\)](#)
  - [ODBC Data Sources \(64-bit\)](#)
  - [Performance Monitor](#)
  - [Recovery Drive](#)
  - [Registry Editor](#)
  - [Resource Monitor](#)
  - [Services](#)
  - [System Configuration](#)
  - [System Information](#)
  - [Task Scheduler](#)
  - [Windows Defender Firewall with Advanced Security](#)
  - [Windows Memory Diagnostic](#)
  - [Windows PowerShell](#)
  - [Windows PowerShell \(x86\)](#)
  - [Windows Server Backup](#)

[Dashboard](#)[Local Server](#)[All Servers](#)[AD DS](#)[AD FS](#)[DNS](#)[File and Storage Services](#) ▾[IIS](#)

## SERVERS

All servers | 1 total

Filter

Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
WIN-E91JJT7KOBQ	192.168.175.142	Online - Performance counters not started	10/28/2024 4:52:41 PM	00454-40000-00001-AA675 (Activated)

## EVENTS

All events | 4 total

Filter

Server Name	ID	Severity	Source	Log	Date and Time
WIN-E91JJT7KOBQ	161	Warning	Device Registration Service	DRS/Admin	10/28/2024 2:51:55 PM
WIN-E91JJT7KOBQ	137	Error	Device Registration Service	DRS/Admin	10/28/2024 2:21:55 PM
WIN-E91JJT7KOBQ	137	Error	Device Registration Service	DRS/Admin	10/28/2024 2:21:55 PM
WIN-E91JJT7KOBQ	278	Warning	AD FS	AD FS/Admin	10/28/2024 2:21:35 PM

## SERVICES

All services | 1 total

Filter



Type here to search



anysearch.local - Remote Desktop Connection

Server Manager

AD FS

File Action View Window Help

Dashboard Local Server All Servers AD DS AD FS DNS Firewall IIS

AD FS Service Attribute Stores Authentication Methods Certificates Claim Descriptions Device Registration Endpoints Scope Descriptions Web Application Proxy Access Control Policies Relying Party Trusts Claims Provider Trusts Application Groups

Relying Party Trusts

Add Relying Party Trust Wizard

Welcome

Steps

- Welcome
- Select Data Source
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Welcome to the Add Relying Party Trust Wizard

Claims-aware applications consume claims in security tokens to make authentication and authorization decisions. Non-claims-aware applications are web-based and use Windows Integrated Authentication in the internal network and can be published through Web Application Proxy for extranet access. [Learn more](#)

Claims aware

Non claims aware

< Previous Start Cancel

Party Trusts

- Add Relying Party Trust...
- New Window from Here
- Refresh
- Local
- Get Federation Metadata...
- Set Access Control Policy...
- Set Claim Issuance Policy...
- Properties
- Help

TASKS

Type here to search

4:56 PM 10/28/2024

The screenshot displays the Microsoft Server Manager interface for managing Active Directory Federation Services (AD FS). On the left sidebar, under the 'AD FS' section, the 'Relying Party Trusts' link is highlighted with a large red arrow. This indicates the user's intention to start the process of adding a new relying party trust. The main window shows the 'Add Relying Party Trust Wizard' welcome screen, which provides instructions for creating a trust. It mentions that claims-aware applications use security tokens for authentication and authorization, while non-claims-aware applications use Windows Integrated Authentication. The 'Claims aware' option is selected. The bottom status bar shows the system time as 4:56 PM on October 28, 2024.



- Dashboard
- Local Server
- All Servers
- AD DS
- AD FS**
- DNS
- File and Storage Services
- IIS

AD FS

File Action View Window Help

Server |

Relying Party Trusts

Add Relying Party Trust Wizard

Select Data Source

Steps

- >Welcome
- Select Data Source
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

Import data about the relying party published online or on a local network  
Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Import data about the relying party from a file  
Use this option to import the necessary data and certificates from a file. Ensure that this validate the source of the file.

Federation metadata address (host name or URL):  
Example: fs.contoso.com or https://www.contoso.com

Federation metadata file location:

Enter data about the relying party manually  
Use this option to manually input the necessary data about the relying party.

Actions

- Add Relying Party Trust...
- New Window from Here
- Refresh
- Cancel

Party Trusts

Add Relying Party Trust... New Window from Here Refresh Cancel

Browse for Metadata File...

This PC > Documents

Organize New folder

Name	Date modified
adfsConfig.xml	10/28/2024 3:23 PM
win10.local.xml	8/15/2024 1:15 PM

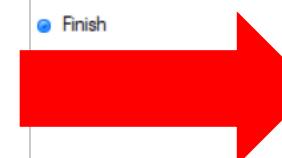
File name: adfsConfig.xml

Metadata files (\*.xml)

Open Cancel

4:57 PM 10/28/2024

TASKS



anysearch.local - Remote Desktop Connection

Server Manager

AD FS

File Action View Window Help

Dashboard Local Server All Servers AD DS AD FS DNS File and Storage Services IIS

Server |

AD FS Relying Party Trusts

Add Relying Party Trust Wizard

Specify Display Name

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Enter the display name and any optional notes for this relying party.

Display name: win10.local

Notes:

< Previous Next > Cancel

Party Trusts

- Add Relying Party Trust...
- New Window from Here
- Refresh
- Properties
- Update from Federation Metadata...
- Set Access Control Policy...
- Set Claim Issuance Policy...
- able
- ete
- p

TASKS

Type here to search

5:07 PM 10/28/2024

This screenshot shows the Microsoft Server Manager interface for managing Active Directory Federation Services (AD FS). The left navigation pane highlights the 'AD FS' service. A modal window titled 'Add Relying Party Trust Wizard' is open, specifically the 'Specify Display Name' step. A red arrow points to the 'Display name' input field, which contains 'win10.local'. The 'Notes' field is empty. Below the wizard are several actions related to Relying Party Trusts, such as 'Add Relying Party Trust...', 'New Window from Here', and 'Refresh'. The bottom right corner shows the current date and time as '5:07 PM 10/28/2024'.

anysearch.local - Remote Desktop Connection

Server Manager

AD FS

File Action View Window Help

Dashboard Local Server All Servers AD DS AD FS DNS File and Storage Services IIS

Relying Party Trusts

Add Relying Party Trust Wizard

Choose Access Control Policy

Steps

- Welcome
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Choose an access control policy:

Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and require multi-factor authentication.
Permit everyone and require MFA for specific group	Grant access to everyone and require MFA for specific groups.
Permit everyone and require MFA from extranet access	Grant access to the intranet users and require MFA from extranet access.
Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and require MFA from unauthenticated devices.
Permit everyone and require MFA, allow automatic device registration	Grant access to everyone and require MFA, allowing automatic device registration.
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more specific groups.

Policy

Permit everyone

I do not want to configure access control policies at this time. No user will be permitted access for this application.

< Previous Next > Cancel

TASKS

4:58 PM 10/28/2024

7

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box in the Microsoft Server Manager. A large red arrow points to the 'Choose Access Control Policy' step in the wizard's progress bar. The 'Choose an access control policy:' section is expanded, showing a list of policy options. The 'Permit everyone' option is selected. Below it, the 'Policy' section displays 'Permit everyone'. At the bottom of the dialog, there is a checkbox labeled 'I do not want to configure access control policies at this time. No user will be permitted access for this application.' The background shows the 'Relying Party Trusts' list in the main pane of the Server Manager.

anysearch.local - Remote Desktop Connection

Server Manager

AD FS

File Action View Window Help

Dashboard Local Server All Servers AD DS AD FS DNS File and Storage Services IIS

Server | Tools View Help

TASKS ▾

AD FS

Relying Party Trusts

Display Name Enabled Type Identifier

Display Name	Enabled	Type	Identifier
win10.local	Yes	WS-Tr...	win10.local

Actions

Relying Party Trusts

- Add Relying Party Trust...
- View
- New Window from Here
- Refresh
- Help

win10.local

- Update from Federation Metadata...
- Edit Access Control Policy...
- Edit Claim Issuance Policy...
- Disable
- Properties
- Delete
- Help

TASKS ▾

TASKS ▾

Type here to search

4:58 PM  
10/28/2024

7

The screenshot shows the Windows Server Manager interface for managing Active Directory Federation Services (AD FS). The left sidebar lists various server roles and services, with 'AD FS' currently selected. The main window displays the 'Relying Party Trusts' configuration. A red arrow points to the 'Service' node in the navigation pane. The 'win10.local' trust is selected in the list, and its details are shown in the Actions pane on the right, including options like 'Update from Federation Metadata...', 'Edit Access Control Policy...', and 'Delete'.

anysearch.local - Remote Desktop Connection

Server Manager

AD FS

File Action View Window Help

Dashboard Local Server All Servers AD DS AD FS DNS File and Storage Services IIS

Server |

AD FS Service Attribute Stores Authentication Methods Certificates Claim Descriptions Device Registrations Endpoints Scope Descriptions Web Application Proxy Access Control Policies Relying Party Trusts Claims Provider Trusts Application Groups

Relying Party Trusts

Display Name	Enabled	Type	Identifier
win10.local	Yes	WS-Tr...	win10.local

Actions

Relying Party Trusts

- Add Relying Party Trust...
- View
- New Window from Here
- Refresh
- Help

win10.local

- Update from Federation Metadata...
- Edit Access Control Policy...
- Edit Claim Issuance Policy...**
- Disable
- Properties
- Delete
- Help

TASKS

4:59 PM 10/28/2024

A large red arrow points from the left margin towards the 'Edit Claim Issuance Policy...' option in the context menu.

anysearch.local - Remote Desktop Connection

Server Manager

Server |

- Dashboard
- Local Server
- All Servers
- AD DS
- AD FS**
- DNS
- File and Storage Services
- IIS

AD FS

Add Transform Claim Rule Wizard

Select Rule Template

Steps

Choose Rule Type

Claim rule template:

Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

< Previous Next > Cancel

Add Rule... Edit Rule... Remove Rule...

OK Cancel Apply

Actions

Relying Party Trusts

- Add Relying Party Trust...
- View
- New Window from Here
- Refresh
- Help

win10.local

- Update from Federation Metadata...
- Edit Access Control Policy...
- Edit Claim Issuance Policy...
- Disable
- Properties
- Delete
- Help

TASKS

Type here to search

4:59 PM 10/28/2024

The screenshot shows the 'Add Transform Claim Rule Wizard' window in the Windows Server Manager. A large red arrow points to the 'Choose Rule Type' step in the 'Steps' list. The 'Send LDAP Attributes as Claims' template is selected in the 'Claim rule template:' dropdown. A detailed description of this template is provided in the 'Claim rule template description:' section. At the bottom of the wizard window, there are buttons for '< Previous', 'Next >', and 'Cancel'. Below these are buttons for 'Add Rule...', 'Edit Rule...', and 'Remove Rule...'. At the very bottom are 'OK', 'Cancel', and 'Apply' buttons. To the right of the wizard window, the 'Actions' pane is open, showing options for 'Relying Party Trusts' and a specific entry for 'win10.local'. The 'win10.local' entry has several actions listed: 'Update from Federation Metadata...', 'Edit Access Control Policy...', 'Edit Claim Issuance Policy...', 'Disable', 'Properties', 'Delete', and 'Help'. The 'Delete' option has a red 'X' icon next to it. The overall interface is typical of Windows Server management tools.

anysearch.local - Remote Desktop Connection

Server Manager

File Action View Window Help

AD FS

Dashboard Local Server All Servers AD DS AD FS DNS File and Storage S IIS

Relying Party Trusts

Display Name	Enabled	Type	Identifier
win10.local	Yes	WS Tr...	win10.local

Actions

Relying Party Trusts

- Add Relying Party Trust...
- View
- New Window from Here
- Refresh
- Help

win10.local

- Update from Federation Metadata...
- Edit Access Control Policy...
- Edit Claim Issuance Policy...
- Disable
- Properties
- Delete
- Help

File Action View Window Help

AD FS

Service

- Attribute Stores
- Authen...
- Certifica...
- Claim D...
- Device F...
- Endpoint...

Relying Party Trusts

Claim Rule Name: User

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
User-Principal-Name	UPN
Display-Name	Name
E-Mail-Addresses	E-Mail Address
Token-Groups - Unqualified Names	Group

View Rule Language... OK Cancel

4:59 PM 10/28/2024

7

Go Back AnySearch Setup

AnySearch | Your personal LLM

Not secure https://win10.local/settings/system-preferences

KT

INSTANCE SETTINGS

- AI Providers
- Admin
  - Users
  - Workspaces
  - Workspace Chats
- Invites
- General Settings
- Agent Skills
- Customization
- Tools

Contact Support

Privacy & Data

Set up Single Sign-On (SSO) with Active Directory Federation Services (ADFS) on SAML 2.0.

You have to complete three steps one by one for ADFS SSO system setup.

Step 1: Generate Configuration File, please provide the endpoint path of ADFS on SAML 2.0, and the system would generate SSO configuration file.  
Step 2: Validate ADFS SSO, your system administrator should upload the file generated and set up the ADFS accordingly.  
Step 3: Convert the system to SSO. Remember that once changed to SSO, it is non reversible.

ADFS SAML Endpoint Path  
`https://anysearch.local/adfs/ls/`

ADFS SAML Issuer  
(e.g. anysearch.local)  
`win10.local`

Callback Host with Port  
(e.g. `https://currentsite.local:3001`)  
`https://win10.local:3001/`

Download and Config at ADFS

Config is validated

If you see this green message, then good to proceed

System preferences updated successfully for single sign-on.

Convert to SSO

4:59 PM 11/8/2024

Type here to search

kt-chan/anysearch at 0.0.1 AnyZearch | Your personal LLM https://win10.local/settings/system-preferences Not secure Apps 百度 Google W3 W3 Meeting iHR 智谱清言 讯飞星火 Kimi.ai Copilot 存储营销装备库 术语库 ChatGPT Pangu-s AnyZearch Work demo Course KT

You have to complete three steps one by one for ADFS SSO system setup.

Step 1: Generate Configuration File, please provide the endpoint path of ADFS on SAML 2.0, and the system would generate SSO configuration file.  
Step 2: Validate ADFS SSO, your system administrator should upload the file generated and set up the ADFS accordingly.  
Step 3: Convert the system to SSO. Remember that once changed to SSO, it is non reversible.

AI Providers

Admin

- Users
- Workspaces
- Workspace Chats
- Invites

General Settings

Agent Skills

Customization

Tools

Contact Support

Privacy & Data

ADFS SAML Endpoint Path  
`https://anysearch.local/adfs/ls/`

ADFS SAML Issuer  
(e.g. anysearch.local)  
`win10.local`

Callback Host with Port  
(e.g. `https://currentsite.local:3001`)  
`https://win10.local:3001/`

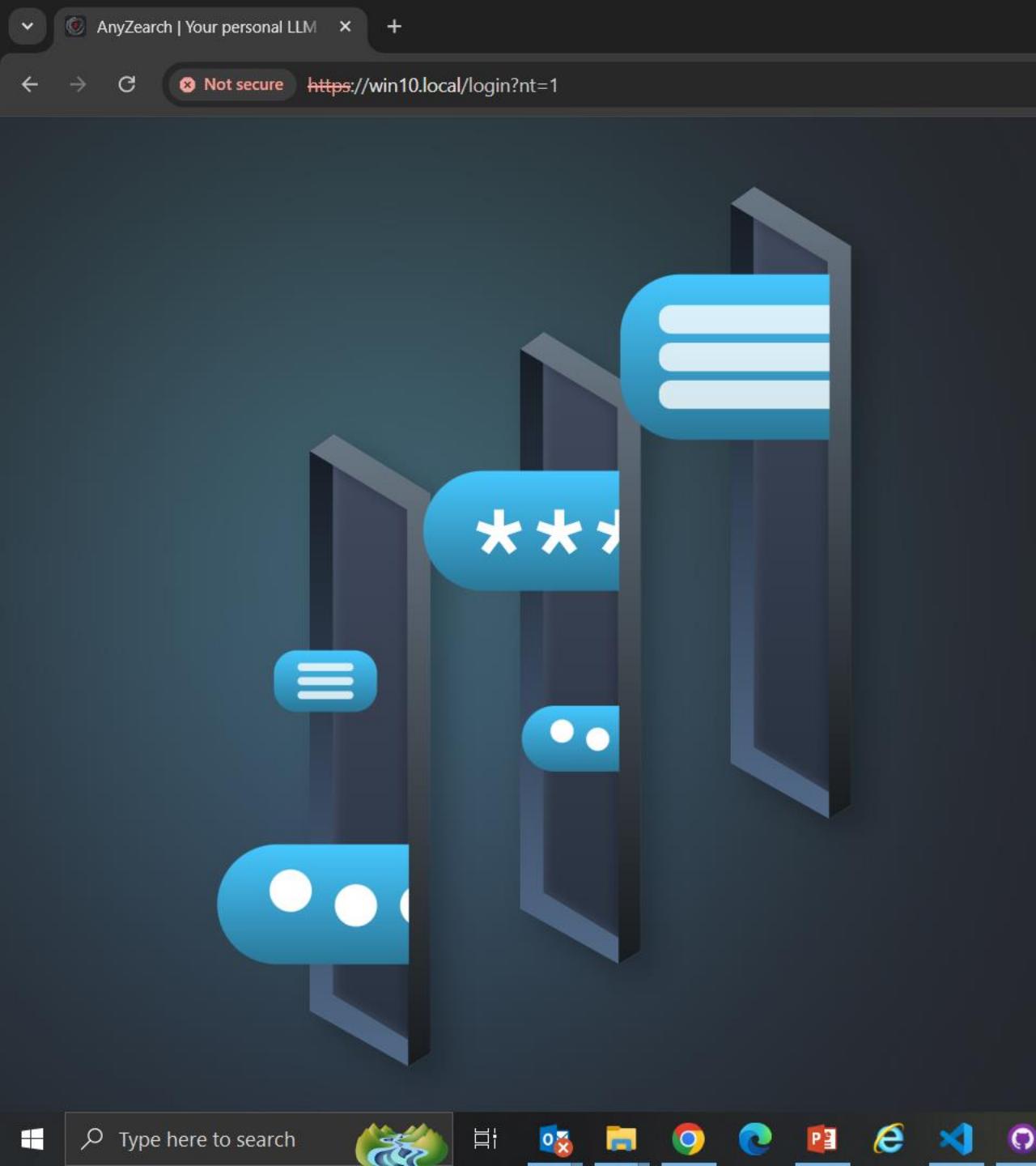
Download and Config at ADFS

Config is validated

Config is generated Config is validated Converted to SSO

Account Support Sign out

5:00 PM 11/8/2024 ENG



AnySearch | Your personal LLM

+

-

□

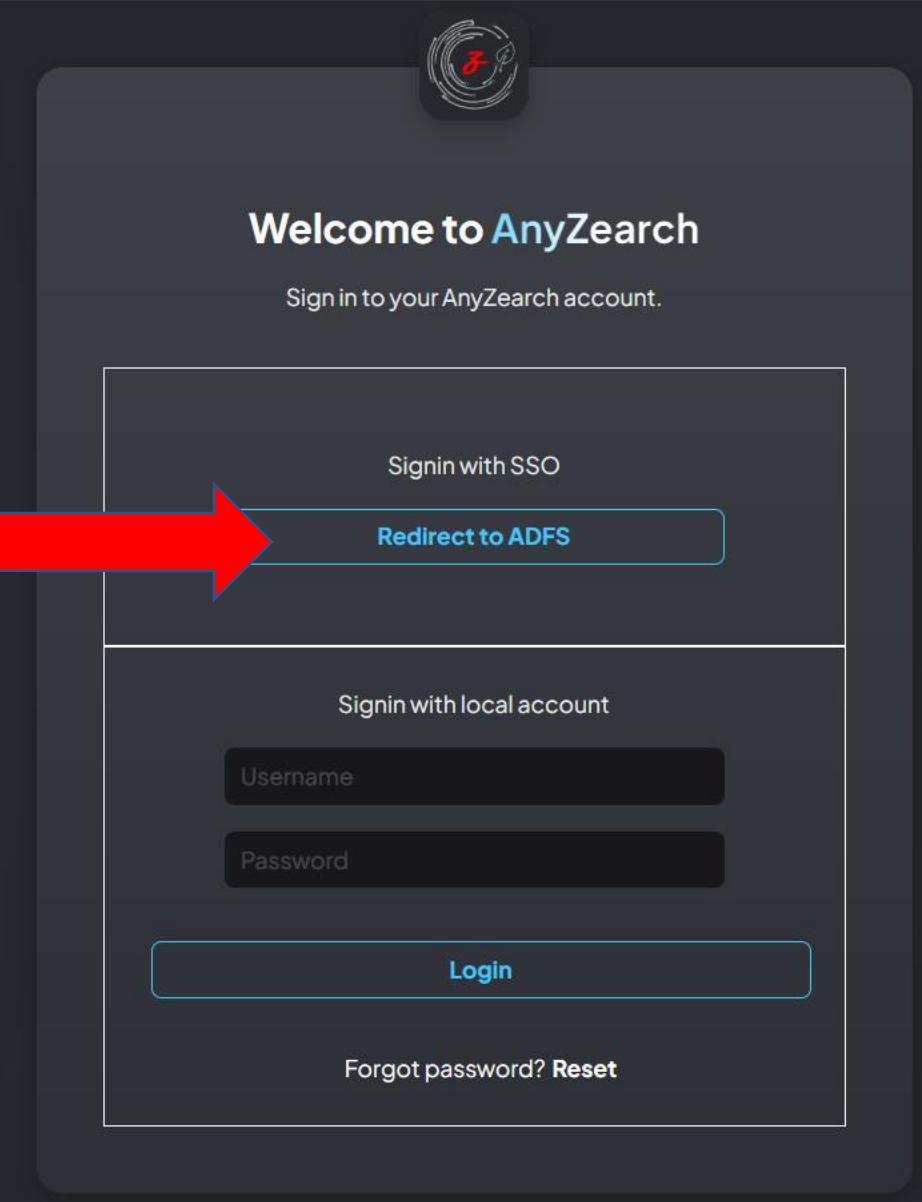
X

< > C

Not secure

https://win10.local/login?nt=1

☆ ⌂ ⌂ ⌂ ⌂



Welcome to AnySearch

Sign in to your AnySearch account.

Signin with SSO

**Redirect to ADFS**

Signin with local account

Username

Password

Login

Forgot password? [Reset](#)

A large red arrow points from the "Redirect to ADFS" button on the login page to the "Redirect to ADFS" link on the desktop icon.

Windows icon

Type here to search

AnySearch icon

File

Folder

Google Chrome

Microsoft Edge

PowerPoint

Excel

OneNote

Word

Teams

Photoshop

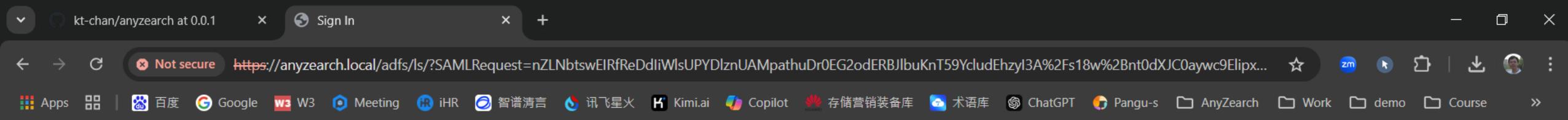
File Explorer

Google Chrome

5:00 PM  
11/8/2024

ENG

9



anysearch.local

Sign in

ANYSEARCH\demoadmin

.....

Sign in

© 2018 Microsoft



Type here to search



5:01 PM  
11/8/2024

AnySearch | Your personal LLM × Error

Not secure https://win10.local

Apps | 百度 Google W3 W3 Meeting iHR 智谱清言 讯飞星火 Kimi.ai Copilot 存储营销装备库 术语库 ChatGPT Pangu-s AnySearch Work demo Course

AnySearch

+ New Workspace

Welcome to AnySearch, AnySearch is an open-source AI tool by iteasoft labs that turns anything into a trained chatbot you can query and chat with.

AnySearch is the easiest way to put powerful AI products like OpenAi, GPT-4, LangChain, PineconeDB, ChromaDB, and other services together in a neat package with no fuss to increase your productivity by 100x.

AnySearch can run totally locally on your machine with little overhead you wont even notice it's there! No GPU needed. Cloud and on-premises installation is available as well.  
The AI tooling ecosystem gets more powerful everyday. AnySearch makes it easy to use.

How do I get started?!

It's simple. All collections are organized into buckets we call "Workspaces". Workspaces are buckets of files, documents, images, PDFs, and other files which will be transformed into something LLM's can understand and use in conversation.  
You can add and remove files at anytime.

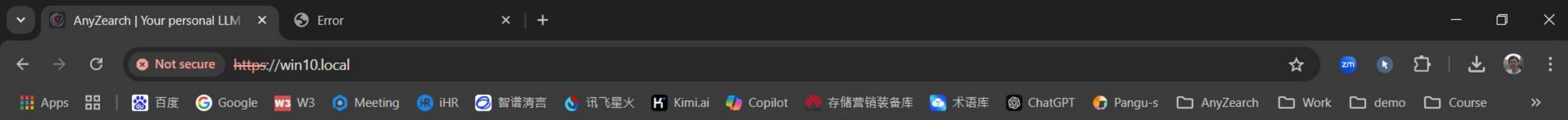
+ Create your first workspace

Is this like an AI dropbox or something? What about chatting? It is a chatbot isn't it?

DE

Type here to search

5:04 PM 11/8/2024



## Edit Account



Profile Picture  
800x800

Username

demoadmin@anysearch.local

New Password

demoadmin@anysearch.local's new password

Preferred language

English ▾

Cancel

Update Account



Type here to search



5:04 PM  
11/8/2024

