

# Data Gateway Architecture and Build Documentation

---

## Table of Contents

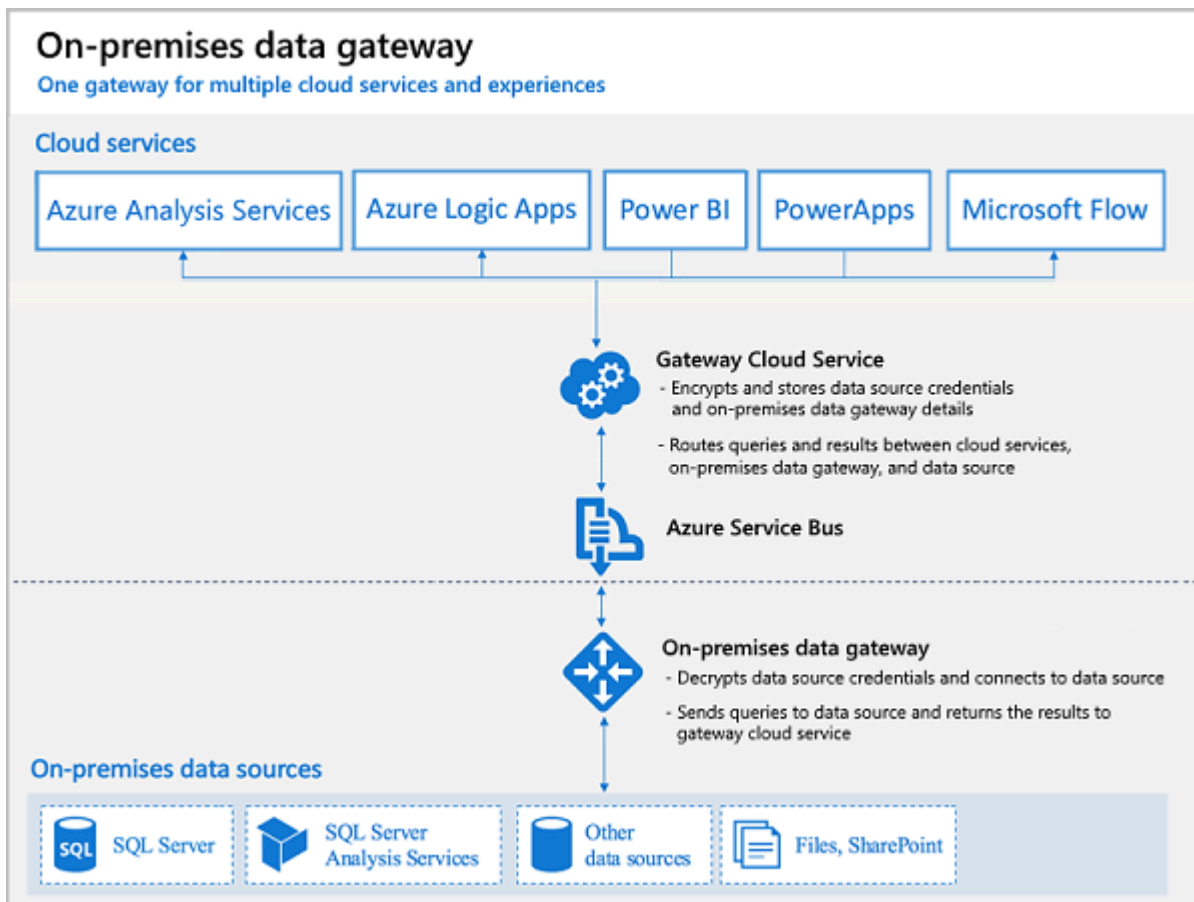
---

- [Infrastructure Requirements](#)
- [Network Architecture](#)
- [Security Configuration](#)
- [High Availability Design](#)
- [Performance Optimization](#)
- [Monitoring and Maintenance](#)

## Infrastructure Requirements

---

The on-premises gateway allows Power Apps and Power Automate to reach back to on-premises resources to support hybrid integration scenarios. The gateway enables Azure Service Bus relay technology to securely allow access to on-premises resources.



## Considerations

- Workloads may have specific requirements around compatible gateway versions. For dataflows, see [using dataflows with on-premises data](#).
- 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 Microsoft Entra environment as the data sources.
- If you use a virtualization layer for your virtual machine, performance might suffer or perform inconsistently.
- When using an on-premises data gateway (standard mode) to access a data source on a remote domain, the gateway has to be installed on a domain joined machine having a trust relationship with the target domain.

## Server Specifications

**Non Production Server Requirements (1 per non production network zone)**

- **Operating System:** Windows Server 2022 Standard/Datacenter
- **Processor:** 8 CPU cores (3.0 GHz or higher)
- **Memory:** 16 GB RAM
- **Storage:** 100 GB SSD (Premium Storage recommended)
- **Network:** 1 Gbps NIC (optional - non production network bandwidth sufficient)

### Production Recommended Requirements ( Min 2 servers for redundancy)

- **Operating System:** Windows Server 2022 Datacenter
- **Processor:** 16 CPU cores (3.5 GHz or higher)
- **Memory:** 32 GB RAM
- **Storage:** 256 GB SSD (Premium Storage required)
- **Network:** 10 Gbps NIC (optional - production network bandwidth sufficient)

## Software Prerequisites

- .NET Framework 4.8 or higher
- PowerShell 5.1 or higher
- TLS 1.2 or higher enabled
- Latest Windows Updates installed

## Network Architecture

---

### DMZ Configuration

```
[Internet] <-> [Azure Load Balancer] <-> [DMZ Gateway Servers] <-> [Internal Firewall] <-> [Backend Services]
```

## Network Segmentation

### 1. External DMZ Segment

- Gateway servers
- Reverse proxy servers
- Load balancers

## 2. Internal Services Segment

- SQL Server instances
- Application servers
- Domain controllers

## 3. Management Segment

- Monitoring tools
- Administrative access
- Backup systems

# Port usage & Firewall Rules

The gateway service creates an outbound connection to Azure Service Bus so there are no inbound ports required to be open. The outbound connection communicates on ports: TCP 443 (default), 5671, 5672 9350 through 9354

## Outbound Rules

- TCP 443 to Azure services
- SQL ports to backend databases
- DNS and NTP to internal services

# Security Configuration

---

## Identity and Access

- **Authentication:** Entra ID integration
- **Authorization:** Role-based access control (RBAC)
- **Service Accounts:** Managed Service Identities where possible

## Encryption and Certificates

- **Transport:** TLS 1.2+ required
- **Certificates:** Auto-renewed SSL certificates
- **Key Management:** Azure Key Vault integration

# Network Security

- IP restriction lists
- Network Security Groups (NSGs)
- Web Application Firewall (WAF)
- DDoS protection

## High Availability Design

---

### Gateway Clustering

- Minimum 2 gateway servers per environment
- Active-Active configuration
- Load-balanced endpoints

### Failover Configuration

```
{
  "cluster": {
    "primaryNode": "gateway-prod-01",
    "secondaryNodes": [
      "gateway-prod-02",
      "gateway-prod-03"
    ],
    "heartbeatInterval": "30s",
    "failoverThreshold": "90s"
  }
}
```

## Performance Optimization

---

### Connection Pooling

```
{
  "poolConfig": {
    "maxPoolSize": 100,
```

```
"minPoolSize": 10,  
"connectionTimeout": "30s",  
"idleTimeout": "300s"  
}  
}
```

## Caching Strategy

- Implement Redis Cache for frequently accessed data
- Cache invalidation policies
- Cache-Control headers configuration

## Monitoring and Maintenance

---

### Health Checks

- Gateway service status
- Connection metrics
- Performance counters
- Error logs

## Alerting Configuration

```
{  
  "alerts": {  
    "cpuThreshold": 80,  
    "memoryThreshold": 85,  
    "responseTimeThreshold": "5s",  
    "errorRateThreshold": 5  
  }  
}
```

## Backup and Recovery

- Regular configuration backups
- Gateway recovery procedures

- Disaster recovery planning

A recovery key is assigned (that is, not autogenerated) by the administrator at the time the on-premises data gateway is installed. The recovery key is required if the gateway is to be relocated to another machine, or if the gateway is to be restored. Therefore, the key should be retained where other system administrators can locate it if necessary.

# Deployment Checklist

---

## Pre-Installation

- ☐ Verify server specifications
- ☐ Configure network segments
- ☐ Set up firewall rules
- ☐ Install prerequisites

## Installation

- ☐ Deploy gateway servers
- ☐ Configure clustering
- ☐ Set up monitoring
- ☐ Test connectivity

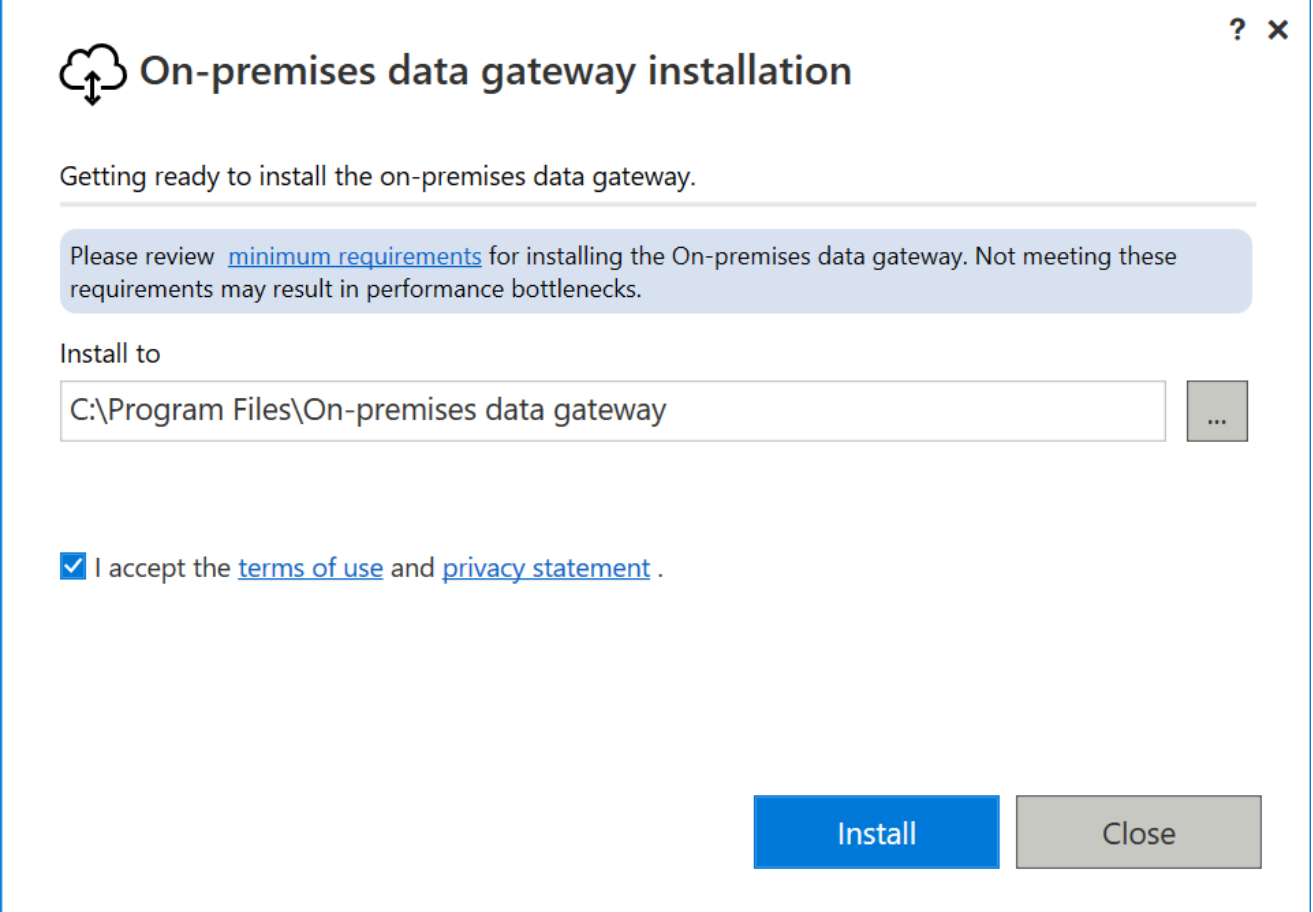
## Post-Installation

- ☐ Verify security settings
- ☐ Test failover
- ☐ Document configuration
- ☐ Train support staff

## Download and install the Standard Gateway

1. [Download file](#)

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



The screenshot shows the 'On-premises data gateway installation' window. It has a title bar with a question mark and a close button. The main heading is 'On-premises data gateway installation' with a cloud and arrow icon. Below the heading, it says 'Getting ready to install the on-premises data gateway.' There is a light blue informational box with text about reviewing minimum requirements. Below that, the 'Install to' section shows a text box with the default path 'C:\Program Files\On-premises data gateway' and a browse button. A checkbox is checked, indicating acceptance of the terms of use and privacy statement. At the bottom right are 'Install' and 'Close' buttons.

On-premises data gateway installation

Getting ready to install the on-premises data gateway.

Please review [minimum requirements](#) for installing the On-premises data gateway. Not meeting these requirements may result in performance bottlenecks.

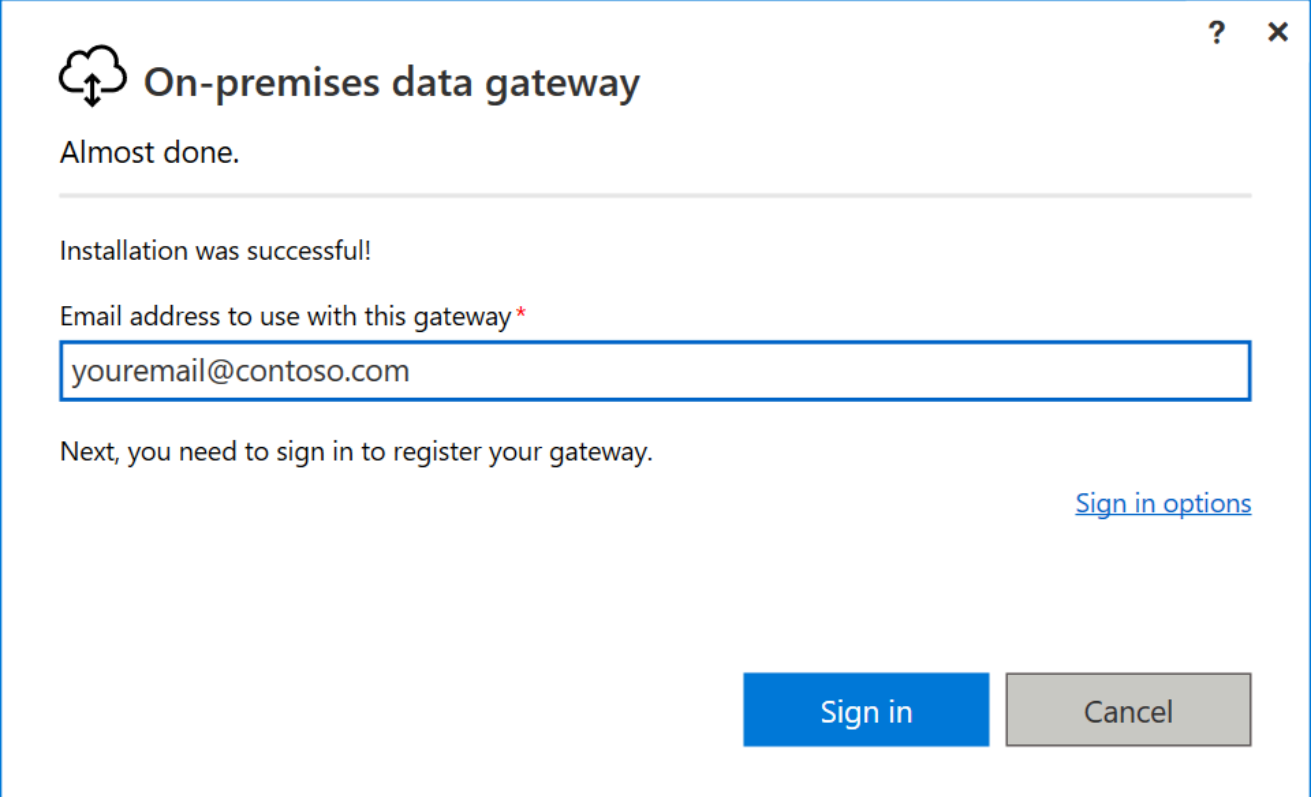
Install to

C:\Program Files\On-premises data gateway

☒ I accept the [terms of use](#) and [privacy statement](#) .

Install Close

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



The screenshot shows the 'On-premises data gateway' sign-in window. It has a title bar with a question mark and a close button. The main heading is 'On-premises data gateway' with a cloud and arrow icon. Below the heading, it says 'Almost done.' and 'Installation was successful!'. There is a text box for the email address, with the placeholder 'youremail@contoso.com'. Below the text box, it says 'Next, you need to sign in to register your gateway.' and a link for 'Sign in options'. At the bottom right are 'Sign in' and 'Cancel' buttons.

On-premises data gateway

Almost done.

Installation was successful!

Email address to use with this gateway \*

youremail@contoso.com

Next, you need to sign in to register your gateway.

[Sign in options](#)

Sign in Cancel

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





## On-premises data gateway



You are signed in as youremail@contoso.com and are ready to register the gateway.

---

- ☒ Register a new gateway on this computer.
- ☐ Migrate, restore, or takeover an existing gateway.
- Move a gateway to a new computer
  - Recover a damaged gateway
  - Take ownership of a gateway
- The old gateway will be disconnected.

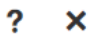
Next

Cancel

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** .



## On-premises data gateway



You are signed in as youremail@contoso.com and are ready to register the gateway.

New on-premises data gateway name \*

☐ Add to an existing gateway cluster [Learn more](#)

Recovery key (8 character minimum) \*

This key is needed to restore the gateway and can't be changed. Record it in a safe place.

Confirm recovery key \*

We'll use this region to connect the gateway to cloud services: West Central US [Change Region](#)

[Provide relay details \(optional\)](#) By default, Azure Relays are automatically provisioned

< < Back

Configure

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**.



## On-premises data gateway



### Status

Service Settings

Diagnostics

Network

Connectors

Recovery Keys

✓ The gateway datagateway is online and ready to be used.

Gateway version number: 3000.142.14 (September 2022)

✓ Help us improve the on-premises data gateway by sending usage information to Microsoft.

[Read the privacy statement online](#)

#### Logic Apps, Azure Analysis Services

West Central US

[Create a gateway in Azure](#)

#### Power Apps, Power Automate

West Central US

✓ Ready

#### Power BI

Default environment

✓ Ready

Close