

Troubleshooting Windows Auth

Last updated by | Vitor Tomaz | Mar 31, 2023 at 6:01 AM PDT

Contents

- [Issue](#)
- [Investigation/Analysis](#)
 - [1. Troubleshooting the setup](#)
 - [If you are using modern interactive flow](#)
 - [If you are using incoming trust-based flow](#)
 - [2. Identifying the failing step](#)
 - [2.1 Check if Kerberos token is provided](#)
 - [2.2 Kerberos ticket cannot be retrieved](#)
 - [2.3 Verify tickets are getting cached](#)
 - [2.4 Verify the sign-ins in ASC Tenant Explorer](#)
 - [3. Advanced Troubleshooting](#)
 - [3.1 Collect logs](#)
 - [3.2 Check the logs](#)
 - [3.3 If needed, get help checking the logs](#)
 - [Learn more about the subject](#)

Issue

Customer is facing issues with Windows Authentication for Azure AD principals on SQL Managed Instance

Investigation/Analysis



1. Troubleshooting the setup

Questions you can use to verify the setup:


- Is your on-premises Active Directory integrated with Azure AD (using Azure AD Connect)?
- What authentication flow are you using (Modern interactive flow / Incoming trust-based flow) ?
- Is the client machine a SharePoint Server?
(SharePoint Server doesn't support connecting to databases hosted in Azure SQL Managed Instance using Windows authentication.)
- Are you using Azure Active Directory credentials from a *Federated domain* or a *Managed Domain*?


If you are using modern interactive flow

- Is the client machine running Windows 10 20H1, Windows Server 2022, or a higher version of Windows?

- Is the client machine on VDI?
(see supported scenarios at <https://learn.microsoft.com/en-us/azure/active-directory/devices/howto-device-identity-virtual-desktop-infrastructure#supported-scenarios> )
- Is the client machine joined to Azure AD or Hybrid Azure AD?
Confirm by running the dsregcmd command: dsregcmd.exe /status
AzureAdJoined must be YES. If it is set to NO, open a collaboration with device registration team, use the SAP *Azure/Azure Active Directory Directories, Domains, and Objects/Devices/Configuring Windows Hybrid Azure AD join*, see more at <https://learn.microsoft.com/en-us/azure/active-directory/devices/troubleshoot-device-dsregcmd#device-state> )
- Is application connecting to the managed instance via an interactive session (like SSMS or web application)?
Note that applications that run as a service are not supported.
- Is the Azure subscription under the same Azure AD tenant you plan to use for authentication?
- Is the group policy 'Administrative Templates\System\Kerberos\Allow retrieving the cloud Kerberos ticket during the logon' enabled?
- Was user Azure AD Primary Refresh Token (PRT) refreshed?
To refresh PRT manually, run this command from a command prompt: dsregcmd.exe /RefreshPrt

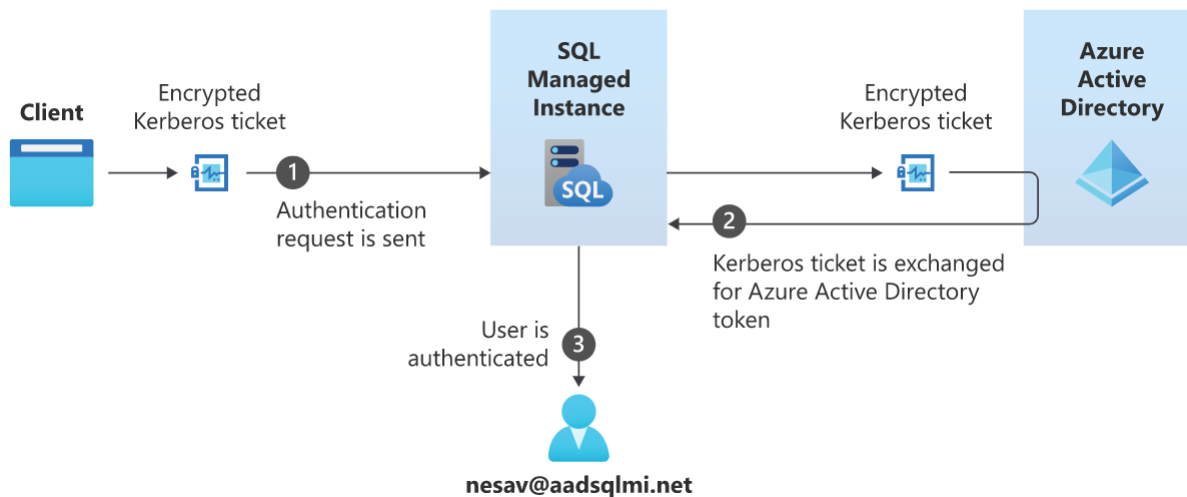
If you are using incoming trust-based flow

- Is the client machine running Windows 10, Windows Server 2012, or a higher version of Windows?
- Is the client machine on VDI?
(see supported scenarios at <https://learn.microsoft.com/en-us/azure/active-directory/devices/howto-device-identity-virtual-desktop-infrastructure#supported-scenarios> )
- Is the client machine joined to AD?
Confirm by running the dsregcmd command: dsregcmd.exe /status
Check DomainJoined under 'Device State' section, must be 'YES'.
What is the DomainName there? What is the TenantId under Tenant Details?
- Is the Azure subscription under the same Azure AD tenant you plan to use for authentication?
What is the TenantId on dsregcmd.exe /status?
- Is Trusted Domain Object created successfully?
Check the updated Kerberos Settings using the Get-AzureAdKerberosServer PowerShell cmdlet, the CloudTrustDisplay field should now return Microsoft.AzureAD.Kdc.Service.

If the Set-AzureAdKerberosServer is failing ask customer if they are configuring a root or a child on premises AD domain.
- Is the Group Policy Object configured?
What is the Value used (it would be something like '<<https://login.microsoftonline.com:443>  :your_Azure_AD_tenant_id/kerberos />')
Confirm there is a space following https and the space prior to the closing / in the value.

2. Identifying the failing step

1. Client has to acquire a Kerberos token, and then send it to SQL MI
2. SQL MI will contact Azure AD service to exchange the Kerberos token for a JWT token
3. That token is then used to authenticate the user



2.1 Check if Kerberos token is provided

Most issues happen on step 1, acquire the Kerberos token but you can start by confirming that it's not during steps 2 or 3.

To do so, use ASC Connectivity tab:

Summarized Managed Instance errors

[Query Link](#)

Shows error summary for connections that failed on a Managed Instance application during the time frame that was selected when report was created. If a database is specified in the support request, the results will be scoped to the specified database only. Otherwise, errors will be collected from all databases on the server. If the query returns 0 rows, no errors were thrown from the Managed Instance application in the selected time frame.

	EarliestErrorOccur...	LatestErrorOccur...	Count	DatabaseName	Error	State	StateDescription	ReadOnlyIntent	AuthenticationType	AADErrorState	AADErrorStateDes...
+	2022-10-18 20:33:28	2022-10-18 20:33:28	1	(DEFAULT_DATAB...	33155	1	Default	No	AAD Universal MFA		
-	2022-10-18 20:33:30	2022-10-18 20:33:30	2	(DEFAULT_DATAB...	18456	188	AzureKerberosAA...	No	Windows Auth	156	AADESTSBadRequ...
EarliestErrorOccurrence 2022-10-18 20:33:30 LatestErrorOccurrence 2022-10-18 20:33:30 Count 2 DatabaseName (DEFAULT_DATABASE) Error 18456 State 188 StateDescription AzureKerberosAADSystemError ReadOnlyIntent No AuthenticationType Windows Auth AADErrorState 156 AADErrorStateDescription AADESTSBadRequestError AppName f8e8925515cb Nodes ["DB8C.1"]											

Connection Analytics Performance Analytics Gateway Analytics SQL Alias Linked Servers **AAD**

MonAzureActiveDirService [Query Link](#)

Shows telemetry from MonAzureActiveDirService

Drag a column header and drop it here to group by that column

	originalEventTime...	logical_database_...	event	connection_type...	operation_type_desc	error_code_desc	error_state_desc	connection_type	operation_type	error_co
+	2022-10-18 20:33:30	master	azure_active_dir...	FedAuthNonSDS	AADOperationESTSGet/JWTForKerberosTicket	-2147467259	AADESTSBadRequestError	1	7	-214746
+	2022-10-18 20:33:30	master	azure_active_dir...	FedAuthNonSDS	AADOperationESTSGet/JWTForKerberosTicket	-2147467259	AADESTSBadRequestError	1	7	-214746

1 - 2 of 2 items

In case there no records for Windows Auth logins, it may be the case that a PreLogin packet was received but nothing else happened because the Kerberos token could not be acquired.

If this is the case, we'll only have records at Tenant Ring level (logical_server_name is empty, and login attempt can belong to any MI in the ring).

The following query may help you find records like these.

Error 17830 state 11 is one of errors seen in matching records. Please ping vitomaz if you see different ones, or to confirm this is what you see on your case (thanks!).

```
let startTime = todatetime('2023-02-23 12:41:52');
let endTime = todatetime('2023-02-23 15:41:52');
let clusterName = 'tr1242.useuapeast2-a.worker.database.windows.net';
MonLogin
| where originalEventTimestamp between(startTime..endTime)
| where ClusterName =~ clusterName
| where event == 'process_login_finish' and isempty(logical_server_name)
| project originalEventTimestamp, NodeName, event, is_success, error, state, peer_address, extra_info
// | where error == 17830 and state == 11
```

In case there are error logs in ASC, but error codes and states listed there are not enough for us to understand the problem, there is a PII telemetry in which we are logging the whole response from ESTS, but only PG has access to it today, since it contains PII.


```
PiiAzureActiveDirService
| where sql_connection_id == "<conn_id">
| where event == "kerberos_to_jwt_service_failure"
```

If information from this table is needed, please raise an lCM to **SQL Managed Instance: AAD** team.

Most common error messages are:

Error message	Issue	Mitigation
AADSTS50076: Due to a configuration change made by your administrator, or because you moved to a new location, you must use multi-factor authentication to access ".	There is CA policy which enforces MFA	Customer needs to exclude Service Principal from CA policy
AADSTS65001: The user or administrator has not consented to use the application with ID " named ". Send an interactive authorization request for this user and resource.	Customer has not granted admin consent to Service Principal	Customer needs to grant admin consent
AADSTS900021: Requested tenant identifier '000000000-0000-0000-0000-000000000000' is not valid. Tenant identifiers may not be an empty GUID.	AAD Admin is not configured on MI	Customer needs to configure AAD Admin on MI
AADSTS53003: Access has been blocked by Conditional Access policies. The access policy does not allow token issuance.	There is CA policy which blocks kerberos ticket exchange	Customer needs to exclude Service Principal from CA policy
AADSTS140010: Kerberos ticket validation failure	There is an issue with kerberos ticket exchange on Identity side	Request assistance from Identity team (Auth Reach - Hybrid Authentication) to diagnose/mitigate the issue

2.2 Kerberos ticket cannot be retrieved

If a Kerberos ticket cannot be retrieved, customer can [enable Kerberos event logging on his computer](#)  and find the reason.

Note: Make sure to disable Kerberos event logging after the troubleshooting session to prevent performance problems on the client machine.

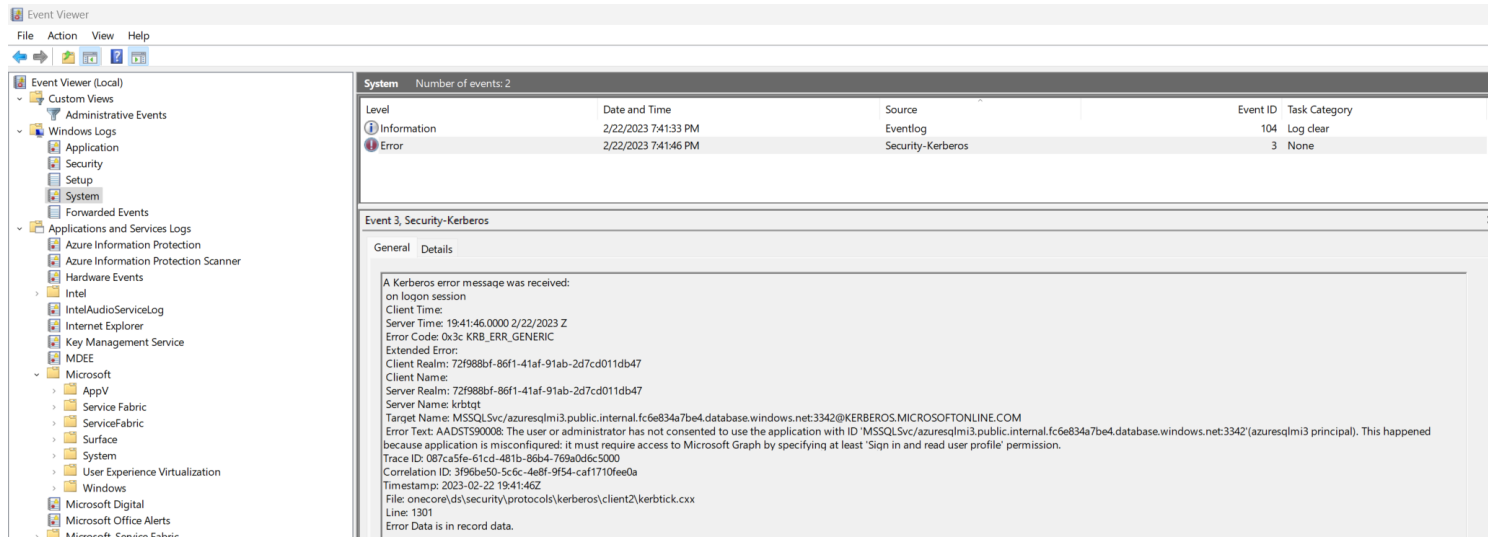
In a nutshell, customer needs to start an elevated command prompt and run:

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters /v LogLevel /t REG_DWORD /d 0x1
```

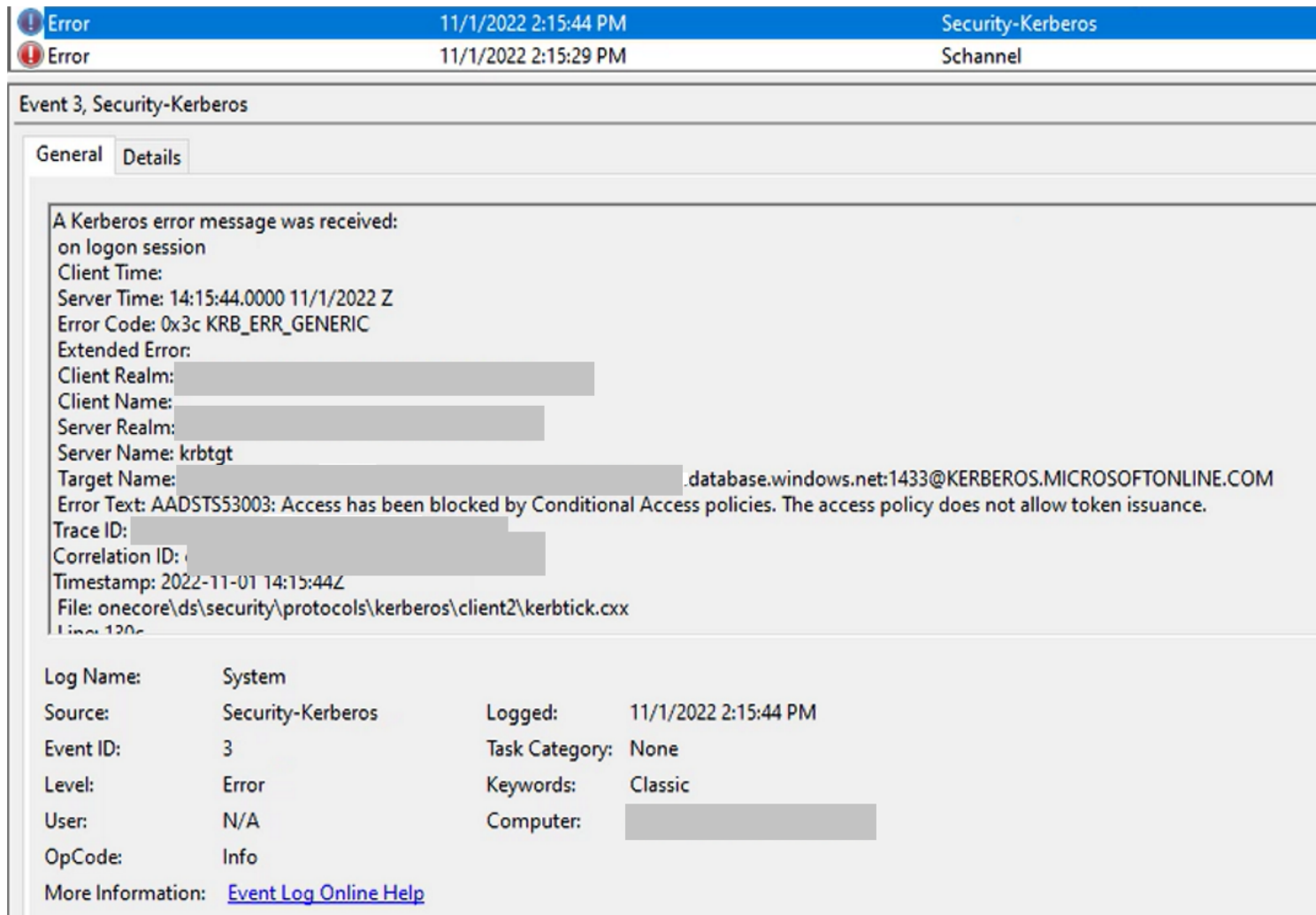
Once that is done, try to connect to SQL MI using Windows Authentication.

Customer can check for logs using Event Viewer.

See source Security-Kerberos on the System log:



or



An alternative is PowerShell, run the following (in PowerShell ISE as an example):

```
Get-EventLog -LogName System -Source Kerberos | Select-Object -Property TimeGenerated, MachineName, EntryType,
```

Results may look like:

```
TimeGenerated : 2/22/2023 7:41:46 PM
MachineName   : VITOMAZ-B00K3-3
EntryType     : Error
Message       : A Kerberos error message was received:
                on logon session
                Client Time:
                Server Time: 19:41:46.0000 2/22/2023 Z
                Error Code: 0x3c KRB_ERR_GENERIC
                Extended Error:
                Client Realm: 72f988bf-86f1-41af-91ab-2d7cd011db47
                Client Name:
                Server Realm: 72f988bf-86f1-41af-91ab-2d7cd011db47
                Server Name: krbtgt
                Target Name: MSSQLSvc/azuresqlmi3.public.internal.fc6e834a7be4.database.windows.net:3342@KRB
                Error Text: AADSTS90008: The user or administrator has not consented to use the application w
                This happened because application is misconfigured: it must require access to Microsoft Graph
                Trace ID: 087ca5fe-61cd-481b-86b4-769a0d6c5000
                Correlation ID: 3f96be50-5c6c-4e8f-9f54-caf1710fee0a
                Timestamp: 2023-02-22 19:41:46Z
                File: onecore\ds\security\protocols\kerberos\client2\kerbtick.cxx
                Line: 1301
                Error Data is in record data.
Index         : 209135
```

2.3 Verify tickets are getting cached

Follow the steps at [Verify tickets are getting cached](#) 

2.4 Verify the sign-ins in ASC Tenant Explorer

1. Identify the correlation_id In ASC, run a troubleshooter report for Connectivity, and check MonAzureActivDirService under AAD tab. Capture the correlation_id that are related with the tests made by the customer.
2. Check login results in AAD

Sign-Ins Last refreshed at: 3/24/2023 22:20:34 PM

Sign-In logs | Diagnostics | Authenticator App logs | Hybrid Sign In Configuration | Authentication Methods | CBA Trusted Authorities

Date Time Range (UTC): 03/22/2023 at 15:55 - 03/22/2023 at 16:00 UTC

Correlation Id: 726F4070-... Request Id: ... Status Error Codes: ...

Cross Tenant Access Type: ... **Run**

The tenant has 30 days of sign-ins logs.

Interactive User | **Non-Interactive User** | Service Principal | Managed Identity

Date	User	Application	Status	Conditional Access	MFA Required	Risk State
2023-03-22 15:55:35	Fail (50079)	failure	Yes	none

1 - 1 of 1 items

- Go to ASC > Tenant Explorer > Sign-ins
- Fill the Date Time range and Correlation Id
- Run
- Select Non-Interactive User
- Click on the plus (+) sign and review each entry, to get a detailed verbose error message

```
"status": {
  "errorCode": 50079,
  "failureReason": "Due to a configuration change made by your administrator, or because you moved to a new location, you must enroll in multi-factor authentication to access {identifier}.",
  "additionalDetails": "Either a managed user needs to register security info to complete multi-factor authentication, or a federated user needs to get the multi-factor claim from the federated identity provider. There could be multiple things requiring multi-factor, e.g. Conditional Access policies, per-user enforcement, requested by client, among others."
},
"deviceDetails": {
```

3. Advanced Troubleshooting

3.1 Collect logs

Please ask customer to:

Download Authentication Scripts from <https://aka.ms/authscripts>

Form elevated PowerShell terminal, navigate to the path where downloaded scripts are and execute:

```
klist purge
.\start-auth.ps1 -v -accepteula
dsregcmd /refreshprt
klist get krbtgt
klist get krbtgt/kerberos.microsoftonline.com
klist get MSSQLSvc/<miname>.<dnszone>.database.windows.net:1433
.\stop-auth.ps1
```

Note: If customer is connecting to the public endpoint change the klist command above `klist get MSSQLSvc/<miname>.<dnszone>.database.windows.net:1433` with the following one `klist`

`get MSSQLSvc/<miname>.public.<dnszone>.database.windows.net:3342`

3.2 Check the logs

While it's likely we'll need help from AAD team, there are some error messages that customer can fix on it's own. Some things you may check:

Check Kerberos errors in error log:

- From the results folder, open System.evtx
- Add a filter for Event Sources: Security-Kerberos

Filter Current Log

Filter XML

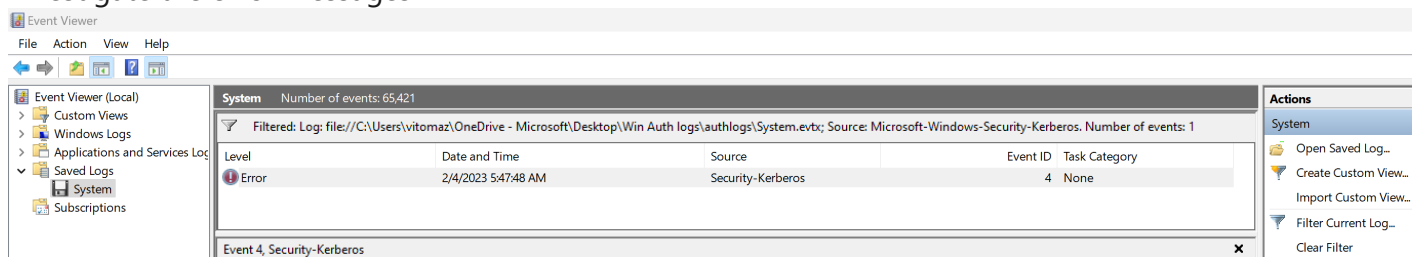
Logged: Any time

Event level: ☐ Critical ☐ Warning ☐ Verbose
☐ Error ☐ Information

☒ By log Event logs: file:///C:/Users/vitomaz/OneDrive - Microsoft/De

☐ By source Event sources: Security-Kerberos

- Investigate the error messages



3.3 If needed, get help checking the logs

Open a collab with AAD support team for help checking the logs.

Kerberos authentication in Azure AD is supported by Hybrid Authentication team.

Support topic:


Azure / Azure Active Directory Sign-In and Multi-Factor Authentication / AD domain-joined Seamless SSO with PTA or PHS\Troubleshoot AD domain-joined Seamless SSO with PTA or PHS

Queue: MSaaS AAD - Applications Premier

Note: if you are not getting relevant progress from the collab with AAD team, please ping vitomaz/Azure SQL MI EEE team.

Learn more about the subject

[What is Windows Authentication for Azure Active Directory principals on Azure SQL Managed Instance?](#) 

[How Windows Authentication for Azure SQL Managed Instance is implemented with Azure Active Directory and Kerberos](#) 

[How to set up Windows Authentication for Azure SQL Managed Instance using Azure Active Directory and Kerberos](#) 

[How to set up Windows Authentication for Azure Active Directory with the modern interactive flow](#) 

[How to set up Windows Authentication for Azure AD with the incoming trust-based flow](#) 

[Configure Azure SQL Managed Instance for Windows Authentication for Azure Active Directory](#) 

[Run a trace against Azure SQL Managed Instance using Windows Authentication for Azure Active Directory principals](#) 

[Troubleshoot Windows Authentication for Azure AD principals on Azure SQL Managed Instance](#) 

How good have you found this content?



-