Azure AD with Integrated Windows Authentication using a Kerberos Constrained Delegation with Qlik Sense

Daniel Pilla, Senior Enterprise Architect

June 19, 2018

Contents

About 3

Assumptions 3

Setup SPN 3

Install Azure AD Connect 6

Install Azure Application Proxy 12

Setup an Enterprise Application 12

Setup the Qlik Sense Proxy 15

Accessing Qlik Sense 17

About

This document describes how to setup authentication with Qlik Sense using Azure AD with Integrated Windows Authentication via a Kerberos Constrained Delegation. You can find detailed information on the subject here: https://community.qlik.com/docs/DOC-19942.

Assumptions

All names in the setup are example names. Make sure to use your company standards.

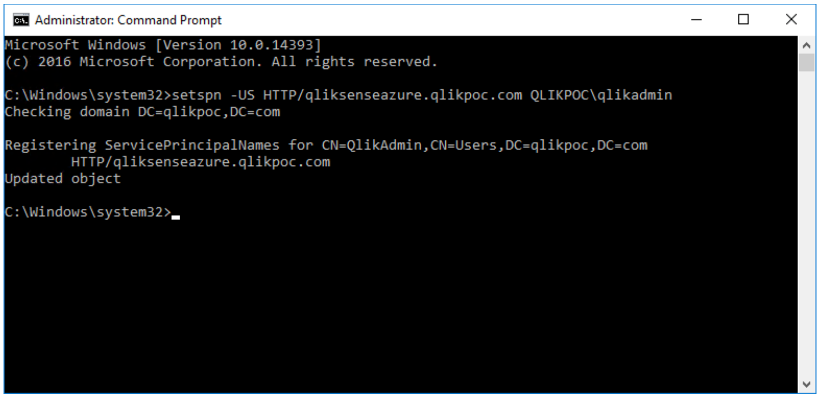
This document assumes the following has been configured, and is only meant to be used as an example. All of these components are not necessarily necessary, and your configuration will vary.

- Single server environment
- Active Directory installed
- Qlik Sense April 2018+ (port 4244 no longer necessary), installed as a domain & machine admin
- A purchased domain name
- A third-party certificate for the above domain, installed on the server and leveraged in the Qlik Sense proxy
- An Azure account with a license/trial of the associated Azure services used throughout this document

Setup SPN

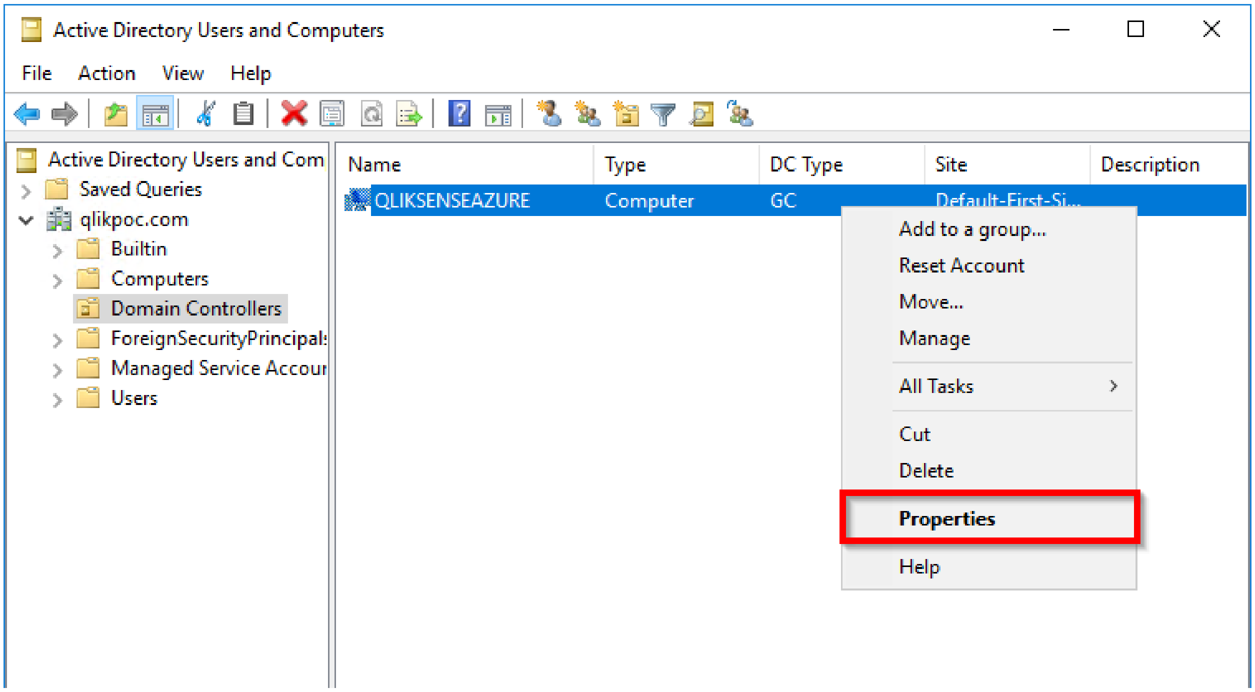
1. Open a command prompt with administrative privileges.
2. Enter in the following command with your FQDN and user that runs the Qlik services. Note the the '-US' parameter. The 'U' indicates that this is a *user* and the *S* ensures that it will check for duplicates (if there are duplicates, it will not work):

   setspn -US HTTP/qliksenseazure.qlikpoc.com QLIKPOC\qlikadmin
3. For more information, see: https://social.technet.microsoft.com/wiki/contents/articles/717.service-principal-names-spns-setspn-syntax-setspn-exe.aspx



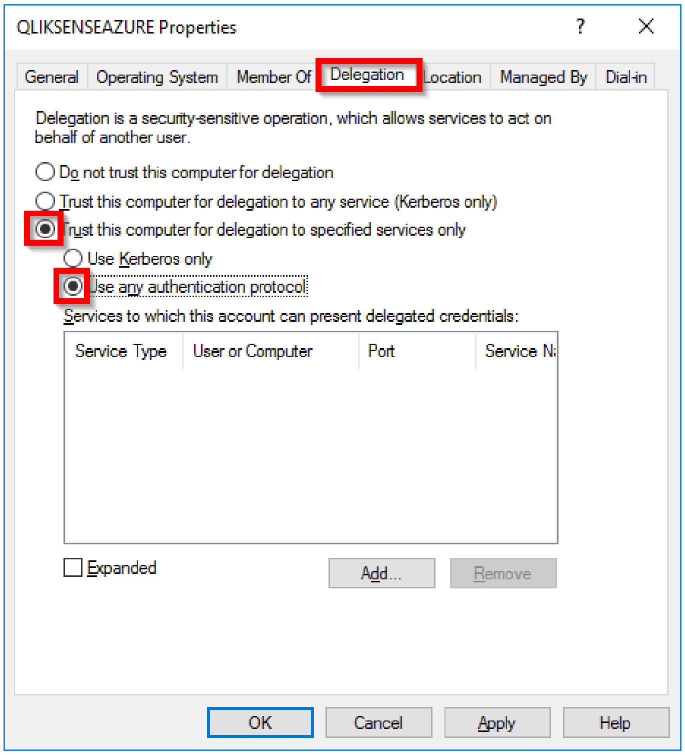
```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>setspn -US HTTP/qliksenseazure.qlikpoc.com QLIKPOC\qlikadmin
Checking domain DC=qlikpoc,DC=com

Registering ServicePrincipalNames for CN=QlikAdmin,CN=Users,DC=qlikpoc,DC=com
        HTTP/qliksenseazure.qlikpoc.com
Updated object

C:\Windows\system32>
```

4. Navigate to ***Active Directory Users and Computers*** and select your target machine. In this case, since this is a single server proof-of-concept, my machine is also the ***Domain*** Controller. Right-click on the machine and select ***Properties***.



Name	Type	DC Type	Site	Description
QLIKSENSEAZURE	Computer	GC	Default-First-Si...	

5. Select the ***Delegation*** tab, and then select ***Trust this computer for delegation to specified services only***, followed by ***Use any authentication protocol***.



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this computer for delegation

○ Trust this computer for delegation to any service (Kerberos only)

● Trust this computer for delegation to specified services only

○ Use Kerberos only

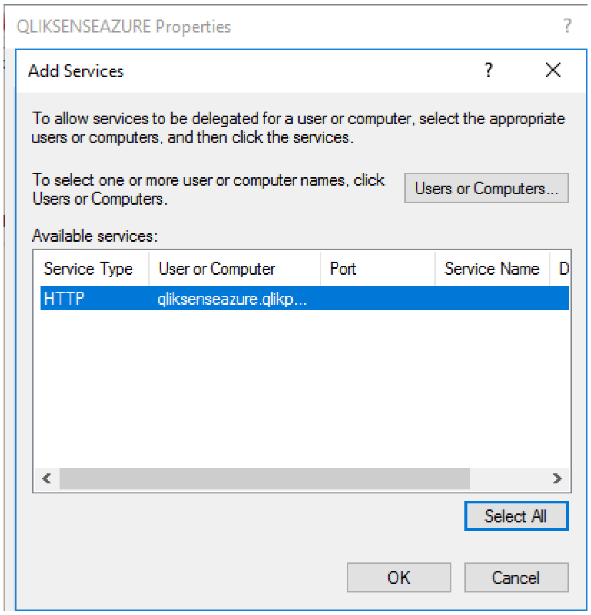
● Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N:

□ Expanded

6. Select ***Add…*** and then select ***Users or Computers…*** -- there, search for your user that runs the Qlik services, and ensure you select ***Select All*** after the fact.



QLIKSENSEAZURE Properties

Add Services

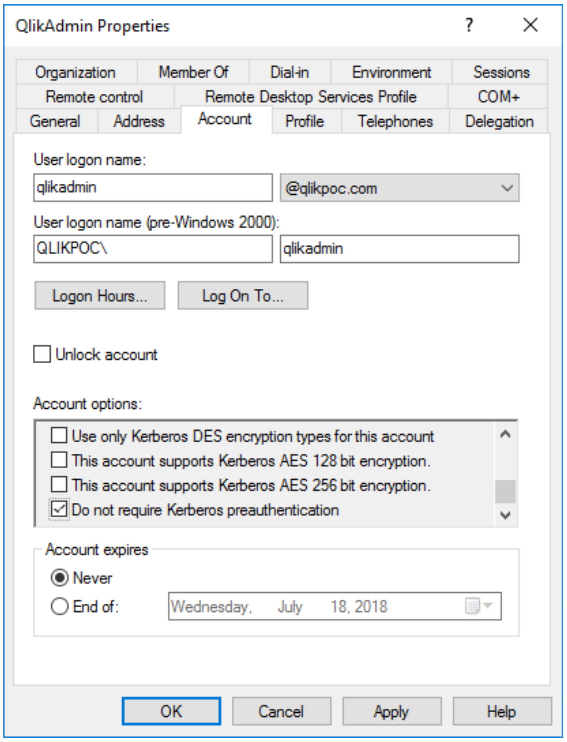
To allow services to be delegated for a user or computer, select the appropriate users or computers, and then click the services.

To select one or more user or computer names, click Users or Computers.

Available services:

Service Type	User or Computer	Port	Service Name	D
HTTP	qliksenseazure.qlikp...			

7. Back under ***Active Directory Users and Computers***, click on ***Users*** and navigate to your user that runs the Qlik services. Right click on that user and select ***Properties***. Click on the ***Account*** tab, and select ***Do not require Kerberos preauthentication*** under the ***Account options*** section. Click ***Apply***.



QlikAdmin Properties

User logon name: qlikadmin @qlikpoc.com

User logon name (pre-Windows 2000): QLIKPOC\ qlikadmin

☐ Unlock account

Account options:

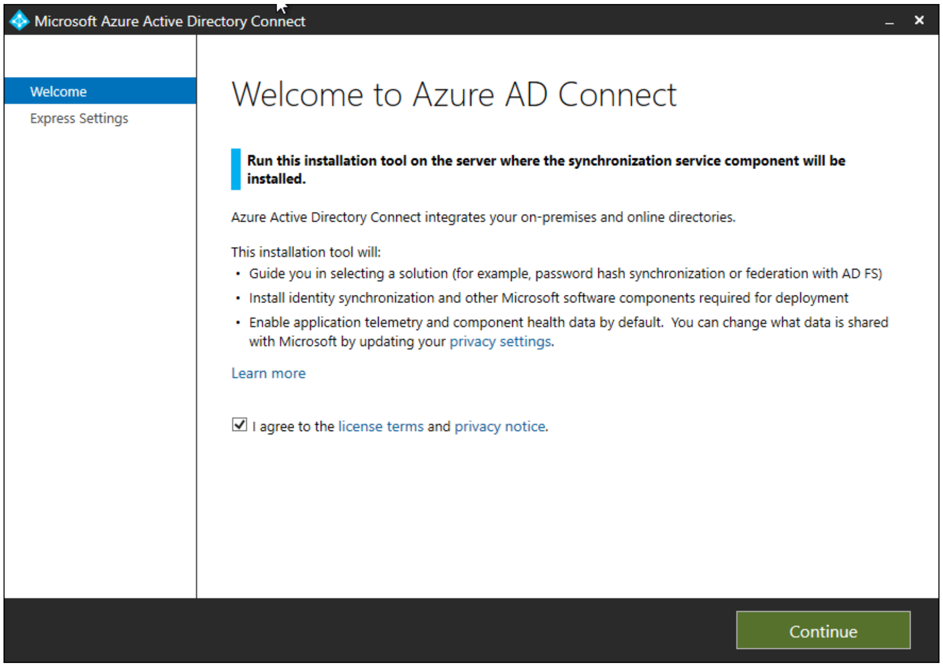
☐ Use only Kerberos DES encryption types for this account
☐ This account supports Kerberos AES 128 bit encryption.
☐ This account supports Kerberos AES 256 bit encryption.
☑ Do not require Kerberos preauthentication

Account expires

● Never
○ End of: Wednesday, July 18, 2018

Install Azure AD Connect

1. Download Azure AD Connect: https://www.microsoft.com/en-us/download/details.aspx?id=47594
2. Execute the installer and click through the initial prompts until you reach ***Welcome to Azure AD Connect***. After reading through the license terms and privacy notes, click ***I agree*** and click ***Continue***.



Welcome to Azure AD Connect

Run this installation tool on the server where the synchronization service component will be installed.

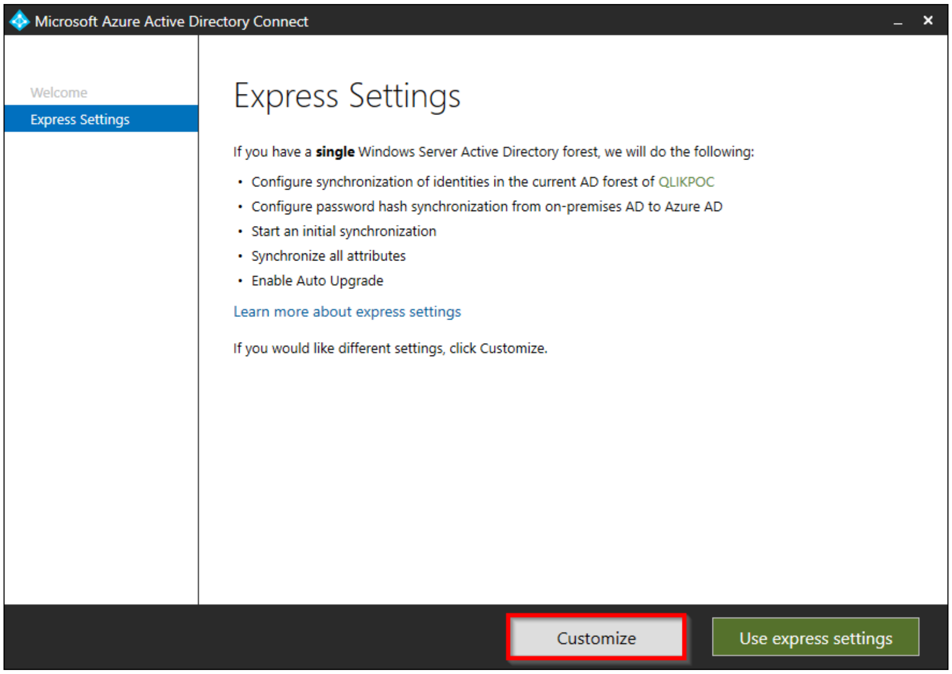
Azure Active Directory Connect integrates your on-premises and online directories.

This installation tool will:
- Guide you in selecting a solution (for example, password hash synchronization or federation with AD FS)
- Install identity synchronization and other Microsoft software components required for deployment
- Enable application telemetry and component health data by default. You can change what data is shared with Microsoft by updating your privacy settings.

Learn more

☑ I agree to the license terms and privacy notice.

3. Select ***customize***.



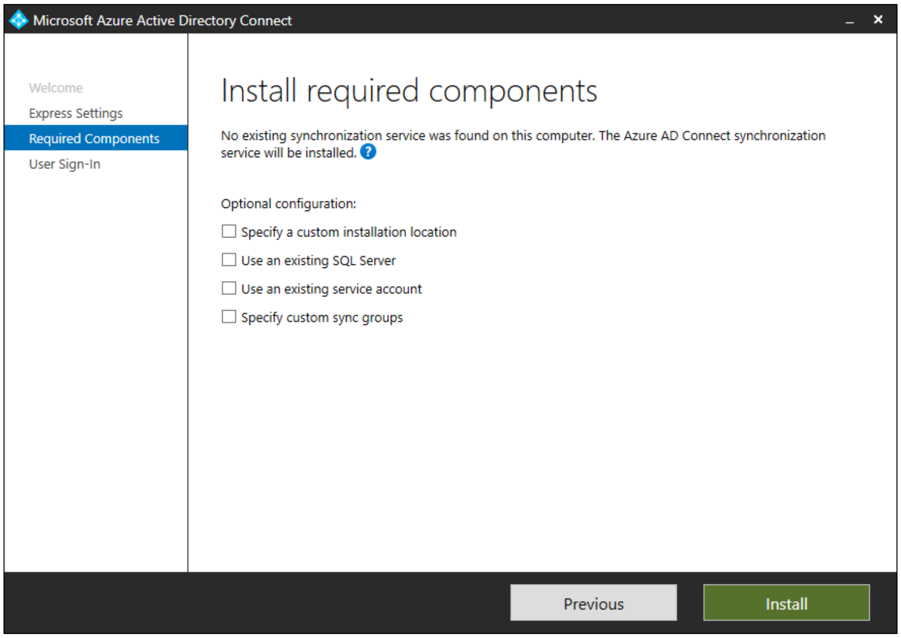
Express Settings

If you have a **single** Windows Server Active Directory forest, we will do the following:
- Configure synchronization of identities in the current AD forest of QLIKPOC
- Configure password hash synchronization from on-premises AD to Azure AD
- Start an initial synchronization
- Synchronize all attributes
- Enable Auto Upgrade

Learn more about express settings

If you would like different settings, click Customize.

4. Do not select any of the optional components and select ***Install***



Microsoft Azure Active Directory Connect

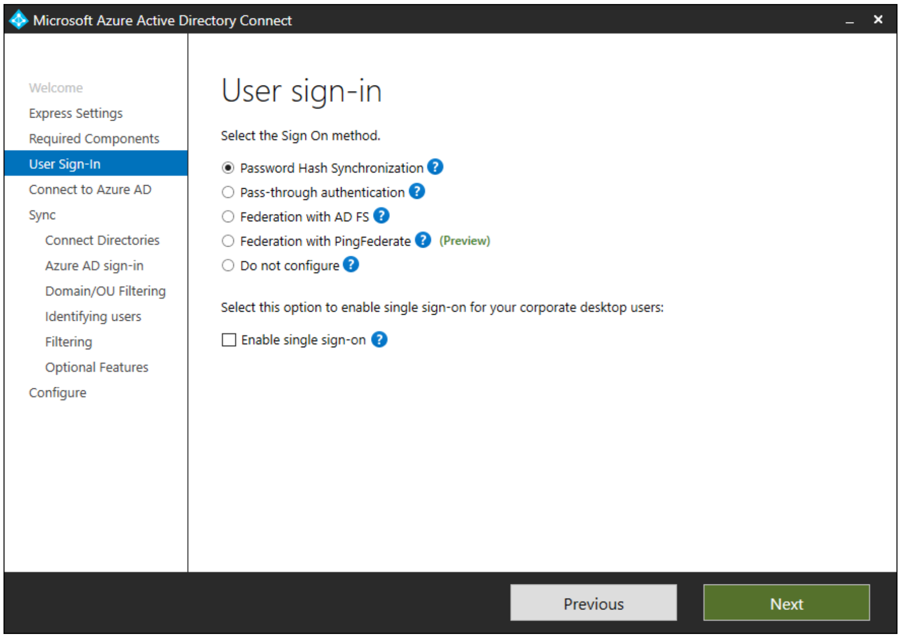
Install required components

No existing synchronization service was found on this computer. The Azure AD Connect synchronization service will be installed.

Optional configuration:

- □ Specify a custom installation location
- □ Use an existing SQL Server
- □ Use an existing service account
- □ Specify custom sync groups

5. Leave the default selection and select ***Next***.



Microsoft Azure Active Directory Connect

User sign-in

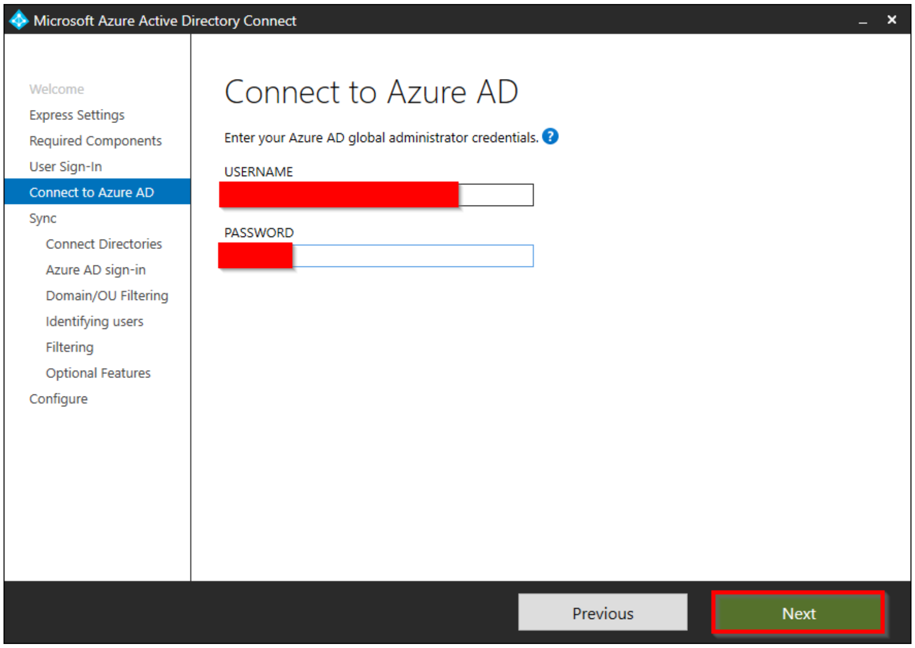
Select the Sign On method.

- ● Password Hash Synchronization
- ○ Pass-through authentication
- ○ Federation with AD FS
- ○ Federation with PingFederate (Preview)
- ○ Do not configure

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

- □ Enable single sign-on

6. Enter in your username and password for your Azure AD global administrator and select ***Next***.



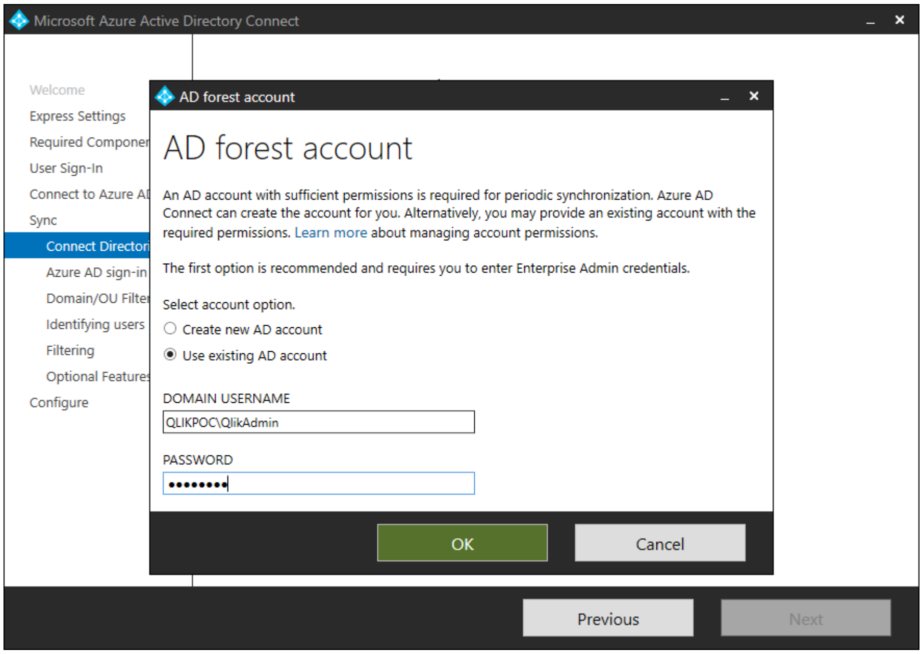
Connect to Azure AD

Enter your Azure AD global administrator credentials.

USERNAME [redacted]

PASSWORD [redacted]

7. Select ***Add Directory*** and either create a new account or select an account with administrative credentials to AD.



AD forest account

An AD account with sufficient permissions is required for periodic synchronization. Azure AD Connect can create the account for you. Alternatively, you may provide an existing account with the required permissions. Learn more about managing account permissions.

The first option is recommended and requires you to enter Enterprise Admin credentials.

Select account option.

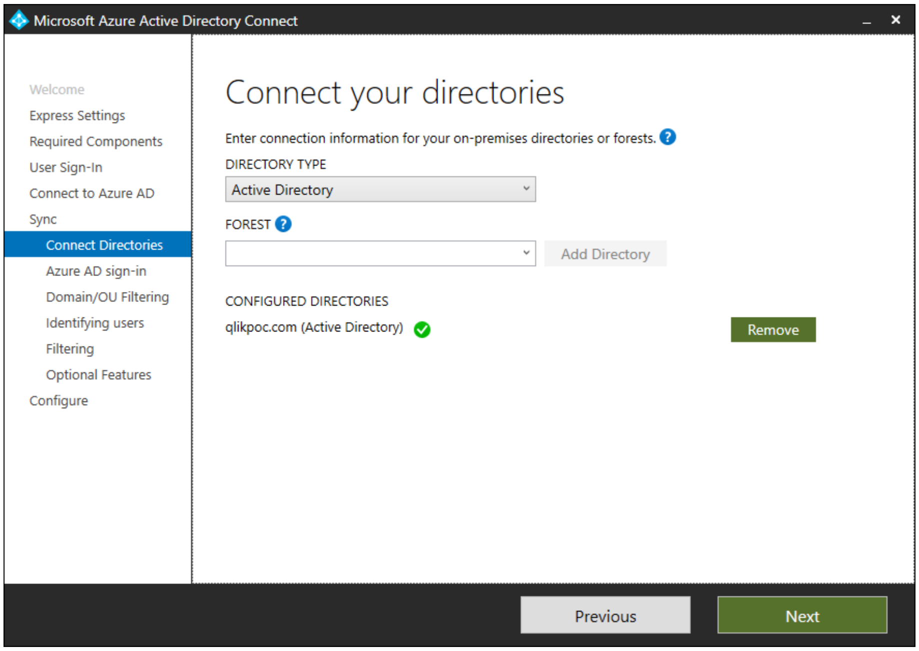
○ Create new AD account

● Use existing AD account

DOMAIN USERNAME: QLIKPOC\QlikAdmin

PASSWORD: ••••••••

8. Once added, you should see a green check, and select ***Next***.



Microsoft Azure Active Directory Connect

Connect your directories

Enter connection information for your on-premises directories or forests.

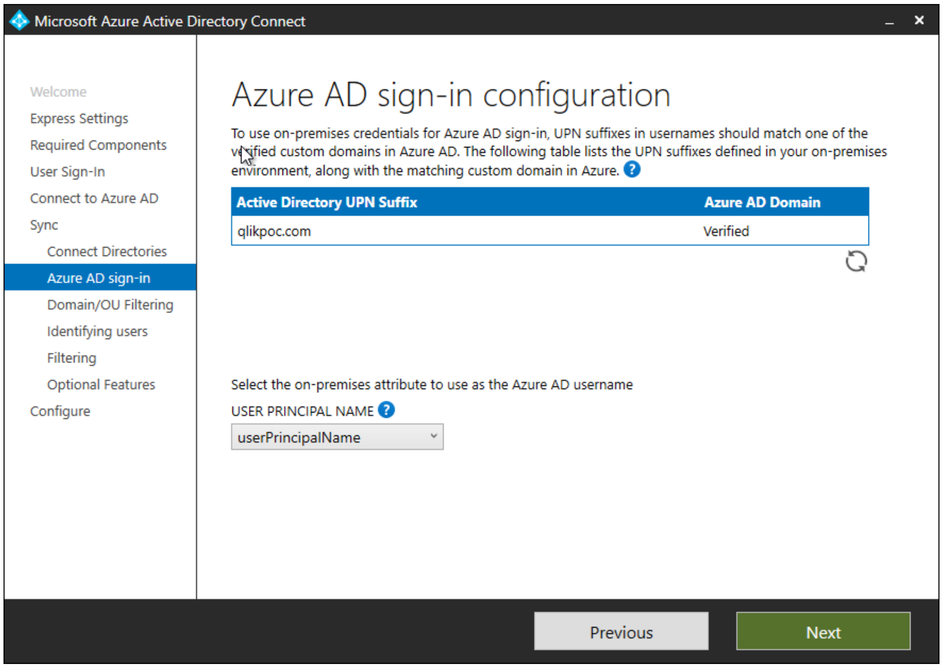
DIRECTORY TYPE: Active Directory

FOREST

CONFIGURED DIRECTORIES

qlikpoc.com (Active Directory) ✓

9. In this case, I have already mapped the qlikpoc.com domain to Azure AD so it has come up as *Verified*. I have also chosen to select ***userPrincipalName*** for the on-premises attribute to use as the Azure AD username.



Microsoft Azure Active Directory Connect

Azure AD sign-in configuration

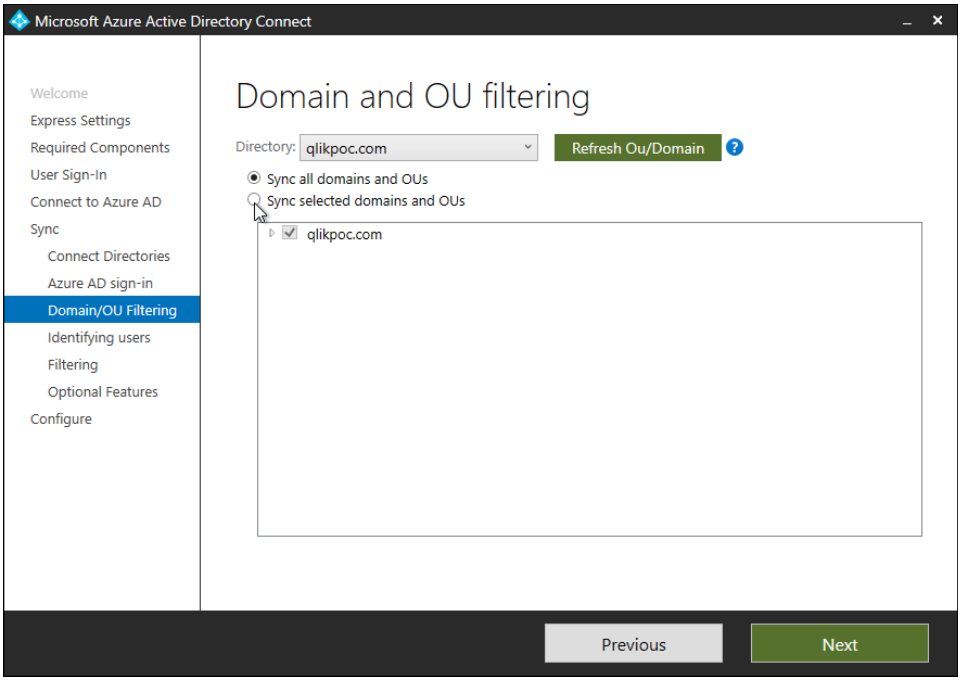
To use on-premises credentials for Azure AD sign-in, UPN suffixes in usernames should match one of the verified custom domains in Azure AD. The following table lists the UPN suffixes defined in your on-premises environment, along with the matching custom domain in Azure.

Active Directory UPN Suffix	Azure AD Domain
qlikpoc.com	Verified

Select the on-premises attribute to use as the Azure AD username

USER PRINCIPAL NAME: userPrincipalName

10. I’ve chosen to sync all domains and OUs – select ***Next***.



Domain and OU filtering

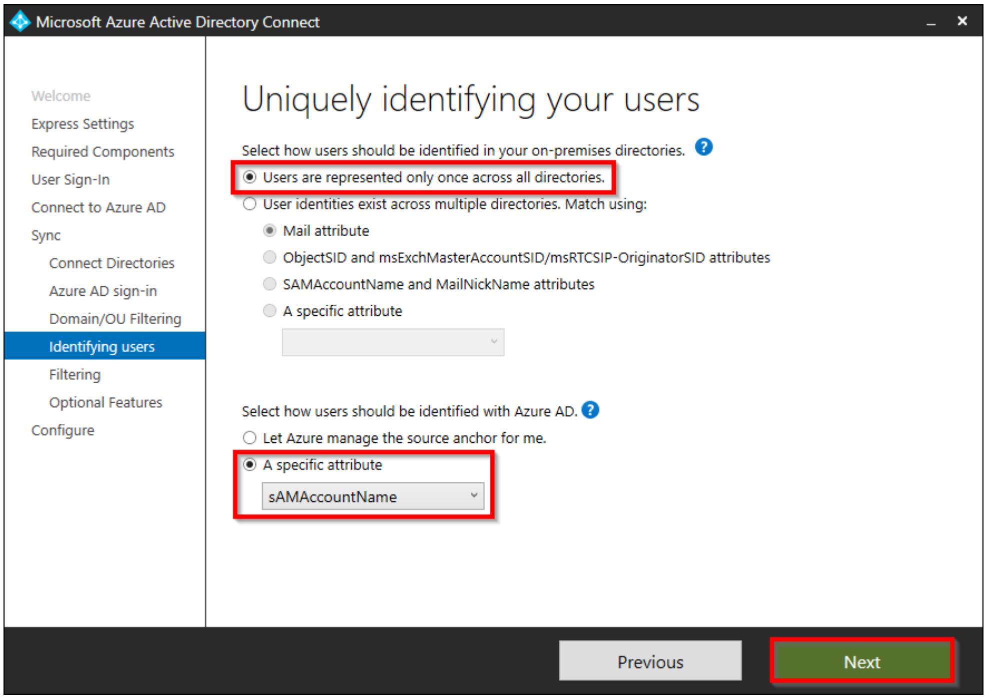
Directory: qlikpoc.com

● Sync all domains and OUs

○ Sync selected domains and OUs

☑ qlikpoc.com

11. I’ve chosen to identify users within Azure AD by ***sAMAccountName***. Select ***Next***.



Uniquely identifying your users

Select how users should be identified in your on-premises directories.

● Users are represented only once across all directories.

○ User identities exist across multiple directories. Match using:

● Mail attribute

○ ObjectSID and msExchMasterAccountSID/msRTCSIP-OriginatorSID attributes

○ SAMAccountName and MailNickName attributes

○ A specific attribute

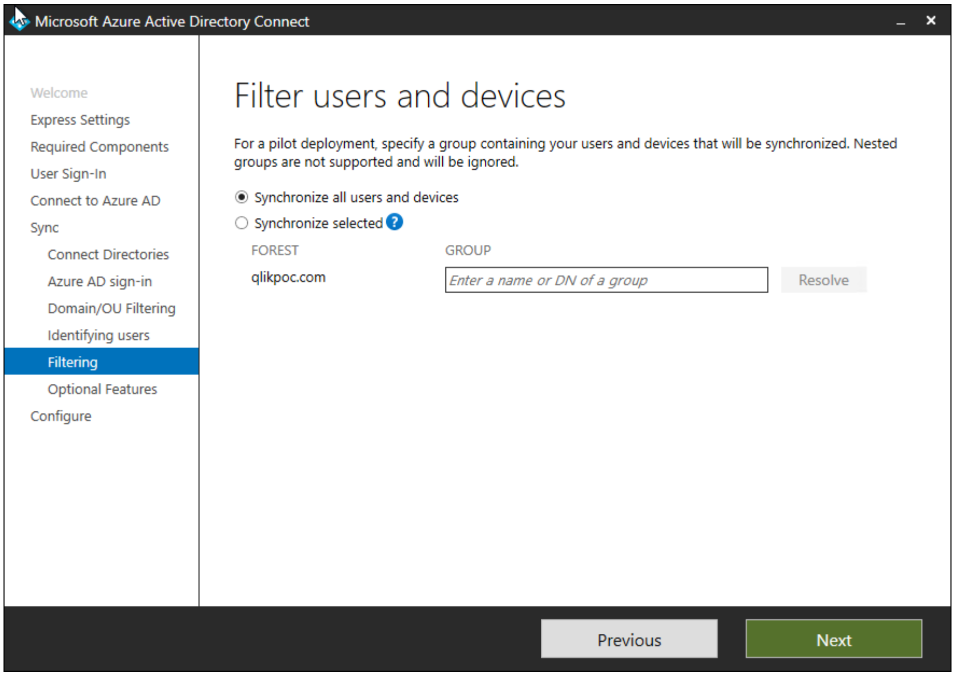
Select how users should be identified with Azure AD.

○ Let Azure manage the source anchor for me.

● A specific attribute

sAMAccountName

12. In this case I've chosen to synchronize all users and devices. Select ***Next***.



Filter users and devices

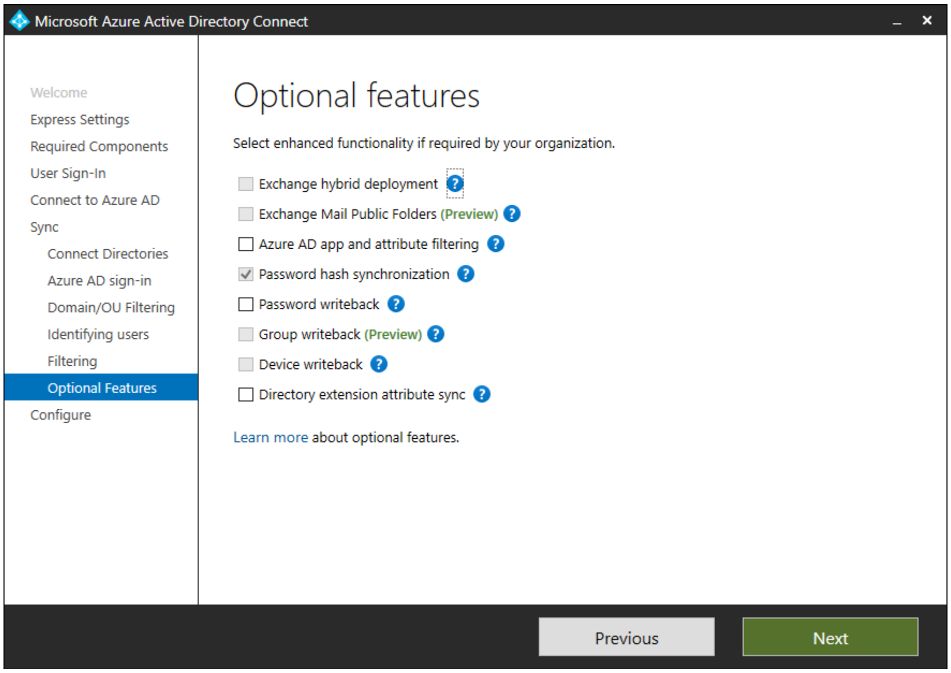
For a pilot deployment, specify a group containing your users and devices that will be synchronized. Nested groups are not supported and will be ignored.

● Synchronize all users and devices

○ Synchronize selected

FOREST	GROUP
qlikpoc.com	Enter a name or DN of a group

13. Leave the default settings and select ***Next***.



Optional features

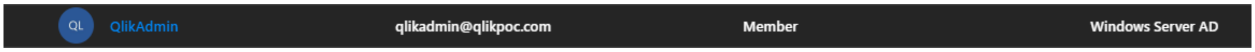
Select enhanced functionality if required by your organization.

- □ Exchange hybrid deployment
- □ Exchange Mail Public Folders (Preview)
- □ Azure AD app and attribute filtering
- ☑ Password hash synchronization
- □ Password writeback
- □ Group writeback (Preview)
- □ Device writeback
- □ Directory extension attribute sync

Learn more about optional features.

14. Leave the default selections and select ***Install***.

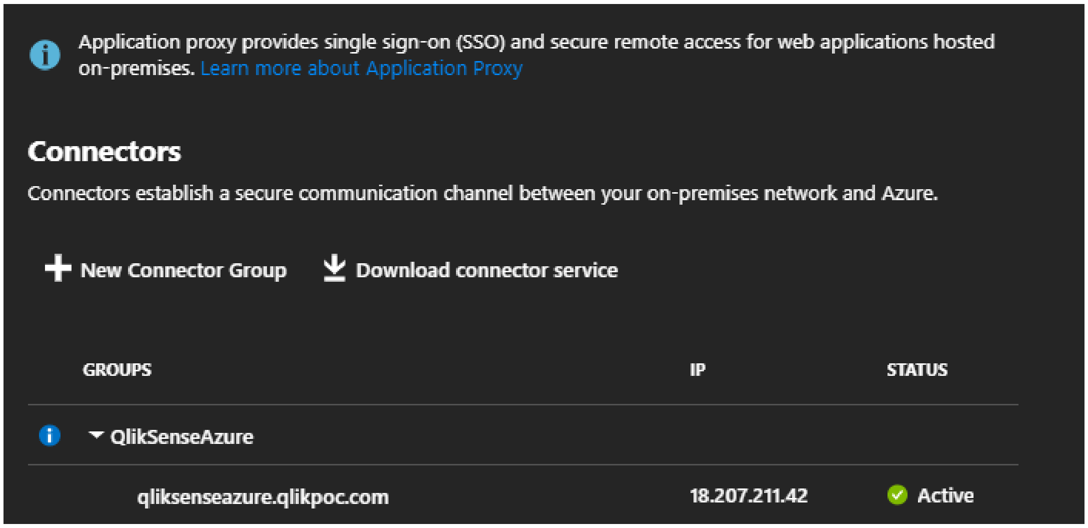
15. Navigate to the ***Azure Portal*** and confirm that your user(s) have been synchronized successfully.



QL QlikAdmin	qlikadmin@qlikpoc.com	Member	Windows Server AD

Install Azure Application Proxy

1. Within the Azure Portal, navigate to ***Azure Active Directory***. Select ***Application proxy***, and then select ***Download connector service***. Download the connector to the target server.
2. Install the connector. You will need to sign into Azure as a part of the installation as a global administrator.
3. Back in the Azure Portal, you should now see your new connector. I've created a new ***Connector Group*** and added the connector to it.



Application proxy provides single sign-on (SSO) and secure remote access for web applications hosted on-premises. Learn more about Application Proxy

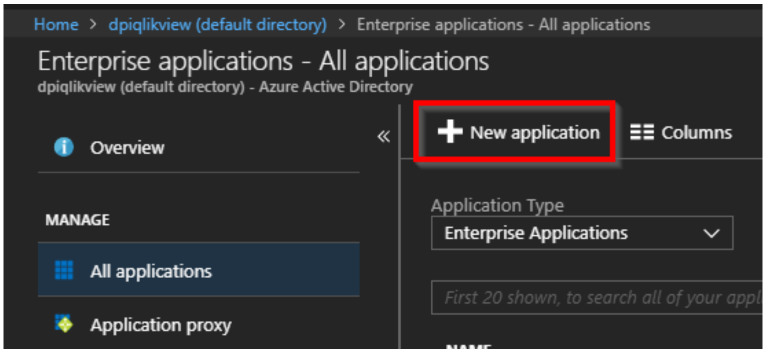
Connectors

Connectors establish a secure communication channel between your on-premises network and Azure.

GROUPS	IP	STATUS
QlikSenseAzure		
qliksenseazure.qlikpoc.com	18.207.211.42	✓ Active

Setup an Enterprise Application

1. In the Azure Portal, select ***Azure Active Directory***, then select ***Enterprise Applications***, and finally ***New application***.



Home > dpiqlikview (default directory) > Enterprise applications - All applications

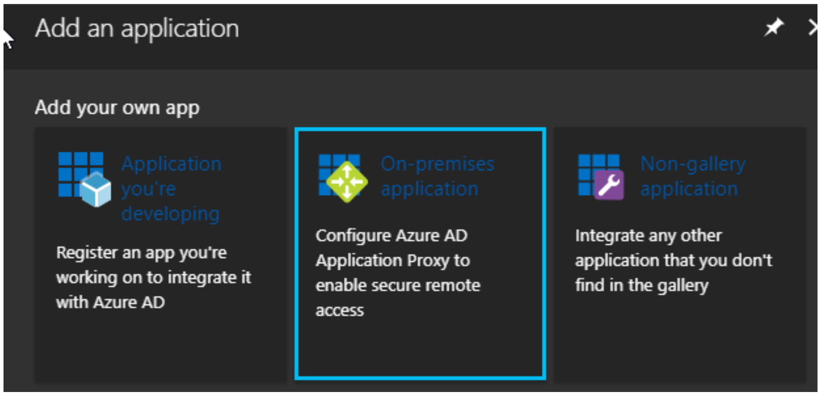
Enterprise applications - All applications

dpiqlikview (default directory) - Azure Active Directory

Application Type: Enterprise Applications

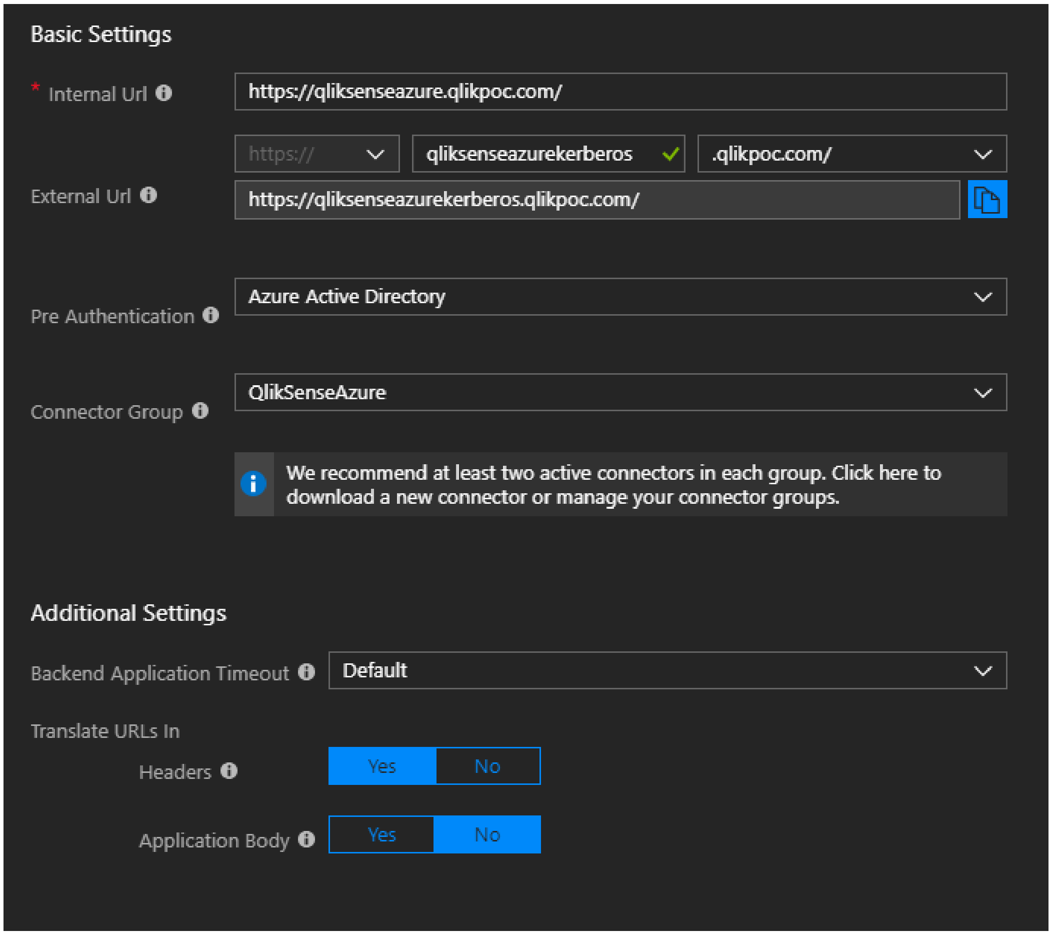
First 20 shown, to search all of your appl

2. Select ***On-premises application***.



Add an application
Add your own app
Application you're developing
Register an app you're working on to integrate it with Azure AD
On-premises application
Configure Azure AD Application Proxy to enable secure remote access
Non-gallery application
Integrate any other application that you don't find in the gallery

3. Fill out the application as follows:
   a. ***Name:*** This is an arbitrary name for the ***Enterprise application*** itself
      i. *QlikSenseAzureKerberos*
   b. ***Internal Url:*** this is the url that you would use on the Qlik Sense machine itself to access it.
      i. *https://qliksenseazure.qlikpoc.com/*
   c. ***External Url:*** In the next component, you are setting up the public url. I've set it to my custom domain, but by default, you would get a *.msappproxy.net/* url.
      i. *https://qliksenseazurekerberos.qlikpoc.com*
   d. ***Pre Authentication***
      i. *Azure Active Directory*
   e. ***Connector Group:*** This will either be the default, or the group you've created for the connector.
      i. *QlikSenseAzure*
   f. The additional settings can remain the default.



Basic Settings

* Internal Url: https://qliksenseazure.qlikpoc.com/

External Url: https:// | qliksenseazurekerberos ✓ | .qlikpoc.com/

https://qliksenseazurekerberos.qlikpoc.com/

Pre Authentication: Azure Active Directory

Connector Group: QlikSenseAzure

We recommend at least two active connectors in each group. Click here to download a new connector or manage your connector groups.

Additional Settings

Backend Application Timeout: Default

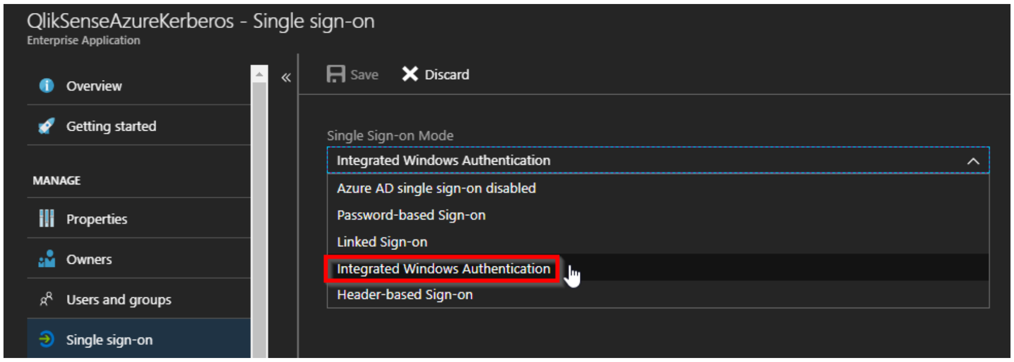
Translate URLs In

Headers: [✓ Yes] No

Application Body: Yes [✓ No]

4. **Note that I am also using a certificate for **.qlikpoc.com* and have set the Qlik Sense ***Proxy*** to use that certificate, and have imported it into the ***Azure Application Proxy***. This guide does not cover the use of third-party certificates.
5. Select ***Add***

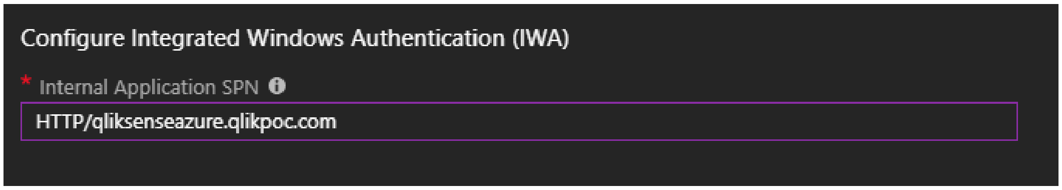
6. Navigate to the new ***Enterprise App*** and select ***Single sign-on***.
7. Under ***Single Sign-on Mode***, select ***Integrated Windows Authentication***.



Single Sign-on Mode: Integrated Windows Authentication

- Azure AD single sign-on disabled
- Password-based Sign-on
- Linked Sign-on
- Integrated Windows Authentication
- Header-based Sign-on

8. Under ***Internal Application SPN***, enter the associated SPN. In this example, it is: *HTTP/qliksenseazure.qlikpoc.com*

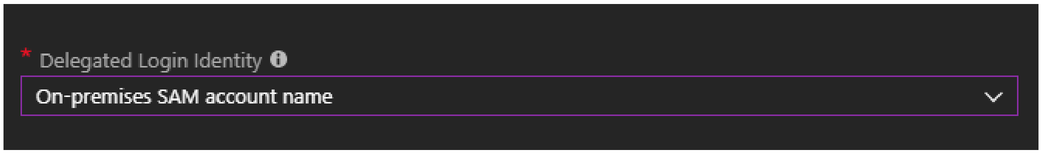


Configure Integrated Windows Authentication (IWA)

* Internal Application SPN

HTTP/qliksenseazure.qlikpoc.com

9. Under ***Delegated Login Identity***, I've selected *On-premises SAM account name*.

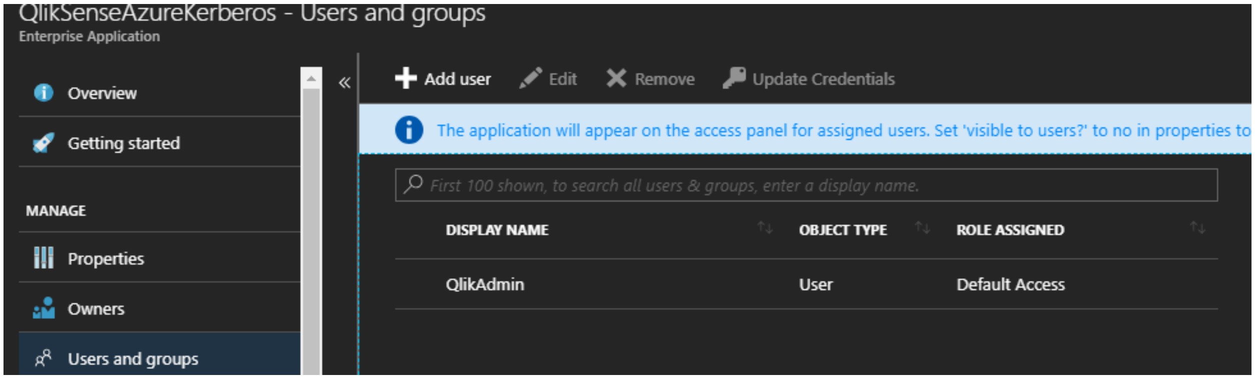


* Delegated Login Identity

On-premises SAM account name

10. Select ***Save***

11. Still within the same ***Enterprise application***, select ***Users and groups***. Select ***Add user***, and select any users or groups that you would like to be able to access the app. In this example, I've granted *qlikadmin@qlikpoc.com* access.



QlikSenseAzureKerberos - Users and groups

Enterprise Application

The application will appear on the access panel for assigned users. Set 'visible to users?' to no in properties to

First 100 shown, to search all users & groups, enter a display name.

DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED
QlikAdmin	User	Default Access

Setup the Qlik Sense Proxy

1. Navigate to the ***Qlik Sense QMC***.

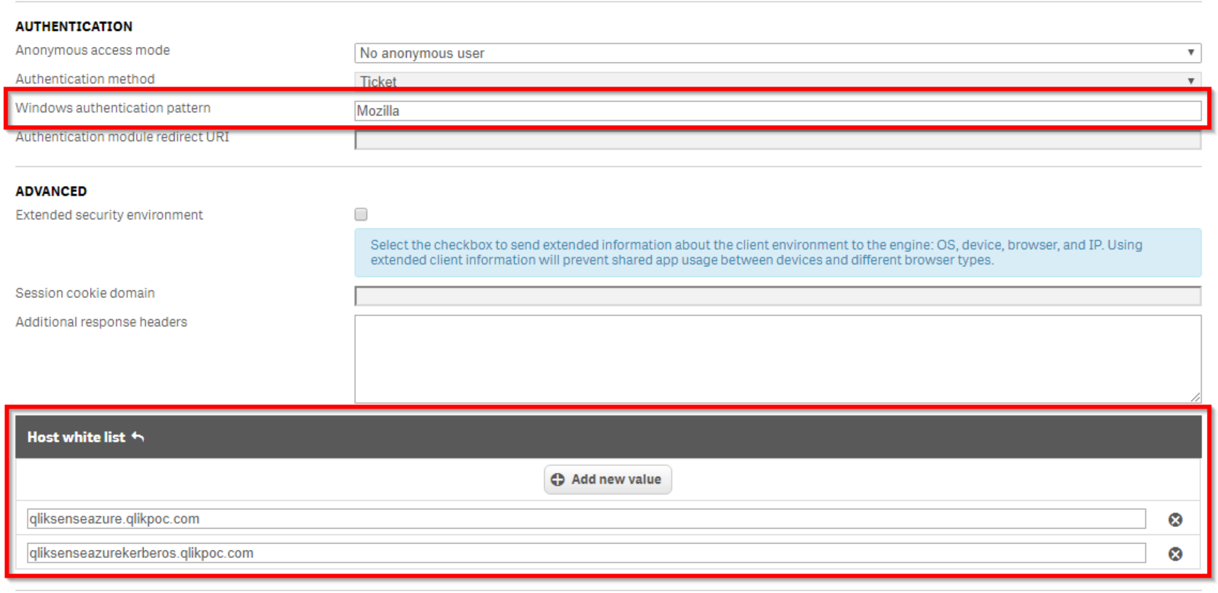
2. Select ***Virtual Proxies***

3. Select the appropriate ***Virtual Proxy***, in this example, it is *Central*.

4. Select Authentication and ***Advanced***.

5. Enter *Mozilla* into the ***Windows authentication pattern*** field as this search criteria is found in more user agents than *Windows*.

6. Enter the urls that you will be accessing Qlik Sense through into the the ***Host white list***. This is the ***Application proxy*** domain as well as the local url. In this example, they are *qliksenseazurekerberos.qlikpoc.com* and *qliksenseazure.qlikpoc.com*.



AUTHENTICATION

Anonymous access mode: No anonymous user

Authentication method: Ticket

Windows authentication pattern: Mozilla

Authentication module redirect URI:

ADVANCED

Extended security environment: □

Select the checkbox to send extended information about the client environment to the engine: OS, device, browser, and IP. Using extended client information will prevent shared app usage between devices and different browser types.

Session cookie domain:

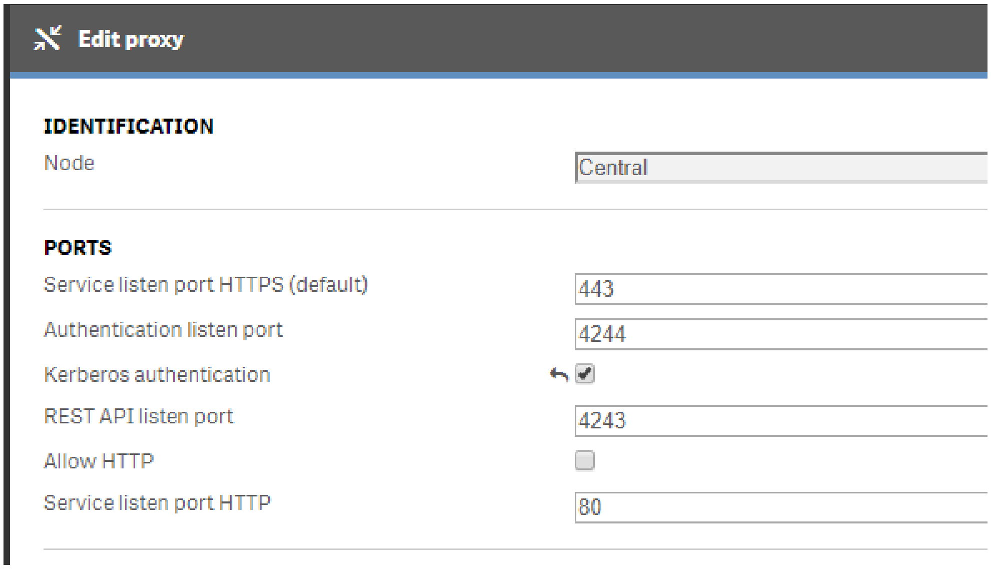
Additional response headers:

Host white list

qliksenseazure.qlikpoc.com

qliksenseazurekerberos.qlikpoc.com

7. The virtual proxy will restart, at which point navigate back to ***Proxies*** and select the appropriate ***Proxy***, in this case it is *Central*.
8. Select the ***Kerberos authentication*** checkbox under ***Ports***. The



Edit proxy

IDENTIFICATION

Node: Central

PORTS

Service listen port HTTPS (default): 443

Authentication listen port: 4244

Kerberos authentication: ☑

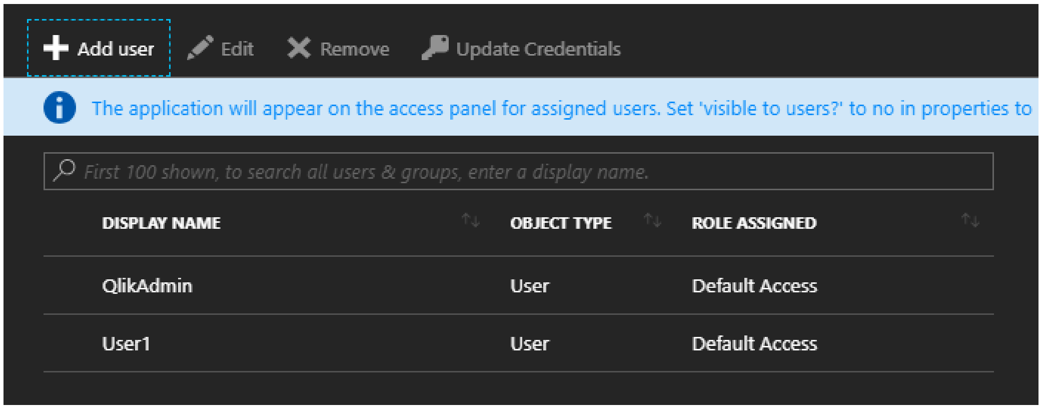
REST API listen port: 4243

Allow HTTP: □

Service listen port HTTP: 80

Accessing Qlik Sense

1. You should now be able to access Qlik Sense from the ***Application Proxy*** url. Ensure that you have granted any user access to the ***Azure Enterprise Application*** that you plan to have log into Qlik Sense. I have gone ahead and granted access to an additional domain user for testing, and have made sure that that user has been synced to ***Azure Active Directory***.

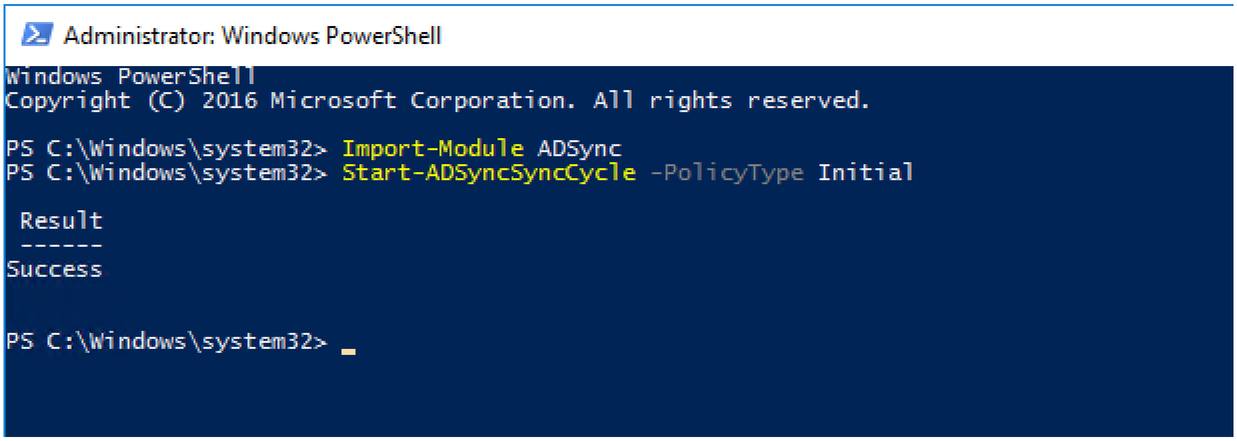


The application will appear on the access panel for assigned users. Set 'visible to users?' to no in properties to

First 100 shown, to search all users & groups, enter a display name.

DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED
QlikAdmin	User	Default Access
User1	User	Default Access

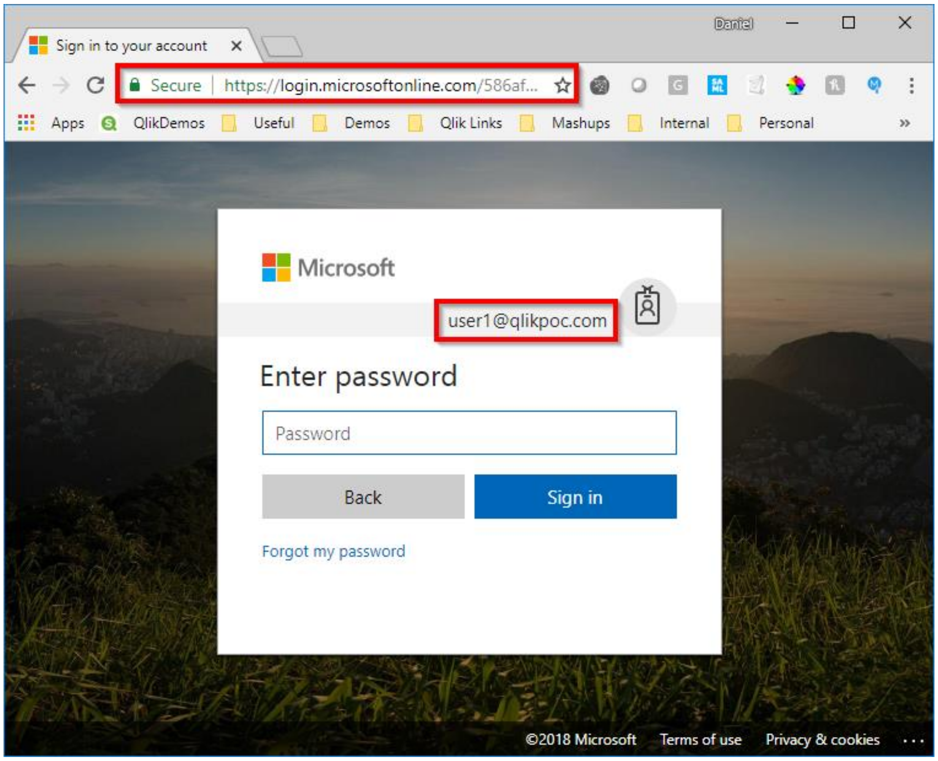
2. If you do not want to wait for the next ***Azure AD Sync Cycle***, you can leverage this bit of ***Powershell*** script to manually sync it:



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Import-Module ADSync
PS C:\Windows\system32> Start-ADSyncSyncCycle -PolicyType Initial

 Result
 ------
Success


PS C:\Windows\system32> _
```

3. Make sure you've closed your current browser session, open a new browser, and navigate to the url. In this example, it is *https://qliksenseazurekerberos.qlikpoc.com*. *If you have issues accessing your url, you may need to disconnect from your vpn, etc.

4. If successful, you will be redirected to the Microsoft login page.



Sign in to your account

Secure | https://login.microsoftonline.com/586af...

Microsoft

user1@qlikpoc.com

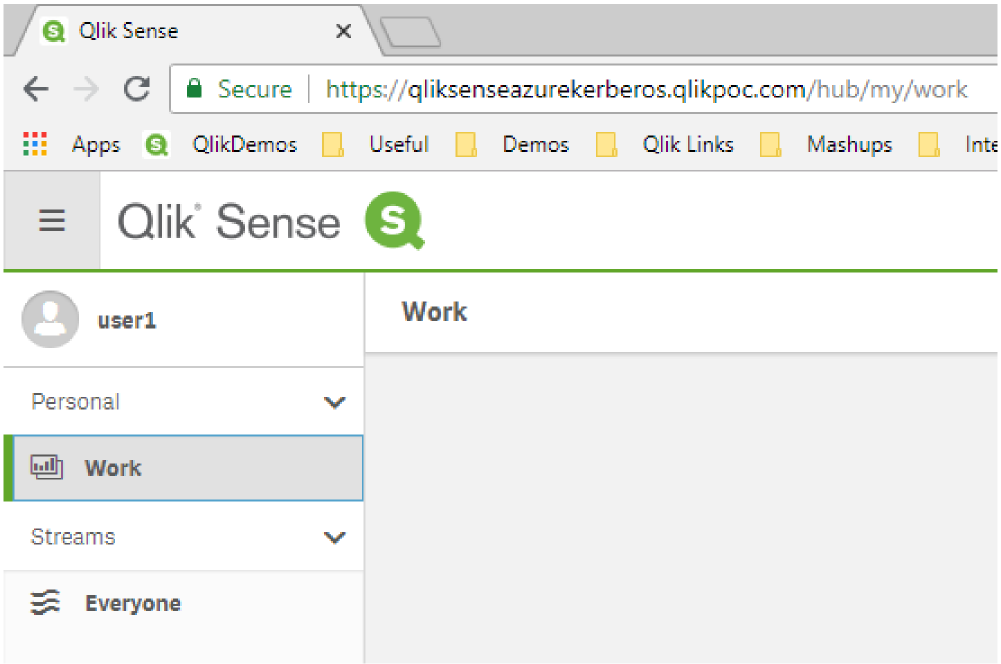
Enter password

Password

Forgot my password

©2018 Microsoft Terms of use Privacy & cookies

5. Enter the user's UPN and password – in this example, I am logging in as *user1@qlikpoc.com*. This user has been assigned access to the ***Azure Enterprise Application*** and has been allocated a license to Qlik Sense already.



Qlik Sense

Secure | https://qliksenseazurekerberos.qlikpoc.com/hub/my/work

user1

Work