On-premises data gateways documentation

The on-premises data gateway provides quick and secure data transfer between on-premises data and several Microsoft cloud services, such as Power BI, Power Apps, Power Automate, Azure Analysis Services, and Azure Logic Apps.

Get started

OVERVIEW

What is an on-premises data gateway?

On-premises data gateway architecture

On-premises data gateway FAQ

Set up and manage

HOW-TO GUIDE

Install gateways

Configure gateways

Manage gateways

Reference and resources

REFERENCE

PowerShell support for gateways clusters

WHAT'S NEW

Previous monthly updates

What is an on-premises data gateway?

Article • 03/02/2023

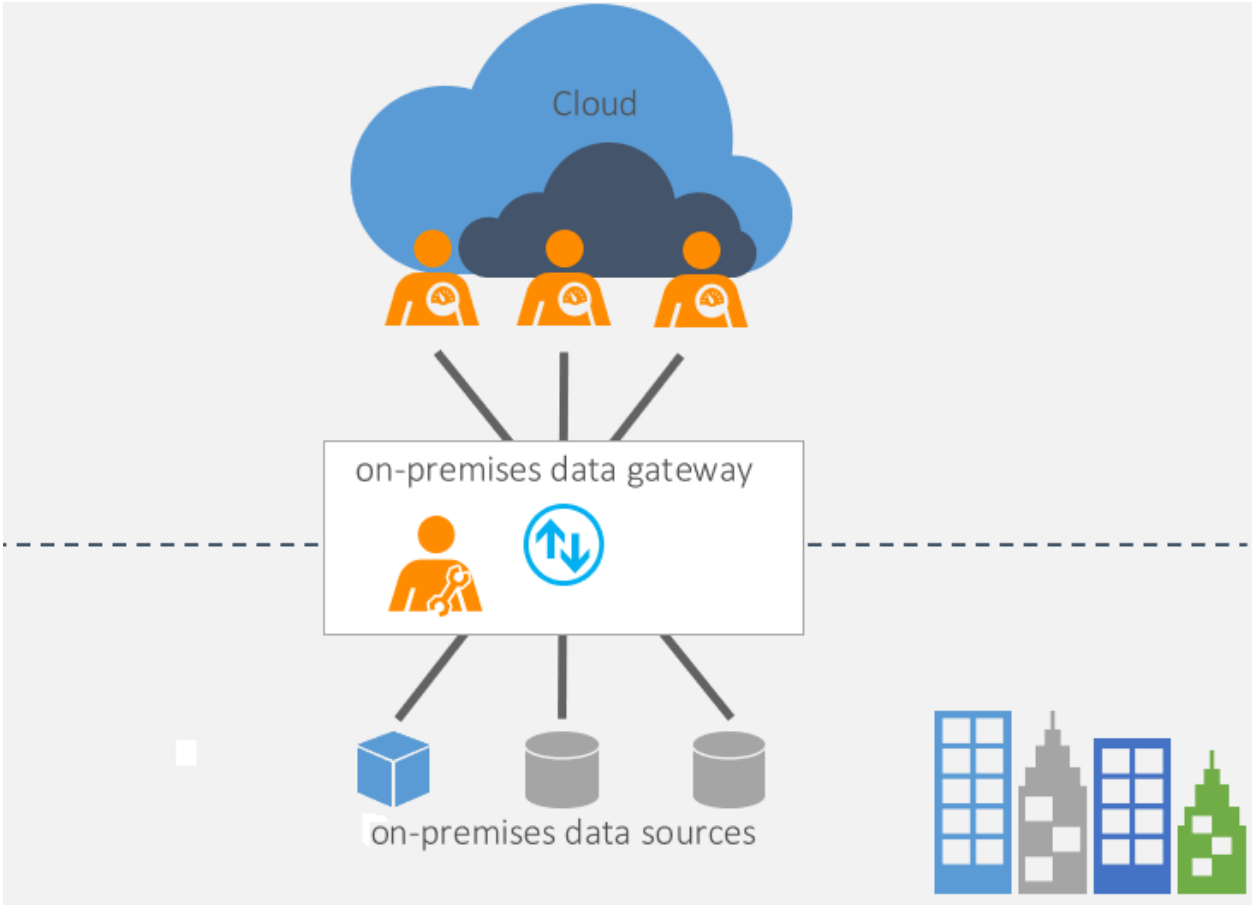
> **Note**
>
> Currently, Microsoft actively supports only the last six releases of the on-premises data gateway. We release a new update for data gateways every month.

> **Note**
>
> Beginning on March 15, 2023, any Power BI dataflow using an on-premises data gateway version older than April 2021 might fail. To ensure your refreshes continue to work correctly, be sure to update your gateway to the latest version and sign in to it.

The on-premises data gateway acts as a bridge. It provides quick and secure data transfer between on-premises data, which is data that isn't in the cloud, and several Microsoft cloud services. These services include Power BI, Power Apps, Power Automate, Azure Analysis Services, and Azure Logic Apps.

By using a gateway, organizations can keep databases and other data sources on their on-premises networks while securely using that on-premises data in cloud services.

How the gateway works



For detailed information on how the gateway works, go to On-premises data gateway architecture.

Types of gateways

There are two different types of on-premises data gateways, each for a different scenario.

- **On-premises data gateway**: Allows multiple users to connect to multiple on-premises data sources. With a single gateway installation, you can use an on-premises data gateway with all supported services. This gateway is well suited to complex scenarios where multiple people access multiple data sources.
- **On-premises data gateway (personal mode)**: Allows one user to connect to data sources and can't be shared with others. An on-premises data gateway (personal mode) can be used only with Power BI. This gateway is well suited to scenarios where you're the only one who creates reports and you don't need to share any data sources with others.

In addition, there's a virtual network (VNet) data gateway that lets multiple users connect to multiple data sources that are secured by virtual networks. No installation is required because it's a Microsoft managed service. This gateway is well suited to complex scenarios in which multiple people access multiple data sources. Virtual

network data gateways are discussed in depth in What is a virtual network (VNet) data gateway.

Using a gateway

There are four main steps for using a gateway.

1. Download and install the gateway on a local computer.
2. Configure the gateway based on your firewall and other network requirements.
3. Add gateway admins who can also manage and administer other network requirements.
4. Troubleshoot the gateway if there are errors.

Considerations

- Logic Apps, Power Apps, and Power Automate support both read and write operations through the gateway:
  - The gateway has a 2-MB payload limit for write operations.
  - The gateway has a 2-MB request limit and an 8-MB compressed data response limit for read operations.
  - URL for the GET request has a 2048 character limit.
- While using the gateway with Power BI in Direct Query Mode, there's a 16-MB uncompressed data response limit.
- For information about installation considerations, go to Related considerations.

Gateway documentation

This document contains general information about the on-premises data gateway that applies to all services that the gateway supports. You can obtain more on-premises data gateway information for specific products by visiting the following product-specific sites.

- On-premises data gateway in-depth - Power BI
- Using an on-premises data gateway in Power Platform Dataflows
- Manage connections in Power Automate
- Connect to on-premises data sources from Azure Logic Apps
- Connecting to on-premises data sources with On-premises data gateway - Azure Analysis Services

Next steps

- Install the on-premises data gateway

On-premises data gateway architecture

Article • 12/05/2022

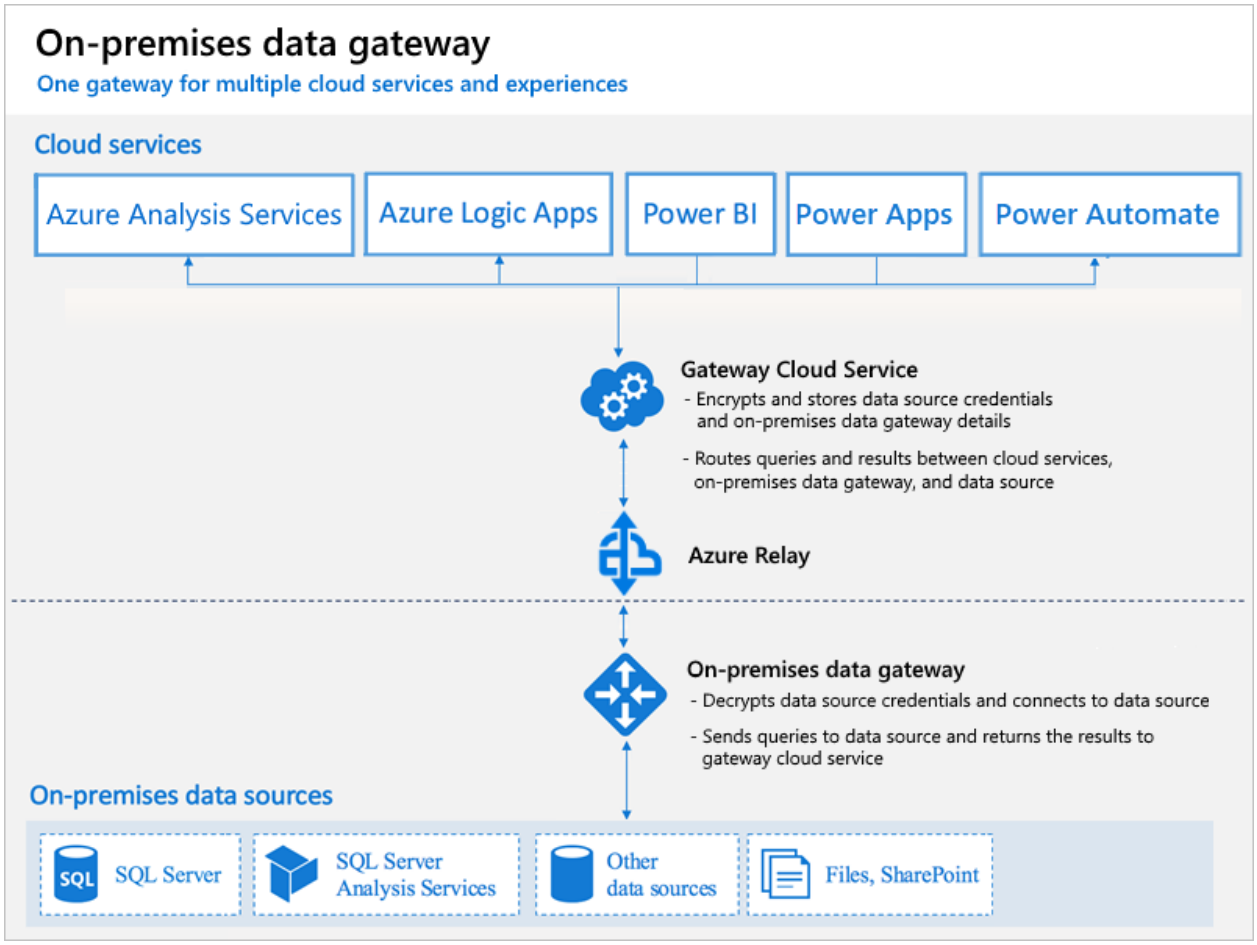
Users in your organization can access on-premises data to which they already have access authorization. But before those users can connect to your on-premises data source, an on-premises data gateway needs to be installed and configured.

The gateway facilitates quick and secure behind-the-scenes communication. This communication flows from a user in the cloud to your on-premises data source and then back to the cloud.

An admin is usually the one who installs and configures a gateway. These actions might require special knowledge of your on-premises servers or Server Administrator permissions.

This article doesn't provide step-by-step guidance on how to install and configure the gateway. For that guidance, go to Install an on-premises data gateway. This article does provide in-depth understanding of how the gateway works.

How the gateway works



Let's first look at what happens when you interact with an element that is connected to an on-premises data source.

> **Note**
>
> Depending on the cloud service, you might need to configure a data source for the gateway.

1. The cloud service creates a query and the encrypted credentials for the on-premises data source. The query and credentials are sent to the gateway queue for processing. For more information about credential encryption in Power BI, go to Power BI security whitepaper.
2. The gateway cloud service analyzes the query and pushes the request to Azure Relay.
3. Azure Relay sends the pending requests to the gateway. Both the gateway and Power BI service are implemented to only accept TLS 1.2 traffic.
4. The gateway gets the query, decrypts the credentials, and connects to one or more data sources with those credentials.
5. The gateway sends the query to the data source to be run.
6. The results are sent from the data source back to the gateway and then to the cloud service. The service then uses the results.

In step 6, queries like Power BI and Azure Analysis Services refreshes can return large amounts of data. For such queries, data is temporarily stored on the gateway machine. This data storage continues until all data is received from the data source. The data is then sent back to the cloud service. This process is called spooling. We recommend you use a solid-state drive (SSD) as the spooling storage.

Authentication to on-premises data sources

A stored credential is used to connect from the gateway to on-premises data sources. Regardless of the user, the gateway uses the stored credential to connect. But there might be authentication exceptions like DirectQuery and LiveConnect for Analysis Services in Power BI. For more information about credential encryption in Power BI, go to Power BI security whitepaper.

Sign-in account

You sign in with either a work account or a school account. This account is your organization account. If you signed up for an Office 365 offering and didn't supply your

actual work email address, your account name might look like nancy@contoso.onmicrosoft.com. A cloud service stores your account within a tenant in Azure Active Directory (Azure AD). In most cases, the User Principal Name (UPN) of your Azure AD account matches your email address.

Network traffic security

Traffic goes from the gateway to Azure Relay to the Power BI backend cluster. This traffic doesn't traverse the public internet. All Azure internal traffic goes over the Azure backbone.

Azure Active Directory

Microsoft cloud services use Azure AD to authenticate users. Azure AD is the tenant that contains usernames and security groups. Typically, the email address that you use for sign-in is the same as the UPN of your account. For more information about authentication in Power BI, go to Power BI security whitepaper.

How do I tell what my UPN is?

You might not know your UPN, and you might not be a domain admin. To find out the UPN for your account, run the following command from your workstation: `whoami /upn`.

Although the result looks like an email address, it's the UPN on your local domain account.

Synchronize an on-premises Active Directory with Azure Active Directory

You want each of your on-premises Active Directory accounts to match an Azure AD account, because the UPN for both accounts must be the same.

The cloud services know only about accounts within Azure AD. It doesn't matter if you add an account in your on-premises Active Directory. If the account doesn't exist in Azure AD, it can't be used.

There are different ways to match your on-premises Active Directory accounts with Azure AD.

- Add accounts manually to Azure AD.

Create an account on the Azure portal or within the Microsoft 365 admin center. Make sure the account name matches the UPN of the on-premises Active Directory account.

- Use the Azure Active Directory Connect tool to synchronize local accounts to your Azure AD tenant.

  The Azure AD Connect tool provides options for directory synchronization and authentication setup. These options include password hash sync, pass-through authentication, and federation. If you're not a tenant admin or a local domain admin, contact your IT admin to get Azure AD Connect configured.

Azure AD Connect ensures that your Azure AD UPN matches your local Active Directory UPN. This matching helps if you're using Analysis Services live connections with Power BI or single sign-on (SSO) capabilities.

> **Note**
>
> Synchronizing accounts with the Azure AD Connect tool creates new accounts within your Azure AD tenant.

Next steps

- On-premises data gateway FAQ
- Azure Relay
- Azure AD Connect

On-premises data gateway FAQ

FAQ

General

Do I need a gateway for cloud data sources, such as Azure SQL Database?

No, services can generally connect to cloud data sources without a gateway. However, you might need a data gateway if your data sources are behind a firewall, require a VPN, or are on virtual networks.

Why do I get the errors "InvalidConnectionCredentials" or "AccessUnauthorized" when accessing cloud data sources using OAuth2 credentials even though the credentials are updated recently.

When using OAuth2 credentials, the gateway currently doesn't support refreshing tokens automatically when access tokens expire (one hour after the refresh started). This limitation for long running refreshes exists for VNET gateways and on-premises data gateways.

What are the requirements for the gateway?

Review the requirements section in the installation article.

Does the gateway have to be installed on the same machine as the data source?

No, the gateway connects to the data source by using the provided connection information. In this sense, consider the gateway as a client application. The gateway just needs to connect to the specified server.

How many releases of the on-premises data gateway does Microsoft actively support?

Currently, Microsoft actively supports only the last six releases of the on-premises data gateway. We release a new update for data gateways every month.

Are there any licensing prerequisites required to install gateways?

There are no licensing restrictions for installing and registering a gateway. But any cloud service might have licensing restrictions on how gateways are used within that service.

Are there any requirements for network bandwidth?

Check that your network connection has good throughput. Each environment is different, and throughput depends on the amount of data that is sent. To ensure a minimum level of throughput between your on-premises data source and Azure datacenters, use Azure ExpressRoute. To help measure your throughput, you can use the Azure Speed Test app.

Where are my credentials stored?

The credentials that you enter for a data source are encrypted and stored in the gateway cloud service. The credentials are decrypted at the gateway on premises. For more information about credential encryption in Power BI, go to Power BI security whitepaper.

What is the actual Windows service called?

On your local computer, in the Services app, the service is called "On-premises data gateway service". In Task Manager, on the Services tab, the service name is "PBIEgwService". By default, the Windows service uses "NT SERVICE\PBIEgwService" as the Service SID (SSID).

Can the gateway Windows service run with an Azure Active Directory (Azure AD) account?

No, the Windows service needs a valid Windows account.

Are there any inbound connections to the gateway from the cloud?

No, the gateway uses outbound connections to Azure Relay.

What if I block outbound connections? What do I need to open?

Go to Enable outbound Azure connections.

Do I need to unblock the Azure Datacenter IP list? Where do I get the list?

If you block outbound IP traffic, you might need to unblock the Azure Datacenter IP list. The gateway communicates with Azure Relay by using an IP address and a fully qualified domain name. The Azure Datacenter IP list is updated weekly. For more information, go to Enable outbound Azure connections.

What is the latency for running queries from the gateway to a data source? What is the best architecture?

To avoid network latency, install the gateway as close as possible to the data source. If you can install the gateway on the actual data source, this closer location minimizes latency.

Also, consider the proximity to the Azure datacenters. For example, if your service uses the West US datacenter, and you have SQL Server hosted in an Azure virtual machine, you might also want your Azure VM in the West US region. This configuration minimizes latency and avoids egress charges on the Azure VM.

How are results sent back to the cloud?

The results are sent through Azure Relay. For more information, go to On-premises data gateway architecture.

Can I place the gateway in a perimeter network (also known as DMZ, demilitarized zone, and

screened subnet)?

The gateway requires connectivity to the data source. So, if the data source isn't reachable in your perimeter network, the gateway might not have access.

For example, assume your SQL Server computer isn't in your perimeter network. Also, assume you can't connect to that computer from the perimeter network. If you place the gateway in your perimeter network, the gateway can't reach the SQL Server computer.

If the server on which the gateway is installed is only using an IPv6 address and connects with a data source (for example, Azure SQL/File Server/Database on Azure VM) using an IPv6 address only, is it possible to communicate from Power BI service to those data sources through the gateway?

Yes.

If the server on which the gateway is installed is using dual stack to be assigned both IPv4 and IPv6 addresses, would IPv4 or IPv6 be the priority for gateway communication?

This priority depends on Windows or the relevant data source drivers. This behavior is configurable in both Windows and various drivers, but isn't under the gateway's control.

Does the gateway support cross-tenant Azure AD access?

No, cross-tenant Azure AD access isn't supported. A Power BI dataset in a tenant can't connect to data sources from a different tenant using an Azure AD account. This limitation applies whether the data source uses an on-premises data gateway or not. To overcome this limitation, use an authentication type other than OAuth.

Can I force the gateway to use HTTPS traffic with Azure Relay instead of TCP?

Yes, for more information, go to Force HTTPS communication with Azure Relay. Turning on this feature has little effect on performance.

Are the on-premises data gateway and Data Management Gateway, which is used by Azure Machine Learning Studio and Azure Data Factory, the same thing?

No, they're different products. To get more information about Data Management Gateway, which is now called Self-hosted Integration Runtime, go to Create and configure a self-hosted integration runtime.

Can the person who sets up the gateway in the Azure portal be different from the one who installs that gateway?

Yes, you must use PowerShell to add other owners to the same gateway. These users can create the gateway in the Azure portal. However, they should connect to the portal and the gateway by using the same tenant.

Does Azure ExpressRoute eliminate the need for a gateway?

No. A gateway is still required when connecting to on-premises data sources.

How can I keep my data within the same region while using an on-premises data gateway?

More information: Keep data in the region where it's stored

High availability and disaster recovery

Are there any plans for enabling high-availability scenarios with the gateway?

To help avoid a single point of failure, you can set up on-premises data gateways as clusters for high availability. By default, cloud services such as Power Apps and Power BI use the primary gateway and fall back to the secondary gateway if the primary is unavailable.

What options are available for disaster recovery?

When you install the gateway, you supply a recovery key. You can use the key to restore or migrate a gateway.

What is the benefit of the recovery key?

The key provides a way to add a new gateway to a cluster or to migrate, recover, or take over a gateway.

Troubleshooting

For more information, go to Troubleshoot the on-premises data gateway.

Where are the gateway logs located?

Go to Troubleshooting tools.

How can I tell what queries are sent to the on-premises data source?

You can enable query tracing by turning on additional logging. The logs include the queries that are sent. Remember to turn off query tracing when you're done troubleshooting. Having query tracing enabled causes the logs to be larger.

You can also look at your data source's tools for tracing queries. For example, if SQL Server and SQL Server Analysis Services are data sources, you can use SQL Server Extended Events or SQL Server Profiler to trace queries.

What do I need to do if I've reached the maximum limit of 1000 data sources per user,

and how do I avoid reaching this limit?

Users are limited to 1000 data sources per user.

If you've reached the maximum number of data sources limit, verify that the number of data sources per user hasn't surpassed the limit. To resolve any related issues, you can manually remove the data sources from the admin center or, alternatively, use the following Gateway PowerShell script to find and bulk-delete any data sources that exceed the limit.

PowerShell

```
## https://learn.microsoft.com/powershell/module/datagateway/?
view=datagateway-ps
## PowerShell version of '7.0.0' to run
## required module "DataGateway" Install-Module -Name DataGateway and sign
in the same user who exceeded the 1000 limit
Connect-DataGatewayServiceAccount

## get the gateway information per the sign in person
$gatewayClusters = Get-DataGatewayCluster | where-Object {$_.Type -EQ
'Personal'};
foreach ($gw in $gatewayClusters)
{
  $datasources = Get-DataGatewayClusterDatasource -GatewayClusterId $gw.Id;
  foreach ($datasource in $datasources)
  {
    $datasource
    "gateway cluster id={0}, Personal Gateway={1}, datasource id={2},
datasourceType={3}, datasource connection details={4}" -f $gw.Id,
$datasource.OnPremGatewayRequired, $datasource.Id,
$datasource.DatasourceType, $datasource.ConnectionDetails

    ## conditional logic to determine if name matches set
    ## Remove-DataGatewayClusterDatasource -GatewayClusterId $gw.Id -
GatewayClusterDatasourceId $datasource.Id
  }
}
```

How do I avoid reaching this limit? If you're an ISV or any other Power BI Embedded app owner with many customers, use service principal profiles for multi-tenancy apps in Power BI embedded. If you're not an ISV, you might reach this limit because you're creating a new data source for every CSV or Excel file. To solve this, you might want to use the "upload file box" in Power BI Desktop to select multiple Excel files, which creates multiple data source connections. In this scenario, to ensure that only a single data source is selected, we recommend that you select the folder containing those Excel files instead.

Administration

Can I have more than one admin for a gateway?

Yes, when you manage a gateway, you can go to the administrator's tab to add more admins. You can also have security groups as admins.

Does the gateway admin need to be an admin on the machine where the gateway is installed?

No, the gateway admin manages the gateway from within the service.

Migration

If gateway migration fails, can gateway activity be continued from the old gateway server? Does this require any manual operation?

If the migration process fails on the new server, the on-premises data gateway still exists in the old server and you can still run that gateway unless the server is offline or the gateway software has been uninstalled. However, to restore the gateway on the old server, you might be asked to use your gateway recovery key.

How long does a complete on-premises data gateway migration take?

Since migration includes only two tasks, installing the gateway and restoration and configuration on new server, migration can usually be completed in 10 to 15 minutes.

If we assume that the whole migration process will take 5 minutes, for all the refreshes that occur in these 5 minutes, where will the traffic go? Will it go through the old gateway server before the migration completes?

Yes. However, there's a good chance of failures during this time, and migrations like these should be done in a downtime window. More information: Minimize migration downtime

Known Issues

Are there any known issues?

- If an OAuth refresh that takes longer that one hour is canceled with the error "Invalid Connection Credentials" or timeout, the issue is likely that the credential expired.

Next steps

- Troubleshoot the on-premises data gateway

Install an on-premises data gateway

Article • 06/06/2023

An on-premises data gateway is software that you install in an on-premises network. The gateway facilitates access to data in that network.

As we explain in the overview, you can install a gateway either in personal mode, which applies to Power BI only, or in standard mode. We recommend standard mode. In that mode, you can install a standalone gateway or add a gateway to a cluster, which we recommend for high availability.

In this article, we show you how to install a standard gateway, how to add another gateway to create a cluster, and how to install a personal mode gateway.

Requirements

Minimum requirements

- .NET Framework 4.7.2 (Gateway release December 2020 and earlier)
- .NET Framework 4.8 (Gateway release February 2021 and later)
- A 64-bit version of Windows 10 or a 64-bit version of Windows Server 2012 R2 with current TLS 1.2 and cipher suites
- 4-GB disk space for performance monitoring logs (in default configuration)

> **Note**
>
> The minimum screen resolution supported for the on-premises data gateway is 1280 x 800.

Recommended

- An 8-core CPU
- 8 GB of memory
- A 64-bit version of Windows Server 2012 R2 or later
- Solid-state drive (SSD) storage for spooling

Related considerations

- Gateways aren't supported on Server Core installations.

- Gateways aren't supported on Windows containers.
- The user installing the gateway must be the admin of the gateway.
- The gateway can't be installed on a domain controller.
- If you're planning to use Windows authentication, make sure you install the gateway on a computer that's a member of the same Active Directory environment as the data sources.
- Don't install a gateway on a computer, like a laptop, that might be turned off, asleep, or disconnected from the internet. The gateway can't run under any of those circumstances.
- If a gateway uses a wireless network, its performance might suffer. We recommend that you set the gateway on a wired device for best network performance.
- If you use a virtualization layer for your virtual machine, performance might suffer or perform inconsistently.
- You could install other applications on the gateway machine, but these applications might degrade gateway performance. If you do install other applications on the gateway machine, be sure to monitor the gateway closely to check if there's any resource contention.
- You can install up to two gateways on a single computer: one running in personal mode and the other running in standard mode. An on-premises data gateway (personal mode) can be used only with Power BI. You can't have more than one gateway running in the same mode on the same computer.
- The on-premises data gateway (standard mode) has to be installed on a domain joined machine having a trust relationship with the target domain.
- When private link is enabled, disable private link before installing the gateway. After installation, you can re-enable it. If private link is enabled, you'll get the following error when trying to register a new gateway or migrate/restore/takeover an existing gateway:

  `System.NullReferenceException: Object reference not set to an instance of an object`

  at Microsoft.PowerBI.DataMovement.GatewayCommon.DmtsGatewayCreation.UpdateGatewayConfiguration.

To disable private link, go to the powerbi.com page, and select **Settings** > **Admin portal**. Look for the **Advanced networking** section at the bottom of the page, and disable the **Azure Private Link** property. After the gateway is configured, you can enable the **Azure Private Link** property.

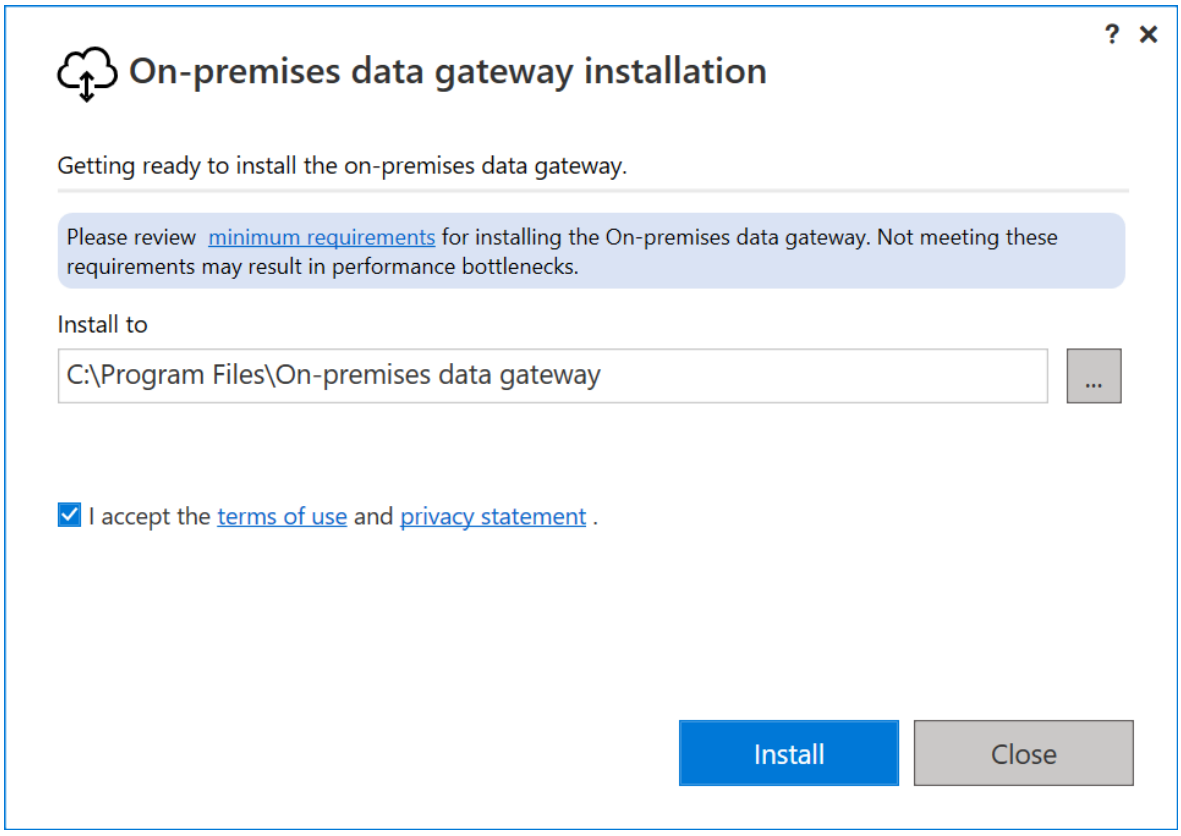
Download and install a standard gateway

Because the gateway runs on the computer that you install it on, be sure to install it on a computer that's always turned on. For better performance and reliability, we recommend that the computer is on a wired network rather than a wireless one.

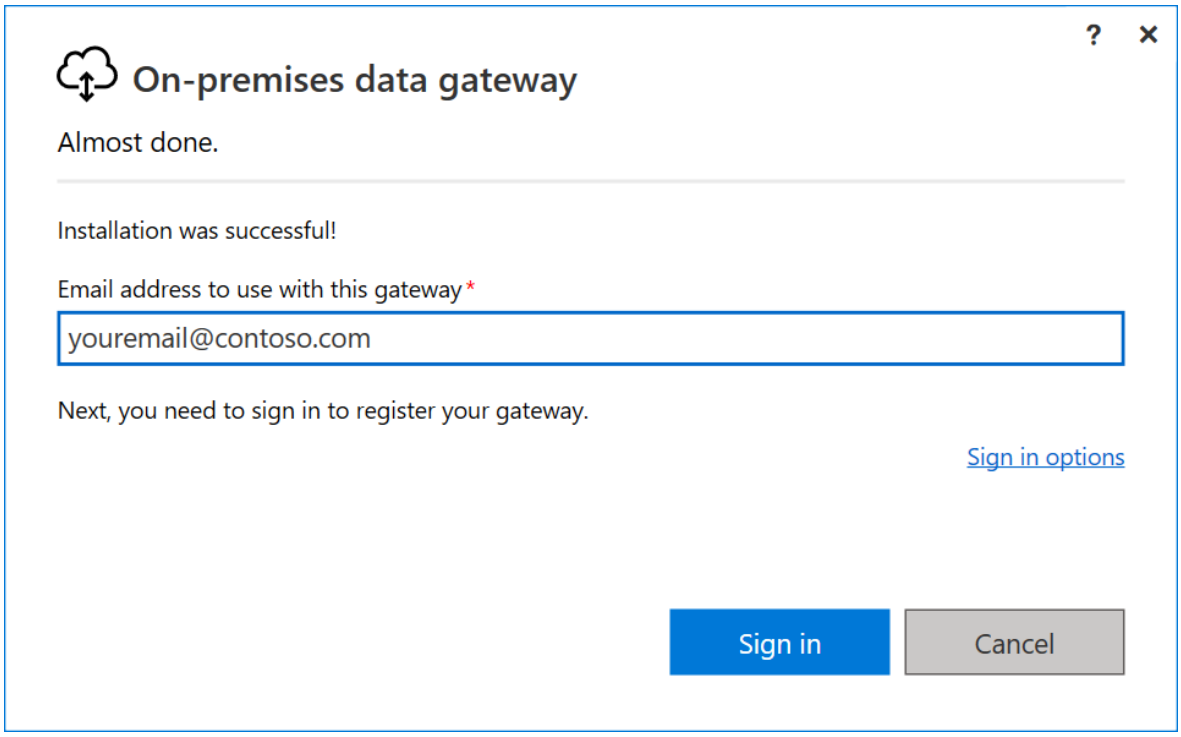
1. Download the standard gateway.

   > **Note**
   >
   > The on-premises data gateway (standard mode) has to be installed on a domain joined machine having a trust relationship with the target domain.

2. In the gateway installer, keep the default installation path, accept the terms of use, and then select **Install**.



3. Enter the email address for your Office 365 organization account, and then select **Sign in**.

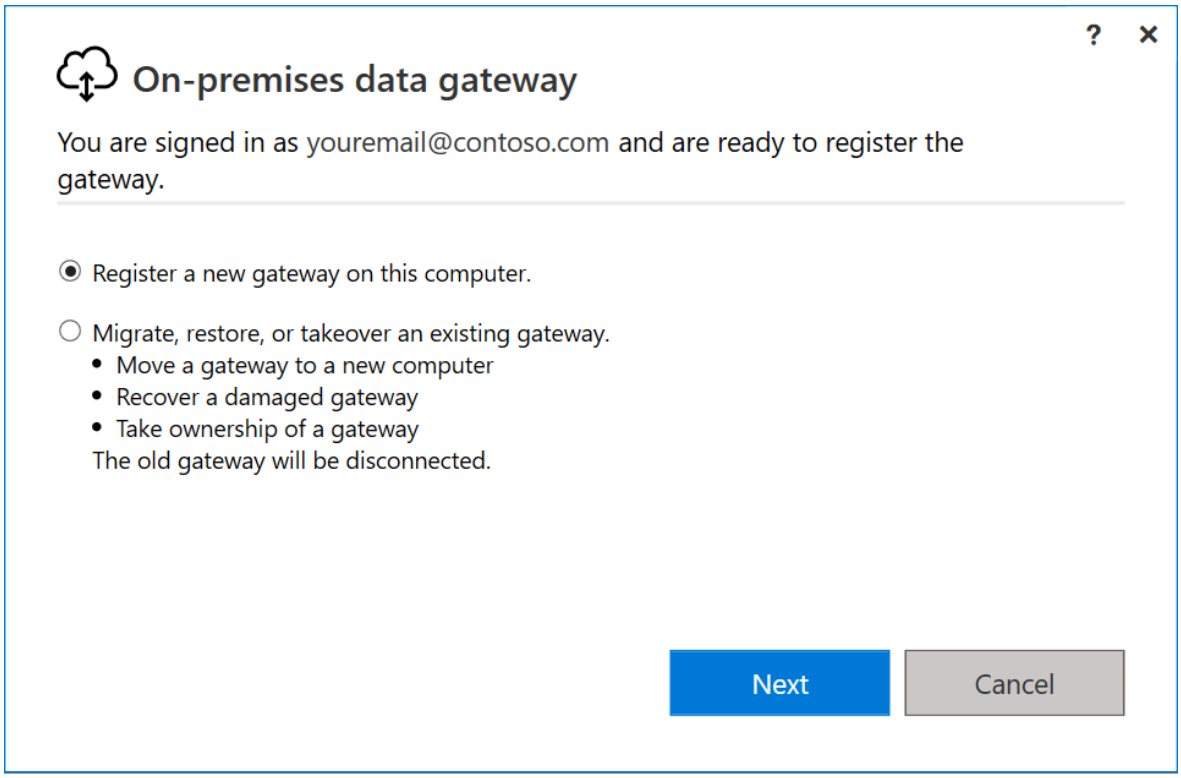


> **Note**
>
> You need to sign in with either a work account or a school account. This account is an *organization account*. If you signed up for an Office 365 offering and didn't supply your work email address, your address might look like nancy@contoso.onmicrosoft.com. Your account is stored within a tenant in Azure AD. In most cases, your Azure AD account's User Principal Name (UPN) will match the email address.

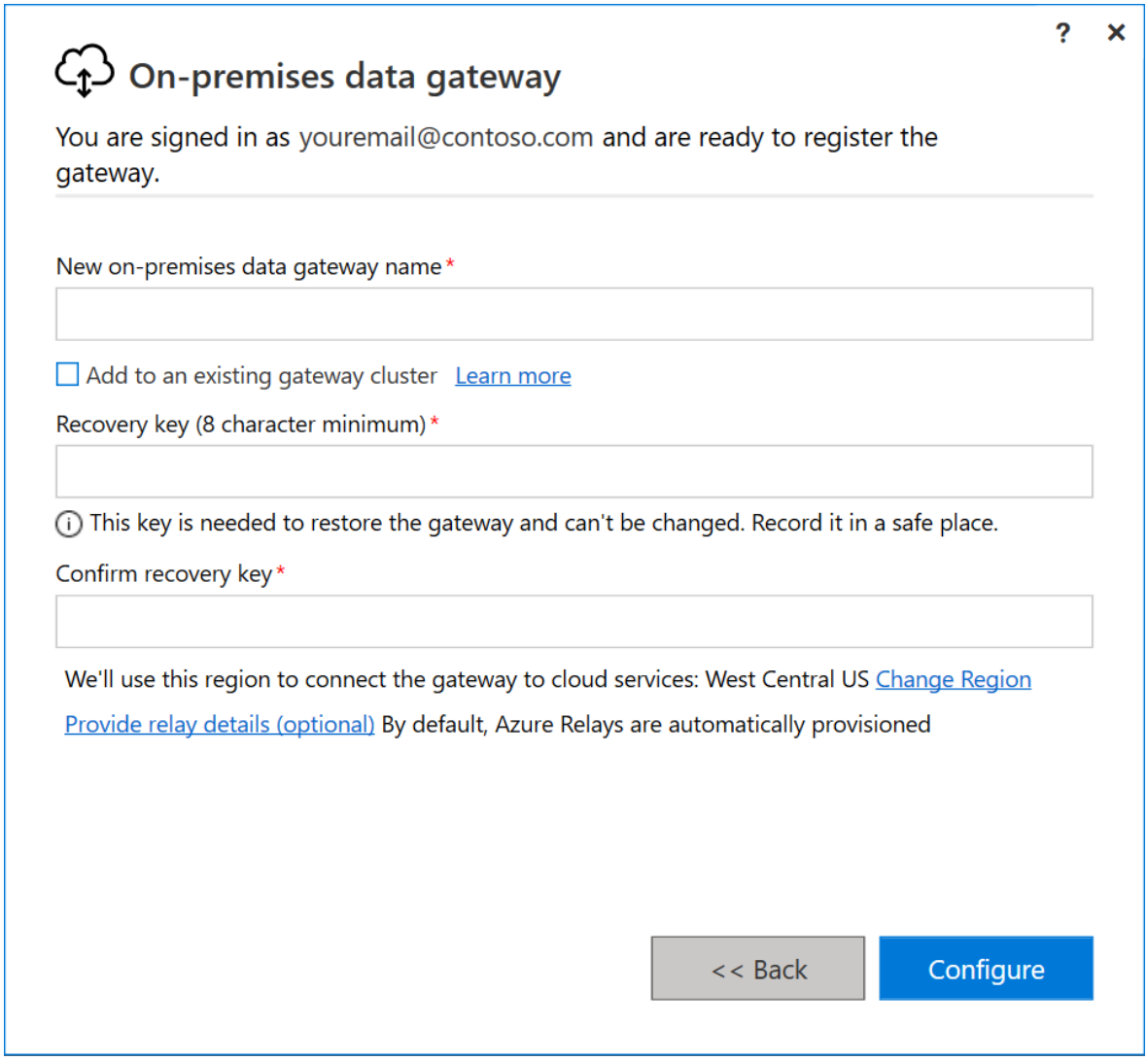
The gateway is associated with your Office 365 organization account. You manage gateways from within the associated service.

You're now signed in to your account.

4. Select **Register a new gateway on this computer** > **Next**.



5. Enter a name for the gateway. The name must be unique across the tenant. Also enter a recovery key. You'll need this key if you ever want to recover or move your gateway. Select **Configure**.



> **Important**
>
> You are responsible for keeping the gateway recovery key in a safe place where it can be retrieved later. Microsoft doesn't have access to this key and it can't be retrieved by us.

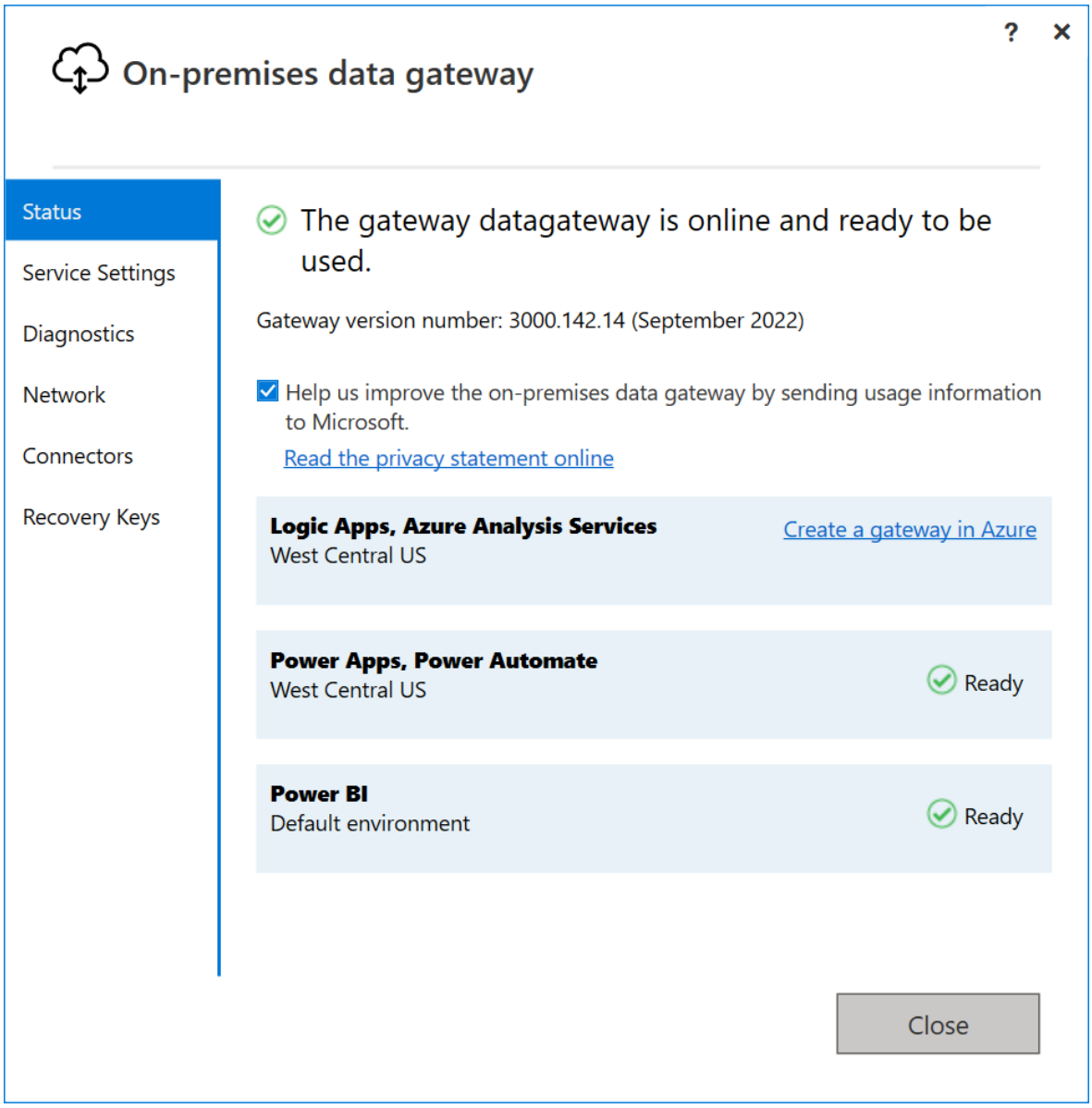
Note the **Add to an existing gateway cluster** checkbox. We'll use this checkbox in the next section of this article.

Also note that you can change the region that connects the gateway to cloud services. For more information, go to Set the data center region.

> **Note**
>
> For sovereign clouds, we currently only support installing gateways in the default PowerBI region of your tenant. The region picker on the installer is only supported for Public cloud.

Finally, you can also provide your own Azure Relay details. For more information about how to change the Azure Relay details, go to Set the Azure Relay for on-premises data gateway.

6. Review the information in the final window. Because this example uses the same account for Power BI, Power Apps, and Power Automate, the gateway is available for all three services. Select **Close**.



Now that you've installed a gateway, you can add another gateway to create a cluster.

Add another gateway to create a cluster

A cluster lets gateway admins avoid having a single point of failure for on-premises data access. If the primary gateway is unavailable, data requests are routed to the second gateway that you add, and so on.

Because you can install only one standard gateway on a computer, you must install each additional gateway in the cluster on a different computer. This requirement makes sense because you want redundancy in the cluster.

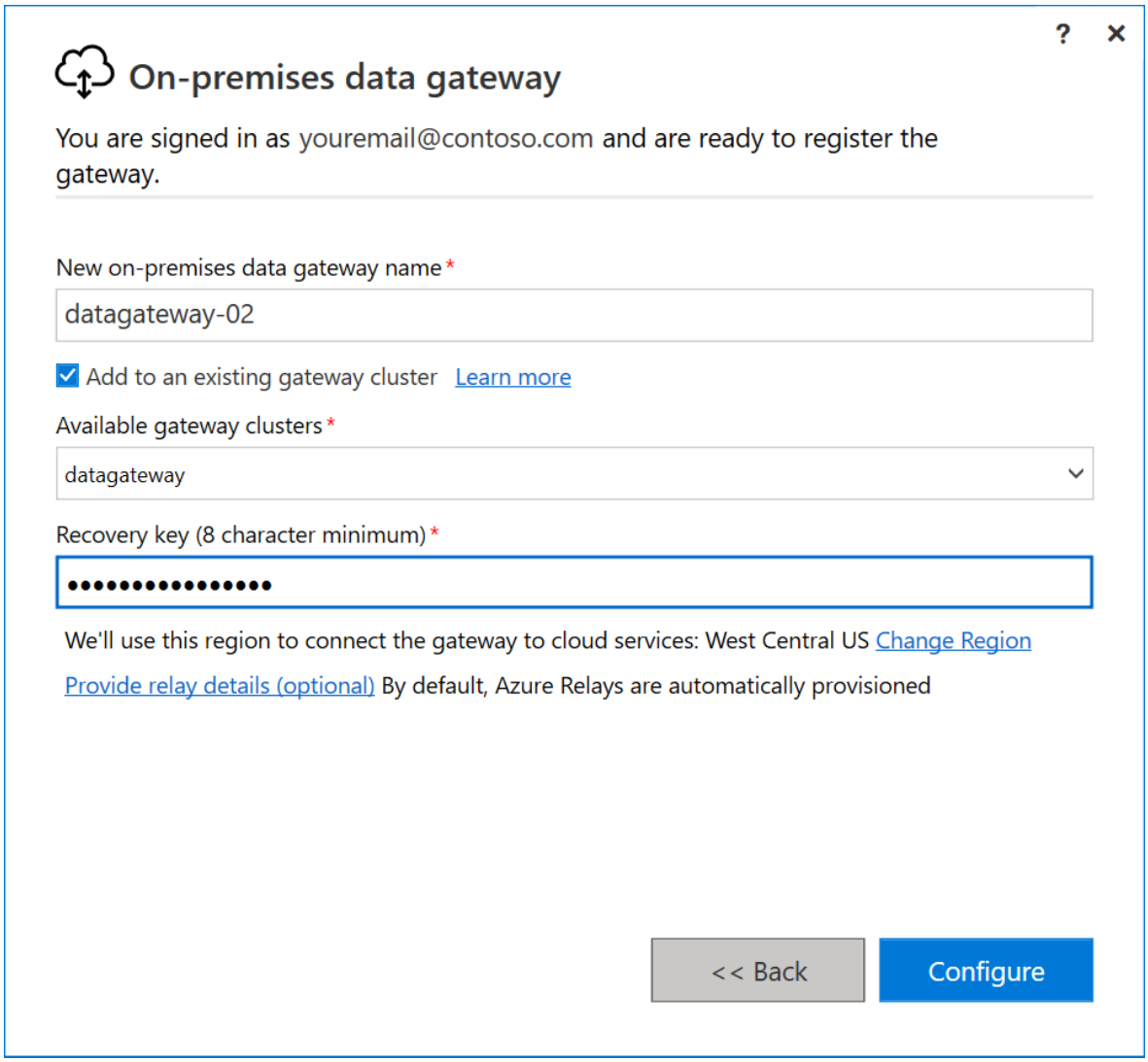
> ⓘ **Note**
>
> Offline gateway members within a cluster will negatively impact performance. These members should either be removed or disabled.

Make sure the gateway members in a cluster are running the same gateway version, as different versions could cause unexpected failures based on supported functionality.

To create high-availability gateway clusters, you need the November 2017 update or a later update to the gateway software.

1. Download the gateway to a different computer and install it.

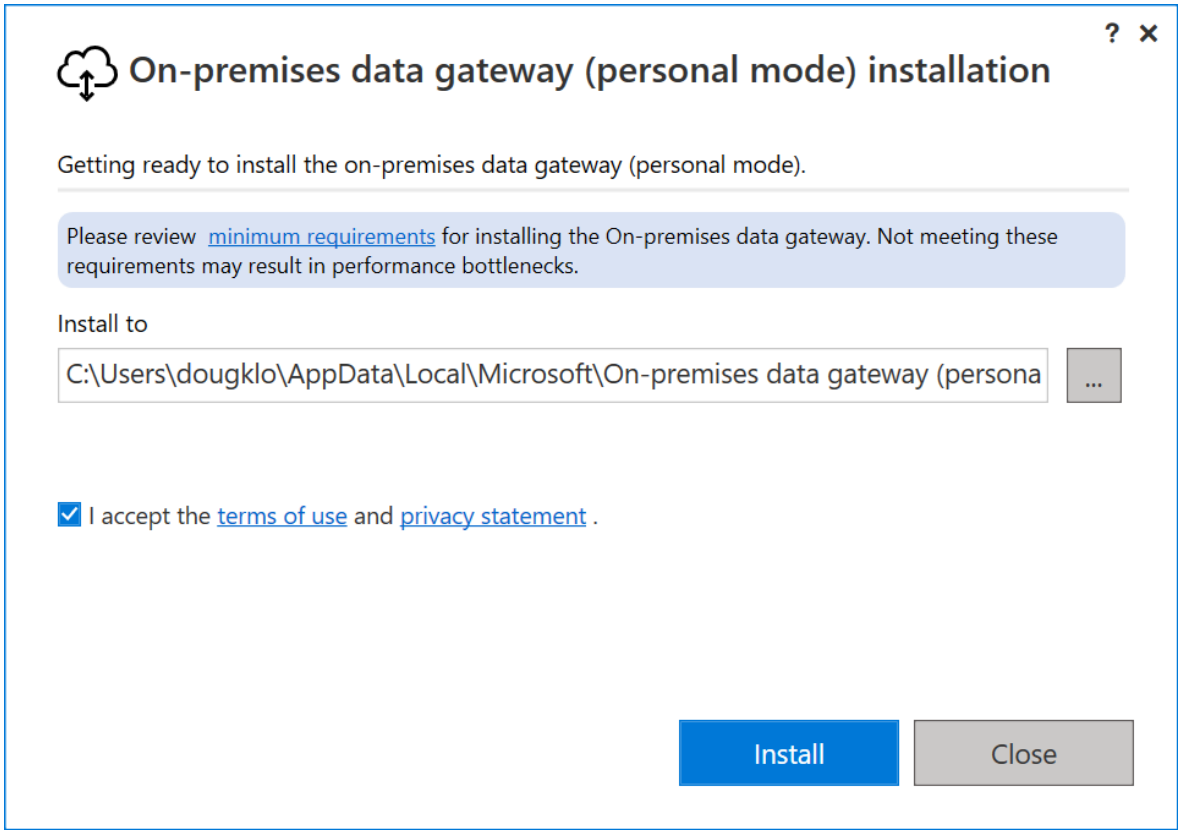
2. After you sign in to your Office 365 organization account, register the gateway. Select **Add to an existing cluster**. In the **Available gateway clusters** list, select the *primary gateway*, which is the first gateway you installed. Enter the recovery key for that gateway. Select **Configure**.



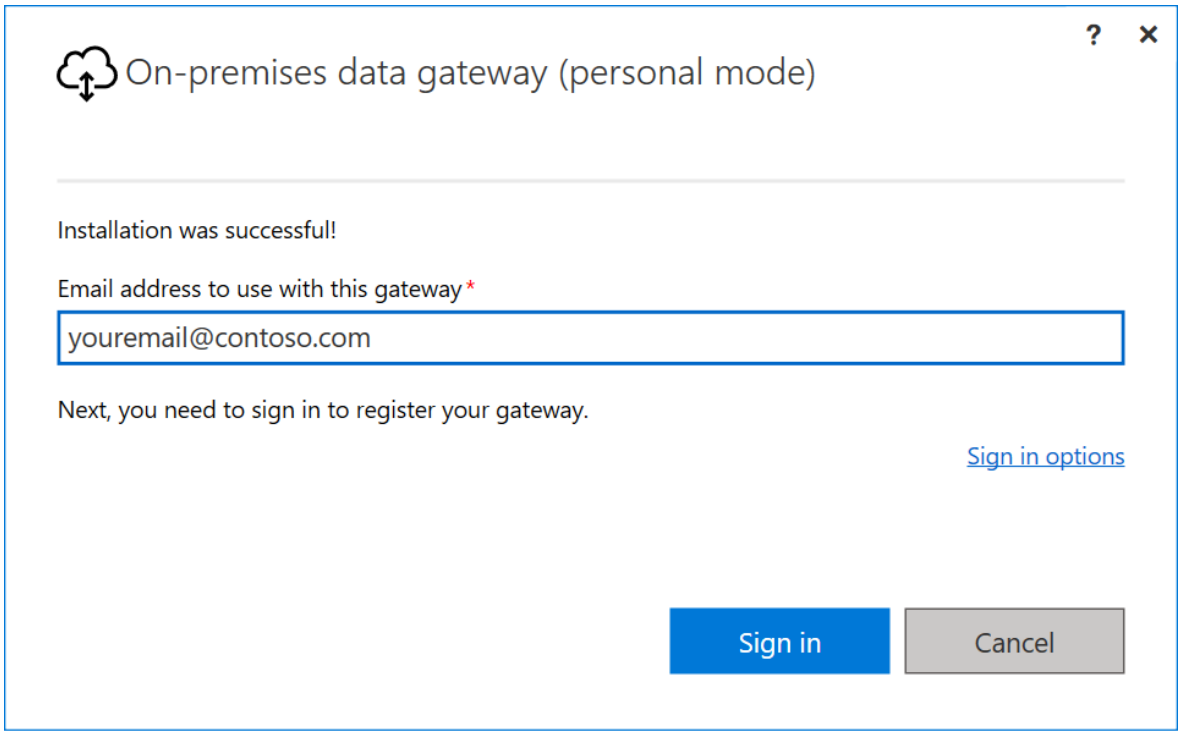
Download and install a personal mode gateway

1. Download the personal mode gateway.

2. In the gateway installer, enter the default installation path, accept the terms of use, and then select **Install**.



3. Enter the email address for your Office 365 organization account, and then select **Sign in**.

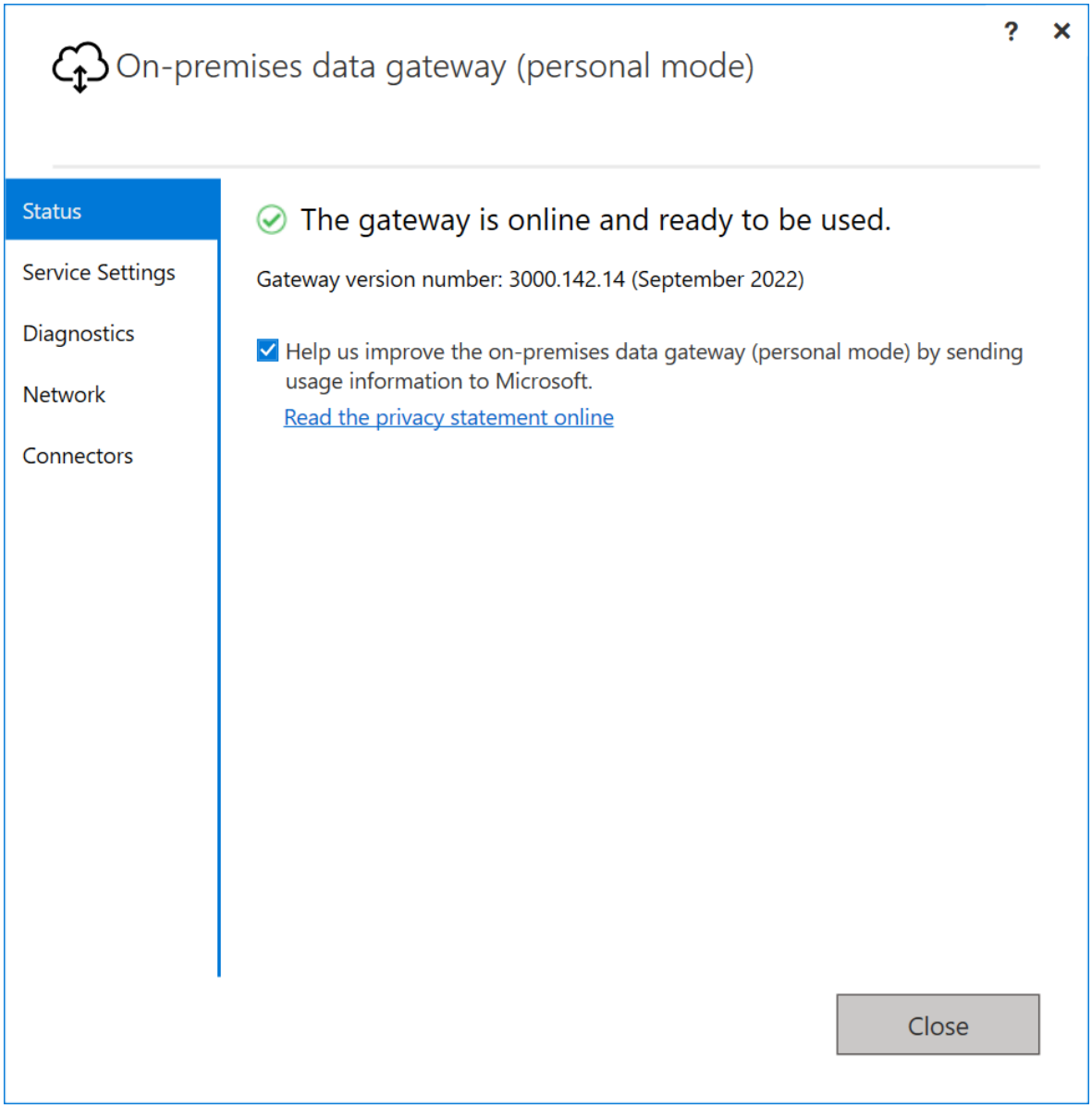


> ⓘ Note

You need to sign in with either a work account or a school account. This account is an *organization account*. If you signed up for an Office 365 offering and didn't supply your work email address, your address might look like nancy@contoso.onmicrosoft.com. Your account is stored within a tenant in Azure AD. In most cases, your Azure AD account's User Principal Name (UPN) will match the email address.

The gateway is associated with your Office 365 organization account. You manage gateways from within the associated service.

4. You're now signed in to your account. Select **Close**.



Next steps

- Configure on-premises data gateways
- Manage an on-premises data gateway

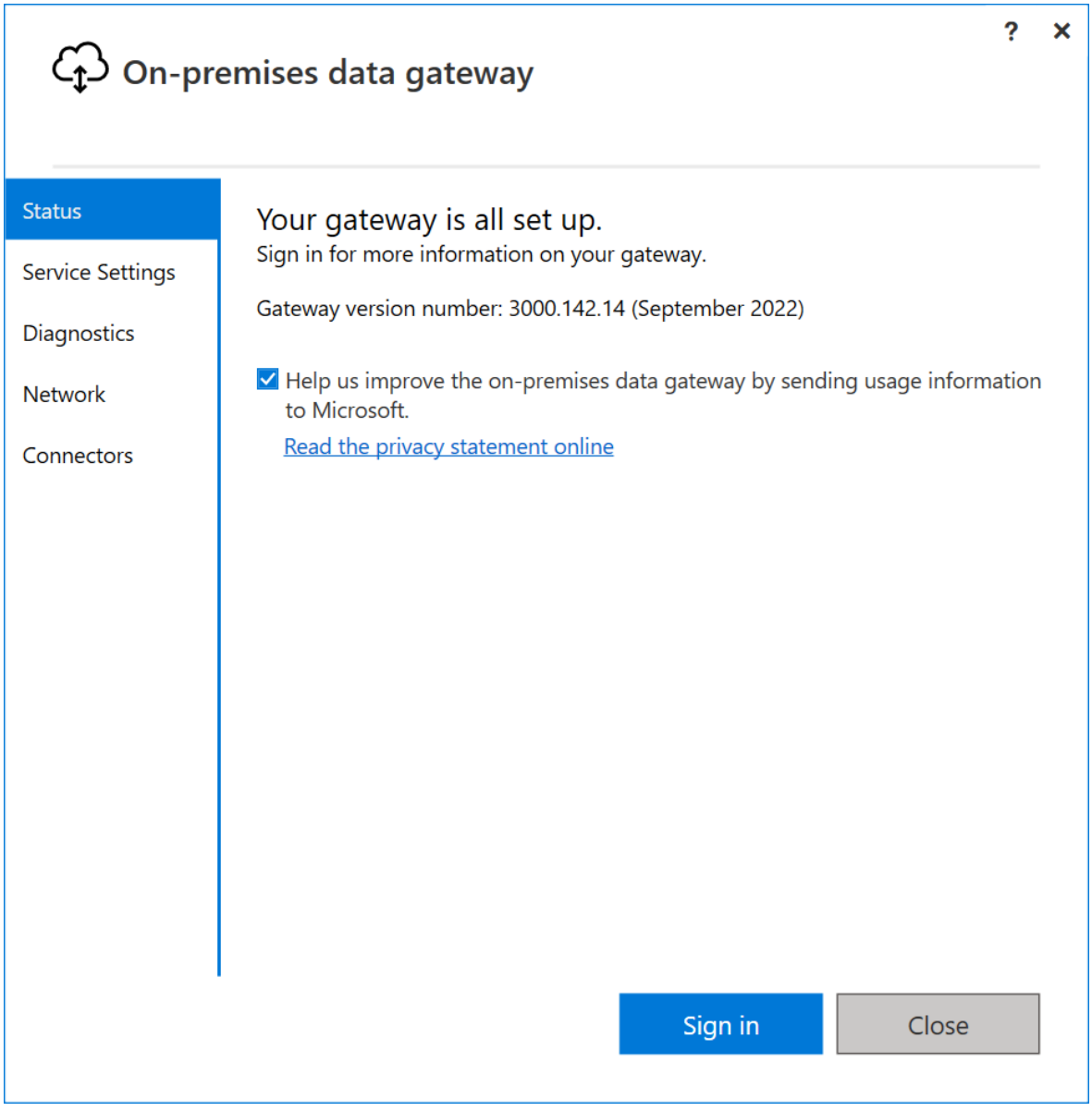
- Monitor and optimize gateway performance

Use the on-premises data gateway app

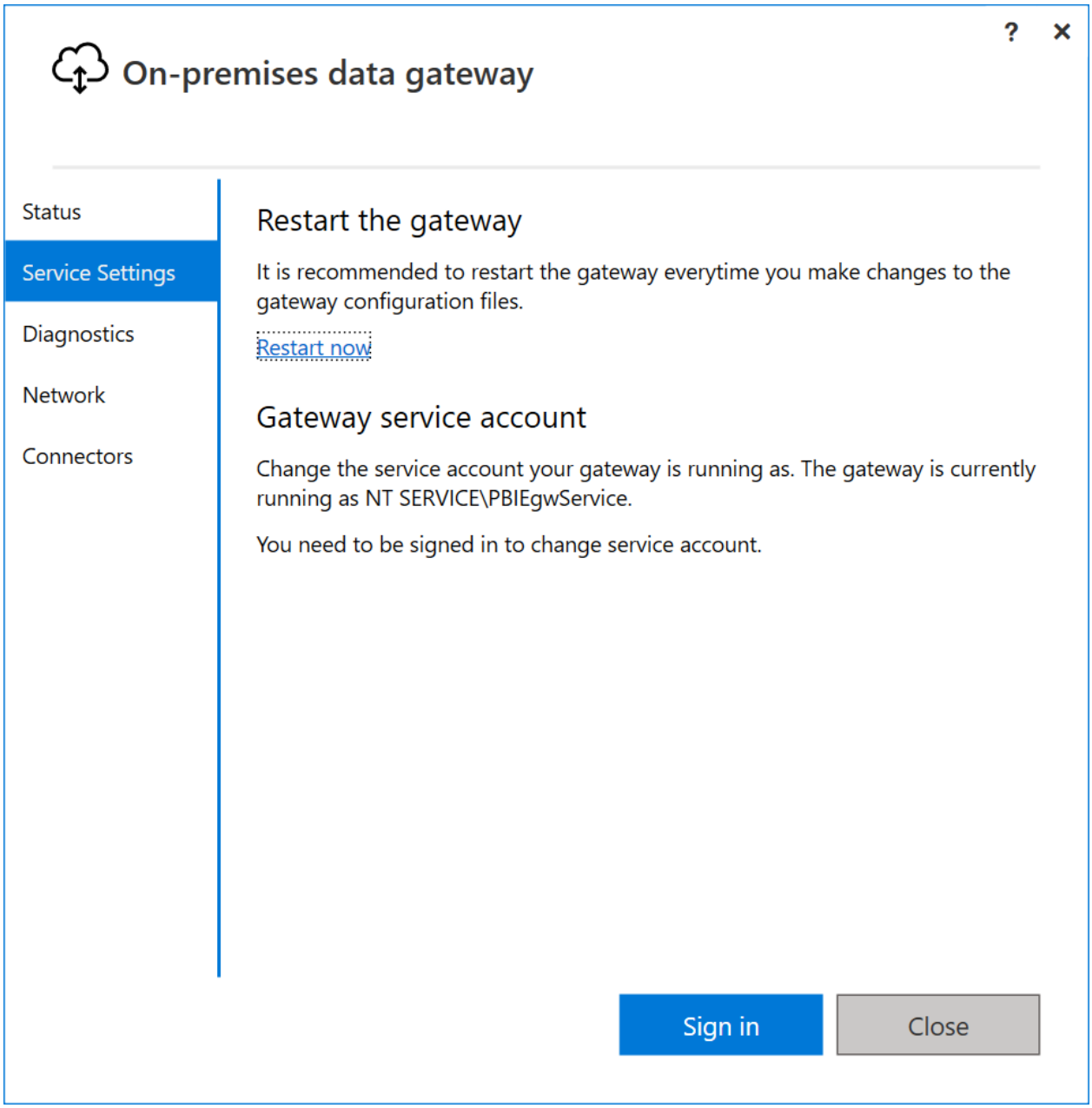
Article • 12/05/2022

To open the on-premises data gateway app:

1. On the machine where the gateway is running, enter **gateway** in Windows search.
2. Select the **On-premises data gateway** app.



Some of the on-premises data gateway app features can be used only after you sign in to your Office 365 account. For example, under the **Service Settings** tab, you can restart the gateway without signing in, but you can't change the service account of your gateway without signing in.



On-premises data gateway app features

After you sign in to your Office 365 account, you have access to the following features in the on-premises data gateway app.

Tab	Service	Description
Status	Status of the gateway cluster	Indicates whether your gateway is online, the version number of the gateway, and a list of any apps currently associated with the gateway.

Tab	Service	Description
Service Settings	Restart the gateway	Provides a way of restarting the gateway whenever a restart is needed.
Service Settings	Gateway service account	By default, the gateway is configured to use *NT SERVICE\PBIEgwService* for the Windows service sign-in credential. You can change the service account to a domain user account within your Active Directory domain. Or, you can use a managed service account to avoid having to change the password.
Diagnostics	Additional logging	Turning on this feature provides additional verbose information in the log file, which includes duration information. This information can be useful in figuring out why some responses through the gateway are slow. Enabling this feature could increase the log size significantly depending on gateway usage. So, we recommend that you don't leave this setting enabled long term.
Diagnostics	Gateway logs	Provides a copy of all of the gateway logs in a single file in .zip format.
Diagnostics	Network ports test	Checks if the gateway has access to all required ports.
Network	Network status	Indicates whether the gateway can reach outside your network. The network status is displayed as either Connected or Disconnected.
Network	HTTPS mode	Forces the gateway to communicate with Azure Relay by using HTTPS instead of TCP when turned on.
Connectors	Custom data connectors	You can connect to and access data from Power BI by using custom data connectors that you develop.
Recovery Keys	Recovery Keys	Changes the recovery key you specified when installing the on-premises data gateway. This feature doesn't appear until you've signed in. Not available in the on-premises data gateway (personal mode).

Next steps

- Troubleshoot the on-premises data gateway

Configure proxy settings for the on-premises data gateway

Article • 05/16/2023

Your work environment might require that you go through a proxy to access the internet. This requirement could prevent the Microsoft on-premises data gateway from connecting to the service.

The following post on superuser.com discusses how you can try to determine if you have a proxy on your network: How do I know what proxy server I'm using? (SuperUser.com) .

Although most gateway configuration settings can be changed by using the on-premises data gateway app, proxy information is configured within a .NET configuration file. The location and file names are different, depending on the gateway you're using.

There are three configuration files associated with using a proxy with the on-premises data gateway. The following two main configuration files apply to the gateway and its configuration process.

- The first file is for the configuration screens that actually configure the gateway. If you're having issues configuring the gateway, look at the following file: *C:\Program Files\On-premises data gateway\enterprisegatewayconfigurator.exe.config*. On the on-premises data gateway (personal mode), the corresponding file is *%LocalAppData%\Microsoft\On-premises data gateway (personal mode)\PersonalGatewayConfigurator.exe.config*.
- The second file is for the actual Windows service that interacts with the cloud service using the gateway. This file handles the requests: *C:\Program Files\On-premises data gateway\Microsoft.PowerBI.EnterpriseGateway.exe.config*. On the on-premises data gateway (personal mode), the corresponding file is *%LocalAppData%\Microsoft\On-premises data gateway (personal mode)\Microsoft.PowerBI.DataMovement.PersonalGateway.exe.config*.

If you're going to make changes to the proxy configuration, these files must be edited so that proxy configurations are exactly the same in both files.

The third configuration file will need to be edited for the gateway to connect to cloud data sources through a proxy.

- *C:\Program Files\On-premises data gateway\m\Microsoft.Mashup.Container.NetFX45.exe.config*

On the on-premises data gateway (personal mode), the corresponding file is *%LocalAppData%\Microsoft\On-premises data gateway (personal mode)\m\Microsoft.Mashup.Container.NetFX45.exe.config*.

The following section describes how to edit these files.

Configure proxy settings

The following sample shows the default proxy configuration found in both of the two main configuration files.

XML

```xml
<system.net>
    <defaultProxy useDefaultCredentials="true" />
</system.net>
```

The default configuration works with Windows authentication. If your proxy uses another form of authentication, you must change the settings. If you aren't sure, contact your network administrator.

We don't recommend basic proxy authentication. Using basic proxy authentication might cause proxy authentication errors that result in the gateway not being properly configured. Use a stronger proxy authentication mechanism to resolve.

In addition to using default credentials, you can add a `<proxy>` element to define proxy server settings in more detail. For example, you can specify that your on-premises data gateway should always use the proxy, even for local resources, by setting the *bypassonlocal* parameter to false. This setting can help in troubleshooting situations in order to track all HTTPS requests that originate from a gateway in the proxy log files. The following sample configuration specifies that all requests must go through a specific proxy with the IP address 192.168.1.10.

XML

```xml
<system.net>
    <defaultProxy useDefaultCredentials="true">
        <proxy
            autoDetect="false"
            proxyaddress="http://192.168.1.10:3128"
            bypassonlocal="false"
            usesystemdefault="true"
        />
    </defaultProxy>
</system.net>
```

You'll also need to edit the *Microsoft.Mashup.Container.NetFX45.exe.config* file if you want the gateway to connect to cloud data sources through a gateway.

In the file, expand the `<configurations>` section to include the following contents, and update the `proxyaddress` attribute with your proxy information. The following example routes all cloud requests through a specific proxy with the IP address 192.168.1.10.

XML

```
<configuration>
    <system.net>
        <defaultProxy useDefaultCredentials="true" enabled="true">
        <proxy proxyaddress="http://192.168.1.10:3128" bypassonlocal="true"
/>
        </defaultProxy>
    </system.net>
</configuration>
```

Configuring this third file might be necessary if your proxy is a requirement for all internet communication, especially for corporate usage where networks are secure and locked-down. If a proxy is required for gateway communication, it's likely also needed for any internet traffic from containers. In this case, the gateway might appear to be operating successfully until any container makes any external (internet) query. This issue is especially applicable to dataflows, which attempt to push the resulting query of on-premises data to Azure Data Lake Storage. But it also applies when a gateway query merges an on-premises dataset with an internet-bound dataset.

To learn more about the configuration of the proxy elements for .NET configuration files, go to defaultProxy Element (Network settings).

Change the gateway service account to a domain user

As explained earlier, when you configure the proxy settings to use default credentials, you might come across authentication issues with your proxy. This situation occurs when the default service account is the Service SID, and not an authenticated domain user. If the proxy on your organization requires a domain account in order to authenticate the request, you can change the service account of the gateway to a domain service account to allow the proper authentication with your proxy. For more information about how to change the gateway service account, go to Change the on-premises data gateway service account.

> **Note**
>
> We recommend that you use a managed service account to avoid having to reset passwords. Learn how to create a **managed service account** within Active Directory.

Next steps

- Step by step guide on configuring your proxy settings
- Firewall information

Step by step guide on configuring your proxy settings

Article • 12/02/2022

If your work environment requires Microsoft on-premises data gateway to go through a Proxy Server for connecting to the service, follow the steps below in order to configure the proxy settings.

Configure proxy settings

1. Create your proxy definition element. To learn more about the configuration of the proxy elements for .NET configuration files, go to defaultProxy Element (Network settings).

   The following example routes all requests through a specific proxy with the IP address 192.168.0.1 on port 8888:

   XML

   ```
   <defaultProxy useDefaultCredentials="true">
       <proxy
           autoDetect="false"
           proxyaddress="http://192.168.0.1:8888"
           bypassonlocal="false"
           usesystemdefault="false"
       />
   </defaultProxy>
   ```

2. Browse the installation folder for the on-premises data gateway, for example, *C:\Program Files\On-premises data gateway*.

3. Open the first file that's used for the configuration screens that configure the gateway, that is, *EnterpriseGatewayConfigurator.exe.config*.

4. Locate the `defaultProxy` element and replace it with your proxy configuration created in the step 1 above, and then save your changes to the file.

5. Open the second file that's used for the actual Windows service that interacts with the cloud service using the gateway and handles the requests, that is, *Microsoft.PowerBI.EnterpriseGateway.exe.config* and repeat step 4.

6. For the third configuration file that's used for the gateway to connect to the data sources—typically cloud data sources—open the subfolder *m* in the installation folder and then the file *Microsoft.Mashup.Container.NetFX45.exe.config*. Repeat step 4 to insert the proxy configuration into this file.

   If the file is in the default state, you'll need to add the `system.net` tag, together with the proxy definition, as in the following example:

   XML

   ```
   <system.net>
       <defaultProxy useDefaultCredentials="true">
           <proxy
               autoDetect="false"
               proxyaddress="http://192.168.0.1:8888"
               bypassonlocal="false"
               usesystemdefault="false"
           />
       </defaultProxy>
   </system.net>
   ```

7. Open the on-premises data gateway application, navigate to **Service Settings** tab and select **Restart now** to restart the Gateway service and apply the new proxy settings.

Verify consistent proxy configuration

1. Ensure you're running September 2022 version or higher.
2. Open the on-premises data gateway application.
3. Navigate to **Diagnostics** tab.
4. Under **Network ports test**, select **Start new test**.
5. Once the network ports test is complete, select **Open last completed test results**.
6. If your proxy configuration is consistent across the three required configuration files, a `Proxy configuration : Proxy settings match for all Gateway process configurations.` message is displayed.
7. Otherwise, if the proxy configuration isn't consistent, the following information is displayed:

   ```
   ```

```
Proxy configuration : Proxy settings are not consistent. Please ensure
that the proxy configuration matches across the files listed below:
C:\Program Files\On-premises data
gateway\EnterpriseGatewayConfigurator.exe.config
C:\Program Files\On-premises data
gateway\Microsoft.PowerBI.EnterpriseGateway.exe.config
C:\Program Files\On-premises data
gateway\m\Microsoft.Mashup.Container.NetFX45.exe.config
Review <https://docs.microsoft.com/data-integration/gateway/service-
gateway-proxy>  for additional information about configuring proxies
for the Gateway.
```

Inconsistent or missing proxy configuration behaviors

If the proxy definition is either missing or inconsistent, you can experience different behaviors with your on-premises data gateway. A few examples are:

- A dataset or dataflow refresh failure, error message example: `Error: Unable to connect to the remote server`.
- While launching on premises data gateway, you fail to sign in, the sign-in prompt appears but its content can't be displayed, or an error message page is displayed.
- The Network Port test results report failures connecting to the servers.

Next steps

https://www.microsoft.com/en-us/videoplayer/embed/RE5cv1m?postJsllMsg=true

- Firewall information

Change the on-premises data gateway service account

Article • 12/02/2022

The on-premises data gateway is configured to use *NT SERVICE\PBIEgwService* for the Windows service sign-in credential. In the context of the machine on which you install the gateway, the account by default has the right of Log on as a service.

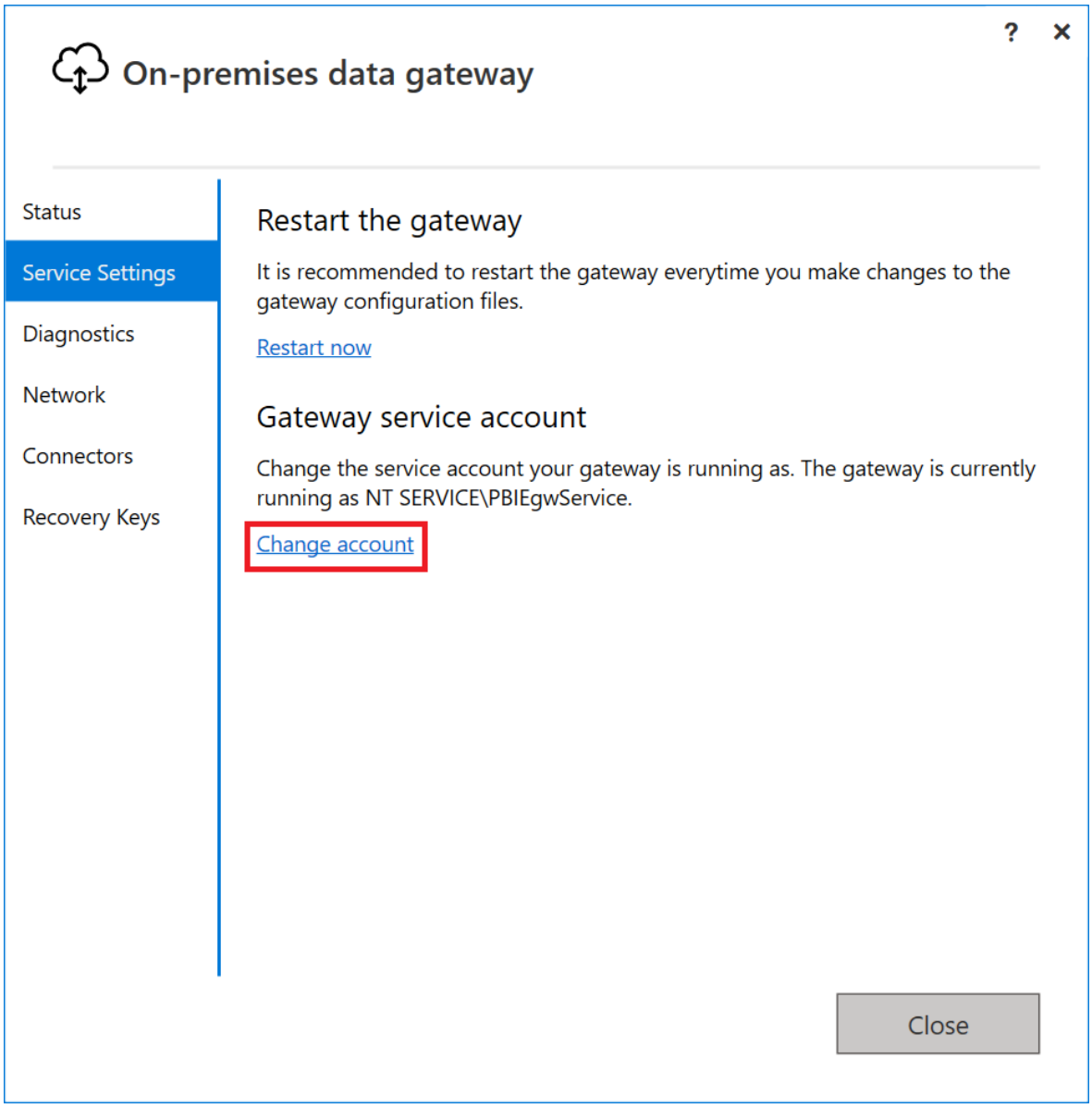
This service account isn't the account used to connect to on-premises data sources. It also isn't the work or school account that you sign in to cloud services with.

Change the service account

To change the Windows service account for the on-premises data gateway:

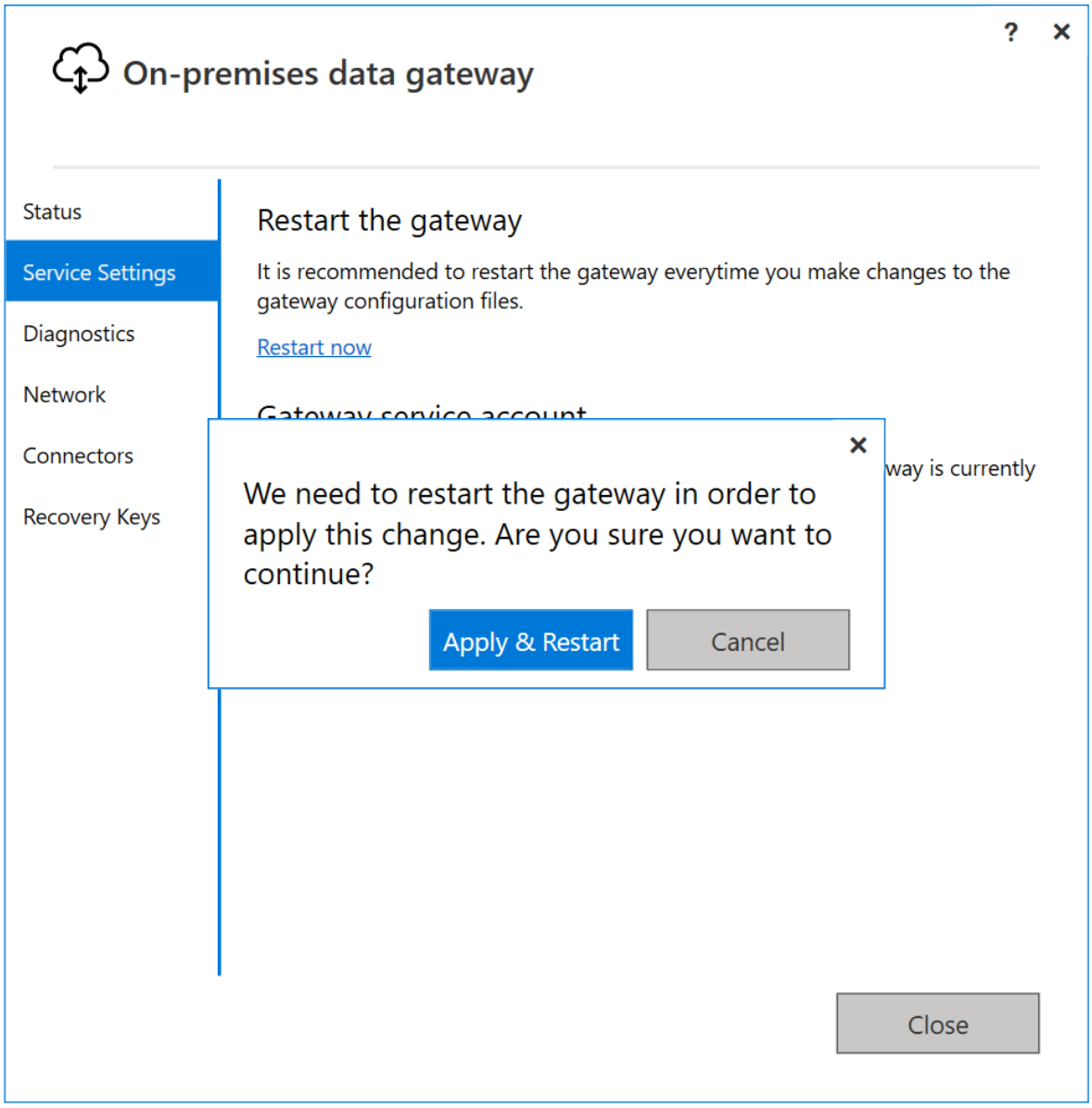
1. Open the on-premises data gateway app, select **Service settings**, and then select **Change account**.

   > **Note**
   >
   > We recommend using the on-premises data gateway app to change the service account instead of the Windows Service app. This will ensure that the new account has all the required privileges. Not using the on-premises data gateway app for this purpose could lead to inconsistent logging and other issues.

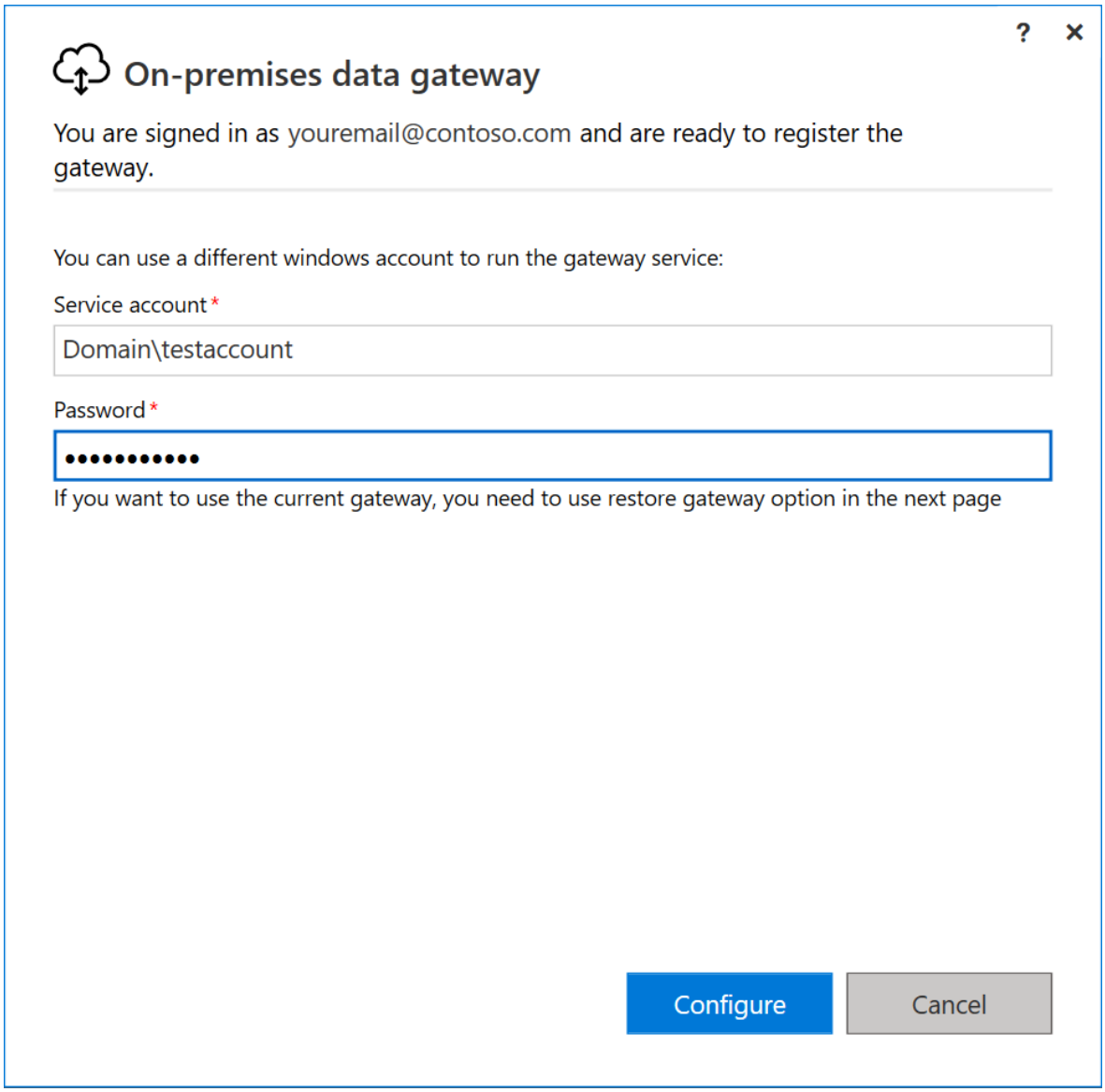


The default account for this service is *NT SERVICE\PBIEgwService*. Change this account to a domain user account within your Windows Server Active Directory domain, or use a managed service account to avoid having to change the password.

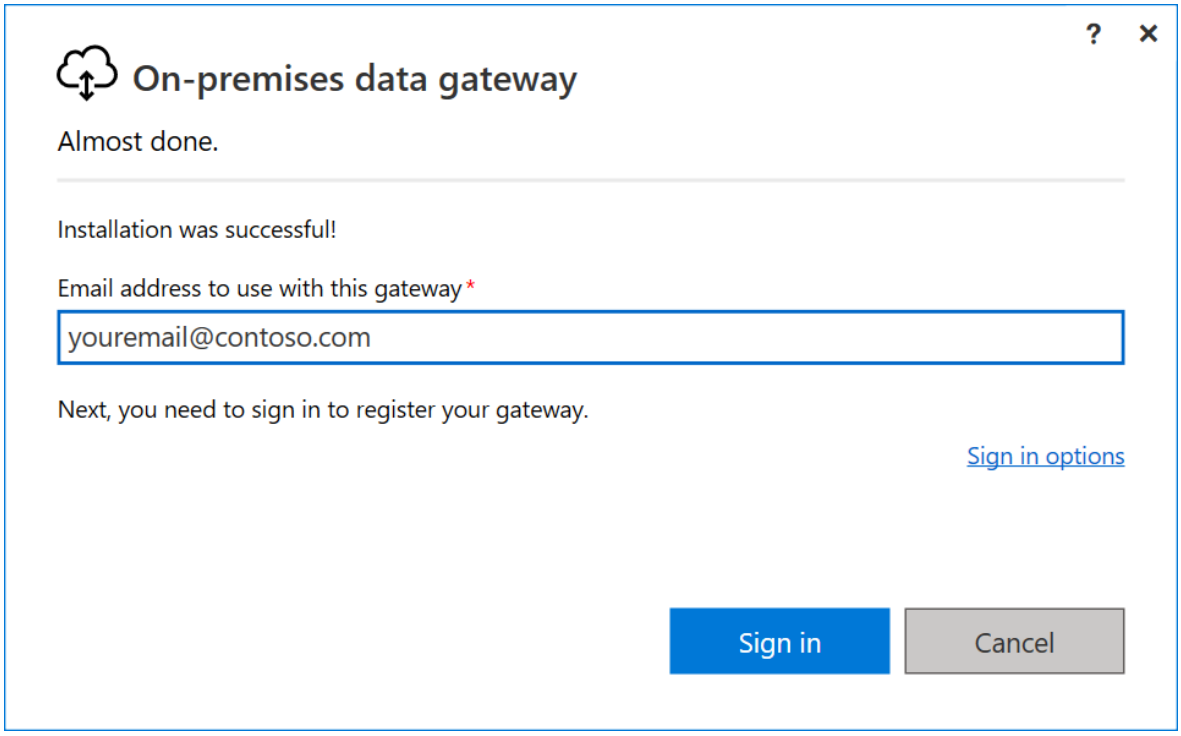
2. Select **Change account**. You need the recovery key to change the service account.



3. Provide the service account and password, and select **Configure**.

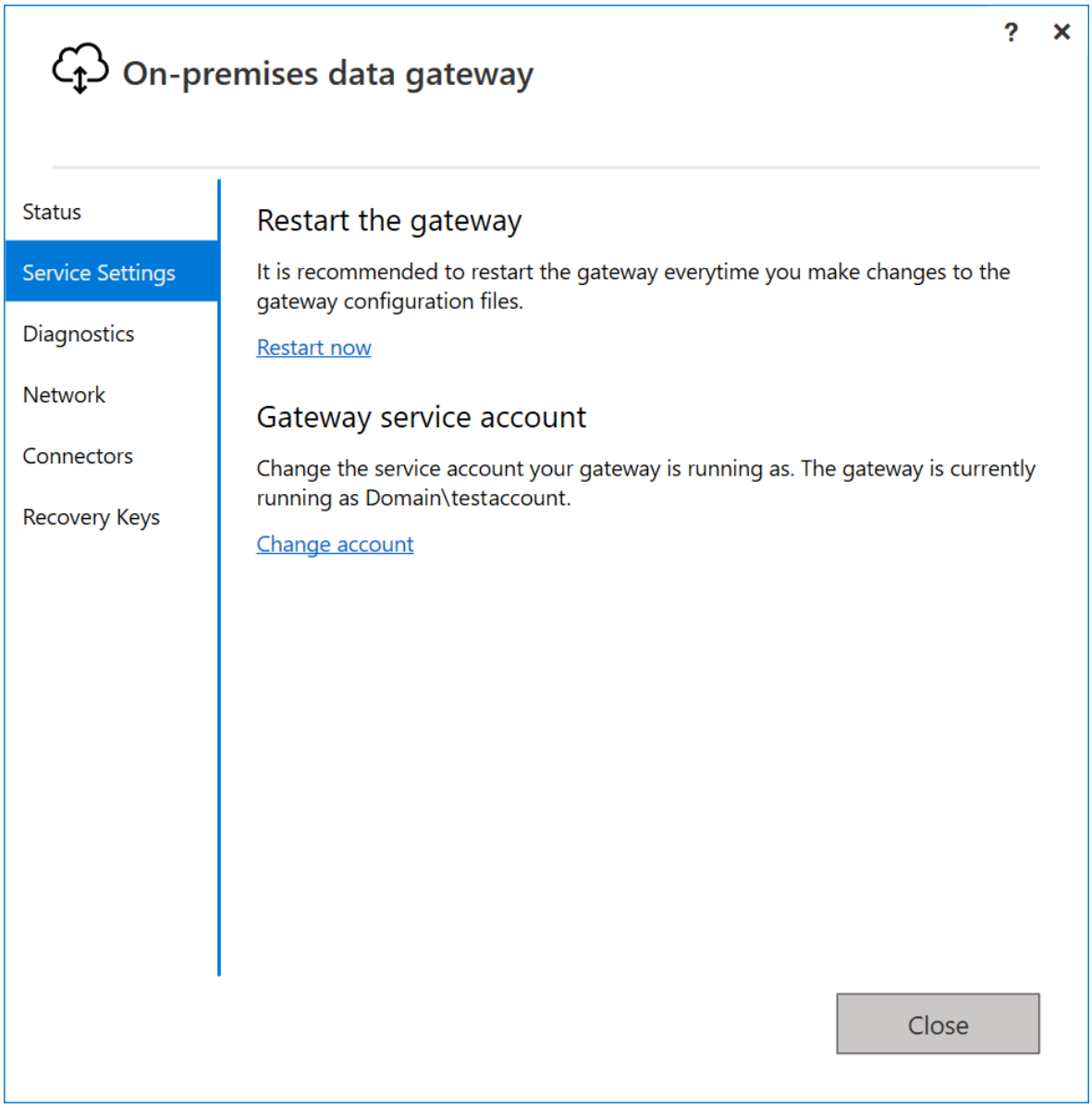


4. Provide your sign-in account, and select **Sign in**.



5. On the next windows, select **Migrate, restore or takeover an existing gateway**, and follow the process for restoring your gateway.

6. After the restoration is complete, the new gateway uses the domain account.



> **Note**
>
> To reset the gateway to the default service account, you need to uninstall and reinstall the gateway. You need the recovery key for this operation.

Next steps

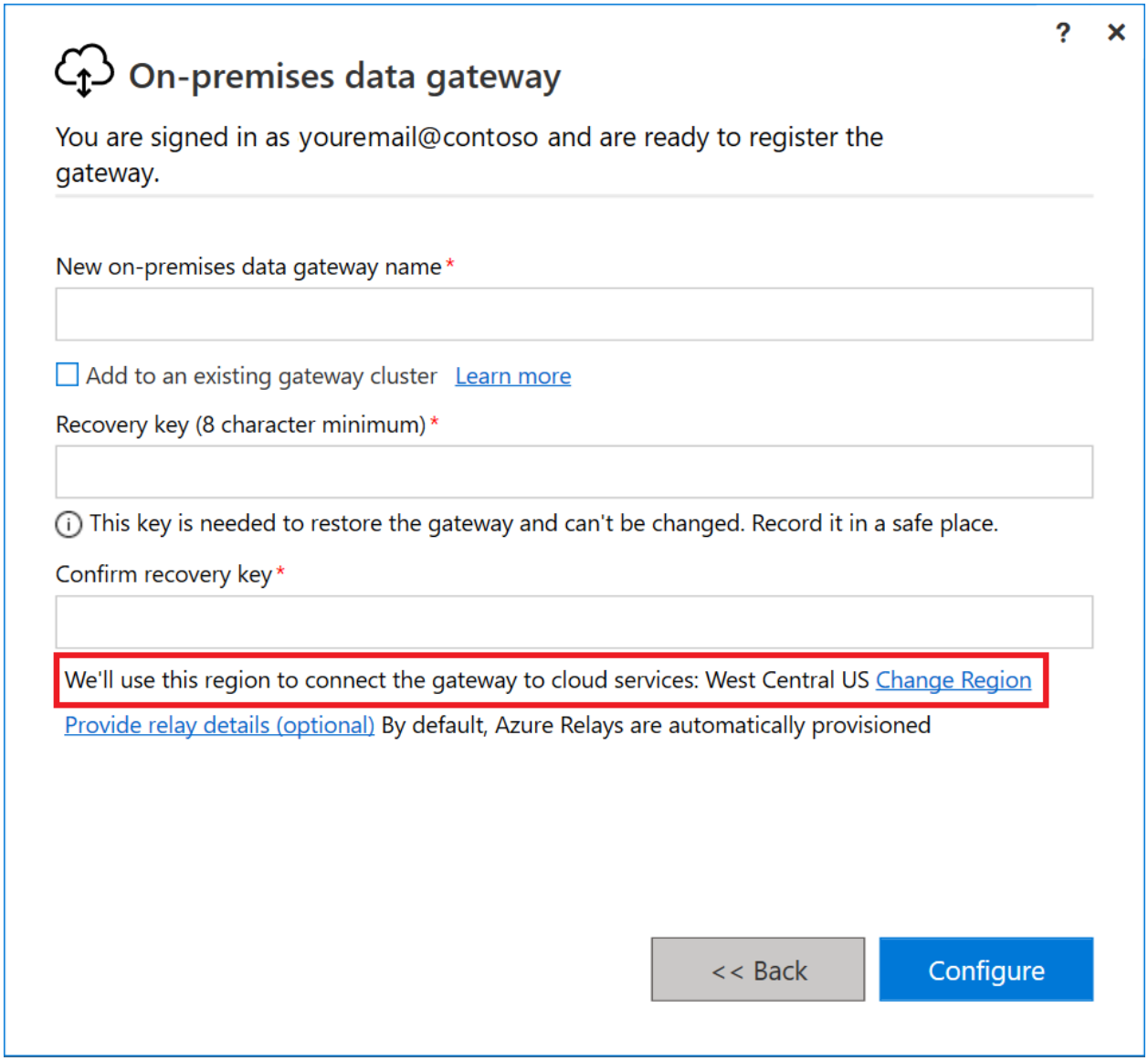
- Set the datacenter region

Set the datacenter region for the on-premises data gateway

Article • 12/02/2022

During installation of the on-premises data gateway, you can set the datacenter region used by the gateway.

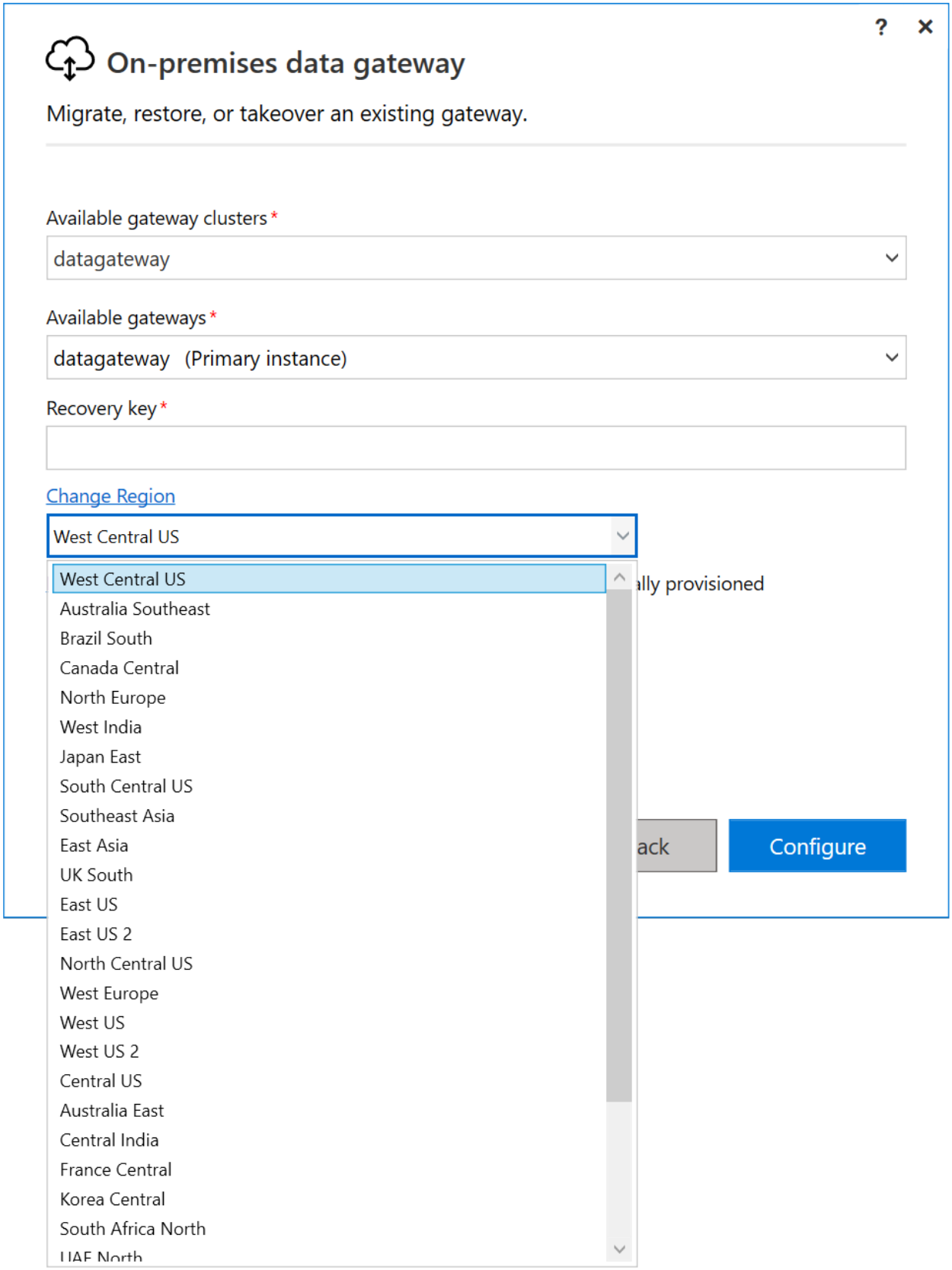
If you've registered for either Power BI or Office 365, the datacenter region by default is the region of the registered service's tenant. Otherwise, the datacenter region might be the Azure region closest to you.



> **Note**
>
> For sovereign clouds, we currently only support installing gateways in the default PowerBI region of your tenant. The region picker on the installer is only supported for Public cloud.

Restore, migrate, or take over a gateway in a non-default region

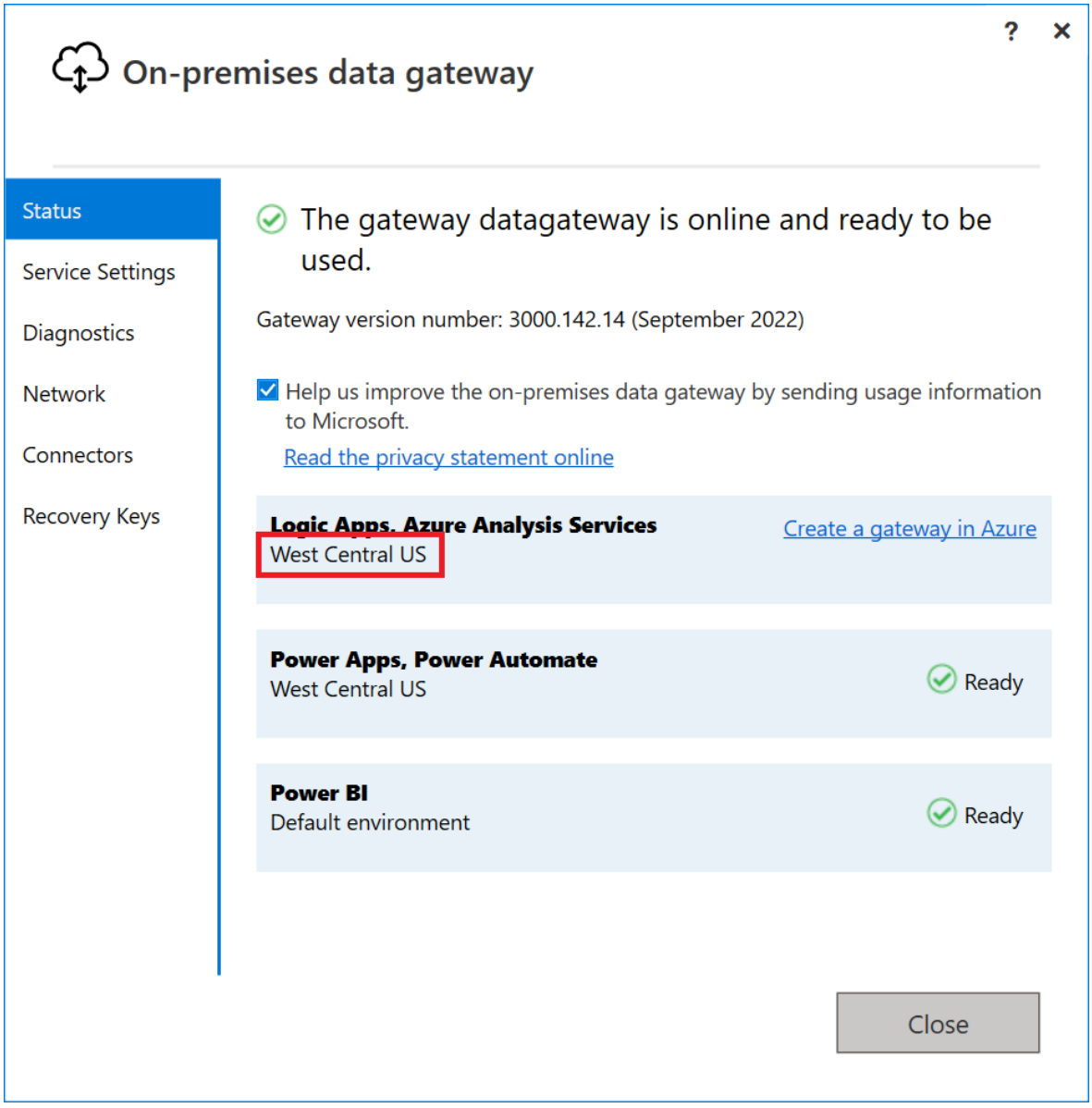
If you want to restore, migrate, or take over a gateway in a non-default Power BI region:



Current datacenter region

To find the current datacenter region after you install the gateway:

1. Open the on-premises data gateway app and sign in to your account.
2. In the **Status** tab, your datacenter region appears under **Logic Apps, Azure Analysis Services**.



For more information about setting the datacenter region for your resources, watch this video.

Next steps

- Adjust communications settings

Set the Azure Relay for on-premises data gateway

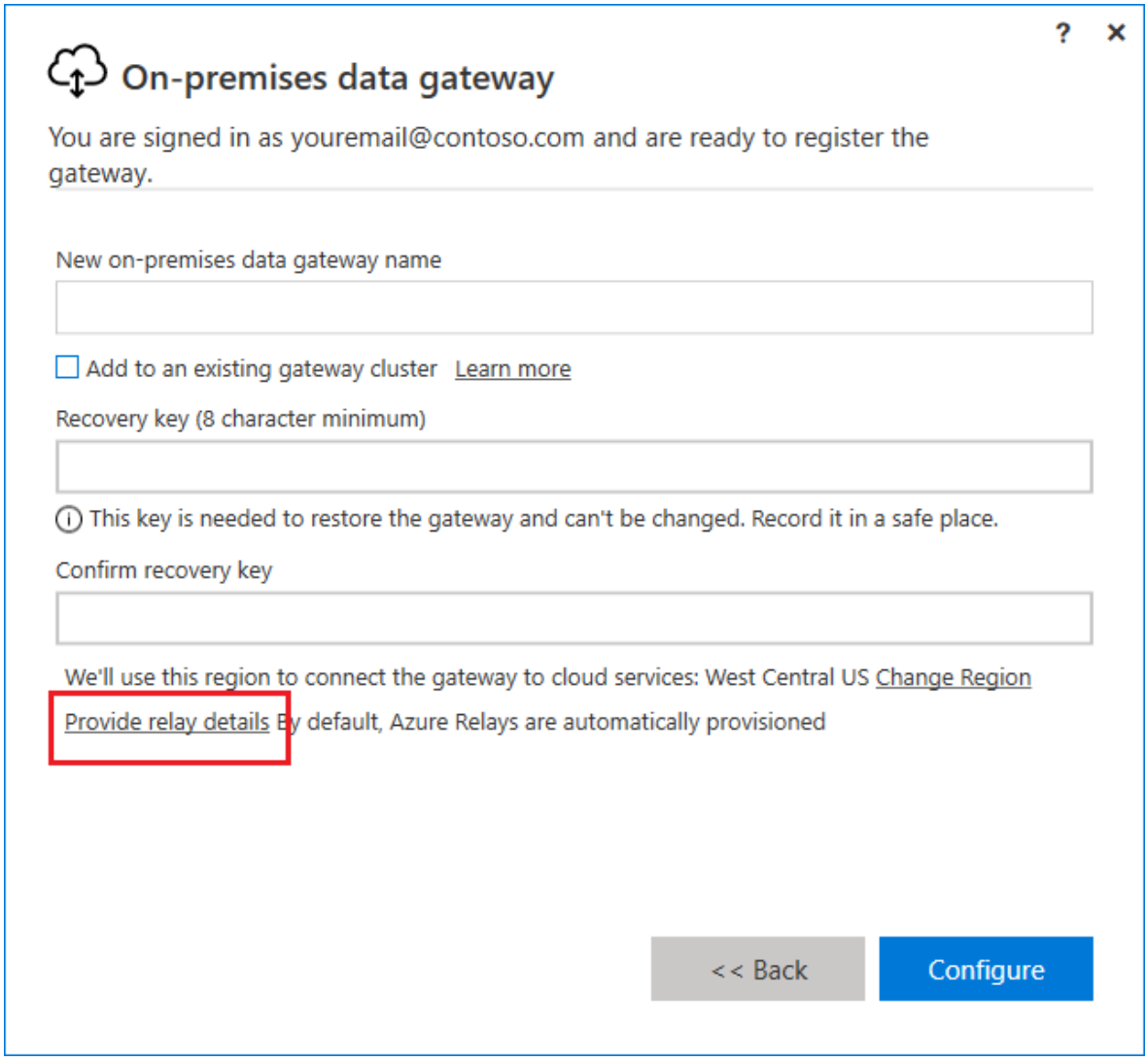
Article • 05/02/2023

During installation of the on-premises data gateway, the Azure Relays are automatically provisioned. However, you can also provide your own relay details. These details help you associate the relay with your Azure subscription and also manage the sender and listener keys for this relay.

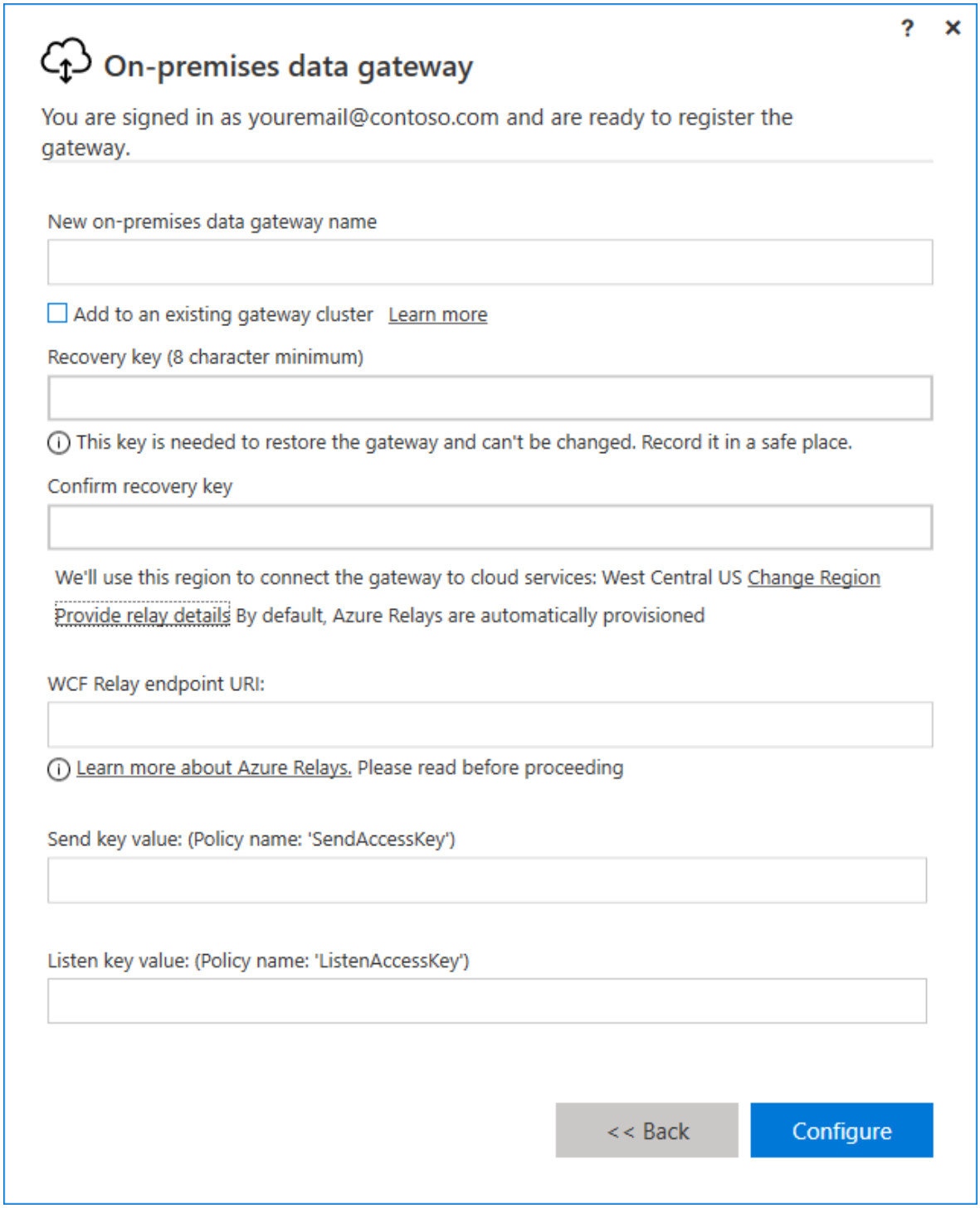
> **Note**
>
> Only WCF relays with NetTcp type are supported for this feature.

Steps to provide your own relay details

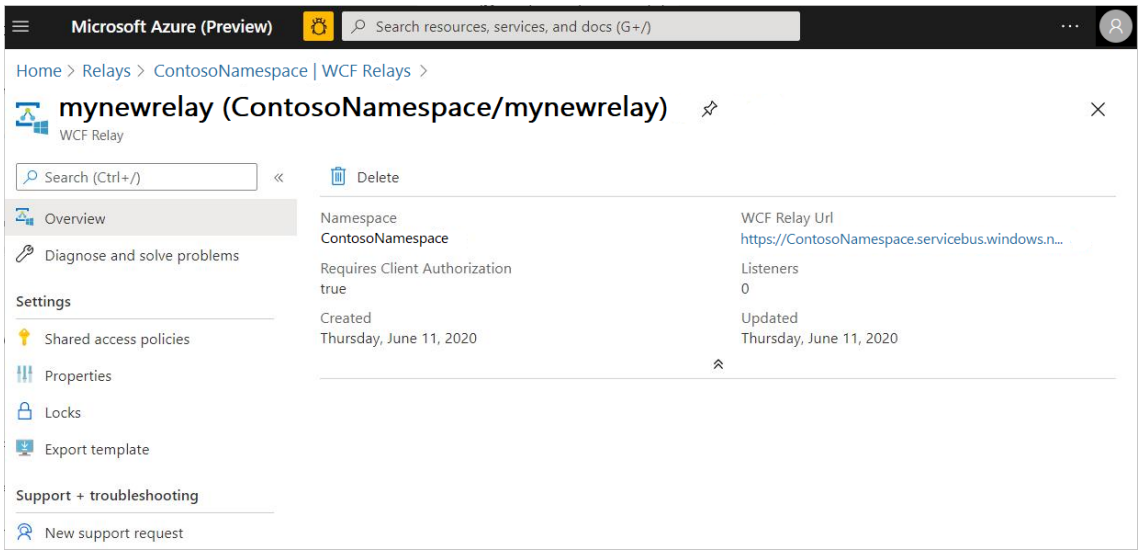
1. Select **Provide Relay details**.



2. You can now provide more details about your relay.

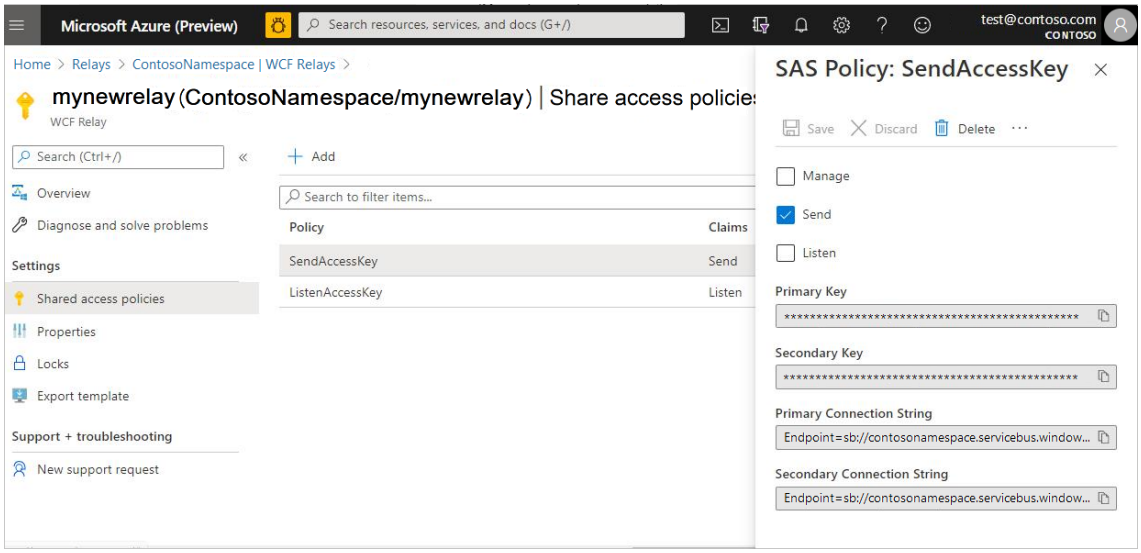


a. **WCF Relay endpoint URI**—Provide the URI (highlighted below) for your WCF relay from the Azure portal.



> **Note**
>
> The WCF Relay endpoint URI must be unique for every gateway and can't be re-used for other gateways.

b. **Send key value and the Listen Key Value**—Create two shared access policies, one called SendAccessKey and the other ListenAccessKey. Provide either the primary or the secondary keys in the on-premises data gateway app. To learn more, go to Azure Relay authentication and authorization.



> **Note**
>
> If you recover an existing gateway with customized relay details to a new machine, you'll have to explicitly uninstall the gateway from the old machine or rotate the sender and listener keys. If this operation isn't done, then queries through this gateway may fail.

Keep data in the region where it's stored

If you want to keep your data within the region where it’s stored, all you need to do is:

- Bring your own relay that lives in the same region as the data.
- Make sure your capacity is in the same region.

When you install an on-premises data gateway, it must be in the home tenant region to work with Power BI. Data from your gateway must travel to the relay, then to the location of your Power BI capacity. An Azure Relay automatically gets installed in the same region as the on-premises data gateway.

However, you have the option to choose your own relay in a different location. Then, the data will transfer through the location of your assigned relay instead. Only metadata will go to the gateway application in the home region and this condition can't be changed. This means you can keep your data within the region it's stored in if your relay, the capacity, and the data are all in the same region.

Next steps

- What is Azure Relay?

Adjust communication settings for the on-premises data gateway

Article • 01/04/2023

This article describes several communication settings associated with the on-premises data gateway. It also describes how to adjust those settings.

Enable outbound Azure connections

The gateway relies on Azure Relay for cloud connectivity. The gateway correspondingly establishes outbound connections to its associated Azure region.

If you registered for either a Power BI tenant or an Office 365 tenant, your Azure region defaults to the region of that service. Otherwise, your Azure region might be the one closest to you.

If a firewall blocks outbound connections, configure the firewall to allow outbound connections from the gateway to its associated Azure region.

Ports

The gateway communicates on the following outbound ports: TCP 443, 5671, 5672, and from 9350 through 9354. The gateway doesn't require inbound ports.

We recommend that you allow the "*.servicebus.windows.net" Domain Name System (DNS). For guidance on how to set up your on-premises firewall and/or proxy using fully qualified domain names (FQDNs) instead of using IP addresses that are subject to change, follow the steps in Azure WCF Relay DNS Support.

Alternatively, you allow the IP addresses for your data region in your firewall. Use the JSON files listed below, which are updated weekly.

- Public Cloud
- US Gov
- Germany
- China

Or, you can get the list of required ports by performing the network ports test periodically in the gateway app.

The gateway communicates with Azure Relay by using FQDNs. If you force the gateway to communicate via HTTPS, it will strictly use FQDNs only and won't communicate by using IP

addresses.

> **Note**
>
> The Azure datacenter IP list shows IP addresses in Classless Inter-Domain Routing (CIDR) notation. An example of this notation is 10.0.0.0/24, which doesn't mean from 10.0.0.0 through 10.0.0.24. Learn more about **CIDR notation**.

The following list describes FQDNs used by the gateway.

Public Cloud Domain names	Outbound ports	Description
*.download.microsoft.com	80	Used to download the installer. The gateway app also uses this domain to check the version and gateway region.
*.powerbi.com	443	Used to identify the relevant Power BI cluster.
*.analysis.windows.net	443	Used to identify the relevant Power BI cluster.
*.login.windows.net, login.live.com, and aadcdn.msauth.net	443	Used to authenticate the gateway app for Azure Active Directory (Azure AD) and OAuth2. Note that additional URLs could be required as part of the Azure Active Directory sign in process that can be unique to a tenant.
*.servicebus.windows.net	5671-5672	Used for Advanced Message Queuing Protocol (AMQP).
*.servicebus.windows.net	443 and 9350-9354	Listens on Azure Relay over TCP. Port 443 is required to get Azure Access Control tokens.
*.frontend.clouddatahub.net	443	Deprecated and not required. This domain will be removed from the public documentation as well.
*.core.windows.net	443	Used by dataflows to write data to Azure Data Lake.
login.microsoftonline.com	443	Used to authenticate the gateway app for Azure AD and OAuth2.
*.msftncsi.com	80	Used to test internet connectivity if the Power BI service can't reach the gateway.
*.microsoftonline-p.com	443	Used to authenticate the gateway app for Azure AD and OAuth2.
*.dc.services.visualstudio.com	443	Used by AppInsights to collect telemetry.

For GCC, GCC high, and DoD, the following FQDNs are used by the gateway.

Ports	GCC	GCC High	DoD
80	*.download.microsoft.com	*.download.microsoft.com	*.download.microsoft.com
443	*.powerbigov.us, *.powerbi.com	*.high.powerbigov.us	*.mil.powerbigov.us
443	*.analysis.usgovcloudapi.net	*.high.analysis.usgovcloudapi.net	*.mil.analysis.usgovcloudapi.net
443	*.login.windows.net, *.login.live.com, *.aadcdn.msauth.net	Go go documentation	Go to documentation
5671-5672	*.servicebus.usgovcloudapi.net	*.servicebus.usgovcloudapi.net	*.servicebus.usgovcloudapi.net
443 and 9350-9354	*.servicebus.usgovcloudapi.net	*.servicebus.usgovcloudapi.net	*.servicebus.usgovcloudapi.net
443	*.core.usgovcloudapi.net	*.core.usgovcloudapi.net	*.core.usgovcloudapi.net
443	*.login.microsoftonline.com	*.login.microsoftonline.us	*.login.microsoftonline.us
443	*.msftncsi.com	*.msftncsi.com	*.msftncsi.com
443	*.microsoftonline-p.com	*.microsoftonline-p.com	*.microsoftonline-p.com
443	*.dc.applicationinsights.us	*.dc.applicationinsights.us	*.dc.applicationinsights.us

For China Cloud (Mooncake), the following FQDNs are used by the gateway.

Ports	China Cloud (Mooncake)
80	*.download.microsoft.com
443	*.powerbi.cn
443	*.asazure.chinacloudapi.cn
443	*.login.chinacloudapi.cn
5671-5672	*.servicebus.chinacloudapi.cn
443 and 9350-9354	*.servicebus.chinacloudapi.cn
443	*.chinacloudapi.cn
443	login.partner.microsoftonline.cn

Ports	China Cloud (Mooncake)
443	No Mooncake equivalent—not required to run the gateway—only used to check network during failure conditions
443	No Mooncake equivalent—used during Azure AD sign in. For more information about Azure AD endpoints, go to Check the endpoints in Azure
443	applicationinsights.azure.cn
433	clientconfig.passport.net
433	aadcdn.msftauth.cn
433	aadcdn.msauth.cn

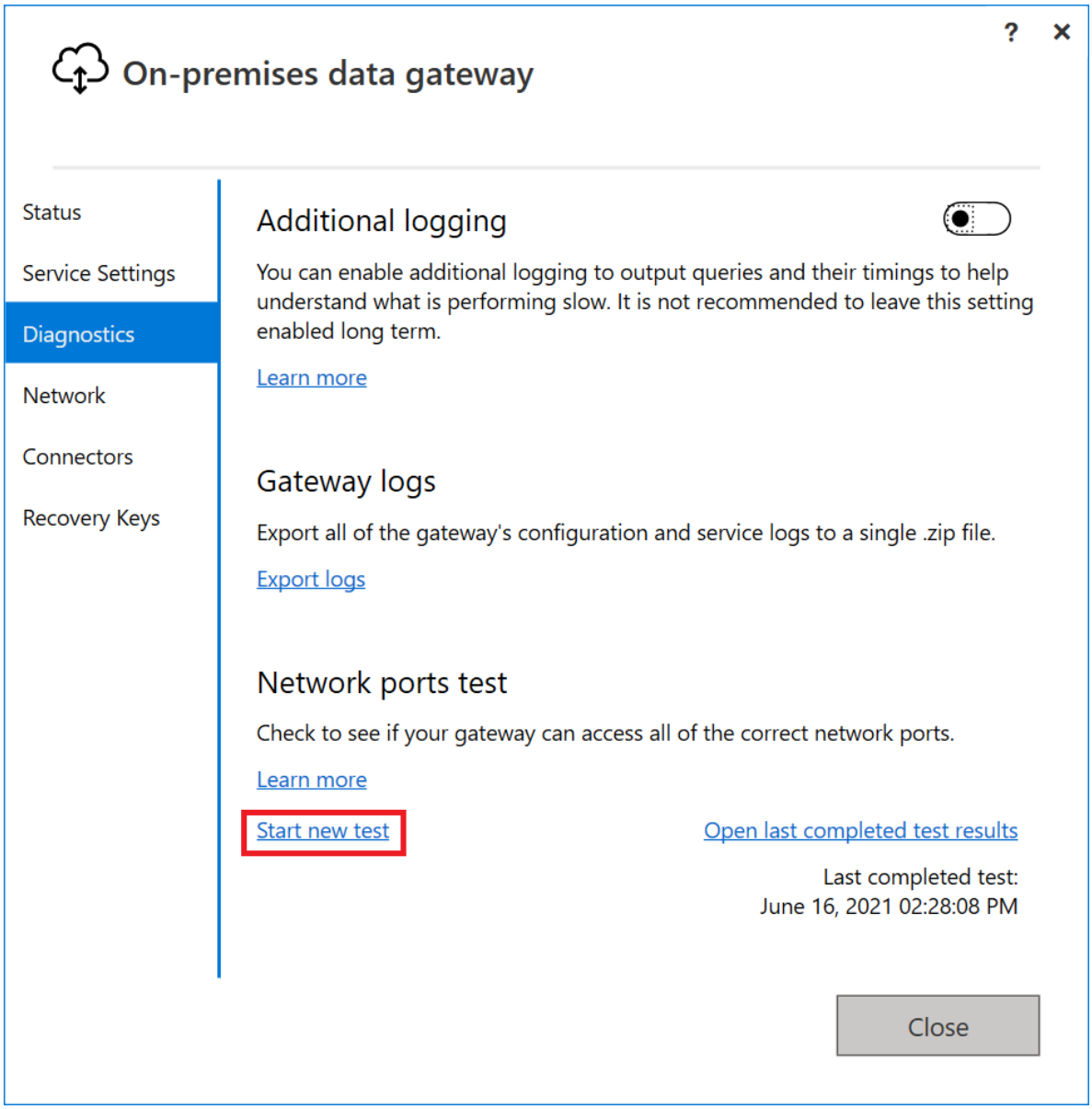
> ⓘ **Note**
>
> After the gateway is installed and registered, the only required ports and IP addresses are those needed by Azure Relay, as described for servicebus.windows.net in the preceding table. You can get the list of required ports by performing the **Network ports test** periodically in the gateway app. You can also force the gateway to **communicate using HTTPS**.

Network ports test

To test if the gateway has access to all required ports:

1. On the machine that is running the gateway, enter "gateway" in Windows search, and then select the **On-premises data gateway** app.

2. Select **Diagnostics**. Under **Network ports test**, select **Start new test**.



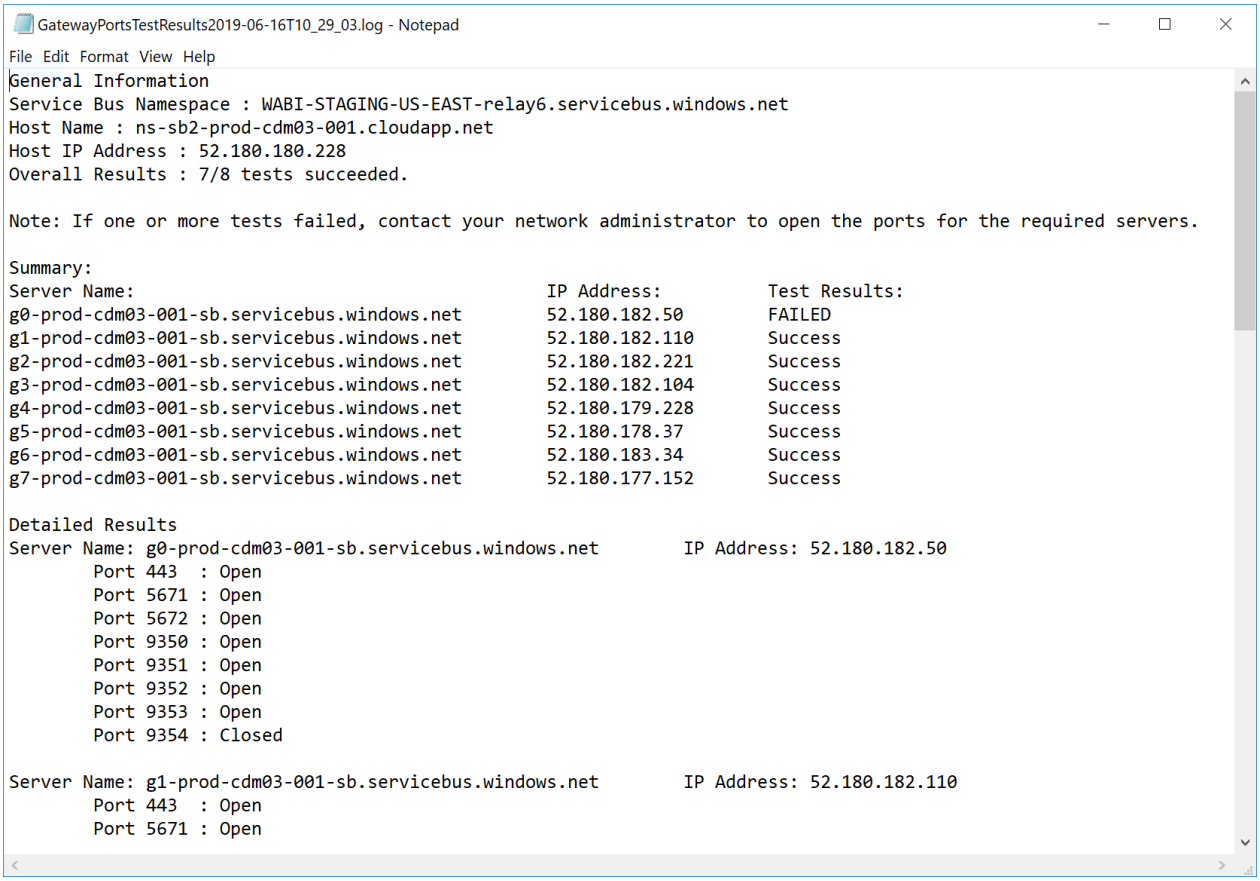
When your gateway runs the network ports test, it retrieves a list of ports and servers from Azure Relay and then attempts to connect to all of them. When the **Start new test** link reappears, the network ports test has finished.

The summary result of the test is either "Completed (Succeeded)" or "Completed (Failed, see last test results)". If the test succeeded, your gateway connected to all the required ports. If the test failed, your network environment might have blocked the required ports and servers.

> **Note**
>
> Firewalls often intermittently allow traffic on blocked sites. Even if a test succeeds, you might still need to allowlist that server on your firewall.

To view the results of the last completed test, select the **Open last completed test results** link. The test results open in your default text editor.

The test results list all the servers, ports, and IP addresses that your gateway requires. If the test results display "Closed" for any ports as shown in the following screenshot, ensure that your network environment didn't block those connections. You might need to contact your network admin to open the required ports.

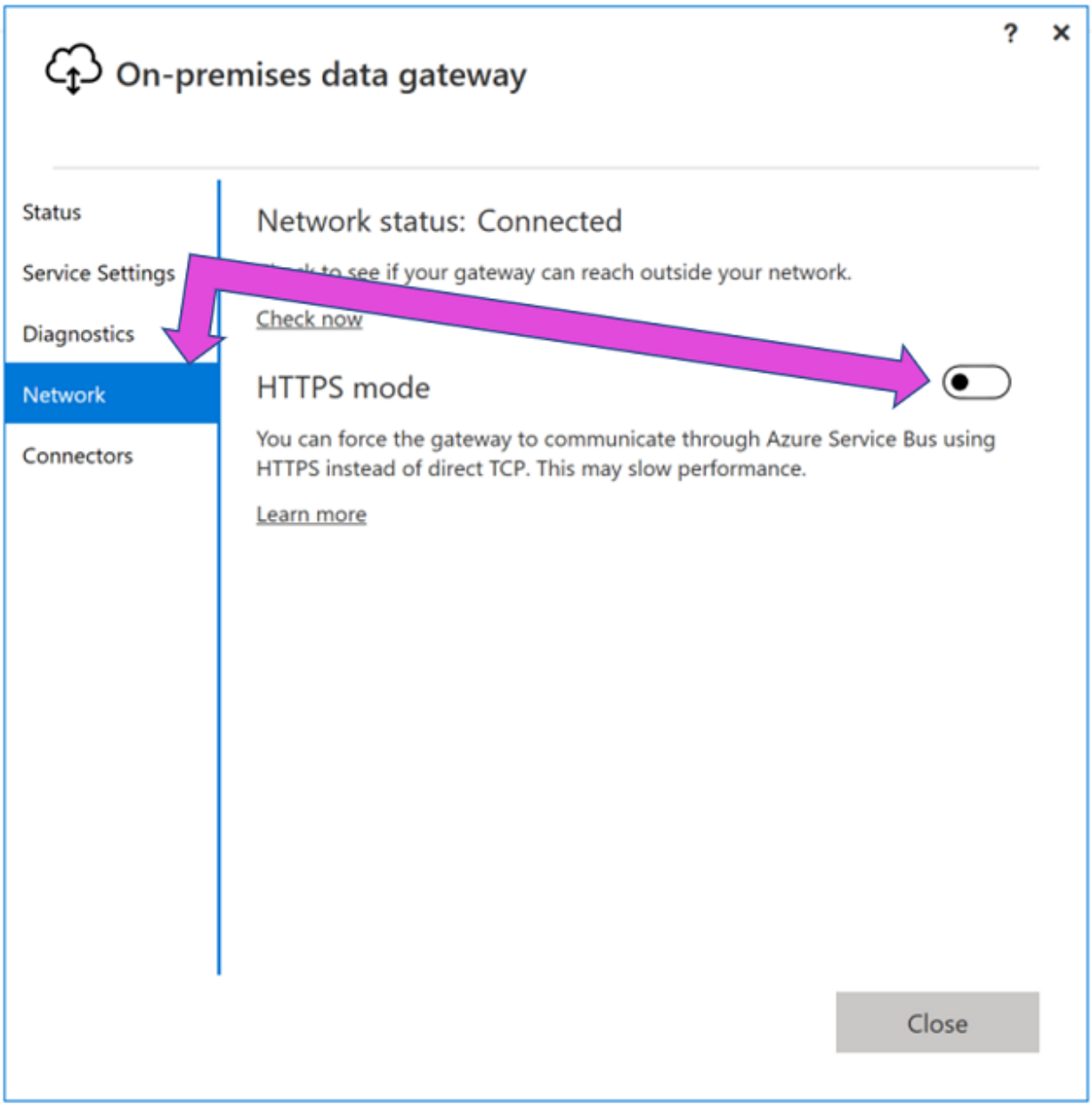


Force HTTPS communication with Azure Relay

You can force the gateway to communicate with Azure Relay by using HTTPS instead of direct TCP.

> **Note**
>
> Starting with the June 2019 gateway release and based on recommendations from Relay, new installations default to HTTPS instead of TCP. This default behavior doesn't apply to updated installations.

You can use the gateway app to force the gateway to adopt this behavior. In the gateway app, select **Network**, and then turn on **HTTPS mode**.



After you make this change and then select **Apply**, the gateway Windows service restarts automatically so that the change can take effect. The **Apply** button appears only when you make a change.

To restart the gateway Windows service from the gateway app, go to Restart a gateway.

> **Note**
>
> If the gateway can't communicate by using TCP, it automatically uses HTTPS. The selection in the gateway app always reflects the current protocol value.

TLS 1.2 for gateway traffic

By default, the gateway uses Transport Layer Security (TLS) 1.2 to communicate with the Power BI service. To ensure all gateway traffic uses TLS 1.2, you might need to add or

modify the following registry keys on the machine that runs the gateway service.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]"SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319]"SchUseStrongCrypto"=dword:00000001
```

> **Note**
>
> Adding or modifying these registry keys applies the change to all .NET applications. For information about registry changes that affect TLS for other applications, go to **Transport Layer Security (TLS) registry settings**.

Service tags

A service tag represents a group of IP address prefixes from a given Azure service. Microsoft manages the address prefixes encompassed by the service tag and automatically updates the service tag as addresses change, minimizing the complexity of frequent updates to network security rules. The data gateway has dependencies on the following service tags:

- PowerBI
- ServiceBus
- AzureActiveDirectory
- AzureCloud

The on-premises data gateway uses Azure Relay for some communication. However, there are no service tags for the Azure Relay service. ServiceBus service tags specifically pertain to the Service queues and topics feature, but not for Azure Relay.

The AzureCloud service tag represents all global Azure Data Center IP addresses. Since Azure Relay service is built on top of Azure Compute, Azure Relay public IPs are a subset of the AzureCloud IPs. More information: Azure service tags overview

Next steps

- Configure the gateway log file

Configure log files for the on-premises data gateway

Article • 02/10/2023

There are three categories of service logs for an on-premises data gateway: information, error, and network. This categorization provides a troubleshooting experience that lets you focus on the specific area for an error or issue.

In order to check your logging configurations, take the following steps:

1. Open the gateway configuration file Microsoft.PowerBI.EnterpriseGateway.exe.config, which by default should be located under \Program Files\On-premises data gateway.
2. Before proceeding further, make a copy of this file just in case you need to restore it later.
3. Locate the listener `ApplicationFileTraceListener` which is under `system.diagnostics`.

The following sections provide the configuration details per retention type, which depends on your gateway version.

Age based retention

Starting in February of 2023, the new age based retention concept within a gateway was introduced. This concept is the default retention type for **new** gateway installations.

For this retention type, there are two main aspects to consider (in order of precedence):

- Maximum disk space to be consumed by gateway logs (GatewayInfo*.log, GatewayError*.log, GatewayNetwork*.log), with a default value of 5 GB.
- Retention period in days, with a default value of 30 days.

In this new logic, we ensure that for every new day a new log file is provisioned. This provisioning ensures the information for a given day is present in log files where the filename matches the log entry dates. Also the file partition within the day is performed if the maximum individual file size (default of 100 MB) is reached.

XML

```
<system.diagnostics>
  <trace autoflush="true" indentsize="4">
    <listeners>
```

```
        <remove name="Default" />
        <add name="ApplicationFileTraceListener"
type="Microsoft.PowerBI.DataMovement.Pipeline.Common.Diagnostics.AgeBasedRet
entionRotatableFilesManagerTraceListener,
Microsoft.PowerBI.DataMovement.Pipeline.Common"
initializeData="%LOCALAPPDATA%\Microsoft\On-premises data
gateway\,30,5120,100" />
      </listeners>
    </trace>
  </system.diagnostics>
```

If you would like to change the retention default parameters values, you should adjust them in the `initializeData` value. The following list describes each parameter:

- Retention period in days (a value between 1 and 365 days).
- Maximum total size in MB which can be consumed by the three log file types.
- Maximum size in MB which each log file can have individually. Each time the limit is reached, a new file is created with an sequential number appended.

> ⓘ **Note**
>
> Gateway logs use UTC based timestamps, and the daily log file rotation will take place at 00:00 UTC.

File count based retention

This was the default log retention logic within a gateway for versions December 2022 and earlier. This logic has two main concepts:

- Number of files to be retained per log type (GatewayInfo*.log, GatewayError*.log, GatewayNetwork*.log).
- Maximum disk space to be consumed per log type (GatewayInfo*.log, GatewayError*.log, GatewayNetwork*.log).

The files are partitioned accordingly with the previously listed criteria, and therefore, whenever you reach the maximum number of files it will typically also be at or close to maximum disk space.

The following excerpt from the gateway configuration file Microsoft.PowerBI.EnterpriseGateway.exe.config contains the three categories: `GatewayInfo.log`, `GatewayErrors.log`, and `GatewayNetwork.log`.

XML

```
  <system.diagnostics>
    <trace autoflush="true" indentsize="4">
      <listeners>
        <remove name="Default" />
        <add name="ApplicationFileTraceListener"

type="Microsoft.PowerBI.DataMovement.Pipeline.Common.Diagnostics.RotatableFi
lesManagerTraceListener, Microsoft.PowerBI.DataMovement.Pipeline.Common"
             initializeData="%LOCALAPPDATA%\Microsoft\On-premises data
gateway\,GatewayInfo.log,GatewayErrors.log,GatewayNetwork.log,20,50" />
      </listeners>
    </trace>
  </system.diagnostics>
```

By default, the gateway configuration file is located in the directory \Program Files\On-premises data gateway. To set the number of log files to retain, change the first number in the file's `initializeData` value. To configure the size of each log file, change the second number.

The following example specifies that 20 log files, the sum total of all files in each category being no more than 50 MB in size, will be retained: `GatewayInfo.log,GatewayErrors.log,GatewayNetwork.log,20,50`

Will the new age based retention logic apply by default to my existing on-premises data gateway installation?

No. This retention logic for now is applied to completely new gateway installations. Existing gateways while upgrading to February 2023 or later versions should keep their current log retention logic (file count based retention).

Next steps

For information on how to export gateway logs for troubleshooting, go to Troubleshooting tools.

Adjust gateway performance based on server CPU

Article • 12/02/2022

The on-premises data gateway has settings that control resource usage on the machine where the gateway is installed. By default, gateway releases starting in June 2019 (3000.6.204) automatically scale these settings, using more or less resources depending on CPU capacity:

Setting	Description
`MashupDefaultPoolContainerMaxCount`	Maximum container count for Power BI refresh, Azure Analysis Services, and others.
`MashupDefaultPoolContainerMaxWorkingSetInMB`	Maximum working set size for Power BI refresh, Azure Analysis Services, and others.
`MashupDQPoolContainerMaxCount`	Maximum container count for Power BI Direct Query.
`MashupTestConnectionPoolContainerMaxInstanceCount`	Maximum container count for test connections.
`MashupAzureConnectorsCachingPoolContainerMaxCount`	Maximum container count for LogicApps, Power Apps, and Power Automate.
`PowerQueryOnlineCachingPoolContainerMaxCount`	Maximum container count for Power Query Online.

Use the `MashupDefaultPoolContainerMaxWorkingSetInMB` setting to change the default pool. Changing the memory set is only possible for the default pool. For the other pools, it isn't possible due to performance and stability reasons. The `MashupDQPoolContainerMaxWorkingSetInMB` settings can't be changed in the config.

Most queries use *mashup containers* to execute. So the number of mashup containers determines the number of queries that can be executed in parallel. A *working set* defines the memory allocated to each container. These settings are available in *\Program Files\On-premises data gateway\Microsoft.PowerBI.DataMovement.Pipeline.GatewayCore.dll.config*.

If you've changed any of these settings manually, for these settings to take effect you must also disable automatic scaling by setting `MashupDisableContainerAutoConfig` to

True in *\Program Files\On-premises data gateway\Microsoft.PowerBI.DataMovement.Pipeline.GatewayCore.dll.config*. If `MashupDisableContainerAutoConfig` is set to *False*, automatic scaling is always enabled.

Configure gateway disk space

Article • 12/02/2022

This article focuses on the configuration settings governing disk space for gateway users who run out of disk space.

Gateway spooling data

Power BI and the on-premises data gateway create temporary cache files when communicating between the on-premises environment and the cloud in a process called *spooling*. Depending on how much disk space you have available for spooling, it's possible for an "out of disk space" error to occur when disk space is full because of the spooler.

> **Note**
>
> We recommend you use a solid-state drive (SSD) as the spooling storage drive for optimal performance.

When spooling causes an "out of disk space" error, use the following steps to change the location of the spooler to a disk with more capacity.

1. Navigate to C:\Program Files\On-premises data gateway.
2. Make a backup copy of the Microsoft.PowerBI.DataMovement.Pipeline.GatewayCore.dll.config configuration file.
3. Edit the Microsoft.PowerBI.DataMovement.Pipeline.GatewayCore.dll.config configuration file.
4. Search for **SpoolerDirectory**.

   XML

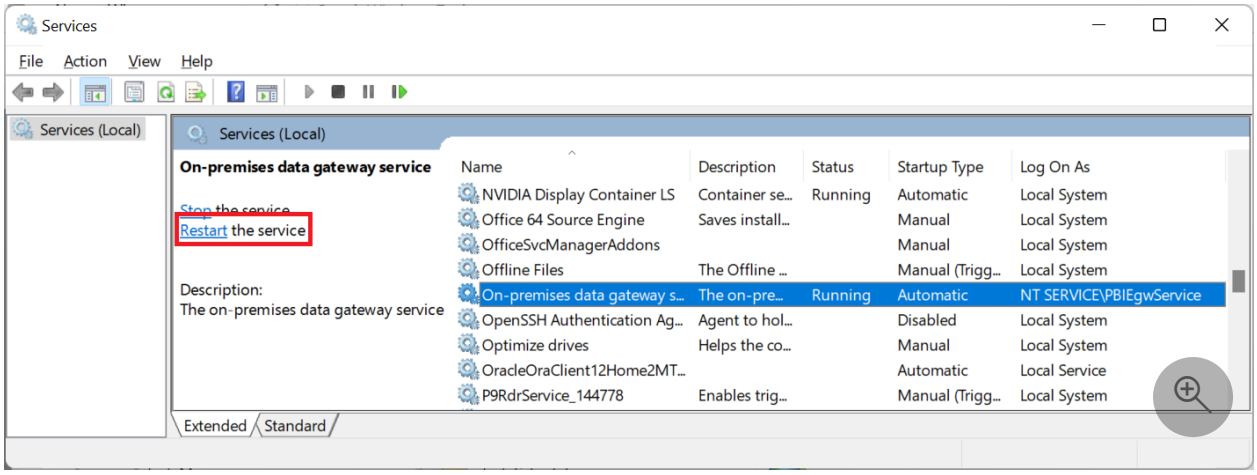
   ```
   <setting name="SpoolerDirectory" serializeAs="String">
       <value>%LOCALAPPDATA%\Microsoft\On-premises data
   gateway\Spooler</value>
   </setting>
   ```

   The <value> tag specifies the location of the SpoolerDirectory.

5. Modify this path to a location that contains enough disk space for your business needs.

6. Once modified, save the file and restart the on-premises data gateway.

> **Note**
>
> If you modify the path, you'll also need to restart the on-premises data gateway service.



Mashup engine persistent cache

If spooling has been mapped to a different drive, but you continue to get "out of disk space" errors, it could be due to the persistent cache. This error could be due to queries that don't fold (for more information about query folding, go to Query folding overview). Or the error could be due to poorly performing queries (for more information on optimizing gateway performance, go to Monitor and optimize on-premises data gateway performance).

If the query can't be optimized, the persistent cache can be moved to a larger capacity drive. The persistent cache (as opposed to the spooler) uses the root drive, and the operating system \temp path. In order to avoid the "out of disk space" error, you'll need to either free up space on the root drive, expand the size of the root drive, or potentially remap the temp folder to a drive with more space.

You can change (or set) the value of the Windows TMP environment variable *for the user account being used to run the gateway* to move the persistent cache to a larger capacity drive. The path used for cache and temp directories is determined through the Win32 GetTempPath function. According to the Win32 documentation, this function uses the first value it finds from the following list:

- The path specified by the TMP environment variable.
- The path specified by the TEMP environment variable.
- The path specified by the USERPROFILE environment variable.
- The Windows directory.

So, change TMP for the gateway user to move the persistent cache onto another drive.

> **Note**
>
> To change the environment variables in Windows, from the **Start** menu, select **Search**, enter **Environment Variables**, select **Edit the system environment variables**, and from **System Properties** select **Environment Variables**.

Manage an on-premises data gateway

Article • 12/02/2022

After you install an on-premises data gateway, you manage it based on your requirements. Because each service might integrate gateways differently, the management options differ depending on the service.

> **Note**
>
> **Manage gateways** won't show up until you're the admin of at least one gateway. You become an admin either by being added as an admin or because you installed and configured a gateway.

Manage a gateway in the Power BI service

For information on how to manage an on-premises data gateway data source in the Power BI service, go to Add or remove a gateway data source.

Manage a gateway in the Power Platform admin center

For information on how to manage an on-premises data gateway data source in the Power Platform admin center, go to On-premises data gateway management.

Manage security roles of an on-premises data gateway

Article • 03/10/2023

You can use the on-premises data gateway to transfer data quickly and securely between Power BI or Power Apps and a data source or connection that isn't in the cloud, such as an on-premises SQL Server database or an on-premises SharePoint site. You can also view all on-premises data gateways for which you have permissions, and manage permissions and data sources for those gateways.

On-premises data gateway and data source permissions

Gateway roles

There are three security roles for the on-premises data gateway. When you install an on-premises data gateway, you automatically become the admin of the gateway. There can be multiple admins on the gateway.

> ⓘ **Note**
>
> These roles don't apply to a virtual network data gateway. Virtual network data gateways only have the admin role.

The three security roles for the on-premises data gateway are:

- **Admin**: An admin can manage and update the on-premises data gateway. An admin is allowed to create connections (data sources) on the gateway. An admin is allowed to manage (add/delete) users with admin, connection creator, and connection creator with sharing roles on the gateway. An admin can also manage access to all connections created on the gateway.
- **Connection creator**: A connection creator is allowed to create connections/data sources on the gateway. A connection creator can also test the status of the gateway cluster and its members. A connection creator can't manage or update the gateway and can't add or remove others on the gateway.

- **Connection creator with sharing**: A connection creator with sharing is allowed to create connections/data sources on the gateway and test the gateway status. This user is allowed to share the gateway with other users as a connection creator but isn't allowed to remove a user from the gateway.

Connection roles

> **Note**
>
> These roles are only applicable for data sources created in the on-premises data gateway. Cloud data sources can't be shared.

When you create a connection (data source) in the on-premises data gateway, you become the owner of the connection (data source). Multiple owners are allowed.

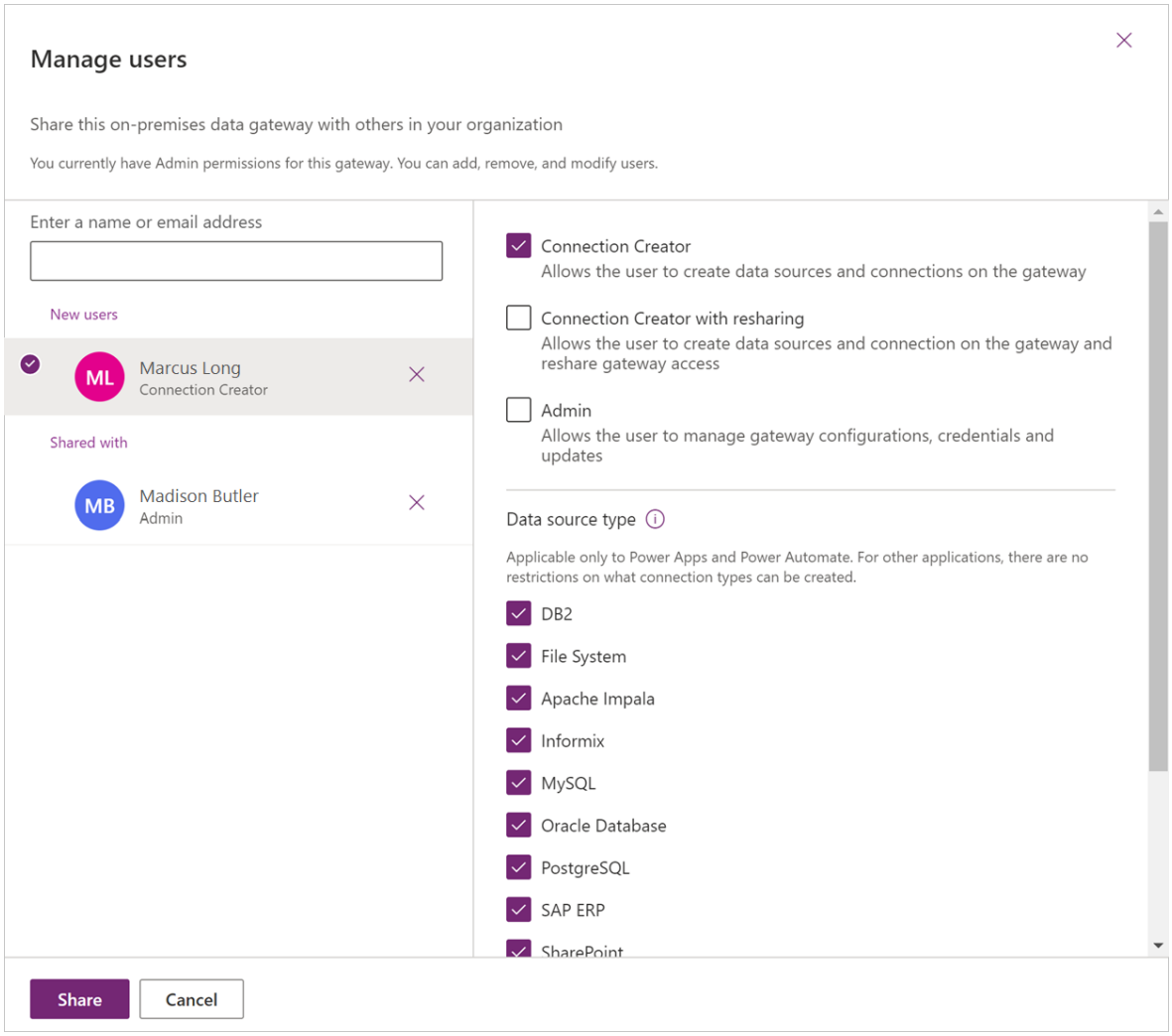
The three connection roles are:

- **Owner**: The owner of the connection (data source) is allowed to update credentials. An owner can also delete the connection. An owner can assign others to the connection with Owner, User, or User with sharing permissions.
- **User**: A user is allowed to use the connection (data source) in Power BI reports and Power BI dataflows. A user isn't allowed to see or update credentials.
- **User with sharing**: A user with sharing is allowed to use the connection (data source) in Power BI reports and Power BI dataflows. A user with sharing is allowed to share the data source with others with User permission.

How to manage the gateway and connection (data source) roles

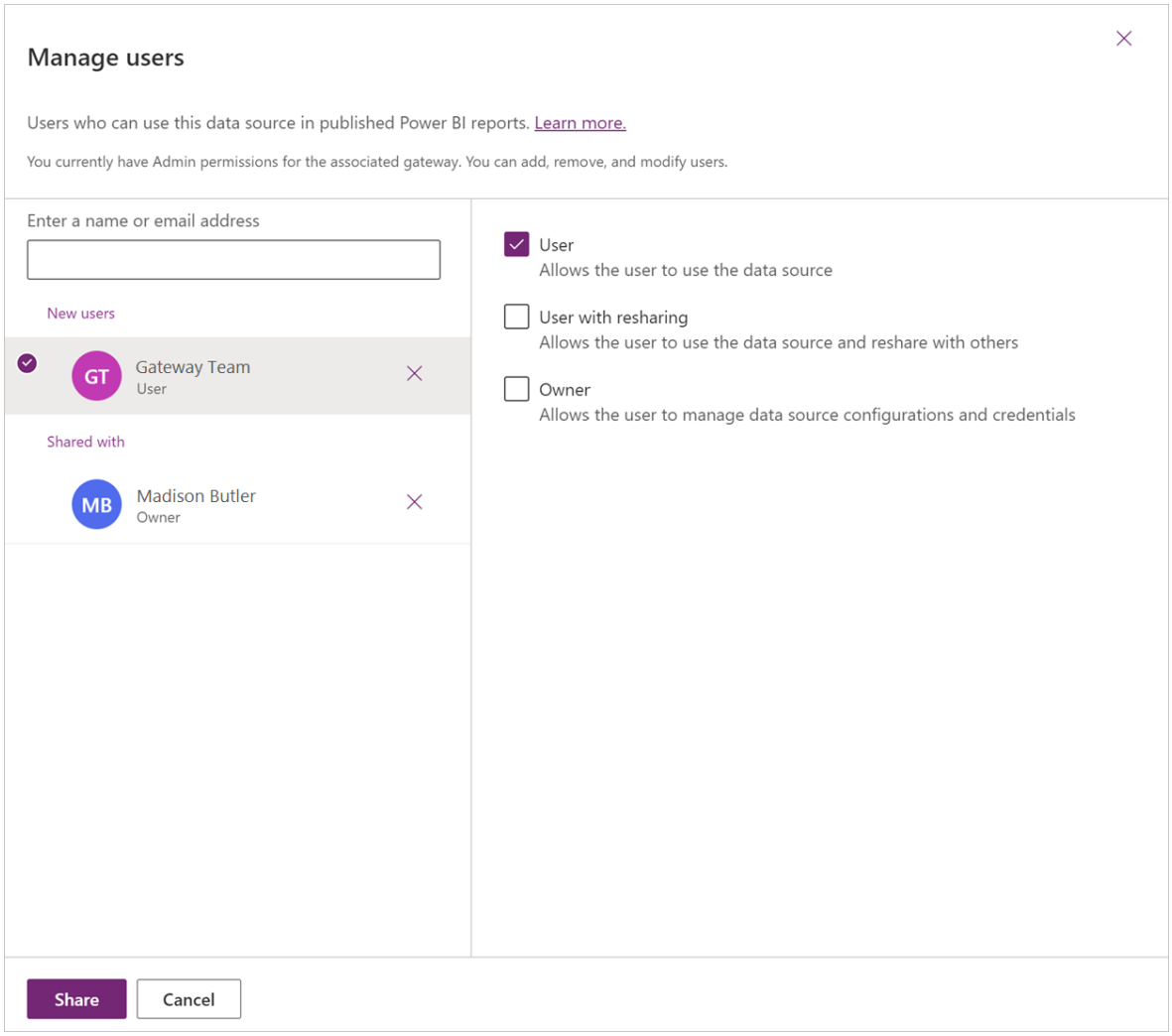
To manage on-premises data gateways:

1. Navigate to the Power Platform admin center.
2. Navigate to the **On-premises data gateways** tab.
3. Select a gateway cluster.
4. In the top ribbon, select **Manage users**.
5. Depending on your role, you can now assign users to the gateway.



To manage data sources:

1. Navigate to the Power Platform admin center.
2. Select a connection (data source).
3. In the top ribbon, select **Manage users**.
4. Depending on your role, you can now assign users to the connection.

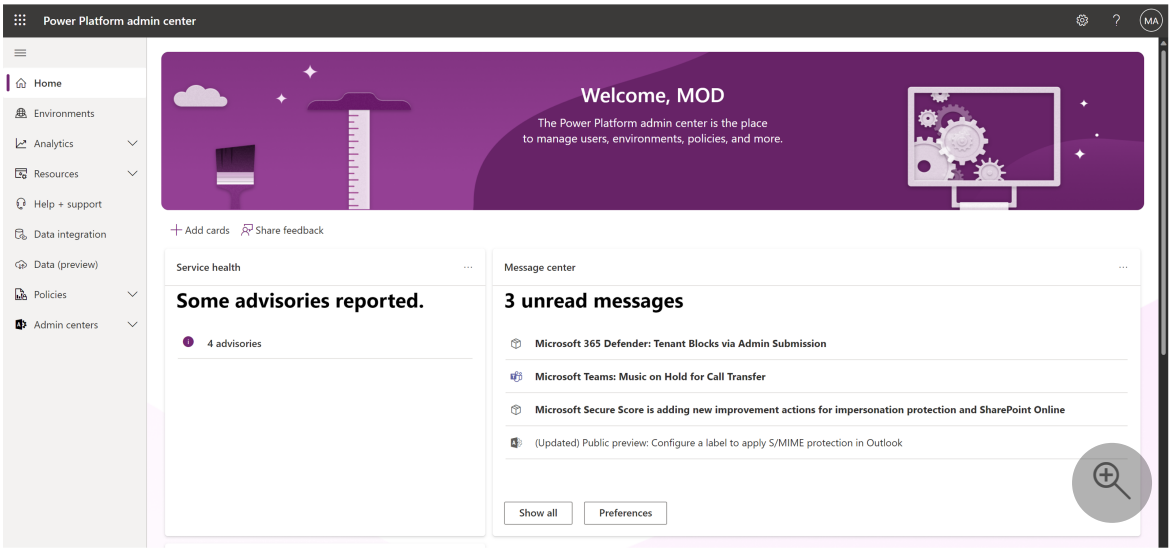


Restricting access for on-premises data gateways

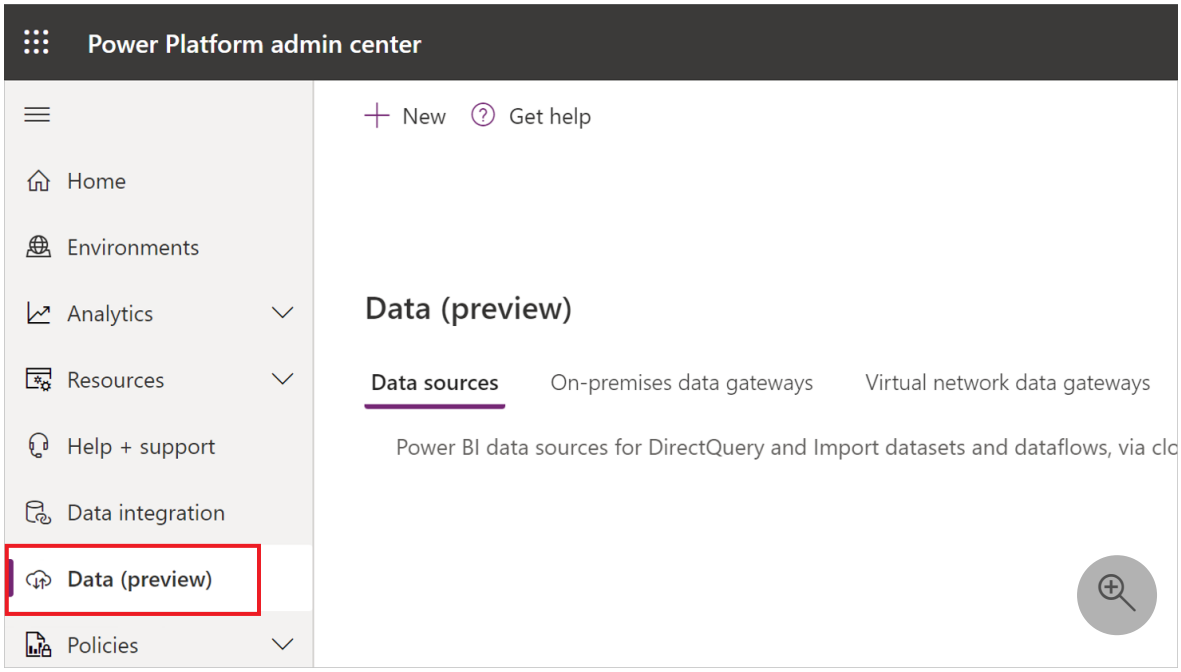
You can restrict access to who can install an on-premises data gateway. This restriction occurs though at the tenant level, not the environment level (default environment or otherwise). In other words, you can't restrict access at the environment level.

Your admin can update the data gateway settings through the Power Platform admin center.

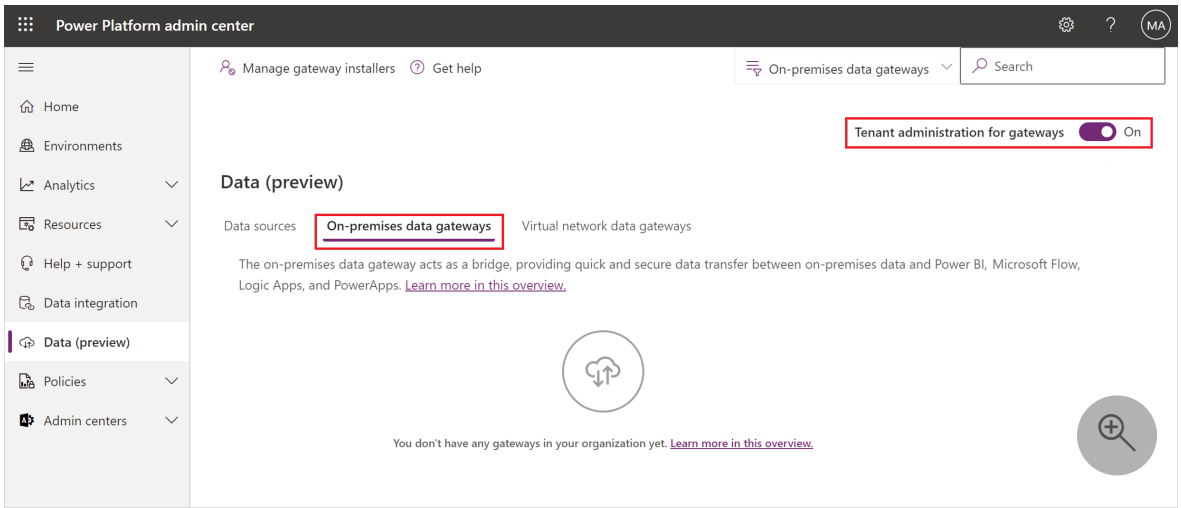
1. Go to the Power Platform admin center.



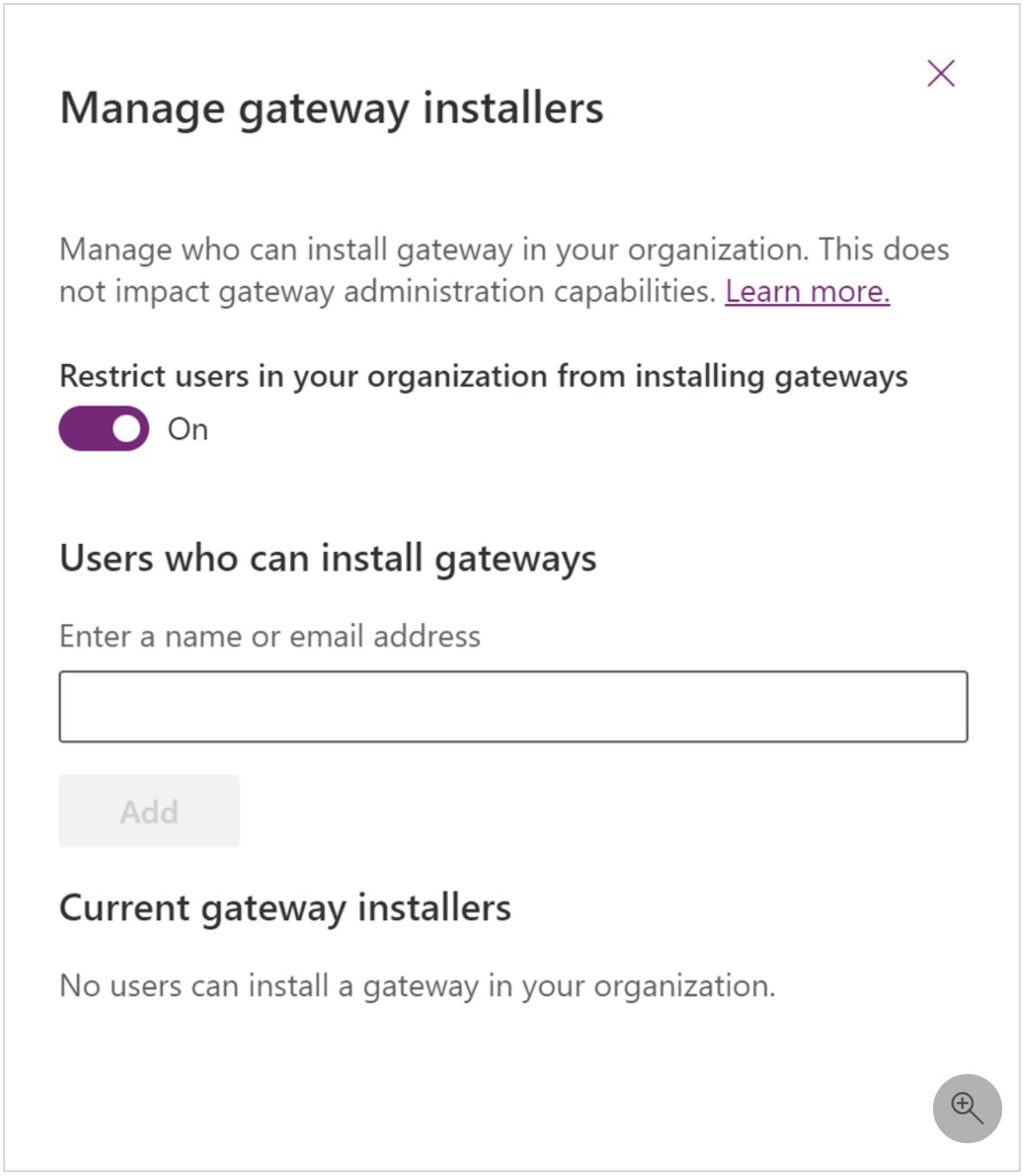
2. Select **Data (preview)**.



3. Select **On-premises data gateway** and turn on **Tenant administration for gateways**.



4. Turn on **Restrict users in your organization from installing gateways**. You can also allow specific users to override the restriction.



Manage on-premises data gateway high-availability clusters and load balancing

Article • 12/02/2022

You can use an on-premises data gateway cluster to avoid single points of failure and to load balance traffic across gateways in a cluster. To add new gateway members to a gateway cluster, go to Add another gateway to create a cluster.

High-availability clusters for an on-premises data gateway

You can create high-availability clusters of gateway installations. The clusters help ensure that your organization can access on-premises data resources from cloud services like Power BI and Power Apps. Gateway admins use such clusters to avoid single points of failure when accessing on-premises data resources.

The gateway cloud service always uses the primary gateway in a cluster unless that gateway isn't available. In that case, the service switches to the next available gateway in the cluster.

> **Note**
>
> Make sure the gateway members in a cluster are running the same gateway version, as different versions could cause unexpected failures based on supported functionality.

Manage a gateway cluster

After you create a cluster of two or more gateways, all gateway management operations apply to every gateway in the cluster. These operations include granting administrative permissions to a gateway and adding data sources or connections.

For example, when admins select **Manage gateways** in Power BI, the list of registered clusters or individual gateways is displayed. But the individual gateway instances that are members of the cluster aren't displayed.

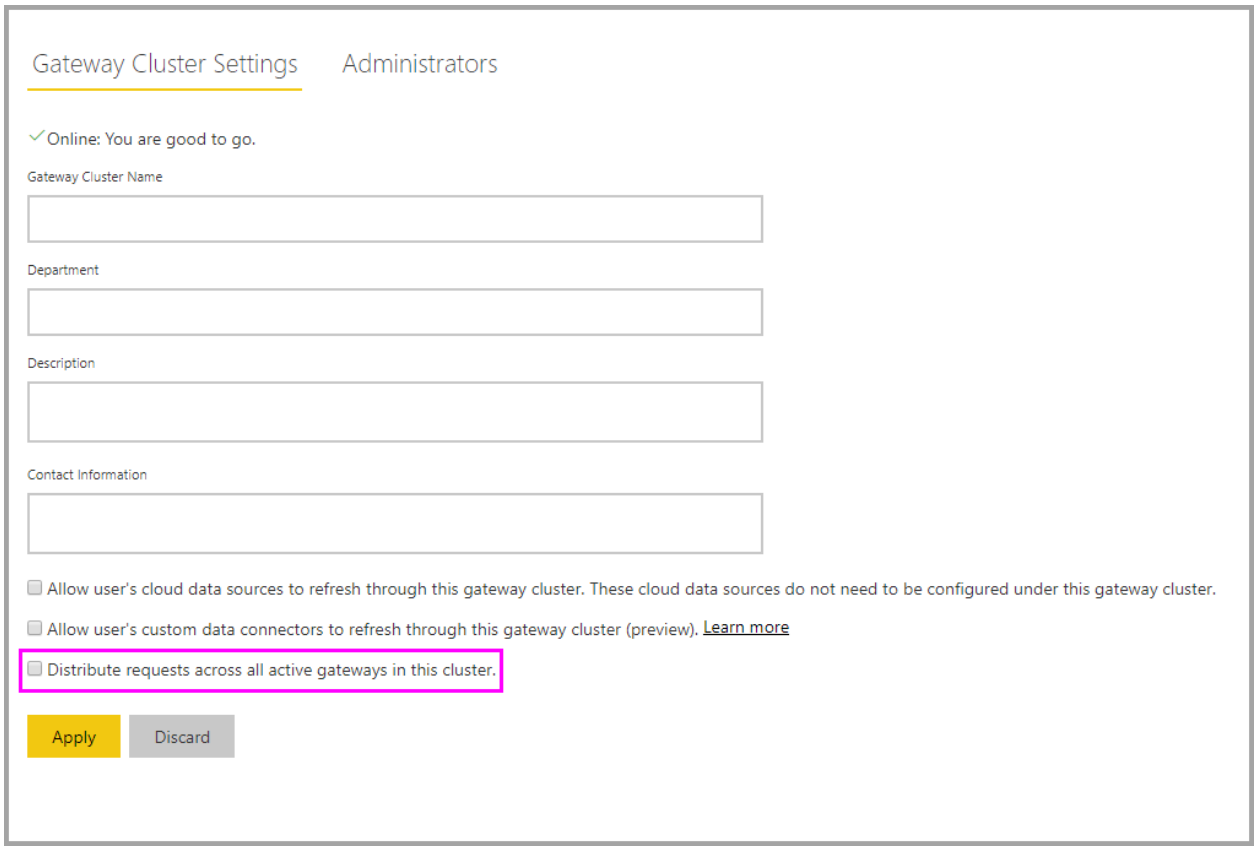
All requests are routed to the primary instance of a gateway cluster. If the primary gateway instance isn't online, the request is routed to another gateway instance in the cluster.

Load balance across gateways in a cluster

You can choose to let traffic be distributed evenly across gateways in a cluster. By default, the selection of a gateway during load balancing—that is, when "Distribute requests across all active gateways in this cluster" is enabled—is random. You can change this setting to distribute the load.

> **Note**
>
> It is recommended to disable or remove an offline gateway member in the cluster. If a gateway member is offline instead of disabled or removed, we may try to excecute a query on that offline member, before moving to the next one. This can negatively impact the performance.

For example, to provide load balancing from the Power BI service, select the gear icon  in the upper-right corner, then select **Manage gateways**. Next, select **Distribute requests across all active gateways in this cluster**.



Load balance based on CPU, Memory, concurrency limits

As mentioned earlier, the selection of a gateway during load balancing is random. Gateway admins can, however, throttle the resource usage of each gateway member. With throttling, you can make sure either a gateway member or the entire gateway cluster isn't overloaded. Overloaded system resources may cause request failures.

If a gateway cluster with load balancing enabled receives a request from one of the cloud services (like Power BI), it randomly selects a gateway member. If this member gateway is already at or over one of the throttling limits specified below, another member within the cluster is selected. If all members within the cluster are in the same state, the request fails.

A gateway admin should update the following settings in the *Microsoft.PowerBI.DataMovement.Pipeline.GatewayCore.dll.config* file available in the *Program Files\On-premises data gateway* folder in order to adjust throttling limits. Concurrency throttling is enabled by default.

- **CPUUtilizationPercentageThreshold** - This configuration allows gateway admins to set a throttling limit for CPU. The permissible range for this configuration is 0 to 100. A value of 0, which is the default, indicates that this configuration is disabled.
- **MemoryUtilizationPercentageThreshold** - This configuration allows gateway admins to set a throttling limit for memory. The permissible range for this configuration is 0 to 100. A value of 0, which is the default, indicates that this configuration is disabled.
- **ResourceUtilizationAggregationTimeInMinutes** - This configuration sets the time in minutes for which CPU and memory system counters of the gateway machine are aggregated. The aggregated values are then compared against the respective threshold limits set for **CPUUtilizationPercentageThreshold** and **MemoryUtilizationPercentageThreshold**. The default value for this configuration is 5.
- **ConcurrentOperationLimitPreview** - This configuration sets concurrent operation limit for the Gateway. **BypassConcurrentOperationLimit** can be set to remove all concurrent operation limits. The default value for this configuration is 40.

> ⓘ **Note**
>
> You can also change the load balancing setting through **PowerShell**.

Example errors when limit encountered

`The gateway you selected can't establish data source connections because it's exceeded the CPU limit set by your gateway admin. Try again later, or ask your gateway admin to increase the limit.`

`The gateway you selected can't establish data source connections because it's exceeded the memory limit set by your gateway admin. Try again later, or ask your gateway admin to increase the limit.`

`The gateway you selected can't establish data source connections because it's exceeded the concurrency limit set by your gateway admin. Try again later, or ask your gateway admin to increase the limit.`

Next steps

PowerShell support for gateway clusters

Update an on-premises data gateway

Article • 06/05/2023

We release an update every month for on-premises data gateways. Each of these updates includes new features along with the latest Mashup Engine.

> **Note**
>
> Currently, Microsoft actively supports only the last six releases of the on-premises data gateway. We release a new update for data gateways every month.

We recommend that you update gateway members one after the other in a timely manner. This process reduces sporadic failures as a query may succeed on one gateway member, but not on the other, based on disparity in capabilities across different versions.

Use the following steps when updating a gateway cluster with two or more members:

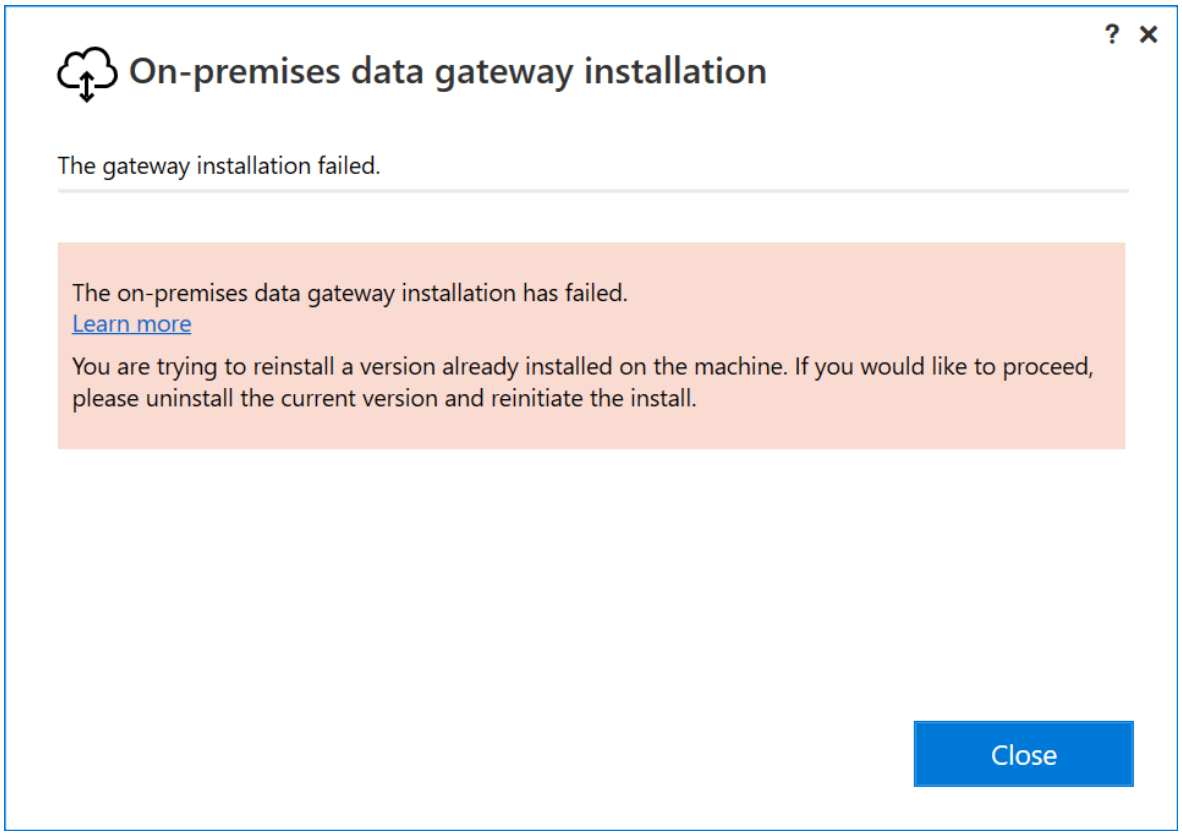
1. Disable one gateway member.
2. Wait for ongoing work to be completed. A waiting period of 30 minutes is sufficient for most workloads, however clusters frequently running critical long running jobs may require more time for requests to drain.
3. Update the gateway member.
4. Enable the updated gateway member.
5. Repeat step 1-4 until all gateway members are updated.

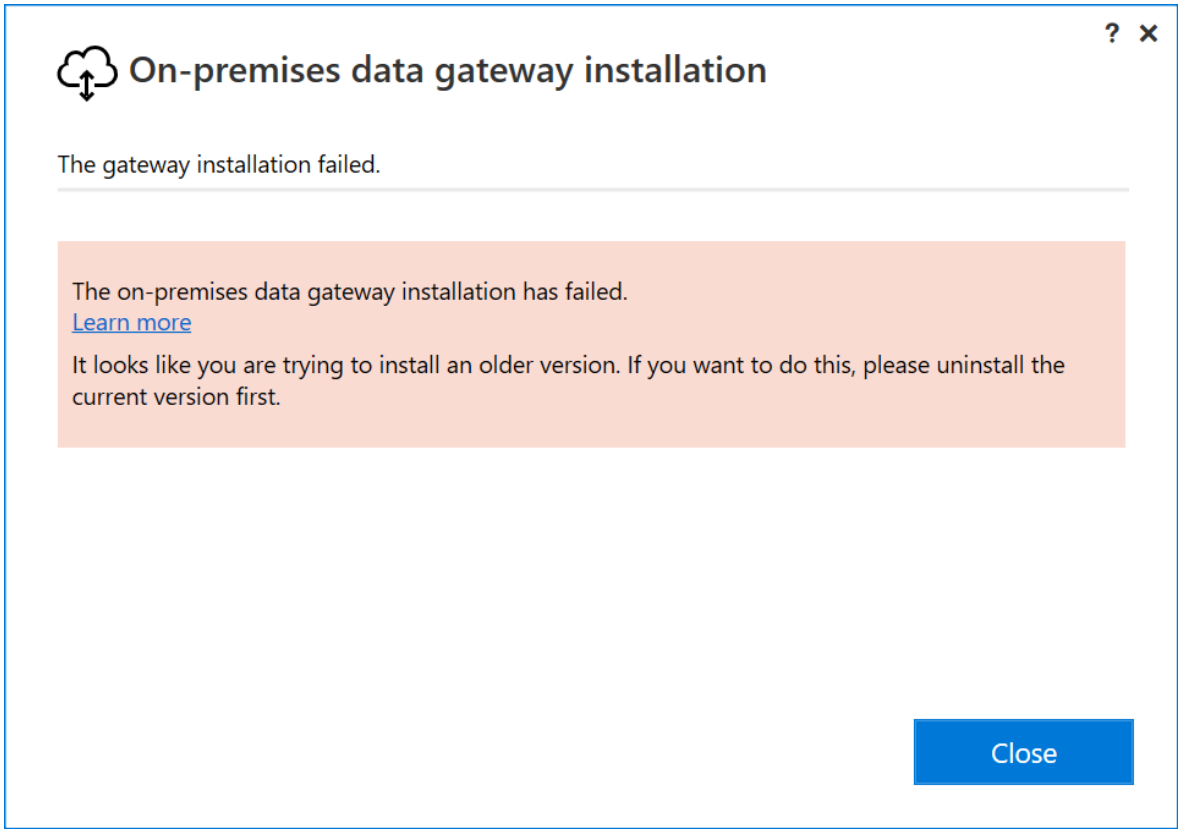
Disabling a gateway makes sure the load balancer doesn't try to execute queries on the member you're updating, hence reducing delays and failures.

Update a gateway

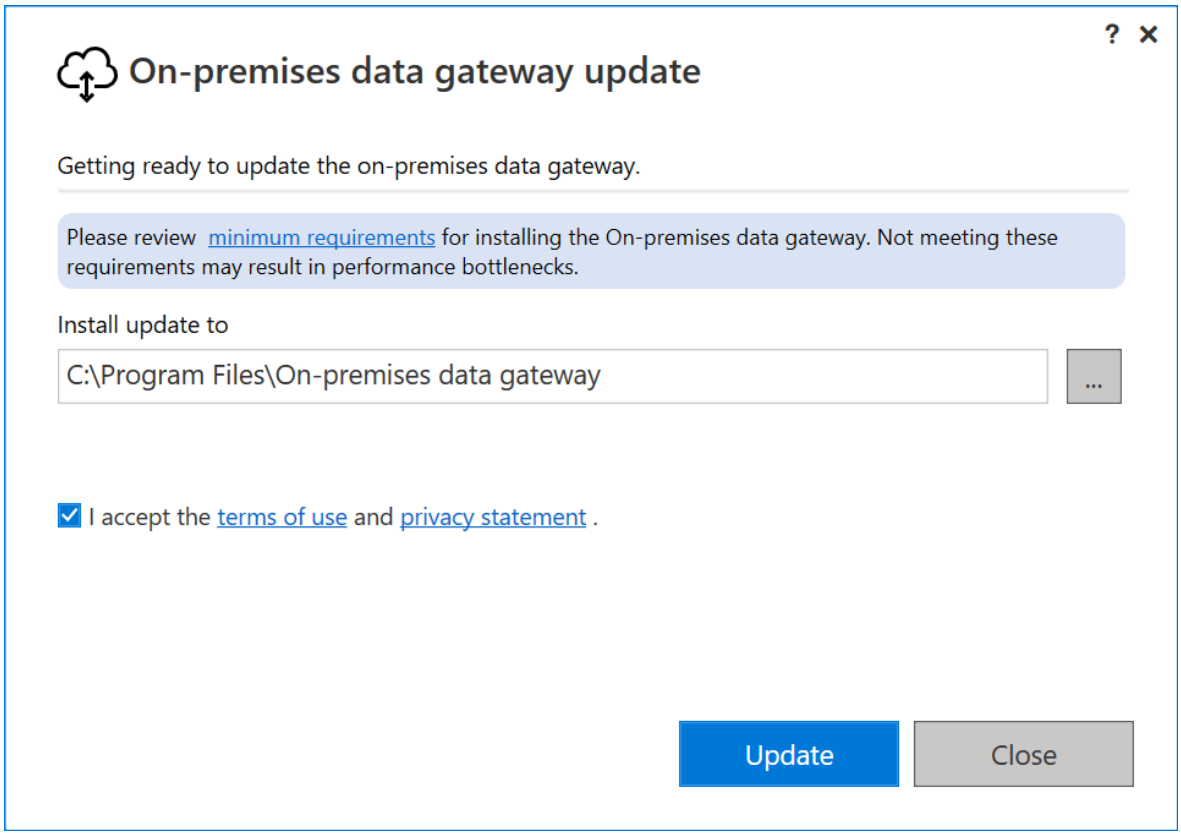
To update a gateway:

1. Download the latest standard mode gateway or personal mode gateway and run the installation program. If the version you're trying to install isn't newer than the version already installed, you'll receive one of the following error messages.

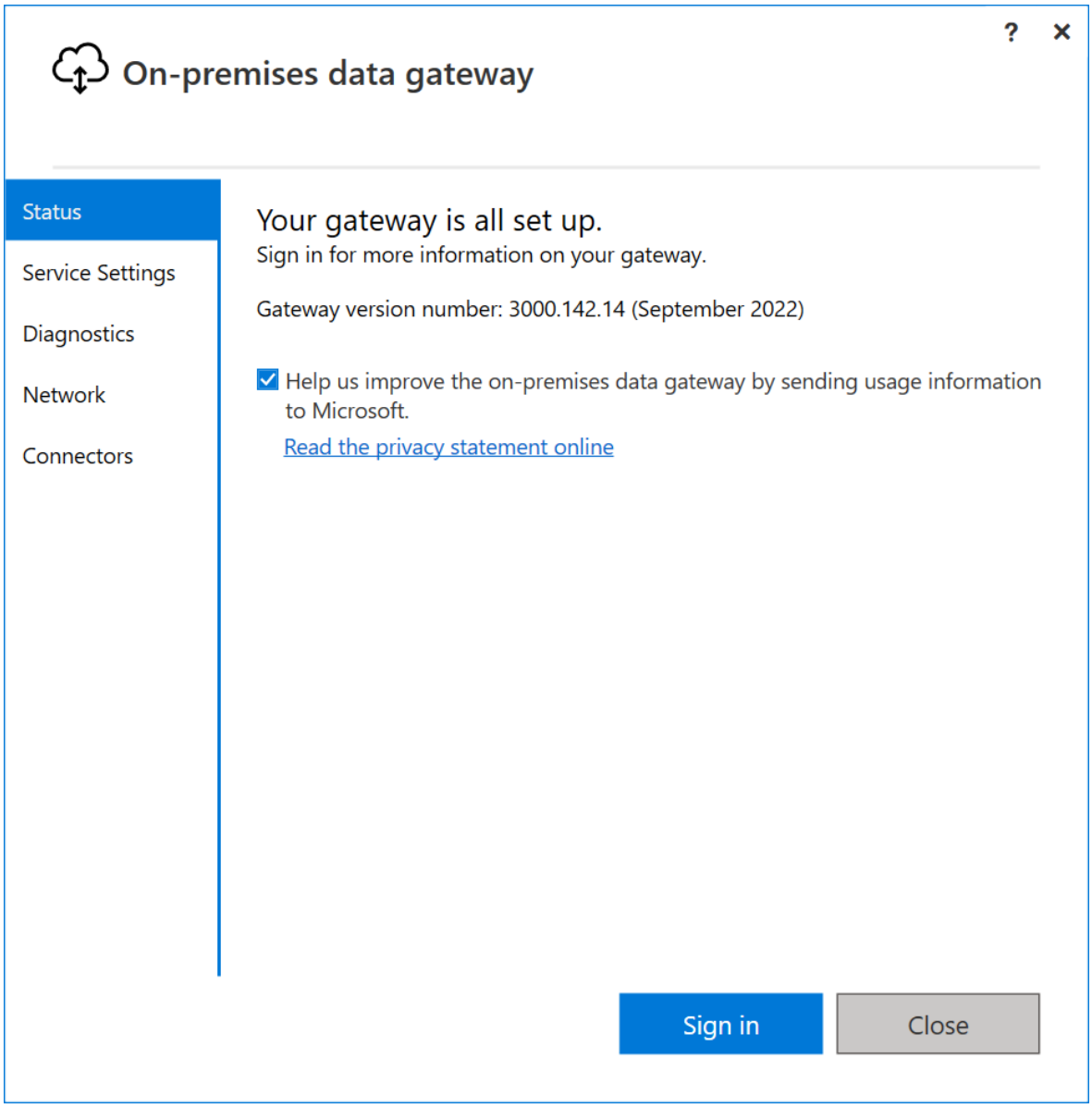




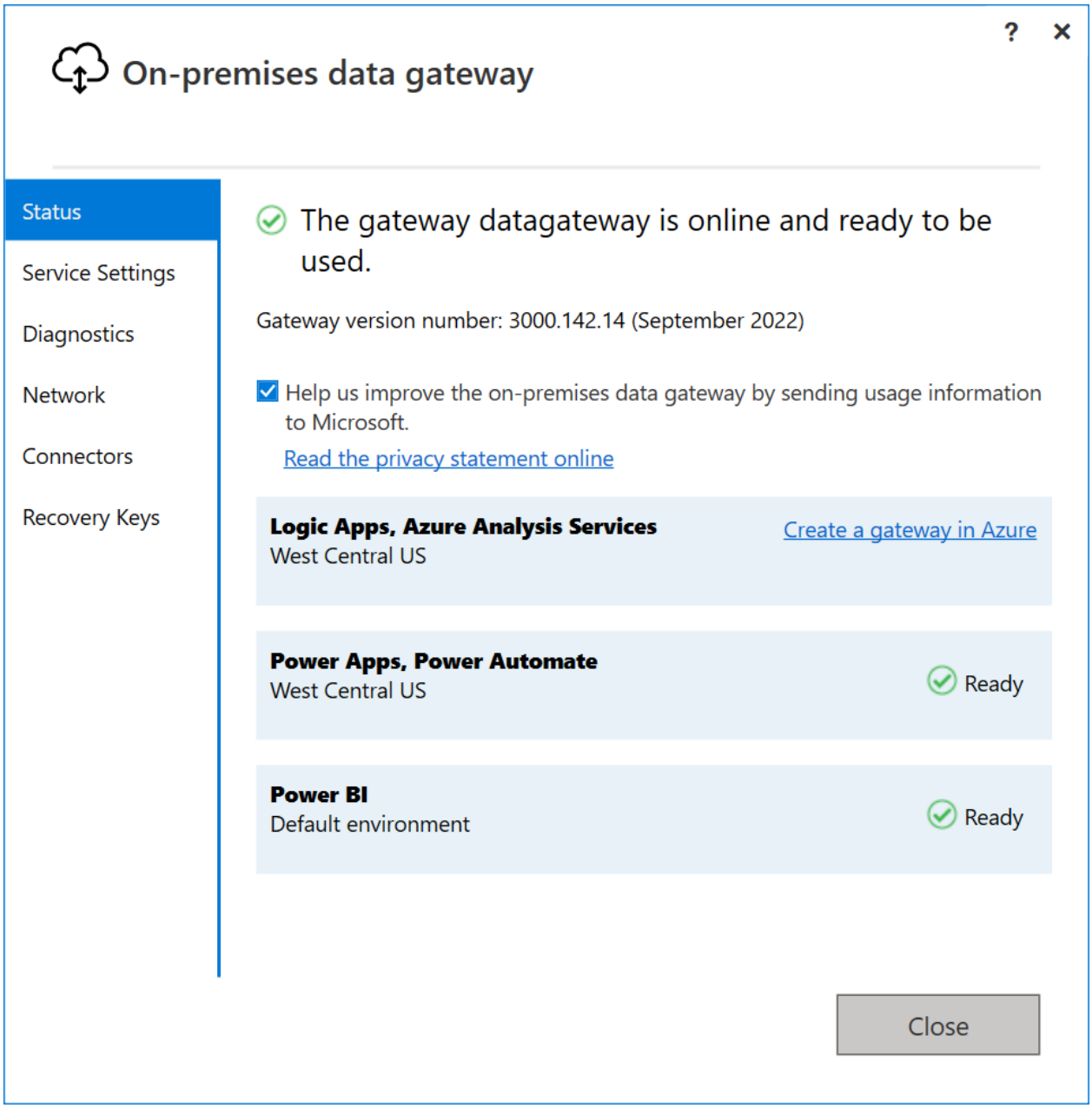
2. If you install a newer version, you'll be prompted to update. Select **Update** to begin updating.



3. After the installation finishes, select **Sign in**.



The gateway update is now complete.



Next steps

- Monitor and optimize gateway performance

Migrate, restore, or take over an on-premises data gateway

Article • 12/02/2022

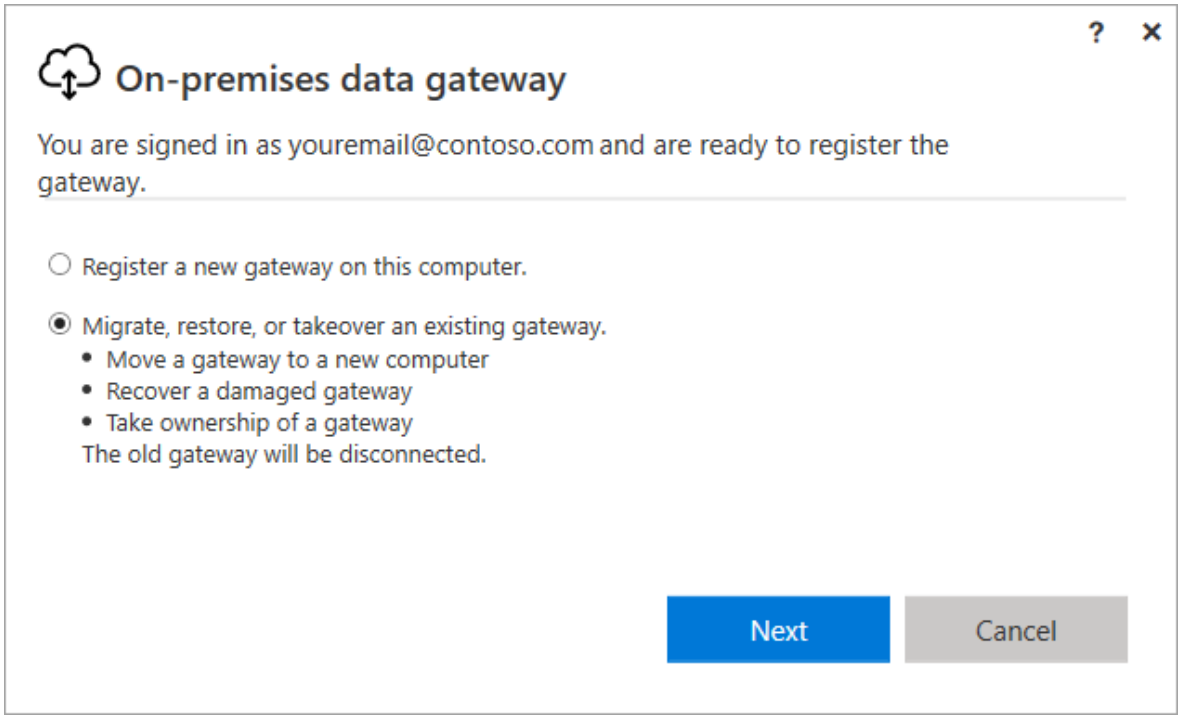
Run the gateway installer on a computer where you want to migrate, restore, or take over an on-premises data gateway.

If you're restoring the gateway on the computer that has the original gateway installation, you must first uninstall the gateway on that computer.

> **Note**
>
> If you **remove or delete a gateway cluster** in any of the cloud services, you won't be able to restore it.

1. Download the gateway and install it. For more information, go to Install an on-premises data gateway.

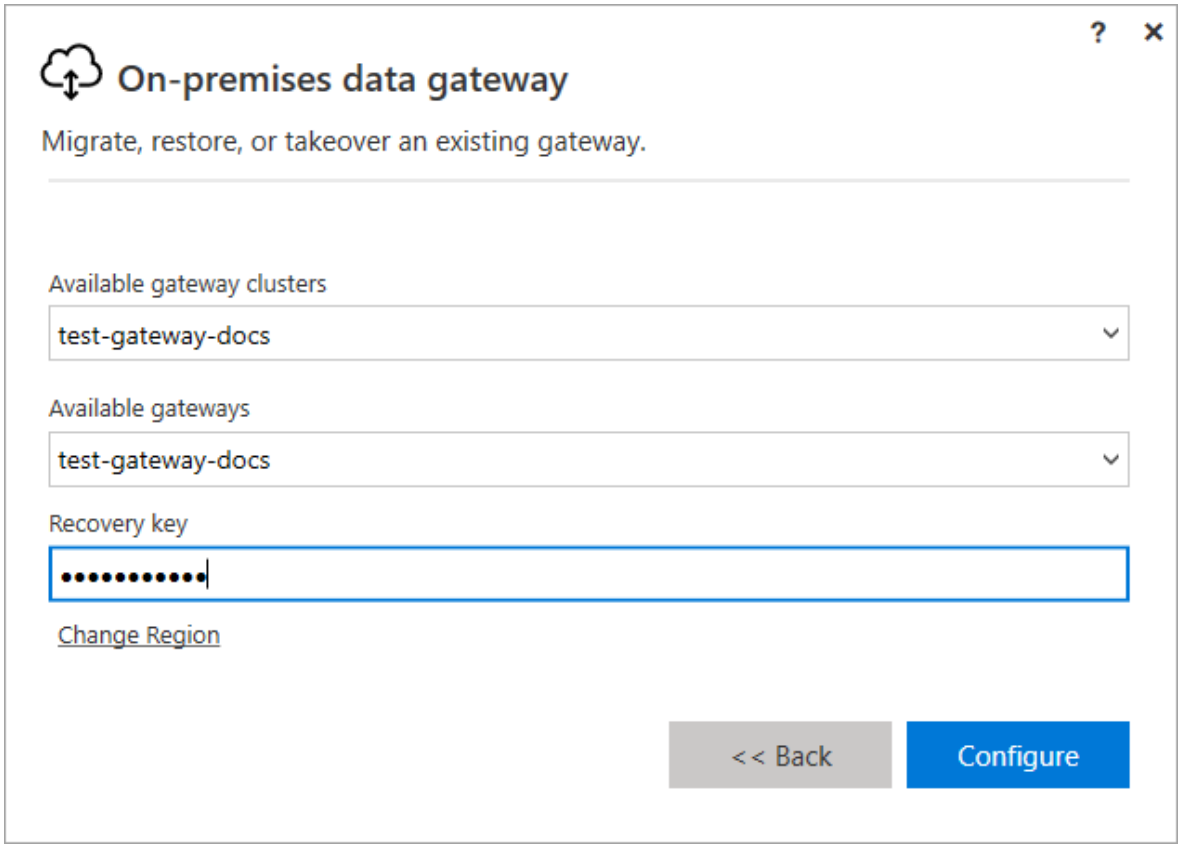
2. After you've signed in to your Office 365 account, register the gateway. Select **Migrate, restore, or takeover an existing gateway** > **Next**.



3. Select from the available clusters and gateways, and enter the recovery key for the selected gateway. You created and safely stored the recovery key when you originally installed the gateway. For more information, go to step 5 in Install an on-premises data gateway.

> **Important**
>
> Microsoft doesn't have access to this key and it can't be retrieved by us.

4. Select **Configure**.



After the configuration finishes, the process of migrating, restoring, or taking over is complete.

Minimize migration downtime

During migration of an on-premises data gateway, some downtime generally occurs. During this downtime, some in-progress refreshes might not succeed.

If a gateway only contains one member, you should expect the following to occur when you migrate the gateway:

- Expect all ongoing refreshes using the previous machine to be unsuccessful.
- Expect new refreshes starting a few minutes after migration to succeed.

The only way to ensure that there's 100% uptime during a migration:

1. Create a gateway with more than one gateway member (a cluster of gateways).

2. Disable the gateway that's going to be migrated (in the Power Platform admin center).
3. Migrate the disabled gateway member.
4. Re-enable the gateway member.

Next steps

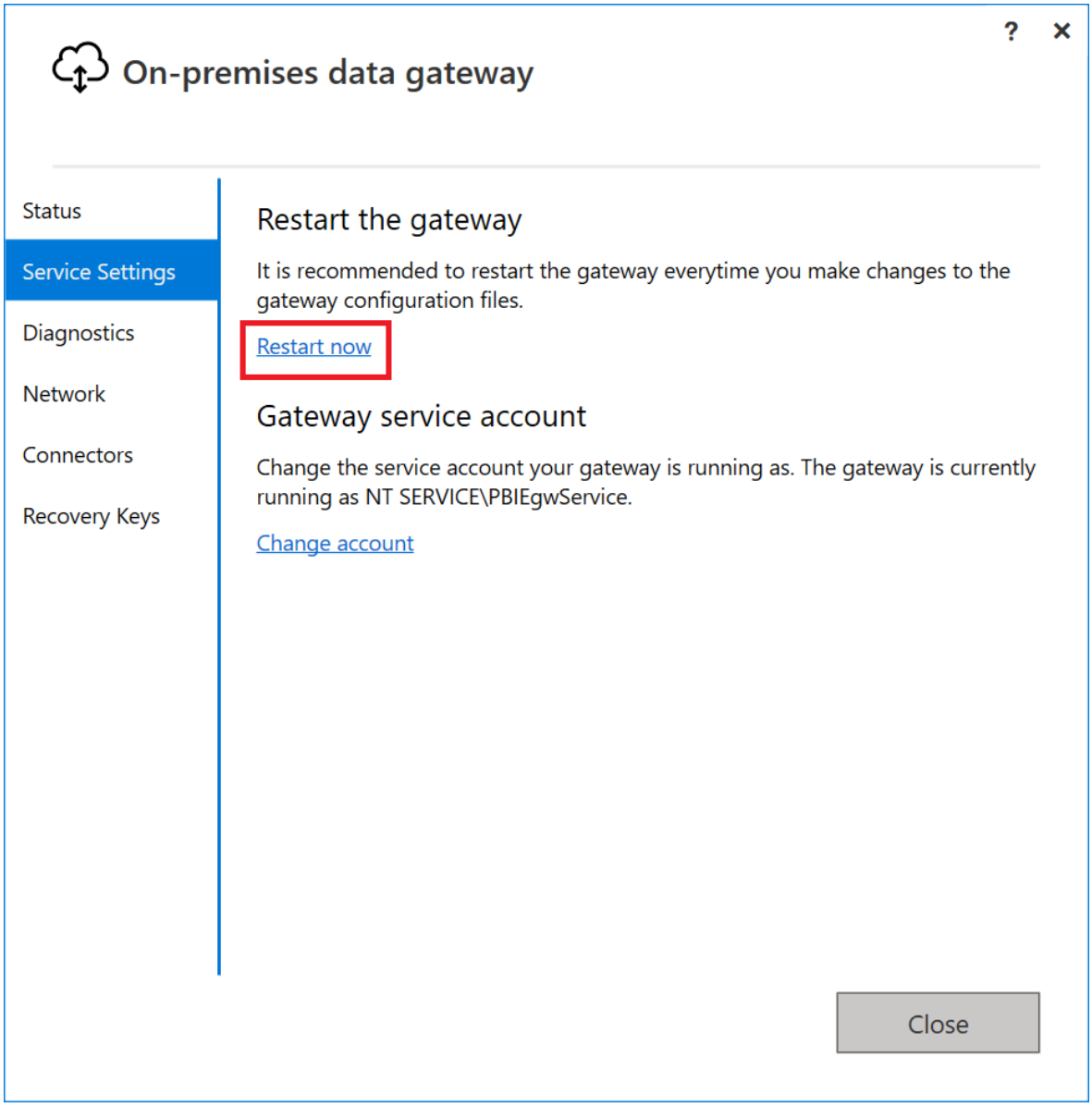
- Troubleshoot the on-premises data gateway

Restart an on-premises data gateway

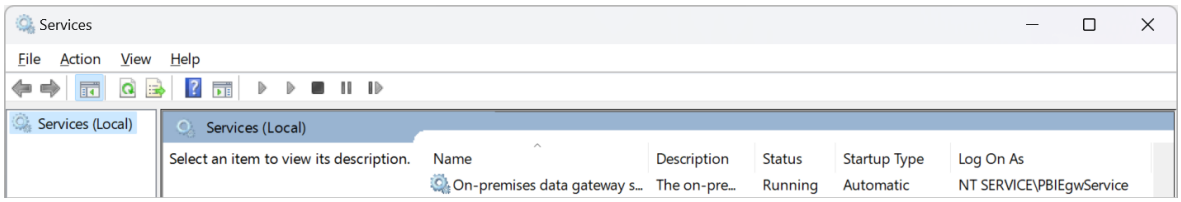
Article • 12/02/2022

Restart the on-premises data gateway service with any of the following methods.

- In the gateway app, select **Service Settings**, then select **Restart now**.



- In the services app, select the gateway service and then restart.



- In an admin Command Prompt window, use the following commands.

```
net stop PBIEgwService
```

```
net start PBIEgwService
```

Next steps

- Tenant level administration

Change the recovery key for an on-premises data gateway

Article • 12/02/2022

Starting with the November 2019 version of the on-premises data gateway (version 3000.14.39), you can change the recovery key that you specified during gateway installation.

The gateway uses the recovery key to create extra keys that encrypt data source and connection credentials. For more information about encryption, go to *When working with the on-premises data gateway, how are recovery keys used and where are they stored?* in the Power BI security whitepaper.

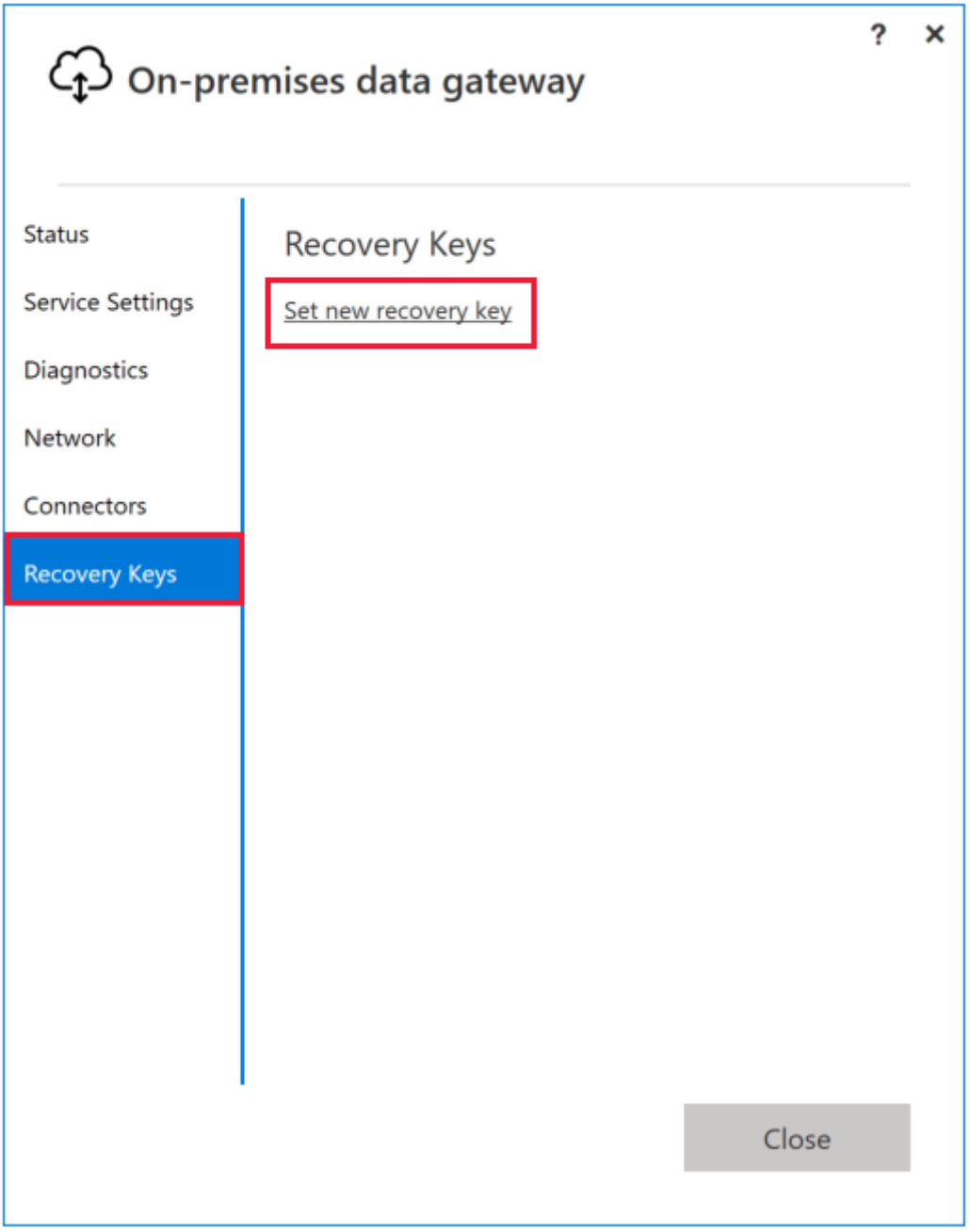
When you change the key, the process depends on whether you're using the gateway with Power BI or with another service:

- For Power BI, credentials for connections that use the gateway are automatically encrypted again with the new key.
- For other services, like Power Apps and Power Automate, connections aren't automatically encrypted with the new key. You must edit each connection to trigger encryption with the new key.

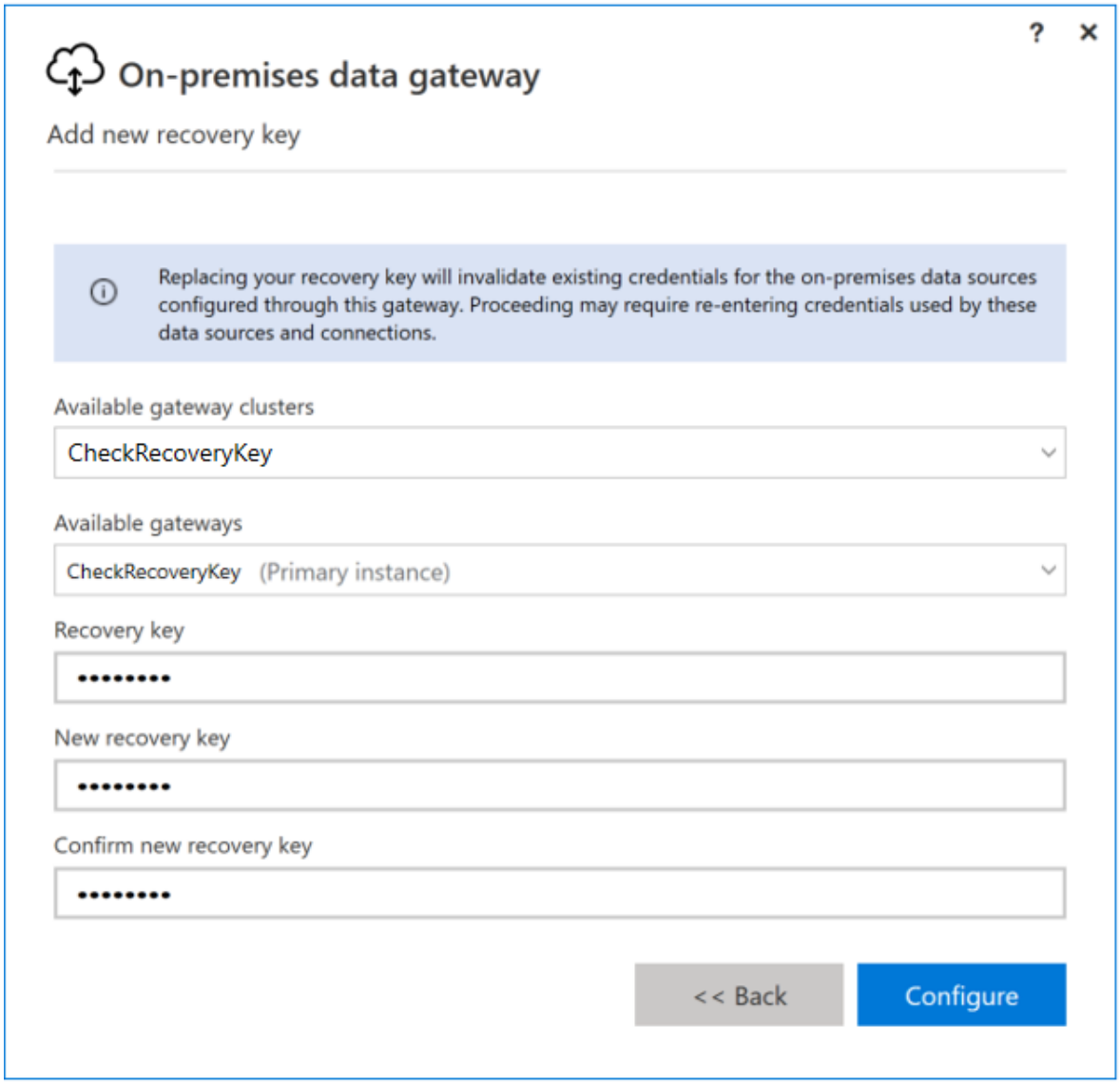
Change the recovery key

Use the following steps to change the recovery key.

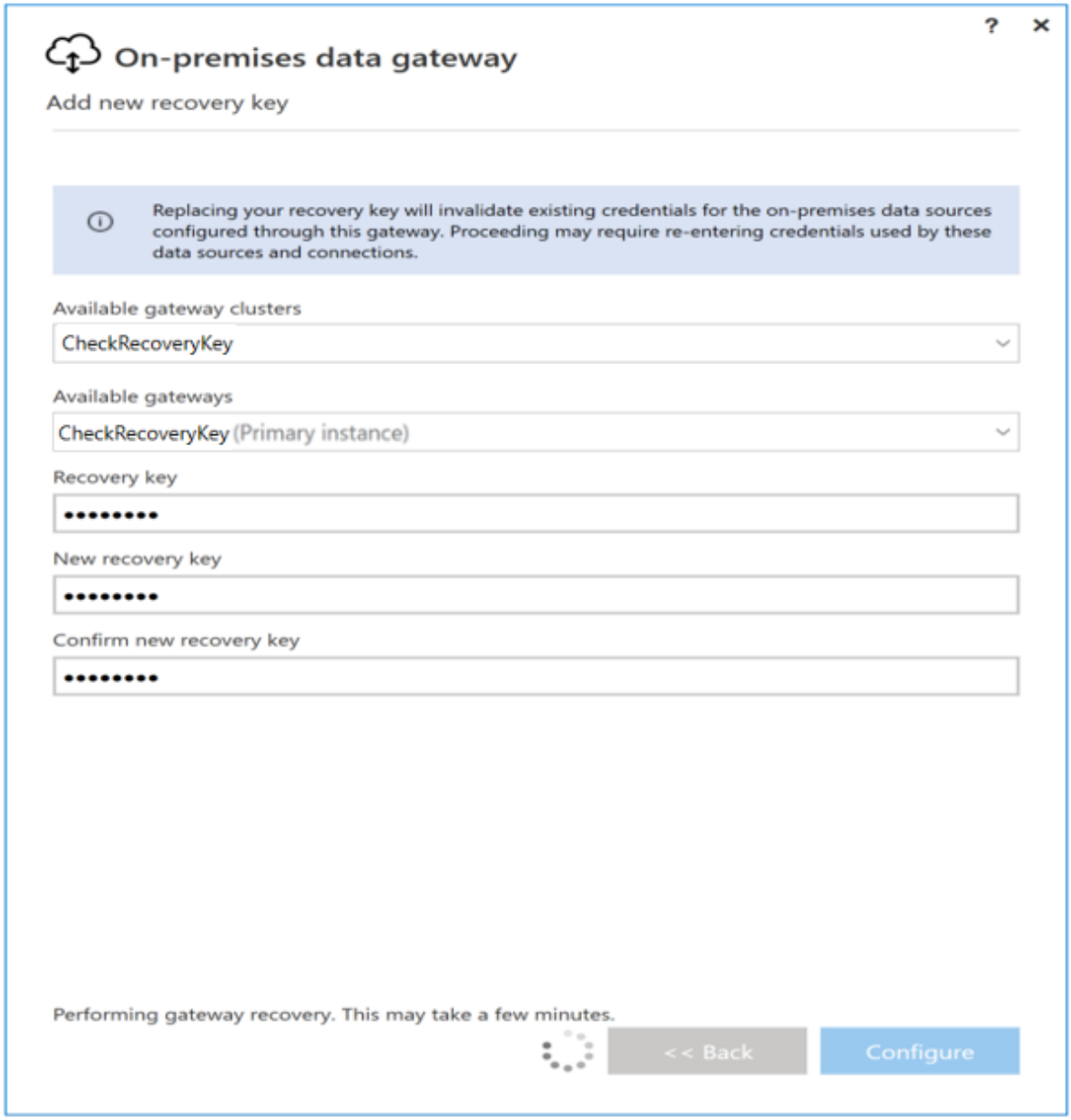
1. Open the on-premises data gateway app and sign in. If you have multiple gateway members in a cluster, you must sign in to the primary member.
2. On the **Recovery Keys** tab, select **Set new recovery key**. In a cluster with more than one member, this action disables all other gateway members. You re-enable these members later in this process.



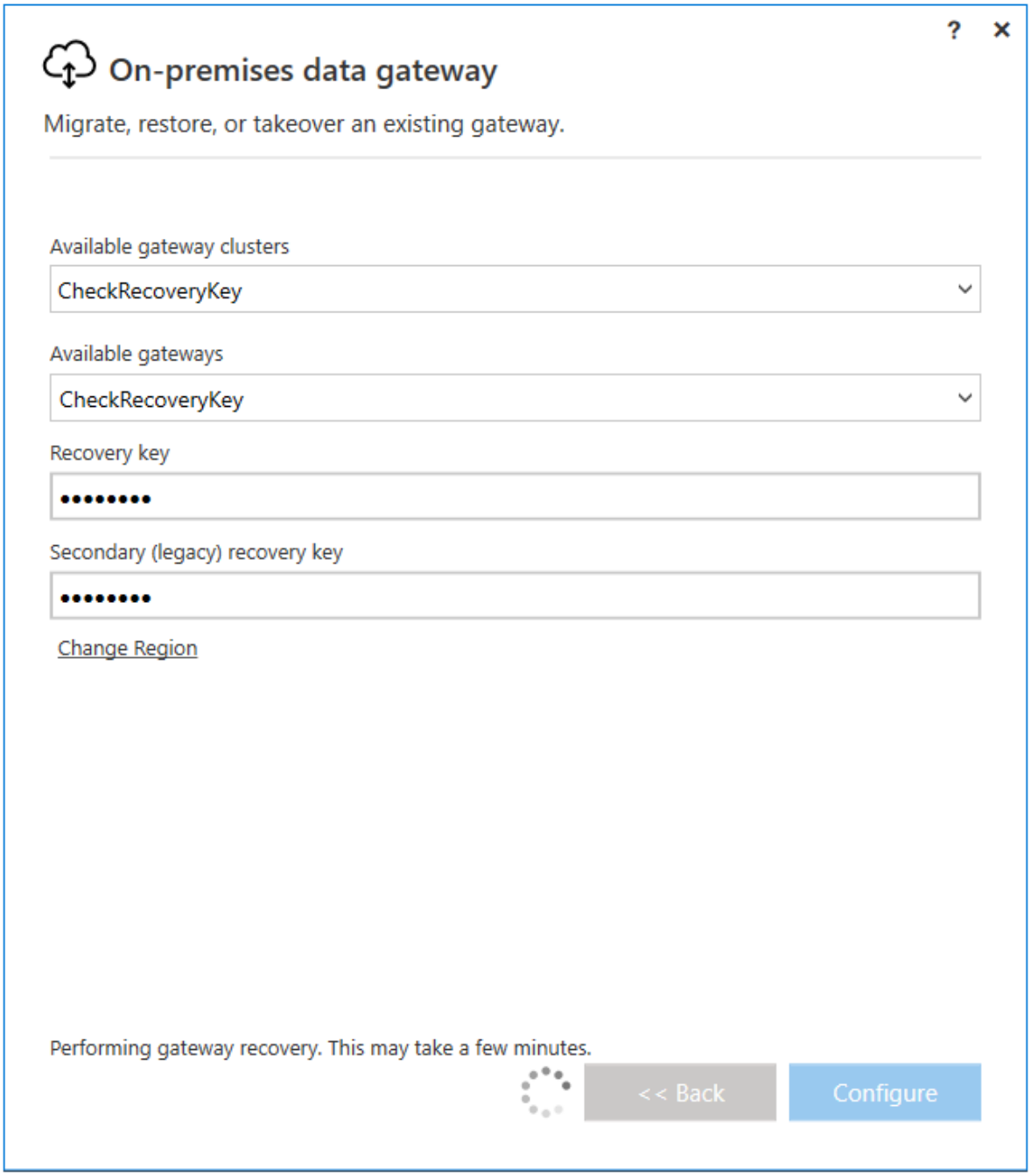
3. Enter the current recovery key and the new one.



4. Select **Configure** to change the recovery key. This step performs a recovery of the gateway and encrypts all Power BI data source credentials using the new recovery key.



After you've created the new key, the app shows that there's now a secondary or *legacy* recovery key. The gateway maintains both keys on the machine where it's installed, so connections that use the legacy recovery key don't fail. If you want to delete the legacy key, go to Delete the legacy recovery key.



5. If you have a gateway cluster with more than one member, perform an uninstall and recovery for each gateway member. The recovery process will ask for both the old and the new key.

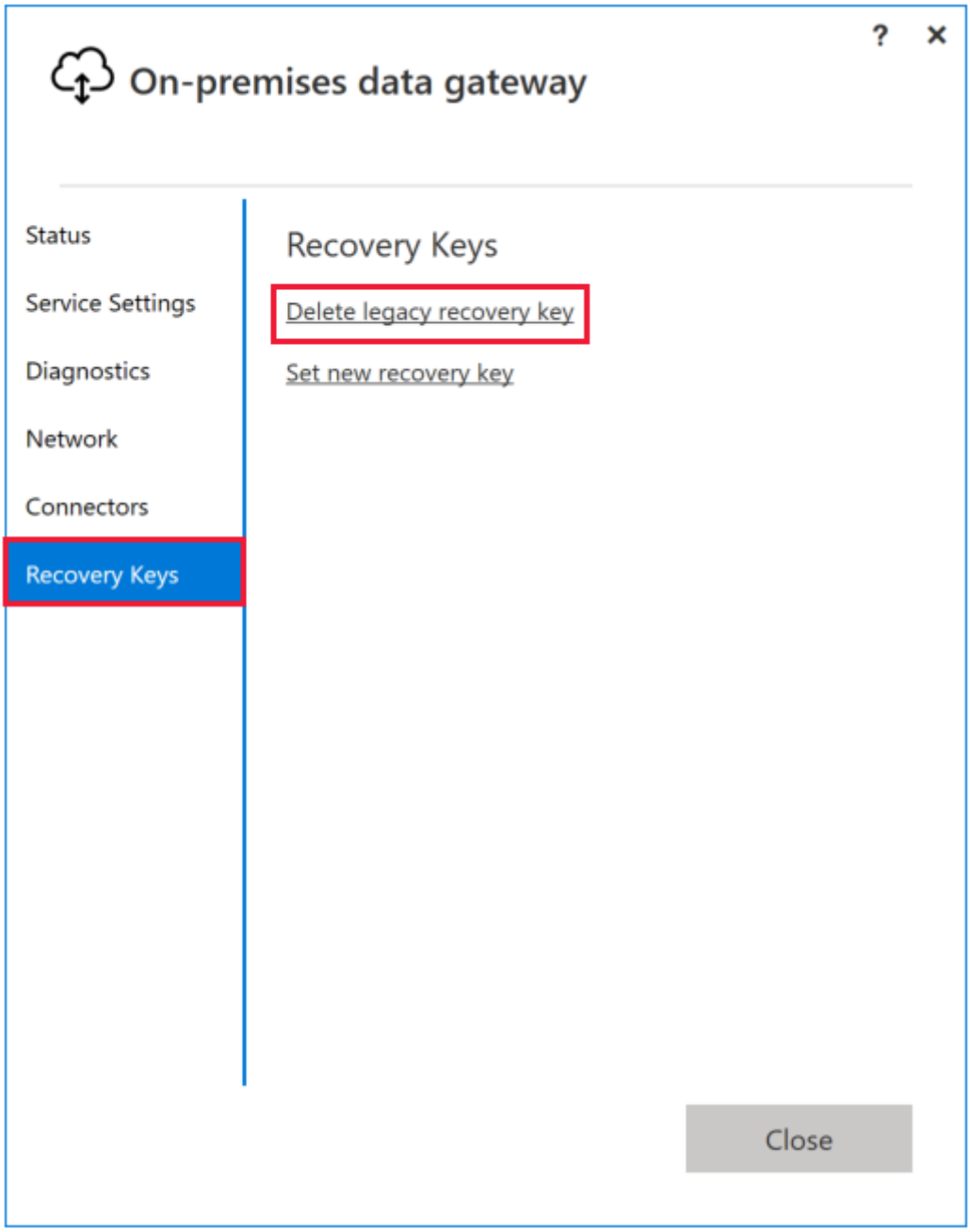
6. If you use the gateway with services other than Power BI, edit each connection to trigger encryption with the new key.

Delete the legacy recovery key

After you've created a new recovery key, you can delete the legacy recovery key. Before deleting the legacy key, make sure all connections using the gateway have had their credentials encrypted with the new key.

1. Open the on-premises data gateway app and sign in. If you have multiple gateway members in a cluster, you must sign into the primary member.

2. On the **Recovery Keys** tab, select **Delete legacy recovery key**.



Plan, scale, and maintain a business-critical gateway solution

Article • 12/02/2022

This article is intended for anyone planning to deploy an on-premises data gateway in a business-critical scenario. An on-premises data gateway is business-critical if it's vital to the normal operation of your business and handles business-critical data.

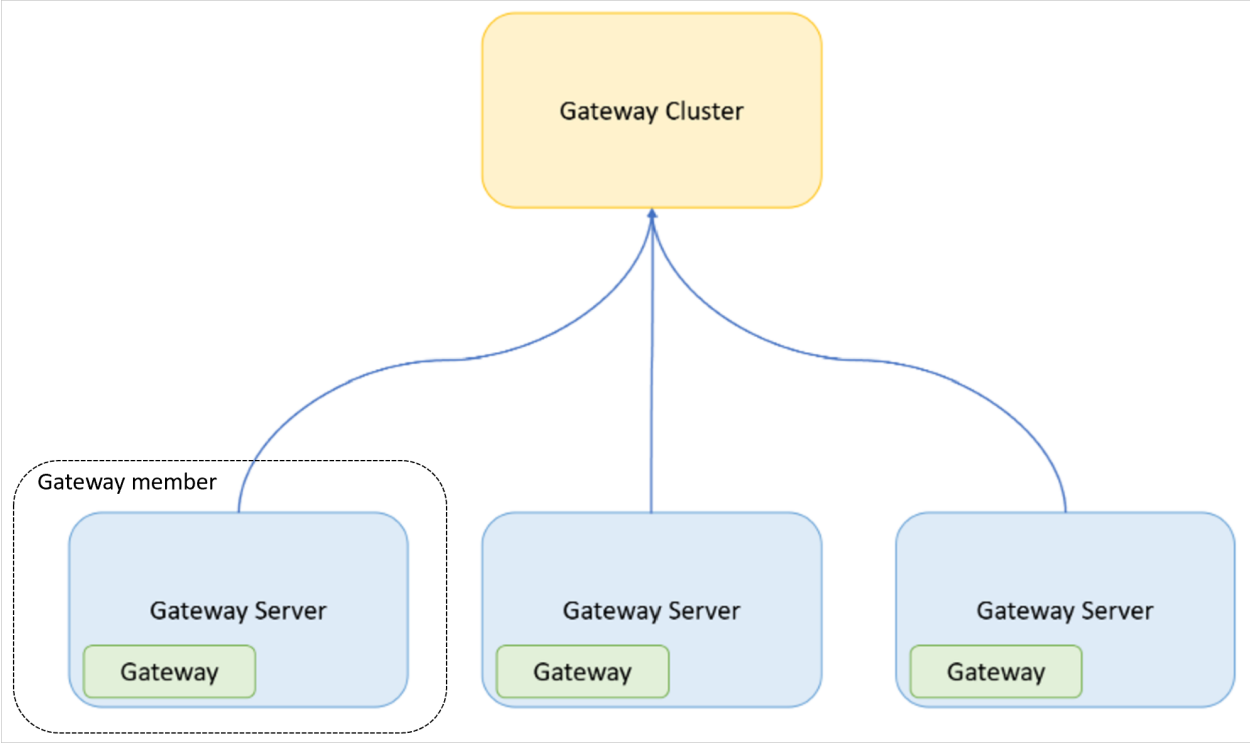
If business-critical gateways aren't managed properly, you might experience failed queries or slow performance. When you properly plan, scale, and maintain your business-critical gateway solution, the likelihood of a business-impacting issue can be minimized.

Terminology

The following important terms are used throughout this article:

- Gateway: The on-premises data gateway application that's installed on a computer.
- Gateway server: A Windows computer (virtual machine or physical computer/server) that has the on-premises data gateway application installed.
- Gateway cluster: A set of gateways that work together (and might be load balanced).
- Gateway member: A gateway that's a part of a gateway cluster.

The following image demonstrates the relationship between the concepts defined above.



Recommendations for business-critical gateways

For business-critical gateways, the gateways need to be deployed and managed properly to ensure high availability, good performance, and maintainable scalability. Deploying gateways incorrectly might result in poor performance, failed queries, and difficulty in diagnosing potential issues. It might also impede your ability to scale the gateways up and out as usage grows.

To ensure optimal scalability, performance, and throughput, follow the recommendations in the next sections.

Know all your gateway recovery keys

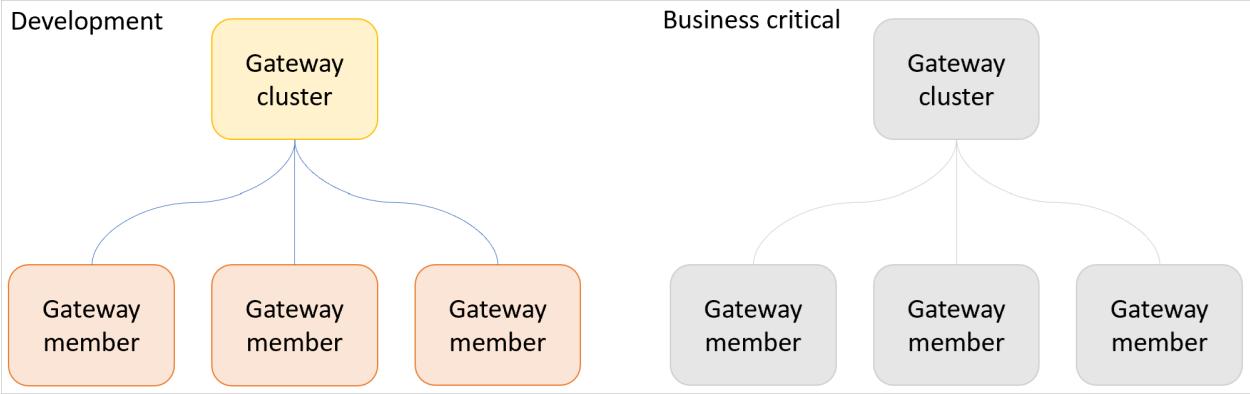
Ensure that all gateway recovery keys are **known and kept in a safe place**. Without a recovery key, gateways can't be recovered or downgraded. This limitation is by design. If you lose your recovery keys, the only option is to create new gateways and recreate the data sources. Also, you can't add new gateways to the cluster without the recovery key, which would limit future scalability.

Store your recovery keys in a secure place just as you would store administrative credentials, such as a password safe, which can be accessed only by authorized administrators.

If you currently don't know all your gateway recovery keys, this is a **significant business risk**. Immediately create new gateway clusters and start migrating workloads to the gateway clusters.

Development workloads and business-critical workloads

Separate development workloads from business-critical ones by setting up one or more development gateway clusters and one or more production gateway clusters as described below.



Use a development gateway cluster to test out new datasets, reports, queries, and so on. Once a new workload has been verified, migrate it to a business-critical gateway cluster. This process prevents new, untested, or experimental workloads from having performance impacts on productions workloads.

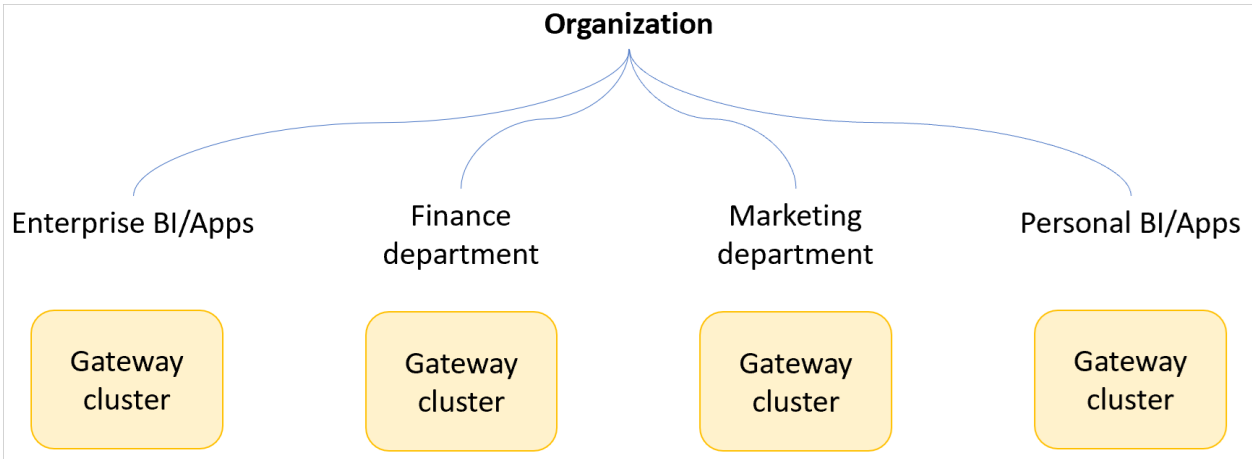
Also use your development gateway cluster(s) to test new gateway updates before applying updates to your business-critical gateway clusters. New gateway updates should be deployed for a minimum of 24 hours in the development gateway cluster(s) before being used on business-critical gateway cluster(s).

Use multiple gateway clusters

If you're creating a gateway cluster for a large number of users in your organization, you need to create multiple gateway clusters based on business units or smaller to limit any potential performance impact to a small subset of users.

We don't recommend that a single business-critical gateway cluster be used for an entire company (unless the company is small). In a single gateway cluster scenario, one user could conceivably send a query that causes a significant performance impact to all traffic across the gateway. If the gateway is used across the entire company, the performance impact could affect the entire company. Also, when a gateway cluster is used across an entire company, it might be more difficult for you to identify which query

might be causing a performance problem when using the gateway performance monitoring feature.



Use the gateway high availability and load balancing features

Always use the gateway high availability and load balancing features for any business-critical gateway cluster.

- High availability: Eliminates having a single point of failure.
- Load balancing: Automatically distributes the workload across all gateway servers in the cluster.

Set up a minimum of two gateways per gateway cluster in case a gateway goes offline for any reason. This setup ensures that a single gateway failure doesn't cause the entire gateway cluster to fail. Additionally, CPU, memory, concurrency limits can be enabled on the gateways to better distribute the load across the gateway cluster.

Plan and maintain gateway cluster scalability

Setting up a gateway cluster using our recommended hardware and software guidelines ensures the cluster runs with good performance. Gateways that aren't scaled properly might result in poor performance. There are many factors you must consider to have good performance on your gateway cluster.

Determine gateway server hardware specifications

Gateway server specifications (CPU, memory, disk, and so on) are an important factor, as in most cases, the Power Query transformations are applied to the data on the gateway server. As such, a gateway server needs to have enough resources, memory, and processing power to handle all the data transformations.

When you need to choose a server size, there are two metrics that are most important: Memory and CPU. You need both ample memory and CPU power to process the Power Query data transformation steps on the gateway. It's important that your gateway server is powerful enough to process the highest workload that you have. If the gateway server isn't able to handle the workload, your direct query or data refresh will fail. It's also important to understand how many queries are executed at the same time.

These different query options have a different effect on your gateway server.

Query Type	**Limit Factor**
Import	Memory
DirectQuery	CPU
LiveConnect	CPU

During an import, the entire set of data needs to be queried and processed, which is a memory heavy task. This importation often takes a longer time as well. DirectQueries and LiveConnections are commonly CPU heavy. In most cases, direct queries are executed many times to process only a small portion of the data. Since only a small portion of the data is processed, these direct queries aren't normally a memory heavy task. However, because the queries get executed many times on demand, this can be CPU intensive.

Depending on your workload, consider optimizing your gateway server for memory or CPU.

When to scale a gateway cluster

Scaling is an important aspect of a business-critical gateway cluster. As your usage with the gateway cluster grows, the gateway cluster needs to be scaled up and/or scaled out to ensure good performance. We recommend that you start scaling out a gateway cluster if you've previously scaled up the gateways in the cluster.

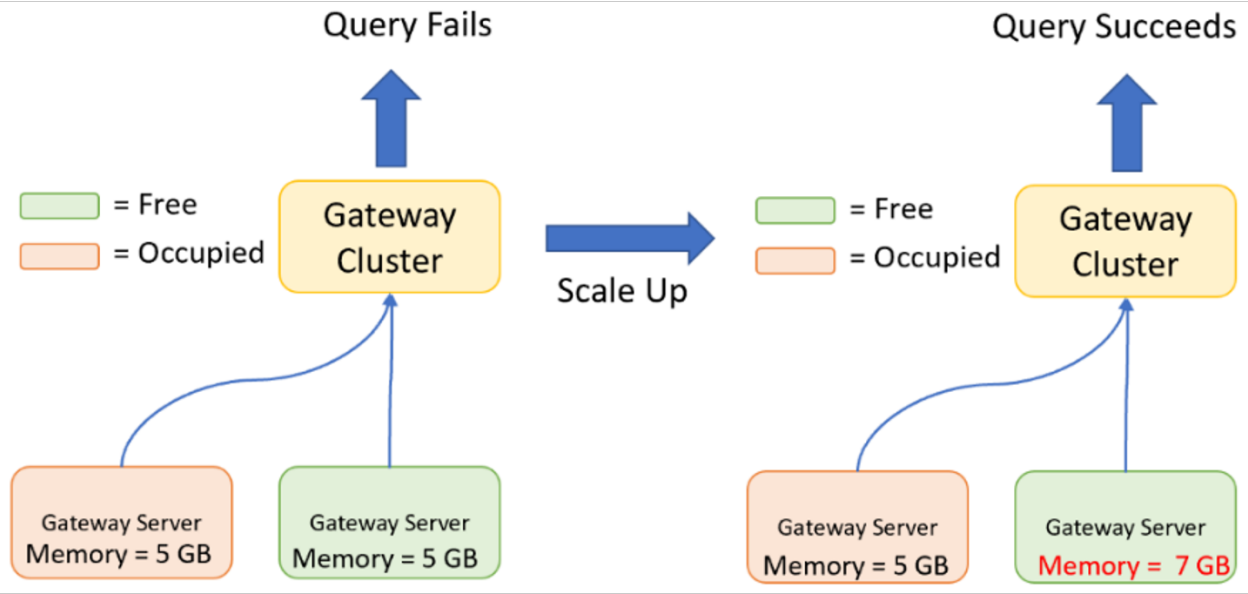
Scaling and distributing traffic load across individual nodes within a cluster is a complex process that varies depending on each individual scenario. While there's no definitive model to ensure that all gateway traffic will be predictably serviced, the limits listed below indicate a scaling need. In general, we recommend scaling out (adding nodes to the cluster) preferentially to scaling up (increasing CPU, RAM, or disk space on individual nodes). Scaling out tends to be more effective overall in the ability of the system as a whole to handle extra traffic. Scaling out also has a positive impact on total bandwidth the cluster can process, whereas scaling up generally doesn't. When one or more

gateway nodes show indications of reaching the thresholds described below, scaling out the cluster should be strongly considered.

- CPU: CPU is above 80% for extended periods of time, however occasional short (under 5 minutes) spikes that max out CPUs aren't abnormal.
- RAM: Available memory dips below 20% regularly.
- Disk: Free disk space dips below 5 GB frequently. This dip could also indicate a need to configure caching or spooling directories more strategically.
- Concurrency: Running more than 40 queries simultaneously on a single node.

Since refreshes and queries distributed across gateway nodes can have vastly different profiles, we also recommend extra scrutiny be placed on long-running or memory-intensive jobs. Query optimization in such cases can have a huge impact on performance and scalability, not only for the individual reports and refreshes, but on the system as a whole. We recommend isolating refreshes in question to a single dedicated gateway cluster to evaluate performance characteristics and perform optimization using query plan diagnostics, folding indicators, and all other published performance recommendations. This isolation minimizes the amount of data retrieved and the amount of post-processing required. This isolation can also be used as a long-term strategy to sequester long-running ETL jobs to a dedicated gateway cluster in order to reduce contention with other typical refreshes across the organization.

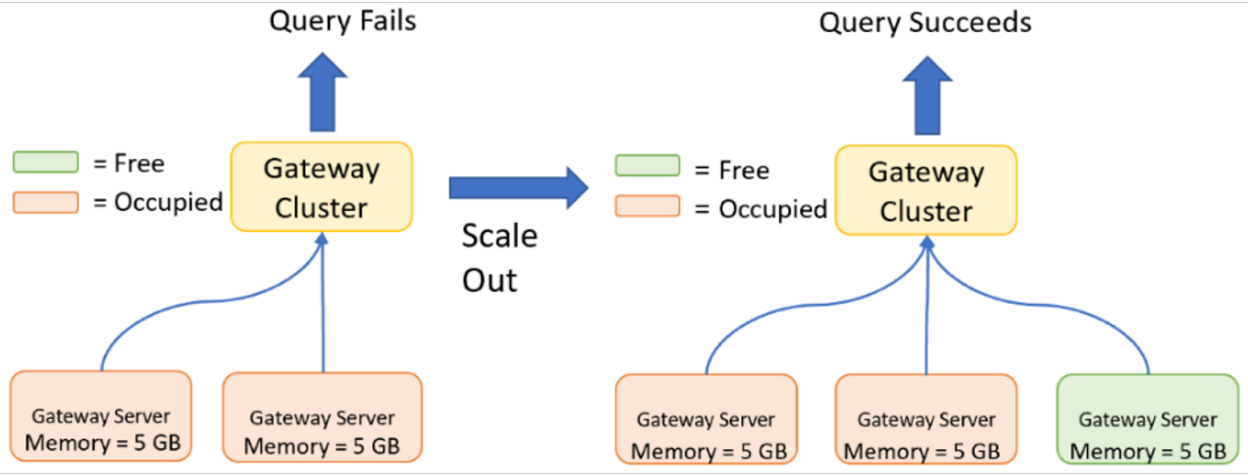
Scaling up a gateway cluster



Scaling up is when you increase the specifications (CPU, memory, disk, and so on) of your gateway servers.

Scaling up might be required if the maximum CPU or memory is reached when the gateway executes one or more queries. A query can only be executed on one gateway server, which is why the gateway server must have enough resources available to process the entire query along with the resulting data.

Scaling out a gateway cluster



Scaling out is required if the gateway server already has high specifications (in other words, the gateway server has been scaling up already), or you've reached the limits of what a single gateway server can manage because of the number of concurrent queries being executed. Broad-based load increase across the entire gateway member set is a good indication that scaling a cluster by adding nodes is the correct course of action. When to scale a gateway cluster provides specific thresholds that indicate when it's time to scale. For more information about scaling out, go to Use the gateway high availability and load balancing features.

Scaling by creating new gateway clusters

If the resource usage of your gateway cluster is high or an exceptionally large number of users rely on a gateway cluster, a new gateway cluster can be created. A subset of the workload can then be migrated to the new gateway cluster. When a large number of users rely on a single gateway cluster, the likelihood a user could send a query that causes a significant performance impact across the entire gateway cluster increases significantly.

An exceptionally large number of users relying on a single gateway cluster is an indicator that a new gateway cluster should be created.

Monitoring and troubleshooting gateway performance

It's important to monitor the overall performance of business-critical gateways using the gateway performance monitoring feature. You can also use this feature to troubleshoot performance problems, identify bottlenecks, and identify queries that are impacting overall gateway performance. This feature is also an important tool in helping you determine when to scale a gateway cluster.

If you identify a query as having a heavy impact on the gateway resulting in poor overall performance, you might be able to rewrite the query to be more efficient and minimize the performance impact.

If Microsoft identifies poor performance caused by a gateway or a gateway-related component, such as a Power BI Premium Capacity that's overloaded, the overloaded component must be remedied by scaling or reducing load. Microsoft doesn't investigate poor performance when a gateway or a gateway-related component is overloaded.

Troubleshoot the on-premises data gateway

Article • 05/08/2023

This article discusses some common issues when you use the on-premises data gateway.

> **Note**
>
> If you encounter an issue that isn't listed here, create a support ticket for the particular cloud service that's running the gateway.

Update to the latest version

It's a good general practice to make sure you're using a supported version. We release a new update of the on-premises data gateway every month. Currently, Microsoft actively supports only the last six releases of the on-premises data gateway. If you're experiencing issues with the version you're using, try upgrading to the latest one as your issue may have been resolved in the latest version.

Inconsistent versions between gateway members in a cluster

Keep the versions of the gateway members in a cluster in sync. Having all the same version in a cluster helps to avoid unexpected refresh failures. These refresh failures might occur because the gateway member that a specific query is routed to might not be capable of executing it due to a lower version.

Troubleshoot Gateway management

Here are a few common management issues and the resolutions that helped other customers.

Error while removing the primary node of a gateway cluster

The primary node of a gateway can't be removed if there are other members in the cluster. Removing the primary node also means removing the gateway cluster.

Troubleshoot common installation issues

Here are a few common installation issues and the resolutions that helped other customers.

Error: Failed to add user to group. (-2147463168 PBIEgwService Performance Log Users)

You might receive this error if you're trying to install the gateway on a domain controller. Deploying on a domain controller isn't supported. You need to deploy the gateway on a machine that isn't a domain controller.

Out-of-date antivirus software

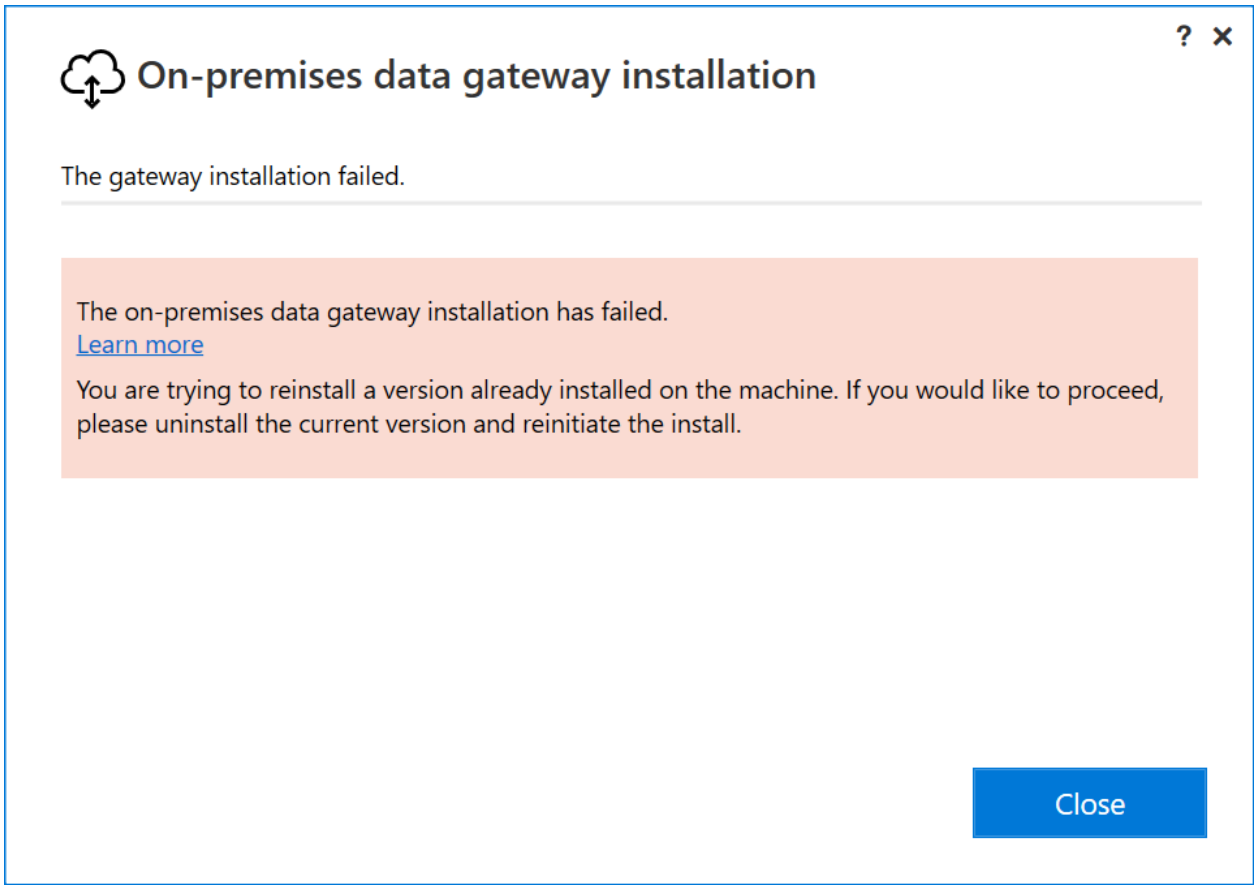
You might encounter installation failures if the antivirus software on the installation machine is out of date. You can either update the antivirus installation or disable the antivirus software only during the gateway installation. After the installation is finished, reenable the antivirus software.

McAfee Endpoint Defender software enabled

You might encounter installation failure when antivirus software, like McAfee Endpoint Defender, is enabled. Configure your antivirus software to ignore the gateway process.

Same or older gateway version

You might come across the following error if you try to install the same version or a previous version of the gateway compared to the one that you already have.



Error: The user profile is a temporary profile

There's an issue with the machine. Contact your internal IT team to remove the temporary profile.

Troubleshoot configuration

Firewall or proxy

To test if the gateway has access to all the required ports, run the network ports test. The results of the test are either Completed (Succeeded) or Completed (Failed, see last test results). If the test succeeded, your gateway successfully connected to all the required ports. If the test failed, your network environment might be blocking these required ports and servers.

For information on how to provide proxy information for your gateway, go to Configure proxy settings for the on-premises data gateway.

A firewall also might be blocking the connections that the Azure Relay makes to the Azure data centers. If that's the case, unblock the IP addresses for your region for those data centers. You can get a list of Azure IP addresses from this website. To find the current data center region you're in, go to Set the data center region.

Authentication to proxy server

Your proxy might require authentication from a domain user account. By default, the gateway uses a Service SID for the Windows service sign-in user. Changing the sign-in user to a domain user can help with this situation. For more information, go to Change the gateway service account to a domain user.

Your proxy only allows ports 80 and 443 traffic

Some proxies restrict traffic to only ports 80 and 443. By default, communication to Azure Relay occurs on ports other than 443.

You can force the gateway to communicate with Azure Relay by using HTTPS instead of direct TCP.

Gateway proxy unable to connect to Managed Data Lake

If you're using a proxy to access on-premises data using an on-premises data gateway, you might not be able to connect to a managed data lake (MDL) using the default proxy settings. To connect to MDL, be sure to add addresses `*.dfs.core.windows.net` and `*.blob.core.windows.net` to the allowlist on your proxy server.

System performance counter data is unavailable

If the current service account that is being used by the on-premises data gateway application isn't a member of the local security group **Performance Log Users**, you may observe in the System Counter Aggregation Report, that only system memory usage value is available.

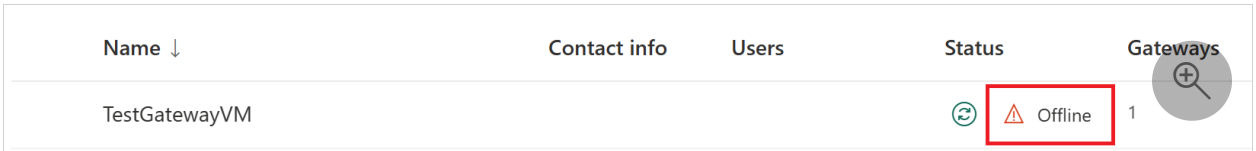
To address this behavior, add the on-premises data gateway service account to the local security group Performance Log Users, and restart the on-premises data gateway service.

Connectivity errors

When a gateway is facing connectivity issues, you might observe different symptoms. Here are a few of the common symptoms.

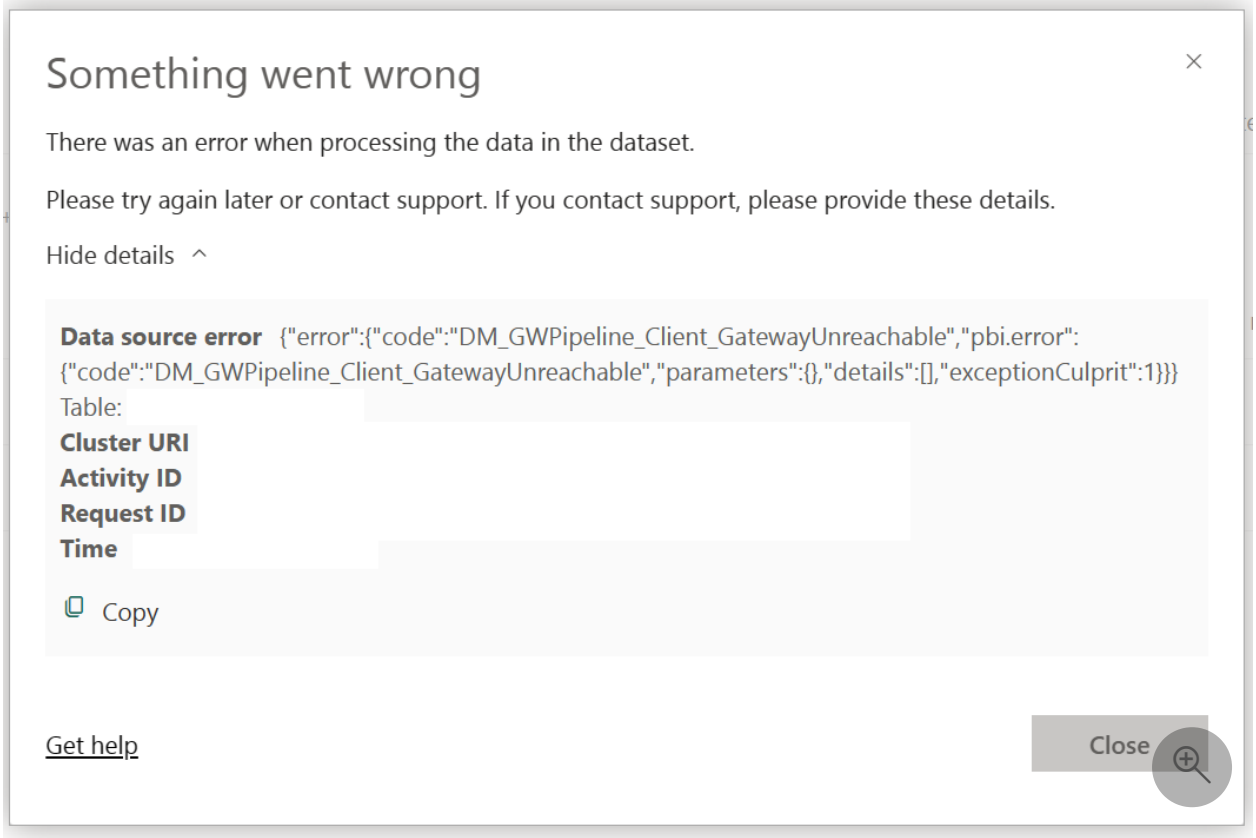
Error: Gateway shows offline status in Manage Gateways page

You might come across one of the following indications in the manage gateways page if there's a connectivity issue.



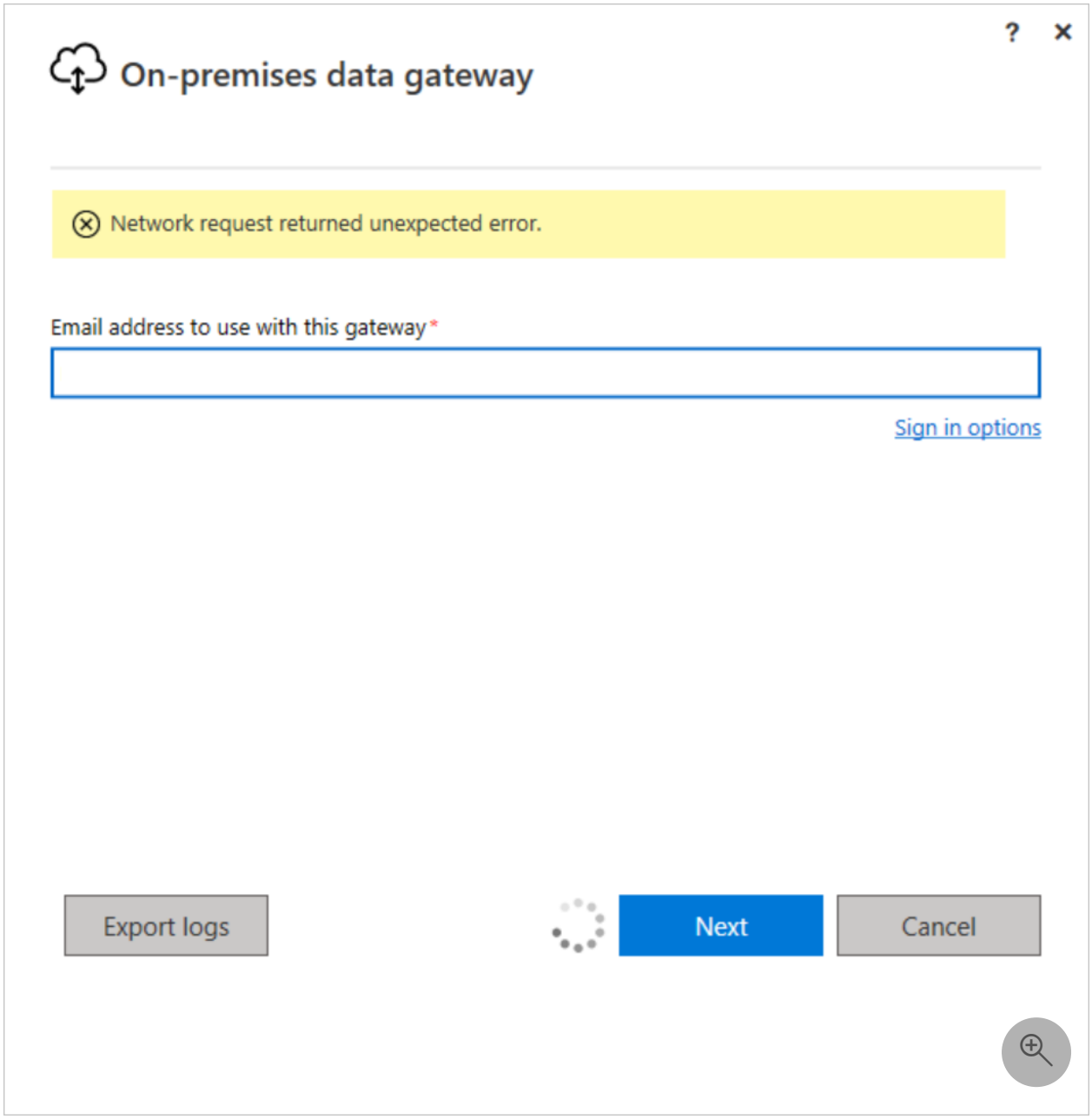
Error: Your data gateway is offline or couldn't be reached.

You might come across one of the following data refresh errors if there's a connectivity issue.



Error: Network request returned unexpected error.

You might come across one of the following errors when trying to sign in to the gateway configurator if there's a connectivity issue.



Connectivity issues can have several different causes. Therefore, if you run into any of the previously mentioned symptoms, perform the following verifications:

1. Are the FQDNs and ports mentioned in our documentation opened/allowed in your firewall and/or proxy?

2. If you are using a proxy server in your environment:
   a. Make sure the proxy server is properly configured in the Gateway config files.
   b. Verify if the proxy configuration is consistent.
   c. Check your proxy logs to check if there are any requests being blocked at the proxy level.

3. Is your Firewall just allowing the communication on ports 80 and 443?
   a. If yes, ensure the HTTPS mode in gateway is enabled.

Common errors

Error: Failed to create a gateway. Try again.

This error could be due to proxy configuration issues. The gateway log provides more details for troubleshooting. For more information, go to Configure proxy settings for the on-premises data gateway.

Error: Power BI service reported local gateway as unreachable. Restart the gateway and try again.

At the end of configuration, the Power BI service is called again to validate the gateway. The Power BI service doesn't report the gateway as *live*. Restarting the Windows service might allow the communication to be successful. To get more details, collect and review the logs, as described in the following section.

Error: Information is needed in order to combine data

You may experience a refresh failure in Power BI service with an error "Information is needed in order to combine data", even though refresh on Power BI Desktop works. This problem occurs when the refresh in Power BI Desktop works with the **File** > **Options and settings** > **Options** > **Privacy** > **Always ignore privacy level settings** option set, but throws a firewall error when other options are selected. If you attempt to preform this refresh in Power BI service, the refresh won't work because **Always ignore privacy level settings** isn't available in Power BI service. To resolve this error, try changing the privacy level in the Power BI desktop **Options** > **Global** > **Privacy** and **Options** > **Current File** > **Privacy** settings so that it doesn't ignore the privacy of data. Republish the file to Power BI service and update the credentials to "Organizational" in Power BI service.

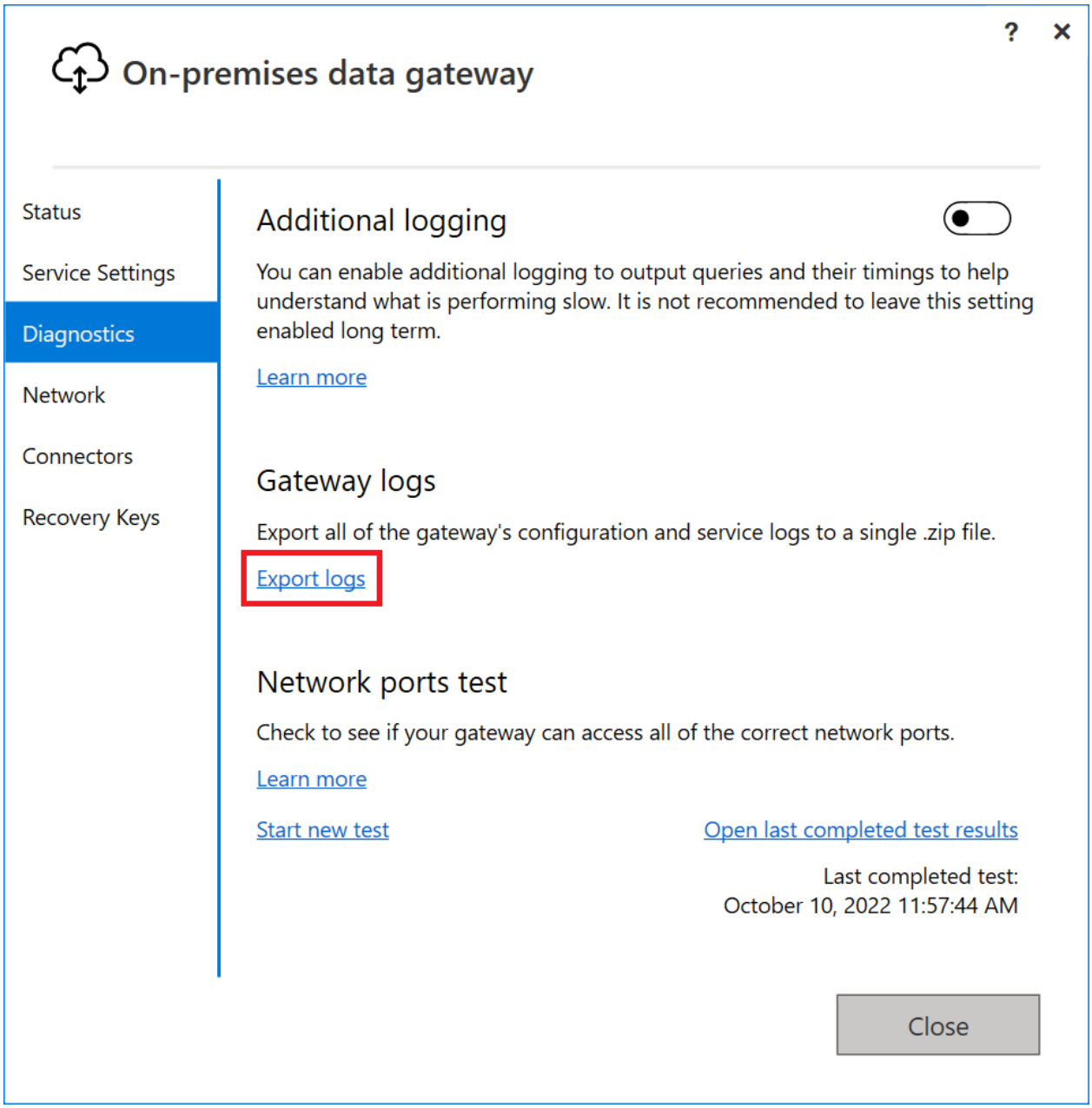
Error: There are too many refreshes occurring concurrently.

The gateway has a concurrency limit of 30. If you're getting this error, it means you reached the concurrency limit. You can monitor the concurrency count with the gateway diagnostics template. To avoid running into this issue, upgrade the number of gateways in a cluster or start a new cluster to load balance the request.

Troubleshooting tools

Collect logs from the on-premises data gateway app

There are several logs you can collect for the gateway, and you should always start with the logs. The simplest way to collect logs after you install the gateway is through the on-premises data gateway app. In the on-premises data gateway app, select **Diagnostics** and then select the **Export logs** link, as shown in the following image.

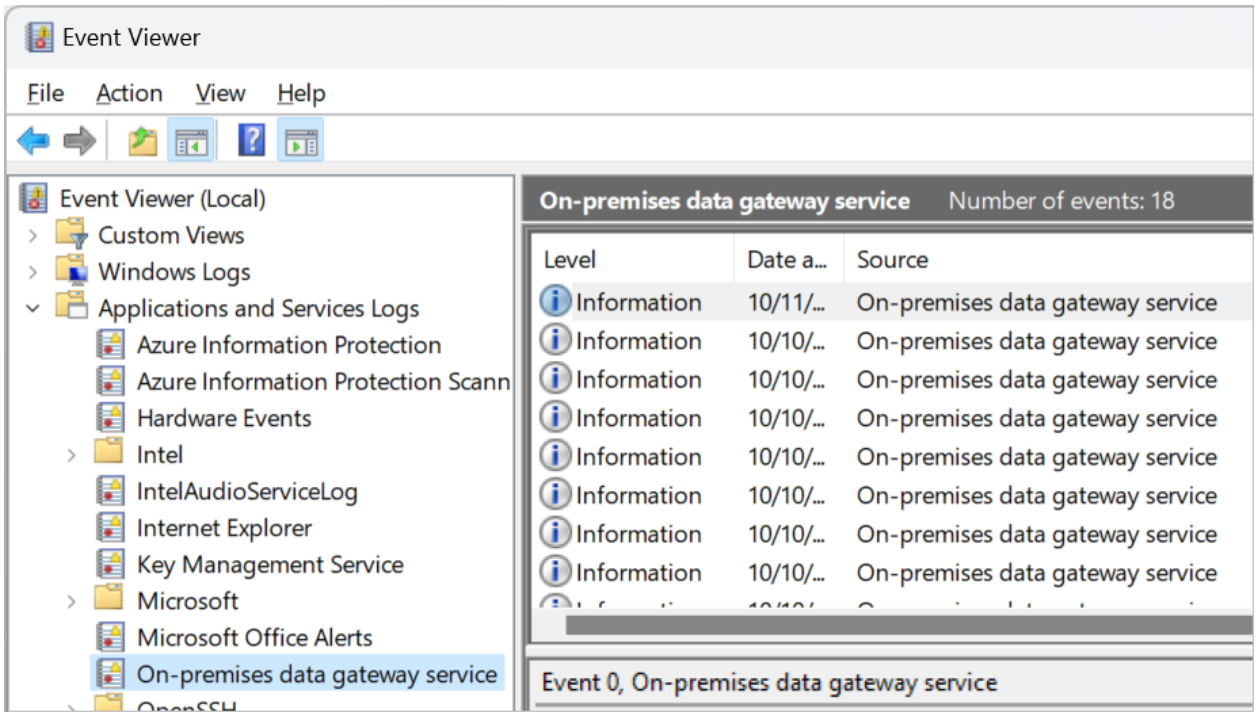


This file is saved to the ODGLogs folder on your Windows desktop in .zip format.

Event logs

To find the event logs for the *on-premises data gateway service*, follow these steps:

1. On the computer with the gateway installation, open the **Event Viewer**.
2. Expand **Event Viewer** > **Applications and Services Logs**.
3. Select **On-premises data gateway service**.



Troubleshoot refresh failures for a specific source

Refreshes utilizing the gateway require that the source be accessible from the computer with the gateway installation. To troubleshoot a data source issue, use Power BI Desktop locally on the gateway computer to test the connection. This test is especially helpful if the data source requires additional components to be installed on the computer, such as a third-party database driver. Also, a local test helps to test data source connections that require additional environment settings, such as access to a shared network drive file or folder. This technique allows you to test iteratively, testing the connection on the gateway computer after each configuration change.

Although it isn't a guarantee of a successful refresh through the gateway, a successful Power BI Desktop refresh from the gateway computer is a strong indicator that everything is configured correctly on the gateway computer. In other words, if you can't refresh in Power BI Desktop from the gateway computer, it's highly unlikely that a refresh through the gateway will succeed. After a successful refresh in Desktop, you can narrow your troubleshooting steps to the configuration of the datasource and the dataset in the Power BI Service.

Limitations and considerations

The Power BI gateways REST APIs don't support gateway clusters.

Next steps

- On-premises data gateway

Monitor and optimize on-premises data gateway performance

Article • 05/22/2023

Gateway performance monitoring (public preview)

To monitor performance, gateway admins have traditionally depended on manually monitoring performance counters through the Windows Performance Monitor tool. We now offer additional query logging and a Gateway Performance PBI template file to visualize the results. This feature provides new insights into gateway usage. You can use it to troubleshoot slow-performing queries.

> **Note**
>
> This feature is currently available only for the on-premises data gateway in the standard mode. It's not available for the personal mode.

> **Note**
>
> Gateway diagnostics doesn't capture diagnostics directly related to the (virtual) machine and its network, like bandwidth or latency. However, these diagnostics might impact your gateway performance. You can use resource monitoring tools to monitor your machine.

Performance logging

This feature is now turned on by default.

> **Note**
>
> - Currently, queries from premium capacity to the gateway are sometimes missed in this logging. We are actively working on fixing this issue.
> - Currently, Power BI paginated report queries aren't logged using this tool.

Configure Performance logging

There are other values in the config file `C:\Program Files\On-premises data gateway\Microsoft.PowerBI.DataMovement.Pipeline.GatewayCore.dll.config` that you can update as needed:

- **ReportFilePath**: Determines the path where the four log files are stored. By default, this path is either *\Users\PBIEgwService\AppData\Local\Microsoft\On-premises data gateway\Report* or *\Windows\ServiceProfiles\PBIEgwService\AppData\Local\Microsoft\On-premises data gateway\Report*. The path depends on the OS version. If you use a service account for the gateway other than *PBIEgwService*, replace this part of the path with the service account name.
- **ReportFileCount**: Determines the number of log files of each kind to retain. The default value is 10.
- **ReportFileSizeInBytes**: Determines the size of the file to maintain. The default value is 104,857,600.
- **QueryExecutionAggregationTimeInMinutes**: Determines the number of minutes for which the query execution information is aggregated. The default value is 5.
- **SystemCounterAggregationTimeInMinutes**: Determines the number of minutes for which the system counter is aggregated. The default value is 5.

After you make the changes to the config file, restart the gateway for these config values to take effect. The report files are now being generated in the location that you specified for **ReportFilePath**.

> ⓘ **Note**
>
> It can take up to 10 minutes plus the amount of time set for **QueryExecutionAggregationTimeInMinutes** in the config file until files start to show up in the folder.

Understand performance logs

When you turn on this feature, four new log files are created:

- The Query Execution Report
- The Query Start Report
- The Query Execution Aggregation Report
- The System Counter Aggregation Report

The Query Execution Report contains detailed query execution information. The following attributes are captured.

Attribute	Description
GatewayObjectId	Unique identifier for the gateway.
RequestId	Unique identifier for a gateway request. It could be the same for multiple queries.
DataSource	Contains both the data source type and data source.
QueryTrackingId	Unique identifier for a query. It may however repeat if a query fails and is retried.
QueryExecutionEndTimeUTC	Time when the query execution completed.
QueryExecutionDuration (ms)	Duration for a query execution.
QueryType	Type of query. For instance, the query passed could be a Power BI refresh or DirectQuery. Or, it could be queries from Power Apps and Power Automate.
DataProcessingEndTimeUTC	Time when data processing activities like spooling, data retrieval, compression, and data processing completed.
DataProcessingDuration (ms)	Duration for data processing activities like spooling, data retrieval, compression, and data processing.
Success	Indicates if the query succeeded or failed.
ErrorMessage	If the query failed, indicates the error message.
SpoolingDiskWritingDuration (ms)	Indicates the amount of time by the gateway to write all data to disk
SpoolingDiskReadingDuration (ms)	Indicates the amount of time by the gateway to read all data to disk
SpoolingTotalDataSize (bytes)	Size(Compressed) of the data that is written to/read from disk
DataReadingAndSerializationDuration (ms)	Indicates the amount of time the gateway takes to read data from the datasource and serialize them into packets.
DiskRead (byte/sec)	Indicates bytes read by the gateway per second. DiskRead(byte/sec) = SpoolingTotalDataSize / SpoolingDiskReadingDuration

Attribute	Description
DiskWrite (byte/sec)	Indicates bytes written by the gateway per second. DiskWrite(byte/sec) = SpoolingTotalDataSize / SpoolingDiskWritingDuration

The Query Start Report contains the query and the query start time. The following attributes are captured.

Attribute	Description
GatewayObjectId	Unique identifier for the gateway.
RequestId	Unique identifier for a gateway request. It could be the same for multiple queries.
DataSource	Contains both the data source type and data source.
QueryTrackingId	Unique identifier for a query. It may however repeat if a query fails and is retried.
QueryExecutionStartTimeUTC	Time when the query execution started.
QueryType	Type of query. For instance, the query passed could be a Power BI refresh or DirectQuery. Or, it could be queries from Power Apps and Power Automate.
QueryText	Complete query encoded with base64.

The Query Execution Aggregation Report contains query information aggregated to a time interval by **GatewayObjectId**, **DataSource**, **Success**, and **QueryType**. The default value is 5 minutes, but you can adjust it. The following attributes are captured.

Attribute	Description
GatewayObjectId	Unique identifier for the gateway.
AggregationStartTimeUTC	Start of the time window for which query attributes were aggregated.
AggregationEndTimeUTC	End of the time window for which query attributes were aggregated.
DataSource	Contains both the data source type and data source.
Success	Indicates if the query succeeded or failed.
AverageQueryExecutionDuration (ms)	Average query execution time for the aggregation time window.

Attribute	Description
MaxQueryExecutionDuration (ms)	Maximum query execution time for the aggregation time window.
MinQueryExecutionDuration (ms)	Minimum query execution time for the aggregation time window.
QueryType	Type of query. For instance, the query passed could be a Power BI refresh or DirectQuery. Or, it could be queries from Power Apps and Power Automate.
AverageDataProcessingDuration (ms)	Average time for data processing activities like spooling, data retrieval, compression, and data processing for the aggregation time window.
MaxDataProcessingDuration (ms)	Maximum time for data processing activities like spooling, data retrieval, compression, and data processing for the aggregation time window.
MinDataProcessingDuration (ms)	Minimum time for data processing activities like spooling, data retrieval, compression, and data processing for the aggregation time window.
Count	Number of queries.

The System Counter Aggregation Report contains system counter values aggregated to a time interval. The default value is 5 minutes, but you can adjust it. The following attributes are captured.

Attribute	Description
GatewayObjectId	Unique identifier for the gateway.
AggregationStartTimeUTC	Start of the time window for the system counters that were aggregated.
AggregationEndTimeUTC	End of the time window for the system counters that were aggregated.

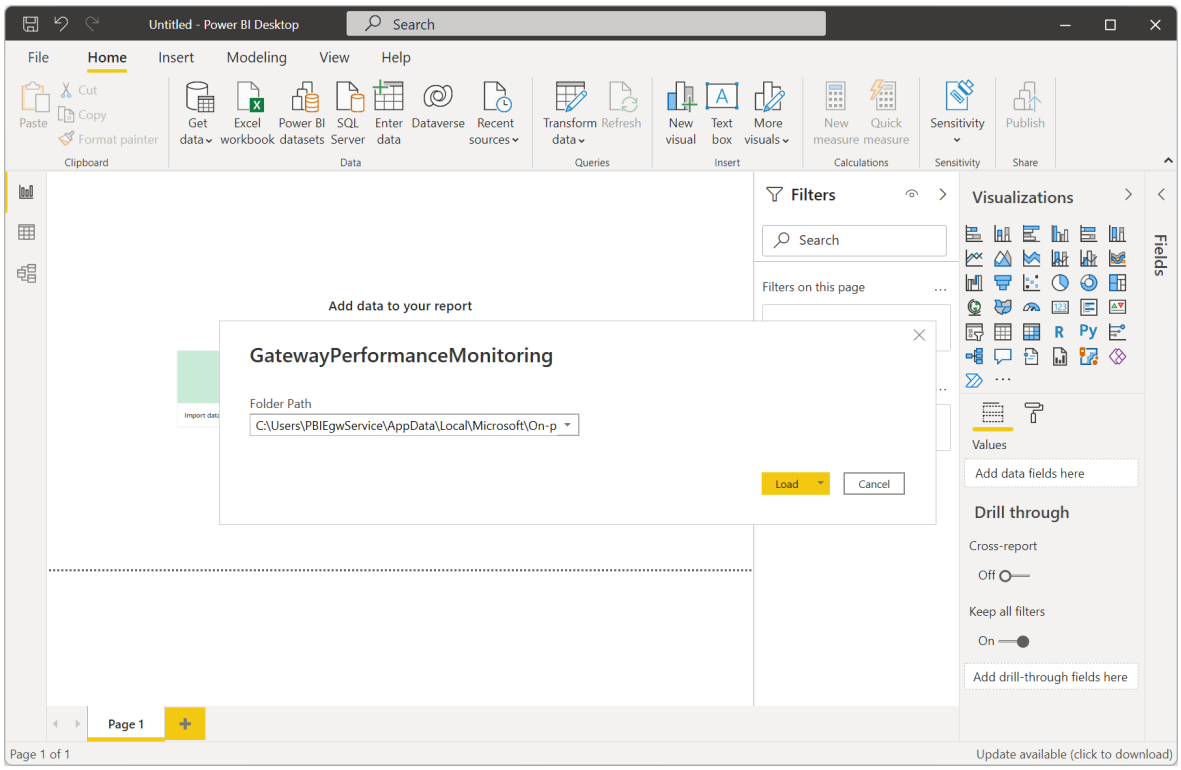
Attribute	Description
CounterName	System counters each apply to one server that is hosting a gateway node and include: • **SystemCPUPercent**: CPU used on the server as a percentage of total available CPU. • **SystemMEMUsedPercent**: Memory used on the server as a percentage of total available memory. • **GatewayCPUPercent**: The sum of the percent of CPU used by the gateway process on each core. To get the percent of the CPU used on the server, divide **GatewayCPUPercent** by the number of cores. • **GatewayMEMKb**: Sum of the total memory in kilobytes used by the gateway process.
Max	Maximum value for the system counter for the aggregation time window.
Min	Minimum value for the system counter for the aggregation time window.
Average	Average value for the system counter for the aggregation time window.

Visualize gateway performance

Now, you can visualize the data that's in the log files.

1. Download the Gateway Performance PBI template, and open it by using Power BI Desktop.

2. In the dialog box that opens, check that the folder path matches the value in **ReportFilePath**.



3. Select **Load**, and the template file starts loading the data from your log files. All visuals are populated by using the data in the reports.

4. Optionally, save this file as a PBIX, and publish it to your service for automatic refreshes. To learn more, go to Publish datasets and reports from Power BI Desktop.

You also can customize this template file to suit your needs. For more information on Power BI templates, go to this Microsoft Power BI blog post.

Monitoring spool storage

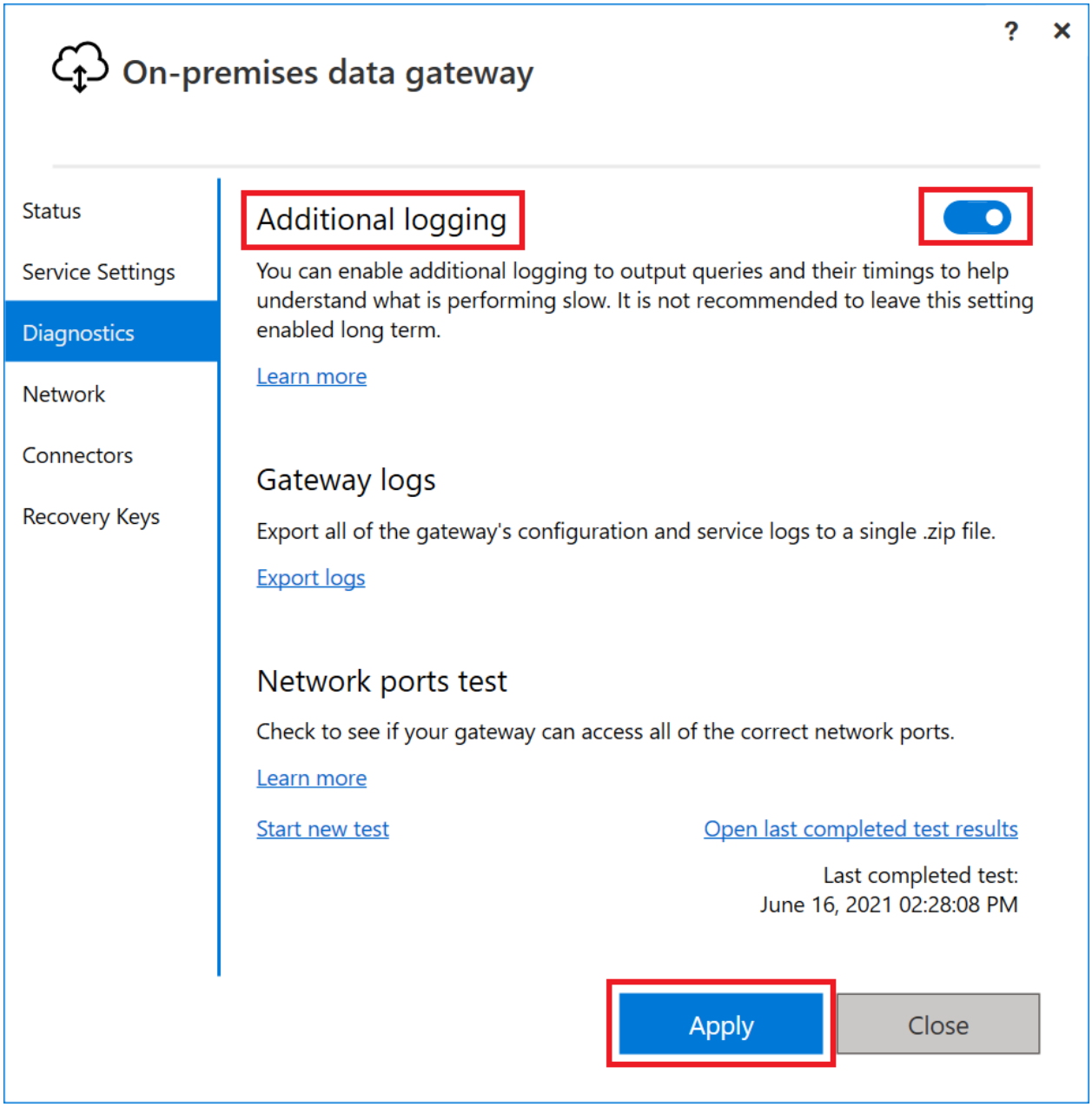
By default, spool storage for the gateway is located at C:\Users\PBIEgwService\AppData\Local\Microsoft\On-premises data gateway\Spooler. Be sure to monitor this location to ensure there is adequate free disk space. More information: Gateway spooling data

Slow-performing queries

Long-running queries might require additional modification on your data source or further optimization of the query itself. This could be either for Power BI refreshes or for direct database queries, like Power BI DirectQuery, Power Apps, or Azure Logic Apps.

By default, the gateway performs basic logging. If you're investigating slow-performing queries, in addition to using the performance monitoring feature, you can temporarily

enable **Additional logging** to gather additional log information. To do this, in the on-premises data gateway app select **Diagnostics** > **Additional logging**.



Enabling this setting likely will increase the log size significantly, based on gateway usage. We recommend that after you finish reviewing the logs that you disable additional logging. We don't recommend leaving this setting enabled during normal gateway usage.

When you turn on this setting, additional information (application context in the following sample) is included in the gateway logs that indicates which dataset or report this query belongs to. Not all services are able to send this information at this time and we are working on known gaps.

```
QueryAdditionalInformation is: {
  "Application": "Dataset-Premium",
```

```
  "ObjectId": "6de5b524-8a04-4578-961d-e65b2bf3dcd4",
  "ApplicationContext": "{\"DatasetId\":\"6de5b524-8a04-4578-961d-
ej67gdf3dcd4\",\"Sources\":[{\"ReportId\":\"e0cec7bc-f53d-4174-b551-
678656fba\"}]}"
}.
```

Optimize performance by streaming data

By default, the on-premises data gateway spools data before returning it to the dataset, potentially causing slower performance during data load and refresh operations. The default behavior can be overridden.

1. In the C:\Program Files\On-Premises data gateway\Microsoft.PowerBI.DataMovement.Pipeline.GatewayCore.dll.config file, set the **StreamBeforeRequestCompletes** setting to **True**, and then save.

   JSON

   ```
   <setting name="StreamBeforeRequestCompletes" serializeAs="String">
      <value>True</value>
   </setting>
   ```

2. In **On-premises data gateway** > **Service Settings**, restart the gateway.

Optimize performance by excluding specific folders from antivirus scanning

In order to avoid potential performance impacts, certain folders can be excluded from antivirus scanning when you use a file-level antivirus software in the server where an on-premises data gateway is installed. If these folders aren't excluded, you might observe performance impacts and potentially other unexpected behaviors since these folders receive a large amount of write operations and are, at the core, data pipelines of the on-premises data gateway.

Folders that might have to be excluded from antivirus scanning in the on-premises data gateway server

> ⓘ **Note**
>
> The following place holder Drive represents the letter of the drive on which the on-premises data gateway is installed. Typically, the driver letter is C. The following

place holder ServiceAccount represents the service account that's running the on-premises data gateway. The default account is PBIEgwService.

- Logging directory: **Drive**:\Windows\ServiceProfiles\ **ServiceAccount** \AppData\Local\Microsoft\On-premises data gateway
- Spool storage directory: **Drive**:\Windows\ServiceProfiles\ **ServiceAccount** \AppData\Local\Microsoft\On-premises data gateway\Spooler

Next steps

- Troubleshooting tools

PowerShell support for on-premises data gateway clusters

Article • 12/02/2022

PowerShell scripts are available in the PowerShell gallery. The scripts described in this article are for PowerShell version 5. When you use PowerShell version 7, refer to PowerShell Cmdlets for on-premises data gateway management. You can use the PowerShell scripts to perform the following operations:

- Retrieve the list of gateway clusters available for a user.
- Retrieve the list of gateway instances registered in a cluster and their online or offline status.
- Modify the enable or disable status for a gateway instance within a cluster and other gateway properties.
- Delete a gateway.

Run the PowerShell commands

To install these cmdlets, run the following command in an elevated PowerShell session:

```PowerShell
Install-Module -Name OnPremisesDataGatewayHAMgmt
```

The entire list of cmdlets can be found using the following command:

```PowerShell
Get-Command -Module OnPremisesDataGateway*
```

Examples and descriptions are included in the cmdlets and you can access them using the following command:

```PowerShell
get-help <cmdlet-name>
```

Now you can use the commands in the following table to manage your gateway clusters.

Command	Description	Parameters
Login-OnPremisesDataGateway	Use this command to sign in to manage your on-premises data gateway clusters. You must run this command and sign in *before* other high-availability commands can work properly. Note: The Azure Active Directory auth token acquired as part of a `login` call is valid for only 1 hour, after which it expires. You can rerun the `login` command to acquire a new token.	Azure Active Directory username and password (provided as part of the command execution, not initial invocation).
Get-OnPremisesDataGatewayClusters	Retrieves the list of gateway clusters for the signed-in user.	Optionally, you can pass formatting parameters to this command for better readability, such as *Format-Table -AutoSize -Wrap*.
Get-OnPremisesDataClusterGateways	Retrieves the list of gateways within the specified cluster and additional information for each gateway like online or offline status and machine name.	*-ClusterObjectID xyz* (where *xyz* is replaced with an actual cluster object ID value, which can be retrieved by using the *Get-OnPremisesDataGatewayClusters* command).
Set-OnPremisesDataGateway	Use this command to set property values for a given gateway within a cluster, which includes the ability to enable or disable a specific gateway instance.	*-ClusterObjectID xyz* (where *xyz* is replaced with an actual cluster object ID value, which can be retrieved by using the *Get-OnPremisesDataGatewayClusters* command). *-GatewayObjectID abc* (where *abc* is replaced with an actual gateway object ID value, which can be retrieved by using the *Get-OnPremisesDataClusterGateways* command, given a cluster object ID).

Command	Description	Parameters
Get-OnPremisesDataGatewayStatus	Use this command to retrieve the status for a given gateway instance within a cluster.	*-ClusterObjectID xyz* (where *xyz* is replaced with an actual cluster object ID value, which can be retrieved by using the *Get-OnPremisesDataGatewayClusters* command). *-GatewayObjectID abc* (where *abc* is replaced with an actual gateway object ID value, which can be retrieved by using the *Get-OnPremisesDataClusterGateways* command, given a cluster object ID).
Remove-OnPremisesDataGateway	Use this command to remove a gateway instance from a cluster. Note: The primary gateway in the cluster can't be removed until all other gateways in the cluster are removed.	*-ClusterObjectID xyz* (where *xyz* is replaced with an actual cluster object ID value, which can be retrieved by using the *Get-OnPremisesDataGatewayClusters* command). *-GatewayObjectID abc* (where *abc* is replaced with an actual gateway object ID value, which can be retrieved by using the *Get-OnPremisesDataClusterGateways* command, given a cluster object ID).

Next steps

- On-premises data gateway app
- Manage high-availability clusters and load balancing
- Remove or delete an on-premises data gateway

Previous monthly updates to the on-premises data gateways

Article • 05/26/2023

This article describes the last six updates for the on-premises data gateways and provides links for downloading any of these versions.

May 2023 update (3000.174.10)

For the most current release of the gateways, check out our recent blog post or download the latest versions:

- Download the latest on-premises data gateway
- Download the latest on-premises data gateway (personal mode)

April 2023 update (3000.170.10)

- List of features released
- Download the April 2023 version of on-premises data gateway
- Download the April 2023 version of on-premises data gateway (personal mode)

March 2023 update (3000.166.9)

- List of features released
- Download the March 2023 version of on-premises data gateway
- Download the March 2023 version of on-premises data gateway (personal mode)

February 2023 update (3000.162.10)

- List of features released
- Download the February 2023 version of on-premises data gateway
- Download the February 2023 version of on-premises data gateway (personal mode)

December 2022 update (3000.154.3)

- List of features released
- Download the December 2022 version of on-premises data gateway
- Download the December 2022 version of on-premises data gateway (personal mode)

November 2022 update (3000.150.11)

- List of features released
- Download the November 2022 version of on-premises data gateway
- Download the November 2022 version of on-premises data gateway (personal mode)

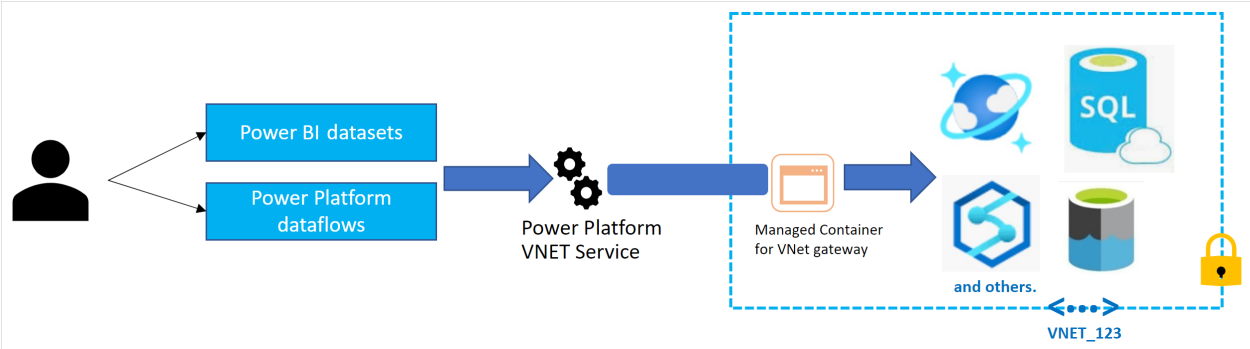
Next steps

Install an on-premises data gateway

What is a virtual network (VNet) data gateway (Preview)?

Article • 03/08/2023

The virtual network (VNet) data gateway helps you to connect from Microsoft Cloud services to your Azure data services within a VNet without the need of an on-premises data gateway. The VNet data gateway securely communicates with the data source, executes queries, and transmits results back to the service.



Limitations

- Currently, this feature is available only for Power BI datasets, Power Platform dataflows, and Power BI paginated reports. Power BI dataflows and datamarts are not supported.
- This feature is currently not supported in sovereign clouds.
- Due to an Azure AD limitation you might encounter failures when the following settings are enabled together:
  - Service endpoint for Azure AD is enabled on the delegated VNet.
  - Conditional access policies are enabled for the tenant.

  To overcome this Azure AD limitation, you can try the following workaround:
  - If you have VNet traffic blocked by a conditional access policy, check your Azure AD sign-in log. Once you've identified the traffic, you can get the IPv6 address being used and exclude it from your policy. More information: Location condition in Azure Active Directory conditional access
- You can't change the region, subscription, or resource group for the VNet on which the VNet data gateway was created. This scenario isn't currently supported.
- Power BI datasets:

    - A list of supported data services for Power BI datasets is available in Supported Azure data services.

- Power Platform dataflows:
    - For Power Platform dataflows, this feature currently doesn't support the ability to write to a privatized data lake or Dataverse.
    - A list of supported data sources for Power Platform dataflows is available in Supported data sources.
    - The physical VNet data gateway is injected into your virtual network and subnet, so it operates in the same region as the virtual network.
    - The VNet data gateway can be accessed through the application only from the home region of your tenant. There's currently no option to change the VNet data gateway region.
    - VNet data gateways currently support only admin roles and not "Can Use and Can Use+Share" for Power Platform dataflows.

- Power BI paginated reports:
    - VNet gateways support paginated reports.
    - A list of supported data sources for Power BI paginated reports is available in Supported data sources for Power BI paginated reports.

What is a virtual network (VNet)?

Article • 01/19/2023

Azure virtual network (VNet) enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. This VNet offers direct connectivity to Azure resources over an optimized route over the Azure backbone network. Azure resources can either be deployed within a VNet or they can be associated to the VNet using service or private endpoints.

Virtual networks, Private Links, and Power BI

Your communication with Power BI with respect to Azure VNets can be categorized as follows:

- Secure Inbound connections to Power BI from your network using Private links.
- Secure Outbound connectivity from Power BI to data sources within a VNet.

The scope of this document is restricted to only *Secure Outbound connectivity from Power BI to data sources within a VNet*. For the *Secure Inbound connections to Power BI from your network using Private links*, go to the Power BI Private Links documentation.

The Azure resources associated with a VNet could include Azure data services like Azure SQL, Synapse Analytics, Azure Data Explorer, and others. A list of supported data services is available at Supported Azure data services.

Before the advent of the VNet gateway, to be able to connect from Power BI to Azure data services within your VNet, you had to install the on-premises data gateway on a virtual machine inside the VNet. This is still an option. The on-premises data gateway enables secure connectivity to these data sources associated with the VNet and manages query execution from one or more of such data sources.

However, an on-premises data gateway brings its own overhead, like monthly updates and monitoring. The VNet gateway will eliminate this overhead and enable secure connectivity to data sources associated with your VNet.

Virtual network data gateway architecture

Article • 02/23/2023

The virtual network (VNet) data gateway facilitates secure connectivity to data sources associated with your VNet.

Users in your organization can access data secured by a VNet to which they already have access. But before these users can connect to these data sources from Microsoft Cloud services, a VNet gateway needs to be registered and configured.

Let's first look at what happens when you interact with a Power BI report that's connected to a data source within a VNet.

1. Power BI cloud service (or one of the other supported cloud services) kicks off a query and sends the query, data source details, and credentials to the Microsoft Power Platform VNet service.

2. The Microsoft Power Platform VNet then securely injects a container running the VNet data gateway into the subnet. This VNet data gateway can now connect to data services accessible from within this subnet.

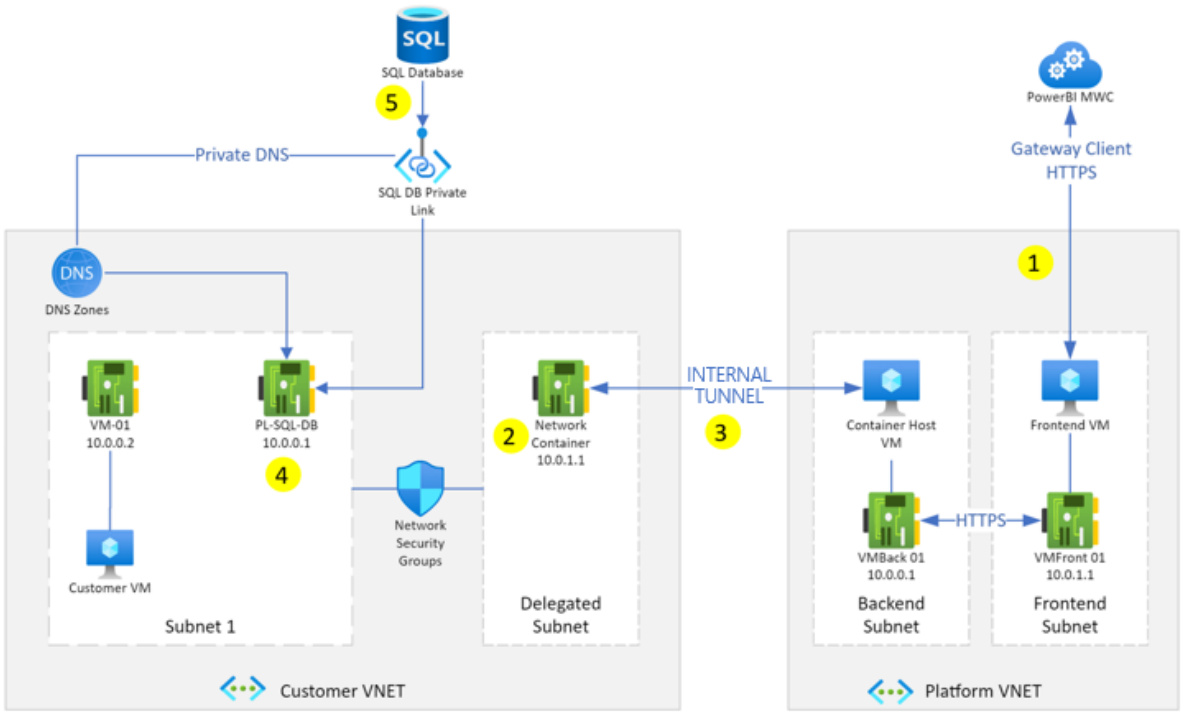
3. The Microsoft Power Platform VNet service then sends the query, data source details, and credentials to the VNet data gateway.

4. The VNet data gateway gets the query and connects to the data sources with those credentials.

5. The query is then sent to the data source for execution.

6. After execution, the results are sent to the VNet data gateway and the Microsoft Power Platform VNet service securely pushes the data from the container to the cloud service.

Here's a network diagram illustrating the data pathway between Power BI cluster and a SQL database data source:



When the workload starts up, the VNet data gateway leases an IP from the delegated subnet, which means it's obeying the network security group (NSG) and network address translation (NAT) rules on the target VNet. Traffic going through this IP address obeys all NSG rules that are applied to the subnet.

The VNet gateway doesn't require any Service Endpoint or open ports back to Power BI. Data from the VNet is returned to Power BI by an internal Microsoft tunnel that doesn't reach the pubic internet, which uses Automatic Private IP Addressing (APIPA) and exists on the infrastructure virtual machine.

> ⓘ **Note**
>
> All traffic uses the Azure backbone, including the internal Microsoft tunnel.

Hardware

Each instance of the VNet data gateway has a maximum capacity of:

- 2 cores
- 8 GB of RAM each

At this time, this is the only available hardware configuration and it can't be scaled or changed.

VNet region and data transfer

The VNet data gateway must be created in the home region of the tenant to work with Power BI. However, when creating it, you can choose an Azure VNet and subnet from any region. Your data will go to this subnet and only metadata is ever moved to the home region.

Create virtual network data gateways

Article • 04/19/2023

Details to consider when creating a VNet data gateway:

- Before creating a VNet data gateway, check that the feature is supported in your region.
- The creation of VNET data gateways across tenant boundaries isn't supported.
- The metadata (name, details, data sources, encrypted credentials, and so on) for all your VNet data gateways are stored in your Power BI home's default region. However, the VNet data gateway runs in the same region as your Azure VNet. Sometimes, there's a difference between the default environment of Power Platform and the default region of Power BI. This might impact the regions you pick.

Creating a virtual network (VNet) data gateway is a three-step process:

> Step 1: Register Microsoft.PowerPlatform as a resource provider

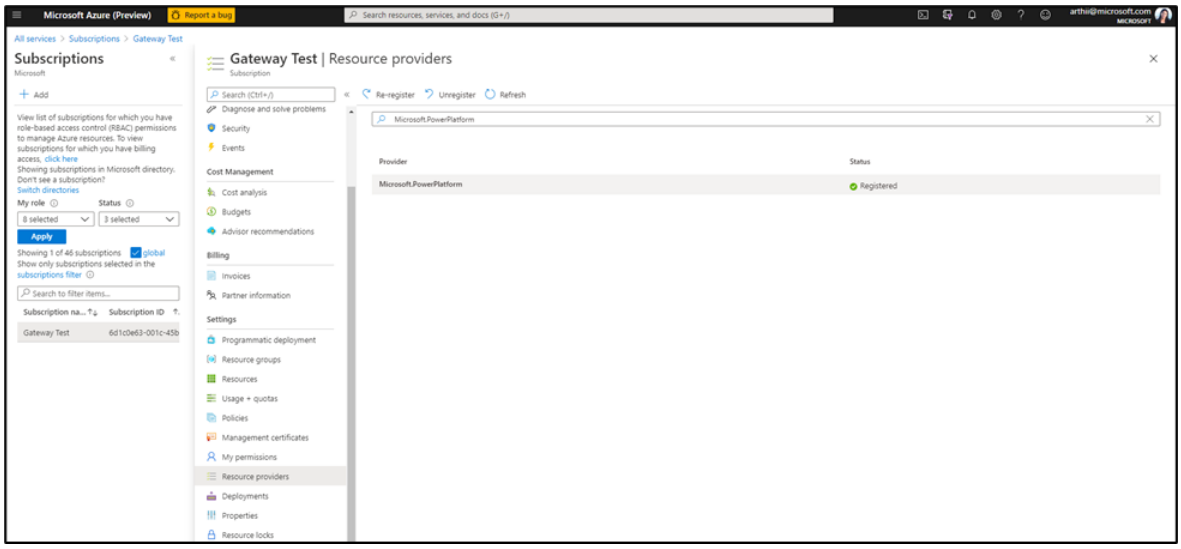
> Step 2: Associate the subnet to Microsoft Power Platform

> Step 3: Create a VNet data gateway

Step 1: Register Microsoft.PowerPlatform as a resource provider

On the Azure portal, sign in as a subscription owner and register `Microsoft.PowerPlatform` as a resource provider for the subscription that contains the VNet. This change enables your subscription to work with this resource provider.

1. Sign in to the Azure portal.
2. Navigate to the specific subscription.
3. Select **Resource providers**.
4. Search for and select **Microsoft.PowerPlatform**, and then select **Register**.



Step 2: Associate the subnet to Microsoft Power Platform

A user in a role with the Microsoft.Network/virtualNetworks/subnets/join/action permission on the VNet, like the Azure Network Contributor role, can delegate the subnet within the same VNet to Microsoft Power Platform. Subnet delegation enables you to designate a specific subnet for an Azure PaaS service of your choice that needs to be injected into your virtual network.

This subnet should have connectivity to the data service.

1. Sign in to the Azure portal.

2. Add a new subnet in the VNet. This new subnet can't be shared with other services, but will be used entirely by the Power Platform VNet service. Five IPs on this subnet will be reserved for basic functionality. In addition to those five, reserve one IP for every other gateway member you plan to create. For example, if you plan to have 2 clusters of 3 gateway members each, you would want a total of 2 x 3 + 5 or 11 IPs in the subnet CIDR range. It's a good idea to add more IPs for future gateways.

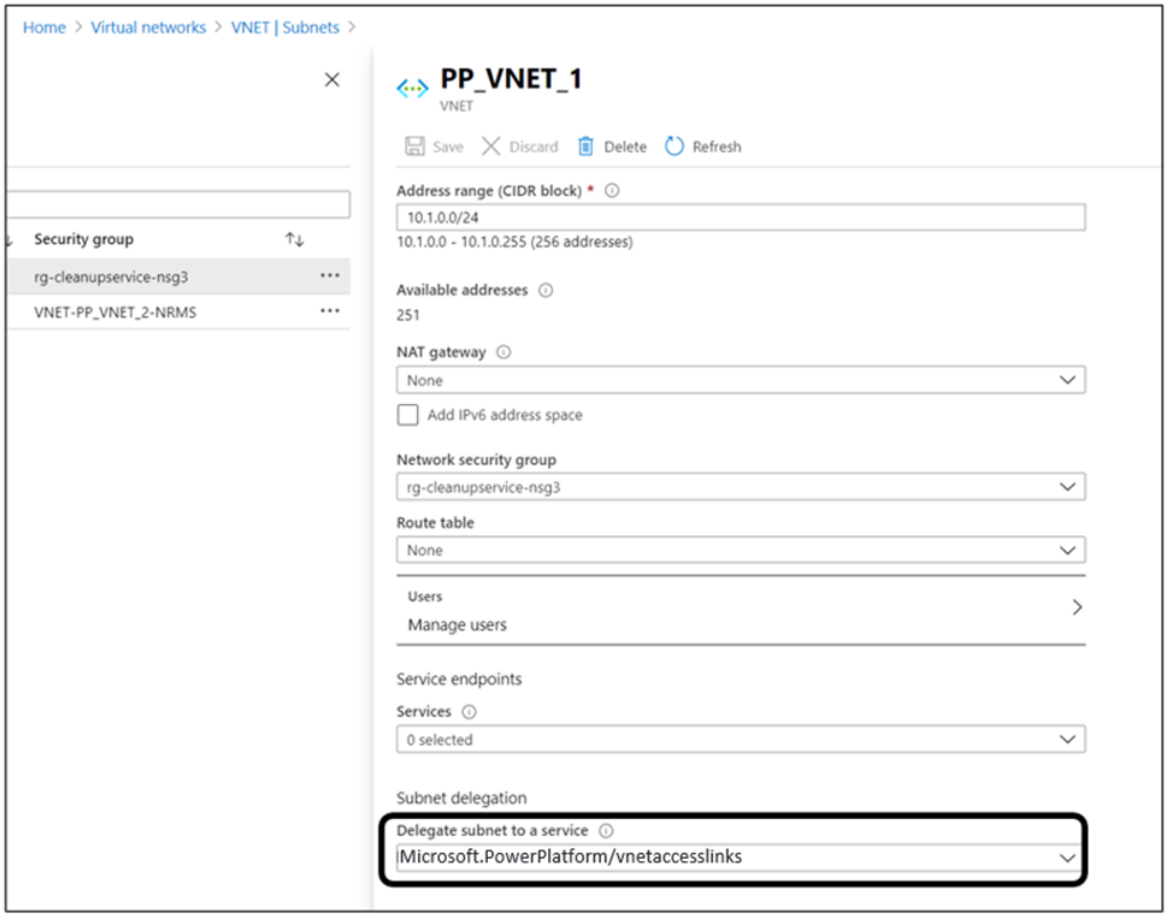
   The gateways within each cluster need to be able to communicate. For this reason, if you are restricting the allowed IPs the delegated subnet can communicate with, don't block the subnet IP range itself.

   > **Note**
   >
   > - Don't use the subnet name "gatewaysubnet" as this is a reserved word for the Azure Gateway Subnet feature. You won't be able to use it to

create a VNet data gateway in Step 3.

- Make sure this subnet doesn't have an IPV6 address space added.
- Make sure the subnet's IP range doesn't overlap with 10.0.1.x.

3. Select **Resource providers**.
4. Select **Microsoft.PowerPlatform/vnetaccesslinks** from the subnet delegation drop-down list.
5. Select **Save**.



Step 3: Create a VNet data gateway

A Microsoft Power Platform user enables the subnet for use in Microsoft Power Platform and creates a VNet data gateway. By doing this process, the user authorizes the Microsoft Power Platform VNet service to inject containers into the subnet. The user also needs to have the Azure Network Contributor role in the subscription to be able to perform this action.

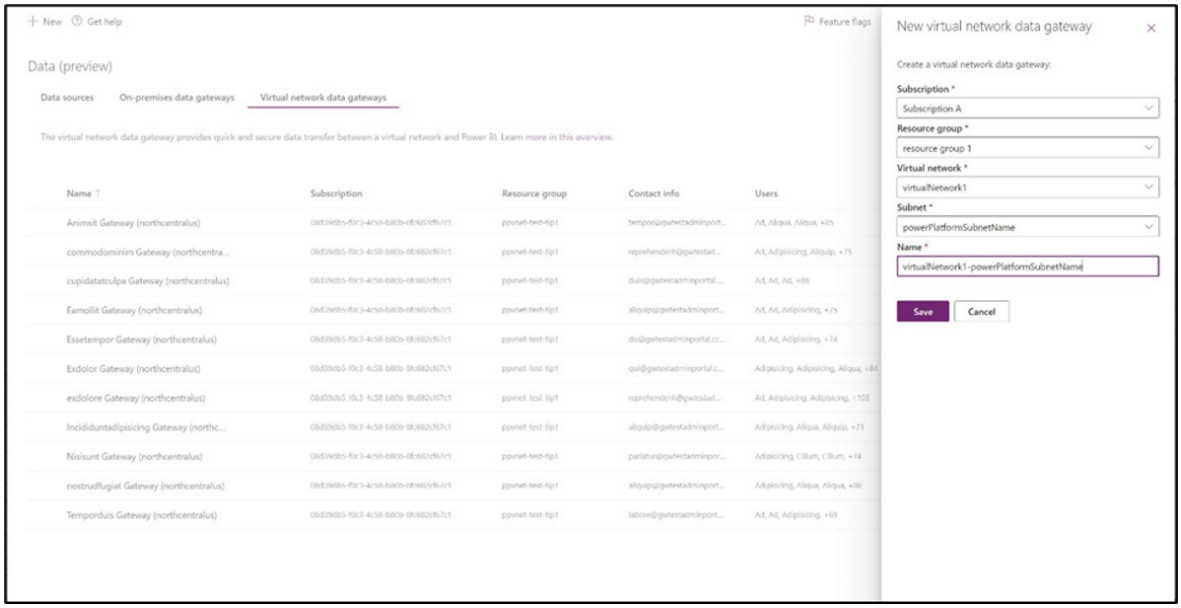
1. Sign in to the Power Platform admin center.
2. In the left navigation pane, select **Data (preview)**.

3. Select **Virtual network (VNet) data gateway** > **New**.

4. Select the subscription, resource group, VNet and the Subnet. Only subnets that are delegated to Microsoft Power Platform are displayed in the drop-down list.

5. By default, we provide a unique name for this data gateway, but you could optionally update it.

6. Select **Save**. This VNet data gateway is now displayed in your **Virtual network data gateways** tab. A VNet data gateway is a managed gateway that could be used for controlling access to this resource for Power platform users.



Regions supported for VNet data gateways

Your Azure VNet region needs to be in one of the following regions for you to be able to create a virtual network (VNet) data gateway:

- Australia East
- Australia Southeast
- Brazil South
- Canada Central
- Central India
- Central US
- East Asia
- East US
- East US 2
- France Central
- Germany West Central
- Japan East

- Korea Central
- North Central US
- North Europe
- Norway East
- South Africa North
- South Central US
- Southeast Asia
- Switzerland North
- UAE North
- UK South
- West Central US
- West Europe
- West India
- West US
- West US 2

See also

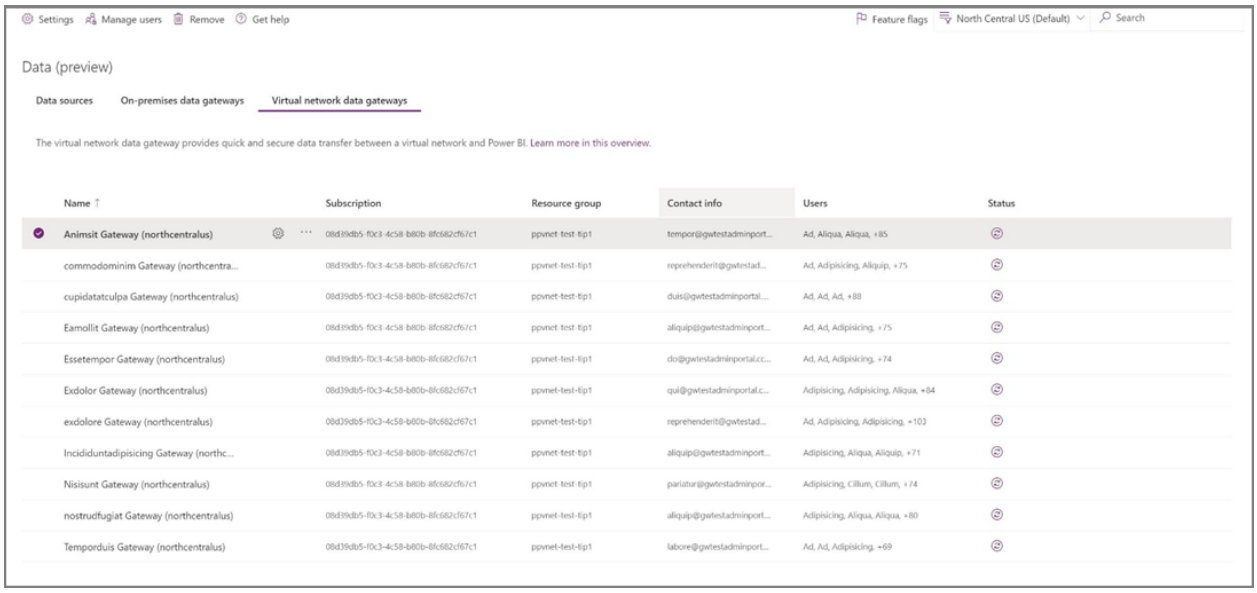
Manage virtual network data gateways

Manage virtual network data gateways

Article • 06/07/2023

After you've created a virtual network (VNet) data gateway, it will be available in the **Data (preview)** > **Virtual network data gateways** tab in the Power Platform admin center for you to manage. Also make sure you select your tenant's default home region in the region dropdown to display and manage all your VNet data gateways. You select your tenant's default region because the metadata (name, details, data sources, encrypted credentials, and so on) for all your VNet data gateways are stored in your tenant's default region.

> **Note**
>
> The **Virtual network data gateways** tab won't be visible when the **Tenant Administration** toggle is turned on.

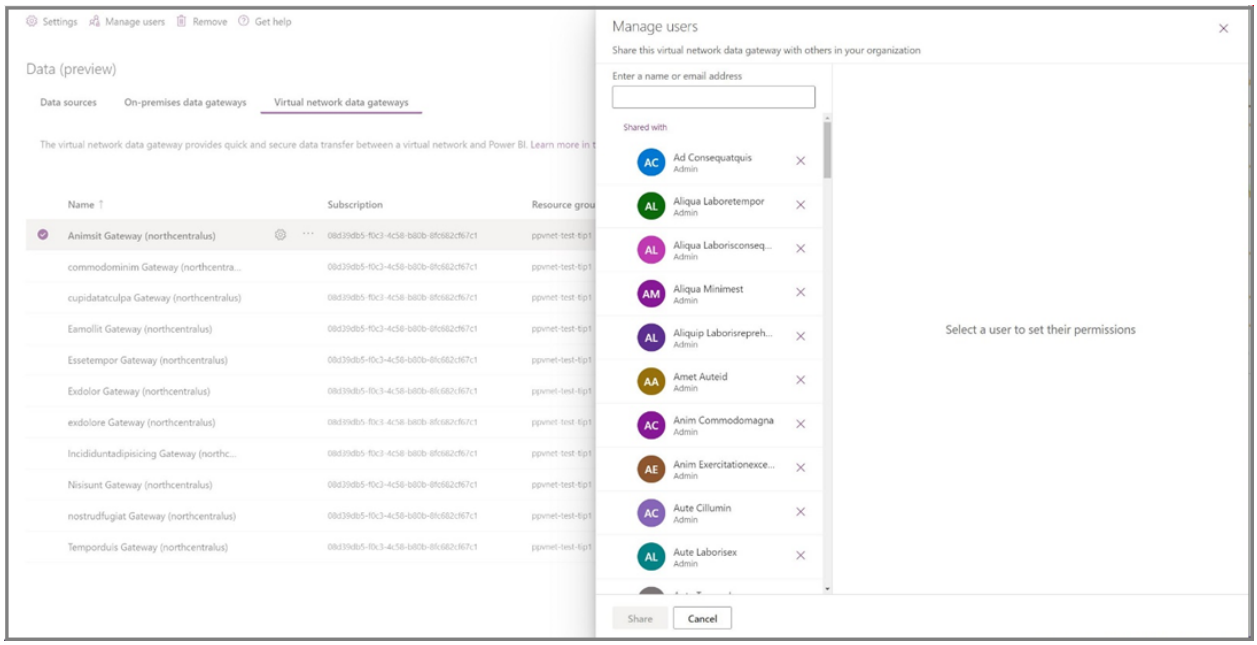


Manage access to creating VNet data gateways (gateway installer setting)

Access to creating a VNet data gateway can be limited to selected people only. To do this limitation, you must be an Azure AD Global administrator (which includes Global admins) or a Power BI service administrator. Use the **Manage gateway installers** option to manage who can create a VNet data gateway in your enterprise. This operation isn't available for gateway admins. Go to the manage gateway installers documentation to learn more.

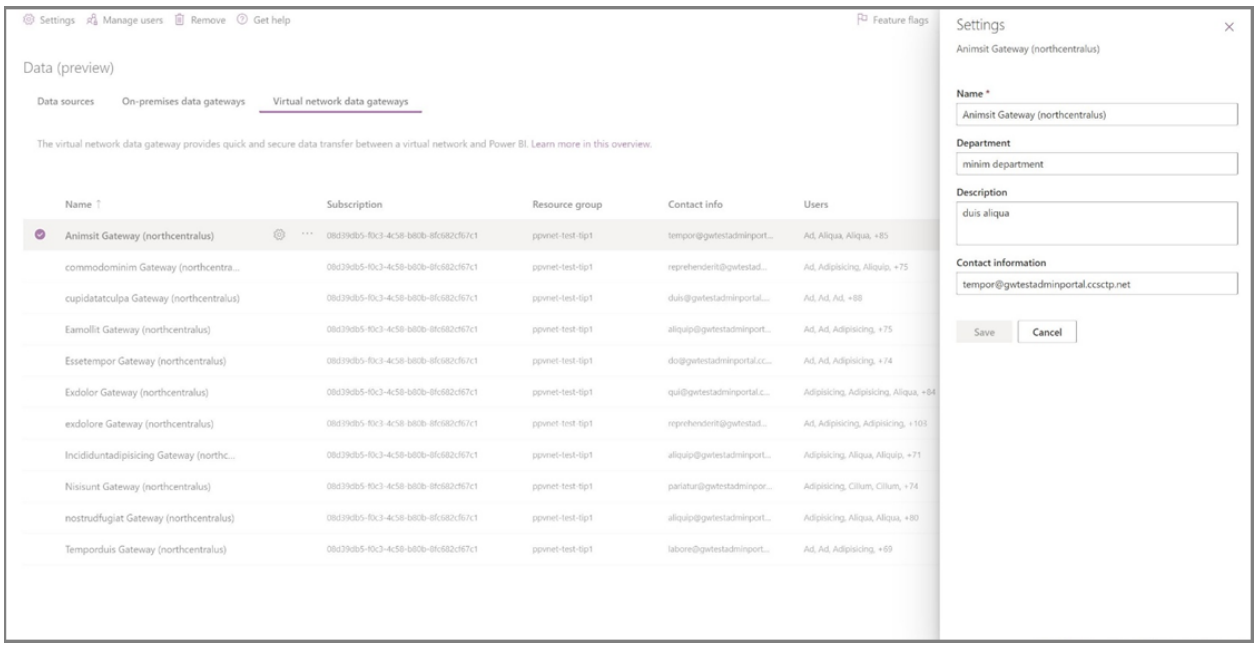
Manage admins

You can manage admins for this VNet data gateway like you do for standard data gateways in the Power Platform admin center. To add or remove admins, select a gateway, and then select **Manage Users**.



Manage settings

You can view properties for a selected VNet data gateway in the Power Platform admin center by selecting **Settings**.

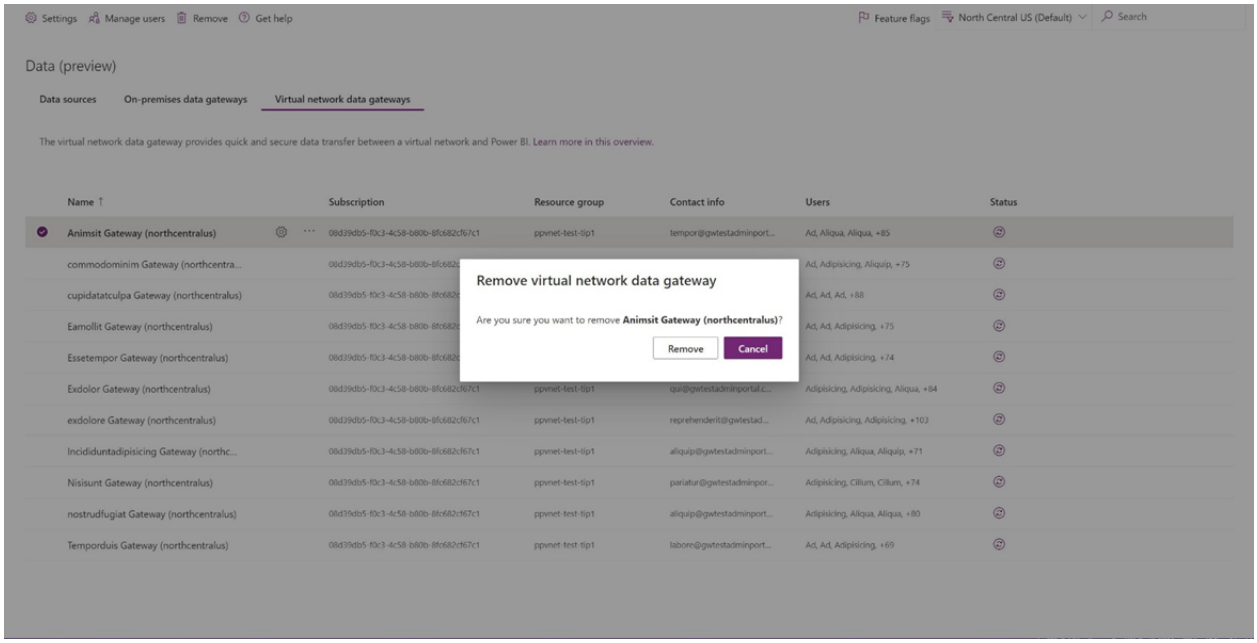


Remove VNet data gateways

You can remove or delete VNet data gateways by selecting the gateway and selecting **Remove**.

> **Note**
>
> When you remove the last gateway associated to a gateway/subnet, it might take up to 48-72 hours before you can delete the subnet or VNet.

> **Important**
>
> To be able to remove or delete a VNet data gateway, you need to:
>
> - Be a gateway admin of the VNet data gateway you want to remove
> - Have the Azure Network Contributor role in the Azure portal
> - Register the Microsoft.PowerPlatform provider as a resource provider



Use virtual network data gateway and data sources in Power BI

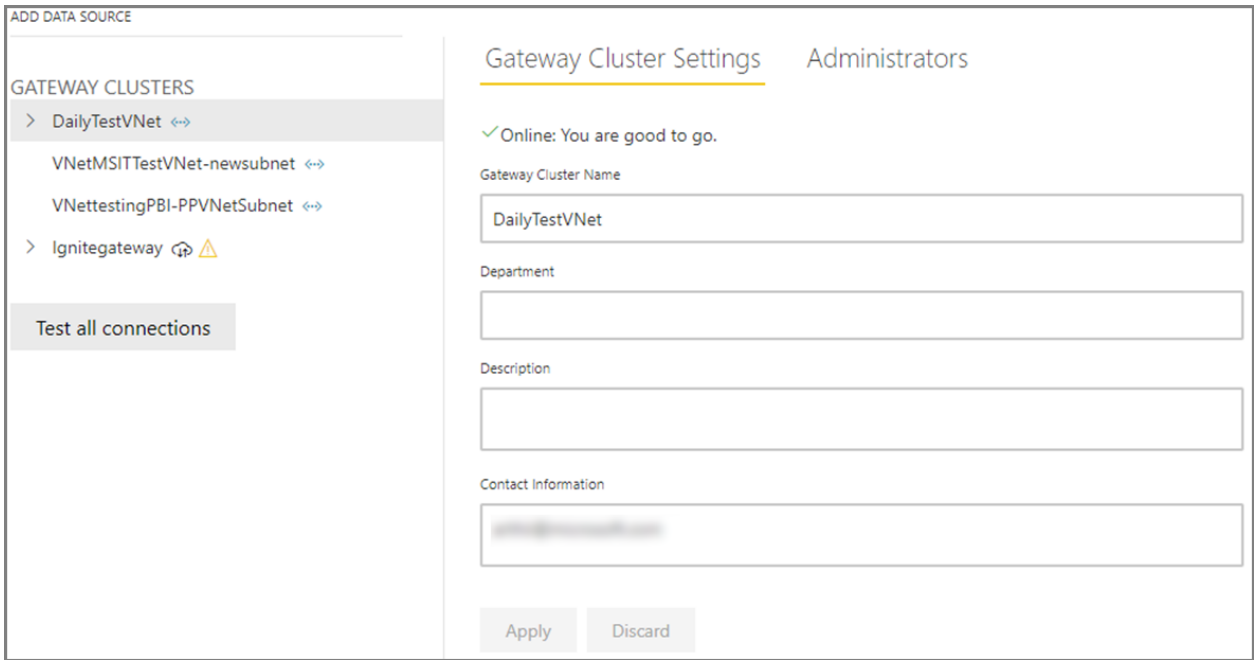
Article • 02/09/2023

Virtual network data gateways allow import or direct query datasets to connect to data services within an Azure VNet without the need of an on-premises data gateway.

> **Note**
>
> Virtual network data gateways is a Premium and Embedded feature, and will be available only in Power BI Premium workspaces, Premium Per User (PPU), and Power BI Embedded for public preview. However, licensing requirements might change when VNet data gateways become generally available.

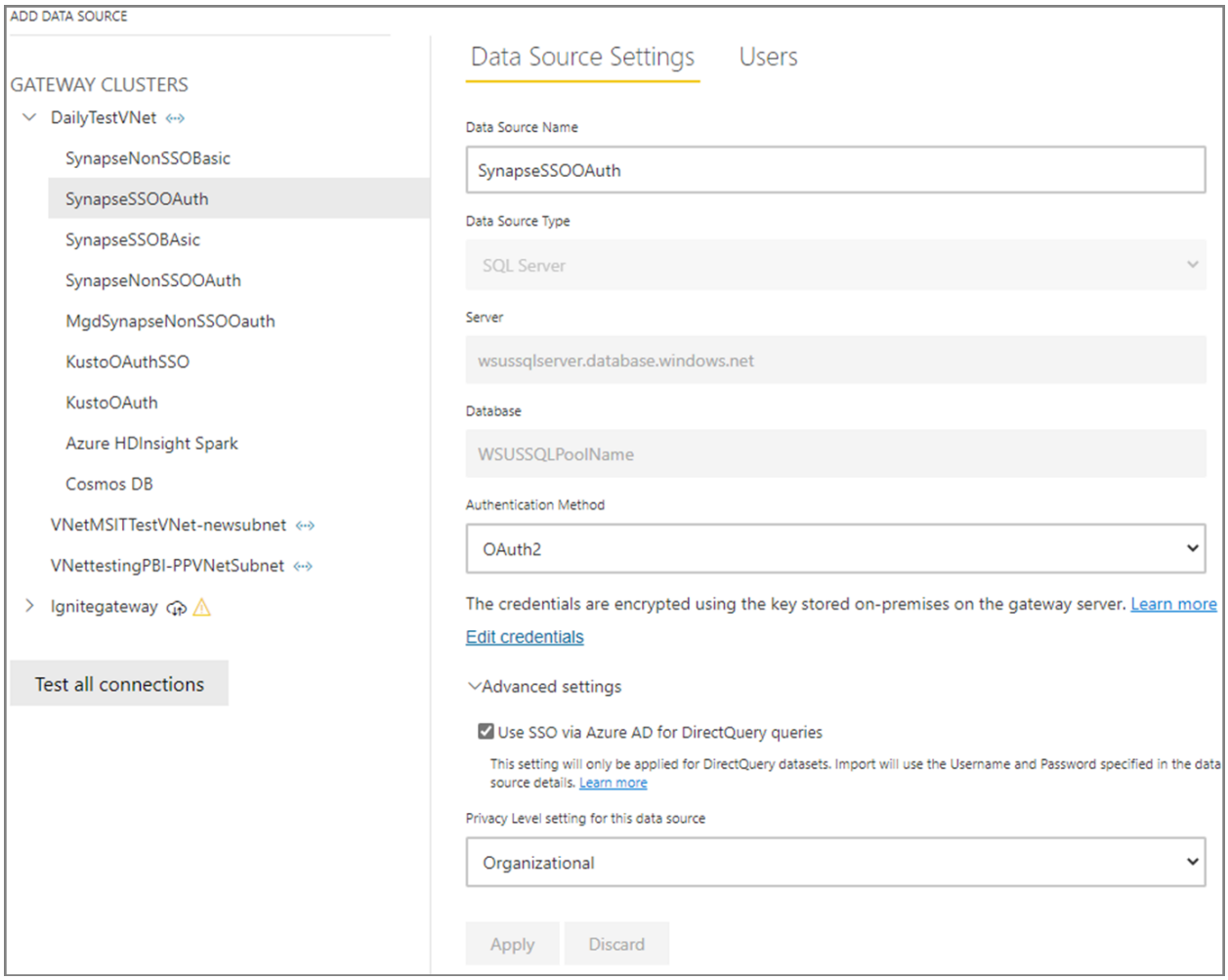
Manage Virtual network data gateways

You can manage admins for a virtual network (VNet) data gateway like you do for standard data gateways either in the Power Platform admin center or on the **Manage gateways** page in Power BI.



Manage data sources

You can also create data sources and share these data sources to users like you do today for data sources created on the standard data gateway.



Supported Azure data services

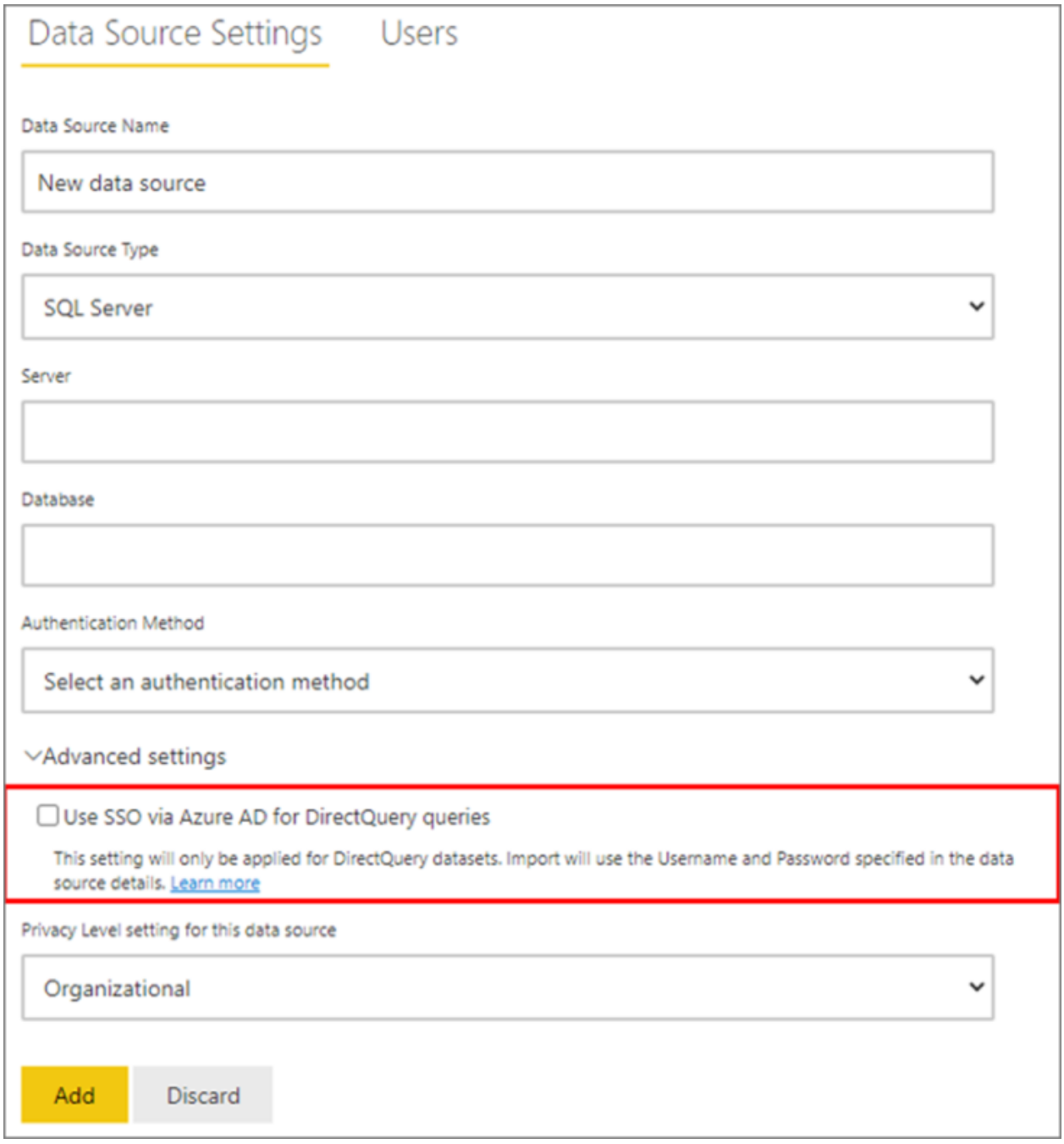
In the current release, VNet data gateways will support connectivity to the following data sources:

- Azure SQL
- Azure Synapse Analytics
- Azure Databricks
- Azure Data Explorer (Kusto)
- Azure Table Storage
- Azure Blob Storage
- Azure HDInsight (Spark)
- Azure Data Lake (Gen2)
- Cosmos DB
- Azure SQL Managed Instance (MI)
- Snowflake on Azure
- PostgreSQL

Azure Active Directory single sign-on for Direct Query

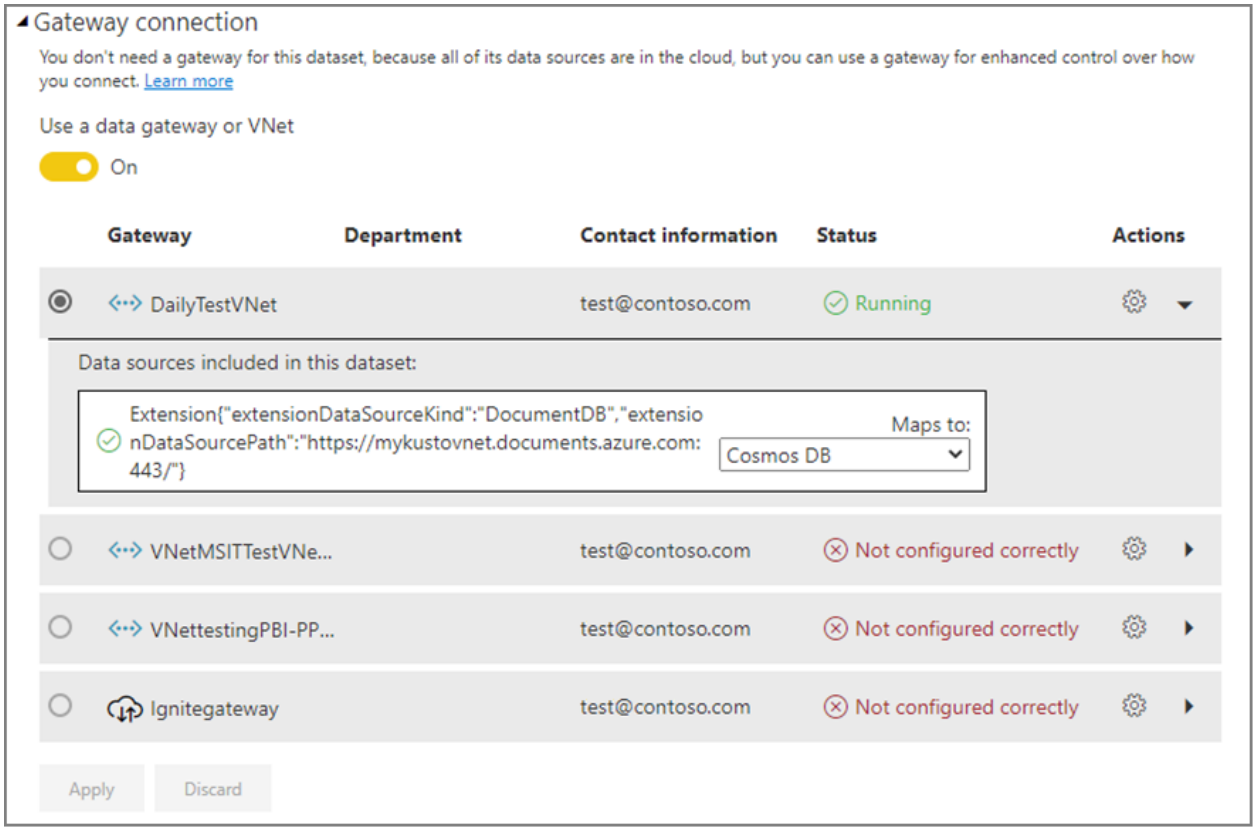
When a user interacts with a DirectQuery report in the Power BI Service, each cross-filter, slice, sort, and report editing operation can result in queries that execute live against the underlying Azure VNet data source. When you configure single sign-on (SSO) for an applicable data source, queries execute under the Azure Active Directory (Azure AD) identity of the user that interacts with Power BI.

To enable Azure AD SSO, on the **Manage Gateways** page in Power BI, go to the **Data source setting** page, and select the **Use SSO via Azure AD for Direct Queries** check box.



Use virtual network (VNet) data gateways in Power BI datasets

A Power BI report maker or creator can now publish a report and associate the dataset to the VNet data gateway data source.



Use virtual network (VNet) data gateway in Power Platform dataflows

Article • 12/02/2022

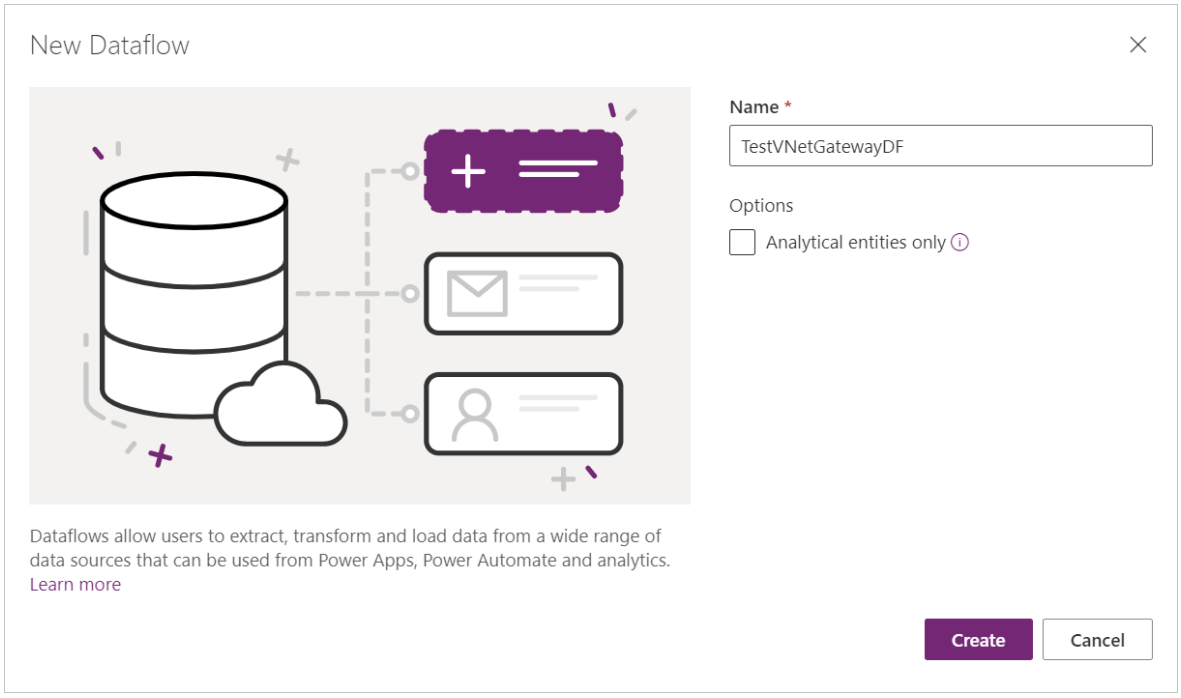
Virtual network data gateways let Power Platform dataflows connect to data services secured in an Azure VNet without the need of an on-premises data gateway. For more information about virtual network data gateways and their limitations, go to What is a virtual network (VNet) data gateway (Preview).

> **Note**
>
> - During public preview, Power platform dataflows users will have access to this feature for *free*. However, licensing requirements might change when VNet data gateways become generally available.
> - For Power Platform dataflows, this feature currently doesn't support the ability to write to a privatized data lake or Dataverse.

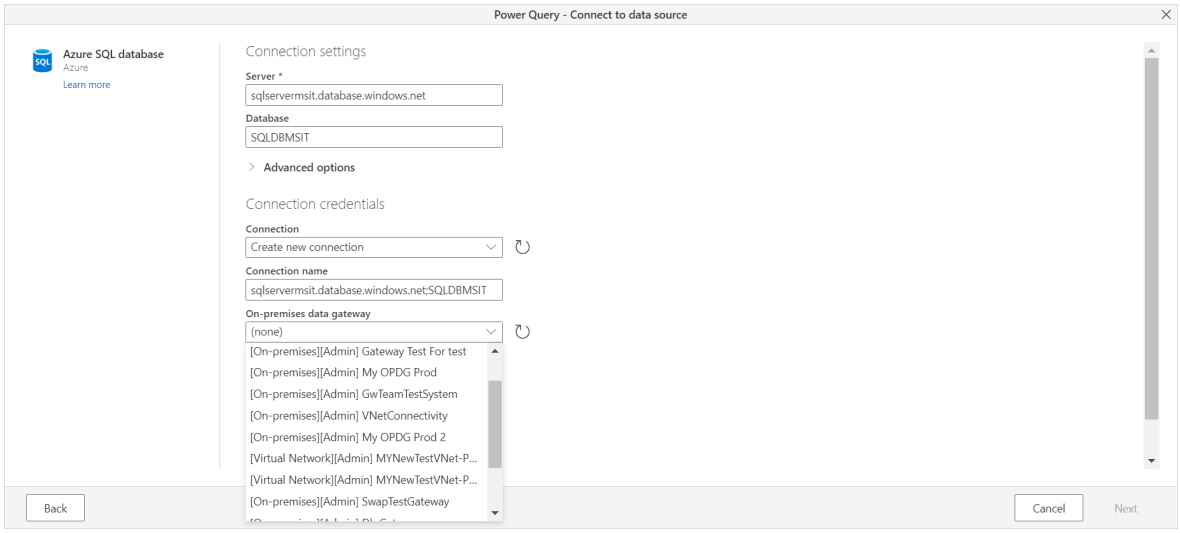
Connect to data using a VNet data gateway

To connect to data using a VNet data gateway:

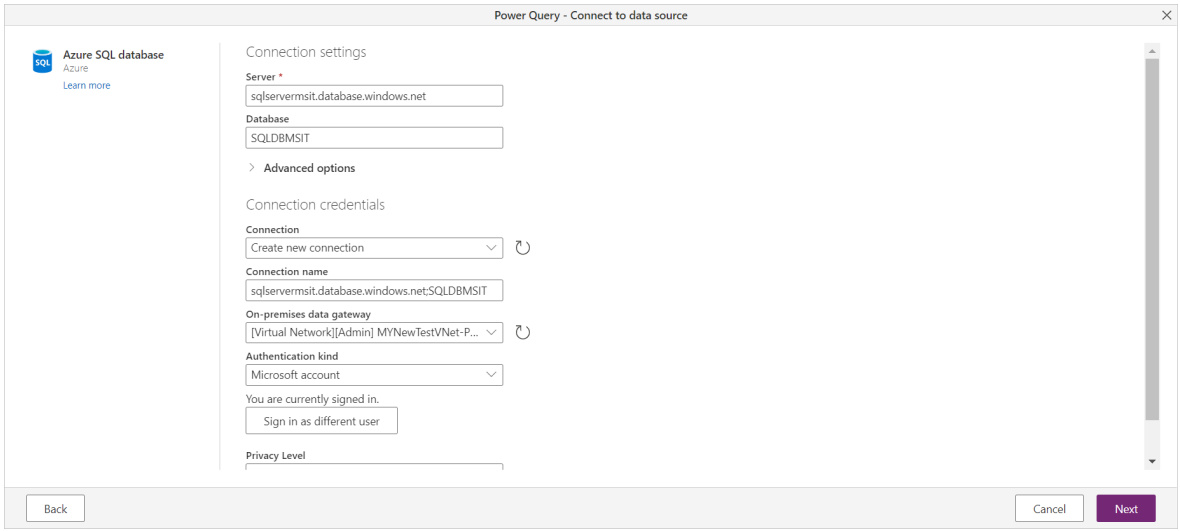
1. Create a new dataflow on the Power Apps maker portal. More information: Create and use dataflows in Power Apps - Power Apps



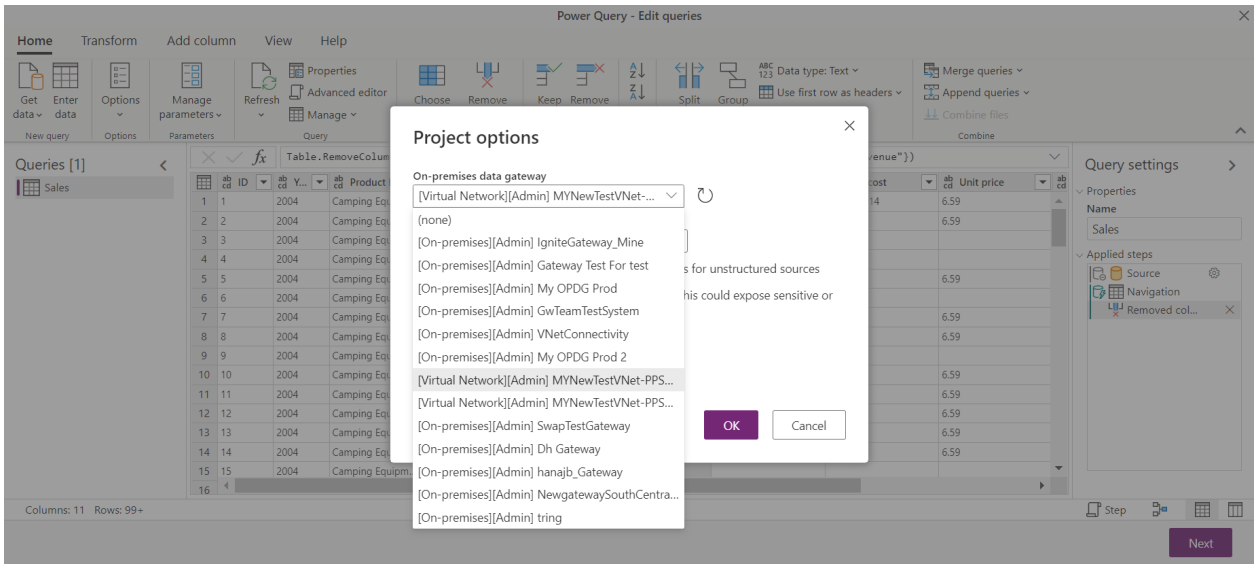
2. Once you provide the connection details and then connect to data, the VNet data gateways are now included in the **On-premises data gateway** selections.



3. Select a VNet data gateway, choose an authentication kind, and then select **Next** to connect and continue with transforming data.



You can also update VNet data gateway details just like you do for an on-premises data gateway. In the Power Query editor, select **Home** > **Options** > **Project options** while editing your dataflow.



Supported data sources

The following Azure data sources already available on Power Query Online are supported:

- Azure Blobs
- Azure Data Explorer
- Azure Data Lake Storage Gen2
- Azure SQL Database
- Azure Synapse Analytics
- Azure Tables

VNet data gateways aren't supported for:

- Data sources requiring third-party drivers like SAP, Oracle, and so on
- The Web connector
- The ODBC connector

> **Note**
>
> - On-premises data sources can be connected using ExpressRoute, but this configuration hasn't been tested and won't be supported by Microsoft during public preview.
> - Other Cloud data sources can be connected using VNet data gateways, but haven't been tested for public preview.

VNet data gateway support for Power Automate SQL Server and custom connectors (Preview)

Article • 12/02/2022

The virtual network (VNet) data gateway helps you to connect Microsoft Cloud services to your Azure data services within a VNet without the need of an on-premises data gateway. VNet data gateway is an alternative data gateway and can be used for most of the connectors that support gateway functionality today. The VNet data gateway securely communicates with the connectors and transmits results back to the service. VNet data gateways are created in your tenant's home region by default and there's currently no option to change the VNet data gateway region. Based on this limitation, VNet data gateways can only be used in Power Automate environments in the home region of your tenant.

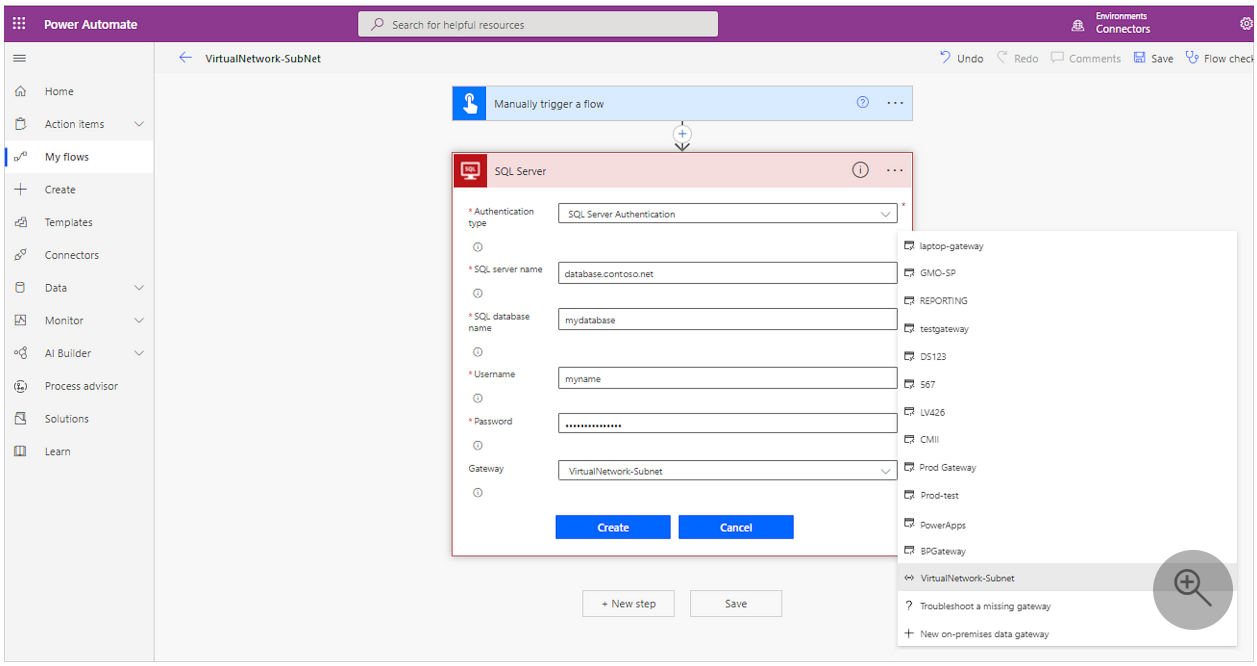
We'll be working on direct VNet functionality soon, which can be used to connect to cloud resources and will support Azure Active Directory (Azure AD) authentication.

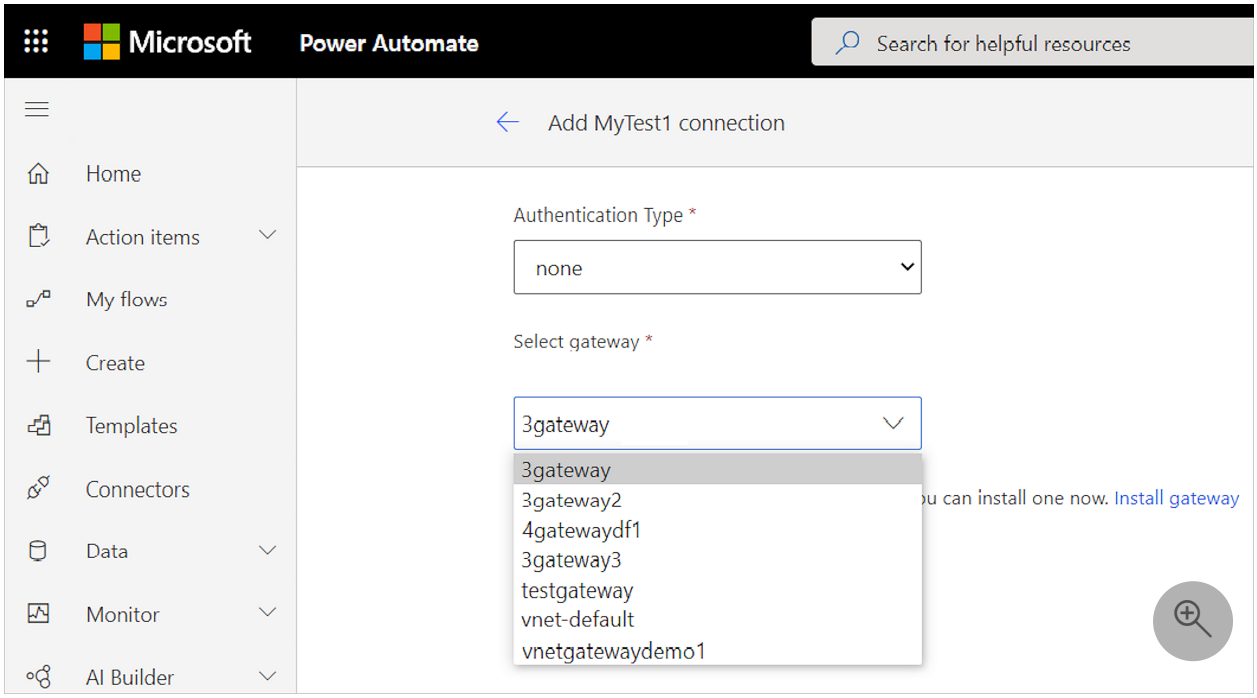
Steps to set up a virtual network data gateway are listed at Create virtual network data gateways.

Power Automate SQL Server connector

When creating the SQL Server connection, choose the VNet data gateway that you created in the Power Platform admin center in the **Gateway** drop-down box, as shown in the following image. The Azure SQL server should be in the same virtual network as the VNet data gateway.

Only SQL server authentication is supported for the SQL Server connector. Windows Authentication isn't supported because the VNet data Gateway can't impersonate the Windows user as it's not domain joined.



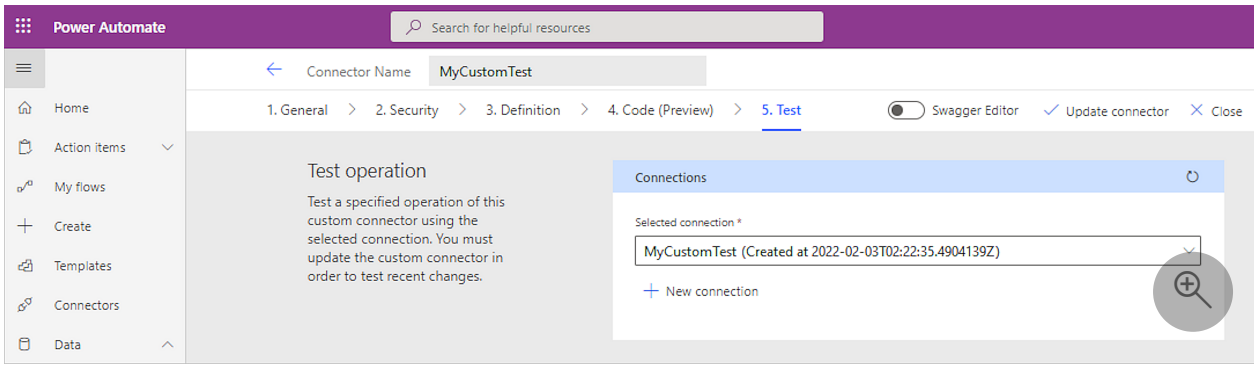


For an on-premises SQL server, the SQL server must be in the same virtual network as the VNet data gateway. If the firewall is blocked on the virtual machine that the SQL server resides on, you might have to unblock the firewall for the required ports.

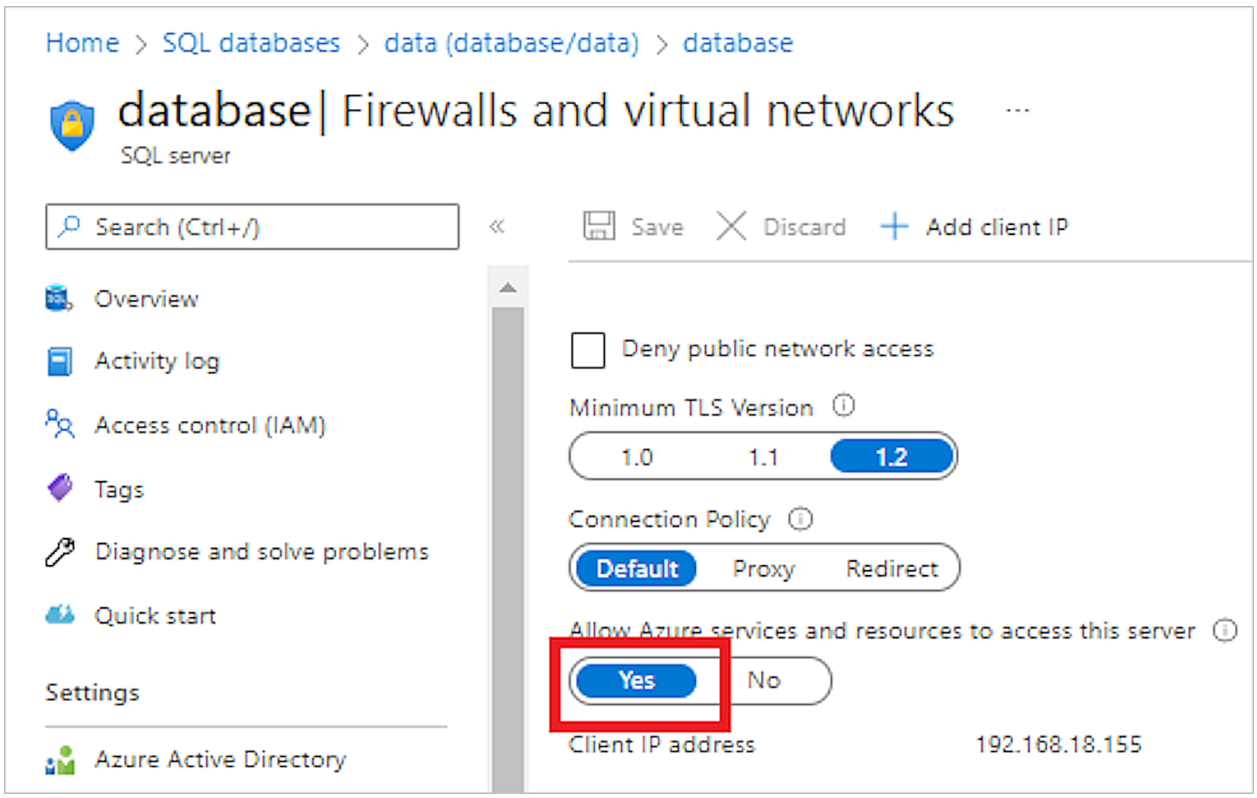
Power Automate custom connectors

When testing the custom connector, create a **New connection** from the **Test** tab by editing the custom connector. Then in the **Select gateway** drop-down box, select the VNet data gateway.

Only basic authentication, no authentication, and Windows authentication are supported through the VNet data gateway for custom connectors.



> **Note**
>
> Make sure that **Allow Azure services and resources to access this server** is set to **Yes** for your SQL Server in the **Firewalls and virtual networks** sections.



The VNet data gateway isn't yet supported in Power Apps SQL server and custom connectors.

Manage virtual network data gateway high availability and load balancing

Article • 10/18/2022

You can use a cluster of virtual network data gateways to load balance the queries executing on the cluster and to avoid a single point of failure.

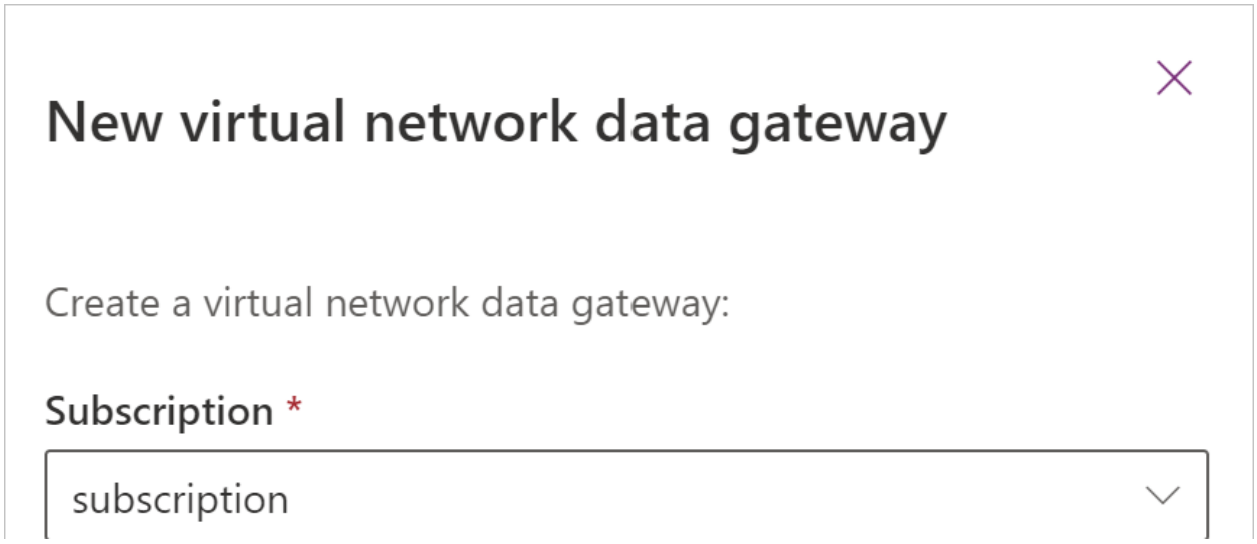
High-availability and load balancing a cluster for a virtual network data gateway

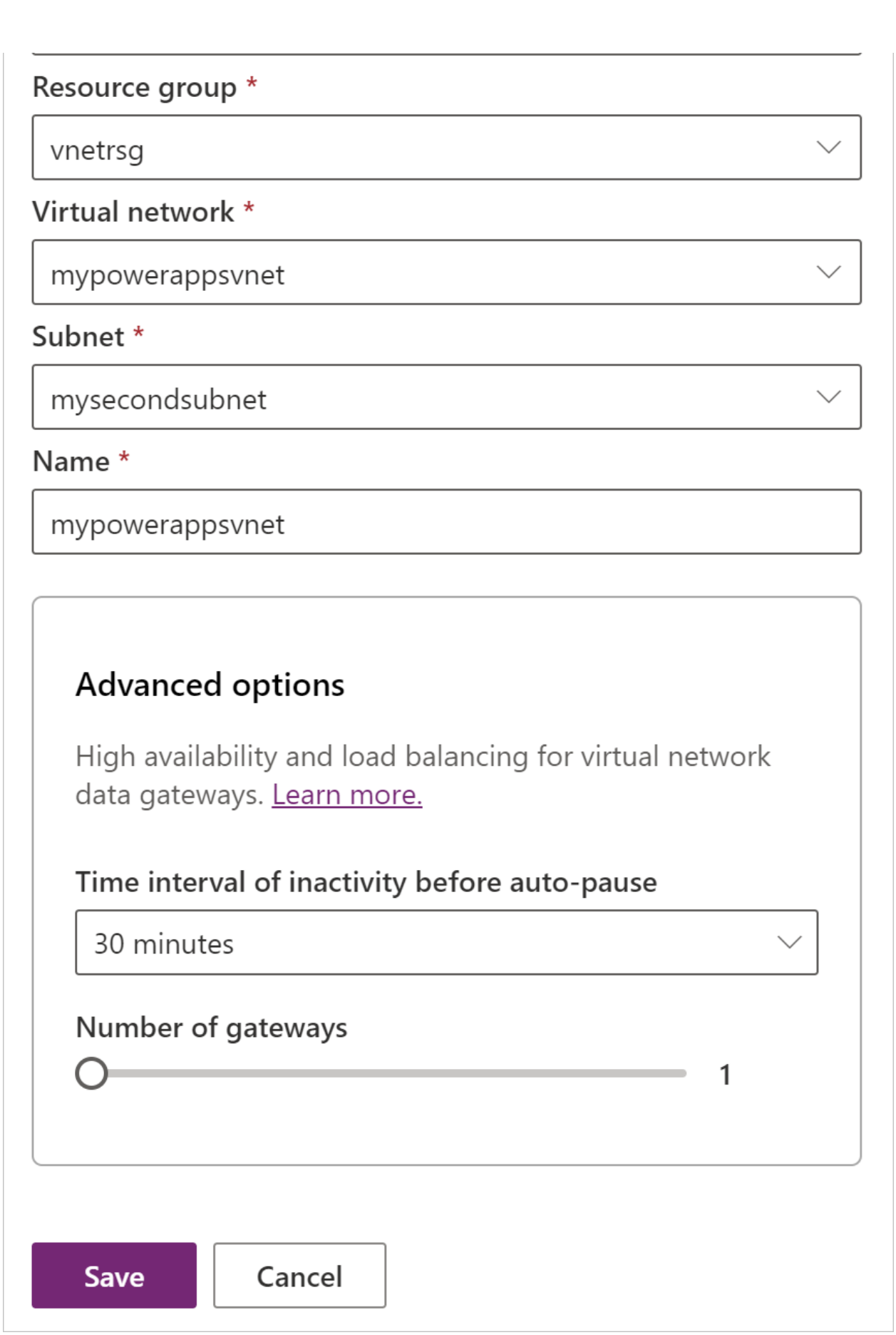
You can create high-availability clusters when creating a new virtual network data gateway. Having multiple gateways in the cluster ensures that your organization can access your data behind the virtual network and avoid a single point of failure when accessing on-premises data resources. A cluster with multiple gateways also allows for load balancing. The selection of a gateway during load balancing is random.

How to create a cluster of multiple virtual network data gateways

There are two ways to create a cluster of virtual network data gateways. The first one is to directly create a cluster with multiple gateways during the first-time creation of the data gateway. The second option is to edit the settings for existing virtual network data gateways.

If you're creating a new virtual network data gateway, you first need to fill out the required information for creating the virtual network from the Power Platform admin center. Afterwards, you're presented with an advanced options menu.

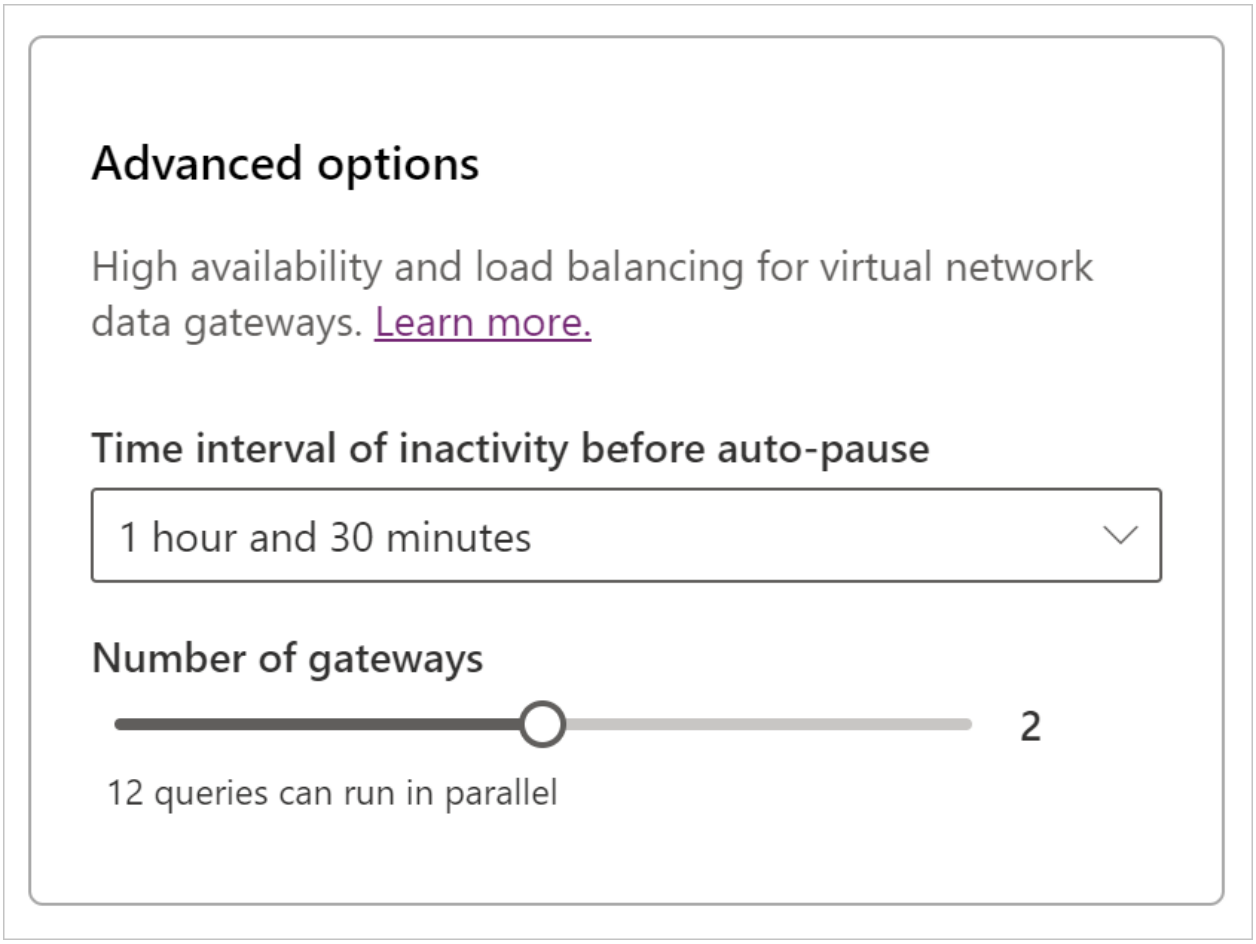




By default, the number of gateways is set to 1. This setting means that only one gateway will be created. You can increase the number of gateways by using the slider. The maximum number of gateways per cluster is 3.

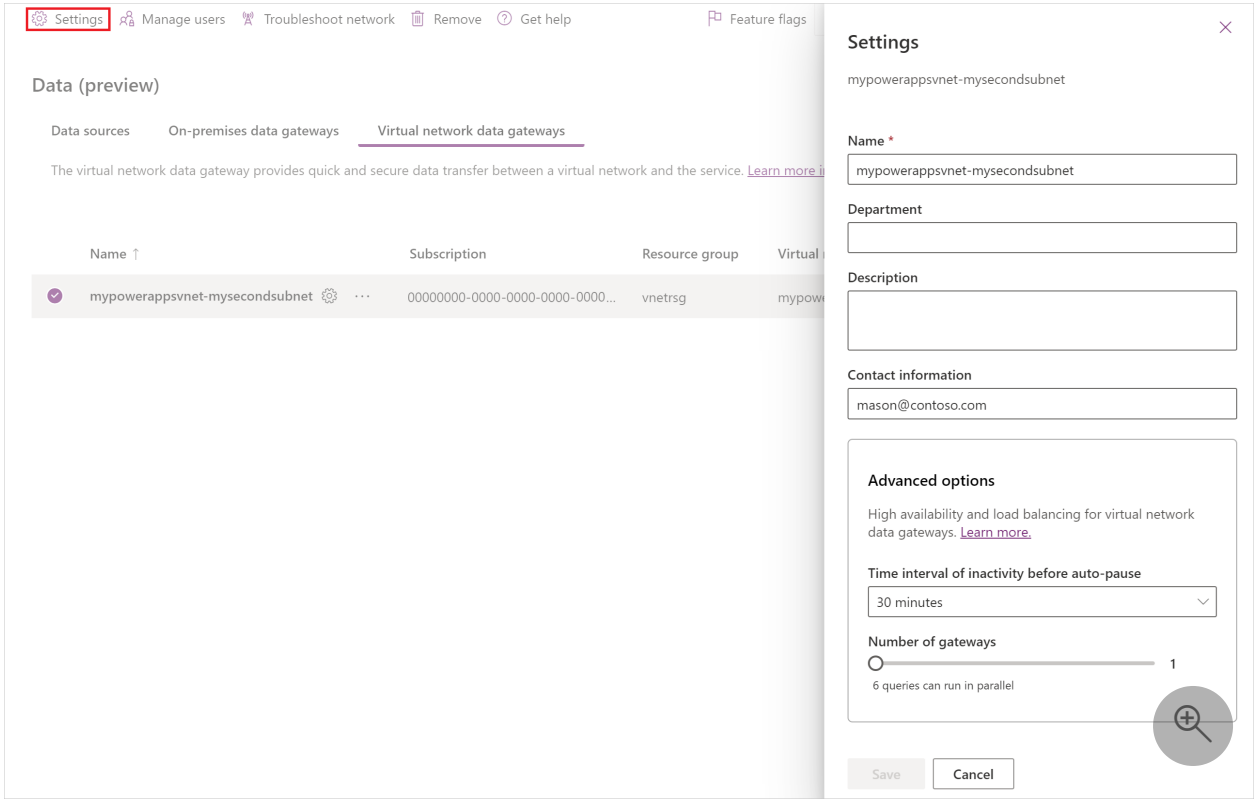
How to ensure your gateway is available for query execution

The virtual network data gateway cluster auto-pauses after a certain time of inactivity. After the gateway is auto paused, it takes about 2 to 3 minutes for the cluster to become available again. By default, the time interval of inactivity before auto-pause is set to 30 minutes. You can increase this time interval to a maximum of 24 hours. There's no support for leaving the virtual network data gateway cluster always on.



How to change the high availability options

At any point in time, you can change the number of gateways you have in the cluster. You can also change the time interval of inactivity before auto pause. To edit these settings, select a virtual network data gateway, and then select **Settings** on the top. You can now change the advanced options on the **Settings** panel.


Settings
Manage users
Troubleshoot network
Remove
Get help
Feature flags
Data (preview)
Data sources
On-premises data gateways
Virtual network data gateways
The virtual network data gateway provides quick and secure data transfer between a virtual network and the service. Learn more i
Name
Subscription
Resource group
Virtual
mypowerappsvnet-mysecondsubnet
00000000-0000-0000-0000-0000...
vnetrsg
mypow
Settings
mypowerappsvnet-mysecondsubnet
Name *
mypowerappsvnet-mysecondsubnet
Department
Description
Contact information
mason@contoso.com
Advanced options
High availability and load balancing for virtual network data gateways. Learn more.
Time interval of inactivity before auto-pause
30 minutes
Number of gateways
1
6 queries can run in parallel
Save
Cancel

Manage security roles of a VNet data gateway

Article • 03/07/2023

You can use the VNet data gateway to transfer data quickly and securely between Power BI or Power Platform and a data source, such as Azure Databricks or Snowflake. From the Power BI manage gateways page, you can also view all VNet data gateways for which you have permissions and manage data sources for those gateways.

VNet data gateways and data source permissions

User roles

There are three security user roles available for the VNet data gateway. When you create a VNet data gateway, you automatically become the admin of the gateway. There can be multiple admins on the gateway.

> ⓘ **Note**
>
> The user roles for the VNet data gateway are the same as for the on-premises data gateway.

The three security roles for the VNet data gateway are:

- **Admin**: When a user becomes an admin, they can view all the connections created on the gateway, and can manage/delete all users and connections. Admins can also use all features applicable to gateways, including checking gateway status, using the network troubleshooting pane, and changing settings.
- **Connection creator**: A connection creator is allowed to create connections/data sources on the gateway. A connection creator can also test the status of the gateway cluster and its members. A connection creator gets read-only access to gateway settings, can't add or remove others on the gateway, and can’t remove gateways.
- **Connection creator with resharing**: A connection creator with resharing is allowed to create connections/data sources on the gateway and share gateways with others. Whomever they share gateways with will have the connection creator permission. They aren't allowed to remove a user from the gateway. Connection

creators with resharing can also test the gateway status and use the network troubleshooting pane.

Connection roles

When you create a connection (data source) with the VNet data gateway, you become the owner of the connection (data source). Multiple owners are allowed.

The three connection roles are:

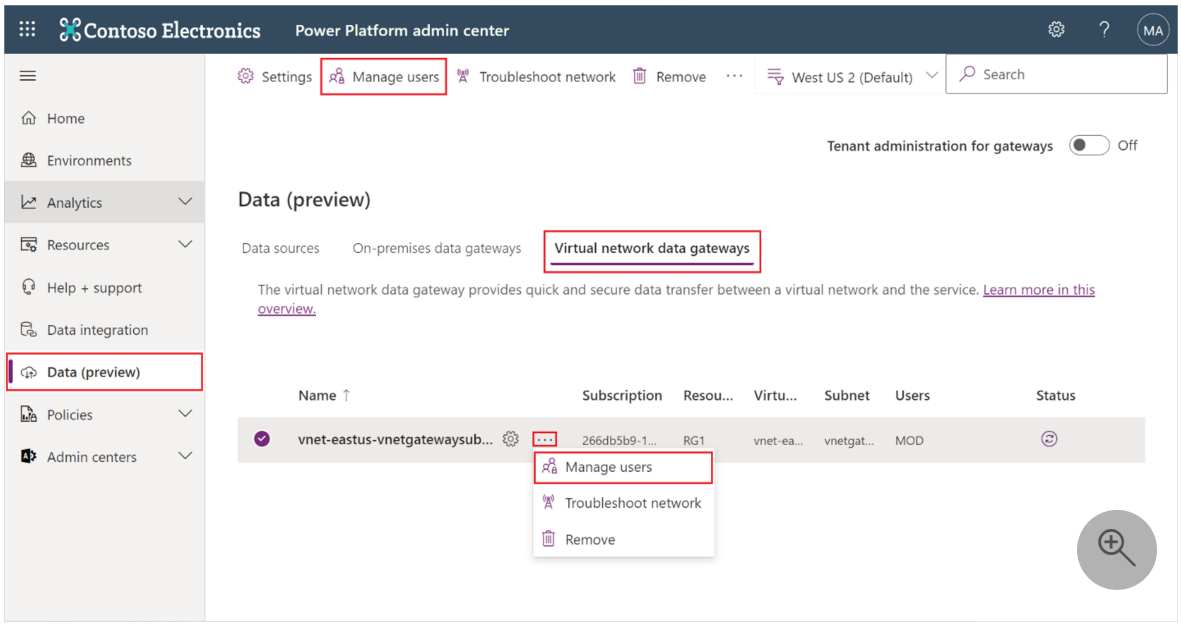
- **Owner**: The owner of the connection (data source) is allowed to update credentials. An owner can also delete the connection. An owner can assign others to the connection with Owner, User, or User with sharing permissions.
- **User**: A user is allowed to use the connection (data source) in Power BI reports, or in Power Apps. A user isn't allowed to view or update credentials.
- **User with sharing**: A user with sharing is allowed to use the connection (data source) in Power BI reports and Power BI dataflows, or in Power Apps. A user with sharing is allowed to share the data source with others with User permission.

These roles are identical to the on-premises data gateway.

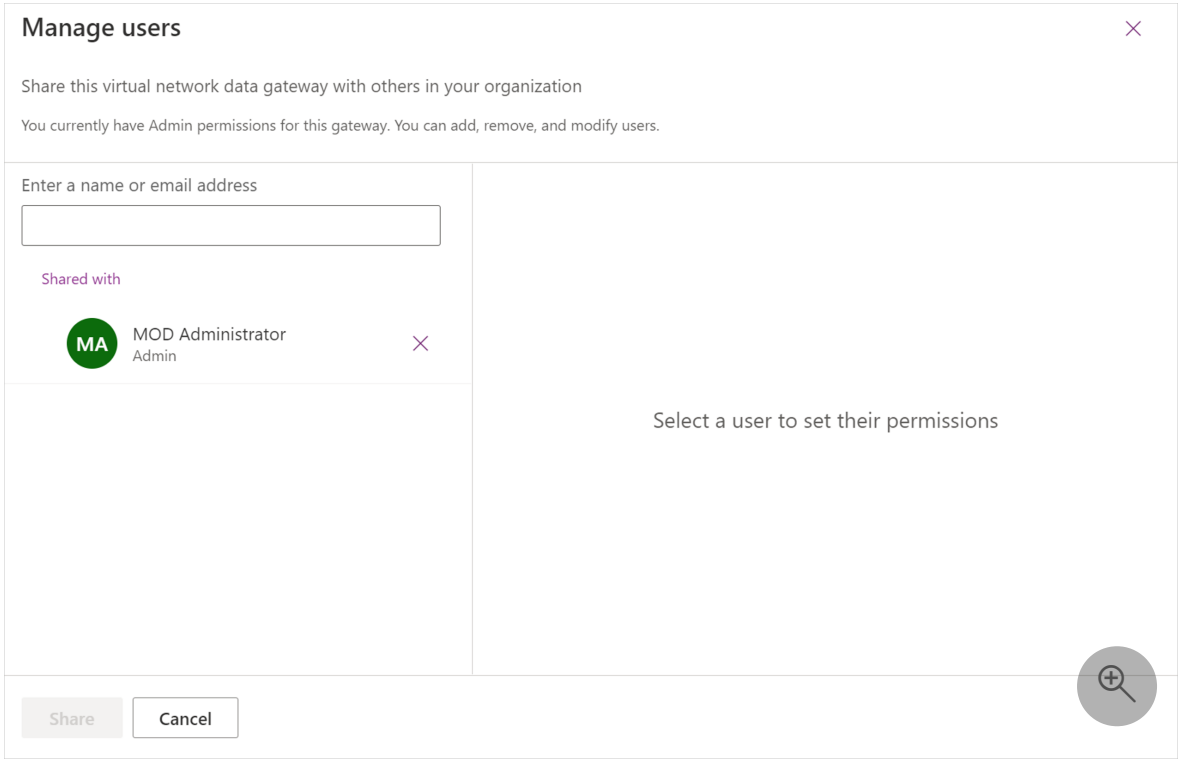
How to manage the gateway and connection (data source) roles

To manage VNet data gateways:

1. Navigate to the Power Platform admin center.
2. Select the **Virtual network data gateways** tab.
3. Select a gateway cluster.
4. In the top ribbon or from the three dot drop-down menu, select **Manage users**.



5. Depending on your role, you can now assign users to the gateway.



To manage data sources, follow the guidance in how to manage on-premises data gateway data sources.

Troubleshoot a virtual network data gateway network

Article • 12/02/2022

You can troubleshoot your virtual network data gateway network if you're experiencing network connectivity issues between the gateway and the data sources it needs to connect to.

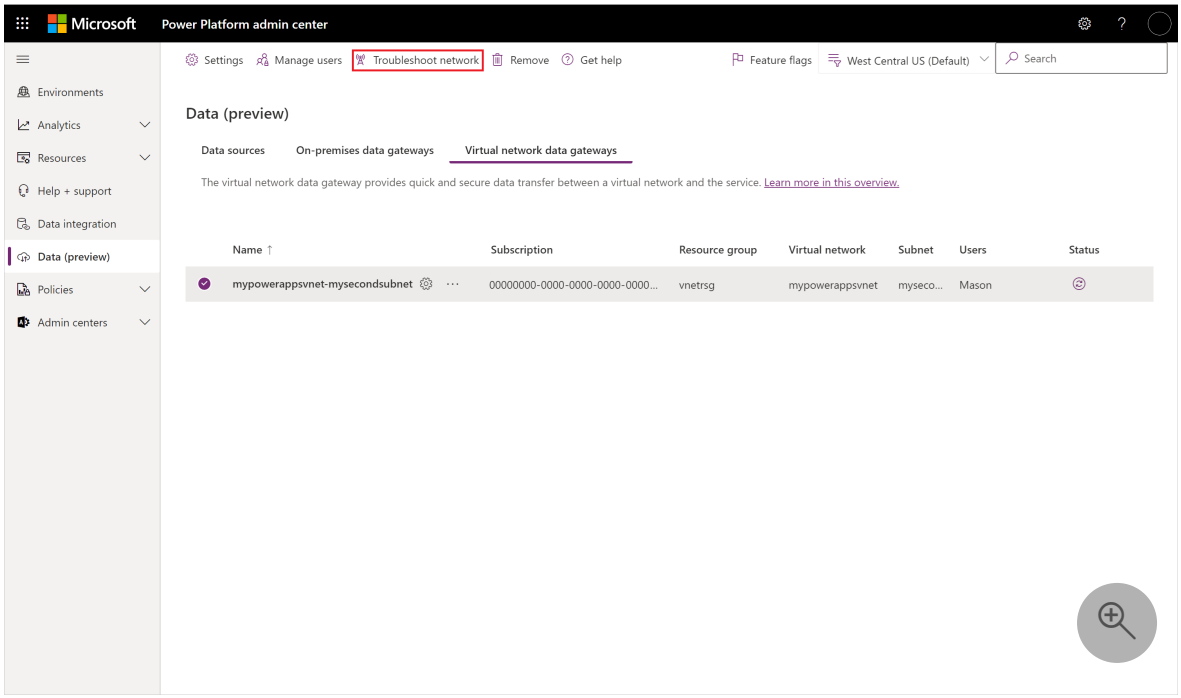
What is virtual network data gateway network troubleshooting?

The troubleshooting information includes the following data:

- **Ethernet adaptor information**: Provides information about the network settings of the gateway. You can use this information to check if the Internet Protocol (IP) is expected in the correct subnet. You can also check if the Domain Name System (DNS) setting is correct.
- **Name resolution and test network connection**: Provides the capability to troubleshoot connectivity between the container and the endpoint using either the IP or domain name and port. If this test fails, it's likely that the container doesn't respond well. This issue can occur when the DNS doesn't respond with an address or when the network is unavailable. If the network test fails, there's likely an issue with the assignment of the IP configuration of the data source.

How to troubleshoot the network of the gateway

1. Navigate to Power Platform admin center.
2. Select **Virtual network data gateways**.
3. Select the gateway you want to troubleshoot and then select **Troubleshoot network** in the ribbon at the top of the page.



The gateway needs to be active. If the gateway is auto paused, it will be started, and it can take up to 2 minutes for the gateway to become active.

Troubleshoot network

Debug any network issues between the container and its data source. Learn more.

Status Testing network connection...

ⓘ Your virtual network data gateway can take up to 2 minutes to start after auto-pausing.

Ethernet adapter information

Loading

Test connectivity to data source

IP or FQDN *

Port *

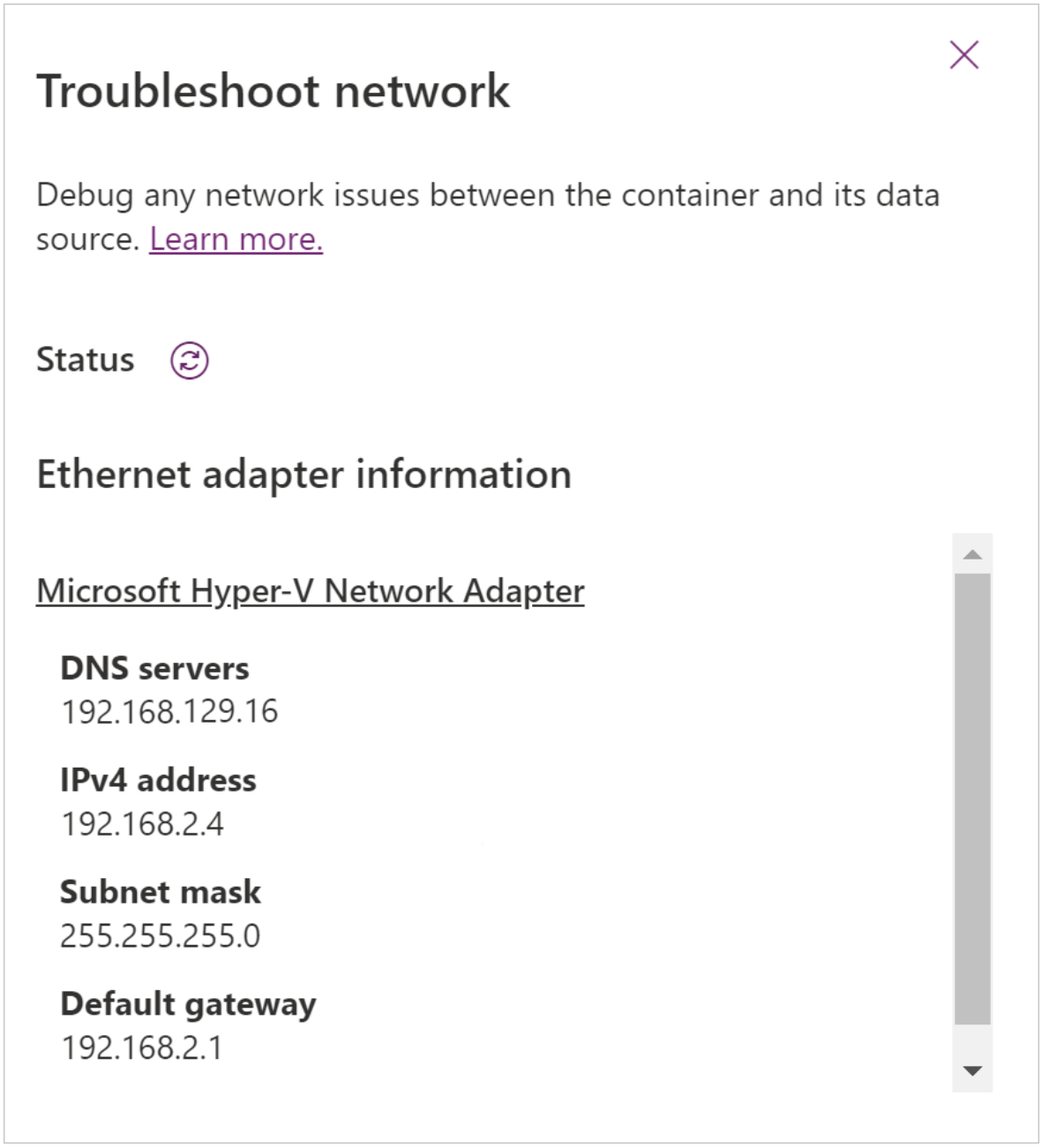
Please enter a whole number e.g. 8080

Troubleshoot | Cancel

Note

The troubleshooting panel automatically triggers a status check. If the status fails, then the troubleshooting button is disabled because the gateway isn't connected. Refreshing the status will clear the troubleshooting result state.

4. If the status check succeeded, you can view your ethernet adapter information, including the DNS servers, IPv4 address, subnet mask, and the default gateway.



5. To test the IP configuration, fill in the IP or Fully Qualified Domain Name (FQDN) and the port number, and then select the troubleshoot button. The input of the port must be a whole number—decimals and strings aren't allowed.

Name resolution (NSLookup)

DNS servers
dr5.westus.database.contoso.net

Addresses
192.168.225.32

Aliases
None

Test network connection

Name of computer contacted
dr5.westus.database.contoso.net

Network alias interface
Ethernet

Remote address
192.168.225.32

Ping source address
192.168.2.4

> ⓘ Note
>
> If you get an `Unable to retrieve <IPConfig/TestNetConnectinon/Host Network> information.` message, retry troubleshooting and ensure you've set the right IP/FQDN and port number.

Virtual network (VNet) data gateway FAQs

FAQ

This article contains a list of frequent asked questions (FAQs) about the virtual network (VNet) data gateways.

How can I secure connectivity from my network to Power BI?

Use Private links to secure this connectivity. More information: Power BI Private Links documentation

Where is my VNet data gateway?

The VNet data gateway is physically in the same region as your Azure VNet. However, the metadata (name, details, data sources, encrypted credentials, and so on) for all your VNet data gateways are stored in your tenant's default region. You can manage all VNet data gateways when you select your tenant's home region in Power platform admin center.

What data sources are supported on the VNet data gateway?

A complete list of supported data services:

- for Power BI is available in Supported Azure data services
- for Power Platform dataflows is available in Supported data sources

What are the licensing requirements in Power BI to use VNet data gateways?

Virtual network data gateways are a premium-only feature, and will be available only in Power BI Premium workspaces and Premium Per User (PPU) for public preview. Licensing requirements might change when VNet data gateways become generally available.

Some of my data sources are connected to my VNet using service endpoint and some using private endpoint. Can I connect to all of them using VNet data gateways?

Yes

Why am I not able to create a service endpoint for my data source in my VNet?

Review Azure VNet documentation for restrictions (for example, region related) on VNets, endpoints, and associated Azure resources.

How do I create a private endpoint for my data sources and associate it to a VNet?

Review the corresponding Azure data service product documentation to check if private endpoints are supported and on how to enable them.

Can I use this feature if my data source is in East US and my Power BI home region is in East US2?

Yes, there's no dependency on the Power BI home region for this feature. If this feature is enabled in the region where the VNet exists, you'll be able to create a new VNet data gateway.

Can I choose the region where VNet data gateways are created?

No. The VNet data gateway is physically in the same region as your Azure VNet. Currently, you also can't choose where the metadata (name, details, data sources, encrypted credentials, and so on) for all your VNet data gateways are stored. It's stored in your tenant's default region.

Does VNet data gateway support cross-tenant scenarios?

No. The VNet data gateway must be created in the same tenant as the Power BI tenant.

Will I be able to use this feature if my tenant is in East US (United States) and Power platform environment is in Europe?

No, VNet gateways are currently available only in your tenant's home region.

Why can't I connect to the data source?

Few areas to check:

- Make sure your data source is up and running.
- Make sure that the data source can be accessed from within the VNet—specifically from the subnet delegated while creating the VNet data gateway. For instance, you could deploy a VM in the subnet and check if you can connect to the data source.
- The following Azure Network Security Groups (NSGs) may be required depending on your scenario:
  - Allow outbound traffic to the Azure Active Directory (Azure AD) endpoint while using OAuth authentication to connect to a data source.
  - Allow outbound traffic to CA (Certificate Authority) while using HTTPS to connect to a data source.

How is the connectivity between the VNet service and your VNet secured?

The connectivity between the new VNet service and your VNet is via HTTPS and TLS 1.2.

Are there any known connectivity issues for SQL serverless with auto-pause?

For SQL serverless with auto-pause, the first request might fail if SQL is in a paused state, but the next ones will succeed.

Is there a delay when the VNet gateway is used for the first time or after a period of inactivity?

When used for the first time, the VNet gateway takes about 2 minutes to get set up. Similarly, if the VNet data gateway isn't used for 30 minutes, you could experience a delay of about a minute the next time you use it.

Is this feature supported in sovereign clouds?

No, only commercial clouds will be supported for the public preview release.

What is the hardware configuration for a VNet data gateway?

Every VNet data gateway has a maximum capacity of:

- 2 cores
- 8 GB of RAM each

At this time, this is the only available hardware configuration and it can't be scaled or changed.

Can I create multiple VNet data gateways for the same Azure data service?

Yes

Why can't I delete the subnet or the VNet that delegated to Power Platform?

Check if there are other gateways using the same VNet and subnet. To be able to delete, it would take up to 48 to 72 hours after the last gateway using this VNet and subnet was removed.

How large does the delegated subnet need to be?

Beyond the five reserved IPs, our recommendation is to have approximately 5-7 more IPs so you can add more VNet gateways to the same VNet and Subnet.

I'm a subscription owner but get an error when I try to create a subscription

Make sure you're explicitly in a role with the Microsoft.Network/virtualNetworks/subnets/join/action permission on the VNet like the Azure Network Contributor role. This permission is required for creating a VNet data gateway.

Does all of the data when using the VNet data gateway remain on Microsoft's backbone network when accessing Azure Data Sources?

How does security compare to the on-premise data gateway? Yes, all the data going through a virtual network data gateway remains on the Azure backbone. We use an internal Microsoft tunnel that doesn't reach the public internet between the virtual network and Power BI service. On the other hand, the on-premise data gateway opens a connection to use Azure Relay to connect to the Power BI service.

Which Azure components need to be in the same region?

Considering the various resources: subscription, Microsoft.PowerPlatform resource provider, virtual network, subnet, and Power BI Service's home tenant. If you're using a service endpoint, the virtual network and subnet should be in the same region as the data to which you're connecting. If you're using a private endpoint, they can be in different regions. The data gateway configuration lives in the Power BI home tenant region.

Is there any way to connect from the subnet of one VNet to the data source of another VNet?

A VNet gateway can generally reach sources that are reachable within that same VNet. If there's another VNet that's completely isolated from the first, then another VNet gateway is necessary.

Any other known issues?

- The VNet's subnet's IP range can't overlap with 10.0.1.x.
- You can't delegate a subnet called `gatewaysubnet` to the Power Platform admin center. This restriction is because it's a reserved word for the Azure Gateway Subnet feature.
- You can't change the region, subscription, or resource group for the VNet on which the VNet data gateway was created. This scenario isn't currently supported.
- If an OAuth refresh that takes longer that one hour is canceled with the error "Invalid Connection Credentials" or timeout, the issue is likely that the credential expired.
- VNet data gateways don't support conditional access policies. When conditional access policies are enabled, Power BI shows a

"DM_GWPipeline_Client_OAuthTokenLoginFailedError" error when you try to update credentials using the OAuth authentication type.