

Using Windows Authentication for Azure AD principals

Last updated by | Vitor Tomaz | Feb 24, 2023 at 3:30 AM PST



Contents

- Self-help content presented in Azure Portal
 - Configure and troubleshoot issues using Windows Authen...
 - How to set up Windows Authentication for Azure SQL Man...
 - Set up using modern interactive flow
 - Set up using incoming trust-based flow
 - Set up the Managed Instance
 - Troubleshooting
 - Resources

Self-help content presented in Azure Portal

(This content was shown to the customer during case submission. It's also visible on 'Diagnose and solve problems' blade.)

Configure and troubleshoot issues using Windows Authentication for Azure AD principals



[Windows Authentication for Azure AD principals on Azure SQL Managed Instance](#)  enables customers to move existing services to the cloud while maintaining a seamless user experience and provides the basis for security infrastructure modernization. To enable Windows Authentication for Azure Active Directory (Azure AD) principals, you will [turn your Azure AD tenant into an independent Kerberos realm](#)  and create an incoming trust in the customer domain.

Review the following section titles and expand the section that best describes your issue or scenario.

How to set up Windows Authentication for Azure SQL Managed Instance

There are two phases to set up Windows Authentication for Azure SQL Managed Instance:

Phase 1: One-time infrastructure setup

- Synchronize Active Directory (AD) and Azure AD, if this hasn't already been done. Use [Azure AD Connect](#)  to integrate on-premises directories with Azure AD.
- Select which authentication flow(s) you will use and implement it. See [how to set up Windows Authentication for Azure SQL Managed Instance using Azure Active Directory and Kerberos](#) 

Phase 2: Configuration of Azure SQL Managed Instance

- Enable a system assigned service principal


- Grant admin consent to a system assigned service principal

See how to [Configure Azure SQL Managed Instance for Windows Authentication for Azure Active Directory](#). 

Set up using modern interactive flow

The modern interactive flow is recommended for organizations with Azure AD joined or Hybrid AD joined clients running Windows 10 20H1 / Windows Server 2022 and higher where clients are joined to Azure AD or Hybrid AD.

The following prerequisites are required to implement the modern interactive authentication flow:


Prerequisite	Description
Clients must run Windows 10 20H1, Windows Server 2022, or a higher version of Windows.	
Clients must be joined to Azure AD or Hybrid Azure AD.	You can determine if this prerequisite is met by running the dsregcmd command  : <code>dsregcmd.exe /status</code>
Application must connect to the managed instance via an interactive session.	This supports applications such as SQL Server Management Studio (SSMS) and web applications, but won't work for applications that run as a service.
Azure AD tenant.	
Azure subscription under the same Azure AD tenant you plan to use for authentication.	
Azure AD Connect installed.	Hybrid environments where identities exist both in Azure AD and AD.

See [How to set up Windows Authentication for Azure Active Directory with the modern interactive flow](#)  for steps to enable this authentication flow.

Set up using incoming trust-based flow

Incoming trust-based authentication flow is recommended for customers who can't use the modern interactive flow, and have AD joined clients running Windows 10 / Windows Server 2012 and higher.

The following prerequisites are required to implement the incoming trust-based authentication flow:


Prerequisite	Description
Client must run Windows 10, Windows Server 2012, or a higher version of Windows.	
Clients must be joined to AD. The domain must have a functional level of Windows Server 2012 or higher.	You can determine if the client is joined to AD by running the dsregcmd command  : <code>dsregcmd.exe /status</code>
Azure AD Hybrid Authentication Management Module.	This PowerShell module provides management features for on-premises setup.
Azure tenant.	
Azure subscription under the same Azure AD tenant you plan to use for authentication.	
Azure AD Connect installed.	Hybrid environments where identities exist both in Azure AD and AD.

See [How to set up Windows Authentication for Azure Active Directory with the incoming trust based flow](#)  for instructions on enabling this authentication flow.

Set up the Managed Instance

The steps to set up Azure SQL Managed Instance are the same for both the incoming trust-based authentication flow and the modern interactive authentication flow.

The following prerequisites are required to configure a managed instance for Windows Authentication for Azure AD principals:



Prerequisite	Description
Az.Sql PowerShell module	This PowerShell module provides management cmdlets for Azure SQL resources. Install this module by running the following PowerShell command: <code>Install-Module -Name Az.Sql</code>
Azure Active Directory PowerShell Module	This module provides management cmdlets for Azure AD administrative tasks such as user and service principal management. Install this module by running the following PowerShell command: <code>Install-Module -Name AzureAD</code>
A managed instance	You may create a new managed instance  or use an existing managed instance.

See [Configure Azure SQL Managed Instance for Windows Authentication for Azure Active Directory](#)  for steps to configure each managed instance.

Troubleshooting




Modern interactive flow

For modern interactive flow, confirm that:









- Client is running Windows 10 20H1, Windows Server 2022, or a higher version of Windows.
- Device is joined to Azure AD or Hybrid Azure AD. Check by running the [dsregcmd command](#) .
- Group policy *Allow retrieving the cloud Kerberos ticket during the logon* is [enabled](#) .

Incoming trust based

For incoming trust based flow, confirm that:

- Client is running Windows 10, Windows Server 2012, or a higher version of Windows.
- Device is Domain Joined. Check by running the [dsregcmd command](#) .
- The [on-premises AD trusts Azure AD](#) . Using Get-AzureAdKerberosServer PowerShell cmdlet, the CloudTrustDisplay field should return *Microsoft.AzureAD.Kdc.Service.TrustDisplay*.
- The group policy [KDC proxy servers for Kerberos clients](#)  is configured.

Resources

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

How good have you found this content?

